وزارة التعليـــم العالـــي والبحـــث العلمـــي
جامـــعـــة يحـــي فـــارس بالمـــديـــة
كلية الحقوق والعلوم السياسية

إجراءات التحري والتحقيق في جرائم الوسط الرقمي

أطروحة لنيل شهادة دكتوراه "ل م د" في الحقوق
تخصص: القانون العام

الطالـــــــــب:
جحيـــش فـــؤاد

المشـــــــــــرف:
د/ غربـــي أسامـــة

لجنـــــــــــــة المنـــــاقشة

د/ بن تغري موســـى	أستاذ محاضر "أ"	جامعة المدية	رئيساً
د/ غربـــي أسامـــــة	أستاذ محاضر "أ"	جامعة المدية	مشرفاً ومقرراً
د/ فخـــــار هشـــام	أستاذ محاضر "أ"	جامعة المدية	عضواً
د/ جلايلـــة دليلـــة	أستاذ محاضر "أ"	جامعة المدية	عضواً
أ.د/ سي يوسف قاسي	أستـــــــــــاذ	جامعة البويرة	عضواً
د/ ملياني عبد الوهاب	أستاذ محاضر "أ"	جامعة الأغواط	عضواً

تاريخ المناقشة: 26-01-2020

بسم الله
الرحمن
الرحيم

إهـــــــــــداء

الإهداء بدايةً، من باب زرع المحبة وتوطيدها؛ إلى كل الأهل والأحباب والأقارب، سيما العائلة الصغيرة، الوالد رحمه الله، والوالدة أطال الله عمرها، وأخواتي جعلني الله سندا وعونا لهن، ولينٌ عطرٌ وروحٌ للمودة كلها.

والإهداء امتدادا، من باب الواجب العلمي؛ إلى كل من يجدنا قد أوفينا بالتزامنا تجاه ما حفظناه وتعلمناه بعد جهلنا، من خلال النشر بعد الإتقان.

والإهداء ختاما، من باب طلب الثواب الأخروي؛ إلى كل باحث ودارس ومختص، يرى أنه سينتفع علما وعملا من دراستنا هذه، راجين منه الدعاء وطلب المغفرة لنا من الله جل جلاله.

شـــــكـــــر

بسم الله الرحمن الرحيم

الشـــــكر لله أولا؛

"نِعْمَةً مِنْ عِنْدِنَا كَذَلِكَ نَجْزِي مَنْ شَكَرَ"؛ الآية 25–سورة القمر.

فالشكر؛ لله سبحانه وتعالى، عرفانا بالعطاء العلمي الذي لا يمنح إلا بإذنه وتدبيره. واعترافا؛ بقلة حيلتنا وقصورنا، فالكمال لله وحده جل جلاله.

الشكر لعباد الله ثانيا؛

"لا يشكر الله من لم يشكر الناس"؛ حديث نبوي شريف.

فالشكر؛ لأولي الألباب بدايةً، سيما الأستاذ المشرف "الدكتور المحترم أسامة غربي"، على كل ما قدمه لنا؛ من دعم وتشجيع وحث على المثابرة والنجاح. وكذا الشكر للجنة المناقشة بتركيبتها الموقرة، التي تكرمت علينا بالتصويب العلمي السديد.

والشكر كذلك؛ لكل من ساعدنا في انجاز بحثنا هذا، خاصةً الطاقم العلمي والإداري لكلية الحقوق بالمدية، والمؤسسات العمومية العلمية وكذا المختصة في الوقاية من جرائم الوسط الرقمي ومكافحتها.

والشكر عموما؛ لكل من ساهم وفق ما استطاع ماديا ومعنويا، وبتوفيق من الله سبحانه وتعالى؛ في انجاز هذا العمل العلمي.

قائمـــة أهـــــــم المختـــصرات

المختصرات باللغة العربية:

الاختصـــــــار	المـــــدلـــــــــــول
المشرع	المشرع الجزائري
القانون	القانون الجزائري
ق ع	قانون العقوبات الجزائري
ق إ ج	قانون الإجراءات الجزائية الجزائري
جرائم المساس	جرائم المساس بأنظمة المعالجة الآلية للمعطيات
ج ر	الجريدة الرسمية للجمهورية الجزائرية
ق ج أ م أ	قانون جرائم أنظمة المعلومات الأردني
الجهاز	جهاز الإعلام الآلي
الشبكة	شبكة الاتصال الدولية
البيانات	البيانات الرقمية
المعلومات	المعلومات الرقمية
المعطيات	المعطيات الرقمية
د ج	دينار جزائري
د أ	دينار أردني
و م أ	الولايات المتحدة الأمريكية
مج	مجلد
د س ن	دون ذكر سنة نشر
الاختصـــــــار	**المـــــدلـــــــــــول**

د ت	دون ذكر التاريخ
د ت ن	دون ذكر تاريخ نشر

المختصرات باللغة الأجنبية (فرنسية وانجليزية):

Abréviation	Signification
ART	Article
O I P C	Organisation internationale de police criminelle
J O U E	Journal officiel de l'Union européenne
U E	L'Union européenne
STAD	Système de traitement automatisé de données.
PUF	Presses universitaires de France
S D	Sans Date
S D P	Sans Date de Publication
TIC	Technologies de l'information et de la communication
ITCIS	International Trade Customs and Invest services
U D	Undated
N P D	No Publication Date

مقـــــــــدمـــــــــــــة

ارتكزت البشرية منذ القدم على متلازمين أساسيين؛ مفادهما التجريم والجزاء الجنائي. فظهرت مقاربة بين الاثنين، بحيث تراوح مصدر التجريم؛ بين القواعد الأخلاقية والشرعية والوضعية، وانحصرت طبيعة نظيره الجزاء في حدود الانتقام الهمجي والقمع القانوني. ولم يبدأ الاثنين –التجريم والجزاء– في اكتساء الطابع القانوني الدقيق والمنظم؛ إلا مع بداية ظهور علماء عصر التنوير في أوروبا، المتزامن وأواخر القرن الثامن عشر، سيما ما جاء به الفقيه "مونتسكيو" من أعمال، على غرار كتابه المعنون بـــ "روح القوانين"، وكذلك الفقيه "بيكاريا" الذي أصدر كتاباً بعنوان "الجرائم والعقوبات"[1]، دون أن ننسى الثورة الفرنسية وما انبثق عنها[2].

وانطلاقا من أهم نتائج عصر التنوير في أوربا عموماً والثورة الفرنسية خاصةً؛ بدأ ما يسمى بمبدأ الشرعية الجنائية في التشكل والبروز تدريجيا. ومع الوقت استقر الفقه الجنائي الحديث ومعه التشريعات المقارنة –والمشرع الجزائري–، على المضمون والمدلول الأساسيين لهذا المبدأ القانوني الحديث الحامل للبعد الجزائي والإنساني في الوقت نفسه. وذلك من خلال القول والتأكيد على أنه لا جريمة ولا جزاء جنائي بغير نص صريح صادر عن السلطة التشريعية المختصة، قبل ارتكاب السلوك من طرف الشخص محل التابعة الجزائية[3].

ومع بروز مبدأ الشرعية الجنائية واستقراره من حيث المضمون والمدلول؛ أخذ التجريم والعقاب في التطور الروتيني على حسب تطور السلوكيات والمصالح المراد حمايتها في المجتمع. إلا أن هذا الأخير –التطور المستمر في تحديد السلوكيات واجبة التجريم–؛ ظل محصورا في الوسط المادي الملموس، الذي ترتكب الجريمة في إطاره ووفق خصوصياته، حيث تمس دائما بالحيز المادي الملموس الذي يعيش فيه الجاني. وفي أغلب الأحيان تنطوي السلوكيات المرتكبة؛ على حركة الجاني الاختيارية التي تغير من المظهر الخارجي الملموس[4].

---

[1] **أنظر:** أحسن بوسقيعة، الوجيز في القانون الجزائي العام، الطبعة الثانية، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2013، ص66.

[2] التي من أهم نتائجها؛ إعلان حقوق الإنسان والمواطن لسنة 1773، الذي نص صراحة على مبدأ الشرعية الجنائية بموجب المادة الرابعة "04" منه. **أنظر في ذلك:** عبد الله أوهايبية، شرح قانون العقوبات الجزائري، المؤسسة الوطنية للفنون المطبعية، الجزائر، 2011، ص 89.

[3] كما يرى الفقه الجنائي الإسلامي؛ أن نظام التجريم والعقاب وفق مبدأ الشرعية الجنائية وجد مع وجود الشريعة الإسلامية، مؤسسين اتجاههم على العديد من الآيات القرآنية والأحاديث النبوية الشريفة، لعل أهمها **الآية 15 من سورة الإسراء** التي جاء فيها: **"... وَمَا كُنَّامُعَذِّبِينَ حَتَّىٰ نَبْعَثَ رَسُولًا". أنظر في ذلك:** المرجع والصفحة نفسهما.

- إلا أن ظهور مبدأ الشرعية الجنائية قد يرجع إلى مرحلة ما قبل وجود الإنسان على الأرض، سيما لو توقفنا عند مدلول ما جاء في **الآية القرآنية رقم 35 من سورة البقرة**، التي يقول فيها جل جلاله: **"وَقُلْنَا يَا آدَمُ اسْكُنْ أَنْتَ وَزَوْجُكَ الْجَنَّةَ وَكُلَا مِنْهَا رَغَدًا حَيْثُ شِئْتُمَا وَلَا تَقْرَبَا هَٰذِهِ الشَّجَرَةَ فَتَكُونَا مِنَ الظَّالِمِينَ"**. الأمر الذي قد يدل على أن التجريم والعقاب؛ هو قاعدة ربانية قبل أن يصبح حكما وضعيا بشريا.

[4] مع القول بوجود بعض الجرائم التي لاتكتسي نتائجها الطابع الملموس، كجرائم الشرف والاعتبار وجرائم الخطر.

وانطلاقا مما توصل إليه الفقه والتشريع الجنائيين، من قواعد موضوعية متصلة بالتجريم والجزاء؛ وجب البحث في آليات إجرائية تكون المحرك الأساس لعمل هذه القواعد الموضوعية، على أن تكون بطابع مادي يتناسب مع مادية الجريمة التقليدية. الأمر الذي أدى إلى وضع قواعد تمكن من التحري والتحقيق وبالنتيجة محاكمة ومعاقبة المدان بالجريمة أو تبرئة البريء بشأنها. حيث قسمت أغلب التشريعات الجنائية –خاصةً الفرنكوجرمانية– هذه الإجراءات إلى أربعة مراحل؛ البحث والتحري أولا والتحقيق القضائي الابتدائي ثانيا والمحاكمة –التحقيق القضائي النهائي– ثالثا والتنفيذ الجزائي رابعا[1].

كما يرى الدكتور "ناصر حمودي" في الإطار ذاته؛ أن دور قانون الإجراءات الجزائية يبدأ حيث ينتهي دور قانون العقوبات[2]. وبالتالي هي عملية مترابطة لا يمكن فصلها، ولا يمكن لقواعد إجرائية من طبيعة ما أن تُفَعل قواعد موضوعية من طبيعة أخرى. الأمر الذي أدى بالمشرع في العديد من المرات؛ إلى تعديل قانون الإجراءات الجزائية بصورة متزامنة مع تعديل قانون العقوبات[3].

وبالتالي لايمكن تصور؛ الاكتفاء –أساسا– بتشريع قواعد موضوعية تجرم وتعاقب من دون قواعد أخرى إجرائية تفعلها، وتضع الشخص المعني –مشتبه فيه ومتهم–؛ موضع الاختبار الجزائي، للفصل في قيام مسؤوليته الجزائية حول السلوك سبب المتابعة من عدمها. كما لا يمكن بالتبعية؛ العمل بقواعد إجرائية تجاوزها الزمن، بخصوص مواجهة جرائم مستحدثة تختلف من حيث الطبيعة عن التقليدية المعروفة.

كل ما ذكر سابقا وأعلاه؛ يقودنا للتطرق إلى ما أحدثته الثورة الصناعية الثانية –أو كما تسمى بالثورة التكنولوجية، أو المرحلة الثانية من الثورة الصناعية الكبرى–؛ في مجال التجريم والجزاء عموماً. حيث نتجت عنها مجموعة من الوسائل التي نسميها بعناصر الوسط الرقمي، المتمثلة أساسا في جهاز الإعلام الآلي وشبكة الاتصال الدولية –ومن في حكمهما–. وهي العاملة كأصل عام بالنظام الرقمي الثنائي –نظام "الـــ 0 والـــ 1"–. فبفضل هذه العناصر يلج المتعامل معها من الوسط المادي الملموس التقليدي، إلى الوسط الرقمي المعنوي الافتراضي الحديث، ما يقود إلى القيام بمجموعة سلوكيات في إطاره وبواسطته.

---

[1] الأمر الذي اعتمده المشرع الجزائري صراحةً؛ بأحكام قانون الإجراءات الجزائية. حيث نظم بالمواد من 11 إلى 65 مكرر 18؛ مرحلة البحث والتحري. وبالمواد من 66 إلى 211؛ مرحلة التحقيق القضائي الابتدائي. وبالمواد من 212 إلى 591؛ مرحلة المحاكمة -التحقيق القضائي النهائي-. وأخيرا بالمواد من 592 إلى 693؛ مرحلة التنفيذ الجزائي. **أنظر في ذلك:** أمر رقم 66-155، مؤرخ في 08 جوان 1966، يتضمن قانون الإجراءات الجزائية، (ج ر) عدد 49، صادر بتاريخ 11جوان 1966، معدل ومتمم.

[2] **أنظر:** ناصر حمودي، (قضاء التحقيق في قانون الإجراءات الجزائية الجزائري-دراسة تحليلية نقدية)، مطبوعة مقدمة لطلبة الماستر، كلية الحقوق والعلوم السياسية، جامعة العقيد آكلي محند أولحاج، البويرة، الجزائر، 2012، ص 03.

[3] وهو ما عمل به المشرع الجزائري في العديد من المرات، لاسيما بخصوص المسؤولية الجنائية للشخص المعنوي، حيث أقرها صراحة بموجب القانون رقم 04-15 المعدل والمتمم لقانون العقوبات، وفي الوقت نفسه أقر إجراءات المتابعة الجزائية للشخص المعنوي بموجب القانون 04-14 المعدل والمتمم لقانون الإجراءات الجزائية. ولو أنه كان من الأجدر عليه -المشرع- أن يسبق في تعديل قانون العقوبات على حساب قانون الإجراءات الجزائية، وهذا إعمالا للمنطق الجنائي السليم، الذي يفرض التجريم قبل المتابعة. إلا أنه ليس بالجديد عن المشرع الجزائري الذي عمل سنة 1966؛ إلى تسبيق قانون الإجراءات الجزائية على قانون العقوبات من حيث الترقيم. فجاء الأول تحت رقم 66-155 والثاني تحت رقم 66-156.

وبعد أن ولج الفرد إلى الوسط الرقمي الافتراضي، وبدأ في التعامل معه وفق إطاره العلمي الحديث؛ أخذت العديد من المفاهيم الحديثة في الظهور والتشكل. على غرار بروز التباين الكبير في الطبيعة –من تكوين وأثر– بين الوسط الرقمي الحديث من جهة، ونظيره التقليدي –الوسط المادي الملموس– المعروف من جهة أخرى. الأمر الذي نتجت عنه العديد من الأضرار التي تعد بالغة الأثر السلبي، اللاحق بالمصالح العامة والخاصة.

فدفعت هذه الأضرار الكبيرة اللاحقة بالمصالح العامة والخاصة، التي تعد في الوقت نفسه إنذارا بالخطر غير المسبوق من حيث المواجهة؛ إلى ضرورة وحتمية ولوج التجريم والعقاب إلى هذا الوسط الرقمي، من خلال محاولة حصر أهم السلوكيات الرقمية واجبة التجريم، ومن ثم تجريمها وفق التكييف اللازم، ووضع الجزاء المناسب لمن يرتكبها بعد تجريمها، مع التأكيد على محاولة إرساء نظرية عامة لهذا النوع من الإجرام الحديث.

ولم يكن الولوج الموضوعي للتجريم والعقاب في الوسط الرقمي، بالسهولة التي يتصورها البعض؛ بل مر ذلك –كما سنرى لاحقا– عبر العديد من المراحل، في حدود ثلاث محطات أساسية على الأقل. مع التأكيد على الصعوبة البالغة، التي واجهت عملية تقسيم جرائم الوسط الرقمي إلى أنواع أساسية، تسهل المواجهة الجزائية عموماً. وان يعد التقسيم الأكثر منطقية ومرونة، ذلك الذي يحدد نوعها الأول؛ في تلك الماسة بالوسط الرقمي ذاته، ويجعل نوعها الثاني منصبا على الجريمة التقليدية، التي ترتكب عبر النطاق الافتراضي للوسط الرقمي أو يكون هو المسهل في ارتكابها[1].

بالإضافة إلى الصعوبات الموضوعية المشار إليها أعلاه؛ طفت إلى السطح العديد من العقبات الأخرى، التي تسببت في بروزها الخصوصية المعقدة لعناصر الوسط الرقمي، بعد أن ولج الإجرام إلى نطاقها الافتراضي وتنوعت سلوكياته. ولعل أبرز عقبة في هذا الإطار؛ تنطوي على السهولة الكبيرة في ارتكاب هذا النوع من الإجرام الحديث، مع بروز ظاهرة عدم التبليغ عنها لأسباب عديدة، سنستعرضها في موضعها المحدد.

الصعوبة في المواجهة الموضوعية التي برزت وفق ما بينا أعلاه وسابقا، بعد أن ولج المشرع إلى الوسط الرقمي ليجرم السلوكيات واجبة التجريم فيه، سواءً الحديثة تماما أو التقليدية المرقمنة؛ شكلت ما نسميه بالخصوصية الموضوعية لجرائم الوسط الرقمي عموماً. التي –الخصوصية– تجعلها جرائم قائمة على العديد من الأحكام القانونية، غير المسبوقة في مجال التجريم والعقاب، ومتصلة بوسط افتراضي حديث مختلف تماما عن نظيره التقليدي الملموس.

[1] التقسيم الذي اعتمده المشرع الجزائري صراحةً. **أنظر في ذلك:** المادة 1/02-أ؛ قانون رقم 09-04، مؤرخ في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، (ج ر) عدد 47، صادر بتاريخ 06 أوت 2009.

رجوعاً إلى قاعدة أن العمل بالأحكام الإجرائية؛ يبدأ بعد انتهاء دور القواعد الموضوعية، يمكن القول بمفهوم المخالفة؛ أن الصعوبة ذاتها التي صاحبت عملية التجريم والعقاب في الوسط الرقمي؛ انتقلت حتما إلى المواجهة الإجرائية لهذا النوع من الإجرام الحديث. فإذا انتهى دور قواعد موضوعية تجرم في الوسط المادي؛ يبدأ دور قواعد إجرائية تتحرى وتحقق في الوسط المادي ذاته. وإذا ما انتهى دور القواعد الموضوعية التي تجرم وتعاقب في الوسط الرقمي؛ يجب التحري والتحقيق بشأنها عن طريق إجراءات تتلاءم مع هذا الوسط الافتراضي المعنوي غير الملموس.

ولعل المواجهة الإجرائية لجرائم الوسط الرقمي، تعد أكثر صعوبةً وتشعبا من المواجهة الموضوعية، وذلك رغم اتصالهما بالوسط نفسه. الأمر الذي يعود إلى الصعوبة البالغة التي تواجه الأجهزة المختصة بالتحري والتحقيق، سيما وأنها تتعامل مع وسط افتراضي معقد من جهة، وجناة يحسنون التعامل معه من جهة أخرى. وعلى العموم يمكن القول؛ أنه للوسط الرقمي خصوصية اكتسبتها جرائمه موضوعيا فاتصفت بالتعقيد والحداثة، وتحملتها النصوص إجرائيا، وفق حتمية التناسق والتطابق مع الطبيعة نفسها، من أجل إنفاذ القانون وإعماله.

تأسيسا على ما ذكر؛ يمكن القول أنه لموضوع الدراسة، المنطوي على إجراءات التحري والتحقيق في جرائم الوسط الرقمي؛ الكثير من الأهمية، التي تتكامل في العادة من الناحيتين المنهجية والموضوعية مع أسباب اختيار الموضوع. التكامل الذي يبرز ويتجلى صراحةً؛ بخصوص موضوع الحال، على نحو يبدوا أكثر تناسقا وتناسبا، سيما وأننا نتطرق إلى الجانب قانوني لجرائم حديثة؛ تعد دراستها من الأهمية بمكان، سواءً في شقها الموضوعي أو نظيره الإجرائي.

فبخصوص الأسباب الشخصية في ذات الباحث، التي دفعتنا لدراسة موضوع إجراءات التحري والتحقيق في جرائم الوسط الرقمي؛ نجد أن أهمها تتمثل في كون الإجراءات الجزائية عموماً وجرائم الوسط الرقمي خاصةً؛ يعدان من بين موضوعات الدراسة التي تلقيناها بمناسبة مزاولة طور الماستر، تخصص القانون الجنائي والعلوم الجنائية. الأمر الذي زرع فينا رغبة البحث في موضوع جرائم الوسط الرقمي، محاولة منا للإلمام بأهم الأحكام والقواعد الجزائية الحديثة، ذات الصلة بهذا النوع من الإجرام موضوعيا وإجرائيا.

وزيادةً عما ما ذكر؛ نؤكد على سبق دراستنا لموضوع جرائم الوسط الرقمي من خلال إعداد ومناقشة مذكرة الماستر في القانون الجنائي والعلوم الجنائية، المعنونة بـــ "جرائم الوسط الرقمي؛ تجريم حديث بأبعاد تقليدية –دراسة تحليلية مقارنة–"[1]. الأمر الذي يعطينا نوعا من المعرفة بخبايا هذا النوع من

[1] إلا أننا اقتصرنا في ذلك على دراسة الشق الموضوعي المتصل بالتجريم والعقاب فقط، دون التطرق إلى الشق الإجرائي، إلا عرضا وفق متطلبات الدراسة.

الإجرام الحديث، الذي يزداد حدةً وشراسةً تزامنا مع التطور التكنولوجي في المجال الرقمي، أو كما سميناه بالوسط الرقمي الافتراضي.

كما أننا برغبة باحث يهوى العلوم الجنائية عموما، وخبايا الوسط الرقمي وما أحدثه على العلوم الجنائية من خصوصية خاصةً؛ توصلنا إلى حتمية الانتقال من دراسة الشق الموضوعي لجرائم الوسط الرقمي؛ إلى نظيره المنطوي على الشق الإجرائي، الذي لم نكن لندرسه لولا اقتناعنا وتأكدنا من تبعيته للشق الموضوعي بخصوص الولوج إلى الوسط الرقمي، والعمل بقواعده الحديثة الرقمية والمرقمنة، بدلا عن التقليدية المعلول بها من قبل، سيما من حيث التحري والتحقيق.

وأما بخصوص الأسباب الموضوعية لاختيار موضوع الدراسة؛ فيمكن القول أن جرائم الوسط الرقمي عموما؛ من بين أهم متطلبات الدراسة في العصر الحديث، إن من حيث جدتها وطبيعتها المختلفة أو من حيث سهولة ارتكابها وإخفاء معالمها. الأمر النابع أساسا من حداثة وتعقيد الوسط الرقمي ذاته، وحيازة أغلب سكان العالم للعناصر الخالقة لهذا الوسط غير المألوف.

وتسليما بالقاعدة الإجرائية المذكورة، التي مفادها؛ أن الأحكام الإجرائية يبدأ سريانها بنهاية دور القواعد الموضوعية؛ اعتبرنا أنه من اللازم والواجب البحث في هذه التكملة الإجرائية، المتصلة بجرائم الوسط الرقمي، ونطاقها الافتراضي الحديث. فبعد ولوج التجريم إلى الوسط الرقمي، ليجرم ويعاقب فيه وفق خصوصية حديثة لم يسبق التعامل مع مثلها؛ وجب على نظيرتها الأحكام الإجرائية أن تلج أيضا إلى الوسط نفسه، بقواعد من النظرة والطبيعة نفسها، لا لشيء إلا لتحقيق الغاية الأساسية من القواعد الإجرائية، المنطوية على إحقاق العدالة بإظهار الحقيقة.

كما نرى أيضا أن موضوع جرائم الوسط الرقمي عموماً؛ هو من بين موضوعات الساعة، التي تتسابق الدراسات الفقهية والتشريعات المقارنة؛ لإيجاد الحلول الناجعة لمواجهتها موضوعيا وخاصةً إجرائيا، الوضع الذي جعل منها موضوع بحث بأهمية جد كبيرة. ومنه تبرز أهمية اختيار موضوع البحث، فالوسط الرقمي وسط معقد وسريع التطور، وجناته أذكياء جدا–إن لم نقل نوابغ–، وللمشرع عموما طرقه الإجرائية، التي تعد تقليدية عديمة الجدوى.

انطلاقا من أهمية موضوع الدراسة وأسباب اختياره؛ يتبين أن له بالنتيجة العديد من الأهداف المبحوث عن الوصول إليها وتحقيقها. التي تدور جلها حول ما تصنعه جرائم الوسط الرقمي، من أضرار بالغة للأشخاص، سواءً أكانت مادية أو معنوية. الأمر الذي تقابله قلة المتابعة الجزائية عادةً –شبه قضائية وقضائية–، وان وجدت تكون وفق إجراءات تقليدية غير نافعة –التي تجاوزها الزمن–؛ نظرا لاختلاف طبيعتها أو لعجزها النسبي والمطلق أحيانا، إن بخصوص الأعمال الإجرائية المتبعة، أو الأجهزة الممارسة لها تكويناً وعملاً.

ولذلك نستهدف من دراستنا هذه؛ البحث في خبايا الوسط الرقمي، التي أدت إلى عجز الإجراءات الجزائية التقليدية عموماً، وإجراءات التحري والتحقيق الواردة من خلالها وفي إطارها خاصةً. ومنه البحث في مدى قابلية هذه الإجراءات التقليدية للتعديل و/أو التتميم فقط، أم أننا نحتاج إلى نصوص إجرائية حديثة بنظرة مستجدة تماما، ترتكز على البعد الافتراضي غير المادي، وتتناسب مع خصوصية وتعقيدات الوسط الرقمي، الذي تحدثه عناصره الرقمية مع اختلاف أنواعها وأصنافها، الأساسية والحكمية كما سنرى لاحقا.

مع التأكيد على استهداف الدراسة؛ البحث في مدى قدرة الأجهزة الإجرائية التقليدية، على ممارسة البحث والتحري بالصورة الناجعة المرجوة، من الإجراءات الجزائية عموماً. دون أن ننسى النظر في مدى عمل المشرع الجزائري، استئناسا ببعض التشريعات الأخرى والاتفاقيات الدولية ذات الصلة –كاستئناس فقط دون مقارنة حقيقية–؛ على إيجاد الحلول القانونية اللازمة لمواجهة الوضع الراهن، الذي أصبح يؤرق كل الفاعلين في مواجهة الجريمة بعد ولوجها إلى الوسط الرقمي، إن عبر الوقاية أو المكافحة أو الاثنين معا.

أيضا يهدف موضوع الدراسة، المنطوي على التحري والتحقيق في جرائم الوسط الرقمي؛ إلى البحث في الحلول القانونية ذات البعد الإجرائي –اللازمة–، التي قد تفيد المشرع والفقه والدارسين عموماً؛ على الوقوف عند الآليات والطرق الناجعة، حتى نصل في الأخير إلى مكافحة –وقبل ذلك الوقاية–، هذا النوع من الإجرام الرقمي الحديث، الذي يمتاز بالكثير من الخصوصية المعقدة، سيما من خلال ممارسة إجراءات التحري والتحقيق في النطاق الافتراضي لهذا الوسط.

هذا دون أن ننسى أن البحث في إجراءات التحري والتحقيق المتصلة بجرائم الوسط الرقمي؛ هو في حد ذاته توطئة لموضوعات قانونية أخرى، سيما في الشق الإجرائي نفسه، المتصل بإجراءات التحقيق القضائي النهائي، الذي يقيمه قاضي الموضوع في الجلسة، ممارسة لمرحلة المحاكمة عموماً. انطلاقا من ترابط وتكامل الإجراءات الجزائية، التي تجعل من المرحلة المحاكمة؛ التالية في الممارسة بعد التحقيق القضائي، إن تمت الإحالة أمام المحكمة بالطرق المقررة قانونا لذلك.

كل ما طرح؛ يقود آليا إلى بروز مشكلة أو إشكالية موضوع الدراسة. فجرائم الوسط الرقمي ذات الطابع الفني الرقمي الافتراضي؛ أصبحت واقعا لا مفر منه، وعجز القواعد الإجرائية التقليدية مادياً وبشرياً؛ أصبح واضحاً وجلياً. وبعد أن ولج المشرع إلى الوسط الرقمي ليجرم فيه العديد من السلوكيات الرقمية والمرقمنة؛ أصبح لابد لقواعد التحري والتحقيق أن تلج إليه هي الأخرى، لكن بطابع حديث يتناسب مع خصوصيات هذا الوسط، إن عبر إجراءات رقمية حديثة أو أخرى مرقمنة بالبعد اللازم الذي يكون له الأثر الايجابي.

ولعل أبر إشكالات موضوع التحري والتحقيق في جرائم الوسط الرقمي؛ تدور حول طبيعة السلوكيات المرتكبة في هذا الوسط الافتراضي الحديث، انطلاقا من الطبيعة التقنية المعقدة للوسط ذاته –غير المسبوق التعامل مع مثلها–. الأمر الذي يجعل من الإجراءات التقليدية للتحري والتحقيق؛ من دون جدوى من جهة، ويصعب ممارسة الإجراءات الحديثة من أشخاص غير مؤهلين لذلك من جهة أخرى. دون أن ننسى أيضا، الطابع الديناميكي سريع التطور لتقنيات الوسط الرقمي، مما يصعب إمكانية مواكبة المشرع لهذه التحولات السريعة.

كما تبرز إشكالية أو صعوبة تحديد مكان ارتكاب الجريمة، وبالنتيجة الجهة المختصة بالتحري والتحقيق؛ نظرا لعالمية الوسط الرقمي. وسهولة إخفاء آثار الجريمة الرقمية، وبالنتيجة صعوبة اكتشافها أو إثباتها إن اكتشفت. وكذلك الدور الوقائي غير المعتاد للقواعد الإجرائية –الذي برز مع بروز جرائم الوسط الرقمي–، ومدى تناسبه مع أحكام ومبادئ الإجراءات الجزائية. وبالإضافة إلى المواجهة الفقهية، التشريعية والقضائية، وخاصة المؤسساتية؛ المدنية، الإدارية، شبه القضائية والقضائية؛ لمرحلتي التحري والتحقيق في جرائم الوسط الرقمي.

وعليه يمكن القول؛ أننا إذا ما سلمنا بخصوصية التجريم في الوسط الرقمي، وبحتمية إِتْبَاْع القواعد الموضوعية بأخرى إجرائية من الطبيعة نفسها؛ ففيم تتمثل أحكام القانون الجزائري النافذة، بخصوص كل من التحري والتحقيق في النطاق الافتراضي للوسط الرقمي ؟

كما تتضمن الإشكالية الأساسية المطروحة؛ العديد من التساؤلات الفرعية. التي يمكن أن نفرعها إلى أربعة أسئلة، على النحو التالي:

– فيم تتمثل الخصوصية الإجرائية الحديثة في مواجهة جرائم الوسط الرقمي، وما مدى تكيفها مع المبادئ الإجرائية التقليدية ؟

– وما هي الأجهزة الممارسة للتحري والتحقيق في جرائم الوسط الرقمي، وما مدى نجاعتها ؟

– وفيم تتمثل الإجراءات المباشرة من أجهزة التحري والتحقيق في جرائم الوسط الرقمي، وما هي نقائصها ؟

– وما مدى مواكبة المشرع الجزائري للتحولات الإجرائية، استئناساً بنظرائه من جهة والاتفاقيات الدولية السارية من جهة أخرى ؟

في سبيل الإجابة عن الإشكالية الأساسية والتساؤلات المتفرعة عنها؛ يتوجب العمل على إتباع منهج علمي سليم، يتناسب مع الطابع النظري للبحث في العلوم القانونية. فبعد التوطئة المقدمة لموضوع الدراسة المعنون بإجراءات التحري والتحقيق في جرائم الوسط الرقمي، مع طرح أهميته والأهداف ذات الصلة،

ربطاً بالمشكلة والإشكالية المذكورة؛ آثرنا كمرجعية منهجية قبل تحديد المنهج العلمي المتبع، العمل ببعد ثلاثي أساسي؛ يدور بين التفوق العلمي التكنولوجي أولا، والاختلاف التشريعي والنصي ثانيا، والجدل الفقهي القانوني ثالثا.

فأدخل التفوق العلمي المتصل بالوسط الرقمي؛ كل المتعاملين معه في دوامة يصعب مواجهتها بالسبل والوسائل المعروفة، ما أسس للاختلاف التشريعي الوطني، والاتفاقي الإقليمي والدولي. كما كان لكل هذا التفوق العلمي والاختلاف التشريعي؛ الأثر البالغ من حيث الدراسات الفقهية ذات الصلة، بخصوص الشقين الموضوعي وخاصةً الإجرائي. حيث كثر الجدل الذي يزداد عمقاً، كلما اتسعت الفوارق بين التفوق العلمي الرقمي سريع التطور والتخلف التشريعي الجنائي. الأمر الذي يعطي مرجعية أساسية لمنهج الدراسة، يُؤَسَسُ لها من منطلق الأبعاد الثلاث المذكورة.

وعليه يمكن القول بعدم إمكانية التطرق إلى الموضوع محل الدراسة، بكل التعقيدات الفنية والقانونية التي تعتريه، والأبعاد الثلاث المذكورة –علمي وتشريعي وفقهي–، التي تزيد من حدة خصوصيته، المتفق على كونها العلامة البارزة في جرائم الوسط الرقمي عموماً؛ إلا عبر الاعتماد بالأساس على المنهج الوصفي التحليلي –في إطار دمج منهجي بين المنهج الوصفي والمنهج التحليلي–، وكذا نظيره الاستدلالي.

فيكون الاعتماد على المنهج الوصفي التحليلي؛ بغرض وصف موضوع التحري والتحقيق في جرائم الوسط الرقمي كما هو، سيما كونه ظاهرة جنائية حديثة تتطلب الدراسة الوصفية، إن تقنيا أو قانونيا أو فقهيا. الأمر الذي يستوجب بعد الوصف العلمي الدقيق؛ الانتقال إلى التحليل والنقد والتركيب، بالاعتماد على المنهج التحليلي، الذي يسمح بالوقوف عند دقائق الأمور الفنية في الوسط الرقمي بعد تحليلها، لإلحاقها بالنصوص الجنائية الجزائرية والدراسات الفقهية الجزائرية وغيرها، التي نحللها وننتقدها بالطريقة العلمية الايجابية.

كما يكون الاعتماد على المنهج الاستدلالي، كمنهج مساعد للوصفي التحليلي المذكور أعلاه. وذلك بغرض تكملة الحلقة البحثية، من خلال تعزيزها بدراسة وتقدير مدى صلاحية كل إجراء أو عمل إجرائي، لأن يكون آلية إجرائية يعمل بها في التحري والتحقيق، انطلاقا من التجارب الميدانية من الفنيين وخاصة المختصين –الشرطة القضائية وغيرها–، والوقوف على المميزات والعيوب.

مع الإشارة إلى إمكانية الاستئناس ببعض الأمثلة من النصوص المقارنة والاتفاقية، بصورة عرضية لا تغير من طبيعة الدراسة الوصفية التحليلية. وذلك من خلال الإشارة عند الحاجة إلى بعض القوانين غير الجزائرية تشريعا واتفاقا، التي تعد متفوقة في هذا المجال، سيما القانون الفرنسي والأردني والإماراتي والأمريكي. والاتفاقيات الدولية السباقة في هذا المجال، كالاتفاقية الأوروبية –بودابست– حول جرائم الوسط الرقمي لسنة 2001.

وعلى العموم يعد موضوع جرائم الوسط الرقمي؛ من أهم موضوعات العصر الحالي على الإطلاق، الأمر الذي أدى بالعديد من المختصين للتعبير عنها؛ بالجرائم المستحدثة –أو جرائم المستقبل–، التي تتطلب إجراءات متابعة حديثة تتناسب مع طبيعتها الرقمية الافتراضية. فتنوعت وتعددت الدراسات الفقهية السابقة بهذا الخصوص في الشقين الموضوعي والإجرائي، إن على المستوى الوطني أو الإقليمي –عربي وإفريقي– أو حتى الدولي العالمي.

ربما يبدو لقارئ الفقرة أعلاه من الوهلة الأولى؛ أننا بصدد دراسة موضوع مستهلك بدراسات متنوعة ومتعددة كما ذكرنا، ما يذهب عن بحثنا أهم عنصر واجب فيه، ألا وهو الجدة والإبداع العلمي. إلا أن الأمر ليس كذلك، فحتى وان وجدت دراسات متعددة؛ يبقى بحثنا هذا يتصف بالجدية، ليس لكونه يطرح الجديد فحسب بل لأسباب أخرى عديدة، منها ما تتصل بالدراسات السابقة، ومنها ما تتعلق بخاصية في الوسط الرقمي ذاته.

فالدراسات السابقة –الجزائرية– المنصبة على الشق الإجرائي في جرائم الوسط الرقمي؛ تذهب في العادة للاعتماد على المنهجين الوصفي والمقارن، عبر مقارنة القانون الجزائري بنظرائه والاتفاقيات الدولية، ومن ثم الاكتفاء بطرح التحليلات والتعاريف الفقهية، التي وضعها الباحثون والفقهاء انطلاقا من دراسة ونقد النصوص القانونية الأجنبية والاتفاقية. بينما في بحثنا هذا اعتمدنا سبيلا آخرا، عبر التركيز على القانوني الجزائري تحليلا ونقدا، مع الإثراء الوصفي بما جاء به النص والفقه المقارنين.

كما أننا لا نؤسس الجدة وعدم التكرار في دراستنا هذه؛ على مجرد حداثة جرائم الوسط الرقمي، وذلك لكون الحداثة من حيث هي؛ تعود إلى ثمانينات القرن الماضي، ما يعد وقتا كافيا لدراستها فقها وقانونا، من قبل علماء وفقهاء القانون الجنائي موضوعيا وإجرائيا. إنما وقوفا عند ديناميكية وسرعة تطور الوسط الرقمي ذاته، الذي كلما وجدت دراسة فقهية له من حيث إجراءات التحري والتحقيق –حتى بخصوص الشق الموضوعي–، اختلق نوابغه آليات حديثة وجد معقدة تتطلب دراسات أخرى جديدة[1].

ونذكر على سبيل المثال أطروحة الدكتوراه، المنجزة سنة 2018 من طرف الباحث "جمال إبراهيمي"، تحت عنوان: "التحقيق الجنائي في الجرائم الإلكترونية"، التي نقول فيها –إثراءً لا تقليلا–، بالإضافة إلى الملاحظات العامة المذكورة؛ أنها تطرقت للتحقيق في الجرائم الإلكترونية، دون الإشارة إلى تقسيمات النطاق الافتراضي، الدائر بين الويب السطحي ونظيره العميق. كما أن هذه الدراسة لم تفرق بين التحري والتحقيق، كمراحل إجرائية منفصلة عن بعضها البعض من حيث الأجهزة والأعمال عموماً.

[1] وبالتالي؛ لايمكن القول بسبق الدراسة في موضوع الحال، ولا أنه مستهلك، فالعنوان نفسه يمكن أن تعاد دراسته العديد من المرات، بعد مرور فترة زمنية قصيرة. وخير دليل على ذلك، سعي الاتحاد الأوروبي الحثيث في إطار مواجهة الإجرام الرقمي، عبر الدراسة المستمرة والدورية لهذا المجال -كما سنرى لاحقا-، وذلك بلا توقف منذ إصداره سنة 2001 لاتفاقية بودابست حول جرائم الوسط الرقي.

مع الإشارة إلى بعض الدراسات الأخرى، على غرار أطروحة الدكتوراه المنجزة سنة 2017 من الباحثة "شرف الدين وردة"، بعنوان: "الإثبات الجنائي بالأدلة الالكترونية". وأطروحة الدكتوراه الأخرى المنجزة سنة 2016 من الباحث "حسن ربيعي"، تحت عنوان: "آليات البحث والتحقيق في الجرائم المعلوماتية". التي نبحث من خلال دراستنا هذه إلى التكامل معها فيما نتفق فيه، والاختلاف عنها فيما نختلف فيه، سيما من حيث ضرورة التفرقة بين التحري والتحقيق أولا، وتقسيم النطاق الافتراضي للوسط الرقمي ثانيا، والتركيز على التحليل والنقد اتصالا مباشرا بنصوص القانون الجزائري ثالثا.

وتحديدا لطبيعة الدراسة؛ نقول أنها إجرائية أساسا وموضوعية عرضا. فنعمل على طرح المضمون العام لجرائم الوسط الرقمي، قبل التوسع في دراسة الشق الإجرائي المتصل بمرحلة التحري، وإجراءات التحقيق القضائي الابتدائي، الممارس بدرجتيه من قاضي التحقيق وغرفة الاتهام –مع إمكانية الإشارة إلى التحقيق القضائي النهائي في مرحلة المحاكمة–. أما من ناحية النصوص القانونية مصدر الدراسة؛ فسنعتمد على القوانين المحلية والاتفاقية التي تعد مصدرا للقانون الجزائري، مع طرح بعض التشريعات المقارنة والاتفاقيات الدولية الأخرى، على سبيل الاستئناس والاستفاضة عند الحاجة.

أما من حيث الدراسة الفقهية المتصلة بآراء الفقهاء واجتهاداتهم، ونظيرتها التقنية المتعلقة بعناصر الوسط الرقمي وتطورها الديناميكي السريع؛ فسنطلق الدراسة بشأنها ولا نقيدها بحدود معينة، نظرا لكون هذه الأخيرة –الفنية– العامل الأساس في دراسة الحال، واعتبار الفقه المفسر والمسقط للنص القانوني على الواقع الرقمي المعقد، مع التأكيد على مفارقة؛ التطور الديناميكي السريع للوسط الرقمي، واستحالة مواكبة الفقه القانوني له.

ولغرض دراسة موضوع إجراءات التحري والتحقيق في جرائم الوسط الرقمي، بكل التعقيدات المذكورة؛ آثرنا عرضا نفرغه في قالب منهجي ثنائي مكون من بابين أساسيين. فنستهل الدراسة بسرد الإطار العام لإجراءات التحري والتحقيق في جرائم الوسط الرقمي(باب أول)، الذي نبرز من خلاله خصوصية هذه الإجراءات المتصلة بمواجهة هذا النوع من الإجرام الحديث، وكذا الطرح المفصل للأجهزة المكلفة بممارسة الإجراءات نفسها، سواءً القضائية منها أو شبه القضائية، الخاصة أو العامة، وحتى الدولية والمقارنة المتعاونة مع نظيرتها الجزائرية.

على أن نتطرق بعد الانتهاء من الإطار العام المذكور؛ إلى ما سميناه بممارسة أو مباشرة إجراءات التحري والتحقيق في جرائم الوسط الرقمي(باب ثانٍ). وذلك من خلال التعريج على ممارسة مختلف الإجراءات التي قسمناها إلى أساسية؛ تتصل بالدليل الرقمي الجنائي كمحور كل الإجراءات محل الدراسة، والأعمال التي وصفناها على أن لها الطابع الجوهري في استخراج هذا الدليل الرقمي الحديث، وأخرى مساعدة لنظيرتها الأساسية، التي تدور بين تلك التقليدية العادية والمرقمنة من جهة والحديثة الرقمية وغيرها من جهة أخرى.

البـــــاب الأول

الإطار العام لإجراءات التحري والتحقيق في جرائم الوسط الرقمي

تعتبر دراسة الإطار العام في العادة من أبسط وأسهل النقاط البحثية، مهما اختلفت الموضوعات الجنائية أو القانونية بصفة عامة. فدراسة الإطار العام للجريمة التقليدية مثلا –النظرية العامة للجريمة–؛ يعد بمثابة البديهية القانونية المتعارف عليها منذ تأسيس القانون الجنائي والعلوم الجنائية، إلا ما حدث فيه تعديل أو تتميم، الذي في كل الأحوال ومهما كان؛ لا ولن يغير كثيرا من الطابع التقليدي المعروف للنص وتفسيره عموماً.

إلا أن بروز عناصر الوسط الرقمي، والنطاق الافتراضي غير المادي الذي تحدثه، جعل من مجرد الحديث عن الإطار العام في أي شق متصل بالجرائم ذات الصلة –موضوعيا أو إجرائيا–؛ بمثابة الدخول في غير الثابت قانونا والمختلف فيه فقها. فبعد أن اختلف الفقه ولا زال كذلك –وكذلك المشرع الوطني والمقارن والاتفاقي–؛ من حيث النظرية العامة لجرائم الوسط الرقمي في شقها الموضوعي، انتقل الوضع نفسه وبحدة أكثر؛ إلى الشق الإجرائي في مواجهة هذا النوع من الإجرام الحديث، سيما بخصوص التحري والتحقيق منها.

ولعل أبرز العوائق البحثية التي تواجه محاولة وضع الإطار العام لإجراءات التحري والتحقيق في جرائم وسط الرقمي؛ تنطوي على الشق التقني الفني قبل نظيره القانوني النصي. فهذا النطاق الافتراضي الذي تحدثه عناصر الوسط الرقمي على اختلاف أشكالها وأجيالها، يعد تقنيا بمثابة الثورة التكنولوجية، التي انتقلت بالمتعامل والمتفاعل معه من النظرة المادية للأمور وصعوبة التعامل، إلى العيش في نطاق افتراضي، يبسط الأفكار ويجعلها قابلة للتعامل والإفادة ولو افتراضيا، بصورة منفصلة عن الواقع المادي المعروف تقليديا.

لكن هذا الوسط نفسه بكل مميزاته الفنية والمجتمعية؛ له جانب آخر يمكن أن ينظر له من خلاله، وهو المنطوي على البعد القانوني عموماً والجنائي خاصةً. فنقول أن المسرح الحديث للجريمة، أو المسرح الجرمي الافتراضي كما سميناه في دراستنا هذه؛ هو من أعقد الأوساط من ناحية التعامل الجنائي –إن لم نقل أنه الأعقد على الإطلاق–، في إطار الخصوصية الرقمية التي تعتريه، لتجعل منه صعب التعامل –أو حتى مستحيل– في الكثير من الأحيان، إن من طرف الأجهزة الشرطية أو غيرها من الأجهزة الفنية والإدارية المساعدة.

كما نجد أن هذا المسرح الجرمي الافتراضي يزداد تعقيدا، كلما رجعنا إلى الجريمة التي ترتكب فيه من الناحية الموضوعية النصية والفقهية، التي للمشرع الجزائري فيها –كغيره من نظرائه–؛ أحكام حديثة وأخرى تقليدية محينة –مرقمنة– تتعلق بالمفهوم والأنواع وغير ذلك. ما يذهب بنا للقول أنه لجرائم الوسط الرقمي؛ إطارا عاما في القانون الجزائري، يختلف عن العديد من نظرائه في التشريعات المقارنة، كما قد يتفق مع العديد منها أيضا.

وفق الطرح نفسه المتعلق بالشق الموضوعي لجرائم الوسط الرقمي، وربطا بالمسرح الجرمي الافتراضي من جهة، وإجراءات المواجهة ذات الصلة من جهة أخرى؛ نجد أنه للقانون الجزائري بخصوص الشق الإجرائي، أحكاما وتوجها نصيا؛ يمكن أن نستنتج منهما العديد من القواعد، لنصبغ عليها وصف الإطار الإجرائي العام، المتصل بالتحري والتحقيق على وجه الخصوص، مع التأكيد على الخصوصية الحديثة المنفصلة عن الطابع التقليدي المادي، التي برزت وأسست لتحري وتحقيق من نوع خاص، يمتاز بالصعوبة والتعقيد أيضا.

هذا من دون أن نتجاوز فكرة الربط القانوني الضروري بين القالب العام للإجراءات والأجهزة الممارسة لها. فالإطار العام يشمل الاثنين معاً، سيما وأنه أسس لخصوصية إجرائية منفصلة عن الجريمة التقليدية –كما ذكرنا أعلاه وسابقا–، التي نشأة بعنوان جرائم الوسط الرقمي عموما ومواجهتها الإجرائية –وقاية و/أو مكافحة– خاصةً، الواجبة والضرورية –الخصوصية في المواجهة–؛ كلما ازداد هذا المسرح الجرمي الافتراضي تعقيدا وتطورا، سيما وأن أبرز خصائصه –كما سنبين لاحقا–؛ تتمثل في كونه ديناميكي وسريع التطور من كل الجوانب الفنية.

وهي الأجهزة التي لنا فيها رأي خاص من حيث طرحها وتقسيمها –كما لنا رأي خاص في كل جوانب البحث، قد يكون مختلفا عن المعهود–، سواءً الوطنية أو الأجنبية، ربطا بالقانون الجزائري والتحري والتحقيق المنجزين أساسا من الأجهزة الجزائرية. حيث لايمكن للأجهزة التقليدية –الجزائرية– أن تمارس التحري والتحقيق في جرائم الوسط الرقمي، بالتشكيلة والمعارف المعهودين. كما لا يمكنها بعد أن تطور نفسها بالوجه المطلوب؛ أن تمارس ذلك في الكثير من الأحيان بصورة انفرادية وطنية، نظرا للطابع العالمي المتجاوز للحدود الإقليمية –افتراضيا–، الذي يمتاز به النطاق الافتراضي للوسط الرقمي.

وعلى العموم؛ آثرنا من باب التطرق إلى الإطار العام لإجراءات التحري والتحقيق في جرائم الوسط الرقمي، انطلاقا من الطرح الخاص بالباحث ترتيبا ومضمونا؛ التركيز على الخصوصية الإجرائية ذات الصلة بالتحري والتحقيق في هذه الجرائم الحديثة(فصل أول)، عبر التعريج على الوسط الجرمي الافتراضي الحديث، والجرائم المرتكبة من خلاله وفي إطاره، والوقوف عند العجز الإجرائي التقليدي، توجها نحو إجراءات حديثة رقمية ومرقمنة.

على أن ننتقل بعد ذلك إلى الطرح المفصل للأجهزة الممارسة للتحري والتحقيق في جرائم الوسط الرقمي(فصل ثانٍ)، التي –الأجهزة– قسمناها إلى وطنية مختصة –جزائرية–، منهما الرئيسية ومنها المساعدة، وأخرى أجنبية متعاونة في إطار التعاون الجنائي الدولي، التي قد تكون دولية عالمية و/أو إقليمية، كما قد تكون وطنية مقارنة، إما نظرا لاختصاصها الإقليمي أو لكونها تعد من الخبرة والتجربة والمعارف الرقمية الحديثة بمكان.

الفـــصل الأول

خصوصية إجراءات التحري والتحقيق في جرائم الوسط الرقمي

يقوم المجال الجنائي كأصل عام على شقين، الأول موضوعي نظري والثاني إجرائي عملي. فتواجه الجريمة موضوعيا؛ بأحكام عامة في إطار النظرية العامة للجريمة، وأحكام خاصة في إطار التجريم والعقاب الخاص بكل سلوك على حدا –أو ما يسمى بالقانون الجنائي الخاص–. كما تواجه –الجريمة– إجرائيا؛ بأحكام الأصل فيها أنها عامة، تطبق بهدف المتابعة الجنائية المتصلة بجل السلوكيات المجرمة. الأمر الذي يجد أساسه في الفكرة الجنائية السابقة بالطرح، التي مفادها التأسيس العلمي والعملي لضرورة –أو حتى حتمية– العمل بالقواعد القانونية الإجرائية؛ بعد انتهاء دور القواعد الموضوعية، القائمة على التجريم النظري.

ووفق الفكرة الجنائية الموضحة أعلاه؛ يجب أن تتناسق القواعد الإجرائية مع القواعد الموضوعية، من حيث الطبيعة المتصلة أساسا بالجريمة محل المتابعة. فلما كانت جل السلوكيات المجرمة؛ متناسقة من حيث الخضوع إلى أحكام النظرية العامة للجريمة؛ ظلت الأحكام الإجرائية مناسبة وناجعة، إن في إطار النص عليها نظريا أو بخصوص تطبيقها عمليا. الأمر الذي لم يظل على حاله، حيث انطلاقا من العديد من مستجدات العصر الحديث؛ ظهرت–إن صح التعبير–نظريات عامة جزئية، تخص بعض الجرائم على وجه الخصوص، سيما جرائم الوسط الرقمي. الأمر الذي أدى أيضا إلى؛ ضرورة العمل بإجراءات جنائية خاصة، خاصةً في إطار مرحلتي التحري والتحقيق.

وعلى العموم؛ عكف المشرع الجزائري خاصةً والمقارن عموما؛ على عدم معاملة أي جريمة كانت معاملة خاصة موضوعيا وإجرائيا؛ إلا إذا اتسمت بطابع الخصوصية، الذي يتباين من جريمة إلى أخرى. فقد تستمد خصوصيتها–الجريمة–، من الخطورة الإجرامية أو من الضرر البالغ الذي تخلفه، أو من الطابع الخاص للمجال محل الاعتداء...الخ. الأمر الذي يتوسع في جرائم الوسط الرقمي، لينطوي على التحول التام في مسرح الجريمة من الماديات الملموسة إلى المعنويات المحسوسة. انطلاقا من الطابع الرقمي الافتراضي للوسط الرقمي نفسه. وهو ما أدى إن صح التعبير إلى بروز أزمة بخصوص القواعد الإجرائية التقليدية، المعمول بها عادة في إطار التحري والتحقيق الجنائي، سيما بالنظر إلى العجز الإجرائي الجزئي وحتى الكلي، في مواجهة هذا النوع من الإجرام الحديث والمعقد.

ولم يتدخل المشرع الجزائري؛ بغرض اعتماد إجراءات جنائية –جزائية– من الطبيعة ذاتها التي تقوم عليها جرائم الوسط الرقمي والمسرح الافتراضي الحديث الذي تتصل به، إن من حيث الأجهزة المختصة بالتحري والتحقيق فيها، أو بخصوص الأعمال والأوامر والأذون الإجرائية المعتمدة في ذلك –كما سنرى لاحقا–؛ إلا بعد أن سلم جنائيا بما ذكر أعلاه، سيما بالخصوصية ذات الصلة بجرائم الوسط الرقمي ومسرحها الافتراضي من جهة(مبحث أول)، والتحري والتحقيق في المسرح الافتراضي نفسه من جهة أخرى(مبحث ثانٍ).

المبحث الأول

جرائم الوسط الرقمي ومسرحها الافتراضي الحديث

ظلت السلوكيات البشرية والى وقت قريب؛ مرتبطة بالوسط المادي الملموس، ما سهل الأمر على المشرع من حيث تجريم منها ما يراها واجبة التجريم، بعد محاولة حصرها وتحديدها. خاصةً إذا ما علمنا أن هذا الوسط المادي؛ هو النطاق الطبيعي الذي وجد فيه الإنسان، وأغلب السلوكيات التي ترتكب من خلاله؛ تعد سهلة التعامل معها موضوعيا، ومنه بساطة متابعتها جنائيا عن طريق تفعيل الإجراءات التقليدية المعروفة.

إلا أنه بظهور الوسط الرقمي؛ أصبح بإمكان الشخص بمجرد التعامل مع عناصره؛ أن يلج من كل ما هو مادي ملموس إلى ما هو رقمي افتراضي. الأمر الذي يحول تصرفات الشخص، ويجعلها ذات أبعاد رقمية تختلف تماما عن الأبعاد المادية للتصرفات التقليدية في الوسط المادي. ومنه كان لزاما على المشرع؛ أن يراعي الخصوصية التقنية للوسط الرقمي كمسرح حديث للجريمة، قبل أن يلج إليه؛ ليضع إجراءات هادفة إلى التحري والتحقيق فيه، بعد أن يجرم السلوكيات واجبة التجريم.

وبمراعاة المشرع لخصوصية الوسط الرقمي كمسرح حديث للجريمة؛ قبل أن يلج إليه موضوعيا وإجرائيا؛ يكون قد أقر ضمنيا باختلافه عن الوسط المادي التقليدي، واحتياجه لنظرة حديثة من الطبيعة الرقمية ذاتها. وهو ما سنبينه بالتطرق أولا إلى الوسط الرقمي كمسرح جرمي افتراضي(مطلب أول)، وتبيان ثانيا الأحكام الموضوعية للجرائم المتصلة به(مطلب ثانٍ).

المطلب الأول: الوسط الرقمي الافتراضي كمسرح جرمي حديث

تتصل المواجهة الجنائية للجرائم محل الدراسة موضوعيا وإجرائيا؛ بالوسط الرقمي الافتراضي، الذي له الطابع المستقل والمنفصل عن نظيره المادي التقليدي. فالوسط الرقمي مع بدايات ظهوره وتطوره؛ استحدث نطاقا افتراضيا من جهة، وسلوكيات ذات الصلة والطبيعة نفسها من جهة أخرى. الأمر الذي أنتج مسرحا جرميا جديدا، لم يسبق التعامل مع مثله جنائيا، لا موضوعيا ولا إجرائيا. وعلى العموم كان من الواجب قانونا قبل إصباغ صفة المسرح الجرمي الحديث على الوسط الرقمي؛ تدخل المشرع ليحصر سلوكياته واجبة التجريم أولا، وليقرر إجراءات تحري وتحقيق من الطبيعة الرقمية الافتراضية نفسها ثانيا.

ولا يمكن الوقوف عند أحكام الوسط الرقمي الافتراضي كمسرح جرمي حديث؛ إلا بعد البحث في مضمونه التقني المحض، من حيث تحديد المفهوم العام(فرع أول)، وإبراز العناصر المادية المحدثة له(فرع ثانٍ)، ومن ثم تبيان على وجه الخصوص؛ نطاقه الافتراضي الذي هو نفسه نطاق مسرح جرائم الوسط الرقمي(فرع ثالث).

الفرع الأول: مفهوم الوسط الرقمي

يأخذ المفهوم المتصل بالوسط الرقمي؛ البعد التقني المحض، الذي من خلاله يمكن الوقوف على أساس الخصوصية التقنية للوسط الرقمي كمسرح للجريمة أولا، وفتح المجال للبحث في عناصره المادية ونطاقه الافتراضي ثانيا. علما أن الفقه الجنائي لم يتطرق إلى الوسط الرقمي بالمفهوم التقني الحديث؛ انطلاقا من كونه وسط مركب ولعدم استقراره تقنيا.

وبغض النظر عن التسميات المختلفة للوسط محل الدراسة-كما سنرى لاحقا-؛ يمكن أن نصل إلى مفهومه التقني المحض، من خلال البحث في مراحل تطوره بعد نشأته(أولا)، ومن ثم الوقوف عند التعريف به(ثانيا)، على أن نبين بعد ذلك أهم الخصائص المميزة له(ثالثا).

أولا: نشأة وتطور الوسط الرقمي

ارتبطت بوادر نشأة الوسط الرقمي؛ بظهور الثورة الصناعية الثانية[1]، في إطار النصف الثاني من القرن التاسع عشر. فمن خلالها دخل العالم إلى ما يسمى بعصر "الأتمتة"-الأوتوماتيكية-، الذي يعتمد على مختلف الاختراعات الصناعية بالأساس، والتي بموجبها أصبحت الآلات الميكانيكية تعمل بالنظام الآلي بدلا عن اليدوي، سيما في مجالات الصلب والنقل عبر السكك الحديدية والكهرباء...الخ[2].

إلا أن البعد "الأوتوماتيكي" الموضح أعلاه؛ ظل في بداياته ضيقا إلى أبعد الحدود، لا يكاد يخرج عن أهم الضروريات الأساسية لمجال التصنيع من جهة، ويعتمد على الكهرباء والبخار من جهة أخرى. الأمر الذي دفع بالباحثين مع بدايات القرن العشرين؛ إلى ضرورة تطوير أساس عمل نظام "الأتمتة"، لجعله شاملا وغير مكلفا، ولينتقل بمعالجة المعطيات من البشرية إلى الرقمية. ومن خلال ذلك انطوى البديل على التكنولوجيا الحديثة، التي تعمل بالأنظمة الرقمية، أو كما يسميها العديد بالأنظمة الالكترونية[3].

ومنه شهد العالم الانتقال التدريجي إلى الثورة الصناعية الثالثة، التي عرفت أهم حلقاتها مع بداية سبعينات القرن الماضي. فمن خلالها؛ اتسع مجال "الأتمتة" كما وتطور كيفا. حيث تم اختراع ما يسمى

---

[1] كما تطلق عليها أيضا تسمية؛ المرحلة الثانية من الثورة الصناعية الكبرى. وهذا نظرا لورودها بعد الثورة الصناعية الأولى، التي ظهرت في انجلترا مع أواخر القرن الثامن عشر، وامتدت إلى غاية بدايات القرن التاسع عشر. ومن خلالها برزت الآلات الميكانيكية اليدوية. **أنظر في ذلك:** أسماء سعد الدين، **"الفرق بين الثورة الصناعية الأولى والثانية"**، تاريخ النشر: 10 أوت 2015، تاريخ التصفح: 19 نوفمبر 2017. الرابط: http://www.almrsal.com/post/262428.

[2] **أنظر:** أنيل كورانا وبدر العلماء، **"الثورة الصناعية الرابعة: بناء المؤسسات الصناعية الرقمية"**، وثيقة معلومات، شركة برايس ووترهاوس كوبرز(في دبليو سي) بالتعاون مع القمة العالمية للصناعة والتصنيع (GMIS) وبمبادرة من منظمة الأمم المتحدة للتنمية الصناعية(اليونيدو) ووزارة الاقتصاد في دولة الإمارات العربية المتحدة، 2016، ص 06. متوفر عبر الرابط: https://www.pwc.com/gx/en/industries/industry-4.0.html.

[3] **أنظر:** أيمن عبد الله فكري، جرائم نظم المعلومات، دراسة مقارنة، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، 2007، ص 24.

بجهاز الإعلام الآلي، الذي يعمل بالأنظمة الرقمية الآلية ذات البعد الافتراضي، وتم اختراع أيضا؛ العديد من الأجهزة المشابهة له والعاملة بالأنظمة الرقمية، سيما تلك الداخلة في حكمه والرجل الآلي...الخ[1]. إلا أن الأمر ورغم تطوه الكبير آن ذاك؛ ظل مقيدا تقنيا وماديا، إلى أن تم اختراع شبكة الاتصال الدولية-كما سنرى لاحقا-، التي فتحت المجال للاتصال والتحكم عن بعد في الأنظمة الرقمية المختلفة.

من خلال ما ذكر؛ أصبح الوسط الرقمي شاملا لأغلب مجالات الحياة-إن لم نقل جلها-. حيث بات موازيا للوسط المادي الحقيقي الذي نعيش فيه، إلى درجة ظهور من ينادي بأننا نشهد حاليا أو نكاد نشهد ثورة صناعية رابعة، تغير من الواقع المعاش كليا، لتجعل من الرقمية أساسا له، سيما في مجالي التصنيع والاقتصاد، فالمصانع أصبحت رقمية أو مرقمنة، والتعامل المالي أصبح رقميا...الخ[2].

وعليه يمكن القول؛ أن الوسط الرقمي لم يأتي هكذا، وإنما جاء بخط نشأة وتطور دفعت إليهما الحاجة البشرية، ولا يزال يتطور يوميا بطريقة ديناميكية سريعة. ورغم الصعوبة التقنية والقانونية المتصلة بإيجاد مفهوم جامع لهذا الوسط؛ يمكن أن نقف فيما يلي عند محاولة تعريفه وبالنتيجة تبيان أهم خصائصه.

ثانيا: تعريف الوسط الرقمي

بغرض تعريف الوسط الرقمي باعتباره المسرح الجرمي الحديث، المضفي للخصوصية الجنائية على الجرائم المتصلة به؛ نقف أمام كونه أمرا مستحدثا من حيث المضمون والدلالة أولا، ومركبا من كلمتي "الوسط" و"الرقمية" ثانيا. فللوسط العديد من المعاني اللغوية والاصطلاحية، وللرقمية أيضا. ولا يمكن الوصول إلى المعنى الاصطلاحي المتصل بالدراسة؛ إلا باستعراض المعنى اللغوي والاصطلاحي الضيق لكل من "الوسط" و"الرقمية"، ومن ثم محاولة دمجهما اصطلاحيا.

1. تعريف "الوسط" و"الرقمية": يستدل بكلمة "الوسط" في دراسة الحال؛ على ما هو مرادف دلالة لمصطلحات "البيئة، المجال، النطاق"، بمعناها الافتراضي المحض دون التطرق إلى الماديات ذات الصلة. حيث نقول الوسط العلمي أي المجال العلمي الافتراضي؛ الذي يخلقه أشخاص العلم من علماء وفقهاء وأساتذة وطلبة ومثقفون، سيما بخصوص طريقة الحديث بينهم والموضوعات المتداولة وأبعادها الفكرية المحسوسة غير الملموسة...الخ، وكأننا نتحدث عن نمط فكري معين[3]. الأمر الذي يجعل النطاق الرقمي الافتراضي أساسا لدراسة الحال، وليس العناصر المادية المحدثة له.

---

[1] **أنظر:** أنيل كورانا وبدر العلماء، مرجع سابق، ص 07.

[2] **أنظر:** المرجع نفسه، ص 06 و07.

[3] على أن تحمل كلمة "الوسط"، التي مصدرها اسم "وَسَط" وبجمعه يصبح "أوساط"؛ العديد من المعاني اللغوية والاصطلاحية، على حسب موضعها في الجملة وتباين تشكيلها اللغوي وتقلب ورودها بين النكرة والتعريف. فـ"وسَط الشيء" بفتح السين وضم الطاء يعني بين طرفيه وهو جزء منه. وقد تدل كلمة "الوسط" أيضا؛ على أحسن وأفضل الشيء، فخير الأمور أوسطها. كما قد يستدل بها؛ على تصرفات الإنسان، فيقال هذا إنسان وسط -وسطي- لا هو متطرف ولا هو متفتح، =

وأما كلمة "الرقمية"؛ فيقصد بها الأنظمة الرقمية المستحدثة[1]. التي تعمل بها الأجهزة التكنولوجية الحديثة، سيما جهاز الإعلام الآلي وماديات شبكة الاتصال الدولية ومن في حكمهما. التي يعد "النظام الرقمي الثنائي Le système numérique binaire" أبرزها وأهمها[2]، نظرا لكونه أساس عمل هذه الأجهزة المحدثة للوسط الافتراضي، الذي يعد بدوره المسرح الجرمي الحديث محل الدراسة. وبمجرد التفاعل الرقمي معها؛ تقوم بجميع العمليات الممكنة؛ بواسطة إعطائها لكل خانة أحد الرقمين الـ 0 والـ 1، أو الرقمين معا 0.1 –1.0–، أو وفق تسلسل منطقي بأشكال مختلفة، مثل 0.1.0.0.0.1.1.1.0[3].

2. تعريف "الوسط الرقمي": عادة ما يتم تجنب وضع تعريف؛ للوسط أو المجال الذي تتصل به الجرائم محل الدراسة. من منطلق أن أغلب الدراسات تحدد مسرح الجريمة؛ في جهاز الإعلام الآلي فتعرفه كجهاز، أو تربطه بشبكة الاتصال الدولية فتعرفها كشبكة، أو يتم الربط بالمجال الالكتروني فتعرفه بالرجوع إلى جهاز الإعلام الآلي عموما، أو يتم الوصف بالمجال المعلوماتي، فيكتفي الباحث بتعريف المعلوماتية فقط...الخ. إلا أننا في إطار دراسة الحال؛ أردنا أن نتطرق بالتعريف إلى الوسط الرقمي، نظرا لكونه شاملا عن كل ما ذكر وسامحا لتحديد مسرح الجريمة محل الدراسة بدقة[4].

وانطلاقا مما ذكر؛ توجب علينا أن نجد تعريفا للمصطلح الجديد الذي أثرنا إطلاقه على المجال التقني محل الدراسة، –الذي يعد بمثابة المسرح الجرمي الافتراضي–. فنقول أن الوسط الرقمي عموما هو: "البيئة أو المجال أو النطاق الافتراضي المحسوس غير الملموس، الذي تحدثه العناصر الرقمية العاملة بالنظام الثنائي على وجه الخصوص، ويمكن للفرد أن يتفاعل معه أو أن يلج إليه افتراضيا، بعد أن يتعامل مع هذه الأجهزة".

= لا يمينيا ولا يساريا. أو نظرا لما يقوم به كوسيط، ليقدم الحل الوسط. **أنظر في ذلك:** مجمع اللغة العربية، المعجم الوسيط، الطبعة الرابعة، مكتبة الشرق الدولية، القاهرة، مصر، 2004، باب الواو، ص 1031. **وأنظر أيضا:** المعاني الجامع، "معجم كلمات رقمي"، د ت ن، تاريخ التصفح: 19 نوفمبر 2017. الرابط: https://www.almaany.com/ar/dict/ar-ar/وسط.

[1] وتدل كلمة "الرقمية" التي مصدرها اسم "رقْم" وبجمعه يصبح "أرقام"؛ على العديد من المعاني. منها الخط الغليظ والعلامة والختم، ومنها أيضا ما تتصل بالحساب؛ فنقول أن الرقْم هو الرمز المستعمل للتعبير عن أحد الأعداد البسيطة من الـ 0 إلى الـ 9. وكل ما يزيد عن الرقم 9 يعد عددا مركبا من رقمين فأكثر. **أنظر في ذلك:** مجمع اللغة العربية، المرجع نفسه، باب الراء، ص 366. **وأنظر أيضا:** المعاني الجامع، المرجع نفسه.

[2] زيادةً إلى الأنظمة الرقمية الأخرى، المنطوية على؛ "النظام العشري Le système décimal numérique" الذي يعمل بالعدد 10، و"النظام السادس عشر Le système numérique hexadécimal" الذي يقوم على العدد 16. وكذلك "النظام الثماني Le système numérique octal" الذي يعمل بالرقم 8. **أنظر في ذلك:** مروة أديب محمد الجوهري، "الحاسوب والإعجاز العددي في القران الكريم"، مجلة كلية العلوم الإسلامية، جامعة الموصل، العراق، مج 08، عدد 1/15، 2014، ص ص 307-309.

[3] **أنظر:** المرجع نفسه، ص 308 و309.

[4] حيث يشمل الوسط الرقمي؛ كل الأجهزة والنطاقات العاملة بالنظام الرقمي الثنائي المزود بأنظمة المعلومات، على غرار جهاز الإعلام الآلي وشبكة الاتصال الدولية. ويخرج من إطاره؛ كل الأجهزة الالكترونية غير الرقمية -كالثلاجة مثلا-. كما يدقق في أن المقصود بالدراسة في الإطار الرقمي؛ هو الوسط الافتراضي الذي تحدثه الأجهزة الرقمية وليس ماديانها. الأمر الذي سيتضح أكثر؛ عند التطرق إلى الفرع بعد الموالي، والمطلب الثاني الذي يليه المتصل بجرائم الوسط الرقمي.

ثالثا: خصائص الوسط الرقمي

لا يقتصر مصدر الخصوصية التقنية المتصل بمسرح جرائم الوسط الرقمي؛ على ما تطرقنا إليه سابقا في هذا الإطار، وإنما يمتد ليشمل الخصائص التقنية للوسط ذاته، بصورة منفصلة عن خصوصيته. فالخصائص التالية بالطرح؛ تعد جزءا مكونا للخصوصية المراد تبيانها، والتي تضفي الطابع الحديث والمنفصل لمسرح الجرائم محل الدراسة. سيما من حيث اعتباره وسطا بمصدر مادي مركب ومتكامل من جهة، وافتراضيا من جهة أخرى[1].

1. تركيب وتكامل ماديات الوسط الرقمي: لا يمكن الحديث عن الوسط الرقمي؛ من دون التأكيد على ضرورة تفاعل عناصره المادية العاملة بالنظام الرقمي الثنائي، وفق ما بينا سابقا. حيث لكل عنصر منها دور محدد، يتصل إما بمعالجة البيانات ليجعل منها معلومات جاهزة للاستعمال والاستغلال الرقمي أو لتراسلها رقميا بعد معالجتها-كما سنرى لاحقا-. وتتحقق ميزة التركيب والتكامل؛ إذا ما تم الاعتماد على جهاز الإعلام الآلي بالأساس وشبكة الاتصال الدولية بالتبعية[2]. حيث الجهاز هو من يعالج البيانات ليجعلها معلومات، والشبكة هي من تتكفل بإظهارها وضمان تراسلها -إرسال واستقبال- بين مستعملي الأجهزة المختلفة[3].

إلا أن التركيب بين جهاز الإعلام الآلي وشبكة الاتصال الدولية؛ لم يصل إلى الصورة الحالية من التكامل التام؛ إلا بعد اكتشاف بروتوكول "الإنترنت"، المعروف علميا في الإطار التقني ببرتوكول الـــ"Transmission Control Protocol-Internet Protocol" "TCP-IP"[4]، والذي يعمل على التبديل الرقمي بواسطة الحزم المعلوماتية بين مختلف الوصلات[5]. وفي الإطار نفسه وزيادةً على ما ذكر؛ يعد بروتوكول الـــ"TCP-IP"؛ بمثابة الأساس التقني للتحري والتحقيق في المسرح الافتراضي محل الطرح، كما سنرى لاحقا[6].

---

[1] وهذا بالإضافة إلى العديد من الخصائص التي لا يمكن حصرها. حيث -وفق ما بينا سابقا- يعد حديث النشأة، وسريع التطور بديناميكية تفوق التوقع. ويتصف بالشمولية، التي تتضح من خلال الجمع بين الخصائص الموضحة أعلاه. ودون أن ننسى أنه يتصف بكل الخصائص ذات الصلة بعناصره التالية بالدراسة، من سرعة ودقة واستقلالية وعالمية.

[2] ومنه قد لا نتحدث عن التركيب والتكامل بين عناصر الوسط الرقمي، سيما إذا ما تم الاعتماد في إطار الولوج الرقمي؛ على جهاز الإعلام الآلي أو من في حكمه، من دون استعمال شبكة الاتصال الدولية أو من في حكمها. إلا أن الولوج المقصود؛ يظل بحيز جد ضيق، لا يخرج عما يحدثه جهاز الإعلام الآلي من وسط رقمي محلي يدور في إطار الجهاز نفسه.

[3] وقد لا يتم الاعتماد بالضرورة على شبكة الاتصال الدولية؛ وإنما يمكن أن يتم التراسل باستعمال شبكة اتصال داخلية ضيقة -الالترانت- أو شبكة اتصال داخلية موسعة-الاكسترانت-. الأمر الذي سنتطرق له بالتفصيل في الفرع الموالي بالدراسة.

[4] **أنظر:** منال هلال المزاهرة، تكنولوجيات الاتصال والمعلومات، الطبعة الأولى، دار المسيرة للطباعة والنشر والتوزيع، عمان، الأردن، 2014، ص 281 و288.

[5] **أنظر:** ممدوح عبد الحميد عبد المطلب، "استخدام بروتوكول TCP/IP في بحث وتحقيق الجرائم على الكمبيوتر"، مقال رقمي، د ت ن، تاريخ التصفح: 10 أكتوبر 2017، الرابط: http:// ArabLawInfo.com، ص 05.

[6] البروتوكول الذي لنا عودة لطرحه بنوع من التوسع؛ في الفرع التالي بالدراسة.

2. افتراضية الوسط الرقمي: لا يقف التكامل في إطار الوسط الرقمي عند عناصره المادية فقط، وإنما يمتد إلى غاية المجال الافتراضي الذي تحدثه هذه العناصر المتكاملة. فرغم كونه –الوسط الرقمي– واحدا من بين العديد من الأوساط الحيوية من جهة، واعتباره كنتيجة لتفاعل عناصر مادية من جهة أخرى؛ إلا أنه يكتسب الصبغة المعنوية الافتراضية المنفصلة عن الاثنين. إلى درجة بروز من ينادي؛ بضرورة اعتباره أكثر من وسط موازي للعيد من الأوساط التقليدية المادية والمعنوية، حيث يعد وفقهم عالم حديث موازي للعالم الحقيقي بكل أوساطه ومنفصلا عنه.

إلا أننا نرى بعدم سلامة التأسيس المتصل باعتبار الوسط الرقي بمثابة العامة الموازي للعالم الحقيقي، ونؤكد بالعكس من ذلك؛ على أن محل الدراسة –الوسط الرقمي– يعد بمثابة الوسط الافتراضي وليس العالم الافتراضي. وهذا انطلاقا من العيد من الحجج، فالعالم واحد ثابت والأوساط متعددة ومتنوعة في إطار العالم نفسه، وهي التي تتكامل ماديا ومعنويا؛ لتقدم العالم الواحد بكل تنوعاته. ومن جهة أخرى؛ نرى أن من يدعم فكرة العالم الافتراضي؛ يكون قد خلق عالما جديدا موازيا للعالم الحقيقي، مما يتطلب قواعد وأحكام وقوانين مستقلة ومن الطبيعة الافتراضية نفسها، الأمر الذي يعد ضربا من الخيال[1].

ومنه نرى أن الوسط الرقمي يقع عموما بين حاجزين، يتمثل الأول في بوابة الولوج من الوسط المادي الملموس إلى الوسط الرقمي الافتراضي، ويعتبر الثاني بمثابة بوابة الخروج منه والعودة إلى الوسط المادي. فمن يلج إلى الوسط الرقمي افتراضيا؛ هو إنسان يعيش في الوسط الحقيقي، ولكي يقوم بذلك يجب عليه أن يستعمل مجموعة أجهزة مادية ملموسة–المتمثلة في عناصر الوسط الرقمي التالية بالدراسة–. إلا أنه يمكن أن نتصور العديد من النتائج المترتبة عن الولوج إلى الوسط الرقمي والتفاعل معه، منها ما قد تأخذ الطابع الافتراضي ومنها ما قد تكون مادية الأثر، كما قد تتصف بالاثنين معا.

يتضح جليا من خلال ما تم طرحة في إطار تحديد مفهوم الوسط الرقمي عموما؛ أننا بصدد دراسة وسط حديث مركب من عناصر مادية تتمثل في الأجهزة الرقمية ذات الصلة –سيما جهاز الإعلام الآلي وشبكة الاتصال الدولية–، التي بتفاعلها تحدث وسطا افتراضيا بنطاق محدد. ومنه سنعمل في الفرعين التاليين بالدراسة؛ على البحث في العناصر المادية للوسط الرقمي بالأساس، والنطاق الافتراضي الذي تحدثه هذه العناصر بالتبعية.

---

[1] كما أن ما يدفع للتساؤل في هذا الإطار؛ ينطوي على مدى إمكانية اعتبار الوسط الرقمي وسطا متكاملا مع باقي الأوساط التقليدية المادية والمعنوية. حيث نرى في ذلك؛ أنه لا حدود للوسط الرقمي، وهذا نظرا لتجاوزه كل الحواجز الفاصلة بين الأوساط التقليدية المعروفة، عن طريق رقمنة أغلب مجالات الحياة-إن لم نقل جلها-، وإصباغ عليها صبغة حديثة غير مسبوقة. ودليلنا في ذلك؛ يكمن في الاعتراف الضمني من المشرع الجزائري -وحتى المقارن في شاكلة المشرع الأردني مثلا-؛ بعدم قدرته على مواجهة جرائم الوسط الرقمي، بحصر السلوكيات واجبة التجريم ومن ثم تجريمها، ومنه الاتجاه لإعمال مبدأ شرعية عام يعتبر كل جريمة تقليدية اتصل ارتكابها بهذا الوسط؛ سلوكا مجرما. **أنظر في ذلك:** المادة 1/02-أ؛ قانون رقم 09-04، مرجع سابق. **وأنظر أيضا:** المادة 15؛ قانون رقم 2015-27، مؤرخ في 04 ماي 2015، يتعلق بالجريمة الالكترونية، الأردن.

الفرع الثاني: عناصر الوسط الرقمي المحدثة للمسرح الجرمي الافتراضي

يتضح جليا من خلال نظرة سطحية إلى العناصر المُحْدِثَة للوسط الرقمي؛ أنها تتعدد وتتنوع على حسب الغرض المراد تحقيقه، أو الأجيال الرقمية المختلفة. إلا أن الدراسة المعمقة لهذا الوسط؛ تثبت أنه يقوم على عنصرين أساسيين، منطويان على جهاز الإعلام الآلي وشبكة الاتصال الدولية. وما العناصر الرقمية الأخرى؛ سوى أصناف حديثة متصلة بأحد العنصرين المذكورين-الأمر الذي سيتضح أكثر عند دراسة كل عنصر على حدا-.

وتعد عناصر الوسط الرقمي وفق ما طرح؛ الأساس المادي للمسرح الجرمي محل الدراسة. التي بالتفاعل معها تُحدث مجالا افتراضيا، قائما على المعلومات وما يتصل بها. الأمر الذي يفرض قبل التطرق إلى الأثر؛ البحث في الأصل المتصل بجهاز الإعلام الآلي(أولا)، وشبكة الاتصال الدولية(ثانيا).

أولا: جهاز الإعلام الآلي

أصبح لجهاز الإعلام الآلي ومن في حكمه؛ مكانة كبيرة تتزايد بالتوازي مع التقدم التقني والتطور الديناميكي للجهاز نفسه. إلى درجة توقع فريق الخبراء التابع للأمم المتحدة والمعني بإجراء دراسة شاملة عن مشكلة الجريمة السيبرانية-جرائم الوسط الرقمي-[1]؛ أن عدد الأجهزة الموصولة بشبكة الاتصال الدولية سيصل إلى 6 أجهزة للشخص الواحد بحلول سنة 2020[2]. ومنه وجب علينا البحث في هذا الجهاز الهام اجتماعيا والخطير جنائيا؛ من حيث تحديد مفهومه، وإبراز أنواعه.

1. مفهوم جهاز الإعلام الآلي: يعد جهاز الإعلام الآلي ومن في حكمه العنصر الأساس في إطار إحداث الوسط الرقمي الافتراضي، حيث بتخلفه لا يمكن تصور قيام شبكة الاتصال الدولية بدورها-التي توصل بالجهاز، وفق الموصولية الموضحة أعلاه-، ولا حتى قيام الوسط الرقمي أصلا، نظرا لتخلف عنصريه معا. ومن هذا المنطلق المتصل بالأهمية الجوهرية لجهاز الإعلام الآلي في إحداث الوسط الافتراضي؛ نقف عند ضرورة طرح سياق ظهوره وتطوره، وتحديد تعريفه، ومن ثم إبراز أهم خصائصه.

أ- ظهور وتطور جهاز الإعلام الآلي: يعود ظهور أول جهاز إعلام آلي بالمعنى التقني الحسابي إلى سنة 1948 بمدينة "مانشستر-بريطانيا"، والذي عرف باسم "يونيفرسال ماشين The Universal Machine".

---

[1] **أنظر:** فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، "دراسة شاملة عن مشكلة الجريمة السيبرانية والتدابير التي تتخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدي لها"، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، منظمة الأمم المتحدة، فيينا، النمسا، 28 فيفري 2013، ص 02. متوفر عبر الرابط: https://www.unodc.org/unodc/en/cybercrime/index.html.

[2] إلا أن الدراسة المنجزة من فريق الخبراء؛ تظل محدودة في إطار الأجهزة المتصلة بشبكة الاتصال الدولية، دون تلك المتصلة بشبكة الاتصال الداخلية الضيقة-الالترانت- أو شبكة الاتصال الداخلية الموسعة-الاكسترانت-. وحتى دون الأجهزة غير الموصولة تماما بأي شبكة اتصال. الأمر الذي يدفع إلى توقع رقم أكبر بكثير من ذلك المذكور أعلاه، والذي قد يزيد عن الـ 10 أجهزة للشخص الواحد.

ومنه بدأت الأبحاث العلمية ذات الصلة بتطوير الجهاز لجعله تدريجيا يتصل بأغلب مجالات الحياة[1]، الأمر الذي مر حسب آخر الدراسات التقنية؛ بخمسة أجيال إلى غاية وقتنا الحالي.

فاتصل الجيل الأول "1950-1957"؛ بصناعة جهاز "آنياك-الجهاز المتكامل الالكتروني"، القائم على الصمامات الكهربائية المفرغة العاملة بـــ "أشعة الكاثود Cathode Ray"، والتي تتطلب كبر حجم الجهاز والتبريد الهوائي المستمر وقدرة كهربائية كبيرة، كما تتسم بالبطء في انجاز العمليات[2]. الأمر الذي دفع بالباحثين في إطار الجيل الثاني "1958-1964"؛ إلى استبدال الصمامات بـــ "الترانزيستور"، فأصبح الجهاز أصغر حجما وأقل تكلفة ولا يحتاج للتبريد المستمر، ويمتاز بسرعة قد تصل إلى الـــ 100.000 عملية في الثانية. بالإضافة إلى الاعتماد لأول مرة على اللغة الآلية، كلغتي "GOBOL"، و" FORTRAN"[3].

كما قام الباحثون في إطار الجيل الثالث "1965-1970"؛ باختراع "الدوائر المتكاملة المندمجة Integrated Circuits"، التي تحتوي على العديد من قطع "الترانزستور". وبفضلها أصبح الجهاز أصغر، وبسرعة أكبر تصل إلى انجاز ملايين العمليات في الثانية. بالإضافة إلى العمل بلغة آلية جديدة باسم "BASIC"[4]. ولم يخرج الجيل الرابع "1971-1984"؛ على نسق التطور المذكور، حيث أوجد الباحثون؛ ما تسمى بالذاكرات المتعددة على شرائح "السيليكون"-الدوائر واسعة التكامل-، المتصفة بصغر الحجم والقدرة على التخزين. بالإضافة إلى الاعتماد على لغة "PASCAL"، وصناعة الأجهزة الصغيرة"Microchips"، والاعتماد على برامج التشغيل المتطورة في صورة الـــ "WINDOWS"[5].

---

[1] ويرى العديد من المختصين؛ القصور التقني في الدراسات التي تجعل من ظهور جهاز الإعلام الآلي اختراع حديث ومنفصل، انطلاقا من كونه نتاج العديد من الاختراعات العلمية والتطبيقات الرياضية السابقة في الظهور. والتي بدأت بوادرها في أواخر القرن الثامن عشر، عن طريق العالم الأمريكي "هرمان هلرث"، الذي صمم آلة "أوتوماتيكية" تعمل على جدولة المعلومات الإحصائية. وبحلول سنة 1930؛ تم اختراع آلة التحليل التفاضلي، التي تستطيع حساب المعادلات التفاضلية. الأمر الذي تلاه مباشرة-بعد مرور سبع سنوات-؛ اختراع العالم الأمريكي "هوارد آكن" بدعم من شركة "IBM"؛ أول حاسبة رقمية تتكون من 78 جهاز فرعي مترابط. **أنظر في ذلك:** منال هلال المزاهرة، مرجع سابق، ص 104 و105 و116.

[2] **أنظر:** دلال محمد بخيت، (مهارات الحاسب CPIT-100)، محاضرات في إطار الحصول على الرخصة الدولية لقيادة الحسب الآلي "ICDL"، المحاضرة الأولى، كلية الحاسبات وتقنية المعلومات، جامعة الملك عبد العزيز، المملكة العربية السعودية، د ت، ص 14. متوفر عبر الرابط: http:// www.kau.edu.sa/Files/0010566/Subjects./المحاضرة%20الأولى. ppt.

[3] ومنه عملت مختلف الشركات المصنعة للجهاز؛ على إضافة العديد من المميزات التقنية، على غرار جهاز شركة "IBM" تحت رقم "1401"، الذي قدم مرونة كبيرة في التعامل، سيما بخصوص الاعتماد على "الأقراص المغناطيسية الصلبة HARD DICKS". **أنظر في ذلك:** منال هلال المزاهرة، المرجع نفسه، ص 118. **وأنظر أيضا:**

- CARIOU Eric, (Historique et Architecture Générale des Ordinateurs), Cours 4, Université de Pau et des Pays de l'Adour UFR Sciences Pau-Département Informatique, France, s d, p 14. Disponible sur le Lien: http://famouspdf.com/search?q=Historique+et+Architecture+Générale+des+Ordinateurs.

[4] ومنه قامت شركة "IBM"؛ ببناء الشبكات وصناعة أجهزة الإعلام الآلي متوسطة الحجم "Minicomputer". **أنظر في ذلك:** منال هلال المزاهرة، المرجع نفسه، ص 118. **وأنظر أيضا:** دلال محمد بخيت، المرجع نفسه، ص 16.

[5] **أنظر:** عبد الله بن عبد العزيز الموسى، مقدمة في الحاسب الآلي والإنترنت، الطبعة السادسة، مؤسسة شبكة البيانات، المملكة العربية السعودية، 2010، ص 11.

ولعل أهم الأجيال المتصلة بجهاز الإعلام الآلي؛ هو الجيل الخامس والأخير–إلى حد الساعة–. والذي كان أول ظهور له مع بدايات ثمانينات القرن الماضي، حيث تركزت أهم مستجداته؛ على الانتقال من الحساب الرقمي إلى الذكاء الرقمي الاصطناعي"Artificial Intelligence" الذي يمكنه أن يقلد عقل الإنسان. فتم التطوير في كل ما يتصل بالجهاز، سيما تصغير الحجم وتوسيع القدرة على الاستيعاب والتخزين، وزيادة السرعة في معالجة البيانات، إلى حدود تكاد تكون خيالية قد تصل إلى بليون عملية في الثانية[1].

ب– تعريف جهاز الإعلام الآلي: انطلاقا من التطور الديناميكي المستمر لجهاز الإعلام الآلي، وفق ما بينا أعلاه وسابقا بخصوص الأجيال ذات الصلة؛ وقف المختصون بالأساس والمشرع بالتبعية أمام إشكالية وضع تعريف جامع للجهاز نفسه[2]. حيث لم يتطرق القانون الجزائري–اتفاقي، تشريعي وتنظيمي– كأغلب نظرائه[3]؛ إلى جهاز الإعلام الآلي بالتعريف التقني القانوني المنفصل عن تقنية المعلومات[4].

ورغم تطرق المختصين إلى جهاز الإعلام الآلي بالتعريف؛ إلا أن الأمر يظل مقيدا بحسب الجيل والنوع المقصودين. ولو أن أغلب التعريفات التقنية المتاحة؛ تحاول ضمان الحد الأدنى من المعطيات التقنية واجبة الإبراز في التعريف المقدم، سيما تلك المتصلة بأساس عمله وهدف الاعتماد عليه. الأمر الذي بإتباعه يعرف جهاز الإعلام الآلي؛ على أنه: "مجموعة من المعدات "Hardware" والبرمجيات "Software"، المستقلة أو المترابطة ببعضها البعض، والتي لها أدوار مختلفة ومتكاملة، تهدف في الأخير

---

[1] **أنظر:** منال هلال المزاهرة، مرجع سابق، ص 119.

[2] وللجهاز العيد من التسميات الأخرى، سيما تسميتي "الحاسوب" و"الكمبيوتر". **أنظر في ذلك:** م.ش.بلعيد، مدخل إلى هندسة الكمبيوتر، دار الصفحات الزرقاء العالمية، الجزائر، د س ن، ص 12.

إلا أننا فضلنا تسمية جهاز الإعلام الآلي؛ نظرا لسلاستها موضوعيا ولسلامتها لغويا. ولقصور تسمية "الحاسوب"، التي تجاوزها التطور التقني للجهاز بجعل الحساب إحدى عملياته وليس كلها. وأيضا لكون تسمية "الكمبيوتر"؛ بمثابة الترجمة الحرفية للكلمة الانجليزية "computer"، والتي تعني الحاسوب اصطلاحا.

[3] وكاستثناء نجد قانون إمارة دبي المتصل بالمعاملات والتجارة الإلكترونية؛ قد عرف جهاز الإعلام الآلي تحت تسمية الحاسب الآلي؛ على أنه: "جهاز إلكتروني يتعامل مع المعلومات والبيانات بتحليلها وبرمجتها وإظهارها وحفظها وإرسالها واستلامها بواسطة برامج وأنظمة معلومات إلكترونية، ويمكن أن يعمل بشكل مستقل أو مع أجهزة أو أنظمة إلكترونية أخرى". **أنظر في ذلك:** المادة 02؛ قانون رقم 2002-02، مؤرخ في 12 فيفري 2002، يتعلق بالمعاملات والتجارة الإلكترونية لإمارة دبي، الإمارات العربية المتحدة.

[4] حيث نجد من يربط بين جهاز الإعلام الآلي وتقنية المعلومات من حيث التعريف، ولو أنها أشمل من الجهاز مضمونا وتعريفا، إلى درجة أنها أشمل حتى من الوسط الرقمي محل الدراسة. ووفق وجهة نظرنا نراها مرادفة لمصطلح تكنولوجيات الإعلام والاتصال، التي تشمل حسب المشرع الجزائري حتى الاتصال الهاتفي التقليدي، وحسب المختصين تشمل أيضا؛ التيلكس والتلتيكس والفيديوتكس، والأقمار الصناعية، وتكنولوجيات الإعلام...الخ. **أنظر في ذلك:** قانون رقم 09-04، مرجع سابق. **وأنظر أيضا:** منال هلال المزاهرة، المرجع نفسه، ص 41.

وفي الإطار نفسه؛ نجد أن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات-التي صدقت عليها الجزائر سنة 2014-؛ قد عرفت تقنية المعلومات على أنها: "أية وسيلة مادية أو معنوية أو مجموعة وسائل مترابطة أو غير مترابطة تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها وفقا للأوامر والتعليمات المخزنة بها ويشمل ذلك جميع المدخلات والمخرجات المرتبطة بها سلكيا أو لا سلكيا في نظام أو شبكة". **أنظر في ذلك:** المادة 1/02-1؛ مرسوم رئاسي رقم 14-252، مؤرخ في 08 سبتمبر 2014، يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21 ديسبر 2010، (ج ر) عدد 57، صادر بتاريخ 28 سبتمبر 2014.

إلى معالجة البيانات لجعلها في شكل معطيات جاهزة للاستعمال"[1]. كما يمكن أن نعرفه انطلاقا من وظيفته الأساسية وطريقة عمله؛ فنقول أنه: "آلة الكترونية تقوم بمعالجة البيانات وتخزينها واسترجاعها وإجراء العمليات الحسابية والمنطقية بناءً على طلب المستخدم"[2].

ج- خصائص جهاز الإعلام الآلي: لا يقتصر مصدر خصوصية مسرح جرائم الوسط الرقمي؛ على ما تطرقنا إليه سابقا من مفاهيم وأحكام تقنية، وإنما يمتد ليشمل الخصائص التقنية لعناصر الوسط نفسه، بشكل متصل ومكون للخصوصية المقصودة، سيما تلك المتصلة بجهاز الإعلام الآلي. والذي إضافة إلى اعتباره أساس قيام الوسط الرقمي[3]؛ نجده يمتاز أيضا بالسرعة، والدقة المتناهية، والقدرة العالية على التخزين.

تعد السرعة أهم ميزة متصلة بجهاز الإعلام الآلي، حيث لطالما ركز الباحثون في هذا المجال؛ على ضرورة التطوير المستمر للجهاز بخصوص السرعة المعمول بها في إطار معالجة البيانات. الأمر الذي وصل إلى حد إمكانية إجراء بلايين العمليات خلال ثوانٍ معدودة[4].

وعلى العكس من أسس عمل الوسط المادي الذي نعيش فيه؛ الرابط دائما بين السرعة وعدم الدقة، فكلما زادت سرعة معالجة الأمور؛ كلما زادت فرضية كثرة الأخطاء. يعد الربط بين السرقة والدقة على درجة كبيره من التناسق، في إطار المعالجة الرقمية ذات الصلة بالجهاز، الذي رغم السرعة الفائقة في المعالجة؛ إلا أنه يضمن الدقة المتناهية؛ بخصوص النتائج المحصلة[5].

كما أنه بالإضافة إلى السرعة الفائقة والدقة المتناهية في معالجة البيانات؛ يمتاز الجهاز بالقدرة الكبيرة على تخزين المعلومات الناتجة عن معالجة البيانات. الأمر الذي يقلص من المساحة التي كانت مطلوبة سابقا؛ لتخزين المعلومات عبر الدعامة الورقية. كما يمتاز الجهاز أيضا؛ بالمرونة العالية من حيث استرجاع المعلومات المخزنة في حال ضياعها، أو حتى في حال احتراق الجهاز نفسه[6].

---

[1] **أنظر:** أروى يحيى عبد الرحمن الإرياني، أساسيات تحليل وتصميم نظم المعلومات، شعاع للنشر والتوزيع، حلب، سوريا، 2008، ص 33 و34.

[2] **أنظر:** عبد الله بن عبد العزيز الموسى، مرجع سابق، ص 11.

[3] فوفق ما بينا سابقا-سيما بخصوص تركيب وتكامل عناصر الوسط الرقمي-؛ يعد جهاز الإعلام الآلي، بالإضافة إلى ماديات شبكة الاتصال الدولية؛ أهم العناصر المادية المتصلة بخلق الوسط الرقمي الافتراضي محل الدراسة. إلا أنه-منطقيا-لجهاز الإعلام الآلي الدور الأساس في ذلك، حيث لا يمكن تصور قيام شبكة الاتصال الدولية بدورها؛ من دون تفاعلها مع جهاز الإعلام الآلي، كما يمكن للجهاز؛ أن يخلق وسطا رقميا افتراضيا من دون التفاعل مع الشبكة-كما سنرى في الفرع الموالي بالدراسة-.

[4] **أنظر:** أروى يحيى عبد الرحمن الإرياني، المرجع نفسه، ص 34.

[5] **أنظر:** منال هلال المزاهرة، مرجع سابق، ص 124. **وأنظر أيضا:** نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2010، ص 24.

[6] **أنظر:** منال هلال المزاهرة، المرجع نفسه، ص 124.

2. أنواع جهاز الإعلام الآلي: تعتبر العديد من الدراسات القانونية ذات الصلة بالجرائم محل الدراسة؛ أن عبارة جهاز الإعلام الآلي؛ تنصب على الجهاز المكتبي المعروف لدى الجميع، خاصةً من حيث تحديد مكوناته ووظائفه[1]. الأمر الذي يعد قاصرا، فللجهاز العديد من الأنواع انطلاقا من المعيار المعتمد، الذي قد يقوم على عناصر خفية لا تتبين إلا للمختص، متصلة إما بالغرض أو طريقة الأداء[2]. كما قد يؤسس على عناصر خارجية من منطلق الحجم، سيما الأجهزة الكبيرة، والمتوسطة، والصغيرة[3].

أ- **أجهزة الإعلام الآلي كبيرة الحجم** "Mainframe Computers": تتميز أجهزة الإعلام الآلي الكبيرة؛ بقدرتها الكبيرة على القيام بالعمليات الممكنة[4]. التي يمكنها أن تصل إلى 64 "بت" في حجم الكلمة، وبسعة رئيسية تصل إلى 32 مليون رمز. كما لها سرعة تشغيل؛ تقاس بأجزاء من البليون في الثانية الواحدة "نانوثانية". إلا أنها تظل أجهزة غالية الثمن، ولا تستعمل إلا في الشركات والمؤسسات الكبيرة[5].

ب- **أجهزة الإعلام الآلي متوسطة الحجم** "Mini Computers": إضافة إلى الأجهزة العملاقة والكبيرة؛ نجد ما تسمى بالأجهزة المتوسطة. التي لها قدرة تنفيذ عالية نسبيا، بسعة ذاكرة أصلية تبدأ من 256,000 رمز. مع إمكانية التوصل بحجم الكلمات إلى 32 "بت"، وبسرعة تشغيل تصل إلى مليون من الثانية "ميكرثانية". إلا أنه ورغم عدم غلاء ثمنها مقارنة بالأجهزة الكبيرة والعملاقة؛ تظل بعيدة عن الاستعمال الشخصي، حيث تستعمل في إطار المؤسسات الصغيرة والمتوسطة[6].

---

[1] المكونات التي تحصرها أغلب الدراسات القانونية ذات الصلة بجرائم الوسط الرقمي؛ في مكونات إدخال-لوحة تحكم، فأرة...الخ-، ومكونات معالجة وتخزين-وحدة المعالجة المركزية، الذاكرة...الخ، ومكونات إخراج-الشاشة، الطابعة...الخ. **أنظر في ذلك:** نهلا عبد القادر المومني، مرجع سابق، ص 25. **وأنظر أيضا:** عبد اللطيف معتوق، (الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن)، مذكرة مكملة لنيل شهادة الماجستير في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، الجزائر، 2012، ص 21 و22.

إلا أننا نرى غير ذلك، حيث تختلف مكونات الأجهزة محل الدراسة؛ بحسب نوع الجهاز نفسه. على غرار اختلاف مكونات الجهاز المكتبي عن المحمول مثلا. وهو ما يتباين بحسب الحجم الدائر بين العملاق والكبير والمتوسط والصغير.

[2] حيث تقسم **الأجهزة حسب معيار الغرض؛** إلى أجهزة بغرض عام، التي يمكن للجميع أن يعتمد عليها لتحقيق النتائج المرجوة، وأجهزة بغرض خاص، تصمم لانجاز عمليات رقمية محددة، على غرار تلك المعتمدة في غرف المستشفيات، ومقرات الشركات...الخ. وتقسم أيضا **الأجهزة وفق معيار طريقة الأداء؛** إلى أجهزة قياسية "Analog Computers"، تعمل بالإشارات التماثلية دون الرقمية -هي خارجة عن إطار الدراسة-، وأجهزة رقمية "Digital Computers" العاملة بالنظام الرقمي الثنائي كما بينا سابقا، والأجهزة المهجنة "Hybird Computers"؛ الجامعة بين سمات الأجهزة الرقمية والقياسية. **أنظر في ذلك:** منال هلال المزاهرة، مرجع سابق، ص 120 و121.

[3] ركزنا على معيار الحجم في تحديد أنواع الجهاز؛ نظرا لكونه الظاهر بسهولة لغير المختص تقنيا من جهة، ولانتشار الأجهزة متعددة الأحجام لدى العامة من جهة أخرى. خاصةً وأن العديد؛ يخلط بين الهاتف المحمول التقليدي والهاتف المحمول الرقمي، بخصوص مدى اعتباره منشئا للوسط الرقمي المتصل بالجرائم محل الدراسة-كما سنرى لاحقا-.

[4] ولو أنه تتفوق عليها في ذلك الأجهزة العملاقة "Super Computers"، التي لها قدرة هائلة على تنفيذ العديد من البرامج في الوقت نفسه وبسرعة هائلة. مع إمكانية ربطها بالعديد من المكونات الطرفية. والقدرة الكبيرة على التخزين. إلا أنها تبقى باهظة الثمن، الذي يقدر بملايين الدولارات. **أنظر في ذلك:** دلال محمد بخيت، مرجع سابق، ص 21.

[5] **أنظر:** منال هلال المزاهرة، المرجع نفسه، ص 121.

[6] **أنظر:** المرجع نفسه، ص 122. **وأنظر أيضا:** عبد الله بن عبد العزيز الموسى، مرجع سابق، ص 13.

ج- أجهزة الإعلام الآلي صغيرة الحجم والدقيقة "Mini and micro Computers": تعد الأجهزة الصغيرة؛ الأهم والأشهر على الإطلاق، نظرا لقلة تكلفتها وتناسب سرعتها وسعتها ومظهرها الخارجي وخاصةً حجمها؛ مع المتطلبات الشخصية للأفراد. ومن أصنافها نجد؛ جهاز الإعلام الآلي المكتبي محل الاستعمال الشخصي "Personal Computers"، والجهاز المحمول "Lap Top"، والجهاز المفكرة "Netbook-Ultrabook"، وجهاز الجيب العامل بالنظام الرقمي "Palm"، الذي يدخل في إطاره الهاتف الذكي بكل أنواعه[1]. بالإضافة إلى الأجهزة الدقيقة؛ العاملة بالمعالج الدقيق كوحدة معالجة رئيسية ضئيلة التكلفة[2].

ثانيا: شبكة الاتصال الدولية

اكتسبت شبكة الاتصال الدولية منذ ظهورها وبدايات تطورها؛ طابع الأهمية لدى العام والخاص، سيما منذ أن أصبحت متاحة للعامة بتكلفة معقولة ومرونة في التعامل. الأمر الذي توقع بخصوصه فريق الخبراء، التابع للأمم المتحدة والمعني بإجراء دراسة شاملة عن مشكلة الجريمة السيبرانية-جرائم الوسط الرقمي-؛ أن عدد الأجهزة المتصلة بالشبكة سيزيد عن عدد سكان الأرض بـــ 6 مرات[3]. ومن منطلق الأهمية الكبيرة لشبكة الاتصال الدولية؛ وجب التوقف عند تحديد مفهومها، وإبراز نظام عملها.

1. مفهوم شبكة الاتصال الدولية: تعد الشبكة أساس تطور الجريمة في الوسط الرقمي، بعد أن ظهرت في إطار النطاق الافتراضي الضيق لجهاز الإعلام الآلي. ويمكن القول؛ أن أساس طابع خصوصية التحري والتحقيق في الجرائم محل الدراسة؛ يعود تقنيا إلى الطابع المعقد لنطاق الشبكة الافتراضي كمسرح للجريمة، سيما بالنظر إلى ولوجها في جل مجالات الحياة العامة والخاصة. وعليه نتساءل عن الأساس المفاهيمي لهذه الشبكة، من حيث ظهورها وتطورها، وتعريفها، وأبرز خصائصها.

أ- ظهور وتطور شبكة الاتصال الدولية: لم تبرز ثورة الاتصال الشبكي هكذا صدفة؛ وإنما كان لها مسار ظهور وتطور وفق العديد من المراحل. وتعد مقتضيات الحرب الباردة بين الـــ"و.م.أ" والاتحاد السوفيتي؛ الدافع الأساس لظهورها. حيث حثت مؤسسة "راندا" الأمريكية المهتمة بالحرب الباردة؛ على ضرورة استحداث وسيلة اتصال لها القدرة على الصمود أمام أي هجوم نووي سوفيتي. الأمر الذي تبنته وزارة الدفاع الأمريكية، بتأسيسها لوكالة الأبحاث المتقدمة "Advanced Research Projects Agency-ARPA". التي أنشأت أول شبكة اتصال حديثة سنة 1969 تحت اسم "ARPANET"[4].

---

[1] **أنظر:** منال هلال المزاهرة، مرجع سابق، ص 122.

[2] **أنظر:** دلال محمد بخيت، مرجع سابق، ص 24. **وأنظر أيضا:** عبد الله بن عبد العزيز الموسى، مرجع سابق، ص 13.

[3] **أنظر:** فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، مرجع سابق، ص 02.

[4] **أنظر:** محمد طارق الخن، "جرائم المعلوماتية (الأحكام الموضوعية و الإجرائية)"، ورقة عمل مقدمة إلى ورشة عمل حول التشريعات الالكترونية السيبرانية وآلية تطبيقها، دمشق، سوريا، فيفري 2015، ص 01. **وأنظر أيضا:** منال هلال المزاهرة، مرجع سابق، ص 282 و283.

إلا أن الاتصال عبر الـــ "ARPANET"؛ ظل محصورا بين أربع نقاط فقط، المنطوية على جامعة "California" في "Los Angeles" و"Santa Barbara"، وجامعة "Botao " ومعهد " Stanford" للأبحاث". ولم يتوسع هذا النطاق إلا بحلول سنة 1972؛ ليشمل حوالي 40 نقطة داخل "الو.م.أ"، بالإضافة إلى دولتي النرويج وانجلترا. الأمر الذي اعترضته العديد من المشاكل بخصوص التحكم في النقل، ما أدى سنة 1974 إلى استحداث بروتوكول الـــ "TCP" عن طريق العالمين "فينتون سيرف" و"روبرت كان". ومنه عرف أول موقع رقمي خاص، أنشأته شركة " Digital Equipment "[1].

ونظرا لازدياد الضغط على الـــ "ARPANET"؛ انتقلت سنة 1984؛ إدارة الشبكة من وكالة الأبحاث المتقدمة للدفاع "ARPA" إلى مؤسسة العلوم القومية الأمريكية "National Science Foundation-NSF". التي قامت بتقسيم الشبكة إلى قسمين، فجعلت الأولى ذات استعمال علمي ومؤسساتي نسبتا إليها تحت تسمية "NSFNET"، وخصصت الثانية للاستعمال العسكري تحت اسم "MILNET". وبحلول سنة 1990؛ أصبحت الشبكة متاحة للعامة تجاريا وخدماتيا، تحت اسم "INTERNET"[2]. وعلى العموم؛ لم تستفد الجزائر من الشبكة إلا بحلول شهر مارس 1994[3].

ب- تعريف شبكة الاتصال الدولية: لم يتطرق القانون الجزائري –اتفاقي وتشريعي وتنظيمي– في البداية؛ إلى شبكة الاتصال الدولية بالتعريف، سواءً بالتسمية ذاتها أو بأية تسمية أخرى[4]. حيث اكتفى على عكس

---

[1] **أنظر:** منال هلال المزاهرة، مرجع سابق، ص 282 و283. **وأنظر أيضا:** مليكة عطوي، (الحماية القانونية لحقوق الملكية الفكرية على شبكة الإنترنت)، أطروحة لنيل درجة الدكتوراه في علوم الإعلام والاتصال، كلية العلوم والاتصال، كلية العلوم السياسية والإعلام، جامعة دالي إبراهيم، الجزائر، 2010، ص 30 و31.

[2] **أنظر:** مليكة عطوي، المرجع نفسه، ص 31. **وأنظر أيضا:** محمد طارق الخن، مرجع سابق، ص 01.

[3] حيث كان مركز البحث والإعلام العلمي والتقني "CERIST" المؤسس عام 1986؛ السباق وطنيا في الاستفادة من الشبكة سنة 1994. إلا أن الارتباط الشبكي؛ كان عن طريق ايطاليا وبسرعة جد ضعيفة تقدر بـ 9600 حرف في الثانية "9,6 KO". الأمر الوارد في إطار مشروع تعاون منظمة اليونسكو لإقامة شبكة افريقية "Réseau d'Information Africain-RINAF". ومنه أخذت سرعة الشبكة تتطور تدريجيا، إلى أن أصبحت تقاس بـ"الميغابيت-Méga Bytes". سيما بعد الربط سنة 1998 مع واشنطن؛ عبر القمر الصناعي بقدرة 01 ميغابيت "01 Méga Bytes". **أنظر في ذلك:** إبراهيم بختي، "الإنترنت في الجزائر"، مجلة الباحث، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة ورقلة، الجزائر، عدد 01، 2002، ص 31.

ولم يصبح ممكنا لغير الـ "CERIST" الاستفادة من الشبكة؛ إلا بعد صدور المرسوم التنفيذي 98-257، الذي يحدد شروط وكيفيات وضع واستغلال الشبكة. **أنظر في ذلك:** مرسوم تنفيذي رقم 98-257، مؤرخ في 25 أوت 1998، يضبط شروط وكيفيات إقامة خدمات "أنترنات" واستغلالها، (ج ر) عدد 63، صادر بتاريخ 26 أوت 1998. معدل ومتمم بمرسوم تنفيذي رقم 2000-307، مؤرخ في 14 أكتوبر 2000، (ج ر) عدد 60، صادر بتاريخ 15 أكتوبر 2000.

[4] تختلف وتتعدد التسميات التي تطلق على الشبكة، حيث بالاعتماد على الترجمة الحرفية للكلمة الانجليزية "Internet"؛ يمكن أن نسميها بـ"الإنترنت". وبالاعتماد على الترجمة الاصطلاحية؛ قد نسميها بـ "شبكة الاتصال الدولية" انطلاقا، من فهم كلمة "Internet" على أنها اختصار لكلمتي "International Network". كما قد نسميها بـ "الشبكة البينية" أو "شبكة الشبكات" أو "شبكة الاتصال" أو "الشبكة العنكبوتية"؛ انطلاقا من فهم كلمة "Internet" على أنها؛ اختصار لكلمتي "network - شبكة" و"Inter - بين". أنظر في ذلك: منال هلال المزاهرة، المرجع نفسه، ص 280. **وأنظر أيضا:**

- Larousse-Encyclopédie en Ligne, Internet, s d p, Date d'Accès: 30 novembre 2017. Lien: http://www.larousse.fr/encyclopedie/divers/Internet/125060.

إلا أننا نستبعد أغلب هذه التسميات ونفضل منها تسمية **"شبكة الاتصال الدولية"**. التي لها دلالة اصطلاحية دقيقة، تبتعد عن الترجمة الحرفية من جهة، وبفضلها نحصر مجال الدراسة في الشبكة ذات البعد العالمي من جهة أخرى.

القوانين المقارنة[1]؛ بتعريفه للبعض من مشتملات خدمات الشبكة التي سماها بـــ "الانترنات"، مثل خدمة "الويب" وخدمة البريد الرقمي–الإلكتروني–...الخ[2]. إلا أنه رجع سنة 2018 بقانون البريد والاتصالات الالكترونية –الجديد–؛ ليعرفها تحت تسمية "الإنترنت" على أنها: "شبكة معلوماتية عالمية تتشكل من مجموعة شبكات وطنية وإقليمية وخاصة، موصولة فيما بينها عن طريق بروتوكول الاتصال IP وتعمل معا بهدف تقديم واجهة موحدة لمستعمليها"[3].

وفي السياق نفسه؛ تتعدد وتتنوع التعريفات التقنية للشبكة، على حسب المنظور التقني المعتمد. والتي تقوم في أغلبها؛ على عنصري الاتصال عن بعد وضرورة الاعتماد على جهاز الإعلام الآلي. ولعل أبرزها تعرفها على أنها: "شبكة معلوماتية دولية ووطنية وجهوية، تسمح بربط أجهزة الإعلام الآلي مع بعضها البعض افتراضيا، في شكل شبكة الطرقات المتداخلة"[4]. أو باعتبارها: "نظام من الشبكات الحاسوبية يصل بين حواسيب حول العالم ببروتوكول موحد هو بروتوكول انترنت"[5].

ج– خصائص شبكة الاتصال الدولية: تتميز شبكة الاتصال الدولية؛ بالعديد من الخصائص التقنية، التي بتفاعلها مع جهاز الإعلام الآلي؛ تعمق من خصوصية الوسط الرقمي، وبالتبعية تعقد من عملية مواجهة الجرائم ذات الصلة موضوعيا وإجرائيا، خاصةً في إطار ممارسة أعمال التحري والتحقيق. ولعل أهم ما يميز شبكة الاتصال الدولية؛ نجد أنها عالمية، ومستقلة، وتنتج وسطا افتراضيا.

---

[1] سيما القانون الإماراتي الاتحادي الذي عرفها تحت تسمية "الشبكة المعلوماتية". واعتبرها بمثابة الترابط بين البرامج المعلوماتية ووسائل تقنية المعلومات، وبغرض تبادل المعلومات بعد الدخول؛ يمكن القول أنه قد استبعد الاتصال الهاتفي التقليدي ومن في حكمه، وضم كل أشكال الاتصال الشبكي "أنترت-الترانت-اكسترانت". **أنظر في ذلك:** المادة 1/01-7؛ مرسوم بقانون اتحادي رقم 2012-05، مؤرخ في 13 أوت 2012، يتعلق بمكافحة جرائم تقنية المعلومات، الإمارات العربية المتحدة، معدل ومتمم.

[2] **أنظر:** المادة 02؛ مرسوم تنفيذي رقم 98-257، مرجع سابق.

ولو أنه وضع سنة 2009؛ تعريفا لما هو أشمل من الشبكة، تحت تسمية "الاتصالات الالكترونية"، الشاملة لمختلف الشبكات الرقمية من "إنترت-الترانت-اكسترانت"، وكذلك تضم وسائل الاتصال التقليدية غير الرقمية كـ"الهاتف" و"الفاكس". حيث اكتفي بالقول؛ أنه يعتمد أي وسيلة الكترونية تمكن من تراسل العلامات أو الإشارات أو الكتابات أو الصور أو الأصوات. **أنظر في ذلك:** المادة 1/02-و؛ قانون رقم 09-04، مراجع سابق.

وتعد **شبكة الاتصال الداخلية الضيقة "الالترانت"** بمثابة؛ الشبكة التي تستعمل لنقل المعلومات بين نقاط محددة متواجدة داخل الجهة الواحدة، وعادة ما يعتمد عليها بين مكاتب الشركة أو الإدارة الواحدة. كما تعتبر **شبكة الاتصال الداخلية الموسعة "الاكسترانت"**؛ امتدادا للأولى، حيث بفضلها يتم إيصال الشبكات الداخلية المتعددة ببعضها البعض، مثل إيصال الشبكات الداخلية لمجموعة شركات ببعضها البعض. **أنظر في ذلك:**

- Logistique Seine-Normandie et La Région Haute-Normandie, "Les nouveaux Usages d'Internet et de L'informatique au Service de Votre Entreprise", France, s d, p 02. Disponible sur le Lien: https://www.logistique-seine-normandie.com/accueil.html.

[3] التعريف الذي نجده قد ركز على الربط الشبكي المبني على بروتوكول الإنترنت، الضامن لواجهة موحدة يستعملها رواد الشبكة. **أنظر في ذلك:** المادة 1/10-5؛ قانون رقم 18-04، مؤرخ في 10 ماي 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، (ج ر) عدد 27، صادر بتاريخ 13 ماي 2018.

[4] **أنظر:**
- Logistique Seine-Normandie et La Région Haute-Normandie, Idem, p 01.

[5] **أنظر:** منال هلال المزاهرة، مرجع سابق، ص 281.

تمتاز الشبكة بالبعد العالمي دون سواها من عناصر الوسط الرقمي، فرغم اقتصارها في البداية -كما تطرقنا سابقا-؛ على الولايات المتحدة الأمريكية، إلا أنها أصبحت منذ ربطها لأول مرة بدولتي النرويج وانجلترا سنة 1973؛ ذات بعد عالمي، أخذ في الاتساع إلى غاية بلوغ عدد المتصلين بالشبكة سنة 2017؛ إلى 3,81 مليار فرد موزعين عبر أغلب دول العالم، ما يشكل 51 ٪ من سكان العالم[1].

كما أن الشبكة وعلى الرغم من اتصالها الوثيق بدولة الولايات لمتحدة الأمريكية، من منطلق كونها ذات الفضل في إنشائها وتطويرها-كما درسنا سابقا-. إلا أنها في الحقيقة تعمل تحت إشراف جهات غير حكومية، التي جعلت منها وسطا افتراضيا متاحا للجميع، من دون استثناء، وهي المنطوية على جمعية الإنترنت؛ التي تهتم بتنسيق عمليات الربط والاتصال بين الشبكات. والاتحاد الدولي للاتصالات "ITU"؛ الذي يشرف على منظومة الاتصالات العالمية. ومنظمة الأيكان "ICANN"؛ التي تعد الجهة المشرفة على أسماء المواقع وعناوينها[2].

ورغم اعتبار شبكة الاتصال الدولية وجهاز الإعلام الآلي؛ العنصرين الأساسيين المحدثين للوسط الرقمي، إلا أن الشبكة تمتاز عن الجهاز؛ بكونها افتراضية بالأساس. حيث يعد الجهاز عنصرا ماديا يخلق وسطا افتراضيا، وأما الشبكة فظاهرها افتراضي متصل بالجهاز -ظاهرها العام بغض النظر عن ماديات الربط التالية بالدراسة-. ومنه يلج الفرد المتعامل معها؛ من الوسط المادي الملموس إلى الوسط الافتراضي الشبكي المحسوس، المنفصل عن نظيره المادي؛ بمجرد تفاعله ماديا مع جهاز الإعلام الآلي المتصل بالشبكة[3].

2. نظام عمل شبكة الاتصال الدولية: حتى يصل الشخص إلى التفاعل مع شبكة الاتصال الدولية، عن طريق استعمالها واستغلالها-بالسلوكيات المشروعة أو غير المشروعة-؛ يجب أن يتوفر على ما تسمى بالموصولية الشبكية. التي لا يمكن تحقيقها؛ إلا بإتباع نظام عمل محدد دوليا بالأساس ووطنيا بالتبعية. حيث يجب أن يتم ربط الدولة بالشبكة الدولية وفق أحكام تقنية وتنظيمية، مع ضرورة إيصال الشخص بعد ذلك بالشبكة في إطار الدولة نفسها.

أ- ربط الدولة بالشبكة الدولية: قبل الحديث عن اتصال الشخص بشبكة الاتصال الدولية؛ يجب أن تكون الدولة التي هو متواجد على أراضيها؛ مرتبطة بالشبكة نفسها. الأمر الذي يتحقق إما بطريقة الكابل

---

[1] **أنظر:** - COEFFE Thomas, Chiffres Internet – 2017, Blog du Modérateur, Date de Publication: 01 Avril 2017, Date d'Accès: 31 novembre 2017. Lien: https://www.blogdumoderateur.com/chiffres-internet/.

[2] **أنظر:** محمد طارق الخن، مرجع سابق، ص 05.

[3] كما عبر عنها الأستاذ "كازينوف" في سبعينات القرن الماضي؛ "بمؤسسة الحضور". **أنظر في ذلك:** مليكة عطوي، (الإنترنت والملكية الفكرية)، مذكرة لنيل شهادة الماجستير في علوم الإعلام والاتصال، كلية العلوم والاتصال، جامعة الجزائر 3، الجزائر، 2004، ص 23.

البحري أو الأقمار الصناعية. حيث يمكن للدولة عبر المخرج الدولي "Gate way"؛ أن ترتبط بالشبكة الدولية؛ من خلال إيصال كابلات الألياف البصرية بالكابل البحري لدولة سبق لها الارتباط[1].

كما يمكن أن يتم ربط إقليم الدولة بالشبكة الدولية؛ عن طريق الأقمار الصناعية كبديل أو كمكمل عن الربط الكابلي. إلا أن العمل بذلك يظل جد محدود على مستوى العالم، سيما في الجزائر. وهذا نظرا لغلاء تكلفة الربط بالشبكة عن طريق الساتل، ولقلة جودتها وسعتها، حيث سعة أكبر قمر صناعي لا تزيد عن "GB 01"، بينما الكابل البحري يحمل سعة 6000 قمر صناعي[2]. وعادة ما يتم اللجوء إلى العمل بهذا النمط؛ لتغطية المناطق النائية غير القابلة لتنصيب محطات أرضية والمد بكابل الألياف البصرية[3].

ب- إيصال الأشخاص بالشبكة الدولية: بعد أن ترتبط الدولة بشبكة الاتصال الدولة وفق ما بينا أعلاه؛ تفتح هذه الأخيرة إمكانية الاتصال بها للأشخاص المتواجدين على إقليمها. الأمر الذي قامت به الجزائر تدريجيا؛ انطلاقا من سنة 1998 كما بينا سابقا. وعلى العموم لا يمكن الاتصال بالشبكة؛ إلا بتوفر مجموعة من الشروط التقنية، التي تختلف على حسب طريقة الاتصال، الدائرة بين الثابتة والمتنقلة.

فللاتصال الشبكي الثابت؛ يتوجب توفر جهاز إعلام آلي، وخط هاتفي ثابت مزود بالاشتراك في الشبكة. بالإضافة إلى ما يسمى بالـــ "مودم Modem"، الذي يحول البيانات الداخلة إلى الجهاز؛ من التماثلية إلى الرقمية، ليعيدها إلى التماثلية قبل خروجها منه[4]. ويمكن الاعتماد على الاتصال الشبكي المتنقل-أجيال الإنترنت "3G و4G...الخ"-. والتي تحتاج إلى جهاز محمول مناسب تقنيا-الجهاز المحمول والمفكرة والهاتف الذكي...الخ-. بالإضافة إلى شريحة اتصال مزودة بخدمة الشبكة[5].

---

[1] وعملت الجزائر سنة 1994؛ بالربط الكابلي مع ايطاليا بسعة "9,6 KO"، التي تم تطوريها فيما بعد لتصل إلى "80 GB". مع إضافة كابل بين عنابة ومارسيليا بسعة "630 GB"، وآخر استثنائي بين عنابة وبنزرت بسعة "40 GB". كما تعتمد الجزائر منذ فيفري 2017؛ على كابل جديد بسعة "435 GB" يربط فالنسيا الاسبانية بوهران والعاصمة. **أنظر في ذلك:** ب. حكيم، **"الجزائر تؤمن شبكة الإنترنت عبر الكابل البحري من اسبانيا"**، تاريخ النشر: 05 جانفي 2017، تاريخ التصفح: 10 أكتوبر 2017، الرابط: /الجزائر-تؤمن-شبكة-الانترنت-عبر-الكابل-البحري-الجديد-من-اسبانيا http://www.eco-algeria.com/content. **وانظر أيضا:** جريدة البلاد، **"كابل الانترنت المتضرر.. اتصالات الجزائر تصدر بينا توضيحيا حول عملية تصليحه"**، تاريخ النشر: 14 أفريل 2017، تاريخ التصفح: 10 أكتوبر 2017، الرابط:
http://www.elbilad.net/artice/detail?titre=حول-عملية-إصلاحية&=كابل-الإنترنت-المتضرر-إتصالات-الجزائر-تصدر-بيانا-69124.

[2] **أنظر:** أحمد عبد القادر، **"إنترنت الأقمار الصناعية وإنترنت الكابلات البحرية لا يتعارضان ولكن يتكاملان"**، تاريخ النشر: 11 أفريل 2009، تاريخ التصفح: 25 نوفمبر 2017، الرابط: https://aitnews.com/2009/02/11/9709.

[3] وأكد المدير العام لاتصالات الجزائر الفضائية؛ شهر أفريل 2015. أن الجزائر ستعمل بهذه التقنية لتوفير الشبكة بالمناطق النائية المعزولة. **أنظر في ذلك:** م. روابح، **"الإنترنت متوفرة عبر الساتل للمواطنين قريبا"**، تاريخ النشر: 17 أفريل 2015، تاريخ التصفح: 20 نوفمبر 2017، الرابط: https://www.echoroukonline.com/ara/articles/240116.html.

[4] وتعتبر كلمة "Modem"؛ بمثابة الاختصار للكلمتين الانجليزيتين "Modulation and Demodulation"، أي **"التعديل وفك التعديل"**. **أنظر في ذلك:** منال هلال المزاهرة، مرجع سابق، ص 286.

[5] مع العلم أننا لا نحتاج إلى الـ **"مودم Modem"** في هذه الحالة؛ نظرا لوصول المعلومات إلى الجهاز وخروجها منه في شكلها الرقمي. **أنظر في ذلك:** ويكيبيديا، **"جيل رابع(اتصالات لا سلكية)"**، تاريخ النشر-آخر تعديل-: 24 سبتمبر 2017، تاريخ التصفح: 04 أكتوبر 2017، الرابط: https://ar.wikipedia.org/wiki/جيل_رابع_(اتصالات_لاسلكية).

الفرع الثالث: نطاق الوسط الرقمي الافتراضي كمسرح للجريمة

تختلف النظرة إلى الوسط الرقمي؛ على حسب طبيعة وهدف الدراسة ذات الصلة. حيث عادةً ما يتم دمج النطاق الافتراضي للوسط محل الطرح؛ في الإطار نفسه المتصل بعناصره السابقة بالذكر. ومنه نتحدث عن الرقمية التقنية على إجمالها. الأمر الذي نجده متبعا في العديد من الدراسات القانونية ذات الصلة بالجرائم محل الدراسة، وكأن عناصر الوسط الرقمي المادية والمعنوية-من دون الفصل بينها-؛ هي من تعد مسرحا للجريمة.

إلا أننا نفرق في إطار تحديد مسرح الجريمة؛ بين العناصر المادية للوسط الرقمي، والنطاق المعنوي الافتراضي الذي تحدثه. حيث في الحالة الأولى؛ نكون بصدد ارتكاب جريمة في المسرح المادي المعروف، وفي الحالة الثانية نصبح أمام ارتكابها في المسرح الرقمي الافتراضي-كما سنرى لاحقا-. وعليه وجب التحديد التقني للنطاق الافتراضي لجهاز الإعلام الآلي(أولا)، ولشبكة الاتصال الدولية(ثانيا).

أولا: النطاق الافتراضي المتصل بجهاز الإعلام الآلي

يعد جهاز الإعلام الآلي بكل أنواعه المذكورة سابقا، ومكوناته ذات الصلة؛ أهم العناصر المادية المحدثة للوسط الرقمي كمسرح جرمي افتراضي. حيث بمجرد التفاعل الرقمي للإنسان مع المكونات المادية للجهاز؛ يكون قد ولج إلى نطاقه الافتراضي المنفصل جنائيا عن الجهاز. وهو الأمر الذي يؤكد على خصوصية التحري والتحقيق في الجرائم ذات الصلة. ويتكون النطاق الافتراضي المقصود؛ من أنظمة المعلومات الرقمية، والمعلومات الرقمية ذات الصلة.

1. أنظمة المعلومات الرقمية: تعد أنظمة المعلومات؛ البوابة الفاصلة بين الشقين المادي والمعنوي لجهاز الإعلام الآلي. حيث لايمكن تصور قيام الجهاز بمعالجة البيانات و/أو تراسل المعلومات الرقمية؛ من دون الاعتماد على أنظمة المعلومات. والتي لا نكاد نجد لها تعريفا جامعا، إن بالمنظور التقني أو القانوني، نظرا لاختلاف الأساس المعتمد في التعريف، من حيث العمل بالمضمون الضيق المتصل بأنظمة التشغيل فقط، أو المضمون الواسع الذي يضم زيادة عن ذلك؛ البرامج التطبيقية[1]. أو المضمون الفضفاض الذي يضم بالإضافة إلى كل ما ذكر؛ المواقع والبرامج ذات الصلة بشبكة الاتصال الدولية[2].

---

[1] حيث تعرف أنظمة المعلومات وفق **المعيار الضيق-أنظمة التشغيل-**؛ على أنها: "البرامج القاعدية التي تشغل الآلة عن طريق تفسير الأوامر الآتية من المستعمل وتحولها إلى إشارات تشغل بها المعدات". كما تعرف وفق المعيار الواسع**-أنظمة التشغيل والبرامج التطبيقية-**؛ على أنها: "مجموعة البرامج المنفصلة أو المتصلة التي تؤدي إلى انجاز العمليات الرقمية عبر الجهاز". وعلى العموم يمكن تصور جهاز بنظام تشغيل فقط، لكن لايمكن تصور جهاز ببرامج تطبيقية فقط. نظرا لوجوب تثبيت البرامج في إطار أنظمة التشغيل. **أنظر في ذلك:** م.ش. بلعيد، مرجع سابق، ص 18 و19.

[2] تعود فكرة التعريف الفضفاض بعيدا عن الدراسات التقنية؛ إلى الفقه الجنائي الفرنسي. حيث اعتمد المعيار الفضفاض؛ لتعريف أنظمة المعالجة الآلية للمعطيات في إطار الجرائم الماسة بها. ويرى الأستاذ **"جون دفراز"** في هذا الصدد؛ أن البريد الالكتروني وكل ما يدور حول شبكة الاتصال الدولية ووظائفها يعد من قبيل الأنظمة المعلوماتية. **أنظر في ذلك: =**

رجوعا إلى القانون الجزائري نجده؛ قد اعتمد في طرحه وتعريفة لأنظمة المعلومات على التسمية والمضمون الفضفاضين. حيث عرفها تحت تسمية المنظومة المعلوماتية[1]، بأنها: "أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين"[2]. حيث يبدوا المضمون الفضفاض واضحا؛ من خلال التسمية الواردة بمصطلح المنظومة وليس النظام، حيث لا يمكن الوصول إلى منظومة معلوماتية؛ إلا بالانطلاق من نظام التشغيل بالأساس والاعتماد على البرامج التطبيقية بالتبعية، والتي قد تكون بغرض المعالجة الرقمية و/أو التراسل الشبكي. بالإضافة إلى الإشارة في التعريف صراحة؛ إلى إمكانية اعتباره نظاما منفصلا –نظام التشغيل–، أو مجموعة أنظمة–نظام التشغيل والبرامج التطبيقية–[3].

2. المعلومات الرقمية: تعد المعلومات الرقمية؛ أهم مكونات النطاق الافتراضي للوسط الرقمي بصفة عامة، ومسرح جرائم الوسط نفسه بصفة خاصة. حيث تعمل أنظمة المعلومات المذكورة أعلاه وسابقا؛ على معالجة البيانات لجعلها معلومات، ومن ثم التعامل معها عن طريق تخزينها وتراسلها. كما ينحصر موضوع التراسل الرقمي عبر شبكة الاتصال الدولية؛ في المعلومات الرقمية باختلاف أشكالها. ومنه وجب الوقوف عند تعريف المعلومات الرقمية، وتبيان أنواعها.

أ- **تعريف المعلومات الرقمية:** على خلاف أنظمة المعلومات السابقة بالذكر؛ لم يجد المختصين في المجال الرقمي ولا الفقه القانوني–الجنائي بالخصوص–؛ أي إشكال في وضع تعريف جامع للمعلومات الرقمية، من منطلق أن كل البيانات التي تأخذ الشكل القابل للاستعمال الرقمي بعد معالجتها[4]؛ تعد بمثابة المعلومات الرقمية. ومنه تعرف المعلومات الرقمية، بموجب العديد من الدراسات التقنية ذات الصلة؛ على أنها: "ناتج معالجة البيانات الخام بأي طريقة من طرق المعالجة، بحيث تنتج معلومات منظمة ومرتبة يمكن الاعتماد عليها"[5].

= نسيم دردور، (جرائم المعلوماتية على ضوء القانون الجزائري والمقارن)، مذكرة لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة منتوري، قسنطينة، الجزائر، 2013، ص 18.

[1] ولو أنه اعتمد تسمية أخرى في إطار قانون العقوبات ذات الصلة بالمجال التجريمي نفسه، والمنطوية على أنظمة المعالجة الآلية للمعطيات "Systèmes de Traitement Automatisé de Données-STAD". **أنظر في ذلك:** المادة 394 مكرر وما يليها؛ أمر رقم 66-156، مؤرخ في 08 جوان 1966، يتضمن قانون العقوبات، (ج ر) عدد 49، صادر بتاريخ 11 جوان 1966، معدل ومتمم.

[2] **أنظر:** المادة 1/2-ب؛ قانون رقم 09-04، مراجع سابق.

[3] وفي الحقيقة لم يخرج المشرع الجزائري كثيرا؛ عن التعريف الوارد في اتفاقية بودابست لسنة2001 ذات الصلة بالجرائم محل الدراسة. والوارد تحت تسمية "Système Informatique". **أنظر في ذلك:**

- Art 01/1-a; Convention sur la cybercriminalité- Budapest, Convention Européenne (Internationale), Conseil de l'Europe, 2001. Disponible sur le Lien : http://www.coe.int/fr/web/conventions.

[4] ومنه يفهم بداهةً؛ أن البيانات هي غير المعلومات. حيث تكون البيانات دائما عكس المعلومات؛ في شكلها الخام غير المفهوم وغير القابل للاستعمال والاستغلال الرقمي.

[5] **أنظر:** أروى يحيى عبد الرحمن الإرياني، مرجع سابق، ص 26.

كما عرف المشرع الجزائري المعلومات الرقمية تحت تسمية "معطيات معلوماتية"، على أنها: "أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها"[1]. ورغم اعتبار التعريف المذكور؛ مجرد نقل حرفي عن التعريف الوارد في إطار اتفاقية بودابست لسنة 2001 –السابقة بالذكر– تحت تسمية "Données Informatiques"[2]؛ إلا أنه معاب من جهة؛ بالإطناب الاصطلاحي من حيث التفرقة بـــ "أو" بين الوقائع والمعلومات والمفاهيم، رغم إمكانية إدخالها ككل في عبارة المعلومات الرقمية. ويتناقض من جهة أخرى؛ مع التعريف الوارد سابقا بخصوص المنظومة المعلوماتية، من حيث اعتبار البرامج الوظيفية بمثابة المعلومات بعد أن تم اعتبارها سابقا بمثابة الأنظمة التطبيقية.

ب– أنواع المعلومات الرقمية: تتعدد المعلومات الرقمية وتتنوع؛ على حسب مجالها الرقمي. إلا أن التفرقة بينها لا يعد مطلوبا في المجال الجنائي؛ إلا بالقدر الضروري لتكييف الجريمة وتحديد الجزاء الجنائي، سيما بخصوص التشديد في العقوبة الأصلية. حيث نجد معلومات ذات طابع خاص، تمس بدفاع الدولة أو هيئاتها ومؤسساتها العمومية أو اقتصادها الوطني، على غرار تلك المتصلة بالإرهاب الرقمي وتبييض الأموال عبر الوسط الرقمي[3]، والتجسس...الخ[4]. كما نجد المعلومات ذات الطابع الشخصي، التي ميزها المشرع الجزائري بحماية خاصة بموجب قانون صادر سنة 2018، أسوةً بالعديد من القوانين المقارنة سيما الفرنسي منها، الذي جرمها بفصل خاص في قانون العقوبات مكون من 16 مادة كاملة[5].

وبالإضافة إلى ما ذكر؛ نجد نوعا آخرا من المعلومات الرقمية، التي تتصف بالطابع المالي. حيث تحمل الصفة المالية؛ كل معلومة رقمية لها قيمة اقتصادية، سيما تلك المتواجدة افتراضيا داخل بطاقات الائتمان، والأرصدة البنكية المحولة رقميا، وكلمات الأغاني، والألعاب والبرامج الرقمية...الخ[6]. كما

---

[1] والظاهر من التسمية والتعريف الذي يليها؛ أنه لا فرق بيم المعطيات والمعلومات. أو على الأقل لا يمكن التفرقة بينهما؛ بخصوص الدراسة المنجزة في إطار القانون الجزائري. **أنظر في ذلك:** المادة 2/1-ج؛ قانون رقم 09-04، مراجع سابق.

[2] **أنظر:**
- Art 01/1-b; Convention sur la cybercriminalité- Budapest, op.cit.

[3] أو حتى تبييض الأموال الرقمية، سيما عملة "البيتكوين Bitcoin"، التي تشهد تطورا كبيرا في أيامنا هذه، والتي لنا رجعة لدراستها في الجزئية الموالية بالدراسة. **أنظر في ذلك:** المادة 394 مكرر 3؛ قانون رقم 66-156، مرجع سابق.

[4] التي قرر لها المشرع الجزائري حماية جنائية موضوعية خاصة، من حيث تجريم المساس بسريتها أو وجودها الرقمي وفق الشكل الأصلي لها.

[5] **أنظر:** قانون رقم 18-07، مؤرخ في 10 جوان 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، (ج ر) عدد 34، صادر بتاريخ 10 جوان 2018. **وأنظر أيضا:**
- Arts de 226-16 à 226-24; code pénale français, Partie législative, Version consolidée au 17 septembre 2017. Disponible sur le Lien: https://www.legifrance.gouv.fr.

[6] وان كان قد ثار خلاف قانوني في بادئ الأمر؛ حول مدى اكتساب المعلومة الرقمية للطابع المالي، من منطلق أن صفة المال مقصورة على الأشياء المادية القابلة للتملك والاختلاس. الأمر الذي تم الحسم فيه من الفقه الفرنسي، القائل باعتبار المعلومة الرقمية من بين الأشياء المعنوية غير الملموسة. **أنظر في ذلك:** أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، الطبعة الخامسة، الجزء الأول، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2013. ص 302 و303. =

توجد العديد من المعلومات الرقمية الأخرى ذات الطابع العام، والتي تعنى بحماية جنائية عادية، على غرار تلك المتصلة بالخدمات العامة؛ كالإعلام والصحة والتضامن الاجتماعي...الخ[1].

ثانيا: النطاق الافتراضي المتصل بشبكة الاتصال الدولية

يبدوا لأول وهلة؛ أن ما تحدثه شبكة الاتصال الدولية بالتفاعل مع جهاز الإعلام الآلي؛ يعد نطاقا افتراضيا هائلا من حيث الخدمات الشبكية المتاحة للموصول بها. خاصة بالنظر إلى تنوعها من جهة، وشفافية وسلاسة الوصول إليها والاستفادة منها من جهة أخرى. إلا أن الأمر لا يعد كذلك، أو على الأقل؛ لا يعد بمثابة القاعدة التقنية المطلقة، التي نجد لها استثناءين، سيما بخصوص الويب "Le Web". وعليه ينقسم النطاق الافتراضي للشبكة إلى قسمين، أحدهما عام، والآخر خاص.

1. النطاق الافتراضي العام لشبكة الاتصال الدولية: يعد النطاق الافتراضي العام للشبكة رغم اعتباره أحد أجزائها؛ بمثابة الشبكة ككل عند الأكثرية الساحقة من الموصولين بها. نظرا لسهولة وسلاسة التعامل اليومي معه، ولإتاحته إمكانية الاستفادة من كل الخدمات الشبكية الممكنة، من بحث واتصال وتواصل...الخ. ونرى في ذلك وجوب الوقوف على أحكام النطاق الافتراضي العام، سيما من حيث تعريفه، وتحديد مكوناته.

أ- تعريف النطاق الافتراضي العام لشبكة الاتصال الدولية: يعد النطاق الافتراضي العام بالنظر إلى الشبكة ككل؛ بمثابة المرادف التقني من حيث المكونات الأساسية، والقسم الظاهر فقط من حيث حجم معلومات الويب. حيث يقوم النطاق الافتراضي العام من حيث المكونات الأساسية؛ على الويب والبريد الرقمي والتطبيقات...الخ، ويقتصر من حيث حجم معلومات الويب؛ على ما يسمى بالويب السطحي فقط "Le web de Surface - Surface Web"، دون الويب العميق "Le Web Profond - Deep Web"[2].

وعليه يعد النطاق الافتراضي العام للشبكة؛ بمثابة المجال الرقمي الذي تحدثه الشبكة منقوصا من أحد عنصري الويب، المنطوي على الويب العميق. الذي يوفر للموصول بالشبكة؛ إمكانية الاستفادة من خدمات الويب، كما يمكنه من الاتصال عبر البريد الرقمي، واستغلال التطبيقات المختلفة...الخ.

= كما يمكن أن نقول باعتماد المشرع الجزائري عموما؛ للمعلومة الرقمية ذات الطابع المالي، انطلاقا من اعترافه في إطار القانون المدني بوجود الأموال غير المادية. **أنظر في ذلك:** المادة 687؛ أمر رقم 75-58، مؤرخ في 26 سبتمبر 1975، يتضمن القانون المدني، (ج ر) عدد 78، صادر بتاريخ 30 سبتمبر 1975، معدل ومتمم.

[1] التي تحمى جنائيا في إطار قانون العقوبات؛ بموجب جرائم المساس بأنظمة المعالجة الآلية للمعطيات كما سنرى لاحقا. **أنظر في ذلك:** المادة 394 مكرر وما يليها؛ قانون رقم 66-156، مرجع سابق.

[2] ومنه يتضح جليا أن الويب؛ هو جزء من الشبكة وليس كلها من جهة، وله قسمين مختلفين من جهة أخرى. **أنظر في ذلك:**

- DIGIMIND, "Découvrir et Exploiter le Web Invisible pour la Veille Stratégique", La Société Digimind-Social Media Monitoring d'e-réputation et de Veille Stratégique, New-York, USA, 2006, p 04. Disponible sur le Lien: http://www.digimind.com/fr/.

ب- مكونات النطاق الافتراضي العام لشبكة الاتصال الدولية: يقوم النطاق الافتراضي العام؛ على مجموعة من المكونات التي تقدم خدمات شبكية مختلفة، على حسب الطلبات المقدمة رقميا من المتعامل معها. والتي تتمثل أهمها في الويب السطحي بالأساس، والمكونات المكملة بالتبعية.

ب-1/ الويب السطحي كمكون أساسي للنطاق الافتراضي العام: يعد الويب عموما؛ بمثابة خليط من المعلومات الرقمية، التي يمكن الولوج إليها عبر المواقع الشبكية المختلفة[1]. وما الويب السطحي إلا جزءا منه، والذي نجده يقوم على أحكام تقنية عامة وواضحة، سيما كونه يعمل بالشبكة العنكبوتية الدولية "World Wide Web-WWW"، التي تتيح لمستخدم البروتوكول العادي "Fil Transfer Protocol-FTP"؛ إمكانية تصفح قواعد المعلومات عبر المواقع الشبكة وخاصة نقل الملفات[2].

وتنطوي المعلومات المتاحة عبر الويب السطحي عموما؛ على تلك الموصوفة على أنها؛ معلومات غير مشفرة ومفهرسة -أو القابلة للفهرسة-، التي تظهر بمجرد بدأ عملية البحث الشبكي، بالاعتماد على المتصفحات العادية، ومحركات البحث المعروفة[3]. وحسب آخر الدراسات الإحصائية؛ فان كل المعلومات الشبكية المتاحة عبر الويب السطحي تتراوح بين الـ 05 ٪ والـ 16 ٪ فقط[4].

ب-2/ المكونات المكملة للنطاق الافتراضي العام: بالإضافة إلى الويب السطحي؛ يتشكل النطاق الافتراض العام للشبكة أيضا من المكونات التبعية، التي نجد أهمها البريد الرقمي والتطبيقات المختلفة. حيث يسمح البريد الرقمي؛ بالتراسل المعلوماتي مع الغير بصورة مجانية ومتاحة للجميع...الخ. كما يمكن أيضا لمن يتعامل مع النطاق الافتراضي العام للشبكة؛ أن يقوم بالاعتماد على التطبيقات المختلفة بالاستفادة من العديد من الخدمات الشبكية، المتصلة أصلا بخدمة الويب السطحي الموضح سابقا، والتي نجد أهمها؛ تطبيقات التخاطب الفوري المختلفة "Chat"، وتطبيقات التراسل البريدي...الخ[5].

---

[1] **أنظر:** منال هلال المزاهرة، مرجع سابق، ص 290.

وللإشارة لا نجد تعريفا للموقع في القانون الجزائري، على عكس العديد من نظرائه، سيما القانون الإماراتي الاتحادي الذي عرفه تحت تسمية "الموقع الالكتروني"؛ على أنه: "مكان إتاحة المعلومات الالكترونية على الشبكة المعلوماتية، ومنها مواقع التواصل الاجتماعي والصفحات الشخصية والمدونات". **أنظر في ذلك:** مرسوم بقانون اتحادي رقم 12-05، مرجع سابق.

[2] وسبق للقانون الجزائري تعريف الـ "WWW"؛ بـ: "خدمة تفاعلية للاطلاع أو احتواء صفحات متعددة الوسائط "MultiMedia" (نصوص، رسوم، بيانية، صوت وصورة) موصولة بينها عن طريق صلات تسمى نصوص متعددة "Hy Pertexte". إلا أننا نرى الإطناب ميزة النص، فمحتوى الصفحات المذكور يمكن اختزاله في المعلومات. كما عرف الـ "FTP"؛ بـ: "خدمة تعبئة الملفات عن بعد بصيغة نقطة إلى نقطة". **أنظر في ذلك:** المادة 1/02-1و4؛ مرسوم تنفيذي رقم 98-257، مرجع سابق.

[3] سيما متصفحات؛ "Google Chrome"، "Mozilla"، "Opera"...الخ. ومحركات البحث؛ "Google"، "Bing"، "Baidu"..الخ.

[4] **أنظر:** هاني سمير علي، "ما لا تعرف عن الإنترنت الخفي Deep Web"، تاريخ النشر: 03 جويلية 2015، تاريخ التصفح: 05 جانفي 2017، الرابط: http://www.arageek.com/tech/2015/07/03/what-you-do-not-know-about-.

[5] **أنظر:** منال هلال المزاهرة، المرجع نفسه، ص 297. **وأنظر أيضا:** عبد الله بن عبد العزيز الموسى، مرجع سابق، ص 453 و454.

2. النطاق الافتراضي الخاص لشبكة الاتصال الدولية: بعد التسليم باكتساب النطاق الافتراضي العام السابق بالدراسة، للأهمية التقنية من منطلق السهولة في التعامل والشمولية؛ نقف عند الجانب الآخر من النطاق ككل، والقائم على أساس تقليص المكونات من جهة، وزيادة كم معلومات الويب وأهميتها وخطورتها من جهة أخرى. والذي نبحث في أحكامه التقنية؛ من حيث تعريفه، وأنواعه.

أ- تعريف النطاق الافتراضي الخاص: على عكس النطاق الافتراضي العام، الذي يقوم على مكونات متعددة، سيما الويب والبريد الرقمي والتطبيقات المختلفة ذات الصلة؛ نجد نظيره النطاق الافتراضي الخاص لا يقوم إلا على ويب موازي للويب السطحي المذكور سابقا، والمتمثل في الويب العميق بالأساس "Le Web Profond - Deep Web"، وويب آخر مدخل في هذا الأخير بالتبعية المسمى بالويب المظلم "Le Web Sombre - Dark Web".

فيشكل الويب العميق؛ بين الـــ 84 ٪ والـــ 95 ٪ من الحجم الإجمالي للمعلومات الشبكية المتاحة على الويب[1]. ويقوم على مواصفات تقنية خاصة، على غرار اعتباره يحتوي على معلومات غير مفهرسة، والتي نظرا لأهميتها وحساسيتها الكبيرة؛ لا تظهر للباحث عنها بمجرد الاعتماد على محركات البحث المذكورة سابقا، بل يجب كتابة عنوان الموقع مباشرة في خانة عناوين الويب[2].

أما الويب المظلم؛ فيحتل مساحة تصل إلى حد الـــ 15 ٪ من حجم الويب العميق، وهو مدخل فيه. ويحمل المواصفات نفسها المتصلة بالويب العميق، إضافة إلى مواصفات أخرى، سيما كون المعلومات المتاحة من خلاله تعد مشفرة، ومفهرسة في إطار ضيق متصل بمتصفحات ومحركات خاصة[3]. بالإضافة إلى ضرورة تلقي دعوة من رواد هذا الويب، الذي يتصل غالبا بالأعمال غير المشروعة[4].

ب- مكونات النطاق الافتراضي الخاص: على عكس الويب السطحي المتصل بالنطاق الافتراضي العام؛ يقوم الويب المتصل بالنطاق الافتراضي الخاص-العميق والمظلم-؛ على مكونات شبكية مميزة. حيث يحتوي على معلومات خاصة، التي لا يمكن الولوج إليها؛ إلا بالاعتماد على متصفحات ومحركات بحث خاصة أيضا.

---

[1] **أنظر:** هاني سمير علي، مرجع سابق.

[2] **أنظر:** محمد الغضبان، **"العالم الخفي! ما هو الديب ويب؟ وكيف تدخل إليه؟"**، د ت ن، تاريخ التصفح: 08 جانفي 2017، الرابط: http://www.netaawy.com/2016/08/What-is-the-deeb-web-and-how-to-access.

[3] **أنظر:** المرجع نفسه. **وأنظر أيضا:**

- DAVADIE Philippe, "La Théorie du Darknet", Chaire De Cyberdéfense Et Cybersecuritè, France, 2015, p 01. Disponible sur le Lien: http://www.chaire-cyber.fr/#&panel1-2.

[4] وبتعبير أدق قائم على احترام مبدأ الشرعية الجنائية؛ نقول أنها مشكوك في عدم مشروعيتها. سيما بالنظر إلى الأعمال الرقمية المنجزة عبر هذا الويب الخاص، على غرار؛ الاتجار بالمخدرات والسلاح و...الخ. **أنظر في ذلك:**

- CAMPBELL Chris, Accédez au dark Web en 5 minutes ou moins, s d p, Date d'Accès: 07 janvier 2017. Lien: http:// libredagir.fr/accedez-dark-web-5-minutes-ou-moins.

ب-1/ معلومات رقمية خاصة: يحتوي الويب المتصل بالنطاق الافتراضي الخاص للشبكة-عميق ومظلم-؛ على العديد من المعلومات ذات الأهمية الخاصة أو الخطيرة غير المشروعة-كأصل عام-. حيث يستعمل الويب العميق؛ لنقل المعلومات الخاصة وذات الأهمية الكبيرة للدول والمؤسسات الدولية[1]. كما يعتمد على الويب المظلم؛ لممارسة العديد من الأعمال التجارية غير المشروعة-أو المشكوك في مشروعيتها-، على غرار بيع السلاح والمخدرات التقليدية والرقمية، وبيع الأطفال...الخ[2]. ولممارسة هذه الأعمال؛ التجارية يتم الاعتماد على عملة افتراضية تنطوي أهمها على البيت كوين "Bitcoin"، التي تعمل وفق الخصوصيات المتصلة بالمتصفحات والمحركات التالية بالدراسة[3].

ب-2/ متصفحات خاصة: لا يمكن الولوج إلى النطاق الافتراضي الخاص، سيما الويب المظلم منه؛ عن طريق متصفحات الويب السطحي المحددة سابقا-Google Crome، Mozilla...الخ-. وإنما يجب العمل بمتصفحات خاصة على غرار "I2P، Freenet، Anon2، Tor...الخ"[4]، التي تعطل دور البروتوكول "TCP-IP"، عن عبر نطاقات بلاحقة "Onion"، وبالتالي تعمل على إخفاء هوية المتعامل معها ومكان تواجده ماديا، وخاصةً خط سير مراسلته رقميا عبر الشبكة وماديا في الإطار الجغرافي الحقيقي[5].

---

[1] **أنظر:** محمد الغضبان، مرجع سابق.

[2] **أنظر:** - BOUNNEFILLE Vincent, (Les Darknets: Extrémités D'un Réseau Aumbiant), Mémoire Master 1, Département Arts Plastiques, Université de Paris 8 Saint-Denis Vincennes, France, 2015, p p 29-30.

[3] ويتم الحصول على العملة الرقمية "Bitcoin"؛ عن طريق إما اشتراها عبر المتاجر الرقمية التي تبيعها عبر مواقع الويب المظلم أيضا، أو الفوز بها عن طريق الألعاب الرقمية المتعددة والمتاحة عبر الويب السطحي والمظلم معا. **أنظر في ذلك:**
- DELAHAYE Jean-Paul, "Le Bitcoin, Première Crypto-Monnaie", Bulletin de la société informatique de France, Numéro 4, France, 2014, p p 68 et 69.

والملاحظ في هذا الشأن؛ أن قيمة الـ"Bitcoin"؛ تعد الأغلى في سوق البورصة العالمية، رغم عدم الاعتراف الرسمي بها إلا من القانون الألماني، الذي يفرض ضريبة على أرباح الشركات المتعاملة بها. وقد وصلت قيمتها في البورصة بتاريخ 27 نوفمبر 2017 إلى حدود الـ 10 000 دولار. **أنظر في ذلك:** العربية.نت؛ **"جنون الـ"البيتكوين" يقترب من عتبة 10 آلاف دولار"**، تاريخ النشر: 27 نوفمبر 2017، تاريخ التصفح: 27 نوفمبر 2017، الرابط:
https://www.alarabiya.net/ar/aswaq/financial-markets/2017/11/27/-10000-عتبة-من-بها-يقترب-المتواصل-البيتكوين-جنون.html.

وللإشارة فان القانون الجزائري؛ منع بموجب قانون المالية لسنة 2018 التعامل بالعملات الافتراضية على إخلاف أنواعها. الأمر الذي نجده بمثابة الاعتراف الضمني؛ بحقيقة وجود هذه العملة على المستوى الرقمي العالمي، وبخطورتها على الاقتصاد الوطني. **أنظر في ذلك:** المادة 117؛ قانون رقم 17-11، مؤرخ في 27 ديسمبر 2017، يتضمن قانون المالية لسنة 2018، (ج ر) عدد 76، صادر بتاريخ 28 ديسمبر 2017.

[4] التي يعد أهمها وأشهرها؛ متصفح "The Onion Roter - Tor - التوجيه البصلي". والذي استعمل لأول مرة سنة 2004 من قبل البحرية الأمريكية، الهادفة إلى تأمين اتصالاتها. **أنظر في ذلك:**
- JOAO FERNANDES Silva, "Le Dark Web: ombre et lumière", date de publication: 02 novembre 2016, date Date d'Accès: 06 janvier 2017. Lien: http://www.cafebabel.fr/style-de-vie/article/le-dark-web-ombre-et lumiere.html.

[5] فبمجرد الولوج الشبكي باستعمال المتصفح "tor"؛ تتم آليا عملية تحويل المعلومات الشبكية والشخصية إلى خوادم وسيطة. حيث تصبح إمكانية التعرف على الاثنين معا أمرا مستحيلا. فإما التعرف على الهوية فقط، أو الاكتفاء بالتعرف على الموقع المزار فقط. **أنظر في ذلك:** موقع علم تعلم، **"كل شئ عن الإنترنت المظلم dark web والنت العميق ..deep web بالتفصيل"**، د ت ن، تاريخ التصفح: 06 جانفي 2017، الرابط: http://www.ta3allamdz.com/2015/11/dark-web-deep-we.html .

ب-3/ محركات بحث خاصة: عادةً ما يتبع المتعامل مع الويب السطحي -المعروف لدى العامة-؛ الطريقة السهلة للتفاعل مع المعلومات الشبكية التي يريدها، والمنطوية على محركات البحث المعروفة، سيما ما يسمى بـــمحرك "Google". الأمر الذي لا يمكن العمل به في إطار النطاق الافتراضي الخاص المتصل بالويب العميق و/أو الويب المظلم. فالويب العميق وان يمكن التفاعل معه بالمتصفحات العادية؛ فانه لايمكن الولوج إليه عبر محركات البحث مهما كان نوعها سواءً العادية أو الخاصة، وهذا نظرا لعدم فهرسته كما بينا سابقا[1].

وأما بالنسبة للويب المظلم؛ فالمعلومات المتصلة به والتي تعد مشفرة؛ لا نجدها متاحة للعامة، ولا يمكن الولوج إليها إلا باستعمال محركات بحث خاصة، نظرا لكونها مفهرسة في إطارها دون سواها، من منطلق أنها قائمة على أبعاد تقنية؛ تحفظ السرية وتعطل دور بروتوكول الـــ "TCP-IP" كما بينا سابق. والمحركات المقصودة في هذا الإطار التي أهمها "Torch، Grams، Ahmia"؛ تتيح للمتعامل معها كم هائل من المعلومات تفوق تلك المتصلة بالويب السطحي، سيما المعروضة عبر المحرك الشهير"Google"؛ بحوالي 500 مرة[2].

يمكن القول من خلال ما تم تقديمه في المطلب الأول من دراسة الحال؛ أننا حاولنا تبيان الوسط الرقمي كمسرح افتراضي حديث للجريمة، الذي يعد دخيلا عن المجال القانوني عموما والمجال الجنائي خاصة. حيث من منطلق عدم إمكانية التطرق إلى الجريمة المتصلة به قبل تحديده تقنيا من جهة، ولضرورة تحديد البعد التقني لهذا الوسط ومدى تدخله في إطار الجرائم الدراسة من جهة أخرى؛ وجب البحث في مفهومه العام أولا، والفصل بين مكوناته المادية والافتراضية ثانيا، التي ستلعب الدور الأساس؛ في تحديد موضوع الجرائم محل الدراسة ومسرحها كما سنرى فيما يلي من الدراسة.

وكما بينا سابقا؛ فان أساس دراسة الحال يقوم على الربط بين إجراءات التحري والتحقيق من جهة، ومدى تطلبها لأحكام حديثة ومن الطبيعة نفسها لمواجهة جرائم الوسط الرقمي المتصلة بالمسرح الجرمي الافتراضي الحديث من جهة أخرى. الأمر الذي لا يمكن الوصول إليه؛ إلا بعد القول بولوج التجريم فقها وقانونا إلى الوسط الرقمي؛ ليضع من خلاله أحكاما موضوعية عامة، تبين مفهوم وأركان الجرائم ذات الصلة، وخاصة تقسيماتها المعتمدة.

---

[1] **أنظر:** محمد الغضبان، مرجع سابق.

[2] **أنظر:** - DAVADIE Philippe, op.cit, p p 06-09.

وأحيانا لا يمكن الولوج إلى الويب المظلم؛ إلا بعد تلقي الرابط المباشر من أحد رواد هذا الويب. التي تكون في صورة مشفرة، لايمكن فكها والوصول إلى معناها، وتنتهي بـعبارة "Onion". وعلى سبيل المثال بغرض الولوج إلى موقع متعلق ببيع القنب بكل أنواع؛ يتوجب استعمال الرابط؛ http://rsohfdikkhddhhbgvfd.onion. وللولوج إلى موقع آخر خاص ببيع قنب المملكة المتحدة؛ يجب الاعتماد على الرابط؛ hthttp://rsohfdiggdgko54lhbgdhbgvfd.onion. للإشارة فإننا في إطار تجنب نشر المواقع الإجرامية؛ نؤكد على أن الروابط المطروحة؛ ليست حقيقة، إلا أنها شبيهة للحقيقية من حيث التركيبة الظاهرة.

المطلب الثاني: جرائم الوسط الرقمي

انطلاقا من المنهج الجنائي السليم؛ لم يتدخل الفقه والقانون الجنائيين لمواجهة السلوكيات الضارة المتصلة بالوسط الرقمي كمسرح لها؛ إلا بعد أن تبين لهما الطابع المستحدث والمنفصل للوسط نفسه كما بينا سابقا. وامتدادا لذلك؛ وجب التدخل الموضوعي قبل الإجرائي. حيث تم التأسيس في الإطار نفسه؛ لما يمكن تسميتها بالنظرية العامة لجرائم الوسط الرقمي، من حيث تحديث أحكامها الجنائية الموضوعية[1]. وهذا رغم الاختلاف في الطرح، سيما من حيث التعاريف والأركان والتقسيمات ذات الصلة، إلا أنها تعد بمثابة النمط العام الذي اتفق على أساسياته الجنائية.

وفي الإطار نفسه عمل الفقه الجنائي بالأساس والمشرع المقارن والجزائري بالتبعية؛ على وضع أحكام موضوعية خاصة تتناسب مع الوسط الرقمي كمسرح جرمي افتراضي. والتي تعد أساس خصوصية إجراءات التحري والتحقيق ذات الصلة. وعلى العموم نحدد الأحكام الموضوعية لجرائم الوسط الرقمي؛ من حيث طرح مفهومها(فرع أول)، وأركانها العامة(فرع ثانٍ)، وتقسيماتها(فرع ثالث).

الفرع الأول: مفهوم جرائم الوسط الرقمي

حاول الفقه الجنائي انطلاقا من المقاربة القانونية؛ بين المفهوم العام للجريمة كسلوك معاقب عليه منذ القدم، وخصوصية الوسط الرقمي كوسط تقني حديث ترتكب الجريمة ضده أو عن طريقه أو بمساعدته؛ التوصل بنوع من الخصوصية إلى تحديد المفهوم الجنائي المتصل بالجرائم محل الدراسة. الأمر الذي وان اختلفت بشأنه الدراسات والآراء الفقهية كما سنرى؛ يعد الأساس الفقهي الحديث الذي تؤسس عليه الدراسات ذات الصلة بجرائم الوسط الرقمي عموما.

وفي سبيل تحديد المفهوم الخاص بجرائم الوسط الرقمي؛ وقع الفقه الجنائي في مفارقة الاتفاق والاختلاف. حيث تم الاتفاق من جهة؛ على حداثة هذا النوع من الإجرام، الذي نشأ وتطور مع ظهور وتطور عناصر الوسط الرقمي(أولا). ووقع الاختلاف من جهة أخرى؛ حول تحديد تعريف جامع لهذا النوع من الإجرام(ثانيا)، وبالتبعية تبيان أهم الخصائص ذات الصلة(ثالثا).

أولا: نشأة وتطور الظاهرة الإجرامية في الوسط الرقمي

تزامنت أولى السلوكيات الافتراضية الضارة بالوسط الرقمي؛ مع دخول جهاز الإعلام الآلي أهم مراحل تطوره في إطار الجيل الثالث الدائر بين سنتي "1965 و1970". حيث برزت منها تلك الهادفة

[1] الأمر الذي يعد مقبولا فقها وقانونا؛ حيث يرى الدكتور محمود نجيب حسني: "...لقد أنتجت دراسة القسم الخاص نظريات لا تقل من حيث الخصوبة عن نظريات القسم العام..وعليه، يمكن القول بوجود نظريات عامة للقسم الخاص". **أنظر في ذلك:** محمود نجيب حسني، شرح قانون العقوبات-القسم الخاص، دار النهضة العربية، القاهرة، مصر، 1992، ص 04. **نقلا عن:** أيمن عبد الله فكري، مرجع سابق، ص 92.

إلى التجسس أو الماسة بالأنظمة المعلوماتية والمعلومات المخزنة فيها. التي رغم تسببها في أضرار معتبرة؛ إلا أنها ظلت ذات بعد تقني محض، وان يمكن اعتبارها بمثابة البادرة الأولى لإجرام رقمي حديث[1]. الأمر الذي تحول بحلول النصف الثاني من سبعينات القرن الماضي؛ إلى حالة من التشكيك والخلاف القانوني. حيث طرح تساؤل فقهي مراده الوقوف عند الطبيعة القانونية لهذه السلوكيات، الدائرة بين إما اعتبارها سلوكيات تقنية بريئة، أو جرائم تقليدية، أو جرائم حديثة.

فاستبعد جانب من الفقه فكرة التجريم تماما، بوصفه للجناة على أنهم أصحاب أهداف بريئة أساسها إظهار التفوق التقني فقط، وربما يساعدون على اكتشاف عيوب وثغرات أنظمة الحماية. الأمر الذي رأى فيه جانب فقهي آخر أنه قاصر، حيث يجب القول بأن السلوكيات الضارة في هذا الإطار؛ هي جرائم تجب مواجهتها بالنصوص التقليدية، وفق ما فعل القضاء الأمريكي بخصوص حادثة "لوس أنجلوس" سنة 1976. التي كيفها على أنها مجرد سلوك تحايل يخضع لأحكام جريمة التحايل التقليدي، رغم اتصال وقائعها بالمعلومات الرقمية، وبصورة افتراضية منفصلة عن الدعامة المادية التي تحملها[2].

وبحلول ثمانينات القرن الماضي؛ أخذت السلوكيات محل الدراسة بالتطور توازيا مع تطور جهاز الإعلام الآلي في إطار الجيل الرابع أولا، وانتشار شبكة الاتصال الدولية بين الأشخاص ثانيا. حيث ظهرت سلوكيات رقمية شبكية تتصل بالاختراق عن بعد ونشر الفيروسات...الخ[3]؛ أدت بالفقه الجنائي إلى التسليم بخصوصية هذا النوع من الإجرام الحديث، وحتمية مواجهته موضوعيا بنصوص ومبادئ تجريمية حديثة تراعي الطبيعة التقنية نفسها. وتبعا لذلك؛ بدأت الجهود الرسمية القائمة على هذا الاتجاه؛ في إصدار التوصيات الاسترشادية، وسن الاتفاقيات والقوانين الدولية والوطنية ذات الصلة[4].

---

[1] **أنظر:** فضيلة عاقلي، "الجريمة الالكترونية وإجراءات مواجهتها من خلال التشريع الجزائري"، أعمال المؤتمر الدولي الرابع عشر حول الجرائم الالكترونية، طرابلس-لبنان، 24-25 مارس 2017، ص 122.

[2] الأمر الثابت من خلال وقائع القضية؛ التي يمكن تلخيصها في قيام شركة "EFI-إكويتي فندنج إنستورنس"، كأكبر الشركات الأمريكية المختصة في التأمين على الاستثمارات المالية؛ بتسجيلها لأكثر من 64 ألف شخص وهمي في حاسوبها الخاص على أنهم عملاء لها، مع التأمين على حياتهم بوثائق تأمين وهمية، بالإضافة إلى بيع الوثائق ذات الصلة إلى شركات أخرى مختصة بإعادة التأمين. وأدت السلوكيات الموضحة؛ إلى تكبد الشركة المعنية لخسائر تزيد عن الـ 02 مليار دولار. مع إدانة أكثر من 22 موظف سامي في الشركة نفسها. **أنظر في ذلك:** يونس عرب، "جرائم الكمبيوتر والانترنت"، ورقة عمل مقدمة إلى مؤتمر الأمن العربي، أبو ظبي، الإمارات العربية المتحدة، 10-12 فيفري 2002، ص 07. **وأنظر أيضا:** يونس عرب، "صور الجرائم الإلكترونية واتجاهات تبويبها"، ورقة عمل مقدمة إلى ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية، مسقط، سلطنة عمان، 02-04 أفريل 2006، ص 06 و07. **وأنظر كذلك:** حسن طاهر داود، جرائم نظم المعلومات، مطابع أكاديمية نايف العربية للعلوم الأمنية، الرياض، السعودية، 2000، ص 31 و32.

[3] **أنظر:** يونس عرب، "جرائم الكمبيوتر والانترنت"، المرجع والصفحة نفسهما.

[4] وكانت البداية بإصدار قرارين هامين وردا في شكل توصية دولية -التي تعد اعتراف صريح بوجود جرائم الوسط الرقمي واستقلاليتها-. والمتمثلان في؛ قرار"هافانا" المتصل بالجرائم ذات الصلة بالكمبيوتر الصادر سنة 1990؛ عن مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة السجناء. وقرار "ريو ديجانيرو" بشأن جرائم الكمبيوتر أيضا، الصادر سنة 1994؛ عن مؤتمر الأمم المتحدة الخامس عشر للجمعية الدولية لقانون العقوبات. **أنظر في ذلك:** قرار هافانا بشأن الجرائم ذات الصلة بالكمبيوتر، مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة السجناء، هافانا، كوبا، 1990. متوفر عبر الرابط: =

ثانيا: تعريف جرائم الوسط الرقمي

دخل الفقه الجنائي انطلاقا من الخصوصية التقنية للوسط الرقمي كمسرح جرمي حديث من جهة، وقلة التعاريف القانونية المقارنة من جهة أخرى؛ في دوامة خلاف فقهي بحثا عن وضع التعريف المناسب للجرائم المتصلة به على اختلاف تسمياتها واتساع مضمونها[1]. ورغم مناداة البعض من الفقه بصعوبة تعريف هذا النوع من الإجرام الحديث والمعقد[2]؛ عمل المشرع الجزائري؛ على تعريفه بالاعتماد على المعايير الفقهية السائدة، سيما تلك القائمة على المدلول الضيق، ونظيرتها المنطوية على المدلول الواسع الذي يجب الأول.

1. التعريف الضيق لجرائم الوسط الرقمي: يعتمد أنصار الاتجاه الضيق في تعريف جرائم الوسط الرقمي؛ على الأساس الواحد المنفصل. حيث ينظر إلى الجريمة؛ بمعيار قانوني منفصل عن باقي المعايير. المنطوية أساسا على أحد المعايير الثلاثة، الدائرة بين المعيار المادي والمعيار الشخصي والمعيار الموضوعي[3].

= http://faculty.mu.edu.sa/nalthobaiti/crime. **وأنظر أيضا:** مقررات وتوصيات مؤتمر ريو دي جانيرو بشأن جرائم الكمبيوتر، مؤتمر الأمم المتحدة الخامس عشر للجمعية الدولية لقانون العقوبات، ريو دي جانيرو، البرازيل، 04-09 أكتوبر 1994. متوفر عبر الرابط: http://www.f-law.net/law/threads/1080.

[1] تختلف وتتعدد التسميات المقررة فقها وقانونا للجرائم محل الدراسة، والتي نراها قاصرة في مجملها نظرا للعديد من الأسباب. حيث نستبعد تسمية جرائم جهاز الإعلام الآلي-الكمبيوتر أو الحاسوب-؛ نظرا لاقتصارها اصطلاحا على الجرائم المتصلة بالجهاز دون الشبكة. ونستبعد تسمية جرائم شبكة الاتصال الدولية-الانترنت-الشبكة-؛ نظرا لإمكانية اتصال الجريمة بمعلومات وأنظمة الجهاز دون الشبكة. كما نستبعد أيضا تسمية الجريمة السيبرانية؛ نظرا لكونها ترجمة حرفية للتسمية الانجليزية "Cyber Crime"، الواردة لأول مرة في إطار اتفاقية بودابست لسنة 2001-المذكورة سابقا-.

كما نستبعد أيضا التسميات المختلفة التي جاء بها المشرع الجزائري –الذي لم يستقر على تسمية معينة-؛ نظرا لقصور الربط بين الجريمة والوسيلة الالكترونية أو المعلوماتية بالمادة 144مكرر/1 "ق.ع"؛ حيث نجد العديد من الأجهزة تعمل بالنبضات الالكترونية من دون أن تحمل نطاقا افتراضيا، مثل التلفاز والثلاجة...الخ. كما أن الاقتصار على المعلومة الرقمية قد يخرج أنظمة المعلومات. ونستبعد أيضا تسمية المساس بأنظمة المعالجة الآلية للمعطيات الواردة بالمادة 394مكرر وما يليها "ق.ع"؛ نظرا لضيق مضمونها فهي تشكل أحد أنواع جرائم الوسط الرقمي-كما سنرى لاحقا-. بالإضافة إلى أننا نستبعد تسمية جرائم تكنولوجيات الإعلام والاتصال التي جاء بها المشرع بـ"القانون رقم 09-04"؛ نظرا لاتساعها جنائيا لتشمل الجرائم المرتكبة عبر أي وسيلة اتصال الكترونية، سيما الاتصال الهاتفي التقليدي، ولكونها قد تضم حتى جرائم الصحافة.

ومنه يمكن القول أننا اعتمدنا في دراسة الحال على تسمية الوسط الرقمي؛ نظرا لشموليتها ومرونتها من جهة، ولقصور التسميات المذكورة أعلاه من جهة أخرى. فيعد مصطلح الرقمية؛ شاملا لعنصريها من جهاز وشبكة ومن في حكمهما. ويعتبر مرنا؛ نظرا لإمكانية تقييده أو إطلاقه قانونيا ورقميا، بمجرد إضافة مصطلح الوسط، الذي يخرج الجرائم المتصلة بالمكونات المادية للعناصر الرقمية، ويقتصر على نطاقها الافتراضي فقط. كما يخرج أيضا الجرائم المتصلة بالأجهزة الالكترونية غير العاملة بالأنظمة الرقمية، على غرار الهواتف التقليدية الثابتة والمحمولة.

[2] الأمر الذي يرجع إلى العديد من الحجج القانونية والتقنية. سيما؛ صعوبة حصر السلوكيات الضارة في إطار قانوني موحد نظرا لطبيعتها الفنية. وتطلب الاتفاق الدولي على التعريف المعتمد؛ نظرا لاتصاف هذه الجرائم بالبعد العالمي. **أنظر في ذلك:** أيمن عبد الله فكري، مرجع سابق، ص 91.

[3] ولو أنه يوجد من يرى من أنصار هذا الاتجاه؛ بإمكانية الاكتفاء بالتعريف القائم على المعيار الضيق الهادف إلى حماية المعلومات والأنظمة، سيما الأستاذ الألماني "أولريش سيبر – Ulrich Seiber"، الذي يعرفها على أنها: "كل سلوك غير مشروع أو غير مرخص له المتصل بالمعالجة الآلية للمعطيات أو بتحويلها". **أنظر في ذلك:**
- ANDRE Lucas et DEVEZE Jean, Le Droit de L'Informatique et de L'Internet, PUF, Paris, France, 2001, p 496.

أ- تعريف جرائم الوسط الرقمي بالنظر إلى المعيار المادي: تقتصر تعاريف جرائم الوسط الرقمي المتصلة بالمعيار المادي؛ على النظر من زاوية وسيلة ارتكاب الجريمة، دون البحث في موضوعها أو صفات مرتكبها. وتتمثل الوسيلة وفق أنصار هذا الاتجاه؛ في عناصر الوسط الرقمي المذكورة سابقا. والمنطوية وفقهم على جهاز الإعلام الآلي وشبكة الاتصال الدولية. ومن أبرز التعاريف ذات الصلة نجد؛ تعريف الفقيه الألماني "تايديمان – Tiedemon"، الذي عرفها انطلاقا من جهاز الإعلام الآلي؛ على أنها:" كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب باستخدام الحاسوب الآلي"[1]. كما عرفها آخرون بالنظر إلى شبكة الاتصال الدولية؛ على أنها: "كل فعل غير مشروع يقع بواسطة الشبكة الدولية للاتصال"[2].

يتبن جليا أن التعاريف الموضحة أعلاه؛ لا تفرق بين ماديات الوسط الرقمي وافتراضية ما تحدثه هذه الماديات. الأمر الذي يعد مجانبا للصواب كما يرى العديد من الفقه، حيث يجب الرجوع وفقهم؛ إلى السلوك الأساسي المكون للجريمة ومدى اتصاله بالمعلومات الافتراضية بصورة منفصلة عن الماديات، وليس إلى العكس –أي الوسائل المستخدمة بصورة منفصلة عن ما تحدثه من وسط افتراضي-. ومن أبرز القائلين بذلك؛ نجد الأستاذ "أندرسون – RF.Anderson"، الذي عبر أنه: "ليس مجرد أن الحاسب قد استخدم في جريمة، أن نعتبرها من الجرائم المعلوماتية"[3].

ب- تعريف جرائم الوسط الرقمي بالنظر إلى المعيار الشخصي: على عكس ما تم بيانه سابقا؛ يقوم المعيار محل الطرح –أو المعيار الشخصي-؛ على القدرات الذهنية والصفات الشخصية للجاني، دون البحث في موضوع الجريمة التي يرتكبها. ومن أهم التعاريف ذات الصلة نجد ما جاء به الأستاذ "توسمون دفيد – Thompson David"، الذي عرفها على أنها: "أية جريمة يكون متطلبا لاقترافها توافر لدى فاعلها معرفة تقنية للحاسب"[4]. الأمر الذي لم تخرج عنه كثيرا وزارة العدل الأمريكية في تعريفها لهذا النوع من الإجرام الحديث، حيث جاء في نصها على أنها: "جريمة لفاعلها معرفة فنية بتقنية الحاسبات تمكنه من ارتكابها"[5].

---

[1] الأمر الذي لم يخرج عنه الفقيه "توم فوستر –Thome Foster"، الذي عرفها على أنها: "فعل إجرامي يتم باستخدام الحاسوب كأداة رئيسية". **أنظر في ذلك:** فضيلة عاقلي، مرجع سابق، ص 118. **وأنظر أيضا:** محمود أمحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2005، ص 15.

[2] **أنظر:** مفتاح بوبكر المطردي، "الجريمة الالكترونية والتغلب على تحدياتها"، ورقة عمل مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية، الخرطوم، السودان، 23-25 سبتمبر 2012، ص 13.

[3] **أنظر:** يونس عرب، "جرائم الكمبيوتر والانترنت"، مرجع سابق، ص 04. **وأنظر أيضا:** يونس عرب، "صور الجرائم الالكترونية واتجاهات تبويبها"، مرجع سابق، ص 03.

[4] **أنظر:** محمود أمحمد عبابنة، المرجع نفسه، ص 16 و17.

[5] **أنظر:** محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت دراسة مقارنة، دار النهضة العربية للنشر، القاهرة، مصر، 2005، ص 34.

يبدوا جليا من خلال التعاريف المقدمة؛ أن المعيار الشخصي يشوبه العديد من القصور، سيما كون أغلب جرائم الوسط الرقمي تعد جرائم مساهمة جنائية واشتراك، يرتكبها العديد من الأشخاص بتوزيع الأدوار-مختصين وغير مختصين-. بالإضافة إلى اعتبار أكثرها؛ ترتكب من قبل أشخاص لا خبرة لهم في الوسط الرقمي[1].

ج- تعريف جرائم الوسط الرقمي بالنظر إلى المعيار الموضوعي: تجاوزا للمعيارين السابقين بالذكر؛ برز معيار ثالث يعتمد في تعريفه؛ على موضوع الجريمة بغض النظر عن وسيلتها وصفة مرتكبها. ومن أهم التعاريف ذات الصلة؛ نجد ذلك الذي جاء به الأستاذ "روزنبلت – Rosenblatt"، حيث اعتبر جرائم الوسط الرقمي على أنها: "نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه"[2]. كما وضعت "منظمة التعاون والتنمية في الميدان الاقتصادي-Organisation de Coopération et de Développement Economiques"؛ تعريفا للجرائم محل الدراسة، جاء فيه أنها: "كل سلوك غير مشروع أو منافي للأخلاق أو غير مسموح يرتبط بالمعالجة الآلية للبيانات أو بنقلها"[3].

لم تسلم التعاريف القائمة على المعيار الموضوعي هي الأخرى من العديد من الانتقادات، سيما اعتبار التعريف الأخير على أنه يقترب أكثر من التعريف الواسع التالي بالدراسة، الأمر الذي يقود بالضرورة إلى صعوبة تحديد السلوكيات واجبة التجريم[4]. بالإضافة إلى أننا نعتبر من جانبنا؛ أن المعيار الموضوعي هو شامل لكل المعايير السابقة، سيما المعيار المادي. فلا يعقل المساس بالمعلومات أو استعمالها افتراضيا؛ من دون العمل بعناصر الوسط الرقمي.

2. التعريف الواسع لجرائم الوسط الرقمي: يقوم التعريف الواسع لجرائم الوسط الرقمي؛ على الجمع بين المعايير السابقة من جهة وفتح مجال التجريم من جهة أخرى. ولعل من أهم التعاريف ذات الصلة نجد؛ ما جاء به الأستاذ الفرنسي "ماس – Masse"، الذي اعتبرها على أنها: "الاعتداءات غير القانونية التي يمكن أن ترتكب بواسطة المعلوماتية بغرض تحقيق الربح[5]". كما عرفت أيضا بأنها: "مجموعة الأفعال والأنشطة المعاقب عليها قانونا والتي تربط بين الفعل الإجرامي والثورة التكنولوجية"[6].

---

[1] **أنظر:** يونس عرب، "صور الجرائم الالكترونية واتجاهات تبويبها"، مرجع سابق، ص 03.

[2] **أنظر:** يونس عرب، "جرائم الكمبيوتر والانترنت"، مرجع سابق، ص 03.

[3] **أنظر:** لجنة الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، "برنامج تعزيز حكم القانون في بعض الدول العربية-مشروع تحديث النيابيات العامة"، برنامج الأمم المتحدة للتنمية، المملكة المغربية، 2007، ص 05.

[4] **أنظر:** يونس عرب، "صور الجرائم الالكترونية واتجاهات تبويبها"، المرجع والصفحة نفسهما.

[5] **أنظر:** محمود أمحمد عبابنة، مرجع سابق، ص 17.

[6] **أنظر:** عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة، مصر 2006، ص 06. **نقلا عن**: فضيلة عاقلي، مرجع سابق، ص 118.

ويرى العديد من الفقه أن الاعتماد على التعريف الواسع وفق التعريفين المذكورين وغيرهما؛ يعد الحل الأنجع لتلافي القصور الذي شاب مختلف التعريفات المتصلة بالتعريف الضيق. فكل سلوك إجرامي يتصل بالمعالجة الآلية للمعطيات سواءً كهدف أو كوسيلة أو كمسهل؛ يعتبر من قبيل جرائم الوسط الرقمي. إلا أنه يظل اتجاه منتقد أيضا نظرا لتوسعه المفرط، الذي قد يصل إلى غاية الاستعمال المادي لعناصر الوسط الرقمي[1].

3. تعريف المشرع الجزائري لجرائم الوسط الرقمي: لم يتطرق المشرع الجزائري في البداية إلى تعريف جرائم الوسط الرقمي، بل تأخر في ذلك إلى غاية سنة 2009 بموجب القانون رقم 09-04 المذكور سابقا. حيث عرف الجرائم محل الدراسة تحت تسمية الجرائم المتصلة بتكنولوجيات الإعلام والاتصال -كما وضحنا سابقا-؛ على أنها: "جرائم المساس بأنظمة المعالجة الآلية للمعطيات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية"[2].

ومن خلال الربط بين التعريف الموضح أعلاه والتعاريف السابقة بالذكر؛ يمكن القول أن المشرع الجزائري قد اعتمد كل المعايير الممكنة باستثناء المعيار الشخصي. حيث عمل بالمعيار الموضوعي؛ من خلال احتواء التعريف على جرائم المساس بأنظمة المعالجة الآلية للمعطيات، وعمل بالمعيار المادي؛ من خلال النص عن الوسيلة المعلوماتية والالكترونية. كما أضاف معيارا آخرا يمكن أن نسميه بالقانوني؛ لتغطية العجز المتصل بمبدأ الشرعية، عن طريق تجريم استعمال الوسيلة المعلوماتية والالكترونية لارتكاب الجريمة التقليدية. إلا أنه يعاب عليه توسعه الكبير الذي شمل حتى الاتصالات الالكترونية غير الرقمية، الممكن انجازها عن طريق الهاتف التقليدي مثلا[3].

---

[1] **أنظر:** محمد أمين الشوابكة، جرائم الحاسوب والإنترنات-الجريمة المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2009، ص 08. **نقلا عن**: نعيم سعيداني، (آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري)، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية تخصص علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، الجزائر 2013، ص 28.

ولو تطرقنا إلى التعريفين المذكورين بالتحليل سنجد أنهما؛ حاولا مراعاة الانتقادات الموجهة إلى المعايير السابقة. لكن يعاب عليهما أن التعريف الأول؛ يربط بين الجريمة محل الدراسة وغرض الربح المالي، رغم كونه أحد دوافع هذه الجرائم وليس الوحيد. بالإضافة إلى ربط التعريف الثاني بين السلوك الإجرامي والثورة التكنولوجية، الأمر الذي سيوسع من مجال الإجرام، نظرا لتعدد وتنوع الوسائل الناتجة عن الثورة التكنولوجية-الثورة الصناعية الثانية- التي نجد منها الرقمية وغير الرقمية، كما ذكرنا سابقا.

[2] **أنظر:** المادة 1/02-أ؛ قانون رقم 09-04، مرجع سابق.

[3] الأمر الذي نراه من دون جدوى. حيث الجرائم التي ترتكب عن طريق الاتصال الهاتفي التقليدي؛ تدخل ضمن إطار الجرائم التقليدية المرتكبة في الوسط المادي، نظرا لاعتبارها وسيلة عادية لا تحتوي على منظومة معلوماتية رقمية، وبالتالي لا تتصف بالخصوصية المعقدة. وللإشارة نجد أن القانون الجزائري في إطاره المدني؛ يعتبر أن التعاقد المنجز عن طريق الهاتف هو تعاقد بين حاضرين، وتطبق عليه الأحكام العامة للتعاقد في مجلس العقد. ولو رأى المشرع أن له خصوصية تقنية؛ لعالجه بموجب قانون التجارة في الوسط الرقمي-القانون المتعلق بالتجارة الالكترونية-. **أنظر في ذلك:** المادة 1/64؛ أمر رقم 75-58، مرجع سابق. **وأنظر أيضا:** قانون رقم 18-05، مؤرخ في 10 ماي 2018، يتعلق بالتجارة الإلكترونية، (ج ر) عدد 28، صادر بتاريخ 16 ماي 2018.

وانطلاقا مما ذكر بخصوص المعايير المختلفة، والتعريف الذي جاء به المشرع الجزائري في هذا الصدد، وخاصةً الانتقادات الموجهة لكل منها؛ يمكن أن نضع تعريفا لجرائم الوسط الرقمي، مركزين في ذلك على النطاق الافتراض للوسط الرقمي باعتباره مسرحها الجرمي. حيث نقول أنها: "كل سلوك مجرم يرتكب في إطار النطاق الافتراضي للوسط الرقمي، بغرض إما المساس به أو استعماله كوسيلة أو كمسهل لارتكاب أي جريمة أخرى يمكن تصور ارتكابها عبره أو بمساعدته".

ثالثا: خصائص جرائم الوسط الرقمي

تتميز جرائم الوسط الرقمي بالمفهوم الجنائي المحض عن باقي جرائم القانون العام وغيرها؛ بالعديد من الخصائص الموضوعية التي تعد ناتج خصوصية الوسط الرقمي كمفهوم تقني، وفي الوقت نفسه؛ أساس الخصوصية الموضوعية لجرائم هذا الوسط بالمفهوم القانوني الجنائي[1]. والتي ستبنى عليها الأركان القانونية العامة والتقسيمات المختلفة التالية بالدراسة. ولعل أبر هذه الخصائص نجد عدم الاتفاق على إطار عام لجرائم الوسط الرقمي، وكونها جرائم سلوك افتراضي بأثر مزدوج الطبيعة، وهي جرائم ذات بعد عالمي، كما تتصف سلوكياتها بالتطور الديناميكي المستمر.

1. عدم الاتفاق على إطار عام لجرائم الوسط الرقمي: وقع الفقه أولا والمشرع ثانيا –الجزائري والمقارن قبله–، من جراء الخصوصية التقنية للوسط الرقمي كمسرح جرمي؛ في حالة من عدم الاتفاق على وضع إطار عام حول نماذج النشاط الإجرامي للجريمة ذات الصلة[2]. فإلى حد الساعة؛ لا نجد نظرية عامة موحدة لهذه الجرائم، لا من حيث التعريف العام لها–كما وضحنا سابقا–، ولا من حيث تجريم السلوكيات اللازم تجريمها بعد حصرها، ولا حتى من حيث معيار تقسيمها–كما سنرى لاحقا–. حيث نجد لكل نظام تشريعي؛ نظرته الخاصة لهذا النوع من الإجرام الحديث[3].

2. الطبيعة المزدوجة لأثر السلوك الافتراضي في جرائم الوسط الرقمي: ينحصر السلوك الإجرامي للجرائم محل الدراسة كما بينا سابقا؛ في ذلك المتصل بالنطاق الافتراضي للوسط الرقمي. حيث بمجرد تفاعل الجاني مع العناصر المادية لهذا الوسط؛ يلج إليه افتراضيا ويرتكب سلوكيات افتراضية، التي قد تفرز أثارا ونتائج إجرامية إما رقمية افتراضية من الطبيعة نفسها، أو مادية ملموسة في الحيز الخارجي

[1] وفي الإطار نفسه نرى أن العديد من الدراسات السابقة؛ لا تفرق بين الخصائص الموضوعية ومظاهر العجز الإجرائي في مواجهة جرائم الوسط الرقمي. حيث الخصائص الموضوعية؛ هي ما سنذكر في النقطة محل الطرح، المنصبة على الشق الموضوعي لهذه الجرائم. وأما مظاهر العجز الإجرائي؛ فهي ما تتصل بالشق الإجرائي أساس دراسة الحال، والتي سنستعرضها في المبحث القادم بالدراسة.

[2] **أنظر:** أيمن عبد الله فكري، مرجع سابق، ص 92.

[3] ونرى بوجهة نظر خاصة؛ أنه يمكن التوصل إلى نموذج عام يحدد عناصر التعريف وفق الذي قدمناه أعلاه، وان بصورة وقتية تتماشى مع التطور التقني الحالي للوسط الرقمي. لكن لايمكن أبدا الوصول إلى إطار عام، سيما بخصوص حصر السلوكيات واجبة التجريم، نظرا للتطور الديناميكي السريع لسلوكيات الوسط الرقمي كما سنرى لاحقا.

أو الاثنين معا[1]. وعلى العموم يحدث الأثر الإجرامي إما المستقل أو الثنائي؛ العديد من الأضرار، سيما الرقمية المتصلة بالمعلومات، أو الماسة بالأشخاص والجهات، أو حتى الاقتصادية والعسكرية والسياسية...الخ[2].

3. عالمية جرائم الوسط الرقمي: يعد الطابع العالمي لجرائم الوسط الرقمي؛ خاصية ناتجة بداهةً عن عالمية الوسط الرقمي نفسه. الذي بمجرد اتساع مجاله المنوط بالاتصال المنجز عبر شبكة الاتصال الدولية؛ أصبح يكتسب البعد العالمي أو الدولي العابر للحدود الوطنية. حيث تنتقل المعلومات الرقمية افتراضيا بين الأجهزة المختلفة والموزعة عبر النقاط المتباينة، وفي سبيل ذلك يقوم مثلا أي شخص متواجد في حدود إقليم دولة –أ– بإرسال معلومات رقمية إلى شخص آخر متواجد في دولة –ب–، على أن تمر هذه المعلومة تماثليا؛ عبر كل الدول المرتبطة بالكابل البحري بين النقطتين المذكورتين[3].

فلا يمكن تصور جريمة إقليمية محضة في إطار جرائم الوسط الرقمي. حيث تعد كلها جرائم ذات بعد عالمي متعدية الحدود الوطنية، لكون السلوك الإجرامي؛ يرتكب في دولة معينة، ثم يمر عبر العديد من الدول في حدود الربط التقني بالكابل البحري، على أن تتحقق النتيجة الإجرامية في دولة أخرى[4].

4. التطور الديناميكي المستمر لجرائم الوسط الرقمي: اكتسب التجريم والعقاب عموما في ظل النظريات التقليدية للجريمة –العامة والخاصة–؛ طابع الجمود النسبي من حيث التطور. الأمر الذي تطلبته طبيعة المجتمع والسلوكيات الإجرامية ذات الصلة، التي استقرت وفق نمط سلوك معين، مع إمكانية ظهور سلوكيات جديدة غير مألوفة أو تطور تلك الموجودة خلال فترات زمنية متباعدة[5].

---

[1] **أنظر:** جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيات الحديثة، الطبعة الثانية، دار النهضة العربية، القاهرة، مصر، 2012، ص 11 و12.

[2] **أنظر:** أمير فرج يوسف، الجرائم المعلوماتية على شبكة الإنترنت، دار المطبوعات الجامعية للنشر، الإسكندرية، مصر، 2008، ص 108 و109 و125 و126.

ونرى بإمكانية قيام الأثر الرقمي الافتراضي؛ لو قام الجاني مثلا بمجرد المساس بمعلومة رقمية لا وجود لها في الحيز المادي. كما يكون الأثر مادي فقط؛ لو تم استعمال المنظومة الرقمية كوسيلة لتحريض شخص من أجل القيام بجريمة مادية معينة. ويكون الأثر مزدوجا رقميا وماديا؛ لو قام الجاني بقرصنة منظومة معلوماتية للحصول على معلومات عسكرية سرية.

[3] وكنا قد وضحنا سابقا؛ آلية الربط بالكابل البحري الحامل للشبكة. حيث لكل دولة سبق لها الارتباط مخرج يمكن أن تربط منه الدول الأخرى التي لم يسبق لها الارتباط. ومنه لا يمكن للمعلومة الرقمية المرسلة من الجزائر عبر الشبكة؛ أن تصل إلى أي نقطة أخرى في الدولة نفسها أو خارجها؛ إلا بعد المرور عبر إحدى الدول أساس الربط الكابلي على حسب الحالة.

[4] **أنظر:** أيمن عبد الله فكري، مرجع سابق، ص 92 و93. **وأنظر أيضا:** رحيمة نديلي، "خصوصية الجريمة الالكترونية في القانون الجزائري والقوانين المقارنة"، أعمال المؤتمر الدولي الرابع عشر حول الجرائم الالكترونية، طرابلس، لبنان، 24 و25 مارس 2017، ص 110 و111.

وفي الحقيقة تعد عالمية جرائم الوسط الرقمي؛ من أهم الأسباب التقنية والقانونية التي أدت إلى اكتساب هذا النوع من الإجرام للخصوصية محل الطرح، ولبروز الأزمة الإجرائية التالية بالدراسة. فتوزع عناصر الركن المادي كما سنرى لاحقا؛ أدى إلى تنازع القوانين موضوعيا، وتنازع جهات التحقيق والحكم إجرائيا.

[5] وأبرز دليل على ذلك، نجد قانون العقوبات الصادر سنة 1966 بقانون رقم 66-156؛ لم يحين من أركان جريمة الإجهاض الواردة بالمادة 304 منه، رغم تعديله وتتميمه لأكثر من 22 مرة. وهو يفترض بداهةً؛ استقرار سلوكها المادي.

إلا أن ولوج التجريم إلى الوسط الرقمي؛ أدى إلى التخلي عن فكرة الجمود النسبي في التعامل التشريعي مع السلوكيات ذات الصلة. وهذا من منطلق التطور الديناميكي السريع للوسط نفسه، سيما إذا ما تعلق الأمر بشبكة الاتصال الدولية ونطاقها الافتراضي المتصل بالويب المتعدد الأقسام كما بينا سابقا[1]. حيث يرى في ذلك العديد من الدارسين؛ أنه تحدٍ حقيقي يواجه المشرع الجنائي، سيما بخصوص تحيين النصوص التقليدية أو الإتيان بأخرى حديثة للموازنة بين احترام مبدأ الشرعية من جهة وضمان حماية التعاملات الرقمية من جهة أخرى[2].

يتضح جليا من خلال ما تم بيانه بخصوص مفهوم جرائم الوسط الرقمي؛ أنها تمتاز بخصوصية قانونية جد معقدة، ناتجة عن خصوصية الوسط الرقمي كمسرح جرمي حديث. الأمر الذي لم يقف عند هذا الحد، بل امتد وفق ترابط جنائي منطقي؛ ليضفي الخصوصية القانونية نفسها على الأركان العامة للجرائم محل الدراسة –انطلاقا من الأركان العامة للجريمة– من جهة، والمعايير المعتمدة لتقسيمها من جهة أخرى.

الفرع الثاني: الأركان العامة لجرائم الوسط الرقمي

تعد من بديهيات القانون الجنائي؛ عدم إمكانية تصور أي جريمة من دون الأركان العامة المنطوية على الركن؛ الشرعي والمادي والمعنوي[3]. وعليه يمكن القول أنه؛ بمجرد وصف السلوكيات محل الدراسة على أنها جرائم؛ يتوجب القول أن لها أركان عامة في إطار ما تسمى بالنظرية العامة. إلا أنه بالرجوع إلى ما تفضلنا بتقديمه سابقا من خصوصية تقنية للوسط الرقمي ومفهوم عام للجرائم المتصلة به؛ نجد أنها جرائم لايمكن أن تخضع للنظرية العامة للجريمة التقليدية.

---

[1] حيث بالاعتماد على الشبكة؛ توسع نطاق ارتكاب السلوكيات الضارة التي وجب تجريمها، أو تحيين النصوص التقليدية ذات الصلة. فبعدما اقتصر الاعتداء في البداية على ماديات الوسط الرقمي-الخارجة عن الدراسة-، تطور ليمس بنظم المعالجة الآلية للمعطيات، ومن ثم ليصل إلى الاحتيال الرقمي والتصيد الاحتيالي...الخ. **أنظر في ذلك:** فريق الخبراء المعني بالجريمة السيبرانية، "مشروع المواضيع المطروحة للنظر في إطار دراسة شاملة بشأن تأثير الجريمة السيبرانية وتدابير التصدي لها"، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، منظمة الأمم المتحدة، فيينا، النمسا، 21 جانفي 2011، ص 04 و05. متوفر عبر الرابط: http://www.unodc.org/unodc/fr/cybercrime/index.html.

وهكذا أخذت السلوكيات الرقمية بالتطور السريع والديناميكي؛ إلى أن بلغت درجة إمكانية ارتكاب أغلب السلوكيات التقليدية المجرمة من خلاله. بالإضافة إلى الظهور اليومي لسلوكيات أخرى حديثة غير مجرمة، سيما ما تسمى بلعبة الحوت الأزرق كما سنرى لاحقا.

[2] **أنظر:** سليم مزيود، "الجرائم المعلوماتية واقعها في الجزائر وآليات مكافحتها"، المجلة الجزائرية للاقتصاد والمالية، مخبر الاقتصاد الكلي والمالية الدولية، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة يحي فارس بالمدية، الجزائر، عدد 01، أفريل 2014، ص 101.

[3] الأمر الذي يؤكد عليه جانب كبير من الفقه الجنائي. بخلاف الجانب الآخر المتبقي الذي وان يؤكد على ضرورة قيام الركنين المادي والمعنوي؛ إلا أنه يعارض اعتبار الركن الشرعي من الأركان العامة للجريمة-وحتى كركن خاص-. وهذا للعديد من الحجج، لعل أهمها؛ أن النص الموجد للجريمة لايمكن أن يكون أحد أركانها أولا، واعتبار النص التجريمي على أنه هو وعاء نموذج الجريمة ثانيا، بالإضافة إلى إمكانية ارتكاب السلوك المجرم بالنص، مع تخلف قيام الجريمة، مثل حالة أسباب الإباحة. **أنظر في ذلك:** عبد الله أوهايبية، شرح قانون العقوبات الجزائري، مرجع سابق، ص 82 و86 و87.

وبمجرد محاولة المقاربة بين ما ذكر؛ نقع في حتمية التسليم بقيام جرائم الوسط الرقمي على أركان عامة ذات خصوصية قانونية مختلفة عن تلك المتصلة بالنظرية العامة للجريمة[1]. الأمر الذي نبينه بالتطرق إلى الركن الشرعي(أولا)، ومن ثم الركن المادي(ثانيا)، وأخيرا الركن المعنوي(ثالثا).

أولا: الركن الشرعي لجرائم الوسط الرقمي

يعد الركن الشرعي للجريمة –أو مبدأ الشرعية الجنائية– بغض النظر عن الاتجاه المعارض لوجوده؛ أول وأهم أركان الجريمة عموما، حيث لا تقوم أي جريمة بتخلفه. فهو النص الموجد لها، والذي يعد أبرز ضمان موضوعي لحقوق وحريات الأفراد، من خلال وروده في صالحهم ولفائدتهم بجعلهم في موقف دراية وتدبر للسلوكيات غير المشروعة. ويكتسي الركن الشرعي في جرائم الوسط الرقمي؛ طابع الخصوصية القانونية، التي لا تبرز إلا بمحاولة المقاربة بين الإطار التقليدي للركن الشرعي، ومستجدات الركن الشرعي في جرائم الوسط الرقمي.

1. الإطار التقليدي لمبدأ الشرعية الجنائية: رغم عدم اتساع المقام للتوسع في طرح مبدأ الشرعية الجنائية؛ يمكن أن نبحث فيه من حيث تعريفه وإبراز نتائجه التي تعد أهم ما يمكن التطرق إليه. فبعيدا عن الاختلافات الفقهية والصياغات التشريعية، ومن دون إسهاب في الطرح؛ يمن القول أن مبدأ الشرعية الجنائية هو: "عدم إمكانية متابعة أي شخص جنائيا إلا بوجود نص يجرم السلوك محل المتابعة وساري المفعول وقت ارتكاب هذا السلوك"[2]. ولم يخرج المشرع الجزائري عن ذلك كثيرا، حيث عرفه بـــ: "لا جريمة ولا عقوبة أو تدبير أمن بغير قانون"[3].

ولمبدأ الشرعية الجنائية وفق التعريف الموضح؛ العديد من النتائج، التي تعطيه طابع السمو والتميز عن باقي الأركان العامة للجريمة من جهة، وصفة الحامي للحقوق والحريات من جهة أخرى. حيث بتجاوز هذه النتائج جزئيا أو كليا؛ نكون أمام تخلف وصف الجريمة عن السلوك محل المتابعة ومنه براءة المتابع. وتتمثل هذه النتائج بالأساس في انفراد التشريع بالتجريم والعقاب، حيث للمشرع الحق الأصيل في ذلك، ولا يمكن للسلطة التنفيذية أن تجرم سلوك لم يجرمه المشرع بقانون، ولا يمكن للسلطة القضائية أن تعاقب على ذلك ولا أن تعاقب على سلوك غير مجرم أصلا[4].

---

[1] الأمر الذي يعد مقبولا قانونا وفقها كما بينا سابقا، في إطار ما جاء به الدكتور محمود نجيب حسني. إلا أننا نؤكد على الصعوبة الواقعية المتصلة بتحديد هذه الأركان؛ نظرا للتطور الديناميكي السريع للوسط الرقمي من منظوره التقني المحض، وعدم استقرار سلوكياته المجرمة وواجبة التجريم قانونيا. فما تعد بمثابة الأركان العامة لجرائم الوسط الرقمي اليوم؛ قد تصبح قاصرةً غدا.

[2] **أنظر:** عبد الله أوهايبية، شرح قانون العقوبات الجزائري، مرجع سابق، ص 86.

[3] **أنظر:** المادة 01؛ أمر رقم 66-156، مرجع سابق.

[4] **أنظر:** ناصر حمودي، (القانون الجنائي العام: الأحكام العامة لقانون العقوبات والنظرية العامة للجريمة)، محاضرات السنة الثانية حقوق، معهد الحقوق، المركز الجامعي العقيد آكلي محند أولحاج، البويرة، الجزائر، 2010، ص 83.

وتنطوي أيضا نتائج مبدأ الشرعية الجنائية؛ على حضر التفسير الواسع للنص الجنائي الموضوعي. حيث يجب على الجهة القضائية المختصة؛ الابتعاد عن التفسير الواسع والالتزام بالتفسير الضيق، القائم على البحث عن الإرادة الحرفية والحقيقية للمشرع وقت وضعه للنص[1]. كما يتوجب أيضا الابتعاد عن القياس في هذا الإطار، حيث لا يمكن متابعة شخص ومعاقبته جنائيا، عن طريق إلحاق واقعة غير مجرمة بواقعة أخرى مجرمة نظرا لاشتراكهما في علة الحكم[2].

بالإضافة إلى ما ذكر؛ يعد تحديد نطاق تطبيق الشق الموضوعي للقانون الجنائي من حيث الزمان والمكان؛ أهم نتائج مبدأ الشرعية الجنائية. فمن حيث الزمان؛ يتم العمل بعدم الرجعية كأصل عام والرجعية كاستثناء. حيث لا يسري النص الجنائي الموضوعي على الماضي إلا ما كان منه أقل شدة. ومنه كأصل عام لا يمكن متابعة أي شخص على أي واقعة؛ إلا إذا كانت مجرمة بنص قبل ارتكابها، مع مراعاة النص الجديد الذي قد يكون أصلح للمتهم[3].

ويجب أيضا التقيد بأحكام تطبيق القانون الجنائي الموضوعي من حيث المكان. حيث كأصل عام نقول أن القانون الجزائري هو المختص انطلاقا من مبدأ الإقليمية؛ إذا ما ارتكب السلوك و/أو حدثت النتيجة في إقليم الدولة الجزائرية بعناصره الثلاث. كما يمكن أن يطبق القانون الجزائري وفق مبدأ الشخصية؛ إذا ما ارتكبت الجناية أو الجنحة من أو ضد جزائري في الخارج. مع إمكانية تطبيقه أيضا وفق مبدأ العينية؛ في حال ارتكاب جناية أو جنحة في الخارج، من قبل شخص لا يحمل الجنسية الجزائرية، ضد أمن الدولة أو عملتها الرسمية أو محلاتها الدبلوماسية أو العاملين فيها[4]. مع التأكيد على أن الأولوية في التطبيق تكون لمبدأ الإقليمية، وفي كل الأحوال يجب مراعاة قاعدة سبق الفصل[5].

2. مبدأ الشرعية الجنائية في جرائم الوسط الرقمي: دفعت خصوصية الوسط الرقمي والجرائم المتصلة به بالمشرع والفقه الجنائي؛ إلى التركيز على تحيين أو تطوير الأحكام ذات الصلة بمبدأ الشرعية المذكورة سابقا وأعلاه. حيث تم الوقوف على العديد من الإشكالات في هذا الخصوص، سيما تلك المتصلة بحالة ارتكاب الجريمة التقليدية في الوسط الرقمي، وتحديد مكان ارتكاب الجريمة، وخاصةً صعوبة مواكبة التشريع للتطور السريع لسلوكيات الوسط الرقمي.

---

[1] **أنظر:** عبد الله أوهايبية، شرح قانون العقوبات الجزائري، مرجع سابق، ص ص 104-108.

[2] **أنظر:** ناصر حمودي، (القانون الجنائي العام: الأحكام العامة لقانون العقوبات والنظرية العامة للجريمة)، مرجع سابق، ص 86 و87.

[3] **أنظر:** المرجع نفسه، ص 87-98. **وأنظر أيضا:** المادة 02، أمر رقم 66-156، مرجع سابق.

[4] **أنظر:** أحسن بوسقيعة، الوجيز في القانون الجزائي العام، مرجع سابق، ص ص 104-111. **وأنظر أيضا:** المادة 03؛ أمر رقم 66-156، المرجع نفسه. **وأنظر كذلك:** المواد 582-591؛ أمر رقم 66-155، مرجع سابق.

[5] **أنظر:** عبد الله أوهايبية، شرح قانون العقوبات الجزائري، مرجع سابق، المرجع نفسه، ص 131 و151.

أ- ارتكاب الجريمة التقليدية بالاعتماد على الوسط الرقمي: مع اتساع نسبة الموصولية العالمية بالشبكة؛ طفت إلى السطح ظاهرة استعمال الشبكة كوسيلة و/أو كمسهل لارتكاب العديد من السلوكيات المجرمة بالنصوص التقليدية، كالسب والقذف والنصب والاحتيال...الخ. الأمر الذي أدخل الفقه الجنائي؛ في خلاف حول مدى شرعية اعتبارها سلوكيات مجرمة بالنص التقليدي. فرأى جانب في ذلك؛ أنه لا فرق بين السلوك الرقمي والسلوك التقليدي المجرم، وكل ما في الأمر أن وسيلة ارتكاب الجريمة قد تحولت من المادية إلى الرقمية. إلا أنه يبقى رأي منتقد، نظرا لتخلف الوسط الرقمي وقت وضع النص[1].

ويرى جانب ثانٍ من الفقه الجنائي؛ أنها جرائم حديثة منفصلة عن تلك التقليدية الشبيهة بها. ومنه يجب تجريمها بنصوص مستقلة تراعي الطبيعة الرقمية. وهو الرأي الذي قوبل بالعديد من الانتقادات، سيما بالنظر إلى وحدة السلوك المرتكب وما الاختلاف إلا في الوسط، وتشريع نصوص تجريمية جديدة سيقود إلى التكرار التجريمي[2]. كما ينادي رأي ثالث في هذا الصدد؛ بضرورة تطوير النصوص التقليدية النافذة، بإضافة فقرات ومصطلحات رقمية مقترحة شكلا وشرحا من قبل المختصين[3].

وبالرجوع إلى النمط التجريمي المعتمد من قبل المشرع الجزائري في هذا الصدد؛ نجده قد عمل بالرأي الأول مع مراعاة الانتقادات الموجهة له. حيث جاء بما يمكن تسميته مبدأ الشرعية العام أو الشامل، وذلك عن طريق تشريع مادة تعرف جرائم الوسط الرقمي وتحدد نطاقها الموضوعي، ليجعل من خلال ذلك كل جريمة تقليدية ترتكب أو يسهل ارتكابها عبر الوسط الرقمي؛ على أنها جرائم معاقب عليها بالنص التقليدي نفسه[4].

ب- صعوبة تحديد مكان ارتكاب جرائم الوسط الرقمي: تتفرق عناصر الركن المادي لجرائم الوسط الرقمي المرتكبة عن طريق الشبكة. حيث قد يكون السلوك في دولة ويمر عبر عدة دول ثم تتحقق النتيجة الإجرامية في دولة أخرى-كما بينا سابقا-. الأمر الذي يصعب من عملية تحديد مكان ارتكاب الجريمة، وعليه القانون الواجب التطبيق. ولو أن الفقه الجنائي في هذا الصدد؛ يكون قد اتفق نسبيا على العمل بالنظرية التقليدية، القاضية بحصر القانون المختص في دولتي ارتكاب الفعل وتحقق النتيجة فقط[5].

---

[1] **أنظر:** محمد عبيد الكعبي، مرجع سابق، ص 53.

[2] وهو ما اعتمدته العديد من التشريعات المقارنة. فحسب استبيان قام به مكتب الأمم المتحدة للمخدرات والجريمة، فان أغلب هذه التشريعات؛ قد قامت بتطوير النصوص التقليدية المجرمة لحوالي 10 سلوكيات تقليدية، لتتماشى مع الوسط الرقمي. **أنظر في ذلك:** فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، مرجع سابق، ص 06 و07. **وأنظر أيضا:** ذياب موسى البداينية، "الجرائم الالكترونية: المفهوم والأسباب"، ورقة عمل مقدمة إلى الملتقى العلمي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، عمان، المملكة الأردنية الهاشمية، 02-04 سبتمبر 2014، ص 07 و08.

[3] **أنظر:** محروس نصار غايب، "الجريمة المعلوماتية"، مجلة التقني، هيئة التعليم التقني، العراق، مجلد 24، عدد 09، 2011، ص 07 و08.

[4] **أنظر:** المادة 1/02-أ؛ قانون رقم 09-04، مرجع سابق.

[5] **أنظر:** مفتاح بوبكر المطردي، مرجع سابق، ص ص 22-28.

ج- عدم مواكبة التشريع لسرعة تطور سلوكيات الوسط الرقمي: وفق ما بينا سابقا؛ فان أهم ما يميز الوسط الرقمي كوسط تقني كونه سريع التطور. حيث كل يوم تظهر سلوكيات إضافية، قد تكون بمثابة تطور لسلوكيات تقليدية معروفة أو عبارة عن أخرى مستحدثة تماما. الأمر الذي يمكن مواجهته؛ بإعمال ما يسمى بمبدأ الشرعية العام المذكور سابقا بخصوص السلوكيات المجرمة سابقا في شلها التقليدية. وفي الوقت نفسه؛ يصعب التصدي بخصوص السلوكيات الأخرى المستحدثة يوميا. حيث يتوجب تدخل المشرع بصفته المصدر الوحيد للتجريم والعقاب؛ لتجريمها، الأمر الذي يأخذ وقتا طويلا بين المبادرة والصياغة والإصدار والنشر[1]. ما قد يؤدي إلى ظهور العديد من السلوكيات الأخرى، وربما حتى التوقف عن العمل بالسلوكيات التي تم تجريمها بعد كل الإجراءات الطويلة[2].

ثانيا: الركن المادي لجرائم الوسط الرقمي

يعد الركن المادي ثاني أهم أركان الجريمة عموما، والمجسد الأساس لمبدأ مادية الجريمة ومظهرها الخارجي. حيث لايمكن تصور التجريم؛ من دون تحديد المصلحة محل الحماية الجنائية. وبتخلفه لايمكن الحديث عن قيام الجريمة ولا عن متابعة المعني. الأمر الذي سنستعرضه فيما هو آتٍ، بالتطرق إلى الإطار التقليدي للركن المادي، ومن ثم إبراز خصوصيته في جرائم الوسط الرقمي.

1. الإطار التقليدي للركن المادي للجريمة: يعد الركن المادي كما بينا أعلاه؛ المجسد لمبدأ مادية الجريمة، والذي بموجبه يتم استبعاد تجريم أو العقاب على مجرد النوايا غير المجسدة ماديا في الوسط المادي الملموس. حيث يقوم المشرع بتجريم السلوكيات المادية الواجبة لذلك بعد أن يحاول تحديدها وحصرها. ومنه يعرفه العديد على أنه: "تطابق الفعل الذي أتاه الجاني مع النموذج القانوني للجريمة"[3].

---

[1] **أنظر:** فريق الخبراء المعني بالجريمة السيبرانية، مرجع سابق، ص 03. **وأنظر أيضا:** عادل يوسف عبد النبي الشكري، "الجريمة المعلوماتية وأزمة الشرعية الجزائية"، مجلة مركز دراسات الكوفة، جامعة الكوفة، العراق، مج 01، عدد 07، 2008، ص 117.

[2] وأبرز دليل على ذالك ما تثيره لعبة تحدي الحوت الأزرق. التي تدفع بروادها إلى الانتحار بشكل آلي بعد كسب ثقتهم. والتي ظهرت لأول مرة سنة 2013 تحت تسميات أخرى بروسيا عبر الموقع "vk.com"، حيث تم إحداثها من قبل طالب جامعي عمرة 21 سنة يدعى "فيليب بوديكين"، الذي اتهم وأدين بجريمة التحريض بعد أن زاد عدد ضحايا اللعبة عن 16 طفل. والغريب في الأمر أن رده كان من منطلق فخر، مؤكدا أنه حاول تخليص العالم ممن هم عالة عليه، مضيفا أنهم كانوا سعداء بالانتحار. وبالمقابل تم التصدي لهذه اللعبة آن ذاك، عن طريق الوقاية الرقمية بحجبها من القائمين على إدارة الموقع. **أنظر في ذلك:** هزار بحبوح، "تحدي الحوت الأزرق...لعبة لانتحار المراهقين"، تاريخ النشر: 31 ماي 2017، تاريخ التصفح: 03 جانفي 2017، الرابط: https://raseef22.com/life/2017/05/31/تحدي-الحوت-الأزرق-لعبة-تؤدي-لانتحار-ا/.

ويعد هذا السلوك أمرا مستجدا عن التشريع الجنائي الجزائري. حيث لايمكن أن يعاقب صاحب اللعبة عن التحريض، لأن التحريض حسب المادة 41 "ق.ع"؛ يجب أن يتصل بسلوك مجرم والمشرع لا يعاقب عن الانتحار. كما لايمكن متابعته على أساس المساعدة على الانتحار المعاقب عليه بالمادة 273 "ق.ع؛ نظرا لكونها تكون بعد أن يقرر الشخص الانتحار، وفي هذه اللعبة القائم عليها هو من يخلق فكرة الانتحار لدى الضحية عن طريق الاحتيال. بالإضافة إلى أن المشرع حدد وسائل المساعدة على سبيل الحصر والتي تعد مادية محضة. **أنظر في ذلك:** المادتان 41 و273؛ أمر رقم 66-156، مرجع سابق.

[3] ناصر حمودي، (القانون الجنائي العام: الأحكام العامة لقانون العقوبات والنظرية العامة للجريمة)، مرجع سابق، ص 162 و163.

ويتجسد الركن المادي للجريمة في الحيز الخارجي عن طريق ثلاثة عناصر أساسية. المنطوية على السلوك والنتيجة والعلاقة السببية. فيقوم السلوك الإجرامي؛ عن طريق إما القيام بفعل يحضره القانون أو عدم القيام بفعل أمر به القانون. وتعد النتيجة الإجرامية؛ الأثر المادي الملموس الذي يحدثه السلوك الإجرامي في العالم الخارجي، والتي لا يتطلبها المشرع؛ إلا في الجرائم المادية أو جرائم الضرر[1]. وفي الجرائم المادية التي تتطلب النتيجة الإجرامية يجب لقيام مسؤولية الفاعل؛ أن تقوم ما تسمى برابطة السببية بين السلوك والنتيجة، حيث تكون هذه الأخيرة كأثر عن الأول[2].

وتتحقق عناصر الركن المادي الموضحة أعلاه؛ بعد المرور عبر العديد من المراحل، التي لا تكتمل إلا في الجرائم المادية القائمة على العناصر الثلاث. فيعد التفكير والعزم أولى المراحل، التي تمتاز بالذاتية، حيث لا يعاقب الشخص الذي يفكر في ارتكاب جريمة ومن ثم يعدل عن ذلك، من منطلق عدم ارتكابه لأي سلوك خارجي ملموس، واستحالة الوصول إلى ذهن الأشخاص ومعرفة نواياهم الكابتة[3]. على أن تأتي بعد ذلك مرحلة التحضير، التي يقوم الجاني من خلالها بالاستعداد المادي لارتكاب الجريمة، والتي تعد كأصل عام؛ غير مجرمة لانعدام أثرها المادي[4]. وتأتي بعد ذلك المرحلة الثالثة المنطوية على البدء بالتنفيذ أو الشروع. حيث يبدأ الجاني فعلا في تنفيذ السلوك الإجرامي؛ فإذا أتمه وتحققت النتيجة نكون أمام جريمة تامة، وإذا لم تتحقق النتيجة لسبب خارجي عن إرادته نكون أمام جريمة الشروع[5].

2. الإطار الحديث للركن المادي في جرائم الوسط الرقمي: بمجرد محاولة إسقاط الأحكام التقليدية للركن المادي على الوسط الرقمي بخصوصيته المعقدة المذكورة؛ يتضح أنه للركن المادي في جرائم الوسط الرقمي خصوصية قانونية معقدة أيضا. التي تخرجه من حيزه الخارجي الملموس وتدفع به إلى النطاق الرقمي الافتراضي، كما تصعب على الجهات القضائية؛ التعامل مع مراحل وعناصر الركن المادي.

---

[1] **أنظر:** أحسن بوسقيعة، الوجيز في القانون الجزائي العام، مرجع سابق، ص ص 116-126.

[2] التي يصعب إقامتها في حال تعدد الأسباب المؤدية إلى النتيجة. ومنه يتم اللجوء إلى العمل بالنظريات الفقهية المعروفة. فقد يعمل بنظرية تعادل الأسباب، التي تساوي بين جميع الأسباب وتجعل الكل مسئول. وقد يعتمد على نظرية السبب المنتج"السبب المباشر"، التي تبحث عن السبب المتصل مباشرة بالسلوك. كما قد يتم الربط بنظرية السبب الملائم، التي تبحث عن السلوك القادر وفق المجرى العادي لأن يحدث النتيجة. **أنظر في ذلك:** ناصر حمودي، (القانون الجنائي العام: الأحكام العامة لقانون العقوبات والنظرية العامة للجريمة)، مرجع سابق، ص ص 172-178.

[3] إلا أنه وكاستثناء؛ يعاقب المشرع عن النية المعلنة في شكل الاتفاق على تكوين جمعية أشرار. كما قد يصبح التفكير والعزم؛ ظرفا مشددا في حالة ارتكاب الجريمة. **أنظر في ذلك:** عبد الله أوهايبية، شرح قانون العقوبات الجزائري، مرجع سابق، ص ص 257-261.

[4] وكاستثناء؛ يمكن أن تجرم الأعمال التحضيرية بنص صريح ومنفصل، على غرار التحضير لارتكاب جرائم المساس بأنظمة المعالجة الآلية للمعطيات، المعاقب عليها بالمادة 394مكرر2 "ق.ع". **أنظر في ذلك:** المادة 394مكرر2؛ أمر رقم 66-156، مرجع سابق. **وأنظر أيضا:** عبد الله أوهايبية، المرجع نفسه، ص 261.

[5] حيث قد يكون في صورة الشروع الناقص، الذي لا يكتمل فيه السلوك الإجرامي. أو الشروع التام، الذي يكتمل فيه السلوك لكن لا تتحقق النتيجة-الجريمة المستحيلة-. والتي بدورها تنقسم إلى نوعين؛ المطلقة والنسبية، وأغلب الفقه يرى العقاب على النسبية دون المطلقة. **أنظر:** أحسن بوسقيعة، المرجع نفسه، ص ص 135-142.

أ- افتراضية مسرح الجريمة والسلوك الإجرامي: على خلاف الجريمة التقليدية المرتكبة في الوسط المادي الخارجي؛ تتصل الجرائم محل الدراسة كما بينا سابقا؛ بالنطاق الافتراضي للوسط الرقمي، الذي تخلقه مادياته المنطوية على جهاز الإعلام الآلي والمكونات الخارجية لشبكة الاتصال الدولية. حيث يرتكب الجاني جريمته؛ في مسرح افتراضي حديث ومنفصل عن ذلك التقليدي المعروف، بعد ولوجه إليه افتراضيا قادما من المادي الملموس. وان كان يمكن تصور النتائج الإجرامية في الحيز الخارجي أيضا، كما يمكن أن يرتكب السلوك؛ وفق العديد من الصور الدائرة بين البسيط والمركب والمتعدد...الخ[1].

ب- صعوبة التعامل القضائي مع مراحل وعناصر الركن المادي: يواجه القضاء الجنائي المختص بالنظر في الجرائم محل الدراسة؛ العديد من الصعوبات ذات الصلة بمراحل ارتكاب الركن المادي وعناصره. حيث يتعذر في العديد من الأحيان؛ التفرقة بين مراحل ارتكاب الركن المادي، التي على أساسها يمكن الحديث عن قيام الجريمة من عدمها كما بينا سابقا. الأمر الذي أدى بالمشرع الجزائري وقبله المقارن، لغرض تفادي الإفلات من العقاب الجنائي؛ إلى تجريم بخصوص أهم جرائم الوسط الرقمي المنطوية على المساس بأنظمة المعالجة الآلية للمعطيات، كل من الشروع والأعمال التحضيرية[2].

كما يجد القضاء الجنائي أيضا؛ العديد من الصعوبات بخصوص الركن المادي. فبالإضافة إلى صعوبة تحديد مكان وزمان ارتكاب الجريمة، وفق ما بينا سابقا بخصوص الركن الشرعي؛ يعد من الصعب -أو من المستحيل-؛ إقامة رابطة السببية في العديد من جرائم الضرر، انطلاقا من توزع وتبعثر السلوكيات المختلفة والنتيجة الواحدة أو حتى المزدوجة في إطار رقمي افتراضي جد معقد، ما قد يضخم من حجم الأسباب المؤدية إلى تحقق النتيجة لتصل إلى ملايين الأسباب[3].

ثالثا: الركن المعنوي لجرائم الوسط الرقمي

يعد الركن المعنوي عموما؛ ثالث أركان الجريمة، الذي يسميه البعض بجانبها الشخصي المتعلق بالجاني. فلا يمكن تصور قيام أي جريمة سواءً تقليدية أو حديثة؛ من دون توفر ركنها المعنوي إن بالقصد أو الخطأ. وهو الذي يتصف كغيره من الأركان السابقة بالذكر؛ بنوع من الخصوصية في إطار الجرائم محل الدراسة، التي لايمكن أن نحددها إلا بالتطرق أولا إلى الإطار التقليدي للركن المعنوي.

---

[1] **أنظر:** عمر عبد العزيز موسى الدبور، "آليات تفعيل الحماية والوقاية من الجرائم الالكترونية"، أعمال المؤتمر الدولي الرابع عشر حول الجرائم الالكترونية، طرابلس، لبنان، 24 و25 مارس 2017، ص 223 و224.

ونرى في ذلك؛ أنه من الغريب ومن غير المنطقي تسمية هذا الركن بالتسمية التقليدية المنطوية على الركن المادي. حيث الجريمة بكل مكوناتها وعناصرها ترتكب في مسرح افتراضي بعيد كل البعد عن الماديات. الأمر الذي يدفع إلى ضرورة البحث عن تسمية أخرى تتماشى وحداثة الجرائم محل الدراسة. والذي نقترح فيه، تسمية الركن الافتراضي أو الرقمي.

[2] **أنظر:** عبد اللطيف معتوق، مرجع سابق، ص 23 و24. **وأنظر أيضا:** المادتان 394مكرر2 و394مكرر7؛ أمر رقم 66-156، مرجع سابق.

[3] **أنظر:** يوسف صغير، مرجع سابق، ص 68.

1. الإطار التقليدي للركن المعنوي للجريمة: يعتقد الفقه الجنائي في هذا الصدد؛ بعدم كفاية ماديات الجريمة لإسناد المسؤولية الجنائية، ومنه القول بعدم جدية متابعة الشخص وإدانته من دون البحث في مدى قيام الخطأ إلى جانبه. حيث يجب التوفر لدى الفاعل قدر من الخطأ أو الإثم. كما تبرز أهمية ذلك؛ في تحديد طبيعة السلوك المرتكب الدائر بين الإباحة والجرم العمدي وغير العمدي. فبتخلف الركن المعنوي نكون أمام انعدام الوصف الجنائي، وبقيامه تكتمل أركان الجريمة الثلاث، ومنه تقرر العقوبة قضائيا انطلاقا من التفرقة الجنائية بين الجريمة العمدية وغير العمدية. الأمر الذي من خلاله يعرف الركن المعنوي للجريمة من طرف العديد من الفقه؛ على أنه: "الصلة النفسية بين الجاني والسلوك المادي[1]".

يقوم الركن المعنوي للجريمة وفق ما بينا أعلاه؛ إما على أساس القصد أو الخطأ. حيث ينطوي القصد الجنائي؛ على اتجاه إرادة الجاني لارتكاب السلوك المجرم، مع علمه بالتجريم وإرادته لتحقق النتيجة[2]. وهو الذي يقسمه الفقه إلى العديد من الأنواع أهمها القصد العام والخاص، والقصد المحدود وغير المحدود[3]. كما يقوم القصد الجنائي؛ على عنصري العلم والإرادة، اللذان لايمكن أن تقوم الجريمة بتخلف أحدها. حيث يقصد بالعلم؛ توفر دراية الجاني بأركان الجريمة وعناصرها وفق نموذجها التشريعي. ويستدل بالإرادة؛ على توجه رغبة الجاني لارتكاب السلوك وتحقق النتيجة معا[4]".

وأما الخطأ الجنائي؛ فيقصد به الإخلال بالتزامات الحيطة والحذر التي يفرضها القانون الجنائي وعدم الحيلولة دون حدوث النتيجة[5]. ويقوم الخطأ الجنائي على عكس ما يعتقد العديد؛ على عنصري العلم والإرادة المذكورين سابقا، والاختلاف البسيط ينصب على النتيجة الإجرامية التي لا يتوقعها الجاني ولا يرغب فيها[6]. كما يرى الفقه أن جوهر الخطأ؛ هو التزام عام يقرره القانون وفق صور محددة حصرا، التي تنطوي عموما على ضرورة مراعاة الحيطة والحذر والحرص على الحقوق والمصالح[7].

---

[1] **أنظر:** عبد الله أوهايبية، شرح قانون العقوبات الجزائري، مرجع سابق، ص 327. **وأنظر أيضا:** ناصر حمودي، (القانون الجنائي العام: الأحكام العامة لقانون العقوبات والنظرية العامة للجريمة)، مرجع سابق، ص ص 217-219.

[2] **أنظر:** منصور رحماني، الوجيز في القانون الجنائي العام، دار العلوم للطباعة والنشر والتوزيع، الجزائر، 2006، ص 114.

[3] حيث يأخذ القصد العام؛ التعريف نفسه المذكور في المتن، وهو المطلوب لقيام جميع الجرائم العمدية. وأما القصد الخاص؛ فيختلف من جريمة لأخرى، بحسب إرادة الجاني لوقائع إضافية. كما ينطوي القصد المحدود؛ على تحديد الجاني للسلوك المراد ارتكابه والنتيجة المراد تحقيقا. وعلى عكسه يعد القصد غير المحدود؛ بمثابة عدم حصر الموضوع والنتيجة. **أنظر في ذلك:** ناصر حمودي، المرجع نفسه، 228. **وأنظر أيضا:** عبد الله أوهايبية، المرجع نفسه، ص 335.

[4] **أنظر:** ناصر حمودي، المرجع نفسه، ص 223.

[5] **أنظر:** أحسن بوسقيعة، الوجيز في القانون الجزائي العام، مرجع سابق، ص 143.

[6] **أنظر:** - GARE Thierry et GINESTET Catherine, Droit Pénal Procédure Pénal, Dalloz, France, 2012, p 145.

[7] التي حددها المشرع الجزائري كأصل عام؛ في الرعونة المنطوية على الطيش وسوء التقدير ونقص المهارة المطلوبة. وعدم الاحتياط، بالاستخفاف بالأمر وعدم اتخاذ الاحتياطات اللازمة لمنع حدوث الضرر الممكن تصوره. والاهمال بعدم بذل عناية للقيام بما يجب. وعدم الانتباه القائم على انحراف الشخص بعدم اكتراثه بضرورة اليقظة. وعدم مراعاة الأنظمة، بعدم احترام القانون بمفهومه الواسع مما يسبب ضررا للغير. **أنظر في ذلك:** منصور رحماني، المرجع نفسه، ص 127 و128.

2. الإطار الحديث للركن المعنوي في جرائم الوسط الرقمي: لم يخرج الركن المعنوي في جرائم الوسط الرقمي؛ كثيرا عن الإطار العام السابق بالذكر، إلا من حيث ما تتطلبه الخصوصية الرقمية والقانونية ذات الصلة. حيث يمكن تصور قيام جريمة من جرائم الوسط الرقمي في صورتها العمدية المتأتية من القصد، كما يمكن قيام أيضا جريمة غير عمدية متأتية من الخطأ. وعلى العموم يعد الركن المعنوي في الجرائم محل الدراسة؛ بمثابة اتجاه إرادة الجاني المتوفر لديه العلم بالتجريم إلى ارتكاب السلوك الرقمي المجرم[1].

وانطلاقا مما ذكر أعلاه من جهة وما بيناه سابقا بخصوص عناصر الركن المادي في الجرائم محل الدراسة من جهة أخرى، سيما الوقوف عند خصوصيتها المستحدثة؛ يمكن القول أن العلم والإرادة يتصلان بالنطاق الافتراضي الرقمي بالأساس والحقيقي الملموس بالتبعية. حيث يتطلب أن يعلم الجاني بأنه بصدد ارتكاب سلوك غير مشروع في النطاق الافتراضي الرقمي، مع توجه إرادته الآثمة إلى القيام بالسلوك نفسه واستهداف تحقق النتيجة، التي في أثرها تكون رقمية افتراضية و/أو مادية ملموسة.

كما ترى العديد من الدراسات ذات الصلة؛ أنه من أصعب ما يواجه الجهات القضائية في مواجهة هذا النوع من الإجرام الحديث؛ يكمن في صعوبة إثبات القصد الجنائي وحتى صور الخطأ. الأمر المتأتي من تشعب النطاق الافتراضي للوسط الرقمي، سيما إذا ما تعلق ذلك بالاتصال عن بعد عبر الشبكة، التي يمكن التفاعل والتراسل من خلالها بطريقة متباعدة، كما قد يتحجج العديد بأن سلوكياتهم الرقمية المجرمة أصلا؛ ارتكبت عن غير قصد من منطلق الجهل والغلط والرغبة في اكتشاف خبايا الشبكة والتسلية والتحدي...الخ[2].

الفرع الثالث: تقسيمات جرائم الوسط الرقمي

عرفت السلوكيات الرقمية الضارة منذ بدايات ظهورها وتطورها كما بينا سابق؛ تشعبا وتطورا ديناميكيا متلازمين، فكلما تطور الوسط الرقمي؛ تشعبت بالنتيجة سلوكياته الافتراضية وازدادت تعقيدا. الأمر الذي أدخل المشرع بالأساس والفقه الجنائي بالتبعية؛ في دوامة تكييف جنائي، انصبت عنها صعوبة تقسيم هذه السلوكيات إلى طوائف كما هو معمول به في الجريمة التقليدية، التي نجدها مقسمة إلى جرائم أشخاص وجرائم أموال وجرائم شرف واعتبار وجرائم أمن دولة...الخ.

---

[1] مع التأكيد على أن الجاني في جرائم الخطأ لا يتوقع النتيجة ولا يريدها. **أنظر في ذلك:** عبد الفتاح ولد باباه، (الركن المعنـوي في الجرائم المعلوماتية في النظام السعـودي-دراسة تأصيلية)، رسالة لنيل درجة الماجستير في العدالة الجنائية، جامعة نايف العربيــة للعلوم الأمنيــة، الرياض، السعودية، 2013، ص 46.

[2] مع العلم أن صعوبة إثبات الركن المعنوي في جرائم الوسط الرقمي؛ تعد نوعا من الصعاب التي تواجه إثبات هذه الجرائم عموما. وهو ما سنتطرق إليه بالتفصيل في المبحث الموالي بالدراسة. **أنظر في ذلك:** يوسف صغير، مرجع سابق، ص 72 و73. **وأنظر أيضا:** مروان بن مرزوق الروقي، (القصد الجنائي في الجرائم المعلوماتية-دراسة تأصيلية مقارنة)، رسالة لنيل درجة الماجستير في العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، 2011، ص ص 119-124.

وفي الإطار نفسه؛ سعى الفقه الجنائي من جهة والدول في الإطار الاتفاقي والتشريعي من جهة أخرى؛ لمحاولة حصر السلوكيات الرقمية واجبة التجريم، ومن ثم تقسيمها إلى طوائف قائمة على معايير مختلفة. الأمر الذي اعتمد منه المشرع الجزائري اتجاها معينا كغيره من التشريعات المقارنة(ثانيا)، القائم بالأساس على مزايا التقسيمات الفقهية والاتفاقية المختلفة(أولا).

أولا: التقسيمات المختلفة لجرائم الوسط الرقمي

لم يقف التعقيد المتصل بالجرائم محل الدراسة عند مفهومها وأركانها السابقة بالذكر؛ بل امتد إلى غاية تقسيماتها التي تعددت وتنوعت بحسب المعيار المنظور من خلاله. الأمر الذي يزيد من خصوصيتها من جهة، ويدفع للتباين الفقهي والتشريعي من جهة أخرى، رغم اتصال هذه الجرائم بالنطاق العالمي العابر للحدود الوطنية، وتطلبها للتناسق بغرض تمكين الوقاية والمكافحة. وعلى العموم ظهرت بعض التقسيمات في إطار المحاولات الأولى لذلك، منها الفقهية ومنها التقنية ومنها الاتفاقية، الأمر الذي جاء أكثر دقة وإلزامية قانونية في إطار اتفاقية بودابست لسنة 2001.

1. المحاولات الأولى لتقسيم جرائم الوسط الرقمي: مع بدايات تجريم المشرع المقارن في بعض الدول للسلوكيات المتصلة بالوسط الرقمي؛ حاول الفقه الجنائي وحتى الجهات الرسمية التدخل بغرض حصرها وتقسيمها، أو على الأقل وضع قائمة حد أدنى[1]. الأمر الذي برز فيه تقسيم الفقيه الألماني "أولريش سيبر – Ulrich Seiber"، ومن ثم تقسيم مشروع القانون النموذجي لجرائم الكمبيوتر والإنترنت لسنة 1998(ب)، وأخيرا التقسيم التقني القائم على أساس الوسط الرقمي.

أ- **التقسيم الفقهي للألماني "أولريش سيبر – Ulrich Seiber"**: اعتمد الفقيه الألماني في تقسيمه لجرائم الوسط الرقمي في بداية تسعينات القرن الماضي؛ على معياري نوع المعلومات ومحل الجريمة. فقسمها إلى ثلاثة طوائف، تتصل الأولى منها بالجرائم الرقمية الاقتصادية -الماسة بقيمة المعطيات الرقمية-، التي تضم أولا؛ الجرائم الماسة بالمعلومات والأنظمة والبرامج، من دخول غير مصرح به سواءً للتجسس أو للاستعمال في قطاع الأعمال، والإتلاف والتشويه وزرع الفيروسات. وثانيا؛ الجرائم الماسة بمحتوى المعلومات المالية في إطار الاحتيال الرقمي. وثالثا؛ الجرائم التقليدية في إطار قطاع الأعمال[2].

---

[1] الأمر الذي نجد فيه العديد من الأمثلة، سيما ما جاء في إطار قرار "ريو ديجانيرو" لسنة 1994، الصادر في شكل توصية عن مؤتمر الأمم المتحدة الخامس عشر للجمعية الدولية لقانون العقوبات. الذي حدد قائمة حد أدنى للسلوكيات الرقمية واجبة التجريم، لكن من دون تقسيمها إلى طوائف. والمتمثلة في؛ جرائم الاحتيال -الغش المرتبط بالكمبيوتر-، وجرائم تزوير الكمبيوتر -التزوير المعلوماتي-، بالإضافة إلى جرائم الإضرار بالبيانات والبرامج-الإتلاف-، وجرائم تخريب وإتلاف الكمبيوتر، وجرائم الدخول غير المصرح به. **أنظر في ذلك:** مقررات وتوصيات مؤتمر ريو دي جانيرو بشأن جرائم الكمبيوتر، مرجع سابق.

[2] **أنظر:** أيمن عبد الله فكري، مرجع سابق، ص 121. **وأنظر أيضا:** يونس عرب، "جرائم الكمبيوتر والانترنت"، مرجع سابق، ص 22 و23.

وتتمثل الطائفة الثانية في الجرائم الماسة بحرمة الحياة الخاصة، المنطوية أساسا على الاستعمال السيئ للمعلومات الشخصية، والجمع غير المصرح به لهذه المعلومات سواءً أكانت صحيحة أم خاطئة، وإفشائها أو مخالفة القواعد والإجراءات الشكلية ذات الصلة بخصوصية هذا النوع من المعلومات الرقمية. كما تتمثل الطائفة الثالثة والأخيرة حسب هذا التقسيم؛ في تلك التي تهدد المصالح القومية أو السلامة الشخصية للأفراد، والتي تنطوي على السلوكيات الرقمية الماسة بأنظمة الدفاع والطيران في الدولة...الخ[1].

ب- التقسيم البحثي بمشروع القانون النموذجي لجرائم الكمبيوتر والإنترنت لسنة 1998: حاولت العديد من الجهات البحثية الأمريكية، إيجاد معايير قانونية تقسم من خلالها جرائم الوسط الرقمي، التي تعددت وتنوعت بحسب المنظور القانوني والتقني. ولعل أهم هذه التقسيمات؛ نجد ذلك الوارد في إطار مشروع القانون النموذجي لجرائم الكمبيوتر والانترنت المعد سنة 1998 من قبل فريق بحث علمي، الذي قسمها إلى ستة أنواع. فتتمثل الطائفة الأولى في تلك التي تستهدف الأشخاص، في صورة الجرائم غير الجنسية كالقتل بالآلة والتحريض على الانتحار والدخول غير المصرح به...الخ. والجرائم الجنسية، كتحريض القصر على الجنس غير المشروع، ونشر أو تسهيل نشر المواد الفاحشة عبر الشبكة...الخ[2].

وأما الطائفة الثانية فتنطوي على جرائم الأموال عدا السرقة والاحتيال، التي تضم جرائم الدخول غير المصرح به المادي والشكلي بكل سلوكياتها الممكنة. كما تحتوي الطائفة الثالثة على جريمتي السرقة والاحتيال، عن طريق التلاعب بالمعلومات والنظم أو استعمالها لغرض السرقة أو الاحتيال. هذا وتم تخصيص طائفة رابعة إضافية لتجريم سلوك التزوير الرقمي، سواءً ذلك المتصل بتزوير الوثائق أو الهوية. ووفق النهج نفسه؛ تم تجريم المقامرة بطائفة منفصلة خامسة، مع إضافة تحت عنوانها باقي جرائم الأخلاق والآداب. ونجد كآخر طائفة؛ ما تم تسميتها بالجرائم ضد الحكومة، التي تشمل كل صور تعطيل أعمال الحكومة وتنفيذ القانون، من عبث بالأدلة القضائية والحصول على معلومات سرية وبث البيانات من مصادر مجهولة...الخ[3].

ج- التقسيم التقني المتصل بالوسط الرقمي: بالإضافة إلى التقسيمات المذكورة وغيرها؛ ظهر فريق يؤسس تقسيمه لجرائم الوسط الرقمي، إما على البحث في دور هذا الوسط، أو على التفرقة بين مكوناته من حيث التدخل في ارتكاب الجريمة. فبالنظر إلى دورها؛ تم تقسيمها إلى الجرائم التي يكون الوسط الرقمي هدفها، والجرائم التي يكون هو أداة ارتكاب الجريمة، والجرائم التي يكون بيئة ارتكابها. حيث يكون النطاق الافتراضي هدفا للجريمة؛ عن طريق الدخول غير المشروع والمساس بالمعطيات والأنظمة الرقمية. كما يكون هو الأداة الإجرامية؛ في حال استعماله لارتكاب الجرائم المتصلة بالطائفة الأولى،

---

[1] **أنظر:** يونس عرب، "جرائم الكمبيوتر والانترنت"، مرجع سابق، ص 22 و23.

[2] **أنظر:** أيمن عبد الله فكري، مرجع سابق، ص 132 و133.

[3] **أنظر:** المرجع نفسه، ص ص 134-163.

أو أي جريمة أخرى يمكن أن ترتكب من خلاله، كالتزوير والتحويل غير المشروع للأموال من الحسابات البنكية...الخ. ويكون الوسط الرقمي بيئة الجريمة؛ في العديد من الحالات، سيما عندما يستعمل لتخزين البرامج المقرصنة[1].

وعلى عكس ما ذكر؛ يفرق البعض الآخر بين الجرائم محل الدراسة، عن طريق التمييز بين جرائم النطاق الافتراضي للجهاز وجرائم النطاق الافتراضي للشبكة. ومنه تعد من قبيل الجرائم المتصلة بالجهاز؛ كل تلك المذكورة سابقا والممكن أن تتعلق تقنيا بالمعلومات الرقمية أثناء مرحلة معالجتها و/أو تخزينها. وتعد الجرائم المتصلة بالشبكية؛ كل الجرائم سابقة الذكر وحتى غيرها التي من الممكن تقنيا أن تتعلق بالمنظومة الشبكية و/أو المعلومات الرقمية المتناقلة عبرها. الأمر الذي يرى فيه العديد من الفقه؛ أنه تقسيم غير دقيق، سيما من حيث التكامل التقني الحديث بين الجهاز والشبكة[2].

2. تقسيم اتفاقية بودابست لجرائم الوسط الرقمي: ظلت الدراسات الفقهية والمؤسساتية؛ تتضارب من حيث وضع معايير قانونية تقسم من خلالها الجرائم محل الدراسة. الأمر الذي أدى بالعديد إلى الاقتناع بعدم إمكانية حصرها وإظهارها في قالب تقسيم معين. ومنه أصبح الهدف وضع قائمة حد أدنى للسلوكيات واجبة التجريم، وتقسيمها وفق معيار أكثر وضوحا وتماشيا مع التطور السريع للوسط الرقمي. وهو ما جاءت به اتفاقية بودابست لسنة 2001–الاتفاقية الأوروبية المتعلقة بالجرائم السيبرانية–، كأول اتفاقية ملزمة في هذا الإطار. والتي تعد المصدر الأول مضمونا وتقسيما؛ لأغلب الاتفاقيات الدولية والإقليمية الواردة بعدها، وحتى للدراسات المؤسساتية ذات الصلة بالجرائم نفسها[3].

وتم تقسيم الجرائم محل الدراسة في إطار اتفاقية بودابست إلى خمسة أنواع. حيث عنونت المجموعة الأولى بـــ "الجرائم المستهدفة لوفرة وسرية وتكامل المعطيات والنظم"، التي تضم؛ الدخول غير المشروع والاعتراض غير القانوني وتدمير المعطيات واعتراض النظم. واتصلت المجموعة الثانية بـــ "الجرائم المرتبطة بالجهاز"، التي تضم جريمتي التزوير والاحتيال المرتبط بالجهاز. كما تضمنت المجموعة الثالثة المعنونة بـــ "الجرائم المرتبطة بالمحتوى"؛ جرائم الأفعال الإباحية وغير الأخلاقية. وأما المجموعة الرابعة فتعلقت بـــ "الجرائم ضد الملكية الأدبية والحقوق المجاورة"، المنطوية على طائفة واحدة بنفس مفهوم

---

[1] **أنظر:** عمرو عيسى القي، الجرائم المعلوماتية-جرائم الحاسب الآلي والإنترنت في مصر والدول العربية، المكتب الجامعي الحديث، مصر، 2006، ص 85. **نقلا عن:** فتيحة رصاع، (الحماية الجنائية للمعلومات على شبكة الإنترنت)، مذكرة لنيل شهادة ماجستير في القانون العام، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، الجزائر، 2012، ص 70. **وأنظر أيضا:** "جرائم الكمبيوتر والانترنت"، مرجع سابق، ص 16.

[2] **أنظر:** يونس عرب، "صور الجرائم الالكترونية واتجاهات تبويبها"، مرجع سابق ص 13 و14.

[3] وأبرز دليل على ذلك؛ نجد الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، التي صدقت عليها الجزائر سنة 2014-كما بينا سابقا-. حيث جرمت كل السلوكيات الوارد تجريمها في إطار اتفاقية بودابست لسنة 2001، مع العمل بنهج آخر منطوي على عدم التقسيم إلى طوائف معينة. **أنظر في ذلك:** المواد من 02 إلى 18؛ مرسوم رئاسي رقم 14-252، مرجع سابق.

العنوان. وأخيرا نجد المجموعة الخامسة التي تسمى بـــ "الجرائم المرتبطة بالأشخاص والأموال"، المجرمة للسرقة والاحتيال والتزوير والإطلاع على البيانات الشخصية والمعلومات المضللة والزائفة، أنشطة الاعتداء على الخصوصية وإساءة استخدام المعلومات، القرصنة...الخ[1].

ثانيا: تقسيم المشرع الجزائري لجرائم الوسط الرقمي

لم يتطرق المشرع الجزائري في البداية إلى تقسيمات جرائم الوسط الرقمي، بل اكتفى بتجريم المساس بأنظمة المعالجة الآلية للمعطيات، والنص في نصوص متفرقة على بعض الجرائم الممكن وصفها على أنها جرائم وسط رقمي بالنظر إلى مسرحها[2]. إلا أنه رجع في مرحلة لاحقة؛ ووضع تقسيما لهذه الجرائم تحت تسمية جرائم تكنولوجيات الإعلام والاتصال كما بينا سابقا. حيث قسمها إلى قسمين، ينطوي الأول على جرائم المساس بأنظمة المعالجة الآلية للمعطيات، ويتصل الثاني بالجرائم التقليدية التي يكون النطاق الافتراضي للوسط الرقمي وسيلتها أو المسهل لارتكابها[3].

1. جرائم المساس بأنظمة المعالجة الآلية للمعطيات: عمل المشرع الجزائري امتدادا ونقلا عن التشريعات المقارن، سيما الفرنسي منها؛ على تجريم السلوكيات الماسة بأنظمة المعالجة الآلية للمعطيات تحت التسمية الموضحة أعلاه. والتي تعد بالأساس قائمة الحد الأدنى للسلوكيات واجبة التجريم في هذا الوسط. حيث جرم المشرع الجزائري من خلال ذلك؛ الدخول و/أو البقاء الشكلي والمادي من جهة،

---

[1] **أنظر:** - Arts de 01 à 10; Convention sur la cybercriminalité- Budapest, op.cit.

[2] حيث بدأ المشرع الجزائري بتجريم بعض السلوكيات الرقمية لأول مرة سنة 2001، بتجريمه للاسائة الموجهة ضد رئيس الجمهورية عن طريق عناصر الوسط الرقمي، وقام بعد ذلك سنة 2004؛ بتجريم المساس بأنظمة المعالجة الآلية للمعطيات في إطار جرائم الأموال. على أنه واصل بعد ذلك تجريم بعض السلوكيات التقليدية المرتكبة عبر النطاق الافتراضي للوسط الرقمي، لكن بنصوص متفرقة من دون تقسيمها وفق معايير معينة. وهو الأمر المستمد أساسا من المشرع الفرنسي الذي اعتمد النهج نفسه، ولو أنه تميز عن نظيره الجزائري؛ بتعديله لأغلب النصوص المتصلة بالجرائم التقليدية التي يمكن تصور ارتكابها عبر الوسط الرقمي، في إطار احترام مبدأ الشرعية الجنائية. **أنظر في ذلك:** المادة 07 المضيفة للمادة 147 مكرر؛ قانون رقم 01-09، مؤرخ في 26 جوان 2001، يعدل ويتمم أمر رقم 66-156، يتضمن قانون العقوبات، (ج ر) عدد 34، صادر بتاريخ 27 جوان 2001. **وأنظر أيضا:** المادة 12 المضيفة للمواد من 394 مكرر إلى 394 مكرر7؛ قانون رقم 04-15، مؤرخ في 10 نوفمبر 2004، يعدل ويتمم أمر رقم 66-156، يتضمن قانون العقوبات، (ج ر) عدد 71، صادر بتاريخ 10 نوفمبر 2004. **وأنظر كذلك:**

- BRETON Thierry, "Chantier sur la lutte contre la cybercriminalité", Rapport remis a Monsieur le Ministre de l'Intérieur, de la Sécurité Intérieure, France, 25 février 2005, p p 20-22. Disponible sur le Lien: http://www.ladocumentationfrancaise.fr/rapports-publics/054000263/index.shtml.

[3] وهو التقسيم الذي اعتمده المشرع الجزائري صراحة بقانون القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الصادر سنة 2009، بنصه: "الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية". **أنظر في ذلك:** المادة 02/1-أ؛ قانون رقم 09-04، مرجع سابق.

كما لا يعد المشرع الجزائري الوحيد الذي انتهج هذا التقسيم، حيث نجد العديد من التشريعات المقارنة العاملة بذلك، على غرار المشرع الأردني. ولو أنه تطرق لذلك بقانون خاص، يوسع من السلوكيات المجرمة بصورة منفصلة عن قانون العقوبات، ومن ثم أكمل باقي الفراغ التشريعي؛ بالنص على أن كل الجرائم التقليدية المتصلة بالوسط الرقمي تعد سلوكيات مجرمة ومعاقب عليها. **أنظر في ذلك:** المادة 15؛ قانون رقم 15-27، يتعلق بالجريمة الالكترونية، الأردن، مرجع سابق.

والمساس المنفصل بالمعلومات الرقمية من جهة أخرى، والسلوكيات الأخرى الإضافية الداخلة في الإطار نفسه من جهة ثالثة.

أ- جرائم الدخول و/أو البقاء الشكلي والمادي: جرم المشرع الجزائري؛ فعل الدخول و/أو البقاء إلى المنظومة المعلوماتية في صورتيه الشكلي والمادي. حيث يعد مجرما مجرد الاعتماد على الغش؛ للدخول و/أو البقاء أو الدخول من دون البقاء أو البقاء بعد الدخول الشرعي؛ في المنظومة المعلوماتية أو في جزء منها أو بما يتجاوز الزمن المحدد[1]. كما يعد مجرما أيضا ما يسمى بالدخول والبقاء المادي؛ الذي يقود إلى المساس بالمعطيات المعلوماتية عن طريق الحذف أو التغيير، أو المساس بالمنظومة المعلوماتية عن طريق التخريب[2].

ب- جرائم المساس المنفصل بالمعلومات الرقمية: جرم المشرع العديد من السلوكيات الأخرى، التي من الممكن أن تقود إلى المساس بالمعلومات الرقمية المتواجدة في المنظومة المعلوماتية من دون لا دخول ولا بقاء[3]. حيث تم تجريم الاعتداء المنفصل على المعلومات الرقمية، عن طريق الإدخال بالغش؛ أي معطيات جديدة أو إزالة أخرى موجودة أو التعديل فيها[4]. كما جرم أيضا التقاط واعتراض المعلومات الرقمية من دون ترخيص، ولو بشكل ضمني في إطار النصوص التقليدية المعدلة[5].

ج- تجريم السلوكيات الأخرى الداخلة في إطار المساس بأنظمة المعالجة الآلية للمعطيات: بالإضافة إلى السلوكيات الموضحة أعلاه؛ عمل المشرع على تجريم بعض السلوكيات الأخرى ذات الصلة بالأولى المجرمة. على غرار تجريم الأعمال التحضيرية والتالية للجرائم الموضحة أعلاه، والشروع فيها. حيث جرم كل عمل متصل بالمعلومات الرقمية المحضرة لغرض ارتكاب الجرائم السابقة بالذكر، في شاكلة التصميم أو البحث أو التجميع أو التوفير أو النشر أو الاتجار بالمعلومات المخزنة أو المعالجة أو المرسلة. كما جرم أيضا؛ حيازة أو إفشاء أو نشر أو استعمال مهما كان الغرض للمعلومات المتحصل عليها من إحدى الجرائم المذكورة أعلاه[6]. وبالإضافة إلى ذلك؛ اعتبر المشرع أن كل الجنح ذات الصلة بالمساس بأنظمة المعالجة الآلية للمعطيات هي جرائم معقب على الشروع فيها[7].

---

[1] **أنظر:** المادة 394 مكرر/1؛ أمر رقم 66-156، مرجع سابق.

[2] **أنظر:** المادة 394 مكرر/2و3؛ المرجع نفسه.

[3] إلا أنه ما يلاحظ على المشرع الجزائري في هذا الإطار؛ أنه أهمل تجريم الاعتداء المنفصل على المنظومة المعلوماتية، رغم كونه أبرز السلوكيات الضارة التي قد تحصل بشكل منفصل عن الدخول والبقاء المادي للمنظومة نفسها. الأمر الذي لم تغفل عنه أغلب التشريعات المقارنة، سيما المشرعان الفرنسي والأردني. **أنظر في ذلك:** المادة 04؛ قانون رقم 15-27، يتعلق بالجريمة الالكترونية، الأردن، مرجع سابق. **وأنظر أيضا:** Art 232-2; code pénale français, op.cit. -

[4] **أنظر:** المادة 394 مكرر1؛ أمر رقم 66-156، المرجع نفسه.

[5] **أنظر:** المادة 303 مكرر؛ المرجع نفسه.

[6] **أنظر:** المادة 394 مكرر2؛ المرجع نفسه.

[7] **أنظر:** المادة 394 مكرر7؛ المرجع نفسه.

2. الجرائم التقليدية التي يكون النطاق الافتراضي للوسط الرقمي وسيلتها أو المسهل لارتكابها: بالإضافة إلى جرائم المساس بأنظمة المعالجة الآلية للمعطيات؛ اعتمد المشرع الجزائري ما يسمى بمبدأ الشرعية العام، الذي بموجبه اعتبر كل السلوكيات المجرمة تقليديا التي يمكن تصور ارتكابها في إطار النطاق الافتراضي للوسط الرقمي أو أن يكون مسهلا لارتكابها؛ من السلوكيات المجرمة والداخلة في إطار جرائم الوسط الرقمي[1].

ومنه يمكن تصور ارتكاب العديد من الجرائم التقليدية في الإطار الرقمي الافتراضي أو بتسهيل منه، سيما جرائم الأموال من سرقة ونصب وخيانة الأمانة[2]. وجرائم الشرف والاعتبار، من قذف وسب واهانة وإساءة واستهزاء[3]. بالإضافة إلى جرائم الآداب، على غرار الترويج للدعارة والاستغلال الجنسي للقصر[4]. كما تعد مجرمة أيضا؛ السلوكيات الرقمية الهادفة إلى الترويج للإرهاب والإشادة به والبحث عن مصادر تمويله[5]. وإضافة إلى كل الجرائم المذكورة؛ يمكن القول أن المشرع الجزائري يدخل ضمن إطار التصنيف محل الطرح؛ كل سلوك مجرم تقليديا مهما كان تكييفه أو تصنيفه، يقبل بطبيعته أن يرتكب عبر النطاق الافتراضي للوسط الرقمي أو أن يكون مسهلا لارتكابه.

وفي ختام المبحث الأول؛ يمكن القول أن التسليم باكتساب جرائم الوسط الرقمي للخصوصية المتأتية من افتراضية وحداثة مسرحها الجرمي؛ أصبح واقعا موضوعيا لا مفر منه. وهو واجب المواجهة بالمنظور الحديث نفسه، الذي يتناسب مع الطبيعة الرقمية الافتراضية نفسها. فولوج التجريم إلى الوسط الرقمي واعتباره مسرحا حديثا للجريمة؛ أكسب هذا النوع من الإجرام الحديث؛ كثيرا من الخصوصية الموضوعية غير المسبوق التعامل معها ولا مع مثلها.

ورجوعا إلى القاعدة الإجرائية المذكورة سابقا، التي مفادها أن دور القواعد الإجرائية يبدأ عند انتهاء دور القواعد الموضوعية؛ نفترض مسبقا وقبل الدراسة الإجرائية المعمقة؛ أن النصوص الإجرائية التقليدية ستكون عاجزة على التحري والتحقيق في جرائم الوسط الرقمي. سيما إذا ما علمنا أنها إجراءات؛ وضعت لمواجهة جرائم ذات مسرح مادي تقليدي قليل التعقيد مقارنةً بنظيره الرقمي الافتراضي. وهو الأمر الذي سنرى مدى صحته قانونا في المبحث الموالي بالدراسة، بعد أن نتطرق إلى إجراءات التحري والتحقيق في المسرح الافتراضي لجرائم الوسط الرقمي، من حيث بيان أهم أحكامها الأساسية، التقليدية والحديثة، والمرقمنة.

---

[1] **أنظر:** المادة 1/02-أ؛ قانون رقم 09-04، مرجع سابق.

[2] **أنظر:** المواد 1/350 و1/372 و1/376؛ أمر رقم 66-156، مرجع سابق.

[3] **أنظر:** المواد 296 و297 و146 و144مكرر2؛ المرجع نفسه.

[4] **أنظر:** المادتان 140 و141؛ قانون رقم 15-12، مؤرخ في 15 جوان 2015، يتعلق بحماية الطفل، (ج ر) عدد 39، صادر بتاريخ 19 جوان 2015.

[5] **أنظر:** المادة 87مكرر4؛ أمر رقم 66-156، المرجع نفسه.

المبحث الثاني

إجراءات التحري والتحقيق في مواجهة المسرح الجرمي الافتراضي

شهدت الإجراءات الجزائية المعتمدة من القانون الجزائري؛ العديد من التعديلات والتتميمات المتتالية منذ أول قانون صادر سنة 1966. الأمر الذي سار وفق نمط معين لا يمس بالمبادئ الإجرائية العامة، المتصلة أساسا بالجريمة التقليدية الظاهرة في الحيز المادي الملموس. حيث كرس المشرع الجزائري بكل تعديلاته وتتميماته لقانون الإجرائية الجزائية؛ القاعدة الإجرائية المنطوية على ضرورة العمل بإجراءات من الطبيعة نفسها للجريمة المرتكبة. وبشكل أدق أقر المشرع في إطار التحري والتحقيق؛ إجراءات استقرت من حيث الأجهزة والأعمال، وان عدلت وتممت بجزئيات لا تغير من طبيعتها المادية.

وبمجرد محاولة المقاربة البحثية بين الخصوصية الافتراضية لمسرح جرائم الوسط الرقمي أولا، والطبيعة المادية لإجراءات التحري والتحقيق الجنائي التقليدية ثانيا؛ تبرز المفارقة القانونية المنطوية على العديد من الصعوبات واجبة المواجهة، سيما أنها إجراءات ذات صلة بحماية حرية الأفراد وسلامة أجسادهم وأموالهم وأرواحهم. الأمر الذي للفقه والمشرع فيه نظرة حديثة، إن من حيث الوجه الحديث للإجراءات محل الدراسة، أو بخصوص استحداث آليات حديثة ذات طابع وقائي.

ولا يمكن التوصل إلى إبراز المواجهة الإجرائية من حيث التحري والتحقيق ذات الصلة بالمسرح الجرمي الافتراضي؛ إلا بتحديد مفهوم هذه الإجراءات من منطلق تقليدي منطقي، مع تبيان عجزها عن مواجهة المسرح الجرمي الافتراضي(مطلب أول)، ومن ثم إبراز التوجه الإجرائي المستحدث لمواجهة العجز المذكور(مطلب ثانٍ).

المطلب الأول: عجز إجراءات التحري والتحقيق التقليدية عن مواجهة المسرح الجرمي الافتراضي

أحدث الوسط الرقمي عموما والمسرح الجرمي الافتراضي الذي أوجدته عناصره خصوصا؛ ما يمكن وصفه بالأزمة الإجرائية من حيث التحري والتحقيق. فبعد أن استقرت النصوص الإجرائية التقليدية ذات الصلة، برز الوسط الرقمي ليأتي بمسرح رقمي ثنائي، بطابع افتراضي غير ملموس ولا يتصل بالحيز الخارجي المعروف. وهو ما واجهت بشأنه الجهات القضائية وشبه القضائية المختصة؛ العديد من الصعوبات التي نؤسس من خلالها للعجز الإجرائي المقصود.

وفي سبيل الوقوف على العجز الإجرائي المذكور؛ وجب البحث أولا في المفهوم التقليدي لإجراءات التحري والتحقيق، من حيث طرح تعريفها وأهم مميزاتها(فرع أول)، ومن ثم إبراز أهم المظاهر الدالة على عجز هذه الإجراءات في مواجهة المسرح الجرمي الافتراضي(فرع ثانٍ).

الفرع الأول: المفهوم التقليدي لإجراءات التحري والتحقيق

رغم الخلط الاصطلاحي الذي تقع فيه العديد من الدراسات القانونية والدارسون بالأساس؛ بخصوص التعامل مع مصطلحي التحري والتحقيق من حيث موضعهما ودلالتهما الإجرائية؛ إلا أنهما مصطلحان منفصلان أصلا ودلالة. حيث يقصد بالتحري أولى المراحل الجزائية، ويستدل بالتحقيق على الإجراءات التي تليها، ولكل منهما مضمون قانوني إجرائي خاص، إن من حيث المفهوم والسمات الأساسية أو بخصوص النطاق والجهات المختصة والأعمال الإجرائية ذات الصلة.

وفي سياق متصل؛ سعى المشرع الجزائري إلى تنظيم التحري والتحقيق بنصوص وأحكام إجرائية، يمكن من خلالها التوصل إلى المفهوم العام التقليدي للإجراءات محل الطرح. وهو ما سنبينه من خلال التطرق أولا إلى مفهوم إجراءات التحري(أولا)، وتبيان ثانيا مفهوم إجراءات التحقيق(ثانيا).

أولا: المفهوم التقليدي لإجراءات التحري

لم يتطرق المشرع الجزائري كغيره من نظرائه إلى إجراءات التحري كمرحلة إجرائية تمهيدية[1]؛ من حيث تحديد مفهومها العام، حيث اكتفى بتبيان الإجراءات ذات الصلة، التي يمكن من خلالها الوصول إلى المفهوم المقصود. وهو ما عمل به الفقه الجنائي الدارس والباحث في هذا الإطار، الذي وضع العديد من التعريفات ذات الصلة بمرحلة التحري، واستنبط من خلال ذلك أيضا العديد من المميزات الإجرائية للمرحلة نفسها.

1. تعريف التحري كمرحلة إجرائية: تتعدد التعريفات المسندة لمرحلة التحري أو مرحلة جمع الاستدلالات الجنائية، سيما بالنظر إلى النظام الإجرائي المتبع. حيث يفهم مما جاء به المشرع الجزائري بخصوص الصلاحيات العادية للشرطة القضائية؛ أن مرحلة التحري هي: "مجموعة الإجراءات الهادفة إلى البحث والتحري عن الظروف والملابسات ذات الصلة بالجرائم ومرتكبيها قبل تحريك الدعوى العمومية"[2].

---

[1] تختلف التسمية القانونية الدالة على مرحلة التحري. حيث نجد المشرع الجزائري يتناقض في طرح التسميات، فعنون الباب الأول من الكتاب الأول "ق.إ.ج" بـ "في البحث والتحري عن الجرائم"، وهو الذي يحتوي على إجراءات متصلة بمرحلة التحري وفق نطاقها التالي بالدراسة. على أنه رجع ليعنون الباب الثاني من الكتاب نفسه بـ "في التحقيقات"، والفصل الثاني من الباب نفسه بـ "في التحقيق الابتدائي"؛ رغم اتصالهما بالمرحلة نفسها. **أنظر في ذلك:** أمر رقم 66-155؛ مرجع سابق.

وفي الإطار نفسه؛ يجد الفقه الجنائي العديد من التسميات لمرحلة التحري. حيث قد تسمى بالتحقيق التمهيدي، أو المرحلة شبة القضائية، أو المرحلة التمهيدية الاستدلالية، أو مرحلة البحث والتحري. **أنظر في ذلك:** عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، الطبعة الرابعة، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2013، ص 191 و192.

[2] **أنظر:** المادة 3/12؛ أمر رقم 66-155، المرجع نفسه.

ويعرفها العديد من الفقه الجنائي، سيما المصري منه؛ على أنها: "مجموعة من الإجراءات التمهيدية السابقة على تحريك الدعوى الجنائية، تهدف إلى جمع المعلومات في شأن جريمة ارتكبت كي تتخذ سلطات التحقيق بناءً عليها القرار فيها إذا كان من الملائم تحريك الدعوى الجنائية". **أنظر في ذلك:** محمود محمد محمود جابر، الأحكام الإجرائية للجرائم الناشئة عن استخدام الهواتف النقالة، الكتاب الثاني، دار الكتب والوثائق القومية، القاهرة، مصر، 2018، ص 15 و16.

وعلى عكس ما يعتقد العديد؛ فان مرحلة التحري لا تهدف إلى الكشف عن الحقيقة، بل يقتصر دورها على مجرد المرحلة التمهيدية لإجراءات التحقيق القضائي التي تهتم بجمع الأدلة. وهي تنجز قبل تحريك الدعوى العمومية، ليتم من خلالها الاستدلال والتنقيب والتحري، بغرض جمع المعلومات اللازمة للتصرف من الجهة المختصة بتحريك الدعوى من عدمها، وليس لتوضيح عناصر الدعوى لقاضي الحكم[1].

2. مميزات التحري كمرحلة إجرائية: تمتاز مرحلة التحري وفق التعريف الموضح؛ بالعديد من السمات الأساسية التي تميزها عن إجراءات التحقيق التالية بالدراسة. حيث تعتبر مرحلة إجرائية تمهيدية، وذات طابع ضروري ولازم، كما تعتبر مرحلة ذات إجراءات تمس مباشرة بالحقوق والحريات الفردية، ويسمى فيها الشخص المتابع بالمشتبه فيه.

أ- **مرحلة تمهيدية:** تعتبر مرحلة التحري؛ بمثابة الإجراءات التمهيدية للإجراءات المتصلة بالتحقيق القضائي. حيث تقوم الجهات المختصة بعد أن يصل إلى علمها ارتكاب جريمة ما؛ بالعديد من الأعمال الإجرائية؛ بغرض الاستدلال وجمع المعلومات الشخصية والموضوعية ذات الصلة، التي تتصرف فيها النيابة العامة وفق الأحكام المقررة لذاك[2]. وتبدأ مرحلة التحري وفق القانون الجزائري؛ بمجرد الوصول إلى علم الشرطة القضائية بوقوع سلوك مجرم قانونا بإحدى الطرق القانونية الممكنة. حيث يكون ذلك إما في إطار ممارسة الشرطة القضائية لمهامها العادية عن طريق تلقي الشكاوى والبلاغات من الأشخاص[3]، أو بمعاصرة ضباط الشرطة القضائية أو ممثل النيابة العامة؛ للجناية أو الجنحة في إطار حالات التلبس المحددة حصرا[4].

كما تنتهي مرحلة التحري؛ بعد القيام بالاستدلالات اللازمة عن طريق الأعمال الإجرائية التالية بالدراسة، وإرسال الملف إلى ممثل النيابة العامة؛ ليتصرف فيه وفق الحالات القانونية الممكنة. والتي تكون عن طريق إعمال سلطة الملائمة؛ بالأمر بمواصلة السير في الإجراءات، أو بوضع نهاية لذلك[5].

---

[1] **أنظر:** محمود نجيب حسني، شرح قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، مصر، 1988، ص 499. **نقلا عن:** محمود محمد محمود جابر، مرجع سابق، ص 15 و16.

[2] **أنظر:** محمود محمد محمود جابر، المرجع نفسه، ص 15 و16. **وأنظر أيضا:** ناصر حمودي، (قضاء التحقيق في قانون الإجراءات الجزائية الجزائري-دراسة تحليلية نقدية)، مرجع سابق، ص 13.

[3] **أنظر:** المادة 1/17؛ أمر رقم 66-155، مرجع سابق.

على أن نفرق بين الشكوى والبلاغ. فالشكوى يتقدم بها المتضرر من الجريمة شخصيا أو عن طريق ممثله القانوني. وأما البلاغ؛ فيتقدم به شخص غير متضرر من الجريمة بطريقة مباشرة، في شكل إخطار أو إخبار للجهة المختصة. **أنظر في ذلك:** فضيل العيش، شرح قانون الإجراءات الجزائية بين النظري والتطبيقي، مطبعة البدر، الجزائر، د س ن، ص 100.

[4] **أنظر:** المادة 41 وما يليها؛ أمر رقم 66-155، المرجع نفسه.

ويعرف التلبس عموما؛ على أنه: "المعاصرة أو المقاربة بين لحظتي ارتكاب الجريمة واكتشافها". **أنظر في ذلك:** عبد الله أوهايبية، مرجع سابق، ص 236.

[5] **أنظر:** المادة 1/36-5؛ أمر رقم 66-155، المرجع نفسه.

حيث تنتهي مرحلة التحري؛ إذا ما أمر وكيل الجمهورية المختص بتحريك الدعوى العمومية عن طريق طلب افتتاحي لإجراء تحقيق[1]، أو برفعها أمام المحكمة المختصة عن طريق الاستدعاء المباشر والتكليف بالحضور والمثول الفوري[2]. كما يمكن لوكيل الجمهورية؛ أن يصدر مقرر الحفظ وفق الشروط اللازمة لذلك. أو يقرر إجراء الوساطة بشأن الوقائع ذات الصلة وفق الشروط القانونية[3].

ب- مرحلة ضرورية: قد يعتقد البعض بأن مرحلة التحري لا تكتسي طابع الأهمية والضرورية، نظرا لاقتصارها على الدور التمهيدي فقط، وخاصةً لكونها غير داخلة في الدعوى العمومية ولا دخل للقضاء في متابعتها من البداية. إلا أن الأمر لا يعد كذلك، حيث أنه يجب انتقال ضابط الشرطة القضائية لمعاينة مصرح الجريمة والحفاظ على الأدلة وسماع الشهود، وإلا قد تزول الأدلة ولا يعرف الشاهد من المتهم بعد ذلك. ولعل أبرز دليل يؤكد ضرورتها؛ إلزام المشرع للجهات المختصة بالقيام بإجراءات التحري حتى في الجرائم التي يتمتع أصحابها بحصانة، ومهما كان نوعها. فلو ارتكب نائب أو عضو برلماني جناية أو جنحة؛ يمكن للشرطة القضائية أن تجمع الأدلة بشأنها، وتقدمها لوكيل الجمهورية المختص، الذي يحفظ الأوراق نظرا لوجود مانع الحصانة[4].

كما تعد نتائج مرحلة التحري؛ من أهم الأسس التي يقوم عليها التحقيق القضائي الذي يليها، والحكم الجنائي الفاصل في الدعوى العمومية فيما بعد. حيث تفيد هذه المرحلة؛ في تهيئة أدلة الدعوى العمومية إثباتا أو نفيا، مما يسهل مهمة قضاء التحقيق والحكم في عملية إظهار الحقيقة القانونية عن طريق إزالة الغموض. كما لها أهمية أخرى، تتصل بحفظ الشكاوى والبلاغات غير الجدية، فيتم تلافي إجهاد جهات التحقيق والحكم في وقائع لا أساس لها[5].

ج- مرحلة تمس بالحقوق والحريات: تتصف مرحلة التحري كأصل عام؛ بعدم القهرية والتزام المشروعية النصية. التي مفادها وجوب التزام ضباط الشرطة القضائية؛ بالأحكام الإجرائية المقررة قانونا وتحت رقابة جهاز النيابة العامة من جهة، وعدم استعمال وسائل القهر والجبر ضد المشتبه فيه من جهة أخرى[6]. الأمر الذي وردت عليه العديد من الاستثناءات، التي تجعل منها مرحلة ماسة بالحقوق والحريات. سيما بخصوص إمكانية تجاوز رجال الشرطة القضائية للأحكام الإجرائية المقررة قانونا، من

---

[1] **أنظر:** المادة 67؛ أمر رقم 66-155، مرجع سابق.

[2] **أنظر:** المادة 333؛ المرجع نفسه.

[3] **أنظر:** المادة 37مكرر وما يليها؛ المرجع نفسه.

[4] **أنظر:** عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، مرجع سابق، ص 193 و194.

[5] **أنظر:** محمود محمد محمود جابر، مرجع سابق، ص 16.

[6] **أنظر:** ناصر حمودي، (قضاء التحقيق في قانون الإجراءات الجزائية الجزائري-دراسة تحليلية نقدية)، مرجع سابق، ص ص 11-13. **وأنظر أيضا:** عبد الله أوهايبية، المرجع نفسه، ص 194.

دون أن يقرر القانون البطلان للإجراء نفسه، وكما هو معروف إجرائيا؛ لا بطلان إلا بنص صريح يقرره. ولعل أبرز دليل على ذلك نجد أن المشرع بالمادة 48 "ق.إ.ج"؛ قد رتب البطلان عن مخالفة أغلب إجراءات التفتيش، إلا تلك المتصلة بالحصول على الإذن بالتفتيش وإجراءات استظهاره للمعني[1].

كما قد تتصف مرحلة التحري كاستثناء بالجبرية والقهرية، ولا تعتد برضا المعني بها –المشتبه فيه–، ما يمس بحقوق الأفراد وحرياتهم. ولعل أبرز دليل على ذلك؛ نجد إجراء التوقيف للنظر الذي قد يؤدي إلى حبس المشتبه فيه لمدة 48 ساعة، قابلة للتجديد في بعض الجرائم لتصل إلى 5 مرات كاملة. وهذا رغم مساس ذلك صراحةً؛ بمبدأ عدم جواز حبس أي شخص قبل استجوابه من القضاء[2]. والأمر نفسه؛ بخصوص تفتيش المنازل في حالة التلبس؛ الذي يكون بصورة جبرية ومن دون رضا صاحبه[3].

وكإجراء جديد معتمد من المشرع بموجب التعديل الوارد سنة 2015؛ يمكن لوكيل الجمهورية أن يأمر بمنع كل شخص توجد ضده دلائل ترجح ضلوعه في جناية أو جنحة من مغادرة التراب الوطني[4]. وهو ما يعد مساسا خطيرا بحق المشتبه فيه في التنقل، سيما أن مصدره لا يمثل القضاء كهيئة مستقلة[5].

د- مرحلة يسمى فيها الشخص المعني بالمشتبه فيه: عادةً ما يستعمل المشرع الجنائي على وجه الخصوص؛ مصطلحات دالة لا نجد لها مرادفات. حيث في إطار مرحلة التحري بكل جزئياتها إلى غاية انتهائها وفق ما بينا سابقا وأعلاه؛ يدعى الشخص الذي يكون تحت الامتحان الجنائي بالمشتبه فيه وليس بالمتهم. وعلى العكس من ذلك؛ يطلق على الشخص الذي يكون متابعا بجريمة بعد تحريك الدعوى العمومية أو رفعها؛ بالمتهم ويستمر بحمل الصفة الجنائية ذاتها إلى غاية صدور الحكم النهائي البات في القضية، ليصبح بعد ذلك إما مدانا أو بريئا[6].

---

[1] **نص المادة:** "يجب مراعاة الإجراءات التي استوجبتها المادتان 45 و47 ويترتب عن مخالفتها البطلان". مع العلم أن الأحكام ذات الصلة بإذن التفتيش؛ نظمت بالمادة 44 من القانون نفسه.

ولو أن المشرع بتعديله لقانون الإجراءات الجزائية سنة 2015؛ قلص من إمكانية إيداع المشتبه فيه الحبس على اختلاف صوره. وهذا باعتماده للمثول الفوري وإلغائه لسلطة الإيداع في حالة التلبس. **أنظر في ذلك:** المادة 16 المضيفة للمادة 339مكرر وما يليها، والمادة 26؛ أمر رقم 15-02، مؤرخ في 23 يوليو 2015، يعدل ويتمم أمر رقم 66-155، يتضمن قانون الإجراءات الجزائية، (ج ر) عدد 40، صادر بتاريخ 23 يوليو 2015.

[2] **أنظر:** فضيل العيش، مرجع سابق، ص 208. **وأنظر أيضا:** المادتان 51 و65؛ أمر رقم 66-155، مرجع سابق.

[3] ولو أن المشرع جعله برضا صاحب المنزل، ومن دون جبرية في الحالة العادية غير المتصلة بالتلبس. **أنظر في ذلك:** المادتان 44 و64؛ أمر رقم 66-155، المرجع نفسه.

[4] **أنظر:** المادة 36مكرر1 المضافة بالمادة 07؛ أمر رقم 15-02، المرجع نفسه.

[5] **أنظر:** أمقران طيبي، "المنع من السفر بين الإطلاق والتقييد"، ورقة عمل مقدمة وفق متطلبات المشاركة في الملتقى الوطني الثالث بعنوان تطورات النظم الإجرائية الجزائية في ضوء التعديلات الإجرائية الأخيرة والتعديل الدستوري لسنة 2016، كلية الحقوق والعلوم السياسية، جامعة أكلي محند أولحاج، البويرة، الجزائر، 23 و24 ماي 2017، ص 14.

[6] **أنظر:** عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، مرجع سابق، ص 195 و196. **وأنظر أيضا:** المواد 40 و45 و2/67 و82 و86 و100 و121 وغيرها؛ أمر رقم 66-155، المرجع نفسه.

ثانيا: المفهوم التقليدي لإجراءات التحقيق

سار المشرع الجزائري وفق النهج نفسه؛ المتصل بالتعامل مع إجراءات التحري السابقة بالذكر. حيث لم يتطرق إلى التحقيق كمرحلة إجرائية ثانية ومنفصلة. بل اكتفى بعرض الإجراءات ذات الصلة، التي يمكن من خلالها التوصل إلى المفهوم العام التقليدي للتحقيق القضائي. وفي سبيل ذلك وجب أن نستعرض تعريف التحقيق على اختلاف صوره، ومن ثم نبين أهم المميزات الإجرائية ذات الصلة. على أن نبرز بعد ذلك نقاط التوافق والتباين بين إجراءات التحقيق ومرحلة التحري.

1. تعريف إجراءات التحقيق: تختلف التعاريف المسندة إلى إجراءات التحقيق القضائي، على حسب النظام القضائي المتبع في الدولة، الدائر بين إما الفصل بين سلطتي الاتهام والتحقيق أو دمجهما في يد جهة واحدة. وعلى العموم يمكن أن نعرف التحقيق القضائي، في إطار القانون الجزائري انطلاقا من مهام قاضي التحقيق على أنها: "مجموعة من الإجراءات القضائية الهادفة إلى الكشف عن الحقيقة، بالبحث في أدلة الاتهام والنفي في الوقت نفسه"[1].

وتنقسم إجراءات التحقيق القضائي في القانون الجزائري؛ إلى مرحلتين ودرجتين[2]. حيث نجد التحقيق الابتدائي والتحقيق النهائي من جهة، والدرجة الأولى والثانية في التحقيق الابتدائي نفسه من جهة أخرى. فالتحقيق الابتدائي؛ هو الذي يمارسه قضاء التحقيق المكون من قاضي التحقيق كدرجة أولى وغرفة الاتهام كدرجة ثانية. ويأتي كمرحلة أولى من مراحل الدعوى العمومية، ومرحلة ثانية من مراحل الإجراءات الجزائية عموما، بعد مرحلة التحري السابقة بالذكر، وقبل مرحلة المحاكمة[3].

ويتصف التحقيق الابتدائي عموما؛ بالطابع الإلزامي في الجنايات، والاختياري في الجنح والاستثنائي في المخالفات. حيث يجب أن يُحَقَقْ في الجنايات من قاضي التحقيق ثم من غرفة الاتهام[4]. ولا يجب التحقيق في الجنح والمخالفات؛ إلا إذا أراد وكيل الجمهورية ذلك، أو بتحريك الدعوى العمومية عن طريق

---

[1] **أنظر:** المادة 1/68؛ أمر رقم 66-155، مرجع سابق.

ويعرفها العديد من الفقه الجنائي، سيما المصري منه؛ على أنها: "اتخاذ جميع الإجراءات والوسائل المشروعة وذلك بهدف الوصول إلى الحقيقة وإظهارها". **أنظر في ذلك:** عاشور محمد أنور، الموسوعة في التحقيق الجنائي العلمي، الطبعة الثانية، عالم الكتب، القاهرة، مصر، د س ن، ص 09. **نقلا عن:** أسامة محمد أحمد سليمان، (ضمانات المتهم في مرحلتي الاستدلال والتحقيق الابتدائي)، رسالة لنيل درجة الماجستير في القانون، كلية الدراسات العليا، الجامعة الأردنية، المملكة الأردنية الهاشمية، 1997، ص 79.

[2] على العكس من مرحلة التحري السابقة بالذكر؛ نجد أن المشرع قد أصاب بعدم تطرقه لإجراءات التحقيق القضائي كمرحلة إجرائية مستقلة، وهذا نظرا لاستحالة ذلك إجرائيا. حيث يتصل التحقيق القضائي بمرحلتين إجرائيتين منفصلتين. تتصل الأولى بالتحقيق الابتدائي، وتنجز الثانية كتحقيق نهائي في إطار مرحلة المحاكمة.

[3] **أنظر:** فضيل العيش، مرجع سابق، ص 145. **وأنظر أيضا:** ناصر حمودي، (قضاء التحقيق في قانون الإجراءات الجزائية الجزائري-دراسة تحليلية نقدية)، مرجع سابق، ص 173.

[4] **أنظر:** المادتان 1/66 و166؛ أمر رقم 66-155، المرجع نفسه.

الشكوى المصحوبة بالادعاء المدني في الجنح[1]. وفي الحالتين يُكْتَفَا بالدرجة الأولى في التحقيق أمام قاضي الحقيق دون غرفة الاتهام، إلا من حيث النظر في استئناف أوامر قاضي التحقيق نفسه[2].

كما نجد ما يسمى بالتحقيق النهائي، وهو الذي يقوم به قاضي الموضوع في الجلسة. أي بعد انتهاء مرحلة التحقيق الابتدائي، ودخول الخصومة مرحلة المحاكمة، التي تعد ثاني مراحل الدعوى العمومية، وثالث المراحل الإجرائية عموما. وعلى عكس التحقيق الابتدائي السابق بالذكر؛ فان التحقيق النهائي يتصف بالإلزامي، حيث لا يمكن لقاضي الموضوع أن يصدر حكمه إلا بناءً على ما دار في الجلسة، وتمت مناقشته بالوسائل القانونية اللازمة[3].

2. مميزات إجراءات التحقيق: تمتاز إجراءات التحقيق القضائي، سيما الابتدائية منها؛ بالعديد من السمات الأساسية، التي تميزها عن مرحلة التحري السابقة بالدراسة، وعن باقي المراحل الجزائية عموما. ولعل أهم هذه المميزات نجد أنها إجراءات قضائية محضة، تستهدف البحث عن الحقيقة –الحقيقة القضائية كأصل عام–، وقائمة على الفصل بين وظيفتي الاتهام والتحقيق، كما يسمى فيها الشخص المتابع بالمتهم الذي يتمتع بضمانات قضائية واسعة.

أ– قضائية إجراءات التحقيق: يقوم التحقيق القضائي عموما؛ على مجموعة من الإجراءات ذات الطابع القضائي المحض. فعلى العكس من مرحلة التحري المتصفة بالبعد الإداري التمهيدي أو على الأكثر الطابع شبه القضائي؛ تكتسي الإجراءات محل الطرح الصفة القضائية المحضة[4]. حيث يبدأ التحقيق القضائي الابتدائي على وجه الخصوص؛ عن طريق أول إجراء قضائي في كل المراحل الجزائية، المنطوي على تحريك الدعوى العمومية أمام قاضي التحقيق المختص، إما بطلب افتتاحي لإجراء تحقيق يصدره وكيل الجمهورية أو بشكوى مصحوبة بادعاء مدني يتقدم بها الضحية نفسه[5].

وإجراء تحريك الدعوى العمومية على اختلاف طرقه وآلياته؛ نرى أنه يكتسب الصفة القضائية، نظرا لسببين اثنين. الأول كونه موجها إلى جهة قضائية محايدة، والثاني كونه سيقود إلى اتخاذ العديد من الأعمال الإجرائية ذات الطابع القضائي المحض، الهادفة إلى حماية النظام العام وحقوق الضحايا بالبحث عن الحقيقة ومعاقبة الجناة من جهة، وضمان حقوق المتهم انطلاقا من قرينة البراءة من جهة أخرى.

---

[1] **أنظر:** المادتان 2/66 و3/38؛ أمر رقم 66-155، مرجع سابق.

[2] **أنظر:** المادة 164 والمادة 170 وما يليها؛ المرجع نفسه.

[3] **أنظر:** المادة 353؛ المرجع نفسه. **وأنظر أيضا:** أبو عامر محمد زكي، الإجراءات الجنائية، منشأة المعارف، الإسكندرية، مصر، د س ن، ص 637. **نقلا عن:** أسامة محمد أحمد سليمان، مرجع سابق، ص 79.

[4] **أنظر:** ناصر حمودي، (قضاء التحقيق في قانون الإجراءات الجزائية الجزائري-دراسة تحليلية نقدية)، مرجع سابق، ص 10 و11.

[5] **أنظر:** المادتان 38 و67؛ أمر رقم 66-155، المرجع نفسه. **وأنظر أيضا:** أحسن بوسقيعة، التحقيق القضائي، الطبعة العاشرة، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2013، ص 29.

ب- البحث عن الحقيقة كهدف لإجراءات التحقيق: يقوم التحقيق القضائي الابتدائي خاصةً؛ على هدف أساس مفاده البحث عن الحقيقة، التي مهدت لها مرحلة التحري عن طريق جمع المعلومات الشخصية والموضوعية اللازمة[1]. ويتوقف دور البحث عن الحقيقة المناط بقضاء التحقيق؛ عند حد التحقيق نفسه، ولا يتعداه إلى الفصل في الوقائع بحكم جنائي، والتي هي مهمة قاضي الموضوع[2].

وفي سبيل البحث عن الحقيقة؛ يمارس قاضي التحقيق مهامه انطلاقا من العديد من الأعمال الإجرائية، المقيدة بحدود قانونية لا يمكن تجاوزها. فمن حيث الحدود؛ نجد أن عمل قاضي التحقيق تحكمه قاعدة أنه يخطر بالوقائع وليس بالأشخاص. حيث يعد ملزما بالتقيد بما جاء في موضوع الدعوى العمومية المرفوعة بالطلب الافتتاحي أو بالشكوى المصحوبة بالادعاء المدني. وفي الوقت نفسه يعد اختصاصه مرنا جدا في خصوص الأشخاص، حيث يمكنه اتهام من يرى له دخلا في الوقائع كما يمكنه الإخراج من دائرة الاتهام من تم اتهامه عند تحريك الدعوى[3].

وأما بخصوص الأعمال الإجرائية؛ فلم يحددها المشرع الجزائري على سبيل الحصر. وإنما ترك الباب مفتوح أمام قاضي التحقيق ليتخذ من تلقاء نفسه أو بطلب من طرفي الدعوى العمومية؛ أي إجراء قانوني يراه مناسبا في سبيل إظهار الحقيقة، بشرط عدم الخروج عن دائرة المشروعية[4]. وعلى العموم تتمثل أهم إجراءات التحقيق الهادفة لإظهار الحقيقة؛ في المعاينة والتفتيش وسماع الشهود والاستجواب والمواجهة وندب الخبرة...الخ[5].

ج- قيام إجراءات التحقيق على أساس الفصل بين وظيفتي الاتهام والتحقيق: تقوم ميزة الفصل بين وظيفتي الاتهام والتحقيق؛ على أساس فكرة حياد قضاء التحقيق المذكورة سابقا، التي نجدها أساس التحقيق القضائي في النظام الإجرائي الجزائري. فللنيابة العامة أصلا سلطة جمع المعلومات في إطار مرحلة التحري ومنه الاتهام والمتابعة، ولقضاء التحقيق سلطة البحث عن الحقيقة وإثباتها إما بتأكيد الاتهام أو بنفيه. على أن تبقى سلطة الفصل في الدعوى إذا ما تمت الإحالة لقاضي الموضوع[6].

---

[1] **أنظر:** محمود محمد محمود جابر، مرجع سابق، ص 51 و52.

[2] وهو ما يفهم بداهةً؛ من خلال الفصل بين وظيفتي التحقيق القضائي والحكم، المؤسس له فقها والمكرس من المشرع الجزائري صراحةً بموجب أوامر التصرف في التحقيق الابتدائي من جهة، وتحديد اختصاصات المحاكم الجنائية المختلفة من جهة أخرى. ولو أنه يمكن لقضاء التحقيق أن يفصل لصالح المتهم؛ كأن يصدر أمر بألا وجه للمتابعة. **أنظر في ذلك:** المادة 162 وما يليها؛ أمر رقم 66-155، مرجع سابق. **وأنظر أيضا:** فضيل العيش، مرجع سابق، ص 145 و146 و164.

[3] **أنظر:** عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، مرجع سابق، ص ص 341-344.

[4] **أنظر:** ناصر حمودي، (قضاء التحقيق في قانون الإجراءات الجزائية الجزائري-دراسة تحليلية نقدية)، مرجع سابق، ص 10.

[5] **أنظر:** المواد من 79 إلى 108 والمواد من 143 إلى 156؛ أمر رقم 66-155، المرجع نفسه.

[6] **أنظر:** أحسن بوسقيعة، التحقيق القضائي، مرجع سابق، ص ص 20- 26.

ويكرس استقلال الوظائف المذكورة؛ العديد من الضمانات واجبة الإعمال في إطار الإجراءات الجزائية عموما. سيما ضمان حياد جهات التحقيق الابتدائي، وعدم مناقشتهم لمواقفهم من وظيفة قضائية أخرى غير وظيفة التحقيق. كما يعد الفصل في الوظائف محل الطرح؛ بمثابة رقابة الجهات القضائية المختلفة لبعضها البعض، ما يفيد كشف الأخطاء وتداركها[1].

د- إجراءات تسمى الشخص المعني بالمتهم: بمجرد تحريك الدعوى العمومية؛ تتحول تسمية الشخص محل المتابعة من المشتبه فيه إلى المتهم، الذي يحمل الصفة نفسها من خلال كل إجراءات التحقيق الابتدائي، وحتى النهائي وفي مرحلة المحاكمة[2]. على أن يتحول بعد ذلك وفق المراحل الجزائية المذكورة سابقا؛ إلى مدان أو إلى بريء بقرار نهائي من المحكمة المختصة تنقضي بموجبه الدعوى العمومية، أو إلى بريء بأمر قاضي التحقيق أو قرار من غرفة الاتهام[3].

وحمل الشخص لصفة المتهم، سيما أثناء مرحلة التحقيق الابتدائي؛ تمنحه العديد من الضمانات الغائبة عن المشتبه فيه في مرحلة الاستدلال. فكل المميزات المذكورة في هذا الإطار؛ تعد من الضمانات المكرسة للمتهم أثناء التحقيق القضائي، التي قد تتصل بقضاء التحقيق كجهاز، أو تتعلق بالأعمال الإجرائية وأحكام القيام بها.

فنجد من أهم ضمانات المتهم أثناء التحقيق الابتدائي؛ أنه يتم التحقيق معه من قبل جهة قضائية محايدة –قضاء التحقيق كما بينا سابقا–. التي يجب أن تمارس مهامها وفق مبدأ التدوين، الذي يتطلبه المشرع على سبيل الإلزام[4]. وفي الوقت نفسه يتوجب أن تسير التحقيقات في سرية تامة إلا من حيث متطلبات إظهار الحقيقة، حيث لا يمكن للغير الاطلاع على أعمال التحقيق؛ إلا إذا ما توفر نص صريح بذلك[5]. وهو ما يحفظ شرف واعتبار المتهم، إلى غاية انقضاء الدعوى العمومية على الأقل[6].

---

[1] **أنظر:** ناصر حمودي، (قضاء التحقيق في قانون الإجراءات الجزائية الجزائري-دراسة تحليلية نقدية)، مرجع سابق، ص 13.

[2] مع العلم أن المشرع الجزائري لا يفرق في النص الوارد باللغة العربية؛ بين مراحل الدعوى العمومية والمحاكم المختلفة في تسميته لمن يكون محلا للمتابعة بالمتهم. وان كان قد اعتمد تسميات مختلفة في النص الوارد باللغة الفرنسية. حيث يسمي المتهم في التحقيق الابتدائي بـ "l'inculpé"، ويسميه أمام محكمة الجنح والمخالفات بـ "le prévenu"، كما يطلق عليه أمام محكمة الجنايات تسمية "l'accusé". وفي الحقيقة هو خلط في ترجمة النص الأصلي الصادر عن المشرع الفرنسي، وان كان هو نفسه يعتبر قد تخلى عن المصطلحات المذكورة، وعوضها بعبارة "personne mise en examen"، أي الشخص الموضوع تحت الاختبار. **أنظر في ذلك: المواد** 67 و329 و268؛ أمر رقم 66-155، مرجع سابق. **وأنظر أيضا:**

- Art 80-1; code de procédure pénale français, Partie législative, Version consolidée au 17 septembre 2017. Disponible sur le Lien: https://www.legifrance.gouv.fr.

[3] **أنظر:** المواد 6 و163 و195؛ أمر رقم 66-155، المرجع نفسه.

[4] **أنظر:** المادة 2/68؛ أمر رقم 66-155، المرجع نفسه. **وأنظر أيضا:** عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، مرجع سابق، ص 339 و340.

[5] **أنظر:** المادة 1/11؛ أمر رقم 66-155، المرجع نفسه.

[6] **أنظر:** محمود محمد محمود جابر، مرجع سابق، ص 52.

وفي الإطار نفسه؛ يعد التحقيق القضائي الابتدائي بمثابة الفرصة القضائية للبحث عن الحقيقة قبل المحاكمة، ومنه الحلول دون المحاكمة العلانية الظالمة[1]. فمن خلاله يقوم القائم على التحقيق؛ إما بإثبات التهمة أو التهم الموجهة للمتهم، ومنه إحالته وفق الطرق القانونية للمحاكمة. كما قد تتبين له براءته فيصدر أمرا بألا وجه للمتابعة الذي يعد بمثابة براءة المتهم، مع الاحتفاظ بحق النيابة العامة في الطعن فيه أمام غرفة الاتهام[2].

كما نجد كأهم ضمان من ضمانات المتهم؛ أنه يتمتع بقرينة البراءة التي تعتبره بريئا حتى تثبت إدانته من الجهة القضائية المختصة. فلا يمكن لقاضي التحقيق أن يلحق مضمون التهمة بالمتهم، بل يحيله إلى جهة الحكم المختصة مرفقا بأدلة الإثبات، التي تعد الوحيدة من لها حق الإدانة. ولو أنه يمكن لقاضي التحقيق أن ينفي التهمة على المتهم قبل المحاكمة، وتبرئته بأمر انتفاء وجه الدعوى كما ذكرنا سابقا. وعلى العموم تعد قرينة البراءة بمثابة الحيلة القانونية، التي بموجبها يضع القانون قناع البراءة على المتهم مؤقتا بغرض التعمق في البحث عن الحقيقة[3].

3. التمييز بين إجراءات التحقيق ومرحلة التحري: بعد السرد الموجز لأهم ما يمكن أن تقوم عليه مرحلة التحري وإجراءات التحقيق في إطارهما التقليدي، وفي سبيل الربط القادم بالدراسة مع جرائم الوسط الرقمي ومسرحها الافتراضي الحديث؛ يمكن أن نقف على العديد من النقاط الإجرائية الأساسية التي تقرب أو تباعد بين الاثنين. فرغم الاتفاق في الكثير من النقاط الأساسية؛ إلا أنهما يختلفان في نقاط أخرى عديدة. سيما من حيث الطبيعة القانونية والهدف من وراء إعمالهما، وطريقة تعامل المشرع معهما من حيث التنظيم والإلزامية والتقييد.

تعامل المشرع الجزائري كغيره من التشريعات المقارنة الفاصلة بين جهتي الاتهام والتحقيق؛ مع مرحلة التحري على أنها ذات طبيعة إدارية غير قضائية–أو شبه قضائية كما يسميها البعض–. التي تمارسها الشرطة القضائية بإدارة وكيل الجمهورية وإشراف النائب العام ضد المشتبه فيه بوسائل غير قهرية، وكمرحلة تمهيدية للدعوى العمومية وأولى المراحل الإجرائية عموما. وهو ما يختلف تماما بخصوص إجراءات التحقيق، التي لها الطابع القضائي يمارسها رجال القضاء، من قاضي تحقيق وقضاة غرفة الاتهام وقاضي الموضوع بالوسائل القهرية، وكأولى إجراءات الدعوى العمومية وثاني الإجراءات الجزائية عموما.

---

[1] **أنظر:** محمود محمد محمود جابر، مرجع سابق، ص 52 و53.

[2] **أنظر:** المادة 162 وما يليها والمادة 170 وما يليها؛ أمر رقم 66-155، مرجع سابق.

[3] ولو أنه يوجد من يرفض فكرة الحيلة القانونية. على أساس أن قرينة البراءة؛ تعد من حقوق الإنسان الخالصة والأساسية. **أنظر في ذلك:** كريمة خطاب، (قرينة البراءة)، أطروحة لنيل شهادة دكتوراه علوم فرع قانون، كلية الحقوق، جامعة الجزائر1، الجزائر، 2015، ص ص 31-34.

وميز المشرع أيضا في تعامله مع مرحلة التحري وإجراءات التحقيق؛ عن طريق تحديده للهدف الأساس من وراء إعمالهما. حيث يُستهدف بمرحلة التحري مجرد جمع الاستدلالات والمعلومات الشخصية والموضوعية عن الجريمة المرتكبة، بغرض الاعتماد عليها بخصوص إعمال سلطة الملائمة. وهو ما يختلف تماما بخصوص إجراءات التحقيق، الهادفة إلى إحقاق الحقيقة عن طريق البحث في أدلة الإدانة وأدلة النفي في الوقت نفسه.

كما يميز المشرع الجزائري كذلك في تعامله مع إجراءات التحقيق ومرحلة التحري؛ من حيث التنظيم والإلزامية والتقييد. فوحد إجراءات التحري من حيث جهاتها المختصة بها وهدفها الإجرائي، ما يسمح بمعالجتها فقها في إطار مرحلة إجرائية منفصلة عن باقي المراحل الجزائية. الأمر الذي نجده مختلفا بخصوص إجراءات التحقيق رغم اتحاد هدفها، التي جاءت موزعة بين التحقيق الابتدائي والتحقيق النهائي–المحاكة–، ما يمنع النظر إليها على أنها مرحلة إجرائية موحدة.

هذا بالإضافة إلى اعتبار مرحلة التحري كما رأينا سابقا؛ بمثابة المرحلة الجزائية الضرورية واللازمة، سيما معاصرتها أو قربها الزمني لوقت ارتكاب الجريمة ما يضمن عدم ضياع الدليل، وأبرز دليل على ذاك نجد أنها تُعمل حتى بخصوص الجرائم التي لايمكن تحريك الدعوى العمومية بخصوصها نظرا لسبب موضوعي أو إجرائي. وهو ما يختلف تماما بخصوص إجراءات التحقيق، التي تتباين بين الإلزامية في الجنايات والاختيارية في الجنح والمخالفات، ولا يمكن إعمالها بخصوص الجرائم التي تتوفر على مانع موضوعي أو إجرائي، حتى وان حملت الجريمة وصف الجناية.

وعلى الرغم مما ذكر بخصوص أوجه الاختلاف والتباين بين مرحلة التحري الاستدلالي وإجراءات التحقيق القضائي–الابتدائي والنهائي–؛ نرى أنهما يتوافقان في بعض النقاط التي تكتسي الطابع العام المنطوي على الهدف الأساس من وجود قانون الإجراءات الجزائية أصلا. حيث يهدف الاثنين عموما؛ إلى مكافحة الجريمة بالكشف عن مرتكبيها وتقديمهم للمحاكمة الجنائية. والتمهيد الاستدلالي الذي تقوم به مرحلة التحري؛ ما هو إلا التسبيق الإجرائي الضروري الذي تنطلق منه إجراءات التحقيق في إطار التكامل القانوني بين الاثنين.

كما أن أهم وجه من أوجه التشابه بين الاثنين؛ يكمن في كونهما مجموعة من الإجراءات القائمة على أعمال تمارسها جهات محددة قانونا؛ في إطار مسرح جرمي مادي تقليدي. حيث يتبع مسرح الجريمة كما بينا سابقا؛ بالضرورة الطبيعة الجرمية المحددة بنص التجريم. فلما جرم المشرع الجزائري منذ أول قانون عقوبات لسنة 1966، سلوكيات تعتبر في مجملها متصلة بالحيز الخارجي الملموس كمسرح جرمي تقليدي؛ وجب عليه أيضا أن يضع إجراءات من الطبيعة نفسها، انطلاقا من احترام المبدأ القائل؛ أن دور قانون الإجراءات الجزائية يبدأ عند انتهاء دور قانون العقوبات.

الفرع الثاني: مظاهر عجز إجراءات التحري والتحقيق التقليدية عن مواجهة المسرح الجرمي الافتراضي

يقوم العجز الإجرائي محل الطرح بالأساس؛ على محاولة المقاربة بين ما خلصنا إليه في الفرع السابق من الدراسة أولا، وما بيناه قبل ذلك بخصوص طبيعة المسرح الجرمي في الجرائم محل الدراسة ثانيا. حيث بالتسليم بأن الإجراءات التقليدية ذات الصلة بالتحري والتحقيق؛ قد أوجدها المشرع الجزائري –كغيره من نظرائه– لمكافحة الجرائم التقليدية المتصلة بالمسرح المادي التقليدي من جهة، وبربط بالطبيعة الرقمية الافتراضية للمسرح الجرمي في إطار جرائم الوسط الرقمي الحديثة من جهة أخرى؛ يبرز نظريا العجز الإجرائي المقصود.

ولم يظل العجز الإجرائي الموضح أعلاه؛ مجرد نتاج مقاربة نظرية سطحية. بل امتد لتبرز له العديد من المظاهر العملية، التي واجهة الجهات المختصة بأعمال التحري والتحقيق؛ عند ممارستها لذلك. التي نجد أهمها العجز الشخصي والمؤسساتي(أولا)، والعجز في الأعمال الإجرائية المتصلة باكتشاف الجريمة والتحري والتحقيق بشأنها(ثانيا).

أولا: مظاهر العجز المتصلة بأجهزة التحري والتحقيق التقليدية

عرفت الأجهزة المعنية بالتحري والتحقيق؛ العديد من الصعاب الإجرائية في إطار مواجهة جرائم الوسط الرقمي عموما، سيما من حيث التجهيزات المادية والخبرات الفردية. حيث اعتادت هذه الأجهزة على مواجهة الجرائم التقليدية ذات المسرح المادي الملموس. الذي يتطلب من جهة؛ التنقل الميداني والعديد من الوسائل المادية ذات الصلة، ويتوجب من جهة أخرى؛ الاستعداد البدني والذهني الميداني لدى أشخاص التحري والتحقيق، على اختلاف صفاتهم وانتماءاتهم القانونية[1].

وفي الحقيقة يقوم العجز الإجرائي محل الطرح؛ على عدم توافر الخبرة والعلم الرقمي الكافيين لدى أشخاص التحري والتحقيق لمواجهة جرائم الوسط الرقمي. حيث ترى العديد من الدراسات؛ أن الاعتماد على أشخاص غير مؤهلين تقنيا، للتحري والتحقيق في جرائم حديثة يرتكبها أشخاص لهم مواصفات ومهارات عالية في المجال الرقمي؛ تعد معادلة جنائية غير متكافئة على كل المستويات. ومنه يؤسسون العجز الإجرائي المقصود[2].

وان كان لنا رأي فيما ذكر، حيث نؤيد فكرة العجز الإجرائي المتصل بعدم خبرة القائمين على التحري والتحقيق في الجرائم محل الدراسة، ولكن ليس من منطلق أنهم يواجهون مجرمون بصفات ومهارات خاصة فحسب، وإنما لأنهم يواجهون بالأساس مسرح جرمي رقمي افتراضي، له سمات خاصة ويتطلب

[1] **أنظر:** عمر عبد العزيز موسى الدبور، مرجع سابق، ص 217.

[2] **أنظر:** غازي عبد الرحمن هيان الرشيد، (الحماية القانونية من جرائم المعلوماتية-الحاسب والإنترنت)، أطروحة لنيل درجة الدكتوراه في القانون، كلية الحقوق، الجامعة الإسلامية، لبنان، 2004، ص 541.

قدر من الدراية الفنية اللازمة لمواجهته. الذي قد يكون الجاني في إطاره متخصصا فائق المهارة، كما قد يكون مبتدءا لا يتقن إلا الأساسيات اللازمة للولوج والتشغيل. والعجز الإجرائي محل الطرح؛ يشمل الاثنين معا–الجاني الرقمي بنوعيه المحترف والمبتدئ–، وان يمكن تصوره أكثر بخصوص مواجهة الجناة الماهرين رقميا، نظرا لقدرتهم على التلاعب بالمسرح الافتراضي للجريمة عن طريق إتلاف آثاره الرقمية، ومنه التغيير في ملامحه الجنائية[1].

كما قد لا يقف العجز الإجرائي عند ما ذكر؛ بل يمتد إلى تعميق العجز نفسه كلما تم تحرٍ أو تحقيق في جريمة من الجرائم محل الدراسة. حيث يمكن أن تصبح وسائل التحري والتحقيق في المسرح الرقمي الافتراضي؛ مكشوفة للجناة المختصين في الوسط الرقمي، ما يفسح المجال أمامهم لدراستها والبحث عن تقنيات تعطل مفعولها الإجرائي. الأمر الذي يوجب عدم الاقتصار على ضرورة التدريب الرقمي لأشخاص أجهزة التحري والتحقيق، من أجل الكشف عن الجريمة ومتابعة الجناة فقط؛ بل يجب البحث عن إجراءات رقمية تضمن المتابعة من جهة، وسرية الأعمال الرقمية المتبعة في سبيل ذلك من جهة أخرى، على شاكلة بروتوكولات ضمان الجودة[2].

ويعد العجز الإجرائي الرقمي لدى القائمين على التحري والتحقيق في جرائم الوسط الرقمي؛ في حد ذاته بمثابة الدافع الإجرامي لدى جناة الوسط الرقمي. حيث اقتناع الجناة بعدم قدرة الشرطة والجهات القضائية على تعقبهم رقميا واكتشاف جرائمهم؛ قد يدفعهم إلى ارتكابها من دون خوف. وبل قد يتم استغلال انعدام الخبرة الرقمية لديهم؛ لارتكاب جرائم أو لإخفاء أخرى. كما هو الحال في القضية التي حصلت بالولايات المتحدة الأمريكية، حيث تلقت إحدى الشركات الأمريكية المتعرضة للقرصنة طلبا من الشرطة؛ لتتوقف مؤقتا عن استعمال جهاز الإعلام الآلي الذي تمت قرصنته من مجهولين، حتى يتم وضعه تحت المراقبة لاكتشاف الجاني أو الجناة. إلا أن النتيجة كانت إتلاف الشرطة لكل الملفات والأدلة ذات الصلة من دون قصد، وبالتالي إفلات الجناة[3].

---

[1] وعلى العموم يرى من يؤسسون عجز الأجهزة محل الطرح؛ على عدم التكافؤ بين المهارة العالية لجناة الوسط الرقمي وقلة الخبرة والعلم الرقمي لدى القائمون بالتحري والتحقيق بشأن الجرائم ذات الصلة؛ أن المجرم الرقمي يتصف بالعديد من السمات الخاصة، التي تميزه عن غيره من الجناة، سيما المجرم التقليدي. وفي سبيل ذلك؛ يعتبرونه مجرم متخصص عائد الإجرام، حيث يقتصر إجرامه وعوده على السلوكيات الرقمية دون الجرائم التقليدية، الأمر الذي يكسبه المهارة ونوع من احتراف الإجرام الرقمي، ما يجعله يكون دقيقا وناجعا وقليل الأخطاء. كما يعد حسبهم؛ صاحب مهارة ومعرفة تقنية رقمية سابقة عن احتراف الإجرام. وقد يضاف إليه الدافع الإجرامي، القائم على انعدام الخوف من مسرح الجريمة نظرا لنعومته، ولاعتباره محققا للأغراض المادية والشخصية بالسهولة المطلوبة. **أنظر في ذلك:** عمر عبد العزيز موسى الدبور، مرجع سابق، ص ص 218-220.

[2] **أنظر:** إيهاب ماهر السنباطي، "الجرائم الالكترونية(الجرائم السيبيرية): قضية جديدة أم فئة مختلفة؟ التناغم القانوني هو السبيل الوحيد!"، ورقة عمل مقدمة إلى الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية، 19 و20 جوان 2007، ص 67.

[3] **أنظر:** يوسف صغير، (الجريمة المرتكبة عبر الإنترنت)، مذكرة لنيل شهادة الماجستير في القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 2013، ص 122.

ثانيا: مظاهر العجز المتصلة بأعمال التحري والتحقيق التقليدية

تهدف أعمال التحري والتحقيق التقليدية وفق ما بينا سابقا، بمجرد اكتشاف الجريمة؛ إلى البحث عن المعلومات الشخصية والموضوعية ذات الصلة بمسرحها المادي، ومن ثم العمل على جمع وتقدير أدلة النفي والاتهام في سبيل البحث عن الحقيقة. الأمر الذي واجهته العديد من الصعاب بخصوص جرائم الوسط الرقمي ذات المسرح الافتراضي، إلى درجة التصريح الفقهي بعجزها النسبي وحتى التام أحيانا. سيما بخصوص صعوبة اكتشافها، وإثباتها.

1. صعوبة اكتشاف الجريمة في المسرح الافتراضي: على عكس أغلب الجرائم التقليدية المتصلة بالوسط المادي الملموس؛ تعترض عملية اكتشاف جرائم الوسط الرقمي الكثير من الصعاب الحديثة، التي قد تجعل ذلك مستحيلا في العديد من الأحيان. وكما بينا سابقا؛ تعد عملية اكتشاف الجريمة بمثابة بداية مرحلة التحري و/أو إجراءات التحقيق. ومنه لها من الضرورة ما يدفع إلى اعتبارها؛ أهم حلقة إجرائية فاصلة بين المتابعة الجنائية من عدمها. وفي الإطار نفسه؛ تتمثل أهم الإشكالات التي تعترض اكتشاف جرائم الوسط الرقمي؛ في حداثة وتعقيد المسرح الجرمي الافتراضي، وعمل الجناة على محو أثر الجريمة بعد ارتكابها مباشرة، وامتناع الأشخاص عن التقدم بالشكاوى والبلاغات.

أ- حداثة وتعقيد المسرح الجرمي الافتراضي: يكتسي الوسط الرقمي كمسرح حديث للجريمة -كما بينا سابقا- الطابع المعقد والمتشعب، الذي يقوم بالأساس على افتراضية ما تحدثه عناصره الرقمية، ومنه التعامل معه من دون ترك أي أثر مادي ملموس. وهو ما يؤدي بالضرورة إلى عدم اكتشاف الجريمة المرتكبة من خلاله وفي إطاره، سيما إذا ما رجعنا إلى قلة خبرة الأجهزة المختصة بالتحري والتحقيق في المجال الرقمي كما ذكرنا سابقا.

وفي العديد من الأحيان ترتكب الجريمة في المسرح الجرمي الافتراضي؛ من دون ترك أي أثر مادي أو حتى افتراضي مرئي، كالذي تخلفه الجريمة التقليدية مثل الكسر في جريمة السرقة[1]. فقد تكون جريمة الدخول المادي إلى المنظومة المعلوماتية من أجل نسخ معلومات معينة؛ جارية في الوقت نفسه الذي يتعامل معها مالكها أو القائم عليها، ولا يمكنه أن يشعر بها. كما أن نسخه لهذه المعلومات لا يترك أي أثر؛ لأنه يكتفي بنقل نسخة رقمية منها، من دون إزالتها ولا حتى المساس بإظهارها الرقمي، إن بخصوص الشكل أو الطريقة[2].

---

[1] **أنظر:** عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت-دراسة متعمقة في جرائم الحاسب الآلي والإنترنت، بهجات للطباعة والتجليد، القاهرة، مصر، 2009، ص 41.

[2] ولو أن المشرع الجزائري لا يجرم السلوك المذكور أعلاه صراحةً. حيث لا يعاقب على فعل النسخ بعد الدخول أو من دون دخول في إطار جرائم المساس بأنظمة المعالجة الآلية للمعطيات. كما لا يمكن اعتبارها جريمة سرقة رقمية حتى وان أعطينا للمعلومة الرقمية الطابع المالي الافتراضي؛ نظرا لكون السرقة تتطلب النقل النهائي للشيء المختلس من حيازة المالك إلى حيازة السارق، وفي عملية النسخ تبقى النسخة الأصلية كما هي تحت تصرف وحيازة القائم عليها. =

إلا أن كل التعقيد الرقمي المذكور، والذي يعد عائقا حقيقيا في سبيل اكتشاف الجرائم محل الدراسة؛ لا يتصل في الحقيقة إلا بالنطاق الافتراضي المحدث من الجهاز، وكأكثر تقدير بالنطاق الافتراضي العام للشبكة، المذكور سابقا والمتصل خاصةً بالويب السطحي المتصف بالفهرسة وعدم التشفير، ومنه السهولة في التعامل معه ومع أثار الجرمية. الأمر الذي يزداد تعقيدا والى حد الاستحالة؛ بخصوص اكتشاف الجرائم المتصلة بالويب العميق وخاصةً الويب المظلم منه، بكل خصائصه القائمة على التشفير وعدم الفهرسة الضامنة للسرية المذكورة سابقا[1].

ب- إتلاف الجناة لأثر الجريمة في المسرح الافتراضي: قد يعمل الجاني الرقمي؛ على إخفاء أثر الجريمة من مسرحها الافتراضي مباشرة بعد ارتكابها، بنظرة مسبقة منه حتى يؤمن نفسه قبل البدء في السلوك الإجرامي. وهو ما ينجز عن طريق العديد من السبل الرقمية، سيما التلاعب بالنبضات الرقمية العاملة على تسجيل البيانات والمعلومات[2]، أو الاعتماد على التشويه الشبكي أو باستعمال هويات مزيفة أو أسماء مستعارة...الخ[3].

كما يمكن أن ترتكب الجريمة بطريقة لا تترك أي أثر رقمي ولا مادي بعد الانتهاء منها، نظرا لطبيعة السلوك المرتكب نفسه. وهو ما ينطبق على ما بيناه سابقا بخصوص نسخ المعلومات الرقمية بعد الدخول أو من دونه. حيث يكون الجاني مرتاح البال من البداية؛ لكونه متأكدا من عدم إمكانية اكتشاف الجريمة من القائم على المعلومات محل النسخ ولا حتى من غيره، نظرا لعدم ترك الأثر الرقمي في مسرح الجريمة. وان كان يمكن اكتشافها فيما بعد؛ عن طريق الوقوف على حيازتها أو استعمالها من الجاني أو غيره، لكن بصورة منفصلة عن مسرح الجريمة نفسها.

ج- امتناع الأشخاص عن التقدم بالشكاوى والبلاغات: تطرقت العديد من الدراسات السابقة؛ إلى الربط بين صعوبة اكتشاف جرائم الوسط الرقمي وامتناع الأشخاص عن التبليغ عنها، من منطلق أن هذا الأخير؛ يعد أبرز الأسباب ذات الصلة بعدم الاكتشاف. الأمر الذي نؤيده في إطار دراسة الحال، لكن بعد توسعته والفصل بين المصطلحات الجنائية ذات الصلة بالدقة اللازمة. حيث نفرق في إطار الامتناع بين الشكوى والبلاغ. ونؤكد بعد ذلك على قلة التقدم من الأشخاص؛ بالشكاوى والبلاغات عن السلوكيات الإجرامية ذات الصلة بالوسط الرقمي.

= أنظر في ذلك: المادتان 394مكرر و394مكرر1؛ أمر رقم 66-156، مرجع سابق. **وأنظر أيضا:** أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، الجزء الأول، مرجع سابق، ص 292.

[1] ولنا عودة إلى دراسة هذه الاستحالة وسبل مواجهتها، في المطلب الموالي القادم بالدراسة، وخاصةً عند التطرق إلى الأعمال الإجرائية في الباب الثاني والأخير من الدراسة.

[2] **أنظر:** عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والإنترنت، منشورات الحلبي الحقوقية، بيروت، لبنان، 2007، ص 31. **وأنظر أيضا:** غازي عبد الرحمن هيان الرشيد، مرجع سابق، ص 539.

[3] **أنظر:** يوسف صغير، مرجع سابق، ص 119.

يعرف في العادة؛ أن الضحية وكأصل عام يعمل على التقدم بالشكوى الجنائية، ضد كل من ألحق به ضررا من جراء ممارسة مجرمة قانونا. الأمر الذي يعد بمثابة الإجراء غير المرغوب فيه إذا ما تعلق بجرائم الوسط الرقمي عموما. والذي يرى فيه الفقه الجنائي أن له سببين اثنين، فإما صونا للسرية أو تجنبا للمسئولية. فللحياة الخاصة –شخص طبيعي أو معنوي– سرية لازمة الحماية من الفضائح والانتقادات، ومنه عدم التقدم بالشكوى الجنائية؛ يضمن عدم المساس بشرف واعتبار الأشخاص، أو بسمعة وأمن الشركات الكبرى والدول والمنظمات[1].

كما أن العديد من الجهات التي تكون ضحية لجرائم الوسط الرقمي –سيما الشركات الكبرى–؛ تتجنب التقدم بالشكوى الجنائية اللازمة، رغم تكبدها لأضرار هائلة؛ جراء السلوكيات الإجرامية. حيث تهدف من وراء ذلك؛ لعدم منح فرصة الاطلاع على المعلومات الرقمية عند معاينة الجهات المختصة بذلك، التي قد يوجد ضمنها ما يعد عملا مجرما قانونا، ربما يصل إلى حد جرائم الفساد. وفي هذا السياق تقدم مكتب التحقيق الاتحادي في الولايات المتحدة الأمريكية؛ إلى الشركات الأمريكية الكبرى بتوصية يدعوها فيها إلى ضرورة التقدم بالشكاوى اللازمة ضد الاحتيال الرقمي، بغرض المساهمة في اكتشاف الجريمة ومكافحتها من جهة، وللوصول إلى الإحصائيات الحقيقية من جهة أخرى[2].

وفي سياق متصل ومغاير؛ يمكن لكل شخص شهد أو عاين أو وصل إلى علمه بالطرق المعتمدة؛ وقوع سلوك إجرامي مهما كان تكييفه القانوني؛ أن يتقدم أمام الجهات المختصة ببلاغ عن ذلك. الأمر الذي وان تدخله أغلب الدراسات السابقة –إن لم نقل كلها–؛ في إطار الشكوى السابقة بالدراسة، نرى أنه منفصل عنها قانونا وواقعا. وهو ما سنبينه، بالتوازي مع التأسيس للامتناع عن التبليغ كإجراء سلبي، وتحديد أسبابه الواقعية وفق النظرة الجنائية الخالصة.

فتجنب التبليغ عن جرائم الوسط الرقمي؛ يعد بمثابة الظاهرة الجنائية الحديثة –وان كان تتطلب دراسة مستقلة–، التي وصلت إلى أرقام مخيفة جدا. إلى درجة أن الجهات المختصة؛ تكتشف يوميا كما هائلا من الجرائم الرقمية، التي يتم معاينتها من الأشخاص الموصولين بالشبكة، من دون التقدم بأي بلاغ رغم علمهم بالوصف الجنائي. وهو ما نعتبره بمثابة انعدام الوعي الرقمي الحديث. سيما وأن الأمر شائع في الدول المتقدمة بالنسبة نفسها مع الدول النامية أو ربما أكثر[3].

---

[1] **أنظر:** سليم مزيود، مرجع سابق، ص 97 و98.

[2] **أنظر:** فريق الخبراء المعني بالجريمة السيبرانية، مرجع سابق، ص 07.

[3] ولتأسيس ما ذكر؛ نجد قيام البرنامج "memex"، الذي أطلقته وكالة "داربا-الذراع البحثية لوزارة الدفاع الأمريكية-" سنة 2014؛ بمسح أكثر من 100 إعلان شبكي جنسي، المتعلق أساسا بالاتجار الجنسي بالأشخاص –سيما الأطفال والنساء-. وهذا دون تلقي بلاغات بشأنها، رغم كونها متاحة عبر الشبكة ويمكن الوصول إليها ومعاينتها من روادها. **أنظر في ذلك:** ايفا الشوفي، "كيف تحارب التكنولوجيا الاتجار بالبشر؟"، تاريخ النشر: 17 أوت 2017، تاريخ التصفح: 09 فيفري 2018، الرابط: http://www.al-akhbar.com/node/281825.

2. صعوبة إثبات الجريمة في المسرح الافتراضي: على عكس ما جاءت به العديد من الدراسات ذات الصلة بجرائم الوسط الرقمي، التي تجمع من حيث الصعاب الإجرائية بين الاكتشاف والإثبات؛ فضلنا في دراسة الحال فصل الاثنين، من منطلق إجرائي محض، متصل بما قدمناه سابقا من حيث التفرقة بين مرحلة التحري التي تبدأ باكتشاف الجريمة، وإجراءات التحقيق الهادفة إلى البحث عن الحقيقة بإثبات الجريمة أو نفيها عملا بالدليل الرقمي[1]. وان كان تتفق الصعاب الإجرائية بين الاكتشاف والإثبات في العديد من النقاط، سيما الامتناع عن الشكوى والتبليغ من جهة، وقلة الخبرة لدى الأجهزة المختصة من جهة أخرى[2]. وعلى العموم نميز في إطار صعوبة الإثبات؛ بين الصعوبة النسبية المتصلة بالمسرح الافتراضي العادي والصعوبة المتعدية المتعلقة بالمسرح الافتراضي الخاص[3].

أ- الصعوبة النسبية لإثبات الجريمة في المسرح الافتراضي العادي: تتصل الصعوبة النسبية وفق ما بينا أعلاه؛ بالمسرح الافتراضي العادي. الذي وصفناه سابقا بالتعقيد الرقمي والحداثة الجنائية. وعلى العموم تقوم الصعوبة محل الدراسة؛ على الطبيعة الافتراضية للدليل الرقمي، وتعطيل الوصول إليه.

أ-1/ الطبيعة الافتراضية للدليل الرقمي: ينطوي المسرح الجرمي للجرائم محل الدراسة؛ على نطاق افتراضي مشكل من أنظمة المعلومات والمعلومات الرقمية، وكل المكونات الافتراضية للشبكة. التي في مجملها؛ تعد بمثابة النبضات غير المرئية ولا الملموسة، ما يجعل التعامل معها كدليل جنائي؛ أمر جد معقد وصعب من جهة ويسهل الإتلاف الرقمي من جهة أخرى. على عكس الجريمة التقليدية، المرتكبة في المسرح المادي الملموس، المتصف بالماديات والبروز في العالم الخارجي؛ على غرار تزوير النقود أو استعمال السلاح الناري في القتل[4].

كما أن عدم صلاحية الدليل الرقمي الافتراضي، أو صعوبة التعامل الجنائي معه؛ يعد بمثابة العائق الإجرائي في العديد من الأحيان، سيما بخصوص الجرائم التي لا تقبل بطبيعتها؛ إلا الإثبات الرقمي، نظرا لاقتصارها على الأثر الرقمي فقط، على غرار جريمة التجسس الشبكي. أو لاقتصار دور الوسيلة التقليدية على مجرد القرينة، كأن توجد بصمات الشخص على الجهاز. وان كان يمكن؛ الاعتماد على الدليل

---

[1] الدليل الرقمي، الذي لنا عودة لدراسته بالتفصيل في الباب الثاني من الدراسة، إن من حيث ماهيته، أو أعمال جمعه أو مشروعيته القانونية.

[2] حيث بالرجوع إلى ما قدمنا سابقا بخصوص المفهوم العام للتحري والتحقيق؛ نجد أن الاكتشاف مرحلة تمهيدية لإثبات الجريمة. والإجراءات التالية للاكتشاف في إطار التحري الأولي؛ تعد من الضرورة بمكان، وهي من تسهل أو تعقد أكثر عملية إثبات الجريمة. كما أن قلة الخبرة لدى الأجهزة المختصة -خاصةً الشرطة القضائية- المذكورة سابقا في إطار الاكتشاف؛ تستمر بالقدر والأثر نفسهما؛ إلى غاية إجراءات التحقيق، سيما بخصوص إثبات الجريمة.

[3] نقصد بالمسرح الافتراضي العادي؛ النطاق الافتراضي الذي يخلقه جهاز الإعلام الآلي من جهة، والنطاق الافتراضي العام الذي تخلقه شبكة الاتصال الدولية. وأما المسرح الافتراضي الخاص؛ فنستدل به على الجزء الثاني للشبكة نفسها، المنطوي على نطاقها الافتراضي الخاص المدروس سابقا.

[4] **أنظر:** عبد الفتاح بيومي حجازي، مرجع سابق، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت-دراسة متعمقة في جرائم الحاسب الآلي والإنترنت، مرجع سابق، ص 36.

التقليدي في الإثبات، إذا ما كان للجريمة الرقمية أثر مادي ملموس، كحجز معلومات سرية لدى الجاني في شكلها الورقي بعد نسخها وطبعها[1].

أ-2/ تعطيل الوصول إلى الدليل الرقمي: يمكن أن يتم تعطيل الوصول إلى الدليل الرقمي؛ بالاعتماد على العديد من الطرق والوسائل، سيما التحجج بالظرف الخارج عن إرادة الجاني، أو إتلاف الدليل، أو تحصينه بوسائل فنية. حيث يمكن أن يرجع الجاني؛ سبب وقوع النتيجة الإجرامية إلى خطأ آلي في الجهاز. أو يقوم بإتلاف الدليل بسرعة تكاد تكون خيالية، بعد اكتشاف الجريمة، وربما يكون ذلك حتى بحضور ضباط الشرطة القضائية قليلي المعرفة الرقمية[2].

كما يمكن أن يكون من أسباب تعطيل الوصول إلى الدليل الرقمي؛ احتواء الجهاز أو الموقع الشبكي على نظام أمني مشفر، قد يتعلق أمر فكه على شخص واحد وهو الجاني. أو يستمر السلوك الرقمي ليعبر العديد من الدول، وتسجل في الأخير المعلومات محل الجريمة في دولة أخرى. ما يجعل إنفاذ إجراءات التحقيق ذات الصلة بالمنظومة المعلوماتية؛ أمرا صعبا أو مستحيلا في العديد من الأحيان[3]. وفي السياق نفسه؛ ثار جدل فقهي جنائي حول مدى مشروعية فك التأمين من الشرطة القضائية، والولوج إلى النظام من دون ترخيص، قياسا بمنع الاطلاع على الأوراق المختومة[4].

ب- الصعوبة المتعدية لإثبات الجريمة في المسرح الافتراضي الخاص: قد تتحول الصعوبة النسبية في الإثبات؛ إلى صعوبة متعدية، تتصف بالتعقيد الرقمي وحتى الاستحالة في العديد من الحالات. سيما إذا ما اتصل الإثبات؛ بالنطاق الشبكي الخاص -الويب المظلم خاصةً-. الأمر المنطوي أساسا على استحالة تحديد هوية الجاني ومكان تواجده، وعدم جدوى أعمال جمع الدليل الرقمي[5].

ب-1/ استحالة التعرف على الجاني ومكان تواجده: إذا كان من الصعب التعرف على هوية الجاني ومكان تواجده؛ في إطار النطاق الافتراضي العام. فإن ذلك يصبح مستحيلا بخصوص النطاق الشبكي الخاص، سيما الويب المظلم منه. الذي يتصف بالتشفير والسرية، الموفرة عن طريق توزيع عناوين الشبكة عبر الخوادم الوسيطة، وتعطيل دور البروتوكول "TCP-IP" كما بينا في المبحث الأول من الدراسة.

---

[1] **أنظر:** محمد حماد مرهج الهيتي، جرائم الحاسوب، الطبعة الأولى، دار المناهج للنشر والتوزيع، عمان، الأردن، 2006، ص 226.

[2] **أنظر:** عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت-دراسة متعمقة في جرائم الحاسب الآلي والإنترنت، مرجع سابق، ص 24 و25.

[3] **أنظر:** أحمد بن عبد الرحمن البعادي، "دعاوى الجرائم الالكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول"، ورقة عمل مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا بالدول العربية، الخرطوم، السودان، 23-25 سبتمبر 2012، ص ص 26-29.

[4] الأمر الذي؛ سنتوسع في طرحه ومناقشته عند استعراض الباب الثاني من الدراسة.

[5] الأمر الذي لم نجد له دراسات جنائية متخصصة ومستفيضة. لذلك نعمل على طرحه من منطلق دراية شخصية للباحث بهذا المجال الشبكي السري. بعد الخوض فيه بغرض البحث الجنائي؛ لتحديد مخاطره ومن ثم الوقوف على سبل مكافحته.

وبالرجوع إلى مواقع الويب المظلم؛ نجد أن رواده يتخذون حيطة كبير جدا عند التعامل مع الغير. سيما بتقنيع الوجه عن طريق وضع ألبسة أو أقنعة في شكل حيوانات أو غيرها. كما يمتنعون عن الكلام الصوتي عند التصوير المسجل والمباشر، وان تحدثوا يقومون بذبذبة النبضات الصوتية، إلى درجة تجعل من تحديد هوية الجاني أمرا مستحيلا[1].

ب-2/ عدم جدوى أعمال جمع الدليل الرقمي: إذا كان الوصول إلى الدليل الرقمي عبر النطاق الافتراضي العام؛ أمرا صعبا وفق ما بينا سابقا. يعد بمثابة الأمر المتعدي الصعوبة أو المستحيل؛ بخصوص النطاق الافتراضي الخاص. حيث بالرجوع إلى مميزاته التقنية المنطوية على السرية والتشفير؛ نجد أن معاينة هذه المواقع يكون بمثابة معاينة بلا جدوى، نظرا لتشفير كل المعلومات ذات الصلة. كما أن التفتيش والحجز؛ لا ينصب إلا على المعلومات ذات الصلة بالواقعة المجرمة، كعرض سلاح للبيع مثلا، لكن من دون تحديد موقع الجاني –البائع– ولا هويته.

وعلى العموم؛ قد يرد على ما قدمناه، بخصوص التحري والتحقيق الجنائي في النطاق الشبكي الخاص؛ أننا أسهبنا في وصفه بالنطاق الذي يستحيل اكتشاف واثبات جرائمه، سيما بالنظر إلى قلة الدراسات الجنائية القائلة بما جئنا به. إلا أننا نؤكد على حقيقته الخطيرة التي نراها بمثابة العدو الأول لمجال التحري والتحقيق الجنائي. وفي سياق متصل؛ قيام وزارة الدفاع الأمريكية بتشجيع الشركات التكنولوجيا لإيجاد برامج حديثة تتعامل مع الويب المظلم، بغرض الوصول إلى هوية الجناة، أو على الأقل تسهيل العملية على جهات إنفاذ القانون، أو كأقل تقدير المحو الآلي للإعلانات ذات الطابع الجنائي، دون البحث عن هوية الجاني[2]؛ يعد بمثابة الاعتراف الضمني منها بفشلها في مكافحة هذا النوع من الويب الحديث.

المطلب الثاني: التوجه نحو إجراءات مستحدثة لمواجهة المسرح الجرمي الافتراضي

بعد التطرق إلى إجراءات التحري والتحقيق التقليدية، وتبيان مظاهر عجزها عن مواجهة جرائم الوسط الرقمي عموما؛ أصبح التسليم بالأزمة الإجرائية ذات الصلة أمرا واقعا ومحتوما. ما يتطلب ضرورة التدخل السريع لإيجاد الحل الأنسب، سيما أننا بصدد الحديث عن فشل إجرائي جنائي، ومدى تعلق ذلك بسلامة الدول والأشخاص والأموال. الأمر الذي يعد أبرز تحدٍ من تحديات العصر الحديث، القائم أساسا على حتمية المقاربة العلمية والعملية؛ بين الجانبين التكنولوجي والقانوني سيما الجنائي منه. إما بالاعتماد على الاثنين معا، أو بتقسيم الأدوار بينهما؛ بغرض ضمان نجاعة مكافحة جرائم الوسط الرقمي.

---

[1] الأمر الذي يقوم به، رواد الاتجار بالأطفال والنساء، عبر البث المباشر للممارسات الجنسية والتعذيبية. سيما ما يتم عبر موقع "الغرفة الحمراء – RED ROOM". التي كان يظهر فيها ما يسمى بـ "الأرنب السيئ - the bad rabbit"، ليقوم بممارسة الجنس و/أو التعذيب على أطفال في سن جد مبكرة، على أنه يظهر بألبسة تخفي الهوية والوجه تماما، ولا يتحدث إلا نادرا، وبنبضات مذبذبة. **أنظر في ذلك:** خبر 24، "the bad rabbi أخطر مجرمي الديب ويب"، تاريخ النشر: 23 جويلية 2017، تاريخ التصفح: 17 فيفري 2018، الرابط: https://www.youtube.com/watch?v=aDCMULEgPdA.

[2] **أنظر:** ايفا الشوفي، مرجع سابق.

وفي سبيل تحقيق ما ذكر؛ برزت العديد من الوسائل التقنية والقانونية ذات الصلة. التي تضمن –إلى حد ما– الوقاية و/أو المكافحة اللازمة لمواجهة عجز إجراءات التحري والتحقيق التقليدية. الأمر الذي يقوم أساسا؛ وفق حتمية الاعتماد على الوقاية الرقمية(فرع أول)، وتحديث الإجراءات التقليدية(فرع ثانٍ).

الفرع الأول: حتمية الاعتماد على إجراءات الوقاية الرقمية

يقوم القانون الجنائي عموما؛ على فكرتي الوقاية من الجريمة ومكافحتها. حيث يختص شقه الموضوعي كأصل عام بالوقاية، ويهتم الشق الإجرائي بالمكافحة. ولا يمكن أن يحقق الأول –النص الموضوعي– غاية الوقاية؛ إلا عن طريق الردع، الواقف على ضرورة نجاعة النص الإجرائي[1]. الأمر الذي نؤسس عليه محدودية الدور الوقائي لنص التجريم في جرائم الوسط الرقمي، سيما بعد التسليم فيما سبق من الدراسة؛ بالأزمة الإجرائية ذات الصلة.

وانطلاق مما ذكر؛ أصبح من الضروري الجمع في إطار الوقاية الجنائية؛ بين نص التجريم المذكور سابقا والأمن الرقمي. الأمر الذي نادت به العديد من الجهات المختصة، سيما الاتحاد الدولي للاتصالات، بموجب برنامجه للأمن السيبراني –الرقمي–، الذي تقدم به سنة 2007[2]. وعلى العموم يمكن تحديد المضمون العام للوقاية الرقمية، بتبيان مفهومها(أولا) ومراحلها(ثانيا)، وطرح وسائل تحقيقها(ثالثا).

أولا: مفهوم الوقاية الرقمية

تقوم الوقاية الرقمية ذات الصلة بجرائم الوسط الرقمي؛ على فكرة الأمن الرقمي –السيبراني–. الذي تربطه العديد من الدراسات القانونية والسياسية؛ بالأمن القومي عموما، نظرا لعالمية الوسط الرقمي ومساس جرائمه بالسيادة الإقليمية للدول[3]. الأمر الذي أكدت عليه منظمة الأمم المتحدة، عن طريق فريق الخبراء المعني بدراسة الجريمة السيبرانية، بالقول أن أغلب مستخدمي الشبكة، سيما في الدول النامية؛ يعتمدون الوقاية الرقمية. وأن ضمان ذلك في نطاق أوسع؛ يتطلب تعزيز الشراكات بين القطاعين العام والخاص وإدماج الاستراتيجيات، من خلال نهج كلي يشمل على زيادة الوعي الرقمي[4]. وعلى العموم يمكن أن نقف عند مفهوم الوقاية الرقمية؛ من خلال تحديد تعريفها، وخصائصها.

---

[1] الردع الذي يقسم عموما إلى عام وخاص. فيعرف العام على أنه: "إيلام الجاني بقدر يمنعه من التفكير في العودة إلى الإجرام". ويعرف الخاص على بكونه: "تحذير باقي الأشخاص من ارتكاب الجريمة، سيما بعد متابعة وإدانة من ارتكبها". **أنظر في ذلك:** أحسن بوسقيعة، الوجيز في القانون الجزائي العام، مرجع سابق، ص 290.

[2] **أنظر:** نشادي عبد الرحمان، (الجرائم المعلوماتية ووسائل الاتصال الحديثة)، أطروحة لنيل شهادة الدكتوراه في علوم الإعلام والاتصال، كلية علوم الإعلام والاتصال قسم الإعلام، جامعة الجزائر 3، الجزائر، 2017، ص 176.

[3] **أنظر:** منى الأشقر جبور، "الأمن السيبراني: التحديات ومستلزمات المواجهة"، ورقة عمل مقدمة إلى اللقاء السنوي الأول للمتخصصين في أمن وسلامة الفضاء السيبراتني، المركز العربي للبحوث القانونية والعربية، جامعة الدول العربية، بيروت، لبنان، 27 و28 أوت 2012، ص 02.

[4] **أنظر:** فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، مرجع سابق، ص 17 و19.

1. تعريف الوقاية الرقمية: عكفت الدراسات القانونية السابقة، سيما الجنائية منها؛ على تعريف الأمن الرقمي تحت تسمية أمن المعلومات أو الأمن السيبراني، وإلحاقه المباشر بالوقاية الرقمية. الأمر الذي نؤيده مبدئيا في إطار دراسة الحال، وان نخالفه في بعض النقاط الجزئية من منطلق جنائي محض. وفي هذا الإطار؛ سنعمل على تعريف الأمن الرقمي، ومن ثم نربطه بالوقاية الرقمية من جرائم الوسط الرقمي.

تختلف وتتعدد التعريفات التقنية الموضوعة للأمن الرقمي –الأمن السيبراني أو الأمن المعلوماتي–. التي نجد أهمها التعريف المقدم في التقرير الصادر عن الاتحاد الدولي للاتصالات، حول اتجاهات الإصلاح للعام 2010–2011. حيث اعتبره على أنه: "مجموعة من المهمات، مثل تجميع وسائل وسياسات، وإجراءات أمنية، ومبادئ توجيهية، ومقاربات لإدارة المخاطر، وتدريبات، وممارسات فضلى وتقنيات، يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين"[1].

كما تعرفه الدكتورة منى الأشقر جبور، بناءً على أهدافه؛ بأنه: "النشاط الذي يؤمن حماية الموارد البشرية، والمالية، المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن إمكانات الحد من الخسائر والأضرار، التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح إعادة الوضع إلى ما كان عليه، بأسرع وقت ممكن بحيث لا تتوقف عجلة الإنتاج، وبحيث، لا تتحول الأضرار إلى خسائر دائمة"[2].

أما الوقاية الرقمية التي نقدمها في دراسة الحال، والتي لم نجد لها تعريفا في إطار الدراسات الجنائية السابقة، بصورة مستقلة عن الأمن الرقمي؛ فنقصد بها: "الوسائل الفنية التي يضعها الأشخاص –طبيعية ومعنوية–، بغرض الحيلولة دون الاعتداء الجرمي في إطار جرائم المساس بأنظمة المعالجة الآلية للمعطيات، دون غيرها من جرائم الوسط الرقمي أو أي جريمة أخرى".

يتضح من خلال ما ذكر؛ أنه للاثنين مضمون مختلف رغم وحدة الطبيعة الرقمية. لكن الأمن الرقمي؛ يعمل على مواجهة المخاطر مهما كان تكييفها ومحلها المادي أو الافتراضي[3]، وبغرض تحقيق الحماية الرقمية بمفهومها العام، التي قد تصل إلى حد إعادة الحال إلى ما كان عليه قبل الاعتداء. أما الوقاية الرقمية التي نقصدها؛ فهي لمنع الاعتداء على النطاق الافتراضي للوسط الرقمي قبل حصوله، والمكيف على أنه جريمة مساس بأنظمة المعالجة الآلية للمعطيات دون سواها[4].

---

[1] **أنظر:** منى الأشقر جبور، مرجع سابق، ص 03.

[2] **أنظر:** المرجع والصفحة نفسهما.

[3] الأمر الذي أكدت عليه العديد من الدراسات السابقة، القائلة باعتبار المحافظة على المكونات المادية للحاسوب؛ من أهم أهداف الأمن المعلوماتي. **أنظر في ذلك:** حسين ربيعي، (آليات البحث والتحقيق في الجرائم المعلوماتية)، أطروحة لنيل شهادة دكتوراه علوم في قانون العقوبات والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة 1، الجزائر، 2016، ص 18.

[4] وفي هذا الإطار نجد أن المشرع الجزائري لا يفرق بين الاثنين. حيث عرف سنة 2018 الوقاية الرقمية تحت تسمية الأمن السيبراني. وذلك من خلال حصر دورها في حماية الاتصالات الالكترونية؛ من المساس بتوفر المعطيات وسلامتها وسريتها. وهي التي لا تحمى جنائيا إلا بجرائم المساس بأنظمة المعالجة الإلية للمعطيات كما بينا سابقا. **أنظر في ذلك:** المادة 03-01/10؛ قانون رقم 18-04، مرجع سابق.

2. خصائص الوقاية الرقمية كصورة من صور الأمن الرقمي: بعد التطرق إلى الوقاية الرقمية بالتعريف التقني الجنائي، بشكل منفصل عن الأمن الرقمي، وتبيان نقاط التلاقي والتباين بينهما؛ أصبح من السهل تحديد المميزات الأساسية، ذات الصلة بالوقاية الرقمية في إطار جرائم الوسط الرقمي. التي نحددها في كونها تُعمل قبل ارتكاب الجريمة، ومتصلة بجرائم المساس بأنظمة المعالجة الآلية للمعطيات دون سواها، ولها صفة الوقاية المكملة بعد تلك المقررة بنص التجريم، كما أنها تمارس من قبل الأشخاص ومن دون الحاجة إلى نص.

أ- الوقاية الرقمية لمنع وقوع الجريمة: يتم الاعتماد على إجراءات الوقاية الرقمية كما بينا؛ في المرحلة السابقة لارتكاب الجريمة. كوسيلة احتياطية عامة، يضعها الشخص القائم على النطاق الافتراضي للوسط الرقمي، بتوفر مجموعة من القواعد الأمنية، سيما عنصر القابلية للعدوان الرقمي[1]. الأمر الذي قد يشكل شروعا في الجريمة بالمفهوم الجنائي، إذا ما توفرت أركانه وعناصره القانونية اللازمة[2].

ب- الوقاية الرقمية لمنع وقوع جرائم المساس بأنظمة المعالجة الآلية للمعطيات دون سواها: تؤكد الدراسات ذات الصلة على أن وضع إجراءات الوقاية الرقمية –تحت تسمية الأمن الرقمي–، يكون بغرض حماية النطاق الافتراضي، من أي مساس خارجي غير مرخص، يطال المعلومات الرقمية من حيث الإتاحة والتكامل والوفرة[3]. الأمر الذي بالبحث في تكييفه الجنائي؛ نجد أنه يتطابق مع جرائم المساس بأنظمة المعالجة الآلية للمعطيات، دون سواها من جرائم الوسط الرقمي. نظرا لكونها الوحيدة من تحمي العناصر الثلاثة المذكورة؛ ممن يمسون بها باستعمال الغش ومن دون رضا القائم عليها[4].

ج- الوقاية الرقمية كمكمل للوقاية الجنائية الموضوعية: تعد الوقاية الرقمية؛ بمثابة العنصر الفني المكمل لنص التجريم والعقاب من حيث الدور الوقائي. حيث يمكن تصور وقاية جنائية عن طريق التجريم ومعها وقاية رقمية بالتبعية، لكن لا يمكن تصور العكس. وكل إجراء أمني من دون سبق التجريم؛ يعد داخلا في مفهوم الأمن الرقمي الذي له صفة العموم، ويقي من جميع الأخطار المجرمة وغير المجرمة[5].

---

[1] **أنظر:** أيمن عبد الحفيظ، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، الطبعة الأولى، دار النهضة العربية للنشر والتوزيع، القاهرة، مصر، 2005، ص ص 194-197.

[2] وهو الجائز نظريا، من منطلق تجريم المشرع الجزائري؛ للشروع في جنح المساس بأنظمة المعالجة الآلية للمعطيات. **أنظر في ذلك:** المادة 394مكرر7؛ أمر رقم 66-156، مرجع سابق.

[3] **أنظر:** حسين ربيعي، مرجع سابق، ص 20.

[4] وأما الجرائم الأخرى التي يستعمل فيها الوسط الرقمي كوسيلة أو كمسهل لارتكاب جريمة تقليدية، مثل عرض المخدرات للبيع الرقمي؛ فهي تحتاج إلى وقاية رقمية من نوع آخر، تمارسها جهات قضائية وشبه قضائية -كما سنرى لاحقا-. وهذا نظرا لاعتماد الجاني على وسيلة رقمية، له الحق في استعمالها، ولم يلج إليها بعد تجاوز الوقاية الرقمية.

كما أنه على العكس من الأمن الرقمي؛ الذي يحمي المكونات المادية والافتراضية للوسط الرقمي؛ نجد اقتصار دور الوقاية الرقمية على جرائم المساس بأنظمة المعالجة الآلية للمعطيات؛ بمثابة الدليل على أنها تهتم بالنطاق الافتراضي دون المادي.

[5] الأمر الذي يعد خارجا عن إطار دراسة الحال، نظرا لتخلف وصف الجريمة عن السلوك الموصوف بالخطير، الذي يواجه بإجراءات الأمن الرقمي. وعلى سبيل المثال؛ سبق وأن تطرقنا إلى عدم تجريم المشرع لنسخ المعلومات الرقمية. ومنه أي =

كما أن الاتفاق الفقهي والقضائي؛ بخصوص المعاقبة على جريمة الدخول و/أو البقاء عن طريق الغش إلى المنظومة المعلوماتية، من دون البحث في مدى اعتماد القائم عليها على إجراءات الوقاية الرقمية من عدمها؛ يعد بمثابة إقرار صريح بالدور المكمل لهذه الوقاية. ومنه يمكن تصور تخلفها وانفراد نص التجريم بالدور الوقائي[1]. كما أنه من البداهة جنائيا القول بذلك؛ فالمشرع الجزائري –والمقارن–؛ يجرم الدخول إلى المنازل وانتهاك حرمتها، انطلاقا من طبيعتها، ولا قيمة لغلق أبوابها من قبل أصحابها أو تركها من دون إقفال[2].

د- الوقاية الرقمية يمارسها الأشخاص من دون نص: تعد فكرة ممارسة الوقاية الرقمية من قبل الأشخاص ومن دون نص؛ بمثابة الحد الفاصل بينها وبين وسائل الأمن الرقمي الأخرى المعتمدة خارج إطارها. حيث تمارس الوقاية الرقمية محل الدراسة؛ من قبل القائم على النطاق الافتراضي وبإرادته الحرة –شخص طبيعي أو معنوي–، الهادف إلى حماية المعلومات الرقمية، من الاعتداءات الخارجية. وهذا على عكس وسائل الوقاية الرقمية الأخرى، كالمراقبة الرقمية قبل ارتكاب الجريمة –القادمة بالدراسة في الفرع الموالي–، التي تمارس من قبل جهات محددة بالنص، على غرار الشرطة القضائية والقضاء والجهات الأخرى المرخص لها قانونا. والهادفة عموما إلى الوقاية من باقي جرائم الوسط الرقمي قبل ارتكابها، أو مكافحتها بعد ارتكابها بالحفاظ على الدليل أو المكافحة بالمسح الرقمي الآلي.

كما أن من يضع ترتيبات الوقاية الرقمية؛ لا يحتاج إلى أي نص قانوني يسمح له بوضعها. سيما وأنه يهدف إلى تأمين نطاقه الافتراضي من الاعتداء الخارجي، بوسائل دفاعية، لا تبحث عن الوصول إلى خصوصية الغير والمساس بها، ومنه التقيد بحدود الحماية الدفاعية. حيث يقتصر دورها على انتظار أي اعتداء خارجي وصده بالطرق الرقمية الممكنة[3].

يتضح من خلال المفهوم العام المقدم للمراقبة الرقمية؛ أنها تختلف تماما عن الأمن الرقمي، الذي تؤسس عليه العديد من الدراسات السابقة فكرة الوقاية الفنية. ومنه فضلنا في دراسة الحال التأسيس لهذا الفرق وفق ما ذكر، والعمل به في إطاره الوقائي الإرادي قبل ارتكاب الجريمة، على أن نترك باقي الوسائل الفنية المتصلة بعمل الجهات القضائية وشبه القضائية المختصة؛ للفرع الموالي بالدراسة.

= مواجهة أي مواجهة فنية لعملية النسخ؛ تكون في إطار الأمن الرقمي وليس الوقاية الرقمية، نظرا لاعتباره بمثابة الخطر غير المجرم تماما. **أنظر في ذلك:** المادتان 394مكرر و394مكرر1؛ أمر رقم 66-156، المرجع نفسه.

[1] وهو ما أكدت عليه العديد من الدراسات الفقهية والأحكام القضائية ذات الصلة. سيما القرار الصادر سنة بتاريخ 05 أفريل 1994 عن غرفة الجنح بمجلس قضاء باريس، في مواجهة مؤسسي شركة "Télématiques" ومن معهم. **أنظر في ذلك:**
- AZZOUZI Ali, La Cybercriminalité au Maroc, Imprimé par Bishops Solution, Casablanca, Maroc, 2010, p 115 et 116.

[2] **أنظر:** المادة 1/295؛ أمر رقم 66-156، المرجع نفسه.

[3] التي يصفها البعض بالأساليب التقليدية لحماية الأجهزة. من منطلق أنها تتشابه مع الأمن التقليدي، المنطوي على الحراسة والتحصين والقفل والفتح. **أنظر في ذلك:** منير محمد الجنبيهى وممدوح محمد الجنبيهى، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتهما، دار الفكر الجامعي للطباعة والنشر، الإسكندرية، مصر، 2006، ص 236 و237.

ثانيا: مراحل الوقاية الرقمية

تقوم الوقاية الرقمية ذات الصلة بالمجال الجنائي عموما؛ على تقنيات رقمية لا مجال لتجاوزها أو الاستغناء عنها، أو على الأقل عدم الخروج عن الأساسيات واجبة الإتباع. التي لا ترد هكذا بصورة منعزلة ومتفرقة؛ وإنما في إطار منظم، أردنا طرحه من خلال دراسة الحال؛ على شكل مراحل وتقنيات مُدْخَلَة فيها. الأمر الذي نلخصه في ثلاثة مراحل، الدائرة بين تحديد المعلومة الهامة أولا، وتحليل المخاطر الإجرامية ثانيا، والتقييم واختيار الوسيلة الوقائية ثالثا وأخيرا.

1. مرحلة تحديد المعلومة الهامة: عادةً ما يتم الربط بين المعلومة الهامة والأشخاص المعنوية على اختلاف طبيعتها وأهدافها. فالشركات والمنشآت الهامة؛ تقوم بتحديد المعلومات الجوهرية واجبة الحماية بالسرية اللازمة، حتى لا يتم الحصول عليها بنسخها أو سرقتها من المنشأة الأخرى المنافسة، فتستقطب عملاء المنشأة الأولى لتكون سببا في إفلاسها[1]. ومنه تحدد المعلومات الهامة واجبة الحماية التقنية؛ من قبل صاحب المنشأة أو القائم عليها. الذي قد يكون مسئولا في وزارة الدفاع مثلا، فيحرص على سرية المعلومات الرقمية المتصلة بعمليات التسليح[2].

ونرى في ذلك أن تحديد المعلومة الهامة؛ لا يقتصر على الأشخاص المعنوية فقط، وإنما يتجاوزها إلى الأشخاص الطبيعية أيضا. كما أنه يبرز رقميا في إطار النطاق الافتراضي الذي يقرر القائم عليه إتاحته للجميع من عدمه. فمن أنشأ موقعا شبكيا مثلا، قد يحدد جزءا منه يخصص له وقاية رقمية عالية، ولا يلج إليه إلا أشخاص محددين بذواتهم، أو يمنع ذلك تماما. كما قد يجعله مقيدا بشروط أمنية معينة، مثل عدم إمكانية الولوج لغير الموظف، أو عدم إمكانية الولوج إلا بعد دفع الاشتراكات اللازمة...الخ.

2. مرحلة تحليل المخاطر الإجرامية: تأتي مرحلة تحليل المخاطر مباشرة بعد المرحلة الأولى المذكورة أعلاه. فبعد تحديد المعلومة الهامة من منطلق ذاتي داخلي يحدده القائم على النطاق الافتراضي الخاص؛ ننتقل إلى تحديد المخاطر الرقمية واجبة الوقاية، من منطلق خارجي تحكمه العوامل الخارجة عن إرادة القائم على النطاق نفسه. الأمر المنطوي على تحديد نوع المخاطر ومدى قابلية حدوثها.

وفي الإطار المذكور؛ يقسم المختصون في أمن المعلومات المخاطر المقصودة عموما؛ إلى تقنية وقانونية. حيث تنطوي المخاطر التقنية؛ على الممارسات الرقمية التي من شأنها أن تمس بالمعلومة الرقمية الهامة. فقيام النطاق الافتراضي؛ على التلازم بين الحركة الحرة للمعلومات والانتقال الميسور للتطبيقات والتقنيات والمهارات؛ قد يؤدي إلى هجمات رقمية بأضرار جد بليغة. على سبيل اختراق الأنظمة الرقمية

[1] **أنظر:** محمد سويلم، الإدارة في القرن الحادي والعشرين، دون دار نشر، القاهرة، مصر، 1997، ص 428. **نقلا عن:** أيمن عبد الحفيظ، مرجع سابق، ص 195.

[2] **أنظر:** أيمن عبد الحفيظ، المرجع والصفحة نفسهما.

والتعرض لسرية الاتصالات، والتلاعب بالمعلومات وسرقتها واستثمارها بصورة غير مشروعة، والتعرض لسلامة النطاق الافتراضي...الخ[1].

وأما المخاطر القانونية؛ فتنطوي على الفراغ التشريعي الذي قد يتصل بالعديد من السلوكيات الرقمية. فعدم وجود نصوص قانونية تنظم آليات التعامل مع النطاق الافتراضي في إطاره المشروع عموما، ويحدد بدقة السلوكيات الضارة به في قالب تجريمي محكم؛ يرفع من منسوب الأخطار محل الطرح[2]. وفي إطار متصل كنا قد بينا سابقا؛ أن المشرع الجزائري لا يجرم نسخ المعلومة الرقمية في إطار المساس بأنظمة المعالجة الآلية للمعطيات[3].

بعد تحديد المخاطر التي يتوجب أن تقتصر على الرقمية منها فقط؛ ينتقل القائم على النطاق الافتراضي في إطار المرحلة نفسها، إلى جزئية تحليل القابلية للعدوان. حيث يدرس الأنماط المحتمل إتباعها للاعتداء على النطاق. الأمر الذي ينجز من خلال النظر إلى النطاق نفسه؛ بنظرة العدو المتربص به. وعليه يمكن تحديد تسلسل زمني لمواجهة العمليات الرقمية العدائية، من خلال المعطيات الرقمية ذات الصلة[4].

3. مرحلة التقييم واختيار الوسيلة الوقائية: بعد أن يتم تحليل المخاطر الإجرامية وفصلها عن المخاطر الرقمية في إطارها الأمني العام؛ يتوجب الانتقال إلى المرحلة الثالثة والأخيرة في هذا الصدد، المنطوية على تقييم مزدوج بين نص التجريم والوسائل الوقائية الممكن الاعتماد عليها. ومنه اختيار الوسيلة التي تظهر على أنها مناسبة إلى حدٍ ما.

وهي المرحلة التي تقوم على عنصريين أساسيين. حيث يتوجب القيام أولا؛ بدراسة حالات الانتهاكات المحتملة، بغرض إبراز سلبيات الإجراءات الوقائية ذات الصلة بالجهات المختلفة. على أن يتم الانتقال بعد ذلك؛ إلى دراسة الأحداث التي وقعت سابقا، من حيث نقاط الضعف المتواجدة في أنظمة الوقاية، التي تم استغلالها للاعتداء على النطاق الافتراضي. ومنه العمل على تطويرها وإصلاح ثغراتها[5].

وبعد الانتهاء من التقييم المذكور؛ يتم الانتقال إلى آخر جزئية، المنطوية على تحديد الوسيلة المناسبة لتحقيق الوقاية الرقمية المطلوبة. وهذا من بين العديد من الوسائل، التي سنبينها فيما يلي من الدراسة.

---

[1] **أنظر:** جبريل بن حسن العريشي ومحمد حسن الشلهوب، أمن المعلومات، الطبعة الأولى، دار المنهجية للنشر والتوزيع، عمان، الأردن، 2016، ص 53.

[2] **أنظر:** المرجع نفسه، ص 54 و55.

[3] **أنظر:** المادتان 394 مكرر و394مكرر1؛ أمر رقم 66-156، مرجع سابق.

وعلى العموم وجود مخاطر تقنية من دون تجريم؛ يعد بمثابة الحالة التقنية الخارجة عن إطار دراسة الحال. وتخلف نص التجريم–كما بينا سابقا-؛ يحول الحماية من إطار الوقاية الرقمية إلى إطار الأمن الرقمي.

[4] **أنظر:** أيمن عبد الحفيظ، مرجع سابق، ص 196.

[5] **أنظر:** المرجع نفسه، ص 197.

ثالثا: وسائل الوقاية الرقمية

يعد تحديد الوسيلة المعتمدة لضمان الوقاية الرقمية من جرائم المساس بأنظمة المعالجة الآلية للمعطيات؛ آخر مراحل الوقاية نفسها. التي من خلالها يقوم الشخص –طبيعي أو معنوي–؛ بالبحث في وسائل الوقاية الرقمية بغرض تحديد المناسبة منها لتحقيق الغرض المستهدف. وعلى العموم تتعدد وتتنوع هذه الوسائل، الهادفة إلى تحقيق الوقاية من الاعتداءات المباشرة و/أو غير المباشرة. التي تنطوي على جدران الحماية، والتحقق من الهوية، ومضادات الفيروسات، والتوقيع الرقمي، وتحديد نطاق الاستخدام، والتعامل مع المعطيات الحساسة والأجهزة الحاملة لها، والمراقبة المرئية.

1. جدران الحماية "الجدران النارية": يعتمد في العادة على جدران الحماية؛ للوقاية الرقمية المتصلة بالشبكات الداخلية الموسعة للشركات والمؤسسات. حيث تعمل هذه الجدران دور المصفاة الرقمية التي تصفي –وتحجز–؛ المعلومات الواردة إلى الشبكة الداخلية قدوما من الشبكة أو الشبكات الخارجية[1]. وفي إطار ذلك؛ تتم عملية مراقبة التفاعلات الرقمية محل المرور والتنقل بالاعتماد على الشبكة، عن طريق العزل النسبي للشبكة الداخلية عن الخارجية، وفق معادلة صعبة التحقق إذا ما تعلق الأمر بشبكة الاتصال دولية. حيث يتم السماح لموظفي المؤسسة أو الشركة؛ الاتصال بالشبكة الخارجية، وفي الوقت نفسه منع الاعتداءات الممكنة ممن يستهدفون ذلك[2].

ولغرض تحقيق الهدف الوقائي في هذا الإطار؛ يتوجب إتباع أحد الأساليب الرقمية الثلاث، المنطوية على غربلة الحزم والغربلة مع استبدال عناوينها ومراقبة السياق[3]. فتعتبر غربلة حزم البيانات المرسلة "Packet Filtering"؛ بمثابة فحص الحزم الرقمية المنقولة عبر الشبكة الخارجية –الإنترنت عادةً–، للتحقق من تطابقها مع الشروط الوقائية المتصلة بالجدار الناري المعد خصيصا لهذا الغرض. كما قد يتم الاعتماد على نظام الغربلة مع استبدال عناوين الحزم الرقمية –أو ما يسمى بنظام الوكيل "Proxy"–، حيث ينصب الجدار نفسه بمثابة الوكيل عن الشبكة الداخلية، فيظهر بدلا عنها لكل من يحاول الاتصال بها من الشبكة الخارجية. أو قد يعتمد على نظام مراقبة السياق "Stateful Inspection"، الذي يقوم بعملية المقارنة بالبحث في مدى التطابق بين الحزم المتشابهة، وكل اختلاف بينها يعتبره بمثابة المحاولة غير المشروعة[4].

---

[1] **أنظر:** حسن طاهر داود، مرجع سابق، ص 159.

[2] **أنظر:** جبريل بن حسن العريشي ومحمد حسن الشلهوب، مرجع سابق، ص 111 و112.

[3] الأمر الذي تنظر إليه بعض الدراسات التقنية الأخرى؛ وفق نهج آخر مغاير. حيث تقسمه إلى طرق ثلاث، قائمة على الموجه الحاسب والوسيط والحارس. فيعتبر الموجه الحاسب بمثابة؛ الجهاز الرابط بين الشبكتين الداخلية والخارجية، ليوجه الرسائل ويحمي الشبكة الداخلية في الوقت نفسه. وأما الوسيط –الحاسب المنيع-؛ فهو برنامج يلعب دور المتصل والمتلقي في الوقت ذاته، حيث يظهر للمرسل الخارجي على أنه هو المستقبل، فيستقبل الرسالة ويتحقق من مشروعيتها، ثم يرسلها للشبكة الداخلية على أن يظهر لها في شكل المرسل الخارجي. كما يعمل الحارس –رغم تشابهه مع الوسيط-؛ على تسيير وحدات البرتوكول، ليسمح أو يمنع بمرورها للشبكة الداخلية. **أنظر في ذلك:** حسن طاهر داود، المرجع نفسه، ص ص 161-168.

[4] **أنظر:** جبريل بن حسن العريشي ومحمد حسن الشلهوب، المرجع نفسه، ص 112 و113.

2. التحقق من الهوية: يعد نظام التحقق من الهوية؛ من بين أهم وسائل الوقاية الرقمية في إطار دراسة الحال. حيث يُعتمد من خلالها على وسائل رقمية معينة، تعمل على تحديد المتصل المباشر وغير المباشر؛ بالنطاق الافتراضي[1]. الأمر المنصب على تحديد هوية الشخص، والنشاط المراد انجازه عبر النطاق محل محاولة الولوج. ويعد هذا النوع من الوقاية الرقمية؛ بمثابة الأنظمة الأكثر شيوعا واستعمالا، نظرا للمزايا الكثيرة التي يقوم عليها. حيث وفق دراسة إحصائية فرنسية، منجزة سنة 2009؛ تم التوصل إلى أن أكثر84% من الشركات الفرنسية، تعتمد على وسيلة التحقق من الهوية[2].

ونرى في ذلك؛ أنها الآلية الوقائية الأكثر إفادة في الإطار الجنائي، سيما إذا ما تم الاعتماد بالتوازي على وسائل وقائية أخرى تمنع الاختراق، كجدران الحماية مثلا. حيث التعرف على هوية الشخص ومنعه من الولوج؛ يسهل من متابعته جنائيا على جريمة الشروع في الدخول عن طريق الغش. والتعرف عليه مع تمكنه من الولوج الافتراضي؛ يسهل أيضا في متابعته جنائيا على جريمة الدخول غير التامة[3].

وعلى العموم يعتمد تقنيا لإعمال نظام التحقق من الهوية؛ على العديد من التقنيات ذات الصلة. التي نجد أهمها مفاتيح الدخول والبطاقات الذكية ووسائل التعرف البيولوجي. حيث تتمثل مفاتيح الدخول؛ في رموز مكونة من أحرف وأرقام، يتم إعدادها وفق أحكام محددة. التي بالإضافة إلى كونها شخصية، يجب أن تزيد عن ستة 6 رموز، مع العمل على تغييرها بشكل دوري وعشوائي، أو لمجرد الشك بمعرفته من شخص آخر غير مرخص له بالدخول. ويستحسن أن يتكون المفتاح من رموز عشوائية غير منطقية، التي لا تحوي أي حرف من الحروف الأولى للمستخدم أو اختصار لاسمه أو تاريخ ميلاده[4].

أما البطاقات الذكية؛ فيتم الاعتماد عليها في إطار الولوج المباشر. حيث بفضلها يتم تجاوز الأقفال المبرمجة، التي تستخدم لغلق أو فتح الأبواب المتصلة بقاعات تواجد أجهزة الإعلام الآلي، المراد المساس بأنظمتها أو بالمعلومات التي تحويها. فتحمل هذه البطاقات معلومات رقمية؛ تبين هويته ومدى الترخيص له قانونا بالدخول من عدمه. كما يمكن الاعتماد على وسائل تعرف أخرى، على غرار الوسائل البيولوجية أو البيومترية "Biometrics". التي تعتمد على الصفات الحيوية المميزة للفرد، المتصفة علميا بالتفرد، حيث لا يمكن نقلها من شخص لآخر ولا يمكن نسيانها أو سرقتها. وهي المنطوية أساسا على بصمات الأصابع وكف اليد وشبكة العين والقزحية...الخ[5].

---

[1] نقصد بالاتصال المباشر؛ التعامل المباشر مع جهاز الأعلام الآلي المراد الوصول إلى نطاقه الافتراضي. وأما الاتصال غير المباشر؛ فيكون عن بعد بالاعتماد على شبكة الاتصال الدولية.

[2] **أنظر:** - ARPAGIAN Nicolas, la Cybersécurité, Imprimé par ITCIS, Algérie, 2014, p 44.

[3] حيث يعاقب المشرع الجزائري على الدخول عن طريق الغش في المنظومة المعلوماتية، كما يعاقب على مجرد الشروع في ذلك. **أنظر في ذلك:** المادتان 394 مكرر و394 مكرر7، أمر رقم 66-156، مرجع سابق.

[4] **أنظر:** منير محمد الجنبيهى، ممدوح محمد الجنبيهى، مرجع سابق، ص 237.

[5] **أنظر:** جبريل بن حسن العريشي ومحمد حسن الشلهوب، مرجع سابق، ص 119.

3. مضادات الفيروسات: بغرض المساس بأنظمة المعالجة الآلية للمعطيات عموما؛ تقوم العديد من الجهات الإجرامية؛ بمحاولة الإرسال عبر الشبكة لبعض البرامج ذات المحتوى الخبيث، ومن ثم تثبيتها في المنظومة المعلوماتية محل الاعتداء. حيث تعمل هذه البرامج باختلاف تسمياتها؛ على تعطيل الوظائف الرقمية للمنظومة أو تدميرها كليا أو جزئيا، أو تخريب المعلومات الرقمية المعدة لتشغيلها أو المحتواة بداخلها[1].

ومن أهم سمات الفيروسات الخبيثة؛ أنها غير مستقرة لا من حيث التسمية ولا من حيث محتواها الإجرامي. حيث نجد من بين أهمها وأشهرها؛ ما تسمى بحصان طروادة والقنبلة المعلوماتية –المنطقية والزمنية– والفخ وفيروس زوتوب...الخ[2]. وفي الإطار نفسه؛ كان قد أعد الاتحاد الأوروبي عبر لجنة اتفاقية جرائم الوسط الرقمي؛ العديد من المذكرات التوجيهية، المحذرة من الفيروسات الخطيرة، سيما المستحدثة منها، على غرار فيروس "Spam" وهجمات "Ddos"[3].

وفي سبيل الوقاية الرقمية من الفيروسات ذات الطابع والهدف الإجرامي –المذكورة وغيرها–؛ يعمل تقنيا بما تسمى بمضادات الفيروسات، التي تمنع وتكتشف وتزيل البرمجيات الخبيثة[4]. وتعد هذه البرامج الأكثر شيوعا واستعمالا بين رواد الشبكة عموما، حيث وصلت نسبة الاعتماد عليها إلى 97% سنة 2009، حسب الدراسة الفرنسية سابقة الذكر[5]. وتكتسب مضادات الفيروسات أهمية كبيرة، نظرا لسهولة وقلة ثمن الاعتماد عليها. الأمر الذي تنادي لضرورة العمل به؛ العديد من الجهات المختصة تقنيا وقانونيا، سيما التأكيد على ضرورة تثبيت برامج مكافحة الفيروسات على جميع الخوادم "Servers"[6].

---

[1] **أنظر:** بهاء فهمي الكبيجي، (مدى توافق أحكام جرائم أنظمة المعلومات في القانون الأردني مع الأحكام العامة للجريمة)، رسالة لنيل درجة الماجستير في القانون العام، كلية الحقوق، جامعة الشرق الأوسط، الأردن، 2013، ص 36 و37.

[2] **أنظر:** وليد عاكوم، "التحقيق في جرائم الحاسوب"، د ت ن، تاريخ التصفح: 25 جانفي 2017، الرابط: http// :ArabLawInfo.com، ص 03 و04.

[3] حيث يعد فيروس "Spam"؛ بمثابة الرسالة الشبكية المرسلة عبر البريد الرقمي إلى عدد غير محدد من الأشخاص، على أن تحمل مضمون خبيث في العديد من الأحيان، بغرض الاعتداء على المنظومة والمعلومات. كما تعتبر هجمات "Ddos" -التي قد تأخذ حكم الفيروس الرقمي-؛ الوسيلة الرقمية المعتمد عليها؛ لتعطيل عمل المنظومة المعلوماتية، عن طريق التقدم بطلبات كثيرة تفوق سعة النظام المقصود، ومنه التسبب في بطئه أو توقفه؛ عن تقديم الخدمات لمن لهم الحق القانوني في ذلك. **أنظر في ذلك:**

- Comité de la Convention Cybercriminalité, "Les Spams", Note d'Orientation: 08, Conseil de l'Europe, Strasbourg-France, 2014, p 03. Disponible sur le Lien: http://www.coe.int/fr/web/conventions. **ET:** Comité de la Convention Cybercriminalité, "Les Attaques DDOS", Note d'Orientation: 05, Conseil de l'Europe, Strasbourg-France, 2013, p 01. Disponible sur le Lien: http://www.coe.int/fr/web/conventions.

[4] على أن يعمل القائمون على صنع مضادات الفيروسات؛ على التماشي الرقمي من حيث التطور التقني للفيروسات نفسها. الأمر الذي مر إلى غاية وقتنا الحالي عبر مراحل وأجيال. آخرها الجيل الرابع، الذي يقوم على الحماية المركبة من كل تقنيات برامج الأجيال السابقة. **أنظر:** جبريل بن حسن العريشي ومحمد حسن الشلهوب، مرجع سابق، ص 113 و114.

[5] **أنظر:**
- ARPAGIAN Nicolas, op.cit, p 44.

[6] **أنظر:** علي زغيب، "أفضل الممارسات الأمنية لمزودي خدمات الإنترنت"، أعمال مؤتمر الأمن السيبراني والدفاع السيبراني، الجامعة اللبنانية والوكالة الجامعية للفرنكوفونية AUF، لبنان، د ت، ص 93.

4. التوقيع الرقمي: ينجز التوقيع الرقمي عموما؛ بالتأشير على الوثيقة المقصودة عن طريق المفتاح الخاص "Private Key"، القائم على كلمة مرور خاصة الذي يحوزه المرسل فقط. حيث يحول الرسالة إلى صورة رقمية مشفرة، تحمل دالة متعلقة بهوية المرسل وأخرى بالتوقيع المنجز بالمفتاح الخاص. على أن يستلمها المستقبل باستخدام المفتاح العام "Public Key"، المعروف لدى الجميع. فتَختبر آلية التوقيع الرقمي ما إذا كان التوقيع قد تم إنشاؤه بالمفتاح الخاص من عدمه. وأهم ميزه وقائية تتصل بالتوقيع الرقمي؛ تنطوي على كونه يضفي صفة التوقيع على كل مشتملات الوثيقة الرقمية، فلا يمكن اقتطاع جزء منها أو إجراء أي تعديل، وإلا يعطل التوقيع آليا[1].

رغم إمكانية الاعتماد على التوقيع الرقمي، كوسيلة لمكافحة الجريمة بعد ارتكابها؛ نظرا لكونه يثبت هوية المرسل. إلا أن له دور تقني جوهري في الوقاية من ارتكاب جرائم المساس بأنظمة المعالجة الآلية للمعطيات، سيما حماية المعطيات الرقمية المتواجدة على الوثيقة الرقمية المرسلة؛ من التعديل فيها أو إزالتها. وهي المحمية مسبقا بنص التجريم[2].

5. تحديد نطاق الاستخدام: قد يقوم المسئول عن النطاق الافتراضي عموما في إطار الوقاية الرقمية؛ بالتحكم في الولوج والوصول إلى المعطيات الرقمية. فيحدد الأشخاص والمعطيات معاً، إن من حيث من لهم الحق في استخدام النطاق عموما أو بخصوص كم وكيف المعطيات المسموح لهم بها، وهو ما يسمى بنظام الترخيص "Authorization". وفي هذا الإطار يمكن الاعتماد على العديد من الآليات الرقمية، سيما نظام مصفوفة التحكم في الوصول "Access Control Matrix"[3].

ويتصل هذا الإجراء بالوقاية الرقمية المسبقة؛ من جريمة الدخول و/أو البقاء عن طريق الغش في المنظومة المعلوماتية أو في جزء منها[4]. التي وان لم يتطرق لها المشرع بالمفهوم الدقيق –الأمر المعتاد والطبيعي–؛ نجد أغلب الدراسات المؤسساتية والبحثية والفقهية وحتى الأحكام القضائية؛ تربط عبارة الدخول عن طريق الغش؛ بعدم حيازة الشخص المعني للترخيص بالولوج، أو بحيازته مع تجاوز مضمونه إما موضوعيا أو شخصيا[5].

---

[1] **أنظر:** جبريل بن حسن العريشي ومحمد حسن الشلهوب، مرجع سابق، ص 115.

[2] **أنظر:** المادتان 394مكرر/2 و394مكرر1؛ أمر رقم 66-156، مرجع سابق.

[3] **أنظر:** جبريل بن حسن العريشي ومحمد حسن الشلهوب، المرجع نفسه، ص 117.

[4] **أنظر:** المادة 394مكرر؛ أمر رقم 66-156، المرجع نفسه.

[5] ولو أننا نرى بمحدودية مدلول مصطلح الغش، الذي يتطلب وجود ثقة مسبقة بين القائم على النطاق الافتراضي والشخص القائم بالولوج. ومنه مصطلح الولوج من دون ترخيص المعتمد بالتسمية التقنية الموضحة أعلاه؛ يعد أدق وأشمل، نظرا لارتباط الترخيص بالمشروعية. وهو الأمر الذي عبرت عنه اتفاقية بودابست بالتجاوز غير المشروع "Accès illégal"، واعتبرته المذكرة التفسيرية للاتفاقية نفسها؛ على أنه اختراق غير مرخص له "Intrusion non autorisée". **أنظر في ذلك:**
- Art 02; Convention sur la cybercriminalité- Budapest, "Rapport explicatif", Conseil de l'Europe, 2001. Disponible sur le Lien: http://www.coe.int/fr/web/conventions.

6. التعامل مع المعطيات الحساسة والأجهزة الحاملة لها: قد تحمل أجهزة الإعلام الآلي نطاقا افتراضيا؛ يحوي معطيات رقمية ذات طابع خاص وحساس. التي بسبب موضوعها أو الأشخاص المتصلة بهم؛ تكون بمثابة الهدف الإجرامي المحتمل. ولغرض حماية سرية هذه المعطيات؛ يتوجب العمل إما بالحفظ الآمن أو التخلص المتعمد. فبخصوص الأجهزة والوسائط السليمة؛ يجب العمل على ضمان حماية معطياتها من حيث السرية والتكامل. وأما بخصوص التالفة منها؛ فيتوجب تقييم المخاطر ذات الصلة بالتخلص منها على حالها، ومن ثم التقرير بين إما العمل على إصلاحها أو إتلافها النهائي[1].

وفي حالة تقرير الإتلاف المادي والنهائي للجهاز؛ يتوجب إزالة القرص الصلب "Disque dur" قبل مباشرة العملية[2]، وذلك لتجنب إمكانية التوصل إلى المعلومات التي تحويها من الغير الباحث عنها، بالطرق غير الشرعية، سيما ممن لهم الهدف الإجرامي المبيت. كما أنه بمجرد استشعار الخطر على المعلومة ذات الطابع الحساس و/أو الخطير؛ يتوجب القيام بعملية النسخ من النطاق الافتراضي المتصل بالجهاز محل الخطر إلى نظيره المرتبط بالجهاز الآخر –الآمن–، الذي قد تتم عملية إتلافه أو استبداله بعد التقييم مباشرةً[3].

كما أنه قد يتم إتلاف المعطيات في شكلها الافتراضي، بغض النظر عن الجهاز الحامل لها. وهذا إما لاستشعار الخطر، أو لفرض القانون أو الاتفاق المسبق لذلك. كأن يطلب أحد الأشخاص من كاتب عمومي أن يحرر له رسالة تحمل معلومات سرية، مع اشتراط إتلافها بمجرد مرور مدة معينة. أو أن يقوم المحامي اختياريا بإتلاف المعلومات الرقمية المتصلة بملف أحد موكليه –الدليل الرقمي مثلا–، بمجرد مرور 05 سنوات عن انتهاء العلاقة بينهم[4]. الأمر الذي يحول دون الوصول إليها، ممن يخترق الجهاز عن بعد، قاصدا الحصول عليها.

7. المراقبة المرئية: تتمثل المراقبة المرئية في اعتماد الجهات المعنية و/أو المختصة؛ على كاميرات مراقبة مزودة بأجهزة التسجيل الصوتي والتحكم. التي يتم تثبيتها –كما يمكن أن تكون متحركة– في المكان المناسب والكاشف لموقع وجود أجهزة الإعلام الآلي المقصودة. على أن يتم توصيلها بكابل مخصص لنقل الصوت والصورة إلى جهاز التسجيل الرقمي، المتصل تقنيا بجهاز الإعلام الآلي المثبت في المكان المخصص له[5].

---

[1] **أنظر:** جبريل بن حسن العريشي ومحمد حسن الشلهوب، مرجع سابق، ص 123 و142.

[2] **أنظر:** إيهاب عبد الرحيم علي، "أمن المعلومات الصحية"، مجلة التقدم العلمي، مؤسسة الكويت للتقدم العلمي، الكويت، عدد 99، أكتوبر 2017، ص 24.

[3] **أنظر:** المرجع نفسه، ص 23.

[4] **أنظر:** المادة 2/18؛ قانون رقم 13-07، مؤرخ في 29 أكتوبر 2013، يتضمن تنظيم مهنة المحاماة، (ج ر) عدد 55، صادر بتاريخ 30 أكتوبر 2013.

[5] **أنظر:** جبريل بن حسن العريشي ومحمد حسن الشلهوب، المرجع نفسه، ص 121.

كما يمكن أن يضاف إلى المراقبة المرئية؛ نظام وقائي آخر يقوم على الإنذار الرقمي. حيث بمجرد ولوج الشخص إلى المكان المراقب؛ تلتقطه محسسات تقنية تطلق إشارات و/أو أصوات معينة، بغرض إعلان الخطر للجهة المشرفة على المراقبة. على أن تختلف أنظمة الإنذار المعتمدة، بين الإنذار باستخدام الأشعة الضوئية، أو الموجات الأثرية، أو الأشعة تحت الحمراء[1].

وفي إطار تحقيق الوقاية الرقمية، ذات الصلة أساسا بجرائم المساس بأنظمة المعالجة الآلية للمعطيات؛ نجد أن الدخول إلى مكان تواجد جهاز الإعلام الآلي، بغرض الحصول على معلومات رقمية محددة، بعد الولوج إليه افتراضيا –الجهاز–؛ يعد بمثابة الشروع في ارتكاب جريمة الدخول والبقاء المادي والمباشر في منظومة معلوماتية. الأمر المجرم من المشرع الجزائري كما بينا سابقا[2].

إلا أن وسيلة المراقبة المرئية؛ لا يمكن أن تكون ذات طابع وقائي بأبعاد جنائية؛ إلا إذا ما حالة دون ارتكاب الجريمة المبينة أعلاه. الأمر الذي لا يمكن أن يتحقق إلا بالمتابعة المرئية لمدة 24/24 ساعة وبالتدخل الفوري بعد ملاحظة الدخول إلى الحجرة. أو بالاعتماد على أنظمة الإنذار الفوري إضافة إلى المراقبة المرئية. التي تسمح بالتدخل المباشر أو تكون سببا في فرار الشخص، ما يحول في كل الأحوال دون المساس بالمعطيات.

وعلى العموم؛ تعد الوقاية الرقمية بمثابة الوسيلة المكملة لنص التجريم، التي برزت انطلاقا من الطابع التقني المعقد للوسط الرقمي نفسه. ورغم كونها فعالة في العديد من الأحيان، إلا أنها تظل تحت سيطرة جهات غير حكومية –أو على الأقل غير قضائية–، التي قد تكون نفسها من تصنع وسائل الاعتداء الرقمي.

الفرع الثاني: حتمية تحيين إجراءات التحري والتحقيق

لم تقتصر جهود مواجهة الأزمة الإجرائية بخصوص التحري والتحقيق في جرائم الوسط الرقمي؛ على توسعة الدور الوقائي من سياقه الموضوعي المتصل بنص التجريم؛ إلى البعد التقني المنصب على الوقاية الرقمية. بل تجاوزه إلى الإجراءات الجزائية نفسها، من حيث الوقوع في حتمية العمل على تطويرها، بطريقة تتناسب مع الطبيعة الرقمية الافتراضية للوسط الرقمي كمسرح جرمي حديث.

وفي سبيل تحقيق ذلك؛ برزت العديد من الأحكام الإجرائية. التي منها ما هي مستحدثة، ومنها ما تعد بمثابة النسخة الحديثة لإجراءات تقليدية معروفة سابقا. الأمر الذي نبينه من خلال التطرق إلى أبرز التحيينات المتصلة بإجراءات التحري والتحقيق، إن بخصوص أجهزتها(أولا)، أو بالنظر إلى الأعمال الإجرائية التي تنجزها(ثانيا).

[1] **أنظر:** جبريل بن حسن العريشي ومحمد حسن الشلهوب، مرجع سابق، ص 121.

[2] **أنظر:** المادة 394مكرر/2؛ أمر رقم 66-156، مرجع سابق.

أولا: تحيين الإجراءات المتصلة بأجهزة التحري والتحقيق

يعد نقص الخبرة والدراية العلمية الرقمية لدى أعضاء أجهزة التحري والتحقيق كما بينا سابقا؛ بمثابة السبب الأساس للعجز الإجرائي في مواجهة جرائم الوسط الرقمي، نظرا لكونها –الأجهزة– هي من تمارس الأعمال الإجرائية ذات الصلة. فلا جدوى من تحيين هذه الأعمال؛ دون التأكد المسبق من إتقان التعامل معها ممن سيمارسها. الأمر الذي تمت معالجته جنائيا، بالعمل على التدريب الرقمي لأعضاء أجهزة التحري والتحقيق، و/أو إنشاء أجهزة متخصصة في ذلك.

1. التدريب الرقمي لأعضاء أجهزة التحري والتحقيق: أد ولوج التجريم إلى الوسط الرقمي، وما ترتبت عنه من أثار إجرائية منطوية على العجز في المواجهة؛ إلى القول بضرورة التدريب الفني المستمر لكل من لهم علاقة بالتحري والتحقيق، سواءً رجال الشرطة القضائية أو رجال القضاء –نيابة وتحقيق–. الأمر الذي يقوم على العديد من الأحكام مزدوجة الطبيعة بين التقنية والقانونية. وفي سبيل تبيان ذلك؛ نطرح المقصود بالتدريب الرقمي، وطرق إعماله.

أ– **المقصود بالتدريب الرقمي:** يعد التدريب الرقمي لأعضاء أجهزة التحري والتحقيق؛ بمثابة إدخال واستحداث تعديلات جوهرية على سلوك المتدربين المتصل بالأعمال ذات الصلة بتخصصهم، وممارسة مهامهم[1]. حيث يتوجب أن يشمل التدريب في إطار مواجهة جرائم الوسط الرقمي؛ برامج ومناهج تبين ماهية جهاز الإعلام الآلي ومهارات برمجته، وتقنيات المعالجة الآلية للمعطيات، وجرائمه بمفهومها القانوني التقني، وأساليب ارتكابها. فضلا عن الأمن الرقمي عموما والوقاية الرقمية خاصةً، إن بخصوص آلية عملها أو طرق الاختراق. مع العمل على دراسة المعالجة السابقة في هذا الإطار؛ لجرائم الوسط الرقمي، سيما في إطار مرحلتي التحري والتحقيق[2].

وتكمن أهمية التدريب الرقمي في نقل الخبرة التقنية اللازمة؛ ممن يحوزونها إلى أشخاص لهم الصفة القانونية لمباشرة أعمال التحري والتحقيق اللازمة في مكافحة جرائم الوسط الرقمي. كما يعد بمثابة الفرصة شبه العملية، لتطبيق المهارات الإجرائية والتعرف على سلبياتها وثغراتها، ومنه وضع الحلول المناسبة. وعلى العموم؛ كلما ازداد الوسط الرقمي تعقيدا –سيما نطاقه الافتراضي– كلما ازدادت أهمية التدريب الدوري والمستمر[3].

---

[1] **أنظر:** يوسف حسن يوسف، الجرائم الدولية للإنترنت، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، مصر، 2011، ص 176. **نقلا عن:** حسين ربيعي، مرجع سابق، ص 210.

[2] **أنظر:** علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المكتب الجامعي الحديث، الإسكندرية، مصر، 2012، ص 22.

[3] **أنظر:** حسين بن سعيد الغافري، "التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الإنترنت"، شبكة قوانين الشرق، د ت ن، تاريخ التصفح: 01 مارس 2018، الرابط: http://www.eastlaws.com، ص ص 2-4.

ثار خلاف فقهي حول تحديد من يتم تدريبهم، بين رجال الشرطة القضائية والقضاة من جهة والمختصين في المجال الرقمي من جهة أخرى. حيث يذهب فريق إلى ضرورة تدريب رجال الشرطة والقضاء؛ على التعامل مع عناصر الوسط الرقمي ونطاقها الافتراضي، على أن تكون لهم دراية مسبقة بهذا المجال التقني لمدة لا تقل عن الخمس 05 سنوات. الأمر الذي يعد صعب التحقق عمليا، نظرا لتكوينهم القانوني السابق[1].

ومنه ظهر جانب فقهي آخر، ينادي بضرورة إضفاء صفة الشرطة القضائية على خبراء الوسط الرقمي، يتم اختيارهم بشروط معينة. وهو الأمر المنتقد أيضا نظرا لقلة خبرتهم في المجال القانوني. ومنه أصبح من الأفضل العمل بنظام الفريق، المتكون من رجال شرطة وقضاء لهم دراية فنية مقبولة، وخبراء متميزون في المجال الرقمي[2].

وعلى العموم؛ يقوم التدريب وفق برنامج معين، الذي ينجز في إطار رسمي أو شكلي. حيث يكون التدريب شكليا –غير رسمي–؛ إذا ما اتصل بالوظيفة ومتطلباتها. فيتدرب الفرد المعني من خلال الممارسة الفعلية إلى جانب من له خبرة في مواجهة جرائم الوسط الرقمي. كما قد يتدرب في إطار المناوبة الوظيفية، التي تفرض عليه الممارسة في أقسام مختلفة من بينها القسم الجنائي الرقمي. وأما التدريب الرسمي؛ فيتم من خلال ورش العمل المنعقدة دوريا، في إطار البرنامج المعد خصيصا لذلك، وفق نقاش تحدد أبعاده من قبل المختصين[3].

أما بخصوص البرامج التدريبية المتبعة؛ فلخصها الفقه الجنائي عموما في إطار مجموعة خطوات واجبة الإتباع، المنطوية على الجوانب الثلاث التقنية والجنائية الموضوعية والإجرائية. حيث يتم التطرق تقنيا إلى الوسط الرقمي، سيما بخصوص مفاهيمه العامة والخاصة من جهة، والأخطار المتصلة به من جهة أخرى. كما يتم وضع برنامج تدريبي آخر؛ يتعلق بالجانب الجنائي الموضوعي، من خلال البحث في أنماط جرائم الوسط الرقمي وكل ما يتصل بها موضوعيا من أحكام عامة وخاصة. وأخيرا يتم ضبط برنامج تدريب إجرائي، متصل بالتحري والتحقيق، من حيث الخطة لازمة الإتباع في إطار فريق العمل الجنائي التقني[4].

---

[1] **أنظر:** هشام محمد فريد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني وآلية التدريب التخصصي للمحققين، مجلة الأمن والقانون، أكاديمية شرطة دبي، الإمارات العربية المتحدة، عدد 02، جويلية 1999، ص 99. **وأنظر أيضا:** يحي محمود عيشان، (الصعوبات التي تواجه التنسيق والتعاون الدولي في مكافحة جرائم الحاسب الآلي والإنترنت-دراسة مقارنة)، رسالة لنيل درجة الماجستير في القانون العام، كلية الدراسات القانونية العليا، جامعة عمان العربية للدراسات العليا، عمان، الأردن، 2008، ص 59.

[2] **أنظر:** يحي محمود عيشان، المرجع والصفحة نفسها. **وأنظر أيضا:** محمد كمال شاهين، الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي-دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، مصر، 2018، ص 164.

[3] **أنظر:** هشام محمد فريد رستم، المرجع نفسه، ص 101.

[4] **أنظر:** المرجع نفسه، ص 100 و101.

وفي الإطار نفسه؛ كانت قد اِقترحت العديد من البرامج التدريبية، من قبل هيئات وطنية ودولية[1]. سيما البرنامج المعد سنة 2009 من قبل الشرطة الاتحادية الألمانية، الذي استفادت منه بعض الدول العربية منها الجزائر. حيث تلقى ضباط جزائريون تكوينا رقميا جنائيا في هذا الإطار، ابتداءً من تاريخ 10 فيفري 2009؛ على مستوى "قسم الإرهاب جريمة الإنترنت" المتواجد بالمركز الإفريقي للدراسات والبحوث حول الإرهاب بالجزائر[2].

كما استفاد ضباط الأمن الوطني الجزائري؛ من دورة تدريب وعمل حول "دليل العرائض والأدلة الرقمية". المنظمة في مقر "الأفريبول - Afripol" الجزائر العاصمة، بين 27 فيفري و01 مارس 2018، بالشراكة بين الأمن الوطني، و"أوروماد شرطة Euromed Police IV - IV"، وبحضور ممثلي المنظمات الجهوية للشرطة الإفريقية، والشركات الرقمية الكبرى، كـــ "Twiter - Facebook – Google"[3].

ب- طرق التدريب الرقمي: تعتمد الجهات المختصة في عمليات التدريب الرقمي الجنائي؛ على العديد من البرامج –المذكورة أعلاه وغيرها-. التي تختلف على حسب الطرق المتبعة في التدريب، الدائر بين التعامل المباشر أو غير المباشر مع المتدرب[4]. وعلى العموم نجد من أهم الطرق التدريبية المتبعة في هذا الصدد؛ طريقتي الفريق المتكامل، والمحاكاة الرقمية.

ب-1/ طريقة الفريق المتكامل: يقوم التدريب الرقمي الجنائي وفق طريقة الفريق؛ على فكرة العمل المتكامل بين مجموعة من المختصين في مجالات مختلفة، سيما المجالين القانوني والرقمي. حيث يتدرب أعضاء الفريق بطريقة مشتركة تقود إلى البراعة والاحتراف، خاصةً بتبادل الخبرات فيما بينهم من منطلق علمي وعملي. الأمر الذي تبرز من خلاله أهمية التدرب على شكل فريق، حيث التكامل الحاصل؛ يزيل عقبة التعقيد والتطور السريع المتصل بالوسط الرقمي عموما[5].

وينجز التدريب وفق مجموعتين. فتتشكل المجموعة الأولى من رجال القانون، برئاسة قائد تحري أو تحقيق على حسب الحالة –ضابط أو قاضي-. الذي يتوجب أن يتصف بالخبرة والمهارة الإجرائية

---

[1] على غرار برامج الاتحاد الأوروبي، في صورة مشروعي فالكون لسنة 2001، وأجيس لسنة 2004. **أنظر في ذلك:** وردة شرف الدين، (الإثبات الجنائي بالأدلة الالكترونية-دراسة مقارنة)، أطروحة لنيل درجة الدكتوراه في الحقوق، كلية الحقوق والعلوم السياسية، ، جامعة محمد خيضر بسكرة، الجزائر، 2017، ص ص 53-55.

[2] **أنظر:** الناشط الجزائري، **"**ألمانيا سلمت 6 دول عربية منها الجزائر معدات وتجهيزات لمراقبة الإنترنت**"**، تاريخ النشر: 03 جويلية 2013، تاريخ التصفح: 23 فيفري 2018، الرابط: http://dzactiviste.info.

[3] **أنظر:** وحيد تاجي –مكتب الموقع الالكتروني، **"**الأفريبول يحتضن اجتماعات العمل حول دليل العرائض والأدلة الرقمية**"**، مجلة الشرطة، المديرية العامة للأمن الوطني، الجزائر، عدد 140، مارس 2018، ص 66 و67.

[4] قد يخضع المعني إلى تدريب جنائي رقمي بالحضور المادي إلى مكان التدريب، كما قد يكون اتصاله غير مباشر -عن بعد-، عبر التواصل الشبكي وفق الأحكام المقررة مسبقا. الأمر الذي –التدرب عن بعد-؛ يمتاز بجعل المتدرب يتعامل أكثر مع الوسط الرقمي، ويخرج من جو التدريب التقليدي إلى الرقمي الحديث، ما يزيد من جودة الأداء الأمني. **أنظر في ذلك:** عبد الله سيف الكيتوب، الأحكام الإجرائية لجريمة الاحتيال المعلوماتي، دار النهضة العربية، القاهرة، مصر، 2013، ص 248.

[5] **أنظر:** محمد كمال شاهين، مرجع سابق، ص 164 و165.

العالية، وبدراية رقمية مقبولة. كما أنه هو من يرأس الفريق بمجموعتيه، ويوزع المهام بين أعضائه، ويصدر الأوامر اللازمة لسير العملية. أما المجموعة الثانية؛ فتتكون من الخبراء المختصين في الجريمة التقليدية والرقمية معا. فيقوم خبراء الوسط الرقمي؛ بالأعمال الرقمية اللازمة، التي تعاين المسرح الافتراضي وتحافظ عليه من جهة، وتقود إلى فك خيوط الدليل الرقمي من جهة أخرى. كما قد تتطلب ضرورات التحري والتحقيق؛ الاستعانة بخبير تقليدي، الذي يرفع البصمات المتواجدة على العناصر المادية للوسط الرقمي، أو يرسم "كروكي" لمسرح الجريمة بطريقة فنية دقيقة[1].

ب-2/ طريقة المحاكاة الرقمية: تعد المحاكاة الرقمية بمثابة الوجه الحديث لإجراء إعادة تمثيل الجريمة، من حيث عناصره وحيثياته، مع اختلافها عنه بخصوص المرحلة والهدف. فإعادة تمثيل الجريمة كما هو معروف جنائيا؛ يكون بعد ارتكاب الجريمة وبغرض الوصول إلى فك خيوطها واتضاح الرؤية الجنائية[2]. أما المحاكاة الرقمية؛ فهي وسيلة تدريب يخضع لها المعنيون بالتحري والتحقيق في إطار فريق متكامل، بغرض مواجهة الواقع الرقمي المتصل بجرائم الوسط الرقمي المحتمل ارتكابها. حيث يتم الاعتماد على تقليد مطابق للأصل الرقمي الجنائي، فيتعايش المتدرب مع الملابسات والاحتمالات ذات الصلة. الأمر الذي سيزيد بالتأكيد من قدرة التعامل مع التحريات والتحقيقات الجنائية الحقيقية[3].

وللقيام بالمحاكاة الرقمية في إطار التحري والتحقيق المتصل جرائم الوسط الرقمي؛ يتوجب الالتزام بمجموعة شروط ومراحل. حيث يتم تحضير فريق متكامل وفق ما سبق بيانه، بالإضافة إلى كاتب سيناريو يقوم بصياغة الأفكار والتفاصيل الرقمية، التي يتوجب أن تكون مطابقة للبعد الافتراضي الحديث. كما يقوم القائم على الفريق بضبط المشكلة المطلوب محاكاتها والهدف المراد تحقيقه، ومدى تحقيق ذلك للفائدة المرجوة. ثم يتم إقامة التصميم الأولي الواقف على المتغيرات الممكن مواجهتها[4]. على أن تلي هذه المرحلة؛ العديد من المراحل الأخرى، المختلفة على حسب طبيعة المحاكاة وموضوعها الجنائي، سيما تخزين المعلومات وتحليلها ومنه التحول من التصميم المبدئي إلى البرنامج الرقمي النموذجي[5].

وتعد المحاكاة الرقمية؛ من أهم وسائل التدريب، سيما بالنظر إلى الفوائد الكبيرة التي تدرها على المتابعة الجنائية عموما. حيث تفتح المجال للتصور الرقمي والتنبؤ بشأنه، ومنه الوقوف على الأخطاء والثغرات المتصلة. كما أنها تدفع لتوسيع دائرة المعرفة الرقمية، لدى جهات التحري والتحقيق[6].

---

[1] **أنظر:** محمد كمال شاهين، مرجع سابق، ص 165 و166.

[2] **أنظر:** محمد حزيط، مرجع سابق، ص 131 و132.

[3] **أنظر:** محمود عبد الحميد عبد المطلب، البحث والتحقيق الجنائي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة، مصر، 2007، ص 150. **نقلا عن:** حسين ربيعي، مرجع سابق، ص 211.

[4] **أنظر:** المرجع نفسه، ص 152.

[5] **أنظر:** وردة شرف الدين، مرجع سابق، ص ص 59-62.

[6] **أنظر:** المرجع نفسه، ص 62 و63.

2. إنشاء أجهزة تحري وتحقيق متخصصة في مواجهة جرائم الوسط الرقمي: ذهب البعض من الفقه الجنائي؛ إلى أبعد مما طرح سابقا بخصوص التدريب الرقمي. حيث أكدوا على حتمية إنشاء أجهزة تحري وتحقيق متخصصة في جرائم الوسط الرقمي دون غيرها، أو على الأقل إنشاء مصالح فرعية ومركزية متخصصة للغرض نفسه[1]. الأمر الذي يكون متصلا بالجهات شبة القضائية –الشرطة القضائية–، التي تمارس المواجهة بقيادة القاضي المختص، وبالتعاون مع جهات أخرى غير قضائية و/أو أجنبية[2]. وبالفعل تم إنشاء العديد من الأجهزة محل الطرح، إن بالآلية الاتفاقية الدولية والإقليمية، أو التشريعية المقارنة والمحلية.

أ- الإنشاء الاتفاقي لأجهزة التحري والتحقيق في جرائم الوسط الرقمي: عرف الإطار الاتفاقي العالمي والإقليمي؛ إنشاء العديد من الأجهزة الشرطية، التي تعمل على مكافحة الجريمة عموما وجرائم الوسط الرقمي خاصةً. حيث نجد من أهم هذه المؤسسات؛ منظمة الشرطة الدولية "الأنتربول – Interpol"، التي لها تنظيم محكم في هذا الإطار. والمنطوي على الوحدة المتخصصة لمكافحة جرائم الوسط الرقمي من جهة، والمجموعة الثامنة من جهة أخرى[3]. كما أنها تضم ما يسمى بالمركز العالمي المتعدد الاختصاصات لمكافحة الجريمة، ومختبر الأدلة الجنائية الرقمية. وعلى العموم؛ تعد كلها بمثابة الأجهزة المساعدة لجهات إنفاذ القانون في الدول الأعضاء[4].

كما تم إنشاء العديد من الأجهزة الشرطية وغيرها على المستوى الإقليمي، التي تهدف إلى التحري والتحقيق في جرائم الوسط الرقمي، كجهة مساعدة لسلطات إنفاذ القانون في الدول الأعضاء. والمنطوية عموما على المصالح أو المراكز المتخصصة، المنشأة في إطار الأجهزة الإقليمية ذات الاختصاص الشرطي العام.

وفي هذا الإطار؛ نجد الشرطة الأوروبية "الأوروبول – Europol" على المستوى الأوروبي، والشرطة الإفريقية "الأفريبول – Afripol" على المستوى الإفريقي[5]. حيث تعمل الشرطة الأوروبية على مكافحة جرائم الوسط الرقمي –وحتى الوقاية منها–، عن طريق الأعمال المنجزة في إطار مهامها الشرطية، سيما

---

[1] **أنظر:** علي عدنان الفيل، مرجع سابق، ص 21 و22.

[2] حيث تقوم الشرطة القضائية بالدور الأساس في عملية التحري والتحقيق محل الدراسة. على أن انجاز ذلك؛ يتطلب تدخل العديد من الجهات، سيما القضاء كجهة مشرفة وقائدة من جهة، والهيئات الإدارية والمدنية والدولية والمقارنة من جهة أخرى. الأمر الذي سنبينه بالتفصيل عند التطرق إلى الفصل الموالي بالدراسة.

[3] **أنظر:** وردة شرف الدين، مرجع سابق، ص 69.

[4] **أنظر:** الإنتربول، "الجريمة السيبيرية"، مشاريع شرطية تركز على المستقبل، د ت. متوفر عبر الرابط: https://www.interpol.int/.../UFS_CYBER_Brochure_feb17_AR_03.

[5] وفي الإطار نفسه؛ نبرز غياب مثل هذه الأجهزة على المستوى العربي، إن كجهاز شرطي عام أو كجهاز متخصص في جرائم الوسط الرقمي. ولو أنه توجد بعض المحاولات التي لم يكتب لها النجاح، سيما اقتراح إنشاء المنظمة العربية لمكافحة جرائم المعلوماتية والإنترنت. **أنظر في ذلك:** عبد الله عبد الكريم عبد الله، مرجع سابق، ص ص 148-168.

العملية منها. فتساعد جهات إنفاذ القانون في الدول الأعضاء على مواجهة هذا النوع من الإجرام الحديث[1]. وهو ما تسعى إليه أيضا منظمة الشرطة الإفريقية المنشأة حديثا، حيث جاء في بيان رقمي صادر عن المديرية العامة للأمن الوطني الجزائري؛ بمناسبة اختتام أشغال دورة التدريب والعمل حول "دليل العرائض والأدلة الرقمية" –المذكورة سابقا–، أنه للمنظمة خارطة طريق يتوجب انجاز عناصرها. التي من أهم تحدياتها؛ نجد التعاون الشرطي والأمني في مجال مكافحة جرائم الوسط الرقمي[2].

ب– الإنشاء التشريعي لأجهزة التحري والتحقيق في جرائم الوسط الرقمي: لم يتوقف أمر إنشاء الهيئات المختصة بمكافحة جرائم الوسط الرقمي؛ عند البعد الدولي والإقليمي المساعد، بل تجاوزه إلى الهيئات الداخلية المنشأة حديثا، إن بطبيعتها شبة القضائية أو الإدارية. الأمر الذي كرسه القانون الفرنسي؛ بإنشائه للعديد من الهيئات المتخصصة، سيما في إطار المديرية المركزية للشرطة القضائية، أو الديوان المركزي لمكافحة الإجرام المرتبط بالوسط الرقمي، الذي يضم العديد من الفرق المركزية والمحلية، وكذلك الهيئة المركزية لردع العنف ضد الأشخاص، وفرقة التحقيق في الاحتيال عبر الوسط الرقمي...الخ[3].

وفق النهج نفسه؛ قامت العديد من القوانين الأخرى بإنشاء هيئات أو مصالح متخصصة، سيما ما جاء في إطار التشريع الإماراتي، الذي أكد على التخصص الشخصي، من حيث إضفاء صفة مأمور الضبط القضائي –الضابط– المختص في جرائم الوسط الرقمي دون سوها[4]. كما قامت عمليا شرطة العديد من الإمارات بإنشاء فرق متخصصة في مكافحة جرائم الوسط الرقمي، على غرار شرطة أبوظبي[5].

وفي الإطار ذاته؛ قامت الجزائر بإنشاء مصالح ومراكز متخصصة في مكافحة جرائم الوسط الرقمي، منها ما تلعب دور الخبير الرقمي، ومنها ما تمارس التحري والتحقيق الجنائي. فتختص بانجاز الخبرة الرقمية؛ أقسام تقنية متصلة بمخابر الشرطة العلمية، والمعهد الوطني للأدلة الجنائية وعلم الإجرام التابع للدرك الوطني. كما تختص بالتحري والتحقيق؛ جهات شبه قضائية مختصة، على غرار الفرق التابعة للأمن الوطني، ومركز الدرك الوطني للوقاية من جرائم الإعلام والجرائم المعلوماتية ومكافحتها[6].

---

[1] الأمر الوارد صراحةً في التقرير الصادر عنها سنة 2014، الذي قدم شرحا مفصلا عن جرائم الوسط الرقمي، وعن آليات المواجهة واجبة الإتباع من سلطات إنفاذ القانون في الدول الأعضاء. **أنظر في ذلك:**

- Groupe de Travail Interministériel Sur la Lutte Contre la Cybercriminalité, "Protéger les Internautes", Rapport sur la Cybercriminalité, Europol, 2014. Disponible sur le Lien: https://www.europol.europa.eu.

[2] **أنظر:** الموقع الرسمي للأمن الوطني الجزائري، "اختتام اجتماعات عمل أفريبول - أوروماد شرطة IV حول-دليل العرائض والأدلة الرقمية"، د ت ن، تاريخ التصفح: 06 مارس 2018، الرابط: http://www.algeriepolice.dz.

[3] **أنظر:** ورد شرف الدين، مرجع سابق، ص ص 72-75.

[4] **أنظر:** المادة 49؛ مرسوم بقانون اتحادي رقم 05-12، الإمارات العربية المتحدة، مرجع سابق.

[5] **أنظر:** أحمد عبد العزيز، "شرطة أبوظبي تشكل فرقاً متخصصة لمكافحة الجرائم الإلكترونية"، تاريخ النشر: 13 فيفري 2012، تاريخ التصفح: 06 مارس 2018. الرابط: http://www.alittihad.ae/details.php?id=15105&y=2012.

[6] **أنظر:** ورد شرف الدين، المرجع نفسه، ص ص 77-83.

كما استحدث المشرع الجزائري سنة 2009؛ هيئة وطنية تهتم بالوقاية من جرائم الوسط الرقمي ومكافحتها. الأمر الذي تنجزه الهيئة وفق العديد من المهام المنوطة بها، سيما في إطار التحري والتحقيق بخصوص جرائم الوسط الرقمي. ولم يجعل منها المشرع هيئة شبه قضائية، وإنما أصبغ عليها الصفة الإدارية المستقلة، التي تساعد الهيئات القضائية وشبه القضائية صاحبة الاختصاص الأصيل[1].

ثانيا: تحيين الإجراءات المتصلة بأعمال التحري والتحقيق

كل ما ذكر سابقا بخصوص تحيين الإجراءات ذات الصلة بأجهزة التحري والتحقيق؛ لا يمكن أن يحدث الأثر الإجرائي الايجابي المرغوب فيه؛ إلا إذا ما تم النظر إلى الأعمال الإجرائية الممارسة من طرفهم بالنظرة نفسها، المؤدية إلى ضرورة تحيينها هي الأخرى. الأمر الذي سارعت إلى التعامل معه العديد من النصوص الاتفاقية والتشريعية المختلفة، سيما الجزائرية منها. وهو ما ورد في إطار قانوني، ينطوي إما على تحديث الأعمال الإجرائية التقليدية لتتماشى مع طبيعة الوسط الرقمي كمسرح افتراضي للجريمة، أو التغيير من طبيعتها القانونية[2].

1. تحديث الأعمال الإجرائية التقليدية: عملت العديد من التشريعات الوطنية؛ على تعديل نصوصها الإجرائية ذات الصلة بالتحري والتحقيق. باحثةً من خلال ذلك الوصول إلى التكيف القانوني اللازم مع مستجدات الوسط الرقمي وطبيعته الافتراضية المعقدة. الأمر الذي نادت به قبل ذلك أول اتفاقية إقليمية –ذات طابع دولي– في هذا الإطار، المنطوية على اتفاقية بودابست لسنة 2001. حيث جاء في مذكرتها التفسيرية؛ أن الاتفاقية قد هيأت الإجراءات التقليدية مثل التفتيش والضبط، للممارسة في البيئة التكنولوجيا الحديثة. وهو ما يفيد التحديث المقصود[3].

وبعد ذلك قامت أغلب الدول في إطار تشريعاتها الداخلية أو الاتفاقيات الإقليمية؛ بإتباع النهج الإجرائي الوارد في اتفاقية بودابست، حول ضرورة تعديل النصوص الإجرائية التقليدية لتتماشى مع المسرح الجرمي الافتراضي. حيث أكدت على ذلك الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، وان بشكل

---

[1] **أنظر:** المادة 1/13؛ قانون رقم 09-04، مرجع سابق. **وأنظر أيضا:** المادة 02؛ مرسوم رئاسي رقم 15-261، مؤرخ 08 أكتوبر 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما، (ج ر) عدد 53، صادر بتاريخ 08 أكتوبر 2015.

على العموم؛ لم نتطرق في هذا الموقع إلى الهيئات المنشأة في إطار القانون الجزائري وغيره؛ إلا على سبيل الذكر والمسايرة للنهج الجنائي من حيث حتمية إنشاء هيئات تحري وتحقيق متخصصة. على أن نستعرض بالتفضيل في الفصل التالي بالدراسة؛ الهيئات ذات الصلة في إطار القانون الجزائري، ومن تتعامل معها في إطار التعاون الدولي.

[2] وفق ما ذكر أعلاه بخصوص الأجهزة؛ نؤكد على أننا نبين في هذا الموقع أهم التحيينات المتصلة بالأعمال الإجرائية، بغرض إبراز الحتمية المؤدية إلى ذلك، انطلاقا من العجز الإجرائي المؤسس له سابقا. على أن نتطرق إلى الأعمال الإجرائية بالتفصيل؛ في الباب الثاني والأخير من الدراسة.

[3] **أنظر:** عمر محمد بن يونس، الاتفاقية الأوروبية حول الجريمة الافتراضية – المذكرة التفسيرية، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، 2005، ص 112.

إجرائي مباشر دون تبيان حتمية التعديل. فتطرقت إلى التفتيش والحجز والاعتراض بالمفهوم الرقمي الحديث[1]، الذي يكاد يكون مطابقا لما ورد في اتفاقية بودابست سابقة الذكر[2].

كذلك الأمر بخصوص النصوص الإجرائية الداخلية؛ التي تضمنت في إطار التعديلات المختلفة لقوانين الإجراءات الجزائية، أو بإصدار نصوص خاصة؛ الأحكام الإجرائية المعدلة، سيما بخصوص التفتيش والحجز واعتراض المراسلات والاتصالات الرقمية. الأمر الذي نذكر فيه على سبيل المثال؛ التشريع الفرنسي، الذي عمل على تحديث النصوص المتصلة بالتفتيش والحجز في أنظمة المعالجة الآلية للمعطيات، بغرض تنسيقها مع ما ورد في اتفاقية بودابست سابقة الذكر[3].

ولم يخرج المشرع الجزائري عن ذلك كثيرا، حيث عمل سنة 2009 على إصدار قانون خاص، يتعلق بالقواعد الخاصة للوقاية من جرائم تكنولوجيات الإعلام والاتصال ومكافحتها –المذكور سابقا–. الذي تضمن أحكاما إجرائية تعدل من نظيرتها التقليدية المتصلة بالتفتيش والحجز، وتصبغ عليها الطابع الرقمي الحديث[4]. كما تضمن أيضا إجراء مراقبة الاتصالات الالكترونية، الذي يعد في جزء منه بمثابة التحديث الرقمي لإجراء المعروف سابقا، المنطوي على التنصت أو اعتراض المراسلات وتسجيل الأصوات[5].

2. إضافة أعمال إجرائية حديثة: زيادة على ما ذكر أعلاه بخصوص تحديث النصوص الإجرائية التقليدية، عملت العديد من التشريعات الوطنية والنصوص الاتفاقية؛ على وضع إجراءات أخرى، تحمل الطابع المستحدث إن بسبب دورها الوقائي الجديد أو نظرا لطبيعتها غير المسبوقة. حيث اكتسبت إجراءات التحري والتحقيق لأول مرة الطابع الوقائي، كما ظهرت إجراءاتها ذات الطابع الكفاحي بطبيعة لم يسبق التعامل بها من قبل.

أ- استحداث الدور الوقائي لأعمال التحري والتحقيق: دفع التعقيد التقني للوسط الرقمي كمسرح جرمي حديث، وقبله الخطورة الموضوعية لجرائمه؛ بالتشريعات المختلفة وقبلها الفقه إلى ضرورة تفعيل الدور الوقائي للأعمال الإجرائية. الأمر الذي يعد بمثابة الدور المستجد تماما عن هذا المجال الجنائي، حيث يعد من بديهيات القانون الجنائي، أن دور قانون الإجراءات الجزائية، يبدأ عند مرحلة البحث والتحري التي تنطلق بعد ارتكاب الجريمة وليس قبلها[6].

---

[1] **أنظر:** المواد 26 و27 و29؛ مرسوم رئاسي رقم 14-252، مرجع سابق.

[2] **أنظر:** - Art 19; Convention sur la cybercriminalité- Budapest, op.cit.

[3] **أنظر:** - Art 57-1; code de procédure pénale français, partie législative, op.cit.

[4] **أنظر:** المادتان 05 و06؛ قانون رقم 09-04، مرجع سابق.

[5] **أنظر:** المادة 04؛ المرجع نفسه. **وأنظر أيضا:** المواد من 65مكرر5 إلى 65مكرر10؛ أمر رقم 66-155، مرجع سابق.

[6] **أنظر:** المادة 3/12؛ المرجع نفسه.

يأخذ الدور الوقائي الممارس من قبل الشرطة القضائية في إطاره الرقمي؛ العديد من الصور التي نفرغها في قالب واحد منطوي على المراقبة الرقمية لنشاط رواد شبكة الاتصال الدولية. حيث نجد على سبيل المثال أن سلطات إنفاذ القانون في دولة الإمارات العربية المتحدة؛ تعمل بما يسمى نظام الرقيب، الذي يمنع الولوج الشبكي إلى المواقع التي يتحسس بأنها غير مشروعة وفق القانون الإماراتي[1].

كما اعتمد المشرع الجزائري بالقانون 09-04؛ على نظام المراقبة الالكترونية –الرقمية–، لتمارس من خلاله الشرطة القضائية والجهات المختصة عموما الدور الوقائي في بعض جرائم الوسط الرقمي، المحصورة قانونا في الجرائم ذات الوصف الخطير عموما، سيما للوقاية من استعمال الوسط الرقمي؛ لارتكاب الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة. أو للاعتداء على أنظمة المعالجة الآلية للمعطيات بغرض المساس بالنظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني[2].

وفي سياق ما ذكر؛ نتساءل عن مدى مشروعية ممارسة الدور الوقائي من قبل الشرطة القضائية. سيما أن الأمر يشكل مساسا خطيرا بحرمة الحياة الخاصة، المحمية أصلا بالنص الجنائي الموضوعي[3]. في الحقيقة يمكن أن نؤسس لذلك بالعديد من الحجج، حيث قد ينظر إلى الأمر على أنه بمثابة الضبط الإداري اللازم، للحيلولة دون المساس بالنظام العام الرقمي –الشكل الحديث للنظام العام–. فنظام الرقيب مثلا؛ يضبط عن طريق منع الولوج إلى المواقع محل قرار الحضر. وهو ما يشبه أيضا فكرة الضبط الإداري الممارس من قبل الجهات الأمنية؛ عن طريق القيام بدوريات المراقبة على مقاهي الإنترنت. وإلزام أصحابها بمسك دفاتر يقيد فيها أسماء وبيانات كل شخص يلج إلى الشبكة[4].

كما يمكن أن نؤسس للدور الوقائي محل الطرح؛ عن طريق التسليم بخطورة الجرائم محل الوقاية المحددة حصرا من المشرع الجزائري. والتي –خطورتها– تعد بمثابة مفتاح قانوني يمكن من خلاله تقديم الصالح العام المتصل بالوقاية من الجرائم الخطيرة؛ عن الصالح الخاص المتعلق بحماية حرمة وسرية الحياة الخاصة للأشخاص. وهذا بالإضافة إلى أن عجز إجراءات التحري والتحقيق في إطار المكافحة الجنائية –كما بينا سابقا–؛ قد يحتم العمل بالوقاية الإجرائية، بالتوازي مع الوقاية الرقمية المذكورة[5].

---

[1] **أنظر:** محمد طارق عبد الرؤوف الخن، جريمة الاحتيال عبر الإنترنت، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2011، ص 236 و237.

[2] **أنظر:** المادة 1/04-أ و ب؛ قانون رقم 09-04، مرجع سابق.

[3] **أنظر:** المادة 303 مكرر؛ أمر رقم 66-156، مرجع سابق.

[4] **أنظر:** محمد كمال شاهين، مرجع سابق، ص 141 و142.

[5] وفي سياق متصل؛ تطرقت العديد من الدراسات إلى وجود ما تسمى بالرقابة الداخلية الوقائية. التي تمارس من الجهة المستخدمة على موظفيها، خوفا على مصالحها المهنية وحفاظا على سرية نشاطاتها. **أنظر في ذلك:** منير محمد الجنبيهى، ممدوح محمد الجنبيهى، مرجع سابق، ص 238.

ب- تحديث طبيعة الدور الكفاحي لأعمال التحري والتحقيق: إضافة إلى الدور الوقائي؛ قامت العديد من النصوص الاتفاقية والوطنية بالمناداة بضرورة التعديل من الدور الكفاحي في العديد من عناصره، سيما بخصوص التعاون الدولي والدليل الرقمي. حيث يعتمد في العادة على التعاون الدولي؛ كوسيلة مساعدة جهات إنفاذ القانون الوطنية، ولا يلجأ إليه إلا في حالات ضيقة، تتصل بتسليم المجرمين أو تبادل الإنابات في الجرائم التي تتطلب ذلك[1]. كما أن الدليل الجنائي القائم على النظام الحر –المعتد من المشرع الجزائري كأصل–؛ يفتح المجال أمام القاضي ليبني قناعته على الدليل الذي يجده مناسبا[2].

إلا أنه بالرجوع إلى جرائم الوسط الرقمي ومسرحها الافتراضي؛ نجد أنها جرائم تكتسي البعد العابر للحدود الوطنية، رغم إمكانية قيامها على سلوك بسيط كالسب عن طريق الشبكة مثلا. الأمر الذي دفع بأغلب الدراسات الرسمية والبحثية، وخاصة النصوص الاتفاقية؛ إلى القول بانقلاب الدور، حيث أصبح الأصل في المكافحة هو التعاون الدولي[3]. كما أن الدليل الجنائي الذي يقوم على نظام حرية الإثبات في التشريع الجزائري؛ يتحول مفهومه إلى الحرية في الاعتماد على أنواع الدليل الرقمي دون غيره. والتقيد بخصوص الأدلة المادية غير الرقمية؛ في إطار اعتبارها على أنها مجرد قرائن فقط[4].

في ختام المبحث الثاني؛ يمكن القول أن جرائم الوسط الرقمي عموما ومسرحها الافتراضي خاصةً؛ قد أحدثا وضعا جنائيا بطابع معقد موضوعيا، وكثير التعقيد إجرائيا. الأمر الذي أدى –كما بينا سابقا–؛ إلى عجز إجرائي واضح بخصوص التحري والتحقيق، سيما بالنظر إلى المظاهر ذات الصلة، التي منها ما هي متصلة بالأجهزة المعنية من منطلق نقص الخبرة والتخصص اللازمين، ومنها ما تتعلق بطبيعة ونجاعة الأعمال التي تمارسها الأجهزة نفسها.

وفي سبيل مواجهة التعقيد الموضح أعلاه؛ سارعت العديد من الجهات الرسمية والبحثية القانونية والتقنية؛ لاستحداث وسائل تقنية وقانونية تمكن من تجاوز الوضع الجنائي الصعب. الأمر الذي دفع من جهة؛ إلى استحداث الوقاية الرقمية كوسيلة مكملة لنص التجريم، والمناداة بضرورة الاعتماد على وسائلها المتعددة على حسب الحالة. والتأسيس من جهة أخرى؛ لحتمية تحيين إجراءات التحري والتحقيق التقليدية، إن بخصوص الأجهزة أو الأعمال أو حتى الطبيعة القانونية. وهو ما قامت به فعلا القوانين المقارنة، سيما الجزائري منها، الذي سنتطرق إلى مستجداته بخصوص الأجهزة والأعمال التي اعتمدها بعد التحيين؛ فيما هو قادم من الدراسة، بنوع من الوصف والتحليل والنقد.

---

[1] **أنظر:** المادة 694 وما يليها؛ أمر رقم 66-155، مرجع سابق.

[2] **أنظر:** المادة 1/212؛ المرجع نفسه.

[3] **أنظر:** الأمر الذي أكدت اتفاقية بودابست –سابقة الذكر–، في مقدمتها. التي اعترفت وأقرت بضرورة التعاون الدولي كسبيل وحيد للمكافحة. **أنظر في ذلك:** Préambule; Convention sur la cybercriminalité- Budapest, op.cit. -

[4] **أنظر:** محمد حماد مرهج الهيتي، مرجع سابق، ص 226.

الفـــصل الثانـي

أجهزة التحري والتحقيق في جرائم الوسط الرقمي

أدى الطابع الرقمي المعقد لجرائم الوسط الرقمي عموما ومسرحها الافتراضي خاصةً؛ إلى القول والتسليم بالخصوصية القانونية ذات الصلة، إن موضوعيا أو إجرائيا. الأمر الذي نتجت عنه العديد من الإشكالات المستجدة والدخيلة عن المجال الجنائي، سيما الإجرائي منه. الذي أصبحت أحكامه التقليدية عاجزة، إلى درجة وصف الوضع بالأزمة الإجرائية الحديثة –كما بينا سابقا–. فتسبب المسرح الرقمي وجرائمه، في إحداث الأزمة الإجرائية المذكورة؛ يعد بمثابة الحلقة الأساسية الدافعة لضرورة إعادة النظر في الإجراءات المعمول بها، إن بخصوص الأجهزة أو الأعمال الإجرائية التي تباشرها عند ممارسة كل من التحري والتحقيق.

كما عكفت العديد من الدول بعد تسليمها بالأزمة الإجرائية المذكورة؛ إلى العمل في الإطارين الدولي والوطني على تحديث الإجراءات الجزائية المتصلة بالتحري والتحقيق في جرائم الوسط الرقمي، سيما بخصوص الأجهزة القائمة بذلك. حيث تم العمل على التدريب المستمر والدوري لأعضاء الأجهزة القضائية والشرطية من جهة، واستحداث أجهزة مختصة بالتحري والتحقيق في مجال جرائم الوسط الرقمي من جهة أخرى –إن كأجهزة رئيسية أو مساعدة–، وخاصةً التوجه نحو العمل الجماعي في إطار الفريق المتكامل وفق خطط إجرائية معدة مسبقا. كما لا ننسى الاعتماد على الدور الوقائي كطابع إجرائي حديث، والارتقاء بالتعاون القضائي والشبه القضائي؛ إلى مصاف الإجراءات اللازمة والضرورية بعد أن كان لا يعتمد عليه إلا في حالات ضيقة.

وفي السياق نفسه؛ لم يخرج القانون الجزائري كثيرا عما ذكر. حيث تعامل مع جرائم الوسط الرقمي بنوع من الخصوصية الإجرائية، سيما بخصوص الأجهزة المختصة بالتحري والتحقيق فيها وقواعد اختصاصها الإقليمي والنوعي من جهة، وتأكيده من جهة أخرى؛ على ضرورة التعاون الوطني في إطار العمل المتكامل بين العديد من الأجهزة المحلية، وفي الإطار الدولي إن مع الأجهزة العالمية والإقليمية أو الأجهزة الوطنية المقارنة. كما ميز في التعامل الإجرائي من حيث الأجهزة وقواعد اختصاصها؛ على حسب نوع الجريمة المتصلة بالوسط الرقمي، التي قد تتصل بالمساس بأنظمة المعالجة الآلية للمعطيات، أو تكون جريمة تقليدية ترتكب عبر النطاق الافتراضي للوسط الرقمي أو يكون مسهلا لارتكابها.

وتدقيقا في نصوص القانون الجزائري ذات الصلة بالأجهزة المختصة بالتحري والتحقيق في جرائم الوسط الرقمي؛ نجد أنه وضع العديد من الأجهزة الوطنية ذات الصلة، التي نقسمها انطلاقا من الخصوصية المعقدة لجرائم الوسط الرقمي؛ إلى رئيسية ومساعدة، مع إمكانية اللجوء وفق شروط محددة إلى التعاون الدولي القضائي والشرطي وحتى الإداري والفني في هذا الإطار. الأمر الذي نبينه بالتطرق أولا إلى الأجهزة الوطنية المختصة(مبحث أول)، ومن ثم نستعرض الأجهزة الأجنبية الممكن التعامل معها في إطار التعاون الدولي(مبحث ثانٍ).

المبحث الأول

الأجهزة الوطنية المختصة بالتحري والتحقيق في جرائم الوسط الرقمي

عملت الجزائر كغيرها من نظرائها على تحيين نصوصها القانونية ذات الصلة بمجال الإجراءات الجزائية، بغرض التماشي مع مستجدات جرائم الوسط الرقمي ومسرحها الافتراضي، سيما لتفادي العجز الإجرائي المذكور سابقا. حيث تم الإبقاء على المظهر التقليدي للأجهزة المختصة تحت غطاء الجهات القضائية وشبه القضائية، مع التعديل في نطاق اختصاصها النوعي والإقليمي. كما تم استحداث نظام الأقطاب والأجهزة والمصالح المتخصصة.

كما أنه في العديد من الأحيان تتطلب الطبيعة المعقدة لجرائم الوسط الرقمي؛ العمل بنظام الفريق المتكامل. حيث نجد أكثر من جهاز تقليدي وحديث؛ يعملون بالتنسيق المستمر للوصول إلى فك خيوط الجريمة. الأمر الذي يؤكد الفقه الجنائي على وجوب إتباعه، سيما بتحديد خطة العمل المناسبة والتخطيط الاستراتيجي، وتشكيل فريق العمل وفق متطلبات القضية نفسها، المتكون من قائد الفريق والمحقق الجنائي والخبير الرقمي وخبير البصمات، بالإضافة إلى أشخاص آخرين على حسب نوع الجريمة[1].

وفي السياق نفسه؛ تعامل القانون الجزائري مع المسرح الجرمي الافتراضي، من حيث الأجهزة المختصة بالتحري والتحقيق فيه؛ بمنهجي التحديث والاستحداث. حيث نجد من خلال ذلك العديد من الأجهزة التي لها الطابع الرئيسي والمباشر في هذا الإطار(مطلب أول)، وأخرى لها الدور المساعد للأجهزة الرئيسية(مطلب ثانٍ).

المطلب الأول: الأجهزة الرئيسية المختصة بالتحري والتحقيق في جرائم الوسط الرقمي

يعد من بديهيات القانون الجنائي، أن الأجهزة المختصة بالتحري والتحقيق؛ هي الجهات القضائية وشبه القضائية. فمرحلة التحري تملكها النيابة العامة، وتمارسها عبر جهاز الشرطة القضائية. وإجراءات التحقيق القضائي؛ يختص بها قضاء التحقيق من قاضي تحقيق وغرفة اتهام، اللذان يمارسانها بالاعتماد عادةً على جهاز الشرطة القضائية في إطار الإنابة القضائية. الأمر الذي نرى فيه تحديدا من المشرع للأجهزة الرئيسية، التي تساعدها أجهزة أخرى، أنشأة لمواجهة المسرح الافتراضي كما سنرى لاحقا.

وفي سبيل التطرق البحثي للأجهزة الرئيسية المختصة بالتحري والتحقيق في جرائم الوسط الرقمي؛ وجب العمل على تبيان نوعيها من قضائية وشبه قضائية، وذلك من حيث التركيبة وقواعد الاختصاص النوعي والإقليمي. الأمر الذي نستعرضه من خلال طرح الأجهزة القضائية أولا(فرع أول)، والأجهزة الشرطية شبه القضائية ثانيا(فرع ثانٍ).

[1] **أنظر:** علي عدنان الفيل، مرجع سابق، ص ص 13-18.

الفرع الأول: الأجهزة القضائية القائدة للتحري والتحقيق في جرائم الوسط الرقمي

تنطوي الأجهزة القضائية القائدة للتحري والتحقيق في الجريمة عموما، وجرائم الوسط الرقمي خاصةً؛ على جهازي النيابة العامة وقضاء التحقيق. حيث تحدد الجهة المختصة؛ على حسب طبيعة الإجراءات المتبعة. فالأعمال الإجرائية الممارسة بخصوص مرحلة التحري؛ تختص بها النيابة العامة[1]، وأما الأعمال الممارسة في إطار إجراءات التحقيق القضائي؛ فيختص بها قضاء التحقيق[2].

وفي السياق نفسه؛ لم يتعرض القانون الجزائري للأجهزة القضائية القائدة للتحري والتحقيق في جرائم الوسط الرقمي بالاستحداث، وإنما أبقى على الأجهزة التقليدية، مع التعديل في قواعد اختصاصها، على حسب نوع الجريمة. وهو ما نبينه من خلال التطرق لجهازي النيابة العامة(أولا)، وقضاء التحقيق(ثانيا).

أولا: جهاز النيابة العامة القائد لمرحلة التحري عن جرائم الوسط الرقمي

تعد النيابة العامة بمثابة الجهاز الأساسي في إطار الإجراءات الجزائية عموما، نظرا لكونه المالك الأصيل لمرحلة التحري أولا، والمباشر الوحيد للدعوى العمومية ثانيا. فلا يمكن تصور قيام أي عمل من أعمال التحري دون تدخل النيابة العامة، إن بالإشراف والإدارة أو بالممارسة المباشرة. الأمر الذي لا يختلف كثيرا؛ بخصوص التحري في جرائم الوسط الرقمي. الذي نستعرضه؛ بالتطرق أولا إلى الأحكام العامة لجهاز النيابة العامة، وتبيان ثانيا قواعد اختصاصها في إطار جرائم الوسط الرقمي.

1. الأحكام العامة لجهاز النيابة العامة: يعرف العديد من الفقه الجنائي؛ جهاز النيابة العامة إطلاقا من دوره في الدعوى العمومية[3]. الأمر الذي نستبعده في إطار دراسة الحال، نظرا لبحثنا عن دور النيابة العامة في مرحلة التحري الوارد بالمادة 2/12 و3 "ق.إ.ج" –سابقة الذكر–، ومنه نعرفه على أنه: "جهاز يناط به إدارة الشرطة القضائية والإشراف على أعمالها بخصوص التحري عن الجرائم المرتكبة".

وتتشكل النيابة العامة عموما من نائب عام ووكلاء جمهورية. حيث نجد على مستوى كل مجلس قضاء نائب عام يمثل المجلس والمحاكم التابعة له، على أن يساعده في مهامه على مستوى المجلس نفسه نواب عامون مساعدون. كما يباشر وكلاء الجمهورية ووكلاء الجمهورية المساعدون؛ صلاحيات النيابة العامة على مستوى المحاكم التابعة للمجلس، المتصل بنطاق اختصاص النائب العام الذي يمثلونه[4].

---

[1] **أنظر:** المادة 2/12و3؛ أمر رقم 66-155، مرجع سابق.

[2] **أنظر:** المادة 13؛ المرجع نفسه.

[3] حيث يعرفها الفقه الجنائي الجزائري انطلاقا من المادة 29 "ق.إ.ج"؛ على أنها: "جهاز يناط به تحريك ومباشرة الدعوى العمومية أمام جهات القضاء الجنائي". **أنظر في ذلك:** ناصر حمودي، (قانون الإجراءات الجزائية الجزائري)، محاضرات السنة الثانية حقوق، معهد الحقوق، المركز الجامعي العقيد آكلي محند أولحاج، البويرة، الجزائر، 2010، ص 174.

[4] **أنظر:** المواد من 33 إلى 35؛ أمر رقم 66-155، المرجع نفسه. **وأنظر أيضا:** عبد الله أوهابية، شرح قانون الإجراءات الجزائية الجزائري، مرجع سابق، ص 60.

كما تقوم النيابة العامة بممارسة الأعمال الإجرائية المتصلة بمرحلة التحري؛ عن طريق قواعد اختصاص نوعي وإقليمي. فمن حيث الاختصاص النوعي؛ نجد أن النيابة العامة عموما سواءً الناب العام أو وكيل الجهورية–سيما أنها لا تتجزأ–؛ تختص بمباشرة الإجراءات اللازمة للتحري عن السلوكيات المجرمة قانونا، إما بنفسها أو عن طريق رجال الشرطة القضائية. ففي الحالة الأولى؛ تتلقى كافة البلاغات والشكاوى ذات الصلة. وفي الحالة الثانية؛ يقوم وكيل الجمهورية بمراقبة وإدارة أعمال الشرطة القضائية في إطار المرحلة نفسها، سيما زيارة أماكن التوقيف للنظر ومراقبة تنفيذه[1].

على العموم ينصب الاختصاص النوعي للنيابة العامة؛ على ممارسة إجراءات مرحلة التحري بخصوص كل السلوكيات المجرمة قانونا في إطار التشريع الجزائري، حتى وان وجد مانع تحريك الدعوى العمومية فيما بعد. وهو ما نجد عليه بعض الاستثناءات الصريحة؛ على غرار الجرائم العسكرية التي لها نظام خاص وتختص بالتحري فيها النيابة العامة العسكرية التي يمثلها وكيل الدولة[2]. أو الجرائم الموصوفة على أنها خيانة عظمى المرتكبة من رئيس الجمهورية، والجنايات والجنح المرتكبة من الوزير الأول أثناء تأدية المهام، والتي لها نظام خاص بنص دستوري[3].

وأما بخصوص الاختصاص الإقليمي للنيابة العامة أثناء مرحلة التحري؛ فنجد أن المشرع حدده وفق أصل واستثناء. حيث الأصل أن يمارس وكيل الجمهورية صلاحيات التحري؛ على الجرائم المتصلة بدائرة اختصاص المحكمة التي يمارس مهامه فيها، إما نظرا لأنها تتصل بمكان ارتكاب الجريمة أو بمكان إقامة المشتبه فيه أو بمكان القبض عليه[4].

كما يمكن كاستثناء أن يوسع اختصاص وكيل الجمهورية، ليمتد إلى دائرة اختصاص المحاكم المتاخمة للمحكمة التي يمارس فيها مهامه، وهذا وفق شروط معينة، سيما تطلب التحري لذلك[5]. كما يمدد الاختصاص إلى محاكم أخرى المحددة عن طريق التنظيم؛ إذا ما تعلق التحري بجرائم المعاملة الخاصة، التي حددها المشرع في ستة 06 جرائم، نجد من بينها تلك الماسة بأنظمة المعالجة الآلية للمعطيات[6].

---

[1] **أنظر:** المادة 36؛ أمر رقم 66-155، مرجع سابق. **وأنظر أيضا:** عبد الله أوهايبة، شرح قانون الإجراءات الجزائية الجزائري، مرجع سابق، ص 65.

[2] **أنظر:** المواد من 24 إلى 40 و42 و44 و49؛ أمر رقم 71-28، مؤرخ في 22 أفريل 1971، يتضمن قانون القضاء العسكري، (ج ر) عدد 38، صادر بتاريخ 11 ماي 1971، معدل ومتمم.

[3] **أنظر:** المادة 177؛ مرسوم رئاسي رقم 96-438، مؤرخ في 07 ديسمبر 1996، يتعلق بإصدار نص تعديل الدستور الجزائري، (ج ر) عدد 76، صادر بتاريخ 08 ديسمبر 1996. معدل ومتمم سيما بقانون رقم 16-01، مؤرخ في 06 مارس 2016، (ج ر) عدد 14، صادر بتاريخ 07 مارس 2016.

[4] **أنظر:** المادتان 35 و1/37؛ أمر رقم 66-155، المرجع نفسه. **وأنظر أيضا:** ناصر حمودي، (قانون الإجراءات الجزائية الجزائري)، مرجع سابق، ص 177.

[5] **أنظر:** المادة 57؛ أمر رقم 66-155، المرجع نفسه. .

[6] **أنظر:** المادة 2/37؛ المرجع نفسه.

2. قواعد اختصاص جهاز النيابة العامة في إطار جرائم الوسط الرقمي: وضع القانون الجزائري العديد من الأحكام ذات الصلة بتحديد قواعد الاختصاص النوعي والإقليمي، التي يباشر من خلالها جهاز النيابة العامة سلطات التحري في جرائم الوسط الرقمي. حيث يختلف الأمر بين جرائم المساس بأنظمة المعالجة الآلية للمعطيات، والجرائم التقليدية التي يكون النطاق الافتراضي للوسط الرقمي الوسيلة أو المسهل في عملية ارتكابها.

أ- قواعد اختصاص جهاز النيابة العامة في إطار جرائم المساس بأنظمة المعالجة الآلية للمعطيات: تختص النيابة العامة نوعيا بالتحري عن جميع الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، المبينة سابقا والمجرمة من المشرع بالمواد من 394مكرر إلى 394مكرر7 "ق.ع"، حتى وان توفر مانع قانوني بشأن تحريك الدعوى العمومية فيما بعد. إلا بخصوص بعض الاستثناءات الضيقة جدا –المذكورة سابقا في إطار الأحكام العامة–، سيما بخصوص الجرائم ذات الوصف العسكري، التي يختص بها وكيل الدولة العسكري، والجرائم الموصوفة على أنها خيانة عظمى المرتكبة من رئيس الجمهورية، والجنايات والجنح المرتكبة من الوزير الأول أثناء تأدية المهام.

أما بخصوص الاختصاص الإقليمي؛ فاعتبر المشرع أن المساس بأنظمة المعالجة الآلية للمعطيات من الجرائم ذات المعاملة الخاصة. التي تتطلب الخروج عن الأصل العام، المتصل بمكان ارتكاب الجريمة أو مكان إلقاء القبض على المشتبه فيه أو مكان إقامته. حيث أقر بجواز تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم[1].

لم تتأخر السلطة التنفيذية كثيرا لتضع التنظيم المبين لنطاق التمديد الإقليمي المشار إليه بالمادة 2/37 "ق.إ.ج" المذكورة. حيث تم إصدار مرسوم تنفيذي سنة 2006 –المعدل سنة 2016–[2]. الذي قسم الاختصاص الإقليمي لوكلاء الجمهورية إلى أربعة أقطاب متخصصة على الصعيد الوطني، وهي المنطوية على محكمة سيدي محمد بالجزائر العاصمة، ومحكمة قسنطينة، ومحكمة ورقلة، ومحكمة وهران[3].

---

[1] **أنظر:** المادة 2/37؛ أمر رقم 66-155، مرجع سابق. .

[2] **أنظر:** مرسوم تنفيذي رقم 06-348، مؤرخ في 05 أكتوبر 2006، يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، (ج ر) عدد 63، صادر بتاريخ 08 أكتوبر 2006، معدل بمرسوم تنفيذي رقم 16-267، مؤرخ في 17 أكتوبر 2016، (ج ر) عدد 62، صادر بتاريخ 23 أكتوبر 2016.

[3] حيث يمتد الاختصاص المكاني لوكيل الجمهورية لدى محكمة سيدي محمد –الجزائر العاصمة-؛ ليشمل ولايات الجزائر، الشلف، الأغواط، البليدة، البويرة، تيزي وزو، الجلفة، المدية، المسيلة، بومرداس، تيبازة، عين الدفلى. كما يمتد الاختصاص المكاني لوكيل الجمهورية لدى محكمة قسنطينة؛ ليشمل ولايات قسنطينة، أم البواقي، باتنة، بجاية، تبسة، جيجل، سطيف، سكيكدة، عنابة، قالمة، برج بعريريج، الطارف، خنشلة، سوق أهراس، ميلة. وأما وكيل الجمهورية لدى محكمة ورقلة؛ فيمتد ليشمل ولايات ورقلة، أدرار، تامنغست، إيليزي، بسكرة، الوادي، غرداية. كذلك بخصوص وكيل الجمهورية لدى محكمة وهران، الذي يمتد اختصاصه الإقليمي ليشمل ولايات وهران، بشار، تلمسان، تيارت، تندوف، سعيدة، سيدي بلعباس، مستغانم، معسكر، البيض، تيسمسيلت، النعامة، عين تموشنت، غليزان. **أنظر في ذلك:** المواد 2 و3 و4 و5؛ المرجع نفسه.

لكن الأمر الذي يطرح إشكالا في هذا الصدد؛ ينطوي على أن المشرع بالمادة 2/37 "ق.إ.ج" عبر بمصطلح "يجوز تمديد الاختصاص المحلي". ما قد يدفع للقول أن التمديد المذكور سابقا والوارد بالمرسوم التنفيذي 06-348؛ يعد بمثابة الأحكام المكملة التي يجوز مخالفتها، وبالتالي يمكن العودة إلى الأصل العام بخصوص الاختصاص الإقليمي. الأمر الذي لنا نظرة مغايرة في تفسيره، حيث نرى أن المشرع بمصطلح "يجوز"؛ هو بصدد مخاطبة السلطة التنفيذية وليس القضاء. حيث فوض للسلطة التنفيذية مسألة تمديد الاختصاص الإقليمي لو أرادت ذلك. وبمجرد استعمالها للتفويض ومنه إصدار المرسوم الذي يمدد، يصبح العمل القضائي بالتمديد بمثابة الأمر الواجب الذي لا يجوز مخالفته.

ب- **قواعد اختصاص جهاز النيابة العامة في إطار الجرائم التقليدية المتصلة بالوسط الرقمي:** تختص النيابة العامة نوعيا أيضا -كأصل عام-؛ بالتحري عن جميع الجرائم التقليدية المرتكبة أو المسهل ارتكابها عبر النطاق الافتراضي للوسط الرقمي. الأمر الذي تحكمه القواعد العامة للاختصاص النوعي المبينة سابقا. حيث كل جريمة تقليدية يمكن تصور اتصالها بالنطاق الافتراضي للوسط الرقمي؛ تكون النيابة العامة مختصة بالتحري بشأنها.

كذلك بخصوص الاختصاص الإقليمي؛ الذي تحكمه القواعد العامة نفسها المطبقة على الجريمة التقليدية كأصل عام. إن بخصوص الاختصاص المحلي الأصلي، القائم على اتصال مكان ارتكاب الجريمة أو مكان إلقاء القبض على المشتبه فيه أو مكان إقامته؛ بدائرة اختصاص وكيل الجمهورية. أو بخصوص إمكانية تمديده متى تطلبت ضرورة التحري ذلك[1].

إلا أنه بخصوص بعض الجرائم التقليدية المنطوية على جرائم المعاملة الخاصة، التي يتم الاعتماد على النطاق الافتراضي للوسط الرقمي من أجل ارتكابها أو تسهيل ارتكابها؛ يتم تمديد الاختصاص الإقليمي إلى دائرة الأقطاب المتخصصة، وفق التوزيع نفسه المذكور سابقا بخصوص جرائم المساس بأنظمة المعالجة الآلية للمعطيات، الدائر بين محكمة سيدي محمد -الجزائر العاصمة- ومحكمة قسنطينة ومحكمة ورقلة ومحكمة وهران[2].

وتتمثل جرائم المعاملة الخاصة -التقليدية- محل تمديد الاختصاص المحلي المذكور أعلاه؛ في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف. على أن نؤكد بحتمية تمديد الاختصاص المحلي للجرائم المذكورة وفق الطريقة المبينة، سواءً تعلقت بالوسط الرقمي، أو ارتكبت في شكلها التقليدي المعروف[3].

---

[1] **أنظر:** المادتان 1/37 و57؛ أمر رقم 66-155، مرجع سابق.

[2] **أنظر:** المادة 2/37؛ المرجع نفسه. **وأنظر أيضا:** المواد 2 و3 و4 و5؛ مرسوم تنفيذي رقم 06-348، مرجع سابق.

[3] **أنظر:** المادة 2/37؛ أمر رقم 66-155، المرجع نفسه.

ثانيا: جهاز قضاء التحقيق القائد لإجراءات التحقيق في جرائم الوسط الرقمي

إذا كانت النيابة العامة هي الجهاز الأساسي في إطار ممارسة مرحلة التحري، يعد جهاز قضاء التحقيق عموما؛ بمثابة القائدة لإجراءات التحقيق بعد تحريك الدعوى العمومية، وذلك رغم مباشرتها من قبل النيابة العامة نفسها. الأمر الذي يستقر نوعا ما؛ في إطار التحقيق المتصل بجرائم الوسط الرقمي. وهو ما نستعرضه فيما يلي؛ من خلال التطرق إلى الأحكام العامة لجهاز قضاء التحقيق، وقواعد اختصاصه في إطار جرائم الوسط الرقمي.

1. الأحكام العامة لجهاز قضاء التحقيق: عكفت أغلب الدراسات الفقهية ذات الصلة بالإجراءات الجزائية عموما وقضاء التحقيق خاصةً؛ على تعريف قضاء التحقيق بصورة منفصلة عن وصف الجهاز. وهذا بغض النظر عن مرحلتي التحقيق القضائي ودرجتي الابتدائي منه. حيث تصب أغلب التعريفات في قالب التحقيق القضائي الابتدائي، الممارس من قاضي التحقيق وغرفة الاتهام قبل مرحلة المحاكمة[1]. الأمر الذي يمكن من خلاله أن نعرف جهاز التحقيق القضائي على أنه: "جهاز قضائي يناط به ممارسة مهام التحقيق القضائي الابتدائي في القضية المخطر بها وفق الأحكام المبينة قانونا".

ويتكون جهاز التحقيق القضائي الابتدائي من تشكيلة مكونة من قاضي التحقيق وقضاة غرفة الاتهام[2]. حيث وفق التوزيع المعتمد من المشرع الجزائري؛ نجد على مستوى كل محكمة قاضي تحقيق –أو أكثر–، يعين بقرار صادر عن وزير العدل لمدة ثلاث 03 سنوات[3]، كما توجد على مستوى كل مجلس قضاء غرفة اتهام أو أكثر، يعين قضاتها بقرار صادر عن وزير العدل أيضا، وللمدة نفسها المقدرة بثلاث 03 سنوات[4].

كما لا يمكن لجهاز التحقيق القضائي أن يمارس إجراءات التحقيق الابتدائي؛ إلا عن طريق وسائل قانونية محددة حصرا. فيمارس قاضي التحقيق مهام الدرجة الأولى من التحقيق الابتدائي؛ بعد اتصاله القانوني بالقضية التي حركة الدعوى العمومية بشأنها، وذلك –كأصل عام– وفق إما طلب افتتاحي لإجراء

---

[1] حيث يعرف التحقيق القضائي بوصفه مجموعة إجراءات قضائية؛ على أنه: "مجموعة من الإجراءات ذات الطبيعة القضائية، التي يجب أن تنجز وفق ما بينه القانون، ومن جهات التحقيق المختصة". **أنظر في ذلك:** ناصر حمودي، (قضاء التحقيق في قانون الإجراءات الجزائية الجزائري-دراسة تحليلية نقدية)، مرجع سابق، ص 10.

[2] وهذا بغض النظر عن جهاز التحقيق القضائي المتصل بالأحداث، الواردة أحكامه بموجب قانون حماية الطفل الصادر بموجب قانون رقم 15-12، المذكور سابقا.

[3] في الحقيقة ثار خلاف فقهي حول طريقة تعيين قضاة التحقيق. الأمر الذي أحدثته التعديلات المتتالية لقانون الإجراءات الجزائية. حيث قبل تعديل سنة 2001؛ كانت المادة 39 "ق.ا.ج"؛ تشير إلا أن قاضي التحقيق يعين في منصبه بقرار من وزير العدل لمدة ثلاث 03 سنوات. لكن بعد التعديل المذكور أصبح يعين بمرسوم رئاسي. إلا أن المشرع رجع بتعديلة الوارد سنة 2006 وألغى المادة 39 تماما. الأمر الذي يعتبره العديد بمثابة الرجوع إلى الأصل. سيما لكون التعيين في وظيفة قاضي تحقيق؛ تعد بمثابة توزيع المهام القضائية المعني بها وزير العدل. **أنظر في ذلك:** أحسن بوسقيعة، التحقيق القضائي، مرجع سابق، ص 19.

[4] **أنظر:** المادة 176؛ أمر رقم 66-155، مرجع سابق.

تحقيق يصدره وكيل الجمهورية المختص[1]، أو بشكوى مصحوبة بادعاء مدني يتقدم بها المتضرر من الجناية أو الجنحة[2].

أما غرفة الاتهام فتمارس إجراءات التحقيق القضائي الابتدائي؛ بعد إخطارها من النائب العام، بخصوص الجنايات التي تسلم مستنداتها من قاضي التحقيق. أو للأسباب القانونية الأخرى، سيما المتصلة بإعادة تكييف الجريمة من الجنحة إلى الجناية، أو إعادة بعث التحقيق بعد صدور قرار بألا وجه للمتابعة، من منطلق الحصول على أدلة جديدة. كما يمكن للغرفة أن تراقب التحقيق القضائي الذي يقوم به قاضي التحقيق، بمناسبة طعن طرفي الدعوى العمومية؛ في الأوامر التي يصدرها، أو سكوته عن الفصل في الطلبات المتصلة بالإفراج والرقابة القضائية، أو الطعن الذي يقدمه الطرف المدني بخصوص الأوامر الماسة بحقوقه المدنية[3].

إلا أنه لا يمكن لجهاز التحقيق القضائي أن يمارس إجراءات التحقيق القضائي؛ إلا وفق قواعد اختصاص نوعي وإقليمي. فمن حيث الاختصاص النوعي نجد أن قضاء التحقيق عموما؛ يمارس إجراءات التحقيق في كل الجرائم المخطر بشأنها عبر الطرق المبينة سابقا وأعلاه. حيث كأصل عام يحقق قاضي التحقيق المتواجد على مستوى المحكمة وجوبا؛ في الجنايات ذات الصلة بدائرة اختصاصه، كما أنه قد يحقق في الجنح والمخالفات إذا ما طُلب منه ذلك[4].

لكن قيد المشرع قاضي التحقيق؛ بالعديد من القواعد، التي تجعله غير مختص بالنظر في الجريمة رغم توفر شروط اختصاصه الإقليمي. حيث قد لا يتم التحقيق فيها أصلا نظرا للحصانة التي يتمتع بها مرتكبها[5]، أو يحقق فيها من قضاة آخرون غير قاضي التحقيق المختص[6].

---

[1] حيث يطلب وكيل الجمهورية المختص من قاضي التحقيق؛ فتح تحقيق قضائي ابتدائي في وقائع معينة. على أن يختار بين قضاة التحقيق من يوجه له الطلب، في حالة وجود أكثر من واحد في المحكمة نفسها. الأمر الذي وان يبدوا على أنه يمس باستقلالية قاضي التحقيق في ممارسة مهامه؛ يجده الفقه الجنائي غير ذلك، نظرا لسحب صلاحية تنحية قاضي التحقيق عن القضية من وكيل الجمهورية ومنحها لغرفة الاتهام أو لرئيسها. **أنظر في ذلك:** المواد 67 و71 و191؛ أمر رقم 66-155، المرجع نفسه. **وأنظر أيضا:** عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، مرجع سابق، ص 335.

[2] **أنظر:** المادة 72؛ أمر رقم 66-155، المرجع نفسه.

[3] **أنظر:** المواد 166 و179 و180 و181 و170 و171 و172 و173؛ أمر رقم 66-155، المرجع نفسه. **وأنظر أيضا:** محمد حزيط، مذكرات في قانون الإجراءات الجزائية الجزائري، الطبعة السادسة، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2011، ص 183 و184.

[4] ورغم ذلك؛ لا يمكنه أن يباشر إجراءات التحقيق في الجريمة حتى وان كانت جناية متلبس بها؛ إلا بطلب افتتاح تحقيق يصدره وكيل الجمهورية المختص. **أنظر:** المادتان 66 و67؛ أمر رقم 66-155، المرجع نفسه.

[5] فلا يمكن التحقيق بدافع الحصانة الداخلية؛ مع نواب وأعضاء البرلمان. ولا مع من يتمتعون بالحصانة الدولية كرؤساء الدول والسفراء وأعضاء البعثات الدبلوماسية والعسكرية. **أنظر في ذلك:** 126 و127 و128؛ مرسوم رئاسي رقم 96-438، مرجع سابق.

[6] وضع المشرع إجراءات خاصة ببعض الفئات التي يتم التحقيق معها بمعرفة قاضي تحقيق غير المختص. على غرار رئيس الجمهورية، وأعضاء الحكومة والولاة، وقضاة المحكمة العليا ورؤساء المجالس القضائية والنواب العامون، =

وأما بخصوص الاختصاص الإقليمي لجهاز التحقيق القضائي؛ فنجد أن المشرع قد حدده أيضا كأصل واستثناء. فالأصل أن يمارس قاضي التحقيق؛ سلطاته وفق الأحكام المبينة سابقا بالاختصاص النوعي؛ على الجرائم المتصلة بدائرة اختصاصه الإقليمي، نظرا لكونها مكان ارتكاب الجريمة أو مكان إلقاء القبض على المتهم أو مكان إقامته[1].

لكن قد يتم تمديد الاختصاص الإقليمي لقاضي التحقيق، فيشمل دائرة اختصاص محاكم متاخمة للدائرة التي يباشر فيها مهامه، إذا ما استلزمت ضرورة التحقيق ذلك. كما يمدد الاختصاص الإقليمي أيضا؛ ليشمل دائرة اختصاص محاكم أخرى يحددها التنظيم، إذا ما تعلق الأمر بجرائم المعاملة الخاصة المبينة سابقا. وقد يصبح الاختصاص وطنيا، في حالة القيام بعمليتي التفتيش والحجز، بخصوص جرائم المعاملة الخاصة أيضا[2].

2. قواعد اختصاص جهاز قضاء التحقيق في إطار جرائم الوسط الرقمي: وفق الطريقة نفسها –تقريبا– المتصلة بجهاز النيابة العامة بخصوص مرحلة التحري؛ عالج القانون الجزائري قواعد الاختصاص النوعي والإقليمي، المباشر من خلالها جهاز قضاء التحقيق لإجراءات التحقيق القضائي الابتدائي. حيث ميز في الطرح بين؛ التحقيق في جرائم المساس بأنظمة المعالجة الآلية للمعطيات، والتحقيق في الجرائم التقليدية التي يكون النطاق الافتراضي للوسط الرقمي الوسيلة أو المسهل في عملية ارتكابها.

أ– قواعد اختصاص جهاز قضاء التحقيق في إطار جرائم المساس بأنظمة المعالجة الآلية للمعطيات: يختص قضاء التحقيق؛ بممارسة أعمال التحقيق القضائي الابتدائي؛ بخصوص كل جرائم المساس بأنظمة المعالجة الآلية للمعطيات المذكورة سابقا –التي تعد كلها جنح–. لكن بشرط أن يتم فتح تحقيق فيها وفق الطرق المبينة سابقا بخصوص وسائل اتصال قاضي التحقيق بالقضية، إما عن طريق طلب افتتاحي لإجراء تحقيق يصدره وكيل الجمهورية المختص، أو بواسطة الشكوى المصحوبة بالادعاء المدني. على أن يكون من الممكن قانونا متابعة مرتكب الجريمة قانونا، من حيث عدم تمتعه بالحصانة السابقة بالذكر. أو فرض القانون لضرورة التحقيق من قاضي التحقيق المختص، على حسب مركز مرتكب الأفعال.

أما بخصوص الاختصاص الإقليمي؛ فعالجه المشرع وفق الطرح نفسه المبين سابقا بخصوص جهاز النيابة العامة. حيث يتم التحقيق في جرائم المساس بأنظمة المعالجة الآلية للمعطيات حصرا؛ من قبل

= قضاة المجالس القضائية ورؤساء المحاكم ووكلاء الجمهورية، وقضاة المحاكم وضباط الشرطة القضائية، والأحداث، والعسكريون. **أنظر في ذلك:** المادة 177؛ مرسوم رئاسي رقم 96-438، المرجع نفسه. **وأنظر أيضا:** 573 و375 و377؛ أمر رقم 66-155، المرجع نفسه. **وأنظر كذلك:** 4/61؛ قانون رقم 15-12، مرجع سابق. **وأنظر:** المادة 75؛ أمر رقم 71-28، مرجع سابق.

[1] **أنظر:** المادة 40؛ أمر رقم 66-155، مرجع سابق.

[2] **أنظر:** المواد 57 و80 و2/40 و4/47؛ المرجع نفسه. **وأنظر أيضا:** عبد الله أوهابية، شرح قانون الإجراءات الجزائية الجزائري، مرجع سابق، ص 147 و148.

قاضي التحقيق الذي يمارس مهامه من خلال الأقطاب المتخصصة، الموزعة –كما بينا سابقا– في إطار أربعة 04 محاكم على المستوى الوطني، المنطوية على محكمة سيدي محمد بالجزائر العاصمة ومحكمة قسنطينة وحكمة ورقلة وحكمة وهران[1]. والذي يصبح اختصاصه وطنيا؛ إذا ما تعلق الأمر بعمليتي التفتيش والحجز بشأن الجرائم نفسها[2].

ب– **قواعد اختصاص جهاز قضاء التحقيق في إطار الجرائم التقليدية المتصلة بالوسط الرقمي:** يختص قضاء التحقيق أيضا –كأصل عام–؛ بالتحقيق في جميع الجرائم التقليدية التي ترتكب عبر النطاق الافتراضي للوسط الرقمي، أو يكون مسهلا لارتكابها. مع ضرورة إخطاره قانونا وفق الطرق المبينة سابقا، من منطلق عدم إمكانيته القيام بالتحقيق من تلقاء نفسه. إلا من حيث الاستثناءات السابقة بالذكر، سيما بخصوص المانع الإجرائي المنطوي على الحصانة، أو القيود الإجرائية المؤدية إلى التحقيق في الجريمة؛ من قاضي تحقيق مختص، على حسب صفة الشخص محل المتابعة الجنائية.

أما بخصوص الاختصاص الإقليمي؛ فيمكن أن نميز فيه بين العديد من الحالات الواردة بالنص الإجرائي المتصل بالجريمة التقليدية عموما. حيث الأصل العام يكون قاضي التحقيق؛ مختصا بالتحقيق في الجرائم التي ترتكب في دائرة اختصاصه أو يتم القبض على المتهم فيها أو يكون ساكنا في إطارها المكاني. على أن يتم تمديده إلى دائرة اختصاص المحاكم المتاخمة متى تطلبت ضرورة التحقيق ذلك[3].

وإذا ما اتصل التحقيق القضائي؛ بجرائم المعاملة الخاصة المنطوية على؛ جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف، التي ترتكب بواسطة النطاق الافتراضي للوسط الرقمي أو يكون المسهل لارتكابها. فيمدد الاختصاص الإقليمي لقاضي التحقيق؛ وفق فكرة الأقطاب المتخصصة. ووفق التوزيع نفسه المذكور سابقا بخصوص جرائم المساس بأنظمة المعالجة الآلية للمعطيات، الدائر بين محكمة سيدي محمد –الجزائر العاصمة– ومحكمة قسنطينة ومحكمة ورقلة ومحكمة وهران[4].

كما أنه يأخذ اختصاص قاضي التحقيق، المحقق في جرائم المعاملة الخاصة وفق الأقطاب المتخصصة المبينة أعلاه؛ الطابع الوطني إذا ما تعلق الأمر بعمليتي التفتيش والحجز، دون سواها من أعمال التحقيق عموما وأعمال جمع الدليل الرقمي خاصةً[5].

---

[1] **أنظر:** المواد 02 و03 و04 و05؛ مرسوم تنفيذي رقم 06-348، مرجع سابق.

[2] **أنظر:** المادة 3/47؛ أمر رقم 66-155، مرجع سابق.

[3] **أنظر:** المادتان 57 و80؛ المرجع نفسه.

[4] **أنظر:** المادة 2/40؛ المرجع نفسه. **وأنظر أيضا:** المواد 2 و3 و4 و5؛ مرسوم تنفيذي رقم 06-348، المرجع نفسه.

[5] **أنظر:** المادة 3/47؛ أمر رقم 66-155، المرجع نفسه.

الفرع الثاني: الأجهزة الشرطية المباشرة للتحري والتحقيق في جرائم الوسط الرقمي

لا يمكن من حيث الواقع والقانون، للأجهزة القضائية المبينة سابقا –جهازي النيابة العامة والتحقيق القضائي–؛ القيام بممارسة الأعمال الإجرائية ذات الصلة بالتحري والتحقيق، سيما المتصلة بجرائم الوسط الرقمي منها. حيث لابد من ذراع قانونية تمتد لتغطي العمل الإجرائي، كما يحدده القانون ويريده رجال القضاء في إطار التحري والتحقيق. الأمر المنطوي أساسا على جهاز شبه قضائي، يدعى قانونا بالشرطة القضائية[1].

فتمارس الشرطة القضائية مهام التحري تحت إشراف وإدارة جهاز النيابة العامة، وبمراقبة غرفة الاتهام. كما أنها تنفذ تفويضات جهاز التحقيق القضائي الابتدائي؛ في إطار ممارستها لأعمال التحقيق[2]. وعلى العموم تختلف الأجهزة الشرطية الممارسة لأعمال التحري والتحقيق، في جرائم الوسط الرقمي؛ بين الأجهزة العامة(أولا) والخاصة(ثانيا).

أولا: الجهاز الشرطي العام المباشر للتحري والتحقيق في جرائم الوسط الرقمي

تعد الشرطة القضائية وفق المادتان 12 و13 "ق.إ.ج" سابقتي الذكر؛ الجهاز الأساسي المختص بممارسة أعمال مرحلة التحري، ولو أنه يمارسها بإدارة وإشراف النيابة العامة. كما أنه يعد بمثابة الجهاز المعتمد عليه غالبا من قبل قضاء التحقيق؛ لممارسة أعمال التحقيق وفق ما بينا أعلاه. والشرطة القضائية وفق الطرح نفسه؛ نظمها المشرع الجزائري بالعديد من النصوص التي يمكن من خلالها الوصول إلى أحكامها العامة، وتبيان قواعد اختصاصها النوعي والإقليمي.

1. الأحكام العامة للجهاز الشرطي العام: تختلف وتتعدد التعاريف القانونية المسندة إلى جهاز الشرطة القضائية. وان كان تصب أغلبها –إن لم نقل جلها– في قالب الجهاز شبه القضائي، الذي يمارس أعمال التحري قبل تحريك الدعوى العمومية وبإدارة وكيل الجمهورية. مع التجاوز عند التعريف الإشارة إلى أعمال التحقيق التي ينجزها؛ في إطار الندب القضائي من قاضي التحقيق المختص[3]. وعلى العموم يمكن أن نعرف جهاز الشرطة القضائية؛ على أنه: "جهاز شبه قضائي يقوم بممارسة أعمال التحري تحت إدارة جهاز النيابة العامة، وأعمال التحقيق القضائي في إطار الانتداب تحت إدارة جهاز قضاء التحقيق".

---

[1] التي أصبح يطلق عليها المشرع تسمية الشرطة القضائية؛ بموجب تعديل "ق.إ.ج" الوارد سنة 2017. بعد أن كان يسميها بالضبطية القضائية. **أنظر في ذلك:** المادة 12 المعدلة بالمادة 04؛ قانون رقم 17-07، مؤرخ في 27 مارس 2017، يعدل ويتمم أمر رقم 66-155، يتضمن قانون الإجراءات الجزائية، (ج ر) عدد 20، صادر بتاريخ 29 مارس 2017.

[2] **أنظر:** المادتان 12 و13؛ أمر رقم 66-155، مرجع سابق.

[3] وعلى العموم يتم تعريف جهاز الشرطة القضائية في إطار مرحلة التحري؛ على أنه: "جهاز يضبط الوقائع التي يضع لها القانون جزاء عقابي، ويبحث عن الجرائم بعد وقوعها ويلاحق المشتبه فيه ليكشف ملابسات الجريمة الواقعة". **أنظر في ذلك:** فضيل العيش، مرجع سابق، ص 92.

قسم المشرع الجزائري الشرطة القضائية في إطار تحديد تشكيلتها؛ إلى ثلاثة أقسام بحسب معيار المنصب الأصلي والمهام الشرطية في إطار التحري والتحقيق. حيث تتكون الشرطة القضائية على سبيل الحصر من ضباط الشرطة القضائية، وأعوان الضبط القضائي، والموظفين والأعوان المنوط بهم قانونا بعض مهام الضبط القضائي بالنص العام أو الخاص[1]. فحددت المادة 15 "ق.إ.ج" المعدلة سنة 2015 على سبيل الحصر؛ الأشخاص الذين لهم أو يمكن لهم أن يحملوا صفة ضابط الشرطة القضائية[2]. والمنطوون على رئيس المجلس الشعبي البلدي، الذي يحمل الصفة بقوة القانون. وآخرون يحملونها بعد تأهيلهم بموجب مقرر يصدر عن النائب العام المختص بعد اقتراح تقدمه السلطة الإدارية المعنية على حسب الحالة[3]، وهم ضباط الدرك الوطني، والموظفين التابعين للأسلاك الخاصة للمراقبين، ومحافظي وضباط الأمن الوطني.

كما يمكن أن يحمل آخرون صفة ضابط الشرطة القضائية بعد التأهيل المذكور، على أن تتوفر فيهم شروط إدارية معينة، تختلف بحسب الصفة والانتماء الإداري السابق. والمحددين في من يثبتون ثلاث سنوات على الأقل؛ بصفات ذوي الرتب ورجال الدرك الوطني والمفتشين وحفاظ والأعوان التابعين للأمن الوطني، المعينون بعد موافقة لجنة خاصة؛ بموجب قرار مشترك صادر عن وزير العدل ووزير الدفاع الوطني أو الداخلية على حسب الحالة –مع التأكيد على ضرورة صدور مقرر تأهيل عن النائب العام المختص قبل البدء في ممارسة المهام–[4]. وبالإضافة إلى ما ذكر؛ يمكن للضباط وضباط الصف المنتمين إلى المصالح العسكرية للأمن حمل الصفة نفسها؛ بعد صدور قرار التعيين عن وزير الدفاع الوطني ووزير العدل، وتأهيلهم من النائب العام المختص[5].

---

[1] **أنظر:** المادة 14؛ أمر رقم 66-155؛ مرجع سابق.

[2] **أنظر:** المادة 15 المعدلة بالمادة 04؛ أمر رقم 15-02، مرجع سابق.

[3] وهو الأمر المستجد بالتعديل الوارد سنة 2017. حيث باستثناء رؤساء البلديات؛ لايمكن للأشخاص المذكورين في المادة 15 الموضحة أعلاه رغم حملهم للصفات الإدارية المطلوبة؛ أن يمارسوا مهام الشرطة القضائية، إلا بعد تأهيلهم من النائب العام المختص، والذي يمكنه أن يسحبهم الصفة وفق أحكام معينة. **أنظر في ذلك:** المادتان 15 مكرر1 و15 مكرر2 المضافتان بالمادة 05؛ قانون رقم 17-07، مرجع سابق.

وهو الأمر الذي لنا فيه قول. فمن حيث استثناء رؤساء البلديات من التأهيل المطلوب؛ وبدراسة ذاتية نستطيع القول أنه استثناء قائم على احترام الإرادة الشعبية. فرئيس المجلس الشعبي البلدي؛ اكتسب الصفة الإدارية والشرطية انطلاقا من الانتخاب الشعبي وليس بالتعيين الإداري السلمي. وأما من حيث التـأهيل وسحبه –في إطاره المذكور أعله فقط-؛ فهو بمثابة التكريس الإجرائي لما جاء في المادة 2/12 "ق.إ.ج" المذكورة أعلاه، عن طريق إعمال الرقابة القبلية والبعدية.

[4] يلاحظ عما ذكر أعلاه؛ أن المشرع بإضافته لشرط التأهيل؛ يكون قد منع الأشخاص المذكورين من ممارسة صفة ضابط الشرطة القضائية إلا بعد التأهيل الصادر عن النائب العام. وهذا رغم اعتبار وزير العدل طرفا في قرار التعيين. وبالرجوع إلى التعديل الوارد سنة 2015؛ نجده قد تمم المادة 33 من القانون نفسه؛ ليعتبر النائب العام المنفذ للسياسة الجزائية التي يعدها وزير العدل. وعليه نتساءل؛ ألا يعد امتناع النائب العام عن تأهيل من عينهم وزير العدل؛ بمثابة تعطيل للسياسة الجنائية المعتمدة من الوزير نفسه؟؟؟. **أنظر في ذلك:** الفقرة 3 من المادة 33 المضافة بالمادة 04؛ أمر رقم 15-02، المرجع نفسه.

[5] ولو أنه بخصوص المنتمين إلى المصالح العسكرية للأمن؛ يكون النائب العام لمجلس قضاء الجزائر العاصمة الوحيد الذي له الحق في منحهم التأهيل المذكور. **أنظر في ذلك:** المادة 15 مكرر1/1 المضافة بالمادة 05؛ قانون رقم 17-07، المرجع نفسه.

وأما بخصوص أعوان الضبط القضائي؛ فحددهم المشرع في من ينتمون إلى الجهات الأمنية والعسكرية الثلاث المذكورة أعلاه، ولا يكتسبون صفة ضباط الشرطة القضائية. والمنطوون على؛ موظفي مصالح الشرطة، وذوي الرتب في الدرك الوطني ورجال الدرك ومستخدمي مصالح الأمن العسكري[1]. على أنه قد نجد بعض النصوص الخاصة التي تضفي الصفة نفسها؛ على طوائف أخرى، سيما اكتساب أعضاء الحرس البلدي لصفة أعوان الضبط القضائي[2].

كما أقر "ق.إ.ج"؛ بحمل الولاة وأعوان الغابات لصفة الضبط القضائي، وبإمكانية حمل الصفة نفسها من بعض الموظفين والأعوان العموميون، إذا منحتهم القوانين الخاصة ذلك[3]. وعلى حسب الدراسات الفقهية السابقة؛ تتعدد وتتنوع القوانين الخاصة المانحة لصفة الضبط القضائي لبعض الموظفين والأعوان. على غرار أعوان الجمارك، ومفتشي العمل، وشرطة المياه، وأعوان الصحة النباتية...الخ[4].

إلا أنه لا يمكن أن تمارس الشرطة القضائية الأعمال الإجرائية التالية بالدراسة؛ إلا في إطار قانوني محدد نوعيا وإقليميا. فمن حيث الاختصاص النوعي وكأصل عام؛ تختص الشرطة القضائية حسب أحكام المادتان 12 و13 "ق.إ.ج" –سابقتا الذكر–؛ بالتحري عن كل الأفعال المجرمة قبل تحريك الدعوى العمومية، وبمساعدة قضاء التحقيق على انجاز أعمال التحقيق بعد تحريكها. على أن تراعى بعض الاستثناءات التي وضعها المشرع، ليقيد اختصاصات بعض الجهات في جرائم محددة حصرا و/أو بشروط واجبة الإتباع. سيما ما جاء به في إطار القانون نفسه لسنة 2017، الذي حصر مهام الضبط القضائي التابع للأمن العسكري؛ في التحري والتحقيق عن الجرائم الماسة بأمن الدولة فقط[5].

كما يحدد الاختصاص الإقليمي للشرطة القضائية، بحسب الضوابط المقررة لاختصاص وكيل الجمهورية وقاضي التحقيق، والمنطوي على إما مكان ارتكاب الجريمة أو محل إقامة المشتبه فيه أو مكان القبض عليه[6]. ومنه قد يكون الاختصاص محليا كأصل عام، فيحدد بالنطاق الذي يباشر فيه الضابط

---

[1] **أنظر:** المادة 19؛ أمر رقم 66-155، مرجع سابق.

[2] **أنظر:** المادة رقم 06؛ مرسوم تنفيذي رقم 96-265، مؤرخ في 03 أوت 1996، يتضمن إنشاء سلك الحرس البلدي ويحدد مهامه وتنظيمه، (ج ر) عدد 47، صادر بتاريخ 07 أوت 1996.

[3] **أنظر:** المواد 21 و27 و28؛ أمر رقم 66-155، المرجع نفسه.

[4] **أنظر:** محمد حزيط، مرجع سابق، ص 53. **وأنظر أيضا:** ناصر حمودي، (قانون الإجراءات الجزائية الجزائري)، مرجع سابق، ص ص 78-80.

[5] **أنظر:** المادة 15 مكرر المضافة بالمادة 05؛ قانون رقم 17-07، مرجع سابق.

وهو الأمر المطبق أيضا على اختصاص الولاة، بشرط الاستعجال واحترام الإجراءات الأخرى. كما يعد من المنطقي ألا يختص الموظفون والأعوان المنظمة مهامهم بقوانين خاصة بالتحري دون التحقيق؛ إلا في الجرائم التابعة لمجالهم المبين بالقوانين نفسها. **أنظر في ذلك:** ناصر حمودي، (قانون الإجراءات الجزائية الجزائري)، المرجع نفسه، ص 76 و77 و92.

[6] **أنظر:** المواد 1/37 و1/40 و13؛ أمر رقم 66-155، مرجع سابق. **وأنظر أيضا:** جمال نجيمي، قانون الإجراءات الجزائية الجزائري على ضوء الاجتهاد القضائي، الطبعة الأولى، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2015، ص 88.

أو العون نشاطه العادي باعتباره عضوا في جهة معينة. مع إمكانية تمديده ليشمل كافة دوائر اختصاص المجلس القضائي في حالة الاستعجال وخشية ضياع الدليل، أو ليصبح وطنيا تنفيذا لأمر أحد رجال القضاء المستعجل. ويمكن كاستثناء أن يكون الاختصاص وطنيا بالأساس، إما بالنظر إلى طبيعة الجهاز، على غرار ما تتمتع به الشرطة القضائية التابعة للأمن العسكري من اختصاص مكاني يشمل كل التراب الوطني. أو من منطلق طبيعة الجرائم محل التحري والتحقيق، سيما ما يتعلق بجرائم المعاملة الخاصة. مع مراعاة التبعية في الاختصاص المحلي، على حسب قواعده المتصلة بجهازي النيابة والتحقيق[1].

2. قواعد اختصاص الجهاز الشرطي العام في إطار جرائم الوسط الرقمي: عالج القانون الجزائري قواعد اختصاص الشرطة القضائية؛ وفق الطريقة نفسها المعمول بها في إطار جهازي النيابة العامة وقضاء التحقيق. إلا من حيث ضرورة التفرقة بين التحري والتحقيق. الأمر الذي نبينه من خلال التطرق إلى قواعد الاختصاص في جرائم المساس بأنظمة المعالجة الآلية للمعطيات، والجرائم التقليدية التي يكون النطاق الافتراضي للوسط الرقمي وسيلتها أو المسهل لارتكابها.

أ- قواعد اختصاص الجهاز الشرطي العام في إطار جرائم المساس بأنظمة المعالجة الآلية للمعطيات: رجوعا إلى القاعدة العامة المنطوية على تبعية الشرطة القضائية، من حيث ممارسة أعمال التحري والتحقيق لجهازي النيابة العامة والتحقيق القضائي –المادتان 12 و13 "ق.إ.ج" سابقتا الذكر–؛ نستطيع القول أنها –الشرطة القضائية– تختص نوعيا بالتحري والتحقيق في كل جرائم المساس بأنظمة المعالجة الآلية للمعطيات، ماعدا تلك المستثنات في إطار عمل وكيل الجمهورية وقاضي التحقيق[2].

وكذلك بخصوص الاختصاص الإقليمي للشرطة القضائية، الذي يتبع الاختصاص الإقليمي نفسه المبين سابقا بالنسبة لوكيل الجمهورية وقاضي التحقيق. فباعتبار جرائم المساس بأنظمة المعالجة الآلية للمعطيات، من الجرائم ذات المعاملة الخاصة؛ تصبح الشرطة القضائية المختصة بالتحري والتحقيق هي التابعة لوكيل الجمهورية وقاضي التحقيق الموجودين على مستوى الأقطاب المتخصصة المذكورة سابقا، والمنطوية على محكمة سيدي محمد بالجزائر العاصمة ومحكمة قسنطينة ومحكمة ورقلة ومحكمة وهران. ولو أن المشرع أكد في إطار مرحلة التحري على الاختصاص نفسه؛ بنص متصل بالضبطية القضائية، وبشكل منفصل عن قواعد الاختصاص الإقليمي لوكيل الجمهورية[3]. هذا مع التأكيد على امتداد الاختصاص في إطار تنفيذ أوامر القاضي المختص؛ للقيام بعمليتي التفتيش والعجز ليصبح وطنيا[4].

---

[1] **أنظر:** المادة 16؛ أمر رقم 66-155، مرجع سابق. **وأنظر أيضا:** فضيل العيش، مرجع سابق، ص 98 و99.

[2] وهي المنطوية –كما ذكرنا سابقا-؛ على عدم إمكانية التحري في جرائم المساس ذات الوصف العسكري، أو الخيانة العظمى المرتكبة من قبل رئيس الجمهورية، والجنايات والجنح المرتكبة من الوزير الأول أثناء تأدية المهام. وعدم إمكانية التحقيق مع من يمتازون بالحصانة الوطنية والدولية.

[3] **أنظر:** المادة 7/16؛ أمر رقم 66-155، المرجع نفسه.

[4] **أنظر:** المادتان 3/16 و4/47؛ المرجع نفسه.

ب- **قواعد اختصاص الجهاز الشرطي العام في إطار الجرائم التقليدية المتصلة بالوسط الرقمي:** يختص جهاز الشرطة القضائية بتشكيلته التقليدية المعروفة؛ بالتحري والتحقيق -كأصل عام- في كل الجرائم التقليدية المرتكبة عبر النطاق الافتراضي للوسط الرقمي، أو التي يكون مسهلا لارتكابها. إلا من حيث الاستثناءات الواردة على عمل جهازي النيابة العامة وقضاء التحقيق، في إطار أعمال التحري والتحقيق. حيث لا يمكن تصور قيام الشرطة القضائية العادية بالتحري في الجرائم العسكرية أو المتصلة بالخيانة العظمى المرتكبة من رئيس الجمهورية أو الجنايات والجنح المرتكبة من الوزير الأول. كما لا يمكن لها أن تحقق مع من هم تحت حماية الحصانة الوطنية والدولية، أو من يخضعون لإجراءات تحقيق خاصة انطلاقا من صفتهم أو مركزهم[1].

أما بخصوص قواعد الاختصاص الإقليمي، التي تمارس من خلالها الشرطة القضائية التقليدية التحري والتحقيق في الجرائم التقليدية المتصلة بالوسط الرقمي؛ فوزعها المشرع بين العديد من الحالات الداخلة في الإطار العام المتصل باختصاص جهازي النيابة العامة وقضاء التحقيق. حيث يحدد النطاق الإقليمي كأصل عام بمكان ارتكاب الجريمة أو مكان إلقاء القبض على المشتبه فيه أو المتهم أو مكان إقامته[2].

لكن يجب أن نفرق بين التحري والتحقيق؛ في العديد من الحالات الخارجة عن الأصل المذكور أعلاه، سيما في إطار تمديد الاختصاص المحلي. حيث يمتد اختصاص جهاز الشرطة القضائية للقيام بأعمال التحري المستعجلة إلى كل إقليم دائرة مجلس القضاء التابع له. كما يصبح الاختصاص وطنيا في حال اتصل التحري بجريمة من جرائم المعاملة الخاصة المرتكبة أو المسهل ارتكابها عبر الوسط الرقمي، مع التأكيد على أن الجهاز الممدد اختصاصه في هذه الحالة؛ هو التابع للقطب المختص على حسب الحالة وكما بينا سابقا[3].

وأما بخصوص القيام بأعمال التحقيق، انطلاقا من تنفيذ تفويضات قاضي التحقيق المختص في إطار الندب القضائي؛ فيمتد اختصاص جهاز الشرطة القضائية للقيام بأعمال التحقيق المستعجلة، إلى دائرة اختصاص المحاكم المتاخمة لمقر ممارسة المهام. كما قد يمتد الاختصاص ليتصل بالأقطاب المتخصصة؛ إذا ما تعلق الأمر بجرائم المعاملة الخاصة، وفق الطرح نفسه المذكور أعلاه. ويصبح وطنيا في حال تعلق الآمر بإجرائي التفتيش والحجز بخصوص جرائم المعاملة الخاصة نفسها[4].

---

[1] على العموم يتم تطبيق الأحكام العامة المذكورة سابقا؛ في إطار قواعد اختصاص جهازي النيابة العامة وقضاء التحقيق.

[2] **أنظر:** المادتان 1/37 و1/40؛ أمر رقم 66-155، مرجع سابق.

[3] **أنظر:** المواد 2/16 و1/57 و2/37 و7/16؛ المرجع نفسه. **وأنظر أيضا:** المواد 02 و03 و04 و05؛ مرسوم تنفيذي رقم 06-348، مرجع سابق.

[4] **أنظر:** المواد 1/57 و2/40 و4/47؛ أمر رقم 66-155، المرجع نفسه. **وأنظر أيضا:** المواد 02 و03 و04 و05؛ مرسوم تنفيذي رقم 06-348، المرجع نفسه.

ثانيا: الأجهزة الشرطية الخاصة المباشرة للتحري والتحقيق في جرائم الوسط الرقمي

إيمانا من السلطتين التشريعية والتنفيذية في الجزائر، بعجز الجهاز التقليدي للشرطة القضائية في مواجهة المسرح الجرمي الافتراضي؛ تم العمل على استحداث العديد من الأجهزة الشرطية الخاصة، في إطار كل من الأمن والدرك الوطنيين، مع ممارسة التحري والتحقيق ذاته؛ من الجهاز الخاص بالشرطة القضائية التابع للأمن العسكري في حدود ضيقة. الأمر الذي نبينه من خلال التطرق إلى هذه الأجهزة المختصة، سواءً تلك التابعة للأمن الوطني، أو الدرك الوطني، أو المصالح العسكرية للأمن.

1. الأجهزة الشرطية الخاصة التابعة للأمن الوطني: في إطار التجديد الواجب لأجهزة الشرطة القضائية المواجهة لجرائم الوسط الرقمي؛ عملت المديرية العامة للأمن الوطني على إعادة الهيكلة، بحيث أوجدت أجهزة متخصصة في التحري والتحقيق الرقميين. الأمر الذي ينقسم فعليا إلى جهاز وطني، منطوي على المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وأجهزة غير مركزية متعددة.

أ- المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: بحلول سنة 2011 استحدثت المديرية العامة للأمن الوطني؛ أول فصيلة تعنى بمحاربة جرائم الوسط الرقمي. الفصيلة التي لم تعمر طويلا، حيث تحولت بعد ذلك إلى مصلحة مركزية تحت تسمية؛ المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، المستحدثة بقرار صادر عن المدير العام للأمن الوطني، وأضيفت فعلا إلى الهيكل التنظيمي لمديرية الشرطة القضائية في شهر جانفي 2015[1]. وتتكون هذه المصلحة؛ من العديد من الفصائل التي تختلف بحسب نوع جرائم الوسط الرقمي محل الاختصاص. فمنها مثلا فصيلة مكافحة الإرهاب الرقمي، والفصيلة المختصة بالأحداث، وفصيلة اليقضة الالكترونية[2].

رغم ورود مصطلح المحاربة في تسمية المصلحة؛ إلا أنها تختص إلى جانب المحاربة بالوقاية والتكوين[3]. ففي إطار المواجهة؛ عملت على الممارسة العملية للتحري والتحقيق في جرائم الوسط الرقمي. ومن ثم تحولت إلى العمل الإداري المحض، عن طريق الإدارة والإشراف على الأجهزة غير المركزية المختصة بالتحري والتحقيق العملي. وعلى العموم؛ عالجت هذه الأجهزة الشرطية المختصة بمواجهة جرائم الوسط الرقمي؛ ما يعادل 1066 قضية سنة 2016، و2130 قضية سنة 2017[4].

---

[1] **أنظر:** مصطفاوي عبد القادر- رئيس المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، "جهود استباقية للأمن الوطني لتحقيق الأمن المعلوماتي والامتياز في الأداء"، مجلة الشرطة، المديرية العامة للأمن الوطني، الجزائر، عدد 129، ديسمبر 2015، ص 142.

[2] مقابلة مع ممثل فرقة مكافحة الجرائم المعلوماتية التابعة للأمن الوطني، "معلومات حول الأجهزة الشرطية المختصة في مكافحة جرائم الوسط الرقمي"، المصلحة الولائية للشرطة القضائية، البويرة، الجزائر، 18 أفريل 2018.

[3] **أنظر:** مصطفاوي عبد القادر، المرجع والصفحة نفسهما.

[4] مقابلة مع ممثل فرقة مكافحة الجرائم المعلوماتية التابعة للأمن الوطني، المرجع نفسه.

ب- الأجهزة الشرطية غير المركزية المختصة بمكافحة جرائم الوسط الرقمي: بعد تحول المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال؛ من الطبيعة العملية إلى الإدارية، وزيادة حجم الإجرام الرقمي على المستوى الوطني؛ أصبح من الضروري إنشاء أجهزة شرطية جهوية ومحلية، تمارس التحري والتحقيق في هذا الشأن، تحت إشراف وإدارة المصلحة المركزية[1].

في السياق نفسه؛ نجد أن المديرية العامة للأمن الوطني، قد استحدثت بواسطة المديرية المركزية للشرطة القضائية؛ 48 فصيلة محلية –فصيلة على مستوى كل ولاية- تحت تسمية فصيلة مكافحة الجرائم المعلوماتية[2]. التي تعمل بالتنسيق مع المصالح الجهوية للبحث والوقاية، المتصلة بمناطق الوسط والغرب والشرق والجنوب الشرقي والجنوب الغربي. كما أنها قد تتعامل مع المصالح الولائية للاستعلامات العامة، التي تختص باليقضة الالكترونية دون سواها[3].

إلا أن الاكتفاء بفصيلة واحدة على مستوى الولاية؛ يجعل من الشرطة القضائية التقليدية هي المختصة بالتحري والتحقيق في جرائم الوسط الرقمي، على حسب قواعد اختصاصها المذكورة سابقا، مع ضرورة إعلام الفصيلة المحلية التي تخبر بدورها المصلحة المركزية. وفي حالة مواجهتها بعض الصعاب الإجرائية، تقوم بطلب يد المساعدة من الفصيلة. وعلى العموم؛ تختص الفصيلة المحلية بالتحري والتحقيق في جميع جرائم الوسط الرقمي إلا ما استثنيت بنص صريح، وذلك بالإضافة إلى أنها تختص بممارسة مهام اليقضة الالكترونية، إلى جانب المصالح الولائية للاستعلامات صاحبة الاختصاص الأصيل[4].

2. الأجهزة الشرطية الخاصة التابعة للدرك الوطني: وفق الطريقة نفسها المتصلة بالأمن الوطني تقريبا، عملت قيادة الدرك الوطني؛ على إيجاد أجهز شرطية خاصة تهتم بمباشرة التحري والتحقيق في جرائم الوسط الرقمي، تحت إدارة جهازي النيابة العامة أو قضاء التحقيق. وهي المنطوية أساسا على الأجهزة المركزية والأجهزة غير المركزية.

أ- الأجهزة الشرطية المركزية المختصة بمكافحة جرائم الوسط الرقمي: تختلف وتتعدد الأجهزة الشرطية المركزية التابعة للدرك الوطني. التي عملت الجهات المعنية في إطار مواجهة العجز الإجرائي الرقمي؛ على تدعيمها بمكتب مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وإنشاء مركز الوقاية من جرائم الإعلام والجرائم المعلوماتية ومكافحتها.

---

[1] مقابلة مع ممثل فرقة مكافحة الجرائم المعلوماتية التابعة للأمن الوطني، مرجع سابق. **وأنظر:** مصطفاوي عبد القادر، مرجع سابق، ص 142.

[2] مقابلة مع ممثل فرقة مكافحة الجرائم المعلوماتية التابعة للأمن الوطني، المرجع نفسه. **وأنظر:** مصطفاوي عبد القادر، المرجع والصفحة نفسهما.

[3] مقابلة مع ممثل فرقة مكافحة الجرائم المعلوماتية التابعة للأمن الوطني، المرجع نفسه.

[4] المرجع نفسه.

أ-1/ مكتب مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: يتصل المكتب، من حيث الإنشاء والتبعية القانونية والهيكلية؛ بالمصلحة المركزية للتحريات الجنائية، التي تهتم بالإسناد العملياتي إلى جانب قسم التوثيق القضائي وفصيلة السينوتقنية والتحليل الإجرامي. حيث يتشكل المكتب هو الآخر من ثلاثة فصائل، المنطوية على فصيلة المساس بالمنظومة الآلية للمعطيات، وفصيلة الإسناد التقني والتنسيق والوثائق العملياتية، وفصيلة الجرائم المرتكبة بوسائل تكنولوجيات الإعلام والاتصال[1].

ويختص مكتب مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال؛ بالعديد من المهام ذات الصلة بالتحري والتحقيق في جرائم الوسط الرقمي. سيما متابعة وتوجيه نشاطات الوحدات المختصة بمكافحة جرائم الوسط الرقمي، والعمل بالتنسيق مع مركز الوقاية ومكافحة جرائم الإعلام الآلي والمعلوماتية للكشف عن مختلف الجرائم، وتحرير طلبات المساعدة والتسخيرات لمختلف الجهات المعنية، ولفت نظر الوحدات الإقليمية للاهتمام بجرائم الوسط الرقمي[2].

أ-2/ مركز الوقاية من جرائم الإعلام والجرائم المعلوماتية ومكافحتها: يعد المركز من أهم الأجهزة الشرطية محل الدراسة. نظرا لامتلاكه الوسائل التقنية والقدرة البشرية على الوقاية من جرائم الوسط الرقمي ومكافحتها. حيث عالج الكثير من الجرائم منذ إنشائه، التي بحسب التقارير الصادرة عنه؛ بلغت حد 538 قضية سنة 2016، و905 قضية سنة 2017[3].

يتكون المركز من ثلاثة مكاتب ومصلحتين. المتمثلة في مكتب التحقيقات المعلوماتية، ومكتب اليقظة المعلوماتية، ومكتب الأمن الرقمي. والمصلحة التقنية والاستغلال، ومصلحة الإدارة والوسائل. وعلى العموم يختص المركز؛ بالتحري والتحقيق في جرائم الوسط الرقمي، عن طريق المساعدة في الوقاية وإجراء الخبرات، وضمان يقظة ومتابعة وتقييم الوضعية العامة للتهديدات الرقمية. كما يختص أيضا بإعداد وتفعيل الإستراتيجية الرقمية، ومتابعة قواعد أمن المعلومات وأنظمتها وتقييمها، والمساهمة في تقوية أمن الأنظمة الوطنية، وإنشاء علاقات تنسيق وتعاون مع الفاعلين في الوسط الرقمي[4].

---

[1] **أنظر:** مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها للدرك الوطني، "الجريمة المعلوماتية ودور الدرك الوطني"، الجزائر، د ت، ص 20 و21.

[2] **أنظر:** المرجع نفسه، ص 21.

[3] الموزعة بين جرائم المساس بالحياة الخاصة، وتلك المتعلقة بالتسريب والنشر الرقميين لأسئلة شهادتي البكالوريا والتعليم المتوسط لسنتي 2016 و2017، والإرهاب، وجرائم المساس بأنظمة المعالجة الآلية للمعطيات، والمساس بالنظام العام، وغيرها. **أنظر في ذلك:**

- Centre de Prévention et de lutte Contre la Criminalité Informatique et la Cybercriminalité de la Gendarmerie Nationale, "Bilan d'activité du Centre Au titre de l'année 2016", Algérie, s d, p 01. **ET:** Centre de Prévention et de lutte Contre la Criminalité Informatique et la Cybercriminalité de la Gendarmerie Nationale, "Bilan d'activité du Centre Au titre de l'année 2017", Algérie, s d, p 02.

[4] **أنظر:** مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها للدرك الوطني، "الجريمة المعلوماتية ودور الدرك الوطني"، المرجع نفسه، ص 23.

ب- الأجهزة غير المركزية المختصة بمكافحة جرائم الوسط الرقمي: بالإضافة إلى الأجهزة الشرطية المركزية، نجد أن التحري والتحقيق في جرائم الوسط الرقمي؛ ينجز أيضا من قبل أجهزة شرطية ذات بعد غير مركزي. وهي المنطوية على فصائل الأبحاث وفرق الأبحاث والفرق الإقليمية. حيث لها البعد العملياتي وتسمى بالتشكيلات المكلفة بالتحقيق القضائي. التي تعد تقليدية من حيث التكوين والمهام العامة، إلا أنها تعمل في إطار اختصاصها النوعي والإقليمي؛ بالتنسيق مع الأجهزة المركزية المذكورة[1].

وفي إطار متصل، أشرف مركز الوقاية من جرائم الإعلام والجرائم المعلوماتية ومكافحتها؛ على العديد من أعمال التحري التي مارستها الفرق وفصائل الأبحاث. على غرار تلك المنجزة من فرقة البحث للدرك الوطني ببئر مراد رايس الجزائر العاصمة سنة 2013، بخصوص النصب الاحتيال عبر الشبكة. كما تم الإشراف أيضا على التحري المنجز من قبل فصيلة الأبحاث للدرك الوطني بالجزائر العاصمة سنة 2017، بخصوص القرصنة المعلوماتية المكيفة على أنها مساس بأنظمة المعالجة الآلية للمعطيات[2].

3. الجهاز الشرطي الخاص التابع للمصالح العسكرية للأمن: لم يستقر القانون الجزائري عموما؛ على نظام معين يخص به المصالح العسكرية للأمن. حيث عرفت هذه المصالح منذ أول إنشاء لها سنة 1982؛ العديد من التغيرات والتطورات على حسب الحاجة القانونية والواقعية لذلك، سيما لمواكبة التطور الحاصل بخصوص النطاق الافتراضي للوسط الرقمي والجرائم ذات الصلة. الأمر الذي نبينه من خلال التطرق إلى الأحكام العامة لجهاز شرطة المصالح العسكرية للأمن، وقواعد اختصاصه بالنظر إلى جرائم الوسط الرقمي.

أ- الأحكام العامة لجهاز شرطة المصالح العسكرية للأمن: لم يتطرق قانون الإجراءات الجزائية الصادر سنة 1966؛ إلى منح صفة الشرطة القضائية للمصالح العسكرية للأمن. واستقر على ذلك رغم تعديله سنتي 1968 و1982 للمادة 15 "ق.إ.ج" المبينة لضباط الشرطة القضائية، ورغم استحداث التنظيم سنة 1982 بموجب مرسوم؛ لما سماها بالمديرية العسكرية للأمن العسكري. الأمر الذي تداركه المشرع سنة 1985 بتعديله للمادة 15 نفسها؛ فمنح الصفة للضباط وضباط الصف التابعين للأمن العسكري[3].

---

[1] **أنظر:** مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها للدرك الوطني، "الجريمة المعلوماتية ودور الدرك الوطني"، مرجع سابق، ص 20. **وأنظر أيضا:**

- Centre de Prévention et de lutte Contre la Criminalité Informatique et la Cybercriminalité de la Gendarmerie Nationale, "Bilan d'activité du Centre Au titre de l'année 2016, op.cit, p 01.

[2] **أنظر:** مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها للدرك الوطني، "حالات ملموسة"، الجزائر، د ت، ص 2-4 و8-12.

[3] **أنظر:** المادة 15؛ أمر رقم 66-155، مرجع سابق. **معدلة** بالأمر رقم 68-10، مؤرخ في 23 جانفي 1968، (ج ر) عدد 09، صادر بتاريخ 30 جانفي 1968. وبالقانون رقم 82-03، مؤرخ في 13 فيفري 1982، (ج ر) عدد 07، صادر بتاريخ 16 فيفري 1982. وبالقانون رقم 85-02، مؤرخ في 26 جانفي 1985، (ج ر) عدد 05، صادر بتاريخ 27 جانفي 1985 **وأنظر أيضا:** مرسوم رقم 82-368، مؤرخ في 20 نوفمبر 1982، يتضمن مهام المديرية العسكرية للأمن العسكري، (ج ر) عدد 48، صادر بتاريخ 30 نوفمبر 1982.

إلا أن القانون الجزائري –تشريع وتنظيم– الذي رغم استقراره من حيث منح صفة الضبطية القضائية المذكورة؛ أدخل عليها العديد من التعديلات المتتالية. التي بدأها المشرع سنة 1995 بتغيير التسمية؛ من مصالح الأمن العسكري إلى المصالح العسكرية للأمن. كما حاول التنظيم بموجب مراسيم رئاسية بعد ذلك؛ تبيان التشكيلة والمهام المتصلة بهذه المصالح، حيث تم إحداث سنة 2008 مصلحة مركزية للشرطة القضائية التابعة للمصالح العسكرية للأمن، تجمع بين مهام التحري والتحقيق في جرائم القانون العام وجرائم القانون العسكري. إلا أن المرسوم المذكور لم يعمر طويلا، حيث تم إلغاؤه سنة 2013[1].

وفي السياق نفسه؛ أعيدت هيكلة المصالح العسكرية للأمن تدريجيا من حيث التشكيلة وطريقة التعيين والمهام وقواعد الاختصاص ذات الصلة –السارية حاليا–. وذلك بموجب المرسوم الرئاسي الصادر سنة 2014، وتعديل "ق.إ.ج" الوارد سنة 2017 بالقانون 17–07 سابق الذكر[2]. حيث ورغم ورود التنظيم قبل التشريع –الأمر الذي يعد مخالفا للمنطق القانوني السليم–؛ إلا أن أحكامهما جاءت متناسقة عموما.

أنشأ المرسوم الرئاسي لسنة 2014 المذكور أعلاه؛ ما سماها بمصلحة التحقيق القضائي لمديرية الأمن الداخلي بدائرة الاستعلام والأمن[3]. التي تتشكل بشريا من أشخاص اكتسبوا صفة الشرطة القضائية، في إطار الأحكام التشريعية المذكورة سابقا بخصوص الوضع التقليدي للشرطة القضائية، التي حينها تعديل "ق.إ.ج" لسنة 2017. حيث تمنح الصفة لضباط وضباط الصف المعينون بقرار مشترك من وزير الدفاع الوطني ووزير العدل، والمؤهلين بعد ذلك بموجب قرار صادر حصرا عن النائب العام لمجلس قضاء الجزائر العاصمة، بناءً على اقتراح من السلطة الإدارية العسكرية المختصة. كما أنها تقسم تنظيميا إلى المصلحة المركزية، وفروع جهوية وفرق متنقلة[4].

وأما بخصوص النطاقين الإقليمي والنوعي، فتختص المصالح العسكرية للأمن؛ بالأعمال الوقائية والتحري والتحقيق بغرض مكافحة الجرائم الماسة بأمن الدولة، المنصوص عليها في إطار قانون

---

[1] **أنظر:** المادة 15؛ أمر رقم 66-155، مرجع سابق. **معدلة** بالأمر رقم 95-10، مؤرخ في 25 فيفري 1995، (ج ر) عدد 17، صادر بتاريخ 29 مارس 1995. **وأنظر أيضا:** مرسوم رئاسي رقم 08-52، مؤرخ في 09 فيفري 2008، يتضمن إحداث مصلحة مركزية للشرطة القضائية للمصالح العسكرية للأمن التابعة لوزارة الدفاع الوطني ويحدد مهامها، (ج ر) عدد 08، صادر بتاريخ 13 فيفري 2008. **ملغى** بالمرسوم الرئاسي رقم 13-309، مؤرخ في 08 سبتمبر 2013، (ج ر) عدد45، صادر بتاريخ 18 سبتمبر 2013.

[2] **أنظر:** مرسوم رئاسي رقم 14-183، مؤرخ في 11 جوان 2014، يتضمن التحقيق القضائي لمديرية الأمن الداخلي بدائرة الاستعلام والأمن ومهامها وتنظيمها، (ج ر) عدد 32، صادر بتاريخ 12 جوان 2014.

[3] ولو أنه لنا ما نقوله بخصوص استعمال مصطلح التحقيق القضائي. فهل يقصد به التحري والتحقيق، أم التحري قبل تحريك الدعوى العمومية، أم التحقيق الذي يلي ذلك. سيما وأنه بالرجوع إلى النسخة الفرنسية من عنوان المرسوم نفسه، نجدها تنص على التحري القضائي "Investigation judiciaire"، وليس التحقيق الذي يعبر عنه بـ "Instruction". الأمر الذي نفصل فيه بأن التنظيم قد وقع سهوا، وهو يقصد التحري والتحقيق معا، وذلك نظرا لاختصاصات المصلحة التي تبين ذلك.

[4] **أنظر:** المادتان 15 و15 مكرر2/1؛ أمر رقم 66-155، المرجع نفسه. **وأنظر أيضا:** المادة 07؛ مرسوم رئاسي رقم 14-183، المرجع نفسه.

العقوبات دون سواه[1]. كما أنها تمارس ذلك تحت إشراف وإدارة، الجهات القضائية المختصة إقليميا ونوعيا، الدائرة بين النيابة العامة وقضاء التحقيق على حسب الحالة، على أنها في كل الأحوال تبقى تحت رقابة غرفة الاتهام لمجلس قضاء الجزائر العاصمة دون سواه[2].

ب- قواعد اختصاص جهاز شرطة المصالح العسكرية للأمن في مواجهة جرائم الوسط الرقمي: تختص المصالح العسكرية للأمن عموما؛ بالتحري والتحقيق في الجرائم الماسة بأمن الدولة المبينة سابقا. التي لو ألحقناها بالنطاق الافتراضي للوسط الرقمي؛ لوجدنا أنها بمثابة الجرائم التقليدية المرتكبة عبره أو بمساعدته[3]. كما قد تختص المصالح العسكرية للأمن بالتحري والتحقيق؛ بمواجهة سلوك مزدوج الطبيعة في إطار جرائم الوسط الرقمي، الدائر بين جريمة مساس بأنظمة المعالجة الإلية للمعطيات، وجريمة تقليدية استعمل الوسط الرقمي كوسيلة تنفيذها. حيث الشخص الذي يقوم بالولوج عن طريق الغش، إلى منظومة معلوماتية تابعة لوزارة الدفاع الوطني بغرض التجسس؛ يكون قد ارتكب جنحة الدخول وجناية محاولة التجسس لو توقف عند الشروع، وجناية التجسس لو أتمها[4].

وأما بخصوص الاختصاص الإقليمي؛ فالمشرع بين صراحةً أنه للشرطة القضائية المتصلة بالمصالح العسكرية للأمن؛ اختصاص واسع يشمل كافة التراب الوطني. كما أنها تتبع وكيل الجمهورية أو قاضي التحقيق المختص على حسب الحالة –كما بينا سابقا-. لكن إذا ما كانت الجريمة الماسة بأمن الدولة من بين جرائم المعاملة الخاصة، المنطوية حصرا على جرائم الإرهاب؛ فتكون المصالح العسكرية للأمن تابعة للقاضي المختص الممارس لمهامه في إطار الأقطاب المتخصصة المذكورة سابقا[5].

---

[1] ولو أنه يوجد تناقض بين النصين التشريعي والتنظيمي. حيث يحدد المشرع الاختصاص بجرائم أمن الدولة، وحدده قبله التنظيم بأربعة جرائم؛ وهي الماسة بأمن الإقليم والإرهاب والتخريب والجريمة المنظمة. وفي هذا الإطار نقول أن النص التشريعي هو النافذ، نظرا لكونه الأقوى من حيث الأثر القانوني، ولوروده بعد نص التنظيم - إلغاء ضمني-. وعلى العموم باعتماد المشرع لمصطلح أمن الدولة؛ يكون قد أخذ بكل الجرائم التي جاء بها التنظيم ووسعها في إطار جرائم أمن الدولة، المتمثلة في؛ الخيانة والتجسس، والتعدي على الدفاع والاقتصاد الوطنيين، والاعتداءات والمؤامرات والجرائم ضد سلطة الدولة وسلامة أرض الوطن، والتقتيل والتخريب إخلالا بالدولة، والجرائم الموصوفة بالأفعال الإرهابية والتخريبية والمساهمة في حركات التمرد. **أنظر في ذلك:** المادة 15 مكرر/1؛ أمر رقم 66-155، مرجع سابق. **وأنظر أيضا:** المادة 05؛ مرسوم رئاسي رقم 14-183، مرجع سابق. **وأنظر كذلك:** المواد من 61 إلى 96مكرر؛ أمر رقم 66-156، مرجع سابق.

[2] **أنظر:** المادتان 15 مكرر/2 و207، أمر رقم 66-155، المرجع نفسه. **وأنظر أيضا:** المادة 03؛ مرسوم رئاسي رقم 14-183، المرجع نفسه.

[3] رغم إسناد التنظيم صراحةً للمصالح العسكرية للأمن مهمة الوقاية من كل جرائم الوسط الرقمي ومكافحتها؛ إلا أننا نرى ذلك غير ممكنا. نظرا لكون القانون الوارد بعد التنظيم؛ قد حدد مهامها في مكافحة جرائم أمن الدولة فقط. كما أن القول بذلك؛ سيجعلها تتداخل في انجاز مهامها مع الأجهزة الشرطية الأخرى، سيما وأن لها اختصاص إقليمي وطني. ومنه الأجدر أن ينص التنظيم على أنها مصلحة؛ تواجه جرائم أمن الدولة المتصلة بالوسط الرقمي والجرائم الأخرى المرتبطة بها. **أنظر في ذلك:** المادة 1/6-5؛ مرسوم رئاسي رقم 14-183، المرجع نفسه.

[4] رغم عدم اختصاصها بالتحري والتحقيق في جرائم المساس؛ إلا أنها في المثال المبين أعلاه تصبح مختصة، نظرا لارتباطها بجناية أمن دولة. فالمختص بالنظر في الجنايات هو المختص أيضا بالنظر في الجنح والمخالفات المرتبطة بها.

[5] **أنظر:** المادة 6/16و7؛ أمر رقم 66-155، المرجع نفسه. **وأنظر أيضا:** المواد 02 و03 و04 و05؛ مرسوم تنفيذي رقم 06-348، مرجع سابق.

المطلب الثاني: الأجهزة الوطنية المساعدة على التحري والتحقيق في جرائم الوسط الرقمي

يُعتمد في العادة لممارسة أعمال التحري والتحقيق؛ على الأجهزة القضائية وشبه القضائية التقليدية المذكورة في المطلب الأول تحت عنوان الأجهزة الرئيسية. التي تعمل وفق ما جاءت به أحكام وقواعد قانون الإجراءات الجزائية والقوانين المكملة له. إلا أنه في إطار جرائم الوسط الرقمي ومسرحها الافتراضي المعقد؛ أصبح الدور التقليدي غير كافٍ ولا يمكنه تحقيق الغرض الإجرائي المراد، ومنه توجب التدخل من العديد من الأجهزة الأخرى في إطار المساعدة اللازمة. التي لن تتحقق إلا بتوزيع الأدوار على حسب نوع القضية وحيثياتها.

وفي الإطار المذكور أوجد القانون الجزائري عموما؛ العديد من الأجهزة المساعدة على التحري والتحقيق الذي تمارسه الأجهزة الرئيسية. التي يمكن أن نحددها في؛ الهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام والاتصال ومكافحتها(فرع أول)، والأجهزة التقنية المساعدة على التحري والتحقيق في جرائم الوسط الرقمي(فرع ثانٍ).

الفرع الأول: الهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام والاتصال ومكافحتها

تعد الهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام والاتصال ومكافحتها؛ من أهم الأجهزة المساعدة للأجهزة الرئيسية المكلفة بالتحري والتحقيق في جرائم الوسط الرقمي. الأمر المستشف أساسا من كونها الجهاز الوحيد من بين الأجهزة المساعدة؛ الذي يعد مستحدثا طبيعةً وضمونا وأثرا. حيث لأول مرة يتم الاعتماد جنائيا؛ على جهة غير الجهات الرئيسية لتشارك في عمليتي التحري والتحقيق.

وعلى العموم عالج القانون الجزائري الهيئة محل الدراسة، في إطار دورها المساعد على التحري والتحقيق في جرائم الوسط الرقمي؛ وفق مجموعة من النصوص التشريعية والتنظيمية. التي يمكن من خلالها التوصل إلى التعريف بها(أولا)، والوقوف على تشكيلتها المختلطة(ثانيا)، وتحديد مهامها المتعددة(ثالثا).

أولا: التعريف بالهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام والاتصال ومكافحتها

بعد التسليم الحتمي من المشرع الجزائري –وقبله التشريعات المقارنة كما بينا سابقا–؛ بحداثة وتعقيد جرائم الوسط الرقمي ومسرحها الافتراضي من جهة، ومن جهة أخرى؛ بالخطورة الإجرائية ذات الصلة، المنطوية أساسا على العجز المتصل بإجراءات التحري والتحقيق التقليدية، إن بخصوص الأجهزة أو الأعمال الممارسة من قبلها؛ تم التوجه تدريجيا إلى ضرورة التحول الجنائي نحو النظرة الحديثة الجامعة بين الوقاية والمكافحة. الأمر الذي لم يكن ممكنا؛ إلا باستحداث هيئة إدارية مستقلة تعمل بالتنسيق مع الجهات التقليدية المختصة وفق شروط محددة، وهي المنطوية على الهيئة محل الطرح.

ورغم بداية المشرع الجزائري لعملية التجريم في الوسط الرقمي بحلول سنة 2001، والتحول في المعاملة الإجرائية انطلاقا من سنة 2004[1]؛ إلا أنه تأخر من حيث التفطن إلى ضرورة إنشاء هيئة إدارية مستقلة تهتم بالوقاية والمكافحة إلى غاية حلول سنة 2009، في إطار القانون رقم 09-04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[2]. الأمر الذي يفهم منه بداهةً؛ أن المشرع لم يعي –أو لم يقتنع على الأقل– حجم خطورة جرائم الوسط الرقمي وتعقيد مسرحها الافتراضي، الدافعين لضرورة المواجهة المزدوجة الدائرة بين الوقاية والمكافحة؛ إلا بعد أن خطت العديد من التشريعات المقارنة أشواطا متقدمة في المسألة ذاتها[3].

كما أن نص إنشاء الهيئة الوطنية محل الدراسة الوارد سنة 2009؛ تضمن فقرة ثانية تحيل إلى التنظيم، الذي عليه أن يحدد تشكيلة وتنظيم الهيئة وكيفيات سيرها[4]. الأمر الذي يعد طبيعيا، نظرا لكون النص التشريعي ينشئ ويضع الأحكام العامة، ثم يأتي النص التنظيمي ليبين الأمور التنظيمية الواجبة لعمل الهيئة كجهاز. إلا أن ما يدفع للاستغراب القانوني؛ ينطوي على تأخر النص التنظيمي في الصدور إلى غاية 2015 أي ما يزيد عن الست 06 سنوات بين القانون والتنظيم[5]. والأكثر غرابة في هذا الإطار؛ يكمن في أنه إلى غاية سنة 2017 لم تكن الهيئة قد بدأت في الممارسة الفعلية لمهامها، والدليل على ذلك أنها فتحت باب التوظيف الإداري لأول مرة بتاريخ أفريل 2017، مع تحديد مكان إيداع الملفات بوزارة العدل. فهل مقر الهيئة هو وزارة العدل أم أن لها مقرا لم يسلم بعد؟؟؟[6].

وعلى العموم حدد المشرع بنص المادة 1/13 من القانون 09-04 سابقة الذكر؛ المهام الأساسية للهيئة المنطوية على الوقاية من جرائم الوسط الرقمي ومكافحتها، كما أن السلطة التنفيذية بموجب المواد من 02 إلى 04 من المرسوم الرئاسي 15-261 سابق الذكر؛ حددت طبيعة الهيئة وأغلب مهامها. الأمر

---

[1] حيث جرم المشرع لأول مرة سلوكيات تقليدية ترتكب عبر الوسط الرقمي؛ في إطار المادة الجديد 144مكرر "ق.ع" المضافة بالقانون 01-09، المتصلة بالإساءة لرئيس الجمهورية. كما تم البدء في المعاملة الإجرائية الخاصة لجرائم المساس بأنظمة المعالجة الإلية للمعطيات كأحد أنواع جرائم الوسط الرقمي؛ لأول مرة بموجب القانون 04-14 المعدل والمتمم للعديد من مواد "ق.إ.ج"، سيما المادة 2/37 المتصلة بتمديد اختصاص وكيل الجمهورية. **أنظر:** المادة 144مكرر المضافة بالمادة 07؛ قانون رقم 01-09، مرجع سابق. **وأنظر أيضا:** المادة 2/37 المضافة بالمادة 03؛ قانون رقم 04-14، مؤرخ في 10 نوفمبر 2004، يعدل ويتمم أمر رقم 66-155، يتضمن قانون الإجراءات الجزائية، (ج ر)، عدد 71، صادر بتاريخ 10 نوفمبر 2004.

[2] **أنظر:** المادة 1/13؛ قانون رقم 09-04، مرجع سابق.

[3] الأمر الذي سيتبين أكثر؛ عند التطرق إلى بعض الأجهزة المقارنة في إطار دراسة الفرع الأخير من الفصل محل الطرح، المتصل بالتعاون مع الأجهزة الوطنية المقارنة.

[4] **أنظر:** المادة 2/13؛ قانون رقم 09-04، المرجع نفسه.

[5] **أنظر:** مرسوم رئاسي رقم 15-261، مرجع سابق.

[6] **أنظر:** مدونة التوظيف في الجزائر، "إعلان عن توظيف في الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها أفريل 2017"، تاريخ النشر: 12 أفريل 2017، تاريخ التصفح: 23 مارس 2018، الرابط: http://www.dzemploi.org/2017/04/2017_92.html.

الذي يمكن من خلاه أن نعرف الهيئة؛ على أنها: "سلطة إدارية وطنية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي، التي توضع لدى الوزير المكلف بالعدل، وينحصر دورها العام في المساعدة على الوقاية من جرائم الوسط الرقمي ومكافحتها"[1].

يفهم من خلال التعريف المستشف من النصين التشريعي والتنظيمي، أنه للهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام والاتصال ومكافحتها؛ طابع السلطة الإدارية المستقلة، الذي يُفترض فيه أن يمنحها الاستقلالية في ممارسة مهامها. الأمر الذي لنا فيه رأي مخالف، فكيف يعقل أن نضع سلطة مستقلة لدى وزير معين، وكيف نقيدها بالرقابة المباشرة للسلطة القضائية[2]. الأمر الذي قد نواجه بخصوصه؛ بأنه لابد من وضعها لدى وزير العدل وتحت الرقابة المباشرة للقضاء، نظرا لحساسية مهامها المتصلة بحرمة الحياة الخاصة وحماية الصالح العام كما سنرى لاحقا. وهو ما نعتبره بمثابة الحجج الواهية، لخرق الطبيعة القانونية ذات الصلة بالهيئات الإدارية المستقلة[3]. ومنه ننوه بضرورة؛ التراجع عن وصف الهيئة كسلطة إدارية مستقلة، مع الاحتفاظ بالوصاية والرقابة كما تقررا، وهذا تأسيسا على حساسية وخطورة المهام التي تمارسها الهيئة.

ثانيا: تشكيلة الهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام والاتصال ومكافحتها

وضع المرسوم الرئاسي رقم 15-261 المذكور سابقا؛ أحكاما تبين تشكيلة الهيئة. فبالإضافة إلى القضاة وضباط وأعوان ومستخدمي الدعم التقني والإداري، المتمين أصلا إلى الأجهزة التقليدية[4]؛ نجدها تتكون من سبعة 07 هياكل داخلية، منطوية على اللجنة المديرة والمديرية العامة ومديرية المراقبة واليقظة الالكترونية ومديرية التنسيق التقني ومركز العمليات التقنية والملحقات الجهوية. وهي التي نقسمها في إطار دراسة الحال إلى ثلاثة أنواع بحسب طبيعة كل منها. فنتطرق أولا إلى الهياكل العامة، ومن ثم الهياكل الفنية، على أن نستعرض في الأخير الهياكل الفرعية.

---

[1] **أنظر:** المادتان 13 و14؛ قانون رقم 09-04، مرجع سابق. **وأنظر أيضا:** المواد 02 و03 و04؛ مرسوم رئاسي رقم 15-261، مرجع سابق.

[2] في الحقيقة تقييد السلطات الإدارية المستقلة؛ لا يعد بالأمر الجديد عن القانون الجزائري. حيث كل السلطات المستقلة الأخرى تخضع لذلك، سيما مجلس المنافسة الذي يوضع لدى الوزير المكلف بالتجارة رغم كونه سلطة إدارية مستقلة. **أنظر في ذلك:** المادة 23؛ أمر رقم 03-03، مؤرخ في 19 جويلية 2003، يتعلق بالمنافسة، (ج ر)، عدد 43، صادر بتاريخ 20 جويلية 2003، معدل ومتمم.

[3] فالسلطة الإدارية المستقلة في أغلب القوانين المقارنة؛ لا توضع لدى أي جهة كانت بما فيها الوزير المختص. والدليل على ذلك؛ نجد المشرع الفرنسي الذي عدل القانون التجاري بالأمر رقم 86-1243 المتضمن تحرير الأسعار والمنافسة، لينشأ مجلس المنافسة "Conseil de la concurrence" ويضعه لدى الوزير المكلف بالاقتصاد. ومن ثم يعدل القانون التجاري نفسه؛ بالقانون رقم 08-776 المتضمن تطوير الاقتصاد، ليسحب وصاية الوزير نفسه على المجلس؛ الذي أصبح يسميه بالسلطة أو الهيئة الإدارية المستقلة بدلا عن المجلس "Autorité de la concurrence". **أنظر في ذلك:**

- Art L461-1; code de commerce français, Version consolidée au 3 mars 2018. Disponible sur le Lien: https://www.legifrance.gouv.fr.

[4] **أنظر:** المواد 06 و18 و19؛ مرسوم رئاسي رقم 15-261، المرجع نفسه.

1. الهياكل العامة للهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام والاتصال ومكافحتها: تتكون الهيئة الوطنية محل الدراسة بالإضافة إلى الهياكل الفنية والفرعية؛ من المكونات الأساسية الحاملة للطابع العام. وهي المنطوية أساسا على اللجنة المديرة، والمديرية العامة.

أ- **اللجنة المديرة:** تتشكل اللجنة المديرة من الوزير المكلف بالعدل كرئيس لها، وعدد من الأعضاء المحددين حصرا؛ في الوزير المكلف بالداخلية، والوزير المكلف بالبريد وتكنولوجيات الإعلام والاتصال، وقائد الدرك الوطني، والمدير العام للأمن الوطني، وممثل لرئاسة الجمهورية، وآخر لوزارة الدفاع الوطني. بالإضافة إلى قاضيين من المحكمة العليا[1]. وهي التشكيلة التي نراها توازن بين السلطة التنفيذية المهتمة بالوقاية في إطار الضبط الإداري والأمني، والقضائية المختصة بالمكافحة بدءا من الضبط القضائي. كما ضمت العنصر التقني، بذكر وزير البريد وتكنولوجيات الإعلام والاتصال[2].

وتختص اللجنة المديرة بالعديد من المهام، التي حددتها السلطة التنفيذية؛ في الدراسة والموافقة على النظام الداخلي للهيئة وميزانيتها وتقريرها السنوي، مع ضبط برنامجها وفق شروط تنفيذ معينة. كما أنها تدرس المسائل ذات الصلة بمهام الهيئة، سيما تلك المتصلة بالمراقبة الالكترونية. هذا بالإضافة إلى التوجيه والإشراف والمراقبة. وخاصةً القيام بعمليتي التقييم والاقتراح، سيما بخصوص تقييم حالة الخطر في مجال الإرهاب والتخريب والمساس بأمن الدولة، وأيضا تبدي الرأي في كل ما يتصل بنشاط الهيئة، وتقترح كل ما هو مفيد بشأن ذلك، سيما نشاطات البحث والتقييم ذات الصلة بمهامها[3]. الأمر الذي نجده بمثابة الوسائل العامة، التي تؤدي في الأخير إلى تحقيق الوقاية من جرائم الوسط الرقمي ومكافحتها.

ب- المديرية العامة: كتكملة للتركيبة العامة، أنشأت السلطة التنفيذية بالمرسوم نفسه؛ ما تسمى بالمديرية العامة لتهتم بالأمور الإدارية والتنظيمية. التي نص التنظيم نفسه على أنها تدار من مدير عام، وأحال من حيث تشكيلتها إلى التنظيم الداخلي[4]، الصادر سنة 2018 بموجب قرار مشترك بين نائب وزير الدفاع ووزير الداخلية ووزير العدل. فزودها بأمانه ومصلحة الإدارة العامة، التي –الإدارة العامة- تتكون من ثلاثة مكاتب، يتصل الأول بالموارد البشرية والثاني بالمالية والوسائل والثالث بالوقاية والأمن[5].

---

[1] **أنظر:** المادة 07؛ مرسوم رئاسي رقم 15-261، المرجع نفسه.

[2] ولو أن بعض الدراسات النقدية السابقة -على ندرتها-؛ نجدها تنادي بعدم التوازن في تشكيلة اللجنة المديرة. سيما بغياب وزير المالية، الذي يعد حامي الاقتصاد الوطني التقليدي والرقمي. والعمل بالتمثيل المزدوج لوزارة الدفاع. وأيضا تقييد تعيين القضاة بالمنتمين للمحكمة العليا فقط، من دون النظر إلى معيار الكفاءة الرقمية. **أنظر في ذلك:** لحسن ناني، التحقيق في الجرائم المتصلة بتكنولوجية المعلوماتية، الطبعة الأولى، دار النشر الجامعي الجديد، الجزائر، 2017، ص 86 و87.

[3] **أنظر:** المادة 08؛ مرسوم رئاسي رقم 15-261، المرجع نفسه.

[4] **أنظر:** المادتان 09 و15؛ المرجع نفسه.

[5] **أنظر:** المادتان 02 و03؛ قرار وزاري مشترك، مؤرخ في 17 ديسمبر 2017، يحدد التنظيم الداخلي لهياكل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، (ج ر) عدد 14، صادر بتاريخ 04 مارس 2018.

أما بخصوص المهام الموكلة إلى المديرية العامة، التي قلنا أنها ذات طابع إداري تنظيمي؛ فتم تحديدها حصرا، في السهر على تحقيق التنظيم الجيد؛ من حيث ضمان السير الحسن وتنفيذ برنامج العمل، وتنشيط نشاطات هياكل الهيئة والتنسيق بينها ومتابعتها ومراقبتها، وتحضير الاجتماعات. كما تقوم بتمثيل الهيئة أمام جميع الهيئات والأعمال الوطنية والدولية. وتقوم كذلك بممارسة الأعمال الإدارية والوظيفية على مستخدميها، من خلال ضمان الحفاظ على السر المهني وإحقاق السلطة السلمية، وإجراءات التأهيل وأداء اليمين. وأخيرا إعداد التقرير السنوي وعرضه على اللجنة المديرة للمصادقة عليه[1].

2. **الهياكل الفنية للهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام والاتصال ومكافحتها:** إضافةً إلى الهياكل العامة ذات الطابع الرئيسي، نجد أن الهيئة الوطنية محل الدراسة؛ تتكون من هياكل أخرى لها الطابع الفني. والمتمثلة في مديرية المراقبة الوقائية واليقظة الالكترونية، ومديرية التنسيق التقني.

أ- **مديرية المراقبة الوقائية واليقظة الالكترونية:** تعد المديرية محل الطرح؛ أهم الهياكل الفنية التي تحويها الهيئة. والتي لم يشر المرسوم الرئاسي 15-261 المذكور سابقا إلى تشكيلتها، إلا من حيث إبراز أن مديرها يعن بمرسوم رئاسي، وأنها السيدة على عمل مركز العمليات التقنية[2]. الأمر الذي حدده التنظيم الداخلي سابق الذكر؛ في مصلحة المراقبة الالكترونية ومصلحة المتابعة والتحليل والتعاون، بالإضافة إلى مركز العمليات التقنية والملحقات الجهوية التي توضع تحت إدارتها[3].

وعلى العموم تختص مديرية المراقبة الوقائية واليقظة الالكترونية؛ بالعديد من المهام المحددة حصرا، الدائرة بين أعمال الوقاية من جرائم الوسط الرقمي ومكافحتها، والأعمال الأخرى ذات الصلة[4]. حيث تمارس المديرية في سبيل الوقاية؛ مراقبة الاتصالات الالكترونية، وجمع ومركزة واستغلال المعلومات السامحة باكتشافها، كما أنها ترسلها بعد ذلك؛ إلى السلطة القضائية والشرطية المختصة. وأما في إطار دور المكافحة فتقوم المديرية؛ بتزويد السلطات القضائية وشبه القضائية المختصة؛ بالمعلومات ذات الصلة بجرائم الوسط الرقمي. وكذلك بخصوص الأعمال الأخرى؛ فتقوم المديرية بعمليات التحسيس الوطني، وتنفيذ طلبات المساعدة القضائية الأجنبية في إطار القانون، وتضع مركز العمليات التقنية والملحقات الجهوية قيد الخدمة، في إطار توجيهات اللجنة المديرة، مع الحفاظ على السر المهني[5].

---

[1] **أنظر:** المادة 10؛ مرسوم رئاسي رقم 15-261، مرجع سابق.

[2] **أنظر:** المادتان 1/13 و37؛ المرجع نفسه.

[3] **أنظر:** المواد 4 و5 و6؛ قرار وزاري مشترك، مؤرخ في 17 ديسمبر 2017، مرجع سابق.

[4] **أنظر:** المادة 11؛ المرجع نفسه.

[5] رغم أهمية تحيد مهام المديرية، سيما للتفرقة بينها وبين مديرية التنسيق التقني؛ إلا أننا نرى ذلك؛ بمثابة الطرح الزائد. فالمديرية؛ تعمل بتوجيهات اللجنة المديرة، وبالتالي هي تتبعها من حيث المهام، وتعد بمثابة ذراعها التقنية. وعلى العموم تعد المديرية؛ بمثابة الذراع التقنية للهيئة ككل، لغرض تحقيق أهداف إنشائها أصلا. كما أنه من جهة أخرى؛ لا يمكن بأي حال من الأحوال تحديد المهام التقنية، نظرا للتطور الديناميكي السريع لوسائل ارتكاب جرائم الوسط الرقمي، كما بينا سابقا.

ب- مديرية التنسيق التقني: تحمل مديرية التنسيق التقني الطابع نفسه تقريبا؛ المتصل بمديرية المراقبة الوقائية واليقظة الالكترونية السابقة بالدراسة. خاصةً من حيث تشكيلتها التي لم يتطرق لها المرسوم الرئاسي، وحددها القرار الوزاري المشترك في مصلحة الدراسات والخبرات القضائية، ومصلحة منظومة الإعلام[1]. وأيضا يمكن القول أنها مكونة من تجهيزات فنية واجبة لممارسة المهام المطلوبة –الأمر المستشف من المهام التالية بالطرح–، وأشخاص مختصون على غرار مستخدمي الدعم التقني[2].

وأما من حيث المهام المسندة إلى مديرية التنسيق التقني؛ فيمكن القول أنها ذات طابع تقني، تخدم اللجنة المديرة بصفة خاصة، والهيئة الوطنية في إطار مواجهة جرائم الوسط الرقمي عموما. وحدد المرسوم الرئاسي نفسه المهام التي تضطلع بها المديرية على سبيل الحصر[3]؛ في مهام تقنية محضة، وأخرى قانونية. حيث تقوم بتسيير منظومة إعلام الهيئة وإدارتها، كما تمارس أعمال قانونية عامة بتكوين قاعدة معطيات تحليلية للإجرام المتصل بالوسط الرقمي واستغلاله، وإعداد الإحصائيات الوطنية ذات الصلة، وعموما القيام التلقائي أو بطلب من اللجنة المديرة؛ بالدراسات والتحاليل والتقييمات المتعلقة بصلاحياتها. على أن تقوم أيضا بانجاز الخبرات القضائية المتصلة بمجال اختصاص الهيئة عموما[4].

3. الهياكل الفرعية للهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام والاتصال ومكافحتها: تتشكل الهيئة الوطنية أيضا؛ من هياكل أخرى لها الطابع الفرعي، نظرا لتبعيتها الهيكلية أو لعدم وجودها الدائم. وهي المنطوية على مركز العمليات التقنية، والملحقات الجهوية، ووحدات المراقبة.

أ- مركز العمليات التقنية: نجد من بين الهياكل الفرعية التي تقوم عليها الهيئة في إطار مواجهة جرائم الوسط الرقمي؛ ما يسمى بمركز العمليات التقنية. الذي توجب المرسوم الرئاسي نفسه؛ تزويده بالمنشات والتجهيزات والوسائل المادية اللازمة، والعدد الكافي من المستخدمين التقنيين. كما قسمه القرار الوزاري المشترك إلى ثلاثة مكاتب، يختص الأول منها بأنظمة المراقبة والمتابعة، والثاني بأنظمة مراقبة الإنترنت، والثالث بأنظمة التموقع الجغرافي ومراقبة الاتصالات عبر الأقمار الصناعية[5].

إلا أن مركز العمليات التقنية لا يعد بمثابة الهيكل المستقل كتلك السابقة بالدراسة من هياكل عامة وفنية، بل هو تابع لمديرية الوقاية واليقظة الالكترونية المذكورة سابقا. ومنه نجده بمثابة الهيكل الفرعي

---

[1] **أنظر:** المادة 37؛ مرسوم رئاسي رقم 15-261، مرجع سابق. **وأنظر أيضا:** المواد 09 و10 و11؛ قرار وزاري مشترك، مؤرخ في 17 ديسمبر 2017، مرجع سابق.

[2] **أنظر:** المادة 3/18؛ مرسوم رئاسي رقم 15-261، المرجع نفسه.

[3] **أنظر:** المادة 12؛ المرجع نفسه.

[4] يتضح جليا أن مهامها تختلف تماما عن تلك المسندة لمديرية المراقبة الوقائية واليقظة الالكترونية، رغم اتفاقهما في الطابع التقني. ويمكن القول أن دور مديرية التنسيق التقني؛ ينحصر في مساعدة الهياكل الأخرى وتطبيق تعليماتها.

[5] **أنظر:** المادة 1/13؛ مرسوم رئاسي رقم 15-261، المرجع نفسه. **وأنظر أيضا:** المادة 07؛ قرار وزاري مشترك، مؤرخ في 17 ديسمبر 2017، المرجع نفسه.

الداخل فيها، سيما وأن النص جاء صريحا، وعبر بأنه يتبع المديرية ويُشَغَل من طرفها[1]. كما أن مهام المركز؛ تنطوي على تنفيذ العمليات التقنية لمراقبة الاتصالات الالكترونية دون غيرها[2]. الأمر الذي يفهم منه بداهةً؛ أن دور المركز ينحصر في التحضير والتنفيذ التقنيين للعمليات الرقمية السامحة بانجاز المراقبة الالكترونية، التي تنجز بطلب محدد وموجه من مديرية الوقاية واليقظة الالكترونية، وتحت إشرافها المباشر.

ب- الملحقات الجهوية: نجد من بين الهياكل الفرعية للهيئة الوطنية أيضا؛ ما تسمى بالملحقات الجهوية. التي لم يتطرق لها المرسوم الرئاسي بالشرح، إلا من حيث اعتبارها بالهيكل الفرعي المتصل بمديرية الوقاية واليقظة الالكترونية، المشرفة عنها والقائمة بعملية بإدارتها وتشغيلها. الأمر الذي بينه التنظيم الداخلي سابق الذكر، الذي اعتبر أنها تتكون من أربعة مكاتب، ينطوي الأول منها على الإدارة العامة، والثاني على المراقبة الالكترونية، والثالث على المتابعة والتحليل، على أن يتصل الرابع والأخير بالعمليات التقنية[3].

ج- وحدات المراقبة: أضاف المرسوم التنفيذي 15-261 المذكور؛ ما تسمى بوحدات المراقبة كأحد الهياكل غير المنصوص عليها في إطار المادة 06 منه، المحددة لتشكيلة الهيئة الوطنية تحت عنوان التشكيلة والتنظيم. وهي التي حددت مكوناتها المادية والبشرية؛ بالوسائل والتجهيزات التقنية الضرورية، والمستخدمون التقنيون العاملين تحت إدارة ومراقبة قاضٍ وضابط شرطة قضائية أو أكثر، ممن ينتمون للهيئة الوطنية دون سواها[4].

وأما بخصوص المهام التي تنجزها وحدات المراقبة –التي قد تكون واحدة أو أكثر–؛ فتنطوي على المهام المتقطعة التي لا تُعمل إلى بخصوص قضية محددة بذاتها، وهذا لغرض إعمال الإجراءات الخاصة الواردة بالقانون 09-04 سابق الذكر، على غرار مراقبة الاتصالات الالكترونية والتفتيش والحجز في النطاق الافتراضي للوسط الرقمي. التي يجب أن تتصل حصرا؛ بعملية الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب والمساس بأمن الدولة[5].

وعلى العموم تبقى كل الهياكل المذكورة والى غاية تحرير النص؛ بمثابة الانجاز القانوني المعتبر. الذي ستبين الممارسات العملية بشأن الوقاية والمكافحة؛ مدى نجاعتها من حيث التشكيلة والمهام المسندة.

---

[1] **أنظر:** المادة 2/13؛ مرسوم رئاسي رقم 15-261، مرجع سابق.

[2] **أنظر:** المادة 1/13؛ المرجع نفسه.

[3] **أنظر:** المادتان 14 و15؛ المرجع نفسه. **وأنظر أيضا:** المادة 08؛ قرار وزاري مشترك، مؤرخ في 17 ديسمبر 2017، مرجع سابق.

[4] **أنظر:** المادة 22/ 1و2؛ مرسوم رئاسي رقم 15-261، المرجع نفسه.

[5] **أنظر:** المادة 21؛ المرجع نفسه.

ثالثا: مهام الهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام والاتصال ومكافحتها

لم ينشأ المرسوم الرئاسي المتصل بالهيئة الوطنية للوقاية من جرائم الوسط الرقمي ومكافحتها، كل الهياكل المذكورة في العنصر السابق بالدراسة؛ إلا بغرض تكامل مهامها المذكورة وفق التشكيلات المختلفة؛ المفضي إلى تحقيق المهام العامة التي وجدت الهيئة ككل من أجلها، والمنطوية أساسا على الوقاية من جرائم الوسط الرقمي ومكافحتها. الأمر الذي نتطرق إليه من حيث؛ تحديد المهام العامة للهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام والاتصال ومكافحتها، وتبيان كيفية سير الهيئة في إطار انجاز المهام ذات الصلة.

1. تحديد مهام الهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام والاتصال ومكافحتها: رجوعا إلى أحكام القانون 09-04 والمرسوم الرئاسي 15-261 المذكورين، نجد أنه للهيئة الوطنية محل الدراسة؛ العديد من المهام التي تنجزها عبر هياكلها المدروسة، وفي إطار طرق السير التالية بالدراسة. وتعد مهامها ذات الصلة محددة حصرا، التي بدراستها يمكن أن نقسمها إلى ثلاثة 03 أقسام أساسية، المنطوية على المهام المتصلة بجرائم الوسط الرقمي، من حيث الوقاية منها، ومكافحتها، والمساهمة في تطوير وتحسين آليات مواجهتها.

أ- مهام الوقاية من جرائم الوسط الرقمي: يعد الدور الوقائي من أهم الأدوار التي تعنى بها الهيئة الوطنية، خاصةً وأنه وارد صراحةً في التسمية القانونية للهيئة. كما أن الهيئة عموما؛ قائمة على مواجهة جرائم الوسط الرقمي عن طريق الوقاية قبل المكافحة، سيما بخصوص الجرائم الأكثر خطورة. الأمر الذي عبر عنه المشرع صراحةً في إطار القانون 09-04 -سابق الذكر-؛ بأنه من مهام الهيئة تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال. وهو ما أكد عليه المرسوم الرئاسي 15-261 سابق الذكر وبالعبارة نفسها[1].

كما تمارس الهيئة أيضا بنص القانون والتنظيم؛ الدور الوقائي الحصري، من بعض الجرائم التقليدية الخطيرة التي ترتكب عبر النطاق الافتراضي للوسط الرقمي. وذلك بضمان مراقبة الاتصالات الالكترونية تحت سلطة القاضي المختص، قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة[2]. إلا أنها تمارس مهام وقائية إضافية بنص التنظيم دون القانون، وذلك عن طريق اقتراح عناصر الإستراتيجية الوطنية للوقاية من جرائم الوسط الرقمي[3].

---

[1] **أنظر:** المادة 1/14-أ؛ قانون رقم 09-04، مرجع سابق. **وأنظر أيضا:** المادة 2/04-2؛ مرسوم رئاسي رقم 15-261، مرجع سابق.

[2] **أنظر:** المادة 1/04-أ و2؛ قانون رقم 09-04، المرجع نفسه. **وأنظر أيضا:** المادة 2/04-4؛ مرسوم رئاسي رقم 15-261، المرجع نفسه.

[3] **أنظر:** المادة 2/04-1؛ مرسوم رئاسي رقم 15-261، المرجع نفسه.

ب- مهام مكافحة جرائم الوسط الرقمي: يعد دور المكافحة الذي تختص به الهيئة في إطار مواجهة جرائم الوسط الرقمي؛ بمثابة المهام الموازية للدور الوقائي. حيث أدت خطورة هذه الجرائم كما بينا سابقا؛ إلى البحث عن الوقاية الإجرائية قبل المكافحة. ومنه نجد من أهم المهام ذات دور المكافحة الإجرائية بعد ارتكاب الجريمة؛ ما تم تقريرهما بالنصين التشريعي والتنظيمي، ومنها ما جاء بها النص التنظيمي دون التشريعي. حيث اتفق النصين من حيث تنشيط وتنسيق عمليات مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال[1]. وكذلك بخصوص مهام مساعدة السلطات القضائية والشرطية في مجال مكافحة جرائم الوسط الرقمي، سيما بخصوص التحريات والتحقيقات وانجاز الخبرات القضائية[2].

كما تقوم الهيئة بتقديم المساعدات في إطار التعاون الدولي، المتصل بتقديم المعلومات الهادفة إلى التعرف على الجناة وتحديد مكان تواجدهم، الأمر الذي لا يكون إلا بعد ارتكاب الجريمة، في إطار مكافحتها[3]. هذا بالإضافة إلى بعض المهام الواردة بنص التنظيم دون القانون، المنطوية على اقتراح عناصر الإستراتيجية الوطنية للوقاية من جرائم الوسط الرقمي[4]. وخاصةً تجميع وتسجيل وحفظ المعطيات الرقمية، وتحديد مصدرها ومسارها؛ من أجل استعمالها في الإجراءات القضائية[5].

ج- مهام المساهمة في تطوير وتحسين آليات مواجهة جرائم الوسط الرقمي: بالإضافة إلى المهام التشريعية و/أو التنظيمية التي تمارسها الهيئة؛ في إطار الوقاية والمكافحة، نجد أن النص التنظيمي الوارد بالمرسوم الرئاسي نفسه؛ قد أوكل لها العديد من المهام الأخرى التي نكيفها على أنها مهام إضافية. الأمر الذي يستشف صراحةً؛ من المهام المنطوية على تطوير التعاون مع المؤسسات والهيئات الوطنية المعنية بجرائم الوسط الرقمي. وكذلك المساهمة بخصوص مجال مواجهة جرائم الوسط الرقمي؛ في تحديث المعايير القانونية من جهة[6]، وتكوين المحققين المختصين من جهة أخرى[7].

---

[1] **أنظر:** المادة 1/14-أ؛ قانون رقم 09-04، مرجع سابق. **وأنظر أيضا:** المادة 2/04-2؛ مرسوم رئاسي رقم 15-261، مرجع سابق.

[2] الأمر الذي نجد فيه تناقضا بين النصين التشريعي والتنظيمي. حيث اقتصر المشرع على التحريات دون التحقيقات، وفتح التنظيم المجال ليشمل الاثنين معا بمصطلح المكافحة. وهو التضارب الذي نرجعه إلى الترجمة من الفرنسية للعربية، حيث نجد النص التشريعي الوارد باللغة الفرنسية؛ متطابقا مع نص التنظيم باستعماله لمصطلح المكافحة وليس التحري، الوارد بعبارة "En matière de lutte contre". **أنظر في ذلك:** المادة 1/14-ب (النسختان عربية وفرنسية)؛ قانون رقم 09-04، المرجع نفسه. **وأنظر أيضا:** المادة 2/04-3؛ مرسوم رئاسي رقم 15-261، المرجع نفسه.

[3] **أنظر:** المادة 1/14-ج؛ قانون رقم 09-04، المرجع نفسه. **وأنظر أيضا:** المادة 2/04-6؛ مرسوم رئاسي رقم 15-261، المرجع نفسه.

[4] **أنظر:** المادة 2/04-1؛ مرسوم رئاسي رقم 15-261، المرجع نفسه.

[5] **أنظر:** المادة 2/04-5؛ المرجع نفسه.

[6] **أنظر:** المادة 2/04-7 و9؛ المرجع نفسه.

[7] ولو أن التنظيم يخلط بين التحري والتحقيق، حيث عبر بـ "تكوين المحققين المختصين في مجال التحريات". الأمر الذي يعد مخالفا للقواعد الجنائية، فإما تكوين المحققين للقيام بالتحقيقات، أو المتحرين للقيام بالتحريات، أو الاثنين معا. وهو الأمر الذي -الاثنين معا- نضنه المقصود بالنص، مع قصور التعبير الاصطلاحي. **أنظر في ذلك:** المادة 2/04-8؛ المرجع نفسه.

2. طريقة سير الهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام والاتصال ومكافحتها: وضع المرسوم الرئاسي 15-261 المذكور، من خلال الفصل الثالث المكون من 17 مادة؛ العديد من الأحكام ذات الصلة بكيفيات سير الهيئة. الأمر المبين انطلاقا من طريقة الاجتماع، مرورا عبر تزويد الهيئة بالموارد البشرية والتجهيزات، وصولا إلى آليات ممارسة دوري الوقاية والمكافحة.

حيث نص المرسوم الرئاسي صراحةً؛ على أن تجتمع اللجنة المديرة بناءً على استدعاء يصدر عن رئيسها –وزير العدل كما بينا من قبل–، أو بناءً على طلب أحد أعضائها المبينة سابقا[1]. ويفهم أيضا من خلال النص الذي يلي ذلك؛ أن سير الهيئة يبدأ بأولى الخطوات المنطوية على إعداد نظامها الداخلي والتصديق عليه[2].

كما أن الهيئة في إطار ممارسة مهامها المتعددة، والهادفة إلى الوقاية من جرائم الوسط الرقمي ومكافحتها؛ تزود بمجموعة من الأشخاص المتباينين على حسب تخصصهم وجهة انتمائهم. حيث نجدها تزود بقضاة من جهة، ومن جهة أخرى؛ بضباط وأعوان للشرطة القضائية المنتمين أصلا لمصالح الأمن العسكري والأمن والدرك الوطنيين، الذين يحدد عددهم بموجب قرار مشترك بين الوزير المكلف بالعدل والمكلف بالدفاع الوطني أو الداخلية على حسب الحالة. هذا بالإضافة إلى تزويدها بعدد من المستخدمين لغرض الدعم الفني والإداري، المنتمين أصلا إلى مصالح الشرطة القضائية المذكورة[3]. كما يمكن للهيئة في إطار ممارسة مهامها؛ أن تستعين بأي خبير أو أي شخص ترى تدخله ضروريا، أو تطلب من أي جهاز أو مؤسسة كل وثيقة أو معلومة ذات أهمية لانجاز المهام[4].

على أن تمارس الهيئة في إطار سيرها بغرض الوقاية من جرائم الوسط الرقمي ومكافحتها وفق المهام المبينة؛ عددا من الأعمال الإجرائية المحددة حصرا. حيث يمكنها أن تقوم بإجراء المراقبة الالكترونية الوقائية –الأمر الذي ينجز عبر وحدات المراقبة المبينة سابقا–، كما تقوم بعمليتي التفتيش والحجز؛ إما تلقائيا في إطار الوقاية، بعد تلقي معلومات عن حيازة شخص لتجهيزات موجهة لمراقبة الاتصالات الالكترونية، أو بطلب من الجهة القضائية المختصة في إطار المكافحة بعد ارتكاب الجريمة[5].

---

[1] غير أن النص التنظيمي المقرر لذلك؛ أخلط بين الهيئة واللجنة. حيث بينا سابقا أن الجهاز محل الدراسة ككل يدعى بالهيئة، وهو يقوم على مجموعة من الهياكل التي من أهمها نجد اللجنة المديرة. الأمر الذي لم يحترمه التنظيم في هذا الإطار، فأطلق مصطلحا جديدا منطوي على "الهيئة المديرة"، وألحق بها دور الاجتماع المقصود أعلاه. وهو ما نرى فيه أنه مجرد سهو من السلطة التنفيذية، التي تقصد اللجنة المديرة وليس الهيئة المديرة. وهذا للعديد من الحجج، أهمها أن اللجنة المديرة المكونة من أعضاء هي من تجتمع، وأما الهيئة فلا يمكنها ذلك نظرا لتكونها من العديد من الهياكل. بالإضافة إلى أن النص نفسه الوارد باللغة الفرنسية؛ عبر صراحة على ذلك بعبارة "Le comité directeur"، وهو الذي عبر عن الهيئة بمصطلح "Organe". **أنظر في ذلك:** المادة 16(النسختان عربية وفرنسية)؛ مرسوم رئاسي رقم 15-261، مرجع سابق.

[2] **أنظر:** المادة 17؛ المرجع نفسه.

[3] **أنظر:** المادة 18؛ المرجع نفسه.

[4] **أنظر:** المادتان 19 و20؛ المرجع نفسه.

[5] **أنظر:** المادتان 21 و30؛ المرجع نفسه.

كخلاصة لاختصاص الهيئة الوطنية ومدى اتصالها بأجهزة التحري والتحقيق التقليدية من جهة، ومهامها في إطار الوقاية من جرائم الوسط الرقمي ومكافحتها من جهة أخرى؛ يمكن القول أنها هيئة تمارس البعض من مهامها تلقائيا والبعض الآخر بعد أن يطلب منها ذلك. حيث تمارس تلقائيا كل عمل بحثي وإرشادي عام وأي عمل آخر غير متصل بواقعة محددة بذاتها، كما تعمل بالوقاية التلقائية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة –التي تعد جريمة تقليدية ترتكب أو يسهل ارتكابها عبر الوسط الرقمي–، عن طريق إجراءات مراقبة الاتصالات الالكترونية، وحتى التفتيش والحجز بخصوص الشك في امتلاك أحد الأشخاص لهذه الأجهزة.

على أن يتوقف دور الهيئة التلقائي؛ عند حد ما ذكر أعلاه؛ فلا يمكنها القيام بالأعمال الوقائية، لا عن طريق مراقبة الاتصالات الالكترونية ولا بأي طريقة أخرى؛ بخصوص جرائم الوسط الرقمي الأخرى. كما أنها لا تقوم بأي دور كفاحي متصل بواقعة محددة حصرا؛ إلا إذا ما طلبت منها الجهات القضائية المختصة ذلك. الأمر الذي يعد مفهوما، سيما بالرجوع إلى الأحكام العامة بخصوص التحري والتحقيق المبينة سابقا، التي تجعل مرحلة التحري من اختصاص وإدارة وإشراف النيابة العامة، وإجراءات التحقيق القضائي؛ من اختصاص قضاء التحقيق.

الفرع الثاني: الأجهزة التقنية المساعدة على التحري والتحقيق في جرائم الوسط الرقمي

بالإضافة إلى الهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام والاتصال ومكافحتها، التي تعمل تحت إشراف القضاء وبتشكيلة تكاد تكون جامعة للطابع القضائي وشبه القضائي والإداري والتقني؛ نجد العديد من الأجهزة المساعدة الأخرى. التي تمارس أعمالا تقنية محضة، بطلب من الجهة المختصة بالتحري والتحقيق في جرائم الوسط الرقمي.

رجوعا إلى النصوص المختلفة؛ نجد أن القانون الجزائري يعتمد العديد من الأجهزة، التي تقدم المساعدة التقنية اللازمة للأجهزة المختصة بالتحري والتحقيق في جرائم الوسط الرقمي. وهي التي يمكن أن نقسمها على حسب جهة انتمائها؛ إلى أجهزة أمنية تابعة لجهازي الأمن والدرك الوطنيين(أولا) وأخرى مدنية لها اختصاص تقني رقمي بالأساس(ثانيا).

أولا: الأجهزة الأمنية ذات الطابع التقني المساعد على التحري والتحقيق في جرائم الوسط الرقمي

يمارس جهازي الأمن والدرك الوطنيين، بالإضافة إلى مهام وأعمال الشرطة القضائية المبينة والعديد من المهام سيما الأمنية منها؛ مهاما أخرى ذات طابع علمي وتقني مساعد للشرطة القضائية، المنطوي أساسا على الأعمال التي تمارسها مصالح الخبرة العلمية والتقنية. الأمر الذي نبينه بالتطرق إلى المخابر التقنية المساعدة على التحري والتحقيق في جرائم الوسط الرقمي، سواءً التابعة للأمن الوطني، أو المتصلة بالدرك الوطني.

1. المخابر التقنية التابعة للأمن الوطني: تعنى بعض الأجهزة التابعة للأمن الوطني؛ بممارسة المهام التقنية ذات البعد الرقمي، في إطار انجاز الخبرات المطلوبة منها من جهات التحري والتحقيق المختصة. الأمر الذي حددته المديرية العامة للأمن الوطني؛ في الأجهزة المختصة بذلك وفق هيكلة معينة، والمهام التقنية المسندة إلى هذه الأجهزة.

أ- هيكلة المخابر التقنية التابعة للأمن الوطني: يتشكل البعد العلمي والتقني في إطار الشرطة العلمية عموما؛ من مجموعة هياكل، تعمل تحت غطاء المديرية الفرعية للشرطة العلمية والتقنية، التابعة للمديرية المركزية للشرطة القضائية. حيث تمارس المديرية الفرعية للشرطة العلمية والتقنية مهامها؛ عن طريق المخبر المركزي والمخابر الجهوية، والمصلحة المركزية لتحقيق الشخصية والمحطات الجهوية، كما يضاف إليها المخبر التابع للمعهد الوطني للبحث في علم التحقيق الجنائي[1].

يمارس دور الخبير العلمي والتقني من قبل؛ المخبر المركزي المتواجد على مستوى الجزائر العاصمة، والمخبرين الجهويين المتواجدين على مستوى كل من قسنطينة ووهران[2]. على أن ترتبط المخابر الثلاث، في إطار التنسيق والتعاون الواجبين؛ لممارسة المهام المنوطة بهم. كما أنه يمارس الدور نفسه في إطار تحقيق الشخصية من قبل؛ مصلحة مركزية ومحطات إقليمية[3]. وهذا بالإضافة إلى المخبر المركزي التابع للمعهد الوطني للبحث في علم التحقيق الجنائي، الذي أنشأ سنة 2004، كمؤسسة عمومية مستقلة ذات طابع إداري، تحت وصاية وزارة الداخلية، والمعزز بمخابر جهوية تابعة له[4].

وعلى العموم؛ تمارس مخابر الشرطة العلمية مهام الخبرة؛ من خلال العديد من الفروع، الموزعة في إطار القسمين العلمي والتقني. حيث ينطوي القسم العلمي على ستة 06 فروع، المتمثلة في فرع البيولوجية والبصمة الوراثية، والكيمياء الشرعية، والمتفجرات والحرائق، والتسمم الشرعي، ومراقبة النوعية الغذائية، والطب الشرعي. وأما القسم التقني فيقوم على؛ فرع الأسلحة والقذائف، والخطوط والوثائق، والتحقيق الجنائي الصوتي، وعلم الأدلة الالكترونية[5].

يتضح من خلال ما ذكر أن المخابر ذات الصلة بانجاز الخبرات في إطار مكافحة جرائم الوسط الرقمي؛ تتصل بالقسم التقني من دون العلمي، وهو ما دفعنا للعنونة بالمخابر التقنية. وعلى العموم ينقسم

---

[1] **أنظر:** مليكة بهلول، (دور الشرطة العلمية والتقنية في الكشف عن الجريمة)، رسالة لنيل شهادة الدكتوراه، طلية الحقوق، جامعة الجزائر 1، الجزائر، 2013، ص 139.

[2] هذا بالإضافة إلى ثلاثة 03 مخابر جهوية أخرى على قيد الانجاز، المتصلة بمناطق؛ ورقلة وبشار وتمنغاست. **أنظر في ذلك:** حسين ربيعي، مرجع سابق، ص 177.

[3] **أنظر:** مليكة بهلول، المرجع نفسه، ص ص 139-142.

[4] **أنظر:** المواد 01 و02 و03 و3/07؛ مرسوم رئاسي رقم 04-432، مؤرخ في 29 ديسمبر 2004، يتضمن إنشاء المعهد الوطني للبحث في علم التحقيق الجنائي، (ج ر) عدد 84، صادر بتاريخ 29 ديسمبر 2004.

[5] **أنظر:** مليكة بهلول، المرجع نفسه، ص ص 147-179.

فرع علم الأدلة الالكترونية المستحدث سنة 2007؛ إلى قسمين بخصوص المخابر الجهوية، المنطوية على قسم استغلال الأدلة الرقمية الناتجة عن الحواسيب والشبكات، وقسم استغلال الأدلة الناتجة عن الهواتف النقالة. وثلاثة أقسام بالنسبة للمخبر المركزي، الذي يضم القسمين المذكورين بالإضافة إلى قسم تحليل الأصوات[1].

ب- مهام المخابر التقنية التابعة للأمن الوطني: تتلخص مهام المخابر التقنية التابعة للأمن الوطني؛ في تقديم الدعم التقني لأجهزة التحري والتحقيق. وذلك عن طريق البحث في المعطيات الرقمية -بيانات ومعلومات-، باستعمال الأجهزة والبرامج الرقمية المناسبة[2]. الأمر الذي يساعد أجهزة التحري والتحقيق على انجاز الأعمال الإجرائية اللازمة، ومنه الوصول إلى المعلومات الرقمية المؤسسة للتصرف في مرحلة التحري، أو الحصول على الدليل الرقمي في إطار التحقيق القضائي.

2. المخبر التقني التابع للدرك الوطني: بالإضافة إلى المخابر التقنية التابعة للأمن الوطني، يندرج في الإطار الهيكلي العام للدرك الوطني؛ أحد أهم وأبرز المخابر التقنية ذات الصلة بالمجال الجنائي، المنطوي على المعهد الوطني للأدلة الجنائية وعلم الإجرام. وهو الذي يضم في تشكيلته دائرة مختصة في جرائم الوسط الرقمي. الأمر الذي نبينه من خلال التطرق إلى هذه الدائرة؛ من حيث الهيكلة والمهام.

أ- هيكلة دائرة الإعلام الآلي والإليكترونيك: مع التزايد الملحوظ في الظاهرة الإجرامية عموما، ودخولها مرحلة التعقيد، سيما بعد الولوج إلى الوسط الرقمي، عملت الجهات المختصة في الجزائر سنة 2004؛ على المبادرة بإصدار مرسوم رئاسي يتضمن إحداث معهد وطني للأدلة الجنائية وعلم الإجرام، التابع للدرك الوطني. الذي أُصبغت عليه صفة المؤسسة العمومية المستقلة ذات الطابع الإداري، مع وضعه تحت وصاية وزارة الدفاع الوطني، ومنه خضوعه للأحكام المطبقة على المؤسسات العسكرية. وهو الذي لم يمنع النص بخصوصه؛ إمكانية إحداث ملحقات عند الحاجة بقرار من وزير الدفاع الوطني[3].

يتكون المعهد من مديريتي الأدلة الجنائية، والدراسات والبحوث الإجرامية، ومصلحتي التنظيم والمناهج، والإدارة والوسائل[4]. وتسند الخبرة الجنائية عموما، في إطار الإسناد التقني والعلمي؛ إلى دوائر مديرية الأدلة الجنائية، على حسب نوع الجريمة واختصاص الخبراء[5].

---

[1] **أنظر:** حسين ربيعي، مرجع سابق، ص 179.

[2] **أنظر:** وردة شرف الدين، مرجع سابق، ص 77 و78.

[3] **أنظر:** المواد 01 و02 و03؛ مرسوم رئاسي رقم 04-183، مؤرخ في 26 جوان 2004، يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، (ج ر) عدد 41، صادر بتاريخ 27 جوان 2004.

[4] **أنظر:** المادة 06؛ المرجع نفسه.

[5] **أنظر:** مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها للدرك الوطني، "الجريمة المعلوماتية ودور الدرك الوطني"، مرجع سابق، ص 20.

وفي إطار الخبرة التقنية المنجزة بعد الإسناد التقني المتصل بالتحري أو التحقيق في جرائم الوسط الرقمي؛ تحدد الجهة المختصة داخل المعهد الوطني للأدلة الجنائية وعلم الإجرام؛ في دائرة الإعلام الآلي والإليكترونيك. التي تتكون من ثلاثة 03 مخابر فرعية، تعنى بانجاز الخبرة التقنية على حسب الوقائع الرقمية محل التحري أو التحقيق، وهي مخبر الإعلام الآلي ومخبر الفيديو ومخبر الصوت[1].

ب- مهام دائرة الإعلام الآلي والإليكترونيك: يختص المعهد الوطني للأدلة الجنائية وعلم الإجرام عموما؛ بإجراء الخبرات العلمية والتقنية الجنائية المطلوبة من أجهزة التحقيق –الابتدائي والنهائي–، وذلك بغرض إقامة الدليل والتعرف على مرتكبي الجنايات والجنح. كما يقدم يد المساعدة العلمية والتقنية، أثناء سير التحريات؛ بغرض تجميع وتحليل الأشياء والآثار والوثائق المأخوذة من مسرح الجريمة[2].

أما بخصوص الخبرات التقنية المنجزة في إطار مواجهة جرائم الوسط الرقمي، من قبل دائرة الإعلام الآلي والإليكترونيك؛ فتنحصر المهام ذات الصلة في معالجة وتقديم كل دليل رقمي وتماثلي[3]، وتقديم المساعدة التقنية للمحققين في التحقيقات المعقدة. كما أنه بغرض ضمان الفعالية المستمرة؛ تسهر الدائرة على تأمين يقظة تكنولوجيا من أجل التحيين المستمر للمعارف، والتقنيات والطرق المستعملة في مختلف الخبرات العلمية[4].

وأنجزت دائرة الإعلام الآلي والإليكترونيك منذ البدء الفعلي لممارسة المهام سنة 2009[5]؛ العديد من الخبرات ذات الصلة بالتحري والتحقيق في جرائم الوسط الرقمي. حيث تم انجاز بين سنتي 2009 و2014 ما يعادل 1090 خبرة رقمية. موزعة على 32 خبرة سنة 2009، و94 سنة 2010، و120 سنة 2011، و251 سنة 2012، و268 سنة 2013، و325 سنة 2014[6]. وهو الأمر الدال صراحةً؛ على التزايد المستمر في ارتكاب جرائم الوسط الرقمي.

---

[1] **أنظر:** مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها للدرك الوطني، "الجريمة المعلوماتية ودور الدرك الوطني"، مرجع سابق، ص 22.

[2] **أنظر:** المادة 1/04-1و2؛ مرسوم رئاسي رقم 04-183، مرجع سابق.

[3] الأمر الذي يمكن القول أنه اختصاص أوسع من دراسة الحال. حيث سبق وفرقنا بين المجال الرقمي والمجال التماثلي. والقول بأن التعقيد والعجز الإجرائي القائد إلى انجاز دراسة الحال؛ يتصل بالمجال الرقمي دون التماثلي.

[4] **أنظر:** مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها للدرك الوطني، "الجريمة المعلوماتية ودور الدرك الوطني"، المرجع نفسه، ص 22.

[5] حيث تعد 2009 بمثابة سنة بداية المعهد للممارسة، وذلك رغم إنشائه بالنص التنظيمي سنة 2004. الأمر الذي برره المدير العام للمعهد، العقيد سي أحمد بورمانة في حوار صحفي مع "ديكانيوز" سنة 2014؛ بتكريس المدة الفاصلة بين سنتي 2004 و2009، للتكوين واقتناء المعدات العلمية والتقنية الضرورية. **أنظر في ذلك:** سيد أحمد بورمانة – المدير العام للمعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني ببوشاوي، "حوار لـ ديكانيوز: نطمح لتوسيع دائرة الاعتماد بإدراج طرق تحليلية لفائدة مخابر أخرى"، تاريخ النشر: 08 ديسمبر 2014، تاريخ التصفح: 24 أفريل 2018، الرابط: HTTP://AR.DKNEWS-DZ.COM/INDEX.PHP/NATION/ACTUALITE/25768-2014-12-08-17-29-20.

[6] **أنظر:** مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها للدرك الوطني، "الجريمة المعلوماتية ودور الدرك الوطني"، المرجع نفسه، ص 13.

ثانيا: الأجهزة المدنية ذات الطابع التقني المساعد على التحري والتحقيق في جرائم الوسط الرقمي

بعد التطرق إلى الأجهزة الأمنية ذات الطابع التقني المساعد على التحري والتحقيق في جرائم الوسط الرقمي، التي تقدم الخبرات اللازمة في ذلك إلى الجهات المختصة، نحاول أن نبرز من خلال العنصر محل الدراسة؛ الأجهزة المساعدة الأخرى التي أعطى لها القانون الصفة المذكورة، رغم عدم اتصالها بالجهات الأمنية المختلفة. وهي التي يمكن أن نحددها في إطار من يطلق عليهم القانون تسمية مقدمي الخدمات، ومن يمنحهم صفت المساعد للعدالة نظرا لكونهم من خبراء الوسط الرقمي.

1. مقدمو الخدمات: لا يمكن أن يتم استغلال النطاق الافتراضي لشبكة الاتصال دولية –كما بينا سابقا–؛ إلا إذا ما تم وضعها حيز الإتاحة من قبل من يسمون بمقدمي أو مزودي الخدمات. كما يتعذر في العديد من الأحيان القيام بالتحري والتحقيق في جرائم الوسط الرقمي؛ إلا إذا قدمت لهم المساعدة التقنية اللازمة من قبل واضعي الشبكة قيد الإتاحة. الأمر الذي نبينه من خلال التطرق إلى التعريف بمقدمي الخدمات، وعرض دورهم في التحري والتحقيق المتصل بجرائم الوسط الرقمي.

أ– التعريف بمقدمي الخدمات: قد يكون لعبارة مقدمي الخدمات؛ العديد من التعريفات والمعاني القانونية، على حسب نوع الخدمة المقدمة، التي تدور بين الاتصالات السلكية واللاسلكية عموما. حيث قد نعرف مقدم الخدمة من منطلق عام متصل بأي وسيلة اتصال تقليدية وحديثة، أو خاص مرتبط بالاتصالات التي توفرها شبكة الاتصال الدولية –المتصلة بأجهزة الإعلام الآلي– دون سواها.

رجوعا إلى القانون الجزائري؛ نجده قد عرف مقدم الخدمة؛ بـــ: "أي كيان عام أو خاص يوفر القدرة على الاتصال بالاعتماد على المنظومة المعلوماتية و/أو أنظمة الاتصالات، كما يضمن لفائدة ذلك معالجة وتخزين المعطيات المعلوماتية"[1]. وهو التعريف الواسع والشامل لكل وسائل الاتصال، والمعالجة والتخزين أيضا[2]. الأمر الذي ورد مختلفا في أغلب التعريفات، سيما الاتفاقية منها. حيث نجد الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، قد تطرقت للاتصالات المنجزة عبر تقنية المعلومات فقط، من دون المعالجة والتخزين[3]، على أن ذكرت اتفاقية بودابست ذلك –المعالجة والتخزين–، وحصرت الوسيلة في أنظمة المعالجة الآلية للمعطيات المعبر عنها بـــ "système informatique"[4].

---

[1] **أنظر:** المادة 1/02-د؛ قانون رقم 09-04، مرجع سابق

[2] كما سبق للمشرع تعريفه تحت تسمية "موفر الخدمة"، بالقانون رقم 2000-03 الملغى بالقانون 18-04 سابق الذكر. ولو بمفهوم واسع من حيث وسائل الاتصال، ومن دون التطرق إلى المعالجة والتخزين. **أنظر في ذلك:** المادة 1/08-8؛ قانون رقم 2000-03، مؤرخ في 05 أوت 2000، يتضمن القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، (ج ر) عدد 48، صادر بتاريخ 06 أوت 2000. الملغى بالمادة 189؛ قانون رقم 18-04، مرجع سابق.

[3] **أنظر:** المادة 1/02-2؛ مرسوم رئاسي رقم 14-252، مرجع سابق.

[4] وعلى العموم يعد التعريف المعتمد من المشرع الجزائري بالقانون 09-04 سابق الذكر؛ بمثابة النقل الحرفي من اتفاقية بودابست، مع إضافة وسيلة أنظمة الاتصالات الأخرى التقليدية إلى جانب أنظمة المعالجة الآلية للمعطيات. **أنظر في ذلك:**
- Art 01/1-c; Convention sur la cybercriminalité- Budapest, op.cit.

لا يدخل في إطار دراسة الحال؛ إلا مقدم الخدمة الذي يوفر الاتصالات المنجزة عبر شبكة الاتصال الدولية دون سواها و/أو يقوم بمعالجة وتخزين المعطيات الرقمية ذات الصلة. كما أن مقدم الخدمة في القانون الجزائري؛ تحكمه ضوابط وله أنواع دائرة بين الاستغلال للأغراض التجارية أو لسد الاحتياجات الخاصة[1]. حيث لا يرخص بإقامة خدمة الشبكة للأغراض التجارية؛ إلا للأشخاص المعنوية الخاضعة للقانون الجزائري، الممولة من أشخاص معنوية خاضعة للقانون العام و/أو أشخاص طبيعية من جنسية جزائرية[2]. كما قد يرخص للأشخاص المعنوية مهما كان نوعها وانتماؤها بلعب دور مقدم خدمة الشبكة، إذا ما رغبت في ربط هياكلها لاحتياجاتها الخاصة بموقع موصول مباشرة بالخارج[3].

ب- الدور المناط بمقدمي الخدمات في التحري والتحقيق المتصل بجرائم الوسط الرقمي: ألحق القانون بمقدمي الخدمات دور جد هام في إطار المساعدة على التحري والتحقيق في جرائم الوسط الرقمي. حيث يلزم القانون عموما –وطني ومقارن– مقدمي الخدمات؛ بتقديم المعطيات المعلوماتية المخزنة لديها بعد معالجتها، والتي توجد مبررات معقولة تدفع للقول بأنها ستساهم في كشف الحقيقة في التحقيق الجنائي الجاري[4]. وعلى العموم لمزودي الخدمة أهمية كبيرة في الكشف عن جرائم الوسط الرقمي ومتابعة وإدانة مرتكبيها، حيث قد تكون المعلومة الوحيدة المؤدية إلى اكتشاف الجرمية أو إثباتها[5].

أما بخصوص القانون الجزائري؛ فوضع أحكاما خاصة متصلة بدور مقدمي الخدمات في المساعدة على التحري والتحقيق بخصوص جرائم الوسط الرقمي. حيث ألحق بهم التزامات عامة وخاصة. تنجز العامة منها؛ قبل ارتكاب الجريمة؛ ويتوجب من خلالها القيام بحفظ؛ المعطيات التي تسمح بالتعرف على مستعملي الخدمة –متصل ومتصل به وموقع– والتجهيزات المستعملة وخصائصها، وتاريخ ومدة الاتصال، ومعطيات الخدمات التكميلية المستعملة ومقدمها. وهي التي وضع المشرع عدم الالتزام بها؛ تحت طائلة المسائلة الجنائية –والإدارية–، متى أدى ذلك إلى عرقلة سير التحريات القضائية[6].

---

[1] **أنظر:** المادتان 04 و3/05؛ مرسوم تنفيذي رقم 98-257، مرجع سابق.

[2] الأمر الذي يفهم منه أن القانون الجزائري يفرق بين مقدم الخدمة ومن يموله. حيث يجب أن يكون مقدم الخدمة شخص معنوي خاضع للقانون الجزائري، بغض النظر عن كونه وطني أو أجنبي. وأما من يموله فيجب أن يكون جزائري سواءً كان شخص معنوي خاضع للقانون العام أو طبيعي أو الاثنين معا، مع استثناء الشخص المعنوي الجزائري الخاص.

[3] فتقدم خدمة الشبكة في الجزائر؛ حصرا من قبل اتصالات الجزائر، بخصوص الثابتة منها. ومن طرف متعاملي الهاتف النقال "موبيليس Mobilis" و"جيزي Djezzy" و"أريدو Ooredoo"؛ بخصوص المتنقلة. على أن تقدم الخدمة بالأساس من قبل؛ "ايكوزنات Icosenet"، المنشأة سنة 1999. **أنظر في ذلك:** الموقع الرسمي لوزارة البريد والمواصلات السلكية واللاسلكية والتكنولوجيات والرقمنة، الجزائر، د ت ن، تاريخ التصفح: 02 أفريل 2018، الرابط: https://www.mpttn.gov.dz.

[4] **أنظر:** محمود محمد محمود جابر، مرجع سابق، ص 61 و62.

[5] حيث حصل في مصر سنة 2013؛ وأن تم الكشف عن جريمة خطف جنود وتصويرهم كأسرى ومن ثم بثهم عبر الشبكة. بالاعتماد على المعطيات المعالجة والمخزنة من مقدم خدمة الشبكة في مصر. **أنظر في ذلك:** مصطفى علي خلف، الضوابط الإجرائية لجرائم التقنية الحديثة-دراسة مقارنة، نادي القضاة، القاهرة، مصر، 2016، ص 291 و292.

[6] ويعاقب على ذلك بالحبس من ستة 06 أشهر إلى خمس 05 سنوات، وبالغرامة من 50.000 دج إلى 500.00 دج **أنظر في ذلك:** المادة 11؛ قانون رقم 09-04، مرجع سابق.

وأما الالتزامات الخاصة؛ فتقع على عاتق مقدمي الخدمات بعد ارتكاب الجريمة. وهي التي حددها المشرع سنة 2009، ورجع سنة 2016 ليضعها تحت طائلة المسؤولية الجنائية –والإدارية–[1]. ورغم الاختلاف في طرح الالتزامات بين النصين؛ إلا أننا نبرز شمولية ودقة النص الوارد سنة 2016 الذي حدد الالتزامات الخاصة في ضرورة تدخل مقدمي الخدمات، بعد إخطارهم من الهيئة الوطنية –المدروسة سابقا– أو بصدور أمر أو حكم قضائي بذلك. على أن يكون التدخل فوري لسحب أو تخزين المحتويات المتاحة أو جعل الدخول إليها غير ممكن، عندما تتضمن محتويات مجرمة. وكالتزام ثانٍ يتم التدخل لوضع الترتيبات السامحة بالسحب والتخزين. وهو الأمر الذي وضع المشرع عدم الالتزام به؛ تحت طائلة المسائلة الجنائية، سواءً مس بمسار التحري والتحقيق أم لا[2].

2. خبراء الوسط الرقمي: زيادةً عن مزودي الخدمات كأجهزة لها الطابع المدني المساعد للجهات المختصة بالتحري والتحقيق في جرائم الوسط الرقمي، نجد أن المشرع الجزائري –وغيره–؛ قد اعتمد على خبراء الوسط الرقمي. الأمر الذي يعد من مستلزمات مواجهة هذا النوع من الإجرام الحديث، خاصةً وأنها عملية تتطلب تضافر جهود أغلب الأجهزة المذكورة تقريبا. وهو ما نبينه بالتطرق إلى التعريف بخبراء الوسط الرقمي، ومن ثم تبيان آلية الاعتماد عليهم في القانون الجزائري[3].

أ– **التعريف بخبراء الوسط الرقمي:** انطلاقا من الفراغ التشريعي في تعريف الخبير الجنائي، وتأسيسا على الأعمال التي يقوم بها وطريقة التعيين والانجاز والأهداف من ذلك؛ قدم الفقه الجنائي سيما الجزائري منه العديد من التعاريف ذات الصلة، حيث اعتبر على أنه: "شخص له كفاءة علمية وفنية معينة يعطي رأيه والإيضاحات اللازمة التي تعد خارجة بحكم الاختصاص عن نطاق معارف القاضي"[4].

لا يعد عمل الخبير الجنائي؛ بمثابة الأمر المستحدث في الإطار الإجرائي. حيث يعتبر من الإجراءات التقليدية، التي تطلب المسرح الافتراضي تحديثها. فالخبير الفني المعرف أعلاه؛ يختلف بحسب التخصص ونوع الجريمة. الأمر الذي يدفع للقول بوجود خبير متخصص في جرائم الوسط الرقمي، الذي وضعت له العديد من التعاريف، على غرار اعتباره بأنه: "ذلك الشخص المؤهل علميا أو علميا والذي يتميز بالكفاءة والتخصص في التعامل مع شبكة الانترنت وأنظمة وبرمجيات الحاسب الآلي وفهم لغته"[5].

---

[1] **أنظر:** المادة 11؛ قانون رقم 09-04، مرجع سابق. **وأنظر أيضا:** المادة 394مكرر8 المضافة بالمادة 02؛ قانون رقم 16-02، مؤرخ في 19 جوان 2016، يعدل ويتمم أمر رقم 66-156، يتضمن قانون العقوبات، (ج ر)، عدد 37، صادر بتاريخ 22 جوان 2016.

[2] حيث يعاقب على مخالفة ذلك بالحبس من 01 سنة إلى ثلاث 03 سنوات، وبالغرامة من 2.000.000 دج إلى 10.000.000 دج أو بإحداهما. **أنظر في ذلك:** المادة 394مكرر8 المضافة بالمادة 02؛ قانون رقم 16-02، المرجع نفسه.

[3] على أن نستعرض الخبرة الرقمية كعمل إجرائي لازم بنوع من التفصيل والتدقيق؛ في الباب الثاني والأخير.

[4] **أنظر:** فضيل العيش، مرجع سابق، ص 350.

[5] **أنظر:** محمد كمال شاهين، مرجع سابق، ص 333.

ب- اعتماد خبراء الوسط الرقمي بخصوص التحري والتحقيق: يعد من أساسيات الإجراءات الجزائية؛ اتصال عمل الخبير بإجراءات التحقيق دون مرحلة التحري. فيستعان به في المسائل الفنية، المعترضة لعمل قضاء التحقيق الابتدائي والنهائي -قضاة التحقيق والحكم-[1]. الأمر الذي تراجع عنه المشرع الجزائري إن صح القول، حيث اعتمد لأول مرة من سماهم بالمساعدين المتخصصين لدى النيابة العامة، واحتفظ بالخبراء المنتدبين من قضاء التحقيق.

ب-1/ المساعدون المتخصصون كخبراء للوسط الرقمي لدى النيابة العامة: جاء في تعديل وتتميم قانون الإجراءات الجزائية الوارد سنة 2015؛ أنه يمكن لجهاز النيابة العامة الاستعانة في المسائل الفنية التي تعترضه بمساعدين متخصصين[2]. الأمر الذي يعد من المستجدات الإجرائية، التي فتحت لأول مرة أمام النيابة العامة؛ إمكانية الاستعانة بالمساعدين المتخصصين.

كما صدر سنة 2017؛ مرسوم تنفيذي ليبين كيفية تطبيق الإجراء المذكور أعلاه. حيث جاء فيه أنه يتم تعيينهم بالمجلس القضائي ويوضعون لدى النيابة العامة، فيوزعهم النائب العام على نيابات الجمهورية التابعة له حسب الحاجة. وهم المنتدبون من الإدارات العمومية، من بين من تتوفر فيهم الشروط القانونية، سيما حصولهم على شهادة الليسانس على الأقل، وخبرة مهنية لا تقل عن الخمس 05 سنوات في التخصص المطلوب. الأمر الذي يتم بالانتقاء من قبل لجنة خاصة تعين بقرار من وزير العدل. كما لا يمكنهم مزاولة المهام؛ إلا بعد تأدية اليمين القانونية واجتياز تكوين قانوني لمدة ثلاثة 03 أشهر[3].

على أن الإشارة بالمرسوم التنفيذي نفسه؛ إلى إمكانية استعانة الجهة القضائية التي لا تملك المساعد في التخصص المطلوب؛ بمن يمارسون مهامهم في جهات قضائية أخرى[4]؛ يدفع للقول بمحدودية المجالس التي ستضم المساعدين. الأمر الذي تم تأكيده فعلا بالقرار الوزاري الصادر سنة 2018[5]، المقرر لتخصص أنظمة المعالجة الآلية للمعطيات -من بين سبعة 07 تخصصات-. مع توزيع المساعدين على المجالس القضائية المتصلة بولايات؛ الجزائر العاصمة ووهران وقسنطينة وورقلة[6].

---

[1] **أنظر:** المادة 143؛ أمر رقم 66-155، مرجع سابق.

[2] **أنظر:** المادة 05 المضيفة للمادة 35مكرر؛ أمر رقم 15-02، مرجع سابق.

[3] **أنظر:** المواد من 02 إلى 08؛ مرسوم تنفيذي رقم 17-324، مؤرخ في 08 نوفمبر 2017، يتضمن شروط وكيفيات تعيين المساعدين المتخصصين لدى النيابة العامة وقانونهم الأساسي ونظام تعويضاتهم، (ج ر) عدد 67، صادر بتاريخ 15 نوفمبر 2017.

[4] **أنظر:** المادة 17؛ المرجع نفسه.

[5] **أنظر:** الجدول الملحق؛ قرار وزارة العدل، مؤرخ في 07 مارس 2018، يحدد قائمة التخصصات التي يعين فيها المساعدون المتخصصون والجهات القضائية المعنية، (ج ر) عدد 22، صادر بتاريخ 18 أفريل 2018.

[6] الأمر الذي قد يظهر المساعدين على أنهم يمارسون مهامهم في إطار الأقطاب المتخصصة المذكورة سابقا، والمتصلة أساسا بجرائم المساس بأنظمة المعالجة الآلية للمعطيات. إلا أن القول بإمكانية الاستعانة بهم من الجهات القضائية الأخرى؛ ينفي فرضية الأقطاب المتخصصة، التي تمارس الاختصاص المانع وفق ما بينا سابقا. وعليه يعد توزيعهم على المجالس الأربعة مجرد تنظيم هيكلي، كما أنهم يختصون في كل جرائم الوسط الرقمي ولا يقتصرون على جرائم المساس بالأنظمة.

لو نظرنا إلى التتميم الإجرائي المبين أعلاه نظرة سطحية؛ يمكن القول أنه بمثابة الإضافة الهامة، سيما بخصوص مواجهة العجز الإجرائي المذكور. لكن إفادتهم بالاختصاص الفضفاض، عبر المساهمة في مختلف مراحل الإجراءات بنص القانون وكل إجراءات الدعوى العمومية بنص التنظيم؛ يعد بمثابة الأمر الدافع للاستغراب. حيث سبق وأن بينا شمولية المراحل الإجرائية عن الدعوى العمومية، التي تبدأ بعد انتهاء التحري كأولى المراحل الإجرائية. ولم يتوقف التنظيم عند هذا الحد، بل أقر صراحةً بالتبعية المباشرة للنيابة العامة، والعمل على مساعدة الشرطة القضائية أثناء سير الدعوى العمومية[1].

نرى أن ما جاء به المشرع في هذا الصدد؛ يعتبر بمثابة الخلط الإجرائي، الذي نجد فيه أن الأصح؛ يتمثل في كون جهاز المساعدين المتخصصين تابعا للنيابة العامة، لتستعمله أثناء مرحلة التحري في مواجهة الكافة، وتستعين به أثناء التحقيق القضائي وهي خصم في الدعوى العمومية، لإثبات الجريمة بإبراز أدلة الاتهام. كما يمكنه أن يساعد الشرطة القضائية على التحري قبل تحريك الدعوى العمومية، ولا يمكنه ذلك أثناء التحقيق نظرا لتبعية الشرطة القضائية أثناء التحقيق؛ لقضاء التحقيق وليس للنيابة العامة.

ب-2/ ندب خبراء الوسط الرقمي من طرف قضاء التحقيق: يدخل إجراء ندب الخبير الرقمي من قضاء التحقيق عموما؛ في إطار الخبرة القضائية المنظمة بالأحكام التقليدية، مع الاختلاف اللازم في تكوين الخبير المتصل بالوسط الرقمي. فلا فرق بين الخبير التقليدي والخبير الرقمي؛ من حيث طريقة الندب وإسناد المهام. حيث يتم انتداب خبير أو أكثر بأمر من قضاء التحقيق تلقائيا أو بطلب من النيابة العامة والخصوم، من بين المسجلين في الجدول على مستوى المجلس القضائي، أو من غيرهم بأمر مسبب مع شرط أداء اليمين القانونية[2].

كما يمارس الخبير المعين بأمر القاضي المختص المهام الرقمية المسندة إليه؛ بنفسه أو بالاستعانة بمن يرى تدخلهم الفني ضروري، لكن بعد الترخيص لهم من القاضي نفسه وبالطريقة نفسها المعتمدة لتعيين الخبير الأول. على أن يقوم بكل إجراء فني مسند إليه بأمر التعيين، بما في ذلك الالتزام بالآجال[3].

كل الأجهزة الوطنية المذكورة من رئيسية ومساعدة؛ في العديد من الأحيان لا يمكنها أو تواجه جرائم الوسط الرقمي حتى وان اتحدت، سيما وأن مسرحها يتسم بالتعقيد، وأنه يصبغ عليها الوصف العالمي العابر للحدود الوطنية. الأمر الذي يتطلب في سبيل المواجهة الفعالة؛ التعامل مع الأجهزة الأجنبية، في إطار التعاون الدولي. وهو ما سنبينه في المبحث الثاني القادم بالدراسة.

---

[1] **أنظر:** المادة 35مكرر/2؛ أمر رقم 66-155، مرجع سابق. **وأنظر أيضا:** المادة 09؛ مرسوم تنفيذي رقم 17-324، مرجع سابق.

[2] **أنظر:** المواد 143 و144 و145 و147؛ أمر رقم 66-155، المرجع نفسه. **وأنظر أيضا:** عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، مرجع سابق، ص 368.

[3] **أنظر:** المواد 146 و148 و149؛ أمر رقم 66-155، المرجع نفسه. **وأنظر أيضا:** عبد الله أوهايبية، المرجع نفسه، ص 368 و369.

المبحث الثاني

الأجهزة الأجنبية المتعاونة على التحري والتحقيق في جرائم الوسط الرقمي

أخذت عملية المواجهة الإجرائية لجرائم الوسط الرقمي من حيث التحري والتحقيق، على غير العادة الطابع المعقد من حيث الأجهزة المختصة بها. حيث استقرت المواجهة الإجرائية المتصلة بالجرائم التقليدية؛ على اختصاص الأجهزة الوطنية الرئيسية المذكورة على التحري والتحقيق، التي قد تستعين في بعض الأحيان بأجهزة وطنية مساعدة، وعلى أكثر تقدير قد تلجأ بخصوص جرائم أو وقائع محددة كالجريمة المنظمة العابرة للحدود الوطنية؛ إلى التعاون مع بعض الأجهزة الأجنبية الدولية و/أو المقارنة.

لكن مع ظهور جرائم الوسط الرقمي وتطورها التقني والقانوني، أصبح العمل الإجرائي الوطني إن من الأجهزة الرئيسية لوحدها أو مع الاستعانة بالأجهزة المساعدة؛ بمثابة السبيل الإجرائي العاجز. خاصةً مع التسليم بعالمية هته الجرائم، انطلاقا من عالمية شبكة الاتصال الدولية. ومنه أصبح من الضروري على القانون الجزائري –عملا بالنهج القانوني الحديث– أن يفتح المجال أمام الأجهزة الوطنية المختصة بالتحري والتحقيق في جرائم الوسط الرقمي؛ للتعاون مع نظيرتها الأجنبية، سواءً الدولية أو المقارنة.

في سبيل تبيان ما ذكر، والتأسيس له بالنص الساري المفعول وطنيا، ومصدره من التطور القانوني الدولي والمقارن المتصل بحتمية التعاون الإجرائي الدولي[1] في مواجهة جرائم الوسط الرقمي؛ توجب علينا التطرق بالدراسة؛ إلى الماهية الخاصة لهذا التعاون الدولي وطريقة اعتماده من القانون الجزائري(مطلب أول)، ومن ثم العمل على تبيان نماذج عن الأجهزة الأجنبية[2] التي تتعاون مع نظيرتها الوطنية(مطلب ثانٍ).

المطلب الأول: التعاون الدولي على التحري والتحقيق في جرائم الوسط الرقمي

اعتمد القانون الجزائري كغيره من القوانين المقارنة؛ على إجراءات التعاون الإجرائي في المجال الجنائي عموما، حيث أقرها بخصوص تبادل الإنابات والمعلومات القضائية وتسليم المجرمين. الأمر الذي لم يظل على حاله، بل تطور مع نشأة وتطور جرائم الوسط الرقمي ومسرحها الافتراضي العالمي، فاكتسب التعاون الإجرائي الطابع الأساسي بعد أن كان لا يُعمل إلا بخصوص جرائم أو وقائع محددة. وهو ما يدل صراحةً على خصوصيته، التي اعتمدها القانون الجزائري بالطابع نفسه.

---

[1] اعتمدنا مصطلح التعاون الإجرائي، بدلا عن المصطلحات الأخرى المعتمدة وطنيا ودوليا، سيما التعاون القضائي والمساعدة القضائية المتبادلة. نظرا لعدم اقتصار التعاون الدولي في مجال التحري والتحقيق المتصل بجرائم الوسط الرقمي؛ على الأعمال المنجزة من الهيئات القضائية، فالتحري ينجز قبل تحريك الدعوى العمومية، كما يمكن تبادل المعلومات للغرض نفسه؛ من الهيئة الوطنية المدروسة، التي لها الطابع الإداري المستقل وليس القضائي ولا حتى الشبه القضائي.

[2] نستدل بمصطلح الدولي المضاف إلى التعاون الإجرائي، أو مصطلح الأجنبية المضاف إلى الأجهزة؛ على التعاون مع الأجهزة العالمية والإقليمية المنشأة بالاتفاق الجماعي، والتعاون الثنائي مع الأجهزة المحلية المنشأة بالقوانين المقارنة.

وعلى العموم يتصف التعاون الإجرائي على التحري والتحقيق في جرائم الوسط الرقمي؛ بالخصوصية المزدوجة، القائمة على خصوصية التعاون الإجرائي التقليدي كإجراء استثنائي، وخصوصية المسرح الجرمي الافتراضي الحامل للطابع العالمي. الأمر الذي نبينه من خلال التطرق إلى ماهية هذا التعاون الإجرائي الدولي(فرع أول)، وطريقة اعتماده من القانون الجزائري(فرع ثانٍ).

الفرع الأول: ماهية التعاون الدولي على التحري والتحقيق في جرائم الوسط الرقمي

يعد التعاون الإجرائي الدولي على التحري والتحقيق في جرائم الوسط الرقمي؛ بمثابة الوجه الحديث للتعاون الجنائي الدولي عموما. حيث يكتسب الماهية نفسها، إن من حيث المفهوم أو الإجراءات، إلا بخصوص المستجدات التي استلزمتها الضرورة التقنية للمسرح الرقمي الافتراضي. وحتى المناداة الرسمية –سيما منظمتي الأمم المتحدة والشرطة الأوروبية– بضرورة الاعتماد على التعاون الدولي لمواجهة جرائم الوسط الرقمي؛ أكدت على حتمية تكييفه مع الطبيعة التقنية المعقدة للوسط الرقمي[1].

وفي السياق نفسه؛ يمكن القول أنه أصبح للتعاون الإجرائي الدولي المتصل بمواجهة جرائم الوسط الرقمي ومسرحها الافتراضي الحديث؛ الطابع الخاص الذي يميزه عن نظيره التقليدي المعروف. وهو ما سنبينه من خلال التطرق إلى مفهومه الحديث(أولا)، والأعمال الإجرائية التي يقوم عليها(ثانيا)

أولا: مفهوم التعاون الدولي على التحري والتحقيق في جرائم الوسط الرقمي

أخذ التعاون الدولي على التحري والتحقيق في جرائم الوسط الرقمي؛ الطابع الخاص المنفصل عن التعاون الجنائي التقليدي، رغم كونه أحد صوره أو أنواعه بالأساس. وذلك نظرا لاتصاله بجرائم الوسط الرقمي ذات الظهور الحديث والشامل لأغلب –إن لم نقل جل– الجرائم التقليدية المعروفة. بالإضافة إلى ارتباطه بالمسرح الجرمي الافتراضي، الحامل للبعد العالمي. الأمر الذي نستعرضه من خلال التطرق إلى التعريف بهذا النوع الحديث من التعاون الدولي، ومن ثم تبيان الخصائص التي يمتاز بها.

1. تعريف التعاون الدولي على التحري والتحقيق في جرائم الوسط الرقمي: في العادة ما يتم التفرقة في التعريف بين التعاون الجنائي الدولي والمساعدة القضائية الدولية المتبادلة في المجال الجنائي، من منطلق أن التعاون الدولي أشمل من المساعدة القضائية، التي تعد أحد صوره، بالإضافة إلى التنسيق التشريعي والأمني[2]. الأمر الذي بإتباعه نعرف التعاون الدولي؛ على أنه: "تبادل العون والمساعدة وتضافر الجهود

---

[1] **أنظر:** فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، "دراسة شاملة عن مشكلة الجريمة السيبرانية والتدابير التي تتخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدي لها"، مرجع سابق، ص 14 و15. **وأنظر أيضا:** فريق الخبراء المعني بالجريمة السيبرانية، "مشروع المواضيع المطروحة للنظر في إطار دراسة شاملة بشأن تأثير الجريمة السيبرانية وتدابير التصدي لها"، مرجع سابق، ص 16 و17. **وأنظر كذلك:**

- Groupe de Travail Interministériel Sur la Lutte Contre la Cybercriminalité, op.cit, p 255 et 256.

[2] **أنظر:** سهيل الخييلي، (مدى إلزامية التعاون القضائي الدولي في المجال الجنائي-دراسة مقارنة)، رسالة لنيل شهادة الماجستير في القانون العام، كلية الدراسات القانونية العليا، جامعة عمان العربية للدراسات العليا، الأردن، 2006، ص 04.

المشتركة بين دولتين أو أكثر لتحقيق نفع أو خدمة أو مصلحة مشتركة في مجال التصدي لمخاطر الإجرام، والمجالات الأخرى ذات الصلة، مثل العدالة الجنائية والأمن المشترك، أو لتخطي مشكلات الحدود والسيادة التي قد تعترض الجهود الوطنية لملاحقة المجرمين وتعقب مصادر التهديد"[1].

أما المساعدة القضائية المتبادلة ذات الصلة بالمجال الجنائي، التي قلنا أنها تعد أحد صور التعاون الجنائي الدولي عموما؛ فوضع لها الفقه المختص العديد من التعاريف، التي تصب أغلبها في قالب التخصيص والتضييق من المفهوم العام للتعاون الدولي المبين أعلا. حيث تعرف عموما على أنها: "مجموعة من الوسائل التي بواسطتها تقدم إحدى الدول بواسطة سلطاتها العامة أو مؤسساتها القضائية المعاونة القضائية إلى سلطة التحقيق أو الحكم أو التنفيذ في دولة أخرى"[2].

يتضح من خلال التعريفين المذكورين أن الأخير منها –المتصل بالمساعدة القضائية الجنائية–؛ هو الأقرب إلى المدلول الذي أردناه في دراسة الحال تحت عنوان التعاون الدولي على التحري والتحقيق في جرائم الوسط الرقمي. وذلك نظرا لحصر التعاون على التحري والتحقيق دون سواها. وان كان يختلفان من حيث أن التعريف المذكور؛ يزيد في مفهومه مرحلتي المحاكمة والتنفيذ الجنائي، ويعبر عن إجراءات التحقيق دون التحري. كما أنه تنقصه خصوصية المواجهة الإجرائية لجرائم الوسط الرقمي، التي أدخلت فكرة التحري قبل ارتكاب الجريمة في بعض الجرائم، الأمر الذي أدى إلى ظهور تعاون من نوع حديث يتجاور السلطات القضائية وشبه القضائية التابعة لها؛ إلى السلطات الإدارية المستقلة، كالهيئة الوطنية السابقة بالدراسة.

وفي السياق نفسه؛ نجد العديد من التعاريف الخاصة بالمساعدة القضائية الدولية ذات الصلة بمواجهة جرائم الوسط الرقمي، من دون العمل بالمفهوم الضيق الذي حددناه أعلاه. حيث يعرف عموما على أنه: "كل إجراء قضائي تقوم به الدولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم"[3].

من خلال كل ما ذكر من تعريفات ذات الصلة بالتعاون الدولي والمساعدة القضائية بمفهومهما العام التقليدي، والتعريف المسند خصوصا إلى المساعدة القضائية المتصلة بمواجهة جرائم الوسط الرقمي، وخاصةً الطرح الذي بيناه بخصوص التفرقة بين كل ما ذكر، سيما وأننا نعتمد مصطلح مركب من

---

[1] **أنظر:** أحمد إبراهيم مصطفى سليمان، الإرهاب والجريمة المنظمة، دار الطلائع للنشر والتوزيع، القاهرة، مصر، 2006، ص 294.

[2] **أنظر:** سالم محمد سليمان الأوجلي، (أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوطنية -دراسة مقارنة)، رسالة لنيل شهادة الدكتوراه، كلية الحقوق، جامعة عين شمس، القاهرة، مصر 1997، ص 425. **نقلا عن:** وردة شرف الدين، مرجع سابق، ص 374.

[3] **أنظر:** حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت-دراسة مقارنة، دار النهضة العربية، القاهرة، مصر، 2009، ص 644.

التعاون الدولي ومحله المنطوي على التحري والتحقيق في جرائم الوسط الرقمي بمفهومها الخاص. يمكن أن نقدم تعريف خاص بالتعاون محل الدراسة، حيث نقول أنه: "مساعدة إجرائية متبادلة، بين السلطات المختصة لدولتين أو أكثر، بغرض انجاز أعمال الوقاية والمكافحة في إطار التحري والتحقيق المتصلين بجرائم الوسط الرقمي".

وعلى العموم يقوم التعاون الدولي المتصل بالتحري والتحقيق في جرائم الوسط الرقمي؛ على العديد من الأحكام والأعمال التي سنراها في العنصر الموالي بالدراسة. المبينة بالاتفاقيات والنصوص الوطنية ذات الصلة بجرائم الوسط الرقمي[1]، على غرار الاتفاقيات الثنائية بين الدول وما جاءت به الاتفاقية الأوروبية للجريمة السيبرانية –بودابست لسنة 2001–[2]، والاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010[3]. بالإضافة إلى النظام الأساسي الذي تقوم عليه المنظمات الشرطية الدولية والإقليمية، على غرار الشرطة الدولية والأوروبية والإفريقية[4].

2. خصائص التعاون الدولي على التحري والتحقيق في جرائم الوسط الرقمي: ينفرد التعاون الدولي المتصل بالتحري والتحقيق في جرائم الوسط الرقمي؛ بالعديد من السمات القانونية، التي تميزه عن التعاون التقليدي باختلاف صوره، وذلك رغم اعتباره من بين هذه الصور. الأمر المكتسب أصلا من الطبيعة الافتراضية المعقدة للوسط الرقمي كمسرح جرمي حديث. وعلى العموم نجد أن التعاون محل الدراسة؛ يمتاز بأهميته التي أصبغت عليه الطابع الضروري، كما تعترضه الكثير من المعوقات، ويعد الموازن بين سمو القانون الدولي وحماية سيادة الدول.

أ- الطابع الضروري للتعاون الدولي المتصل بالتحري والتحقيق في جرائم الوسط الرقمي: يكتسي التعاون الدولي الطابع الضروري واللازم؛ في المواجهة الإجرائية المتصلة بأغلب جرائم الوسط الرقمي.

---

[1] وهذا بغض النظر عن الاتفاقيات التقليدية الأخرى المبينة لأحكام وآليات المساعدة القضائية المتبادلة، على غرار المعاهدة النموذجية للأمم المتحدة بشأن تبادل المساعدة في المسائل الجنائية، المعتمدة بقرار الجمعية العامة رقم 1117/45 بتاريخ 14 ديسمبر 1990. **أنظر في ذلك:** أبو المعالي محمد عيسى، "الحاجة إلى تحديث آليات التعاون الدولي في مجال مكافحة الجريمة المعلوماتية"، ورقة عمل مقدمة إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، ليبيا، 28 أكتوبر 2009، ص 04.

[2] الاتفاقية الأوروبية التي تعد أول وأهم اتفاقية في هذا الصدد، ومنها تستشف أغلب الاتفاقيات الثنائية والجماعية الأخرى ذات الصلة بمجال الدراسة. حيث نظمت التعاون الدولي بموجب الفصل الثالث تحت العنوان نفسه، وذلك من حيث التطرق بـ 12 مادة؛ إلى تسليم المجرمين والمساعدة القضائية المتبادلة. **أنظر في ذلك:**

- Art(s) de 23 à 35; Convention sur la cybercriminalité- Budapest, op.cit.

[3] الاتفاقية العربية التي صدقت عليها الجزائر سنة 2014 -كما بينا سابقا-، ومنها تستشف الأحكام الخاصة بالتعاون الإجرائي بخصوص التحري والتحقيق في جرائم الوسط الرقمي. حيث نظمت ذلك من خلال فصلها الرابع المكون من 14 مادة، تحت عنوان المساعدة القانونية والقضائية. **أنظر في ذلك:** المواد من 30 إلى 43؛ مرسوم رئاسي رقم 14-252، مرجع سابق.

[4] وهي الأجهزة الشرطية –العالمية أو الإقليمية- التي سنتطرق لها فيما هو قادم بالدراسة المفصلة، من حيث الهيكلة والمهام المتصلة بالتعاون الدولي مع الجهات الوطنية المختصة -الجزائرية- على التحري والتحقيق في جرائم الوسط الرقمي.

الأمر الناتج عن الخصائص التي تتصف بها الجرائم نفسها ومسرحها الافتراضي المعقد، سيما البعد العالمي العابر للحدود الوطنية. بالإضافة إلى الصعوبات الإجرائية سابقة الذكر، خاصةً العقبات التي تواجهها الأجهزة الوطنية المختصة بالتحري والتحقيق، وما تنتجه من صعوبة بخصوص اكتشاف الجريمة وإثباتها بالدليل الرقمي اللازم، الذي يتطلب التدخل الفوري والمناسب على غرار حفظ المعلومات[1].

كما ترى العديد من الدراسات أن التعاون الدولي يكتسي طابع الأهمية والضرورة؛ نظرا لكونه السبيل السلس الذي تتبعه الأجهزة الوطنية المختصة بالتحري والتحقيق، من أجل مواجهة عالمية جرائم الوسط الرقمي، وسهولة إخفاء الهوية وتدمير وإتلاف الدليل الرقمي المترتب أثناء ارتكاب الجريمة وبعدها. الأمر الذي يولد الصعوبة المتصلة بالمواجهة الوطنية المنعزلة عن نظيرتها الدولية والمقارنة[2].

وفي الإطار نفسه؛ تتصل الأهمية والضرورة الملحة للتعاون الإجرائي على مواجهة جرائم الوسط الرقمي؛ بالعديد من النقاط الفرعية، منها ما وردت بخصوص التعاون القانوني والقضائي العام، ومنها ما لها علاقة مباشرة وخاصة بالتحري والتحقيق دون سواها من الأحكام القانونية. حيث يعتبر هذا النوع من التعاون بمثابة الخطوة نحو تدويل القانون الجنائي، فالتعاون والتنسيق الجنائي بين الدول من شأنه أن يقارب بين النصوص الموضوعية والإجرائية المقارنة[3].

كما يعتبر التعاون الدولي محل الدراسة على وجه الخصوص؛ بمثابة العلاج المناسب لتلافي فكرة الملاذ الرقمي –أو الملاذ الالكتروني–. الذي ينطوي على استعمال شبكة الاتصال الدولية، من أجل ارتكاب الجرائم ذات الصلة، مع العمل على التخفي الرقمي، عن طريق إخفاء الهوية وأثار الدليل الرقمي بالسهولة المبينة سابقا[4]. كما أن البعد العالمي لجرائم الوسط الرقمي ومسرحها الافتراضي، بكل سماته ونتائجه المبينة؛ يدفع إلى البحث عن التنسيق الدائم بيم الأجهزة الدولية والمقارنة، بغرض اتخاذ الإجراءات الرقمية المناسبة في الوقت المناسب، وحفظ المعلومات المنطوية على الدليل الرقمي[5].

وعلى العموم يمكن القول؛ أن الأهمية أو الضرورة المذكورة؛ تتطلب أن تتعامل الجهات الدولية والمقارنة المختصة بالسرعة اللازمة، وعدم مقابلة طلبات المساعدة الإجرائية بالرفض أو الرد البطيء، مع ضمان احترام القانون والمعاملة بالمثل.

---

[1] **أنظر:** علي حسن الطوالبة، "التعاون الدولي في مجال مكافحة الجرائم الالكترونية"، مركز الإعلام الأمني، وزارة الداخلية، مملكة البحرين، د ت، ص 02. متوفر عبر الرابط:
https://www.policemc.gov.bh/research/cyber-economic-and-criminal-crimes/.

[2] **أنظر:** محمد كمال شاهين، مرجع سابق، ص 210.

[3] **أنظر:** المرجع نفسه، ص 211.

[4] **أنظر:** المرجع والصفحة نفسهما.

[5] **أنظر:** فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، "دراسة شاملة عن مشكلة الجريمة السيبرانية والتدابير التي تتخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدي لها"، مرجع سابق، ص 14.

ب- معوقات التعاون الدولي على التحري والتحقيق في جرائم الوسط الرقمي: يكتسي التعاون الدولي على التحري والتحقيق المتصل بجرائم الوسط الرقمي؛ الطابع المعقد الناتج عن المعوقات والصعوبات العديدة المعترضة لانجازه. التي منها ما هي عامة قد تتعلق بالشق الموضوعي الوطني لجرائم الوسط الرقمي، أو بنطاقها الدولي الاتفاقي، ومنها ما هي خاصة لها علاقة مباشرة بالتحري والتحقيق في جرائم الوسط الرقمي على وجه الخصوص. وعليه نتطرق فيما يلي إلى الطابع المعقد محل الطرح؛ من حيث تبيان المعوقات العامة والخاصة.

ب-1/ المعوقات العامة للتعاون الدولي على التحري والتحقيق في جرائم الوسط الرقمي: أكدت دراسة قام بها فريق الخبراء المعني بجرائم الوسط الرقمي التابع للأمم المتحدة، بعد التسليم بضرورة اللجوء إلى التعاون الدولي في مجال التحري والتحقيق؛ على أن هذا التعاون تعترضه العديد من المعوقات المرتبة للتعقيد المدروس، وهي المنطوية أساسا على الاختلافات القائمة في التشريعات الوطنية من جهة، وقلة الاتفاقيات الدولية الخاصة بالتعاون الإجرائي لمواجهة جرائم الوسط الرقمي من جهة أخرى[1].

ومن خلال ذلك يمكن القول أن المعوقات العامة محل الطرح؛ تنطوي على ثلاثة نقاط. وهي المتصلة بعدم التناسق التجريمي بين النصوص الوطنية أولا، وتنازع الاختصاص القانوني بين النصوص المقارنة ثانيا، وقلة الاتفاقيات الدولية الخاصة بالتعاون الإجرائي على مواجهة جرائم الوسط الرقمي ثالثا. فمن حيث تخلف التناسق التجريمي؛ سبق وأن بينا أنه من خصائص جرائم الوسط الرقمي عدم الاتفاق على مفهوم عام لها. الأمر الذي أدى إلى الاختلاف في تحديد السلوكيات الرقمية المجرمة، وتحديد أركان الجريمة للسلوكيات المجرمة، وكذلك تكييفها القانوني[2]. ومنه لا يمكن لدولة أن تتعاون إجرائيا مع دولة أخرى لمواجهة سلوك رقمي؛ غير مجرم لدى الدولة المطلوب التعاون معها[3].

أما بخصوص تنازع الاختصاص القانوني؛ فيعد من أهم المتلازمات القانونية لجرائم الوسط الرقمي. حيث بمجرد وصف هذه الجرائم على أنها ذات بعد عالمي عابر للحدود الوطنية؛ تبرز إشكالية تحديد القانون الواجب التطبيق ومنه الجهة القضائية المختصة. المتصلة أساس بالبعد الإقليمي دون الشخصي والعيني. فالدولة الراغبة في طلب يد العون الإجرائي من منطلق أنها المعنية إقليما بتحقق أثر الجريمة الرقمية؛ تجد نفسها تائهة بين دولة ارتكاب السلوك الإجرامي والدول التي مر عبرها هذا السلوك قبل

---

[1] **أنظر:** فريق الخبراء المعني بالجريمة السيبرانية، "مشروع المواضيع المطروحة للنظر في إطار دراسة شاملة بشأن تأثير الجريمة السيبرانية وتدابير التصدي لها"، مرجع سابق، ص 16.

[2] **أنظر:** يوسف صغير، مرجع سابق، ص 133 و134.

[3] الأمر الذي نضرب بخصوصه مثال سبق طرح سياقه الموضوعي في المبحث الأول من الدراسة. حيث لا يمكن للجهات الفرنسية المختصة بالتحري والتحقيق في جرائم الوسط الرقمي؛ أن تطلب يد العون من نظيرتها الجزائرية بخصوص سلوك نسخ معلومة رقمية، المجرم في القانون الفرنسي دون الجزائري. **أنظر في ذلك:** المادتان 394 مكرر و394 مكرر1؛ أمر رقم 66-156، مرجع سابق. **وأنظر أيضا:** - Arts 323-1 et 323-2; code pénale français, Partie législative, op.cit.

تحقق النتيجة[1]. خاصةً بالرجوع إلى فكرة الاختلاف التجريمي من دولة لأخرى. ولو أن المنطق الجنائي السليم؛ يفرض التعاون بين جميع الدول المذكورة، سيما صاحبة قاعدة المعلومات الرقمية، على أن تنحصر المتابعة الجنائية بين بلدي ارتكاب السلوك وتحقق النتيجة، والأولوية للسباقة بينهما.

كذلك فيما يخص قلة الاتفاقيات الدولية الخاصة بالتعاون الإجرائي على مواجهة جرائم الوسط الرقمي، التي تعد من أهم الصعوبات المرتبة للتعقيد المدروس. حيث بمجرد التطرق إلى المظاهر العامة المذكورة أعلاه؛ يتبادر إلى الذهن غياب التنظيم الدولي الاتفاقي للتعاون المدروس، فلو وجد هذا التنظيم لما تحدثنا عن قلة التناسق التجريمي وتنازع الاختصاص. وعلى العموم تكتفي العديد من الدول؛ على العمل بالاتفاقيات الثنائية على حساب الجماعية –إن وجدت–، التي في أغلبها تعد عاجزة للعديد من الأسباب، سيما أنها غير كافية ولا تواكب التطور الديناميكي السريع للوسط الرقمي[2]. والأكثر إبرازا لصعوبة التعاون الدولي الإجرائي المتصل بجرائم الوسط الرقمي؛ ينطوي على كونه ينجز انطلاقا من اتفاقيات ثنائية عامة، التي تحث على التعاون الجنائي المتصل بمختلف الجرائم الممكن التعاون بشأنها[3].

ب–2/ المعوقات الخاصة للتعاون الدولي على التحري والتحقيق في جرائم الوسط الرقمي: إضافة إلى المعوقات العامة المذكورة، نجد أن الطابع المعقد للتعاون الإجرائي المتصل بجرائم الوسط الرقمي؛ يصبح أكثر تعقيدا إذا ما نظرنا إليه بنوع من التخصيص الإجرائي الرقمي المحض. المتصل أساسا بغياب التنسيق والتناسق الإجرائي، والصعوبة في انجاز مرحلة التحري الوقائي والكفاحي من خلال تبادل المعلومات الرقمية، والصعوبة ذات الصلة بالتحقيق القضائي من خلال الانابات القضائية.

يدفع الطابع الخاص لجرائم الوسط الرقمي؛ من حيث عالميتها من جهة وسرعة تنفيذها وإخفاء دليلها الرقمي من جهة أخرى، إلى القول بأن أي خلل في التنسيق السريع بين الجهات المختصة في الدول المتعاونة؛ ينتج لا محال حالة عدم جدوى كل إجراءات التعاون نظرا لفقدان الدليل الرقمي. سيما وأن أي تعاون من هذا النوع؛ يجب أن يمر عبر الطريق الدبلوماسي المتصف بالتعقيد والبطء[4].

كما أن اختلاف النظم الإجرائية المقارنة المتصلة بالتحري والتحقيق في جرائم الوسط الرقمي؛ تنشئ نوعا من عدم التناسق القانوني، بين الأحكام الإجرائية المتبعة في الدول المتعاونة. حيث يمكن أن نقع في

---

[1] **أنظر:** يوسف صغير، مرجع سابق، ص 134 و135 و136. **وأنظر أيضا:** يحي محمود عيشان، مرجع سابق، ص ص 117-123.

[2] **أنظر:** يحي محمود عيشان، المرجع نفسه، ص ص 113-117.

[3] وفي إطار التسليم بالاعتماد على الاتفاقيات العامة التقليدية، نظرا لغياب نظيرتها الخاصة بالتحري والتحقيق في جرائم الوسط الرقمي؛ تنص أرقام صادر عن الأمم المتحدة؛ بأن الاعتماد على الاتفاق الثنائي لتحقيق ذلك بلغ نسبة 60 %، بمقابل نسبة 20 %، المتصلة بالاعتماد على الاتفاق الجماعي. **أنظر في ذلك:** فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، "دراسة شاملة عن مشكلة الجريمة السيبرانية والتدابير التي تتخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدي لها"، مرجع سابق، ص 14 و15.

[4] **أنظر:** وردة شرف الدين، مرجع سابق، ص 372.

عدم اعتماد بعض القوانين لإجراءات معينة، أو اعتمادها من دون إحداث الأثر الايجابي، أو اعتماد الدولة الطالبة للمعاونة على نظام الإثبات المقيد، والدولة المنفذة للمساعدة على نظام الإثبات الحرة...الخ. الأمر الذي ينطبق على العديد من الإجراءات، سيما التسليم المراقب والعمليات المستمرة[1] والمراقبة الالكترونية...الخ[2].

وفي السياق الإجرائي نفسه، يعترض أيضا التعاون الدولي على التحري والتحقيق في جرائم الوسط الرقمي؛ ما هو متصل بتبادل المعلومات الرقمية في إطار تنفيذ مرحلة التحري، السابقة بالذكر والشرح من حيث أجهزتها المختصة بها ونطاقها الإجرائي. حيث ندرة وضعف قنوات الاتصال بين معظم الأجهزة المقارنة، يعد بمثابة أهم المعوقات محل الدراسة. فالاتصال بين جهات التحري المقارنة؛ يهدف أساسا إلى جمع المعلومات التي تفيد في سير مرحلة التحري والتصرف في نتائجها[3].

لا يقتصر تبادل المعلومات الرقمية المتصلة بمرحلة التحري؛ على الأجهزة المختصة به في الدول المعنية بالجريمة فقط، بل تعد كل الجهات المقارنة والدولية التي لها الإمكانية على المساعدة في تقديم المعلومات؛ معنية بذلك بمجرد التقدم إليها بطلب المساعدة، ومع احترام الاتفاق الجماعي أو الثنائي الذي يحث على ذلك. وهو ما تم التأكيد عليه في وقت سابق بمناسبة انعقاد مؤتمر الاتحاد الدولي للاتصالات في إطار الأمم المتحدة، الذي حث على ضرورة تشكيل فريق دولي قانوني لمواجهة هذا الشأن وضمان تبادل المعلومات الأمنية والجرمية[4].

وكذلك بخصوص الإنابات القضائية المتصلة بإجراءات التحقيق القضائي خاصةً، التي تعترضها العديد من العقبات والصعوبات، المعقدة من عملية التعاون الدولي المتصل بها. حيث تسير وفق النهج نفسه المذكور أعلاه، المتصف بالبطء والتعقيد من حيث وجوب مرورها عبر الطريق الدبلوماسي، وصعوبة التعامل مع الفوارق الهيكلية والبشرية العلمية والتقنية واللغوية بين الدول المتعاونة. ولو أن بعض الدول تجاوزت ذلك، عن طريق الاتفاق الثنائي. حيث يمكن أن يتم تبادل الإنابات القضائية شفاهة في حالة الاستعجال الملح، وبطريقة مباشرة بين الأجهزة المختصة[5].

---

[1] **أنظر:** يوسف صغير، مرجع سابق، ص 134.

[2] لو أخذنا المراقبة الالكترونية على سبيل المثال، نجد أن منها ما تفرض على المتهم من قضاء التحقيق، أثناء إجراءات التحقيق الابتدائي. فلو فرضنا أن الجهة الطالبة تابعة للقانون الفرنسي والمطلوب منها خاضعة لنظيره الجزائري؛ لوقعنا في حالة من التضارب التشريعي. حيث أن المشرع الجزائري وضعها كمجرد وسيلة متصلة بالمراقبة القضائية، فتضمن تنفيذها. وأما نظيره الفرنسي فلا يعتبرها كذلك، حيث أقرها كإجراء منفصل، يسميه بالإقامة الجبرية تحت المراقبة الالكترونية، وهي التي لا تعد ضمانا لتنفيذ المراقبة القضائية ولا بديلا عن الحبس المؤقت. **أنظر في ذلك:** المادة 125 مكرر 5/1؛ أمر رقم 66-156، مرجع سابق. **وأنظر أيضا:** Art 137; code de procédure pénale français, Partie législative, op.cit. -

[3] **أنظر:** يحي محمود عيشان، المرجع نفسه، ص 91.

[4] **أنظر:** المرجع نفسه، ص 93.

[5] **أنظر:** يوسف صغير، المرجع نفسه، ص 138 و139.

ج- الطابع الموازن للتعاون الدولي على التحري والتحقيق في جرائم الوسط الرقمي: بالإضافة إلى الخصائص السابقة بالذكر؛ نجد أنه للتعاون الدولي محل الدراسة خاصية ينفرد بها عن أغلب الإجراءات القانونية الجامعة بين القانونين الدولي والوطني، المنطوية على صفة الموازن بين سيادة الدول وسمو القانون الدولي. حيث في العادة ما تثار إشكالية سيادة الدول على إقليمها وشعبها، التي تحولت إلى الطابع النسبي بعد أن بلغ التنظيم الدولي مرحلة المجتمع الدولي المعاصر. فدائما ما ينظر إلى أي اتفاق دولي ثنائي أو جماعي على أنه تقييد من سيادة الدولة.

لو نظرنا إلى التعاون الدولي على التحري والتحقيق في جرائم الوسط الرقمي، بالنظرة السطحية الفوقية؛ لوجدنا أنه قائم على الاتفاق الدولي ومنه هو ينتقص من سيادة الدول، ولا مجال للحديث عن لعبه للدور الموازن المذكور. سيما وأنه يقوم على أربعة مصادر قانونية وضعتها دراسة للأمم المتحدة، التي تتذيلها النصوص الوطنية، الواردة بعد الاتفاقيات الدولية الجماعية، ذات الطابع العالمي وبعدها الإقليمي، ومن ثم الاتفاقيات الثنائية[1].

إلا أن الأمر لا يعد كذلك بخصوص التعاون محل الطرح. حيث عالمية شبكة الاتصال الدولية وتبعيتها لدولة المنشأ ودول الاتصال السابق -كما سبق بيانه-؛ يفتح المجال أمام فرضية ولوج أي جهة أجنبية مختصة بالحري والتحقيق إلى أي نطاق افتراضي وطني، من دون ترخيص من الجهات المختصة وطنيا. الأمر الذي يعد بمثابة الوجه الرقمي الحديث لأعمال الاعتداء على سيادة الدول. الذي لا يمكن مواجهته إلا بالتعاون الدولي، الضامن إلى حدٍ ما احترام السيادة الوطنية، من خلال الالتزام باتفاق التعاون المبرم، عن طريق الولوج بصفة رسمية وبعد الإخطار وتلقي الرد بالقبول، مع التأكيد على العمل المشترك والمعاملة بالمثل[2].

ثانيا: إجراءات التعاون الدولي على التحري والتحقيق في جرائم الوسط الرقمي

بعد التسليم بالطابع العالمي لجرائم الوسط الرقمي؛ كان لزاما التعامل معها على أنها ذات البعد العابر للحدود الوطنية من حيث إجراءات التحري والتحقيق، سيما بخصوص التعاون الدولي الإجرائي. الأمر الذي أنجز من خلال تفعيل الإجراءات التقليدية، المنظمة بالاتفاقيات الجماعية والثنائية السارية. التي ثبت أنها قاصرة وتحتاج لإجراءات حديثة تكملها. ومنه جاءت اتفاقية بودابست لسنة 2001، كأول صك دولي بخصوص جرائم الوسط الرقمي، لينظم الأمر وفق الطبيعة الرقمية الافتراضية. فأصبح ينجز التعاون الدولي الإجرائي على جرائم الوسط الرقمي؛ وفق أحكام عامة تقليدية، وأخرى خاصة حديثة.

[1] **أنظر:** فريق الخبراء المعني بالجريمة السيبرانية، "مشروع المواضيع المطروحة للنظر في إطار دراسة شاملة بشأن تأثير الجريمة السيبرانية وتدابير التصدي لها"، مرجع سابق، ص 17.

[2] **أنظر:** فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، "دراسة شاملة عن مشكلة الجريمة السيبرانية والتدابير التي تتخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدي لها"، مرجع سابق، ص 15.

1. الإجراءات العامة للتعاون الدولي على التحري والتحقيق في جرائم الوسط الرقمي: يمكن من خلال الرجوع إلى أهم الاتفاقيات الدولية التقليدية المتصلة بمختلف الجرائم المتعاون بشأنها[1]، والدراسات الفقهية ذات الصلة؛ الوقوف على أهم الإجراءات العامة المعمول بها بخصوص التعاون الدولي الجنائي في شقه الإجرائي، المعمول بها بخصوص التعاون على التحري والتحقيق في جرائم الوسط الرقمي. التي يمكن أن نحددها في تبادل المعلومات والإنابات، ونقل الإجراءات، والحجز والمصادرة، وتسليم المجرمين.

أ- **تبادل المعلومات والإنابات:** ينطوي أهم ما يقوم عليه التعاون الدولي الإجرائي التقليدي؛ على تبادل المعلومات الوقائية والكفاحية في إطار مرحلة التحري، وتبادل الإنابات القضائية أثناء سير إجراءات التحقيق القضائي. حيث تأخذ عملية تبادل المعلومات العديد من الصور، التي قد تتصل بكل ما يخص أحد رعايا الدولة الموجود في الخارج، الذي ارتكب الجريمة في الدولة الطالبة للمعلومات، كما قد يتعلق طلب المساعدة بالمعلومات المتصلة بالواقعة المجرمة، ومتابعة النشاط الإجرامي[2].

ونظرا لأهمية تبادل معلومات جرائم الوسط الرقمي، حث مؤتمر الأمم المتحدة السادس لمنع الجريمة ومعاملة المجرمين؛ على ضرورة تطوير التبادل المنهجي للمعلومات ومنه التوصية بإنشاء قاعدة معلوماتية لإعلام الدول الأطراف بالاتجاهات العالمية ذات الصلة[3]. وذلك بغض النظر عن الأجهزة الشرطية المعروفة، على غرار منظمة الشرطة الدولية، التي من أبرز مهامها التشجيع على التعاون الدولي بين مختلف الأجهزة الشرطية الوطنية والدولية، عن طريق تجميع المعلومات وتبادلها[4].

ولا يقف التعاون الدولي عند الحد الشرطي، حيث يمتد إلى غاية إمكانية تبادل الإنابات القضائية -التي قبولها لا يعد لازما-. التي لا تختلف كثيرا عن تبادل المعلومات، إلا من حيث بعض الجزئيات، خاصةً وأنها تنجز بعد تحريك الدعوى العمومية، تحت إمرة ورقابة قضاء التحقيق المختص[5].

---

[1] التي نجد منها العالمية والإقليمية. فمن أهم العالمية منها؛ اتفاقية الأمم المتحدة لمكافحة الاتجار غير المشروع في المخدرات والمؤثرات العقلية لسنة 1988، واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لسنة 2000، وبروتوكوليها المكملين المتصلين بمكافحة تهريب المهاجرين، ومنع وقمع ومعاقبة الاتجار بالأشخاص وبخاصة النساء والأطفال. واتفاقية قمع تمويل الإرهاب لسنة 1999، واتفاقية الأمم المتحدة لمكافحة الفساد لسنة 2003. وأما بخصوص الاتفاقيات الإقليمية؛ فنجد أهمها اتفاقية الرياض العربية للتعاون القضائي لسنة 1983، واتفاقية التعاون القانوني والقضائي بين دول اتحاد المغرب العربي لسنة 1991، والاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية لسنة 2010، واتفاقية منظمة الوحدة الإفريقية لمنع الإرهاب ومكافحته لسنة 2001. **أنظر في ذلك:** إبراهيم الوسلاتي ومن معه، "دليل تطبيقي للانابات القضائية الدولية في المادة الجزائية"، وزارة العدل، تونس، 2015، ص ص 15-19. متوفر عبر الرابط:
https://www.idlo.int/sites/default/files/pdfs/highlights/Tunisia%20%20Guide%20to%20Letters%20Rogatory.pdf.

[2] **أنظر:** وردة شرف الدين، مرجع سابق، ص 375. **وأنظر أيضا:** أبو المعالي محمد عيسى، مرجع سابق، ص 07.

[3] **أنظر:** أبو المعالي محمد عيسى، المرجع نفسه، ص 07 و08.

[4] **أنظر:** محمد كمال شاهين، مرجع سابق، ص 216.

[5] **أنظر:** المرجع نفسه، ص 219.

ب- نقل الإجراءات: بالإضافة إلى تبادل المعلومات والإنابات ؛ يمكن أن ينجز في إطار التعاون الدولي ما يسمى بنظام نقل الإجراءات. حيث تقوم من خلاله السلطات المختصة في الدولة بتقديم طلب إلى دولة أخرى، تلتمس منها مباشرة إجراءات جنائية معينة، في مواجهة شخص موجود على أراضيها ارتكب جريمة في دولة أخرى. الأمر الذي يتم اللجوء إليه في حال وجود اتفاق سابق أو قبول لاحق، مع استحالة تسليم الشخص المعني للدولة الطالبة. وذلك وفق شروط معينة، على غرار التناسق القانوني الموضوعي والإجرائي، من حيث وحدة التجريم والعقاب، وإجراءات المتابعة التي ستؤدي لإظهار الحقيقة. بالإضافة إلى قبول الدولة المطلوب منها، التي يمكنها أن ترفض في حالة سبق الفصل، أو عدم تبرير النقل، أو تأسيسه على اعتبارات غير محققة للعدالة، أو يخالف التزامات الدولة أو مبادئها القانونية[1].

ج- الحجز والمصادرة: نظمت الاتفاقية الدولية لمكافحة الجريمة المنظمة عبر الوطنية بمادتها رقم 13؛ فكرة حجز ومصادرة الأموال المستعملة والمتحصلة من الجريمة. ويعد ذلك من الأهمية بمكان، سواءً للدولة الطالبة التي تضمن المتابعة الجزائية الفعالة، أو الدولة المطلوب منها التي بمجرد اتصالها بالطلب؛ تصبح على علم بالمال الوسخ الموجود على إقليمها. على أن تختلف النظرة الوطنية باختلاف التشريعات السارية، حيث يمكن الاعتماد على النهج القائم على الممتلكات، أو النهج القائم على القيمة، أو الاثنين معا[2]. إلا أنه ما يعاب على الإجراء محل الطرح؛ ينطوي على عدم إمكانية تنفيذه بصورة منعزلة عن الجاني، حيث تصادر الأموال، لكن لا يتم تسليمها إلى الدولة الطالبة؛ إلا مع تسليم الجاني نفسه[3].

د- تسليم الأشخاص: يعد تسليم الأشخاص؛ الوسيلة الأكثر فعالية من حيث الأثر القانوني والواقعي عند تنفيذها في إطار التعاون الإجرائي الجنائي عموما. حيث يتم تسليم الشخص المعني من أجل التحقيق معه ومحاكمته، أو لتنفيذ العقوبة عليه لو كان قد صدر ضده حكم نهائي بات[4]. وهو ما يتم -وفق شروط معينة-؛ بالنقل الجسدي من إقليم الدولة المطلوب منها إلى إقليم الدولة الطالبة[5]. الأمر الذي يدل صراحةً على أنه في إطار دراسة الحال، لا يمكن تصور التسليم؛ إلا بخصوص التحقيق القضائي دون مرحلة التحري.

---

[1] **أنظر:** وردة شرف الدين، مرجع سابق، ص 375 و376.

[2] فمن خلال النهج القائم على الممتلكات؛ يتم مصادرة وسائل ارتكاب الجريمة وعائداتها. وأما النهج القائم على القيمة؛ فتحصر الأموال المتصلة بالجريمة، وتحصى، لكي يتم مصادرة أموال مكافئة لها في القيمة. **أنظر في ذلك:** إمام حسنين خليل، "التعاون القضائي الدولي لمواجهة الجريمة المنظمة-دراسة مقارنة"، مجلة رؤى إستراتيجية، مركز الإمارات للدراسات والبحوث الإستراتيجية، أبو ظبي، الإمارات العربية المتحدة، عدد 09، جانفي 2015، ص 23.

[3] **أنظر:** المرجع نفسه، ص 25.

[4] التفرقة في الغرض بين التحقيق والمحاكمة من جهة، وتنفيذ العقوبة من جهة أخرى؛ يعد السبب الأساس الذي جعلنا نعبر عن عنوان هذه الجزئية بعبارة تسليم الأشخاص، بدلا عن تسليم المجرمين. فمن يسلم للتحقيق والمحاكمة يكيف على أنه متهم يحضا بقرينة البراءة، ومن يسلم لتنفيذ العقوبة؛ يعتبر بمثابة المدان الذي يحمل وصف المجرم.

[5] **أنظر:** فافة لحمر، (إجراءات تسليم المجرمين في التشريع الجزائري على ضوء الاتفاقيات الدولية)، مذكرة لنيل شهادة الماجستير في القانون، كلية الحقوق والعلوم السياسية، جامعة وهران، الجزائر، 2014، ص 08 و09.

2. الإجراءات الخاصة بالتعاون الدولي على التحري والتحقيق في جرائم الوسط الرقمي: إضافةً إلى الإجراءات العامة المذكورة التي يمكن اللجوء إليها بغرض تنفيذ التعاون الدولي المتصل بالتحري والتحقيق في جرائم الوسط الرقمي؛ أوجدت اتفاقية بودابست لسنة 2001 كأول اتفاقية خاصة بجرائم الوسط الرقمي –وهي الأهم–؛ العديد من الإجراءات ذات الطابع الخاص، التي تتناسب مع المسرح الجرمي الافتراضي. وهي المنظمة بمجموعة مبادئ، وطريقة تفعيل، وصور معينة.

أ- مبادئ الإجراءات الخاصة بالتعاون الدولي على التحري والتحقيق في جرائم الوسط الرقمي: وضعت اتفاقية بودابست مجموعة من المبادئ الأساسية، التي يتوجب إتباعها في إطار التعاون الدولي محل الطرح. منها ما هي متصلة بالتعاون الدولي المطلق من حيث الشق الموضوعي والإجرائي والأمني"coopération internationale"، ومنها ما هي خاصة بتسليم الأشخاص "Extradition" من جهة، والتعاون الإجرائي أو المساعدة "l'entraide" من جهة أخرى. ونظرا لاتصال مجال الدراسة بالشق الإجرائي بخصوص التحري والتحقيق؛ سنكتفي بالتطرق إلى المبادئ ذات الصلة بالتسليم والمساعدة.

قيدت الاتفاقية عملية تسليم الأشخاص؛ بالعديد من المبادئ. على غرار أن يكون السلوك المرتكب من بين جرائم الوسط الرقمي الواردة بالاتفاقية نفسها –المذكورة سابقا–. والمعاقب عليها من دولتي عملية التسليم؛ بعقوبة سالبة للحرية لا تقل عن سنة أو بعقوبات متعددة. كما عالجت الاتفاقية عملية التسليم بين الوجوب والجواز، فإذا ما وجدت اتفاقية سابقة للتسليم بين الدولتين؛ يصبح التسليم في جرائم الوسط الرقمي الواردة بالاتفاقية واجبا، وإذا تخلف الاتفاق يصبح من الجائز إتباع أحكام التسليم الحالية، وأما إذا ما كان التعاون بين دولتين لا يشترطون الاتفاق المسبق للتسليم؛ فيمكنهم بمجرد الانضمام إلى اتفاقية بودابست أن يخضعوا لأحكامها. وعلى العموم؛ يخضع التسليم لأحكام اتفاقية التسليم أو القانون الوطني للدولة الموجه لها الطلب. وفي حالة الرفض بسبب الاختصاص أو الجنسية؛ تعمل الدولة الرافضة على إحالة الشخص على قضائها مع إبلاغ الدولة الطالبة بالنتائج في حينها[1].

أما بخصوص المبادئ ذات الصلة بالتعاون الدولي الإجرائي أو المساعدة؛ فحددتها الاتفاقية في وجوب التعاون الكبير من حيث تبادل المعلومات وجمع الأدلة الرقمية، وتبادل الطلبات المستعجلة والرد عليها؛ بالوسائل السريعة الرقمية وغير الرقمية. بالإضافة إلى إمكانية اشتراط الدولة الموجه لها طلب المساعدة؛ لازدواجية التجريم نصا ومضمونا، على ألا يكون ذلك لازما إذا حمل تكييف الجريمة في قانون الدولة المطلوب منها وصف الجناية[2].

---

[1] **أنظر:** المادة 24؛ مجلس أوربا، "التقرير التفسيري لاتفاقية الجريمة الالكترونية"، بودابست، هنغاريا، 2001. متوفر عبر الرابط: https://rm.coe.int/explanatory-report-budapest-convention-in-arabic/1680739174. **وأنظر أيضا:** - Art 24; Convention sur la cybercriminalité- Budapest, op.cit.

[2] **أنظر:** المادة 25؛ مجلس أوربا، المرجع نفسه. **وأنظر أيضا:**
- Art 25; Convention sur la cybercriminalité- Budapest, idem.

ب- تفعيل الإجراءات الخاصة بالتعاون الدولي على التحري والتحقيق في جرائم الوسط الرقمي:
لا تكتفي الجهات المختصة في الدول المتعاونة بالتقيد بالمبادئ السابقة؛ حتى تستفيد من التعاون الإجرائي المطلوب، وإنما يتوجب عليها المرور عبر تفعيل الإجراءات التي ستستفيد منها فيما بعد على شكل صور متعددة. التفعيل الذي جعلته اتفاقية بودابست إما تلقائي أو طلبي، مع احترام الاتفاق الإجرائي إن وجد.

يمكن أن يتم تناقل وتبادل المعلومات الرقمية ذات المحتوى الإجرامي، بين الجهات المتعاونة بصورة تلقائية ومن دون تقديم أي طلب. الأمر الذي يتم من خلال قيام الدولة التي يسمح لها قانونها الداخلي؛ بإرسال المعلومات المتحصل عليها في الإطار المشروع؛ إلى الدولة المعنية بغرض مساعدتها على مواجهة السلوك المجرم بالاتفاقية، التي قد يلجأ بخصوصها إلى المساعدة المتبادلة. كما يمكن أن تشترط الدولة قبل إرسالها التلقائي على الدولة محل الإرسال؛ أن تحافظ على السرية وتتقيد بالاستخدام على النحو القانوني الضروري فقط، وفي حالة الرد بالرفض يمكنها الامتناع عن الإرسال[1].

كما يمكن أن يفعل التعاون الإجرائي؛ عن طريق التقدم بطلب من الدولة الطالبة إلى الدولة المطلوب منها. الطلب الذي يتم تراسله مباشرة بين الهيئات المركزية المختصة أو غيرها التي تكون المسئولة عن ذلك. كما يمكن في حالة الاستعجال أن يتم تقديم الطلب مباشرة إلى الأجهزة القضائية المختصة، التي لها أن تحيله على نظيرتها المختصة في حالة عدم الاختصاص، مع إعلام الجهة الطالبة، وإرسال نسخة بعد ذلك إلى الهيئة المذكورة[2]. وعلى العموم يمكن أن يقابل الطلب بالرفض في حالة؛ اعتباره من الجهة المستقبلة أنه متعلق بوقائع تشكل جريمة سياسية أو لها اتصال بها، أو لها الطابع المالي، كما يمكنها الرفض إذا ما تبين أن تنفيذها سيؤدي إلى انتهاك سيادة الدولة أو نظامها العام أو مصالحها الكبرى[3].

وفي السياق نفسه؛ يتم تنفيذ الطلب؛ بالاعتماد على الإجراءات السارية في دولة الطلب، إلا إذا ما تعارضت مع قانون الطرف المقدم له الطلب. الأمر الذي قد يُشترط في تنفيذه المحافظة على السرية اللازمة، التي يتوجب إخطار مورد الطلب بإمكانية ذلك من عدمه، فيقرر مواصلة السير في الطلب أو التراجع عنه. وهو الذي يمكن إرجاء تنفيذه إذا كان من شأنه الإضرار بالوسط الرقمي المعتمد في ذلك. كما يمكن بعد تشاور الطرفين؛ أن تقرر جهة التنفيذ ما إذا ستنفذه جزئيا أو وفق شروط محددة. وعلى العموم يجب على الجهة مستقبلة الطلب؛ أن تخطر الجهة المصدرة عن نتائج الدراسة الأولية[4].

---

[1] **أنظر:** المادة 26؛ مجلس أوربا، "التقرير التفسيري لاتفاقية الجريمة الالكترونية"، مرجع سابق. **وأنظر أيضا:**
- Art 26; Convention sur la cybercriminalité- Budapest, op.cit.

[2] حيث أقر النص نفسه بإمكانية انجاز ذلك عبر منظمة الشرطة الدولية "الإنتربول"، مع عدم التطرق إلى الشرطة الأوروبية "الأوروبول"، رغم كونها آلية أوروبية باشرت عملها كمكتب؛ قبل إبرام اتفاقية بودابست بسبع سنوات.

[3] **أنظر:** المواد 4/25 و27/ 2-أ و4/27 و9/27؛ مجلس أوربا، المرجع نفسه. **وأنظر أيضا:**
- Arts 25/4 et 27/2-a et 27/4 et 27/9; Convention sur la cybercriminalité- Budapest, idem.

[4] **أنظر:** المواد 3/25 و27/ من 5 إلى 8؛ مجلس أوربا، المرجع نفسه. **وأنظر أيضا:**
- Arts 25/3 et 27/de 5 à 8; Convention sur la cybercriminalité- Budapest, idem.

ج- صور الإجراءات الخاصة بالتعاون الدولي على التحري والتحقيق في جرائم الوسط الرقمي: حددت اتفاقية بودابست العديد من صور المساعدة المتبادلة –التعاون الدولي الإجرائي–، التي تم تقسيمها إلى طائفتين، تتصل الأولى بالمساعدة المنصبة على التدابير المؤقتة، وتتعلق الثانية بالمساعدة التي تخص سلطات التحقيق.

ج-1/ التعاون المنصب على التدابير المؤقتة: ينطوي التعاون محل الطرح؛ على صورتين. حيث قد يتصل بالتحفظ السريع على المعلومات المخزنة، الذي ينجز بطلب الجهة المختصة في الدولة الأولى إلى نظيرتها في الدولة الأخرى؛ بغرض التحفظ على المعلومات المتصلة بالمنظومة المتواجدة على إقليمها. التي ينوي مقدمه أن يرسل طلب المساعدة المتبادلة من أجل مواصلة أعمال التحقيق. وهو ما لايمكن رفضه بحجة تخلف الازدواج التجريمي، إذا ما تعلق بالسلوكيات المجرمة بالاتفاقية. كما قد تتصل التدابير المؤقتة بالإفصاح السريع عن معلومات التراسل المتحفظ عليها؛ المنجزة في إطار طلب التحفظ السريع المبين أعلاه، المنصب حصرا على معلومات التراسل. حيث يلتزم الطرف المنفذ بالإفصاح السريع والعاجل لمقدم الطلب؛ عن أي معلومات تفيد بمساهمة مقدم خدمة الشبكة من دولة أخرى في نقل الاتصال المعني. ويمكن رفض العمليتين في حال تعلقهما بجريمة سياسية أو متصلة بها، أو لها أثر على سيادة الدولة أو نظامها العام أو مصالحها الكبرى[1].

ج-2/ التعاون الذي يخص سلطات التحقيق: بالإضافة إلى التدابير المؤقتة المذكورة؛ وضعت الاتفاقية العديد من الصور الإجرائية الخاصة، التي تخص سلطات التحقيق وأعمالها. حيث يمكن للجهة المختصة بالتحقيق أن تطلب من نظيرتها في الدولة الثانية؛ أن تقوم بالولوج إلى المنظومة المعلوماتية المتواجدة على إقليمها؛ بغرض تفتيشها أو الحصول معلوماتها أو الكشف عنها. الأمر الذي قد ينجز بسرعة كبيرة؛ في حال الخوف من الضياع الرقمي أو الانصياع للاتفاق المبرم الذي يتطلب ذلك. كما قد يتعلق الطلب بالوصول إلى المعلومات المخزنة عبر الحدود، من دون تصريح الطرف الآخر في حال كانت متاحة للجمهور، أو يتلقى من نظام معلوماتي محلي معلومات مخزنة في دولة أخرى[2].

ويمكن أيضا أن ينصب التبادل بين الجهات المختصة؛ على جمع وتقديم المعلومات المتصلة بالمرور في وقتها، التي يجب أن تنجز على الأقل في إطار الجنايات. كما قد يصل التعاون إلى حد اعتراض المعلومات ذات المحتوى المجرم أو المتصل بالدليل الرقمي[3].

---

[1] **أنظر:** المادتان 29 و30؛ مجلس أوربا، "التقرير التفسيري لاتفاقية الجريمة الالكترونية"، مرجع سابق. **وأنظر أيضا:**
- Arts 29 et 30 ; Convention sur la cybercriminalité- Budapest, op.cit.

[2] **أنظر:** المادتان 31 و32؛ مجلس أوربا، المرجع نفسه. **وأنظر أيضا:**
- Arts 31 et 32; Convention sur la cybercriminalité- Budapest, idem.

[3] **أنظر:** المادتان 33 و34؛ مجلس أوربا، المرجع نفسه. **وأنظر أيضا:**
- Arts 33 et 34; Convention sur la cybercriminalité- Budapest, idem.

الفرع الثاني: اعتماد القانون الجزائري للتعاون الدولي على التحري والتحقيق في جرائم الوسط الرقمي

بعد التطرق بالشرح المفيد إلى كل ما هو متصل بالتعاون الدولي على التحري والتحقيق في جرائم الوسط الرقمي، من منظور قانوني عام. إما في إطار التعاون الدولي الإجرائي عموما –المساعدة المتبادلة–، أو في إطار ذلك المتعلق بجرائم الوسط الرقمي دون سواها، من خلال أهم اتفاقية دولية في هذا الصدد المنطوية على اتفاقية بودابست لسنة 2001. يتوجب علينا تبيان التعاون المذكور من وجهة نظر القانون الجزائري، الذي يعد أساس دراسة الحال.

يمكن القول أن القانون الجزائري لم يخرج كثيرا عن الطرح المذكور. سيما وأن المواجهة الإجرائية لجرائم الوسط الرقمي؛ قد أخذت البعد العالمي، الذي يتطلب التنسيق الدولي إلى أبعد الحدود. الأمر الذي يمكن تأكيده؛ من خلال إبراز اعتماد القانون الجزائري للتعاون محل الدراسة، عن طريق ضبط مصادره(أولا) وتبيان إجراءاته(ثانيا).

أولا: مصادر القانون الجزائري المتصلة بالتعاون على التحري والتحقيق في جرائم الوسط الرقمي

اعتمد القانون الجزائري كغيره من نظرائه –للضرورة الإجرائية–؛ على العديد من الأحكام التي أقر من خلالها مسألة التعاون على التحري والتحقيق في جرائم الوسط الرقمي. التي منها ما هي تقليدية يمكن الاعتماد عليها، لعدم تعارضها مع المسرح الجرمي الافتراضي، ومنها ما هي مستجدة تم الاتفاق عليها أو وضعها حديثا. وعلى العموم يمكن أن نلخص الأحكام محل الطرح؛ في مصادر القانون الجزائري المعتمدة للتعاون على التحري والتحقيق في جرائم الوسط الرقمي، القائمة على الازدواجية في الطرح، من خلال المصادر الدولية الاتفاقية والمصادر الوطنية الوضعية.

1. المصادر الدولية الاتفاقية: ترتبط الجزائر في إطار التعاون الجنائي الإجرائي عموما والتعاون الإجرائي بخصوص مواجهة جرائم الوسط الرقمي خاصةً؛ بمجموعة من الاتفاقيات الدولية الملزمة بعد التصديق عليها وفق الشروط والإجراءات القانونية. التي منها ما تحمل الطابع الجماعي العالمي أو الإقليمي، ومنها ما لها البعد الثنائي المباشر.

أ– الاتفاقيات الدولية الجماعية: تعد الجزائر من الدول المصدقة على العديد من الاتفاقيات الدولية ذات الصلة بالمجال الجنائي عموما. التي في مجملها تضم أحكاما متصلة بالتعاون الإجرائي لمكافحة الجريمة محل المواجهة الاتفاقية. فعلى المستوى العالمي؛ نجد من أهمها اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لسنة 2000، التي صدقت عليها الجزائر سنة 2002[1]. حيث يعد التعاون الدولي

[1] **أنظر:** مرسوم رئاسي رقم 02-55، مؤرخ في 05 فيفري 2002، يتضمن التصديق بتحفظ على اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، المعتمدة من طرق الجمعية العامة لمنظمة الأمم المتحدة يوم 15 نوفمبر سنة 2000، (ج ر)، عدد 09، صادر بتاريخ 10 فيفري 2002.

الإجرائي الوارد بهذه الاتفاقية؛ الأقرب من بين الأحكام العامة العديدة إلى التطبيق على التحري والتحقيق في جرائم الوسط الرقمي. وذلك نظرا لاتصاف جرائم الوسط الرقمي بالعالمية من جهة، ومن جهة أخرى؛ لاحتوائها على كل الإجراءات العامة المتصلة بالتعاون الإجرائي المذكورة سابقا[1].

كما تعتبر أيضا من بين المصادر الدولية، ذات الصلة بالتعاون الإجرائي في مواجهة جرائم الوسط الرقمي؛ تلك التي لها البعد الإقليمي العربي. من خلال النسخة العربية –إن صح القول– لاتفاقية الأمم المتحدة المبينة أعلاه. حيث تم التوصل سنة 2010 بالقاهرة؛ إلى اتفاق عربي لمكافحة الجريمة المنظمة عبر الوطنية، الذي صدقت عليه الجزائر سنة 2014[2]. وهو الذي يضم فصلا كاملا –الفصل الثالث– مكونا من 15 مادة؛ يهتم بالتعاون القانوني والقضائي. كما أكد المتفقون من خلال المادة 21؛ أن مكافحة جرائم الوسط الرقمي يعد من بين أهداف الاتفاقية[3].

أما بخصوص الاتفاقيات الخاصة بجرائم الوسط الرقمي، التي صدقت عليها الجزائر وتعد من بين مصادر القانون الجزائري في هذا الإطار عموما والتعاون الإجرائي خصوصا؛ فلا نجد منها الكثير. سيما وأنه إلى حد الساعة؛ لا يوجد أي اتفاق دولي عالمي لمكافحة جرائم الوسط الرقمي. ومنه يرجع في العادة إلى الاتفاقية الأوروبية الصادر سنة 2001 –اتفاقية بودابست سابقة الذكر–، التي تعد أول وأهم هذه الاتفاقيات الخاصة، إلى درجة إضفاء عليها الطابع العالمي من حيث إمكانية الانضمام إليها. الأمر الذي كان له الأثر المباشر على الدول العربية، التي أبرمت سنة 2010؛ أول اتفاقية خاصة بهذا المجال، تحت تسمية الاتفاقية العربية لمكافحة جرائم تقنية المعلومات –سابقة الذكر–. التي صدقت عليها الجزائر سنة 2014، وهي تضم فصلا كاملا –الفصل الرابع– بعنوان التعاون القانوني والقضائي[4].

---

[1] كما توجد أيضا اتفاقيتي الأمم المتحدة لمكافحة الاتجار غير المشروع بالمخدرات والمؤثرات العقلية من جهة، ومكافحة الفساد من جهة أخرى، لسنتي 1988 و2003 على التوالي. **أنظر في ذلك:** مرسوم رئاسي رقم 95-41، مؤرخ في 28 جانفي 1995، يتضمن التصديق مع التحفظ على اتفاقية الأمم المتحدة لمكافحة الاتجار غير المشروع بالمخدرات والمؤثرات العقلية، الموافق عليها في فيينا بتاريخ 20 ديسمبر 1988، (ج ر) عدد 07، صادر بتاريخ 15 فيفري 1995. **وأنظر أيضا:** مرسوم رئاسي رقم 04-128، مؤرخ في 19 أفريل 2004، يتضمن التصديق بتحفظ على اتفاقية الأمم المتحدة لمكافحة الفساد، المعتمدة من قبل الجمعية العامة للأمم المتحدة بنيويورك يوم 31 أكتوبر 2003، (ج ر) عدد 26، صادر بتاريخ 25 أفريل 2004.

[2] **أنظر:** مرسوم رئاسي رقم 14-251، مؤرخ في 08 سبتمبر 2014، يتضمن التصديق على الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية، المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، (ج ر) عدد 56، صادر بتاريخ 25 سبتمبر 2014.

[3] ونجد أيضا العديد من المصادر الاتفاقية العامة، التي تحوي أحكاما متصلة بالتعاون الإجرائي الدولي، الممكن الرجوع إليها عند مباشرة التحري والتحقيق في جرائم الوسط الرقمي. على غرار الاتفاقية العربية لمكافحة الفساد والاتفاقية العربية لمكافحة غسل الأموال وتمويل الإرهاب، المحررين سنة 2010، والمصدق عليها من الجزائر سنة 2014. **أنظر في ذلك:** مرسوم رئاسي رقم 14-249، مؤرخ في 08 سبتمبر 2014، يتضمن التصديق على الاتفاقية العربية لمكافحة الفساد، المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، (ج ر) عدد 54، صادر بتاريخ 21 سبتمبر 2014. **وأنظر أيضا:** مرسوم رئاسي رقم 14-250، مؤرخ في 08 سبتمبر 2014، يتضمن التصديق على الاتفاقية العربية لمكافحة غسل الأموال وتمويل الإرهاب، المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، (ج ر) عدد 55، صادر بتاريخ 23 سبتمبر 2014.

[4] **أنظر:** مرسوم رئاسي رقم 14-252، مرجع سابق.

ب- الاتفاقيات الدولية الثنائية: تسليما من السلطات الجزائرية بمساس التعاون الإجرائي الجنائي المتبادل بسيادتها الوطنية؛ ركزت -كغيرها من الدول- على تنظيمه بالاتفاقيات الثنائية، التي تعد أكثر دقة وتحديدا من الجماعية المذكورة. الأمر الذي نجد بخصوصه العديد من الاتفاقيات المبرمة منذ الاستقلال. المتصلة بالمادة الجزائية عموما؛ من حيث تبادل الأشخاص والمساعدة الإجرائية المتبادلة.

ونظرا لحداثة جرائم الوسط الرقمي؛ سنعمل على ذكر أهم الاتفاقيات الثنائية في مجال التعاون الإجرائي الجنائي، التي أبرمتها الجزائر مؤخرا مع نظيراتها. حيث نجد آخر اتفاق في هذا الإطار تم إبرامه مع دولة فرنسا بمدينة باريس سنة 2016، ولم يدخل حيز النفاذ إلا بعد التصديق عليه مع بداية سنة 2018. وهو المعنون بالاتفاقية المتعلقة بالتعاون القضائي في المجال الجزائي بين الدولتين[1]. كما تعد أيضا من بين مصادر القانون الجزائري بخصوص التعاون الإجرائي محل الدراسة؛ الاتفاقية الثنائية المبرمة مع دولة الكويت سنة 2010، تحت تسمية اتفاقية التعاون القانوني والقضائي في المجال الجزائي بين الدولتين، التي لم تصبح نافذة في أواخر سنة 2015[2].

هذا وكانت قد دخلت قبل ذلك حيز النفاذ القانوني من بين مصادر القانون الجزائري؛ العديد من الاتفاقيات الثنائية ذات الهدف الإجرائي التعاوني نفسه. خاصة تلك التي كانت مع الولايات المتحدة الأمريكية سنة 2010. وتمت المصادقة عليها في السداسي الأول من سنة 2011، تحت عنوان المعاهدة المتعلقة بالتعاون القضائي في المجال الجزائي بين الدولتين[3].

2. المصادر الوطنية الوضعية: بالإضافة إلى المصادر الاتفاقية المذكورة[4]؛ أصدرت الجهات المختصة في الجزائر بعض النصوص التشريعية والتنظيمية، ذات الصلة بالتعاون الدولي على التحري والتحقيق في جرائم الوسط الرقمي، إن وفق أحكام عامة تقليدية يعمل بها في المجال الجزائي عموما أو خاصة مستحدثة تطلبتها الضرورة الرقمية. وهي التي نبينها فيما يلي، من حيث التطرق إلى النصوص التشريعية، من ثم النصوص التنظيمية المطبقة لها.

---

[1] **أنظر:** مرسوم رئاسي رقم 18-73، مؤرخ في 25 فيفري 2018، يتضمن التصديق على الاتفاقية المتعلقة بالتعاون القضائي في المجال الجزائي بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وحكومة الجمهورية الفرنسية، الموقعة بباريس بتاريخ 05 أكتوبر 2016، (ج ر) عدد 13، صادر بتاريخ 28 فيفري 2018.

[2] **أنظر:** مرسوم رئاسي رقم 15-255، مؤرخ في 05 أكتوبر 2015، يتضمن التصديق على اتفاقية التعاون القانوني والقضائي في المجال الجزائي بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وحكومة دولة الكويت، الموقعة بالجزائر بتاريخ 12 أكتوبر 2010، (ج ر) عدد 53، صادر بتاريخ 08 أكتوبر 2015.

[3] **أنظر:** مرسوم رئاسي رقم 11-184، مؤرخ في 03 ماي 2011، يتضمن التصديق على المعاهدة المتعلقة بالتعاون القضائي في المجال الجزائي بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وحكومة الولايات المتحدة الأمريكية، الموقعة بالجزائر بتاريخ 07 أفريل 2010، (ج ر) عدد 30، صادر بتاريخ 01 جوان 2011.

[4] التي قمنا بسردها على سبيل المثال لا الحصر، نظرا لاستحالة حصرها في إطار دراسة الحال، سيما وأن التعاون محل الطرح يعد أحد العناصر المكونة للدراسة وليس أساسها.

أ- النصوص التشريعية: لعل أهم نص تشريعي يبن الأعمال الإجرائية عموما؛ ينطوي على قانون الإجراءات الجزائية. الذي يحوي أحكاما عامة يتوجب الخضوع إليها، إلا إذا ما ورد نص أو اتفاق خاص بشأنها. الأمر الذي عمل به المشرع الجزائري بموجب القانون 09-04، الذي يعد بمثابة النص الإجرائي الخاص المتصل بجرائم الوسط الرقمي.

احتوى قانون الإجراءات الجزائية على أحكام عامة تنظم إجراءات تسليم الأشخاص وتنفيذ الإنابات القضائية وتبليغ الأوراق والأحكام. وذلك بموجب الكتاب السابع والأخير، من خلال 31 مادة[1]. إلا أن حداثة وتعقيد الوسط الرقمي كمسرح جرمي حديث، يدفع لعدم التناسق مع هذه النصوص التقليدية، التي بادر المشرع الجزائري بشأنها سنة 2009 بالقانون رقم 09-04، ووضع إجراءات خاصة بالتعاون الإجرائي على التحري والتحقيق فيها. حيث خصص له الفصل السادس المكون من أربعة 04 مواد، تحت عنوان التعاون والمساعدة القضائية الدولية[2].

ب- النصوص التنظيمية: في العادة يتم الاعتماد من حيث المصادر القانونية ذات الصلة بالتعاون الدولي؛ على الاتفاقيات الدولية الجماعية والثنائية، والنصوص التشريعية الوطنية التي تفرغ فيها الاتفاقيات المذكورة. إلا أنه بخصوص التعاون محل الدراسة، ونظرا لخصوصيته المستحدثة المترتبة عن الطبيعة الرقمية الافتراضية لمسرح الجريمة؛ توجبت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 -سابقة الذكر- ضرورة إنشاء جهاز متخصص ومتفرغ على مدار الساعة، من بين مهامه ضمان توفير التعاون[3]. الجهاز الذي أنشأته الجزائر قبل أن يتم تحرير الاتفاقية المذكورة، وهو المنطوي على الهيئة الوطنية السابقة بالذكر، الواردة بالقانون 09-04[4].

وعلى العموم بغرض تبيان المهام المسندة للجهاز المتخصص -الهيئة-؛ لم يكتفي المشرع بأحكام القانون 09-04، الذي اقتصر على الإنشاء وتحديد المهام العامة، بل أسند مهمة الهيكلة وتحديد المهام بدقة إلى التنظيم[5]، الوارد بالمرسوم الرئاسي الصادر سنة 2015. ومن أهم هذه المهام؛ نجد السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون[6]. الأمر الذي يجعل التنظيم من بين مصادر القانون الجزائري، المتصلة بالتعاون الدولي على التحري والتحقيق في جرائم الوسط الرقمي.

---

[1] **أنظر:** المواد من 694 إلى 725؛ أمر رقم 66-155، مرجع سابق.

[2] **أنظر:** المواد من 15 إلى 18؛ قانون رقم 09-04، مرجع سابق.

[3] **أنظر:** المادة 43؛ مرسوم رئاسي رقم 14-252، مرجع سابق.

[4] **أنظر:** المادة 1/13؛ قانون رقم 09-04، المرجع نفسه.

[5] **أنظر:** المادة 2/13؛ المرجع نفسه.

[6] **أنظر:** المادتان 2/04-6 و1/11-3؛ مرسوم رئاسي رقم 15-261، مرجع سابق.

ثانيا: إجراءات القانون الجزائري الخاصة بالتعاون على التحري والتحقيق في جرائم الوسط الرقمي

انطلاقا من مصادر القانون الجزائري ذات الصلة بالتعاون الإجرائي الجزائي عموما، والمتصل بالتحري والتحقيق في جرائم الوسط الرقمي خصوصا؛ يمكن أن نحدد الإجراءات سارية المفعول، التي لها الطابع المزدوج التقليدي والحديث. حيث يتم الاعتماد على الإجراءات التقليدية الواردة بالمصادر الدولية والمحلية، المطبقة في مجال التعاون الجزائي عموما، إلا من حيث تلك الحديثة الواردة بالمصادر المستحدثة، المنطوية على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، والقانون رقم 09-04، والمرسوم الرئاسي المتصل به رقم 15-261[1]. الأمر الذي نبينه من خلال التطرق إلى مبادئ إجراءات القانون الجزائري الخاصة بالتعاون الدولي على التحري والتحقيق في جرائم الوسط الرقمي، وطرق تفعيلها، وصور أعمالها.

1. مبادئ إجراءات القانون الجزائري الخاصة بالتعاون الدولي على التحري والتحقيق في جرائم الوسط الرقمي: حددت مصادر القانون الجزائري ذات الصلة بمواجهة جرائم الوسط الرقمي؛ العديد من المبادئ الأساسية واجبة الإتباع، بخصوص تفعيل إجراءات التعاون الدولي على التحري والتحقيق في جرائم الوسط الرقمي. المنطوية على تحديد الاختصاص القضائي وآليات تسليم المجرمين –الأشخاص– والمساعدة المتبادلة[2].

تم تحديد الاختصاص القضائي الملزم للتعاون من عدمه؛ في إطار الاتفاقية العربية لمكافحة جرائم تقنية المعلومات والقانون رقم 09-04، وذلك وفق أحكام تبدوا في ظاهرها على أنها متناسقة، أو على الأقل مضمون الاتفاقية يشمل محتوى النص القانوني. حيث اكتفى النص القانوني الصادر سنة 2009؛ بإبراز اختصاص القضاء الجزائري بالنظر في جرائم الوسط الرقمي المرتكبة في الخارج من قبل شخص أجنبي، إذا ما استهدفت مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني[3]. وهو ما يعد بمثابة تكريس لمبدأ عينية جديد، بالإضافة إلى نظيره العام الوارد بقانون الإجراءات الجزائية، والمعتمد كتكملة لمبدأ الإقليمية.

---

[1] ولو أنه يتوجب التفرقة بين التعاون الرسمي وغير الرسمي. فغير الرسمي المنجز بين أجهزة الشرطة؛ يعد كثير الاستعمال في مواجهة جرائم الوسط الرقمي. وان كان بخصوص التعاون الرسمي؛ يتم الاعتماد على الأشكال التقليدية بشكل واسع، سيما الواردة باتفاق التعاون الإجرائي الثنائي، الذي -حسب منظمة الأمم المتحدة- يعتمد عليه بنسبة 60 %، على حساب الاتفاق الجماعي الذي يحضا بنسبة 20 % فقط. **أنظر في ذلك:** فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، "دراسة شاملة عن مشكلة الجريمة السيبرانية والتدابير التي تتخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدي لها"، مرجع سابق، ص 14 و15.

[2] وان كان نخرج من إطار ذلك؛ المبادئ ذات الصلة بتسليم الأشخاص -وحتى الإجراءات ذات الصلة-. وهذا نظرا لقيامها على أحكام تواجه جرائم معينة، من دون إبراز الخصوصية الرقمية الحديثة. على أنها ترجع دائما إلى أحكام الاتفاقيات الدولية الثنائية والقوانين الداخلية القائمة مسبقا. **أنظر في ذلك:** المادة 31؛ مرسوم رئاسي رقم 14-252، مرجع سابق. **وأنظر أيضا:** المواد من 694 إلى 720؛ أمر رقم 66-155، مرجع سابق.

[3] **أنظر:** المادة 15؛ قانون رقم 09-04، مرجع سابق.

لكن بالرجوع إلى الاتفاقية العربية المحررة سنة 2010-المصدق عليها سنة 2014-؛ نجد أنها تتعامل مع التعاون محل الطرح بنظرة أشمل وأوسع. حيث تلزم كل دولة طرف بوضع أحكام إجرائية؛ تضمن اختصاصها القضائي بالنظر في جرائم الوسط الرقمي الواردة بالاتفاقية، وذلك في حالة ارتكاب السلوك الإجرامي -جزئيا أو كليا- و/أو تحققت النتيجة؛ في إقليمها أو على متن سفنها أو طائراتها -مبدأ الإقليمية-، أو خارج كل ذلك من قبل شخص حامل لجنسيتها -مبدأ الشخصية الايجابي-، أو كانت تمس بمصالحها العليا -مبدأ العينية-[1]. الأمر الذي لا يتعارض مع النص القانوني الوطني، الذي يضمن بـــ "ق.إ.ج"؛ مبادئ الإقليمية والشخصية الايجابي والعينية -العامة-[2]، ويتطرق إلى مبدأ العينية الخاص بجرائم الوسط الرقمي؛ بالمادة 15 من القانون رقم 09-04 المذكور أعلاه.

إلا أن الجديد بهذا الخصوص؛ ينطوي حول أن الاتفاقية قد أخلطت الأحكام العامة، التي تجعل من مبدأ الإقليمية الأصل وتمنح لمبدئي الشخصية والعينية صفة المكمل. حيث أعطت الأولية للجهات القضائية التابعة للدولة المعتدى على مصالحها الأساسية -العينية-، ومن ثم الدولة التي وقعت الجريمة على إقليمها -الإقليمية-، وبعد ذلك الدولة التي يعد الشخص المطلوب من رعاياها -الشخصية الايجابي-. وفي حال اتحاد الظروف نرجع إلى الدولة السابقة في طلب التسليم[3].

وفي سياق المبادئ العامة للتعاون الدولي على التحري والتحقيق في جرائم الوسط الرقمي؛ نجد أن الاتفاقية العربية أوجبت التعاون الإجرائي بين الأطراف إلى أبعد الحدود، سيما في إطار التحقيقات القضائية، وذلك من خلال العمل على تنسيق قوانينها الداخلية، مع الأحكام ذات الصلة الواردة بالاتفاقية نفسها. كما أن الرضوخ إلى التعاون مطلوب؛ في حال ازدواجية التجريم، بغض النظر عن التكييف القانوني للجريمة محل الطلب[4]. وهو ما عالجه المشرع الجزائري عن طريق فتح مجال التعاون بخصوص جرائم الوسط الرقمي[5]، على أن يدور التعاون في إطار قواعد الاختصاص المبينة أعلاه.

2. تفعيل إجراءات القانون الجزائري الخاصة بالتعاون الدولي على التحري والتحقيق في جرائم الوسط الرقمي: نظرا لعدم توضيح القانون الوطني لكيفية تفعيل إجراءات التعاون محل الدراسة؛ يتوجب الرجوع إلى نص الاتفاقية العربية لمكافحة جرائم تقنية المعلومات -والاتفاق الثنائي إن وجد-. التي ميزت بين التعاون التلقائي والطلبي، وفق طريقة تكاد تكون متطابقة مع مضمون اتفاقية بودابست المذكورة سابقا.

---

[1] **أنظر:** المادة 1/30؛ مرسوم رئاسي رقم 14-252، مرجع سابق.

[2] **أنظر:** المواد من 582 إلى 591؛ أمر رقم 66-155، مرجع سابق.

[3] **أنظر:** المادة 2/30؛ مرسوم رئاسي رقم 14-252، المرجع نفسه.

الأمر الذي يدفع إلى التضارب بين النص التشريعي الوطني الذي يميز مبدأ الإقليمية بجعله الأصل انطلاقا من السيادة الوطنية، والنص الاتفاقي الملزم، الذي يجعله في المرتبة الثانية بعد نظيره القائم على العينية.

[4] **أنظر:** المادة 32؛ مرسوم رئاسي رقم 14-252، المرجع نفسه.

[5] **أنظر:** المادة 1/16؛ قانون رقم 09-04، مرجع سابق.

فمن حيث التعاون التلقائي؛ يمكن أن تقوم الجهة المختصة في الدولة الطرف؛ بإرسال محتوى رقمي إجرامي إلى نظيرتها في دولة عضو أيضا. وذلك من دون التقدم بطلب وفي حدود سماح قانونها الداخلي بذلك. على أن يستهدف ذلك مساعدة الطرف المرسل إليه على مواجهة السلوك المجرم بالاتفاقية، للبدء في التحري أو التحقيق أو لمواصلتها، أو استقبال طلب مساعدة قضائية بشأنها. كما يمكن الاشتراط قبل الإرسال التلقائي ضرورة الحفاظ على السرية، التي في حال الرد بعدم إمكانيتها يمكن وقف الإرسال[1].

يمكن وفق سبيل تفعيل آخر أن تبدأ إجراءات التعاون؛ بعد تقديم طلب من الدولة الطرف الراغبة في ذلك إلى نظيرتها التي يمكنها المساعدة. الأمر الذي حددته الاتفاقية بإجراءات خاصة، لا تتبع إلا في حال غياب الاتفاق الدولي والنص الوطني الساري بهذا الخصوص، أو مع وجوده والاتفاق على تجاوزه. وعلى العموم لا تختلف الإجراءات كثيرا عن تلك الواردة باتفاقية بودابست –المذكورة–. المنطوية على إنجاز التراسل بين الجهات المركزية المختصة، المحددة في القانون الجزائري بالهيئة الوطنية. مع إمكانية الإرسال المباشر إلى السلطة القضائية المختصة في حالة الاستعجال –وهو ما يمكن إتمامه عن طريق "الإنتربول"–. على أن تحيل الجهة المستقبلة الطلب إلى نظيرها المختصة في حال عدم اختصاصها[2].

وقد تقابل طلبات المساعدة بالرفض، في حال اعتبار الدولة المطلوب منها؛ أنها تتعارض مع قوانينها السارية، أو لها وصف الجريمة السياسية، أو تنفيذ الطلب يعد انتهاكا لسيادة الدولة أو أمنها أو نظامها أو مصالحها الأساسية[3]. وفي حالة القبول؛ تباشر عملية تنفيذ طلب المساعدة؛ وفق قوانين الدولة الطالبة، إلا في حالة عدم التوافق مع تلك السارية في الدولة المطلوب منها. وهو ما ينجز بالسرية اللازمة في حالة طلبها من الدولة المنفذة، التي يمكنها الالتماس المسبق لذلك، تحت طائلة عدم المباشرة[4].

كما يمكن تأجيل التنفيذ إذا كان من شأن ذلك؛ أن يؤثر على التحقيقات الجنائية الجارية. وعلى العموم يتوجب على الدولة الموجه لها الطلب قبل رفضه أو تأجيله، أن تقوم بعد التشاور مع الجهة الطالبة؛ بتقرير التصرف اللازم بخصوص التنفيذ الجزئي أو الكلي أو الرفض، أو الشروط المقيدة للعملية، مع الإبلاغ في الوقت المناسب بالنتائج المتوصل إليها إلى الجهة الطالبة[5].

---

[1] **أنظر:** المادة 33؛ مرسوم رئاسي رقم 14-252، مرجع سابق.

[2] **أنظر:** المادة 1/34 و2-أوب و المادة 8/34-أ وب وج؛ المرجع نفسه.

[3] مع الإشارة إلى الاختلاف في الطرح بين القانون رقم 09-04 والاتفاقية. حيث جاءت الاتفاقية أشمل وبكل ما ذكر أعلاه، واكتفى القانون بالرفض المؤسس على المساس بالسيادة الوطنية والنظام العام. **أنظر:** المادتان 4/32 و35؛ المرجع نفسه. **وأنظر أيضا:** المادة 1/18؛ قانون رقم 09-04، مرجع سابق.

[4] **أنظر:** المادتان 7/34 و36؛ مرسوم رئاسي رقم 14-252، المرجع نفسه. **وأنظر أيضا:** المادة 2/18؛ قانون رقم 09-04، المرجع نفسه.

[5] **أنظر:** المادة 4/32 والمادة 3/34 و4 و5 و6؛ مرسوم رئاسي رقم 14-252، المرجع نفسه.

3. صور إجراءات القانون الجزائري الخاصة بالتعاون الدولي على التحري والتحقيق في جرائم الوسط الرقمي: تباينت المعالجة الإجرائية محل الطرح في إطار مصادر القانون الجزائري، بين الطرح العام الوارد بالقانون رقم 09-04، والآخر الخاص المحدد بالاتفاقية العربية ذات الصلة. حيث فصلت الاتفاقية في مختلف الإجراءات المبينة لمجالات التعاون، التي حددها القانون عموما في الإجراءات التحفظية و/أو العاجلة، وتبادل المعلومات و/أو الإنابات[1].

أ- **الإجراءات التحفظية و/أو العاجلة:** في إطار هذا النوع من الإجراءات؛ يمكن التقدم بطلب الحفظ العاجل للمعلومات المخزنة في أنظمة المعلومات المتواجدة على إقليمها، وذلك بغرض التقدم لاحقا بطلب المساعدة المتبادلة بشأنه. الطلب الذي لايمكن رفضه لغياب الازدواجية في التجريم، متى تعلق بالسلوكيات المجرمة بالاتفاقية العربية. على أن يمكن رفضه إذا ما تعلق بجريمة ذات طابع سياسي في نظر الدولة المطلوب منها، أو يهدد سيادتها أو أمنها أو نظامها أو مصالحها، وعلى العموم يجب ألا يقل التحفظ في حالة تنفيذه عن الـــ 60 يوما[2].

وفي حالة الاكتشاف في إطار تنفيذ الطلب المتصل بتتبع المستخدمين الخاصة باتصالات معينة؛ أن مزود خدمة في دولة أخرى قد اشترك في بث الاتصال؛ يتوجب الكشف العاجل للدولة الطالبة عن المعلومات الكافية لتحديد المزود ومسار البث. كما يمكن خارج ذلك أن تتم عملية الجمع الفوري؛ لمعلومات تتبع المستخدمين، المصاحبة للاتصال المنجز عبر إقليمها بواسطة تقنية المعلومات. وذلك على الأقل بخصوص الجرائم المسموح داخليا بتتبع الاتصالات في إطار مكافحتها. أو الجمع الفوري في الإطار المسموح به قانونا واتفاقا؛ لمعلومات محتوى الاتصال الرقمي[3].

ب- **تبادل المعلومات و/أو الإنابات:** قد يتم اللجوء في إطار البحث عن الدليل الرقمي؛ إلى تبادل المعلومات و/أو الإنابات القضائية. من خلال التعاون والمساعدة الثنائية المتعلقة بالوصول إلى المعلومات المخزنة[4]. حيث يجوز للدولة الطرف أن تطلب من نظيرتها البحث أو الوصول أو الضبط أو التأمين أو الكشف عن المعلومات الواقعة ضمن إقليمها، سواءً المخزنة بالطريقة العادية العامة أو في إطار التحفظ العاجل المبين أعلاه[5].

---

[1] الإجراءات التي أحال القانون رقم 09-04 صراحةً، مسألة تحديد الأحكام المبينة لطريقة الاستجابة إليها؛ إلى الاتفاقيات الدولية المصدق عليها والمعاملة بالمثل. وهي المنطوية أساسا على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 -محل الدراسة-. **أنظر في ذلك:** المادتان 3/05 و17؛ قانون رقم 09-04، مرجع سابق.

[2] **أنظر:** المادة 37؛ مرسوم رئاسي رقم 14-252، مرجع سابق.

[3] **أنظر:** المواد 38 و41 و42؛ المرجع نفسه.

[4] الأمر الذي قد ينجز من دون تعاون ولا مساعدة ولا تفويض مسبق من الدولة المعنية، في حال تعلق بمعلومات متاحة للعامة. أو في حال الحصول على المعلومات الخاصة؛ من خلال تقنية معلومات متصلة بإقليمها، بعد موافقة من له السلطة القانونية لكشف هذه المعلومات إلى الدولة الأجنبية المتواجدة على إقليمها. **أنظر في ذلك:** المادة 40؛ المرجع نفسه.

[5] **أنظر:** المادة 1/39؛ المرجع نفسه.

تنجز الطلبات المبينة أعلاه؛ في إطار تبادل المعلومات لو تعلقت بمرحلة التحري، والإنابة القضائية لو تعقلت بإجراءات التحقيق. حيث تلتزم الجهات المختصة في الجزائر؛ بأن تستجيب للطلب وفق ما بينته الاتفاقية نظرا لعدم تطرق قانونها الداخلي لذلك بالتفصيل، وإحالته للاتفاقية وفق ما بينا سابقا. كما قد تتم الاستجابة وفق التعجيل اللازم إذا ما تعلق الطلب بمعلومات معرضة للفقدان أو التعديل[1].

وعلى العموم يمكن القول أن النصوص القانونية الوطنية –الجزائرية–، ذات الصلة بالإجراءات الجزائية عموما ومواجهة جرائم الوسط الرقمي خصوصا؛ لم تتطرق إلى التعاون الدولي الإجرائي المتصل بالتحري والتحقيق في جرائم الوسط الرقمي، بالقدر الكافي والمتناسب مع حداثة وتعقيد مسرحها الافتراضي، بل تحيل صراحةً إلى الاتفاقيات الدولية ذات الصلة. الأمر الذي يتطلب العمل بالاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، سيما وأنها الوحيدة من نوعها، الملزمة في إطار القانون الجزائري.

المطلب الثاني: نماذج الأجهزة الأجنبية المتعاونة على التحري والتحقيق في جرائم الوسط الرقمي

يختلف التعاون الدولي المتصل بالتحري والتحقيق في جرائم الوسط الرقمي؛ بين من ينجز في إطاره الأمني الوقائي–الذي يحمل وصف التحري في بعض جرائم الوسط الرقمي، كما بينا سابقا–، أو الإجرائي الشرطي المتصل بمرحلة التحري أو القضائي المتعلق بإجراءات التحقيق. الأمر الذي بدوره قد ينجز في إطار التعاون مع الأجهزة الدولية و/أو المقارنة. التي قد تكون ذات اختصاص جنائي عام –أمني أو شرطي أو قضائي–، أو مختصة بمواجهة جرائم الوسط الرقمي دون سواها.

وعلى العموم تعمل الأجهزة الوطنية –الجزائرية–، الممارسة لأعمال التحري والتحقيق في جرائم الوسط الرقمي، التابعة لنطاق اختصاصها؛ على التعاون مع نظيرتها الأجنبية –دولية ومقارنة–، على حسب الاتفاق المبرم أو الضرورة الدافعة إلى ذلك تحت غطاء مبدأ المعاملة بالمثل. الأمر الذي نبينه بالتطرق إلى هذه الأجهزة الأجنبية المتعاونة، إن بالمنظور الدولي(فرع أول) أو المقارن(فرع ثانٍ).

الفرع الأول: الأجهزة الدولية المتعاونة على التحري والتحقيق في جرائم الوسط الرقمي

تتعدد وتتنوع الأجهزة الدولية المتعاونة على التحري والتحقيق في جرائم الوسط الرقمي، على حسب نطاقها الجغرافي وطبيعتها القانونية. حيث قد يحمل الجهاز الوصف العالمي أو الإقليمي، كما قد يتصف بالجهاز الشرطي أو القضائي أو المساعد للاثنين –أو الحامل للبعدين الجغرافي والقانوني–. وهو التنوع المطلوب لانجاز التعاون الواجب، ومنه مواجهة العجز الإجرائي الرقمي.

[1] **أنظر:** المادة 2/39 و3؛ مرسوم رئاسي رقم 14-252، مرجع سابق.

وعلى العموم يمكن أن تتعاون الأجهزة الوطنية –الجزائرية–، المختصة بالتحري والتحقيق في جرائم الوسط الرقمي؛ مع العديد من الأجهزة الدولية. سيما ذات البعد العالمي(أولا)، أو البعد الإقليمي بمفهومه المادي المتصل بالقارة الأوروبية(ثانيا)، أو الإقليمي بالمفهوم المادي الإفريقي والمعنوي العربي(ثالثا).

أولا: الأجهزة العالمية المتعاونة على التحري والتحقيق في جرائم الوسط الرقمي

تتمثل أهم الأجهزة الدولية العالمية، التي يمكن لنظيرتها الوطنية –نظيرتها من حيث المهام وطبيعة الأعمال المنجزة– المختصة بالتحري والتحقيق في جرائم الوسط الرقمي التعاون معها؛ في جهازين أساسيين. يحمل الجهاز الأول والأهم الطبيعة الشرطية العامة، وهو المنطوي على منظمة الشرطة الجنائية الدولية "الإنتربول–Interpol"، ويعنى الآخر بدور المساعد لمختلف الأجهزة الشرطية والقضائية المختصة، المتمثل في مركز شكاوى جرائم الإنترنت "IC3".

1. منظمة الشرطة الجنائية الدولية "الإنتربول–Interpol": تعد منظمة الشرطة الجنائية الدولية؛ أول وأهم الآليات الشرطية الدولية، التي تهتم بتجسيد التعاون الجنائي الدولي على وجه العموم. وهي التي بادرت إلى الحث النظري والتجسيد العملي؛ للتعاون الشرطي الدولي في إطار مواجهة جرائم الوسط الرقمي، ذات المسرح الافتراضي العالمي. وعليه سنعمل على طرح الإطار العام لهذه المنظمة الشرطية العالمية، ومن ثم تبيان مظاهر تعاونها على التحري والتحقيق في جرائم الوسط الرقمي.

أ– الإطار العام لمنظمة الشرطة الجنائية الدولية: يرتكز التعاون الشرطي العالمي على "الإنتربول"، كأقدم جهاز شرطي عام وعالمي. حيث بدأ الوجود الفعلي للمنظمة في سنة 1923، تحت تسمية اللجنة الدولية للشرطة الجنائية، كنتيجة عن المؤتمر الدولي للشرطة المنعقد في فيينا عاصمة النمسا، إلا أنها لم تعمر طويلا نظرا لاندلاع الحرب العالمية الثانية. على أن تمت إعادة بعثها بتاريخ 06 جوان 1946، من خلال المؤتمر الدولي المنعقد ببلجيكا، مع نقل مقر اللجنة إلى باريس عاصمة فرنسا. وفي إطار انعقاد الجمعية العامة للأمم المتحدة في فيينا –النمسا– بين 07 و13 جوان 1956؛ تم وضع القانون الأساسي للجنة مع تغيير اسمها من اللجنة إلى المنظمة. التي تحول مقرها سنة 1989؛ إلى مدينة ليون الفرنسية[1].

وتتكون "الإنتربول"، وفق ما هي عليه حاليا؛ من تشكيل عضوي ومادي، تمارس من خلاله المهام الشرطية المنوطة بها. حيث وصلت عضوية الدول فيها إلى حد الـــ 192 دولة، منهما الجزائر المنظمة بتاريخ 21 أوت 1963، مع انعقاد الجمعية العامة للمنظمة –الإنتربول–، بهلسنكي عاصمة فنلندا[2].

---

[1] **أنظر:** حاسين فنور، (المنظمة الدولية للشرطة الجنائية والجريمة المنظمة)، مذكرة لنيل شهادة الماجستير في القانون الدولي والعلاقات الدولية، كلية الحقوق، جامعة الجزائر 1، الجزائر، 2013، ص ص 06-11.

[2] **أنظر:** - Site officiel de l'Interpol, Pays membres-Afrique-Algérie, Date de Publication: 2018, Date d'Accès: 30 avril 2018, Lien Numérique: https://www.interpol.int/fr/Pays-membres/Monde.

أما بخصوص التكوين المادي، فتتهيكل "الإنتربول"؛ من جمعية عامة ولجنة تنفيذية وأمانة عامة ومكاتب مركزية وطنية، ومكاتب إقليمية[1]. التي لكل منها الدور المناط بها بنص القانون الأساسي، على أن تأخذ المكاتب المركزية الوطنية –بالإضافة إلى المكاتب الإقليمية التي تربط بين دول الإقليم الواحد–؛ الأهمية الكبرى نظرا لاتصالها بالعمل الشرطي الدائم والمباشر في الدولة المعنية. وفي هذا الصدد استحدثت الجزائر بعد انضمامها إلى المنظمة؛ المكتب المركزي الوطني، في إطار مديرية الشرطة القضائية التابعة للمديرية العامة للأمن الوطني، الذي يخضع للقانون الوطني وأحكام المنظمة[2].

وعلى العموم تعنى منظمة الشرطة الجنائية الدولية "الإنتربول"؛ بالعديد من الاختصاصات ذات الأهداف المعينة بقانونها الأساسي، التي يكيفها الفقه الجنائي عموما على أنها عامة وخاصة. حيث تتمثل الاختصاصات العامة في تجميع المعلومات الجنائية وتبادلها، ومكافحة جرائم القانون العام، مع حماية الأمن الدولي، وتبادل الخبرات والمساعدات اللازمة، كما تقوم بضمان التنسيق اللازم من حيث الجهود المتصلة بفرار الجناة. وأما من حيث الاختصاصات الخاصة؛ فتقوم المنظمة بضمان التدريب الشرطي المستمر والفعال وخدمات الاتصال العالمي، والتعامل المطلوب مع الأجهزة المختصة بالتحري والتحقيق والتنفيذ في الدولة المعنية[3].

ب– مظاهر تعاون منظمة الشرطة الجنائية الدولية على التحري والتحقيق في جرائم الوسط الرقمي:

سعت "الإنتربول" كأهم جهاز شرطي عالمي؛ إلى المضي قدما بخصوص مساعدة الدول الأعضاء على مواجهة جرائم الوسط الرقمي في إطار التحري والتحقيق، وحتى من حيث الوقاية والتدريب والمساعدة النظرية والتقنية. حيث أنشأت بغرض تسهيل مرور الرسائل؛ عدة مراكز اتصالات إقليمية، في كل من طوكيو ونيوزيلاندا ونيروبي وأذربيجان وبيونس أيرس، والمكتب الإقليمي في بانكوك[4]. وهذا بالإضافة إلى المركز الرئيسي لتبادل المعلومات الجنائية والتواصل بين الدول الأعضاء "I-Link"[5]، الذي يؤمن الاتصالات المنجزة في إطار التحري والتحقيق، عبر منظومة الـــ "I–24/7"[6].

---

[1] **أنظر:** - Art 05; Statut de L'O.I.P.C - Interpol, Version consolidée au 2017. Disponible sur le Lien: https://www.interpol.int/fr/Internet.

[2] **أنظر:** - Site officiel de l'Interpol, Pays membres-Afrique-Algérie, op.cit.

[3] **أنظر:** حاسين فنور، مرجع سابق، ص ص 19-30. **وأنظر أيضا:** - Art 02; Statut de l'O.I.P.C - Interpol, idem.

[4] **أنظر:** نجاة بن مكي، السياسة الجنائية لمكافحة جرائم المعلوماتية، دار الخلدونية للنشر والتوزيع، الجزائر، 2017، ص 150.

[5] **أنظر:** - AHOUTY Charlotte, "Quels Mécanismes de coopération policière pour faire face à la cybercriminalité dans l'espace francophone ?", ORS Interpol BR Abidjan, Côte d'Ivoire, 08-10 février 2016, P 04 et 05 et 16. Disponible sur le Lien: https://www.interpol.int/fr.

[6] كما كانت قد أنشأت مجموعة دول الثمانية "G8"، في إطار اهتمامها بمكافحة جرائم الوسط الرقمي؛ شبكة نقاط اتصال وطنية، القائمة أساسا على النظام الوطني للنقطة المرجعية المركزية "للإنتربول". التي يمكنها أن تستجيب لطلبات المساعدة على مدار اليوم والأسبوع. **أنظر في ذلك:** محمد كمال شاهين، مرجع سابق، ص 217 و218.

كما أكدت "الإنتربول" من خلال دراسة متخصصة؛ أنها تهتم بمساعدة الأجهزة الوطنية على التحري والتحقيق في جرائم الوسط الرقمي، من خلال عديد الأجهزة والأعمال، سيما المركز العالمي المتعدد الاختصاصات –ومركز مكافحة الجريمة الرقمية–، الذي يضم خبراء في "الإنترنت"، ويضمن التزويد بالمعلومات الإجرامية. كما تضم المنظمة أيضا ما يسمى بمختبر الأدلة الجنائية، المزود بالأجهزة والخبرات اللازمة لاستخراج الأدلة الرقمية وحفظها؛ بغرض إرسالها إلى الجهات الوطنية المختصة[1].

وكان لمنظمة الشرطة الجنائية الدولية؛ العديد من العمليات الشرطية المساعدة على التحري والتحقيق في جرائم الوسط الرقمي. حيث سبق وأن أنجزت بتاريخ 09 أفريل 2015؛ عملية تنسيق عالمي لتفكيك شبكة "البوتنت – Simda"، التي ألحقت الضرر بأكثر من 000 770 جهاز إعلام آلي عبر العالم، من خلال سرقة المعلومات الرقمية ونصب البرمجيات الخبيثة، بعد الاختراق. الأمر الذي أنجز بالأساس من قبل مجمع "الإنتربول" العالمي للابتكار في سنغافورة –ماليزيا–، المتعاون مع الأجهزة الوطنية المختصة في كل من هولندا والو.م.أ وليكسمبرغ وروسيا، كما حصل على معلومات وتحليلات تقنية؛ من طرف أكبر الشركات الرقمية، سيما وحدة مكافحة الجريمة الرقمية في شركة "مايكروسوفت – Microsoft"[2].

2. مركز شكاوى جرائم الإنترنت "IC3": بالإضافة إلى "الإنتربول"، الذي يعنى بالدور الأساس من حيث التعاون الشرطي العالمي؛ برز جهاز عالمي آخر يمكن أن نصفه على أنه جهاز مساعد من الدرجة الثانية. حيث قد يساعد الأجهزة الوطنية المختصة بطريقة مباشرة، أو غير مباشرة عبر الأجهزة الشرطية العالمية والإقليمية. وهو المنطوي على مركز شكاوى جرائم الإنترنت "IC3"، الذي نستعرضه من حيث تبيان إطاره العام، ومظاهر تعاونه بخصوص التحري والتحقيق في جرائم الوسط الرقمي[3].

أ– الإطار العام لمركز شكاوى جرائم الإنترنت: بدأت فكرة إنشاء المركز سنة 1998 بالو.م.أ، بعد التسليم بلوج الجريمة إلى الوسط الرقمي، وضرورة التفرقة بينها وبين الجريمة التقليدية. حيث أراد مكتب التحقيقات الفدرالي "F.B.I" إيجاد آلية رقمية تمكنه من تعقب الجناة. ومنه تم تأسيس سنة 1999؛ أول مكتب للمركز في مدينة "موروغانتون بولاية واست فيرجينيا"، الذي سمي بمكتب شكاوى الاحتيال على الإنترنت، الموضوع بالشراكة مع المركز القومي لجرائم موظفي المكتب. وبحلول سنة 2002 تحولت التسمية إلى "مركز شكاوى جرائم الإنترنت – Internet crime complaint center"[4].

---

[1] **أنظر:** الإنتربول، **"**الجريمة السيبيرية**"**، مشاريع شرطية تركز على المستقبل، مرجع سابق، ص 06.

[2] **أنظر:** - Site officiel de l'Interpol, Criminilaté-Cybercriminalité-Operations-Simda botnet, Date de Publication: 13 Avril 2015, Date d'Accès: 01 mai 2018, Lien: https://www.interpol.int/fr/Centre-des-médias/Nouvelles/2015/N2015-038/.

[3] رجوعا إلى المفاهيم العامة حول جرائم الوسط الرقمي، المبينة في الفصل الأول؛ يمكن القول أن المركز يهتم بالجرائم التي تستعمل فيها شبكة الاتصال الدولية، وهو غير مختص بتلك المرتكبة عبر جهاز الإعلام الآلي غير المتصل بالشبكة.

[4] **أنظر:** نجاة بن مكي، مرجع سابق، ص 139،

يختص مركز شكاوى جرائم الإنترنت عموما؛ باستقبال التبليغات المتصلة بجرائم الإنترنت، من كل أنحاء العالم، وإجراء الأبحاث وإعداد ملف أولي بشأنها، مع إحالتها إلى الجهات المعنية[1]. الأمر الذي ينجز عبر الفصيلة رقم 08، المختصة بالعمليات السيبرانية في مكتب التحقيقات الفدرالي، والمختصين في الكشف والتحقيق الشبكي. مع إمكانية التعاون مع الشركات الشبكية والمؤسسات المالية ومقدمي الخدمات، والأجهزة المختصة الدولية والمقارنة[2]. وفي السياق نفسه جاء في التقرير السنوي لسنة 2016، الصادر عن المركز؛ أنه تلقى بين سنتي 2000 و2016 ما يعادل "348 762 3" شكوى. وهي المتصلة في أغلبها بعمليات الاحتيال الشبكي الموزعة عبر أغلب دول العالم[3].

ب- مظاهر تعاون مركز شكاوى جرائم الإنترنت على التحري والتحقيق في جرائم الوسط الرقمي:

ينطوي التعاون الدولي الذي ينجزه المركز؛ على الإخطارات والمساعدات التي يقدمها. فإذا ما رأى المركز أن القضاء الجزائري مختص بالنظر في الجريمة المبلغ عنها؛ يقوم بمعالجتها وإعداد ملفها الأولي ومن ثم يخطر الأجهزة الوطنية المختصة -بطريقة مباشرة أو غير مباشرة-، ويتعاون معها لفك الخيوط الرقمية والوصول إلى الدليل الرقمي. الأمر الذي لا يمكن تفعيله؛ إلا بعد تلقي الشكوى التي تتطلب ولوج الشاكي إلى الموقع: "www.IC3.gov"، ومن ثم إتباع الخطوات المبينة عبر صفحة الاستقبال، التي تبدأ بالنقر على زر "تقييد شكوى – File a complaint"، الذي يفتح إمكانية ذلك عبر الرابط "IC3.gov"[4].

وبمجرد الولوج الشبكي عبر الرابط المذكور؛ يتوجب على الشخص أن يصدق على شروط تقديم الشكوى. التي تبين بأنه قد يتعرض للمسائلة الجنائية عن المعلومات الخاطئة التي يقدمها، كما تعلمه بأنه سيتم وفقا للقانون؛ معالجة هذه المعلومات، مع إمكانية إحالتها إلى الأجهزة المختصة بالتحري والتحقيق في جرائم الإنترنت، التي قد تكون في الو.م.أ أو خارجها. بالإضافة إلى إبراز طريقة العمل المشفر الذي يعمل به المركز المنطوي على تقنية طبقة المقابس الآمنة "SSL"، ما يؤمن المعلومات والأدلة الرقمية المقدمة. وبعد التصديق على الشروط المذكورة؛ يقوم الشاكي بملء الفراغات التي تبين المعلومات الشخصية والتقنية ووقائع السلوك الشبكي محل الشكوى، وأي معلومات تفيد في فك خيوط الجريمة[5].

---

[1] **أنظر:** عبد الله عبد الكريم عبد الله، مرجع سابق، ص 115 و118 و120.

[2] **أنظر:** - Internet crime complaint center, "IC3-Brochure", USA, u d, p 02. Available on Link: https://www.ic3.gov/media/IC3-Brochure.pdf.

[3] **أنظر:** - Internet crime complaint center, "2016 Internet Crime Report", USA, u d, p 02. Available on Link: https://pdf.ic3.gov/2016_IC3Report.pdf.

[4] كما يحيل النقر على زر تقييد الشكوى نفسه؛ إلى رابطين آخرين. ينطوي الأول على شكوى متصلة بجريمة إرهاب أو تهديد مقدمة إلى مكتب التحقيقات الفدرالي، من خلال الرابط "FBI.gov". ويتصل الثاني بالشكوى المقدمة إلى المركز الوطني للأطفال المفقودين والمستغلين، حول الجرائم ذات الصلة، وذلك عبر الرابط "NCMEC". **أنظر في ذلك:**
- Official website of the Internet Crime Complaint Center, File a complaint-IC3.gov-I accept, n p d, Date of Access: 01 May 2018, Link: https://www.ic3.gov/default.aspx.

[5] **أنظر:** - Idem.

ثانيا: الأجهزة الأوروبية المتعاونة على التحري والتحقيق في جرائم الوسط الرقمي

زيادةً عن الأجهزة العالمية المتعاونة مع نظيرتها الوطنية، بخصوص التحري والتحقيق في جرائم الوسط الرقمي؛ توجد العديد من الأجهزة الأخرى ذات الاختصاص الدولي الإقليمي. على غرار الأوروبية منها، الحاملة للبعدين الشرطي والقضائي. وهي المتمثلة في وكالة الاتحاد الأوروبي للتعاون في مجال إنفاذ القانون "الأوروبول–Europol"، ووحدة التعاون القضائي الأوروبي "الأوروجست–Eurojust".

1. وكالة الاتحاد الأوروبي للتعاون في مجال إنفاذ القانون "الأوروبول–Europol": بعد أن انفراد "الإنتربول"، بالعمل الشرطي الدولي، لمدة طويلة من الزمن؛ عمل المجلس الأوروبي على إنشاء جهاز، يعنى بالتعاون الجنائي على مكافحة الإجرام التقليدي –والرقمي– في القارة الأوروبية. وهو ما نبينه من خلال التطرق إلى إطاره العام، ومظاهر تعاونه على التحري والتحقيق في جرائم الوسط الرقمي.

أ– الإطار العام لوكالة الاتحاد الأوروبي للتعاون في مجال إنفاذ القانون: بادر المجلس الأوروبي سنة 1992 عبر اتفاقية معالجة المعلومات حول النشاط الإجرامي في أوروبا؛ إلى إنشاء أول مكتب أوروبي للشرطة الجنائية. الذي باشر مهامه تدريجيا؛ بعد اعتماد الاتفاقية بتاريخ 26 جويلية 1995، ودخولها حيز النفاذ في 01 أكتوبر 1998[1]. على أن تعزز دوره سنة 2009 بموجب قرار صادر عن المجلس الأوروبي، ليسمى بـــ "المكتب الأوروبي للشرطة – L'office européen de police"، مقره مدينة "لاهاي بهولندا"[2]. الأمر الذي استقر من حيث المقر، وتطور بخصوص التسمية ليصبح سنة 2016 بموجب نظام صادر عن البرلمان الأوروبي ومجلس أوربا؛ يسمى بـــ "وكالة الاتحاد الأوروبي للتعاون في مجال إنفاذ القانون – L'Agence de l'Union européenne pour la coopération des services répressifs"[3].

ويتشكل "الأوروبول" الذي يضم 28 دولة أوروبية؛ من مجلس إدارة ومديرية تنفيذية وبعض الهيئات الاستشارية، التي يمكن للمجلس إنشاؤها بعد استشارة المدير التنفيذي. مع ضرورة إنشاء وحدة وطنية مزودة بضابط ارتباط أو أكثر في كل دولة، لضمان الاتصال بين الوكالة والسلطات المختصة فيها[4].

---

[1] **أنظر:** - GATTOLIN André, "Europol et Eurojust: perspectives d'avenir", Rapport d'information fait au nom de la commission des affaires européennes, N° 477, Assemblée Nationale, France, 17 Avril 2014, p 07 et 08. Disponible sur le Lien: https://www.senat.fr/rap/r13-477/r13-4771.pdf.

[2] **أنظر:** - BOOS Romain, (La lutte contre la cybercriminalité au regard de l'action des états), Thèse de doctorat, Droit privé et sciences criminelles, faculté de droit et sciences économiques et gestion de Nancy, Université de Lorraine, France, 2016, p 247.

[3] **أنظر:** - Règlement (UE) N° 2016/794, du 11 mai 2016, Relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol), Parlement Européen et Conseil de l'Union européenne, (J O U E) du 24 mai 2016. Disponible sur le Lien: https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0794.

[4] **أنظر:** - Official website of Europol, Partners and agreements-Member States, n p d, Date of Access: 02 May 2018, Link: https://www.europol.europa.eu/partners-agreements/member-states. **ET:** Art 07 et 08 et 09 et 11-1-s et 77/2; règlement (UE) N° 2016/794, op.cit.

على العموم تختص وكالة الاتحاد الأوروبي للتعاون في مجال إنفاذ القانون "الأوروبول"؛ بالعديد من المهام التي تباشرها من أجل تحقيق أهدافها الأساسية. حيث تهدف بالتعاون مع السلطات الوطنية؛ إلى الوقاية من الجرائم الخطيرة التي تمس دولتين أو أكثر من الدول الأعضاء، سيما تلك المبينة بالملحق الإضافي لنظام الوكالة الصادر سنة 2016. ولغرض تحقيق ذلك تمارس الوكالة العديد من المهام، التي تنطوي أهمها على معالجة المعطيات وتبادلها مع السلطات الوطنية المختصة، والتنسيق معها من خلال تنفيذ التحقيقات والإجراءات الداعمة لها، أو لوحدة التعاون القضائي الأوروبي "الأوروجست–Eurojust". كما تشارك في فرق التحقيقات المشتركة، وتفيد بالخبرات الإجرائية...الخ[1].

ب– مظاهر تعاون وكالة الاتحاد الأوروبي للتعاون في مجال إنفاذ القانون على التحري والتحقيق في جرائم الوسط الرقمي: أُرْفِق النظام الجديد للـــ "أوروبول" الصادر بتاريخ 24 ماي 2016 –النافذ منذ 01 ماي 2017–؛ بقائمة الجرائم التي يختص بالتعاون بشأن الوقاية منها ومكافحتها مع الدول أعضاء. حيث قسمها إلى 32 صنف، التي نجد من بينها جرائم الوسط الرقمي، الواردة تحت تسمية "إجرام المعالجة الآلية للمعطيات – Criminalité informatique"[2].

واقتناعا من "الأوروبول" بخصوصية جرائم الوسط الرقمي، خاصةً من حيث التحري والتحقيق والتعاون المنجز بشأنهما؛ تمت المبادرة بإنشاء العديد من الآليات المتخصصة، سيما المنطوية على؛ المركز الأوروبي لمكافحة جرائم الوسط الرقمي "EC3"، المستحدث سنة 2013؛ بغرض تدعيم الوقاية من هذه الجرائم ومكافحتها في إطار الاتحاد الأوروبي. الذي له اهتمام ثلاثي الأبعاد، استراتيجي وتقني وعملياتي. فيقوم من خلال ذلك بضمان التعاون اللازم مع الأجهزة المختصة في الدول الأعضاء. كما أنه مدعم بفرقة عمل مشتركة لمكافحة جرائم الوسط الرقمي "J-CAT"، التي تختص بمكافحة جرائم الوسط الرقمي الأكثر خطورة، الماسة بدول الاتحاد الأوروبي ومن ينتمون إليها من أشخاص[3].

وعلى العموم اعتبار "الأوروبول" على أنه إقليمي –أوروبي–؛ لا يعني استحالة تعاونه مع الأجهزة الجزائرية على التحري والتحقيق في جرائم الوسط الرقمي. حيث عالمية وتعقيد هذا النوع من الإجرام الحديث، وسبق إبرام "الأوروبول" لاتفاقيات تعاون مع دول خارج إطار الاتحاد الأوروبي[4]؛ يجزم بإمكانية التعاون مع الأجهزة الجزائرية.

---

[1] **أنظر:** - Arts 03 et 04; règlement (UE) N° 2016/794, op.cit.

[2] **أنظر:** - Annexe 01; idem.

[3] **أنظر:** - Official website of Europol, About Europol-European cybecrime centre "EC3", n p d, Date of Access: 02 May 2018, Link: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

[4] حيث سبق وأن أبرم اتفاقيات عملياتية، مع الشرطة الأمريكية والروسية والصينية والأسترالية...الخ. **أنظر في ذلك:**
- Official website of Europol, Partners and agreements-Operational agreements, n p d, Date of Access: 02 May 2018, Link: https://www.europol.europa.eu/partners-agreements/operational-agreements#.

2. وحدة التعاون القضائي الأوروبي "الأوروجست–Eurojust": لم يكتفي الاتحاد الأوروبي في إطار التعاون الإقليمي، المتصل بالوقاية من الإجرام ومكافحته؛ بجهاز "الأوروبول" المبين سابقا، رغم اختصاصاته الواسعة وتنظيمه المحكم. بل امتد الأمر إلى غاية إيجاد جهاز أوروبي آخر، له الوصف القضائي. وذلك بغرض تكملة حلقة الأجهزة الجنائية، التي تتوجب البعدين القضائي والشرطي. وهو الجهاز المنطوي على وحدة التعاون القضائي الأوروبي "الأوروجست–Eurojust"، الذي نبين فيما يلي؛ إطاره العام، ومظاهر تعاونه على التحري والتحقيق في جرائم الوسط الرقمي.

أ– الإطار العام لوحدة التعاون القضائي الأوروبي: تعد "الأوروجست" بمثابة الجهاز الإقليمي الحامل للطابع القضائي، الذي أنشأه مجلس الاتحاد الأوروبي بموجب قرار سنة 2002[1]. حيث يتواجد مقره على مستوى مدينة "لاهاي بهولندا"، ويتكون من تركيب بشري ينطوي على ممثلي الدول الأعضاء –28 دولة أوروبية، وحتى غيرها كالـــ"و.م.أ" والنرويج–، الذين يتوجب أن تتوفر فيهم صفة قضاة النيابة أو قضاة موضوع متمرسين أو ضباط شرطة قضائية بالتمرس نفسه، ليعملون على تنسيق عمليات التحقيق القضائي بين الأجهزة المختصة في الدول الأعضاء، متى تطلبت الضرورة المشروعة ذلك[2].

ويهتم "الأوروجست"؛ عموما بمكافحة كل أشكال الجرائم التي يختص بها "الأوروبول"، عندما تمس بدولتين أو أكثر من الدول الأعضاء، أو المصالح المشتركة لدول الاتحاد الأوروبي. كما يمكنها بموجب اتفاق خاص أن تختص في الجرائم التي تمس بدولة من الاتحاد وكيان دولي آخر، خاصةً من دول العام الثالث[3]. وفي هذا الصدد يعالج "الأوروجست"؛ حوالي 000 2 ملف سنويا، عن طريق مباشرة التحقيقات الجنائية أو طلب ذلك من الأجهزة الوطنية المختصة –مع ضرورة التنسيق–، سيما بخصوص الانتهاكات الماسة بالمصلحة المالية للاتحاد. كما يعزز التعاون القضائي، خاصةً من حيث حل إشكالات تنازع الاختصاص، بالتعاون مع الشبكة القضائية الأوروبية "EJN"[4].

ب– مظاهر تعاون وحدة التعاون القضائي الأوروبي على التحري والتحقيق في جرائم الوسط الرقمي: تعد جرائم الوسط الرقمي؛ من بين الجرائم التي تختص "الأوروجست" في التعاون مع الأجهزة الوطنية بشأن مكافحتها. والتي أطلقت عليها التسمية نفسهـــا الواردة في إطـــار عمل "الأوروبول"، المنطوية على

---

[1] **أنظر:** - Décision (UE) N° 2002/187/JAI, du 28 février 2002, Instituant Eurojust afin de renforcer la lutte contre les formes graves de criminalité, Conseil de l'Union européenne, Journal officiel de l'Union européenne, du 06 mars 2002. **amendée** par la décision du Conseil, N° 2003/659/JAI, du 18 juin 2003, (J O U E) du 29 septembre 2003. **Et par;** la décision du Conseil, N° 2009/426/JAI, du 16 décembre 2008, (J O U E) du 04 juin 2009. Disponible sur le Lien: http://www.eurojust.europa.eu/Pages/languages/fr.aspx.

[2] **أنظر:** - GATTOLIN André, "Europol et Eurojust: perspectives d'avenir", op.cit, p 22.

[3] **أنظر:** - Idem, p 21. **ET:** Art 27; Décision (UE) N° 2002/187/JAI, idem.

[4] **أنظر:** - Art 03; Décision (UE) N° 2002/187/JAI, idem. **ET:** Site officiel d'Eurojust, Bienvenue sur le site d'Eurojust, s d p, Date d'Accès: 05 mai 2018, Lien: http://www.eurojust.europa.eu/Pages/languages/fr.aspx.

"إجرام المعالجة الآلية للمعطيات – Criminalité informatique"[1]. وفي إطار ممارسة هذه المهام؛ كانت قد درست "الأوروجست" سنة 2016؛ حوالي 60 ملف جنائي متصل بجرائم الوسط الرقمي، وعقدت 13 اجتماع تنسيقي وشكلت 08 فرق تحقيق مشترك[2].

بالإضافة إلى الأعمال المذكورة؛ كان قد دخل "الأوروجست" في العديد من أعمال التعاون على التحقيق القضائي. سيما من حيث تبادل الخبرات والمعارف مع العديد من الجهات، مثل مقدمي خدمات "الإنترنت" على مستوى الـــ "و.م.أ". كما كان له الدور الفعال في إنشاء الشبكة الأوروبية لجرائم الوسط الرقمي "EJCN"، التي تسهل التعاون بين السلطات المختصة في الدول الأعضاء، عن طريق تبادل المعرفة الرقمية ذات الصلة بالتحقيقات الجنائية[3]. كما لا ننسى أن القرار المنشئ للـــ "أوروجست"؛ كان قد سمح –وفق ما بينا سابقا–؛ بإمكانية التعاون عبر اتفاقية خاصة مع دول العالم الثالث، ما يدفع لإمكانية تصور ذاك مع الأجهزة الجزائرية المختصة بالتحري والتحقيق في جرائم الوسط الرقمي.

ثالثا: الأجهزة الإفريقية والعربية المتعاونة على التحري والتحقيق في جرائم الوسط الرقمي

إذا كان بإمكان الأجهزة الجزائرية المختصة بالتحري والتحقيق في جرائم الوسط الرقمي؛ التعاون مع نظيرتها العالمية من منطلق الانتماء القانوني والجغرافي من جهة، والإقليمية الأوروبية تأسيسا على عدم معارضة نصوصها لذلك من جهة أخرى –النصوص الأوربية–؛ يمكن لها التعاون ومن باب أولى مع الأجهزة الإقليمية التي تنتمي إلى نطاقها، إما في إطار الانتماء الإفريقي الجغرافي، أو العربي القومي. الأمر الذي يمكن انجازه عبر آلية الاتحاد الإفريقي للتعاون الشرطي "الأفريبول–Afripol"، والمكتب العربي للشرطة الجنائية.

1. آلية الاتحاد الإفريقي للتعاون الشرطي "الأفريبول–Afripol": عملت الدول الإفريقية من خلال منظمة الاتحاد الإفريقي؛ على استحداث جهاز شرطي، كنسخة افريقية عن "الأوروبول" و"الأنتربول"، من حيث المهام الداخلة في اختصاصه وطريقة العمل والتركيبة المادية والعضوية. وهو ما تم تجسيده من خلال إنشاء ما تسمى قانونا بآلية الاتحاد الإفريقي للتعاون الشرطي "الأفريبول–Afripol"، التي نبين فيما يلي؛ إطارها العام، ومظاهر تعاونها على التحري والتحقيق في جرائم الوسط الرقمي.

أ– الإطار العام لآلية الاتحاد الإفريقي للتعاون الشرطي "الأفريبول–Afripol": بدأ الحديث الجاد عن ضرورة إنشاء آلية افريقية شرطية؛ من خلال إعلان الجزائر الصادر في 11 فيفري 2014، المعتمد من قبل رؤساء هيئات أركان الشرطة. الأمر الذي أجازه المجلس التنفيذي للاتحاد الإفريقي بالمقرر

[1] **أنظر:** - Art 04/1-b; Décision (UE) N° 2002/187/JAI, op.cit.

[2] **أنظر:** - Eurojust, "Rapport annuel 2016 d'Eurojust", La Haye, Pays-Bas, 2017, 30. Disponible sur le Lien: http://www.eurojust.europa.eu/doclibrary/corporate/Pages/annual-reports.aspx.

[3] **أنظر:** - Idem, p 30 et 31.

"EX.CL/Dec.820(XXV)"، خلال الدورة العادية الخامسة والعشرون المنعقدة بمدينة "ملابو دولة غينيا الاستوائية" بين 20 و24 جوان 2014. ولم تصبح "الأفريبول" موجودة قانونا؛ إلا بعد اعتماد نظامها الأساسي من قبل مؤتمر الاتحاد، المنعقد بمدينة "أديس أبابا دولة إثيوبيا" بتاريخ 30 جانفي 2017[1]. كما انعقدت أول جمعية عامة لها؛ بتاريخ 14 إلى 16 ماي 2017 بالجزائر العاصمة[2].

تتكون "الأفريبول" عضويا من دول الاتحاد الإفريقي، المنطوية على 55 دولة. كما تتشكل ماديا من مقر رئيسي متواجد على مستوى الجزائر العاصمة، ومكاتب اتصال. حيث يتوجب على كل دولة عضو في إطار قانونها الداخلي؛ إنشاء مكتب اتصال دائم مع المقر الرئيسي، الذي بدوره –المقر الرئيسي– يتكون من جمعية عامة ولجنة توجيه وأمانة[3]. كما يمكنها التعاون مع أجهزة أخرى افريقية وغير افريقية، على غرار "الإنتربول"، الذي اعتمد التعاون الرسمي مع "الأفريبول"؛ من خلال قرار الجمعية العامة السادسة والثمانون، المنعقدة بين 26 و29 سبتمبر 2017، بمدينة "بيكين الصينية"[4].

ويختص "الأفريبول" عموما؛ بالمساعدة على التحري والتحقيق الجنائي –بغض النظر عن المهام الأخرى–، من خلال مساعدة الأجهزة الشرطية الوطنية على التعاون فيما بينها، ومع الدول والمنظمات الخارجة عن الإطار الإفريقي. كما يضمن تبادل الخبرات والمعلومات لمنع ومكافحة الجريمة، سيما العابرة للحدود الوطنية وجرائم الإرهاب وجرائم الوسط الرقمي. الأمر الذي ينجز في إطار مبادئ عامة، تنطوي أساسا على عدم تدخل الدولة العضو في الشؤون الداخلية لدولة عضو أخرى، واحترام حقوق الإنسان والأخلاقيات الشرطية والمبادئ القانونية العامة، سيما قرينة البراءة[5].

ب– مظاهر تعاون آلية الاتحاد الإفريقي للتعاون الشرطي على التحري والتحقيق في جرائم الوسط الرقمي: مبدئيا لايمكن الحديث حاليا –على الأقل–؛ عن تعاون "الأفريبول" مع الأجهزة الوطنية المختصة بالتحري والتحقيق في جرائم الوسط الرقمي –ولا حتى بخصوص الجريمة التقليدية–. حيث تعد بمثابة الآلية الشرطية حديثة النشأة، التي لا تزال إلى غاية وقت تحرير العمل محل الطرح؛ في طور التأسيس ووضع الأسس النظرية والعملية العامة.

---

[1] **أنظر:** الديباجة؛ النظام الأساسي لآلية الاتحاد الإفريقي للتعاون الشرطي **"أفريبول"**، معتمد في الدورة العادية الثامنة والعشرون لمؤتمر الاتحاد الإفريقي، أديس أبابا، إثيوبيا، 30 جانفي 2017.

[2] **أنظر:** الموقع الرسمي للأمن الوطني الجزائري، **"**الاجتماع الأول لآلية التعاون الشرطي الإفريقي أفريبول**"**، تاريخ نشر: 14 ماي 2017، تاريخ التصفح: 05 ماي 2018، الرابط: http://www.algeriepolice.dz.

[3] **أنظر:** المواد 07 و23 و24؛ النظام الأساسي لآلية الاتحاد الإفريقي للتعاون الشرطي **"أفريبول"**، المرجع نفسه.

[4] **أنظر:** المادة 20؛ المرجع نفسه. **وأنظر أيضا:**

- Résolution N° 16, GA-2017-86-RES-16, Coopération avec le mécanisme africain de coopération policière (Afripol), Assemblée générale de l'Interpol, 86ème session, Beijing, Chine, du 26 au 29 septembre 2017. Disponible sur le Lien: https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2017/Le-President-Xi-Jinping-ouvre-l-Assemblee-generale-d-INTERPOL.

[5] **أنظر:** المواد 03 و04 و05؛ النظام الأساسي لآلية الاتحاد الإفريقي للتعاون الشرطي **"أفريبول"**، المرجع نفسه.

إلا أن الإطار العام المتصل بـــ "الأفريبول"؛ يدل على أنها ستكون مختصة بممارسة التعاون على التحري والتحقيق في جرائم الوسط الرقمي. التي أعطاها النظام الأساسي تحت تسمية الجريمة الالكترونية؛ الأهمية اللازمة إلى جانب الجريمة المنظمة وجرائم الإرهاب[1]. كما أكد رئيس "الأفريبول" السابق، اللواء عبد الغني هامل، في العديد من المناسبات أن الآلية؛ تعني أهمية كبيرة للتعاون من أجل مكافحة الجريمة المستحدثة العابرة للحدود[2]، التي تعد جرائم الوسط الرقمي أبرز صورها كما بينا سابقا.

2. المكتب العربي للشرطة الجنائية: في إطار تفعيل التعاون الأمني والشرطي بين الدول العربية؛ تمت المبادرة سنة 1982 بضرورة إنشاء مجلس وزراء الداخلية العرب. الذي وضع له نظام أساسي تم اعتماده بموجب قرار مجلس الجامعة رقم 4218 بتاريخ 23 سبتمبر 1982. ومن بين التركيبة الهيكلية للمجلس الجديد؛ نجد المكاتب المتخصصة، التي تنطوي على واحد منها له البعد الشرطي تحت تسمية المكتب العربي للشرطة الجنائية[3].

يختص المكتب المحدد مقره بالنص في مدينة دمشق "سوريا"؛ بالمجال الشرطي في إطار التعاون مع الدول الأعضاء، في جامعة الدول العربية أصلا ومجلس وزراء الداخلية العرب بالتبعية –22 دولة–. وفي هذا الإطار يهتم بتأمين وتنمية التعاون بين أجهزة الشرطة في الدول الأعضاء، بخصوص المكافحة الجنائية عموما، كما يقدم المعونة اللازمة في إطار التكوين والتدعيم الأجهزة الشرطية العربية[4]. الأمر الذي يمكن في إطاره التعاون مع منظمة الشرطة الجنائية الدولية "الإنتربول"، بموجب مذكرة التفاهم المبرمة سنة 1999. التي فتحت المجال أمام "الإنتربول" للمطالبة بإنشاء مقر إقليمي له في منقطة الشرق الأوسط وشمال إفريقيا، وهو ما قوبل بالرفض بموجب قرار مجلس وزراء الداخلية العرب رقم 557 لسنة 2009، المؤسس بعدم الحاجة لذلك[5].

وفي الإطار نفسه؛ عاودت منظمة الشرطة الجنائية الدولية "الإنتربول" محاولة إنشاء مقر إقليمي في المنطقة، من خلال الاجتماع المنظم من طرفه بتاريخ أكتوبر 2016، وهو ما نال الرضا المبدئي[6]. الذي

---

[1] **أنظر:** المادة 1/04-د؛ النظام الأساسي لآلية الاتحاد الإفريقي للتعاون الشرطي **"أفريبول"**، مرجع سابق.

[2] أهمها في إطار الكلمة التي ألقاها نيابةً عنه رئيس مكتب التعاون الدولي للمديرية العامة للأمن الوطني الجزائري؛ في إطار اجتماعات العمل المنعقدة بمقر **"**الأفريبول**"** بين 27 فيفري و01 مارس 2018؛ حول دليل العرائض والأدلة الرقمية بالتعاون مع **"**أوروماد – شرطة IV**"**. **أنظر في ذلك:** وحيد تاجي –مكتب الموقع الالكتروني، مرجع سابق، ص 66 و67.

[3] **أنظر:** المادتان 11 و16؛ النظام الأساسي لمجلس وزراء الداخلية العرب، معتمد في الدورة العادية الثامنة والسبعون لمجلس جامعة الدول العربية، القاهرة، مصر، 23 سبتمبر 1982. متوفر عبر الرابط:
http://leagueofarabstates.net/ar/legalnetwork/Pages/agreements_treaties.aspx.

[4] **أنظر:** المادة 1/11-3؛ المرجع نفسه.

[5] **أنظر:** أحمد جواد ربيعي ومن معه – عن الأمين العام للإنتربول، **"**منظمة التفاهم المبرمة بين الإنتربول ومجلس وزراء الداخلية العرب تبقى أساسا للتعاون بين المنظمتين**"**، مجلة أصداء الأمانة، الأمانة العامة لمجلس وزراء الداخلية العرب، ضفاف البحيرة، تونس، عدد 41، مارس 2017، ص 69 و70. متوفر عبر الرابط: http://www.aim-council.org.

[6] **أنظر:** المرجع نفسه، ص 69.

قاد في الأخير –بتاريخ أفريل 2018– إلى التصويت بالإجماع من قبل ممثلي الدول العربية المجتمعين بمقر "الإنتربول" بمدينة "ليون الفرنسية"؛ على استضافة مدينة الرياض "السعودية" للمقر الإقليمي[1]. الأمر الذي نراه بمثابة؛ استغلال "الإنتربول" للفراغ الشرطي العربي؛ الناتج عن عدم رقي عمل المكتب العربي للشرطة الجنائية إلى المستوى المطلوب بدايةً، وتعطل عمله الفعلي فيما بعد، سيما بعد تدهور الأوضاع الأمنية في سوريا.

الفرع الثاني: الأجهزة المقارنة المتعاونة على التحري والتحقيق في جرائم الوسط الرقمي

زيادةً عن الأجهزة الدولية المتعاونة على التحري والتحقيق في جرائم الوسط الرقمي، من منطلق الاتفاق الدولي الجماعي –العالمي والإقليمي–؛ يمكن أن تتعاون الأجهزة الجزائرية المختصة، مع نظيرتها ذات الاختصاص المحلي في الدول الأجنبية. التي ترتبط معها إما بالاتفاق الجماعي في إطار التعاون العام، أو بالاتفاق الثنائي الذي يبرم بين الدولتين بخصوص المسائل الجنائية، الذي يعد الأساس الغالب للتعاون مع الأجهزة المقارنة.

وفي هذا الإطار؛ تتعاون الأجهزة الجزائرية المختصة بالتحري والتحقيق في جرائم الوسط الرقمي؛ مع العديد من الأجهزة الأجنبية المقارنة. التي منها ما هي تقليدية تمت عصرنتها، ومنها ما تعد مستحدثة وفق متطلبات مواجهة جرائم الوسط الرقمي. الأمر الذي نحصره بخصوص دراسة الحال في الأجهزة الشرطية؛ الفرنسية(أولا) والأمريكية –الو.م.أ–(ثانيا)[2].

أولا: الأجهزة الفرنسية المتعاونة على التحري والتحقيق في جرائم الوسط الرقمي

تعتمد المنظومة القانونية الفرنسية ذات الصلة بمكافحة جرائم الوسط الرقمي، سيما في إطار التحري والتحقيق بشأنها؛ على العديد من الأجهزة منها من لها البعد الوطني المركزي ومنها ما هي إقليمية، التي تتوزع أساسا بين جهتي الأمن والدرك الوطنيين. حيث تهتم هذه الأجهزة بعد تكليفها القانوني بانجاز مضمون طلب التعاون محل الدراسة، كما أنها قد تحتاج له فتنبه الجهة المركزية المختصة، التي بدورها تطلبه من الجهة الأجنبية –التي قد تكون جزائرية–. وعليه سنعمل على التطرق إلى الإطار التنظيمي للأجهزة الفرنسية المختصة بالتحري والتحقيق في جرائم الوسط الرقمي، ومن ثم نبرز مظاهر تعاونها مع نظيرتها الجزائرية.

---

[1] **أنظر:** نواف القبيسي، "السعودية مقرا إقليميا لـ «الإنتربول» بالشرق الأوسط"، تاريخ النشر: 13 أفريل 2018، تاريخ التصفح: 10 ماي 2018، الرابط: https://thenewkhalij.news/سياسة/السعودية-مقرا-إقليميا-لـ«الإنتربول»-بالشرق-الأوسط .

[2] حيث اقتصرنا على الأجهزة الفرنسية والأمريكية؛ نظرا لسبقها وتميزها في مجال مكافحة جرائم الوسط الرقمي، عن طريق أجهزة جد فعالة، سبق لها التعاون مع نظيرتها الجزائرية. واكتفينا بالشرطية منها دون القضائية؛ نظرا لكونها الحلقة الأساس في عملية التعاون الدولي من حيث ممارسة إجراءات تنفيذه، أو الاعتماد على نتائجه بعد التنفيذ إذا كانت هي الجهة طالبة التعاون.

1. الإطار التنظيمي للأجهزة الفرنسية المختصة بالتحري والتحقيق في جرائم الوسط الرقمي: تُوَاجَهُ جرائم الوسط الرقمي إجرائيا في إطار القانون الفرنسي عموما؛ عن طريق العديد من الأجهزة، التي تنتمي أساسا إلى الجهات الأمنية ذات الاختصاص الأصيل في مكافحة الجريمة عموما –الأمن والدرك الوطنيين–[1]. الأمر الذي نبينه من خلال التطرق إلى الأجهزة الفرنسية المختصة بالتحري والتحقيق في جرائم الوسط الرقمي، التي تتبع الأمن الوطني، والدرك الوطني[2].

أ- أجهزة الأمن الوطني الفرنسي المختصة بالتحري والتحقيق في جرائم الوسط الرقمي: بالإضافة إلى الأجهزة الشرطية التقليدية، أنشأ الأمن الوطني الفرنسي؛ العديد من الأجهزة الحديثة التي تهتم حصرا بمكافحة جرائم الوسط الرقمي. حيث استحدث بموجب قرار وزير الداخلية بتاريخ 29 أفريل 2014، على مستوى المديرية المركزية للشرطة القضائية "DCPJ"؛ ما تسمى بنيابة المديرية لمكافحة جرائم الوسط الرقمي "Sous-direction de lutte contre la cybercriminalité-SDLC"، لتعوض الفرقة المركزية لمكافحة الإجرام المعلوماتي Brigade centrale de la répression de la criminalité informatique-BCRCI""، التي كانت قد استحدثت سنة 1994 بقرار من وزير الداخلية أيضا[3].

تمارس نيابة المديرية لمكافحة جرائم الوسط الرقمي "SDLC"، مهام مكافحة هذا النوع من الإجرام الحديث عن طريق ثلاثة 03 أجهزة رئيسية. التي تتمثل أهمها في الديوان المركزي لمكافحة الإجرام المتصل بتكنولوجيا الإعلام والاتصال " L'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication-OCLCTIC"، المستحدث بتاريخ 15 ماي 2000، ليتبع إلى غاية سنة 2014؛ نيابة مديرية الجريمة المنظمة والمالية[4].

---

[1] هذا بالإضافة إلى أجهزة أخرى، تعمل على تقديم المساعدة التقنية والمعلوماتية اللازمة للأجهزة الشرطية المختصة. التي تعتبر من أهمها؛ اللجنة الوطنية للحريات والمعلوماتية "La commission nationale de l'informatique et libertés"، والمركز الوطني لأمن أنظمة المعلومات "Agence nationale de la sécurité des systèmes d'information-ANSSI". **أنظر في ذلك:** -BOOS Romain, op.cit, p 293 et 294.

[2] للإشارة؛ تكاد تتفق أغلب الدراسات الفرنسية الحديثة؛ على عدم كفاية أجهزة مواجهة جرائم الوسط الرقمي. سيما مع عدم الاعتماد على هيئة وطنية متنوعة التركيبة. وفي هذا الإطار تتم المناداة بضرورة إنشاء هيئة وزارية مشتركة " Organisme interministériel de lutte contre la cybercriminalité"، بالإضافة إلى مركز نجدة وتحرك خاص بكل جرائم الوسط الرقمي"Centre d'alerte et de réaction aux attaques informatique-CERT"، الذي يوحد عمل المراكز الموجودة مسبقا، التي منها ما تخص بجرائم الوسط الرقمي الموجهة للإدارات والمؤسسات الكبيرة، ومنها ما تقتصر على مؤسسة محددة بذاتها كالمركز الخاص بمؤسسة "أورنج" "CERT-Orange-cc". **أنظر في ذلك:** .Idem, p p 293-300 -

[3] **أنظر:** - Site officiel de la police nationale française, Organisation-Direction centrale de la police judiciaire -Sous-direction de lutte contre la cybercriminalité, Date de Publication: 19 janvier 2015, Date d'Accès: 09 mai 2018, Lien: https://www.police-nationale.interieur.gouv.fr

[4] للإشارة يتمثل الجهازين الآخرين؛ في مكتب التنسيق الاستراتيجي "Le bureau de la coordination stratégique"، المتصل مباشرة بنيابة المديرية، بغرض تحديد إستراتيجيتها وفلسفة عملها. وجهاز ثانٍ ينطوي على قسم التوقع والتحليل " La division de l'anticipation et de l'analyse"، الذي يهتم بتوفير استجابة عامة للأفراد والشركات، غير المصنفة على أنها من بين المتعاملين أصحاب القيمة الحيوية، المعرضين لجرائم الوسط الرقمي. وهو القسم الذي يضم في تكوينه وحدة معلومات عامة، تحدد الآليات الرقمية المناسبة للوقاية من جرائم الوسط الرقمي ومكافحتها. **أنظر في ذلك:** .Idem -

ويختص الديوان "OCLCTIC"؛ بالعديد من المهام المتصلة بمكافحة جرائم الوسط الرقمي، إن عن طريق التنسيق، أو مباشرة الأعمال الإجرائية تنفيذا لأوامر القضاء، أو الربط كنقطة اتصال مع الأجهزة الأجنبية المتعاونة. وهو ما ينجز من خلال فصيلة الإنترنت "Section de l'internet"، المزودة بمنصة التوحيد والتوفيق وتوجيه البلاغات ضد المحتوى الشبكي غير القانوني "PHAROS"، والفصيلة العملياتية "Section opérationnelle" التي تباشر أعمال المكافحة. إضافةً إلى فصيلة أخرى تهتم بالعلاقات الدولية "Section des relations internationales"، التي تنجز كل ما يتصل بالمساعدة الدولية المتبادلة[1].

كما يحوي الهيكل التنظيمي للشرطة الفرنسية؛ العديد من الأجهزة الفرعية الأخرى. التي تهتم بالتحري والتحقيق في جرائم الوسط الرقمي. فزيادةً عن التقليدية منها؛ نجد بعض الفرق غير المركزية، التي قد يكون لها دور في التعاون الدولي محل الانجاز أو الطلب. وهي المنطوية بالدرجة الأولى على فرقة حماية العائلة "Brigade de protection de la famille-BPF"، المكونة من مجموعة التحري في جرائم القصر، سيما الاستغلال الجنسي عبر الإنترنت[2]. وكذلك فرقة التحري عن غش تكنولوجيا المعلومات "Brigade d'enquêtes sur les fraudes aux technologies de l'information-BEFTI". بالإضافة إلى فرقة مكافحة غش وسائل الدفع "Brigade des fraudes aux moyens de paiement-BFMD"[3].

ب- أجهزة الدرك الوطني الفرنسي المختصة بالتحري والتحقيق في جرائم الوسط الرقمي: بالتوازي مع الأجهزة الشرطية التابعة للأمن الوطني، تختص بالتحري والتحقيق في جرائم الوسط الرقمي أيضا؛ الأجهزة الشرطية التابعة للدرك الوطني. التي تنطوي أهمها على جهاز مركزي يسمى بمركز مكافحة الإجرام الرقمي "Le centre de lutte contre les criminalité numériques-C3N"، المستحدث بموجب الأمر الصادر في 13 مارس 2015. ليمارس مهام التحري والتحقيق من حيث التنسيق والمباشرة من جهة، وتقديم الدعم التقني للفرق المحلية من جهة أخرى[4].

---

[1] بالإضافة إلى فصيلة رابعة متصلة بالتكوين "Section de la formation". وأخرى خامسة مختصة بالمساعدة التقنية للبحث والتطوير "Section d'assistance technique, de recherche et de développement"، **أنظر في ذلك:**

- Site officiel de la police nationale française, Organisation-Direction centrale de la police judiciaire-Sous-direction de lutte contre la cybercriminalité, op.cit.

[2] الفرقة استحدثت سنة 2009 لتعوض فرقة حماية القصر "Brigade de protection des mineurs-BPM"، في كل المحافظات الفرنسية، ما عدا محافظة باريس، التي لا تزال قائمة في إطارها. **أنظر في ذلك:** .Idem -

[3] **أنظر:** حسين ربيعي، مرجع سابق، ص 164 و165.

[4] حيث يمارس مهام التحري والتحقيق في جرائم الوسط الرقمي؛ عن طريق التشكيلات المختلفة التابعة للدرك الوطني الفرنسي، بالإضافة إلى 03 ثلاثة دوائر مستحدثة -متصلة به- المنطوية على دائرة المساس بأنظمة المعالجة الآلية للمعطيات "Le département des atteintes aux système de traitement automatisé de données-DSTAD". ودائرة نشاطات الإنترنت غير القانونية "Le département des activités illicites sur internet-DA2I". بالإضافة إلى دائرة غير عملياتية تنطوي على؛ دائرة التوقع والحيوية الإقليمية "Le département de l'anticipation et de l'animation territoriale-D2AT". **أنظر في ذلك:**

- BOISSERIE Daniel, "Sécurités gendarmerie nationale", Avis fait au nom de la commission de la défense et des forces armées sur le projet de loi de finances pour 2016, N° 3115, Assemblée Nationale, France, 08 octobre 2015, p 51 et 52. Disponible sur le Lien: http://www.assemblee-nationale.fr/index.asp.

وفي إطار التنظيم المركزي أيضا؛ نجد ثلاثة 03 أجهزة أخرى لا تقل أهمية عن "C3N". حيث تعزز الدرك الوطني الفرنسي في إطار مكافحة جرائم الوسط الرقمي منذ سنة 1998 تدريجيا؛ بدائرة الإجرام الرقمي للخدمة التقنية المتصلة بالبحث القضائي والتوثيق " Département cybercriminalité du service technique de recherches judiciaires et de documentation-STRJD". ودائرة الإعلام الآلي والاليكترونيك لمعهد البحث الجنائي " Département informatique et électronique de l'institut de recherche criminelle de la gendarmerie nationale-IRCGN"[1]. بالإضافة إلى المركز الوطني للصور الإباحية للأطفال "Le centre national d'images pédopornographiques-CNAIP"[2].

كما يتوفر الهيكل التنظيمي للدرك الوطني الفرنسي المكافح لجرائم الوسط الرقمي؛ على العديد من الأجهزة الإقليمية التي تعمل أغلبها بالتنسيق مع نظيرتها المركزية المذكورة. على غرار فرق البحث الإقليمية "Les unités territoriales et de recherches"، التي تتعاون مع الأجهزة المركزية المختصة نظرا لتركيبتها العامة. بالإضافة إلى تشكيلات أخرى، سيما تلك المنطوية على دوائر البحث والتحري القضائي "Les Brigades départementales de renseignements et d'investigations judiciaires-BDRIJ"، التي تعد بمثابة القطب الجنائي للدرك الوطني، فتقدم الخبرات والتحليلات الرقمية اللازمة[3].

2. مظاهر تعاون الأجهزة الفرنسية المختصة بالتحري والتحقيق في جرائم الوسط الرقمي مع نظيرتها الجزائرية: بالعودة إلى التعاون الدولي على التحري والتحقيق في جرائم الوسط الرقمي؛ يمكن القول أنه جائز الممارسة بين الأجهزة الجزائرية والفرنسية المختصة بمواجهة هذا النوع من الإجرام الحديث. حيث القانون الوطني الجزائري لا يمنع ذلك –بشروط وفق ما بينا سابقا–، سيما بما ورد في القانون 09-04، والمرسوم الرئاسي رقم 15-261 المتصل بالهيئة الوطنية للوقاية من جرائم الوسط الرقمي ومكافحتها.

كما أن دخول الجزائر مع فرنسا في اتفاق تعاون قضائي في المجال الجزائي –ثنائي–، المصدق عليه بالمرسوم الرئاسي رقم 18-73 المبين سابقا؛ يجعل من باب التعاون بين الأجهزة المدروسة أمرا متوقعا ومشروعا، سيما إن حصل وفق الشروط المبينة محل الاتفاق، مع احترام مبدأ المعاملة بالمثل[4].

---

[1] حيث يختص الجهاز الأول "STRJD"؛ بمراقبة النطاق الشبكي بحثا عن المعلومات ذات المحتوى المجرم الماس بالأشخاص والأموال. وأما الجهاز الثاني "IRCGN"؛ فيهتم بتطوير الوسائل والطرق والبرامج التي تسمح باستشعار الصور الإباحية للأطفال أو استخراج المعطيات. **أنظر في ذلك:**

- Site officiel de la Gendarmerie nationale française, Accueil-Zooms-Cybercriminalité, s d p, Date d'Accès: 10 mai 2018, Lien: https://www.gendarmerie.interieur.gouv.fr/Zooms/Cybercriminalite.

[2] الذي له الدور المساعد للفرق والوحدات المباشرة لعمليات التحري والتحقيق ذات الصلة بالجرائم الإباحية للأطفال، بواسطة قاعدة البيانات الثرية بالصور التي تحتوي حاليا حوالي "470 000" صورة. إلا أنه مركز يعمل بالتعاون بين الدرك والأمن الوطنيين الفرنسيين. **أنظر في ذلك:** .Idem -

[3] **أنظر:** .Idem -

[4] الاتفاق الذي عوض الشق الجزائي من البروتوكول القضائي بين الجهاز التنفيذي الجزائري المؤقت وحكومة الجمهورية الفرنسية الموقع بباريس في 28 أوت 1962. **أنظر في ذلك:** المادة 29؛ مرسوم رئاسي رقم 18-73، مرجع سابق.

وبالفعل كانت قد أُنجزت بعض أعمال التحري والتحقيق في جرائم الوسط الرقمي، من الأجهزة الجزائرية المختصة؛ بطلب مساعدة وارد من نظيرتها الفرنسية. وعلى سبيل المثال قامت فصيلة البحث للدرك الوطني للجزائر العاصمة بتاريخ 11 مارس 2010، في إطار إنابة قضائية دولية صادرة عن محكمة استئناف باريس الفرنسية؛ بالتحقيق في قضية متصلة بمحاولة النصب الشبكي على مواطنين فرنسيين "Phishing"[1].

وانطلاقا من التقرير التقني الصادر عن الديوان المركزي لمكافحة الإجرام المتصل بتكنولوجيا الإعلام والاتصال "OCLCTIC" –الفرنسي المدروس سابقا–، وأعمال التحقيق التقني المنجزة من الفصيلة الجزائرية المدعمة بتقنيين 02 في مجال الوسط الرقمي؛ تم فك خيوط القضية وتحديد المشتبه فيهم مع توقيفهم وحجز الأجهزة الرقمية المتصلة بهم. وبالولوج إلى النطاق الافتراضي لهذه الأجهزة، سيما المتصل بذاكرة التحركات الشبكية والذاكرة الميتة؛ تم التوصل إلى عدد لا بأس به من المعلومات الرقمية التي تشكل الدليل الرقمي ضدهم[2].

ثانيا: الأجهزة الأمريكية (و.م.أ) المتعاونة على التحري والتحقيق في جرائم الوسط الرقمي

سيرا في الطرح نفسه المتصل بخصوصية جرائم الوسط الرقمي ومسرحها الافتراضي، سيما من حيث المواجهة الإجرائية وطابعها المعقد؛ بادرت قوانين الـــ "و.م.أ"؛ إلى التحيين والاستحداث اللازمين في مجال الأجهزة الممارسة للتحري والتحقيق في هذا النوع من الإجرام الحديث. التي قد تمارس ذلك في الإطار الداخلي الروتيني، أو اتصالا بالتعاون الدولي المنطوي على تنفيذه أو طلبه من نظيرتها الأجنبية وفق الشروط المحددة. الأمر الذي نبينه من خلال التطرق إلى أجهزة الـــ "و.م.أ" المختصة بالتحري والتحقيق في جرائم الوسط الرقمي، ومن ثم نبرز مظاهر تعاونها مع نظيرتها الجزائرية.

1. الإطار التنظيمي للأجهزة الأمريكية (و.م.أ) المختصة بالتحري والتحقيق في جرائم الوسط الرقمي:
يقوم الإطار التنظيمي السائد في الولايات المتحدة الأمريكية، من حيث مواجهة جرائم الوسط الرقمي ومسرحها الافتراضي المعقد؛ على العديد من التشكيلات. التي تنطوي أهمها على الأجهزة الفدرالية، الممارسة للتحري والتحقيق بالتنسيق مع الأجهزة المحلية. على أن تتمثل أهم هذه الأجهزة الفدرالية؛ في مكتب التحقيقات الفدرالي "FBI"، ودائرة الأمن الداخلي "DHS"[3].

---

[1] **أنظر:** - Centre de Prévention et de lutte Contre la Criminalité Informatique et la Cybercriminalité de la Gendarmerie Nationale, "Exécution des commissions rogatoires internationales-Exemples d'affaires traitées par les unités de la gendarmerie nationale et la sureté nationale se rapportant aux infractions liées aux TIC", Algérie, s d, p 02.

[2] **أنظر:** - Idem, p 03.

[3] بالإضافة إلى الأجهزة القضائية الخاصة ببعض قضايا جرائم الوسط الرقمي، على غرار نيابة الملكية الفكرية والقرصنة الالكترونية "Computer Hacking and Intellectual Property-CHIP"، المستحدثة سنة 1995 تحت تسمية؛ قسم الادعاء في جرائم الحاسوب والاتصالات "CTC". **أنظر في ذلك:** محمود محمد محمود جابر، مرجع سابق، ص 55.

أ- مكتب التحقيقات الفدرالي "Federal Bureau of Investigation-FBI": يعد الـــ "FBI"؛ أهم الأجهزة الأمريكية المكافحة لجرائم الوسط الرقمي عموما، سيما بخصوص جرائم أنظمة المعلومات التابعة للإدارات الأمريكية. الأمر الذي ينجز عبر العديد من الفروع، سيما القسم الرقمي "Cyber Division" المعاد تنظيمه سنة 2012؛ ليضمن الأمن الشبكي. والقسم الجنائي "Criminal Division"، الذي يختص بالتحري والتحقيق في جرائم المحتوى الرقمي. بالإضافة إلى الفرقة الوطنية المشتركة للتحقيق الرقمي "National Cyber Investigative Joint Task Force"، المستحدثة سنة 2008 لتعمل بالشراكة مع القطاع الخاص؛ على اكتشاف ومنع الاختراق والقرصنة الرقميين، زيادةً على تطوير آليات الوقاية الرقمية من الهجمات التي تستهدف الشركات والأشخاص[1].

كما استحدث الـــ "FBI" سنة 1997 ما يسمى بالتحالف الوطني لتكوين خبراء جرائم الوسط الرقمي "National Cyber Forensics Training Alliance-NCFTA"، الذي يحلل التهديدات الشبكية ثم يقوم بإبلاغ الجهات المعنية –الضحية المحتمل والشرطة–، كما يقوم بالتحريات والتحقيقات ذات الصلة. وبالإضافة إلى ذاك قام التحالف بالشراكة مع مركز شكاوى جرائم الإنترنت "IC3" –المدروس سابقا–؛ باستحداث وحدة المبادرة الرقمية ودمج الموارد "Cyber Initiative and Resource Fusion Unit-CIRFU"، التي تعد بمثابة منصة حوار القطاعين العام الخاص، من حيث البحث والتوجيه المتصلين بالتهديدات الرقمية[2].

ب- دائرة الأمن الداخلي "Department of Homeland Security-DHS": تم إنشاء دائرة الأمن الداخلي بعد أحداث الـــ 11 سبتمبر 2001؛ بهدف التنسيق بين مختلف الوكالات الفدرالية. حيث تتكون من العديد من المصالح التي كانت متصلة في السابق بوزارتي العدل والخزينة وبعض الجهات المستقلة. وتتمثل مهامها الأساسية في حماية الحدود، التي تم تطويرها لتشمل جرائم الوسط الرقمي، عن طريق مركز متكون من ثلاثة 03 وحدات رئيسية[3].

وتنطوي الوحدات المذكورة؛ على وحدة خبراء الوسط الرقمي "Computer Forensics Unit"، التي تهتم بتحليل الأجهزة الرقمية المضبوطة أثناء التحري والتحقيق. ووحدة جرائم الوسط الرقمي "Cyber Crimes Unit"، التي تباشر تحقيقات خاصة، سيما التسرب لتحديد الغش والتقليد والتهرب الجمركي. وأخيرا وحدة استغلال الأطفال "Child Exploitation Unit"، المهتمة حصرا بمكافحة الإجرام الشبكي المتصل بالمحتوى الإباحي للأطفال[4].

---

[1] **أنظر:** - LegiGlobe, "Cybercriminalité (br, cn, es, us, nl, uk)", Projet de développement du Réseau Francophone de Diffusion du Droit-Droit comparé, paris, France, 2013, p 13 et 14. Disponible sur le Lien: http://legiglobe.rf2d.org/cybercriminalite-2/2013/09/05/.

[2] **أنظر:** - Idem, p 14 et 15.

[3] **أنظر:** - Idem, p 15.

[4] **أنظر:** - Idem, p 15 et 16.

2. مظاهر تعاون الأجهزة الأمريكية (و.م.أ) المختصة بالتحري والتحقيق في جرائم الوسط الرقمي مع نظيرتها الجزائرية: رجوعا إلى التعاون الدولي على التحري والتحقيق في جرائم الوسط الرقمي؛ يمكن القول أن الأجهزة الجزائرية المختصة؛ تتعاون أيضا مع التعاون مع نظيرتها الأمريكية –و.م.أ–. وذلك وفق الإطار القانوني الوطني نفسه، المحدد بما ورد في القانون رقم 09–04، والمرسوم الرئاسي رقم 15–261 المتصل بالهيئة الوطنية للوقاية من جرائم الوسط الرقمي ومكافحتها.

أما بخصوص الأساس القانوني الاتفاقي، فبغض النظر عن الصكوك الدولية الجماعية ذات الصلة بالتعاون الدولي في المسائل الجزائية المذكورة سابقا؛ كانت قد أبرمت الجزائر سنة 2010 اتفاقية ثنائية مع الـــ "و.م.أ" بخصوص التعاون القضائي في المجال الجزائي، التي أصبحت نافذة في الجزائر بعد التصديق عليها ونشرها بتاريخ 03 ماي 2011، عبر المرسوم الرئاسي رقم 11–184[1].

وفي إطار التكريس العملي للتعاون الجنائي بين الجزائر و الـــ "و.م.أ"؛ تم انجاز العديد من الطلبات، المتصلة بالتعاون الجنائي على مواجهة جرائم الوسط الرقمي –والتقليدية أيضا–. حيث حدث وأن تم التعاون سنة 2009 بين المديرية العامة للأمن الوطني الجزائري ومكتب التحقيقات الفدرالي الأمريكي "FBI"[2]، بخصوص جريمة مساس بأنظمة المعالجة الآلية للمعطيات، المنطوية على الاحتفاظ والمتاجرة بمعلومات رقمية تم الحصول عليبيها عن طريق الغش[3].

تلقى وزير العدل الجزائري بتاريخ 17 ديسمبر 2009؛ برقية من قبل فرع الجزائر لمكتب الـــ "FBI"، يتضمن طلب مساعدة قضائية بخصوص التحقيق الجاري من قبل مكتب "دوتروا – Detroit"، حول وقائع منطوية على قيام جهة مجهولة بقرصنة أكثر من "000 10" بطاقة ائتمان "VISA"، عن طريق القيام بتنصيب برنامج خبيث يحتفظ بالمعلومات ذات الصلة بمجرد استعمالها من قبل أصحابها، مع تحويلها إلى خادم آخر متواجد بألمانيا. وبعد قيام الـــ"FBI"؛ بالتحقيقات اللازمة بالتعاون أجهزة وطنية مقارنة، سيما الألمانية منها؛ تم التوصل إلى شخصين كمشتبه فيهما، واحد منهما يتواجد بمدينة عنابة الجزائرية. الذي بعد تنفيذ المساعدة القضائية بشأنه من قبل الشرطة القضائية التابعة للأمن الوطني؛ تم توقيفه وتقديمه أمام وكيل الجهورية لمحكمة عنابة بتاريخ 07 ماري 2010[4].

---

[1] على أن الاتفاقية نفسها؛ تؤكد على إمكانية ممارسة التعاون؛ انطلاقا من أحكام اتفاقيات أخرى أو نصوص القانون الداخلي، أو أي إجراء تلقائي يكون مقبولا من الطرفين. **أنظر:** المادة 19؛ مرسوم رئاسي رقم 11-184، مرجع سابق.

[2] المساعدة التي بما أنها أنجزت قبل إبرام الاتفاقية الثنائية المبينة أعلاه؛ يمكن تحديد الأساس القانوني لتنفيذها؛ في الاتفاقيات الدولية الجماعية ذات الصلة، سيما المتعلقة بمكافحة الجريمة المنظمة عبر الوطنية لسنة 2000 -سابقة الذكر-، وخاصةً مبدأ المعاملة بالمثل الذي يحكم مثل هذه الحالات في العادة.

[3] **أنظر:** - Centre de Prévention et de lutte Contre la Criminalité Informatique et la Cybercriminalité de la Gendarmerie Nationale, "Exécution des commissions rogatoires internationales-Exemples d'affaires traitées par les unités de la gendarmerie nationale et la sureté nationale se rapportant aux infractions liées aux TIC", op.cit, p 01.

[4] **أنظر:** - Idem, p 01 et 02.

كخلاصة للباب الأول من دراسة الحال؛ يمكن القول أن المشرع الجزائري والمقارن وقبلهما الفقه الجنائي المعاصر؛ لم يصلوا إلى مرحلة تحيين الأعمال الإجرائية ذات الصلة بالتحري والتحقيق في جرائم الوسط الرقمي –القادمة بالدراسة–؛ إلا بعد أن سلموا بحداثة وتعقيد كل ما ذكر في الباب الأول، سيما تلك المتعلقة بالخصوصية القانونية الموضوعية والإجرائية من جهة، أو الأجهزة المختصة بالمتابعة الجنائية من جهة أخرى.

فمنذ بدايات ظهور وتطور العناصر المادية المكونة للسوط الرقمي عموما، من جهاز إعلام آلي وشبكة اتصال دولية، سيما بعد استحداثهما للنطاق الافتراضي المعقد؛ بدأت السلوكيات الإنسانية في التطور نحو التعقيد غير المسبوق. خاصةً مع ولوج السلوكيات ذات الطابع الضار إلى هذا الوسط، ومنه ولوج التجريم بالتبعية ليضفي الشرعية اللازمة قبل المتابعة وتوقيع الجزاء الجنائي المناسب. وهو ما دفع بالمشرع إلى ضرورة العمل على إيجاد التوافق بين النص التشريعي والطابع الرقمي الحديث.

ولج المشرع ليجرم ويعاقب على العديد من السلوكيات الرقمية، المتمثلة في جرائم المساس بأنظمة المعالجة الآلية للمعطيات، والعديد من السلوكيات الأخرى المرقمنة؛ المنطوية على تلك التقليدية التي ترتكب عبر النطاق الافتراضي للوسط الرقمي أو يكون المسهل لارتكابها. الأمر الذي أكسبها نوع من الخصوصية القانونية المنفصلة عن النظرية العامة للجريمة، انطلاقا من الخصوصية الرقمية ذاتها، المنفصلة عن الوسط المادي التقليدي.

كل ما ذكر من تفاعل حاصل بين الوسط الرقمي بالبعد التقني والجرائم المتصلة به بالبعد القانوني الجنائي؛ أدى بالضرورة إلى العمل القانوني للوصول إلى توافق إجرائي اللازم، في إطار حلقة جنائية واجبة التسلسل والترابط، انطلاقا من القاعدة القائلة أن دور النص الإجرائي يبدأ عند انتهاء دور النص الموضوعي. مع ضرورة أن تكون القاعدة الإجرائية من الطبيعة نفسها القائمة عليها القاعدة الموضوعية، وإلا وقعنا في العجز المؤدي إلى تعطيل دور النص الموضوعي في المجتمع.

والحقيقة أن النص الإجرائي في بداية الأمر بقي عاجزا أمام مواجهة هذا النوع من الإجرام الحديث، للعديد من الأسباب سيما ما تتصل منها بالأجهزة المباشرة للتحري والتحقيق. الأمر الذي أدى إلى التوجه نحو التحيينات المتتالية، عبر تدريب الأجهزة التقليدية و/أو استحداث أخرى جديدة قضائية وغير قضائية، مع ضرورة الاعتماد على العمل الجماعي كفريق أولا، واللجوء إلى التعاون الدولي ثانيا. بالإضافة إلى الاعتماد على الوقاية الرقمية، كوسيلة تقنية تقي من جرائم المساس المذكورة.

إلا أن كل التحيينات المتصلة بالأجهزة المذكورة؛ تظل غير مجدية، إلا إذا ما أردفها المشرع بتحيينات أخرى تنصب على إجراءات التحري والتحقيق الممارسة من طرفها. التي قد تكون تقليدية فترقمن، أو رقمية مستحدثة. وهي التي سنتطرق إليها بنوع من التفصيل؛ في الباب الثاني من الدراسة.

البـــــاب الثانـي

مباشرة إجراءات التحري والتحقيق في جرائم الوسط الرقمـي

يعد الإطار العام لإجراءات التحري والتحقيق في جرائم الوسط الرقمي، وفق الطرح المذكور بالخصوصية المعقدة نفسها؛ بمثابة القاعدة المرجعية التي تنطلق منها عملية مباشرة الإجراءات عموما. فالمباشرة تكون من الأجهزة المذكورة بكل أحكامها وتفريعاتها، كما أنها تمارس أساسا؛ في النطاق الافتراضي للوسط الرقمي كمسرح جرمي حديث –التي قد تمارس عرضا في غير ذلك، فتعتبر مساعدة–. بالإضافة إلى الفصل قولا وممارسةً؛ من حيث حمل إجراءات التحري والتحقيق في جرائم الوسط الرقمي؛ للخصوصية الإجرائية الحديثة غير المعهود التعامل مع مثلها في السابق، سيما من الأجهزة التقليدية المعروفة، سواءً الشرطية أو القضائية.

وعلى كل حال تعد مباشرة إجراءات التحري والتحقيق؛ الحلقة الأهم في الدراسة، نظرا لكون الخصوصية السابقة بالذكر والأجهزة الداخلة في الإطار العام المذكور؛ بمثابة التوطئة الإجرائية، حتى تباشر الإجراءات فعلا، لنصل في الأخير إلى المواجهة المرجوة لجرائم الوسط الرقمي، عبر مكافحتها –أو حتى الوقاية منها، كما سنرى لاحقا–. سيما وأن من بديهيات الإجراءات الجزائية عموما؛ مباشرتها من خلال الأعمال والأذون الأوامر؛ وصولا إلى محورها الاساس، ألا وهو الدليل الجنائي –على غرار الدليل الرقمي الحديث–، الذي يقتصر بخصوص التحري على دليل الإدانة، وفي التحقيق على دليل الحقيقة بالإدانة أو البراءة.

فمباشرة إجراءات التحري والتحقيق في جرائم الوسط الرقمي؛ تقوم على الطرح نفسه المذكور. وان آثرنا برغبة باحث في دراستنا هذه؛ أن نميز من حيث المباشرة بين الإجراءات الأساسية والأخرى المساعدة. وذلك انطلاقا من طبيعة الإجراءات محل المباشرة، التي اكتسبت بدورها الكثير الخصوصية الحديثة الرقمية و/أو المرقمنة –على حسب الحالة والحاجة–. مع التأكيد على أن الطرح التقليدي في سرد هذه الإجراءات محل المباشرة؛ قد تجاوزه الزمن هو الآخر، سيما وأننا نمحور كل هذه الإجراءات حول الدليل الرقمي الجنائي بالأساس، الذي له أعمال إجرائية أساسية لاستخراجه، وأخرى مساعدة تقليدية وحديثة رقمية وغيرها.

وفي السياق نفسه المتصل بالدليل الرقمي الجنائي؛ يمكن القول أنه أحدث ثورة إجرائية غير معهودة، التي غيرت كل المفاهيم المعمول بها، حول وسائل الإثبات عموما والدليل الجنائي خاصةً. حيث أصبحت له ماهية قانونية مختلفة عن تلك المتصلة بالدليل التقليدي المعروف، إن من حيث المفهوم الدائر بين التعريف والخصائص، أو بخصوص المميزات، التي يظهر من خلالها؛ أننا بصدد النظر إلى نتائج الخصوصية المعقدة للمسرح الجرمي الافتراضي السابقة بالدراسة. مع التأكيد على البعد التقني، الذي يؤسس للخصوصية والمميزات، خاصةً من حيث كثرة تفريعاته من خلال الأقسام والمصادر وما إلى ذلك، من مظاهر مختلفة للمعلومات والبيانات الرقمية.

كما أن الحديث عن الدليل الجنائي الرقمي؛ يفتح الباب حول التساؤل في مدى حجيته القانونية والقضائية. الأمر الذي يدفع لا محال إلى الدخول في دوامة النظر المزدوج؛ إلى النص التشريعي من جهة، والاجتهاد القضائي والتفسير الفقهي من جهة أخرى، سيما من حيث النظرة التشريعية القائمة، ومدى إمكانية التعامل مع النطاق الافتراضي المعقد، الذي اكتسب الكثير من الخصوصية الحديثة، المتزايدة بوتيرة تطور ديناميكي غير مألوفة.

ولايمكن أن تصل الأجهزة المختصة بالتحري والتحقيق في جرائم الوسط الرقمي؛ إلى الدليل الجنائي الرقمي، كمحور أساس في مباشرة الإجراءات عموما؛ إلا عبر الاعتماد على أعمال جوهرية –جوهرية في نظر الباحث–، تنطوي على المعاينة والتفتيش المرقمنين. مع مراعاة البعد التقني لكل منهما، من خلال الاعتماد على الدعم التقني من المختصين في الوسط الرقمي أولا، وممارسة الحجز المرقمن بالدقة اللازمة ثانيا.

كما يمكن أن تعتمد الأجهزة المختصة في مواجهة جرائم الوسط الرقمي؛ على إجراءات مساعدة لتلك الجوهرية المشار إليها أعلاه. فتقوم في هذا الإطار بمباشرة إجراءات تقليدية مساعدة؛ على غرار أعمال التنصت والتسرب والسماع والاستجواب. بالإضافة إلى بعض الأوامر والأذون ذات الاتصال المباشر بالشخص محل التابعة –مشتبه فيه أو متهم–، كالإذن بالتوقيف للنظر والأمر بالوضع تحت المراقبة القضائية أو الأمر بالإيداع في الحبس المؤقت.

مع إمكانية العمل على مباشر إجراءات مساعدة ذات طابع حديث، التي منها ما وجدت خصيصا لمواجهة جرائم الوسط الرقمي؛ كعمل مراقبة الاتصالات الالكترونية –الاتصالات الرقمية–، والتحفظ العاجل على المعطيات الرقمية المخزنة، وتحديد هوية المشتبه فيه الرقمي، وممارسة الأمر بإنتاج وتقديم المعطيات الرقمية. بالإضافة إلى الأمر بمنع المشتبه فيه من مغادرة التراب الوطني، أو بوضع المتهم تحت المراقبة الالكترونية.

وعلى العموم؛ آثرنا من باب التطرق إلى مباشرة إجراءات التحري والتحقيق في جرائم الوسط الرقمي، انطلاقا من طرح الباحث الخاص؛ التركيز على الإجراءات الأساسية للتحري والتحقيق في هذه الجرائم الحديثة(فصل أول)، بدايةً من محورها الأساس المنطوي على الدليل الجنائي الرقمي، والأعمال الجوهرية المعتمدة لاستخراجه.

على أن ننتقل بعد ذلك للتعريج على الإجراءات المساعدة، المعتمدة من طرف الأجهزة المختصة عند مباشرة التحري والتحقيق في الجرائم نفسها(فصل ثانٍ)، التي تلعب دور المساعد و/أو المكمل للأعمال الجوهرية المشار إليها أعلاه، وذلك عبر العديد من الإجراءات التقليدية والحديثة –الرقمية والمرقمنة–، الدائرة بين الأعمال والأذون والأوامر.

الفـــصل الأول

الإجراءات الأساسية للتحري والتحقيق في جرائم الوسط الرقمي

وفق ما بينا من خلال التقديم للباب الثاني محل الدراسة، نرى بوجهة نظر خاصة؛ أن تعقيد جرائم الوسط الرقمي، المستمد أساسا وأصلا من جانبه التقني الحديث وسريع التطور؛ دفع بإجراءات التحري والتحقيق ذات الصلة إلى اكتساء طابع الحداثة والتعقيد نفسه، مخرجا إياها من بوتقة الاستقرار الإجرائي الذي شهدته في ظل الإجرام التقليدي منذ مدة ليست بالقريبة، وحتى نظيره الحديث غير المتصل بالوسط الرقمي على اختلاف أشكاله.

ولعل أساس التحول الإجرائي المذكور؛ ينطوي أصلا على التحول في طبيعة الدليل الجنائي المعتمد لإثبات الجريمة من عدمها –البحث القضائي عن الحقيقة–. حيث بعد أن كان يتعامل القاضي –تحقيق وحكم–، مع الدليل المادي الملموس أو حتى غير المادي –التقليدي غير الرقمي، الذي قد لا يكون ماديا–؛ وجد نفسه مضطرا للتجاوب مع دليل رقمي قائم على معطيات رقمية افتراضية معقدة أو فائقة التقيد، سيما بالنسبة إلى قاضٍ بتكوين قانوني محض. الأمر الذي قد يكون معقدا ويستحيل التعامل معه، حتى من قبل مختصي الوسط الرقمي.

فرغم إمكانية لجوء الجهات المختصة بالتحري والتحقيق في جرائم الوسط الرقمي، كما سنرى لاحقا؛ إلى ممارسة العديد من الإجراءات، التي منها الرقمية ومنها المرقمنة وحتى غير ذلك، خاصةً وأن المشرع الجزائري يعتمد –كأصل عام– مبدأ الإثبات الحر في المواد الجنائية، ولا يقيد القضاء الجزائي بوسيلة إثبات معينة. إلا أن الطابع الرقمي المعقد؛ يدفع ضمنا إلى التمييز بين الإجراءات التي منها، ما نعتبرها جوهرية أساسية، لها علاقة مباشرة باستخراج الدليل الرقمي، ومنها ما هي مساعدة أو داعمة للأولى الجوهرية.

كما خلق الدليل الرقمي نوعا من التضارب الفقهي، القائم على العديد من الأسباب والمعايير، التي لها ما يؤسسها وما يجعلها جديرة بالدراسة، بحثا عن الوصول إلى ما يقتنع به الباحث ويقنع من خلاله. وعلى العموم سواءً رجحت كفت الاتجاه المعارض أو المؤيد؛ فالدليل الرقمي أصبح أمرا واقعا لا مفر منه، يتوجب على القضاء التعامل معه والبحث فيه، بعد استخراجه بالأعمال اللازمة لذلك. التي تختلف وتتنوع على حسب منظور الدارس لها، خاصةً في ظل غياب حصر قانوني تشريعي لها، وهو الأمر المفهوم نظرا للتطور الديناميكي السريع للوسط الرقمي نفسه.

وعلى العموم يمكن القول؛ أن الإجراءات الأساسية المعتمدة عند مباشرة التحري والتحقيق في جرائم الوسط الرقمي؛ تقوم أصلا على محور قانوني يتمثل في الدليل الرقمي الجنائي، الحامل للخصوصية الرقمية الحديثة المعقدة نفسها القائم عليها الوسط الرقمي، والذي سنعمل فيما يلي على تحديد ماهيته الفنية والقانونية(مبحث أول)، ومن ثم محاولة إبراز أهم –إلى حد الآن– الأعمال الجوهرية المعتمدة لاستخراجه(مبحث ثانٍ).

المبحث الأول

الدليل الرقمي محور التحري والتحقيق في جرائم الوسط الرقمي

تتركز إجراءات التحري والتحقيق في جرائم الوسط الرقي عموما على الدليل الرقمي، الذي تمهد له إجراءات التحري الأولي وتستخرجه إجراءات التحقيق القضائي. حيث تنطوي النتيجة النهائية لكل الإجراءات المتبعة –التالية بالدراسة–؛ على الدليل الرقمي الذي قد يثبت الجريمة في جهة المتهم أو ينكرها. الأمر الذي يبدوا وكأنه لا يتعدى مفهوم الدليل الجنائي التقليدي مضمونا وأثرا، إلا أنه في الحقيقة؛ يخرج عن ذلك بالعديد من الأحكام المستحدثة ذات الطابع الخاص المعقد.

وفي الإطار نفسه؛ وضع الفقه الجنائي انطلاقا من النصوص التشريعية السارية والمواقف القضائية ذات الصلة؛ العديد من الأحكام التي تتماشى مع الطبيعة الرقمية الافتراضية لجرائم الوسط الرقمي، والدليل الجنائي المتصل بها. ولو أن الأمر يختلف من نظام إثبات إلى آخر، سيما في ظل التباين الجوهري بين الإثبات الجنائي في النظام "الفرنكوجرماني" –اللاتيني– ونظيره النظام "الأنجلوسكسوني".

وعلى العموم لم يكن القانون الجزائري –تشريعا وفقها–؛ بمنأى عن التحول المذكور بخصوص الدليل الجنائي المتصل بجرائم الوسط الرقمي. حيث وان كان يعمل بالأحكام العامة للنظام "الفركوجرماني"، إلا أن له ما يميزه. الأمر الذي نبينه بالتطرق أولا إلى ماهية الدليل الرقمي الجنائي(مطلب أول)، على أن نبرز بعد ذلك حجيته القانونية والقضائية في المنظومة الجزائرية وغيرها(مطلب ثانٍ).

المطلب الأول: ماهية الدليل الرقمي الجنائي

لم يستقر الفقه الجنائي الحديث على الأحكام العامة المحددة لماهية الدليل الرقمي، إن من حيث الشكل سيما بخصوص التسميات المعتمدة[1]، أو من حيث المضمون المتصل بالمفهوم والبعد التقني. حيث يختلف الوضع من دراسة إلى أخرى، وان نجد في إطارها العديد من النقاط التي تقارب بينها، سيما بخصوص المغزى العام الرامي إلى مواجهة جرائم الوسط الرقمي، عبر إثباتها ومعاقبة مرتكبيها.

وفي سبيل تحديد ماهية الدليل الرقمي الجنائي؛ يتوجب علينا التطرق إليه من العديد من الزوايا. المنطوية أساسا على إبراز مفهومه العام(فرع أول)، الذي من خلاله يمكننا التوصل إلى البعد التقني المنطوي على التنوع الذي يقوم عليه(فرع ثانٍ).

[1] حيث تطلق على الدليل الرقمي العديد من التسميات الأخرى. على غرار تلك الشائعة المنطوية على الدليل الالكتروني، وغيرها مثل الدليل السيبراني -أو السيبيري- والدليل الافتراضي والمعلوماتي...الخ. إلا أنا نعتمد تسمية الدليل الرقمي، للأسباب نفسها المبينة سابقا بخصوص اعتماد تسمية جرائم الوسط الرقمي، بدلا عن الجرائم الالكترونية وغيرها من التسميات. بالإضافة إلى أننا نقصد تضييق المفهوم، فكل دليل غير رقمي حتى وان كان الكتروني؛ يعد خارجا عن المفهوم المقصود. وان كان من الممكن اعتماده كدليل جنائي لإثبات جرائم الوسط الرقمي، رغم خروجه عن مفهوم الدليل الرقمي.

الفرع الأول: مفهوم الدليل الرقمي الجنائي

في الإطار القانوني عموما والجنائي خاصةً، لا يمكن الحديث عن الحق وإحقاقه؛ إلا عبر إثباته بالدليل المناسب والمقرر قانونا. فتعدد وسائل الإثبات[1] الجنائي وتنوعها؛ ما هو إلا وسيلة لإقامة الدليل –دليل الإدانة أو النفي لإظهار الحقيقة–[2]. الأمر الذي يعطي أهمية كبيرة للدليل الرقمي، سيما من حيث ضرورة مواجهة تعقيداته، بغرض مكافحة جرائم الوسط الرقمي.

ومن أجل تحديد المفهوم العام للدليل الرقمي؛ يتوجب علينا دراسته من زاويتين أساسيتين، يقوم عليهما التركيب المنهجي لمصطلح المفهوم. حيث نتطرق بنوع من التفصيل إلى التعريف به(أولا)، ومن ثم نبرز أهم مميزاته كدليل جنائي حديث(ثانيا).

أولا: تعريف الدليل الرقمي الجنائي

انطلاقا من الأهمية القانونية للدليل الجنائي عموما والمتصل بالوسط الرقمي خاصةً؛ توجب علينا إبرازه من خلال البحث في تعريفه من العديد من الزوايا، وذلك بالتطرق أولا إلى التعريف العام للدليل الجنائي، ومن ثم التطرق إلى التعريف الخاص بالدليل الرقمي الجنائي.

1. التعريف العام للدليل الجنائي: قد يختلف المفهوم المراد الوصول إليه بخصوص الدليل عموما، سيما إذا ما فرقنا بين الدلالة اللغوية والاصطلاحية. ولو أن الأمر يقود في النهاية إلى المعنى العام المراد الوصول إليه. فالدليل لغةً؛ يعني المرشد وجمعه أَدِلَة وأَدِلاَء. كما قد ينطوي معنى الدليل بجمعَ أَدِلَة؛ على ما يستدل به[3]. وهو ما نجده الأقرب إلى المعنى الاصطلاحي المراد الوصول إليه في دراسة الحال، فالقاضي يستدل بوسيلة الإثبات كدليل يقوده للوصول إلى الحقيقة الجنائية –الحقيقة القضائية–.

وأما اصطلاحا فللدليل في العلوم القانونية العديد من المعاني، سيما بالوقوف عند التفرقة بين المواد المدنية –المدني بمفهومة العام– والمادة الجنائية من جهة، ودمج مفهومه من عدمه مع مفهوم الإثبات القانوني من جهة أخرى. وعلى العموم؛ يعرف العالم عبد الرزاق السنهوري، الإثبات القانوني بصفة عامة؛ على أنه: "إقامة الدليل أمام القضاء، بالطرق التي حددها القانون، على وجود واقعة قانونية ترتب

---

[1] والإثبات لغةً من "الثُبَتُ"، أي الحجة. **أنظر في ذلك:** مجمع اللغة العربية، المعجم الوسيط، مرجع سابق، باب الثاء، ص 93.

[2] حيث يعد مفهوم الإثبات عموما أشمل من مفهوم الدليل. الأمر الذي وفق المفهوم نفسه؛ يعرف من خلاله الدكتور محمود نجيب حسني، الإثبات الجنائي على أنه: "إقامة الدليل إلى السلطات المختصة بالإجراءات الجنائية على حقيقة ذات أهمية قانونية وذلك بالطرق التي حددها القانون وفق القواعد التي أخضعها لها". **أنظر في ذلك:** محمود نجيب حسني، مرجع سابق، ص 767. **نقلا عن:** أمير فرج يوسف، الإثبات الجنائي للجريمة الالكترونية والاختصاص القضائي لها، مكتبة الوفاء القانونية، الإسكندرية، مصر، 2016، ص 15.

[3] **أنظر:** مجمع اللغة العربية، المعجم الوسيط، المرجع نفسه، باب الدال، ص 294.

آثارها"[1]. وهو التعريف الذي يفهم من خلاله؛ أن الدليل القانوني هو وسيلة الإثبات المتصل بالواقعة المعنية، على أن يختلف الدليل إلى العديد من الطرق المحددة قانونا.

دائما ما يدخل الفقه القانوني في دوامة الاختلاف، بحثا عن التعريف المناسب للمسألة التي تغاضى عنها المشرع من حيث التعريف بها. فالدليل القانوني عموما، إن المدني أو الجنائي؛ لا نجد له تعريفا قانونيا واضحا في أغلب التشريعات المقارنة. وان عرفته بعض التشريعات التي لا تكاد تذكر، على غرار المشرع الروسي، الذي عرف الدليل الجنائي في إطار قانون أسس الإجراءات الجنائية؛ على أنه: "المعلومات الحقيقية التي على ضوئها يحدد المحقق أو المحكمة –طبقا للطرق القانونية المقررة قانونا– توافر أو تخلف فعل خطر اجتماعيا، وتأثيم الشخص الذي ارتكب الفعل"[2].

ونظرا لقلة التعريفات القانونية للدليل الجنائي عموما؛ سعت العديد من الدراسات الفقهية إلى تعريفه على حسب الزاوية المنظور منها، والأحكام ذات الصلة بوسائل الإثبات المختلفة. ولعلنا نجد أهم هذه التعريفات، ذلك الذي عرف الدليل؛ على أنه: "إظهار لنشاط عام أو خاص داخل الخصومة أو من أجلها يؤدي مباشرة إلى التأثير في تطور رابطة الخصومة، أو بمعنى آخر هو كل عمل يجرى في الخصومة أو يهدف إلى إعدادها أو له قيمة في الخصومة –أيا كانت طبيعته أو معناه– نظمه القانون بقصد الوصول إلى تطبيق القانون فيها"[3].

من خلال التعريفين السابقين للدليل، إن بالمنظور العام –الذي ينسب عادةً إلى المواد المدنية–، أو بالمفهوم الجنائي المحض؛ يتضح جليا الفرق بين الاثنين. الأمر الذي يرى فيه الفقه القانوني؛ أن دليل الإثبات في المواد المدنية يهيأ قبل النزاع وقبل البدء في إقامة الدعوى، ومنه الوسائل التي يثبت بها الحق هي نفسها التي تعد دليل الدعوى إن رفعت. وأما في المادة الجنائية؛ فالدليل يبدأ التعامل معه بعد رفع الدعوى –أو على الأرجح بعد ارتكاب الجريمة–، حيث يعمل الجاني على طمس الدليل، وعلى العكس من ذلك تعمل النيابة العامة وقضاء التحقيق والحكم[4].

وبوجهة نظر خاصة؛ يمكن القول أنه للدليل الجنائي نوع من الخصوصية القانونية والقضائية. التي تعطيه الطابع القضائي أكثر من التشريعي. فالتحقيق الجنائي يبحث عن أي دليل مناسب –في نظام الإثبات

---

[1] **أنظر:** عبد الرزاق السنهوري، الوسيط في شرح القانون المدني-نظرية الالتزام بوجه عام-الإثبات وآثار الالتزام، الجزء الثاني، دار النهضة العربية، القاهرة، مصر، 1968، ص 13 و14.

[2] **أنظر:** سامي جلال فقي حسين، الأدلة المتحصلة من الحاسب الآلي وحجيتها في الإثبات الجنائي، دار الكتب القانونية، القاهرة، مصر، 2011، ص 16. **نقلا عن:** حازم محمد حنفي، الدليل الالكتروني ودوره في المجال الجنائي، دار النهضة العربية، القاهرة، مصر، 2017، ص 07.

[3] **أنظر:** ناصر إبراهيم محمد زكي، (سلطة القاضي الجنائي في تقدير الأدلة-دراسة مقارنة)، رسالة دكتوراه، كلية الشريعة والقانون، جامعة الأزهر، القاهرة، مصر، 1987، ص 210. **نقلا عن:** حازم محمد حنفي، المرجع نفسه، ص 06 و07.

[4] **أنظر:** أمير فرج يوسف، الإثبات الجنائي للجريمة الالكترونية والاختصاص القضائي لها، مرجع سابق، ص 18.

الحر كأصل عام–، الذي من خلاله يمكن الوصول إلى الحقيقة –الحقيقة القضائية التي قد لا تكون هي نفسها الواقعية–. ومنه يمكن أن نعرف الدليل الجنائي على أنه: "الوسيلة الواقعية التي من خلال إتباعها بعد استظهارها؛ يمكن الوصول إلى الحقيقة القضائية التي يقتنع بها القاضي، فيحكم بناءً عليها بإدانة أو ببراءة المتهم".

2. التعريف الخاص للدليل الرقمي الجنائي: مقارنة بالدليل الجنائي المبين أعلاه وسابقا؛ يأخذ الدليل الرقمي في المواد الجنائية الطابع الخاص، المستمد أساسا من الطابع الافتراضي المعقد للوسط الرقمي، وما أضفاه من حداثة جرمية على كل الأصعدة لم يسبق مواجهة مثلها من قبل. الأمر الذي دفع بالعديد من الفقهاء والجهات الرسمية وغير الرسمية؛ إلى التسابق من أجل إيجاد تعريف مناسب لهذا الدليل الجنائي المستحدث، سيما في ظل غياب التعريف التشريعي الدقيق.

ومن خلال البحث في مختلف التعريفات ذات الصلة بالدليل الرقمي الجنائي؛ توصلنا إلى إمكانية القول بأنها تنقسم إلى ثلاثة أقسام بمعايير معينة. فمنها ما تعتمد على المعيار الضيق، ومنها ما تقوم على نظيره الواسع، كما نجد منها ما تعمل بالمعيار الفضفاض.

أ- تعريف الدليل الرقمي الجنائي وفق المعيار الضيق: يقوم المعيار الضيق؛ على الربط بين جهاز الإعلام الآلي والدليل الرقمي. حيث العامل الأساس لاستنتاج الدليل الرقمي وفق هذا المعيار؛ يتمثل في جهاز الإعلام الآلي والمعلومات التي يحتويها. وهو المعيار المعتمد في التقرير الأميريكي المقدم إلى الندوة العلمية لـــ "الإنتربول" حول الدليل الرقمي عام 2001، حيث تم تعريفه على أنه: "بيانات يمكن إعدادها وتراسلها وتخزينها رقميا بحيث تمكن الحاسب الآلي من تأدية مهمة ما"[1].

بالتطرق إلى التعريف المذكور بنوع من التحليل والمناقشة؛ يمكن أن نلاحظ العديد من النقاط السلبية. حيث اِسْتُعْمِلَ في التعريف مصطلح البيانات، وهو الذي سبق وأن بينا قصر مدلوله التقني، حيث يقتصر على البيانات غير المعالجة. وعليه كان من الأرجح استعمال مصطلح المعطيات الذي يشمل كل من هذه الأخيرة والمعلومات المعالجة. كما أنه تعريف يكتفي بالبيانات الرقمية المعدة لتأدية مهام جهاز الإعلام الآلي فقط، وهو ما يهمل النطاق الافتراضي الخارج عن اطار الجهاز من جهة، والمعطيات المعدة لغير تشغيله من جهة أخرى.

كما يعرف الدليل الرقمي وفق المعيار الضيق أيضا؛ على أنه: "الدليل المأخوذ من أجهزة الحاسب الآلي ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة وهو مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة

[1] **أنظر:** حازم محمد حنفي، مرجع سابق، ص 08.

أو الصور والأصوات والأشكال والرسوم وذلك من أجل الربط بين الجريمة والمجرم والمجني عليه وبشكل قانوني يمكن الأخذ به أمام أجهزة إنفاذ وتطبيق القانون"[1].

لا يخلوا هذا التعريف الثاني أيضا من العديد من الملاحظات، التي نلخصها في كونه تعريف جنائي أكثر منه تقني وقانوني عام، سيما وأنه تطرق إلى استعمال الدليل الرقمي من قبل الجهات المختصة؛ للربط بين أطراف الجريمة ومسرحها الرقمي. إلا أنه لم يتفادى الأخطاء التي وقع فيها التعريف السابق، سيما من حيث ربط الدليل بجهاز الإعلام الآلي دون غيره، واستبدال مصطلح البيانات بالمعلومات بدلا عن المعطيات الذي يعد هو المصطلح الصحيح.

ب- تعريف الدليل الرقمي الجنائي وفق المعيار الواسع: على العكس من المعيار الضيق في تعريف الدليل الرقمي الجنائي؛ يقوم نظيره المعيار الواسع على تلافي الملاحظات المقدمة للأول من جهة، ومحاولة مواكبة التطور الرقمي من جهة أخرى. حيث نجد العديد من التعريفات ذات الصلة، التي نذكر منها الذي جاء فيه؛ أن الدليل الرقمي هو: "مجموعة البيانات داخل الوسط الافتراضي سواءً كانت صورا أم تسجيلات أم نصوصا تأخذ شكل أرقام على هيئة الرقمين (0 و1) ويتم تحويل هذه الأرقام عند عرضها لتكون في شكل صورة أو مستند أو تسجيل"[2].

يبدوا التعريف المذكور أكثر اتساعا، من حيث المفهوم بالنظر إلى سابقيه القائمين على المعيار الضيق. الأمر الذي يتأكد بخلو التعريف من مصطلح جهاز الإعلام الآلي –الحساب الآلي–، وتدعيمه بمصطلحي الوسط الافتراضي من جهة والبيانات التي تأخذ شكل الرقمين "0 و1" –الرقمية الثنائية– من جهة أخرى. حيث يفهم من ذلك، أن أي وسط افتراضي يعمل بالرقمية الثنائية؛ يصلح لأن يكون محلا للبحث عن الدليل الرقمي الجنائي.

إلا أنه يعاب على التعريف؛ كونه استعمل مجددا مصطلح البيانات بدلا عن المعطيات كما وضحنا سابقا. بالإضافة إلى أنه حصر هذه البيانات في الصور والتسجيلات والنصوص، رغم كونها تعد بعض أنواع المعطيات الرقمية وليس كلها. حيث يمكن أن يستخلص الدليل الرقمي مثلا من المعطيات التي تكون في شكل قطع فيديو على المباشر، فهي ليست بالتسجيلات ولا بالصور.

كما يعرف جانب من الفقه الجنائي الدليل الرقمي، وفق وجهة نظر أخرى قائمة على المعيار الواسع أيضا؛ بأنه: "معلومات يقبلها المنطق والعقل ويعتمدها العلم، يتم الحصول عليها بإجراءات قانونية وعلمية بترجمة البيانات الحسابية المخزنة في أجهزة الحاسب الآلي وملحقاتها وشبكات الاتصال، ويمكن

[1] **أنظر:** أمير فرج يوسف، الإثبات الجنائي للجريمة الالكترونية والاختصاص القضائي لها، مرجع سابق، ص 287.

[2] **أنظر:** عماد الدين وادي وحنان أوشن، الإثبات الجنائي والوسائل العلمية الحديثة، دار الخلدونية للنشر والتوزيع، الجزائر، 2015، ص 97.

استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بجريمة أو جانٍ أو مجني عليه"[1].

يتسع المفهوم الوارد في التعريف المذكور؛ ليشمل البيانات المخزنة في جهاز الإعلام الآلي بالإضافة إلى تلك المتصلة بملحقات الجهاز نفسه وشبكة الاتصال الدولية. إلا أن ما يعاب على التعريف أنه؛ عبر بمصطلح البيانات بدلا عن المعطيات من جهة، واقتصر على تلك المخزنة دون غيرها. الأمر الذي وفقه لايمكن أن يعتمد المحقق على معطيات السير غير المخزنة، سيما التي تتصل بالذاكرة الحية للجهاز.

ج- تعريف الدليل الرقمي الجنائي وفق المعيار الفضفاض: بالإضافة إلى المعيارين الضيق والواسع المعتمدين لتعريف الدليل الرقمي، نجد أن العديد من الفقه الجنائي؛ قد اعتمد معيارا أكثر اتساعا، إن من حيث المجال الافتراضي للبحث عن الدليل الرقمي نفسه، أو بخصوص تجاوز ذلك إلى كل المجالات بما فيها المادية التقليدية. وهو ما يعد بمثابة الحيلة لتوسعة مجال البحث الجنائي في مجال مكافحة جرائم الوسط الرقمي، من منطلق حتمية ذلك، خاصةً بالنظر إلى خطورة هذا النوع من الإجرام الحديث والمعقد.

فمن حيث تجاوز المعيار الفضفاض للبعد الرقمي إلى غاية البعد الافتراضي؛ نجد أن الدليل الرقمي يعرف من خلاله؛ على أنه: "الدليل الذي يجد له أساسا في العالم الافتراضي ويقود إلى الواقعة غير المشروعة ومرتكبها الحقيقي"[2].

يتضح جليا من خلال التعريف المذكور؛ أنه وسع مجال البحث عن الدليل الرقمي كثيرا، فربطه بالعالم الافتراضي –الذي سميناه فيما سبق بالوسط أو النطاق الافتراضي-. حيث وفق ذلك كل دليل افتراضي غير ملموس حتى وان لم يكن رقميا؛ هو دليل حديث تثبت من خلاله جرائم الوسط الرقمي. فالإثبات بالتصنت الهاتفي التقليدي، يعد وفق ذلك إثباتا رقميا لأنه افتراضيا غير ملموس، حتى وان خلى الهاتف التقليدي من البعد الرقمي الثنائي. الأمر الذي يعد غير منطقيا، سيما وأننا حصرنا المجال الرقمي فيما سبق؛ في النطاق الافتراضي الذي تحدثه عناصر الوسط الرقمي السابقة بالدراسة.

ومن زاوية أخرى ضمن الإطار نفسه، يعرف الدليل الرقمي الجنائي وفق المعيار الفضفاض أيضا، بطريقة تتجاوز حتى الحدود الافتراضية المذكورة إلى نظيرتها المادية التقليدية –ما يمكن تسميته بالمعيار الجد فضفاض-؛ على أنه: "الأدلة أو الطرق التي يتم من خلالها الكشف عن الجرائم التي يتم ارتكابها في بيئة الكترونية"[3].

---

[1] **أنظر:** محمد الأمين البشري، التحقيق في الجرائم المستحدثة، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، 2004، ص 234. **نقلا عن:** حازم محمد حنفي، مرجع سابق، ص 08.

[2] **أنظر:** حازم محمد حنفي، المرجع والصفحة نفسهما.

[3] **أنظر:** عماد الدين وادي وحنان أوشن، مرجع سابق، ص 97.

جاء التعريف الأخير؛ بنوع من التوسع إلى درجة وصفنا له بالمعيار الجد فضفاض. حيث من خلاله كل دليل تثبت به جريمة من جرائم الوسط الرقمي –التي عبر عنها التعريف بالجرائم المرتكبة في البيئة الالكترونية–؛ هو دليل رقمي. الأمر الذي يعد غير مقبولا لا جنائيا ولا تقنيا ولا منطقيا. حيث يمكن إثبات جريمة من جرائم الوسط الرقمي بالدليل التقليدي، مثل الاعتراف مثلا. وهو ما يعد خارجا عن الدليل الرقمي محل الدراسة، رغم كونه دليلا مشروعا قانونا.

وعلى العموم؛ يمكن من وجهة نظر خاصة أن نضع تعريفا جنائية للدليل الرقمي، انطلاقا من التعريفات السابقة بالذكر. محاولين في ذلك تفادي العيوب والثغرات والتركيز على المزايا ذات الصلة. حيث نخرج من مفهوم التعريف كل ما هو غير رقمي، سواءً كان ماديا ملموسا أو معنويا افتراضيا. كما نؤكد على ضرورة الاعتماد على مصطلح المعطيات بدلا عن البيانات والمعلومات، نظرا لكونهما من مكوناته التقنية. كما أنا نؤكد في ذلك على كونه الرابط التقني بين أطراف الجريمة وشهودها ومخلفاتها الرقمية، بغرض إظهار الحقيقة القضائية.

ومن خلال ذلك يمكن أن نعرف الدليل الجنائي الرقمي؛ على أنه: "معطيات رقمية ثنائية –بيانات و/أو معلومات–، يتم التوصل إليها رقميا عبر البحث في النطاق الافتراضي الذي تخلقه عناصر الوسط الرقمي –جهاز الإعلام الآلي وشبكة الاتصال الدولية ومن في حكمهما–، والتي من خلالها يتم الربط جنائيا بين أطراف الجريمة وشهودها وأحداثها الافتراضية، بغرض الوصول إلى الحقيقة الواقعية أو كأقل تقدير الحقيقة القضائية"[1].

ثانيا: مميزات الدليل الرقمي الجنائي

لم يمتد أثر الاختلاف الفقهي الكبير بخصوص تحديد تعريف جامع مانع للدليل الجنائي الرقمي، كما بينا سابقا؛ إلى المميزات ذات الصلة. حيث يكاد يستقر الفقه –إلى حد الساعة ومراعاةً للتطور الديناميكي السريع للوسط الرقمي–؛ على السمات الأساسية التي يمتاز بها الدليل الرقمي عن الدليل التقليدي من جهة ونظيره الافتراضي غير الرقمي من جهة أخرى.

ومنه يمكن القول أن الدليل الرقمي الجنائي؛ يمتاز عن غيره من أدلة الإثبات التقليدية وغير التقليدية، بالعديد من السمات الأساسية، على غرار كونه مزدوج الطبيعة، وعلمي تكنولوجي، ومتنوع ديناميكي التطور، كما أن له حصانة آلية من الزوال، بالإضافة إلى اعتباره بمثابة المحدد الدقيق لكل ما يتعلق بأطراف الجريمة وتحركاتهم الرقمية.

[1] على أننا نؤكد مرةً أخرى؛ بأن الدليل المعرف أعلاه هو الدليل الجنائي الرقمي، دون التقليدي ولا الافتراضي الحديث غير الرقمي. اللذان يمكن الاعتماد عليهما لإثبات جريمة من جرائم الوسط الرقمي، لكن من دون حملهما لصفة الدليل الرقمي. الأمر الذي سنتوسع فيه؛ بمناسبة دراسة الفصل الثاني والأخير من الدراسة. الذي نبرز من خلاله العديد من الوسائل المساعدة على التحري والتحقيق في جرائم الوسط الرقمي.

1. ميزة الازدواجية في الطبيعة: تختلف الأدلة الجنائية عموما وتتنوع، إلا أنها في مجملها لا تخرج عن النوعين الأساسيين، المتصلين بالدليل المادي والدليل المعنوي. فالأول –المادي– يعد بمثابة الشيء الملموس الذي يأخذ له مكانا في الحيز الخارجي الملموس –التقليدي–، ومنه يكون قابلا للإدراك باستعمال حاسة اللمس. على غرار سلاح جريمة القتل المنطوي على المسدس الناري، أو وسيلة الدخول للمنزل محل جريمة السرقة، المتمثلة في المفتاح المقلد أو قضيب تكسير المداخل. ومنه يكون التأثير على قناعة القاضي؛ بطريقة مباشرة وحاسمة.

وأما النوع الثاني من أدلة الإثبات المعروفة؛ فينطوي على الدليل المعنوي. الذي يخرج عن إطار الماديات الملموسة، فلا يأخذ مكانا في الحيز الخارجي. وإنما يكون محسوسا يمكن إدراكه بكل الحواس ما عدا حاسة اللمس. الأمر الذي له العديد من الأمثلة، على غرار الإيحاء والتلقي بالسمع وغيرها. ومنه يكون التأثير على القاضي؛ بطريقة غير مباشرة، وهو ما يندرج جنائيا ضمن خانة الأدلة الناطقة[1].

الدليل الرقمي الجنائي كذلك، لا يمكن أن يخرج عن النوعين السابقين المادي والمعنوي. لكن أي النوعين يكتسي، هل الطابع المادي أم المعنوي. في الحقيقة الأصل في الوسط الرقمي محل الدراسة عموما؛ أنه ذوا طابع معنوي افتراضي. حيث سبق وأن بينا أن ماديات الوسط الرقمي بصورة منفصلة عن النطاق الافتراضي الذي تخلقه؛ تعد بمثابة الدعامة المادية الخارجة عن مجال الدراسة، وان تعرضت لفعل إجرامي كالسرقة مثلا؛ فتخضع للأحكام التقليدية للجريمة.

وفق ما ذكر تعتبر المعطيات الرقمية كأصل عام؛ هي المحور الأساس لاستخراج الدليل الرقمي. وهي التي تعد ذات طابع افتراضي محض. الأمر الذي يدفع بالقول بأن هذا الدليل هو ذا طابع معنوي افتراضي لا مادي[2]. لكن بنوع من التدقيق المنطقي والواقعي؛ يمكن القول بأن له طابع مزدوج معنوي ومادي. حيث الدليل الرقمي الذي يكون عبارة عن مقال منشور على موقع التواصل الاجتماعي "فايسبوك–Facebook" مثلا؛ تتم معاينته رقميا افتراضيا في البداية مع حجزه بالطريقة نفسها، لكن العمل القضائي يتطلب طباعته على ورق ابيض ليوضع في ملف القضية. وهو ما يجعل منه رقميا بالأصل وماديا بالنتيجة[3].

---

[1] **أنظر:** حازم محمد حنفي، مرجع سابق، ص 15.

[2] الأمر الذي جاءت به العديد من الدراسات الجنائية. حيث يعتبرون أن الدليل الرقمي هو دائما معنويا غير ملومسا، وترجمته إلى الشكل المادي؛ ما هو إلا عملية نقل من الهيئة الافتراضية إلى المادية؛ بغرض الاستدلال بها فقط. **أنظر في ذلك:** مركز هردو لدعم التعبير الرقمي، "الجريمة الالكترونية وحجية الدليل الرقمي في الإثبات الجنائي"، تقرير، القاهرة، مصر، 2014، ص 23.

[3] مع الإشارة إلى قول بعض الفقه الجنائي؛ أننا لا نحتاج إلى إخراج الدليل الرقمي من نطاقه الافتراضي إلى الحيز الخارجي الملموس، حتى نعتبره قد تحول من طابعه المعنوي إلى المادي. فمجرد معالجته وحجزه رقميا في صورته النهائية للدليل؛ يعتبر قد أصبح ماديا. وذلك لإمكانية إدراكه بحاسة الرؤيا أو السمع. ومثال ذاك الدليل الموضوع في ملف "Word". **أنظر في ذلك:** حازم محمد حنفي، المرجع نفسه، ص 16.

وعلى العكس من ذلك؛ لو تصورنا ارتكاب جريمة سرقة جهاز إعلام آلي محمول، بهدف إعادة بيعه مثلا، دون البحث عن المعطيات الرقمية التي يحويها. لاعتبرناه بمثابة الدعامة المادية فقط. التي بحجزها من الشرطة القضائية بعد القبض على المتهم؛ تعد بمثابة الدليل المادي على ارتكاب جريمة سرقة تقليدية مادية، ولا علاقة لها لا بالدليل الرقمي ولا بجرائم الوسط الرقمي.

2. ميزة البعد العلمي التكنولوجي: لا شك في أنه بالإضافة إلى تقسيم الأدلة الجنائية إلى مادية ومعنوية وفق ما سبق ذكره؛ يمكن تقسيمها أيضا إلى أدلة واقعية وأدلة علمية. فكل دليل تقليدي يمكن التعامل معه من أي شخص من دون الحاجة إلى معرفة علمية مسبقة يعتبر بمثابة الدليل الواقعي العادي. وأما الدليل العلمي فأكيد لا يتم التعامل معه وفك شفرته؛ إلا من المختص في المحل المقصود[1].

فالدليل الرقمي؛ يعد بمثابة أحد أنواع الدليل العلمي الحديث. حيث يقوم على النبضات الرقمية الثنائية، التي تتطلب للتعامل معها كدليل رقمي، إخضاعه لقاعدة لزوم التجاوب مع الحقيقة الكاملة وفق قاعدة؛ "إن القانون مسعاه العدالة، أما العلم فمسعاه الحقيقة". فالدليل الرقمي لكي لا يفقد الغرض التقني والقانوني المراد منه؛ يتوجب ألا يخرج عما توصل إليه العلم في المجال الرقمي عموما[2]. كما يصف البعض الدليل الرقمي؛ على أنه الدليل المستمد من الآلة[3]، ما يدفع للقول بحتمية كونه علمي حديث.

بالإضافة إلى اعتبار الدليل الرقمي دليلا علميا؛ هو أيضا يحمل الطابع التقني المتصل بالبعد العلمي أصلا. حيث يستمد الميزة الرقمية من الوسط الرقمي ذاته، ومنه يتوجب أن يستنتج ويستنبط من الوسط الرقمي ذاته الذي يتواجد من خلاله[4]. وبتعبير آخر يتوجب أن يحمل الدليل الرقمي؛ الصفة الرقمية نفسها التي يحملها النطاق الافتراضي للوسط الرقمي الذي يعد أساسا له.

وكنتيجة عن الطابع العلمي بالأساس والتقني بالتبعية للدليل الرقمي والوسط المتواجد من خلاله؛ يضع الفقه الجنائي شرط أساسي لاعتبار الدليل على أنه رقمي حديث يدخل في مجال الدراسة. حيث فهم مضمونه يتوقف على استعمال أجهزة وبرامج رقمية خاصة، تجمعه وتحلله بالطريقة الرقمية نفسها. ومنه كل ما يستحيل أو يتعذر تجميعه وتحليله بهذه الوسائل الرقمية؛ يعد خارجا عن إطار الدليل الرقمي. وذلك لتعذر إمكانية الاستدلال به على المعطيات المعنية، ما ينفي قيمته الثبوتية من جهة ورابطته السببية نسبتا إلى الجاني من جهة أخرى[5].

---

[1] وعلى العموم؛ اتساع رقعة العلم في المجتمع؛ جعل من الإثبات العلمي بكل أنواعه بمثابة الأمر الطبيعي والمقبول قانونا وقضاءً. فالاعتماد على العلوم الحديثة وأجهزتها العلمية لا يحدث تعارضا على الإطلاق بين التطور العلمي الأخذ بأسباب الأساليب المستحدثة للاثبات الجنائي. **أنظر في ذلك:** عماد الدين وادي وحنان أوشن، مرجع سابق، ص 37.

[2] **أنظر:** حسين ربيعي، مرجع سابق، ص 262.

[3] **أنظر:** مركز هردو لدعم التعبير الرقمي، مرجع سابق، ص 23.

[4] **أنظر:** حسين ربيعي، المرجع نفسه، ص 263.

[5] **أنظر:** مركز هردو لدعم التعبير الرقمي، المرجع والصفحة نفسهما.

بالإضافة إلى ضرورة استعمال الأجهزة والبرامج الرقمية اللازمة لاستخلاص الدليل الرقمي؛ نجد من أهم النتائج الأساسية لميزة البعد العلمي التكنولوجي للدليل الرقمي؛ أنه من الممكن نسخه من محله الأصلي دون الحاجة إلى نقله أو محوه. ويكون ذلك وفق صورة طبق الأصل، التي تصلح لأن تكون دليلا، بالآثار القانونية نفسها للأصل المنسوخ منه. الأمر غير المتاح في الأدلة الجنائية الأخرى التقليدية وحتى الحديثة غير الرقمية. وهو ما يعد ضمانا للتلف أولا، ولمقارنته بالأصل لو حدث أي تعديل بعد النسخ ثانيا[1].

يمكن القول انطلاق من الميزة محل الدراسة؛ أن الطابع العلمي التلكنولوجي للدليل الرقمي، بقدر ما يحدد مفهوم الدليل نفسه، بقدر ما يجعله أكثر اتساعا ومرونةً من الدليل التقليدي وحتى الحديث غير الرقمي. فاستعمال البرامج والأجهزة الرقمية يجعل من الدليل الرقمي أكثر دقة واقترابا من الحقيقة الواقعية لا القضائية. وقابليته للنسخ يضمن الحجية نفسها في الثبات من جهة ويعد الضامن لعدم التلاعب بالدليل انطلاقا من إمكانية المقارنة بالدليل الأصلي.

3. ميزة التنوع والتطور الديناميكي: سبق وأن قلنا أنه رغم ظهور المعطيات الرقمية في العديد من الأشكال، منها البيانية غير الجاهزة ومنها المعلوماتية الجاهزة بعد معالجتها أليا، ومنها الصور والأشكال والكتابات والفيديوهات...الخ –التي قد تكون بيانات كما قد تكون معلومات–. إلا أنها في الأخير تحمل الوصف العام المنطوي على المعطيات الرقمية، التي لها العديد من الأنواع والأشكال الفرعية، المشكلة للدليل الرقمي، إن منفردة أو مجتمعة.

لو تطرقنا إلى الأمر نفسه بمفهوم المخالفة في إطار الدليل الرقمي، لا بخصوص المعطيات الرقمية بصفة عامة؛ لتوصلنا إلى أن الدليل الرقمي متنوع ومتعدد. فقد يكون –الدليل الرقمي– عبارة عن وثيقة معالجة رقميا، التي تخزن أو ترسل عبر الوسائل المعدة لذلك. كما قد يكون عبارة عن مجموعة وثائق رقمية أو وثيقة ومعلومات أخرى، أو غير ذلك من أشكال المعطيات الرقمية، كالمتصلة بنظام التشفير منها. الأمر الذي يفتح المجال لاتساع مفهوم الدليل الرقمي وشموليته، لكل المركبات الافتراضية للوسط الرقمي عموما[2].

وأما من حيث ديناميكية التطور؛ فالأمر يعد عادي ومفهوم. حيث يكتسب الدليل الرقمي هذه الميزة انطلاقا من الوسط الرقمي، الذي يعد ديناميكيا وسريع التطور. فكلما تطور الوسط الرقمي، كلما تطور الدليل الرقمي. وأي تأخر من حيث تطور الدليل تزامنا مع التطور المتصل بالوسط الرقمي يعد بمثابة الثغرة الجنائية، التي ستؤدي إلى إفلات الجنات وانتشار الجريمة، انطلاقا من اقتناع الجاني الرقمي بأنه بأمان من كل متابعة جنائية محتملة.

---

[1] **أنظر:** نعيم سعيداني، مرجع سابق، ص 123.

[2] **أنظر:** المرجع نفسه، ص 124.

وعلى سبيل المثال أحدث التطور المشهود بخصوص القرص الصلب، وسرعات الإدخال والإخراج ذات الصلة؛ جدلا كبيرا حول المعادلة الرقمية[1]. ومنه يمكن الحديث عن الصعوبات التقنية التي ستواجهها جهات التحري والتحقيق لدى تعاملها مع جرائم الوسط الرقمي عموما، وبحثها عن الدليل الرقمي واستخراجه خاصةً.

4. ميزة التحصين الآلي من الزوال: قد تبدوا ميزة التحصين من زوال الدليل؛ بمثابة الأمر غير المنطقي أو غير المفهوم لدى العديد. سيما بالرجوع إلى السمات التقليدية للدليل الجنائي الذي يمكن محوه وتعديله أو التخلص منه نهائيا بأسهل الطرق. إلا أنها حقيقة تقنية لابد من التعامل معها، سيما وأنها تميز الدليل الرقمي عن نظيره التقليدي والحديث غير الرقمي.

ففهم هذه الميزة؛ يتطلب توفر المعرفة العامة بالوسط الرقمي أولا وجرائمه ثانيا. حيث القاعدة الرقمية العامة في هذا الإطار؛ أن كل عمل رقمي يتصل بالمعطيات ذات الصلة؛ يقود إلى الحفظ الآلي، ما يصعب التخلص منها ولو بالعمل على محوها وما إلى ذلك. ومنه محو الدليل الرقمي لا يعد بأي حال من الأحوال؛ بمثابة العائق أمام استرجاع المعطيات الملغاة. حيث باستعمال برامج رقمية معينة–كما سنرى لاحقا–، يمكن استرداد أي معطيات نريدها حتى وان احترق الجهاز[2].

يجد الفقه الجنائي في هذه الميزة؛ الحجر الأساس للتفرقة بين الدليل الرقمي والدليل التقليدي. حيث بالرجوع إلى الدليل التقليدي؛ نجد أن الجهات المختصة بالتحري والتحقيق؛ كانت قد عانت ولا تزال تعاني، من مسألة التخلص من الدليل الجنائي المادي. حيث على سبيل المثال؛ يمكن التخلص من الوثائق التي تحمل دليلا قاطعا؛ عبر إتلافها بالتمزيق أو الحرق. كما يمكن التخلص من الشهود بقتلهم...الخ. ما يجعل أمر استرجاع الدليل؛ مستحيلا استحالة مطلقة[3].

إلا أن الأمر لا يعد على إطلاقه؛ حيث يمكن أن يتعرض الدليل الرقمي للتعديل، أو المحو غير المقصود من الجاني أو غيره من رواد الوسط الرقمي، أو من المحقق نفسه، سيما إذا لم يكن متمكنا من المجال الرقمي و/أو لم يستعن بخبير رقمي[4]. الأمر الذي قد يقوم به غير المحقق –جاني أو غيره– بصورة غير متعمدة، سواءً قبل التدخل القضائي وشبه القضائي أو بعد ذلك. ولو أن التعديل الحاصل بعد التفتيش والحجز لا يشكل أي إشكال، نظرا لتطلبهما القيام بنسخ الدليل بمجرد حجزه.

---

[1] **أنظر:** حازم محمد حنفي، مرجع سابق، ص 21.

[2] **أنظر:** المرجع والصفحة نفسهما.

[3] ويشبه الفقه الجنائي هذه الميزة التي يتصف بها الدليل الرقمي؛ بالدليل الجنائي المستنبط من الحمض النووي "ADN"، الذي يمكن استرجاعه في حالة التخلص منه. وفي الإطار نفسه؛ سبق وأن استعادة جهات التحقيق في قضية إيران لعام 1986؛ كل المعطيات الرقمية –المنطوية على رسائل- بعد أن حذفها العقيد "أوليفر نورد" من جهاز الإعلام الآلي التابع له، من دون علمه بإمكانية الاسترجاع، عبر نظام الحفظ "Backup". **أنظر في ذلك:** وردة شرف الدين، مرجع سابق، ص 08.

[4] **أنظر:** المرجع والصفحة نفسهما.

وخلافا للتعديل أو المحو غير المتعمد؛ يمكن تصور قيام الجاني نفسه بذلك متعمدا التخلص من الدليل، الرقمي ومنه الإفلات من المسؤولية الجنائية. حيث يتعمد الجاني القيام بإتلاف الدليل الرقمي، وكل ما تتصل به من معطيات رقمية، قد تقود إلى اكتشاف الجريمة، أو على الأقل محو كل معلومة قد تؤدي إلى اكتشاف مرتكبها.

وأمام الجاني للقيام بذلك وسيلتين أساسيتين. حيث إما أن يعتمد الطريقة البعدية اليدوية أو القبلية "الأوتوماتيكية". فباعتماد الجاني على الطريق الأولى –البعدية اليدوية–؛ يتوجب عليه أن يقوم بعد ارتكابه للجريمة بالبحث الرقمي في النطاق الافتراضي، عن كل معطيات رقمية تؤدي إلى اكتشاف الجريمة و/أو معرفة فاعلها، ومنه يزيلها نهائيا، وذلك عبر الحذف أو إحراق جهاز الإعلام الآلي مثلا، أو إتلافه ماديا عبر تكسيره[1].

كما يمكن للجاني أن يعتمد الوسيلة القبلية "الأوتوماتيكية"، التي مفادها القيام قبل ارتكاب الجريمة بإعداد برنامج خاص يعول عليه خصيصا للتخلص من الدليل الرقمي بمجرد ارتكاب الجريمة. وذلك عبر برمجة الجهاز ليقوم بالمحو الآلي لكل المعطيات غير المفيدة بمجرد تحسس وجودها، التي يعد الدليل الرقمي واحدا من صورها[2].

وفي كل الأحوال، سواءً قام الجاني بالاعتماد على الطريقة الأولى أو الثانية؛ فان مجرد التحسس التقني بالتدخل العمدي للجاني بطريقة مباشرة أو غير مباشرة في عملية التخلص من الدليل الرقمي الذي يدينه؛ يعد بمثابة الدليل على ارتكابه للجريمة المحقق فيها. كما قد يساهم في تشديد العقوبة عليه في إطار السلطة التقديرية للقاضي[3].

ولو أننا نرى أن التشديد في العقوبة وفق آلية السلطة التقديرية للقاضي في هذا الصدد؛ يعد غير كافيا. وذلك لسببين اثنين، أولهما أن فكرة الردع العام التي يفرضها المشرع تعد غائبةً في هذا الإطار. فالجاني الرقمي الذي يعمل على محو الدليل؛ يعلم بأنه سيتابع بجريمة واحدة وهي الجريمة الأصلية، إضافة إلى علمه بأن القاضي قد يشدد في العقوبة، وقد لا يعمد إلى ذلك. سيما وأن الوسط الرقمي في تطور سريع، ما قد يكون دافعا للتطوير من وسائل إتلاف الدليل الرقمي من الجناة. وأما السبب الثاني؛ فالتشديد القضائي يجب أن يقابله البحث العلمي الرقمي، حيث مجرد التشديد؛ هو اعتراف بعدم القدرة على مواجهة التطور التقني نفسه.

---

[1] كما ذكرنا سابقا؛ الحذف والحرق لا يعاد عائقا أمام استرجاع المعطيات بالبرامج المعدة لذلك. لكن التكسير النهائي للجهاز قد يكون عائقا إذا ما كانت الجريمة متصلة بنظام المعلومات غير المربوط بشبكة الاتصال الدولية، ومنه محدودية أثر الجريمة في الجهاز نفسه.

[2] **أنظر:** حازم محمد حنفي، مرجع سابق، ص 22.

[3] **أنظر:** المرجع والصفحة نفسهما. **وأنظر أيضا:** وردة شرف الدين، مرجع سابق، ص 08.

5. ميزة المحدد الدقيق لأطراف الجريمة وتحركاتهم الرقمية: زيادةً على المميزات السابقة بالذكر؛ ينفرد الدليل الرقمي عن غيره من وسائل الإثبات الجنائي؛ بكونه يحدد المعلومات الجنائية بدقة. حيث كل ما يتعلق بالجريمة كواقعة رقمية من جهة، والجاني والضحية والشهود من جهة أخرى؛ يمكن التوصل إليه بالاعتماد على الوسائل الرقمية المعدة للتحري والتحقيق في جرائم الوسط الرقمي، ومنه الوقوف بدقة على كل المعطيات الإجرامية.

فيمكن عبر الدليل الرقمي الجنائي؛ الوقوف بدقة عند كل ما يخص الجاني والضحية والشهود –والأهم هو الجاني–. حيث تحلل المعطيات ذات الصلة بالجاني، بعد رصدها بدقة. الأمر الذي يمكن من خلاله التوصل إلى تحركاته وسلوكياته الرقمية –وحتى غيرها من السلوكيات غير الرقمية، عبر الاستنباط–، والعديد من المعلومات الشخصية المتصلة به وبعائلته وظروف عمله وغيرها. وهو ما يسهل عملية الوصول إلى إقامة المسؤولية الجنائية في جانبه من عدمها، سيما وأنه دليل يجمع العديد من الجوانب ذات الصلة بالجاني[1].

كما يمكن في حال خروج الدليل الرقمي عن إطار الدولة الواحدة؛ القيام باستخراجه في أجال جد معقولة، وذلك عبر اللجوء إلى المساعدة الدولية، أو الولوج الرقمي العابر للحدود الوطنية –كما سنرى لاحقا–. ما يساهم في التحديد الدقيق لكل ما يتصل بالجريمة وأطرافها. وذلك دون أن ننسى أن الدليل الرقمي بطبيعته أو بمكان تواجده الافتراضي من جهة والدعامة الحاملة له بعد نسخه في إطار التحري والتحقيق من جهة أخرى؛ له سعة تخزين عالية، ما يساهم في إنشاء سجل كامل للجاني الرقمي محل المتابعة الجنائية[2].

الفرع الثاني: البعد التقني للدليل الرقمي الجنائي

يمكن القول أننا توصلنا فيما سبق بمناسبة طرحنا لمفهوم الدليل الرقمي؛ إلى إبراز الشق النظري من ماهية هذا الدليل الجنائي المستحدث. حيث بالتطرق إلى مختلف التعريفات ذات الصلة وما تستنبط منها من مميزات أساسية؛ نكون قد مهدنا الطريق أمام الجانب التقني العملي، الذي عنوناه بالبعد التقني للدليل الرقمي. والذي يعد أساس الدراسة، نظرا لكونه الجزء الدخيل على العلوم الجنائية، في شقها المتعلق بالإثبات والدليل المناسب لذلك.

وفي هذا الإطار، نكون قد حددنا عنصرين أساسيين لتبيان البعد التقني للدليل الرقمي الجنائي، والمتمثلين في البعد التقني العام(أولا)، ونظيره الخاص الذي يختلف على حسب الوسيلة الرقمية المستعملة في ارتكاب الجريمة(ثانيا).

---

[1] **أنظر:** حسين ربيعي، مرجع سابق، ص 263. **وأنظر أيضا:** وردة شرف الدين، مرجع سابق، ص 09.

[2] **أنظر:** وردة شرف الدين، المرجع نفسه، ص 09.

أولا: البعد التقني العام للدليل الرقمي الجنائي

عمل الفقه الجنائي المختص بالبحث في جرائم الوسط الرقمي؛ على إيجاد أحكام قانونية من أصل تقني محض، يمكن أن تشكل البعد التقني العام للدليل الرقمي المعتمد في إثبات هذا النوع من الإجرام الحديث. الأمر الذي تختلف بخصوصه الدراسات، سيما وأنها لم تضع الأحكام ذات الصلة تحت عنوان البعد التقني، وإنما تمت دراستها بشكل منفصل. وهو ما نتجاوزه منهجيا، بحيث آثرنا دمج كل من أقسام الدليل الرقمي ومصادره في إطار البعد التقني العام[1].

1. أقسام الدليل الرقمي الجنائي: يتعدد الدليل الرقمي ويتنوع وفق العديد من الأقسام، التي تتكون من طوائف قائمة على العديد من المعايير ذات الأساس التقني المحض. حيث تؤثر على عملية البحث التقني على الدليل الجنائي واستخراجه. إلا أنها في الأخير لا علاقة لها بحجية الإثبات من عدمه، نظرا لكونها تقسيمات تقنية لا قانونية. وهي المنطوية أساسا على نوعين من الأقسام، القائمة إما على أساس معيار الطبيعة، أو وفق المعيار الموضوعي[2].

أ- أقسام الدليل الرقمي الجنائي وفق معيار الطبيعة: يعد معيار الطبيعة المعتمد لتقسيم الدليل الرقمي، من أهم المعايير المعمول بها. نظرا لكونه المعيار الأسهل من حيث التعامل معه، سيما وأنه يلاحظ بالعين المجردة ولا يحتاج لمجهود معين حتى نقوم بالتفرقة. وعلى العموم؛ يختلف الدليل الرقمي ويتنوع وفق معيار طبيعة الدليل نفسه؛ الى الدليل المادي ونظيره المعنوي الافتراضي. حيث قد يرد الدليل الرقمي في دعامة مادية كما قد يرد في دعامته الرقمية الافتراضية.

أ-1/ الدليل الرقمي الجنائي الوارد في الدعامة المادية: يمتاز الدليل الرقمي الوارد في الدعامة المادية؛ بكونه الدليل القابل للظهور في العالم الخارجي، والتعامل معه بالطرق التقليدية المعروفة كاللمس والإتلاف وغيرها. ومن أمثلة ذلك؛ نجد الأوراق المطبوعة، التي تحمل معطيات رقمية بالأساس، المنطوية على تقارير وقوائم بيانات معالجة آليا -أو قد تكون غير معالجة-. كما قد تحوي رسومات وغيرها[3].

---

[1] الدمج الذي نؤسس له؛ باعتبار أن المستجد في الدليل الرقمي عموما هو بعده التقني الرقمي. وهو ما يتركز أساسا على أقسامه ومصادره.

[2] ولو أننا نجد العديد من الدراسات الأخرى، التي تقسم الدليل الرقمي إلى أنواع متعددة، وذلك انطلاقا من العديد من المعايير. على غرار وزارة العدل الأمريكية التي قسمته سنة 2002 إلى ثلاثة أقسام، منطوية على السجلات المحفوظة في جهاز الإعلام الآلي مثل البريد الالكتروني، والسجلات التي تم إنشاؤها بواسطة الجهاز مثل فواتير الأجهزة، بالإضافة إلى السجلات التي تم حفظ جزء منها بالإدخال وإنشاء الجزء الآخر بواسطة الجهاز نفسه، مثل أوراق العمل المالية. وبالإضافة إلى المعيار المذكور برز تقسيم فقهي آخر، يقسم الدليل الرقمي إلى أربعة أنواع، المتمثلة في الأدلة الخاصة بجهاز الإعلام الآلي وشبكاته، والأدلة الخاصة بالانترنت، والأدلة الخاصة ببروتوكولات تبادل المعلومات بين أجهزة الشبكة، وأخيرا الأدلة الخاصة بالشبكة. **أنظر في ذلك:** أمير فرج يوسف، الإثبات الجنائي للجريمة الالكترونية والاختصاص القضائي لها، مرجع سابق، ص 289.

[3] **أنظر:** هلالي عبد الله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية-دراسة مقارنة، الطبعة الثانية، دار النهضة العربية، القاهرة، مصر، 2008، ص 16 و17.

كما قد تأخذ الدعامة المادية للدليل الرقمي؛ العديد من الصور الأخرى، على غرار طباعة الصور ذات الصلة بمسرح الجريمة –المسرح الرقمي– أو أطرافها أو غير ذلك. بالإضافة إلى الدليل الرقمي المحجوز الذي قد يحفظ في دعامات غير رقمية –قد تكون مادية أو افتراضية–، مثل حفظ التسجيل الصوتي الرقمي في جهاز تسجيل تماثلي تقليدي.

إلا أن ظهور الدليل الرقمي في الشكل المادي على الدعامة المادية غير الرقمية، المنطوي على الأوراق المطبوعة وغيرها؛ لايمس بالطبيعة الرقمية الافتراضية للدليل. وذلك لكون أصله رقمي مستخرج من مسرح الجريمة الرقمي بالأساس[1]. وما ظهوره على الدعامة المادية إلا لاحقا عن تحصيله من الوسط الرقمي من جهة، ولاستعماله الحسن والسلس في عملية الإثبات من جهة أخرى[2].

أ–2/ الدليل الرقمي الجنائي الوارد في دعامته الافتراضية: على العكس من الدليل الرقمي الظاهر في الدعامة المادية؛ يعد نظيره الوارد في دعامته الافتراضية، بمثابة الدليل الرقمي بالأساس والظهور. فاستخراجه يكون رقميا واستظهاره لاستعماله كدليل إثبات جنائي يكون رقميا أيضا، حيث يرد في دعامته الرقمية الأصلية ذات الطابع الافتراضي، المنطوية أصلا على النطاق الافتراضي –العام والخاص– للوسط الرقمي السابق بالدراسة[3].

وعلى العموم يتخذ الدليل الرقمي في هذه الحالة؛ صورتين، إما الصورة الحقيقة أو المعلوماتية المعنوية. فتكون الصورة الحقيقية بمثابة الإظهار الأصلي للدليل الرقمي، في شكله الرقمي الثنائي القائم على الرقمين الـــ "0 و01"، والذي لا يفهمه إلا الجهاز بصورة آلية وأصلية، لايمكن الوصول إلى مغزاها إلا بعد ترجمتها إلى لغة غير رقمية[4].

وأما بخصوص الصورة المعلوماتية المعنوية؛ فهي النتيجة أو الخلاصة التي يظهر من خلالها الدليل الرقمي. فيكون قابلا للفهم البشري وترجمته لاستعماله كدليل جنائي. ومن أمثلة ذلك؛ أن يظهر الدليل الرقمي في شكل رسالة مكتوبة على أحد برمجيات المعالجة الآلية للنصوص كالبرنامج المسمى بـــ "Microsoft Office Word". التي –الرسالة– يمكن قراءتها عبر شاشة الجهاز أو وحدة العرض

---

[1] **أنظر:** محمد كمال شاهين، مرجع سابق، ص 367.

[2] وكمثال عن ذلك؛ البحث الرقمي عن كلمات السب، التي عبر عنها الجاني بالكتابة الرقمية في إطار حسابه الخاص بـ "الفايسبوك". ومن ثم حجز الدليل الرقمي المتصل، وطباعته في ورق أبيض لمواجهة الجاني بذلك من جهة وتسهيلا للمحاكمة والإثبات من جهة أخرى؛ يعد بمثابة إظهار للدليل الرقمي وفق الشكل المادي، وليس دليلا ماديا بذاته وأصله.

[3] ولو أن حتى الدعامة الرقمية الافتراضية نفسها التي يرد فيها الدليل الرقمي؛ لا يمكن أن ترد بصورة منفصلة أبدا. حيث هي الأخرى تتصل تقنيا بالدعامة المادية الحديثة -وليست تقليدية-. فالفيديو الرقمي كدليل إثبات، يرد رقميا في دعامته الافتراضية المنطوية على نظام المعلومات، والاثنين معا يردان في الدعامة المادية الحديثة، المنطوية على جهاز الإعلام الآلي أو من في حكمه.

[4] **أنظر:** محمد كمال شاهين، المرجع نفسه، ص 368.

المرئي الموصولة بالجهاز[1]. كما قد يكون الدليل الرقمي الوارد في الدعامة الرقمية؛ عبارة عن أوعية لا ورقية، كالأقراص الممغنطة والضوئية والمصغرات الفلمية وغيرها الكثير –مع التذكير بالتطور الرقمي الديناميكي المستمر من حيث هذه الأنواع–[2].

ب– أقسام الدليل الرقمي الجنائي وفق المعيار الموضوعي: ينقسم الدليل الرقمي الجنائي وفق المعيار الموضوعي؛ إلى قسمين أساسيين. القائمين أساسا على مدى اعتبار الدليل الرقمي نفسه؛ بمثابة المعطيات الرقمية الموجودة آليا في الوسط الرقمي، أو تم استحداثها بمناسبة ارتكاب الجريمة. الأمر الذي من خلاله يمكن أن نقسم أدلة الإثبات الجنائي الرقمي؛ إلى الدليل الآلي والدليل المستحدث[3].

ب–1/ الدليل الرقمي الآلي: يعد الدليل الرقمي الآلي الذي تسميه أغلب الدراسات بالدليل الذي أعد ليكون وسيلة إثبات؛ بمثابة المعطيات الرقمية التي يعد إنشاؤها و/أو الاحتفاظ بها، من المهام الأساسية للجهاز. حيث يقوم بذلك بمجرد تلقيه أوامر تلقائية أو من الشخص المتعامل معه، في إطار المعالجة الرقمية، من دون البحث عن إعداده ليكون دليلا جنائيا.

ومن أهم الأمثلة عن الدليل الرقمي الآلي؛ نجد السجلات التي تنشأ بواسطة جهاز الإعلام الآلي تلقائيا. على غرار مخرجات الجهاز نفسه، التي لا علاقة للأفراد بإنشائها، والتي تكون على شاكلة سجلات الهاتف وفواتير البطاقات البنكية مثلا[4]. كما قد يكون مثالا لذلك؛ أن يحفظ جهاز الإعلام الآلي تلقائيا النص الذي كان الشخص بصدد كتابته عبر برنامج "Microsoft Office Word"؛ قبل أن ينقطع التيار الكهربائي بصورة مفاجئة.

بالإضافة إلى ما ذكر، يمكن أن يتكون الدليل الرقمي الآلي؛ من السجلات التي تم حفظ جزء منها بالإدخال، وإنشاء الجزء الآخر عبر الجهاز. الأمر الذي له علاقة مباشرة باستعمال "الإنترنت". على غرار حفظ رسائل غرف المحادثة ورسائل البريد الرقمي[5]. كما قد يتعلق الأمر بالذاكرة الآلية المتصلة بمتصفحات الشبكة، حيث تحفظ آليا كل ما يتعلق بتحركات الشخص عبر الشبكة ولفترة طويلة نوعا ما.

---

[1] **أنظر:** عمر محمود أبو بكر يونس، الجرائم الناشئة عن استخدام الإنترت-الأحكام الموضوعية والجوانب الإجرائية، دار النهضة العربية، القاهرة، مصر، 2004، ص 992. **نقلا عن:** محمد كمال شاهين، المرجع نفسه، ص 368.

[2] **أنظر:** هلالي عبد الله أحمد، مرجع سابق، ص 16.

[3] العديد من الدراسات تقسم الدليل الرقمي وفق هذا المعيار –من دون تسميته بالمعيار الموضوعي-؛ إلى الدليل الذي أعد ليكون وسيلة إثبات، والدليل الذي لم يعد ليكون وسيل واثبات. الأمر الذي لم نرغب في إتباعه نظرا للعديد من الأسباب. منها القول بوجود أدلة أعدت مسبقا لتكون وسيلة إثبات؛ هو أمر مجانب للصواب. حيث بالبحث في مضمون ذلك؛ نجدها مجرد وسائل رقمية أعدت للعديد من الأغراض، والإثبات ما هو إلا أحد المزايا المتصلة. كما أنه بالتعمق في دراسة؛ القسمين نجد أن الأول منها -الذي أعد ليكون وسيلة إثبات-؛ هو دليل موجود في كل الأجهزة بصورة آلية، كخاصة الحفظ مثلا. والثاني -الذي لم يعد ليكون وسيلة إثبات-؛ هو مستحدث يخلفه الجاني عند ارتكاب جريمته.

[4] **أنظر:** أمير فرج يوسف، الإثبات الجنائي للجريمة الالكترونية والاختصاص القضائي لها، مرجع سابق، ص 290.

[5] **أنظر:** المرجع والصفحة نفسهما.

ب-2/ الدليل الرقمي المستحدث: على العكس من الدليل الرقمي الآلي، يقوم نظيره الدليل الرقمي المستحدث؛ على فكرة الإنشاء المتزامن مع وقت ارتكاب الجريمة أو بعدها مباشرة. وهذا من دون أي دخل لإرادة الجاني في ذلك، الذي لا يرغب في ترك أي أثر رقمي قد يكون دليلا عن ارتكابه لجريمة من جرائم الوسط الرقمي.

يسمي العديد من دارسي هذا المجال الدليل الرقمي المستحدث؛ بالبصمة الرقمية –الإلكترونية-. المتمثلة في الآثار التي يُخلفها مستخدم النطاق الرقمي الافتراضي بصورة عامة، وشقه المتصل بشبكة الاتصال الدولية خاصةً. سيما بسبب تسجيل الرسائل الشبكية المتراسلة –التي يرسلها و/أو يستقبلها-. وعلى العموم؛ تسجيل أي عمل رقمي ينجز عبر الاتصال الشبكي[1].

ولو رجعنا إلى الأمور التقنية ذات الصلة بهذا النوع من الدليل الرقمي؛ لوجدنا أنه –الدليل الرقمي- لم يعد خصيصا للحفظ الرقمي من قبل الشخص الذي أحدثه، وإنما البرامج والتقنيات الرقمية المستعملة في عملتي التحري والتحقيق؛ هي التي تؤدي إلى استخراجه، ولو بعد مرور مدة زمنية معتبرة. حيث الاتصالات الشبكية؛ هي قابلة للضبط بواسطة التقنيات الخاصة لذلك[2].

وعلى العموم يستنتج من دراسة أقسام الدليل الرقمي وفق المعيار الموضوعي؛ أنه لكل من الدليل الآلي والدليل المستحدث، مجموعة مزايا تجعله قابلا للاستخراج والاستعمال من نظيره، وحتى من باقي الأدلة الرقمية الواردة وفق المعايير والمصادر الأخرى عموما. الأمر الذي نبحث فيه من خلال طرح مزايا كل دليل مقارنةً بالآخر.

يمتاز الدليل الرقمي الآلي؛ بكونه سهل التحصيل والاستخراج. وذلك نظرا لأنه أعد مسبقا ليكون وسيلة إثبات على ما يتضمنه من وقائع، وهو ما يعد صعبا بالنسبة للدليل الرقمي المستحدث، الذي لا يمكن تحصيله إلا باستعمال برامج وتقنيات خاصة، التي قد تتصف بالتعقيد. كما أنه –الدليل الآلي-، نظرا لكونه أعد مسبقا ليكون وسيلة إثبات؛ قد يعمد إلى حفظة حتى يتم الاحتجاج به فيما بعد، وبالتالي تقل فرضية فقدانه. الأمر الذي يعد عكس ذلك تماما في الدليل المستحدث؛ الذي قد يفقد بسهولة[3].

وأما بالنسبة لمزايا الدليل الرقمي المستحدث؛ فانه يعد أكثر أهمية من نظيره الدليل الآلي. نظرا لكونه لم يعد أصلا ليكون وسيلة إثبات، ومنه فهو عبارة عن واقعة لا علاقة لإرادة من صدر عنه. الأمر الذي سيجعله يتضمن معطيات مفيدة للكشف عن الجريمة وأطرافها[4].

---

[1] **أنظر:** أمير فرج يوسف، الإثبات الجنائي للجريمة الالكترونية والاختصاص القضائي لها، مرجع سابق، ص 290.

[2] **أنظر:** المرجع نفسه، ص 290 و291.

[3] **أنظر:** عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت-دراسة متعمقة في جرائم الحاسب الآلي والإنترنت، مرجع سابق، ص 92.

[4] **أنظر:** المرجع والصفحة نفسهما.

2. مصادر الدليل الرقمي الجنائي: لم يأتي الدليل الرقمي هكذا دفعة واحدة ونوعا واحدا، وإنما ورد في إطار مصادر معينة تختلف بحسب النطاق الافتراضي المعتمد لارتكاب الجريمة المقصودة. حيث للدليل الرقمي في المواد الجنائية العديد من المصادر الرقمية الأساسية الحديثة، التي تعد أساس تعقيد وصعوبة التعامل مع هذا النوع من الدليل الجنائي.

إلا أنه بالرجوع إلى الأحكام التقنية ذات الصلة بالوسط الرقمي؛ يمكن القول باستحالة حصر وتحديد الدليل الرقمي، بصورة نهائية، سيما بالنظر إلى ديناميكية تطور الوسط الرقمي نفسه. وان كان يمكن أن نحدد مصدره العام، المنطوي على المعطيات المشكلة للنطاق الافتراضي الذي تحدثه عناصر الوسط الرقمي عموما.

ورغم ورود في العديد من الدراسات الجنائية السابقة –في هذا الصدد–؛ أن مصادر الدليل الرقمي تتعدد وتتنوع، إلى درجة لا يمكن حصرها. إلا أننا نقول بعكس ذلك، فالدليل الرقمي له مصدر واحد منطوي على المعطيات الرقمية، التي قد تتفرع على حسب المعيار المعتمد للتقسيم. الأمر الذي نجد فيه ثلاثة معايير أساسية، فقد نقسم المعطيات إلى بيانات أو معلومات، وفق ما بينا سابقا بخصوص دراسة الوسط الرقمي كمسرح للجريمة. إلا أن لهذا التقسيم أهمية جنائية من حيث المعطيات محل الجريمة، ولا أثر له بخصوص الدليل الرقمي إلا من حيث سهولة التعامل معه، من منطلق كون البيانات ترد غير مفهومة والمعلومات تكون قابلة للفهم.

كما قد تقسم المعطيات الرقمية التي تكون بمثابة الدليل الرقمي، وفق المعيار الوارد باتفاقية بودابست لسنة 2001 –المذكورة سابقا–؛ إلى "معطيات المشترك– Données relatives aux abonnées"، و"معطيات المرور– Données relatives aux trafic"، و"معطيات المضمون– Données de contenu". حيث تعتبر معطيات المشترك، بمثابة المعلومات الشخصية التي يعالجها المشترك بصورة إرادية، بمناسبة فتح حساب شبكي وغير شبكي. وأما معطيات المرور؛ فهي كل المعلومات التي تعالج من قبل الجهاز في إطار الاتصالات الشبكية وغيرها. فيحدد من خلالها؛ مصدر الاتصال ووجهته ومساره وتاريخه وحجمه ومدته وكذلك نوع الخدمة الأساسية[1].

وأما معطيات المحتوى، فثار خلاف فقهي فرنسي حول تصنيفها ودلالتها القانونية. حيث أكد جانب من الفقه؛ على ضرورة التفرقة بين المحتوى "Le Contenu" وحامل المحتوى نفسه "Le contenant". سيما وأن هذا الأخير قد يضم في طياته ما يتخلف عن مفهوم المحتوى، على غرار معطيات الاتصال، التي لا تأخذ مفهوم المحتوى رغم تواجدها ضمن حامل المحتوى، وهي التي تعني المعطيات السامحة بتوجيه الاتصالات الرقمية. وأما الجانب الثاني من الفقه؛ فصرح بعدم إمكانية التفرقة بين المصطلحين، وأسس

[1] **أنظر:** - Art 01/01-d, 21; Convention sur la cybercriminalité- Budapest, op.cit.

لذلك بما ورد في المداولة الصادرة بتاريخ 17 ديسمبر 2015 تحت رقم 455-2015، التي اعتبرت عنوان الانترنت "URL"؛ بمثابة العامل اللازم لانجاز الاتصالات الرقمية، رغم حمله بطبيعته لمعطيات متضمنة تمت معالجتها والتعامل معها[1].

كما يمكن أن نقسمها أيضا إلى العديد من الأنواع بحسب معيار ظهورها العام، على غرار ورودها في إطار محتوى البطاقات المغناطيسية، والتسجيل السمعي والسمعي المرئي، والبريد الرقمي، والتوقيع الرقمي...الخ. حيث تتضمن بطاقات الائتمان معطيات رقمية؛ قد تكون وسيلة إثبات رقمية، كما يعتبر التسجيل السمعي وخاصةً السمعي المرئي –الفيديو–؛ من أهم وسائل الإثبات الرقمي، خاصةً وأنها قد تبين وقائع الجريمة وتحدد أطرافها بدقة. وهذا بالإضافة إلى البريد الرقمي، الذي قد يحوي معطيات مرسلة لها علاقة مباشرة بالجريمة –مثله مثل مواقع التواصل الاجتماعي–. مع الإشارة إلى التوقيع الرقمي، الذي يعد –بكل أنواعه–؛ بمثابة الحجة القاطعة على صاحبها[2].

ثانيا: البعد التقني الخاص للدليل الرقمي الجنائي

إضافة إلى البعد التقني العام للدليل الرقمي، الذي يتعلق بالنطاق الافتراضي للوسط الرقمي عموما، دون التمييز بين العناصر الرقمية المحدثة له؛ يمكن أن نتعامل مع أبعاد تقنية خاصة، تختلف من جهاز لآخر. فجهاز الإعلام الآلي المنزلي يختلف عن الجهاز المفكرة، وهذا الأخير يختلف عن جهاز الجيب –أو كما يسمى بالهاتف المحمول "متعدد الوسائط–Multimédia"، أو الهاتف الجوال–. ولو أخذنا على سبيل المثال هذا الأخير –جهاز الجيب–؛ لوجدنا أن للدليل الرقمي المستخرج منه؛ بعد تقني خاص، ينطوي على أربعة مناطق أساسية.

1. المنطقة الأولى: تتمثل المنطقة الأولى؛ في كل دعامة رقمية تسمح بنقل وانتقال المعطيات، عبر وصلها بالهاتف المحمول. على غرار "جهاز الإعلام الآلي صغير الحجم من النوع المحمول– Laptop"، أو "البلوتوث– Bluetooth"، أو "بطاقة الإيثرنت– Ethernet card"، بالإضافة إلى "جهاز تخزين الشبكة– Network storage device"[3]، و"بطاقة الذاكرة– Memory card". وغيرهم الكثير من الدعامات الرقمية الموصولة بجهاز الجيب، أو التي يمكن أن تكون محلا لذلك، على أن يكون لها علاقة بالواقعة محل التحري والتحقيق طبعا.

---

[1] وهو ما أكدته المداولة رقم 01-2016 الصادرة بتاريخ 14 جانفي 2016، عن اللجنة الوطنية الفرنسية لرقابة تقنيات المعلومات "CNCTR". **أنظر في ذلك:**

- QUEMENER Myriam, Le Droit Face à La Disruption Numérique, Imprimé par Gualino éditeur, Paris, France, 2018, p 131 et 132.

[2] **أنظر:** وردة شرف الدين، مرجع سابق، ص 14 و15 و17 و18-24.

[3] **أنظر:** محمود محمد محمود جابر، مرجع سابق، ص 124.

2. المنطقة الثانية: تشمل المنطقة الثانية؛ النطاق الرقمي المتصل بمعطيات الهاتف النقال نفسه. المنطوية على مكوناته وأي قطعة منه تكون مؤهلة للتخزين الرقمي، يمكن التعامل معها تقنيا بنزعها أو تصليحها أو استبدالها...الخ. على أن تحوي الهواتف النقالة؛ ما تسمى بمكانين الحفظ، التي تحفظ الأدلة الرقمية المراد الوصول إليها جنائيا. على غرار "كارت التخزين–Memory card"، و"بطاقة تعريف المشترك– SIM"[1]، التي تستبعد من الدليل الرقمي محل الدراسة، لو كانت من البطاقات غير العاملة بالنظام الرقمي الثنائي.

3. المنطقة الثالثة: على العكس من المنطقتين السابقتين بالذكر، تخرج المنطقة الثالثة من حدود الهاتف النقال وما يحتويه، إلى المعطيات ذات الصلة بـــ "الشبكة اللاسلكية– Wireless network" من جهة، و"مركز التبديل– Mobile Switching Center" من جهة أخرى، التي ينجز المتهم من خلالها الاتصالات المقصودة. على أننا نشير إلى ضرورة الاستبعاد من دراستنا؛ لكل اتصال ينجز بالطريقة التقليدية للهاتف النقال، من دون الاعتماد على "شبكة الاتصال الدولية– Internet"، من منطلق أن وقائعه الإجرامية تعد بمثابة الجريمة التقليدية لا الرقمية الحديثة كما بينا سابقا، مع إمكانية اعتبار أي معطيات مخزنة في الهاتف الرقمي الحديث، بمثابة الدليل الرقمي، ولو لم يتصل من قبل بأي شبكة كانت.

ومن هذا المنطلق؛ تمتد المنطقة الثالثة لتصل إلى "سجل مواقع الزوار– Visitor location register"، الذي يحوي معلومات المشترك. و"سجل الموقع المحلي– Home location register"، الحامل لمعلومات المستخدم كعنوانه ورقمه. و"مركز التشغيل والصيانة– Operational and maintenance center"، الذي يبرز صورة الأنشطة الشبكية، ويضمن التنصت ومراقبة الاتصالات الكترونية. بالإضافة إلى "مركز التوثيق– Authentication center"، الذي يحفظ المعطيات الضرورية للتحقق من هوية طالب الخدمة. وأخيرا "سجل التعرف على المعدات– Equipment identity register"، الذي يحفظ المعطيات الخاصة بالهاتف المحمول، للتأكد من أنه مسجل، وطريقة استعماله صحيحة ومسموحة[2].

4. المنطقة الرابعة: تشمل المنطقة الرابعة في إطار الدليل الرقمي المتصل بالهاتف المحمول؛ الشبكات المحيطة –الشبكات التابعة–. التي إن وجدت قد يتصل بها الشخص المقصود بالتحري والتحقيق الجنائي، على غرار الشبكة الداخلية والشبكة الداخلية الموسعة السابقتين بالدراسة. وذلك بالإضافة إلى الشبكات الأجنبية العاملة بـــ "اتفاقيات التجوال– Roaming agreements". التي قد يلج إليها ويستعملها الشخص المشترك أصلا مع الشركة المحلية الطرف في الاتفاقية. ولو أنها تستعمل جنائيا؛ للتحقق من تواجد الشخص في منطقة معينة لا أكثر[3].

---

[1] **أنظر:** محمود محمد محمود جابر، مرجع سابق، ص 124.

[2] **أنظر:** المرجع نفسه، ص 124 و125.

[3] **أنظر:** المرجع نفسه، ص 125 و126.

المطلب الثاني: حجية الدليل الرقمي في الإثبات الجنائي

بعد التطرق إلى الدليل الجنائي الرقمي، من حيث ماهيته القانونية، التي سمحت بتحديد معالمه القانونية كدليل إثبات حديث ومختلف. يتوجب المرور إلى البحث في حجيته القانونية –النصية والقضائية–، التي تعد أهم ما يتطلب الدراسة في هذا الإطار، سيما وأن وسيلة الإثبات التي لا تحوز على الحجية اللازمة؛ تعد من قبيل ما يستأنس به القاضي، لتدعيم قناعته المتأتية من الدليل الأساسي لا أكثر، كما قد يقوم باستبعادها تماما.

وفي سبيل التطرق إلى حجية الدليل الرقمي في الإثبات الجنائي؛ سنعمل على تحديدها –الحجية– بصورة عامة في إطار أنظمة الإثبات الجنائي المختلفة(فرع أول)، وبالنظر إلى القضاء الجنائي عموما(فرع ثانٍ)، على أن نركز في الأخير؛ على حجية هذا الدليل الحديث في القانون والقضاء الجزائريين(فرع ثالث).

الفرع الأول: حجية الدليل الرقمي في أنظمة الإثبات الجنائي المختلفة

تتباين أنظمة الإثبات الجنائي المعتمدة من التشريعات المقارنة، فتدور بين الاتجاه الحر من جهة والمقيد من جهة أخرى، ونظام ثالث يجمع بينهما يقوم على محاسنهما. الأمر الذي يقول فيه الأستاذ "شارل جلييروز – GILLIERON Charles"؛ أن الإنسانية منذ القدم تسعى جاهدة في بحثها عن العدالة، للعثور على وسيلة تسمح بالوصول إلى الحقيقة بأقل خطأ ممكن. وهو ما تم إفراغه بعد تأرجح العقل البشري من أقصى حد إلى أقصى حد؛ فيما تسمى بأنظمة الإثبات الجنائي[1].

ونظرا لكون الدليل الجنائي الرقمي، بمثابة وسيلة من وسائل الإثبات الجنائي التي لا تخرج عن الأنظمة الثلاث؛ يتوجب علينا دراسته في القالب العام لهذه الأنظمة مع التركيز على الخصوصية التي يقوم عليها كدليل حديث. وهو ما سنبينه من حيث التطرق إلى حجية الدليل الرقمي في نظام الإثبات الجنائي الحر(أولا)، وحجيته في نظام الإثبات المقيد(ثانيا)، ونظام الإثبات المختلط(ثالثا).

أولا: حجية الدليل الرقمي في نظام الإثبات الجنائي الحر

يعتبر نظام الإثبات الحر؛ أهم أنظمة الإثبات الجنائي عموما. حيث يتناسب مع العقل البشري ومسألة البحث عن الحقيقة الواقعية لا القضائية. ونظرا لصعوبة الوصول إلى ذالك في إطار جرائم الوسط الرقمي

[1] ويرى الأستاذ؛ أن تأرجح العقل البشري في هذا الصدد دار بين اتجاهين أساسيين. فمن جهة؛ تم تصور اليقين القضائي على أنه مسألة خاضعة للتنظيم المسبق من القانون، ومنه الرسو عند نظام الإثبات المقيد -أو القانوني-. ومن جهة أخرى؛ يرى التصور المضاد، أن اليقين مسألة بطبيعة معنوية ذاتية تصدر من ضمير الشخص الذي يتولى البحث عنها، وهو ما نتج عنه نظام الإثبات الحر -أو المعنوي أو الاقتناع الشخصي-. **أنظر في ذلك:** محمد مروان، نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري، ديوان المطبوعات الجامعية، الجزائر، 1999، ص 33 و34.

والتعقيدات التي تعتريها؛ نجده أهم نظام يمكن العمل به في هذا الصدد. الأمر الذي يدفعنا للبحث في مفهومه التقليدي كنظام إثبات جنائي، ومن ثم ربطه بالدليل الرقمي الحديث.

1. مفهوم نظام الإثبات الجنائي الحر: يقوم نظام الإثبات الجنائي الحر –أو المعنوي–؛ على الاقتناع الشخصي، المتحكم دون سواه في قرار القاضي الجنائي، الذي لا يخضع إلا لضميره الشخصي. ومنه يمتنع القانون الوضعي؛ على إلزام القاضي بالعمل بدليل محدد دون سواه. وكل الوسائل التي يأتي بها المشرع؛ ما هي إلا نماذج تذكر على سبيل المثال لا الحصر. كما نجد **أن** العديد من التشريعات الوضعية؛ قد أخذت بنظام الإثبات الجنائي الحر، سيما القانونين الفرنسي والمصري...الخ[1].

من خلال ما ذكر نجد أن نظام الإثبات الجنائي الحر؛ يمتاز بخاصيتين أساسيتين. فهو نظام لا يستبعد أي دليل جنائي، يحوز على الشروط العامة لقبوله، فلا يستبعد القاضي الدليل الجنائي المعروض عليه؛ إلا بعد تفحصه من حيث قيمته الثبوتية. ومن جهة أخرى؛ يمتاز هذا النظام بكونه لا يفرض على القاضي أدلة إثبات جنائي محددة حصرا. حيث يحكم القاضي بما يمليه عليه ضميره، في إطار مشروعية الدليل المطروح. وهو ما سبق لمحكمة النقض المصرية أن أكدته، بقولها بعدم جواز مطالبة القاضي بالأخذ بدليل معين[2].

ومن أهم المبررات التي يتحجج بها أصحاب الاتجاه الحر في الإثبات الجنائي؛ نجد قولهم بأن هذا النظام يأخذ في الحسبان طبيعة الفعل في المواد الجنائية الذي يختلف عن المواد المدنية، من حيث التباين بين الوقائع والظروف المحيطة بها. كما أن اليقين القضائي لا يجد مصدرا له إلا في ضمير الإنسان، المتمثل في القاضي الناظر في الدعوى. بالإضافة إلى أنه نظام متصل أساسا بالأفكار التحررية، التي سادت أوروبا في القرن الثامن عشر تزامنا مع الثورة الفرنسية[3].

إلا أن نظام الإثبات الحر المبين أعلاه وفق الأحكام المتصلة؛ لا يدفع للقول بعدم التدخل المطلق للمشرع الجنائي في إطار الإثبات الجنائي. فقد نجد أحكاما تشريعية عامة تبين وسائل الإثبات الجنائي. كما قد نجد أحكاما أخرى تقيد حرية القاضي بطريقة مباشرة، بخصوص اختيار الوسيلة المناسبة لإثبات جريمة محددة بالذات[4].

---

[1] وللإشارة فان البعض من فقهاء الإسلام؛ قد أخذوا بنظام الإثبات الجنائي الحر، على غرا الفقيه ابن القيم الجوزية، الذي جاء في جزء من قوله، بخصوص تحقيق العدالة عبر جهاز القضاء عموما: "...فأي طريق استخرج به العدل والقسط فهو الدين، وليست مخالفته". **أنظر في ذلك:** عبد الله بن سعيد أبو داسر، إثبات الدعوى الجنائية-دراسة مقارنة، بحث في إطار برنامج الدكتوراه، قسم السياسة الشرعية، جامعة الإمام محمد بن سعود الإسلامية، الرياض، المملكة العربية السعودية، 2011، ص 14.

[2] **أنظر:** حازم محمد حنفي، مرجع سابق، ص ص 232-235.

[3] **أنظر:** محمد مروان، مرجع سابق، ص ص 39-42.

[4] **أنظر:** المرجع نفسه، ص 42.

2. الدليل الرقمي ونظام الإثبات الجنائي الحر: استقرت التشريعات الجنائية المقارنة على قبول الدليل الرقمي كوسيلة إثبات، نظرا لقيمته الثبوتية في مجال جرائم الوسط الرقمي، وحتى الجريمة التقليدية في العديد من الأحيان[1]. سيما وأن الوضع لا يطرح أي إشكال قانوني في إطار نظام الإثبات الحر، نظرا لكونه لا يقيد القاضي بأنواع معينة يعتمد عليها كوسائل إثبات جنائي.

فالمشرع المصري الذي يأخذ بنظام الإثبات الجنائي الحر، بالمادة 302 من قانون الإجراءات الجزائية، التي تنص صراحةً؛ على أن القاضي يحكم بحسب عقيدته المكونة بكامل حرية. ومنه هو حر في قبول الأدلة الرقمية التي ستؤدي للكشف عن الحقيقة، كما هو حر في عملية تقديرها للوصول إلى القناعة التي يبني عليها حكمه[2].

كذلك اعتبرت المادة 291 من القانون نفسه؛ أنه للمحكمة أن تأمر أثناء نظر الدعوى بتقديم أي دليل تراه لازما لظهور الحقيقة. مع العلم أن قانون تنظيم التوقيع الالكتروني الصادر سنة 2004 تحت رقم 15؛ قد وسع من مفهوم المحرر ليشمل إضافةً إلى المحرر التقليدي المكتوب؛ نظيره الالكتروني. حيث اعترفت المادة 15 من القانون نفسه؛ للمحرر الالكتروني بالحجية في الإثبات للمحرر الالكتروني مثله مثل المحرر التقليدي[3]. وهو ما يمتد ليطبق جنائيا في مجال تزوير المحررات الرقمية مثلا.

بالإضافة إلى المشرع المصري نجد أيضا نظيره الفرنسي، الذي يعتمد بدوره نظام الإثبات الجنائي الحر كما بينا سابقا. حيث أقرت المادة 426 من قانون الإجراءات الجنائية الفرنسي؛ بمبدأ الإثبات الحر، عبر نصها الوارد بـــ؛ تثبت الجرائم بجميع طرق الإثبات وبحكم القاضي تبعا لقناعته الخاصة. وعليه يعد الدليل الرقمي مقبولا في الإثبات الجنائي أمام القضاء الفرنسي، على أن يخضع لتقدير القاضي من حيث مشروعيته ونزاهته[4].

كما أن المشرع الفرنسي بموجب القانون رقم 2000-230 الصادر بتاريخ 13 مارس سنة 2000، والمتعلق بالإثبات في مجال تكنولوجيا المعلومات والتوقيع الالكتروني؛ وسع من مفهوم الكتابة التقليدية والالكترونية، إلى درجة ضم مفهومها للأرقام والأحرف والإشارات والرموز، أيا كانت دعامتها والوسيط الذي تنتقل من خلاله. مع التأكيد على اعتبار الكتابة الالكترونية بمثابة الدليل القضائي شأنه شأن الكتابة التقليدية[5]. وهو ما قد يعتمد أيضا في إطار إثبات جريمة تزوير المحررات الرقمية.

---

[1] **أنظر:** محمود محمد محمود جابر، مرجع سابق، ص 126 و127.

[2] **أنظر:** محمد كمال شاهين، مرجع سابق، ص 379.

[3] **أنظر:** محمود محمد محمود جابر، المرجع نفسه، ص 132 و133.

[4] **أنظر:** محمد كمال شاهين، المرجع نفسه، ص 380.

[5] **أنظر:** محمود محمد محمود جابر، المرجع نفسه، ص 127 و128.

ثانيا: حجية الدليل الرقمي في نظام الإثبات الجنائي المقيد

يعد نظام الإثبات الجنائي المقيد؛ ثاني أنظمة الإثبات في المسائل الجنائية عموما. الذي وجد ليقابل نظام الإثبات الحر، من كل الجوانب والأحكام القانونية ذات الصلة. حيث يقوم على عكس الأول، ويمتاز بالبعد القانوني لا القضائي، ومن خلاله القاضي يكون مقيدا. وعلى العموم لا يمكن التطرق إلى التعامل القانوني مع الدليل الجنائي الرقمي في إطار نظام الإثبات المقيد –أو القانوني–؛ إلا بعد تبيان المفهوم الجنائي العام لهذا النظام.

1. مفهوم نظام الإثبات الجنائي المقيد: يعتبر نظام الإثبات الجنائي المقيد –القانوني–؛ بأنه النظام الذي لا يعطي الحق للقاضي الجنائي لأن يستخدم وسائل الإثبات غير المحددة قانونا. ولا يملك حرية الاقتناع الشخصي؛ إلا في إطار الأدلة المحددة حصرا ومسبقا من المشرع. فالقانون هو من يحدد نوع الدليل وقيمته من حيث الحجية، وإجراءات تقديمه إلى الجهات المختصة. ومنه أصبحت يد القاضي مكبلة في إطار منهج سلبي محصور[1].

قد يصل الحد بالمشرع في إطار نظام الإثبات المقيد إلى تحديد قائمة تدرجية، يبين فيها مجموعة من وسائل الإثبات الواردة حصرا، ليتقيد بها القاضي ولا يخرج عنها، حتى وان تبينت له الحقيقة بدليل آخر غير وارد في هذه القائمة. ورغم ورود هذا النوع من الأنظمة لمنع تسلط القضاة، وضمانا لحماية المتهم؛ إلا أنه يكبل القاضي النزيه ويجعله يبتعد عن الحقيقة التي تتطلب وسائل إضافية للوصول إليها. كما أن هذا النظام في الإثبات الجنائي؛ يجعل القاضي غير ملزما لتسبيب حكمه، حيث مجرد اعتماده السليم على وسيلة الإثبات المقررة قانونا، يعفيه من تسبيب حكمه[2].

كما أن الدليل الجنائي في إطار نظام الإثبات المقيد؛ يخضع لقواعد خاصة، على غرار تقسيم الاعتراف إلى درجات، دائر بين الاعتراف التلقائي والمنتزع والكامل والجزئي، مع الاشتراط بوجوب توفر الشاهد؛ على سيرة حسنة ونزيهة مع الجزم في الشهادة. وهو ما يسهل عمل القاضي إلى أبعد الحدود، حيث يصبح همه الوحيد توفر عناصر وسيلة الإثبات المعتمدة وفق النموذج التشريعي لا أكثر. من دون وصوله إلى القناعة الشخصية، التي قد تغيب تماما فتكون مخالفة لما ورد في منطوق الحكم[3].

---

[1] **أنظر:** عبد الله بن سعيد أبو داسر، مرجع سابق، ص 13.

[2] سبق للقانون الفرنسي أن عمل بنظام القائمة –قبل أن يتحول للعمل بنظام الإثبات الحر-. حيث ورد في الأمر الصادر سنة 1970؛ قائمة أدلة إثبات جنائي مقسمة إلى ثلاثة أنواع أساسية. وهي "الأدلة الكاملة- Les preuves pleins"، التي تقيد القاضي تقيدا مطلقا، وبتوفرها يصبح مجبرا بترتيب أثرها القانوني في حكمه. و"الأدلة الناقصة- Démi-preuves"، كشهادة شاهد واحد، التي لا تسمح للقاضي بتسليط العقوبة المقررة قانونا، وإنما ينزل إلى عقوبة أخف. وأخيرا "الأدلة الخفيفة- Légère preuves"، التي لا تكفي لوحدها لإدانة المتهم أو تبرئته، بل يصدر حكما وسطا مثل أن يوقف الدعوى إلى غاية ظهور أدلة جديدة تضاف إلى الأولى. **أنظر في ذلك:** محمد مروان، مرجع سابق، ص ص 34-37.

[3] **أنظر:** المرجع نفسه، ص 37 و38.

إلا أنه يضل نظاما منتقدا لدى الكثير من الفقه الجنائي المعاصر، وذلك نظرا لاحتوائه على العديد من العيوب والسلبيات، سيما أنه يبعد القضاء عن الحقيقة الواقعية التي وجد من أجل الوصول إليها. كما أنه لا يجعل للدليل قيمة أكثر مما حدده القانون له مسبقا. ومنه القاضي لا يملك سوى أن يقضي بما نتج عن هذه الأدلة الواردة حصرا، والتي قد لا تتناسب مع وقائع الدعوى أصلا، فتقود إلى حقيقة قضائية قد لا تتوافق مع الواقع الحقيقي[1].

2. الدليل الرقمي ونظام الإثبات الجنائي المقيد: على العكس من الدليل الرقمي في نظام الإثبات الجنائي الحر، الذي تعتبر حجيته أمرا مفروغا منه، حيث يخضع لقناعة القضائي شأنه شأن أي دليل جنائي آخر –تقليدي وحديث–؛ يتطلب نظام الإثبات الجنائي المقيد، لقبول الدليل الرقمي كوسيلة إثبات جنائي؛ أن يكون مقررا مسبقا من المشرع الذي يعتبره وسيلة إثبات جنائي بصورة صريحة ومباشرة[2]. ولعل أبرز مثال عن هذا النظام؛ نجد التشريعين البريطاني والأمريكي –و.م.أ–.

يعد التشريع البريطاني –إلى جانب نظيره الأمريكي– من بين أبرز الأنظمة المقارنة التي تعتمد نظام الإثبات الجنائي المقيد، والذي اعتمد الدليل الرقمي كوسيلة إثبات جنائي صراحةً. حيث ورد ذلك بموجب قانون البوليس والإثبات الجنائي الصادر سنة 1984، الذي حددت مادته رقم 69 مجموعة شروط لازمة التوفر للقول بقيام حجية الدليل الرقمي، كوسيلة إثبات جنائي. والمتمثلة في ضرورة غياب أي ادعاء يصلح ليكون أساسا لاعتبار المعطيات الرقمية، غير دقيقة بسبب الاستخدام الخاطئ أو غير المناسب لعناصر الوسط الرقمي. بالإضافة إلى عمل جهاز الإعلام الآلي بطريقة سليمة كليا، أو جزئيا ما يستبعد فرضية الاستخراج الخاطئ للدليل الرقمي. مع ضرورة الوفاء بكل الشروط المتعلقة بالمستند الرقمي المحددة طبقا لقواعد المحاكمة، سيما المتصلة بطريقة تقديمها[3].

وفق المنهج المقيد نفسه؛ عمل المشرع الأمريكي –و.م.أ–؛ بخصوص الإثبات الجنائي عموما والإثبات بالدليل الرقمي خاصةً. حيث نص صراحةً على الدليل الرقمي في الإثبات الجنائي، بموجب العديد من القوانين. التي نذكر أهمها ما ورد بالمادة 16/1716 من قانون الحاسب الآلي، الصادر سنة 1984 في إطار ولاية "IOWA"، المقررة صراحةً لمخرجات جهاز الإعلام الآلي، على أنها مقبولة بوصفها أدلة إثبات بالنسبة للبرامج والبيانات المخزنة فيه[4].

---

[1] **أنظر:** عبد الله بن سعيد أبو داسر، مرجع سابق، ص 13.

[2] الأمر الذي نراه بمثابة العقبة الإجرائية التي تواجه مكافحة جرائم الوسط الرقمي، سيما وأنها جرائم تتصف بالتطور الديناميكي السريع كما بينا سابقا، ما يجعل المشرع في تأخر دائم من حيث إيجاد وسيلة الإثبات اللازمة والفعالة. بالإضافة إلى أن نظام الإثبات المقيد عموما؛ يعد في تراجع من حيث الاعتماد من التشريعات المقارنة.

[3] **أنظر:** محمود محمد محمود جابر، مرجع سابق، ص 130 و131.

[4] **أنظر:** محمد كمال شاهين، مرجع سابق، ص 383.

كما يقر المشرع الأمريكي، عن طريق قانون الإثبات لولاية "كاليفورنيا–California" الصادر سنة 1983؛ بتوفر الحجية الجنائية في كل دليل رقمي تتوفر فيه الأصالة والثقة، حتى وان كان مسترجعا رقميا بعد حذفه. وهو ما تطرقت إليه صراحةً المادة 3/1001 من قانون الإثبات، التي جاء فيها: "إذا كانت البيانات مخزونة في حاسوب أو آلة مشابهة فان أية مخرجات طابعة منها أو مخرجات مخزونة برؤية العين تبرز انعكاساً دقيقاً للبيانات تعد بيانات أصلية، والدليل الأصلي في الإثبات الجنائي هو الدليل الذي يتحدث عن نفسه"[1].

ثالثا: حجية الدليل الرقمي في نظام الإثبات الجنائي المختلط

بالإضافة إلى نظامي الإثبات الجنائي الدائرين بين الحرية والتقييد في اختيار وسيلة الإثبات؛ تعمل بعض التشريعات المقارنة بنظام وسط بين الاثنين، يطلق عليه وصف النظام المختلط. الذي يقوم على مزايا النظامين السابقين بالدراسة، ومنه يتفادى بالضرورة الانتقادات ذات الصلة. وعلى العموم سنحاول التطرق إلى هذا النظام الثالث؛ من حيث تبيان مفهومه العام، وعرض مدلوله الحديث المتصل بالإثبات عبر الدليل الرقمي.

1. مفهوم نظام الإثبات الجنائي المختلط: يقوم نظام الإثبات الجنائي المختلط؛ على فكرة الجمع بين النظامين السابقين بالدراسة، الحر والمقيد. حيث يحاول إعمال النظامين معا في الوقت نفسه، مع العمل بمحاسنهما وتفادي مساوئهما. فالقاضي ليصدر حكمه وفق هذا النظام المختلط؛ يتوجب أن يكون مقتنعا قناعة شخصية تامة، وفي الوقت نفسه يحترم الاتجاه القانوني المتصل بوسيلة الإثبات[2]. ومنه يمكن القول؛ أن هذا النظام يحمي المتهم من تعسف القضاة عبر تحديد وسائل الإثبات، وفي الوقت نفسه؛ يعطي حرية نسبية للقاضي من حيث الاقتناع الشخصي بالدليل المعتمد في الحكم.

يقوم نظام الإثبات الجنائي المختلط؛ وفق صورتين لا ثالث لهما. فإما يتم الجمع بين الحقيقتين في كل الأحول سواءً في حالة البراءة أو الإدانة، عن طريق تطابق قناعة القانون مع قناعة القاضي. وهو ما تم انتقاده نظرا لعدم إمكانية حدوث التطابق في كل الأحوال، الأمر الذي يقود وفق أنصار هذا الاتجاه؛ بالقاضي إلى ضرورة التصريح بالبراءة مراعاةً لمصلحة المتهم. وأما الصورة الثانية؛ فتلزم القاضي في الحالة النطق بالإدانة؛ أن يجع بين القناعتين القانونية والشخصية[3]. ومنه يتم تلافي الانتقاد الموجه للصورة الأولى، بطريقة منطقية تقيد القاضي في الإدانة ولا تقيده في البراءة، الأمر الذي يستبعد حتى فرضية التعسف القضائي.

---

[1] **أنظر:** محمد كمال شاهين، مرجع سابق، ص 384.

[2] **أنظر:** محمد مروان، مرجع سابق، ص 42.

[3] **أنظر:** المرجع نفسه، 43 و44.

يعد نظام الإثبات الجنائي المختلط؛ من الأنظمة التي لا يعمل بها كثيرا من الناحية القضائية، من منطلق عدم تقريرها تشريعيا في أغلب التشريعات المقارنة، ولو أننا نجد أبرز مثالين على ذلك التشريعين الياباني والشيلي[1]. وفي الإطار نفسه؛ يعود عدم التقرير التشريعي لهذا النظام إلى النقد الفقهي الموجه له، من حيث اعتباره نظام نظري أكثر منه عملي. حيث من الناحية النظرية يبدوا واضحا كنظام مستقل، لكن تطبيقيا يؤدي إما للعمل بالنظام الحر أو المقيد[2].

2. الدليل الرقمي ونظام الإثبات الجنائي المختلط: لا يمكن القول بتغاضي نظام الإثبات المختلط عن الدليل الرقمي الجنائي، سيما وأن الوسط الرقمي بصفة عامة؛ لم يستثني لا دولة ولا مجتمع إلا ولج إليه وفق ما سبق بيانه. ووفق هذا المفهوم، يتوجب على التشريع المعتمد لنظام الإثبات الجنائي المختلط؛ أن يتطرق إلى الدليل الرقمي، أو على الأقل تنظر إليه الدراسات الفقهية ذات الصلة؛ بالدراسة والتحليل لإدراجه ضمن خانة الوسائل المعتمدة مسبقا، ما يسهل على القضاء عملية الاعتماد عليه لإثبات العديد من جرائم الوسط الرقمي، التي تتصف بالتعقيد والخطورة.

وفي هذا الإطار نجد أن التشريع الياباني المعتمد للنظام المختلط؛ قد حصر وسائل الإثبات الجنائي في أقوال المتهم وشهادة الشهود والقرائن والخبرة، من دون التطرق الصريح إلى الدليل الرقمي. الأمر الذي دفع بالفقه الجنائي الياباني للتدخل، عبر القول بأن السجلات الالكترومغناطيسية –التي تعد السجلات الرقمية واحدة منها– تكون غير مرئية في حد ذاتها، ولذلك لا يمكن أن تستخدم كدليل إثبات، إلا إذا ما تم تحويلها إلى الصورة المرئية المقروءة، عبر الوسائل الرقمية المستعملة لذلك، مثل الطابعة وما إلى ذلك. ومنه تصبح سجلات مقبولة جنائيا كوسيلة إثبات، سواءً وردت في صورتها الأصلية أو في شكل نسخة مطابقة للأصل[3].

بالإضافة إلى التشريع الياباني نجد أيضا التشريع الشيلي، الذي يعتمد نظام الإثبات الجنائي المختلط. حيث حصر وسائل الإثبات في شهادة الشهود وتقارير الخبراء والمعاينة القضائية والمستندات الرسمية والاعتراف والقرائن والأدلة الظرفية. كما منح السلطة التقديرية للقاضي عبر المادة 456 من قانون الإجراءات الجنائية، حيث نصت على ضرورة الاقتناع الشخصي للقاضي قبل أي إدانة. وأما بخصوص الدليل الرقمي الجنائي؛ فالمشرع الشيلي لم يذكره صراحةً؛ إلا أن القول الفقهي يذهب إلى الفكرة نفسها الواردة بخصوص الفقه الياباني، حيث يتوجب إخراج الدليل الرقمي في صورته المرئية المقروءة ومن ثم إلحاقه بأي وسيلة إثبات معتمدة، حتى يعتمد كدليل إثبات[4].

---

[1] **أنظر:** محمد كمال شاهين، مرجع سابق، ص 385.

[2] **أنظر:** محمد مروان، مرجع سابق، ص 44.

[3] **أنظر:** محمد كمال شاهين، المرجع نفسه، ص 285 و286.

[4] **أنظر:** المرجع نفسه، ص 386.

الفرع الثاني: حجية الدليل الرقمي أمام القاضي الجنائي

تقوم حجية الدليل القانوني عموما والدليل الجنائي الرقمي خاصةً؛ على بعدين أساسيين، الأول قانوني والثاني قضائي. حيث يتطلب في الدليل الرقمي حتى يكون وسيلة من وسائل الإثبات الجنائي؛ أن يتوفر على الحجية القانونية السابقة بالدراسة، التي تقوم وفق نظام الإثبات المعتمد قانونا، والشروط ذات الصلة. وبالتبعية يتوجب أن يحوز الدليل الرقمي على الحجية القضائية، التي لها شروط ومتطلبات صحة يتطلبها القاضي حتى يعتمد هذا الدليل، ويؤسس عليه الحكم الصادر بالبراءة أو الإدانة.

ورغم حداثة الدليل الجنائي الرقمي –من حداثة الوسط الرقمي ذاته–، وتباين المواجهة القضائية المقارنة لهذا النوع من الدليل الجنائي الحديث، الدائرة بين الاعتماد الرفض من جهة، وتقييمه بعد مناقشته من جهة أخرى؛ إلا أنه أصبح أمرا واقعا وضروريا لمكافحة جرائم الوسط الرقمي سيما الخطيرة منها. ومنه سنستعرض فيما يلي؛ الحجية القضائية للدليل الرقمي، عبر التطرق إلى متطلبات صحته القضائية(أولا)، وطرح بعض نماذج هذه المواجهة القضائية في الإطار المقارن(ثانيا).

أولا: المتطلبات القضائية لصحة الدليل الرقمي الجنائي

لا يمكن القول بصحة كل الأدلة الرقمية المستوحاة من مصادرها –الرقمية أيضا– التي سنحددها فيما بعد. فلابد لاعتبار أي دليل رقمي على أنه صحيح وقابل للاستعمال القضائي الجنائي؛ من البحث في متطلبات صحته، من حيث العديد من النقاط. التي يمكن تلخيصها في ضرورة توفر المشروعية في طرق تحصيل الدليل، والنزاهة ذات الصلة، مع ارتباطه بموضوع الجريمة محل التحري والتحقيق، بالإضافة إلى يقينيته من جهة وقابليته للمناقشة من جهة أخرى.

1. مشروعية الدليل الرقمي: تعد من أهم متطلبات الصحة القضائية للدليل الجنائي الرقمي؛ أن يكون محصلا بالطرق القانونية السليمة. حيث يتوجب توفر الاتفاق بين الإجراء المتخذ لتحصيل الدليل الرقمي، والقواعد القانونية السارية في هذا الشأن، التي تجد أساسها في المبادئ السامية لحقوق الإنسان وقواعد النظام العام وحسن الآداب في المجتمع المتمدن. ويعد هذا الشرط الأساسي؛ شرطا تقليديا يتطلبه الدليل التقليدي على اختلاف صوره، وأنظمة الإثبات المعتمدة، وما تطبيقه في إطار الدليل الرقمي، إلا إسقاطا للقواعد التقليدية على هذا النوع الجديد من وسائل الإثبات الجنائي[1].

[1] الأمر الذي دفع بالفقه الجنائي؛ إلى الاختلاف حول مسألة استعمال الأشخاص -المتهم وغيره-، للوصول إلى الدليل الرقمي إذا كان يعرف السبيل لذلك، سواءً برضاه أو بغير رضاه. حيث يرى الفريق الأول بعدم جواز جبر الأشخاص، فالمتهم لا يجوز إلزامه باتهام نفسه، والشاهد غير مجبر على تقديم المساعدة للحصول على الدليل الرقمي، فالشاهد الذي يعرف كلمة السر مثلا، يعد غير مجبرا على تقديمها، وان قدمها أو فكها؛ فعمله يعد أقرب إلى الخبرة من الشهادة. وأما الفريق الثاني؛ فيوافق الرأي الأول من حيث عدم جواز إجبار المتهم، لكن بخصوص الشاهد فله موقف آخر، حيث يتوجب على الشاهد؛ أن يقوم بالمساعدة الرقمية –مثل تقديم كلمة السر أو المعطيات الرقمية اللازمة-، إلا ما تعلق منها بالسر المهني. **أنظر في ذلك:** حسين ربيعي، مرجع سابق، ص 265 و266.

إلا أن مشروعية طرق تحصيل الدليل الجنائي الرقمي، تختلف على حسب أثر الدليل نفسه، الدائر بين دليل الإدانة ودليل البراءة. فبخصوص دليل الإدانة؛ يتطلب أن يكون مشروعا، وكل ما تخلف ذلك سيؤدي إلى إهدار أحد أهم ضمانات المحاكمة العادلة، الأمر الذي يؤدي إلى كسر قرينة البراءة انطلاقا من دليل محصل بالطرق غير المشروعة. كأن يتم الحصول على الدليل الرقمي؛ عن طريق مراقبة الاتصالات الرقمية، من دون مراعاة الإجراءات الشكلية التي يتطلبها القانون[1].

والقاعدة الإجرائية؛ أن بطلان الإجراء الأصلي؛ يؤدي حتما إلى القول ببطلان كل الإجراءات التي جاءت بعده. الأمر الذي أكدت عليه التوصية رقم 18 الصادرة عن المؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات، في مجال حركة إصلاح الإجراءات الجنائية وحماية حقوق الإنسان. التي ورد فيها أن كل الأدلة التي تم الحصول عليها عن طريق انتهاك حق أساسي للمتهم والأدلة الناتجة عنها تكون باطلة ولا يمكن التمسك بها أو مراعاتها في أي مرحلة من مراحل الإجراءات[2].

وأما فيما يخص الدليل الرقمي غير المشروع المقرر لبراءة المتهم؛ فلم يستقر الفقه الجنائي على رأي ثابت، وإنما انقسم إلى ثلاثة آراء. فيرى الفريق الأول أن المشروعية؛ لازمة سواءً في دليل الإدانة أو البراءة، ولا فرق بين الاثنين. بينما ذهب الفريق الثاني؛ إلى القول بأن المشروعية متطلبة في دليل الإدانة دون البراءة، لأن الأصل في الإنسان البراءة ولا حاجة لإثباتها. وأما الفريق الثالث والأخير؛ فاعتبر بإمكانية الأخذ بالدليل الرقمي المحصل بالطريقة غير المشروعة، طالما لم تصل طريقة تحصيله إلى حد الوصف الجرمي، وانطوت على مخالفة قاعدة إجرائية لا أكثر[3].

2. نزاهة الدليل الرقمي: أوردت العديد من الدراسات عنصر النزاهة في تحصيل الدليل الجنائي عموما والرقمي خاصةً؛ ضمن إطار المشروعية السابقة بالدراسة. وذلك نظرا للتقارب الكبير بين المشروعية والنزاهة، إن لم نقل أن هذه الأخيرة هي جزء من الأولى. إلا أن الحقيقة القضائية تدل على غير ذلك، سيما في إطار الدليل الرقمي المعتمد من القضاء الفرنسي، الذي –القضاء الفرنسي– تطرق إلى النزاهة

---

[1] الأمر الذي دفع بالفقه الجنائي؛ إلى الاختلاف حول مسألة استعمال الأشخاص -المتهم وغيره-، للوصول إلى الدليل الرقمي إذا كان يعرف السبيل لذلك، سواءً برضاه أو بغير رضاه. حيث يرى الفريق الأول بعد جواز جبر الأشخاص، فالمتهم لا يجوز إلزامه باتهام نفسه، والشاهد غير مجبر على تقديم المساعدة للحصول على الدليل الرقمي، فالشاهد الذي يعرف كلمة السر مثلا، يعد غير مجبرا على تقديمها، وان قدمها أو فكها؛ فعمله يعد أقرب إلى الخبرة من الشهادة. وأما الفريق الثاني؛ فيوافق الرأي الأول من حيث عدم جواز إجبار المتهم، لكن بخصوص الشاهد فله موقف آخر، حيث يتوجب على الشاهد؛ أن يقوم بالمساعدة الرقمية –مثل تقديم كلمة السر أو المعطيات الرقمية اللازمة- إلا ما تعلق منها بالسر المهني. **أنظر في ذلك:** حسين ربيعي، مرجع سابق، ص 265 و266.

[2] **أنظر:** نعيم سعيداني، مرجع سابق، ص 212 و213.

[3] **أنظر:** المرجع نفسه، ص 213.

ونرى في ذلك؛ أن المشروعية في التحصيل تنطبق على دليل الإدانة دون البراءة. وذلك لأن غياب دليل الإدانة لوحده؛ يعد كافيا للقول ببراءة المتهم، الذي هو في الأصل بريء. وما دليل البراءة المتحصل بالطريق غير المشروعة؛ إلا سببا داعما للبراءة، التي تخلف دليل كسرها وتحويلها إلى إدانة.

بصورة منفصلة عن المشروعية من جهة، مع التأكيد على اتساع الفجوة بينها وبين المشروعية في الإطار الرقمي من جهة أخرى.

فيعتمد القضاء الفرنسي في العادة؛ على مصطلح نزاهة الأدلة، كمبدأ إجرائي يتصل بالإثبات الجنائي عموما، وذلك بعبارة "Principe de Loyauté des Preuves"[1]. إلا أنه ما يعاب على القضاء الفرنسي؛ أنه لم يضع تعريفا دقيقا لهذا المبدأ، إن في الإطار العام أو بخصوص الدليل الجنائي الرقمي. ولو أنه بمراجعة العديد من الأحكام والقرارات القضائية ذات الصلة؛ نجده قد أعطى العديد من الأمثلة الإجرائية التي يشكل العمل بها مساسا بمبدأ النزاهة.

ومن أهم الإجراءات التي تعد مساسا بمبدأ نزاهة إجراءات التنقيب عن الدليل الجنائي الرقمي؛ نجد عدم احترام الأفراد، عبر استعمال طرق رقمية احتيالية تنطوي على الحيلة والمكر والخديعة والغش والتدليس...الخ. أو المساس بحريتهم وكرامتهم في الإطار الرقمي. حيث قد تنطوي العديد من الإجراءات الرقمية الرامية للوصول إلى الدليل الرقمي؛ على مكونات تؤدي إلى عدم نزاهة الإجراء المستعمل[2]، مثل خداع المتهم بطريقة تقنية تؤدي به؛ إلى الكشف عن كلمة سر حسابه الشبكي من دون علمه ورضاه.

3. علاقة الدليل الرقمي بموضوع الجريمة: يتطلب الدليل الجنائي الرقمي أيضا لضمان صحته القضائية؛ أن تكون له علاقة بموضوع الجريمة. الشرط الذي يعد من المبادئ الأساسية في الإثبات الجنائي عموما والإثبات الجنائي الرقمي بالتبعية. سيما وأنه يقوم على جزئية رقمية حديثة، تتطلب التوافق التام بين الدليل الرقمي المستخرج والأصل المستخرج منه، الذي يكون في شكل رقمي لا يتعامل معه سوى الخبير المختص في الوسط الرقمي[3].

الدليل الجنائي الرقمي كغيره من أدلة الإثبات الجنائي عموما؛ يتطلب أن يكون له علاقة بالجريمة المراد إثباتها، من حيث الإسناد المادي والمعنوي معا. فمن خلاله –الدليل الرقمي–؛ يمكن للقاضي أن يقوم بالإسناد المادي بين السلوك والنتيجة، حيث يلحق هذه الأخيرة بالأول، عبر القول بأنه سبب حصولها. ومن ينتقل من خلال الدليل الرقمي نفسه؛ إلى الإسناد المعني، عبر إلحاق السلوك والنتيجة معا بالمتهم، الذي تتوفر فيه شروط قيام المسؤولية الجنائية[4].

---

[1] **أنظر:** حازم محمد حنفي، مرجع سابق، ص 261.

[2] **أنظر:** - BENSOUSSAN Alain et LEPAGE Agathe et QUEMENER Myriam, "Loyauté de la preuve et nouvelles technologies: entre exigences processuelles et efficacité répressive", Cycle de conférences 2013, La Cour de cassation, paris, France, 2013, p p 236 – 239.

[3] **أنظر:** ضياء علي أحمد النعمان، الغش المعلوماتي-الظاهرة والتطبيقات، المطبعة الوطنية، الرباط، المملكة المغربية، 2011، ص 313 و314. **نقلا عن:** حسين ربيعي، مرجع سابق، ص 267.

[4] كمثال عن الإسناد بالدليل الرقمي. قد يسند القاضي نتيجة وجود صورة خاصة لفتاة في جهاز المتهم، إلى فعل نسخها رقميا من جهازها. ومن ثم يسند السلوك والنتيجة إلى المتهم؛ من خلال وجود الصورة في جهازه الخاص.

4. يقينية الدليل الرقمي: كما يتوجب أن يكون الدليل الرقمي؛ يقينيا غير قابلا للشك، فلا مجال لدحض قرينة البراءة إلا بالدليل القطعي الجازم واليقيني، يسير إرادة القاضي. وهو ما يعد أكثر يقينا في إطار الدليل الرقمي، حيث أكد الفقه الكندي على كون مخرجات الجهاز؛ من أفضل الأدلة، نظرا لتحقيقها اليقين المنشود في الإثبات الجنائي[1].

وينقسم اليقين الإجرائي عموما إلى قسمين أساسيين، قانوني ومعنوي. فيعني اليقين القانوني؛ الحالة الناتجة عن القيمة التي يضفيها القانون على الأدلة، حيث يتلقاه القاضي مباشرة من إرادة المشرع، ما يجعله يتعلق بنظام الإثبات المقيد. وأما اليقين المعنوي؛ فعلى العكس من الأول يتلقاه القاضي من شخصه، انطلاقا من الحرية في الإثبات، وهو الأمر السائد في إطار نظام الإثبات الحر[2].

5. مناقشة الدليل الرقمي: بالإضافة إلى متطلبات الصحة المذكورة؛ نجد عنصر آخر يتمثل في قابلية الدليل الرقمي للمناقشة. حيث لا يمكن للقاضي أن يؤسس قناعته؛ إلا على الوسائل التي طرحت للمناقشة في الجلسة، وخضعت لحرية المناقشة من أطراف الدعوى العمومية. فيتوجب عرض الدليل الرقمي ومناقشته، سواءً أكان واردا في الدعامة المادية كالأوراق المطبوعة مثلا، أو في شكله المعنوي الرقمي الأصلي، كحفظه في جهاز الإعلام الآلي نفسه[3].

وتكمن أهمية مناقشة الدليل الجنائي الرقمي –والدليل الجنائي عموما–؛ في مراقبة عمل القاضي ومنع التعسف. حيث يمكن للقاضي أن يختار بكل حرية؛ الدليل المناسب في إطار نظام الإثبات الحر مثلا. لكن يعد محظورا عليه أن يبني قناعته؛ على أي دليل لم يطرح في الجلسة ليناقش من أطراف الدعوى العمومية[4].

ثانيا: نماذج عن تعامل القضاء المقارن مع الدليل الرقمي الجنائي

تأكيدا لحجية الدليل الجنائي الالكتروني، أمام القضاء الجنائي المختص، سواءً المعتمد لنظام الإثبات الحر أو المقيد أو المختلط؛ كانت قد أصدرت العديد من الجهات القضائية المقارنة، أحكاما وقرارات جنائية ذات صلة بجرائم الوسط الرقمي، التي تم الاعتماد لإثباتها على الدليل الرقمي. وذلك عملا بشروط صحة الدليل المبينة سابقا. الأمر الذي سنبينه بطرح بعض نماذج القضايا في إطار نظام الإثبات الحر المعتمد من القضاء الفرنسي، ونظام الإثبات المقيد المعتمد من القضاء الأمريكي –و.م.أ–.

---

[1] **أنظر:** ضياء علي أحمد النعمان، الغش المعلوماتي-الظاهرة والتطبيقات، المطبعة الوطنية، الرباط، المملكة المغربية، 2011، ص 313 و314. **نقلا عن:** حسين ربيعي، مرجع سابق، ص 267.

[2] **أنظر:** وردة شرف الدين، مرجع سابق، ص 44.

[3] **أنظر:** علي حسن الطوالبة، التفتيش الجنائي على نظم الحاسوب والإنترنت-دراسة مقارنة، عالم الكتب الحديث، اربط، الأردن، 2004، ص 193.

[4] **أنظر:** محمد كمال شاهين، مرجع سابق، ص375.

1. نماذج عن تعامل القضاء الفرنسي مع الدليل الرقمي الجنائي: لا يمكن الحديث عن الاعتماد الفعلي للدليل الجنائي الرقمي في أي دولة؛ إلا بعد أن يتم العمل به فعليا في الإطار القضائي، من خلال إصدار أحكام وقرارات قضائية بالبراءة أو الإدانة، اعتمادا على الدليل الرقمي. الأمر الذي عمل به القضاء الفرنسي في العديد من الأحكام والقرارات، التي لا يمكن حصرها نظرا لكثرتها. على أن أهم ما صدر عن القضاء الفرنسي في هذا الصدد؛ ينطوي على قرارات الغرفة الجنائية بمحكمة النقض، التي تعد مرجعا هاما في هذا الإطار؛ نظرا لكونها محكمة قانون، تنظر في مدى صحة تطبيق القانون من قاضي الموضوع، ومنه صحة اعتماده على الدليل الرقمي.

ونذكر على سبيل المثال لا الحصر، أن محكمة النقض الفرنسية؛ قد اعتمدت على الدليل الرقمي في القضية الصادر قرارها بتاريخ 07 فيفري 2017. حيث تتلخص وقائع القضية، في أن مدير موقع شبكي هدفه الاحتيال؛ قام بإعادة نشر مقال يتضمن عبارات قذف ضد أحد الأفراد، بعد أن تمت إدانته ومعاقبته جنائيا من قبل على النشر الأول بالطريقة نفسها، مع الحكم كعقوبة تكميلية بالغلق المؤقت للموقع الخاص به أيضا. فاعتبرت الغرفة الجنائية بمحكمة النقض، أن إعادة النشر بعد إعادة فتح الموقع مرة ثانية –بعد استنفاذ عقوبة الغلق المؤقت–؛ يشكل جريمة قذف جديدة لا علاقة لها بالجريمة الأولى المحكوم فيها بإدانة مدير الموقع[1].

يفهم من خلال القرار الصادر عن محكمة النقض الفرنسية –المبين أعلاه–؛ أن القضاء الفرنسي قد اعتمد على الدليل الرقمي للقول بإدانة الشخص، الذي أعاد نشر مقال القذف. وهو الأمر الذي يفهم بداهةً؛ نظرا لكون النشر قد حدث شبكيا واكتشافه كان بالطريقة نفسها، وأيضا معاينته من الجهات المختصة وحجز نسخة عن ذلك؛ كان بالطريقة الشبكية نفسها. ولو أنه يمكن في الأخير أن يتم إظهار الدليل الرقمي المحجوز؛ في الدعامة المادية المنطوية على الورقة المطبوعة من الموقع محل الجريمة.

كما لم تخرج محكمة النقض الفرنسية كثيرا في باقي قراراتها؛ عن نهجها المتبع في القرار السابق بالذكر، من حيث اعتمادها على الدليل الرقمي لإثبات جرائم الوسط الرقمي. حيث في قضية مشابهة للقضية الأولى، تقدمت شركة أعوان عقاريين بشكوى؛ عن إعادة نشر محتوى شبكي يتضمن قذف موجه ضد الأفراد؛ عبر محرك البحث "Google". إلا أن الغرفة الجنائية بمحكمة النقض؛ قررت هذه المرة بقرارها الصادر بتاريخ 10 جانفي 2017؛ أن التواجد الآلي على محرك البحث لعبارات القذف المعاقب عليها في السابق؛ لا تشكل جريمة جديدة؛ نظرا للخصوصية الشبكية التي يتمتع بها المحرك، الذي له ذاكرة تحتفظ آليا بكل ما نشر سابقا[2].

---

[1] **أنظر:** - CHAVENT-LECLERE Anne-Sophie, "Droit pénal de l'internet", Revue Pénitentiaire, Numéro 1, France, Janvier-Mars 2017, p 216.

[2] **أنظر:** - Idem, p 215.

2. نماذج عن تعامل القضاء الأمريكي –و.م.أ– مع الدليل الرقمي الجنائي: تعد الولايات المتحدة الأمريكية؛ الدولة الرائدة في مجال الوسط الرقمي عموما، سواءً في الشق التقني المحض أو القانوني المنظم أو المعاقب على التجاوزات الممكن حدوثها من خلاله –موضوعيا وإجرائيا–. الأمر الذي يعد بديهيا، نظرا لكونها الدولة التي نشأ فيها الوسط الرقمي والعناصر المحدثة له، وفق ما بيناه سابقا. كما أن القضاء الجنائي الأمريكي عموما وجهات المتابعة الجنائية خاصةً؛ هي محاطة بخبراء وسط رقمي من نوابغ هذا المجال.

وفي الإطار نفسه؛ كان قد تعامل القضاء الأمريكي في إطار العديد من قضايا جرائم الوسط الرقمي، من خلال الدعاوى المرفوعة من جهات الادعاء العام –وبالطرق المحددة قانونا لذلك–. التي تبحث دائما عن دليل الإدانة، الذي يكون رقميا من الطبيعة نفسها للجريمة موضوع المتابعة. وكما بينا سابقا فالدليل الجنائي الرقمي؛ هو عبارة عن معطيات رقمية –بيانات ومعلومات– تأخذ أشكال وصور مختلفة، تظهر من خلالها للمتعامل معها، على غرار الكتابات والصور والسجلات والتسجيلات الصوتية والمرئية وغيرها الكثير.

لعل من أهم وأحدث القضايا التي شكلت فيها المعطيات الرقمية الدليل الذي يبحث عنه المدعي العام؛ نجد قضية شركة "Microsoft" ضد الوليات المتحدة. التي صدر بشأنها قرار عن محكمة الاستئناف الاتحادية بتاريخ 24 جانفي 2017. حيث تقدم المدعي العام لولاية "New York"؛ بطلب إصدار أمر قضائي يقضي بأمر شركة "Microsoft"؛ لتقوم بإفشاء معطيات متعلقة بمواطن ايرلندي مقيم بايرلندا، بغرض الإثبات الرقمي لجريمة إرهابية أجنبية. مع العلم أنها معطيات مخزنة في خوادم متواجدة في ايرلندا. وهو الطلب الذي قوبل بالرفض من محكمة الاستئناف؛ بسبب عدم الاختصاص الإقليمي للقضاء الأمريكي. الأمر الثابت من قبل اجتهادات المحكمة العليا الاتحادية في وقت سابق[1].

يتبين من خلال مضمون القضية المبينة أعلاه؛ أن المدعي العام يبحث عن دليل يثبت من خلاله الجريمة الإرهابية التي يشتغل عليها. الأمر الذي رأى أنه لا يمكن أن يتحقق إلا عبر المعطيات الرقمية، التي تتضمنها خوادم شبكية متواجدة إقليميا داخل دولة ايرلندا. والرفض القضائي لم يكن بسبب عدم الاعتماد القضائي العام للدليل الرقمي كوسيلة إثبات جنائي حديثة، وإنما كان بسبب تخلف الاختصاص الإقليمي لدى القضاء الأمريكي عموما. وهو ما يثبت أن القضاء الأمريكي يعتمد الدليل الرقمي، وبل يهتم بضمان مشروعية وسائل تحصيله، فلو حصله المدعي العام من دون الرجوع إلى القضاء أو بما يخالف قرار الرفض؛ لكان بمثابة الدليل غير المشروع، الذي لا أثر قضائي له.

[1] **أنظر:** - ROUSSELET-MAGRI Alexandre, "Les Perquisitions «informatiques» à l'épreuve du principe de souveraineté dans un contexte de mondialisation du stockage de données-étude comparée en droit français et États-Unien", Revue de science criminelle et de droit comparé, Numéro 4, France, Octobre-Décembre 2017, p 671 et 672.

الفرع الثالث: حجية الدليل الرقمي الجنائي في القانون والقضاء الجزائريين

يبدوا أن الدليل الرقمي؛ قد أخذ مكانةً هامة من بين وسائل الإثبات الجنائي المعتمدة من التشريعات المقارنة، بغض النظر عن نظام الإثبات المتبع. الأمر الذي دفعت إليه –كما بينا سابقا– الضرورة الجنائية الملحة، الناتجة أساسا من خطورة جرائم الوسط الرقمي، وصعوبة –إن لم نقل استحالة– إثباتها بالوسائل التقليدية المعروفة. وبالإضافة إلى ذلك يتضح من خلال ما سبق، أن القضاء الجنائي المقارن، قد اقتنع يقينا بضرورة العمل بالدليل الرقمي، إلى درجة اعتباره من بديهيات القانون الجنائي الحديث، الذي –الدليل الرقمي– يعد مقبولا؛ ما دام توفرت شروط صحته سابقة الذكر.

وفي الإطار نفسه، تعد الجزائر تشريعا وقضاءً من الدول التي بادرت إلى العمل بالنهج نفسه المذكور بخصوص التعامل التشريعي والقضائي المقارن مع الدليل الجنائي الرقمي. وهو الأمر الثابت من خلال النصوص القانونية والأحكام والقرارات القضائية ذات الصلة بالدليل الجنائي الرقمي، والدراسات الفقهية المتعلقة بهما. وفي سبيل تبيان ذلك؛ يتوجب علينا التطرق إلى كل من حجية الدليل الجنائي الرقمي في القانون الجزائري(أولا)، وحجيته أمام القضاء الجنائي الجزائري(ثانيا).

أولا: حجية الدليل الرقمي الجنائي في القانون الجزائري

رجوعا إلى القانون الجزائري الذي يعد أساس الدراسة؛ يمكن القول أنه تعامل مع الدليل الجنائي الرقمي وفق الأطر القانونية المبينة سابقا. مع الأخذ في الاعتبار بخصوصية نظام الإثبات المعتمد وشروط صحة الدليل نفسه. الأمر الذي يدفع للقول بضرورة التطرق إلى نظام الإثبات الجنائي الحر، المعتمد بالأساس من المشرع الجزائري، وذلك قبل التعريج بنوع من التدقيق؛ إلى الاعتماد الضمني للدليل الرقمي في الإثبات الجنائي.

1. الاعتماد القانوني الصريح لنظام الإثبات الجنائي الحر: يقوم القانون الجزائري عموما على النهج اللاتيني أو كما يسمى بـــ "الفرنكوجرماني"–، الذي يعتمد بالأساس على نظام الإثبات الجنائي الحر المبين سابقا. حيث يبحث القاضي الجنائي عن الحقيقة –القضائية–؛ انطلاقا من اقتناعه الشخصي، المبني أساسا على الوسيلة أو الوسائل التي يراها مناسبة وتقود لا محال لإظهار هذه الحقيقة.

ويعد نظام الإثبات الجنائي الحر؛ النظام الوحيد الذي عرفته الجزائر المستقلة. حيث اِعتمد منذ إصدار أول قانون إجراءات جزائية سنة 1966، ولم يتم المساس به لا بالتعديل ولا بالتغيير. الأمر الثابت من خلال المادة 1/212 "ق.إ.ج"، التي جاءت بموجب القانون الصادر أول مرة سنة 1966، ولم تعدل إلى غاية يومنا هذا[1].

[1] وذلك رغم تعديل وتميم قانون الإجراءات الجزائية لأكثر من 24 مرة، منذ صدوره لأول مرة سنة 1966. **أنظر في ذلك:** المادة 1/212؛ أمر رقم 66-155، مرجع سابق.

ورد في مفهوم المادة 1/212 "ق.إ.ج"؛ أن الأصل في الإثبات الجنائي يقوم على حرية الإثبات. فيمكن أصلا إثبات الجريمة؛ بأي وسيلة من وسائل الإثبات المتاحة[1]، التي يعمل بها القاضي على حسب اقتناعه الخاص، الدائر بين وسيلة من وسائل الإثبات التي جاء بها المشرع[2]، أو أي وسيل واثبات أخرى يراها مناسبة لتبيان الحقيقة.

إلا أنه كاستثناء عن الأصل، أكدت المادة نفسها؛ على إمكانية تقييد الإثبات الجنائي، بنص تشريعي خاص، يحدد حصرا الوسائل التي لايمكن للقاضي أن يخرج عنها، حتى وان اقتنع بدليل آخر غير منصوص عليه قانونا. بل حتى وان كان الدليل الخارج عن ذلك المعتمد قانونا؛ هو الوحيد الذي سيقود إلى الحقيقة الواقعية، التي تحقق العدالة الحقيقية.

وتطبيقا لذلك أورد المشرع الجزائري في حالات جد ضيقة؛ وسائل إثبات محددة حصرا، لايمكن للقاضي أن يخرج عنها، حيث يكون مطالبا على بناء قناعته من خلالها فقط. الأمر الثابت من خلال وسائل إثبات جريمة الزنا مثلا، التي لا تثبت إلا بثلاث وسائل محددة حصرا، المنطوية على محضر قضائي يحرره أحد رجال الضبط القضائي عن حالة التلبس، أو إقرار وارد في رسائل أو مستندات صادرة من المتهم، أو إقرار قضائي[3].

ركز قانون الإجراءات الجزائية في إطار نظام الإثبات الحر؛ على حث القاضي للبحث عن الحقيقة باستعمال أي وسيلة إثبات يراها مناسبة، بشرط أن تتصف إجراءات جمعها بالمشروعية القانونية اللازمة. حيث أكد على استهداف الحقيقة في العديد من المواقع، على غرار ما ورد بالمادة 1/68 "ق.إ.ج"، التي تسمح لقاضي التحقيق باتخاذ أي إجراء مشروع يراه مناسبا للبحث عن الحقيقة[4]. والمادة 1/69 من القانون نفسه، التي تعطي الحق لوكيل الجمهورية، لأن يطلب من القاضي المحقق كل إجراء يراه مناسبا لإظهار الحقيقة، وذلك سواءً بموجب الطلب الافتتاحي لإجراء تحقيق أو في أي مرحلة يكون عليها التحقيق القضائي[5].

---

[1] **نص المادة:** "يجوز إثبات الجرائم بأي طريق من طرق الإثبات ماعدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص".

[2] وهي الواردة على سبيل المثال، في إطار الاعتراف ومحاضر الشرطة القضائية، والخبرة وشهادة الشهود، واستجواب المتهم، والانتقال للمعاينة. **أنظر في ذلك:** المواد 213-235؛ أمر رقم 66-155، مرجع سابق.

[3] **أنظر:** المادة 341؛ أمر رقم 66-156، مرجع سابق.

[4] **نص المادة:** "يقوم قاضي التحقيق وفقا للقانون، باتخاذ جميع إجراءات التحقيق التي يراها ضرورية للكشف عن الحقيقة، بالتحري عن أدلة الاتهام وأدلة النفي".

[5] **نص المادة:** "يجوز لوكيل الجمهورية سواء في طلبه الافتتاحي لإجراء التحقيق أو بطلب إضافي في أية مرحلة من مراحل التحقيق، أن يطلب من القاضي المحقق كل إجراء يراه لازما لإظهار الحقيقة".

ولو أننا لنا رأي في ذلك. حيث من المعروف أن النيابة العامة ممثلتا في وكيل الجمهورية أو غيره؛ هدفها الأساس هو البحث عن أدلة الاتهام فقط، وذلك نظرا لكونها خصما في الدعوى العمومية. والحقيقة تتطلب البحث عن أدلة الإثبات والنفي معا. الأمر الذي نجده يتعارض مع المهام الأساسية لجهاز النيابة العامة.

كما منح قانون الإجراءات الجزائية؛ لقاضي الموضوع في الجلسة كل الصلاحيات اللازمة التي تمكنه من الوصول إلى الحقيقة المبحوث عنها. الأمر الثابت من خلال المادة 1/286و2 المتعلقة بجلسات محكمة الجنايات[1]، التي أعطت لرئيس جلسة محكمة الجنايات سلطة ضبطها وإدارة المرافعات الدائرة في إطارها، وذلك بغرض ضمان حسن سيرها وفرض الاحترام الواجب للمحكمة نفسها، وبالأخص اتخاذ أي إجراء يراه مناسبا لإظهار الحقيقة.

وبالإضافة إلى ما ذكر؛ قيد قانون الإجراءات الجزائية القاضي ببعض القواعد، التي لا تمس بأي حال من الأحوال بأسس نظام الإثبات الحر. حيث وفق المادة 2/212 "ق.إ.ج"؛ يعد القاضي ملزما ببناء قراره وفق قناعته الخاصة، القائمة على الأدلة المقدمة في الجلسة، والتي حصلت المناقشة بخصوصها حضوريا وبمعيته شخصيا[2]. وإلا شكل ذلك وجها من أوجه الطعن أمام المحكمة العليا، انطلاقا من اعتباره بمثابة الخطأ الجوهري في الإجراءات، أو المخالفة الصريحة للقانون[3].

كما لايمكن للقاضي أن يبني قناعته في إطار نظام الإثبات الحر المعتمد من المشرع الجزائري؛ إلا بالدليل المشروع أو المحصل بالطرق الإجرائية المشروعة. حيث نص قانون الإجراءات الجزائية صراحةً بالمادة 1/157 منه؛ على بطلان كل إجراءات استجواب المتهم وسماع المدعي المدني، المنجزة بالمخالفة لأحكام المادتين 100 و105، بالإضافة إلى بطلان كل الإجراءات التي تليها[4]. الأمر الذي يضفي صفة عدم المشروعية؛ على الدليل المستنتج من الاستجواب الباطل.

2. الاعتماد القانوني الضمني للدليل الرقمي في الإثبات الجنائي: لم يتطرق المشرع الجزائري إلى الدليل الجنائي الرقمي بنص صريح، وإنما اكتفي بالقاعدة العامة المؤدية إلى القول بالاعتماد على نظام الإثبات الجنائي الحر. الذي لا يفرق بين أدلة الإثبات الجنائي، من حيث الأقدمية والحداثة من جهة والنص الصريح عليها من عدمه من جهة أخرى. وإنما يعد بمثابة النافذة القانونية، التي من خلالها يمكن اعتماد أي دليل قانوني تتوفر فيه شروط الصحة اللازمة.

ووفق ما بيناه أعلاه وسابقا، فان المادة 212 "ق.إ.ج" –سابقة الذكر–؛ قد فتحت المجال للقاضي الجنائي لأن يعتمد أي دليل جنائي حديث سواءً كان رقميا أو غير ذلك، ما دام تتوفر فيه المشروعية

---

[1] **نص المادة:** "ضبط الجلسة وإدارة المرافعات منوطان بالرئيس. له سلطة كاملة في ضبط حسن سير الجلسة وفرض الاحترام الكامل لهيئة المحكمة واتخاذ أي إجراء يراه مناسبا لإظهار الحقيقة".

[2] **نص المادة:** "ولا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه".

[3] **أنظر في ذلك:** المادة 500؛ أمر رقم 55-155، مرجع سابق.

[4] **نص المادة:** "تراعى الأحكام المقررة في المادة 100 المتعلقة باستجواب المتهمين والمادة 105 المتعلقة بسماع المدعي المدني وإلا ترتب على مخالفتها بطلان الإجراء نفسه وما يتلوه من إجراءات".

اللازمة، وتتم مناقشته في جلسة علنية تحت إمرته. وكل مخالفة لذلك؛ ستؤدي إلى القول ببطلان الإجراءات المؤدية إلى تحصيله، ومنه استبعاده من دائرة الدليل الجنائي السليم.

وعلى العموم للقول بصحة إجراءات تحصيل الدليل الرقمي؛ يتوجب الرجوع إلى شروط الصحة القضائية المذكورة سابقا[1]. المنطوية على المشروعية المتصلة بحقوق الإنسان عموما، وقواعد الإجراءات الجزائية خاصةً. سيما من حيث التفرقة بين الدليل الرقمي المعد كدليل إدانة ونظيره المعد كدليل براءة، وما تطلبته الدراسات الفقهية ذات الصلة، التي تم التطرق إليها فيما سبق.

كما يتوجب على الأجهزة الجزائرية المكلفة بالبحث عن الدليل الرقمي–قضائية وشبه قضائية وغيرها–؛ أن تراعي مبدأ النزاهة –السابق بالشرح–، عند جمعها للدليل الرقمي. وذلك بالاعتماد على الطرق التي تحفظ وقار الإجراءات ونزاهتها. ومن أمثلة ذلك، الابتعاد عن الحيلة والمكر والخديعة وغيرها. وبالإضافة إلى ذلك؛ يتطلب أن يكون للدليل الرقمي علاقة مباشرة مع موضوع الجريمة، التي يراد البحث عن الحقيقة بشأنها.

ومن أهم شروط صحة الدليل الجنائي الرقمي في إطار القضاء الجزائري؛ نجد أيضا ضرورة يقينية الدليل الرقمي وتلافيه للشك، الذي لو حصل عند القاضي لفسره لصالح المتهم، وفق القاعدة العامة في هذا الإطار. مع القول بضرورة توفر المشروعية الإجرائية وفق الأطر العامة نفسها المذكورة سابقا، بخصوص اعتماد المشرع الجزائري لنظام الإثبات الجنائي الحر.

بالإضافة إلى الاعتماد الضمني للدليل الرقمي في الإثبات الجنائي، الوارد بنص قانون الإجراءات الجزائية؛ نجد أيضا نص وارد في إطار القانون المدني، يتعلق بالإثبات في المواد المدنية. الذي أقر صراحةً بالاعتماد على الكتابة الالكترونية –الرقمية–، كدليل قانوني لإثبات التصرفات المدنية. حيث ورد بالمادة 323مكرر1 من القانون المدني؛ أن الإثبات بالكتابة الالكترونية يعد كالإثبات بالكتابة على الورق. ولو أن النص قد قيد ذلك على شرط واقف، مفاده أن تتوفر إمكانية التأكد من هوية مصدر الوثيقة الالكترونية من جهة، وأن تعد وتحفظ من جهة أخرى؛ في ظروف تضمن سلامة الدليل[2].

وفي الإطار نفسه؛ نجد أن النص الصريح على الكتابة الالكترونية كدليل إثبات في المواد المدنية؛ هو بمثابة النص الضمني على حجية الكتابة الالكترونية، في المادة الجنائية. حيث يمكن الاعتماد عليه مثلا؛ للقول بتزويره جنائيا من جهة، أو في إطار قيام جريمة خيانة الأمانة من جهة أخرى.

---

[1] الأمر الذي نتبع فيه النهج الفقهي والقضائي المقارنين –المذكوران سابقا–، نظرا لتخلف الدراسات الجزائرية في هذا الإطار، التي تؤسس في العادة على غياب الأحكام والقرارات القضائية المبينة لذلك.

[2] **نص المادة:** "يعتبر الإثبات بالكتابة في الشكل الالكتروني كالإثبات بالكتابة على الورق، بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها".

ثانيا: حجية الدليل الرقمي الجنائي أمام القضاء الجزائري

تكريسا للأحكام التشريعية السابقة بالذكر، سيما تلك المتعلقة باعتماد نظام الإثبات الجنائي الحر؛ صدر عن القضاء الجزائري عموما العديد من الأحكام والقرارات، التي تبين بالأساس ذلك الاعتماد الصريح وتجسده على أرض الواقع. الأمر الذي نبينه فيما يلي؛ من خلال التطرق إلى هذا التكريس في إطاره القضائي التقليدي، على أن نعرج بعد ذلك للبحث عن مدى عمل القضاء الجزائري؛ بالدليل الرقمي في الإثبات الجنائي.

1. التكريس القضائي لنظام الإثبات الجنائي الحر: صدر عن القضاء الجزائري العديد من الأحكام والقرارات الجنائية، التي تكرس فعليا العمل بنظام الإثبات الجنائي الحر كأصل عام، مع التأكيد على الاستثناء الوارد عنه بخصوص جرائم محددة حصرا. الأمر الثابت بالوضوح والفصل الواجبين؛ من خلال القرارات الصادر عن المحكمة العليا –المجلس الأعلى سابقا–.

فمن حيث الاعتماد الأصلي والأساسي على نظام الإثبات الحر؛ صدر عن المحكمة العليا العديد من القرارات في هذا الصدد. سيما تلك التي تكرس الإثبات الحر بصريح العبارة، على غرار القرار رقم 70690 الصادر سنة 1991، الذي عبر صراحةً بـــ: "من المقرر قانونا أنه يجوز إثبات الجرائم بأي طريق من طرق الإثبات ماعدا الأحوال التي ينص فيها القانون على غير ذلك، ومن ثم القضاء بما يخالف هذا المبدأ يعد خرقا للقانون"[1].

كما سبق للمجلس الأعلى وأن أكد؛ على ضرورة مناقشة الدليل الجنائي أثناء المرافعات. مع القول بعدم إمكانية تأسيس قاضي الموضوع لحكمه على الدليل، الذي لم يقدم في الجلسة ولم تتم مناقشته حضوريا. وهو الأمر الوارد في العديد من القرارات، على غرار ذلك الصادر سنة 1982 تحت رقم 23008، الذي جاء فيه: "لايمكن لقضاة الموضوع أن يؤسسوا قرارهم إلا على الأدلة المقدمة لهم أثناء المرافعات والتي تتم مناقشتها حضوريا وذلك عملا بالمادة 212 من ق.إ.ج"[2].

وفي الإطار نفسه، أكد المجلس الأعلى أيضا في قرارات أخرى؛ على السلطة التقديرية للقاضي الجنائي الذي يعمل بمبدأ الاقتناع الخاص. حيث أكد على خضوع الاعتراف شأنه شأن باقي وسائل الإثبات إلى تقدير القاضي. وهو الأمر الوارد بالقرار الصادر سنة 1983 تحت رقم 29342، الذي جاء فيه: "متى كان من المقرر قانونا أن الاعتراف شأنه كشأن جميع عناصر الإثبات يترك لحرية تقدير

---

[1] **أنظر:** قرار رقم 70690، صادر بتاريخ 29 جانفي 1991، قضية (ب.ص) ضد النيابة العامة، المحكمة العليا. **نقلا عن:** جمال سايس، الاجتهاد الجزائري في مادة الجنح والمخالفات، منشورات كليك، الجزء الثاني، الجزائر، 2014، ص 639.

[2] **أنظر:** قرار رقم 23008، صادر بتاريخ 21 جانفي 1982، قضية (ف.ل) ضد النيابة العامة، المجلس الأعلى. **نقلا عن:** جمال سايس، الاجتهاد الجزائري في مادة الجنح والمخالفات، منشورات كليك، الجزء الأول، الجزائر، 2014، ص 134.

القاضي، فانه لذلك لا ينبغي تأسيس وجه للطعن بالنقض اعتمادا عليه، ذلك أنه كغيره من وسائل الإثبات يخضع لتقدير سلطة قضاة الموضوع"[1].

وأما بخصوص الاستثناء عن الأصل، المتصل بالخروج عن نظام حرية الإثبات الجنائي، وتقييد القاضي بوسائل محددة حصرا؛ فنجد أن القضاء الجزائري قد كرس ذلك في العديد من الأحكام والقرارات، سيما تلك الصادرة عن المحكمة العليا في إطار وسائل إثبات جريمة الزنا. حيث نجد على سبيل المثال؛ القرار رقم 443709 الصادر سنة 2009، الذي جاء فيه: "لا يعد شريط ((الفيديو)) دليلا من أدلة إثبات جريمة الزنا. أدلة إثبات الزنا متعددة على سبيل الحصر وهي: – محضر معاينة التلبس بالجريمة، يحرره أحد ضباط الضبطية القضائية. – إقرار وارد في رسائل أو مستندات صادرة من المتهم. – إقرار قضائي"[2].

2. العمل القضائي بالدليل الرقمي في الإثبات الجنائي: يمكن القول أن القضاء الجزائري كغيره من نظرائه، سيما بخصوص ذلك القائم على نظام الإثبات الجنائي الحر؛ يعتمد الدليل الرقمي كوسيلة من وسائل الإثبات الجنائي، سواءً تعلق الأمر بإثبات جرائم الوسط الرقمي أو حتى بإثبات الجريمة التقليدية في العديد من الأحيان. ما يقود للقول باتساع الدليل الرقمي من حيث الاعتماد، ليشمل الإجرام الرقمي الحديث والمادي التقليدي معا. الأمر غير المجدي بالنسبة للدليل التقليدي، الذي في العادة يكون عاجزا عن إثبات الإجرام الرقمي.

وفي هذا الإطار سبق للشرطة القضائية المختصة بالتحري والتحقيق في جرائم الوسط الرقمي؛ أن نقبت عن الدليل الرقمي وقدمته للقضاء الجزائري، الذي بدوره اعتمد عليه بعد التأكد من توفر شروط صحته، سيما من حيث مشروعية وسائل جمعه. الأمر الذي ورد في دراسات صادرة عن الأجهزة الشرطية المتخصصة، التي تؤكد مكافحتها لجرائم الوسط الرقمي على اختلاف أنواعها؛ عبر التنقيب عن الدليل الرقمي وإبرازه لقضاء التحقيق والموضوع.

ونجد ابرز الأجهزة الشرطية الجزائرية القائمة بذلك؛ مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها التابع للدرك الوطني –المدروس سابقا–. الذي قدم إلى القضاء الدليل الرقمي الجنائي في العديد من القضايا، المحكوم فيها بالإدانة من خلال ذلك. حيث ورد في الحوصلة الصادرة عن المركز، بخصوص نشاطه خلال سنة 2017 –إلى غاية شهر نوفمبر–؛ أنه عالج خلال هذه السنة ما

---

[1] **أنظر:** قرار رقم 29342، صادر بتاريخ 22 نوفمبر 1983، قضية شركة (س) ضد (ق.م.ن.ح.ن.ع)، المجلس الأعلى. **نقلا عن:** جمال سايس، الاجتهاد الجزائري في مادة الجنح والمخالفات، الجزء الأول، مرجع سابق، ص 228.

[2] **أنظر:** قرار رقم 443709، صادر بتاريخ 24 جوان 2009، قضية (ب.ف) ومن معها ضد النيابة العامة، المحكمة العليا. **نقلا عن:** جمال سايس، الاجتهاد الجزائري في مادة الجنح والمخالفات، منشورات كليك، الجزء الرابع، الجزائر، 2014، ص 1689.

يعادل الـــ 905 قضية في إطار جرائم الوسط الرقمي عموما. التي قدم فيها أدلة رقمية جنائية للقضاء، تفيد الإدانة –أو تنفي المسؤولية–، خاصةً في إطار الإنابة القضائية الصادرة عن قاضي التحقيق، الذي يبحث عن الحقيقة القضائية[1].

كما يؤكد المركز من خلال الحوصلة نفسها، على أنه قدم الدليل الرقمي إلى القضاء المختص، بالنظر في الجرائم المتصلة بتسريب أسئلة شهادتي البكالوريا والتعليم المتوسط لسنة 2017. الذي اعتمد على ذلك –الدليل الرقمي–؛ ليعاقب الجناة البالغ عدد قضاياهم الـــ 92 قضية. هذا بالإضافة إلى العديد من القضايا، التي تم الحكم فيها بالإدانة أو البراءة انطلاقا من الدليل الرقمي المحصل من عناصر المركز نفسه. على غرار 56 قضية متصلة بالمساس الرقمي بالنظام العام ومؤسسات الدولة، و76 قضية تمس بأمن الدولة، و14 قضية أخرى تتصف بجرائم الأموال، و571 قضية لها وصف جرائم الأشخاص، و19 قضية متعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات...الخ[2].

وبنوع من التدقيق بخصوص الدليل الجنائي المقدم للقضاء من المركز نفسه؛ نجد أنه بمناسبة معالجته سنة 2017 لقضية تنطوي على جريمة من جرائم المساس بأنظمة المعالجة الآلية للمعطيات؛ قد استخرج الدليل الرقمي الذي يثبت الجريمة من جهة ويبين هوية مرتكبها من جهة أخرى. حيث تتلخص وقاع القضية في قيام أحد الأشخاص بقرصنة البريد الرقمي التابع لوزارة البريد وتكنولوجيات الإعلام والاتصال. وعلى العموم تم التوصل إلى الدليل الرقمي؛ انطلاقا من المعلومات الرقمية المستنتجة من المعاينة التي سمح بإجرائها مقدم خدمة الانترنت للوزارة –مجمع اتصالات الجزائر ببن عكنون–. كما تم تحديد هوية المشتبه فيه من خلال ذلك أيضا. الذي تمت إدانته من القضاء المختص، بعد توقيفه وتقديمه محملا بالدليل الرقمي[3].

في ختام دراسة المبحث الأول من الباب الثاني عموما، يمكن القول أن لإجراءات التحري والتحقيق في جرائم الوسط الرقمي؛ خصوصية إجرائية تتجاوز من حيث التعقيد الخصوصية الموضوعية السابقة بالذكر. سيما وأنها تقود في الأخير للبحث والتنقيب عن الدليل الرقمي، الذي بينا أنه معقد وتقني يحتاج إلى معرفة وتكوين في هذا المجال الدخيل عن العلوم الجنائية عموما. الأمر الذي يزداد خصوصية في إطار الوسائل والأعمال التي تقود إلى جمع الدليل الرقمي نفسه، خاصةً تلك الجوهرية التي سنعمل على تبيان أحكامها القانونية والتقنية في المبحث الثاني التالي بالدراسة.

---

[1] **أنظر:** - Centre de Prévention et de lutte Contre la Criminalité Informatique et la Cybercriminalité de la Gendarmerie Nationale, "Bilan d'activité du Centre Au titre de l'année 2017", op.cit, p 02.

[2] **أنظر:** - Idem, p 04.

[3] **أنظر:** مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها للدرك الوطني، "حالات ملموسة"، مرجع سابق، ص ص 08-12.

المبحث الثاني
الأعمال الجوهرية لاستخراج الدليل الرقمي الجنائي

تتعامل أجهزة التحري والتحقيق في العادة، مع الجرائم محل المتابعة الجزائية؛ بالاعتماد على مجموعة من الإجراءات التقليدية. التي لا تكاد تتباين بينها من حيث الأهمية الإجرائية، إلا بالنظر إلى الإجراءات الدائرة بين التحري والتحقيق. الأمر الذي دفع بالدراسات التقليدية المتعلقة بالإجراءات الجزائية عموما، إلى التطرق للأعمال الإجرائية؛ دفعة واحدة من دون التمييز بينها، إلا ما هي متعلقة بمرحلة دون الأخرى، كالاستجواب مثلا الذي يتصل بالتحقيق القضائي دون مرحلة البحث والتحري، التي تسبق ذلك.

إلا أننا نرى غير ذلك بخصوص أعمال التحري والتحقيق المتصلة بجرائم الوسط الرقمي. وذلك انطلاقا من الطبيعة الحديثة المعقدة للدليل الرقمي السابق بالدراسة. الذي أحدث شرخا إجرائيا واضحا، يقوم على التباين من حيث القيمة العملية بين الأعمال الإجرائية، الأمر الذي قادنا لتقسيمها –الأعمال الإجرائية– إلى الجوهرية منها، التي يستنبط منها الدليل الرقمي بالأساس، والأخرى المساعدة التي سنتطرق إليها في الفصل الموالي من الدراسة.

وعلى العموم تتمثل الأعمال الإجرائية الأساسية، التي تعمل بها أجهزة التحري والتحقيق في جرائم الوسط الرقمي؛ في المعاينة والتفتيش. اللذان لهما الدور الأساس في الوصول إلى الدليل الرقمي الجنائي(مطلب أول)، كما لايمكن التأكيد على هذا الدور الأساسي؛ إلا بعد الوقوف عند الأبعاد ذات الصلة، المنطوية على الدعم التقني السابق والمزامن للمعاينة والتفتيش من جهة، والنتيجة العملية المتعلقة بحجز ما يترتب عن ذلك من جهة أخرى(مطلب ثانٍ).

المطلب الأول: المعاينة والتفتيش أساس استخراج الدليل الرقمي الجنائي

بحثاً في الأعمال الإجرائية المنجزة بخصوص التحري والتحقيق في جرائم الوسط الرقمي؛ يمكن القول أن أهمها وأساسها يقوم على المعاينة والتفتيش بدرجة أولى. فلا يمكن الوصول إلى الدليل الرقمي الجنائي؛ بالاعتماد اكتفاءً على الإجراءات الأخرى التي أعطيناها الوصف المساعد –القادمة بالدراسة في الفصل الموالي–، نظرا لكونها بمثابة الأعمال المكملة للمعاينة والتفتيش.

ومن خلال ما ذكر؛ يمكن القول بضرورة الحفاظ على الترابط الإجرائي الحديث، الناتج عن حداثة وتعقيد الدليل الرقمي الجنائي. الذي لايمكن الوصل إليه إلا عملا بالمعاينة والتفتيش بالأساس، وباقي الأعمال المساعدة بالتبعية، على حسب الحالة والضرورة الدافعة لذلك. الأمر الذي نبينه أساسا بالتطرق فيما يلي؛ إلى كل من المعاينة(فرع أول) والتفتيش(فرع ثانٍ).

الفرع الأول: المعاينة في جرائم الوسط الرقمي

تعد المعاينة –أو الانتقال للمعاينة–؛ من أهم الأعمال الإجرائية المعمول بها عموما لممارسة إجراءات التحري والتحقيق. حيث إعمالها في مجال مكافحة جرائم الوسط الرقمي؛ لا يعد بمثابة الأمر المستحدث أو الدخيل على الإجراءات الجزائية. وهو ما يدفع للقول بكون المعاينة في جرائم الوسط الرقمي؛ من الإجراءات المرقمنة لا الرقمية[1].

وتعد المعاينة من الأعمال الإجرائية الأساسية، للوصول إلى الدليل الرقمي كما بينا سابقا، سواءً تمت في إطار مرحلة التحري أو كإجراء من إجراءات التحقيق القضائي. الأمر الذي يدفع للبحث في مفهوم المعاينة المرقمنة(أولا)، ومن ثم التطرق إلى الخصوصية التي اكتسبتها بسبب رقمنتها(ثانيا).

أولا: مفهوم المعاينة في جرائم الوسط الرقمي

وقوفاً عند المفهوم العام للمعاينة في جرائم الوسط الرقمي؛ نجدها لا تكتسي أي طابع خاص. سيما وأن المشرع الجزائري نفسه؛ اكتفى بالأحكام التقليدية المعروفة، ولم يتطرق للمعاينة المرقمنة بقواعدها وأحكامها الحديثة، خاصةً وأنه تطرق دون المعاينة؛ للتفتيش والحجز في صورتهما المرقمنة الحديثة[2]. الأمر الذي تداركه الفقه الجنائي؛ انطلاقا من الدراسات التقنية والممارسات القضائية –وهو ما سنبينه في الخصوصية القادمة بالدراسة–. وعلى العموم يمكن أن نحدد مفهوم المعاينة في جرائم الوسط الرقمي؛ عبر التطرق إلى تعريفها وطبيعتها وأهميتها.

1. تعريف المعاينة في جرائم الوسط الرقمي: تعد المعاينة بمثابة أول إجراء يتم العمل به في إطار إجراءات التحري والتحقيق عموما –إلا أنه قد لا يكون الأول، كما قد لا يتم العمل به تماما–. وعلى العموم؛ يمكن أن نعرف المعاينة انطلاقا من هدفها الأساس؛ على أنها: "الانتقال لأماكن وقوع الجريمة بغرض البحث من خلالها عن الأدلة اللازمة أو لمطابقة أقوال الأطراف بحالة هذه الأماكن، ومنه الوقوف عند التوافق بينهما، أو لإعادة تمثيل الجريمة"[3].

والمعاينة كعمل إجرائي أوردها المشرع الجزائري، في إطار قانون الإجراءات من دون التعريف بها. حيث تضمنها بالنص الصريح، مع التفرقة بين المعاينة المعمول بها في مرحلة البحث والتحري،

[1] حيث نفرق بين الإجراء الرقمي ونظيره الإجراء المرقمن. فنقصد بالأول -الرقمي-؛ الإجراء الحديث الذي يحمل الطبيعة الرقمية الافتراضية من جهة، ومن جهة أخرى؛ لم يسبق التعامل معه من قبل، نظرا لارتباط ظهوره بظهور جرائم الوسط الرقمي والإجراءات الخاصة بمكافحتها. وأما الإجراء المرقمن؛ فنستدل به على الإجراء التقليدي المعروف في إطار مكافحة الجريمة التقليدية، الذي تمت رقمنته إجرائيا للتناسب مع المسرح الجرمي الافتراضي، كالمعاينة والتفتيش مثلا.

[2] **أنظر:** المواد من 05 إلى 09؛ قانون رقم 09-04، مرجع سابق.

[3] **أنظر:** ناصر حمودي، (قضاء التحقيق في قانون الإجراءات الجزائية الجزائري-دراسة تحليلية نقدية)، مرجع سابق، ص 73.

والأخرى المنجزة في إطار إجراءات التحقيق القضائي، سيما من حيث الأجهزة المختصة بها، كما بينا سابقا بخصوص قواعد الاختصاص[1].

إلا أن المشرع الجزائري الذي اكتفى بالنص على المعاينة في شكلها التقليدي من دون تعريفها؛ امتنع تماما –كما بينا سابقا– عن التطرق إلى المعاينة المرقمنة، التي تنجز لمكافحة جرائم الوسط الرقمي. الأمر الذي لم يخرج بخصوصه –المشرع الجزائري– كثيرا عن التشريعات المقارنة، التي لم تتطرق أغلبها إلى المعاينة المرقمنة، وان اعتمدها بنص صريح تكتفي بسرد أحكامها من دون التعريف بها.

وعلى العموم حاول الفقه الجنائي في العديد من الدراسات؛ العمل على وضع تعريف قانوني يتناسب مع المعاينة في شكلها المرقمن الحديث، انطلاقا من النص التقليدي للمعاينة من جهة، وخصوصية الوسط الرقمي كمسرح جرمي حديث من جهة أخرى. الأمر الذي تم تعريف المعاينة المرقمنة من خلاله على أنها: "معاينة الآثار والبصمات الالكترونية التي يتركها مستخدم الشبكة المعلوماتية أو الإنترنت وتشمل الرسائل المرسلة منه أو التي يستقبلها وكافة الاتصالات التي تمت من خلال الكمبيوتر والشبكة العالمية"[2].

يبدوا القصور واضحاً في التعريف المبين أعلاه. حيث المعاينة لا تقتصر على النطاق الافتراضي فقط، فقد تنصب على ماديات ومعنويات الجهاز –كما سنبين لاحقا–، وأيضا هي لا تتعلق بالاتصالات فقط كما ذكر التعريف، بل قد تنصب على المنظومة المعلوماتية غير المربوطة بالشبكة أصلا، بالإضافة إلى كونه تعريف بعيد كل البعد عن الأحكام الإجرائية، التي جاء بها المشرع الجزائري في المادتين 64 و79 سابقتي الذكر. ومنه يمكن أن نعرف المعاينة المرقمنة، على أنها: "فحص الوسط الرقمي بعناصره المادية ونطاقه الافتراضي بغرض المحافظة على المسرح الجرمي الافتراضي كمرحلة أولى، أو لإثبات الجريمة، أو لإعادة تمثلها وفق المحاكاة الرقمية، كما قد تستهدف مطابقة أقوال الأطراف مع الواقع الرقمي".

2. الطبيعة القانونية للمعاينة في جرائم الوسط الرقمي: تقوم الطبيعة القانون للمعاينة التقليدية عموما؛ على نطاقين أساسيين. يتمثل الأول في الطابع الاختياري للإجراء، ويتصل الثاني بازدواجية العمل بها، الدائرة بيم مرحلة البحث والتحري من جهة، وإجراءات التحقيق القضائي من جهة أخرى. حيث رجوعا إلى نص قانون الإجراءات الجزائية؛ نجد أن المشرع قد سمح لوكيل الجمهورية بممارسة إجراء المعاينة، خلال مرحلة التحري، وذلك في كل الحالات عدا حالة التلبس، كما سمح لقاضي التحقيق أيضا أن يمارس المعاينة خلال إجراءات التحقيق القضائي، بعد تحريك الدعوى العمومية[3].

---

[1] **أنظر:** المادتان 64 و79؛ أمر رقم 66-155، مرجع سابق.

[2] **أنظر:** محمد كمال شاهين، مرجع سابق، ص 259.

[3] **أنظر:** المادتان 64 و79؛ أمر رقم 66-155، المرجع نفسه.

وأما بخصوص مدى إلزامية لجوء وكيل الجمهورية أو قاضي التحقيق –على حسب الحالة–، إلى ممارسة إجراء المعاينة؛ فيفهم من عبارات المشرع أنه جعل منه إجراءً اختياريا مثله مثل باقي الإجراءات الأخرى –سيما المتعلقة منها بالتحقيق القضائي–[1]، لايمكن اللجوء إليه إلا عندما ترى الجهة المختصة الإمكانية والضرورة لذلك[2].

إلا أن الطبيعة القانونية للمعاينة في جرائم الوسط الرقمي، لا تتطابق كل التطابق مع المعاينة التقليدية المذكورة، حيث تتفق معها في جزئيات وتختلف عنها في جزئيات أخرى. الأمر الذي يعد بديهيا، نظرا لاتصالها بالوسط الرقمي ومسرحه الجرمي الحديث، الذي يتصف بالخصوصية السابقة بالذكر. فينطوي التوافق المذكور؛ على الازدواجية الدائرة بين مرحلة التحري وإجراءات التحقيق القضائي، وفق الطرح نفسه المذكور. إلا أنها تختلف عنها من حيث مدى إلزامية العمل بها. حيث تعتبر ذات طابع إلزامي وضروري، بمصدر واقعي عملي لا قانوني، فلا يمكن عمليا؛ مواجهة هذا النوع من الجرائم من دون معاينة مسرحها الرقمي الافتراضي.

3. أهمية المعاينة في جرائم الوسط الرقمي: قد تكتسي المعاينة عموما الأهمية البالغة، سيما في بعض الجنايات الخطيرة كالقتل العمد. حيث الانتقال السريع لمعاينة مسرح الجريمة مباشرةً؛ يعزز من فرص حفظ الدليل وعدم ضياعه. سواءً الدليل المادي أو الشخصي المتصل بالمتهم والشهود والضحايا. كما أن انتقال قاضي التحقيق لمعاينة مسرح الجريمة، بعد تحريك الدعوى العمومية؛ يعد بمثابة الفرصة الحقيقية لتقربه من ملابسات الجريمة من جهة، ومقارنة ذلك بما ورد إليه في ملف الدعوى من جهة أخرى[3].

إلا أنه وعلى العكس مما ذكر بخصوص أهمية المعاينة في الجريمة التقليدية؛ نجدها أقل أهمية في إطار جرائم الوسط الرقمي. وذلك لسببين أساسيين، فالمجرم الرقمي قلما يترك آثاراً مادية خارجية، كما أن طول الفترة الزمنية بين تاريخ ارتكاب الجريمة –جريمة من جرائم الوسط الرقمي– واكتشافها أو التبليغ عنها؛ يعد بمثابة العائق الفعلي لتحديد هوية الجاني، نظرا للعدد الهائل من الأشخاص الذين يترددون على المسرح الجرمي الافتراضي نفسه –سواءً بحسن نية أو بسوء نية–، هذا بغض النظر عن مشاركتهم الإرادية أو غير الإرادية في إتلاف الدليل الرقمي إن وجد[4].

---

[1] ولو أن النص على عدم إلزامية إجراء المعاينة كان صريحاً بخصوص تلك التي يمارسها قاضي التحقيق، باستعمال مصطلح "يجوز" في بداية المادة 79 "ق.إ.ج". مع عدم تبيان ذلك بخصوص المعاينة الممارسة من وكيل الجمهورية، الواردة بالمادة 64 من القانون نفسه. ولو أن الواقع يجعلها اختيارية، نظرا لعدم الحاجة إلى إعمالها في العديد من الأحيان، سيما بخصوص جرائم الشرف والاعتبار.

[2] **أنظر:** المادتان 64 و79؛ أمر رقم 66-155، مرجع سابق. **وأنظر أيضا:** عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، مرجع سابق، ص 357.

[3] **أنظر:** محمد حزيط، مرجع سابق، ص 115.

[4] **أنظر:** علي عدنان الفيل، مرجع سابق، ص 32 و33.

ثانيا: خصوصية المعاينة في جرائم الوسط الرقمي

تكتسي المعاينة في جرائم الوسط الرقمي، وفق المفهوم المبين سابقا؛ نوعاً من الخصوصية المتعددة الأوجه، التي ترجع بالأساس إلى الوسط الرقمي والخصوصية الحديثة التي يتصف بها. حيث رغم عدم تطرق المشرع إلى المعاينة المرقمنة، واكتفائه بالنص التقليدي المتصل، إلا أن البعد التقني لمسرح الجريمة الافتراضي؛ دفع بها لاكتساب الخصوصية الحديثة نفسها. التي تتصل عموما؛ بمحلها وبالقواعد الإجرائية والفنية المستعملة لانجازها، وكذلك صعوبة انجازها بالطريقة المطلوبة نظرا للعديد من المعوقات التي تعترضها.

1. محل المعاينة في جرائم الوسط الرقمي: تتطرق العديد من الدراسات المتصلة بالمعاينة في جرائم الوسط الرقمي؛ إلى فكرة ازدواجية المحل المقصود بالمعاينة، الدائر بين المكونات المادية –عناصر الوسط الرقمي– والمكونات غير المادية –النطاق الافتراضي للوسط الرقمي–. حيث تكون معاينة الماديات؛ بالانتقال إلي مكان تواجد عناصر الوسط الرقمي –من جهاز وملحقاته ولوازم الشبكة ...الخ–، والتحفظ عليها ماديا قبل العبث فيها[1]. الأمر الذي نجده مجانباً للصواب، انطلاقا مما توصلنا إليه في الفصل الأول من الدراسة. حيث التعامل مع ماديات الوسط الرقمي –عناصره–، بصورة منفصلة عن نطاقها الافتراضي؛ يعد بمثابة التعامل مع الأشياء المادية. ومنه القول بإعمال المعاينة التقليدية العادية، وليس المعاينة المرقمنة الحديثة.

وأما المحل الثاني للمعاينة، المتصل بالمكونات غير المادية –النطاق الافتراضي للوسط الرقمي–؛ فيعد أساس المعاينة المرقمنة محل الدراسة. حيث يتصل بالنطاق الافتراضي الذي يعد وسط ارتكاب الجريمة عموما، ومسرحها الافتراضي خاصةً. فتقوم الأجهزة المختصة بالتحري والتحقيق؛ بمعاينة النطاق الافتراضي للوسط الرقمي بعد الولوج إليه؛ إما بالانتقال إلى مكان تواجد العناصر التي أحدثته، أو عن بعد باستعمال الشبكة[2].

يتضح مما بيناه أعلاه؛ أن الأجهزة المختصة بالتحري والتحقيق لتقوم بالمعاينة في النطاق الافتراضي للوسط الرقمي؛ يتوجب عليها الانتقال إما ماديا أو افتراضيا. حيث قد تنتقل ماديا إلى مكان تواجد عناصر إحداث هذا النطاق الافتراضي، لتلج من خلالها افتراضيا للنطاق نفسه، وهو الأمر الذي لا يمكن انجازه منطقيا إلا إذا ما كانت العناصر متواجدة داخل الإقليم الوطني، أو خارجه –كاستثناء– في إطار الإنابة القضائية الدولية.

---

[1] **أنظر:** حازم محمد حنفي، مرجع سابق، ص 56.

[2] ولو أن العديد من الفقه الجنائي، يرى بعدم قابلية النطاق الافتراضي للوسط الرقمي؛ ليكون محلا للمعاينة. وذلك انطلاقا من العديد من الصعوبات والمعوقات -التي سنتطرق إليها فيما يلي-، سيما وأنها ناتجة عن التعقيد الرقمي الحديث، الذي يعد أكبر إشكال تواجهه إجراءات التحري والتحقيق عموما.

وأما الانتقال الافتراضي؛ فيكون بولوج جهات التحري والتحقيق افتراضيا –عن بعد– في النطاق الافتراضي محل المعاينة، انطلاقا من النطاق الافتراضي الذي تستعمله هي، وهو ما ينجز عبر شبكة الاتصال الدولية كأصل عام. الأمر الذي يكون مقبولا قانونا؛ إذا ما تواجد النطاق الافتراضي محل المعاينة عن بعد داخل الإقليم الوطني –أو بتعبير أدق؛ تواجد العناصر المحدثة لهذا النطاق داخل إقليم الدولة–. إلا أنه يطرح إشكالا إجرائيا؛ في حالة تواجد هذه الأجهزة ونطاقها الافتراضي خارج إقليم الدولة. الأمر الذي لم يتطرق إليه المشرع الجزائري بأي نص إلى حد الساعة، ما يدفع للقول بضرورة إعمال ذلك وفق المساعدة الدولية المتبادلة، القائمة على الأحكام العامة الواردة في الاتفاقيات الدولية الجماعية والثنائية، السابقة بالذكر.

2. القواعد الإجرائية والفنية للمعاينة في جرائم الوسط الرقمي: لايمكن ممارسة المعاينة في جرائم الوسط الرقمي عموما؛ إلا عبر قواعد فنية رقمية، يفترض أن يؤسس لها بالنص الإجرائي القانوني. الأمر الذي نظرا لتخلف المشرع الجزائري، عن وضع نص حديث ينظمه ويحدد أحكامه وفق الدقة نفسها التي يقوم عليها الوسط الرقمي ويتطلبها؛ برز تباعد بين القواعد التقنية اللازمة والقواعد الإجرائية الغائبة أو غير الكافية. وعليه سنتطرق فيما يلي؛ إلى كل من القواعد الإجرائية إن وجدت، والقواعد الفنية اللازمة تقنيا لانجاز المعاينة في جرائم الوسط الرقمي.

أ– القواعد الإجرائية للمعاينة في جرائم الوسط الرقمي: لم يتطرق المشرع الجزائري للمعاينة في جرائم الوسط الرقمي؛ بنص جديد يتناسب مع خصوصية هذا الوسط الحديث. الأمر الذي يدفع للقول بتطبيق الإجراءات التقليدية على المعاينة المرقمنة، التي تعد ناقصة وقاصرة في العديد من النقاط الأساسية. خاصةً وأنها لا تصلح عمليا؛ إلا للمعاينة المادية المعروفة، المنجزة بالتنقل المادي للأجهزة المختصة بالتحري والتحقيق.

فمن جهة قرر المشرع الجزائري؛ إجراء المعاينة لكل من مرحلة البحث والتحري وإجراءات التحقيق القضائي. إلا أنه اكتفى من حيث تبيان الإجراءات المتبعة لانجاز ذلك؛ على المعاينة المتصلة بمرحلة التحقيق القضائي بقيادة قاضي التحقيق، دون تلك المنجزة في إطار مرحلة البحث والتحري بإدارة وكيل الجمهورية[1]. وعليه وضع المشرع بعض الإجراءات التي يتبعها قاضي التحقيق لغرض انجاز المعاينات عموما –في جرائم الوسط الرقمي أيضا–. حيث يتوجب عليه أن يتنقل شخصيا، مع إخطار وكيل الجمهورية المختص، الذي يمكنه مرافقته. كما يصطحب معه كاتب التحقيق وجوبا تحت طائلة البطلان، الذي يقوم بتحرير محضر المعاينة[2].

[1] **أنظر:** المواد 64 و79 و80؛ أمر رقم 66-155، مرجع سابق.

[2] **أنظر:** المادة 79؛ المرجع نفسه.

كما يمكن في إطار التحري والتحقيق معا؛ التنقل ماديا و/أو افتراضيا إلى عناصر الوسط الرقمي ونطاقها الافتراضي محل المعاينة –لمعاينة النطاق الافتراضي–، حتى وان كان خارج دائرة الاختصاص. الأمر الذي تحكمه قواعد الاختصاص السابقة بالدراسة. حيث يمدد الاختصاص الإقليمي لوكيل الجمهورية وقاضي التحقيق، في إطار الأقطاب المتخصصة ليصبح جهويا؛ بخصوص المعاينات المنجزة لمتابعة جرائم المساس بأنظمة المعالجة الآلية للمعطيات[1].

كما يصبح الاختصاص الإقليمي جهوي وفق الشكل نفسه؛ في حال تعلقت المعاينة بجرائم المعاملة الخاصة –جرائم؛ المخدرات والجريمة المنظمة عبر الحدود الوطنية، وجرائم تبييض الأموال والإرهاب، والجرائم المتعلقة بالتشريع الخاص بالصرف–، التي ترتكب بالنطاق الافتراضي أو يُسَهِلُ ارتكابها[2]. إلا أن الانتقال للمعاينة في إطار الجرائم التقليدية المتصلة بالوسط الرقمي؛ فالتمديد يقتصر على التحقيق دون التحري، فيمكن لقاضي التحقيق أن يمدد الاختصاص الإقليمي للمحاكم المجاورة، بشرط توفر ضرورة ذلك التي ينوه لأسبابها في محضر الانتقال، مع إخطار وكيل الجمهورية بالمحكمة المنتقل لدائرتها[3].

وأما بخصوص الانتقال الافتراضي لمعاينة النطاق الافتراضي المتصل بالعناصر المادية المتواجدة خارج الإقليم الوطني؛ فلم يتطرق المشرع الجزائري إلى ذلك بنص صريح حديث. وعليه يتوجب العمل بالقواعد التقليدية، الواردة في الاتفاقيات الدولية ذات الصلة، سواءً الجماعية منها أو الثنائية.

ب– القواعد الفنية للمعاينة في جرائم الوسط الرقمي: نظرا لعدم تطرق المشرع الجزائري –كأغلب نظرائه في العالم–، للقواعد الفنية المعتمدة لإجراء المعاينة المرقمنة؛ توجب علينا البحث عن ذلك في الإطار الفقهي، الذي يعتمد أساسا على الممارسات الفعلية لهذه الأجهزة من جهة والدراسات الفنية من جهة أخرى. حيث يمكننا تقسيم هذه القواعد إلى أولية مساعدة ونهائية أساسية[4].

ب–1/ القواعد الفنية الأولية المساعدة: تنطوي القواعد المساعدة؛ على كل إجراء أولي تمارسه أجهزة التحري والتحقيق لغرض معاينة المسرح الجرمي الافتراضي[5]، من دون الولوج الافتراضي إلى هذا المسرح. حيث تمهد هذه الإجراءات للولوج الافتراضي، من خلال التعامل مع عناصر الوسط الرقمي وكل الماديات المحيطة بها.

---

[1] **أنظر:** المادة 01؛ مرسوم تنفيذي رقم 06-348، مرجع سابق.

[2] **أنظر:** المادة والمرجع نفسهما.

[3] **أنظر:** المادة 80؛ أمر رقم 66-155، مرجع سابق.

[4] الأمر الذي يكون كذلك؛ بخصوص المعاينة بعد التنقل المادي إلى مكان تواجد الأجهزة الرقمية. ويقتصر على النهائية فقط؛ في حال انجاز المعاينة عن بعد من دون تنقل.

[5] الأجهزة التي يُشترط فيها؛ أن تكون على قدر من المعرفة القانونية والفنية، سيما وأنها تعمل في إطار الفريق المتكامل وفق ما بينا سابقا. الفريق الذي يتكون في فرنسا مثلا؛ من 13 شرطي متخصص في الوسط الرقمي، بالإضافة إلى اختصاصهم القانوني الأصيل، المنطوي على الشرطة القضائية. **أنظر في ذلك:** علي عدنان الفيل، مرجع سابق، ص 35.

وعلى العموم تتمثل أهم هذه القواعد الفنية الأولية؛ في تصوير عناصر الوسط الرقمي وكل الماديات المتواجدة بمحيطها، مع التركيز على الوقت بدقة. وتحديد خصائص الأجهزة الرقمية بدقة، من نوع وصنف وقيمة مالية وغيرها. بالإضافة إلى ملاحظة التوصيلات والكابلات بكل مكوناتها، بغرض المقارنة القضائية اللاحقة. كما يتوجب وضع مخطط تفصيلي للمنشأة التي تتواجد داخلها عناصر الوسط الرقمي، وتحديد طاقمها بالتسمية والوظيفة. مع ضرورة الفصل الفوري للكهرباء عن الموقع، لمنع الجناة من محو الآثار الرقمية للجريمة من جهة، وإبعاد كل المتواجدين بالمنشأة عن الأجهزة الرقمية من جهة أخرى[1].

كما يتوجب على الجهاز المتنقل للمعاينة؛ أن يمتنع عن نقل أي معلومة من المسرح المادي الخارجي للجريمة، قبل التأكد من خلو المحيط الخارجي نفسه من أي مؤثرات مغناطيسية قد تتسبب في محو المعطيات المسجلة. مع التحفظ العاجل على كل ما هو متواجد بسلة المهملات من أوراق وأقراص وأشرطة وغيرها، ومستندات الإدخال والمخرجات الورقية للجهاز ذات الصلة بالجريمة، لرفع البصمات ذات الصلة ومضاهاتها[2].

ب-2/ القواعد الفنية النهائية الأساسية: بعد أن يقوم فريق التحري أو التحقيق بالمعاينة المادية اللازمة، المتصلة بالعناصر المادية للوسط الرقمي ومحيطها الخارجي؛ ينتقل إلى المرحلة الثانية، المنطوية على المعاينة النهائية الأساسية، التي تكون بالولوج في المسرح الجرمي الافتراضي. مع التأكيد على إمكانية الاقتصار على هذه المرحلة الثانية فقط، وفق ما بينا سابقا.

تبدأ القواعد الفنية النهائية؛ بمجرد الولوج إلى المسرح الجرمي الافتراضي، وملحقاته الافتراضية أيضا. حيث يتوجب فحص كل المعطيات المتواجدة بالجهاز، من ملفات سطحية ومخفية، بالإضافة إلى تصفح "سلة المهملات الرقمية-Recycle bin"، والعمل على إعادة الملفات المحذوفة باستعمال البرامج المناسبة، كبرنامج "Recovery". مع التأكيد على ضرورة الاستعانة ببرامج أخرى بأغراض متباينة، على غرار برنامج "كسر كلمة السر-Password break". وبرنامج "فحص الهواتف النقالة-Mobile edit"[3].

كما يتطلب على الممارس لعملية المعاينة المرقمنة؛ أن يقوم بالفحص الدقيق لملفات "Log file". التي تمكنه من التعرف على جميع العمليات الرقمية التي قام بها المرتاد على الجهاز، والمواقع الشبكية التي زارها وتعامل معها، وكل الأسماء التي يستعملها لفتح الحسابات الشبكية وغيرها، بالإضافة إلى كلمات السر المتصلة بها[4].

---

[1] **أنظر:** علي عدنان الفيل، مرجع سابق، ص 33 و34.

[2] **أنظر:** المرجع نفسه، ص 34.

[3] **أنظر:** حازم محمد حنفي، مرجع سابق، ص 57.

[4] **أنظر:** المرجع والصفحة نفسهما.

3. معوقات انجاز المعاينة في جرائم الوسط الرقمي: في العادة ما يكون للمعاينة في إطار التحري والتحقيق المتصل بالجريمة التقليدية؛ أثرا ايجابيا يقود لا محال للكشف عن خيوط الجريمة، سيما فيما يخص الجرائم التقليدية الأكثر خطورة، كالقتل مثلا. إلا أن الأمر لا يعد كذلك بخصوص المعاينة المرقمنة، التي تعمل في المسرح الجرمي الافتراضي. حيث تواجهها العديد من المعوقات والصعوبات، التي تنقص من فعاليتها المعروفة.

فالمعاينة ترتبط من حيث الفعالية بالماديات الملموسة، وجرائم الوسط الرقمي؛ لا تخلف في العادة الآثار المادية، وإنما تقتصر على الرقمية المعقدة. كما أن أغلب مجرمي الوسط الرقمي المحترفين؛ يعمدون إلى حذف وتغيير تسجيلات الولوج غير المشروع، لإخفاء الأدلة على السلوكيات المجرمة. بالإضافة إلى كثرة المترددين على المسرح الجرمي الافتراضي، في الفترة الفاصلة بين ارتكاب الجريمة واكتشافها، الأمر الذي ينقص من قيمة نتائج المعاينة، التي حصلت في وسط افتراضي تم العبث به من العديد من الأشخاص بعد ارتكاب الجريمة، سواءً بطريقة إرادية أو غير إرادية. هذا مع التأكيد على الدور السلبي للضحية ومقدمي الخدمات. عبر عدم احتفاظ الضحية و/أو مقدمي الخدمات بمعطيات الولوج وما يترتب عنها، أو اكتشاف الضحية المتأخر للجريمة التي أضرت به[1].

وترى العديد من الدراسات أنه من أجل التغلب على المعوقات المذكورة؛ يتطلب العمل بالعديد من الإجراءات الفنية ذات الطابع الاحتياطي، التي نجد أهمها تفعيل الدور الايجابي لمقدمي الخدمات. حيث يتوجب على مقدم الخدمة؛ أن يقوم بتحديد هوية المشتركين بشبكات الاتصال، لتسهيل انجاز المعاينة بعد اكتشاف أي جريمة من جرائم الوسط الرقمي[2]. الأمر الذي ينجز قبل بدء الزبون من الاستفادة العملية من النطاق الافتراضي[3].

وفي الإطار نفسه؛ نجد بأن المشرع الجزائري قد تفطن لهذا الأمر. حيث أمر مقدمي الخدمات –كما بينا سابقا–؛ ليقوموا بتحديد كل المعطيات ذات الصلة بالزبون واتصالاته مضمونا وسيرا وزمانا. وهو ما جاء على سبيل الإلزام تحت طائلة المسائلة الجنائية. فاعتبر عدم الالتزام بالإجراءات المذكورة –التي سماها بالالتزامات العامة كما بينا سابقا–؛ بمثابة السلوك المجرم تحت وصف الجنحة[4].

---

[1] **أنظر:** محمود محمد محمود جابر، مرجع سابق، ص 154 و155.

[2] ولو أنه حل يقتصر على الجرائم التي ترتكب باستعمال النطاق الافتراضي للشبكة، دون تلك التي يكتفي الجاني من خلالها باستعمال النطاق الافتراضي لجهاز الإعلام الآلي فقط. إلا أن الأمر يعد مفهوما ومعقولا، نظرا لقلة خطورة جرائم الجهاز دون الشبكة من جهة، ولسهولة المعاينة المتصلة بجرائم الجهاز من جهة أخرى.

[3] **أنظر:** محمود محمد محمود جابر، المرجع نفسه، ص 155 و156.

[4] هذا بالإضافة إلى تجريم عدم الالتزام بالإجراءات الخاصة، التي تطلب من مقدمي الخدمات بعد ارتكاب الجريمة. ولو أن تجريم هذه الأخيرة ورد بالقانون 09-04، وأعيد التأكيد عليه بمفهوم يخلط المعنى بتعديل "ق.ع" الوارد سنة 2016. **أنظر في ذلك:** المادة 11؛ قانون رقم 09-04، مرجع سابق. **وأنظر أيضا:** المادة 394مكرر8 المضافة بالمادة 02؛ قانون رقم 16-02، مرجع سابق.

الفرع الثاني: التفتيش في جرائم الوسط الرقمي

زيادةً عن المعاينة السابقة بالطرح؛ يكتسي التفتيش في جرائم الوسط الرقمي الطابع الجوهري، الذي يجعل منه الحلقة الأساس بين كل ما تحويه الإجراءات ذات الصلة بالتحري والتحقيق في الجرائم نفسها. ووفق الطرح نفسه؛ يمكن القول أن التفتيش في جرائم الوسط الرقمي؛ هو من قبيل التفتيش المرقمن لا الرقمي، نظرا لكونه من الإجراءات التقليدية المعروفة بالأساس ضمن الإطار الإجرائي العام.

ونظرا لكون التفتيش إلى جانب المعاينة، أهم الأعمال الإجرائية التي يستنتج من خلالها الدليل الرقمي الجنائي؛ يتوجب علينا البحث فيه من كل الجوانب القانونية ذات الصلة، سيما تلك المنطوية على مفهومه(أولا)، وخصوصيته المترتبة عن الرقمنة الحديثة(ثانيا).

أولا: مفهوم التفتيش في جرائم الوسط الرقمي

على العكس من المعاينة؛ تطرق المشرع الجزائري للتفتيش المرقمن، بصورة منفصلة عن التفتيش التقليدي –ولو أنه يحيل إلى العديد من الأحكام التقليدية كما سنرى لاحقا–. حيث أورد نص خاص يبين الأحكام التقنية الحديثة التي ترقمن التفتيش المعروف، ليتماشى مع خصوصية النطاق الافتراضي للوسط الرقمي، الذي يعد هو نفسه المسرح الجرمي الحديث. الأمر الذي أكسب التفتيش المرقمن الطابع الخاص بمفهوم حديث لم يسبق التعامل معه إجرائيا من قبل. وهو ما سنبينه فيما يلي، من خلال التطرق إلى تعريفه التفتيش المرقمن وطبيعته وأهميته.

1. تعريف التفتيش في جرائم الوسط الرقمي: يصعب في العادة التوصل إلى تعريف جامع مانع يخص التفتيش الجنائي بمفهومه العام. الأمر الناتج عن تعدد أنواع وحالات العمل به، الدائرة بين مرحلة التحري وإجراءات التفتيش أساساً، وانقسام هذه الأخيرة إلى فروع بالتبعية. حيث ينقسم التفتيش المنجز في مرحلة التحري؛ إلى تفتيش الأماكن وتفتيش المشتبه فيه من جهة، والتفتيش في الحالة العادية وفي إطار حالة التلبس من جهة أخرى. إلا أنه اقتصر على الأماكن –بمفهومها العام– دون الأشخاص؛ بخصوص التفتيش المنجز في إطار إجراءات التحقيق القضائي[1].

وعلى العموم يمكن أن نقتصر التعريف؛ على ذلك المتصل بالتفتيش في إطار مرحلة التحري أولا، وبخصوص إجراءات التحقيق ثانيا. فلو تطرقنا إلى هذا الأخير –التفتيش في التحقيق القضائي–؛ لقلنا أنه: "البحث في مكنون سر الأفراد –المساكن والأماكن– على دليل للجريمة المرتكبة، أو البحث عن الدليل، وهو إجراء من إجراءات التحقيق الابتدائي الذي يخوله القانون لقاضي التحقيق أصلا"[2].

[1] **أنظر:** المواد من 44 إلى 48 والمادة 64 والمواد من 79 إلى 85؛ أمر رقم 66-155، مرجع سابق.

[2] **أنظر:** عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، مرجع سابق، ص 266.

وأما فيما يخص التفتيش الذي ينجز في إطار مرحلة البحث والتحري؛ فيعتبر بمثابة الإجراء الاستثنائي، الذي خرج فيه المشرع عن الأصل المتصل بالتحقيق القضائي، ومنحه للشرطة القضائية بإدارة وكيل الجمهورية في حالات معينة وبشروط أساسية[1]. وهو ما يدفع لتعريفه على أنه: "البحث في مكنون سر الأفراد –المساكن– على ملابسات الجريمة للحفاظ عليها، بغرض الاستفادة منها قضائيا فيما بعد، وذلك إما في حالات التلبس بالجنايات والجنح، أو في الحالة العادية، على أن يحتكموا إلى شروط معينة تحت طائلة البطلان"[2].

يتضح أن النص العام لقانون الإجراءات الجزائية؛ قد اعتمد إجراء التفتيش في إطار مكافحة الجريمة التقليدية، وذلك إن بخصوص مرحلة البحث والتحري أو في إطار إجراءات التحقيق القضائي. كما أنه حدد لذلك شروط موضوعية وإجرائية يتوجب إتباعها، وإلا اتصفت نتائج التفتيش بعدم المشروعية، ما يرتب البطلان الإجرائي للإجراء نفسه وكل ما تليه من إجراءات، ومنه عدم الاعتماد القضائي على الدليل المحصل من وراء ذلك[3].

وأما التفتيش المتصل بجرائم الوسط الرقمي؛ فرغم التطرق القانوني له بصورته الحديثة من المشرع الجزائري، إلا أنه لم يعرفه تاركاً ذلك للفقه الجنائي والدراسات ذات الصلة. حيث اعتمده المشرع لأول مرة سنة 2009، بموجب القانون 09-04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها –سابق الذكر–[4]. وعلى العموم؛ تعددت التعريفات المتصلة بالتفتيش في جرائم الوسط الرقمي، التي نجد منها ما تعتبره؛ على أنه: "الاطلاع على محل منحه القانون حماية خاصة باعتباره مستودع صاحبه ويستوي في ذلك أن يكون هذا المحل جهاز الحاسوب أو أنظمة أو الإنترنت"[5].

يؤخذ على التعريف المذكور؛ أنه توسع في تحديد محل التفتيش، إلى حد القول بتفتيش جهاز الإعلام الآلي. الأمر الذي يعد خارجا عن التفتيش المرقمن خاصةً، وعن دراستنا كليا. نظرا لوجوب القول بوقوع

---

[1] **أنظر:** المواد من 44 إلى 48 والمادة 64؛ أمر رقم 66-155، مرجع سابق.

[2] كما يمكن لضابط الشرطة القضائية؛ أن يفتش المشتبه فيه جسديا في حالات معينة. المنطوية على تلك الواردة ببعض النصوص الخاصة، أو ما تكون ناتجةً عن بعض الإجراءات المقررة بالنص العام "ق.إ.ج". فقرر قانون الجمارك مثلا بالمادة 42 منه؛ إمكانية تفتيش الأشخاص المتوقع إخفائهم بنية الغش لبضائع ووسائل للدفع عند اجتياز الحدود. وكذلك يمكن تفتيش ضابط الشرطة القضائية؛ في الحالات العامة للمشتبه فيه فور توقيفه، أو كإجراء مكمل لتفتيش المسكن. **أنظر في ذلك:** عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، مرجع سابق، ص 266 و277 و278.

[3] آثرنا عدم التطرق المفصل للشروط الموضوعية والإجرائية في هذا المقام، تفاديا للتكرار. نظرا لأننا سنستعرضها فيما يلي، عند عرض خصوصية التفتيش في جرائم الوسط الرقمي.

[4] **أنظر:** المادة 05؛ قانون رقم 09-04، مرجع سابق.

[5] **أنظر:** علي حسن الطوالبة، التفتيش الجنائي على نظم الحاسوب والإنترنت-دراسة مقارنة، مرجع سابق، ص 13.

التفتيش على المسرح الجرمي الافتراضي الذي تخلقه عناصره –الجهاز أساس ذلك–، وليس على هذه العناصر بوصفها المادي، الذي يعد أقرب إلى التفتيش التقليدي منه إلى الحديث المرقمن. ولو أنه يحسب للتعريف بوصفه لمحل التفتيش بمستودع صاحبه. الذي نعتبره كذلك، نظرا لحمله المعطيات الرقمية التي يريد أن يحتفظ بها أو يستعملها صاحبها.

كما يُعَرَفُ التفتيش المرقمن أيضا؛ على أنه: "إجراء من إجراءات التحقيق يهدف إلى البحث في داخل نظام حاسوبي معين بإذن قضائي مسبق، سواءً أكان هذا النظام مكونا من حاسوب واحد أو عدة حواسيب مرتبطة فيما بينها بشبكة في محل له حرمة منحه إياه القانون، والغرض استخراج أدلة معلوماتية متمثلة بالمعلومات أو البيانات، والتي تساعد في الكشف عن الحقيقة في جريمة من نوع جناية أو جنحة وقعت وجار التحقيق فيها"[1].

يتبين من التعريف المبين أعلاه؛ أن صاحبه قد ضيق من المفهوم القانوني ووسع من نظيره التقني. حيث اقتصر التفتيش على إجراءات التحقيق القضائي، دون مرحلة البحث والتحري، من خلال الاعتماد على مصطلح "التحقيق" من جهة، و "البحث عن الحقيقة من جهة أخرى". إلا أنه توسع من الناحية التقنية، ليشمل أنظمة الجهاز المنفصلة أو المتصلة عبر الشبكة، مع وصفها على أنها ذات حرمة محمية قانونا. الأمر الذي نعتبره توسعا ايجابيا ودقيقا، سيما وأنه لم يتطرق إلى ماديات الوسط الرقمي بشكل منفصل، وجعل من غرض التفتيش البحث عن البيانات والمعلومات التي نعبر عنها مجتمعة بالمعطيات.

وعلى العموم يمكن من خلال التعريفات المقدمة –التقليدية والحديثة–، والمناقشة التي قدمناها، بالإضافة إلى أحكام المادة 05 من القانون 09-04 سابقة الذكر؛ أن نقدم بوجهة نظر خاصة، التعريف الذي نراه مناسبا للتفتيش في جرائم الوسط الرقمي –التفتيش المرقمن–. فنقول أنه: "إجراء جاء به المشرع ليمارس في إطار مرحلة البحث والتحري و/أو إجراءات التحقيق القضائي، عبر البحث الرقمي في المسرح الجرمي الافتراضي، بغرض الوصول إلى المعطيات الرقمية –البيانات و/أو المعلومات– التي تكون أساسا لإثبات جريمة من جرائم الوسط الرقمي، أو لإظهار الحقيقة المبحوث عنها".

2. الطبيعة القانونية للتفتيش في جرائم الوسط الرقمي: يقوم التفتيش التقليدي عموما؛ على الطبيعة المزدوجة نفسها، التي تمتاز بها المعاينة سابقة الطرح، الدائرة بين ازدواجية العمل بها أولا، والطابع الاختياري ثانيا. وكذلك الأمر بخصوص التفتيش المرقمن، الذي يكتسي الطابع المزدوج من حيث العمل به، في إطار كل من مرحلة البحث والتحري وإجراءات التحقيق القضائي، الأمر الذي أكد عليه المشرع من خلال "ق.إ.ج"، وفق ما بيناه سابقا في إطار تعريف التفتيش عموما[2].

---

[1] **أنظر:** سامي جلال فقي حسين، مرجع سابق، ص 55.

[2] **أنظر:** المواد من 44 إلى 48 والمادة 64 والمواد من 79 إلى 85؛ أمر رقم 66-155، مرجع سابق.

وأما بخصوص الطابع الاختياري؛ فالمشرع أقر صراحةً بجوازية ممارسة أجهزة التحري والتحقيق للتفتيش. حيث عبر عن ذلك بمصطلح "يجوز" بخصوص التفتيش الممارس أثناء التحقيق. وألزم القائم بالتفتيش في إطار مرحلة البحث والتحري لو أراد اللجوء إلى ذلك؛ باحترام الشروط الموضوعية والإجرائية اللازمة عند ممارسته لذلك. ما يعني أن اللجوء إلى التفتيش؛ هو بطابع اختياري[1].

كما أقر المشرع صراحةً بجوازية التفتيش المرقمن، المتبع في التحري والتحقيق عموما. وذلك بموجب القانون رقم 09-04 الصادر سنة 2009، الذي استعمل مصطلح "يجوز" بتعبيره: "يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية..."[2]. إلا أن المشرع بالقانون نفسه؛ يكون قد أخلط المفهوم المتصل بالجوازية. حيث استعمل بخصوص إحدى حالات إعمال التفتيش المرقمن، التي تتصل بالتحري والتحقيق في جرائم الوسط الرقمي عموما –وهي أساس الدراسة–، أنه لا يتم العمل بالتفتيش المرقمن؛ إلا في حالة صعوبة الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إليه[3].

يتبين من خلال ما ذكر؛ أن التفتيش المرقمن سيكون بمثابة العمل الاستثنائي الذي لا يُعمل إلا عند تعذر فك خيوط القضية المتصلة بإحدى جرائم الوسط الرقمي. إلا أن الواقع الرقمي المعقد في هذا النوع من الإجرام الحديث؛ يغلب الوصف القانوني. فيجعل من التفتيش المرقمن بمثابة العمل الأصلي الوجوبي في أغلب القضايا –إن لم نقل كلها–، نظرا للصعوبة الدائمة للوصول إلى الدليل الجنائي المتصل بها.

3. أهمية التفتيش في جرائم الوسط الرقمي: رغم عدم اكتساء التفتيش المرقمن للطابع الملزم من حيث العمل به كما بينا أعلاه؛ إلا أن له أهمية كبيرة من حيث إثبات الجريمة في المسرح الافتراضي، سيما عبر مواجهة المتهم بالأدلة الرقمية المحصلة من التفتيش المرقمن. ما يقوي الاتهام نفسه، ويحول دون إفلات الجاني من العقاب الجنائي المناسب[4].

كما أن للتفتيش في جرائم الوسط الرقمي؛ أهمية كبيرة للكشف عن ملابسات الجريمة وأطرافها. فيمكن من خلاله إثبات وقوع الجريمة ووقت ارتكابها، عبر الوصول إلى آثارها، واستنتاج النية الإجرامية لدى الفاعل حتى قبل تحديد هويته. كما يمكن تحديد هوية الجاني أو الجناة إن تعددوا، مع الوقوف عند دوافعهم ودرجة خطورتهم من حيث احترافهم للإجرام الرقمي من عدمه[5].

---

[1] **أنظر:** المواد 44 و64 و79؛ أمر رقم 66-155، مرجع سابق.

[2] **أنظر:** المادة 1/05؛ قانون رقم 09-04، مرجع سابق.

[3] **أنظر:** المادة 1/04-ج؛ المرجع نفسه.

[4] **أنظر:** أسامة بن غانم العبيدي، "التفتيش عن الدليل في الجرائم المعلوماتية"، المجلة العربية للدراسات الأمنية والتدريب، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، مج 29، عدد 58، نوفمبر-ديسمبر 2013، ص 88.

[5] **أنظر:** عبد الله بن عبد العزيز بن عبد الله الخثعمي، (التفتيش في الجرائم المعلوماتية في النظام السعودي-دراسة تطبيقية)، رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير في العدالة الجنائية، كلية الدراسات العليا، قسم العدالة الجنائية، تخصص السياسة الجنائية، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، 2011، ص 40 و41.

ثانيا: خصوصية التفتيش في جرائم الوسط الرقمي

انطلاقا من مفهوم التفتيش في جرائم الوسط الرقمي –السابق بالذكر–؛ يمكن القول –إن لم نسلم– باكتساب التفتيش بعد رقمنته لنوع من الخصوصية التي تفوق في مداها المعاينة المرقمنة. سيما وأن رقمنه التفتيش ورد بالنص التشريعي الصريح، على العكس من المعاينة التي يعود مصدر رقمنتها والخصوصية ذات الصلة؛ إلى الفقه والقضاء الجنائيين. وعلى العموم يمكن أن نبرز هذه الخصوصية من خلال التطرق إلى محل التفتيش المرقمن وفصله عن المحل التقليمي من جهة، مع التركيز على القواعد الإجرائية المتبعة في ذلك من جهة ثانية، بالإضافة إلى القواعد الفنية المعتمدة من قبل الأجهزة المختصة في هذا المقام من جهة أخرى[1].

1. محل التفتيش في جرائم الوسط الرقمي: لايمكن الحديث عن التفتيش المرقمن للنطاق الافتراضي الناتج عن عناصر الوسط الرقمي –الذي يعد أساس الدراسة–، بشكل منفصل عن هذه العناصر نفسها. وذلك لاستحالة الوصول إلى الدليل الرقمي الجنائي؛ من دون التعامل مع العناصر التي تحويه، عن طريق الولوج المباشر و/أو غير المباشر من خلالها وباستعمالها. الأمر الذي يضفي صفة الازدواجية لمحل التفتيش في جرائم الوسط الرقمي، ولو أن هذه الازدواجية نفسها، تقوم على أساس معيار الطبيعة، القائم على تفتيش عناصر الوسط الرقمي، الذي يأخذ الطابع المادي التقليدي، وتفتيش نطاقها الافتراضي الذي يتصف بالحديث المرقمن.

تطرقت العديد من الدراسات إلى تفتيش ماديات الوسط الرقمي –عناصره–، على أنها تدخل ضمن إطار التفتيش المرقمن الحديث. الأمر الذي لا نجده كذلك، نظرا لتعامل أجهزة التحري والتحقيق مع هذه العناصر على أنها أشياء مادية، وتفتيشها ماديا من دون التعامل مع نطاقها الافتراضي الذي تحويه. وهو ما يدفع للقول بتطبيق الأحكام التقليدية للتفتيش، ومنه خروج ذلك عن إطار الدراسة. وعلى العموم ينطوي محل التفتيش المتصل بعناصر الوسط الرقمي؛ على جهاز الإعلام الآلي –ومن في حكمه–، والماديات التي توفر من خلالها شبكة الاتصال الدولية –ومن في حكمها– كـ "المودم" مثلا. وكل العناصر الرقمية الأخرى المتصلة بالاثنين، على غرار الماسح الضوئي والطابعة وغيرهما. بالإضافة إلى مكان تواجد كل ذلك كالمسكن والمحل...الخ[2].

---

[1] مع الإشارة إلى عدم التطرق للمعوقات الفنية والعملية التي تعترض التفتيش المرقمن، وذلك نظرا لكونها لا تخرج كثيرا عن تلك المذكورة في إطار المعاينة المرقمنة، سيما وأنهما يتقاربان -المعاينة والتفتيش- في العديد من النقاط الأساسية.

[2] يعد محل التفتيش المذكور أعلاه؛ خارجا عن إطار الدراسة، لكونه لا ينصب على النطاق الافتراضي للوسط الرقمي من جهة، ولكونه لا يبحث عن الدليل الرقمي من جهة أخرى، وكل دليل يستنتج منه يكون بمثابة الدليل التقليدي المعروف. الأمر الذي نظمه المشرع الجزائري؛ بالأحكام التقليدية الواردة بقانون الإجراءات الجزائية، سيما في إطار مرحلة البحث والتحري أو إجراءات التحقيق القضائي، المحددة بالمواد من 44 إلى 48 و64 ومن 79 إلى 85 -سابقة الذكر-. ولو أنه يمكن إثبات جرائم الوسط الرقمي بالدليل المادي المستنتج من التفتيش التقليدي المتصل بعناصر الوسط الرقمي ومحيطها المادي المتواجدة من خلاله.

وأما بخصوص تفتيش النطاق الافتراضي للوسط الرقمي؛ فالأمر عرف اختلافا فقهيا كبيرا، خاصةً في ضل غياب النص التشريعي الفاصل في البداية، واختلاف النظرة التشريعية بعد ذلك؛ الدائرة بين تطلب النص الحديث وتقبل تطبيق النص التقليدي. فبخصوص مدى قابلية النطاق الافتراضي للتفتيش أصلا، يرى جانب من الفقه الجنائي؛ أنه جائز انطلاقا من تفسير نص التفتيش التقليدي على أنه يشمل "كل شيء" مادي وغير مادي. الأمر الذي قابلة رأي فقهي آخر بالرفض المطلق، لكون عدم تطابق المفهوم المادي مع المعطيات الرقمية، غير المرئية ولا الملموسة. ومنه يتوجب لاعتبار النطاق الافتراضي بمثابة محل التفتيش؛ تدخل المشرع لينص على ذلك صراحةً[1].

كما برز رأي فقهي ثالث، يستبعد فكرة البحث في مدلول كلمة الشيء من حيث احتوائها لمضمون النطاق الافتراضي من عدمه. وإنما العبرة بالحاجة العملية، التي تقود إلى ضبط الماديات المتضمنة للنطاق الافتراضي، ومنه التفتيش يكون من خلالها وفي إطارها. وهو ما كان أساس ظهور رأي فقهي رابع، ببعد علمي محض. حيث يرى أصحابه؛ بضرورة تجنب الخلط بين الحق الذهني للشخص على البرامج والكيانات المنطقية وبين طبيعة هذه الأخيرة. وإنما يتوجب البحث على مدلول مصطلح "المادة" في العلوم الطبيعية، التي تعرف –المادة– على أنها: "كل ما يشغل حيزاً مادياً في فراغ معين يمكن قياسه والتحكم فيه". الأمر الذي يعطي للمعطيات التي تكون على شكل نبضات رقمية ثنائية، وتشغل حيزاً مادياً في ذاكرة الجهاز يمكن قياسه؛ وصف المادة قياسا بالتيار الكهربائي الذي يعتبر بمثابة القوة المحرزة[2].

في خضم كل الاختلافات الفقهية المبينة أعلاه؛ الدائرة عموما بين الرفض والقبول لاعتبار النطاق الافتراضي محلا للتفتيش. ظهر إشكال آخر ينطوي على محل التفتيش المنجز عن بعد، امتدادا للتفتيش في النطاق الافتراضي الصادر إذن التفتيش بخصوصه. وهو المنطوي على النطاق الافتراضي البعيد عن مكان تواجد أجهزة التحري والتحقيق. الأمر الذي نظر إليه الفقه الجنائي من منظورين، فإما المحل الافتراضي المتواجد داخل إقليم الدولة أو المتواجد خارجه.

فبخصوص المحل الافتراضي المتواجد داخل الدولة نفسها؛ يرى جانب من الفقه بجواز امتداد التفتيش ليصل إليه، انطلاقا من محل التفتيش الافتراضي الأصلي. وذلك استنادا إلى طبيعة الأدلة الرقمية المبحوث عنها، التي قد تتواجد في نطاق افتراضي آخر بعيد ومتصل بالنطاق الأصلي الذي تم الحصول على إذن بشأنه. كما يذهب رأي فقهي ثانٍ –وهو مصري–؛ إلى القول بعدم جواز ذلك، قياسا برفض محكمة النقض المصرية لانتقال مأمور الضبط للتفتيش من منزل مقابل للمنزل المأذون بتفتيشه، بعد إلقاء صاحب المنزل الأصلي للفافة في المنزل المجاور. وأما بخصوص المحل الافتراضي المتواجد خارج

[1] **أنظر:** شريف أحمد الطباخ، البحث الجنائي والأدلة الجنائية في ضوء القضاء والفقه، دار الفكر الجامعي، الإسكندرية، مصر، 2017، ص 726.

[2] **أنظر:** المرجع نفسه، ص 726 و727.

الدولة؛ فلم تثر إشكالات فقهية كبيرة، نظرا لكون المسألة تخضع للأحكام العامة –في حالة غياب النص الخاص–، المنطوية على الاتفاقيات القضائية الدولية الجماعية والثنائية[1].

وعلى العموم ورغم كل الاختلافات الفقهية المذكورة، بشأن جواز تفتيش النطاق الافتراضي بالأساس، وإمكانية امتداده ليصل إلى نطاق افتراضي آخر سواءً داخل الدولة نفسها أو خراجها بالتبعية، فان المشرع الجزائري وقبله المقارن –وحتى الاتفاق الدولي–[2]؛ قد أقر بإمكانية ذلك بالنص الاتفاقي والوضعي معا. حيث تبنت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات –التي صدقت عليها الجزائر كما بينا سابقا–، التفتيش المرقمن الذي ينصب على النطاق الافتراضي عوما، كما ألزمت كل دولة عضو بضرورة التعامل مع التفتيش عن بعد، ما يجعل المحل الافتراضي البعيد قابلا للتفتيش الجنائي[3].

وكذلك التشريع الوضعي الجزائري، نجده قد أقر صراحةً بإمكانية اعتبار المنظومة المعلوماتية؛ كمحل مشروع للتفتيش المرقمن، وذلك بموجب القانون رقم 09-04 الصادر سنة 2009. كما أقر بالقانون نفسه؛ إمكانية تمديد التفتيش إلى المحل الافتراضي المتواجد داخل الإقليم الوطني وفق الأحكام القانونية اللازمة، والآخر المتواجد خارجه وفق الاتفاقيات الدولية سارية المفعول[4]. إلا أنه لم يتطرق إلى التفتيش في النطاق الافتراضي المتصل بالشبكة، الأمر الذي نتعامل معه وفق الطرح نفسه المبين سابقا، بخصوص مدلول المنظومة المعلوماتية، الذي يشمل أيضا النطاق الافتراضي المتصل بالشبكة.

2. القواعد الإجرائية للتفتيش في جرائم الوسط الرقمي: يقوم التفتيش عموما والتفتيش المرقمن خاصةً؛ على العديد من الأحكام والشروط القانونية الواجب إتباعها. التي قد يترتب عن تخلفها البطلان الإجرائي[5]، ما يخرج الدليل المترتب عنها؛ من دائرة المشروعية المطلوبة لاعتماده القضائي. وعلى العموم تتلخص أهم هذه القواعد الإجرائية؛ في إذن التفتيش ومواقيت ممارسته وأعمال تنفيذه[6].

---

[1] **أنظر:** مصطفى علي خلف، مرجع سابق، ص 86 و87 و97.

[2] تتجه أغلب التشريعات المقارنة والاتفاقيات الدولية ذات الصلة بمكافحة جرائم الوسط الرقمي؛ إلى القول بمشروعية التفتيش في المحل الافتراضي، ولقبول تمديده الوطني والخارجي وفق أحكام مبينة مسبقا. الأمر الذي أقرته اتفاقية بودابست لسنة 2001 حول جرائم الوسط الرقمي المبينة سابقا، والتشريع الفرنسي الوارد بقانون الإجراءات الجزائية. **أنظر في ذلك:** مصطفى علي خلف، المرجع نفسه، ص 76 و79 و93 و95. **وأنظر أيضا:** شريف أحمد الطباخ، مرجع سابق، ص 728 و729.

[3] **أنظر:** المادتان 26 و39؛ مرسوم رئاسي رقم 14-252، مرجع سابق.

[4] **أنظر:** المادة 05؛ قانون رقم 09-04، مرجع سابق.

[5] حيث ترتب المادة 48 "ق.إ.ج"؛ البطلان الإجرائي للتفتيش المنجز بالمخالفة لأحكام المواد من 45 إلى 47 من القانون نفسه، وهي المتصلة بكل القواعد الإجرائية التالية بالدراسة في هذا المقام، دون المتعلقة بالإذن منها، الذي ترتب المادة 3/44 من القانون نفسه؛ البطلان الإجرائي على عدم تضمنه الشكليات اللازمة، من دون الامتداد إلى وجوب استظهاره واختصاص الجهة المصدرة والمنفذة له. **أنظر في ذلك:** المادتان 3/44 و48؛ أمر رقم 66-155، مرجع سابق.

[6] مع التأكيد على خضوع التفتيش المرقمن للإجراءات التقليدية المعروفة، إلا ما جاء مخالفا لها في إطار القانون 09-04، الذي يحيل بدوره إلى الإجراءات العامة التقليدية. **أنظر في ذلك:** المادة 1/05؛ قانون رقم 09-04، المرجع نفسه.

أ- **إذن التفتيش المرقمن:** يخضع إذن التفتيش المرقمن إلى العديد من الأحكام، الواردة بقانون الإجراءات الجزائية عموما، والقانون 09-04 سابق الذكر خاصةً. حيث قد يصدر الإذن عن وكيل الجمهورية المختص، في حالة ممارسة التفتيش في مرحلة البحث والتحري -سواءً في الحالة العادية أو في حالة التلبس-. أو يصدر عن قاضي التحقيق المختص، بعد تحريك الدعوى العمومية، وبمناسبة ممارسته لإجراءات التحقيق القضائي الابتدائي. على أنه قد لا تتطلب العملية استصدار أي إذن بالتفتيش، إذا ما مارس وكيل الجمهورية أو قاضي التحقيق -على حسب الحالة- التفتيش المرقمن بنفسه[1].

كمنا أنه جاء في المواد نفسها أن الإذن بالتفتيش لا يصدر إلا مكتوبا، ويسلم إلى ضابط الشرطة القضائية الذي يحدده وكيل الجمهورية أو قاضي التحقيق في الإذن نفسه، الذي يمكنه أن يستعين بأعوان الشرطة القضائية لتنفيذ الإذن فيما بعد. مع التحديد الدقيق للجريمة محل التحري أو التحقيق، التي لا تخرج في هذا الإطار عن؛ جرائم المساس بأنظمة المعالجة الآلية للمعطيات من جهة، وأي جريمة تقليدية ترتكب أو يسهل ارتكابها عبر النطاق الافتراضي للوسط الرقمي من جهة أخرى.

إلا أن المادة 05 من القانون 09-04، قد أكدت على أن التفتيش المرقمن؛ ينجز انطلاقا من الأحكام العامة وأيضا في إطار أربع حالات محددة حصرا[2]. الأمر الذي يتطلب التدوين في الإذن إلى جانب الجريمة محل المتابعة؛ حالة أو أكثر من الحالات التي تطلبها المشرع. وعلى العموم تتمثل هذه الحالات الأربعة في القيام بالتفتيش المرقمن؛ للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة. ولتفادي اعتداء محتمل على منظومة معلوماتية ما يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني[3]. بالإضافة إلى تطلب مقتضيات التحريات والتحقيقات القضائية ذلك، نظرا لصعوبة الوصول إلى النتيجة المرجوة. كما قد يتم إصدار إذن بالتفتيش الرقمي؛ في حالة العمل على تنفيذ طلبات المساعدة القضائية الدولية المتبادلة[4].

كما يتوجب حسب المادة 05 نفسها أن يتضمن الإذن؛ التحديد الدقيق لمحل التفتيش المرقمن، المنطوي على المنظومة المعلوماتية -أو جزء منها- والمعطيات المعلوماتية المخزنة فيها أولا، ومنظومة التخزين المعلوماتية من ثانيا، مع إهمال المشرع كالعادة للنطاق الافتراضي الشبكي، وملاحظة أنه ركز على المعطيات المخزنة دون تلك المتعلقة بتشغيل المنظومة نفسها وأيضا معطيات السير. إلا أن الأمر

---

[1] **أنظر:** المواد 1/44 و1/64 و81؛ أمر رقم 66-155، مرجع سابق.

[2] **أنظر:** المادتان 04 و05؛ قانون رقم 09-04، مرجع سابق.

[3] تتصف كل من الحالة الأولى والثانية؛ بالطابع الوقائي. الذي سبق وأن قلنا أنه من أهم الخصائص الحديثة التي اكتسبتها الإجراءات الجزائية في إطار جرائم الوسط الرقمي. حيث نادرا ما يكون لها الدور الوقائي، نظرا لكونها تبدأ ممارسة مهامها القانونية بعد ارتكاب الجريمة وليس قبلها. وعلى العموم وضع المشرع ذلك لتوخي الأضرار الكبيرة التي قد تلحق جراء جرائم خطيرة، تتعلق بالإرهاب وأمن الدولة والنظام العام والاقتصاد الوطني ومؤسسات الدولة والدفاع الوطني.

[4] تعد كل من الحالة الثالثة والرابعة؛ بمثابة ممارسة الدور الحقيقي لقانون الإجراءات الجزائية، الذي يقرر التفتيش وباقي الأعمال الإجرائية؛ بعد ارتكاب الجريمة، في إطار ممارسة التحري والتحقيق فيها، أو لتنفيذ التعاون الدولي في الإطار نفسه.

لا يطرح أي إشكال، نظرا للقول سابقا بدخول النطاق الافتراضي الشبكي وكل المعطيات الأخرى؛ ضمن المفهوم الواسع للمنظومة المعلوماتية، ولقول المشرع في المادة نفسها بإمكانية انجاز التفتيش عن بعد.

ب- مواقيت التفتيش المرقمن: لم يتطرق المشرع بالقانون 09-04 المستحدث للتفتيش المرقمن؛ إلى مواقيته القانونية. وإنما ترك ذلك إلى الأحكام الإجرائية العامة. وبالرجوع إلى "ق.إ.ج"؛ نجد أنه نظم مواقيت التفتيش وفق أصل واستثناء. الأمر الذي سنحاول إسقاطه على جرائم الوسط الرقمي بأنواعها المحددة سابقا، مع مراعاة الفرق -إن وجد- بين مرحلة التحري وإجراءات التحقيق.

ب-1/ مواقيت التفتيش في جرائم المساس بأنظمة المعالجة الآلية للمعطيات: لم يفرق المشرع الجزائري بخصوص مواقيت التفتيش في كل من مرحلة التحري وإجراءات التحقيق القضائي، المتصلة بجرائم المساس بأنظمة المعالجة الآلية للمعطيات. حيث اعتبرها من جرائم المعاملة الخاصة التي تفتح في إطارها المواقيت، لتصبح بلا حدود زمنية معينة. الأمر الذي جاءت به المادة 3/47 المتصلة بالتفتيش في حالة التلبس ضمن إطار مرحلة التحري، وعممه المشرع عبر الإحالة إليها؛ على كل من التفتيش المنجز في الحالات العادية ضمن مرحلة التحري، والتفتيش الممارس بخصوص التحقيق القضائي أيضا[1].

يفهم مما ورد في المواد المبينة أعلاه؛ أن المشرع قد فتح مواقيت التفتيش ولم يحددها بساعات معينة. لكن السؤال المطروح؛ هل يتصل ذلك بتفتيش النطاق الافتراضي للوسط الرقمي، أم محيطه المادي من مسكن أو مكان أم الاثنين معا. فلو قلنا أن ذلك يقتصر على النطاق الافتراضي، لوصلنا إلى أن الدخول إلى مكان تواجد الأجهزة الرقمية بعد الساعة الثامنة ليلا؛ يقود إلى تفتيش نطاقها الافتراضي دون محيطها المادي. إلا أننا نرى بأنها تخص تفتيش النطاق الافتراضي ومكان تواجد الأجهزة الرقمية التي تحويه.

ب-2/ مواقيت التفتيش في الجرائم التقليدية المتصلة بالوسط الرقمي: على العكس من جرائم المساس بالأنظمة، تقوم المواقيت المتصلة بالتفتيش في الجرائم التقليدية المرتكبة عبر النطاق الافتراضي للوسط الرقمي أو بتسهيل منه؛ على مواقيت أصلية وأخرى استثنائية. حيث الأصل العام أن يمارس التفتيش سواءً المتصل بمرحلة التحري أو بإجراءات التحقيق؛ وفق مواعيد محددة حصرا تدور بين الخامسة 05 صباحاً والثامنة 08 مساءً[2]. ولا يجوز ممارسة التفتيش قبل هذه المواقيت ولا بعدها، مع القول بإمكانية محاصرة مكان تواجد الأجهزة الرقمية إلى غاية حلول المواعيد القانونية. وعلى العموم العبرة تكون بوقت البدء في التفتيش، فإذا ما بدأ على السابعة 07 مساءً يمتد إلى أن ينتهي حتى وان تجاوز المواقيت القانونية[3].

---

[1] **أنظر:** المواد 3/47 و3/64 و82؛ أمر رقم 66-155، مرجع سابق.

[2] **أنظر:** المواد 1/47 و3/64 و82؛ المرجع نفسه.

[3] مع التأكيد على أن محاصرة محل التفتيش إلى غاية حلول المواقيت القانونية؛ هو إجراء متصل بالتفتيش التقليدي الذي استنتجه الفقه من المادة 1/47 المذكورة أعلاه، ولغرض الحلول دون هرب المشتبه فيه أو المتهم أو لتهريب الدليل المادي الذي بحوزتهم. **أنظر في ذلك:** ناصر حمودي، (قانون الإجراءات الجزائية الجزائري)، مرجع سابق، ص 111.

تعد فكرة المحاصرة إلى غاية حلول المواقيت القانونية؛ بمثابة الإجراء الناجع بخصوص مكافحة الجريمة التقليدية، التي تثبت بالدليل المادي الملموس. لكن نرى عكس ذلك بخصوص مكافحة الجريمة التقليدية المتصلة بالوسط الرقمي، التي تثبت بالدليل الرقمي الافتراضي. حيث إجراء المحاصرة يعد بمثابة الإعلان الصريح لمن يتواجد داخل المكان المحاصر؛ بأن له فرصة أخيرة ليعبث بالدليل الرقمي المتصل بالنطاق الافتراضي الذي هو بحوزته. وقد يكون ذلك بمثابة اعذار للمتهم أو المشتبه فيه، المتواجد داخل المكان المحاصر أو خارجه، الذي يمكنه الاتصال بأي شخص مختص في الوسط الرقمي ليقوم بإتلاف الدليل عن بعد...الخ. الأمر الذي يقود للقول بضرورة فتح مواعيد التفتيش في كل جرائم الوسط الرقمي، وعدم الاكتفاء بجرائم المساس فقط.

وعلى العموم اعتمد المشرع بعض الاستثناءات عن الأصل، التي تفتح مواقيت التفتيش في الجريمة التقليدية المتصلة بالوسط الرقمي، سواءً بخصوص مرحلة التحري أو إجراءات التحقيق. حيث تتصل هذه الاستثناءات بما تسمى بجرائم المعاملة الخاصة، المنطوية على جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف. التي سبق لنا تبيان خصوصيتها المتصلة بالأجهزة المختصة بمكافحتها في إطار الأقطاب المتخصصة[1].

كما فتح المشرع بالنص العام مواقيت التفتيش، في حال طلب صاحب المنزل أو وجهت نداءات من الداخل، وبخصوص أيضا تفتيش الفنادق والمساكن المفروشة والمحلات للجمهور[2]. الأمر الذي بإسقاطه على الجرائم التقليدية المتصلة بالوسط الرقمي، التي يتم البحث عن دليلها الرقمي لمكافحتها؛ تبرز العديد من التساؤلات. على غرار طلب صاحب المنزل –وكذلك بخصوص توجيه نداءات من الداخل–، الذي يؤدي إلى الدخول لتفتيش المنزل برخصة من صاحبه، ولا يمتد إلى النطاق الافتراضي للجهاز المتواجد بالمنزل، الذي قد لا يكون تابعا لصاحب المنزل، ومنه توجب صدور طلب آخر منفصل من صاحب المنظومة، الذي يمكنه التمسك بمواقيت التفتيش. وأيضا تفتيش الفنادق ونظيراتها؛ لا يقود للقول بالتفتيش المرقمن للأجهزة التابعة لمن يتواجدون بالمكان إلا برضاهم، كما يمكنهم التمسك بالمواقيت.

كما فتح المشرع مواقيت التفتيش في كل الجنايات –دون الجنح– المتصلة بالوسط الرقمي، الذي يمارس في إطار إجراءات التحقيق –دون مرحلة التحري–، على أن ينجز هذا التفتيش في النطاق الافتراضي المتصل بالأجهزة الرقمية المتواجدة داخل منزل المتهم، ومن طرف قاضي التحقيق شخصيا، وبعد إخطار وكيل الجمهورية المختص الذي يتوجب أن يحضر شخصيا عملية التفتيش[3]. الأمر الذي يعد

[1] الأمر الذي له المعاملة نفسها المتصلة بجرائم المساس بأنظمة المعالجة الآلية للمعطيات، سيما وأن هذه الأخيرة هي أيضا من بين جرائم المعاملة الخاصة. **أنظر في ذلك:** المواد 3/47 و3/64 و82؛ أمر رقم 66-155، مرجع سابق.

[2] **أنظر:** المادة 1/47 و2 والمادة 2/64 والمادة 82؛ المرجع نفسه.

[3] **أنظر:** المادة 82؛ أمر رقم 66-155، المرجع نفسه.

قاصرا بالنظر إلى خصوصية الوسط الرقمي، وإمكانية العبث بالدليل المتصل بالجنح أو بالجنايات والجنح خلال مرحلة التحري، ما يدفع للقول بضرورة فتح مواقيت التفتيش في الجريمة التقليدية المرقمنة.

ج- تنفيذ التفتيش المرقمن: ينفذ إذن التفتيش المرقمن بالطريقة نفسها التي ينفذ بها إذن التفتيش المادي، إلا ما تتطلبه الطبيعة الرقمية، التي منها ما نص عليها المشرع صراحةً، ومنها ما يبقى من دون نص. حيث يتوجب على ضابط الشرطة المختص، أن يستظهر إذن التفتيش للشخص المعني قبل البدء في العملية، مع التأكيد على عدم تطلب ذلك في حالة ممارسة التفتيش؛ من وكيل الجمهورية أو قاضي التحقيق شخصيا. وعلى العموم تنفيذ التفتيش المرقمن يختلف باختلاف أنواع جرائم الوسط الرقمي.

ج-1/ تنفيذ التفتيش في جرائم المساس بأنظمة المعالجة الآلية للمعطيات: انطلاقا من اعتبار المشرع لجرائم المساس بأنظمة المعالجة الآلية للمعطيات، على أنها من جرائم المعاملة الخاصة؛ يمكن القول أن منفذ التفتيش المرقمن لا يحتاج لرضا الشخص المعني، ولا ينتظر حضوره أو حضور من ينوبه في عملية التفتيش، بل يباشر ذلك بمجرد تسلمه للإذن[1]. إلا أنه يجد نفسه ملزما ببعض القواعد القانونية والتقنية، المنطوية على كتمان السر المهني والحجز وطلب الدعم التقني[2]. حيث يلتزم بالحفاظ على السر المهني وجرد الأشياء -مادية وغير مادية-، مع حجز الأجهزة الرقمية ونطاقها الافتراضي. كما يعد ملزما بالاستعانة بمن لهم المعرفة الرقمية اللازمة، لغرض الوصول إلى الدليل الرقمي وعدم إتلافه[3].

وعلى العموم يكون التفتيش المرقمن في المحل الافتراضي، الذي عبر عنه المشرع بالمنظومة المعلوماتية -أو جزء منها- والمعطيات المخونة من خلالها، وكذا منظومة التخزين المعلوماتي. إلا أن ممارس هذا التفتيش المرقمن قد تواجهه بعض الأمور، على غرار اكتشافه أن المعطيات التي تتضمن الدليل الرقمي؛ هي متواجدة في منظومة معلوماتية أخرى يمكن الولوج إليها انطلاقا من المنظومة محل التفتيش. الأمر الذي عالجه المشرع، من خلال القول بجواز تمديد التفتيش بسرعة إلى المنظومة الثانية، بعد إعلام وكيل الجمهورية أو قاضي التحقيق على حسب الحالة[4].

---

[1] الشخص المعني، الذي قد يكون مشتبها فيه أو مشتبها في حيازته لمعطيات تتعلق بالجريمة، أو متهما أو غير متهما؛ في حالة تنفيذ التفتيش المرقمن عن بعد. أو أحد المذكورين مع إضافة صاحب المنزل في حالة حدوث التفتيش المباشر، مع التباين بين صاحب الأجهزة الرقمية وصاحب المنزل المتواجدة من خلاله. الأمر الذي نستنتجه من خلال الأحكام التقليدية، التي تنص على أن التفتيش التقليدي يكون في منزل المشتبه فيه أو منزل المشتبه في حيازته لأوراق أو أشياء تتعلق بالجريمة، أو منزل المتهم أو غير المتهم. **أنظر في ذلك:** المواد 1/45 و2/64 و82 و2/83؛ أمر رقم 66-155، مرجع سابق.

[2] **أنظر:** المواد 6/45 و2/64 و82 و2/83؛ المرجع نفسه. **وأنظر أيضا:** المادة 4/05 والمواد من 06 إلى 08؛ قانون رقم 09-04، مرجع سابق.

[3] وعلى العموم؛ عبرنا على الحجز المرقمن والدعم التقني؛ بأبعاد المعاينة والتفتيش في جرائم الوسط الرقمي. وهو ما سنبينه بنوع من التفصيل في المطلب الموالي من الدراسة.

[4] إلا أن المشرع أكد على أن إمكانية التمديد؛ تكون انطلاقا من المنظومة المعلوماتية دون منظومة التخزين المعلوماتي. وهو ما يعد مفهوما تقنيا، لكون المنظومة المعلوماتية دون منظومة التخزين؛ تتيح عملية التواصل عن بعد، نظرا لكون الشبكة أحد مكوناتها. **أنظر في ذلك:** المادة 2/05؛ قانون رقم 09-04، المرجع نفسه.

وإذا تبين أن المنظومة المعلوماتية الثانية المراد التمديد إليها، متصلة بأجهزة رقمية متواجدة خارج الإقليم الوطني؛ يتوجب على القائم بعملية التفتيش المرقمن، الامتناع عن الولوج إليها، مع تبليغ القاضي المختص –وكيل الجمهورية أو قاضي التحقيق–، الذي يقوم بإتباع إجراءات المساعدة القضائية الدولية طبقا للاتفاقيات الدولية ذات الصلة، وعملا –أيضا– بمبدأ المعاملة بالمثل[1].

ج–2/ تنفيذ التفتيش في الجرائم التقليدية المتصلة بالوسط الرقمي: يأخذ تنفيذ إذن التفتيش المرقمن بخصوص الجرائم التقليدية المتصلة بالوسط الرقمي حكمين مختلفين. حيث ينجز وفق القواعد الإجرائية نفسها المبينة أعلاه بخصوص جرائم المساس؛ إذا ما تعلق الأمر بأي جريمة من جرائم المعاملة الخاصة، التي ترتكب عبر النطاق الافتراضي أو يكون المسهل لارتكابها –الجرائم المذكورة سابقا–. فلا يكون ممارس التفتيش المرقمن؛ ملزما بحضور المعني لإجراءات التفتيش، الذي –التفتيش– ينجزه في المحل الافتراضي المقصود، مع إمكانية التمديد الداخلي والخارجي وفق الشروط نفسها المبينة سابقا. مع التزامه بالسر المهني والجرد والحجز، والاستعانة بالمتخصصين في الوسط الرقمي.

إلا أن الأمر يختلف نوعا ما إذا ما تعلق التفتيش بباقي الجرائم التقليدية المتصلة بالوسط الرقمي؛ حيث يلتزم ممارس التفتيش بالقواعد المبينة أعلاه؛ بالإضافة إلى التزامات أخرى، المنطوية أساسا على ضرورة حضور الشخص المعني أو من ينوبه لعملية التفتيش[2]. حيث يتوجب في إطار مرحلة التحري، لتفتيش النطاق الافتراضي المتصل بالمشتبه فيه، أو تلك المتصلة بمن يشتبه في حيازته لمعطيات تتعلق بالجريمة، حال تفتيش منظومة المشتبه فيه؛ حضور صاحب هذا النطاق الافتراضي شخصيا، أو يعين من ينوبه في حال تعذر ذلك، وإذا كان غائبا يستدعي ضابط الشرطة القضائية؛ شاهدين من غير الموظفين الخاضعين لسلطته. ولو تواجد الجهاز الرقمي الحامل للنطاق الافتراضي محل التفتيش، في منزل شخص آخر غير صاحب هذا النطاق؛ يتوجب حضور صاحب المنزل أو من ينوبه وفق الإجراءات نفسها[3].

وكذلك يتبع ممارس التفتيش المرقمن في إطار إجراءات التحقيق القضائي؛ القواعد نفسها بخصوص تفتيش النطاق الافتراضي المتصل بالمتهم والمحيط المادي المتواجد من خلاله. مع التأكيد على ضرورة حضور غير المتهم إذا كان نطاقه الافتراضي محلاً لتفتيش، وإذا رفض أو كان غائبا يجرى ذلك بحضور اثنين من أقاربه أو أصهاره الحاضرين بمكان تواجد الأجهزة الرقمية، وإذا لم يوجد أي أحد منهم فيكون ذلك بحضور شاهدين لا علاقة لهم بالسلطة القضائية والشبه قضائية[4].

---

[1] **أنظر:** المادة 3/05؛ قانون رقم 09-04، مرجع سابق.

[2] الأمر الذي استنتجناه من خلال إسقاط الأحكام التقليدية ذات الصلة بالطبيعة الرقمية للمحل الافتراضي. خاصةً وأن المشرع في إطار المادة 1/05 من القانون 09-04؛ يحيل إلى الأحكام التقليدية المتعلقة بالتفتيش، ما يتوجب تكييفها عمليا ليمكن تطبيقها على النطاق الافتراضي.

[3] **أنظر:** المادة 1/45-1 و2 والمادة 2/64؛ أمر رقم 66-155، مرجع سابق.

[4] **أنظر:** المادتان 82 و83؛ المرجع نفسه.

3. القواعد الفنية للتفتيش في جرائم الوسط الرقمي: بالإضافة إلى القواعد الإجرائية واجبة الإتباع في التفتيش المرقمن لضمان المشروعية اللازمة، يفرض الواقع الرقمي المعقد المتصل بالمسرح الجرمي الافتراضي؛ الاعتماد على العديد من القواعد الفنية القائمة على الطبيعة الرقمية نفسها، التي بتخلفها يصعب –أو يستحيل أحيانا– الوصول إلى النتيجة المرجوة من التفتيش المرقمن. وعلى العموم يمكن أن نقسم هذه القواعد؛ إلى الوسائل الأساسية والأعمال المكملة.

أ– الوسائل الأساسية المستعملة في التفتيش المرقمن: يعتمد فريق التفتيش المرقمن –الضابط والأعوان والمختصين في الوسط الرقمي– لانجاز مهمتهم؛ على العديد من الوسائل الرقمية، التي تختلف وتتعدد على حسب كل قضية، كما أنها لا تعد ثابتة بل تتغير وتتطور؛ بحسب التطور السريع والديناميكي للوسط الرقمي. وعلى العموم يمكن أن نتطرق إلى هذه الوسائل عبر تقسيمها إلى عامة وخاصة.

أ–1/ الوسائل الأساسية العامة: تنطوي الوسائل الأساسية العامة؛ على تلك البرامج والأدوات التي يمكن من خلالها الولوج إلى النطاق الافتراضي المراد تفتيشه من جهة، والوصول إلى معطيات الجهاز بصفة عامة –من دون تحديد– من جهة أخرى. الأمر الذي يمكن تحديده في ثلاثة وسائل أساسية، تتصل الأولى بـــ "النسخ الأصلي العام–Exact copy"، الذي يؤدي إلى نسخ كل المعطيات المخزنة في الجهاز قبل تشغيله، وذلك لتفادي أي ضياع للدليل تتسبب فيع عملية التشغيل. وتتمثل الثانية؛ في الانتقال إلى مرحلة تشغيل الجهاز، الذي قد يكون محميا كليا أو عبر كلمة سر معينة، فيقوم المختص بتشغيله عبر برامج معدة خصيصا لذلك، أو بتجاوز كلمة السر بالبرنامج المناسب أيضا[1].

وبالإضافة إلى ذلك قد يتبع فريق التفتيش المرقمن؛ وسائل فنية أخرى، كالبرامج التي تمنع الكتابة الرقمية المتصلة بالقرص الصلب. وبرامج نسخ و"استرجاع المعطيات–Retrieval of files"، التي يعمد في الكثير من الأحيان الجاني لحذفها بعد ارتكابه الجريمة بغرض إتلاف الدليل الرقمي. كما قد يذهب فريق التفتيش إلى أبعد من ذلك، فيقوم بالتعامل المباشر مع البيانات الأصلية الظاهرة على شكلها الثنائي "0 و01"، عبر استعمال "برمجيات الملفات الست عشرية–Hexadecimal editors"[2].

أ–2/ الوسائل الأساسية الخاصة: يمكن لفريق التفتيش المرقمن؛ أن يعتمد أيضا على العديد من الوسائل الخاصة المتصلة بجزء معين من النطاق الافتراضي. ومنه قد ينصب التفتيش المرقمن على "العناوين الشبكية–Internet protocol address" المتعلقة بالمواقع والبريد الرقمي. كما قد يستعمل ما يسما بـــ "البروكسي–Proxy" للوصول إلى المعطيات الشبكية المتوفرة عبر "الذاكرة الجاهزة–Cache memory"[3].

---

[1] **أنظر:** أسامة بن غانم العبيدي، مرجع سابق، ص 114 و119 و120.

[2] **أنظر:** المرجع نفسه، ص 119 و120.

[3] **أنظر:** شريف أحمد الطباخ، مرجع سابق، ص 730 و731.

ويمكن الاعتماد على أدوات "تدقيق ومراجعة العمليات الحاسوبية–Auditing tools"، التي تقوم بمراقبة العمليات المختلفة المنجزة على ملفات ونظام تشغيل جهاز إعلام آلي محدد بالذات، ومن ثم تسجيلها في ملفات خاصة ومنفصلة يطلق عليها اسم "Logs"، ولعل أبرز هذه الأدوات نجد؛ ما تسمى بـــ"أداة بيئة النوافذ–Event viewer"، و"أداة بيئة يونيكس–Syslogd". كما قد يعتمد فريق التفتيش المرقمن؛ على "نظام كشف الاختراق–Intrusion detection system"، الذي يراقب بعض العمليات المنجزة على الأجهزة والشبكة، مع تحليلها بحثاً عن أية إشارة قد تدل على وجود مشكلة، التي قد تأخذ الوصف الجزائي[1].

ب– الأعمال المكملة المستعملة في التفتيش المرقمن: لايمكن للوسائل الفنية المبينة أعلاه –التي لها الطابع الأساسي–، أن تحدث الأثر الفني المراد منها –ومنه الأثر القانوني–؛ إلا إذا ما صاحبتها العديد من الأعمال المكملة، التي يتوجب على ممارس التفتيش المرقمن التقيد بها، وإلا تعذر عليه الوصول إلى الدليل الرقمي الجنائي، الذي قد يكون هو –القائم بالتفتيش– سبب إتلافه لعدم إتباع الإجراءات اللازمة ضمن إطار الأعمال المكملة.

بعد توفر الشروط القانونية السابقة بالذكر، المفرغة في إذن التفتيش المرقمن، المستوفي للشكليات والمضمون القانونيين اللازمين، يتوجب على ممارس التفتيش المرقمن؛ أن يقوم بالتعرف قدر الإمكان على النطاق الافتراضي المراد تفتيشه، قصد إعداد الخطة اللازمة. على أن يقوم الفريق بعد ذلك؛ بالتنقل المادي إلى مكان تواجد الأجهزة الرقمية المقصودة –ومن دون تنقل في حالة التفتيش عن بعد–. الأمر الذي تتلوه عملية الحفاظ على المحيط المادي لمسرح الجريمة الافتراضي، بغرض رفع البصمات والإشارات المتاحة. كما يراعى الحذر الشديد لدى ممارسة النقل المادي للأجهزة الرقمية من مكان لآخر، مع التأكيد على ضرورة أخذ الصور الفوتوغرافية للمكان[2].

كما يقوم فريق التفتيش المرقمن بالإضافة إلى كل الإجراءات المادية المبينة أعلاه[3]؛ بقطع التيار الكهربائي الموصول بالأجهزة الرقمية، لتجنب أي ولوج غير مباشر –عن بعد–. على ألا يتم إشعال ولا إطفاء أي جهاز رقمي؛ إلا بمعية المختص في الوسط الرقمي –الذي هو عضو في فريق التفتيش–، وذلك لتفادي إتلاف الدليل الرقمي. كما يتوجب ضبط الأجهزة وإزالة ملحقاتها ومراجعة المحتويات خارج الموقع، مع توثيق جميع هذه النشاطات بدقة في محاضر التفتيش[4].

---

[1] وغيرها الكثير من البرامج الأساسية الخاصة، التي تتغير وتتطور على حسب تطور الوسط الرقمي نفسه. مثل برامج التتبع و"نظام جرة العسل-Honey pot"، والاستعانة بالذكاء الاصطناعي...الخ. **أنظر في ذلك:** شريف أحمد الطباخ، مرجع سابق، ص 732 و733.

[2] **أنظر:** أسامة بن غانم العبيدي، مرجع سابق، ص 113 و114.

[3] التي لا علاقة مباشرة لها بالدليل الرقمي المتصل بالنطاق الافتراضي، وإنما تعد بمثابة الأعمال المادية المساعدة على الوصول إلى الهدف الأساس، المتمثل في إثبات الجريمة.

[4] **أنظر:** أسامة بن غانم العبيدي، المرجع نفسه، ص 114 و115.

المطلب الثاني: أبعاد المعاينة والتفتيش في جرائم الوسط الرقمي

بعد التسليم باكتساب المعاينة والتفتيش صفة الأعمال الجوهرية، المعمول بها لاستخراج الدليل الرقمي الجنائي، نظرا للأسباب المبينة المتأتية أساسا من خصوصية الوسط الرقمي نفسه؛ تبين لنا أن هذه الأعمال تقوم على أبعاد تقنية، يتوجب الاعتماد عليها وفق أحكام قانونية تقليدية تمت رقمنتها تشريعيا، أو على الأقل ترقمن في إطار الممارسة القضائية وشبه القضائية، المتصلة بالتحري والتحقيق في جرائم الوسط الرقمي.

وعليه يمكن القول أن رقمنة المعاينة والتفتيش؛ يتطلب بالضرورة المصاحبة التقنية في إطار الأبعاد محل الطرح. التي قد تنجز في المرحلة السابقة لممارسة المعاينة والتفتيش و/أو بمناسبة ذلك، من خلال تقديم الدعم التقني اللازم(فرع أول)، كما قد تتصل بالمرحلة النهائية في إطار اختتام المعاينة والتفتيش من خلال ممارسة ما يسمى بالحجز(فرا ثانٍ).

الفرع الأول: الدعم التقني لانجاز المعاينة والتفتيش في جرائم الوسط الرقمي

استقر الوضع القانوني ومعه الممارسة القضائية الجنائية؛ على فكرة الطابع المكل الاستثنائي للخبرة الفنية، التي لا يتم اللجوء إليها إلا نادرا وفي بعض القضايا المتشعبة، التي يصعب على القاضي بحكم تكوينه القانوني المحض الوصول إلى فك خيوطها. الأمر الذي جعلته خصوصية المسرح الجرمي الافتراضي؛ بمثابة الإجراء اللازم والضروري، سيما لانجاز المعاينة والتفتيش المرقمنين.

وعلى العموم لايمكن لفريق المعاينة أو التفتيش المرقمنين، الاستغناء عن العضو المختص في الوسط الرقمي، الذي يلعب دور الخبير الرقمي المساعد على التحري والتحقيق. وهو ما سنتطرق إليه فيما يلي عبر تبيان كل ما يتعلق؛ بالدعم التقني المقدم لانجاز المعاينة والتفتيش في إطار مرحلة التحري(أولا)، ونظيره المتصل بإجراءات التحقيق(ثانيا).

أولا: الدعم التقني المقدم من المساعدين المتخصصين أثناء مرحلة التحري

لم يَعْرِفْ المشرع الجزائري فكرة الدعم التقني في إطار مرحلة التحري؛ إلا بعد تعديله لقانون الإجراءات الجزائية سنة 2015[1]. حيث اعتمد لأول مرة من سماهم بالمساعدين المتخصصين لدى النيابة العامة، بعد أن اقتصر في السابق بخصوص الدعم التقني؛ على الخبرة الفنية التي يلجأ إليها قضاء التحقيق والحكم. الأمر الذي سنبينه من خلال التطرق إلى ماهية هذا الدعم التقني الحديث، والقواعد الفنية التي يتبعها المساعدين المتخصصين لانجاز المهام المسندة إليهم.

[1] **أنظر:** المادة 05 المضيفة للمادة 35مكرر؛ أمر رقم 15-02، مرجع سابق.

1. ماهية الدعم التقني المقدم من المساعدين المتخصصين أثناء مرحلة التحري: تقل الدراسات الفقهية المتصلة بالمساعدين المتخصصين –إن لم نقل تنعدم–، وذلك لحداثة اعتمادهم التشريعي. فالمشرع استجدهم سنة 2015 كما بينا سابقا، وحاول تحديد ماهيتهم القانونية بالنص التشريعي والإحالة للتنظيم في الوقت نفسه. الأمر الذي سبق دراسته بنوع من الإيجاز، عند التطرق إلى الأجهزة المدنية ذات الطابع التقني. وسنؤكد عليه بالتفصيل اللازم فيما يلي، من حيث تبيان تعريف الدعم التقني المقدم من المساعدين المتخصصين، وتحديد تشكيلتهم وطريقة سير الإجراءات التي يمارسونها.

أ- تعريف الدعم التقني المقدم من المساعدين المتخصصين أثناء مرحلة التحري: لم يتطرق المشرع الجزائري؛ إلى تعريف المساعدين القضائيين، ولا الدعم الذي يقدمونه في شتى القضايا الجزائية. الأمر الذي يعد منطقيا نظرا لعدم اعتياده على تقديم التعريفات الإجرائية، فاتحاً في ذلك المجال أمام الفقه الجنائي الدارس للقانون الجزائري؛ ليقدم التعريف المناسب انطلاقا من الأحكام الإجرائية ذات الصلة.

وبالبحث في النصوص القانونية –تشريعية وتنظيمية– التي تبين الأحكام الإجرائية ذات الصلة بالمساعدين المتخصصين؛ نجد أنها تطرقت إلى تشكيلة هذا الجهاز وقواعد سير الأعمال الإجرائية التي يمارسها، بالإضافة إلى التحديد الدقيق للمهام الموكلة إليه. الأمر الذي يمكن من خلاله الوصول إلى وضع التعريف المناسب بالمساعدين المتخصصين، والدعم التقني الذي يقدمونه في مجال دراستنا. على أننا نركز في ذلك على المهام التي يختصون بها، التي تعد سبب وجودها أصلا.

بالرجوع إلى النصوص القانونية المنظمة للمساعدين المتخصصين؛ نجد أن المشرع حدد مهامها العامة وترك المجال للتنظيم حتى يفصل في ذلك. حيث يبين المشرع صراحةً؛ أن دورهم ينطوي على مساعدة النيابة العامة بخصوص المسائل الفنية[1]. ويرجع التنظيم ليؤكد على ذلك، ويفصل فيه بالقول أن مهام المساعدين؛ تنحصر في إبداء الرأي في المسائل الفنية، ومساعدة ضباط الشرطة القضائية في المسائل الفنية التي تعترضهم[2].

كما حصر التنظيم بنص قرار وزارة العدل؛ قائمة التخصصات الفنية التي يقوم المساعدين بتقديم المساعدات الفنية بخصوصها. وهي المنطوية على 07 سبعة مجالات، تتمثل في المحاسبة والمالية، الصفقات العمومية، التقنيات والعمليات المالية والمصرفية، التقنيات الجمركية، التجارة الدولية، المناجم والمعادن النفيسة، وأخيرا مجال أنظمة المعالجة الآلية للمعطيات، الذي يعد المحل الافتراضي لممارسة المعاينة والتفتيش المرقمنين[3].

[1] **أنظر:** المادة 05 المضيفة للمادة 35مكرر/1؛ أمر رقم 15-02، مرجع سابق.

[2] **أنظر:** المادة 1/09-1و3؛ مرسوم تنفيذي رقم 17-324، مرجع سابق.

[3] **أنظر:** الجدول الملحق؛ قرار وزارة العدل، مؤرخ في 07 مارس 2018، مرجع سابق.

لو حاولنا البحث في المهام ذات الصلة بالمساعدين المتخصصين، سواءً الواردة بالنص التشريعي، أو المكرسة بالتنظيم المتصل؛ لتوصلنا إلى إمكانية وضع تعريف عام لهؤلاء المساعدين. حيث يتضح أنهم جهة متصلة بالنيابة العامة، كما لهم مهام المساعدة الفنية المحضة وفي مجالات محددة حصرا بنص القانون. ومنه يمكن أن نعرف المساعدين المتخصصين على أنهم: "جهاز مساعد للعدالة يتكون من متخصصين في مجالات فنية محددة حصرا، يوضع تحت تصرف النيابة العامة، لتستعين به في المسائل الفنية المعقدة أثناء ممارسة مهام التحري والمتابعة الجزائية عموما".

على أن يعد الدعم التقني المقدم من المساعدين المتخصصين أثناء مرحلة التحري؛ من بين المهام الأساسية التي يمارسها هؤلاء المساعدين. فالمعاينة والتفتيش المرقمنين المنجزين أثناء مرحلة التحري؛ يمارسان –كما بينا سابقا– بإذن وكيل الجمهورية المختص، من قبل ضابط الشرطة القضائية المعين من طرفه، الذي يستعين بفريق عمل يضم في تشكيلته؛ مساعدا أو أكثر من المتخصصين في الوسط الرقمي –أو في مجال أنظمة المعالجة الآلية للمعطيات كما ورد في قرار وزارة العدل–. حيث يساعدون الضابط المنفذ للإذن في المسائل الرقمية، كما يقدمون له النصائح ويبدون الآراء التقنية اللازمة لإنجاح العملية.

وعليه يمكن أن نعرف الدعم التقني المقدم من المساعدين المتخصصين أثناء مرحلة التحري؛ على أنه: "مساعدة فنية رقمية يقدمها متخصصون في الوسط الرقمي، لضابط الشرطة القضائية المختص بمناسبة تنفيذه لإذن المعاينة أو التفتيش المرقمنين، وذلك عبر إبداء الآراء والنصائح، وممارسة الأعمال التقنية اللازمة تحت إشراف الضابط نفسه"[1].

ب– تشكيلة المساعدين المتخصصين المقدمين للدعم التقني أثناء مرحلة التحري: تعامل القانون مع تشكيلة المساعدين المتخصصين، بنوع من التنظيم المحكم والدائم. حيث بمجرد اكتسابهم الصفة؛ يصبحون تحت التصرف المانع والدائم للنيابة العامة المعينون لديها، ولا يمارسون أي مهام أخرى خارجة عن إطار المساعدة المعنيون بها، حتى وان تعلق الأمر بالإدارة الأصلية التي ينتمون إليها.

وعلى العموم يكتسب الشخص صفة المساعد المتخصص؛ عن طريق الانتداب من الإدارات العمومية المختلفة –الانتداب الذي يمكن إلغاؤه من قبل وزارة العدل أو بطلب من المعني–. على أن تتوفر فيه الشروط القانونية اللازمة، المتمثلة في حصوله على شهادة الليسانس على الأقل، وخبرة مهنية لا تقل عن 05 خمس سنوات في التخصص المطلوب. بالإضافة إلى ضرورة المرور عبر مرحلة الانتقاء، التي تمارسها لجنة خاصة تعين بقرار من وزيل العدل، وأخيرا توجب تأدية اليمين القانونية واجتياز تكوين قانوني لمدة 03 ثلاثة أشهر[2].

---

[1] كما قد تكون لهم ادوار أخرى خارج إطار المعاينة والتفتيش المرقمنين، على غرار المساعدة على تنفيذ عملية مراقبة الاتصالات الرقمية مثلا. الأمر الذي سنتطرق إليه في حينه، بمناسبة معالجة الفصل الموالي من الدراسة.

[2] **أنظر:** المواد من 04 إلى 08 والمادة 14؛ مرسوم تنفيذي رقم 17-324، مرجع سابق.

بعد اكتساب صفة المساعد المتخصص –بتوفر الشروط والإجراءات المذكورة–؛ يتم تعيين المعنيين وتوزيعهم لدى جهاز النيابة العامة، في إطار 04 أربعة مجالس محددة حصرا، في مجلس قضاء الجزائر ومجلس قضاء وهران ومجلس قضاء قسنطينة وأخيرا مجلس قضاء ورقلة. على أن يقوم النائب العام بعد ذلك؛ بتوزيعهم على نيابات الجمهورية التابعة لمجلسه القضائي، بحسب احتياجات كل منها. مع القول بإمكانية الاستعانة بهم عند الحاجة؛ من الجهات القضائية التي لا تملك مساعدين متخصصين، بناءً على طلب النائب العام[1].

ج- سير إجراءات الدعم التقني المقدم من المساعدين المتخصصين أثناء مرحلة التحري: تسير إجراءات الدعم التقني المقدم من المساعدين المتخصصين أثناء مرحلة التحري؛ وفق الأحكام الإجرائية المتصلة عموما بانجاز المعاينة أو التفتيش المرقميين من جهة –السابقة بالذكر–، والأحكام الخاصة بمهامهم من جهة أخرى. حيث يمارس المساعد المعني مهامه في إطار المعاينة أو التفتيش المرقمنين؛ من خلال فريق عمل متكامل ومرؤوس من ضابط الشرطة القضائية المحدد في الإذن –أو من وكيل الجمهورية بشخصه–. كما يكون ذلك خلال مرحلة البحث والتحري، ولغرض تقديم المساعدة الرقمية اللازمة دون سواها.

أما بخصوص الإجراءات الخاصة؛ فيتوجب على المساعدين المتخصصين التقيد بالعديد من الأحكام، على غرار التزام الموضوعية والحياد في تأدية المهام، والخضوع إلى السلطة المباشرة لقضاة النيابة المختصين، وعدم تنفيذ التعليمات الصادرة عن إداراتهم الأصلية مهما كلف الأمر. كما يلتزمون بالسرية المهنية المتعلقة بالمعطيات الرقمية المتعامل معها، أثناء تأدية المهام أو بمناسبة ذلك، وهذا تحت طائلة المسائلة الجنائية. مع إمكانية منعهم من المشاركة في المعاينة أو التفتيش المرقمنين–وأي عمل إجرائي آخر–؛ إذا ما تبين أن ذلك سيؤثر على السير الحس للعدالة. على أن يستفيدون من حماية الدولة أثناء تأدية مهامهم القانونية[2].

وأخيرا يكون عمل المساعدين المتخصصين؛ بمثابة الأساس التقني –الذي قد يشكل الدليل الرقمي الجنائي فيما بعد– الذي تبني عليه النيابة العامة الاتهامات الموجهة ضد الأشخاص، بارتكابهن لجريمة أو أكثر من جرائم الوسط الرقمي. حيث تُنْجَزُ الأعمال الفنية في إطار الدعم اللازم المتصل بالمعاينة أو التفتيش الرقميين؛ على شكل تقارير تلخيصية أو تحليلية، يمكن للنيابة العامة أن ترفقها بالتماساتها المقدمة للاتهام وإثباته القانوني[3].

---

[1] **أنظر:** المادتان 02 و17؛ مرسوم تنفيذي رقم 17-324، مرجع سابق. **وأنظر أيضا:** الجدول الملحق؛ قرار وزارة العدل، مؤرخ في 07 مارس 2018، مرجع سابق.

[2] **أنظر:** المواد من 10 إلى 12؛ مرسوم تنفيذي رقم 17-324، المرجع نفسه.

[3] **أنظر:** المادة 05 المضيفة للمادة 35مكرر4؛ أمر رقم 15-02، مرجع سابق.

2. القواعد الفنية للدعم التقني المقدم من المساعدين المتخصصين أثناء مرحلة التحري: لم تتطرق النصوص القانونية المقررة لمهام المساعدين المتخصصين –التشريعية والتنظيمية المذكورة–؛ إلى القواعد الفنية التي يتبعونها بمناسبة تأدية المهام الموكلة إليهم. الأمر الذي يعد مفهوما ومعقولا، حيث لايمكن سرد الآليات الفنية المتصلة بكل التخصصات السبعة لهؤلاء المساعدين، كما يتعذر قانونا من جهة أخرى تحديد قائمة –ولو على سبيل المثال–؛ للقواعد الفنية المتبعة من المساعدين المتخصصين، لدى ممارستهم للمعاينة والتفتيش المرقمنين.

وعليه يمكن القول أنه بخصوص القواعد الفنية؛ سيعمل المساعدين حتما بكل ما يعد مشروعا ونزيها تحت إشراف قائد فريق المعاينة أو التفتيش. مع مراعاة التطور الديناميكي السريع للوسط الرقمي، حيث ما تعد وسائل فنية مناسبة اليوم، قد تصبح غير ذلك بعد مرور يوم أو يومين فقط. الأمر الذي –الوسائل– سنؤجل الحديث عنده، لنبينه بنوع من التفصيل عند التطرق فيما يلي إلى القواعد الفنية للدعم التقني المقدم لانجاز المعاينة والتفتيش في إطار التحقيق القضائي –الخبرة–، وذلك تفاديا للتكرار، نظرا للتطابق التقني الكبير بينهما[1].

ثانيا: الدعم التقني المقدم من الخبراء أثناء إجراءات التحقيق

على العكس من الدعم التقني المقدم من المساعدين المتخصصين أثناء مرحلة التحري، يعد نظيره المقدم من الخبراء أثناء إجراءات التحقيق؛ من الأعمال الإجرائية المعروفة التي جاء بها قانون الإجراءات الجزائية، منذ صدوره أول مرة سنة 1966. حيث يعتمد عليه –الدعم التقني– قاضي التحقيق؛ لفك خيوط القضايا المتعبة ذات البعد الفني. ومنه يمكن القول أننا بصدد رقمنة الأحكام التقليدية المتعلقة بالخبرة، بإسقاطها على الدعم التقني المقدم أثناء إجراءات التحقيق المتصلة أساسا بالمعاينة والتحقيق المرقمنين. الأمر الذي نبينه فيما يلي؛ من خلال التطرق إلى ماهية هذا الدعم التقني المرقمن، والقواعد الفنية التي يتبعها الخبراء لانجاز المهام المسندة إليهم.

1. ماهية الدعم التقني المقدم من الخبراء أثناء إجراءات التحقيق: تعد الخبرة القضائية، من أهم الوسائل التي يستعين بها القضاء عموما –والقضاء الجزائي من طرف قاضي التحقيق خاصةً–؛ من أجل مواجهة التعقيدات التي تعترض القضايا محل التحقيق، سيما تلك التي يكون لها الطابع الفني المعقد، الخارج عن إطار دراسة وتكوين القاضي القائم على البعد القانوني المحض. وهو ما ينطبق فعلا على الخصوصية المعقدة للمسرح الجرمي الافتراضي، الذي يواجهه قاضي التحقيق في العادة؛ عبر الاستعانة بالدعم التقني المقدم من الخبراء، الذي نستعرضه فيما يلي عبر التطرق إلى تعريفه وتشكيلة خبرائه وطريقة سيره.

[1] حيث يقتصر الاختلاف بين الدعم التقني المقدم في مرحلة التحري والآخر المتصل بإجراءات التحقيق؛ على الأحكام القانونية ذات الصلة فقط، وذلك من حيث المرحلة الإجرائية والتشكيلة والتبعية وسير الإجراءات القانونية.

أ- تعريف الدعم التقني المقدم من الخبراء أثناء إجراءات التحقيق: اعتادت الدراسات ذات الصلة بالخبرة الفنية في المادة الجزائية؛ على التطرق إليها بشكل منفصل عن المعاينة والتفتيش، وذلك نظرا لاعتمادها المنفصل من قاضي التحقيق وكذا نظرا لاعتبارها من المشرع بمثابة العمل الإجرائي المستقل. الأمر الذي نجد أنه يظهر بالشكل العكسي بخصوص التحقيق في جرائم الوسط الرقمي، حيث تتصل الخبرة كأصل عام بالمعاينة والتفتيش الرقميين، نظرا لكونهما أهم الأعمال الإجرائية من جهة، ونظرا لعم إمكانية الاستغناء عن الخبراء عند تنفيذهما من جهة أخرى.

وعلى العموم عالج المشرع الجزائري الخبرة في إطارها التقليدي غير المرقمن، التي يأمر بها قاضي التحقيق المختص -أو قاضي الحكم-؛ في إطار قانون الإجراءات الجزائية، بالمواد من 143 إلى 156. حيث بين من خلال ذلك مهام الخبير وطريقة تعينه وسير الخبرة التي ينجزها، من دون التطرق لا إلى تعريف الخبرة ولا الخبير الذي ينجزها. الأمر الذي توصل إليه الفقه الجنائي؛ انطلاقا من المهام التي يقوم بها الخبير بالأساس، وكل القواعد الإجرائية الحاكمة للخبرة بالتبعية.

لم يتطرق المشرع صراحةً إلى المهام الأساسية التي يختص بها الخبراء، بل اكتفى بتبيان الحالة العامة التي يمكن لقاضي التحقيق -أو الحكم- إذا توفرت أن يلجأ إلى الخبرة. الأمر الذي عبر عنه بـــ: "يجوز لجهات التحقيق أو الحكم عندما تعرض لها مسألة ذات طابع فني أن تأمر بندب خبير..."[1]. وهو ما يستشف منه؛ أن مهام الخبير تتمثل في تنوير القاضي المعني في المسائل الفنية، التي يعجز بحكم تكوينه القانوني المحض؛ عن فك خيوطها والوصول إلى الحقيقة المبحوث عنها.

ومن خلال ذلك ظهرت العديد من التعريفات الفقهية، المتصلة بالخبرة التقليدية -غير المرقمنة-. التي نجد منها ما تعتبرها؛ على أنها: "إدلاء أهل العلم والفن والدراية برأيهم في مسائل فنية تتعلق بمجالات اختصاصاتهم، بطلب من قاضي التحقيق الذي تخرج هذه التخصصات عن إطار معرفته نظرا لتكوينه القانوني المحض"[2]. كما تعرف الخبرة على أنها: "استشارة فنية يستعين بها قاضي التحقيق لتقدير المسائل الفنية التي يحتاج تقديرها إلى معرفة فنية أو دراية علمية لا تتوفر لدى قاضي التحقيق بحكم تكوينه"[3].

وأما الخبرة المرقمنة المنجزة في إطار مكافحة جرائم الوسط الرقمي، فنظرا لعدم التطرق التام لها من المشرع الجزائري -وحتى نظرائه-؛ ظهرت العديد من الدراسات الفقهية المحاولة لإرساء القواعد الأساسية ذات الصلة. الأمر الذي وردت من خلاله العديد من التعريفات، المتعلقة بالخبرة والخبير في

---

[1] **أنظر:** المادة 1/143؛ أمر رقم 66-155، مرجع سابق.

[2] **أنظر:** ناصر حمودي، (قانون الإجراءات الجزائية الجزائري)، مرجع سابق، ص 230.

[3] **أنظر:** أحسن بوسقيعة، التحقيق القضائي، مرجع سابق، ص 107.

الوسط الرقمي. حيث يعرف الخبير الرقمي؛ على أنه: "الخبير المتخصص والمدرب على معالجة جميع أنواع الأدلة الرقمية وفحصها وتحليلها". كما تعرف الخبرة المرقمنة عموما؛ على أنها: "تنقيب وبحث يرتبط بمادة تتطلب معارف علمية أو فنية خاصة لا تتوافر لدى المحقق الجنائي في الجريمة الالكترونية"[1].

يتضح من خلال ما تم بيانه أعلاه؛ أنه لا فرق بين الخبرة التقليدية والمرقمنة بخصوص التعرف المسند. إلا من حيث تخصص الثانية –الخبرة المرقمنة–؛ في المجال الفني المتمثل في الوسط الرقمي دون سواه، وهو الذي يعد أحد المجالات الفنية التي يختص بها الخبير عموما.

وعلى العموم يمكن من خلال كل التعريفات المقدمة للخبرة التقليدية، والأخرى المتصلة بالخبرة والخبير في الوسط الرقمي؛ أن نصل إلى وضع التعريف المناسب بالدعم التقني المقدم من خبراء الوسط الرقمي أثناء إجراءات التحقيق، في إطار كل من المعاينة والتفتيش المرقمنين. حيث نقول أنه: "مساعدة فنية رقمية يقدمها خبراء الوسط الرقمي، لقاضي التحقيق أو ضابط الشرطة القضائية في إطار الإنابة بمناسبة ممارسة المعاينة أو التفتيش المرقمنين، وذلك عبر إبداء الآراء والنصائح، وممارسة الأعمال التقنية اللازمة تحت إشراف المسئول عن العملية"[2].

ب– تشكيلة الخبراء المقدمين للدعم التقني أثناء إجراءات التحقيق: تقوم تشكيلة الخبراء على الفكر الفردي أو الجماعي على حسب الحالة والحاجة. حيث بمجرد اكتساب الفرد لصفة الخبير الفني في المسألة التي يختص بها؛ يصبح تحت تصرف القضاء، سواءً قضاء التحقق أو الحكم، الذي يمكنه الاستعانة به بمناسبة سير إجراءات الدعوى العمومية.

وعلى العموم يوجد على مستوى كل مجلس قضائي؛ جدول معد مسبقا يتضمن قائمة بالخبراء الفنيين، كل على حسب تخصصه العلمي –من بينهم خبراء الوسط الرقمي–[3]. وهم اللذين يحلفون اليمين القانونية عند التقييد في الجدول لأول مرة. الأمر الذي يدفع للقول بأن القاضي المختص –قاضي تحقيق أو قاضي حكم–؛ إذا أراد اللجوء إلى الخبرة الفنية، فما عليه سوى أن يختار خبير أو أكثر من المسجلين في الجدول المتصل بالمجلس القضائي الذي يمارس فيه مهامه. كما سمح المشرع بإمكانية تعيين خبير أو أكثر من خارج الجدول، على شرط تأدية اليمين القانونية قبل ممارسة المهام الفنية[4].

---

[1] **أنظر:** وردة شرف الدين، مرجع سابق، ص 267. **وأنظر أيضا:** محمد كمال شاهين، مرجع سابق، ص 333.

[2] كما قد تكون لهم ادوار أخرى أيضا خارج إطار المعاينة والتفتيش المرقمنين، وفق الطريقة نفسها المتصل بالدعم التقني المقدم أثناء مرحلة التحري. وهو ما سنتطرق إليه في حينه، بمناسبة معالجة الفصل الموالي من الدراسة.

[3] الأمر الذي يختلف عن التوزيع المتصل بالمساعدين المتخصصين، الذي نجدهم -كما بينا سابقا- على مستوى أربع مجالس قضائية فقط. **أنظر في ذلك:** المادة 1/144؛ أمر رقم 66-155، مرجع سابق.

[4] **أنظر:** المواد 144 و145 و147؛ المرجع نفسه.

يقود التحليل السطحي للنص التقليدي المتصل بالخبرة الفنية، إلى افتراض ضم التشكيلة العامة لجدول الخبراء المعد من قبل المجلس القضائي؛ لخبراء متخصصين في الوسط الرقمي، الذين أدوا اليمين القانونية بمجرد اكتسابهم لصفة الخبير القضائي. وفي حالة تخلف ذلك؛ يمكن لقاضي التحقيق الممارس لإجراءات التحقيق في جرائم الوسط الرقمي؛ أن يعين شخص أو أكثر من بين المتخصصين في الوسط الرقمي ليمارسوا الخبرة القضائية المطلوبة منهم، بعد تأدية اليمين القانونية اللازمة.

ج- سير إجراءات الدعم التقني المقدم من الخبراء أثناء إجراءات التحقيق: يمكن لقاضي التحقيق في إطار ممارسته لإجراءات التحقيق المتصلة بجريمة أو أكثر من جرائم الوسط الرقمي؛ أن يلجأ إلى الخبرة الفنية، عبر ندب خبير أو أكثر من خبراء الوسط الرقمي –من الجدول أو خارجة–، سيما لإنجاح عملية المعاينة و/أو التفتيش المرقمنين.

يمكن لقاضي التحقيق الراغب في اللجوء إلى الخبرة في جرائم الوسط الرقمي؛ أن يقوم بتعيين خبير أو أكثر من تلقاء نفسه، كما يمكنه ذلك بناءً على طلب أحد الخصوم في الدعوى العمومية –النيابة العامة والمتهم– أو في الدعوى المدنية –المتهم والضحية والمسئول المدني–. إلا أنه يمكنه رفض اللجوء إلى الخبرة، التي تكون محل طلب أحد الخصوم، وذلك بموجب أمر مسبب في أجل أقصاه 30 يوما من تاريخ استلام الطلب نفسه[1].

وفي حالة قرر قاضي التحقيق اللجوء إلى الخبرة في جرائم الوسط الرقمي؛ تكون عملية تنفيذها تحت رقابته المباشرة. على أن يبين الأمر الصادر باللجوء إلى الخبرة، العديد من النقاط الأساسية والجوهرية، المتصلة أساسا بالتحديد الدقيق للمهمة الرقمية المطلوبة، والمدة التي يتوجب انجاز الخبرة في إطارها[2]. الأمر الذي قد يرتبط بعملية المعاينة أو التفتيش المرقمنين، فتكون المهمة إنجاح العملية وفي المدة المتصلة بالمعاينة أو التفتيش –على حسب الحالة–، أو خارجها إذا ما مورست الخبرة لتحليل النتائج المترتبة.

وفي كل الأحوال يتوجب على الخبير –أو الخبراء– المعين في إطار إجراءات التحقيق في جرائم الوسط الرقمي؛ أن يبقى دائما على اتصال بقاضي التحقيق الذي عينه، حيث يطلعه بكل كبيرة وصغيرة تخص القضية، ما يمكنه من اتخاذ الإجراءات اللازمة في الوقت المناسب. على أن منح القانون لخبراء الوسط الرقمي –والخبراء عموما–؛ بعض الحقوق اللصيقة بممارسة مهامهم، على غرار إمكانية الاستعانة بخبراء من خارج تخصصهم بأمر من قاضي التحقيق المختص، والتعامل مع المحجوزات الرقمية التي تكون في أحراز مادية و/أو افتراضية. بالإضافة إلى مقابلة الأشخاص الذي يحددونهم، على أن يشترط إذا

---

[1] **أنظر:** المادة 143/ 1 و2؛ أمر رقم 66-155، مرجع سابق.

[2] على أنه يمكن أن تمدد المدة المحددة في أمر الخبرة، بطلب مسبب من الخبير الرقمي نفسه. مع إمكانية استبدالهم في حالة عدم احترام المواعيد المحددة في الأمر، بالإضافة إلى تحملهم للمسؤولية التأديبية وفق القواعد المعمول بها في هذا الشأن. **أنظر في ذلك:** المادتان 146 و148؛ المرجع نفسه.

تعلق الأمر بالمتهم؛ حضور قاضي التحقيق المختص مع مراعاة الإجراءات المتصلة بالاستجواب –مع إمكانية استغناء المتهم عن هذا الشرط–[1].

وعلى العموم يتوجب على خبير الوسط الرقمي المعين من قاضي التحقيق المختص لممارسة الخبرة في جرائم الوسط الرقمي؛ أن يقوم بتحرير تقرير الخبرة المنجزة، سواءً أنجزت في إطار إجراءات التحقيق عموما، أو بمناسبة ممارسة أعمال المعاينة و/أو التفتيش المرقمنين خصوصاً. حيث يحدد في التقرير بعد أن يشهد بأنه مارس الإجراءات بنفسه؛ الوصف الكامل لما قام به من أعمال وما توصل إليه من نتائج، مع التوقيع على التقرير نفسه، الذي قد يشهد توقيعات على آراء مختلفة إذا مورست الخبرة من عدد من الخبراء، توصلوا إلى نتائج بقناعات مختلفة[2].

2. القواعد الفنية للدعم التقني المقدم من الخبراء أثناء إجراءات التحقيق: يقوم الدعم التقني المقدم من خبراء الوسط الرقمي–وأيضا المقدم من المساعدين المتخصصين–؛ على العديد من القواعد الفنية، التي يعمل بها انطلاقا من الضرورة الرقمية ذات الصلة، ونظرا لغياب النص القانوني المنظم لذلك[3]. الأمر الذي له العديد من الأوجه التقنية المحضة، القائمة أساسا على مجالات هذا الدعم التقني، وعملياته ومتطلبات انجازها.

تتم ممارسة الدعم التقني محل الطرح في إطار العديد من المجالات التي لها الطابع التقني –الرقمي–. على أن تدخل كل هذه المجالات في المفهوم العام للوسط الرقمي، وتكون من بين مكوناته الأساسية في الإطار المشروع. وعلى العموم يرى الفقه الجنائي، أن أهم مجالات الخبرة المرقمنة؛ تتمثل في التعامل مع التزوير الرقمي والمرقمن المتصل بالمعطيات والمستندات المدخلة أو المستخرجة من الجهاز. والبحث في التلاعب بالمعطيات –بيانات و/أو معطيات–. بالإضافة إلى التلاعب في الأنظمة المعلوماتية عموما –برامج قاعدية وتطبيقية وشبكية–، كما يمكن أن ينصب مجال الخبرة المرقمنة؛ على موضوع الغش المتصل بالمعطيات والعمليات ذات الصلة[4].

ينجز الدعم التقني المقدم من الخبراء أثناء إجراءات التحقيق في إطار المجالات المبينة أعلاه وغيرها؛ من خلال ممارسة العديد من العمليات الرقمية والمرقمنة. التي يرى العديد من المتخصصين بضرورة تقسيمها إلى ثلاثة مراحل أساسية، يمكن أن ندخل فيها بعض الآليات الفنية اللازمة التي تتصل أساسا بالمرحلة الثالثة والأخيرة.

---

[1] **أنظر:** المواد 2/148 و1/149 و1/150 و151؛ أمر رقم 66-155، مرجع سابق.

[2] **أنظر:** المادة 1/153 و2؛ المرجع نفسه.

[3] غياب النص المنضم للقواعد الفنية ذات الصلة؛ يعد بمثابة الأمر الايجابي، نظرا لاستحالة حصر هذه القواعد، سيما إذا ما رجعنا إلى الطابع الديناميكي سريع التطور الذي يتصف به الوسط الرقمي عموما.

[4] **أنظر:** حازم محمد حنفي، مرجع سابق، ص 66.

تنطوي المرحلة الأولى من بين العمليات الرقمية والمرقمنة المنجزة في إطار الدعم التقني محل الطرح؛ على تجميع المعطيات المخزنة لدى مقدم الخدمة، بتتبع الأجهزة الخوادم التي استعملها المتهم عبر الولوج من خلالها أو إليها أو بمساعدتها. الأمر الذي تتلوه مرحلة ثانية أساسية أيضا، تتمثل في المراقبة، التي تفترض عودة المتهم ليحوم حول المسرح الجرمي الافتراضي، لأسباب عديدة منها إتلاف الدليل الرقمي. على أن تقوم هذه المراقبة على العديد من الأعمال، أهمها المراقبة باستخدام برامج خاصة تسمح بتسجيل المعطيات المتصلة بالمتهم، سيما المتعلقة منها بالولوج والخروج[1].

كما قد يعتمد الخبير الرقمي لانجاز هذه المراقبة؛ على الحشرات الرقمية أو كاميرات مراقبة الجهاز. بالإضافة إلى إمكانية الاعتماد على عمليات أخرى أكثر تعقيدا، على غرار زرع فيروس الجهاز أو دودة حصان طروادة مثلا. التي تمتاز بمراقبتها لأكثر من جهاز في الوقت نفسه، على أن يراعى في ذلك التحصين الرقمي، من الانتشار السلبي للفيروس، وإلا سيصبح مستهدفا من برامج الوقاية الرقمية السابقة بالدراسة[2].

وكمرحلة أخيرة في إطار عمليات الدعم التقني المقدم من الخبراء، يقوم الخبراء بعد حجز المعطيات الرقمية والأجهزة التي تحويها؛ بعملية الفحص التي تتصل أساسا بمبدأ "لوكارد التبادلي"، الذي مفاده أن كل من يلج إلى الوسط الرقمي؛ سيأخذ منه أشياءً ويترك وراءه أشياءً أخرى. ولا يمكن أن تمارس هذه العملية إلا بعمل يسبقها وآخر يتلوها. حيث يتوجب أولا حفظ المعطيات ذات الصلة بمسرح الجريمة، مع استعادة الضائعة منها، ومن ثم التعامل معها عبر تحليلها وإعادة بنائها[3].

تتم عملية حفظ المعطيات من قبل الخبير الرقمي؛ عبر نسخها بعد حجزها من الجهات المختصة بذلك، بطريقة تجعل من النسخة الأولى محفوظة وفق الصورة نفسها التي حجزت عليها، وتفتح المجال لفحص وتحليل النسخة الثانية التي بحوزة الخبير. مع إمكانية العمل على استعادة تلك الضائعة منها، سيما تلك المحذوفة بإرادة المتهم أو من يساعده[4]، الأمر الذي يفتح المجال لاستعادة أغلب المعطيات –إن لم نقل كلها–، التي قد تبين الحقيقة المبحوث عنها[5].

---

[1] **أنظر:** حازم محمد حنفي، مرجع سابق، ص 69.

[2] **أنظر:** المرجع والصفحة نفسهما.

[3] **أنظر:** المرجع نفسه، ص 69 و70. **وأنظر أيضا:** وردة شرف الدين، مرجع سابق، ص ص 269-271.

[4] **أنظر:** وردة شرف الدين، المرجع نفسه، ص 270 و271.

[5] سبق لوزارة العدل الأمريكية؛ أن وضعت إطارا يحدد الخطوات الأساسية لجمع الأدلة وفحصها وتحليلها وكتابة نتائجها في تقرير الخبرة. ولعل أهم ما يتميز به هذا الإطار؛ ينطوي على توضيحه لأنواع الأدلة الرقمية وأماكن تواجدها رقميا، مع ربطه بين المعطيات المحددة ونوع الجريمة المتصلة بها. على غرار تحديده لقائمة الأماكن المعتادة، التي يمكن العثور من خلالها على الملفات الخفية والملغاة وغيرها -كلمة سر وأرقام البطاقات...الخ-، في إطار التحقيق -وحتى التحري- في بعض الجرائم المحددة، مثل تلك المتصلة بالتعدي الرقمي على الهوية ونشر الصور الفاضحة وغيرها. **وأنظر أيضا:** حازم محمد حنفي، المرجع نفسه، ص 69.

بعد قيام الخبير بالحفظ والاستعادة المتصلين بالمعطيات الرقمية المهمة في فك خيوط القضية؛ يصبح أمام حتمية التحول إلى آخر عنصرين أساسيين في هذا الصدد، المنطويين على التحليل وإعادة البناء. حيث يحلل الخبير المعطيات التي بحوزته عبر تقييم محتواها، لتحديد وسائل ارتكاب الجريمة والدوافع المؤدية إلى ذلك. على أن يقوم بعد ذلك بإعادة بناء القضية، من خلال البحث وتفسير كل الأحداث الرقمية التي حصلت بين الضحية والمتهم أساسا ومن حولهما بالتبعية[1].

وعلى العموم لايمكن للخبير الرقمي، القيام بممارسة الدعم التقني أثناء إجراءات التحقيق –ولا نظيره المنجز أثناء مرحلة التحري من قبل المساعدين المتخصصين–؛ إلا وفق متطلبات فنية أساسية يستحيل الاستغناء عنها. حيث يتوجب على قاضي التحقيق قبل اختياره للخبير الرقمي؛ أن يتثبت من امتلاكه للعلم النظري والخبرة العملية في الوسط الرقمي[2]، سيما بخصوص الإلمام الفني بكل ما يتصل بعناصر الوسط الرقمي ونطاقها الافتراضي، والقدرة على إتمام الخبرة بنجاح ودون ترتب أعطاب فنية ولا إتلاف للآلة الرقمية. بالإضافة إلى ضمان عملية التعامل الرقمي مع الأدلة دون تلفها. هذا علاوةً على ضرورة إلمام الخبير الرقمي؛ بكل الوسائل الفنية التي تستعمل للتعامل القضائي مع الدليل الرقمي في إطار التحري أو التحقيق، على غرار البرامج المؤدية لاسترجاع المعطيات وغيرها[3].

الفرع الثاني: الحجز المترتب عن المعاينة والتفتيش في جرائم الوسط الرقمي

أحدثت الخصوصية الافتراضية للمعاينة والتفتيش المرقمنين خاصةً، وأعمال استخراج الدليل الرقمي عموما؛ نوعا من التعقيد الإجرائي الذي يتطلب بالإضافة إلى وجوبيه اللجوء للدعم التقني؛ التعامل مع حجز ما ينتج عن المعاينة والتفتيش بطريقة مغايرة عن تلك المعروفة تقليديا، ما نجده بمثابة رقمنة للحجز وفق الطريقة نفسها المتصلة بالمعاينة والتفتيش. الأمر الذي يعد طبيعياً، فالحجز يتبع المعاينة والتفتيش من حيث الأثر والطبيعة.

وعليه يمكن القول أن رقمنة الحجز هو من رقمنة المعاينة والتفتيش أصلا، سيما وأن نتائج التحري والتحقيق في جرائم الوسط الرقمي؛ تحدد في العادة انطلاقا من التحليل والتدقيق المتصلين بما تم حجزه من عناصر رقمية ونطاق افتراضي متصل بها. الأمر الذي نتوسع في تبيانه فيما يلي، عبر التطرق إلى مفهوم الحجز المترتب عن المعاينة والتفتيش المرقمنين(أولا)، وتحديد الخصوصية ذات الصلة(ثانيا).

---

[1] **أنظر:** وردة شرف الدين، مرجع سابق، ص 271.

[2] الأمر الذي يعد ممكنا -في كل الأحوال- بالنسبة لقاضي التحقيق، الذي منحه القانون حق اختيار خبير رقمي -أو أكثر- من الجدول أو خارجه. لكن يعد غير ذلك بالنسبة لوكيل الجمهورية أثناء مرحلة التحري، الذي يعد ملزما باختيار المساعد المتخصص من بين الموجودين تحت تصرفه فقط، كما قد يضطر إلى طلبهم من الجهات القضائية المزودة بهم، إذا لم يكن تابعا لأحد المجالس القضائية الأربعة المزودة بهم.

[3] **أنظر:** حازم محمد حنفي، مرجع سابق، ص 67 و68.

أولا: مفهوم الحجز المترتب عن المعاينة والتفتيش في جرائم الوسط الرقمي

يعد الحجز في المواد الجزائية عموما؛ بمثابة الإجراء التقليدي المعروف، الذي قد يترتب عن ممارسة إجراء التفتيش. الأمر الذي بإسقاطه على الوسط الرقمي والمسرح الجرمي الافتراضي الحديث الذي أحدثه من جهة، وعلى المعاينة والتفتيش المرقمنين الممارسين في إطاره من جهة أخرى؛ يمكن أن نصل إلى وجوب التطرق إلى الحجز المرقمن الذي يتبع العمليتين، انطلاقا من التسليم بحتمية التلازم في الطبيعة المرقمنة. ومنه لايمكن الوصول إلى تحديد الخصوصية الحديثة للحجز المرقمن؛ إلا بعد تبيان مفهومه من حيث التعريف به وتحديد طبيعته وإبراز أهميته.

1. تعريف الحجز المترتب عن المعاينة والتفتيش في جرائم الوسط الرقمي: لم يتطرق قانون الإجراءات الجزائية إلى تعريف الحجز عموما، وإنما اكتفى بتبيان بعض الإجراءات المتعلقة بممارسته، من أعمال وأجهزة. حيث يتبين من خلال المواد المقررة للحجز؛ أنه قابل للممارسة في إطار كل من مرحلة التحري وإجراءات التحقيق[1]، ولو أنه –المشرع– ركز على تبيان القواعد الإجرائية المتعلقة بإجراءات التحقيق أكثر من مرحلة التحري، فاكتفى بخصوص هذه الأخيرة بمجرد الإشارة على إمكانية الحجز كنتيجة عن التفتيش، وضرورة الحفاظ على السر المهني[2].

إلا أننا بتفحص النصوص المقررة للحجز المتصل بكل من مرحلة التحري وإجراءات التحقيق القضائي؛ نجد أن المشرع ربطه صراحةً بالتفتيش دون المعاينة. الأمر الذي يمكن أن نتجاوزه، لنقول بإمكانية ترتبه –الحجز– عن ممارسة إجرائي الانتقال والمعاينة المرقمنين. حيث يفهم من بعض نصوص قانون الإجراءات الجزائية؛ أن المشرع يقصد ضمناً ترتب الحجز عن المعاينة، وذلك انطلاقا من المادة 1/64 "ق.إ.ج"، التي تربط في إطار إجراءات التحري المتصلة بالحالة العادية؛ بين المعاينة والتفتيش والحجز[3]. وكذلك المادة 1/84 من القانون نفسه، المتصلة بإجراءات التحقيق القضائي، التي أوردت نصاً عاماً يسمح بالحجز في كل إجراءات التحقيق، المنطوية كل الأعمال التي يمارسها قاضي التحقيق، بما فيها المعاينة والتفتيش[4].

---

[1] **أنظر:** المادتان 3/44 و2/45 و4 و5 والمواد 2/47 و1/64 و84 و85؛ أمر رقم 66-155، مرجع سابق.

[2] الأمر الذي يعد غير مفهوماً، حيث يفترض أن يقوم المشرع بالعكس، من منطلق أن الحجز في مرحلة التحري؛ يمارس من قبل الشرطة القضائية تحت إدارة وكيل الجمهورية، ضد المشتبه فيه الذي لا يتمتع بالضمانات القضائية الكافية –من منطلق كون النيابة العامة خصم في الدعوى العمومية بعد رفعها أو تحريكها-، ومنه توجب تحديد المشرع صراحةً لقواعد الحجز حمايةً للمشتبه فيه من تعسف الأجهزة المختصة. وهو ما لا نقول فيه أي شيء لو غاب النص تماما عن الحجز في إجراءات التحقيق القضائي، لكون ممارسته تحت إدارة قاضي التحقيق؛ يعد بمثابة الضمانة الكافية لعدم التعسف من جهة، ولكونه يتقيد بالمشروعية العامة لا النصية من جهة أخرى.

[3] **نص المادة:** "لا يجوز تفتيش المساكن ومعاينتها وضبط الأشياء المثبتة للتهمة...".

[4] **نص المادة:** "إذا اقتضى الأمر أثناء إجراء تحقيق وجوب البحث عن مستندات فإن لقاضي التحقيق أو ضباط الشرطة القضائية المنوب عنه الحق في الاطلاع عليها قبل ضبطها".

وعلى العموم وضع الفقه الجنائي التقليدي؛ العديد من التعريفات المتعلقة بالحجز المترتب عن التفتيش –والمعاينة–. الأمر الذي يؤسس له بالقواعد الإجرائية المبينة للأحكام المتبعة بخصوص هذا الحجز[1]. ولو أن أغلب هذه التعريفات؛ تتصل بالحجز المنجز كأثر للتفتيش الممارس خلال إجراءات التحقيق القضائي، تحت إشراف وإدارة قاضي التحقيق المختص. ومن أهمها نجد أن الحجز هو: "التحفظ على الأشياء وضبطها ووضعها في أختام التي تنفع في إظهار الحقيقة"[2].

يتضح من خلال التعريف الفقهي المبين أعلاه؛ أنه بطابع تقليدي مادي، يتصل بالجريمة التقليدية التي تثبت في العادة بالدليل التقليدي المنطوي على الشيء المادي، القابل للمس والتعامل المادي معه، والقابل أيضا للتحفظ عليه في الأختام والأحراز المغلقة بعد ضبطه بالطرق اللازمة لذلك –التي تكون مادية أيضا–. الأمر الذي يُصَعِبُ من عملية الإسقاط القانوني لهذا المفهوم التقليدي على الحجز المرقمن، الذي يتصل بالنطاق الافتراضي للوسط الرقمي كمسرح جرمي حديث، وان تجاوزه فسيقع على العناصر الرقمية التي أحدثته دون سواها.

أدت الصعوبة –إن لم نقل الاستحالة– المتصلة بتطبيق قواعد الحجز التقليدي على الحجز المرقمن بالمشرع الجزائري –والمقارن–؛ إلى التدخل لسن نصوص إجرائية توضح القواعد الخاصة بالحجز المرقمن، مع الاحتفاظ بتلك التقليدية التي تكون قابلة للتطبيق الحديث الافتراضي. الأمر الذي جاء به المشرع الجزائري في إطار القانون 09–04 سابق الذكر[3]، الذي يحوي على 04 أربعة مواد كاملة، تبين القواعد الحديثة للحجز المرقمن[4].

عمل الفقه الجنائي على البحث في موضوع وضع التعريف المناسب بالحجز المرقمن، وذلك انطلاقا من النصوص القانونية الحديثة والتقليدية التي يمارس من خلالها. الأمر الذي أدى إلى اعتبار البعض للحجز المرقمن؛ على أنه: "وضع اليد على المكونات المادية للحاسوب والأدلة المعلوماتية المخزنة في

---

[1] إلا أن ما يعاب على المشرع الجزائري في هذا الإطار؛ كونه لم يستقر في إطار قانون الإجراءات الجزائية على مصطلح واحد ثابت يعبر به عن الحجز التقليدي -وحتى المرقمن-. حيث عبر عنه بالمصطلح نفسه في العديد من المواقع، على غرار ما ورد في المواد؛ "3/44 و45 و2/47"، ثم رجع ليعبر عنه -الحجز- بمصطلح آخر منطوي على "الضبط" في مواقع أخرى، سيما بالمادتين؛ "1/64 و84". وهذا رغم وحدة المصطلح الفرنسي المقابل لكل من الحجز والضبط، في النص نفسه الوارد باللغة الفرنسية، الذي عبر بـ "Saisie".

[2] **أنظر:** عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، مرجع سابق، ص 366.

[3] **أنظر:** المواد من 06 إلى 09؛ قانون رقم 09-04، مرجع سابق.

[4] ولو أنه يعاب على المشرع أنه حصر تطبيق أحكام الحجز المرقمن؛ على ذلك المترتب عن عملية التفتيش دون المعاينة. الأمر الذي نتجاوزه ونؤسس له عبر القول؛ أن الحجز المرقمن يتصل بالمعاينة والتفتيش المرقمنين معا، وذلك لسببين. ينطوي السبب الأول على الأساس التقليدي نفسه المذكور سابقا، حيث دائماً ما يربط المشرع بخصوص مرحلة التحري؛ بين المعاينة والتفتيش والحجز من جهة، ويفتح مجاله ليتصل بكل إجراءات التحقيق من جهة أخرى. وأما السبب الثاني؛ فمؤداه أن المشرع بالقانون 09-04؛ قد أهمل أصلا المعاينة المرقمنة، التي تطبق في إطارها الأحكام التقليدية، سواءً بخصوص تنفيذها أساساً أو تنفيذ الحجز المترتب عنها تبعيةً.

الحاسوب محل التفتيش أو في الشبكة أو في الحاسوب الخادم والتي تفيد في كشف الحقيقة في جريمة وقعت وجاري التحقيق فيها"[1].

يتبين من التعريف المبين أعلاه، أن صاحبه أحسن بالقول أن الحجز المرقمن؛ قد يشمل النطاق الافتراضي بصورة مستقلة عن العناصر الرقمية الحاملة له، أو الاثنين معا –حجز العناصر وما تتضمنه من نطاق افتراضي–. إلا أنه جانب الصواب عند اعتباره؛ بأن الحجز هو الأثر المباشر للتفتيش فقط. وهذا لكونه قد يكون أثرا للمعاينة المرقمنة، وحتى أثرا لتصرف خارج إطار المعاينة والتفتيش أصلا، كحجز المعطيات التي يسلمها المتهم بمحض إرادته.

وعلى العموم يمكن من خلال التعريف الفقهي لكل من الحجز التقليدي والمرقمن، وكذا الأحكام القانونية التقليدية والمرقمنة، التي جاء بها المشرع الجزائري في هذا الصدد؛ أن نضع تعريفا يتناسب مع الحجز المرقمن، حيث نقول أنه: "وضع اليد على النطاق الافتراضي بالأساس والعناصر الرقمية المحدثة له بالتبعية، كنتيجة للمعاينة و/أو التفتيش المرقمنة –كأصل عام–، ما يمكن أن يفيد في فك خيوط القضية، على نحوٍ يقود لاتهام المشتبه فيه من عدمه أو إظهار الحقيقة بخصوص الدعوى المرفوعة ضد المتهم".

2. طبيعة الحجز المترتب عن المعاينة والتفتيش في جرائم الوسط الرقمي: يقوم الحجز المرقمن على الطبيعة المزدوجة نفسها المتصلة بالمعاينة والتفتيش المرقمنين –نفسها من حيث الازدواجية لا من حيث مضمون هذه الازدواجية–، كيف لا وهو الأثر المباشر لممارستهما في العديد من الأحيان. حيث يكتسي الحجز المرقمن الطابع المزدوج، الذي يجعل منه غير مقيدا بالتحري دون التحقيق –أو العكس–، إلا أن اللجوء إليه من الجهات المختصة به؛ يكون بصورة إلزامية عكس المعاينة والتفتيش المرقمنين.

سبق وأن بينا أن الحجز التقليدي؛ قابل للممارسة في كل من مرحة التحري وإجراءات التحقيق. حيث يلجأ إليه وكيل الجمهورية في إطار ممارسة المعاينة أو التفتيش –أو بصورة منفصلة عن الاثنين–، كما قد يعتمد عليه قاضي التحقيق وفق الطريقة نفسها، أثناء سير إجراءات التحقيق القضائي[2]. الأمر الذي أكد عليه المشرع بخصوص الحجز المرقمن؛ في إطار القانون 09-04 سابق الذكر، حيث ألحق ممارسة الحجز المرقمن؛ بالسلطة التي تمارس التفتيش[3]، وهي التي كان قد حددها بالقانون نفسه؛ في السلطات القضائية وضباط الشرطة القضائية، ما يفتح المجال للقول بإمكانية انجاز ذلك؛ في إطار كل من مرحلة التحري وإجراءات التحقيق[4].

---

[1] أنظر: سامي جلال فقي حسين، مرجع سابق، ص 263.

[2] **أنظر:** المادتان 3/44 و2/45 و4 و5 والمواد 2/47 و1/64 و84 و85؛ أمر رقم 66-155، مرجع سابق.

[3] **أنظر:** المادة 1/06؛ قانون رقم 09-04، مرجع سابق.

[4] **أنظر:** المادة 1/05؛ المرجع نفسه.

وأما بخصوص إلزامية الحجز المترتب عن المعاينة والتفتيش عموما؛ فالمشرع الذي اعتبرهما –المعاينة والتفتيش– بمثابة الإجراءين الاختياريين؛ هو نفسه الذي أقر ضمنياً بإلزامية الحجز المترتب عنهما. الأمر الذي يعد منطقياً، فاللجوء إلى المعاينة والتفتيش من عدمه؛ يتصل بالسلطة التقديرية لوكيل الجمهورية أو قاضي التحقيق –على حسب الحالة–، الذي لا يلجأ إلى ذلك إلا بعد تبين الضرورة الملحة، لكن بمجرد إصداره للإذن أو الأمر بذلك؛ يصبح حجز الأشياء –المادية والافتراضية– التي تفيد في فك خيوط القضية؛ أمرا إلزاميا على من ينفذه، وإلا زالت القيمة الإجرائية للمعاينة والتفتيش.

كما يفهم صراحةً من نص المشرع المتصل بالحجز المرقمن، أنه يلزم من يمارس التفتيش المرقمن، الذي يكتشف بمناسبة ذلك؛ معطيات مخزنة في منظومة معلوماتية، لها الفائدة في الكشف عن الجرائم أو مرتكبيها؛ بضرورة حجزها متصلة بالمنظومة المعلوماتية التي تحويها، أو على الأقل حجز هذه المعلومات منفصلةً عن منظومتها، لو تبين عدم ضرورة حجز المنظومة ككل[1]. الأمر الذي يتبين منه؛ أن الحجز المرقمن المتصل بالمعطيات المرقمنة هو إلزامي عند تنفيذ التفتيش المرقمن.

3. أهمية الحجز المترتب عن المعاينة والتفتيش في جرائم الوسط الرقمي: سبق وأن بينا الأهمية الكبيرة للمعاينة والتفتيش المرقمنين المتصلين بالتحري والتحقيق عموماً، وذلك رغم عدم إلزامية العمل بهما قانونا. مؤسسين ذلك بالخصوصية المعقدة للمسرح الجرمي الافتراضي، الذي لا يمكن الوصول إلى فك خيوطه إلا عبر اللجوء إلى هذين الإجراءين، وخاصةً انجازهما انطلاقا من الدعم التقني المبين سابقاً.

وعليه يمكن القول أنه للحجز المرقمن؛ الأهمية الإجرائية الكبيرة نفسها المتصلة بالمعاينة والتفتيش المرقمنين –وربما أكثر–، الأمر الذي نؤسس له بكون الحجز هو الأثر المباشر للمعاينة والتفتيش من جهة، ولكونه من جهة أخرى؛ يحمل الطابع الإلزامي الذي خصه به المشرع دون المعاينة والتفتيش، ويكرسه المنطق الجنائي السليم، سيما في إطار جرائم الوسط الرقمي والخصوصية ذات الصلة.

وعلى العموم للحجز المرقمن أهمية كبيرة من حيث إثبات جرائم الوسط الرقمي، خاصةً عبر المواجهة بالأدلة الرقمية المحصلة من المعاينة والتفتيش المرقمنين. ما يحول دون إفلات الجنات من المسؤولية الجنائية. كما أنه للمعطيات الرقمية المحجوزة؛ دوراً كبيراً في الكشف عن ملابسات الجريمة. فيمكن من خلال ذلك إثبات الجريمة وتحديد وقت ارتكابها، سيما بالوصول إلى الآثار الرقمية التي تشكل الدليل الجنائي الرقمي، ومنه استنتاج النية الإجرامية لدى الفاعل حتى قبل تحديد هويته. كما يمكن أيضا؛ تحديد الهوية الدقيقة للجناة، مع التعرف على الدوافع الإجرامية لديهم ودرجة خطورتهم[2].

---

[1] **أنظر:** المادة 1/06؛ قانون رقم 09-04، مرجع سابق.

[2] تقريباً لا فرق بين أهمية المعاينة والتفتيش المرقمنين من جهة، والحجز المرقمن من جهة أخرى. كيف لا وهو الأثر المباشر لممارستهما. حيث التفتيش مثلا يهدف للوصول إلى الدليل الرقمي، وهذا الأخير لايمكن تبيانه في العديد من الأحيان؛ إلا عبر حجز المعطيات اللازمة ومن ثم التعامل معها جنائيا؛ بفحصها وتحليلها وإعادة بناء القضية.

ثانيا: خصوصية الحجز المترتب عن المعاينة والتفتيش في جرائم الوسط الرقمي

وفق معادلة جنائية أساسية، أكتسب الحجز من الوسط الرقمي الدخيل على العلوم الجنائية؛ العديد من السمات الرقمية التي جعلته يمتاز بالخصوصية الافتراضية المعقدة نفسها، القائم عليها الوسط الرقمي ذاته، وكذلك الجرائم ذات الصلة. الأمر الذي يتعلق أساسا بالمعاينة والتفتيش المرقمنين، اللذان أبرزنا خصوصيتهما فيما سابق، وعلى العموم يمكن أن نحدد هذه الخصوصية التي اكتسبها الحجز بعد رقمنته، عبر التطرق إلى محله وتحديد القواعد الإجرائية التي ينفذ من خلالها، مع التأكيد أنها غير مجدية إذا لم تنجز في إطار قواعد فنية فرضتها الخصوصية الرقمية نفسها.

1. محل الحجز المترتب عن المعاينة والتفتيش في جرائم الوسط الرقمي: كلما فتح مجال الحديث الجنائي حول إجراءات التحري والتحقيق في جرائم الوسط الرقمي عموما؛ أثير إشكال محل هذه الإجراءات، الذي يتم الانقسام من خلاله حول إما اقتصاره على النطاق الافتراضي للوسط الرقمي، أو العناصر المادية التي تخلقه أو شموليته للاثنين معاً. فإشكال المحل الذي سبق طرحه بخصوص المعاينة والتفتيش المرقمنين؛ هو نفسه يعاد إبرازه في إطار الحجز المرقمن. ولو أنه لا يختلف عنها كثيرا، نظرا للارتباط الوثيق بين كل هذه الإجراءات.

يرى جانب من الفقه في هذا الإطار؛ أن الحجز ينصب حصراً على المكونات المادية –عناصر الوسط الرقمي–، التي لها وصف الشيء القابل للحجز المادي، وفق ما جاء به النص التشريعي التقليدي المتصل بالحجز عموما. حيث تكون قابلةً للحجز وفق هذا الرأي؛ الأسلاك ووحدة الإدخال والمودم ووحدة الذاكرة ووحدة التحكم...الخ. وما النطاق الافتراضي المتواجد داخلها إلى أحد مكوناتها الخفية، التي يمكن الوصول إليها عبر تشغيل العناصر الحاملة له بعد حجزها[1].

ويعتبر الرأي الفقهي نفسه؛ أن النطاق الافتراضي للوسط الرقمي؛ هو بمثابة الكيان المعنوي غير القابل للحجز. وذلك لعدم إمكانية تطابق الأحكام التشريعية المتصلة بالتفتيش والحجز التقليديين؛ مع المتطلبات الفنية الافتراضية للحجز المرقمن. ويؤسسون ذلك، بالقول أن عبارة "البحث عن الشيء"؛ تقتصر فقط على المال ذي الحيز المادي المحسوس، ما يقتضي إخراج النطاق الافتراضي غير المادي، من دائرة الحجز الذي يقصده المشرع[2].

إلا أن الأمر لم يقف عند الاقتصار على الحجز المادي، واستبعاد الحجز المرقمن المتصل بالنطاق الافتراضي للوسط الرقمي، بل ظهر اتجاه فقهي ثانٍ يقول بإمكانية تصور الحجز المرقمن، بصورة منفصلة عن نظيره المادي المتصل بعناصر الوسط الرقمي. عبر قولهم بأنه رغم اتصال الحجز بالمكونات

[1] **أنظر:** مفتاح بوبكر المطردي، مرجع سابق، ص 46.

[2] **أنظر:** نجاة بن مكي، مرجع سابق، ص 224.

المادية أصلا؛ إلا أنه يمكن أن يمتد ليشمل المعطيات الرقمية المجردة. الأمر الذي جسدته العديد من التشريعات المقارنة بخصوص إجراءات التحقيق القضائي، على غرار التشريع الكندي واليوناني والأمريكي –و.م.أ–[1].

وأما بخصوص القانون الجزائري، فنجد أن النص التقليدي للحجز؛ يكون قابلاً للتطبيق على الحجز المرقمن المنجز في إطار إجراءات التحقيق القضائي، وذلك لعدم تقييد المشرع لقاضي التحقيق بوسائل معينة، بل يمكنه أن يبحث عن الحقيقة بأي وسيلة يراها مناسبة مع احترام المشروعية اللازمة. إلا أنه يكون عاجزاً تماماً عن التطبيق في إطار مرحلة التحري، نظرا لتقيد وكيل الجمهورية بالمفهوم الضيق للحجز التقليدي، المنصب على الشيء المادي دون المعنوي، والذي سينصب أساساً على عناصر الوسط الرقمي ذات البعد المادي.

إلا أن المشرع الجزائري تدخل سنة 2009 بالقانون 09–04 سابق الذكر؛ ليقنن الحجز المرقمن المتصل بالنطاق الافتراضي للوسط الرقمي، بصورة منفصلة عن العناصر التي تحمله. الأمر تجاوز من خلاله الخلاف الفقهي المبين بنص صريح، يضم في طياته الحجز المرقمن بطبيعته المزدوجة، سواءً ذلك المنجز في إطار مرحلة التحري أو من خلال إجراءات التحقيق القضائي[2].

2. القواعد الإجرائية للحجز المترتب عن المعاينة والتفتيش في جرائم الوسط الرقمي: حدد المشرع بالقانون 09–04، العديد من القواعد الإجرائية الأساسية المتصلة بالحجز في جرائم الوسط الرقمي، التي تضل غير كافية، مع التأكيد على أنها تستكمل بالقواعد الفنية –التالية بالدراسة– التي تستعملها السلطة الممارسة لهذا الحجز، التي تتطور بديناميكية سريعة تتناسب مع التطور السريع للوسط الرقمي نفسه. وعلى العموم؛ تتمثل هذه القواعد الإجرائية الأساسية في تلك المتصلة بطريقة الحجز والأخرى المنصبة على الطريقة التي يتم التعامل من خلالها مع الحجوزات.

مكن المشرع الجهة الممارسة للتفتيش في المنظومة المعلوماتية المقصودة، التي تكتشف معطيات مخزنة تفيد في الكشف عن الجريمة أو مرتكبها؛ لأن تقوم بالحجز وفق طريقتين أساسيتين. فإما تمارس الحجز الفعلي، الذي قد ينصب مادياً على كل المنظومة المعلوماتية –عناصر الوسط الرقمي عموماً–، أو يقع افتراضيا عبر نسخ المعطيات محل البحث، وكذا المعطيات اللازمة لفهمها. على أن توضع بعد نسخها في دعامة تخزين رقمية، تكون قابلة للحجز المادي عبر وضعها في الأحراز[3].

---

[1] **أنظر:** نجاة بن مكي، مرجع سابق، ص 224. **وأنظر أيضا:** مفتاح بوبكر المطردي، مرجع سابق، ص 46.

[2] حيث نص على إمكانية حجز المعطيات الرقمية؛ بصورة منفصلة عن المنظومة التي تحويها. **أنظر في ذلك:** المادة 1/06؛ قانون رقم 09-04، مرجع سابق.

[3] **أنظر:** المادة 1/06؛ المرجع نفسه.

كما قد تتم ممارسة ما يسميه المشرع؛ بالحجز عن طريق منع الوصول إلى المعطيات. الذي يعد بمثابة الإجراء الاحتياطي غير القابل للإعمال إلا عند تحقق الاستحالة التقنية لتنفيذ الحجز الفعلي سابق الذكر. حيث يقوم القائم على الحجز في هذه الحالة؛ باستعمال التقنيات المناسبة لمنع الوصول و/أو نسخ المعطيات المتصلة بالمنظومة، الموضوعة تحت تصرف الأشخاص المرخص لهم بذلك[1].

وعلى العموم بين المشرع بالقانون 09-04 نفسه؛ العديد من الإجراءات التي يتبعها القائم على الحجز المرقمن. على غرار العمل على ضمان السرية والسلامة. حيث يجب في كل الأحوال العمل على ضمان سلامة المعطيات في المنظومة المعلوماتية محل إجراء الحجز المرقمن، مع إمكانية العمل على تشكيل هذه المعطيات أو إعادة تشكيلها رقميا، بغرض جعلها قابلة للاستغلال القضائي، بشرط عدم تسبب ذلك في المساس بمحتواها[2].

كذلك يمكن –دون إلزام– للقائم على الحجز المرقمن؛ بالعمل على ضمان السرية اللازمة بخصوص المعطيات المحجوزة ذات المحتوى المجرم. حيث يمكن أن يأمر باتخاذ الإجراءات التي تضمن عدم الاطلاع على المعطيات ذات المحتوى المجرم، كأن يكلف أي شخص له دراية وخبرة في التعامل مع الوسط الرقمي محل التعامل[3].

3. القواعد الفنية للحجز المترتب عن المعاينة والتفتيش في جرائم الوسط الرقمي: رجوعاً إلى القواعد الإجرائية المذكورة؛ نجد أن الحجز المادي المنصب على كل المنظومة المعلوماتية؛ لا يحتاج إلى قواعد فنية من طابع خاص وحساس، وإنما يكتفي القائم عليه بالحفاظ على التكامل المادي للمنظومة، وعدم تشغيلها إلا ممن له دراية وخبرة في التعامل مع الوسط الرقمي.

لكن الحجز الفعلي للمعطيات ونظيره المنطوي على المنع من الوصول؛ يتوجب العمل بالعديد من القواعد الفنية، التي لم يتطرق إليها المشرع نظرا لاستحالة حصرها والتعامل القانوني معها. حيث تعتري الصعوبة هذا النوع من الحجز المرقمن، سيما وأنه ينطوي على نطاق افتراضي معقد، قد لا يسمح باكتشاف المعلومة المبحوث عنها، كما قد يتسبب الباحث عنها في إتلافها قبل حجزها، أو بمناسبة القيام بذلك، أو حتى في مرحلة حفظها في الدعامة المادية المشكلة للحرز.

وعليه يرى العديد من الفقه الجنائي –انطلاقا من الدراسات التقنية–؛ أنه على ممارس الحجز المرقمن إتباع العديد من القواعد الفنية، التي تسهل عليه انجاز العملية بنجاح. حيث يجب عليه التعامل مع المجني عليه سيما إذا ما كانت له قدرات رقمية مقبولة، بحكم أنه الأعرف بنظامه المعلوماتي من غيره، واللجوء

[1] **أنظر:** المادة 07؛ قانون رقم 09-04، مرجع سابق.

[2] **أنظر:** المادة 2/06 و3؛ المرجع نفسه.

[3] **أنظر:** المادة 08؛ المرجع نفسه.

إلى العمل في الفريق المتكامل الذي يضم خبراء ومساعدين متخصصين يسهلون عليه العملية، خاصةً وأنهم يستعملون في ذلك العديد من القواعد الفنية اللازمة التي تعد مغيبة عن رجل القانون عموماً[1].

كما أن الحجز المرقمن والتحريز الذي يتلوه؛ يقوم على العديد من القواعد الأخرى. التي تراعي الخصوصية الافتراضية للمعطيات محل الحجز، سيما وأنها تتكون من ذبذبات وثنائية رقمية لها البعد المعقد صعب الفهم والتعامل، التي تكون مسجلة أو مخزنة في ذاكرة جهاز الإعلام الآلي. وعليه كل عمل تقني غير سليم قد يؤدي إلى إتلاف الدليل المبحوث عنه[2].

ومن خلال ذلك يتوجب على ممارس الحجز المرقمن؛ مراعاة القواعد الفنية، التي تلزمه بضرورة تحديد المادة المعلوماتية المراد حجزها، من خلال وضع عليها علامة مادية خاصة، مع نقلها إلى أقراص أو دعامات خارجية، التي توضع بدورها في علب مخصصة للحفظ. كما يقوم بتأمين الأنظمة المعلوماتية المحجوزة قبل تشغيلها، مع الالتزام بإتباع القواعد الخاصة بكيفية نقل الأحراز المعلوماتية، ومراعاة ظروف الحرارة والرطوبة المناسبة لتخزين هذه الأحراز، التي تختلف بطبيعتها عن نظيرتها المادية التقليدية. بالإضافة إلى ضرورة القيام بحجز كل الدعامات المادية والمعطيات التي تحويها، وعدم الاكتفاء بحجز النسخ الرقمية[3].

في ختام المبحث الثاني من هذا الفصل –والفصل الأول من الباب الثاني عموماً–؛ يمكن القول أن ولوج التجريم إلى الوسط الرقمي، الذي تبعه الولوج الإجرائي أيضا؛ أدى إلى تقسيم الأعمال الإجرائية إلى أساسية جوهرية وأخرى مساعدة، وذلك انطلاقا من الخصوصية الافتراضية المعقدة للدليل الرقمي الجنائي المبحوث عنه، عبر ممارسة إجراءات التحري والتحقيق في جرائم الوسط الرقمي. الأمر الذي تضمن منه هذا الفصل الأول؛ الدليل الرقمي الجنائي والأعمال الجوهرية المؤدية إلى استخراجه.

فبعد أن بينا الدليل الرقمي الجنائي، الذي اعتبرناه محور التحري والتحقيق في جرائم الوسط الرقمي؛ تطرقنا إلى الأعمال الجوهرية التي تتبعها الجهات المختصة للوصول إلى هذا الدليل، المنطوية أساسا على المعاينة والتفتيش المرقمنين، والأبعاد ذات الصلة، على غرار الدعم التقني والحجز المرقمن. وهو ما سنستكمله من خلال التطرق في الفصل الثاني والأخير من الدراسة؛ إلى باقي الإجراءات المساعدة على التحري والتحقيق في جرائم الوسط الرقمي.

---

[1] **أنظر:** وليد عاكوم، مرجع سابق، ص 07.

[2] **أنظر:** وردة شرف الدين، "المساعدة القضائية الدولية في مجال مكافحة جرائم الاتجار بالأشخاص والمرتكبة بواسطة تقنية المعلومات-وفقاً للاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، ورقة عمل مقدمة إلى المؤتمر الدولي الثاني حول جريمة الاتجار بالبشر-الأشكال الجديدة والتحديات الراهنة، مخبر الدولة والإجرام المنظم، كلية الحقوق والعلوم السياسية، جامعة البويرة، الجزائر، 16 و17 أفريل 2018، ص 14.

[3] **أنظر:** المرجع نفسه، ص 14 و15.

الفـــصل الثانـي

الإجراءات المساعدة علـى التحري والتحقيق في جرائم الوسط الرقمي

يتمثل الهدف الأساس من إجراءات التحري والتحقيق في جرائم الوسط الرقمي عموما؛ في البحث والتنقيب عن الدليل الرقمي الجنائي. الذي يختلف عن نظيره التقليدي نظرا لحمله للخصوصية الحديثة نفسها، التي يقوم عليها المسرح الجرمي الافتراضي محل هذه الإجراءات. الأمر الذي دفعنا للقول وإعادة التأكيد؛ على الاختلاف الكبير بين الإجراءات التقليدية المعروفة في إطار الجريمة التقليدية ونظيرتها الحديثة المعمول بها بخصوص جرائم الوسط الرقمي، حتى وان ظهر التوافق من خلال التسمية العامة للإجراء المتبع، كالتفتيش مثلا.

ولا يمكن الوصول إلى الدليل الرقمي كمحور أساسي لإجراءات التحري والتحقيق في جرائم الوسط الرقمي، ومنه إثبات الجريمة أو الوصول إلى الحقيقة القضائية المبحوث عنها؛ إلا عبر ممارسة الأعمال الجوهرية السابقة بالذكر، المنطوية على المعاينة والتفتيش المرقمنين، وأبعادهما التقنية والقانونية المنطوية على الدعم التقني والحجز. الأمر الذي سلمنا به وبينا أسبابه والأحكام الداعمة له؛ من خلال ما قدمناه في الفصل السابق بالدراسة.

إلا أن الضرورة العملية لإجراءات التحري والتحقيق في جرائم الوسط الرقمي –الناتجة عن الخصوصية الرقمية المعقدة للمسرح الجرمي الافتراضي–، قد تتطلب اللجوء زيادةً على المعاينة والتفتيش المرقمنين، بكل ما يتصل بهما من مضمون وأبعاد فنية وحجز مرقمن نصا وواقعا، وكذا اتصال مباشر بالدليل الرقمي؛ إلى العديد من الإجراءات الأخرى التي أضفينا عليها الوصف المساعد. حيث يجوز الاستعانة بإجراء أو أكثر من هذه الإجراءات المساعدة، إلى جانب المعاينة والتفتيش اللذان لا يمكن الاستغناء عنهما عمليا.

وتقوم هذه الإجراءات على الاختلاف والتنوع من حيث البعد القانوني والتقني، المتصل أساسا بالطبيعة القانونية من جهة ونظيرتها التقنية من جهة أخرى. حيث قد يتم اللجوء إلى إجراء أو أكثر من الإجراءات القانونية التقليدية قانونا ومضمونا، فنكون بصدد التعامل مع إجراءات غير رقمية وغير حديثة تشريعيا. كما يمكن أن يتم العمل بإجراء أو أكثر من الإجراءات القانونية الحديثة، سواءً تشريعا أو طبيعةً، فنصبح أمام التعامل مع إجراءات حديثة رقمية أو حديثة غير رقمية.

قد يكون لهذه الإجراءات المساعدة الدور الهام؛ في عملية الوصول إلى الدليل الرقمي خاصةً، وانجاز التحري والتحقيق في جرائم الوسط الرقمي عموما. حيث يتم اللجوء إلى واحد منها أو أكثر –الإجراءات المساعدة–؛ على حسب الحاجة التقنية والقانونية لذلك، بغض النظر عن الاختلاف في الطبيعة المبينة أعلاه. وعلى العموم يمكن أن نتطرق فيما يلي إلى هذه الإجراءات المساعدة، التي نقسمها على حسب ورودها التشريعي؛ إلى إجراءات تقليدية مساعدة(مبحث أول) وإجراءات أخرى تحمل الوصف الحديث المساعد(مبحث ثانٍ).

المبحث الأول

الإجراءات التقليدية المساعدة على التحري والتحقيق في جرائم الوسط الرقمي

قد يتم اللجوء من القائم على التحري والتحقيق في جرائم الوسط الرقمي عموما؛ إلى العديد من الإجراءات التقليدية، الممكن من خلالها التوصل إلى فك خيوط القضية، التي عجزت المعاينة والتفتيش المرقمنين عن الوصول إلى ذلك، أو تمكنت من تحقيق الفك الجزئي من دون التوصل إلى النتيجة النهائية المبحوث عنها، المنطوية على تبيان الحقيقة المنشودة.

وتتمثل هذه الإجراءات التقليدية؛ في تلك المعروفة والمعمول بها بخصوص التحري والتحقيق في الجريمة التقليدية. التي تنطوي على العديد من الأعمال والأوامر، المنصبة على الواقعة المجرمة بالأساس، وعلى أشخاصها بالتبعية، سيما المشتبه فيه والشهود والمتهم –أطراف الجريمة–. فإلى جانب المعاينة والتفتيش المرقمنين؛ يمكن اللجوء إلى واحدة أو أكثر من هذه الإجراءات التقليدية غير الرقمية، التي قد ترقمن كما قد يعمل بها على شكلها التقليدي دون رقمنة.

ورجوعا إلى الإجراءات التقليدية المتصلة بالتحري والتحقيق في الجريمة التقليدية، يمكن القول بعد فرزها والبحث فيها من حيث مدى تناسبها مع المتابعة المتصلة بجرائم الوسط الرقمي؛ أنها تنقسم إلى بعض الأعمال الإجرائية المساعدة على التحري والتحقيق في جرائم الوسط الرقمي(مطلب أول)، وأيضا بعض الأذون والأوامر الإجرائية ذات الدور المساعد نفسه(مطلب ثانٍ)[1].

المطلب الأول: الأعمال التقليدية المساعدة على التحري والتحقيق في جرائم الوسط الرقمي

تتعدد وتتنوع الأعمال الإجرائية التقليدية، التي يتم اللجوء إليها في العادة ضمن إطار إجراءات التحري والتحقيق. على غرار المعاينة والتفتيش والحجز والسماع والاستجواب وغيرها. الأمر الذي فصلنا فيه سابقا، بإضفاء الخصوصية على المعاينة والتفتيش المرقمنين عموماً، ونزيد عليه بإسباغ الطابع التقليدي على التنصت والتسرب المنجزين في إطار التحري والتحقيق في جرائم الوسط الرقمي، رغم أخذهما للوصف الحديث في أغلب الدراسات الفقهية الجنائية، سواءً المتصلة أو المنفصلة عن جرائم الوسط الرقمي[2].

---

[1] إلا أن هذه الإجراءات التقليدية المساعدة؛ لا تقود كأصل عام إلا لاستخلاص الدليل التقليدي المعروف كالاعتراف والتسجيل الصوتي التماثلي مثلا، الذي يدفع للقول بإثبات جرائم الوسط الرقمي بالدليل التقليدي. كما قد يكون وسيلة الوصول إلى الدليل الرقمي، كأن يعترف المتهم بالجريمة ويفصح عن المعطيات الرقمية الحاملة للدليل الرقمي، التي يسلمها للجهات المختصة فتحجزها.

[2] نؤسس لاعتبار التنصت والتسرب من الإجراءات التقليدية؛ بالعديد من الأسباب. حيث ينجزان في الوسط التقليدي المعروف، ولا يتصلان بالوسط الرقمي الحديث بأي شكل من الأشكال، فالتنصت لا يقع على المكالمات الرقمية، وإلا ما كان المشرع ليتدخل سنة 2009؛ ليشرع مراقبة الاتصالات الالكترونية -كما سنرى لاحقا-. كما أن المشرع نفسه أورد التنصت والتسرب؛ بتتميمه لقانون الإجراءات الجزائية سنة 2006 بالقانون 06-22، التاريخ الذي يعد قديما نوعا من جهة، =

نجد أن من أهم الأعمال الإجرائية التقليدية، المساعدة على التحري والتحقيق في جرائم الوسط الرقمي؛ تلك المتصلة بالأشخاص سواءً بطريقة مباشرة أو غير مباشرة. الأمر الذي ينطوي أساسا على التنصت والتسرب من جهة(فرع أول)، والسماع والاستجواب من جهة أخرى(فرع ثانٍ).

الفرع الأول: أعمال التنصت والتسرب المساعدة على التحري والتحقيق في جرائم الوسط الرقمي

وضع المشرع الجزائري أعمال التنصت والتسرب لأول مرة سنة 2006؛ بالمواد من 65 مكرر5 إلى 65 مكرر18 المتممة لقانون الإجراءات الجزائية، التي –أعمال التنصت والتسرب– وصفت فقها على أنها من الأعمال الحديثة المعمول بها في إطار كل من مرحلة التحري وإجراءات التحقيق القضائي. رغم أننا في إطار دراسة الحال؛ فصلنا في القول على أنها أعمال إجرائية تقليدية وفق التأسيس سابق الذكر.

وفي إطار دراستنا تبين لنا أنه للتنصت والتسرب؛ أهمية معتبرة من حيث المساعدة على التحري والتحقيق في جرائم الوسط الرقمي. الأمر الذي سنعمل على تبيانه من خلال التطرق إلى الأحكام القانونية التي يقوم عليها كل من التنصت(أولا) والتسرب(ثانيا)، مع التركيز على دورهما المساعد على التحري والتحقيق في جرائم الوسط الرقمي.

أولا: التنصت المساعد على التحري والتحقيق في جرائم الوسط الرقمي

يعد التنصت الذي نضمه المشرع بالمواد من 65مكرر5 إلى 65مكرر10 "ق.إ.ج"؛ بمثابة الإجراء التقليدي القريب فنيا إلى العديد من الإجراءات الحديثة، على غرار مراقبة الاتصالات الرقمية الذي سنبينه لاحقا، وذلك نظرا لتطلب تنفيذه وضع الترتيبات التقنية اللازمة والتعامل عن بعد مع الشخص المعني. وعلى العموم حتى نحدد المضمون العام للتنصت المساعد على التحري والتحقيق في جرائم الوسط الرقمي؛ يتوجب التطرق إلى تعريفه والجرائم الجائز إعماله في إطار متابعتها وكذا إجراءات انجازه.

1. تعريف التنصت المساعد على التحري والتحقيق في جرائم الوسط الرقمي: عبر المشرع عن التنصت في المواد المبينة أعلاه؛ باعتراض المراسلات وتسجيل الأصوات والتقاط الصور. كما يعبر عنه الفقه الجنائي سيما الجزائري؛ بالتصنت وليس التنصت كما عبرنا في دراستنا. الأمر الذي نؤسس له بإتباعنا التلخيص الفقهي لاعتراض المراسلات وتسجيل الأصوات والتقاط الصور في مصطلح واحد، إلا أننا نفضل التنصت بدلا عن التصنت، وذلك من منطبق لغوي محض، حيث نقول أنصت ولا نقول أصنت[1].

= وجاءت بعده العديد من الإجراءات التي نجدها أكثر حداثةً، على غرار الإجراءات الرقمية الواردة بالقانون 09-04. كما أن العديد من التشريعات المقارنة؛ قامت باستحداث أعمال إجرائية رقمية لتُعْمَلَ بدلاً عن التسرب، كإجراء "التحقيق بالاسم المستعار-L'enquête sous psydonaime"، المستحدث من المشرع الفرنسي -كما سنرى لاحقا-. وهو ما نعتبره بمثابة الاعتراف التشريعي الصريح بتقليدية وقصور إجراء التسرب، الذي تم الإبقاء عليه ليمارس في إطاره التقليدي المحض.

[1] **أنظر:** المعجم الوسيط-قاموس اللغة العربية المعاصر-قاموس عربي عربي-قاموس رقمي، "تعريف ومعنى تنصت"، د ت ن، تاريخ التصفح: 29 نوفمبر 2018، الرابط: https://www.almaany.com/ar/dict/ar-ar/تنصت/.

لم تتطرق الدراسات الجنائية الملخصة لأعمال اعتراض المراسلات وتسجيل الأصوات والتقاط الصور في مصطلح واحد؛ إلى تعريف التنصت عموما بغض النظر عن مكوناته الإجرائية. حيث تم الاكتفاء بتعريف كل نوع من أنواعه –التنصت– على حدا، انطلاقا من النص التشريعي المقرر للأحكام ذات الصلة.

فيعرف عمل اعتراض المراسلات وفق ذلك؛ على أنه: "اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية، ويقصد به أساسا التنصت التليفوني". كما يعرف عمل تسجيل الأصوات؛ بأنه: "وضع الترتيبات التقنية دون موافقة المعنيين، من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية". ويعرف عمل التقاط الصور أيضا؛ على أنه: "وضع الترتيبات التقنية دون موافقة المعنيين من أجل التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص"[1].

يتضح من خلال التعريفات السابقة؛ أن التنصت عموما لا يقع إلا على المحل غير الرقمي. فاعتراض المراسلات، يقصد به أساسا التنصت التليفوني المنجز عبر وسائل الاتصال السلكية واللاسلكية، الخارجة عن إطار الوسط الرقمي كما بينا سابقا. وتسجيل الأصوات؛ يكون باستعمال وسائل تسجيل في محل تواجد المعني بها، من دون أي اتصال شبكي، بالإضافة إلى أن التقاط الصور؛ يكون باستعمال وسائل التصوير دون اللجوء إلى الوسط الرقمي[2].

من خلال ما تم بيانه أعلاه؛ يمكن أن نصل إلى وضع تعريف عام يتصل بالتنصت التقليدي المعروف، والمكون من أعمال اعتراض المراسلات وتسجيل الأصوات والتقاط الصور. فنقول أنه: "لجوء جهات التحري والتحقيق إلى العمل بتقنيات غير رقمية كأصل عام، تسمح على وجه التحديد باعتراض المراسلات وتسجيل الأصوات والتقاط الصور، وذلك في إطار جرائم محددة حصرا وبإتباع إجراءات تتطلبها المشروعية اللازمة".

وأما التنصت المساعد على التحري والتحقيق في جرائم الوسط الرقمي، فرغم قيامه على المفهوم العام الوارد في التعريف التقليدي المقدم أعلاه؛ إلا أنه يتصف بكونه إجراءً مساعدا يتم اللجوء إليه عند الحاجة. ومنه يمكن أن نعرفه؛ على أنه: "لجوء جهات التحري والتحقيق في جرائم الوسط الرقمي إلى عمل أو أكثر من أعمال إجراء التنصت، كعمل مساعد غير رقمي تدعيما للمعاينة والتفتيش المرقمنين، في إطار بعض جرائم الوسط الرقمي المحددة حصرا، وبإتباع الإجراءات اللازمة قانونا".

---

[1] **أنظر:** محمد حزيط، مرجع سابق، ص 70. **وأنظر أيضا:** فضيل العيش، مرجع سابق، ص 125 و126.

[2] ولو أن تسجيل الأصوات والتقاط الصور؛ قد يخلق لنا معطيات رقمية، تصلح لأن تكون بمثابة الدليل الرقمي فيما بعد، نظرا لإمكانية تخزينها في جهاز الإعلام الآلي ومن في حكمه. إلا أنه يضل بمثابة الدليل الرقمي المصطنع من سلطات التحري والتحقيق، وليس من أثار جرائم الوسط الرقمي التي خلفها الجاني في المسرح الجرمي الافتراضي.

2. جرائم الوسط الرقمي الجائز التنصت بخصوص ممارسة التحري والتحقيق فيها: رجوعا إلى النص القانوني الواضع لإجراء التنصت بأعماله الثلاث؛ نجده يحدد على سبيل الحصر الجرائم الجائز التنصت بشأنها، إن في إطار مرحلة التحري أو بخصوص إجراءات التحقيق القضائي. الأمر الذي يقيد عمل وكيل الجمهوري وقاضي التحقيق –على حسب الحالة–، سيما وأنه قد تعترضه بعض القضايا المتشعبة –بغض النظر عن خطورة الجريمة–، التي لايمكن حلها إلى بإعمال التنصت.

وعلى العموم لايمكن لوكيل الجمهورية ضمن إطار ممارسة مرحلة البحث والتحري، أن يلجأ إلى عمل أو أكثر من أعمال إجراء التنصت عموما؛ إلا إذا تعلق الأمر بالجريمة المتلبس بها المكيفة على أنها جناية أو جنحة، أو بخصوص التحري عن جرائم المعاملة الخاصة –السابقة بالذكر– بالإضافة إلى جرائم الفساد، سواءً في حالة التلبس أو في الحالة العادية. وتتمثل هذه الجرائم عموما؛ في جرائم المخدرات والجريمة المنظمة العابرة للحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف، بالإضافة إلى جرائم الفساد[1].

كما لايمكن لقاضي التحقيق ضمن إطار ممارسة إجراءات التحقيق القضائي؛ أن يلجأ إلى إجراء التنصت عموما؛ إلا إذا ما تعلق الأمر بجرائم المعاملة الخاصة بالإضافة إلى جرائم الفساد المبينة أعلاه، من دون الجرائم المتلبس بها ولا باقي الجرائم الأخرى[2]. حيث تغل يده عن استعمال التنصت للبحث عن الحقيقة المتصلة بأي جريمة أخرى خارج قائمة جرائم المعاملة الخاصة والفساد، حتى وان أخذت وصف الجناية الخطيرة[3].

وأما بخصوص التنصت الممارس في إطار مكافحة جرائم الوسط الرقمي؛ فيمكن التطرق إليه من خلال التمييز بين جرائم المساس بأنظمة المعالجة الآلية للمعطيات من جهة، والجرائم التقليدية التي ترتكب عبر النطاق الافتراضي للوسط الرقمي أو يكون المسهل لارتكابها من جهة أخرى. حيث بخصوص جرائم المساس؛ يمكن اللجوء إلى التنصت في كل الأحوال، سواءً في إطار مرحلة التحري أو إجراءات التحقيق، كما أنه لا فرق بين الجريمة المتلبس بها والجريمة العادية. الأمر الذي له المعاملة نفسها بخصوص باقي جرائم المعاملة الخاصة وجرائم الفساد المتصلة بالوسط الرقمي –التي تعتبر من الجرائم التقليدية–، المتمثلة في جرائم المخدرات والجريمة المنظمة العابرة للحدود الوطنية وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف، علاوةً على جرائم الفساد.

---

[1] **أنظر:** المادة 65مكرر1/5؛ أمر رقم 66-155، مرجع سابق.

[2] **أنظر:** المادة 65مكرر4/5؛ المرجع نفسه.

[3] الأمر الذي نرى فيه؛ أنه منطقي بخصوص استبعاد الجرائم المتلبس بها، التي لا تحضا بالمعاملة الخاصة أثناء إجراءات التحقيق على عكس مرحلة التحري. الا أنه يعد قاصرا بخصوص تقييد قاضي التحقيق بجرائم محددة حصرا، من دون باقي الجرائم، سيما وأننا نتحدث عن قاضي تحقيق محايد، غير طرف في الدعوى العمومية من جهة، وأن البحث عن الحقيقة يتطلب استعماله لأي إجراء يراه مناسبا لإظهارها من جهة أخرى.

إلا أن الأمر يختلف بخصوص باقي الجرائم التقليدية. التي لايمكن لوكيل الجمهورية المختص ممارسة التنصت بخصوص التحري فيها؛ إلا في الجنايات والجنح المتلبس بها. كما يمنع على قاضي التحقيق المختص أيضا؛ اللجوء إليها في إطار إجراءات التحقيق القضائي الابتدائي، حتى وان تعلق الأمر بجريمة متشعبة ومن الخطورة بمكان[1].

3. إجراءات اللجوء إلى التنصت المساعد على التحري والتحقيق في جرائم الوسط الرقمي: حدد المشرع بالمواد من 65مكرر إلى 65مكرر10 "ق.إ.ج"؛ عددا من الإجراءات واجبة الإتباع بخصوص عمل التنصت عموما، ونظيره المساعد على التحري والتحقيق في جرائم الوسط الرقمي خصوصاً. حيث يمكن أن نستخلص من هذه المواد؛ الأحكام الإجرائية المتصلة بإذن التنصت وتنفيذه.

يتوجب لممارسة التنصت المساعد على التحري والتحقيق في جرائم الوسط الرقمي، بالإضافة إلى الاقتصار على الجرائم المبينة سابقا؛ أن يتم استصدار الإذن بذلك. الذي يتطلب توفر الضرورة الدافعة إليه، التي تتعلق بالتشعب الرقمي غير القابل للفك إلا باللجوء إلى التنصت المساعد[2]. كما أن المشرع حدد لهذا الإذن، في الإطار الإجرائي؛ أطرافا وبيانات شكلية ومدة انجاز. حيث يصدر الإذن عن وكيل الجمهورية المختص إلى ضابط الشرطة القضائية، في حال تعلق الأمر بمرحلة التحري، أو يصدر عن قاضي التحقيق المختص أيضا إلى ضابط الشرطة القضائية المنتدب، إذا كنا بصدد إجراءات التحقيق القضائي. وفي كل الأحوال، يتوجب أن يتضمن الإذن البيانات المتصلة بصفة هؤلاء الأطراف، مع التأكيد على بيانات الشخص محل التحري أو التحقيق[3].

ويتوجب أيضا أن يقوم الإذن على شكليات جوهرية، منطوية على التحديد الدقيق للعملية محل التنصت، والجرائم محل التحري أو التحقيق، والأماكن أو المساكن التي يمكن الدخول إليها في سبيل تنفيذه، والتقنيات غير الرقمية المستعملة في ذلك، على غرار تلك المتعلقة بالاتصالات السلكية واللاسلكية –الاتصال التليفوني مثلا–. كما أن الإذن بالتنصت؛ لا يصدر إلا للتنفيذ في مواعيد محددة قانونا، يبينها وكيل الجمهورية أو قاضي التحقيق في الإذن نفسه. حيث يتبين من نص قانون الإجراءات الجزائية؛ أنه لا يصدر لينفذ إلا في مدة أقصاها 04 أربعة أشهر. التي –المدة– سمح المشرع بإمكانية تجديدها لأكثر من مرة –كل مرة لا تتجاوز 04 أشهر–، إذا اقتضت ضرورة التحري أو التحقيق ذلك[4].

---

[1] الأمر الذي يقلل من فرص اللجوء إلى التنصت، كإجراء مساعد على التحري والتحقيق في جرائم الوسط الرقمي. حيث يقتصر على الجنايات والجنح المتلبس بها في مرحلة التحري، وجرائم المعاملة الخاصة عموما، التي من بينها جرائم المساس بأنظمة المعالجة الآلية للمعطيات، التي تتصل بالتحري والتحقيق معا.

[2] **أنظر:** المادة 65مكرر1/5؛ أمر رقم 66-155، مرجع سابق.

[3] **أنظر:** المادة 65مكرر1/5 و4 والمادة 65مكرر8؛ المرجع نفسه.

[4] **أنظر:** المادة 65مكرر7؛ المرجع نفسه.

بعد صدور إذن التنصت وفق الأحكام والشروط القانونية المبينة؛ يتم المرور إلى مرحلة التنفيذ في إطار ما تتطلبه القضية محل التحري أو التحقيق –في جرائم الوسط الرقمي–، والعمل الإجرائي الذي سيمارس، الدائر بين؛ اعتراض المراسلات و/أو تسجيل الأصوات و/أو التقاط الصور. حيث يقوم الشخص المكلف بوضع الترتيبات التقنية اللازمة لممارسة التنصت، بطريقة تضمن السرية اللازمة لإنجاح العملية، على غرار الاستغناء عن إعلام المعنيين ومن دون الحصول على رضاهم[1].

وتتطلب عملية وضع الترتيبات التقنية اللازمة لممارسة التنصت؛ بالضرورة الدخول إلى المحلات السكنية وغيرها. الأمر الذي ينجز سرا ومن دون علم صاحب المحل كما بينا أعلاه، بالإضافة إلى إمكانية الدخول إلى هذه الأماكن للغرض نفسه؛ في أي وقت يراه وكيل الجمهورية أو قاضي التحقيق –على حسب الحالة– مناسبا، وذلك دون التقيد بالمواقيت العامة المقررة للتفتيش، أي أن مواقيت وضع ترتيبات التنصت؛ تأخذ الحكم المفتوح المطلق غير المقيد[2].

بمجرد الانتهاء من كل الإجراءات السابقة بالذكر؛ يدخل إذن التنصت مرحلة التنفيذ الفعلي، المنطوي على استعمال الترتيبات التقنية المثبتة في أماكنها، للغرض الموضوعة من أجله، في إطار الاعتراض والتسجيل والالتقاط. الأمر الذي يتطلب العمل على تحرير محضر تنفيذ التنصت وما يترتب عن ذلك، بطريقة تفصل بين كل عملية والأخرى. مع التأكيد على ضرورة تأريخ هذا المحضر، وتحديد ساعات بداية ونهاية التنصت، وترجمة الكلام والعبارات التي قد ترد بغير اللغة العربية، وذلك بالاستعانة بمترجم يسخر وفق شروط المعرفة العلمية والسرية المهنية[3].

ثانيا: التسرب المساعد على التحري والتحقيق في جرائم الوسط الرقمي

بالإضافة إلى أعمال التنصت السابقة بالذكر والبيان؛ وضع المشرع أيضا ما يسمى بإجراء التسرب، الذي قد يتم اللجوء إليه من وكيل الجمهورية أو قاضي التحقيق؛ كإجراء مساعد على التحري والتحقيق في جرائم الوسط الرقمي، وذلك وفق البعد التقليدي المساعد نفسه المتصل بالتنصت. ولو أنه كإجراء فصلنا في كونه تقليدي؛ نجده قد تجاوزه الزمن والتطور الرقمي، بدليل استحداث العديد من التشريعات المقارنة؛ لأعمال إجرائية مشابهة له قائمة على البعد الرقمي الحديث. الأمر سنبين معالمه القانونية؛ بالتطرق إلى تعريف التسرب والجرائم الجائز إعماله في إطار متابعتها، بالإضافة إلى إجراءات انجازه.

---

[1] **أنظر:** المادة 65مكرر1/5 و2؛ أمر رقم 66-155، مرجع سابق.

[2] الأمر الذي يعد مفهوما، رغم تعارضه مع الأحكام العامة لدخول الأماكن من أجل تفتيشها، الواردة بالمادة 47 "ق.إ.ج". من منطلق أن إنجاح عملية التنصت يتطلب السرية الفائقة، والتقيد بالمواعيد قد يدفع لاكتشاف الأمر من صاحب المكان أو المتردد عليه. لذلك ربما ساعات الليل تعد الأفضل لوضع الترتيبات التقنية، نظرا للسكينة والفراغ اللذان يمتاز بهما. **أنظر في ذلك:** المادة 65مكرر2/5؛ المرجع نفسه.

[3] **أنظر:** المادة 65مكرر 9 و10؛ المرجع نفسه.

1. تعريف التسرب المساعد على التحري والتحقيق في جرائم الوسط الرقمي: نظم المشرع عمل التسرب بالمواد من 65مكرر11 إلى 65مكرر18 "ق.إ.ج"، المستحدثة سنة 2006، بالتميم القانوني نفسه المتصل بالتنصت السابق بالذكر. حيث استحدثه ووضع له أحكاما خاصة تتشابه في العديد من النقاط مع تلك المطبقة على التنصت، مع الاختلاف الواضح في مضموم كل منهما.

وعلى عكس العادة عمل المشرع في هذا الإطار؛ على تعريف التسرب كعمل إجرائي مستحدث –آن ذاك–، حيث يقصد –المشرع– من التسرب: "قيام ضابط أو عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه معهم أو شريك لهم أو خاف"[1].

يتبين من التعريف التشريعي المبين أعلاه؛ أنه إجراء يقوم على الحيلة في مراقبة الأشخاص المعنيين. حيث يركز الممارس للتسرب على عنصر الإيهام، الذي يتعامل به لكسب ثقة الأشخاص المتعامل معهم. الأمر الذي قد يفيد في العديد من الأحيان، سيما بخصوص الجنايات والجنح المتشعبة صعبة الإثبات. إلا أن ما يلاحظ على التعريف؛ كونه عبر بمصطلح المشتبه فيهم من جهة، وعناصر الشرطة القضائية –ضابط وعون– دون القاضي المختص من جهة أخرى، ما يدفع للقول بأنه عمل يتم اللجوء إليه في إطار مرحلة التحري دون إجراءات التحقيق القضائي، التي يتم التعامل في إطارها مع المتهم وليس المشتبه فيه. كما أنه لم يحدد الجرائم؛ التي يكون مسموحاً ممارسة التسرب في إطار متابعة أشخاصها.

لكن بتفحص باقي النصوص القانونية المتعلقة بالتسرب؛ نجد أن المشرع فتح المجال للجوء إليه في كل من مرحلة التحري وإجراءات التحقيق معاً، وما الاقتصار على مصطلح المشتبه فيه دون المتهم؛ سوا السهو الشكلي لا أكثر[2]. حيث بالرجوع إلى المادة الافتتاحية لإجراءات التسرب؛ نجدها تعبر بـــ "عندما تقتضي ضرورات التحري أو التحقيق...يجوز لوكيل الجمهورية أو قاضي التحقيق". كما أنه بين صراحةً؛ أنه –التسرب– إجراء يعمل بخصوص متابعة جرائم محددة حصرا[3].

وبغض النظر عما بيناه أعلاه؛ يظهر من خلال المصطلحات المستعملة في تعريف التسرب؛ أنه يمارس بأعمال مادية تقليدية لا علاقة لها بالوسط الرقمي الافتراضي. حيث ينجز بالإيهام، القائم على التواجد المادي مع المشتبه فيهم أو المتهمين، في الأمكنة المعتادين عليها، وحتى ممارسة الأعمال المادية المتعودين عليها. الأمر الذي يؤكد قولنا السابق بإضفاء الوصف التقليدي على إجراء التسرب.

---

[1] **أنظر:** المادة 65مكرر1/12؛ أمر رقم 66-155، مرجع سابق.

[2] ما يدفع للقول أن عدم تطرق المشرع بالتعريف للعديد من الإجراءات الجزائية؛ كان خياراً صائباً. حيث في المرات القليلة التي يعرف فيها إجراء معين؛ يقع في المحظور، ويخلق العديد من الإشكالات والتأويلات، ولعل تعريف التسرب أبرز دليل على ذلك.

[3] **أنظر:** المادة 65مكرر11؛ أمر رقم 66-155، المرجع نفسه.

إلا أننا قد نواجه في هذا الإطار؛ بالقول بإمكانية انجاز التسرب القائم على الإيهام؛ في الإطار الرقمي الافتراضي، فتتحول الأعمال من الماديات إلى المعنويات، مع الإبقاء على مضمون التسرب كما هو. الأمر الذي لنا فيه قول آخر، حيث نجد العديد من التشريعات المقارنة، على غرار المشرع الفرنسي؛ قد اعترف بقصر التسرب التقليدي، من خلال تشريعه لإجراء جديد –مع الإبقاء على التسرب ليعمل به في غير جرائم الوسط الرقمي– يتشابه مع التسرب من حيث المضمون، ولا يمارس إلا في المسرح الجرمي الافتراضي[1]. الإجراء الذي سمي بـــ "التحقيق تحت الاسم المستعار–L'enquête sous psydonaime"[2].

ونظرا لعدم تطرق المشرع إلى إجراء التحقيق تحت الاسم المستعار؛ يتوجب علينا التعامل مع الوضع، من خلال محاولة إسقاط أحكام التسرب على المسرح الجرمي الافتراضي، المميز بالخصوصية المعقدة. الأمر الذي من خلاله يمكن أن نعرف التسرب المساعد على التحري والتحقيق في جرائم الوسط الرقمي؛ بأنه: "لجوء جهات التحري والتحقيق في جرائم الوسط الرقمي، كعمل مساعد تدعيما للمعاينة والتفتيش المرقمنين؛ إلى مراقبة المشتبه فيهم أو المتهمين بارتكاب بعض جرائم الوسط الرقمي المحددة حصرا، وذلك عن طريق استعمال ضابط أو عون يوهمهم رقمياً بأنه فاعل معهم أو شريك أو خاف".

2. جرائم الوسط الرقمي الجائز التسرب بخصوص ممارسة التحري والتحقيق فيها: لم يفرق المشرع بين التنصت والتسرب، من حيث الجرائم التي ينجز في إطار متابعتها عموما. حيث حدد –المشرع– الجرائم نفسها التي يتقيد بها كل من وكيل الجمهورية في مرحلة التحري، وقاضي التحقيق في إجراءات التحقيق القضائي. وذلك عبر الإحالة للمادة 65مكرر5 –سابقة الذكر–، المبينة للجرائم الجائز انجاز التنصت في إطار متابعتها[3].

فوفق الطرح نفسه –مضموناً وتحليلاً– المبين سابقا بخصوص التنصت؛ يمكن القول بالإمكانية المطلقة للجوء إلى إجراء التسرب، بخصوص متابعة جرائم المساس بأنظمة المعالجة الآلية للمعطيات. وذلك نظرا لاعتبارها من المشرع؛ على أنها من بين جرائم المعاملة الخاصة. حيث يمكن في هذه الحالة؛ لكل من

---

[1] ولو أنه عمل يقوم على العديد من الأوجه الإجرائية، وما التسرب الرقمي إلا أحد هذه الأوجه. وهو الذي يعرف على أنه: "إجراء يسمح للمحقق المختص والمؤهل بالمشاركة عبر التبادل الرقمي المتصل بشبكة الاتصال الدولية، انطلاقا من استعمال اسم مستعار يخفي الهوية الحقيقية للمحقق". ويرى الفقه الجنائي الفرنسي؛ أنه يمتاز عن التسرب بكونه رقمي حديث الطبيعة من جهة، ومرن من حيث الاستعمال من جهة أخرى، نظرا لعدم الحاجة للموافقة المسبقة للقاضي المختص، حتى يمارس من الشرطة القضائية المختصة -الأمر الذي يعد أفضل حل لمواجهة سرعة التعامل الإجرامي في الوسط الرقمي-. **أنظر في ذلك:** QUEMENER Myriam, Le Droit Face à La Disruption Numérique, op.cit, p 155 et 156.

[2] إلا أنه إجراء رقمي حديث لايمكن اللجوء إليه؛ إلا بخصوص جرائم وسط رقمي محددة بالذات وعلى سبيل الحصر. فبخصوص جرائم المساس بأنظمة المعالجة الآلية للمعطيات؛ لا يُعْمَلُ إجراء التحقيق تحت الاسم المستعار؛ إلا لمواجهة جريمة الدخول والبقاء عن طريق الغش في منظومة معلوماتية موضوعة من طرف الدولة، التي ترتكب على شكل الجريمة المنظمة. وأما بخصوص الجريمة التقليدية المتصلة بالوسط الرقمي؛ فاكتفى المشرع الفرنسي ببعض الجرائم، المتمثلة في تلك الماسة بالأطفال، والاتجار بالأشخاص، والدعارة، والتجاوزات المتصلة بمواد الصحة، والإرهاب والجريمة المنظمة عموما. **أنظر في ذلك:** Idem, p 155.

[3] **أنظر:** المادة 65مكرر11؛ أمر رقم 66-155، مرجع سابق.

وكيل الجمهورية في إطار مرحلة التحري، وكذا قاضي التحقيق بخصوص إجراءات التحقيق؛ إصدار الإذن بممارسة وتنفيذ التسرب، مع التأكيد على عدم التباين بين الجريمة المتلبس بها والعادية في هذا الصدد.

كما أنه يمكن أيضا، لوكيل الجمهورية وقاضي التحقيق في إطار التحري والتحقيق –على حسب الحالة–؛ اللجوء إلى التسرب بخصوص متابعة باقي جرائم المعاملة الخاصة والفساد. وهي المنطوية كما بينا سابقا؛ على جرائم المخدرات والجريمة المنظمة العابرة للحدود الوطنية وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف، علاوةً على جرائم الفساد. مع التأكيد على منع المشرع لوكيل الجمهورية –دون قاضي التحقيق– اللجوء إلى إجراء التسرب بخصوص متابعة باقي الجرائم العادية؛ إلا إذا ما وصفت على أنها جنايات أو جنح متلبس بها.

3. إجراءات اللجوء إلى التسرب المساعد على التحري والتحقيق في جرائم الوسط الرقمي: بين المشرع بالمواد من 65مكرر1 إلى 65مكرر18 "ق.إ.ج"؛ العديد من الأحكام الإجرائية واجبة الإتباع بخصوص اللجوء إلى إجراء التسرب عموماً، والتسرب المساعد على التحري والتحقيق في جرائم الوسط الرقمي خصوصاً. التي –الأحكام الإجرائية– تقوم على قواعد، دائرة بين إذن التسرب أولا وتنفيذه ثانياً.

لا يمكن ممارسة التسرب المساعد على التحري والتحقيق في جرائم الوسط الرقمي، حتى وان توفر شرط الضرورة المتصل بمتابعة الجرائم المحددة حصرا؛ إلا انطلاقا من إذن مكتوب ومسبب يصدر وفق القواعد المحددة قانونا. حيث يصدر الإذن بالتسرب عن وكيل الجمهورية أو قاضي التحقيق، إلى ضابط الشرطة القضائية المرؤوس أو المناب على حسب الحالة. مع ضرورة تضمن الإذن نفسه؛ للعديد من البيانات التي تبين صفة أطرافه والشخص محل المتابعة. بالإضافة إلى تضمنه –الإذن–؛ للبيانات الدقيقة المتصلة بتحديد عملية التسرب، والجريمة أو الجرائم محل التحري أو التحقيق[1].

كما يتوجب أن يتضمن الإذن بالتسرب؛ البيانات التي تبرز مدة انجازه. حيث لا يصدر عن وكيل الجمهورية أو قاضي التحقيق –المختص–؛ إلا لينفذ في مواعيد محددة مسبقاً. التي حددها قانون الإجراءات في مدة أقصاها 04 أربعة أشهر، قابلة للتجديد لأكثر من مرة وفق الشروط والمواعيد نفسها؛ إذا اقتضت ضرورة التحري أو التحقيق ذلك[2].

بعد حصول الضابط على إذن التسرب وفق الإجراءات المبينة أعلاه؛ ينتقل إلى مرحلة التنفيذ –التنفيذ المادي التقليدي–، التي تتطلب منه لعب دور المنسق الذي يعهد بالعملية لضابط آخر أو عون منفذ.

---

[1] **أنظر:** المادة 65مكرر11 والمادة 65مكرر1/15 و2؛ أمر رقم 66-155، مرجع سابق.

[2] مع إمكانية توقيف ممارسة إجراء التسرب قبل انتهاء المدة المقررة قانونا، في أي وقت يراه وكيل الجمهورية أو قاضي التحقيق المصدر للإذن -على حسب الحالة- مناسبا لذلك. **أنظر في ذلك:** المادة 65مكرر3/15 و4؛ المرجع نفسه.

فيستعمل هذا الأخير –الضابط أو العون المنفذ–؛ هوية مستعارة تتناسب مع ملابسات الجريمة، حتى تسمح له بالاندماج الناجح في الجماعة الإجرامية محل التسرب[1].

وفي إطار تنفيذ التسرب؛ منح القانون للضابط أو العون المنفذ؛ الحق في القيام ببعض الأعمال التي تتشكل في الأصل من سلوكيات مجرمة قانونا. حيث يمكن للضابط أو العون المنفذ عند الضرورة دون أن يكون مسئولا جنائيا؛ التعامل مع الأموال والمنتوجات والوثائق والمعلومات المتحصل عليها من ارتكاب الجرائم أو المستعملة في ارتكابها، عبر اقتنائها أو حيازتها أو نقلها أو تسليمها أو إعطائها. كما يمكنه أيضا أن يقوم باستعمال أو وضع تحت تصرف مرتكبي هذه الجرائم؛ الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل أو التخزين أو الإيواء أو الحفظ أو الاتصال[2].

بعد تمكن الضابط أو العون المنفذ من التسرب الفعلي داخل الجماعة الإجرامية المقصودة؛ يقوم الضابط منسق العملية بإعداد ما سماه القانون بالتقرير –وليس محضر–، فيبين من خلاله المعاينة الحقيقية للجرائم محل التحري والتحقيق الصادر إذن التسرب بشأنها. من خلال التطرق إلى الملابسات ذات الصلة، وكل ما قد يفيد في إظهار الحقيقة المبحوث عنها[3].

يتضح من خلال الأحكام الإجرائية المبينة، أن التسرب المقصود من خلالها يقوم على البعد التقليدي المادي، حيث يؤدي إلى الاندماج والتعايش الماديين في إطار الجماعة الإجرامية. الأمر الذي يتأكد من خلال السلوكيات التي سمح القانون بارتكابها من الشخص المنفذ للتسرب، التي تظهر على أنها مادية تنجز في الوسط المادي الحقيقي، على غرار الاقتناء والحيازة والنقل والتخزين...الخ.

وأما التسرب المساعد على التحري والتحقيق في جرائم الوسط الرقمي؛ فنرى أنه ممكن الانجاز بطريقتين أساسيتين. حيث قد يمارس تقليديا بالطريقة نفسها المذكورة، عبر الاختراق الفعلي للجماعة الإجرامية التي ارتكبت الجريمة –الجائز التسرب في إطارها–، ما قد يترتب عنه الوصول إلى الدليل المادي أو تسهيل الوصول إلى الدليل الرقمي. كما يمكن أن يمارس بطريقة رقمية، فنقول أنه تسرب مرقمن ينجز بالاختراق الافتراضي الشبكي للجماعة الإجرامية، الذي يقود للوصول إلى الدليل الرقمي دون المادي، وهو ما يشبه التحقيق تحت الاسم المستعار المستعمل من المشرع الفرنسي المذكور سابقاً.

---

[1] ومنع المشرع تحت طائلة المسائلة الجنائية على الضابط أو العون المنفذ للتسرب؛ الكشف عن هويته الحقيقية على مدار المراحل الإجرائية. مقررا لذلك عقوبة قد تصل إلى 20 سنة حبس. إلا أنه يجوز سماع الضابط المنسق؛ كشاهد بهويته الحقيقية. **أنظر في ذلك:** المواد 65مكرر12/2 و65مكرر16 و65مكرر18؛ أمر رقم 66-155، مرجع سابق.

[2] كما يمكن للضابط أو العون المنفذ؛ أن يواصل القيام بالسلوكيات المبينة أعلاه ضامنا لأمنه وسلامته، حتى بعد انقضاء مدة التسرب المحددة في الإذن غير المجدد أو بعد الأمر بتوقيف التسرب أصلا، دون أن يكون مسئولا جزائيا، وذلك لمدة 04 أربعة أشهر قابلة للتجديد مرة واحدة فقط. ما يدفع للقول بقيام مسؤوليته الجزائية عن هذه السلوكيات، لو ارتكبها بعد انقضاء الـ 08 أشهر، أو المواصلة من دون الترخيص القانوني أصلا، حتى وان كان معرضا للخطر فعلا. **أنظر في ذلك:** المواد 65مكرر12/2 و65مكرر14 و65مكرر17؛ المرجع نفسه.

[3] **أنظر:** المادة 65مكرر13؛ المرجع نفسه.

الفرع الثاني: أعمال السماع والاستجواب المساعدة على التحري والتحقيق في جرائم الوسط الرقمي

زيادةً على أعمال التنصت والتسرب السابقين بالذكر؛ يمكن أن يتم اللجوء في إطار التحري والتحقيق المتصلين بجرائم الوسط الرقمي؛ إلى العديد من الأعمال الإجرائية التقليدية الأخرى، التي لها الدور المساعد للمعاينة والتفتيش المرقمنين. الأعمال التي حددناها في سماع واستجواب الأشخاص –على حسب الحالة–، التي قد يكون لها الأثر الفعال في الوصول إلى إثبات جرائم الوسط الرقمي، سواءً عبر الاكتفاء بالتصريحات، على غرار الشهادة والاستجواب، أو بتقفي الدليل الرقمي المستدل عنه انطلاقا من التصريحات المختلفة.

وعلى العموم نظم المشرع أعمال السماع المتصلة بالتحري والتحقيق من جهة، والاستجواب المقتصر على إجراءات التحقيق من جهة أخرى؛ بالعديد من النصوص التقليدية التي لا إشكال في إعمالها بخصوص متابعة جرائم الوسط الرقمي، مع احترام توفر التخصص الرقمي الحديث لدى القائم على ذلك. الأمر الذي سنبينه فيما يلي؛ عبر التطرق إلى السماع الممارس في إطار التحري والتحقيق في الجريمة عموما(أولا)، وكذا الاستجواب المساعد على التحقيق في الجريمة أيضا(ثانيا).

أولا: السماع المساعد على التحري والتحقيق في جرائم الوسط الرقمي

لا يختلف سماع الأشخاص بخصوص متابعة جريمة من جرائم الوسط الرقمي؛ عن السماع المتصل بالجريمة التقليدية، إلا من حيث التقنيات الحديثة التي يتوجب إتباعها، تماشيا مع الطبيعة الرقمية الافتراضية لمسرح الجريمة محل التحري والتحقيق. فيتوجب أن تتوفر في القائم على سماع الأشخاص؛ المعرفة الفنية اللازمة للتعامل مع الوسط الرقمي، حتى يتمكن من الاستفادة مما يتلقاه من تصريحات. الأمر الذي يمكن أن نتطرق إليه عبر تبيان السماع المساعد على التحري والتحقيق في الجريمة عموماً، على أن نستعرض بعد ذلك؛ الوجه الرقمي الحديث لهذا السماع المساعد، في إطار متابعة جرائم الوسط الرقمي على وجه الخصوص.

1. القواعد الإجرائية العامة للسماع الممارس للتحري والتحقيق في الجريمة: عمل المشرع في العديد من المواقع المختلفة المتصلة بقانون الإجراءات الجزائية؛ على تنظيم السماع التقليدي المعمول به في مواجهة الجريمة عموما، وجرائم الوسط الرقمي خاصةً. الأمر الذي يمكن أن نقسمه إلى قسمين، فنجعل من السماع الأول متصلا بمرحلة التحري، وهو الممارس من قبل ضابط الشرطة القضائية تحت إدارة وكيل الجمهورية، ونعتبر الثاني –السماع–؛ منجزا في إطار إجراءات التحقيق القضائي، من طرق قاضي التحقيق المختص أو ضابط الشرطة القضائية الذي ينوبه[1].

[1] رجوعاً إلى نصوص قانون الإجراءات الجزائية؛ نجد أن السماع؛ يقع عموما في إطار مرحلة التحري عند ممارسة الاستدلال، الذي يسمح بسماع الشاكي والمشتكى منه والشهود. كما قد يمارس بخصوص إجراءات التحقيق، عبر سماع الشهود والمدعى منه مدنيا. **أنظر في ذلك:** المادتان 3/12 و17 والمواد من 88 إلى 99؛ أمر رقم 66-155، مرجع سابق.

أ- عمل السماع الممارس للتحري عن الجريمة: لم يتطرق المشرع إلى السماع المساعد على التحري عموما؛ كعمل مستقل بأحكام خاصة منفصلة. وإنما يشير إلى ذلك ضمنيا أو صراحةً، عند تطرقه للأحكام العامة المتصلة بمهام الشرطة القضائية في إطار التحري الذي تنجزه. الأمر الذي من خلال تفحص نصوص قانون الإجراءات الجزائية؛ يمكن أن نقسمه إلى السماع المتصل بمهام جمع المعلومات عموما، وسماع الشاكي وكذا سماع المشتكى منه والشهود.

فتح المشرع بنص قانون الإجراءات الجزائية المجال أمام الشرطة القضائية؛ للقيام بمهام البحث والتحري عموما من خلال جمع الأدلة والبحث عن مرتكبي الجرائم محل المتابعة[1]. الأمر الذي يدخل ضمن إطاره سماع العديد من الأشخاص؛ في إطار تلقي الشكاوى والبلاغات –سماع الشاكي والمبلغ– من جهة، وسماع المشتكى منه والشهود من جهة أخرى.

وفي الإطار نفسه؛ ألزم المشرع ضباط الشرطة القضائية أن يحرروا محاضر بكل الأعمال التي يمارسونها[2]، التي نجد من أهمها محاضر سماع الأشخاص على اختلاف مراكزهم. بالإضافة إلى فتح مجال مهام أعوان الشرطة القضائية؛ ليتصل بمهام ضباط الشرطة القضائية، بصفتهم تابعين لهم ويأتمرون بأمرهم[3]، ومن أبرز هذه مهام الأعوان عموماً؛ نجد تحرير محاضر السماع.

رجع المشرع وأكد بنوع من التخصيص؛ أن من أهم اختصاصات ضباط الشرطة القضائية؛ سماع الأشخاص الذين يخبرون عن وقوع الجريمة. حيث أكد صراحةً على أنهم يتلقون الشكاوى والبلاغات، عن الجريمة المرتكبة، سواءً من قبل الضحية –الشاكي– أو غيره –المبلغ–. ولو أنه بالمادة نفسها؛ تحدث أيضا بأسلوب التعميم، فأسند مهام جمع الاستدلالات وإجراءات التحقيقات الابتدائية، المبينة أعلاه[4]. الأمر الذي يدفع للقول؛ بإمكانية سماع بالإضافة إلى الشاكي أو المبلغ؛ كل من المشتكى منه والشهود.

وأكد المشرع أيضا بنصوص أخرى أكثر دقة وتخصيصاً؛ على إمكانية سماع كل من المشتبه فيه والشهود في محاضر. على غرار قيام ضباط الشرطة القضائية؛ بسماع المشتبه فيه الذي يكون موقوفاً للنظر، وفق الشروط القانونية المحددة لذلك[5]. بالإضافة إلى جوازية سماع الشهود، الذين يمكن أن تكون تصريحاتهم مفيدة في التحري عن الجريمة المقصودة. وهو ما فتحه المشرع على مصراعيه، بإعطاء ضابط الشرطة القضائية؛ الحق في توجيه نداء للجمهور قصد تلقي المعلومات والشهادات المفيدة[6].

---

[1] **أنظر:** المادتان 12/ 3 و1/17؛ أمر رقم 66-155، مرجع سابق.

[2] **أنظر:** المادة 18؛ المرجع نفسه.

[3] **أنظر:** المادة 20؛ المرجع نفسه.

[4] **أنظر:** المادة 1/17؛ المرجع نفسه.

[5] **أنظر:** المادة 1/52؛ المرجع نفسه.

[6] **أنظر:** المادة 5/17؛ المرجع نفسه.

ب- عمل السماع الممارس للتحقيق في الجريمة: على العكس من السماع المساعد على التحري، نجد نظيره المتصل بالتحقيق القضائي؛ قد تطرق إليه المشرع بنوع من التفصيل والخصوصية في نصوص محددة ومنفصلة، وكذلك الفقه الجنائي الذي وصف وحلل هذه النصوص. الأمر الذي نبينه من خلال التطرق إلى هذا السماع، المتصل أساسا بسماع أقوال الشهود -أو الشهادة- وسماع المدعى المدني والمدعي منه مدنيا قبل اتهامه.

ب-1/ سماع الشهود: نضم المشرع الشهادة[1] المنجزة في إطار مرحلة التحقيق القضائي الابتدائي؛ بالمواد من 88 إلى 99 "ق.إ.ج"[2]. حيث يستمع قاضي التحقيق أو ضابط الشرطة القضائية المناب عنه؛ لأقوال الشهود[3] التي تحرر في محاضر ترفق بملف القضية. وعلى العموم يقوم عمل سماع الشهود على العديد من الأحكام القانونية، المتمثلة أساسا في تلك المتصلة بالشاهد ونظيرتها المتعلقة بالشهادة.

وضع المشرع العديد من الأحكام والقواعد الإجرائية ذات الصلة بالشاهد، التي يصفها الفقه الجنائي على أنها الالتزامات الواقعة على عاتقه، وتقود في الأخير إلى سماع شهادته. حيث يلتزم أساسا بالحضور أمام قاضي التحقيق بمجرد استدعائه، وإلا كان محلا للإحضار الجبري مع الحكم عليه بغرامة مالية تدور بين 200 و2000 دج. وفي كل الأحوال بمجرد حضور الشاهد أمام قاضي التحقيق أو الضابط الذي ينوبه؛ يكون ملزما بأداء اليمين القانونية إذا طلبها من يسمعه -مع التأكيد على وجود حالات لا يؤدي فيها الشاهد اليمين-، وإلا يكون محلا لعقوبة الغرامة نفسها[4].

وفق نهج تسلسلي قانوني منطقي، يتوجب على الشاهد الذي حضر وأدى اليمين؛ أن يدلي بالشهادة التي استدعي من أجل سماعها. حيث يلزمه المشرع بذلك، ويضعه الأمر تحت طائلة عقوبة الغرامة نفسها المبينة أعلاه. بالإضافة إلى إمكانية تحمله للمسؤولية الجنائية، لو صرح علانية بأنه يعرف مرتكب الجنحة أو الجناية، ومع ذلك يرفض الإدلاء بالشهادة. حيث يجوز لقاضي التحقيق؛ أن يحيله أمام محكمة الجنح في جريمة قد تصل عقوبتها إلى حد الـــ 01 سنة حبس والـــ 000 10 دج[5].

---

[1] كما أنه تطرق إلى الشهادة التي تكون أمام جهات الحكم؛ في موقع آخر منطوي على المواد من 220 إلى 234 "ق.إ.ج".

[2] الشهادة التي تعرف؛ على أنها: "معلومات يدلي بها شخص من غير أطراف الدعوى العمومية، يرتئي قاضي التحقيق سماعه كشاهد، سواءً بطلب من الأطراف أو من تلقاء نفسه". **أنظر في ذلك:** ناصر حمودي، (قانون الإجراءات الجزائية الجزائري)، مرجع سابق، ص 225.

[3] يعرف الفقه الشاهد؛ على أنه: "كل شخص يرى قاضي التحقيق من سماع شهادته فائدة لإظهار الحقيقة، ولا يشترط فيه أن يكون شاهد عيان، بل يكفي أن تكون شهادته مفيدة لإظهار الحقيقة". **أنظر في ذلك:** أحسن بوسقيعة، التحقيق القضائي، مرجع سابق، ص 76 و77.

[4] ويمكن إعفاء الشاهد من عقوبة الغرامة، في حال حضر فيما بعد وبرر سبب عدم الحضور. كما قد يسمع في مكان تواجده، إذا تعذر عليه الحضور لأي سبب مجدي كان، مع البحث في عدم كذبه واختلاقه للعذر، وإلا كان محلا لعقوبة الغرامة نفسها. **أنظر في ذلك:** المواد 1/89 و97 و99؛ أمر رقم 66-155، مرجع سابق.

[5] **أنظر:** المواد 1/89 و3/97 و98؛ المرجع نفسه.

زيادةً عن الإجراءات السابقة بالذكر، المتعلقة بالشاهد من حيث الالتزامات القانونية القائمة على عاتقه؛ بين المشرع العديد من الإجراءات القانونية المتعلقة بالشهادة نفسها، التي تبين الأعمال المتبعة من سامع الشهادة –قاضي تحقيق أو ضابط الشرطة القضائية الذي ينوبه–. فبعد أن يدلي الشاهد بالمعلومات المتعلقة بهويته من اسم ولقب وسن ومحل إقامة ومهنة وعلاقته بأطراف الدعويين...الخ؛ يشرع في تأدية الشهادة التي يدونها كاتب التحقيق، والتي تكون كأصل عام باللغة العربية ومن شخص سليم، وفي حالة العكس يتم استدعاء مترجم أو مساعد صحي أو غيره لفهم الشهادة[1].

وبعد أن يدلي الشاهد بالشهادة التي يريد؛ يتوجب عليه التوقيع على محضر سماع الأقوال، الذي يوقع عليه أيضا كل من قاضي التحقيق والكاتب والمترجم وأي شخص شارك في عملية السماع. على أن يدعى الشاهد إلى إعادة تلاوة فحوى المحضر المتضمن الشهادة التي أدلى بها، وفي حال الامتناع عن التوقيع أو حدوث أي مانع؛ يتم التنويه في المحضر عن هذا الامتناع[2].

ب–2/ سماع المدعي المدني والمدعى منه مدنيا: بالإضافة إلى سماع الأشخاص المتصل بالشهادة عموما، يمكن لقاضي التحقيق أو من ينوبه قانونا؛ أن يسمع أشخاص آخرين إن كطرف في الدعوى المدنية التبعية، أو كشاهد من نوع خاص. حيث يمكن سماع المدعي المدني –كطرف في الدعوى المدنية– أثناء إجراءات التحقيق، وذلك وفق ضمانات خاصة لا يتمتع بها الشاهد عند سماعه، وتكاد تفوق حتى تلك المقررة للمتهم. فيمكنه الاستعانة بمحامي أثناء السماع، وهو ما لا يحضا به الشاهد، كما لا يجوز سماعه إلا بحضور محاميه أو بعد دعوته قانونا[3]. الأمر الذي يدفعنا للقول بأنه يتمتع بضمانات المتهم، رغم خضوعه للسماع كشاهد وليس للاستجواب كمتهم.

ويمكن أيضا أن يتم سماع المدعى منه بالشكوى المصحوبة بالادعاء المدني؛ كشاهد من نوع خاص. حيث ألزم القانون قاضي التحقيق؛ بأن يسمع المدعى منه مدنيا عند أول مرة كشاهد وليس كمتهم، الأمر الذي ينجز وفق الإجراءات نفسها المتعلقة بالشهادة المبينة سابقا. إلا أن القانون نفسه؛ منح الحق لهذا الشخص في رفض سماعه كشاهد[4]، وفرض على قاضي التحقيق أن يحيطه علما بهذا الحق بعد إحاطته بحيثيات الشكوى المقدمة ضده. وفي حال تمسك المدعى منه مدنيا برفض سماعه كشاهد، لايمكن لقاضي التحقيق استجوابه إلا بعد توجيه الاتهام الرسمي له[5].

---

[1] **أنظر:** المواد من 90 إلى 93؛ أمر رقم 66-155، مرجع سابق.

[2] **أنظر:** المادة 94؛ المرجع نفسه.

[3] **أنظر:** المواد من 103 إلى 105؛ المرجع نفسه. **وأنظر أيضا:** أحسن بوسقيعة، التحقيق القضائي، مرجع سابق، ص 75 و76.

[4] الحق الذي يستعمله المدعى عليه مدنيا؛ ليستفيد من الضمانات القانونية المقررة للمتهم دون الشاهد، ولتجنب أداء اليمين الذي قد يجعله شاهدا على نفسه. **أنظر في ذلك:** ناصر حمودي، (قانون الإجراءات الجزائية الجزائري)، مرجع سابق، 226.

[5] **أنظر:** المادة 1/89؛ أمر رقم 66-155، المرجع نفسه.

2. الوجه الرقمي الحديث للسماع المساعد على التحري والتحقيق في جرائم الوسط الرقمي: مبدئياً لا نجد أي فرق قانوني عام؛ بين السماع في مواجهة الجريمة التقليدية، ونظيره المتصل بجرائم الوسط الرقمي؛ إلا من حيث ما تتطلبه الخصوصية الرقمية الحديثة. حيث تطبق الأحكام القانونية نفسها المذكورة سابقا؛ على السماع المساعد على التحري والتحقيق في جرائم الوسط الرقمي. إلا أن الخصوصية الرقمية للمسرح الجرمي الافتراضي؛ أنتجت لنا بعض القواعد الفنية –فنية لا قانونية– واجبة الإتباع، يمكن من خلالها أن نبين تعريف هذا النوع من السماع الحديث، والخصوصية الفنية المتصلة بانجازه.

أ- تعريف عمل السماع المساعد على التحري والتحقيق في جرائم الوسط الرقمي: لم يتطرق لا المشرع ولا الفقه الجنائي؛ إلى تعريف السماع المساعد على التحري والتحقيق في جرائم الوسط الرقمي، وفق الطريقة التي اعتمدناها في إطار دراستنا. حيث يتم الرجوع في العادة؛ إلى الشهادة التقليدية من حيث موضوعها ومؤديها، دون التعريج على باقي الأشخاص الممكن سماعهم –كالمدعي المدني والمدعى عليه مدنيا–، ولا على البعد الرقمي المختلف فنيا عن الشهادة التقليدية خاصةً والسماع التقليدي عموما.

وعلى العموم نجد بعض التعريفات الفقهية، التي اقتصرت على تبيان المقصود من الشاهد في جرائم الوسط الرقمي، من خلال إسقاط الأحكام القانونية التقليدية على الخصوصية الرقمية. فيعرفون الشاهد في جرائم الوسط الرقمي؛ على أنه: "ذلك الشخص الفني صاحب الخبرة والتخصص في تقنية وعلوم الحاسب الآلي، والذي تكون لديه معلومات جوهرية أو هامة لازمة للدخول –الولوج– في نظام المعالجة الآلية للبيانات إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة داخله"[1].

يتضح أن التعريف المذكور أعلاه؛ يشوبه العديد من القصور. حيث من جهة يقتصر على الشاهد دون باقي الأشخاص الممكن سماعهم، ومن جهة أخرى يتطلب القدرة الفنية في الشاهد، وكأنه سيلعب دور الخبير لا الشاهد. الأمر الذي يهمل صفة الشخص محل السماع بالطريقة التقليدية، الذي قد تساعد تصريحاته في الوصول إلى الدليل الرقمي، كأن تساعد تصريحات المدعي المدني؛ في الوصول إلى تحديد كلمة السر الملعوب فيها مثلا.

يمكن من خلال ما بيناه أعلاه؛ أن نقترح تعريف جامع يشمل كل أنواع السماع المساعد على التحري والتحقيق في جرائم الوسط الرقمي. حيث نقول أنه: "تلقي أجهزة التحري والتحقيق في جرائم الوسط الرقمي؛ لتصريحات وشهادات من أشخاص لا علاقة لهم بالدعوى العمومية –شاهد ومدعي مدني ومدعى منه مدنيا قبل اتهامه–، قد تؤدي إلى جمع الاستدلالات اللازمة أو تفيد في الوصول للحقيق المبحوث عنها–على حسب الحالة–، وينجز هذا التلقي بالإجراءات التقليدية المعروفة، مع ضرورة التقيد ببعض الالتزامات الفنية الحديثة".

[1] **أنظر:** حازم محمد حنفي، مرجع سابق، ص 72.

ب- الخصوصية الفنية في عمل السماع المساعد على التحري والتحقيق في جرائم الوسط الرقمي:
انطلاقا من التعريف الذي وضعناه بخصوص السماع المساعد على التحري والتحقيق في جرائم الوسط الرقمي؛ يمكن القول أن هذا النوع من السماع الحديث؛ يقوم قانونا على الإجراءات التقليدية المعرفة والمبينة سابقا. إلا أن خصوصية المسرح الجرمي الافتراض، جعلته يكتب بعض الخصوصية نفسها من خلال قيامه على مجموعة التزامات فنية. وعليه نقول أن الشخص المسموع قد يكون عاديا وفق الأحكام التقليدية –شاهد عادي ومدعي مدني ومدعى منه مدنيا قبل الاتهام–، كما قد يكون خاصا له دراية فنية معتبرة –شاهد فني فقط–، الذي نركز عليه في هذا الإطار من حيث ذكر بعض أنواعه والتزاماته.

تبين العديد من الدراسات الجنائية القائمة على نظيرتها الفنية؛ أن الشاهد الفني يتعدد ويتنوع بحسب عدد الطوائف القائم عليها. فقد يكون عبارة عن مشغل للجهاز –جهاز الإعلام الآلي ومن في حكمه–، كما قد يكون محلل رقمي أو مبرمج أو مهندس صيانة واتصالات بالإضافة إلى إمكانية أن يكون مديرا للنظم[1]. مع التأكيد على إمكانية اللجوء إلى غير هؤلاء، ليسمع لهم في إطار الشهادة المساعدة على التحري والتحقيق في جرائم الوسط الرقمي، مع مراعاة التطور الرقمي السريع الذي قد يفرض طوائف فنية أخرى في أي وقت.

وفي الإطار نفسه نؤكد على أن الشاهد الفني المبين أعلاه، الذي يسمع له في إطار السماع المساعد على التحري والتحقيق في جرائم الوسط الرقمي؛ يقوم بممارسة ذلك وفق التزامات فنية أساسية لا يمكن تصور تخلفها. حيث يلتزم أساسا بما يسمى بالإعلام، الذي يدفعه للإدلاء بالشهادة في جرائم الوسط الرقمي متى كانت له معلومات مفيدة، سيما وأننا نتحدث عن جرائم معقدة وصعبة الإثبات. كما أن هذا الالتزام يدل على التعاون ويحقق التوازن الإجرائي المطلوب من حيث المعطيات، بين مرتادي الوسط الرقمي والشهود وأجهزة التحري والتحقيق[2].

كما أنه بالإضافة إلى الالتزام العام بتقديم الشهادة؛ يتوجب أن تتضمن الشهادة الفنية العديد من النقاط الأساسية. على غرار المعلومات الجوهرية، التي يوجب أن تصل إلى علم أجهزة التحري والتحقيق في جرائم الوسط الرقمي، كالمعطيات الرقمية والملفات المطبوعة وكلمات المرور والشفرات...الخ. ويلتزم الشاهد الفني أيضا؛ أن يتقيد ببعض المواصفات الأساسية المتصلة بالشهادة التي يقدمها، كأن تكون شهادته بسيطة ومفهومة لا تدع مجالا للتأويل الفني ولا القانوني، وأن يكون مضمون التصريحات والمساعدات الفنية دقيقا ومحددا، بالإضافة إلى تطلب التزام آخر مأخوذ من الشهادة التقليدية أصلا، المنطوي أساسا على الصدق والأمانة في الشاهد[3].

---

[1] **أنظر:** حازم محمد حنفي، مرجع سابق، ص 72. **وأنظر أيضا:** وردة شرف الدين، مرجع سابق، ص 248 و249.

[2] **أنظر:** وردة شرف الدين، المرجع نفسه، ص ص 250-252.

[3] **أنظر:** المرجع نفسه، ص 254 و255.

ثانيا: الاستجواب المساعد على التحقيق في جرائم الوسط الرقمي

يعد الاستجواب من أهم الأعمال الإجرائية التقليدية، التي تستعمل في مواجهة الشخص المعني بعد توجيه الاتهام الرسمي له. حيث على عكس سماع الأشخاص، الذي قلنا بإمكانية ممارسته في كل من مرحلة التحري وإجراءات التحقيق؛ يقتصر اللجوء إلى عمل الاستجواب على مرحلة التحقيق القضائي فقط[1]. وهو ما سنبينه بنوع من التفصيل فيما يلي من الدراسة، من خلال التطرق إلى القواعد الإجرائية العامة لعمل الاستجواب الممارس للتحقيق في الجريمة عموماً، ومن ثم تبيان الخصوصية التي اكتسبها هذا الاستجواب بعد أن أصبح يستعمل في مواجهة المتهم الرقمي.

1. القواعد الإجرائية العامة للاستجواب الممارس للتحقيق في الجريمة: نظم المشرع عمل الاستجواب والإجراءات التي يمارس من خلالها؛ بموجب المواد من 100 إلى 108 "ق.إ.ج"[2]. المواد التي تحوي قواعد إجرائية عامة تقليدية، تمارس في مواجهة المتهم التقليدي، غير أنه لا يوجد ما يمنع أن تطبق على المتهم الرقمي أيضا، نظرا لكون المشرع لا يفرق في هذا الإطار؛ بين أنواع الجناة وصفاتهم العلمية والفنية. وعلى العموم يمكن من خلال هذه النصوص القانونية والدراسات الفقهية ذات الصلة؛ أن نبين تعريف عمل الاستجواب التقليدي وإجراءاته المقررة قانوناً.

أ- تعريف عمل الاستجواب الممارس للتحقيق في الجريمة: لم يتطرق المشرع بالمواد المذكورة أعلاه كعادته؛ إلى تعريف الاستجواب الممارس من قاضي التحقيق في مواجهة المتهم. إلا أن الفقه الجنائي -سيما الجزائري-؛ حاول الخوض في ذلك من خلال طرح العديد من التعريفات المتصلة بالاستجواب، الذي يعتبر عموما؛ على أنه: "مناقشة المتهم بالتهمة الموجهة إليه ومواجهته بالأدلة القائمة ضده، مع الإبقاء على حقه في الامتناع عن الرد، من دون اعتبار ذلك قرينة ضده"[3].

يمكن من خلال التعريف المبين أعلاه، والنصوص القانونية المبينة لإجراءات عمل الاستجواب؛ القول بأنه عمل قد يقود إلى الحسم القضائي، من خلال اعتراف المتهم بالتهم الموجهة إليه بعد انهياره أمام الأدلة القائمة التي يواجه بها، خاصةً وأنه يكون أمام قاضٍ محايد يتمثل في قاضي التحقيق، الذي يفيد المتهم بالعديد من الضمانات القانونية، انطلاقا من اعتباره القاضي الباحث عن الحقيقة المنطوية على أدلة الاتهام والنفي معاً.

---

[1] الاستجواب الذي يمكن كاستثناء؛ أن يمارسه وكيل الجمهورية في إطار مرحلة التحري قبل اتهام المشتبه فيه. وذلك بخصوص مواجهة الجريمة المتلبس بها دون سواها. حيث يجوز لوكيل الجمهورية؛ أن يصدر أمرا بإحضار المشتبه فيه لاستجوابه. **أنظر في ذلك:** المادة 58؛ أمر رقم 66-155، مرجع سابق.

[2] غير أنها مواد قانونية تتعلق بالاستجواب الممارس من قبل قاضي التحقيق، في إطار ممارسته للدرجة الأولى من التحقيق القضائي الابتدائي. مع التأكيد على إمكانية اللجوء إليه في باقي إجراءات التحقيق القضائي، سيما بخصوص التحقيق القضائي النهائي الذي يمارسه قاضي الموضوع في الجلسة. **أنظر في ذلك:** المادة 353؛ المرجع نفسه.

[3] **أنظر:** محمد حزيط، مرجع سابق، ص 101.

ب- إجراءات سير عمل الاستجواب الممارس للتحقيق في الجريمة: بين المشرع بالمواد من 100 إلى 108 "ق.إ.ج" سابقة الذكر؛ العديد من الإجراءات التي يتوجب على قاضي التحقيق إتباعها أثناء ممارسته لعمل الاستجواب في مواجهة المتهم، سيما تلك المتعلقة بالضمانات الأساسية الممنوحة له –المتهم- قانونا. حيث يفهم من خلال ذلك؛ أن المشرع قسم عمل الاستجواب إلى مرحلين أساسيتين، تنطوي الأولى على الاستجواب عند المثول الأول، وتتعلق الثانية بالاستجواب في الموضوع[1].

يقوم قاضي التحقيق في إطار الاستجواب عند المثول الأول؛ باستجواب المتهم الماثل أمامه لأول مرة في كل ما يتعلق به شخصيا وبالتهمة المنسوبة إليه من دون مناقشة، الأمر الذي يعد بمثابة سؤال وإعلام أكثر منه استجواب. حيث يسأل قاضي التحقيق المتهم عن كل ما يتعلق بهويته ليتأكد من أنه الشخص المطلوب فعلاً، ومن ثم ينتقل إلى مرحلة الإعلام، المتصلة بإعلام المتهم بالتهم المنسوبة إليه –من دون مناقشة-، وبكل الحقوق القانونية التي منحها له القانون، على غرار حقه في الصمت الذي يمكنه التنازل عنه بمحض إرادته، وفي الاستعانة بمحامي الذي قد يستعمله المتهم ليستعين بمحامي معين، أو يطلب من قاضي التحقيق تعيين له أي محامي، كما قد يتنازل عن هذا الحق صراحةً فيستجوب من دون حضور أي محامي[2].

بعد أن يفرغ قاضي التحقيق من الاستجواب المتعلق بالمثول الأول؛ ينتقل إلى مرحلة الاستجواب في الموضوع، التي تنطوي أساسا على الاستفسار والمواجهة. حيث يباشر قاضي التحقيق عملية طرح الأسئلة على المتهم، وتقديم الأدلة أمامه ليبدي رأيه فيها. ويعد هذا الاستجواب –الاستفسار في الموضوع-؛ بمثابة الإجراء الجوهري الذي يتوجب على قاضي التحقيق إعماله ولو لمرة واحدة فقط. مع إمكانية الاستغناء عنه في حالة إدلاء المتهم بتصريحات مفيدة لإظهار الحقيقة عند المثول الأول، أو إذا كان المتهم في حالة فرار، أو إصدار قاضي التحقيق لأمر انتفاء وجه الدعوى قبل الاستجواب[3].

ويحضا المتهم بالعديد من الضمانات القانونية عند استجوابه في الموضوع، فبالإضافة إلى الضمانات المبينة أعلاه المتصلة بالاستجواب عند المثول الأول –الحق في الصمت والاستعانة بمحامي والاستجواب من قاضي التحقيق-؛ يتمتع المتهم أساساً بحقه في الاستجواب قبل أن يؤمر بوضعه في الحبس المؤقت، ولا يمكن في أي حال من الأحوال أن يحلف اليمين القانونية التي يلتزم بها الشاهد. كما أن للمتهم ضمان آخر يمكن أن نسميه بضمان الضمان، المتمثل في محاضر الاستجواب، التي تدون فيها كل الإجراءات

---

[1] على أن تجرى كل الاستجوابات، سواءً المتعلقة بالمثول الأول أو المتصلة بالموضوع؛ من قبل من يحمل صفة القاضي، دون ضباط الشرطة القضائية. حيث الأصل إن ينجز من قبل قاضي التحقيق المختص، أو من قبل أي قاضٍ آخر ينوب عنه وفق إجراءات محددة. **أنظر في ذلك:** ناصر حمودي، (قانون الإجراءات الجزائية الجزائري)، مرجع سابق، ص 240.

[2] الإجراءات التي يرتب القانون على مخالفتها البطلان. **أنظر في ذلك:** المواد 100 و101 و157؛ أمر رقم 66-155، مرجع سابق. **وأنظر أيضا:** أحسن بوسقيعة، التحقيق القضائي، مرجع سابق، ص ص 64-67.

[3] **أنظر:** أحسن بوسقيعة، التحقيق القضائي، المرجع نفسه، ص 68.

السابقة بالذكر، ما يسمح بمراقبتها من خلال البحث في مدى احترام قاضي التحقيق لكل الضمانات القانونية المذكورة[1].

بالإضافة إلى الاستفسار الوجوبي؛ يمكن جوازا لقاضي التحقيق أن يلجأ إلى إجراء المواجهة. فإذا رأى قاضي التحقيق أن مواجهة المتهم بالأطراف الأخرى –كل شخص يحدده قاضي التحقيق–، من شأنها أن تؤدي إلى إظهار الحقيقة أو تساعد على ذلك؛ يمكنه أن يقرر اللجوء إليها، لكن بشرط أن يحترم القواعد الإجرائية السابقة بالذكر، المتصلة باستجواب المتهم بحضور محاميه أو بعد دعوته قانونا، مع وضع نسخة من ملف الإجراءات تحت تصرفه[2].

2. الوجه الرقمي الحديث للاستجواب المساعد على التحقيق في جرائم الوسط الرقمي: وفق الطرح نفسه المتصل بعمل السماع المساعد على التحري والتحقيق في جرائم الوسط الرقمي؛ لم يفرق المشرع بين الاستجواب التقليدي ونظيره المتصل بالمتهم الرقمي. حيث تطبق عليه كل الأحكام التقليدية المبينة، إلا من حيث ضرورة احترام الخصوصية الفنية المعقدة للمسرح الجرمي الافتراضي. الخصوصية التي أنتجت لنا العديد من القواعد الفنية، الواجب إتباعها من قاضي التحقيق عند استجوابه للمتهم، وإلا كلل الاستجواب بالفشل. الأمر الذي نبينه من خلال التطرق؛ إلى تعريف هذا النوع من الاستجواب الحديث، والتعريج على الخصوصية الفنية التي يقوم عليها.

أ- تعريف عمل الاستجواب المساعد على التحقيق في جرائم الوسط الرقمي: لم يتطرق المشرع أيضا إلى تعريف عمل الاستجواب المساعد على التحقيق في جرائم الوسط الرقمي، فاتحا بذلك المجال كعادته أمام الفقه الجنائي، الذي لم يتدخل في هذه الحالة ليطرح التعريفات المناسبة بهذا العمل الإجرائي الحديث. حيث يتم المرور في ذلك مباشرة؛ إلى تبيان الأساليب الناجحة في استجواب المتهم في جرائم الوسط الرقمي، أو يتم التطرق كأكثر تقدير؛ إلى أهمية هذا النوع من الاستجواب الحديث، التي يمكن من خلالها الوصول إلى التعريف المراد.

فتتمثل أهمية اللجوء إلى هذا الاستجواب المساعد الظاهر بالوجه الرقمي الحديث؛ في تفادي النقص الفني الذي يقوم عليه الاستجواب التقليدي. وذلك كون العمل به؛ تعترضه العديد من المعوقات العملية، على غرار نقص أو انعدام القدرة الفنية لدى المحقق التقليدي –قاضي التحقيق–، سيما وأن له تكوين قانوني غير متصل بالخصوصية الرقمية المعقدة[3].

---

[1] **أنظر:** المواد من 100 إلى 108؛ أمر رقم 66-155، مرجع سابق. **وأنظر أيضا:** ناصر حمودي، (قانون الإجراءات الجزائية الجزائري)، مرجع سابق، ص ص 239-243.

[2] **أنظر:** المادة 105؛ أمر رقم 66-155، المرجع نفسه.

[3] فعادةً ما يطلق مجرمو الوسط الرقمي على أنفسهم صفة النخبة، ويصفون أجهزة التحري والتحقيق في جرائم الوسط الرقمي عموما؛ بالضعفاء والقاصرين. **أنظر في ذلك:** حسين ربيعي، مرجع سابق، ص 251 و252.

يتبين من خلال الأهمية المذكورة، أن الاستجواب المساعد على التحقيق في جرائم الوسط الرقمي؛ يزيد عن نظيره التقليدي من حيث الأسلوب الفني المتبع من قاضي التحقيق عند ممارسته للاستفسار والمواجهة. وبالتالي بإسقاط البعد الفني الحديث للاستجواب على مفهومه التقليدي والإجراءات ذات الصلة؛ يمكن أن نعرفه –الاستجواب الحديث– على أنه: "مناقشة ومواجهة المتهم من طرف قاضي التحقيق المستعين بخبير رقمي، بخصوص التهم الموجهة إليه، والأدلة الرقمية –وغيرها– القائمة ضده، مع التأكيد على ضرورة حماية الحقوق القانونية المقررة للمتهم".

ب– الخصوصية الفنية في عمل الاستجواب المساعد على التحقيق في جرائم الوسط الرقمي: بعد التسليم بحصر الاختلاف بين الاستجواب التقليدي، ونظيره الحديث المساعد على التحقيق في جرائم الوسط الرقمي، في الأسلوب الرقمي واجب الإتباع من قاضي التحقيق القائم على ذلك؛ توجب علينا العمل على تبيان هذا الأسلوب، الذي ينقسم إلى جزأين، يتصل الأول بالمرحلة السابقة لممارسة الاستجواب، وينطوي الثاني على المرحلة الثانية والأخيرة المتصلة بممارسته.

فيتوجب على قاضي التحقيق قبل الشروع في استجواب المتهم في جرائم الوسط الرقمي؛ أن يستعين بخبير رقمي، وأن يتبادل معه أغلب المعلومات المتعلقة بالجريمة، سواءً الإجرائية الأساسية أو الفنية الفرعية. حيث يزود قاضي التحقيق الخبير؛ بإجراءات سير الاستجواب من ترتيب للمتهمين وغير ذلك من إجراءات سير الاستجواب والمواجهة إن تطلب الأمر، وبدوره الخبير يزود قاضي التحقيق نفسه؛ بكافة المصطلحات الفنية الضرورية في الاستجواب، ومنه وضع خطة شاملة للاستجواب ومراحله وأطواره، قبل الشروع فيه[1].

وبعد أن يقوم قاضي التحقيق بمساعدة الخبير الرقمي، في ضبط خطة الاستجواب المساعد على التحقيق في جرائم الوسط الرقمي؛ ينتقل إلى المرحلة الثانية والأخيرة، التي تنطوي على الشروع الفعلي في ممارسة هذا الاستجواب. حيث يتوجب على القاضي أن يسمح للخبير بحضور جلسة الاستجواب، وطرح الأسئلة الفرعية التي يراها مناسبة –المتفق مسبقا على إطارها العام في خطة الاستجواب–. كما يمكن للخبير أن يستعين بأوراق يضعها أمام قاضي التحقيق، لتبين له الأسئلة الرقمية الواجب طرحها والوقت الأنسب لذلك. وفي الإطار نفسه يرى الفقه المقارن؛ بضرورة تفادي إضاعة الوقت في استجواب متهم حول جريمة يستحيل إثباتها من جهة، ووجوب حضور الخبير في كل أطوار الاستجواب من جهة أخرى، وإذا منع القانون ذلك، يتم اللجوء إلى تكوين لجان تحقيق من أجل ضمان حضور الخبير. خاصةً وأن أخذ رأي الخبير عند تدوين محضر الاستجواب؛ يعد من الأهمية بمكان[2].

---

[1] **أنظر:** حسين ربيعي، مرجع سابق، ص 253 و254.

[2] **أنظر:** المرجع نفسه، ص 254.

المطلب الثاني: الأذون والأوامر التقليدية المساعدة على التحري والتحقيق في جرائم الوسط الرقمي

تمارس في إطار إجراءات التحري والتحقيق عموماً، بالإضافة إلى الأعمال سابقة البيان؛ العديد من الإجراءات الأخرى، التي تكون في مواجهة الشخص محل الاختبار، سواءً كان مشتبها فيه أو متهما، فتقيد من حريته بطريقة أو بأخرى بغرض ضمان السير الحسن للتحري أو التحقيق على حسب الحالة. الأمر الذي ينجز عبر أذون أو أوامر تصدر وفق أشكال مختلفة عن الجهة المختصة، المنطوية على وكيل الجمهورية في إطار مرحلة التحري أو قاضي التحقيق بخصوص إجراءات التحقيق.

وفي هذا الصدد، يمكن أن يكون للأذون والأوامر المقيدة لحرية المشتبه فيه والمتهم؛ الدور المساعد على التحري والتحقيق في جرائم الوسط الرقمي، سيما وأنهما يمنعانه –المشتبه فيه أو المتهم– من العبث بالدليل الرقمي. وعلى العموم يمكن لوكيل الجمهورية أن يقيد حرية المشتبه فيه في جرائم الوسط الرقمي؛ عبر الإذن بتوقيفه للنظر(فرع أول)، كما يمكن لقاضي التحقيق أن يقيد حرية المتهم، من خلال وضعه تحت الرقابة القضائية(فرع ثانٍ)، أو إيداعه رهن الحبس المؤقت(فرع ثالث).

الفرع الأول: الإذن بتوقيف المشتبه فيه للنظر المساعد على التحري عن جرائم الوسط الرقمي

يعد توقيف المشتبه فيه للنظر؛ من أهم الصلاحيات القهرية التي منحها المشرع للنيابة العامة خلال مرحلة التحري، خاصةً بعد تراجعه عن سلطة الحبس لمدة 08 أيام في الجريمة المتلبس بها، عبر إلغائها النهائي واستحداث إجراء المثول الفوري[1]، حماية للمشتبه فيه من تعسف النيابة العامة، التي ستصبح خصما له بعد تحريك أو رفع الدعوى العمومية.

وللتوقيف للنظر بخصوص التحري في جرائم الوسط الرقمي؛ دوراً هاماً سيما وأنه يقيد حرية المشتبه فيه ليمنعه بطريقة أو بأخرى من المساس بالدليل الرقمي، وحتى القرينة التقليدية التي قد تقود للدليل الرقمي نفسه. الأمر الذي نتطرق إليه من خلال تبيان القواعد العامة المشتركة لإذن التوقيف للنظر(أولا)، ومن ثم التعريج على خصوصية الإذن نفسه المساعد على التحري عن جرائم الوسط الرقمي(ثانيا).

أولا: القواعد الإجرائية العامة للتوقيف للنظر

نضم المشرع التوقيف للنظر؛ في موقعين مختلفين متصلين بمرحلة التحري. حيث وضع له أحكاماً مفصلة في مواجهة المشتبه فيه بجناية أو جنحة متلبس بها، بالمواد من 51 إلى 55 "ق.إ.ج"، وفي الحالة العادية بالمادتين 65 و65–1 من القانون نفسه. التي من خلالها يمكن أن نصل إلى القواعد الإجرائية الممارس في إطارها إذن التوقيف للنظر، فنحدد مفهومه ومدته وضمانات المشتبه فيه الذي يكون محلاً له.

[1] المثول الفوري الذي يعد خارجاً عن دراستنا، نظرا لتعلقه بمرحلة المحاكمة أكثر منه بمرحلة التحري وإجراءات التحقيق. **أنظر في ذلك: المادة** 16 المضيفة للمواد من 339مكرر إلى 339مكرر7 والمادة 26؛ أمر رقم 15-02، مرجع سابق.

1. مفهوم التوقيف للنظر: يعد التوقيف للنظر من أبرز الصلاحيات القهرية الممنوحة لأجهزة التحري عموما، حيث بموجبه يستطيع ضابط الشرطة القضائية –بعلم وكيل الجمهورية التابع له–؛ أن يمس بحرية المشتبه فيه، عن طريق توقيفه لمدة معينة. الأمر الذي تعرفه بعض الدراسات الفقهية الجنائية؛ على أنه: "إجراء يقوم به ضابط الشرطة القضائية عن طريق توقيف شخص لمدة لا تزيد عن 48 ساعة قابلة للتجديد، وهذا لأنه من الضروري توقيفه تلبية لإجراءات البحث والتحري، على أن يطلع وكيل الجمهورية فورا بذلك مع وجوبية توفر قرائن قوية ضده"[1].

يبين التعريف المذكور أعلاه؛ المفهوم العام للتوقيف للنظر، من دون التطرق إلى العديد من النقاط التي كان من الواجب أن يتضمنها التعريف. وهو ما نصفه بالقصور الذي تعتريه أيضا معظم التعريفات الأخرى، حيث نجدها إما عامة وفق الطريقة نفسها المذكورة أعلاه، أو خاصة بالتوقيف للنظر المنجز في مواجهة الجريمة المتلبس بها دون الحالة العادية أو العكس[2]، وقد تعرف التوقيف للنظر من دون وصفه بالإذن –كما هو الحال في دراستنا–[3]، بالإضافة إلى أنها تعد بمثابة التعريفات القاصرة قانونا، لكون المشرع تدخل سنة 2015، ليعدل في العديد من المفاهيم الأساسية المتصلة بالتوقيف للنظر[4].

وعلى العموم يمكن من خلال ما قدمناه أعلاه مضموناً ومناقشةً، سيما بالانطلاق من فكرة "إذن" التوقيف للنظر وفق القواعد الإجرائية المعدلة والمتممة –إلى غاية تعديل سنة 2015–، المتعلق بحالة التلبس والحالة العادية معاً، أن نضع تعريفا عاما لهذا الإذن؛ فنقول أنه: "إذن إجرائي يصدر عن وكيل الجمهورية المختص إلى ضابط الشرطة القضائية التابع له، في حالة التلبس والحالة العادية، ليقوم في إطاره بتوقيف المشتبه فيه للنظر، بخصوص جناية أو جنحة، وذلك وفق شروط ومدد وضمانات محددة مسبقا من المشرع".

وضع المشرع بالنصوص القانونية ذات الصلة بالتوقيف للنظر؛ العديد من الشروط القانونية، التي يتوجب على ضابط الشرطة القضائية مراعاة توفرها عند ممارسته لهذا الإجراء القهري، الماس بحرية

---

[1] **أنظر:** حسين طاهري، الوجيز في شرح قانون الإجراءات الجزائية، الطبعة الثالثة، دار الخلدونية للنشر والتوزيع، الجزائر، 2005، ص 39 و40.

[2] حيث ينظر إلى التوقيف للنظر المتصل بالجريمة المتلبس بها على أنه؛ من صلاحيات ضابط الشرطة القضائية المعاين للجرم المشهود؛ أن يوقف للنظر الشخص الذي توجد ضده قرائن قوية ومتماسكة، تفيد أنه حاول أو اشترك في ارتكاب الجريمة. **أنظر في ذلك:** جمال نجيمي، مرجع سابق، ص 119 و120.

[3] يتبين أن أغلب الدراسات الجنائية -إن لم نقل جلها-؛ تتطرق للتوقيف للنظر بالتسمية نفسها دون إضافة مصطلح "الإذن"، عكس ما تفعله بخصوص الرقابة القضائية أو الحبس المؤقت، بإضافة مصطلح "الأمر". وهو ما لنا فيه رأي، حيث آثرنا التطرق إلى هذا العنصر بعبارة "إذن التوقيف للنظر". انطلاقا من كونه لا يمارس إلا بإذن من وكيل الجمهورية المختص، إما صراحةً أو ضمنا. فيكون الإذن صريحا عند الحديث عن تمديد مدة التوقيف للنظر، ويكون ضمنيا عند التوقيف لأول مرة، حيث إخطار وكيل الجمهورية بمجرد التوقيف وسكوته عن ذلك، وإمكانية زيارته لأماكن التوقيف المعلومة لديه مسبقا، وكونه المدير المباشر لجهاز الشرطة القضائية؛ يعد بمثابة الإذن الضمني. **أنظر في ذلك:** المواد 2/12 ومن 51 إلى 55 و65 و65-1؛ أمر رقم 66-155، مرجع سابق.

[4] **أنظر:** المادة 09 المعدلة والمتممة للمواد 51 و51مكرر و51مكرر1 و52 و65؛ أمر رقم 15-02، مرجع سابق.

الأشخاص لمدة زمنية معتبرة. فبخصوص تحديد الشخص الموقوف للنظر؛ نجد أن المشرع قد حصره في واحد أو أكثر من الموجودين في مسرح الجريمة المتلبس بها، على أنه لم يتطرق إلى ذلك تماما في الحالة العادية، ما يفتح المجال للقول بعدم تحديده. لكن بتعديل سنة 2015[1]، أضاف المشرع عبارة هامة في الحالتين –التلبس والعادية–، تقيد ضابط الشرطة القضائية من حيث تحديد الشخص الموقوف للنظر، حيث اشترط –المشرع– أن يتعلق الأمر بجناية أو جنحة معاقب عليها بعقوبة سالبة للحرية، وأن توجد ضد الموقوف دلائل تحمل على الاشتباه في ارتكابه للجريمة[2].

وبالإضافة إلى الشروط المذكورة أعلاه؛ يتوجب أن ينفذ التوقيف للنظر من ضابط الشرطة القضائية، بعد إخطاره لوكيل الجمهورية الذي يتبعه –إذن ضمني–، مع ضرورة توضيح الأسباب الدافعة إلى ذلك. كما أنه إجراء يمارس في مدة أصلية محددة مسبقا من المشرع، التي لايمكن تمديدها وفق مدد محددة مسبقا أيضا من المشرع؛ إلا بإذن صريح من وكيل الجمهورية المختص. كما أن من أهم الشروط المتصلة بتنفيذ إذن التوقيف للنظر؛ نجد أن المشرع قرر للمعني به العديد من الضمانات القانونية[3].

2. مدة تنفيذ إذن التوقيف للنظر: حدد المشرع في إطار تنفيذ إذن التوقيف للنظر؛ مدد زمنية لايمكن تجاوزها في أي حال من الأحوال، وذلك وفق تنظيم ينطوي على أصل واستثناء. حيث الأصل العام ألا يتجاوز التوقيف للنظر مدة 48 ساعة، التي تقود إما لإطلاق سراح الموقوف ضمن آجالها دون تجاوزها، أو اقتياده في إطار المدة نفسها –دون تجاوزها–؛ إلى وكيل الجمهورية في حال قامت ضده دلائل قوية متماسكة من شأنها التدليل على اتهامه[4].

وخروجاً عن الأصل العام المتصل بمدة التوقيف للنظر، المحددة بـــ 48 ساعة –يومين–؛ أجاز المشرع التمديد إلى مدد أخرى بإذن مكتوب من وكيل الجمهورية المختص. وذلك وفق نهج متفاوت تختلف المدد من خلاله؛ بحسب اختلاف نوع الجناية أو الجنحة محل التحري من جهة، ومدى كونها جريمة –جناية أو جنحة– متلبس بها من عدمها من جهة أخرى.

فيمكن أن يمدد التوقيف للنظر في إطار حالة التلبس بإذن مكتوب من وكيل الجمهورية المختص، ليصل إلى 05 مرات كأكثر تقدير. حيث يكون التمديد لمرة واحدة –لتصبح المدة الإجمالية 96 ساعة أي 04 أيام– بخصوص التحري في جرائم المساس بأنظمة المعالجة الآلية للمعطيات، ولمرتين –144 ساعة أي 06 أيام– في جرائم الاعتداء على أمن الدولة، وثلاث مرات –192 ساعة أي 08 أيام– بخصوص

[1] **أنظر:** المادة 09 المعدلة للمادة 1/51؛ أمر رقم 15-02، مرجع سابق.

[2] ولو أنه شرط معمول به قبل تعديل سنة 2015، نظرا لوروده ضمنا بقول المشرع بعدم إمكانية توقيف الأشخاص الذين لا توجد ضدهم دلائل قوية إلا للمدة اللازمة لأخذ أقوالهم. **أنظر في ذلك:** المادة 3/51؛ أمر رقم 66-155، مرجع سابق.

[3] **أنظر:** المواد من 51 إلى 55 والمادتان 65 و65-1؛ المرجع نفسه.

[4] **أنظر:** المادة 1/51 و2 و3 والمادة 65/ 1 و2؛ المرجع نفسه.

جرائم المتاجرة بالمخدرات والجريمة المنظمة عبر الحدود الوطنية وجرائم تبييض الأموال والجرائم المتعلقة بالتشريع الخاص بالصرف. وأخيرا يمكن أن يصل التمديد إلى خمس مرات –288 ساعة أي 12 يوم– إذا ما تعلق التحري بالجرائم الموصوفة بالأفعال الإرهابية والتخريبية[1].

كما يمكن أن يمدد التوقيف للنظر في الحالة العادية –خارج إطار التلبس–، بإذن مكتوب من وكيل الجمهورية المختص، ليصل إلى 05 مرات كأكثر تقدير أيضا. لكن وفق طرح تشريعي فيه بعض الاختلافات عن التمديد المتصل بحالة التلبس. حيث لايمكن التمديد لمرة واحدة، مع إمكانية التمديد إلى مرتين ولخمس مرات بالطريقة والمضمون نفسهما[2].

وأما بخصوص التمديد إلى ثلاث مرات؛ فيكون بالطريقة نفسها، لكن بمضمون مختلف نوعا ما، حيث قبل تعديل سنة 2015، كان التمديد يقتصر على الجريمة المنظمة العابرة للحدود الوطنية وجرائم تبييض الأموال والجرائم المتعلقة بالتشريع الخاص بالصرف، دون جرائم المتاجرة بالمخدرات. الأمر الذي تم الاحتفاظ به بموجب تعديل سنة 2015، مع زيادة هذه الأخيرة –جرائم الاتجار بالمخدرات– من جهة، وجرائم الفساد من جهة أخرى[3]. ليتساوى المضمون مع نظيره المتصل بالجريمة المتلبس بها، مع انفراد الحالة العادية بالمكانية التمديد لثلاث مرات بخصوص جرائم الفساد غير المذكورة في حالة التلبس[4].

3. ضمانات الموقوف للنظر: يتمتع المشتبه فيه الموقوف للنظر بالعديد من الحقوق، التي تشكل الضمانات المقررة له قانونا من تعسف أجهزة التحري، سيما ضباط الشرطة القضائية. التي منها ما هي شكلية إجرائية ومنها ما هي إجرائية ومنها ما تعد موضوعية، يتم العمل بها سواءً في إطار التوقيف للنظر المتصل بحالة التلبس أو في الحالة العادية[5].

فمن حيث الضمانات الشكلية الإجرائية؛ نجد أن المشرع ألزم ضابط الشرطة القضائية بإخبار الموقوف للنظر عند توقيفه –مع الاستعانة بمترجم عند الحاجة–؛ ببعض حقوقه الإجرائية، المحددة حصرا في حقي الاتصال والزيارة من جهة والفحص الطبي من جهة أخرى، اللذان يلتزم بعد ذلك بتنفيذهما وفق قواعد محددة مع مراعاة سرية وحسن سير التحري. حيث يلزم أن يضع تحت تصرف الموقوف للنظر وسائل

[1] **أنظر:** المادة 5/51؛ أمر رقم 66-155، مرجع سابق.

[2] **أنظر:** المادة 3/65-1و3؛ المرجع نفسه.

[3] **أنظر:** المادة 3/65-2؛ المرجع نفسه.

[4] الأمر الذي يطرح التساؤل حول اقتصار التمديد في إطار جرائم الفساد؛ على الحالة العادية دون حالة التلبس. فهل سقط ذلك سهوا من المشرع، أم هي قناعة منه بعدم إمكانية التلبس بجرائم الفساد.

[5] نقصد بالضمانات الشكلية الإجرائية؛ تلك التي يلتزم ضابط الشرطة القضائية بها، مع ضرورة إخبار الموقوف للنظر بها بمجرد توقيفه. ونستدل بالضمانات الإجرائية؛ على التي يلتزم بها ضابط الشرطة القضائية، من دون ضرورة إخبار الموقوف للنظر بها. وأما الضمانات الموضوعية؛ فهي التي تقرر المسؤولية الجنائية الموضوعية على ضابط الشرطة القضائية، وتجرم بعض السلوكيات التي يمارسها في مواجهة الموقوف للنظر.

الاتصال الفوري بشخص واحد يحدده هو، الذي قد يكون أحد أصوله أو فروعه أو إخوته أو زوجته أو محاميه، وفي حال كان الموقوف أجنبي الجنسية، وتعذر عليه أو فضل عدم الاتصال بمن ذكروا؛ تتاح له الوسائل اللازمة للاتصال بمستخدمه و/أو بالممثلية الدبلوماسية أو القنصلية لدولته بالجزائر[1].

كما قرر المشرع للموقوف للنظر؛ الحق في زيارة أحد أقاربه المختار من بين الذين ذكروا من دون محاميه، الذي لايمكنه أن يزوره إلا بعد تمديد مدة التوقيف للنظر كأصل عام، وبمرور نصف المدة القصوى للتوقيف للنظر في حالة جرائم المعاملة الخاصة[2]. على أن تتم الزيارة في غرفة خاصة على مرأى ومن دون مسمع ضباط الشرطة القضائية، ضماناً للسرية اللازمة، وفي كل الأحوال لايمكن أن تتجاوز الزيارة مدة 30 دقيقة[3].

بالإضافة إلى حق الاتصال والزيارة؛ أقر المشرع أيضا حق الفحص الطبي كضمان شكلي إجرائي. حيث يعد الضابط ملزما بإجراء فحص طبي للموقوف للنظر، بمجرد طلبه لذلك بنفسه أو عبر محاميه أو عائلته. الذي ينجز من طرف طبيب يختاره الشخص الموقوف؛ من بين اللذين يمارسون مهامهم في دائرة اختصاص المحكمة، وفي حالة تعذر ذلك يعين من طرف الضابط نفسه. مع إمكانية سماح وكيل الجمهورية بإجراء الفحص؛ خلال سريان مدة التوقيف للنظر[4].

وأما من حيث الضمانات الإجرائية، التي يلتزم بها ضابط الشرطة القضائية من دون إخبار الموقوف للنظر بها؛ فيتوجب عليه أن ينظم فترات السماع والراحة بشكل يتناسب مع الجهد المعقول للشخص. بالإضافة إلى التوقيف في أماكن تضمن احترام كرامة الإنسان، التي تكون معلومة مسبقاً لدى وكيل الجمهورية، الذي يمكنه زيارتها في أي وقت أراد[5].

كما أنه بالإضافة إلى الضمانات الشكلية و/أو الإجرائية؛ وضع المشرع ضمانات أخرى ذات طابع موضوعي؛ ترتب المسؤولية الجنائية على ضابط الشرطة القضائية، الذي يمارس بعض التجاوزات في حق الموقوف للنظر[6]. حيث جرم المشرع تجاوز الآجال القانونية المقررة للتوقيف للنظر، تحت وصف

---

[1] **أنظر:** المادة 51مكرر1/1و2؛ أمر رقم 66-155، مرجع سابق.

[2] فلا يمكن أن يستفيد الموقوف للنظر من زيارة محاميه؛ إلا بعد مرور 48 ساعة -أي يومين- من توقيفه كأصل عام. ولا يسمح بالزيارة إلا بعد مرور 96 ساعة -أي 04 أيام- من التوقيف؛ في جرائم المتاجرة بالمخدرات والجريمة المنظمة عبر الحدود الوطنية وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف، بالإضافة إلى جرائم الفساد في الحالة العادية دون التلبس. **أنظر في ذلك:** المادة 5/51 والمادة 51مكرر1/1 و2و3 والمادة 3/65و5؛ المرجع نفسه.

[3] **أنظر:** المادة 51مكرر5/1و6؛ المرجع نفسه.

[4] **أنظر:** المادتان 51مكرر8/1 و6/52؛ المرجع نفسه.

[5] **أنظر:** المادة 1/52و4 و5؛ المرجع نفسه.

[6] مع الإشارة إلى عدم ترتيب المشرع؛ للبطلان الإجرائي على مخالفة ضابط الشرطة القضائية للضمانات الشكلية و/أو الإجرائية المذكورة. الأمر الذي يفهم من غياب النص المقرر لذلك، سيما وأننا نعلم أنه لا بطلان إلا بنص صريح يقرره.

جناية الحبس التعسفي[1]. كما أنه جرم أيضا تحت وصف الجناية؛ أي استعمال للتعذيب ضد الموقوف للنظر بهدف الحصول على اعترافات أو معلومات أو غيرها[2].

ثانيا: خصوصية التوقيف للنظر المساعد على التحري عن جرائم الوسط الرقمي

لم يفرق المشرع الجزائري في إطار التوقيف للنظر عموماً؛ بين الجريمة التقليدية وجرائم الوسط الرقمي بنص خاص منفصل، مثل ما فعل مع التفتيش والحجز المرقمنين. إلا أننا نؤكد على خصوصية إذن التوقيف للنظر المساعد على التحري في جرائم الوسط الرقمي، انطلاقا من النصوص نفسها سابقة الذكر، التي يمكن أن نستشف منها العديد من النقاط المميزة له، سيما وأنها قواعد فرقت بين العديد من الجرائم كما بينا سابقا. الأمر الذي يمكن من خلاله؛ أن نقف عند خصوصية إذن التوقيف للنظر المساعد على التحري في جرائم الوسط الرقمي انطلاقا من أنواعها، المنطوية على جرائم المساس بأنظمة المعالجة الآلية للمعطيات من جهة، ونظيرتها الجريمة التقليدية المتصلة بالوسط الرقمي من جهة أخرى[3].

1. خصوصية التوقيف للنظر في مواجهة جرائم المساس بأنظمة المعالجة الآلية للمعطيات: أضفى المشرع على جرائم المساس بأنظمة المعالجة الآلية للمعطيات، بالإضافة إلى بعض الجرائم الأخرى –جرائم المعاملة الخاصة– نوعا من الخصوصية، من خلال معاملة إجرائية خاصة في كل أطوار التحري والتحقيق عموما. الأمر الذي لم يخرج عنه بخصوص إذن التوقيف للنظر، سيما من حيث آجاله وقواعد تمديدها، وكذلك الاستفادة من بعض الضمانات الإجرائية المتصلة أساسا بحق زيارة المحامي.

فمن حيث آجال التوقيف للنظر؛ فرق المشرع بين الحالة العادية وحالة التلبس. من خلال اقتصاره في الحالة العادية؛ على المدة الأصلية غير القابلة للتجديد، المنطوية إجمالا 48 ساعة –أي يومين–، وفي الوقت نفسه سماحه بتمديدها لمرة واحدة في حالة التلبس، لتصبح 96 ساعة –أي 04 أيام–[4]. وكذلك

---

[1] **أنظر:** المادة 6/51؛ أمر رقم 66-155، مرجع سابق. **وأنظر أيضا:** المادة 291؛ أمر رقم 66-156، مرجع سابق.

[2] **أنظر:** المادتان 263مكرر و263مكرر1، أمر رقم 66-156، المرجع نفسه.

[3] مع التأكيد على تخلف الخصوصية، عن الأحكام العامة التي لا تختلف من جريمة إلى أخرى. على غرار تحديد الشخص محل التوقيف للنظر، وإفادته بضمان الاتصال والفحص الطبي والراحة عند السماع والتوقيف في الأماكن اللائقة المعلومة. بالإضافة إلى الضمانات الموضوعية، المقيمة للمسؤولية الجنائية على تجاوزات الشرطة القضائية.

إلا أن بعض هذه الأحكام العامة؛ قد يكون لها الدور السلبي على عملية التحري انطلاقا من الطبيعة الرقمية المعقدة للمسرح الجرمي الافتراضي. فتحديد الشخص الموقوف للنظر في حالة التلبس من بين الحاضرين في مسرح الجريمة؛ قد يكون قاصرا نظرا لكون أغلب جرائم الوسط الرقمي تقوم على الاشتراك عن بعد، وترك الشريك البعيد هو بمثابة الفرصة الصريحة للعبث بالدليل الرقمي. كما أن السماح للموقوف للنظر بالاتصال بالأقارب المحددين بالطريقة نفسها المتصلة بالجريمة التقليدية؛ قد يسمح بتلقينهم طريقة العبث بالدليل الرقمي.

[4] الأمر الذي يعد غير مفهوما ومخالفا للمنطق الرقمي السليم. ففي الحالة العادية -خارج إطار التلبس- لايمكن أن تمدد المدة، رغم الحاجة العملية لذلك، نظرا لإمكانية ضابط الشرطة القضائية أن يوقف للنظر؛ أي شخص توجد ضده دلالات جرمية، ما يسمح بتوقيف الفاعل الأصلي والشريك عن بعد وغيرهما. وفي التلبس الذي لايمكن من خلاله إلا توقيف من وجد بمسرح الجريمة، دون الشريك عن بعد وغيره؛ يفتح مجال التمديد لمرة واحدة من أجل التعامل مع حلقة صغيرة من الأشخاص.

بخصوص الحق في الزيارة من قبل المحامي، وفق الشروط المبينة سابقا؛ فلا يمكن أن تكون في كل الأحوال إلا بعد مرور يومين –48 ساعة– من بدأ التوقيف للنظر، أي بعد انتهائه تماما في الحالة العادية –خارج إطار التلبس–، لأن المشرع لم يسمح بالتمديد في هذه الحالة، وبعد تمديده للمرة الواحدة والأخيرة المسموح بها في حالة التلبس، أي بعد مرور نصف المدة القصوى للتوقيف للنظر في هذه الحالة[1].

2. خصوصية التوقيف للنظر في مواجهة الجريمة التقليدية المتصلة بالوسط الرقمي: تختلف خصوصية التوقيف للنظر في مواجهة الجريمة التقليدية المتصلة بالوسط الرقمي، عن نظيرتها المتصلة بجرائم المساس بأنظمة المعالجة الآلية للمعطيات، إلا ما وصفت منها على أنها من جرائم المعاملة الخاصة. الأمر الذي أدت إليه العديد من النقاط الإجرائية، على غرار التباين في التعامل مع الجريمة عموماً وجرائم المعاملة الخاصة خصوصاً، وكذلك الفرق بين قواعد التحري في الحالة العادية من جهة وفي حالة التلبس من جهة أخرى. وهو ما يظهر جليا من خلال الآجال القانونية المعمول بها في التوقيف للنظر، والضمانات الإجرائية المتعلقة بالحق في زيارة المحامي بالأساس.

فمن حيث آجال التوقيف للنظر؛ نجد أنها 48 ساعة –يومان– غير قابلة للتجديد كأصل عام، مهما كان نوع وخطورة الجناية أو الجنحة التقليدية المتصلة بالوسط الرقمي، وسواءً تعلق الأمر بالحالة العادية أو حالة التلبس. إلا أن هذه الآجال قابلة للتمديد إذا ما تعلق الأمر؛ بالتحري في بعض جرائم المعاملة الخاصة المحددة حصرا. ففي الحالة العادية وحالة التلبس معاً؛ يمدد التوقيف للنظر مرتين بخصوص جرائم الاعتداء على أمن الدولة، وثلاث مرات إذا تعلق الأمر بجرائم المتاجرة بالمخدرات والجريمة المنظمة عبر الحدود الوطنية وجرائم تبييض الأموال والجرائم المتعلقة بالتشريع الخاص بالصرف، كما تمدد خمس مرات إذا تعلق الأمر بجرائم موصوفة بأفعال إرهابية أو تخريبية. على أن ينفرد التمديد لثلاث مرات في الحالة العادية –دون التلبس–، إذا تعلق الأمر بجرائم الفساد[2].

وأما بخصوص الحق في الزيارة من قبل المحامي، ففي الجريمة التقليدية المتصلة بالوسط الرقمي عموما؛ لا يمكن تصورها إلا بعد انتهاء مدة التوقيف للنظر المنطوية على 48 ساعة غير قابلة للتمديد، سواءً تعلق الأمر بالحالة العادية أو حالة التلبس، وبعد تمديدها للمرة الواحدة والأخيرة في جرائم أمن الدولة. الأمر الذي له حكم آخر بخصوص جرائم المعاملة الخاصة المتصلة بالوسط الرقمي، حيث لايمكن أن يستفيد الموقوف للنظر من زيارة محاميه؛ إلا بعد مرور نصف المدة القانونية القصوى[3].

---

[1] **أنظر:** المادة 5/51 والمادة 51مكرر4/1 والمادة 3/65 و5؛ أمر رقم 66-155، مرجع سابق.

[2] **أنظر:** المادتان 5/51 و3/65؛ المرجع نفسه.

[3] فلا يمكن أن يستفيد الموقوف للنظر من زيارة محاميه؛ إلا بعد مرور 96 ساعة -أي 04 أيام- من التوقيف؛ في جرائم المتاجرة بالمخدرات والجريمة المنظمة عبر الحدود الوطنية وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف، بالإضافة إلى جرائم الفساد في الحالة العادية دون التلبس. **أنظر في ذلك:** المادة 51مكرر2/1و3 والمادة 5/65؛ المرجع نفسه.

الفرع الثاني: الأمر بوضع المتهم تحت الرقابة القضائية المساعد على التحقيق في جرائم الوسط الرقمي

إذا كان قد منح المشرع صلاحيات وسلطات قهرية لأجهزة التحري، في مواجهة المشتبه فيه قبل رفع أو تحريك الدعوى العمومية، من خلال ممارسة إذن التوقيف للنظر؛ فمن باب أولى أن يمنح ذلك لقاضي التحقيق، بعد تحريك الدعوى العمومية، سيما وأنه يمثل السلطة القضائية المحايدة عن أطراف الدعوى العمومية. وهو ما عمل به المشرع فعلاً، من خلال منح قاضي التحقيق بعض السلطات القهرية في مواجهة المتهم، على غرار إمكانية إصدار أمر الوضع تحت الرقابة القضائية.

وفي الإطار نفسه؛ لم يفرق المشرع الجزائري –ولا المقارن إلا حد الساعة– بين المتهم العادي والرقمي، بخصوص ممارسة أمر الوضع تحت الرقابة القضائية. ما يدفع للقول بضرورة طرح القواعد الإجرائية العامة لأمر وضع المتهم تحت الرقابة القضائية(أولا)، ومن ثم التطرق إلى ممارسة هذا الأمر في التحقيق المتصل بجرائم الوسط الرقمي(ثانيا).

أولا: القواعد الإجرائية العامة للوضع تحت الرقابة القضائية

يعد أمر الوضع تحت الرقابة القضائية؛ بمثابة السلطة الأقل قهرا، التي يمكن أن يستعملها قاضي التحقيق في مواجهة المتهم، نظرا لامتلاكه أيضا؛ القدرة على إيداعه رهن الحبس المؤقت –كما سنرى في الفرع الموالي من الدراسة–. الأمر الذي أقره المشرع في إطار قانون الإجراءات الجزائية بالمادة 123، ونظم حالاته وإجراءاته بالمواد من 125مكرر1 إلى 125مكرر3 من القانون نفسه. وهو ما سنستعرضه فيما يلي؛ عبر التطرق إلى مفهوم أمر الوضع تحت الرقابة القضائية، وتبيان الالتزامات القانونية التي يفرضها على المتهم، مع إبراز أهم الإجراءات المتعلقة بإصداره وتنفيذه.

1. مفهوم الوضع تحت الرقابة القضائية: مكن المشرع قاضي التحقيق من إصدار أمر وضع المتهم تحت الرقابة القضائية، أثناء ممارسته لإجراءات التحقيق القضائي الابتدائي، الذي يلي مباشرة تحريك الدعوى العمومية. حيث الأصل في المتهم الحرية احتراما لقرينة البراءة، ولكن يمكن لقاضي التحقيق استثناءً أن يقيد هذه الحرية بطريقتين أساسيتين، فإما يعمل بالتقييد الجزئي فيأمر بوضع المتهم تحت الرقابة القضائية، أو بالتقييد الكلي التام فيأمر بإيداعه الحبس المؤقت –كما سنرى لاحقا–[1].

يفهم مما ذكر أعلاه؛ أن المشرع يعمل بنظام تدرجي هرمي من حيث التعامل مع حرية المتهم. فالأصل الحرية، والاستثناء الأول الرقابة القضائية –تقييد جزئي–، والاستثناء الثاني الحبس المؤقت –تقييد كلي–. ولايمكن في أي حال من الأحوال تجاوز أو خلط هذا الترتيب التشريعي، الذي يلتزم به قاضي التحقيق، سيما وأنه –المشرع– يضع قاعدة عامة في هذا الإطار، تنطوي على عدم انتقال قاضي التحقيق من حالة إلى أخرى؛ إلا بعد التأكد من ضرورة ذلك، القائمة على عدم جدوى الحالة المعمول بها.

[1] **أنظر:** المادة 123؛ أمر رقم 66-155، مرجع سابق.

ورجوعاً إلى أغلب الدراسات الإجرائية –سيما في إطار القانون الجزائري–؛ نجدها تعتبر الرقابة القضائية بمثابة الإجراء الاستثنائي البديل عن الحبس المؤقت. الأمر الذي نؤيده في جزء ونخالفه في جزء آخر، فنتفق مع القول بأنه إجراء استثنائي، نظرا لكونه الاستثناء عن الأصل المنطوي على الحرية. إلا أننا نختلف مع كونه بديلا عن الحبس المؤقت، نظرا لكونه أسبق في الدرجة من الحبس المؤقت، وبالتالي هو البديل المؤقت عن الحرية، الذي قد يستبدل فيما بعد بالحبس المؤقت.

وعلى العموم؛ تختلف التعريفات الفقهية المنصبة على الرقابة القضائية[1]، سيما من حيث مدى اعتبارها بديلا للحبس المؤقت من عدمها، وفق المناقشة المطروحة أعلاه. مع التأكيد على التطرق إليها كعمل إجرائي من دون إضافة وصف "الأمر"، كما هو عليه الحال في دراستنا. حيث تعتبر الرقابة القضائية؛ أنها: "إجراء وسط بين الحبس المؤقت والإفراج، فيكيف على أنه تدابير تحوطية أو أمنية، الغرض منها الإبقاء على المتهم تحت تصرف القضاء ومراقبته"[2].

يتبين من التعريف المقدم أعلاه؛ أنه الأقرب إلى الصواب من حيث تحديده لطبيعة الرقابة القضائية والهدف من اللجوء إليها. حيث يعتبرها بمثابة الإجراء الوسط من جهة، وبهدف المراقبة والوضع تحت التصرف القضائي من جهة أخرى. إلا أنه مجانب للصواب –التعريف– من حيث القول بوسطية الرقابة بين الحبس المؤقت والإفراج، والحقيقة أنه إجراء وسط بين الحرية الأصلية والحبس المؤقت[3]. كما أن الهدف منه لا يقتصر على المراقبة والوضع تحت التصرف القضائي؛ بل فيه هدف أنساني ينطوي على صون حرية المتهم من الحبس المؤقت، سيما وأنه بريء حتى تثبت إدانته بحكم نهائي بات حائز للقوة.

يمكن من خلال التعريف الفقهي المبين أعلاه، والمناقشة المؤسسة التي تقدمنا بها القائمة على مضمون النصوص القانونية المتصلة؛ أن نصل إلى وضع تعريف عام يتصل بالرقابة القضائية، انطلاقا من إضافة مصطلح الأمر، خاصةً وأن الآمر بها في إطار إجراءات التحقيق القضائي الابتدائي؛ هو قاضي التحقيق دون سواه، الذي يصدر أمرا صريحا ومكتوبا، ولا مجال للأمر الضمني في هذا الإطار كما هو معمول به بخصوص إذن التوقيف للنظر. ومنه نعتبر أمر الرقابة القضائية؛ على أنه: "أمر إجرائي يصدر عن قاضي التحقيق المختص، في إطار ممارسته لإجراءات التحقيق القضائي الابتدائي، ليقيد حرية المتهم بالتزام أو أكثر من تلك الواردة قانونا أو غيرها، وذلك بشرط أن يكون متهما بجناية أو جنحة معاقب عليها بعقوبة سالبة للحرية، وبإتباع إجراءات إصدار وتنفيذ محددة مسبقا من المشرع".

---

[1] التي تسمى بـ "الرقابة القضائية-Le contrôle judiciaire" وليس بـ "المراقبة القضائية- La surveillance judiciaire". سيما وأنه يوجد فرق في المدلول الإجرائي؛ بين مصطلح "الرقابة" ونظيره مصطلح "المراقبة"، من حيث العديد من النقاط، التي سنستعرضها عند التطرق إلى المراقبة الالكترونية، كآخر عنصر من دراسة الحال.

[2] **أنظر:** عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، مرجع سابق، ص 429.

[3] خاصةً وان المشرع بالمادة 123 سابقة الذكر؛ رتب هذه الحالات كالأتي؛ الحرية أولا والرقابة القضائية ثانيا والحبس المؤقت ثالثا والإفراج بعد الحبس المؤقت رابعا.

2. الالتزامات التي يفرضها أمر الوضع تحت الرقابة القضائية: حدد المشرع على سبيل المثال أنواع الالتزامات الإجرائية، التي تحد من حرية المتهم الموضوع تحت الرقابة القضائية، وتعطي فكرة لقاضي التحقيق عن التدابير التي يمكن فرضها، فيختار واحدة أو أكثر من الالتزامات المنصوص عليها أو يفرض غيرها على حسب الحاجة إلى ذلك. كما له الحرية والسلطة التقديرية، من حيث اختيار اللجوء إلى الرقابة أصلا من عدمها –ترك المتهم من دون رقابة–، وحتى من حيث التعديل فيها؛ عن طريق التغيير والإضافة بعد الأمر بها وأثناء مرحلة تنفيذها[1]. وعلى العموم يمكن أن نتطرق إلى هذه الالتزامات الواردة على سبيل المثال، عبر تقسيمها إلى التزامات ايجابية تفرض على المتهم القيام بأعمال معينة، ونظيرتها السلبية التي تمنعه من القيام بأعمال أخرى[2].

أ– الالتزامات الايجابية التي يفرضها أمر الوضع تحت الرقابة القضائية: حدد المشرع 04 أربع التزامات ايجابية، يمكن أن يأمر قاضي التحقيق بواحدة منها أو أكثر في إطار الرقابة القضائية، فيتقيد بها المتهم الذي يكون محلا لها. فقد ينطوي أمر الرقابة القضائية؛ على إلزام المتهم بالمثول الدوري أمام المصالح والسلطات المعينة من قاضي التحقيق بالأمر نفسه، التي تتمثل عادةً في جهاز الشرطة القضائية. كما يمكن أن يُأْمَرَ المتهم بتسليم بعض الوثائق إلى أمانة الضبط أو مصلحة أمن معينة مقابل وصل، على ألا تخرج هذه الوثائق؛ عن تلك المستعملة في السفر خارج التراب الوطني –سيما جواز السفر–، أو في ممارسة مهنة أو نشاط يخضع إلى ترخيص. ويمكن أيضا أن يكون المتهم؛ محلا لبعض الإجراءات الطبية، التي لم يحددها المشرع، وان ذكر الفحص العلاجي الذي قد يكون في المستشفى أو في غيره، وأعطى مثالا باستهداف إزالة التسمم[3].

كما أضاف المشرع سنة 2015 بمناسبة تعديله لقانون الإجراءات الجزائية بالأمر 15–02 سابق الذكر؛ التزاما ايجابيا جديدا، يتمثل في المكوث في إقامة محمية يعينها قاضي التحقيق، يمنع مغادرتها إلا بإذن هذا الأخير. الذي ميزه المشرع عن باقي الالتزامات سواءً الايجابية أو السلبية؛ ببعض القواعد الموضوعية والإجرائية الخاصة، التي سنستعرضها بالتفصيل بمناسبة التطرق إلى عنصر الإجراءات[4].

---

[1] **أنظر:** المادتان 2/123 و125مكرر1؛ أمر رقم 66-155، مرجع سابق.

[2] الالتزامات التي لم يتطرق إليها المشرع الجزائري لا بالحصر ولا بالتمثيل؛ في بادئ الأمر بموجب وضعه للرقابة القضائية أول مرة سنة 1986، حيث ترك المجال مفتوحا أمام قاضي التحقيق ليأمر بالالتزام الذي يراه مناسبا. على أنه رجع بعد ذلك؛ ليعطي أمثلة عنها في حدود 08 أنواع بالتعديل الوارد سنة 1990. ومن ثم يتممها سنة 2015؛ بإضافة التزامين ليصبح المجموع 10 التزامات واردة على سبيل المثال. **أنظر في ذلك:** المادة 125مكرر1؛ المضافة بقانون رقم 86-05، مؤرخ في 04 مارس 1986، يعدل ويتمم أمر رقم 66-155، يتضمن قانون الإجراءات الجزائية، (ج ر) عدد 10، صادر بتاريخ 05 مارس 1986. معدلة بالمادة 03؛ قانون رقم 90-24، مؤرخ في 18 أوت 1990، يعدل ويتمم أمر رقم 66-155، يتضمن قانون الإجراءات الجزائية، (ج ر) عدد 36، صادر بتاريخ 22 أوت 1990. معدلة بالمادة 12؛ أمر رقم 15-02، مرجع سابق.

[3] **أنظر:** المادة 125مكرر1/2-3و4؛ أمر رقم 66-155، المرجع نفسه.

[4] **أنظر:** المادة 12 المتممة للمادة 125مكرر/1 بالبند رقم 09 من الفقرة رقم 02؛ أمر رقم 15-02، المرجع نفسه.

ب- الالتزامات السلبية التي يفرضها أمر الوضع تحت الرقابة القضائية: زيادةً عن الالتزامات الايجابية؛ جاء المشرع بستة 06 التزامات أخرى سلبية، تقود إلى امتناع المتهم عن القيام ببعض الأعمال المحددة. التي تضاف إلى الالتزامات الايجابية الأربعة 04 المذكورة، ليصبح المجموع 10 التزامات كما بينا سابقا. ومن خلالها يحدد قاضي التحقيق في أمر الرقابة القضائية؛ تدبير أو أكثر يتوجب على المتهم أن يلتزم به، من خلال الامتناع عن القيام بعمل أو أعمال معينة.

فقد ينطوي الالتزام السلبي؛ على منع المتهم من مغادرة الحدود الإقليمية التي يحددها قاضي التحقيق في أمر الرقابة القضائية، ما لم يأذن له القاضي نفسه بذلك. كما قد يُمْنَعَ المتهم في إطار الالتزام السلبي أيضا؛ من الذهاب إلى بعض الأماكن المحددة من طرف قاضي التحقيق في أمر الرقابة. بالإضافة إلى إمكانية منعه من القيام ببعض النشاطات المهنية التي قد يكون لها علاقة بالجريمة، من خلال ارتكابها إثر ممارستها أو بمناسبة ذلك من جهة، أو خشية ارتكاب جريمة جديدة من جهة أخرى[1].

ويمكن لقاضي التحقيق أيضا، أن يفرض على المتهم محل الرقابة القضائية؛ التزامات سلبية أخرى. كأن يمنعه من رؤية أو الاجتماع بعض الأشخاص، المحددين منه في أمر الرقابة القضائية. ويمكن أن يكون المتهم محلا؛ لتدبير سلبي فيه نوع من الالتزام الايجابي أيضا، المنطوي على منعه من إصدار الشيكات واستعمال الصكوك إلا بإذن قاضي التحقيق مصدر الأمر بالمنع، وذلك بعد أن يلتزم بإيداع نماذج عنها لدى أمانة الضبط[2].

كما لم يقتصر المشرع عند تعديله لقانون الإجراءات الجزائية سنة 2015 بالأمر 15-02؛ على إضافة الالتزام الايجابي السابق بالذكر فقط –التزام المكوث في إقامة محمية–، بل أضاف أيضا التزاما سلبيا جديدا؛ ينطوي على عدم مغادرة مكان الإقامة إلا بشروط وفي مواقيت محددة، أو ما يمكن أن نسميه بالوضع تحت الإقامة الجبرية[3].

3. إجراءات إصدار وتنفيذ أمر الوضع تحت الرقابة القضائية: تمارس الرقابة القضائية وفق إجراءات محددة مسبقا من المشرع، حيث بعد توفر الشروط الموضوعية –كأصل عام–، المنطوية على كون الجريمة المتابع بها المتهم؛ من التي يعاقب عليه قانونا بعقوبة سالبة للحرية[4]؛ ينتقل قاضي التحقيق

---

[1] **أنظر:** المادة 125مكرر1/2-1و2و5؛ أمر رقم 66-155، مرجع سابق.

[2] **أنظر:** المادة 125مكرر1/2-6 و8؛ المرجع نفسه.

[3] **أنظر:** المادة 12 المتممة للمادة 125مكرر/1 بالبند رقم 10 من الفقرة رقم 02؛ أمر رقم 15-02، مرجع سابق.

[4] عبر المشرع عن ذلك؛ بـ: "...إذا كانت الأفعال المنسوبة للمتهم قد تعرضه لعقوبة الحبس أو عقوبة أشد"، ما قد يدفع للقول؛ أن الرقابة القضائية معمول بها في المخالفات والجنح المعاقب عليها بالحبس والجنايات المعاقب عليها بالسجن. إلا أن الأمر في الحقيقة لا يعد كذلك؛ فالمنطق الجنائي السليم؛ يخرج المخالفات من دائرة الرقابة القضائية ويبقي على الجنح والجنايات. كما أن النص الجزائري باللغة الفرنسية للمادة نفسها؛ عبر عن الحبس بـ "L'emprisonnement correctionnel"، مع العلم أن المشرع الفرنسي المنقولة منه هذه المادة، لا يستعمل مصطلح "correctionnel"؛ إلا عند تطرقه للجنح -دون المخالفات-، سيما بخصوص العقوبات المقررة للجنح. **أنظر في ذلك:** Art 131-3; code pénale français, op.cit.

المختص إلى مرحلة إصدار أمر الرقابة القضائية، الذي يحوي ويأمر بالتزام أو أكثر من الالتزامات السابقة بالبيان، القابلة للتغيير والتعديل والإضافة في أي لحظة بعد بدأ تنفيذ الأمر[1].

وعلى العموم يبدأ سريان أمر الرقابة القضائية؛ ابتداءً من التاريخ المحدد في الأمر الصادر عن قاضي التحقيق. ولا ينتهي كأصل عام إلا بانتهاء التحقيق، إما بصدور أمر أو قرار بألا وجه للمتابعة أو بالإحالة أمام جهة الحكم المختصة. التي يمكنها أن ترفع الرقابة القضائية؛ من تلقاء نفسها أو بعد صدور الحكم القاضي في الدعوى العمومية. كما يمكن لقاضي التحقيق خلال سير التحقيق القضائي وقبل الإحالة؛ أن يأمر برفع الرقابة، سواءً من تلقاء نفسه أو بطلب من وكيل الجمهورية أو المتهم بعد استشارة وكيل الجمهورية[2].

إلا أن المشرع خرج بتعديل قانون الإجراءات الجزائية لسنة 2015؛ عن الشروط الموضوعية والإجرائية العامة المذكورة. وذلك بخصوص واحد من الالتزامات العشرة دون البقية، وهو المنطوي على التزام المكوث في إقامة محمية، المستجد أيضا بالتعديل نفسه كما بينا سابقا. حيث لايمكن أن يلجأ إليه قاضي التحقيق؛ إلا بخصوص الجرائم الموصوفة بأفعال إرهابية أو تخريبية، ولمدة أقصاها ثلاث 03 أشهر، قابلة للتمديد وفق المدة نفسها مرتين 02 على الأكثر، على يساءل جنائيا عن جريمة إفشاء سرية التحقيق، كل من يفشي أي معلومة تتعلق بمكان مكوث المتهم[3].

ثانيا: ممارسة أمر الوضع تحت الرقابة القضائية كمساعد على التحقيق في جرائم الوسط الرقمي

على العكس من إذن التوقيف للنظر، الذي أبرزنا خصوصيته الحديثة المتصلة بجرائم الوسط الرقمي ومسرحها الافتراضي، نتطرق إلى نظيره أمر وضع المتهم تحت الرقابة القضائية؛ من منظور آخر مختلف عن الخصوصية الحديثة. نظرا للتعامل التشريعي المتباين مع الاثنين، سيما وأنه –المشرع– راعى خصوصية جرائم المساس بأنظمة المعالجة الآية للمعطيات مثلا؛ فمكن من تمديد مدة التوقيف للنظر، ولم يراعي هذه الخصوصية في إطار الرقابة القضائية. الأمر الذي نتعامل معه من خلال القول بإمكانية اللجوء الإجرائي إلى أمر الوضع تحت الرقابة القضائية في مواجهة جرائم الوسط الرقمي عموما، مع محاولة إبراز البعض من المعوقات الفنية التي تحول دون نجاعة هذا الإجراء التقليدي.

1. إمكانية اللجوء إجرائيا إلى الوضع تحت الرقابة القضائية في مواجهة جرائم الوسط الرقمي: لا يوجد ما يمنع قاضي التحقيق؛ من إصدار أمر الوضع تحت الرقابة القضائية في مواجهة المتهم بخصوص أي جريمة من جرائم الوسط الرقمي، على أن تكتسي تكييف الجناية أو الجنحة المعاقب عليها بعقوبة سالبة

[1] **أنظر:** المادة 125مكرر1/1 و4؛ أمر رقم 66-155، مرجع سابق.

[2] **أنظر:** المادتان 125مكرر1/2 و125مكرر1/3؛ المرجع نفسه.

[3] **أنظر:** المادة 125مكرر1/2-9؛ المرجع نفسه.

للحرية، وفق الشرط الموضوعي العام الذكور سابقا، والمتصل بالجريمة التقليدية والحديثة معا، سيما وأن المشرع لم يتطرق إلى أي شرط موضوعي يفرق بين جرائم الوسط الرقمي والجريمة التقليدية المنفصلة عنها، أو على الأقل يميز جرائم المساس بأنظمة المعالجة الآلية للمعطيات كما فعل مع إذن التوقيف للنظر وأغلب إجراءات التحري والتحقيق.

كما أن كل القواعد العامة الأخرى المذكورة تبقى على حالها، فتضل الرقابة القضائية بمثابة الإجراء الوسط بين الحرية الأصلية والحبس المؤقت، ويصدر الأمر المقرر لها عن قاضي التحقيق المختص في مواجهة المتهم. بالإضافة إلى إتباع كل الإجراءات التقليدية المتعلقة بإصدار الأمر وتنفيذه، الذي سيتضمن لا محال التزام أو أكثر من الالتزامات العشر 10 المذكورة –أو غيرها–. مع التأكيد على عدم إمكانية تطبيق الالتزام التاسع –المكوث في إقامة محمية–؛ إلا على المتهم بالجرائم الموصوفة بالأفعال الإرهابية أو التخريبية المتصلة بالوسط الرقمي، وفي المدد المحدد قانونا.

2. معوقات نجاعة الوضع تحت الرقابة القضائية كمساعد على التحقيق في جرائم الوسط الرقمي: كل من ينظر إلى القواعد العامة لأمر الوضع تحت الرقابة القضائية بنظرة إجرائية سطحية؛ يمكنه أن يصل إلى القول بأنها قد تساعد على التحقيق في جرائم الوسط الرقمي، سيما وأنها تحد من حرية الجاني الرقمي بالتزامات يختارها قاضي التحقيق من القائمة التشريعية المحددة أو غيرها. وهو ما يفيد من إبقاء الحال على ما هو عليه، إلى غاية الانتهاء من التحقيق بالتوصل إلى الدليل الرقمي، أو القرينة التقليدية التي تقود إليه. وحتى وان لم تكون ناجعة؛ يمكن استبدالها بالحبس المؤقت الذي يقيد المتهم الرقمي كليا.

إلا أن الأمر لا يعد كذلك في وجهة نظرنا، حيث المشكل الأساس الذي يحول دون نجاعة أمر الوضع تحت الرقابة القضائية في مواجهة المتهم الرقمي؛ ينطوي على الاختلاف في الطبيعة بين الالتزامات التي أعطى المشرع أمثلة عنها، والسلوكيات التي قد يرتكبها المتهم الرقمي للعبث بالدليل الرقمي عموما. فالالتزامات الايجابية والسلبية التي جاء بها المشرع؛ تقوم على الطبيعة المادية التقليدية، غير المفيدة في التعامل مع التصرفات الافتراضية الرقمية، التي قد يقوم بها المتهم أثناء فترة الرقابة[1].

وعليه يمكن التساؤل؛ عن فائدة المثول الدوري للمتهم الرقمي أمام مصالح الشرطة القضائية للإمضاء، إن كان بإمكانه العبث بالدليل الرقمي طيلة النهار باستعماله عناصر الوسط الرقمية الشخصية وغيرها، قبل أن يمثل أمامهم في المساء –وان كان لذلك فائدة تقليدية تضمن عدم الفرار–. وكذلك بخصوص التزام تسليم وثائق السفر والوثائق المهنية، الذي يبعد المتهم عن السفر والاتصال المادي بمهنته

[1] وحتى القول بإمكانية استبدال الرقابة القضائية غير المفيدة في مواجهة جرائم الوسط الرقمي، بالحبس المؤقت؛ لا يعد بمثابة الحل الأصلح. نظرا لمساس هذا الأخير بحرية المتهم الذي قد يكون بريئا، كما أنه قد لايكون ممكنا في العديد من الجنح المتصلة بالوسط الرقمي -كما سنرى لاحقا-. بالإضافة إلى إمكانية العبث في الدليل الرقمي من أشخاص آخرين، غير المتهم المتواجد رهن الحبس المؤقت.

المعتادة. بالإضافة إلى إخضاع المتهم للفحص العلاجي، الذي لا علاقة له بأي حال من الأحوال بالوسط الرقمي، سيما وأن المشرع قد ربطه –كما بينا سابقا– بإزالة التسمم. هذا من دون أن ننسى التزام المكوث في مكان محمي، الذي ينطوي على الإقامة الجبرية –المادية– في مكان معين.

بالإضافة إلى الالتزامات الايجابية، نجد أن نظيرتها السلبية؛ هي أيضا لها الطابع المادي المنفصل عن الوسط الرقمي الذي قد يتعامل معه المتهم طيلة فترة تنفيذ الرقابة القضائية. على غرار المنع من مغادرة الحدود الوطنية ومن الذهاب إلى بعض الأماكن المحددة، والمنع من القيام ببعض النشاطات المهنية المتصلة بالجريمة، ورؤية بعض الأشخاص المحددين[1] وإصدار الشيكات. بالإضافة إلى المنع من مغادرة مكان الإقامة إلا بشروط وفي مواقيت محددة.

وعليه يمكن القول أن الالتزامات المادية، التي قد يؤمر بها في مواجهة المتهم الرقمي؛ تعد بلا جدوى، وان قلنا العكس فيسكون ذلك بنسبة ضئيلة جدا، قد تقود إلى المساعدة على التحقيق بفائدة جد ضيقة. الأمر الذي نرى أنه لا يمكن أن يواجه إلا وفق طريقتين أساسيتين، تقوم الأولى على العمل القضائي الميداني، وتنطوي الثانية على التدخل التشريعي المساعد للعمل القضائي.

فتتمثل الطريقة الأولى المتصلة بالمواجهة العملية القضائية؛ عن طريق فرض قاضي التحقيق على المتهم واحدة أو أكثر من الالتزامات المادية المذكورة، التي قد تكون لها فائدة إجرائية، كمنعه من الالتقاء بالأشخاص الذين لهم خبرة رقمية معتبرة. بالإضافة إلى فرض تدابير أخرى ذات طابع رقمي افتراضي، ينصحه بها الخبير الرقمي الذي يساعده، على غرار منع المتهم من الولوج إلى نطاق افتراضي معين، أو إلزامه بالإفصاح عن كلمات المرور للحسابات الشبكية التي يديرها...الخ.

وأما الطريقة الثانية القائمة على التدخل التشريعي المساعد؛ فتنطوي على ضرورة تدخل المشرع ليتمم المادة 125مكرر2/1 بمجموعة من الالتزامات الرقمية الافتراضية، المدروسة من قبل فرق بحث فنية متفوقة في الوسط الرقمي. على أن يكون لها الأثر الإجرائي المزدوج، فإما يستعملها قاضي التحقيق عبر فرض واحدة منها أو أكثر على المتهم الرقمي، أو يستند عليها كأمثلة رقمية لفرض تدابير أخرى غير منصوص عليها بالمادة نفسها[2].

مع التأكيد على أن الوضع الإجرائي الحالي؛ سيقود لا محال للاستعمال المفرط من قاضي التحقيق لأمر الوضع رهن الحبس المؤقت في مواجهة المتهم الرقمي، كحل سطحي وحيد؛ لتفادي العبث بالدليل الرقمي. ولو أننا سبقنا وقلنا؛ بإمكانية العبث به من غير المتهم الذي يكون حرا طليقا.

[1] ولو أن التزام المنع من الالتقاء ببعض الأشخاص وغيره؛ قد يقود إلى المنع المادي من استفادة المتهم غير المتمرس في الوسط الرقمي، من تعليمات ومساعدات من يلتقي بهم، سيما إن كانوا من خبراء هذا الوسط.

[2] الأمر الذي يعد صعب المنال، سيما وأن الدول المتقدمة في الوسط الرقمي والمصنعة لعناصره؛ هي نفسها تواجه مشاكل كبيرة بخصوص منع المتهم وغيره من العبث بالدليل الرقمي.

الفرع الثالث: الأمر بإيداع المتهم في الحبس المؤقت المساعد على التحقيق في جرائم الوسط الرقمي

بالإضافة إلى سلطة الوضع تحت الرقابة القضائية، التي منحها المشرع لقاضي التحقيق في مواجهة المتهم –التقليدي والرقمي– وفق القواعد الإجرائية سابقة البيان؛ تمت إفادته –قاضي التحقيق– أيضا بسلطة الإيداع في الحبس الوقت، كإجراء قهري ثاني أكثر مساسا بحرية الأفراد عبر الحد الكلي منها، بحبس المتهم خلال المدة المحددة قانونا. سيما وأن ذلك قد يعد الحل العملي الوحيد، المتاح أمام قاضي التحقيق –حاليا–، لتجاوز العجز الإجرائي المتصل بالالتزامات التقليدية للرقابة القضائية.

إلا أن المشرع عمل بالنهج نفسه المتصل بعدم التدخل لرقمنة العديد من الإجراءات، فترك ممارسة أمر الوضع في الحبس المؤقت وفق القواعد نفسها التقليدية –أو الحديثة غير المرقمنة–. ما يدفع للقول؛ بضرورة تحديد القواعد العامة المشتركة لهذا الأمر(أولا)، ومن ثم التطرق إلى ممارسته كمساعد على التحقيق في جرائم الوسط الرقمي(ثانيا).

أولا: القواعد الإجرائية العامة للإيداع في الحبس المؤقت

بمفهوم مقابل لطبيعة أمر الوضع تحت الرقابة القضائي، يعد أمر الوضع في الحبس المؤقت؛ بمثابة السلطة الأكثر قهرا، التي منحها المشرع لقاضي التحقيق في مواجهة المتهم عموما، عبر الحد الكلي من حرية المتهم لمدة زمنية محددة قانونا. وهو ما نظمه –المشرع– في إطار قانون الإجراءات الجزائية بالمواد من 123 إلى 137[1]، التي يمكن من خلالها –ومن خلال بعض الدراسات الفقهية أيضا–؛ الوصول إلى تحديد مفهوم أمر الوضع في الحبس المؤقت، ومبررات اللجوء إليه من قبل قاضي التحقيق، مع إبراز المدد القانونية التي ينفذ من خلالها[2].

1. مفهوم الإيداع في الحبس المؤقت: لم تتطرق أغلب التشريعات المقارنة –ومنها المشرع الجزائري– للحبس المؤقت، لا كعمل إجرائي ولا كأمر يصدر عن قاضي التحقيق المختص؛ بالتعريف القانوني الدقيق. الأمر الذي دفع بالعديد من الدراسات الفقهية الجنائية للتطرق إلى ذلك، فمنهم من عرف الحبس المؤقت على أنه: "سلب حرية المتهم بإيداعه في الحبس المؤقت في خلال مرحلة التحقيق التحضيري"[3]. ويعرف أيضا تقريبا بالمضمون نفسه؛ على أنه: "حبس المتهم خلال فترة التحقيق الابتدائي كلها أو بعضها أو إلى أن تنتهي بصدور حكم نهائي في الموضوع"[4].

[1] ما عدا المواد من 125 مكرر 1 إلى 125 مكرر3، المتصلة بأمر الوضع تحت الرقابة القضائية، كما بينا سابقا.

[2] على ألا نركز في هذا الإطار على إجراءات إصدار وتنفيذ أمر الوضع في الحبس المؤقت، نظرا لكونها تتفق مع تلك المقررة بخصوص أمر الوضع تحت الرقابة القضائية، سيما من حيث مرحلتها -التحقيق القضائي- وأطرافها وكونها تأتي بأمر قضائي مكتوب.

[3] **أنظر:** أحسن بوسقيعة، التحقيق القضائي، مرجع سابق، ص 130.

[4] **أنظر:** ناصر حمودي، (قانون الإجراءات الجزائية الجزائري)، مرجع سابق، ص 254 و255.

كما يعرف الحبس المؤقت بالنظر إلى أحكامه القانونية في التشريع الفرنسي –التي تختلف عن نظيرتها في التشريع الجزائي من حيث من يأمر بالإيداع–؛ على أنه: ""إجراء مؤقت يرد بأمر مسبب من قاضي الحريات والحبس بطلب من قاضي التحقيق في مواجهة المتهم بجناية أو جنحة معاقب عليها قانونا بعقوبة سالبة للحرية لا تقل عن 03 سنوات"[1].

يتبين من خلال التعريفات السابقة بالطرح، أن الحبس المؤقت عموما؛ يعد بمثابة الإجراء الذي يعطي المختص بالأمر به نوعا من السلطة القهرية المباشرة، من خلال إمكانية إيداع المتهم في الحبس لمدد زمنية محددة قانونا، وفي إطار شروط موضوعية وإجرائية يتوجب إتباعها. وهو ما أكد عليه قانون الإجراءات الجزائية بموجب المادة 123 وما يليها –السابقة بالذكر–، فجعل من قاضي التحقيق الجهة القضائية المخولة قانونا؛ بإصدار أمر الإيداع في الحبس المؤقت ضد المتهم بجناية أو جنحة، يسمح قانونا بالحبس المؤقت في إطارها.

وأما من حيث طبيعة الحبس المؤقت؛ فله الطابع الإجرائي الاستثنائي كما بينا سابقا، حيث لايمكن اللجوء إليه إلا استثناءً وبعد توفر مبرر أو أكثر من المبررات المحددة من المشرع –التي سنبينها فيما يلي–. الأمر الذي ترى فيه العديد من الدراسات، أن تحديد المشرع لعدد من المبررات؛ يعد بمثابة الإقرار الصريح منه بالطابع الاستثنائي للحبس المؤقت[2].

يمكن من خلال التعريفات الفقهية المتصلة بالحبس المؤقت عموما، والطرح الذي تلاها من حيث المناقشة وتحديد القواعد ذات الصلة؛ أن نضع تعريفا للحبس المؤقت مع ربطه بالأمر القضائي الذي يقرره في مواجهة المتهم، صادرا عن قاضي التحقيق المختص. حيث نقول أن أمر الإيداع في الحبس المؤقت هو: "أمر إجرائي يصدر عن قاضي التحقيق المختص، في إطار ممارسته لإجراءات التحقيق القضائي الابتدائي، ليحد من حرية المتهم بجناية أو جنحة يسمح قانونا الحبس المؤقت فيها، وذلك عبر حبسه لمدة معينة، مع الالتزام بالقواعد المقررة قانونا في هذا الإطار سيما مبررات الإيداع ومدده".

2. مبررات إصدار أمر الإيداع في الحبس المؤقت: ربط المشرع الجزائري بموجب قانون الإجراءات الجزائية، إمكانية لجوء قاضي التحقيق المختص إلى إصدار أمر إيداع المتهم الحبس المؤقت؛ بأربع حالات ينظر إليها الفقه الجنائي على أنها مبررات الإيداع. فلا يمكن إصدار أمر الإيداع؛ إلا بعد التأكد من توفر حالة أو أكثر من هذه الحالات، وإلا يكون اللجوء إليه بمثابة التصرف القضائي التعسفي في حق المتهم، الذي يفترض أنه بريء إلى أن تثبت إدانته بحكم نهائي بات حائز للقوة.

---

[1] **أنظر:** - THI Thuy Linh Phi, (La détention provisoire-Etude de droit comparé droit français et droit vietnamien), Thèse de doctorat, Ecole doctorale de droit, faculté de droit et de sciences politique, Université Montesquieu, Bordeaux IV, France, 2012, p 02.

[2] **أنظر:** ناصر حمودي، (قضاء التحقيق في قانون الإجراءات الجزائية الجزائري-دراسة تحليلية نقدية)، مرجع سابق، ص 111.

كان يربط المشرع إلى وقت قريب –قبل تعديل سنة 2015–، مبررات الحبس المؤقت في إجمالها؛ بفكرة عدم كفاية التزامات الرقابة القضائية –السابقة بالذكر–، وكأنه يكيف المبررات الأربعة؛ على أنها أمثلة حصرية عن مظاهر عدم كفاية التزامات الرقابة القضائية. وهو ما تراجع عنه –المشرع– بموجب تعديل سنة 2015؛ عبر قوله بأن أمر الحبس المؤقت يؤسس على معطيات مستخرجة من ملف القضية، التي قد تفيد في اعتبار أن مبرر من المبررات الأربعة على الأقل قد توفر[1].

وعلى العكس مما ذكر أعلاه؛ حافظ المشرع على الحالات الأربعة كما هي من دون أي تعديل أو تغيير. حيث ربط الحالة الأولى؛ بانعدام موطن مستقر للمتهم أو عدم تقديمه ضمانات كافية للمثول أمام القضاء أو كانت الأفعال جد خطيرة. على أن جعل من الحالة الثانية؛ تقوم على استحالة الحفاظ على الأدلة المادية ومنع الضغط على الشهود أو الضحايا أو التواطؤ المؤدي إلى عرقلة الكشف عن الحقيقة؛ إلا باللجوء إلى الحبس المؤقت[2].

زيادةً عن الحالتين الأولى والثانية، يمكن لقضائي التحقيق أن يستشف من ملف القضية حالة أخرى، تدفعه للأمر بإيداع المتهم الحبس المؤقت. وهي المنطوية على ضرورة اللجوء إلى الحبس المؤقت؛ لحماية المتهم أو وضع حد للجريمة أو للوقاية من حدوثها مرة أخرى. وكذلك كحالة رابعة وأخيره؛ يمكن أن يقوم التأسيس على عدم تقيد المتهم بالالتزامات الرقابة القضائية المفروضة عليه من قاضي التحقيق نفسه، من دون أي سبب جدي يدفع لذلك[3].

3. مدة الحبس المؤقت المحددة بأمر الإيداع: عرف الحبس المؤقت في إطار قانون الإجراءات الجزائية قبل تعديل 2015؛ مددا تصل إلى الحد غير المعقول الذي يتجاوز كل الخطوط، ويضرب بقرينة البراءة عرض الحائط، سيما وأنه يمكن أن يصل إلى حد الـــ 60 شهر في الجناية العابرة للحدود الوطنية. الأمر الذي كان يعالج بمدتين أساسيتين، متمثلتين في الـــ 20 يوم والأربعة 04 أشهر، قابلتين لتجديد وفق قواعد وشروط محددة[4]. غير أن المشرع بعد تعديله لقانون الإجراءات الجزائية بالأمر 15–02 سابق الذكر؛ عدل من المدد المذكورة، بطريقة ترجعها إلى الحد المعقول في حدود احترام قرينة البراءة وحقوق الإنسان. وهو ما سنبينه من خلال التمييز بين مدد الحبس المؤقت في الجنح والجنايات.

أ– **مدد الحبس المؤقت في الجنح:** تطرق المشرع إلى الحبس المؤقت في الجنح، بطريقة تميز بين الجنح من حيث مدة العقوبة المقررة لها قانونا. حيث لايمكن كأصل عام أن يحبس المتهم مؤقتا؛ إذا كان متابعا

[1] **أنظر:** المادة 12 المعدلة والمتممة للمادة 123مكرر؛ أمر رقم 15-02، مرجع سابق.

[2] **أنظر:** المادة 123مكرر/1؛ أمر رقم 66-155، مرجع سابق.

[3] **أنظر:** المادة والمرجع نفسهما.

[4] **أنظر:** المواد من 124 إلى 125 مكرر (قبل تعديل سنة 2015)؛ المرجع نفسه. **وأنظر أيضا:** ناصر حمودي، (قضاء التحقيق في قانون الإجراءات الجزائية الجزائري-دراسة تحليلية نقدية)، مرجع سابق، ص ص 113-116.

في جنحة تساوي أو تقل عقوبتها عن الثلاث 03 سنوات حبس. لكن يمكن في الحالة نفسها؛ أن يحبس المتهم مؤقتاً لمدة لا تزيد عن 01 شهر؛ إذا ما نتج عن الجنحة وفاة الضحية، أو ترتب عنها إخلالا ظاهرا بالنظام العام[1].

وأنا بخصوص الجنح التي تتجاوز العقوبة المقررة لها قانونا حد الـــ 03 سنوات حبسا؛ فيمكن أن يأمر قاضي التحقيق بإيداع المتهم بها الحبس المؤقت، لمدة لا تزيد عن الـــ 04 أربعة أشهر. التي تكون قابلة للتجديد مرة واحدة من قاضي التحقيق نفسه؛ عندما يكون من الضروري الإبقاء على المتهم محبوسا، وذلك بالإضافة إلى إمكانية التمديد من غرفة الاتهام لـــ 04 أشهر أخرى، بطلب من قاضي التحقيق، عند أمره بإجراءات خارج التراب الوطني لنتائجها قدرا من الأهمية في إظهار الحقيقة[2]. وهو ما يدفع للقول أن مدة الحبس المؤقت في الجنح؛ لا يمكن في أي حال من الأحوال أن تتجاوز حد الـــ 12 شهر.

ب- مدد الحبس المؤقت في الجنايات: وفق الطريقة نفسها المتصلة بالجنح؛ تعامل المشرع مع الحبس المؤقت في الجنايات، سيما من حيث التفرقة بين الجنايات انطلاقا من العقوبة المقررة لها قانونا. حيث تنطوي مدة الحبس المؤقت في الجنايات التي تقل عقوبتها عن الـــ 20 سنة سجن؛ على 04 أربعة أشهر، قابلة للتمديد مرتين من قاضي التحقيق نفسه ووفق الشروط والإجراءات نفسها، لتصل المدة إجمالا إلى حد الـــ 12 شهر[3].

وأما إذا ما تعلق الأمر بجناية معاقب عليها بالسجن المؤقت لمدة تساوي أو تزيد عن الـــ 20 سنة، أو بالسجن المؤبد أو الإعدام؛ فيمكن أن يمدد قاضي التحقيق بأمر مسبب أيضا، ووفق الشروط والإجراءات نفسها؛ المدة الأصلية المتمثلة في 04 أشهر لثلاث 03 مرات كاملة[4]، فتصل مدة الحبس المؤقت إجمالا إلى حد الـــ 16 شهر.

وفي كل الأحوال؛ يمكن لقاضي التحقيق أن يطلب من غرفة الاتهام تمديد الحبس المؤقت في كل الجنايات. وهو ما يكون دائما لمرة واحدة فقط –أربعة أشهر–، سواءً في الحالة العادية أو في حالة أمر قاضي التحقيق بأعمال إجرائية خارج التراب الوطني[5]. ما يسمح بالتمديد لمدة 08 أشهر إضافية، لو تقدم قاضي التحقيق بالطلبين[6].

---

[1] **أنظر:** المادة 124؛ أمر رقم 66-155، مرجع سابق.

[2] **أنظر:** المادتان 125 و125مكرر/1و2؛ المرجع نفسه.

[3] **أنظر:** المادة 125-1/1؛ المرجع نفسه.

[4] **أنظر:** المادة 125-1/2/ المرجع نفسه.

[5] **أنظر:** المادة 125-1/4و10 والمادة 125مكرر/1و2؛ المرجع نفسه.

[6] وعليه يمكن القول، أن المشرع بعد أن كان يسمح بالحبس المؤقت لمدة تصل إلى 60 شهر -05 سنوات- في الجناية العابرة للحدود الوطنية؛ أصبح لا يسمح في الحالة نفسها و في غيرها من الجنايات الخطيرة؛ كأثر تقدير إلا بـالحبس المؤقت لمدة 24 شهر -أي 02 سنة-، وذلك باحتساب 16 شهر التي يأمر بها قاضي التحقيق، و08 أشهر التي تقررها غرفة الاتهام.

ثانيا: ممارسة أمر الإيداع في الحبس المؤقت كمساعد على التحقيق في جرائم الوسط الرقمي

تعامل المشرع الجزائري مع أمر الإيداع في الحبس المؤقت؛ بالطريقة نفسها تقريبا التي تعامل بها مع أمر الوضع تحت الرقابة القضائية، من حيث الاكتفاء بالنصوص التقليدية المعروفة، التي عدلت وتممت مؤخرا بالأمر 15-02، من دون الإشارة لجرائم الوسط الرقمي، أو على الأقل لأهم أنواعها المنطوي أساسا على جرائم المساس بأنظمة المعالجة الآلية للمعطيات. الأمر الذي يدفع للبحث فيما يلي، من حيث مدى إمكانية اللجوء إلى الحبس المؤقت في جرائم الوسط الرقمي عموما، مع التركيز على المدد القانونية الممارس في إطارها بخصوص الجرائم نفسها.

1. إمكانية اللجوء إجرائيا إلى الإيداع في الحبس المؤقت بخصوص جرائم الوسط الرقمي: وفق الطريقة نفسها المتصلة بالوضع تحت الرقابة القضائية؛ نقول أنه لا يوجد ما يمنع قاضي التحقيق من إصدار أمر وضع المتهم الرقمي في الحبس المؤقت، كلما توفرت الشروط الموضوعية والإجرائية العامة –السابقة بالذكر-. فينظر قاضي التحقيق إلى جرائم الوسط الرقي بخصوص الحبس المؤقت؛ بالنظرة نفسها المتصلة بالجريمة التقليدية، سيما من حيث البحث في توافر مبرر أو أكثر من المبررات السابقة بالذكر، والاقتناع باستثنائية الحبس المؤقت، التي تسبقه الرقابة القضائية وقبل ذلك الحرية.

وزيادةً على ذلك؛ يتوجب على قاضي التحقيق أن يتبع كل القواعد التقليدية في إصدار وتنفيذ أمر الحبس المؤقت، إن من حيث أطرافه أو شروطه الموضوعية المتصلة بإمكانية اللجوء إليه في كل الجنايات وفي الجنح المعاقب عليها بالحبس لمدة تزيد عن الـــ 03 سنوات كأصل عام. ولو أنه كان بالإمكان أن يتدخل المشرع ليضيف بعض النقاط الإجرائية في هذا الصدد، التي تظهر تميز مواجهة جرائم الوسط الرقمي، كأن يضيف مصطلحات ترقمن من المبررات الأربعة المذكورة، أو يعتمد إجراء الإقامة الجبرية تحت المراقبة الالكترونية، كعمل مستقل عن الرقابة القضائية وحل وسط بينها وبين الحبس المؤقت[1].

2. مدد الحبس المؤقت في جرائم الوسط الرقمي: يتبين من خلال ما تم التطرق إليه أعلاه؛ أنه من الممكن قانونا إصدار أمر الحبس المؤقت في مواجهة المتهم الرقمي. وبما أننا سبق وأكدنا على عدم تطرق المشرع لهذا الأمر في صورته الرقمية الحديثة؛ لا يسعنا في هذا المقام سوى البحث في القواعد الإجرائية التقليدية المحددة لمدد الحبس المؤقت –المذكورة سابقا-، ومن ثم محاولة إسقاطها على جرائم الوسط الرقمي. وهو ما نبينه من خلال التفرقة بين نوعي هذه الجرائم، الدائرة بين المساس بأنظمة المعالجة الإلية للمعطيات، ونظيرتها التقليدية المتصلة بالوسط الرقمي.

---

[1] الإجراء الذي جاء به المشرع الفرنسي تحت تسمية "L'Assignation à résidence avec surveillance électronique"، بموجب تعديله لقانون الإجراءات الجزائية سنة 2009. وذلك باعتباره بمثابة الإجراء المنفصل والمستقل عن الرقابة القضائية والحبس المؤقت. **أنظر في ذلك:** Art 137; code de procédure pénale français, Partie législative, op.cit.

أ- **مدد الحبس المؤقت في مواجهة جرائم المساس بأنظمة المعالجة الآلية للمعطيات:** أكدنا سابقا أن المشرع الجزائري؛ تعامل مع مدد الحبس المؤقت عبر التفرقة بين الجنايات والجنح بالأساس. ولو رجعنا في هذا الصدد إلى جرائم المساس بأنظمة المعالجة الآلية للمعطيات؛ لتوصلنا إلى أن تكييفها القانوني لا يخرج عن إطار الجنح، إن كجنحة عادية أو مشددة من حيث العقوبة دون التغير في التكييف.

ومن خلال ما ذكر، يمكن القول أنه لا يسمح قانونا بحبس المتهم الرقمي مؤقتا كأصل عام؛ في كل جنح المساس بأنظمة المعالجة الآلية للمعطيات، وذلك لكونها جنح لا تتجاوز العقوبة الأشد المقررة لها قانونا حد الـــ 03 سنوات حبس كأقصى حد[1]. إلا إذا كان من شأنها المساس بالنظام العام، فيسمح بحبس المتهم الرقمي مؤقتا لمدة لا تزيد عن 01 شهر. كما يمكن أن يحبس المتهم الرقمي مؤقتا في جرائم المساس -دون جريمة الدخول والبقاء الشكلي-، لمدة 04 أشهر قابلة للتجديد مرة واحدة من قاضي التحقيق نفسه، ولمرة أخرى إضافية تسمح بها غرفة الاتهام بطلب من قاضي التحقيق، في حال أمر بإجراءات خارج التراب الوطني -لتصبح المدة الإجمالية 12 شهر-، وذلك إذا ما استهدفت جرائم المساس؛ الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام[2].

ب- **مدد الحبس المؤقت في مواجهة الجريمة التقليدية المتصلة بالوسط الرقمي:** زيادةً عن مدد الحبس المؤقت في جرائم المساس بأنظمة المعالجة الآلية للمعطيات؛ يمكن -وفق القواعد التقليدية المذكورة سابقا- لقاضي التحقيق أن يودع المتهم الرقمي الحبس المؤقت، في الجنايات والجنح التقليدية المتصلة بالوسط الرقمي. فيسمح بذلك في الجنح التي يعاقب عليها قانونا بالحبس لأكثر من ثلاث 03 سنوات، على ألا تزيد مدة الحبس المؤقت عن 12 شهرا كأثر تقدير، ويمنع ذلك في الجنح الأخرى، إلا إذا مست بالنظام العام أو أدت إلى وفات أحد الأشخاص، ليسمح بالحبس المؤقت حينها لمدة لا تزيد عن 01 شهر.

وأما في الجنايات التقليدية المتصلة بالوسط الرقمي؛ فيسمح بالحبس في مواجهة المتهم بها -بالقواعد التقليدية نفسها-، ولو أن المدة تختلف على حسب العقوبة الأشد المقررة قانونا. فقد تصل المدة إلى 12 شهر بعد التمديد، في الجنايات التي تقل عقوبتها الأشد عن 20 سنة سجن، والى 16 شهر في غير ذلك، مع إمكانية التمديد لمرة واحدة من غرفة الاتهام بطلب عادي من قاضي التحقيق، ولمرة أخرى بطلب مؤسس على القيام بإجراءات في الخارج، لتصل المدة الإجمالية لـــ 24 شهر.

---

[1] فالعقوبة الأشد في جنحة الدخول والبقاء؛ لا تتجاوز سنتين 02 حبس، وكذلك بخصوص جنحة المساس المنفصل بالمعطيات الرقمية، التي لا تزيد عن 03 سنوات حبس، والأمر نفسه بالنسبة للأعمال التحضيرية والتالية لارتكاب الجرائم المذكورة. **أنظر في ذلك:** المواد من 394مكرر إلى 394مكرر2؛ أمر رقم 66-156، مرجع سابق.

[2] حيث القول بإمكانية الحبس المؤقت للمدد المحددة أعلاه؛ يتطلب أن تزيد عقوبة الحبس المقررة قانون للجريمة عن الـ 03 سنوات. وهو ما يكون ممكنا بخصوص جريمة الدخول و/أو البقاء المادي -دون الشكلي-، والمساس المنفصل بالمعطيات المعلوماتية، والأعمال التحضيرية والتالية للجرائم المذكورة وجريمة الدخول الشكلي أيضا، التي تضاعف عقوبتها ليزيد حدها الأقصى عن 03 سنوات حبس، في حال استهدفت الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، كما هو مبين أعلاه. **أنظر في ذلك:** المادة 394 مكرر3؛ المرجع نفسه.

المبحث الثاني

الإجراءات الحديثة المساعدة على التحري والتحقيق في جرائم الوسط الرقمي

زيادةً عن الإجراءات التقليدية السابقة بالذكر، يتوجب في إطار المساعدة على التحري والتحقيق المتصلين بجرائم الوسط الرقمي؛ الاعتماد على العديد من الإجراءات الأخرى التي نضفي عليها الطابع الحديث. سيما وأننا أكدنا في السابق على ضرورة العمل بإجراءات من الطبيعة الرقمية المعقدة نفسها، التي يتصف بها المسرح الجرمي الافتراضي. ولو أننا نضيف إليها بعض الإجراءات الحديثة غير الرقمية، على غرار المنع من مغادرة التراب الوطني.

لم يتفق الفقه الجنائي إلى حد الساعة على قائمة معينة، تضم هذه الإجراءات الحديثة المتصلة عموما بالتحري والتحقيق في جرائم الوسط الرقمي، خاصةً وأن التشريعات المقارنة نفسها –ومنها المشرع الجزائري– تتباين من حيث الاعتماد على إجراء دون الآخر. وهو ما انطلقنا منه لنضع قائمة بهذه الإجراءات، التي سميناها بالمساعدة، فقسمناها إلى أعمال وأوامر.

قد يذهب القضاء الجنائي عموما؛ إلى العمل بإجراءات تساعد عملي المعاينة والتفتيش المرمقنين، بغرض الوصول إلى النتيجة الإجرائية المرجوة. وهو ما قد نجده مؤسسا بنص قانوني صريح، أو يدخل ضمنا في إطار أحد الإجراءات المعمول بها بالنص. الأمر الذي نبينه فيما يلي، من خلال التطرق إلى الإجراءات الحديثة المساعدة على التحري والتحقيق في جرائم الوسط الرقمي، التي نقسمها إجرائيا إلى أعمال (مطلب أول)، وأوامر(مطلب ثانٍ).

المطلب الأول: الأعمال الحديثة المساعدة على التحري والتحقيق في جرائم الوسط الرقمي

تَبِعَ المشرع الجزائري من خلال نصوصه الحديثة، سيما القانون 09-04 السابق بالذكر؛ النهج الدولي والمقارن المعمول بهما في إطار القوانين الجنائية للدول والاتفاقيات الدولية ذات الصلة –سيما المصدق عليها–. فقنن بعض الأعمال الإجرائية الحديثة ذات الطابع الرقمي الافتراضي، كمراقبة الاتصالات الإلكترونية والتحفظ العاجل عن المعطيات الرقمية المخزنة. كما أنه حاول تقنين الأعمال المؤدية إلى تحديد هوية المشتبه فيه، وان بطريقة غير كافية، ما يدفع للبحث عن تحديد هويته؛ عبر الاعتماد على أي عمل من الأعمال الأساسية و/أو المساعدة.

وعلى العموم؛ يتم الاعتماد على الأعمال الإجرائية الحديثة، التي تعد رقمية افتراضية في مجملها؛ بغرض المساعدة على الوصول إلى النتيجة الإجرائية المرجوة. التي حددناها في ثلاثة أعمال، منطوية أساسا على مراقبة الاتصالات الإلكترونية(فرع أول)، والتحفظ العاجل على المعطيات الرقمية المخزنة(فرع ثانٍ)، وتحديد هوية المشتبه فيه(فرع ثالث).

الفرع الأول: مراقبة الاتصالات الإلكترونية

تعد "مراقبة الاتصالات الإلكترونية–Surveillance des communications électroniques"؛ من أهم الأعمال الإجرائية الحديثة ذات الطابع الرقمي الافتراضي، التي جاء بها المشرع الجزائري لأول مرة سنة 2009 بالقانون 09–04 سابق الذكر. حيث وضع لهذه المراقبة كمعل إجرائي رقمي حديث، العديد من الأحكام القانونية، التي يمكن من خلالها أن نصل إلى تحديد مفهومها القانوني، الذي نجده متميزا عن نظيره في القوانين المقارنة والاتفاقيات الدولية(أولا)، مع تحديد مجموعة من الشروط الموضوعية والإجرائية –العامة والخاصة–، التي يتوجب الالتزام بها عند إعمال هذا النوع من مراقبة الاتصالات الإلكترونية(ثانيا).

أولا: مفهوم مراقبة الاتصالات الإلكترونية

تختلف الدراسات الجنائية المتطرقة إلى إجراءات التحري والتحقيق الحديثة في مواجهة جرائم الوسط الرقمي؛ من حيث المفهوم المقدم لعمل مراقبة الاتصالات الإلكترونية، ولو أنها تتفق في المضمون التقني لهذه المراقبة. الأمر الذي يعد نتاج اختلاف قانوني بين التشريعات المقارنة، التي تعاملت مع الوضع بحسب نظرتها الخاصة من حيث تحديد العديد من القواعد على غرار الحالات والإجراءات المتبعة. وهو ما سنبينه من خلال محاولة تبيان تعريف ومميزات مراقبة الاتصالات الإلكترونية، وتمييزها عما يشابهها من أعمال إجرائية وفنية.

1. تعريف مراقبة الاتصالات الإلكترونية: كعادته لم يتطرق المشرع الجزائري بالتعريف لعمل مراقبة الاتصالات الإلكترونية، بل ترك ذلك للفقه والقضاء، حيث اكتفى بالتعرض إلى الشروط والإجراءات. الأمر الذي سنسعى في إطار دراستنا إلى التطرق إليه، من خلال البحث في التعريف المناسب لعمل مراقبة الاتصالات الإلكترونية، انطلاقا من قواعده الإجرائية الواردة في أهم الاتفاقيات الدولية ذات الصلة، والقانونين الفرنسي والجزائري، دون أن نتجاوز بعض التعريفات الفقهية القريبة إلى المعنى.

بالرجوع إلى الأحكام المنظمة لمراقبة الاتصالات الإلكترونية؛ نجد أن المشرع الجزائري قد انفرد بالتسمية، واستفاض من حيث المضمون. فتطرقا المشرع الفرنسي مثلا؛ نجده يعتمد هذا النوع من المراقبة في موضعين منفصلين، حيث اعتمد بالنص التقليدي لقانون الإجراءات الجزائية ما سماه بـــ "اعتراض المعطيات–Interception de données"، واستحدث بتعديله للقانون نفسه سنة 2011 ما سماه؛ بـــ "التقاط المعطيـــات–Captation de données". وهما عملان إجرائيان؛ يقتصر مضمونهما على المراقبة والاعتراض المتصلين بالمعطيات الرقمية ذات الصلة بالنطاق الافتراضي للوسط الرقمي فقط[1].

[1] **أنظر:** - QUEMENER Myriam, op.cit, p 152 et 157.

كما اكتفى النص الوارد في إطار اتفاقية بودابست لسنة 2001 –سابقة الذكر–؛ بعمل "اعتراض المعطيات–" دون الالتقاط، مع التأكيد على أن محل الاعتراض يقتصر على معطيات المحتوى، تحت تسمية "اعتراض المعطيات المتعلقة بالمحتوى–Interception de données relatives au contenu "، مع التأكيد على ضرورة تقنين القوانين الداخلية؛ لآليات تقنية تمكن من جمع معطيات المحتوى وتسجيلها في حينها[1]. ومنه القول بأنه مفهوم أكثر ضيقا من الذي جاء به المشرع الفرنسي، سيما وأن الاعتراض لا يتعلق إلا بمعطيات المحتوى دون باقي الأنواع، على غرار معطيات المرور أو السير.

ولم تخرج الاتفاقية العربية لمكافحة جرائم تقنية المعلومات –التي صدقت عليها الجزائر–؛ كثيرا عن التسمية والمضمون الواردين في اتفاقية بودابست المبين أعلاه، إلا من حيث استبدال مصطلح المعطيات بالمعلومات. حيث تم الاعتماد على تسمية "اعتراض معلومات المحتوى"، مع التأكيد على ضرورة التزام الدول الأطراف؛ بتبني الإجراءات القانونية الضامنة لانجاز الجمع أو التسجيل من خلال استعمال الوسائل الفنية اللازمة[2]. مع التأكيد على أن الاتفاقية العربية؛ لم تتطرق إلى عمل مراقبة الاتصالات الإلكترونية، لا بالتسمية نفسها ولا بالمضمون المستفيض نفسه[3].

رجوعا إلى المشرع الجزائري؛ نجده قد عمل بالإطار الوارد في كل من اتفاقية بودابست والاتفاقية العربية المبينين أعلاه، وكذلك قانون الإجراءات الجزائية الفرنسي. لكن مع استعمال تسمية ومضمون مغايرين نوعا ما، حيث اعتمد تسمية مراقبة الاتصالات الإلكترونية، مع التأكيد على أنها معمول بها لغرض التجميع والتسجيل المنصبين على كل الاتصالات الإلكترونية، دون الاكتفاء بتلك المتصلة بالمعطيات الرقمية[4].

وعلى العموم يتبين مما ورد بالقانون 09–04 سابق الذكر؛ أن المشرع قد وضع أحكاما إجرائية تقوم عليها مراقبة الاتصالات الإلكترونية. فبالإضافة إلى كونها لا تقتصر على مراقبة الاتصالات الرقمية؛ يتوجب أن تنجز وفق شروط عامة وأخرى خاصة تنطوي على الحالات المحددة حصرا، بالإضافة إلى إلزامية إتباع القواعد الإجرائية على حسب الحالة، الدائرة أساسا بين الدورين الوقائي والكفاحي[5].

---

[1] **أنظر:** - Art 21; Convention sur la cybercriminalité- Budapest, op.cit.

[2] **أنظر:** المادة 29؛ مرسوم رئاسي رقم 14-252، مرجع سابق.

[3] ولو أن ذلك يعد أمرا منطقيا ومقبولا قانونا، لكون الاتفاقية بطبيعتها لا تهتم بتحديد التسمية والقواعد الإجرائية الدقيقة. حيث بمجرد أن المادة 29 المبينة أعلاه؛ قد نصت بضرورة الاعتماد على الوسائل الفنية للجمع والتسجيل؛ يعد أمرا كافيا، يفتح المجال أمام المشرع الوطني لإيجاد الآلية الرقمية المناسبة. ولو أن المشرع الجزائري؛ تجاوز المضمون الرقمي إلى غيره، كما بين أدناه.

[4] الأمر الذي نفهمه بداهةً؛ من التعريف الفضفاض الذي اعتمده المشرع الجزائري بخصوص الاتصالات الإلكترونية. التي جعلها لكل أشكال التراسل المنجزة عبر أي وسيلة الكترونية، التي قد تتمثل في شبكة الاتصال الدولية، كما قد تنطوي على الاتصال الهاتفي التقليدي، والفاكس والتيلكس...الخ. **أنظر في ذلك:** المادة 3 والمادة1/2-و؛ قانون رقم 09-04، مرجع سابق.

[5] **أنظر:** المادة 29؛ مرسوم رئاسي رقم 14-252، المرجع نفسه.

يمكن القول أن المشرع الجزائري في هذا الإطار؛ قد أعطى الكثير من الخصوصية لمراقبة الاتصالات الإلكترونية. الأمر الذي يمكننا من خلاله أن نضع تعريفا لها، يتناسب مع قواعد التشريع الجزائري المختلفة عن نظيرتها المقارنة. إلا أننا نعرج قبل ذلك لطرح بعض التعريفات الفقهية ذات الصلة، التي نجدها الأقرب إلى مفهوم القانون الجزائري.

فيعرف البعض مراقبة الاتصالات الإلكترونية، تحت تسمية "المراقبة التقنية"؛ على أنها: "التقاط أو تجميع البيانات ومحتوى الاتصالات أثناء بثها أي لحظة النقل عبر الاتصال –في الزمن الفعلي لنقلها بين الأطراف–"[1]. كما تعرف أيضا وفق تسمية "اعتراض مضمون البيانات"؛ بأنها: "جمع أو تسجيل مضمون البيانات التي تنقل عبر وسائل الاتصالات في حينها، حتى تتمكن السلطات المختصة في الدولة من التعرف على الاستخدامات غير المشروعة لأنظمة الاتصالات بما يكفي منع ارتكاب العديد من الجرائم"[2].

انطلاقا مما قدمناه في هذا الإطار، سيما من حيث القول بأن مراقبة الاتصالات الإلكترونية؛ عمل إجرائي معتمد ومعمول به في الإطارين الاتفاقي الدولي والمقارن، وان بتسميات ومضمون مغايرين عن الوارد في القانون الجزائري، ووقوفا عند القواعد القانونية الواردة بالمادتين 03 و04 من القانون 09-04 السابقة بالذكر –التي سنتسع فيها فيما هو قادم–؛ يمكن أن نضع تعريفا دقيقا لهذه المراقبة الفنية، وفق الخصوصية التي أضفاها عليها القانون الجزائري.

فنقول أن مراقبة الاتصالات الإلكترونية؛ عبارة عن: "عمل إجرائي رقمي حديث، يقود إلى وضع الترتيبات التقنية اللازمة لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها، جاء به المشرع الجزائري سنة 2009، ليمارسه جهاز الشرطة القضائية في كل من مرحلة التحري وإجراءات التحقيق، بشروط موضوعية وإجرائية معينة، وذلك بهدف الوقاية من بعض الجرائم الخطيرة أو لمكافحة الجريمة صعبة المواجهة".

2. مميزات مراقبة الاتصالات الإلكترونية: يمكن من خلال الأحكام القانونية التي استحدثها المشرع الجزائري بالقانون 09-04 –سابق الذكر– لينظم بموجبها عمل مراقبة الاتصالات الالكترونية؛ أن نقف عند العديد من المميزات سابقة الذكر والإشارة في التعريف المقترح أعلاه. التي –المميزات– تبين لنا أنها تقوم على الازدواجية في الطرح، من خلال القول بأن مراقبة الاتصالات الإلكترونية؛ هو عمل إجرائي مزدوج من حيث الممارسة التقنية، والطبيعة والبعد الجنائي الموضوعي وكذا الإجرائي.

---

[1] **أنظر:** مصطفى علي خلف، مرجع سابق، ص 204.

[2] يبدوا أن هذا التعريف يجعل من مراقبة الاتصالات الإلكترونية؛ بدور واحد ينطوي على الوقاية، ويستبعد الدور الكفاحي، ما يجله تعريف قاصر موضوعا. **أنظر في ذلك:** مفتاح بوبكر المطردي، مرجع سابق، ص 50.

أ- **ميزة الازدواجية التقنية بين المراقبة القبلية والتجميع والتسجيل عند الاتصال:** يتبين مما ورد في المادة 03 من القانون 09-04 سابق الذكر؛ أن المشرع فصل بين مراقبة الاتصالات التقنية من جهة، وتجميع وتسجيل محتواها في حينها من جهة أخرى. حيث أكد على أن الجهة المختصة تقوم بوضع الترتيبات التقنية اللازمة؛ بغرض مراقبة الاتصالات الإلكترونية في الأصل، مع تجميع وتسجيل محتواها إن وجد، ولم يعبر بمراقبة الاتصالات الإلكترونية من أجل التجميع والتسجيل. فالعمل هو وضع الترتيبات التقنية؛ والغرض مزدوج يدور بين المراقبة من جهة والتجميع والتسجيل من جهة أخرى[1].

فصل المشرع بين المراقبة أولا والتسجيل والتجميع ثانيا؛ يقود للقول والجزم أن ممارسة عمل المراقبة الإلكترونية سيكون بصورة مطلقة، حيث يقوم المعني بها بالمراقبة الرقمية لوسائل اتصال المشتبه فيه أو المتهم –أو ربما غيره–؛ بصورة دورية فيترقب أي اتصال ليجمعه ويسجله، حتى وان كان اتصالا عاديا لا علاقة له بالإجرام. وهذا ما يفتح المجال للتساؤل حول حرمة الحياة الخاصة، التي تنتهك بجمع وتسجيل معلومات غير مفيدة جنائيا[2].

ب- ميزة الازدواجية في الطبيعة بين الوقاية والمكافحة: يتبين لنا أيضا أن المشرع؛ لم يقف عند حد تقرير العمل بمراقبة الاتصالات الإلكترونية من أجل مكافحة الجريمة، بل تجاوز ذلك إلى حد القول بأنه قابل للممارسة بغرض الوقاية من بعض الجرائم المحددة حصرا، وبشروط وإجراءات خاصة[3]. الأمر الذي يتبين صراحةً من خلال الحالات الأربعة المحددة حصرا من المشرع لممارسة هذه المراقبة، التي نجد منها حالتين تمارس المراقبة من خلالهما قبل ارتكاب الجريمة[4]، وهو ما نعتبره بمثابة الإجراء الإداري الممارس في إطار الضبط الإداري لا القضائي.

وعليه نقف عند الملاحظة نفسها المقدمة في الميزة الأولى، فنقول أن ممارسة الدور الوقائي سيقود إلى مراقبة الاتصالات الإلكترونية في مجملها قبل ارتكاب الجريمة ولمجرد الشك في أنها سترتكب. هذا من يضرب بقواعد حقوق الإنسان المقررة لحماية حرمة الحياة الخاصة عرض الحائط، وان كان من الممكن تبرير ذلك، بالقول باستهداف هذه المراقبة الوقاية؛ من أخطر الجرائم الممكن ارتكابها كالجريمة الإرهابية، وبالتالي حماية الصالح العام على حساب انتهاك سرية الأفراد والمؤسسات.

---

[1] **نص المادة:** "...وضع ترتيبات تقنية **"لـ"** مراقبة الاتصالات الإلكترونية **"و"** تجميع وتسجيل محتواها في حينها...".

[2] حيث قد يتقبل أمر تجميع وتسجيل معطيات رقمية؛ لها علاقة بالجريمة وتقود إلى إظهار الحقيقة، من منطلق ميل كفة تحقيق المصلحة العامة التي تفرض متابعة الجناة على حساب ضمان المصلحة الخاصة التي تفرض حماية الحياة الخاصة. لكن لا يمكن بأي شكل من الأشكال؛ أن نتصور السماح بمراقبة وتجميع وتسجيل معطيات رقمية، جد خاصة للأفراد، وهي لا تفيد لا من قريب ولا من بعيد في إظهار الحقيقة الجنائية المبحوث عنها.

[3] وهذا هو أساس قولنا فيما سبق باكتساب إجراءات متابعة جرائم الوسط الرقمي؛ لخاصية الدورين الوقائي والكفاحي معا. رغم استقرار الدور الكفاحي الوحيد للإجراءات الجزائية عموما؛ في مواجهة الجريمة التقليدية والحديثة غير الرقمية.

[4] **أنظر:** المادة 1/04-أ وب؛ قانون رقم 09-04، مرجع سابق.

ج- ميزة الازدواجية الموضوعية بين جرائم الوسط الرقمي والجريمة التقليدية: الثابت من خلال مضمون القانون 09-04؛ أن المشرع يبحث من خلال ممارسة عمل مراقبة الاتصالات الإلكترونية -وحتى التفتيش والحجز المرقمنين-؛ على استخراج الدليل الرقمي السابق بالدراسة. وذلك من دون النص على أنه سيستعمل في إثبات جرائم الوسط الرقمي أو الجريمة التقليدية أو الاثنين معا. حيث تخلوا المادتين 03 و04 منه -سابقتي الذكر-؛ من أي إشارة تحديد نوع الجريمة المتعامل معها إجرائيا.

وبالإضافة إلى ذلك قد نص المشرع صراحةً على أن مراقبة الاتصالات الإلكترونية -والتفتيش والحجز المرقمنين-؛ يستعمل في مواجهة الإجرام بكل أنواعه التقليدي والرقمي، وذلك بنصه: "...يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية..."[1]. ما يفيد أن الدور الوقائي معياره النظام العام وليس نوع الجريمة -التقليدية أو الحديثة-، وكذلك الدور الكفاحي معياره التحري والتحقيق الجاري، سواءً تعلق بجريمة تقليدية أو حديثة رقمية أو حديثة غير رقمية.

د- ميزة الازدواجية الإجرائية بين التحري والتحقيق: يبدوا أن المشرع قد تعامل مع مراقبة الاتصالات الإلكترونية بالطريقة الإجرائية نفسها المتصلة بعمل التنصت، حيث أضفى عليها ميزة الازدواجية الإجرائية، فجعلها ممكنة الممارسة في إطار مرحلة التحري وكذلك من خلال إجراءات التحقيق القضائي. والدليل على ذلك نصه -المشرع-؛ بـــ:"...يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية..."[2]، وكذلك بـــ: "لمقتضيات التحريات والتحقيقات القضائية..."[3].

وعليه يمكن القول؛ أن المشرع بعد أن جاء بالازدواجية التقنية، ونظيرتها من حيث الطبيعة وكذلك الازدواجية الموضوعية؛ أكد على النهج نفسه بخصوص إجراءات التحري شبه القضائي والتحقيق القضائي معا. ما يجعل من مراقبة الاتصالات الإلكترونية؛ بمثابة العمل الرقمي الحديث المقيد نوعا ما في إطار ممارسة الدور الوقائي، خاصةً عبر الاقتصار على الوقاية من أخطر الجرائم المحددة حصرا، ومن دون تقييد لا تقني ولا موضوعي بخصوص الدور الكفاحي.

3. تمييز مراقبة الاتصالات الإلكترونية عما يشابهها: نظرا لتقارب العديد من المفاهيم الإجرائية الحديثة، ذات العلاقة بالوسط الرقمي عموما؛ يتوجب علينا البحث في عناصر التمييز بينها، سيما تلك التي يمكن أن ينظر إليها غير المختص على أنها لا فرق بينها وبين عمل مراقبة الاتصالات الالكترونية. حيث نفرق من خلال ذلك بين هذه الأخيرة -مراقبة الاتصالات الإلكترونية-، والتنصت الهاتفي من جهة والتحفظ العاجل على المعطيات الرقمية المخزنة من جهة أخرى.

---

[1] **أنظر:** المادة 03؛ قانون رقم 09-04، مرجع سابق.

[2] **أنظر:** المادة والمرجع نفسهما.

[3] **أنظر:** المادة 1/04-ج؛ المرجع نفسه.

أ- التمييز بين مراقبة الاتصالات الإلكترونية والتنصت الهاتفي: لو أخذنا بالمفهوم العام للاتصالات الإلكترونية الذي جاء به المشرع الجزائري عنده تعريفه لها بالقانون 09-04؛ لقلنا أنه لا فرق بين الاثنين، بل التنصت الهاتفي هو نوع من أنواع مراقبة الاتصالات الإلكترونية. خاصةً وأنه -المشرع- يعتبر الاتصال ممكن الانجاز بأي وسيلة الكترونية كانت، التي قد تتمثل في شبكة الاتصال الدولية -التي تعد إلكترونية رقمية-، والهاتف التقليدي والحديث غير الرقمي وكذا التيليكس والفاكس...الخ[1].

وهو ما أكد عليه الفقه المصري عند محاولته التفرقة بين الاتصالات التقنية والاتصالات الهاتفية، حيث تم التوصل إلى أنهما متشابهين ولا فرق بينهما نظرا لاعتمادهما على خطوط الهاتف -الألياف أو الكابلات-، كقاعدة أساسية للنقل والاتصال. وذهب بعد ذلك -الفقه المصري-؛ إلى حد القول بإمكانية تطبيق قواعد الاتصالات الهاتفية على الاتصالات التقنية لما بينهما من تماثل[2].

إلا أننا نرى غير ذلك؛ فالفرق بين الاثنين واضح وجلي. حيث التنصت الهاتفي هو إجراء تقليدي وجد -كما بينا سابقا- لمواجهة النطاق الافتراضي الهاتفي غير الرقمي، وفق أحكام المواد من 65مكرر05 إلى 65مكرر 10 "ق.إ.ج" السابقة بالذكر. ولو كان هذا الإجراء كافيا لمراقبة الاتصالات الرقمية؛ لما تدخل المشرع سنة 2009 ليستحدث مراقبة الاتصالات الإلكترونية بالقانون 09-04. ولو قلنا بغير ذلك، لسلمنا بإحدى الفرضيتين، فإما أن المشرع لا يتقن التفرقة بين الاثنين، أو أنه يتقنها وما استحداثه لمراقبة الاتصالات الإلكترونية بالقانون 09-04؛ إلا إلغاءً ضمنيا لأحكام التنصت الهاتفي، وتعويضها بالمراقبة الحديثة، مع فتح مجالها وفق ما بينا بالمميزات سابقة الذكر[3].

ب- التمييز بين مراقبة الاتصالات الإلكترونية والتحفظ العاجل على المعطيات الرقمية المخزنة: ينقسم التحفظ العاجل على المعطيات -كما سنبين- إلى قسمين أساسيين. حيث قد يتحفظ بصورة عاجلة على معطيات المحتوى، كما قد يتحفظ بالطريقة نفسها على معطيات السير أو المرور. فتتفق مراقبة الاتصالات الإلكترونية مع التحفظ العاجل على معطيات المحتوى؛ في كونهما يتعلقان بمعطيات المحتوى، وكون المراقبة قد تكون مرحلة سابقة للتحفظ الذي ينجز بعد المراقبة والتجميع والتسجيل. إلا أنهما يختلفان من حيث؛ أن المراقبة دائما تتعلق بجمع وتسجيل المعطيات عند انجاز الاتصال، وأما التحفظ العاجل عن معطيات المحتوى، فينصب على تلك المخزنة سواءً كنتيجة للمراقبة أو كنتيجة لعمل رقمي آخر[4].

---

[1] **أنظر:** المادة 1/02-و؛ قانون رقم 09-04، مرجع سابق.

[2] **أنظر:** مصطفى علي خلف، مرجع سابق، ص 205 و206.

[3] كان من الأجدر على المشرع؛ أن يستحدث مراقبة الاتصالات الإلكترونية -تحت تسمية مراقبة الاتصالات الرقمية- التي لا تنجز إلا في النطاق الافتراضي الرقمي، تاركا بذلك تنظيم مراقبة الاتصالات الهاتفية للنص التقليدي المتصل بالتنصت.

[4] هذا ما نستنتجه من قواعد القانون الجزائري سارية المفعول في هذا الصدد، سيما ما ورد بالقانون 09-04 والاتفاقية العربية لمكافحة جرائم تقنية المعلومات. **أنظر في ذلك:** المواد 03 و04 و10؛ قانون رقم 09-04، المرجع نفسه. **وأنظر أيضا:** المواد من 23 إلى 29؛ مرسوم رئاسي رقم 14-252، مرجع سابق.

وأما من حيث التمييز بين مراقبة الاتصالات الإلكترونية والتحفظ العاجل على معطيات السير أو المرور؛ فلا تشابه بينهما على الإطلاق، نظرا لكون المراقبة تنصب على معطيات المحتوى، وأما التحفظ العاجل في هذه الحالة، فيتعلق بمعطيات السير أو المرور التي لها علاقة بالمستخدم وليس بمحتوى الاتصال. كما أن المراقبة تتعلق بجمع وتسجيل المعطيات في حين الاتصال، وأما التحفظ فيتعلق بمعطيات السير سابقة التخزين من قبل مقدمي الخدمات[1].

ثانيا: شروط ممارسة مراقبة الاتصالات الإلكترونية

يمكن من خلال التطرق إلى أحكام القانون 09-04 المتعلقة بعمل مراقبة الاتصالات الإلكترونية، بنوع من التحليل والنظرة القانونية الدقيقة؛ أن نستخرج العديد من الشروط واجبة الاحترام لممارسة مراقبة الاتصالات الإلكترونية. التي يتبين أن المشرع قد قسمها ضمنا إلى شروط عامة وأخرى خاصة، حيث يتوجب أن تتوفر في كل ممارسة لمراقبة الاتصالات الإلكترونية –وحتى في التفتيش والحجز الرقميين–؛ مجموعة من الشروط العامة، التي لا تكفي لوحدها بل تتطلب توفر شروط خاصة أخرى تختلف من حالة إلى أخرى، مع مراعاة الدورين الوقائي والكفاحي.

1. الشروط العامة للممارسة مراقبة الاتصالات الإلكترونية: يتبين من خلال أحكام المادة 03 من القانون 09-04؛ أن المشرع قد حدد شرطين عامين لممارسة مراقبة الاتصالات الإلكترونية[2]، اللذان نسميهما بالشرط الموضوعي والشرط الإجرائي. حيث ينطوي شرط الإطار الموضوعي؛ على ضرورة عدم مساس مراقبة الاتصالات الإلكترونية بسرية المراسلات والاتصالات، ما يقود للقول بأن منفذ هذه المراقبة؛ عليه أن يكتم السر المهني المتعلق بمضمون الاتصالات محل التجميع والتسجيل وغيرها، ولا يفشي به إلا في الإطار الإجرائي المسموح به، وإلا يكون قد ارتكب جريمة المساس بحرمة الحياة الخاصة المعاقب عليها بموجب قانون العقوبات[3].

وأما الشرط الإجرائي؛ فيتمثل في جزئيتين أساسيتين. ينطوي الأول على الهدف الإجرائي من وراء ممارسة مراقبة الاتصالات الالكترونية، ويتعلق الثاني باحترام القواعد الإجرائية. حيث تهدف هذه المراقبة؛ إلى إما الوقاية عبر حماية النظام العام قبل المساس به –وهي المقيدة بالشروط الخاصة التالية بالدراسة–، أو مكافحة الجريمة بعد ارتكابها من خلال مساعدة التحريات أو التحقيقات الجارية.

---

[1] هذا ما نستنتجه أيضا؛ من قواعد القانون الجزائري سارية المفعول، سيما ما ورد بالقانون 09-04 والاتفاقية العربية لمكافحة جرائم تقنية المعلومات. **أنظر في ذلك:** المواد 03 و04 و10 و11؛ قانون رقم 09-04، المرجع نفسه. **وأنظر أيضا:** المادتان 24 و28؛ مرسوم رئاسي رقم 14-252، مرجع سابق.

[2] **نص المادة:** "مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون...".

[3] **أنظر:** المادة 303مكرر وما يليها؛ أمر رقم 66-156، مرجع سابق.

كما أنه كجزئية إجرائية ثانية؛ يتوجب على منفذ مراقبة الاتصالات الإلكترونية؛ أن يتقيد بالقواعد الإجرائية الخاصة الواردة بالقانون 09-04 نفسه –التي سنتطرق إليها مع طرح الشروط الخاصة–، وفي حال مواجهة أي فراغ يتوجب الرجوع إلى القواعد العامة الواردة بقانون الإجراءات الجزائية، المتمثلة على الأرجح في الأحكام التقليدية المطبقة على التنصت سابقة الذكر.

2. الشروط الخاصة للممارسة مراقبة الاتصالات الإلكترونية: حدد المشرع بالقانون 09-04 أيضا مجموعة من الشروط الخاصة، التي يجب احترامها عند ممارسة عمل مراقبة الاتصالات الإلكترونية. حيث يتوجب أولا التفرقة بين المراقبة المنجزة بطلب من الجهات الوطنية المختصة أو من نظيرتها الأجنبية. حيث بخصوص هذه الأخيرة؛ لم يوضح المشرع الشروط الخاصة لمارستها بل ترك المجال مفتوحا، لينظم بالاتفاقيات الدولية ذات الصلة بالمساعدة الدولية المتبادلة ومبدأ المعاملة بالمثل[1].

أما بخصوص الطلبات الصادرة عن الجهات القضائية الوطنية؛ ففرق المشرع بين حالتين. حيث يمكن أن تنجز مراقبة الاتصالات الإلكترونية بهدف وقائي، لتوخي وقوع جرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة –حصرا–. التي لم يبين –المشرع– هل هي جرائم تقليدية ترتكب أو يسهل ارتكابها عبر النطاق الافتراضي للوسط الرقمي، أم جرائم تقليدية غير مرقمنة أم الاثنين معا، ولو أننا نجدها تقصد الاثنين معا، فينتج عن مراقبة الاتصالات الالكترونية؛ دليل رقمي تثبت به الجريمة التقليدية والمرقمنة في الآن نفسه. مع التأكيد على أنها تمارس من قبل الشرطة القضائية التابعة للهيئة الوطنية –السابقة بالذكر–، لمدة 06 أشهر قابلة للتجديد، بموجب إذن صادر عن النائب العام بمجلس قضاء الجزائر العاصمة[2].

كما أنه في إطار الدور الوقائي نفسه؛ يمكن للشرطة القضائية أن تمارس وفق الإجراءات العادية الواردة في قانون الإجراءات الجزائية؛ عمل مراقبة الاتصالات الإلكترونية، لتفادي الاعتداء المحتمل على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني[3]. الأمر الذي نجده متصلا بنوع محدد من جرائم المساس بأنظمة المعالجة الآلية للمعطيات، التي سبق للمشرع وأن شدد من العقوبة المقررة لها، نظرا لمساسها بمصالح جد حساسة في الدولة، ما يكسبها طابع الإجرام الخطير[4].

---

[1] مع التأكيد على أن طلب المساعدة القضائية الدولية، الذي يرد لممارسة مراقبة الاتصالات الإلكترونية -أو لأي إجراء آخر-؛ يجب أن يقابل بالرفض إذا كان من شأنه المساس بالسيادة الوطنية أو النظام العام. **أنظر في ذلك:** المادة 1/04-د والمادة 18؛ قانون رقم 09-04، مرجع سابق.

[2] **أنظر:** المادة 1/4-أ والمادة 03؛ المرجع نفسه.

[3] **أنظر:** المادة 1/4-ب؛ المرجع نفسه.

[4] لكن طابع الإجرام الخطير؛ يتطلب بداهةً أن نصف السلوك بالجناية لا الجنحة. وهو ما نجد أن المشرع بخصوصه في إطار قانون العقوبات؛ قد جعل من الاعتداء على المنظومة المعلوماتية بما يهدد المصالح الحساسة المبينة أعلاه؛ بمثابة =

بالإضافة إلى الدور الوقائي؛ يمكن أن ينجز عمل مراقبة الاتصالات الإلكترونية؛ بغرض مكافحة الجريمة عموما. حيث سمح المشرع لأجهزة التحري والتحقيق معا؛ اللجوء إلى هذا النوع من المراقبة الحديثة لكن بشرطين أساسيين، يتمثل الأول في تعذر الوصول إلى النتيجة الإجرائية المرجوة من دون الاعتماد على المراقبة، وينطوي الثاني على ضرورة الحصول على الإذن المكتوب من الجهة القضائية المختصة خاصةً، والتقيد بالقواعد الإجرائية عموما[1].

فيتبين مما ذكر أعلاه؛ أن المشرع لم يربط ممارسة المراقبة الكفاحية بجرائم الوسط الرقمي، بل جاء بمعيار إجرائي مفاده تعذر الوصول إلى النتيجة الإجرائية من دون اللجوء إلى مراقبة الاتصالات الالكترونية. وهو ما لنا فيه قول، حيث بخصوص الجريمة التقليدية غير المرقمنة؛ لايمكن تصور قيام التعذر الإجرائي إلا نادرا وفي أخطر وأعقد الجرائم، إلا أنه بخصوص جرائم الوسط الرقمي بنوعيها؛ فالتعذر يكون قائما في أغلب الأحيان، نظرا لخصوصية مسرحها الافتراضي. ما يقود للقول أن الواقع الإجرائي؛ سيضفي الطابع الاستثنائي على مراقبة الاتصالات الإلكترونية، بخصوص مكافحة الجريمة التقليدية غير المرقمنة، والطابع الأصلي الأساسي؛ إذا ما تعلق الأمر بمكافحة جرائم الوسط الرقمي.

وأما بخصوص الإذن المكتوب؛ فالمشرع لم يبين الجهة القضائية التي تصدره ولا تلك التي تنفذه، وذلك سواءً بخصوص المراقبة الكفاحية وحتى الوقائية المتصلة بالاعتداء على المنظومة المعلوماتية الحساسة. الأمر الذي لو ربطناه بالشرط الإجرائي العام السابق بالذكر والوارد بالمادة 03 من القانون 09-04؛ لقلنا بحتمية إعمال القواعد الإجرائية نفسها المتصلة بالتنصت السابقة بالذكر.

الفرع الثاني: التحفظ العاجل على المعطيات الرقمية المخزنة

بالإضافة إلى عمل مراقبة الاتصالات الإلكترونية؛ ذهب المشرع الجزائري كغيره من نظرائه، وتنفيذا لالتزاماته الدولية؛ على تقنين عمل إجرائي آخر يقوم على الحداثة الرقمية نفسها، ويتمثل في التحفظ العاجل على المعطيات الرقمية المخزنة. العمل الذي يعد من أهم ما استحدثه المشرع، بخصوص الإجراءات الرقمية غير المسبوق التعامل مع مثلها في النطاق التقليدي المعروف. الأمر الذي سنحاول التطرق إليه؛ عبر تبيان المفهوم العام لعمل التحفظ العاجل على المعطيات الرقمية المخزنة(أولا)، ومن ثم التعريج على أنواع المعطيات المخزنة محل التحفظ(ثانيا).

= الجنحة مشددة العقوبة وليس الجناية. ما يفتح المجال للتساؤل حول مدى السماح بالمراقبة الوقائية الماسة بحرمة الحياة الخاصة، للوقاية من مجرد جنحة مشددة وليس جناية خطيرة. ولو أن الأمر يعد أبعد من ذلك؛ حيث سمح المشرع بالمراقبة الوقائية من الاعتداء على منظومة معلوماتية اقتصادية؛ رغم أنه يعتبره مجرد جنحة بسيطة، لها العقوبة نفسها المقررة للمساس بالمنظومة العادية، نظرا لعدم ورودها ضمن أحكام الجنحة المشددة، المتصلة بالدفاع الوطني والهيئات ومؤسسات القانون العام. مع التأكيد على إمكانية تكييف هذه الجرائم بوصف الجناية، إذا ما وجد نص تقليدي بذلك، وهو ما أكدت عليه المادة نفسها المقررة للتشديد في إطار الجنحة. **أنظر في ذلك:** المادة 394مكرر3؛ أمر رقم 66-156، مرجع سابق.

[1] **أنظر:** المادة 1/04-ج والمادة 2/4؛ قانون رقم 09-04، مرجع سابق.

أولا: مفهوم التحفظ العاجل على المعطيات الرقمية المخزنة

يعد عمل التحفظ العاجل من بين أهم الأعمال الإجرائية الرقمية، غير المسبوق التعامل معها ولا مع مثلها جنائيا. الأمر الذي وسع درجة التباين بين الدراسات الفقهية ذات الصلة، التي لم تستقر على مفهوم واحد، خاصةً وأن أغلبها تتطرق إلى التحفظ العاجل على معطيات السير دون المحتوى. ما يضفي صفة القصور؛ على التعريفات المطروحة بالأصل والأحكام الناتجة عنها بالتبعية. وعلى العموم؛ سنذهب فيما يلي؛ إلى دراسة عمل التحفظ العاجل على المعطيات الرقمية المخزنة، بمفهومه العام الموسع، وذلك من حيث التعريف به، ومحاولة إبراز أهم النتائج المترتبة عنه.

1. تعرف التحفظ العاجل على المعطيات الرقمية المخزنة: أول ما يلاحظ على أغلب الدراسات السابقة، ذات الصلة بالمواجهة الإجرائية لجرائم الوسط الرقمي؛ أنها عند التطرق إلى عمل التحفظ العاجل على المعطيات الرقمية المخزنة، تكتفي بتلك المتعلقة بحركة السير أو المرور من دون نظيرتها المتصلة بالمحتوى. الأمر الذي يؤسس في العادة، على أن القانون الجزائري الداخلي والاتفاقي –وحتى غير ذلك كاتفاقية بودابست لسنة 2001 سابقة الذكر–؛ لم يتطرق من حيث التحفظ العاجل على المعطيات المخزنة إلا لتلك المتعلقة بحركة السير أو المرور، أو كما تسمى في الإطار الاتفاقي بـــ "معطيات تتبع المستخدمين–données relatives au trafic"[1].

إلا أننا بالرجوع إلى المواد القانونية نفسها المؤسس عليها القول السابق؛ نجدها تتباين في النص على ذلك. حيث اكتفى القانون الجزائري –بالنص التشريعي– بعمل التحفظ العاجل المتصل بمعطيات حركة السير دون المحتوى، في إطار القانون 09–04 سابق الذكر[2]. على أنه اعتمد بالنص الاتفاقي؛ على الاثنين معا، وان بالذكر الصريح للتحفظ المتعلق بمعطيات حركة السير وبالورود الضمني لنظيره المتصل بالمحتوى. حيث عبرت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010؛ بـــ "تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأمر أو الحصول على الحفظ العاجل للمعطيات المخزنة بما في ذلك معلومات تتبع المستخدمين"[3].

---

[1] **أنظر:** المادتان 23 و24؛ مرسوم رئاسي رقم 14-252، مرجع سابق. **وأنظر أيضا:** المادتان 10 و11؛ قانون رقم 09-04، مرجع سابق. **وأنظر كذلك:** Art 16 et 17; Convention sur la cybercriminalité- Budapest, op.cit. -

[2] وهو ما يفهم من نص المادة 10 منه، التي عبرت بـ: "...لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها، وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 أدناه...". حيث جمع وتسجيل معطيات المحتوى في حينها؛ يدخل ضمن إطار عمل مراقبة الاتصالات الإلكترونية وليس الحفظ العاجل لمعطيات المحتوى المخزنة، نظرا لكون المراقبة أحد مصادر معطيات المحتوى المخزنة التي يمكن حفظها فيما بعد. وأما المعطيات التي يتعين حفظها وفق المادة 11؛ فالمقصود بها معطيات حركة السير، كما سنوضح لاحقا.

[3] وهو النص المنقول حرفيا من اتفاقية بودابست لسنة 2001. والذي استنتاجا من عبارة "بما في ذلك"؛ يمكن القول أن المقصود بالأساس هي معطيات المحتوى السابق تخزينها، مع إمكانية ممارسة عمل الحفظ العاجل نفسه على معطيات المستخدمين السابق تخزينها أيضا -معطيات حركة السير-. **أنظر في ذلك:** المادة 1/23؛ مرسوم رئاسي رقم 14-252، المرجع نفسه. **وأنظر أيضا:** Art 16/1; Convention sur la cybercriminalité- Budapest, idem. -

لايمكن الانطلاق من خلو القانون 09-04، من التطرق إلى التحفظ العاجل على معطيات المحتوى المخزنة؛ للقول بأنه عمل غير معتمد في إطار القانون الجزائري، حيث يمكن لجهات التحري والتحقيق الاعتماد عليه في مواجهة جرائم الوسط الرقمي -وحتى غيرها-، مع التقيد بالقواعد الإجرائية العامة الواردة بقانون الإجراءات الجزائية. ونؤسس لذلك، بالقول أنه إجراء وارد في الاتفاقية العربية التي تعد من مصادر القانون الجزائري بعد التصديق عليها سنة 2014. وكذلك لكون المشرع بالقانون نفسه؛ قد اعتمد نوعين من مزودي الخدمات[1].

ونرجع وقوع المشرع بالقانون 09-04؛ في هفوة الاكتفاء بالتحفظ العاجل على معطيات السير المخزنة دون نظيرتها المتعلقة بالمحتوى؛ إلى تطرقه لذلك، على أساس أنه أحد التزامات مقدمي الخدمات، وليس بكونه عمل إجرائي مستقل. وهو ما عقد الأمر أيضا من حيث فهمه والتفرقة بينه وبين عمل مراقبة الاتصالات الالكترونية من جهة، والحجز بعد التفتيش المرقمن من جهة أخرى[2].

فقد يفهم البعض أن التحفظ العاجل على معطيات المحتوى المخزنة؛ هو نفسه عمل مراقبة الاتصالات الإلكترونية -ما دفع المشرع لتفادي التكرار-، سيما وأنهما يقعان على معطيات المحتوى. الأمر الذي نستبعده تماما، حيث تعد المراقبة؛ بمثابة العمل المنجز في الوقت الفعلي للاتصال بهدف تجميع وتسجيل محتواه في حينه، وأما التحفظ العاجل فيقع على معطيات المحتوى السابق تخزينها، التي لها العديد من المصادر، على غرار إمكانية التحفظ على معطيات المحتوى التي سبق تجميعها وتسجيلها في وقت سابق، كنتيجة عن عمل مراقبة الاتصالات الإلكترونية[3]. وأما بخصوص الحجز بعد التفتيش الرقمن فينجز -كما بينا سابقا-؛ من قبل السلطة القضائية أو شبه القضائية المختصة، على المعطيات التي تم العثور عليها في النطاق الافتراضي محل التفتيش، ولا يتحفظ بها لدى مزود الخدمة.

وعلى العموم قد نجد من يعرف عمل التحفظ العاجل على المعطيات الرقمية المخزنة، ولو في إطاره الضيق المتصل بمعطيات حركة السير دون نظيرتها المتصلة بالمحتوى؛ على أنه: "عملية من مهام مقدمي الخدمات، يهدف إلى حماية المعطيات التي سبق وجودها في شكل مخزن من كل ما يمكن أن يتسبب في إتلافها أو تجريدها من صفتها أو حالتها الأصلية"[4].

---

[1] وهو ما سنبينه؛ عند التطرق إلى أنواع المعطيات الرقمية المخزنة محل التحفظ العاجل.

[2] الأمر الذي لم تقع فيه الاتفاقية العربية -واتفاقية بودابست لسنة 2001 بالأساس-، التي نصت على العديد من الأعمال الإجرائية بصورة مستقلة عن التزامات مزودي الخدمات. فأوردت التحفظ العاجل على المعطيات المخزنة بنوعيه في عمل واحد، ونصت على عمل مراقبة الاتصالات الإلكترونية بصورة مستقلة؛ تحت عنوان اعتراض معلومات المحتوى. كما نصت على الحجز بعد التفتيش المرقمن المتصل بالمحتوى وغيره تحت عنوان ضبط المعلومات المخزنة. **أنظر في ذلك:** المواد 23 و27 و29؛ مرسوم رئاسي رقم 14-252، مرجع سابق.

[3] **أنظر:** مفتاح بوبكر المطردي، مرجع سابق، ص 50.

[4] **أنظر:** جمال براهيمي، (التحقيق الجنائي في الجرائم الإلكترونية)، أطروحة لنيل درجة دكتوراه علوم، تخصص القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، الجزائر، 2018، ص 101.

كما يعرف البعض الآخر، عمل التحفظ العاجل على المعطيات المخزنة؛ على أنها: "قيام شخص أو مزود الخدمات –حارس البيانات– بأمر من السلطات القضائية المختصة بتجميع المعطيات المعلوماتية والاحتفاظ بها في المستقبل في انتظار اتخاذ إجراءات قانونية أخرى كالتفتيش وغيره"[1]. التعريف الذي يعاب عليه؛ أنه يجمع بين مراقبة الاتصالات الإلكترونية والتحفظ العاجل، من حيث التجميع والاحتفاظ.

يمكن أن نصل بعد الطرح الموسع، لكل ما يتعلق بعمل التحفظ العاجل على المعطيات المخزنة، سيما من حيث أساسه القانوني وضرورة تقسيمه إلى قسمين أساسيين من جهة، وتمييزه عما يشابهه من جهة أخرى؛ إلى وضع تعريف دقيق بخصوصه؛ فنقول أنه: "عمل إجرائي رقمي حديث، يمارس من قبل مزودي الخدمات بطلب من أجهزة التحري والتحقيق، وذلك من أجل التحفظ العاجل والفوري على معطيات رقمية محددة، سبق تخزينها لديهم، التي يمكن أن يتم اللجوء إليها إجرائيا في المستقبل القريب".

2. نتائج التحفظ العاجل على المعطيات الرقمية المخزنة: يقود عمل التحفظ العاجل على المعطيات الرقمية المخزنة، بغض النظر عن نوع المعطيات محل التحفظ؛ إلى العديد من النتائج منها الإجرائية المنظمة بالنص القانوني الصريح، ومنها الرقمية واجبة التعامل معها بالنص التقليدي. إلا أننا حاولنا دمج هذه النتائج في نتيجتين اثنين، تتمثل الأولى في الإفشاء العاجل عن المعطيات الرقمية المخزنة محل التحفظ، وتنطوي الثانية على مساس هذا التحفظ بحرمة الحياة الخاصة للأشخاص.

أ- الإفشاء العاجل عن المعطيات الرقمية المخزنة محل التحفظ: يعد الإفشاء العاجل عن المعطيات الرقمية المخزنة محل التحفظ؛ بمثابة النتيجة الآلية للتحفظ المنجز بطلب من الجهة المختصة، التي لا تحتاج إلى نص صريح يقول بها. الأمر الذي يفهم ضمنا من خلال ما جاء بأحكام القانون 09-04، الذي يلزم مقدمي الخدمات بالعمل على ضمان التحفظ العاجل للمعطيات الرقمية، بطلب من الجهة المختصة، ما يقود للقول بضرورة الإفشاء العاجل لهذه المعطيات للجهة المختصة نفسها، عند طلبها[2].

إلا أنه يعاب على المشرع بالقانون 09-04 نفسه؛ كونه ربط الإفشاء العاجل بالقواعد نفسها المقررة من قبله بخصوص التحفظ العاجل على المعطيات، سيما وأنه حصرها في تلك المتصلة بحركة السير دون نظيرتها المتعلقة بالمحتوى. ولو أن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 –المصدق عليها سنة 2014–؛ رغم فصلها الضمني من حيث التحفظ بين معطيات المحتوى وعطيات حركة السير –معطيات حركة السير–؛ إلا أنها لم تتطرق من حيث الإفشاء الفوري إلا لمعطيات حركة السير دون معطيات المحتوى[3]، ما يعد بمثابة الفراغ الذي سيواجه لا محال بالإجراءات التقليدية.

---

[1] **أنظر:** وردة شرف الدين، مرجع سابق، ص 345.

[2] **أنظر:** المادتان 10 و11؛ قانون رقم 09-04، مرجع سابق.

[3] **أنظر:** المادة 24؛ مرسوم رئاسي رقم 14-252، مرجع سابق.

وعلى العموم يرى البعض أن النص التشريعي والاتفاقي المقرر للإفشاء العاجل عن معطيات حركة السير المتحفظ عنها؛ يهدف إلى الإفشاء السريع للجهة المختصة عن المعطيات المتعلقة بحركة المرور، ووضعها تحت تصرفهم لفحصها قبل المساس بها، وذلك بهدف الوصول إلى تحديد هوية مقدم الخدمة وكل ما يتعلق بالجانب الرقمي للاتصال، دون التطرق إلى المحتوى[1].

ونرى أن تخلف النص القانوني الصريح –التشريعي وحتى الاتفاقي– عن الإفشاء العاجل لمعطيات المحتوى محل التحفظ؛ لا يسبب أي إشكال إجرائي، خاصة وأن التحفظ الممارس قبل الإفشاء؛ قد فصلنا في كونه منصوص عليه ضمنا في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، التي تعد من مصادر القانون الجزائري، وما الإفشاء عن معطيات المحتوى إلا عمل لاحق للتحفظ عنها. هذا بالإضافة إلى منح النص الإجرائي التقليدي –كما بينا سابقا–، لكل من وكيل الجمهورية وقاضي التحقيق –على حسب الحالة–؛ سلطة إصدار أمر تسليم المعطيات الرقمية المتحفظ عليها في أي لحظة من لحظات لتحري أو التحقيق الساري أحدهما.

ب– المساس المباشر بحرمة الحياة الخاصة للأشخاص المعنيين: من المؤكد أن عمل التحفظ العاجل عن المعطيات الرقمية المخزنة –بنوعيها–؛ يمس بطريقة مباشرة بسرية الاتصالات الرقمية وحرمة الحياة الخاصة للأشخاص. فالتحفظ المتصل بمعطيات حركة السير؛ يجعل من جوانب الاتصال الرقمي الذي قام به الشخص مكشوفا لدى الجهة التي مارست التحفظ –مقدم الخدمات–. وبدرجة أكثر خطورة، يؤدي التحفظ المتعلق بمعطيات المحتوى؛ إلى كشف أسرار الأشخاص وكل ما يتعلق بتصرفاتهم الرقمية. الأمر الذي يدفع للتساؤل عن مدى أمانة مقدمي الخدمات من جهة، وعن الضمانات التي أقرها القانون الجزائري؛ لحماية سرية مراسلات الأشخاص المتحفظ عليها رقميا من جهة أخرى.

ب–1/ مدى أمانة مقدم الخدمات بخصوص المعطيات محل التحفظ: يمكن أن نتعرض إلى مدى أمانة مقدمي الخدمات، بخصوص المعطيات الرقمية التي تكون مخزنة لديهم بالأساس أو تم التحفظ عليها بالتبعية. حيث يطرح الفقه تساؤلا في هذا الإطار، عبر القول بمدى اعتبار مقدم الخدمة أمينا على الأسرار، فله أن يمتنع عن إفشاء المعلومات التي يحوزها، سواءً كانت متعلقة بحركة السير أو بالمحتوى.

يتعامل المشرع الجزائري كغيره من نظرائه مع فكرة الأمانة؛ عبر إلزام بعض الأشخاص بحكم وظيفتهم أن يكتموا السر المهني ويكونوا أمناء عليه[2]. حيث جعل الإفشاء ممنوعا كأصل ومسموحا كاستثناء في الحالات المقررة قانونا، سيما بخصوص الإدلاء بالمعلومات أمام الجهات القضائية وشبه القضائية المختصة.

---

[1] **أنظر:** جمال براهيمي، مرجع سابق، ص 107 و108.

[2] **أنظر:** المادة 301؛ أمر رقم 66-156، مرجع سابق.

إلا أن الأمانة الواجبة بنص قانون العقوبات التقليدي المبينة أعلاه؛ لا تنطبق إعمالا لمبدأ الشرعية الجنائية؛ إلا على أشخاص بمهام تقليدية كالطبيب والمحامي وغيرهما، رغم ورودهم –الأشخاص الأمناء– على سبيل المثال لا الحصر، وهذا نظرا لكون النص تم وضعه تشريعيا في وقت لم يكن مزود خدمة شبكة الاتصال الدولية معروفا في الجزائر على الأقل.

وفي السياق نفسه، واجه جانب من الفقه الفرنسي الإشكال المطروح أعلاه؛ عبر القول بأن مقدمي الخدمات لا يتمتعون بسر المهنة، لأنهم لا ينتمون إلى الطوائف التي يلزمها القانون بالسر المهني، على غرار الأطباء والصيادلة...الخ. ويؤسسون رأيهم بما جاء في المادة "L32-3-1/2" من قانون البريد والاتصالات الالكترونية، التي تلزم مقدمي الخدمات بإفشاء المعطيات المخزنة لديهم إلى الجهات المختصة قانونا، إذا ما كان من شأنها أن تفيد في التحري أو التحقيق، التي هو ملزم –مقدم الخدمة– أصلا بالتحفظ عليها لمدة لا تزيد عن سنة[1].

كما يوجد من يرى بخلاف ذلك، حيث يَعْتَبِرْ أن مقدم الخدمة –سيما مقدم خدمة الإنترنت– من الأمناء على الأسرار. فالمعطيات التي يحوزها سواءً كانت متعلقة بحركة السير أو بالمحتوى؛ لم يحصل عليها إلا بسبب وظيفته التي يؤديها إلى الأشخاص. وكل تجاوز منه أو إفشاء في غير ما سمح به القانون؛ يكون عملا مجرما بسبب انتهاك الأمانة المطلوبة في مقدمي الخدمات كغيرهم من الأمناء التقليديين[2].

وأما بخصوص رأي الباحث المتصل بالقانون الجزائري؛ فنجد أن مقدم الخدمة هو أمين على المعطيات التي يخزنها أو يتحفظ عليها أو يفشيها. فالأصل أنه يخزن ويحفظ السر، الذي لا يبوح به إلا عند الحاجة القضائية دون سواها، بعد أن يتحفظ عل المعطيات بطلب من الجهة المختصة –جهة تحري أو تحقيق– ، ثم يفشيها بأمر من الجهة نفسها.

ب–2/ الضمانات القانونية من الإفشاء غير القانوني للمعطيات محل التحفظ: سعيا من المشرع إلى تفادي الاختلاف الفقهي المبين أعلاه، وعدم الدخول في دوامة المساس غير المجرم صراحةً –بالنص التقليدي– من مقدمي الخدمات بحرمة الحياة الخاصة؛ تدخل المشرع ليضع بعض الضمانات القانونية الحديثة، التي تحول دون المساس بالحياة الخاصة للأشخاص، من خلال التعامل غير القانوني مع المعطيات محل التخزين والتحفظ، سيما عبر الإفشاء بها لغير الجهات المختصة[3].

---

[1] **أنظر:** مصطفى علي خلف، مرجع سابق، ص 204 و205. **وأنظر أيضا:**
- Art L-32-3-1/2 Code des postes et des communications électroniques français, Version consolidée au 01 janvier 2019. Disponible sur le Lien: https://www.legifrance.gouv.fr.

[2] **أنظر:** مصطفى علي خلف، المرجع نفسه، ص 205.

[3] هي ضمانات جاء بها القانون رقم 09-04 سابق الذكر، قبل أن يعدل فيها بموجب تعديل وتميم قانون العقوبات سنة 2016. **أنظر في ذلك:** المادة 11؛ قانون رقم 09-04، مرجع سابق. **وأنظر أيضا:** المادة 394مكرر08؛ أمر رقم 66-156، مرجع سابق.

ألزم المشرع الجزائري بموجب القانون 09-04؛ مقدمي الخدمات على الاحتفاظ بالمعطيات المخزنة المتعلقة بحركة السير[1]، لمدة لا تزيد عن 01 سنة[2]. وهو الشرط المعمول به في أغلب التشريعات المقارنة والاتفاقيات الدولية، وان بمدد متباينة، فحددها -المدة- القانون الفرنسي بـــ 01 سنة كما بينا سابقا، وقلصتها كل من اتفاقية بودابست لسنة 2001 والاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010؛ إلى 90 يوما -أي 03 أشهر-[3].

وفي هذا الصدد لم يحدد المشرع مآل معطيات حركة السير، المخزنة أو المتحفظ عليها؛ بعد مرور مدة 01 سنة المقررة قانونا. إلا أنه ترى بعض الدراسات في هذا الإطار؛ بضرورة تدخل مقدم الخدمة تحت طائلة العقوبة الإدارية والجزائية بعد مرور هذه المدة، من أجل سحبها وإزالتها أو على الأقل وضع ترتيبات تقنية تستبعد إمكانية الاطلاع عليها حفاظا على سريتها وخصوصيتها[4].

بالإضافة إلى التزام الاحتفاظ لمدة 01 سنة بمعطيات حركة السير؛ ألزم المشرع مزودي الخدمات بضرورة التقيد بالسر المهني عموما، تحت طائلة المسائلة الجنائية في إطار جريمة إفشاء أسرار التحري والتحقيق، وبالتالي إفشاء كل معطيات رقمية مخزنة لديهم، قدم بخصوصها طلب التحفظ العاجل، يعتبر بمثابة المساس بسرية التحري والتحقيق[5]. وفي حال حدوث الإفشاء قبل تلقي طلب التحفظ؛ تطبق الأحكام العامة لقانون العقوبات، المنطوية على جريمة إفشاء السر المهني السابقة بالذكر[6].

ثانيا: أنواع المعطيات الرقمية المخزنة محل التحفظ العاجل

تختلف المعطيات الرقمية عموما، فتنقسم إلى العديد من الطوائف على حسب المعيار المعتمد لذلك. إلا أنه في بخصوص تلك المتصلة بالمعطيات المخزنة محل التحفظ العاجل؛ فلا يمكن تقسيمها إلا لنوعين، سبق الإشارة إليهما عند التطرق إلى تعريف التحفظ العاجل على المعطيات الرقمية المخزنة. وعلى العموم تتمثل هذه المعطيات؛ في تلك المتعلقة بحركة السير أو المرور، ونظيرتها المتصلة بالمحتوى.

---

[1] مع التذكير؛ بأن هذا الالتزام أقره المشرع على المعطيات المتعلقة بحركة السير، دون تلك المتصلة بالمحتوى. الأمر الذي قد يفهم أنه بمثابة خلاص لمقدمي الخدمات من مدة الحفظ المقررة بـ 01 سنة، أو أن حفظ معطيات المحتوى؛ التزام دائم غير محدد بمدة. وهو ما يميل إليه الباحث، نظرا لتعلق ذلك مباشرة بالدليل الرقمي الالكتروني، ولكون الاحتفاظ الدائم لن يمس بسرية الأشخاص، طالما أن المشرع يضع على عاتق مقدمي الخدمات؛ واجب الحفاظ على السر المهني كما سنرى فيما يلي.

[2] **أنظر:** المادة 03/11؛ قانون رقم 09-04، مرجع سابق.

[3] **أنظر:** Art 16-2; Convention sur la cybercriminalité- Budapest, op.cit. - **وأنظر أيضا:** المادة 23-2؛ مرسوم رئاسي رقم 14-252، مرجع سابق.

[4] **أنظر:** جمال براهيمي، مرجع سابق، ص 105.

[5] وهو ما جاءت به أيضا كل من اتفاقية بودابست لسنة 2001، والاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010. **أنظر في ذلك:** المادة 2/10؛ قانون رقم 09-04، المرجع نفسه. **وأنظر أيضا:** المادة 23-3؛ مرسوم رئاسي رقم 14-252، المرجع نفسه. **وأنظر كذلك:** Art 16-3; Convention sur la cybercriminalité- Budapest, idem. -

[6] **أنظر:** المادة 301؛ أمر رقم 66-156، مرجع سابق.

1. التحفظ العاجل على المعطيات المخزنة المتعلقة بالمحتوى: سبق وأن بينا في إطار تعريف التحفظ العاجل على المعطيات المخزنة عموما؛ أن القانون الجزائري تباين من حيث القول بإمكانية ذلك. حيث لم ينص لا صراحةً ولا ضمنا في إطار القانون 09-04؛ على التحفظ المتصل بمعطيات المحتوى. واعتمد ذلك ضمنا بالتصديق سنة 2014؛ على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010[1].

كما أكدنا فيما سبق أيضا؛ أن المشرع أخلط الأمر عند تناوله للتحفظ العاجل، على أساس أنه التزام من بين الالتزامات الواقعة على مقدمي الخدمات، وليس كعمل إجرائي مستقل، ما جعله مرتبط بدور مقدمي الخدمات، المعروف –أو المتاعرف عليه– أنه يقدم خدمة الاتصال، ولا علاقة له بخدمة المعالجة المتصلة بالمحتوى الرقمي.

إلا أننا نقول بإمكانية ممارسة مقدم الخدمة؛ لعمل التحفظ العاجل على معطيات المحتوى السابق تخزينها، وذلك للعديد من الأسباب. فبالإضافة إلى الأساس العام المذكور سابقا في التعريف، الذي أسسناه بالورود الضمني لهذا العمل في الاتفاقية العربية التي صدقت عليها الجزائر[2]، نجد أن المشرع بالقانون 09-04 نفسه؛ قد قسم مقدمي الخدمات إلى نوعين اثنين، يعمل الأول على ضمان خدمة الاتصال عموما، وأما الثاني فيعالج ويخزن المعطيات المعلوماتية لفائدة خدمة الاتصال نفسها أو لمستعمليها[3]. حيث ترى بعض الدراسات –ونرى أيضا– أن الأول؛ هو من يمارس التحفظ المتعلق بمعطيات حركة السير، على أن يهتم الثاني؛ بالتحفظ المتعلق بمعطيات المحتوى نظرا لكونه المعالج والمخزن[4].

ولو تطرقنا إلى النوع الثاني من مقدمي الخدمات الذي يعالج ويخزن معطيات المحتوى، بالمفهوم العملي المكرس لدى العامة؛ لقنا أنه ينقسم إلى العديد من الأنواع، فيتصل ببرامج ومواقع شبكية عديدة، حيث يلعب أصحابها دور مقدمي الخدمات. ولو تحدثنا عن تطبيق "فايبر–Viber" مثلا؛ لقلنا أن صاحبه الذي أوجده، يحتوى على قاعدة معطيات المحتوى –وحتى غيرها–، المنطوية على نسخة من كل ما أرسله واستقبله مستعمليه[5].

---

[1] **أنظر:** المادة 23-1؛ مرسوم رئاسي رقم 14-252، مرجع سابق.

[2] مع التأكيد على ضرورة التفرقة -كما بينا سابقا عند التعريف-؛ بين التحفظ العاجل على معطيات المحتوى، ومراقبة الاتصالات الالكترونية من جهة والحجز بعد التفتيش المرقمن من جهة أخرى. حتى ندحض الآراء التي قد تؤسس لعدم تطرق المشرع بالقانون 09-04 صراحةً؛ لعمل التحفظ العاجل عن معطيات المحتوى؛ بتفادي التكرار.

[3] **أنظر:** المادة 1/02-د؛ قانون رقم 09-04، مرجع سابق.

[4] **أنظر:** مصطفى علي خلف، مرجع سابق، ص 294.

[5] سبق لمركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها التابع للدرك الوطني -المدروس سابقا-؛ أن طلب من صاحب موقع "واد كنيس-ouedkniss"، الشهير في مجال بيع وشراء الأشياء المستعملة في الجزائر-الذي يعتبر في الوقت نفسه مقدم خدمات معالجة وتخزين-؛ إنتاج معطيات محتوى المخزنة لديه بعد التحفظ العاجل عليها. وعليه تم تزويد المركز؛ بجميع المعطيات المنطوية على محتوى المحادثات -وحتى معطيات حركة السير الممكن إنتاجها- التي أجراها المشتبه فيه، الذي له حساب في الموقع. **أنظر في ذلك:** مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها للدرك الوطني، "حالات ملموسة"، مرجع سابق، ص 07.

2. التحفظ العاجل على المعطيات المخزنة المتعلقة بحركة السير: على العكس من التحفظ العاجل على المعطيات المخزنة المتعلقة بالمحتوى؛ تطرق المشرع الجزائري –كما بينا سابقا– صراحةً إلى التحفظ العاجل المتصل بمعطيات حركة السير أو المرور –أو معطيات المستخدمين–. حيث اتبع في ذلك ما ورد في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات –المصدق عليها–، وما جاء قبلها في إطار أهم اتفاقية في هذا الإطار، المنطوية على اتفاقية بودابست لسنة 2001[1].

نص المشرع بالقانون 09-04، في إطار التطرق إلى التزامات مقدمي الخدمات؛ على عمل التحفظ العاجل على المعطيات المخزنة المتعلقة بحركة السير، الذي ينجز من أجل تقديم هذه المعطيات إلى سلطات التحري والتحقيق المختصة عند طلبها[2]. الأمر الذي بين له المشرع بالقانون نفسه؛ أغلب الأحكام القانونية واجبة الإعمال، على غرار تلك المتصلة بتحديد المقصود بمعطيات حركة السير، وأنواعها وطبيعة مقدم الخدمة الذي يتحفظ عليها والمسؤولية التي تقوم على عاتقه.

حدد المشرع المقصود بمعطيات حركة السير[3]؛ عبر القول بأنها: "أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة اتصال، توضح مصدر الاتصال، والوجهة المرسل إليها، والطريق الذي يسلكه، ووقت وتاريخ وحجم ومدة الاتصال ونوع الخدمة"[4]. كما أنه –المشرع– انطلاق من التعريف الذكور؛ حاول حصر قائمة بأنواع معطيات حركة السير أو المرور، فقسمها إلى خمسة أنواع.

وتتمثل أنواع معطيات السير الخمسة المذكورة؛ في تلك التي تسمح بالتعرف على مستعملي الخدمة أولا، ونظيرتها المتعلقة بالتجهيزات الطرفية المستعملة في الاتصال ثانيا، بالإضافة إلى كل الخصائص التقنية وتاريخ ووقت ومدة كل اتصال ثالثا، مع إضافة معطيات الخدمات التكميلية المطلوبة أو المستعملة ومقدميها رابعا، وأخيرا المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها. مع التأكيد على أن مدة التحفظ على هذه المعطيات؛ محددة في واحد سنة على الأكثر، من تاريخ تسجيلها أو تخزينها[5].

---

[1] **أنظر:** Arts 16 et 17; Convention sur la cybercriminalité- Budapest, op.cit. - **وأنظر أيضا:** المادتان 23 و24؛ مرسوم رئاسي رقم 14-252، مرجع سابق.

[2] **أنظر:** المادة 1/10؛ قانون رقم 09-04، مرجع سابق.

[3] **أنظر:** المادة 1/02-ه؛ المرجع نفسه.

[4] وهو ما يعد نسخة موسعة المفهوم، من التعريف الوارد باتفاقية بودابست لسنة 2001، الذي جاء فيه أنها: "صنف من بيانات الحاسب التي تشكل محلا لنظام قانوني محدد، إذ يتم توالد هذه المعطيات من الحواسيب عبر تسلسل حركة الاتصالات لتحديد مسلك الاتصال من مصدرها إلى الجهة المقصودة". **أنظر في ذلك:** جمال براهيمي، مرجع سابق، ص 102.

[5] مع التأكيد على أن مقدم خدمات الهاتف غير الرقمي -الخارج عن دراستنا-؛ لا يلتزم إلا بالتحفظ على المعطيات المؤدية إلى التعرف على مستعملي الخدمة، وتلك السامحة بالتعرف على مصدر الاتصال ومكانه. **أنظر في ذلك:** المادة 1/11؛ قانون رقم 09-04، المرجع نفسه.

يتبين من أنواع المعطيات المذكورة أعلاه؛ أنها متعلقة بالاتصال والمستخدمين دون المحتوى. الأمر الذي يقود للقول بأن مقدم الخدمة الملزم بالتحفظ العاجل عليها؛ هو ذلك الذي يوفر خدمة الاتصال عموما، وليس من يعالج ويخزن معطيات المحتوى السابقة بالدراسة. وعليه يتصل بالنوع الأول، من نوعي مقدمي الخدمات الذين جاء بهما المشرع بالمادة 1/02-د من القانون 09-04 نفسه[1].

وعلى العموم وضع المشرع التزام التحفظ العاجل على المعطيات الرقمية المخزنة المتعلقة بحركة السير-وفق ما بينا سابقا-؛ تحت طائلة المسائلة الإدارية وحتى الجنائية. حيث يتوجب على مقدم خدمة الاتصال؛ الالتزام بالتحفظ العاجل بكل أنواع معطيات حركة السير المبينة سابقا، لمدة سنة كاملة، مع التأكيد على ضرورة الحفاظ على السر المهني، في إطار ضمان الأمانة المهنية[2].

الفرع الثالث: تحديد هوية المشتبه فيه الرقمي

تعد مسألة التعرف على هوية المشتبه فيه المتصل بالمسرح الرقمي الافتراضي؛ من أصعب وأعقد العقبات التي تواجه الأجهزة المختصة عموما. حيث قد يتم الوصول بسهولة إلى المعطيات الرقمية ذات المحتوى المجرم، من دون وجود أي إشارة لأي شخص كان، أو بوجود إشارات لكن تقود للاشتباه في عدد كبير جدا من الأشخاص. كما قد تتضمن هذه المعطيات؛ أدلة رقمية قاطعة ضد المشتبه فيه؛ الذي تحدد هويته الافتراضية الرقمية، المختلفة في العديد من الأحيان عن الهوية الحقيقية[3]. الأمر الذي عجل بظهور العديد من الطرق الرقمية وغيرها؛ المتمثلة أساسا في بروتوكول الـــ "TCP-IP"(أولا)، والعديد من الطرق الأخرى غير القائمة على هذا البروتوكول الأساسي(ثانيا).

أولا: التحديد الرقمي لهوية المشتبه فيه عبر تتبع بروتوكول الـــ "TCP-IP"

يعد الـــ "TCP-IP"؛ من أهم البرتوكولات المتصلة بشبكة الاتصال الدولية، سيما وأن له الدور الأساس في تحديد هوية مرتادي هذه الشبكة. إلا أنه ما يعد سلبيا في هذا الإطار؛ يتمثل في كون المشرع -الجزائري وغيره- وكذا الاتفاق الإقليمي والدولي؛ لم يتطرقوا إلى برتوكول الـــ "TCP-IP"؛ إن كتقنية رقمية تتحكم في النقل الشبكي، أو كوسيلة إجرائية حديثة تستعمل في التحري والتحقيق، رغم كونه الأساس الإجرائي العملي في تحديد هوية المشتبه فيه. وهو ما سنبينه فيما يلي؛ من خلال تحديد المضمون التقني لبروتوكول الـــ "TCP-IP"؛ وعرض كيفية الاعتماد عليه لتحديد هوية المشتبه فيه.

---

[1] مقدم خدمات الاتصال الذي عرفه المشرع بالمادة نفسها؛ على أنه: **"**أي كيان عام أو خاص يقدم لمستعملي خدماته، القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام للاتصالات**"**.

[2] **أنظر:** المادة 2/10 والمادة 3/11 و4 و5؛ قانون رقم 09-04، مرجع سابق.

[3] مع الإشارة إلى أن المشرع سمح بفتح تحقيق قضائي ضد المشتبه فيه المسمى أو غير المسمى، الذي قد يقود التحقيق القضائي إلى التعرف على هويته، ومنه اتهامه، قبل إحالته أمام المحكمة. كما قد يبقى مجهول الهوية، ما يدفع قاضي التحقيق وجوبا؛ لإصدار أمر بانتفاء وجه الدعوى. **أنظر في ذلك:** المادتان 2/67 و1/163؛ أمر رقم 66-155، مرجع سابق.

1. المضمون التقني لبرتوكول الـــ "TCP-IP": يكتسي بروتوكول الـــ "TCP-IP"؛ الطابع المعقد نفسه السابق بالطرح في إطار دراسة المسرح الجرمي الافتراضي، المنطوي على النطاق الافتراضي للسوط الرقمي عموما، كيف لا وهو أحد أبرز مكوناته، الذي لا يمكن لشبة الاتصال الدولية أن تؤدي مهامها التقنية بتخلفه. وعلى العموم، لايمكن أن نحدد المضمون التقني لهذا البروتوكول، الذي يعد الأساس الإجرائي الأول لتحديد هوية المشتبه فيه؛ إلا عبر التطرق إلى تعريفه وتبيان أقسامه وطريقة عمله.

أ- **تعريف برتوكول الـــ "TCP-IP":** يعد الـــ "TCP-IP"؛ أحد أهم أنواع بروتوكولات الاتصال عموما. التي تعتبر -"بروتوكولات الاتصال-Communications Protocol"-[1]؛ بمثابة التقنية المصممة خصيصا لانجاز مهام الاتصال بين الأجهزة الرقمية المختلفة. وهي التي تعرف تقنيا؛ على أنها: "مجموعة من القوانين والمقاييس، المصممة لتمكين عدة أجهزة من الاتصال ببعضها البعض، وتبادل البيانات بأقل قدر ممكن من الأخطاء"[2].

ويتألف برتوكول الاتصال عموما؛ من سبع طبقات من الأجهزة والبرمجيات المعروفة بتسمية ربط الأنظمة المفتوحة-Open Systems Interconnection/OSI". كما أنه -برتوكول الاتصال- يختلف من حيث تعقيده على حسب وظيفته، فقد نتعامل مع بروتوكولات بسيطة، كما أننا قد نواجه أخرى معقدة كبروتوكول "OSI"[3] أو بروتوكول الـــ "TCP-IP"[4].

وبغض النظر عن بروتوكول "OSI" -الذي يعد خارجا عن دراستنا-؛ يمكن القول أن بروتوكول الـــ "TCP-IP"، الذي يستعمل للتعرف على هوية المشتبه فيه كما سنرى لاحقا؛ يعد من التقنيات المعقدة التي يصعب التعامل معها. وفي ذلك يعرف تقنيا؛ على أنه: "حزمة[5] قواعد ومعايير متعددة -البرتوكولات- مرتبطة ببعضها البعض، لتعمل مجتمعة على تحقيق التوافق اللازم لإنجاح عمليات الاتصال الشبكي بين الأجهزة المختلفة"[6].

---

[1] على أن يعتبر بروتوكول الاتصال هو الأخر؛ أحد أنواع البروتوكولات عموما. الذي يعرف البروتوكول؛ على أنه: "اتفاق يحكم إجراءات تبادل المعلومات بين كيانين متعاونين -جهازين متصلين مثلا-، يشمل تحديد كيفية الاتصال وعدد مراته وطريقة الرجوع إلى الوضع العادي". **أنظر في ذلك:** ممدوح عبد الحميد عبد المطلب، مرجع سابق، ص 04.

[2] **أنظر:** المرجع والصفحة نفسهما.

[3] حيث يعرف بروتوكول "OSI"؛ على أنه: "بروتوكول انترنت وجد لأول مرة سنة 1984، ليهتم بضمان الاتصال الشبكي عن بعد، بين أجهزة الإعلام الآلي". **أنظر في ذلك:**

- LALITTE Eric, Apprenez le fonctionnement des réseaux TCP/IP, 3eme édition, Imprimé par Eyrolles, Paris, France, 2016, p 08 et 09.

[4] **أنظر:** ممدوح عبد الحميد عبد المطلب، المرجع والصفحة نفسهما.

[5] تعرف حزم المعلومات؛ على أنها؛ "جزء بحجم صغير من ملف معلوماتي ثابت، يحمل رقما خاصا ومعلومات تعريفية بكل من المرسل والمرسل إليه، فيتراوح حجم الحزمة الواحدة بين 40 و32 000 بيت". **أنظر في ذلك:** المرجع نفسه، ص 05.

[6] **أنظر:** حازم محمد حنفي، مرجع سابق، ص 87.

ب- أقسام بروتوكول الـــ "TCP-IP": لا يقوم بروتوكول الـــ "TCP-IP" المعرف أعلاه -وفق التركيبة التقنية الحديثة-؛ على تكوين تقني واحدة، وإنما له ثلاثة أقسام تتصل اتصالا وثيقا ببروتوكول "OSI"، وهو ما يزيده تعقيدا وتشعبا. حيث بعمل هذه الأقسام الثلاث مع بعضها البعض؛ يتم نقل المعطيات الخاصة بالمستخدم تبعا لنظام هيكلة تبادل المعلومات المسمى بـــ"With OSI TCP/IP"[1].

وتتمثل هذه الأقسام الثلاث الحديثة، الواجبة لعمل بروتوكول الـــ "TCP-IP"؛ في القسمين الأساسيين للبروتوكول نفسه، المتمثلين في؛ برتوكول "Transmission Control Protocol-TCP"، وكذا بروتوكول الإنترنت "Internet Protocol-IP". بالإضافة إلى القسم الثالث -الذي يزيد من التعقيد الرقمي-، المتصل ببروتوكول "OSI" السابق بالذكر، الذي يسمى ببرتوكول User Data Gsam Protocol-UDP"[2].

ج- طريقة عمل برتوكول الـــ "TCP-IP": لايمكن الحديث عن طريقة عمل برتوكول الـــ "TCP-IP"؛ في شكله التقني المركب، وإنما لكل جزء من أجزائه -أو بالأحرى جزئيه الأساسيين-؛ دور خاص به. حيث يهتم برتوكول الإنترنت "IP"؛ بتوزيع النطاقات الشبكية، وذلك وفق تسلسل منطقي عبر ثلاث مستويات أساسية. فبعد أن تحصل الدولة على عنوان الـــ "IP" الخاص بها، من طرف المنظمة الدولية المسئولة عن توزيع هذه العناوين "IANA"؛ تقوم بتقسيم النطاق الذي يتضمنه إلى حصص معينة، قبل أن توزعها -الحصص- على مقدمي الخدمات الشبكية المعتمدين[3].

وبعد أن يحصل مقدمي الخدمات على حصصهم من نطاقات عناوين الـــ "IP"؛ يقومون بتقسيمها من جديد إلى العديد من العناوين الجزئية، لتوزع فيما بعد على المشتركين لديها. على أن ينقسم هذا التوزيع إلى نوعين أساسيين، يتمثل الأول في النطاق الثابت "Static IP"، الذي يحجز لمشترك بعينه يحصل عليه في كل مرة يقوم بتحقيق أي اتصال شبكي، وينطوي الثاني على النطاق المتغير "Dynamic IP"، الذي يحصل عليه المشترك لحظة ولوجه إلى الشبكة لينتهي دوره مع انتهاء الولوج نفسه، على أن يحصل المشترك على عنوان جديد؛ في حال ولج من جديد إلى الشبكة، بغض النظر عن محل الولوج[4].

وأما بروتوكول الـــ "TCP" فتختلف طريقة عمله عن نظيره المبين أعلاه، حيث تتصف طريقة عمله بالتعقيد وطول المراحل الفنية. فأولا يسلم بروتوكول الـــ "TCP"؛ مجموعة المعلومات المطلوب إرسالها. على أن ينجز ذلك بمساعدة بروتوكول "UDP"؛ في حال الإخفاق المتصل بازدحام الشبكات وغير ذلك، الذي يواجه بتقسيم المعلومات عن طريق تقنية "Pac Kets"، لترقم بعد ذلك عبر نظام "Port"[5].

---

[1] **أنظر:** ممدوح عبد الحميد عبد المطلب، مرجع سابق، ص 11.

[2] **أنظر:** المرجع والصفحة نفسهما.

[3] **أنظر:** حازم محمد حنفي، مرجع سابق، ص 89 و90.

[4] **أنظر:** المرجع نفسه، ص 90.

[5] **أنظر:** ممدوح عبد الحميد عبد المطلب، المرجع نفسه، ص 13.

كما يقوم بروتوكول الـــ "TCP" بعد الترقيم مباشرة؛ بتحقيق الاتصال بالجهاز المرسل إليه باستخدام تقنية "SYN" أو تقنية "ACK" أو الاثنين معا. وفي خلال فترة معينة، إذا لم يستلم بروتوكول الـــ "TCP" بأن الاتصال قد تم؛ يعيد الاتصال من جديد. وإذا ما تم الاتصال؛ يتحقق البروتوكول من أن "الباكت" قد أرسلت فعلا إلى وجهتها الرقمية، وفق القواعد الفنية اللازمة. وبمجرد أن ينتهي الاتصال يقوم بروتوكول الـــ "TCP"؛ بإرسال "باكت" يفيد الانتهاء "FIN"[1].

2. الاعتماد الإجرائي على برتوكول الـــ "TCP-IP" لتحديد هوية المشتبه فيه: يتم الاعتماد إجرائيا بخصوص إجراءات التحري –وكذا التحقيق– في جرائم الوسط الرقمي، على بروتوكول الـــ "TCP-IP" أو بنوع من التدقيق على بروتوكول الانترنت "IP"، الذي يعد الأساس التقني الصريح، المعمول به من قبل الأجهزة الإجرائية المختصة، سيما من أجل التعرف على الهوية الحقيقية للمشتبه فيه. الأمر الذي نبينه فيما يلي؛ من خلال التطرق إلى كيفية انجاز ذلك، وأهم المعوقات التقنية الذي تحول دون التعرف على الهوية الحقيقية للمشتبه فيه.

أ– كيفية الاعتماد الإجرائي على برتوكول الـــ "TCP-IP" لتحديد هوية المشتبه فيه: تذهب أغلب أجهزة التحري والتحقيق في جرائم الوسط الرقمي –الوطنية والأجنبية–، بغرض تحديد هوية المشتبه فيه؛ إلى الاعتماد الإجرائي الصريح والمكثف على برتوكول الـــ "TCP-IP"، أو على الأقل الاعتماد على أحد أقسامه الثلاث المنطوي على برتوكول الإنترنت "IP"، الذي يمكن –لوحده– أن يكون مفيدا للتعرف على هوية المشتبه فيه في الكثير من الأحيان[2].

ويتم إتباع في سبيل ذلك، أحد الوسيلتين على حسب الحالة. فإذا تعلق الأمر بمعطيات رقمية مرسلة عبر البريد الرقمي؛ يمكن تحديد عنوان الـــ "IP" الخاص بالمرسل، بعد فحص البريد الوارد مباشرة، سيما باستعمال ما يعرف بـــ "Full Headers"، وعليه التقدم بطلب المعلومات الكاملة عن المرسل من مقدم الخدمة المعني، ما يساهم في التعرف على هويته الحقيقية[3].

---

[1] **أنظر:** ممدوح عبد الحميد عبد المطلب، مرجع سابق، ص 13 و14.

[2] الأمر الذي سبق لأجهزة التحري الاعتماد عليه في العديد من الأحيان. على غرار مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها التابع للدرك الوطني، الذي عالج سنة 2017 حالة متعلقة بجرائم المساس بأنظمة المعالجة الآلية للمعطيات، المتصلة بقرصنة البريد الرقمي لوزارة معينة. وكان التصدي من خلال تحديد عنوان الـ "IP" للمشتبه فيه، ومن ثم تقديمه لشركة اتصالات الجزائر، التي حددت كل المعلومات الشخصية للمشتبه فيه المسمى بـ "ت.أ"، الساكن بحي براهيم رايس الجزائر العاصمة، وفعلا بعد التنقل إلى مكان سكناه؛ تم حجز الأجهزة الرقمية المستعملة في الجريمة، ومنه تقديمه للعدالة. **أنظر في ذلك:** مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها للدرك الوطني، **"حالات ملموسة"**، مرجع سابق، ص ص 08-12.

[3] إلا أنه يمكن سواءً في الطريقة الأولى هذه أو الثانية التالية بعدها؛ تصور التعرف على هوية المشتبه فيه من دون تحمل عناء تحديد عنوان الـ "IP"، وذلك في حالة ما كان المرسل يستعمل هويته الحقيقية في النطاق الافتراضي، كأن يسمي البريد الرقمي أو حسابه على الموقع الشبكي باسمه الحقيقي، مع إمكانية إتاحته للعامة كل المعلومات الخاصة به، كمكان إقامته وسنه وطبيعة عمله...الخ.

وأما الطريقة الثانية؛ فتتصل بالتصرفات الرقمية المنجزة عبر المواقع الشبكية سيما المشهورة منها، كـــ "Facebook، ouedkniss..."، التي تتطلب مخاطبة صاحب الموقع أو القائم عليه، للحصول على عنوان الـــ "IP"، الخاص بالمشتبه فيه باستعمال ملفات الموقع "Log Filles"، ومن ثم تقديم ذلك لمقدم خدمة الاتصال، حتى يكشف عن المعلومات المفيدة في التعرف على الهوية الحقيقية للمشتبه فيه[1].

ب- معوقات الاعتماد الإجرائي على برتوكول الـــ "TCP-IP" لتحديد هوية المشتبه فيه: يتبين من خلال سرد الإجراءات السابقة بالذكر المؤدية إلى تحديد عنوان الـــ "IP"؛ أن أمر تحديد هوية المشتبه فيه لا تعتريه أي عقبات فنية وهو محقق لا محال. إلا أنه يمكن الوقوع في العديد من الإشكالات الفنية، التي تحول دون التعرف على الهوية الحقيقية للمشتبه فيه، رغم استخراج عنوان الـــ "IP".

فيمن في هذا الإطار؛ تصور العديد من الحالات الفنية، التي تحول دون تحديد الهوية الحقيقية للمشتبه فيه. حيث يعد برتوكول الإنترنت "IP"؛ بمثابة العنوان المحدد لهوية صاحب الاشتراك في الاتصال الشبكي، الذي قد لا يكون بالضرورة هو نفسه الفاعل في الجريمة، كما قد يكون بعيدا كل البعد عن ذلك.

ومن أمثلة ذلك[2]؛ نجد أن المؤسسات الكبرى تستخدم عن طريق "الراوتر-Router"؛ ما يسمى ببرتوكول الرقم الثابت "Static IP" -المبين سابقا-، الذي يوزع عدد من الـــ "IP" بين المستخدمين الذين يلجون إلى الشبكة باسم الشركة أو المؤسسة. ما قد يدفع للاشتباه في كل مستخدمي الشركة، الذين قد يكون عددهم كبير جدا. كما يمكن لأي مقرصن العمل على كسر إجراءات التأمين، للولوج الشبكي عبر"IP" المؤسسة وارتكاب الجرائم التي يريد باسمها[3].

إلا أن الإشكال الأكبر تعقيدا في هذا الإطار؛ يكمن في الإجرام الرقمي المتصل بـــ "الويب المظلم Dark Web-" المبينة خصائصه التقنية سابقا. حيث باستعمال متصفح "TOR"؛ يتم العبث في بروتوكول "TCP-IP"، ما يجعله مشفرا بتوزيعه بين خوادم وسيطة بأعداد خيالية. ومنه استحالة التعرف على "IP" المشتبه فيه، واستحالة تحديد هويته الحقيقية. وفي هذه الحالة لا يبقى أمام جهات التحري سوى العمل بنظام التسرب التقليدي، بغرض محاولة استدراج المشتبه الذي قد يكشف عن هويته الحقيقية.

---

[1] **أنظر:** حازم محمد حنفي، مرجع سابق، ص 90.

[2] كما يمكن تصور الأمر نفسه؛ بخصوص الولوج الشبكي الذي يتم عبر مقاهي الإنترنت، من خلال الـ **"IP"** التجاري لصاحب المقهى. وكذا في حالات الولوج الشبكي عبر **"IP"** شخص آخر، من خلال تقنية الـ **"Wifi"** أو **"**نقطة الوصول Access Point-" المتصلة بشبكة الهاتف المحمول "3G و4G و5G...". ويمكن أيضا؛ تصور ذلك من خلال؛ الولوج الشبكي عبر شبكة الهاتف المحمول، التي يستفيد منها المشتبه فيه، من خلال استعماله لشريحة يشتريها من دون تقديم وثائق الهوية، أو مع تقديم وثائق مزورة. هذا من دون أن ننسى الحالة؛ التي يتسبب فيها مقدم الخدمة نفسه؛ الذي لا يلتزم بالإجراءات المترتبة على عاتقه بالمادتين 10 و11 من القانون 09-04، ولا يتحفظ على معطيات حركة السير، وان كان سيتحمل المسؤولية الإدارية والجزائية جراء هذا التقصير، مع إمكانية أن تحمله للمسؤولية الجزائية عن الجريمة الرقمية محل التحري بصفه شريكا، لو ثبت تعمده عدم التحفظ على معطيات حركة السير، بغرض استبعاد التعرف على هوية المشتبه فيه الأصلي.

[3] **أنظر:** حازم محمد حنفي، المرجع نفسه، ص 92.

ثانيا: التحديد الرقمي لهوية المشتبه فيه من دون تتبع بروتوكول الـــ "TCP-IP"

يمكن أن تصل الجهة القائمة بالتحري أو التحقيق، إلى تحديد الهوية الحقيقية للمشتبه فيه؛ من دون الاستناد على تتبع بروتوكول الـــ "TCP-IP". وذلك إما لعجزه كما بينا سابقا انطلاقا من المعوقات التي تحول دون تحقيق الغاية منه، أو لأسباب أخرى على غرار سهولة تحديد الهوية؛ من دون اللجوء إلى برتوكول الإنترنت أو باستعمال وسائل رقمية أخرى تشابهه. وان كان قد تعجز هي الأخرى عن تحقيق الغاية منها، وفق معوقات فنية عديدة أخرى. وعلى العموم تتمثل هذه الوسائل؛ في تلك المتصلة بتتبع بطاقات الهاتف المحمول، أو عبر الاستنتاج من الأعمال الأخرى؛ الرقمية وكذا التقليدية.

1. التحديد الرقمي لهوية المشتبه فيه عبر تتبع بطاقات الهاتف المحمول: يتعلق هذا الإجراء؛ ببطاقات الهاتف المحمول مسبقة الدفع "Les cartes de téléphonie prépayées". الذي تعتبره الكثير من الدراسات ذات الصلة؛ من الأعمال الإجرائية الحديثة، الواردة في العديد من القوانين المقارنة، تزامنا مع زيادة حدة التهديدات الإرهابية. حيث تتم من خلاله تتبع البطاقات، التي ستقود لا محال إلى تحديد الهوية الحقيقية لحاملها، سواءً مباشرة، أو بالرجوع إلى السجل الوطني المتصل بمقدم خدمة هذه البطاقة[1].

ومن الملاحظ أنه في الجزائر وبتعليمات غير منشورة؛ ألزمت الحكومة كل مزودي خدمات الهاتف النقال، بضرورة مسك المعلومات الشخصية لكل متعامل معها قبل بدئه في استغلال الشريحة[2]. وهو ما زامن انطلاق خدمات شبكة الجيل الثالث، واستمر إلى غاية وقتنا الحالي. الأمر الذي قامت به بلجيكا مثلا وبالطريقة نفسها سنة 2016، ولو أن الدراسات الفقهية في هذا البلد، تساءلت عن مدى نزاهة ذلك، سيما وأنه يمس بالحياة الخاصة للأشخاص، وأنه سبق رفضه في بريطانيا بعد طرحة للمناقشة[3].

2. التحديد الرقمي لهوية المشتبه فيه عبر الاستنتاج المتصل بالأعمال الرقمية الأخرى: بالإضافة إلى العمل الإجرائي المبين أعلاه، يمكن اللجوء في سبيل تحديد هوية المشتبه فيه؛ إلى الاستنتاج من العديد من الأعمال الإجرائية الرقمية الأخرى. على غرار إمكانية تحديد الهوية انطلاقا من إجرائي المعاينة والتفتيش المرقمنين السابقين بالدراسة –والحجز المرقمن أيضا–، انطلاقا من المعطيات المتعامل معها، التي قد تدل بطريقة أو بأخرى على الفاعل، سيما من خلال الصور والعبارات والفيديوهات...الخ[4].

---

[1] **أنظر:** - DECHAMPS Frédéric et LAMBILOT Caroline, Cybercriminalité-Etat des lieux, Imprimé par Anthemis, Limal, Belgique, 2016, p 79.

[2] ولو أنه إجراء قد تعترضه أيضا العديد من العقبات، في سبيل الوصول إلى تحديد هوية صاحب عنوان الـ "IP". على غرار عدم الالتزام بتحديد الهوية قبل الاقتناء، أو بالالتزام لكن عبر التصريح بهوية مزورة...الخ.

[3] **أنظر:** - DECHAMPS Frédéric et LAMBILOT Caroline, Idem, p 79 et 80.

[4] هذا مع التأكيد على إمكانية الاستنتاج أيضا؛ من عمل التحفظ العاجل على المعطيات المخزنة بنوعيها. حيث حتى وان كانت معطيات حركة السير محل التحفظ، غير حقيقية أو ناقصة؛ يمكن بنوع من الخبرة الإجرائية أن تستشف منها الهوية الحقيقية للمشتبه فيه.

كما أنه قد تتم عملية استنتاج هوية المشتبه فيه؛ من خلال استعمال عمل رقمي حديث، يقود في الأصل إلى تحديد المكان الجغرافي لتواجده، الذي يسمى بـــ "La Géolocalisation". حيث تصل أجهزة التحري والتحقيق من خلال الاتصال الشبكي والهاتفي التقليدي –أو بوضع بطاقة على الجهاز– الذي يجريه المشتبه فيه؛ إلى تحديد النطاق الإقليمي المتواجد فيه. وهو ما يسهل لا محال من عملية تحديد هوته، بعد حصر الفرضيات في منطقة واحدة بدلا عن العديد من المناطق[1].

الإجراء الذي يعد معمولا به من أجهزة التحري والتحقيق في الجزائر، ولو بموجب النصوص الإجرائية العامة، نظرا لغياب النص الخاص الصريح الذي يقرر ذلك، وهذا سواءً بخصوص الجريمة التقليدية أو تلك المنطوية على جرائم الوسط الرقمي. وان كان في الإطار التشريعي المقارن؛ تم التدخل لتقنين هذا العمل نظرا لأهمية الكبيرة سيما بخصوص متابعة جرائم الوسط الرقمي. ونجد كأبرز مثال على ذلك، المشرع الفرنسي، الذي وضع الإجراء صراحةً سنة 2014 عبر تعديله لقانون الإجراءات الجزائية، بموجب القانون رقم 2014–44، المتعلق بتحديد الموقع الجغرافي[2].

3. التحديد الرقمي لهوية المشتبه فيه عبر الاستنتاج المتصل بالأعمال التقليدية الأخرى: زيادةً عن الأعمال الإجرائية السابقة بالذكر؛ يمكن لأجهزة التحري والتحقيق الوصول إلى تحديد الهوية الحقيقية للمشتبه فيه، عبر اللجوء إلى الطرق التقليدية، سواءً كعمل إجرائي مساعد وروتيني، أو كعمل يشكل الفرصة الوحيدة لتحديد الهوية. حيث قد يعتمد في ذلك على شهادة الشهود وفق القواعد الإجرائية السابقة بالذكر، أو على الاعتراف المباشر الطوعي؛ من الشخص غير المشتبه فيه أصلا.

وأما بخصوص كون العمل الإجرائي التقليدي هو الوسيلة الوحيدة لتحديد هوية المشتبه فيه؛ فقد يحدث ذلك عندما ترتكب الجريمة عبر "الويب المظلم–Dark Web"، الذي يخفي الهوية الحقيقية لرواده، عبر تقنية التشفير والخوادم الوسيطة –كما بينا سابقا–، على نحو يعدم تماما فرصة التعرف على هوية المشتبه فيه وفق كل الوسائل السابقة بالذكر.

ولعل السبيل الوحيد أمام أجهزة التحري والتحقيق في الجزائر لمواجهة ذلك؛ يتمثل في الاعتماد على عمل التسرب التقليدي، الذي اعتمده ونظمه المشرع الجزائري؛ بالأحكام السابقة بالذكر –مع التذكير ببروز تسرب حديث في التشريعات المقارنة يسمى بالتحقيق الرقمي تحت الاسم المستعار السابق بالذكر–. حيث يقوم المتسرب؛ بالولوج إلى الويب المظلم؛ للتعامل المستمر مع المشتبه فيه، حتى يوهمه أنه صديق ويحب الإجرام مثله، ما قد يدفعه للإفصاح عن هويته الحقيقية، وهو أمر جد نادر الحصول.

---

[1] وهو العمل الإجرائي الذي يتأسس فنيا على تقنية الـ "GPS"، التي اكتسبت في شكلها الحديث؛ ميزة الدقة واستبعاد الخطأ.
أنظر في ذلك: - BENSOUSSAN Alain et LEPAGE Agathe et QUEMENER Myriam, Op.cit, P 258.

[2] **أنظر:** - QUEMENER Myriam, Op.cit, p 159 et 160.

المطلب الثاني: الأوامر الحديثة المساعدة على التحري والتحقيق في جرائم الوسط الرقمي

زيادةً عن الأعمال الحديثة المساعدة على التحري والتحقيق في جرائم الوسط الرقمي، التي تحمل الطبيعة الرقمية المعقدة نفسها للمسرح الجرمي الافتراضي؛ يمكن أن يتم التعامل مع جرائم الوسط الرقمي بإجراءات حديثة أخرى، تكون في شكل أوامر تصدر عن الجهة القضائية المختصة على حسب الحالة. التي أصبغنا عليها الطابع الحديث، إن من منطلق رقمي افتراضي أو مستجد من حيث التشريع والعمل بها. خاصةً؛ وأننا تطرقنا فيما سبق إلى أبرز الأعمال الإجرائية التقليدية والحديثة من جهة، والأوامر الإجرائية التقليدية من جهة أخرى.

وعلى العموم؛ يتبين من خلال التطرق الدقيق إلى الأوامر الإجرائية الحديثة، الممكن إصدارها من الجهات القضائية المختصة لمواجهة جرائم الوسط الرقمي –وحتى الجريمة التقليدية–؛ أن أهمها –كونها الأهم؛ لا يعني أنها بالضرورة هي الأنجع والأفضل– ما ينطوي على الأمر بإنتاج وتقديم المعطيات الرقمية(فرع أول)، والأمر بمنع المشتبه فيه من مغادرة التراب الوطني(فرع ثانٍ)، وأخيرا الأمر بوضع المتهم تحت المراقبة الإلكترونية(فرع ثالث).

الفرع الأول: الأمر بإنتاج وتقديم المعطيات الرقمية

يعد الأمر بإنتاج وتقديم المعطيات الرقمية؛ من الإجراءات الحديثة المرقمنة، الذي سبق التعامل مع مثله في الإطار التقليدي بغرض الوصول إلى العديد من المعلومات غير الرقمية، التي من الممكن أن تفيد في سير إجراءات التحري و/أو التحقيق عموما. حيث تسارع أغلب التشريعات المقارنة؛ إلى تقنين هذا الأمر في قوانينها الداخلية، بإجراءات وقواعد رقمية حديثة تتناسب مع الطابع الافتراضي المعقد، الذي يمتاز به المسرح الجرمي الافتراضي. الأمر الذي سنعمل على تبيانه فيما يلي؛ من خلال التطرق إلى مفهوم الأمر بإنتاج وتقديم المعطيات الرقمية(أولا)، والإجراءات التي ينجز من خلالها هذا الأمر في القانون الجزائري ساري المفعول(ثانيا).

أولا: مفهوم الأمر بإنتاج وتقديم المعطيات الرقمية

التسليم بحقيقة التعامل الإجرائي مع أوامر تقديم المعلومات غير الرقمية، سواءً في مرحلة التحري أو بخصوص إجراءات التحقيق، بالاستناد إلى النص الإجرائي العام؛ الذي لا يطرح أي إشكال في هذا الصدد؛ لا يشكل بأي حال من الأحوال أساسا للقول بإمكانية اللجوء إلى ممارسة الأمر بإنتاج وتقديم المعطيات الرقمية، من دون الوقوف عند ضرورة تحديد مفهومه الحديث المستقل عما يشابهه في الإطار التقليدي، سيما وأننا نتعامل مع نطاق افتراضي فائق التعقيد والحداثة. وهو ما سنعمل على تبيانه فيما يلي؛ من خلال التعريف بأمر إنتاج وتقديم المعطيات الرقمية، وتحديد أهم خصائصه الحديثة.

1. تعريف الأمر بإنتاج وتقديم المعطيات الرقمية: كما سبق وبينا فان الأمر بإنتاج وتقديم المعطيات الرقمية؛ يعد بمثابة الأمر المرقمن إجرائيا، الذي سبق التعامل مع مثله في الإطار التقليدي أو حتى الحديث غير الرقمي. ويرجع السبب الأساس وراء رقمنته إلى الضرورة الملحة لذلك، المتصلة بالخصوصية الحديثة المعقدة للوسط الرقمي، التي تعد نفسها الدافعة إلى رقمنه العديد من الإجراءات التقليدية، كالمعاينة والتفتيش السابقين بالدراسة.

وكانت أول مرة يتم الإشارة فيها قانونا إلى الأمر بإنتاج وتقديم المعطيات الرقمية؛ بمناسبة الاتفاق على معاهدة بودابست لسنة 2001 –السابقة بالذكر–. حيث تضمنته بالمادة 18 مباشرة بعد عمل التحفظ العاجل على المعطيات الرقمية، تحت عنوان "Injonction de produire". فألزمت –الاتفاقية– كل دولة طرف بضرورة تبني إجراءات تشريعية وغيرها، بغرض تأهيل سلطاتها المختصة لتأمر كل شخص على إقليمها بإرسال المعطيات الرقمية المبحوث عنها، التي هي بحوزته أو تحت سيطرته. وكذا أمر مزود الخدمة الممارس لمهامه في إقليم الدولة نفسها؛ لإرسال معطيات حركة السير والخدمات ذات الصلة بها، التي تكون في حوزته أو تحت سيطرته[1].

ولم تخرج الاتفاقية العربية لمكافحة جرائم تقنية المعلوماتية لسنة 2010 –السابقة بالذكر أيضا–؛ عن الطرح الوارد في اتفاقية بودابست المبين أعلاه. حيث اعتمدت إجراء الأمر بإنتاج وتقديم المعطيات الرقمية؛ بموجب المادة 26 منها، تحت عنوان "أمر تسليم المعلومات". فألزمت بموجبها كل دولة طرف؛ بضرورة تبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر، إلى الأشخاص ومزودي الخدمات بالطريقة نفسها المبينة أعلاه؛ من أجل تسليمها المعطيات الرقمية المبحوث عنها، التي تكون في حيازة أو تحت سيطرة الجهة المأمورة[2].

وأما على المستوى المقارن؛ فاعتمدت العديد من التشريعات المقارنة إجراء الأمر بإنتاج وتقديم المعطيات الرقمية، وان كان بطريقة غير مباشرة في العديد من الأحيان. فلو أخذنا التشريع الفرنسي على سبيل المثال؛ لقلنا أنه لم يتطرق صراحةً؛ إلى هذا الأمر، بل تعرض له ضمنا في إطار عمل التحفظ العاجل على المعطيات الرقمية المخزنة. وذلك من خلال القول بأنها معطيات يتم التحفظ عليها بغرض مساعدة الأجهزة المختصة، بخصوص إجراءات التحري والتحقيق الجارية[3].

وبغرض تقديم المساعدة المبينة أعلاه؛ ينجز الشخص المطلوب منه –مقدم خدمة في العادة–؛ عمل التحفظ العاجل على المعطيات الرقمية المخزنة، بطلب من الجهاز المختص في التحري أو التحقيق

---

[1] **أنظر:** - Art 18-1; Convention sur la cybercriminalité- Budapest, op.cit.

[2] **أنظر:** المادة 25؛ مرسوم رئاسي رقم 14-252، مرجع سابق.

[3] **أنظر:** - Art L32-3-1/2; Code des postes et des communications électroniques français, Op.cit.

بخصوص جرائم الوسط الرقمي. ومن ثم يسلمها للجهاز نفسه؛ بعد تلقيه الأمر منه بذلك، وهو ما تمت معالجته عالجه بنص قانون الإجراءات الجزائية، في إطار ما تسمى بـــ "التسخيرة–La Réquisition"[1]. التي جاءت بمفهوم عام تشمل التسخير التقليدي والرقمي، وكذا التسخير المتصل بإنتاج وتقديم المعطيات الرقمية وغيرها من الأعمال الرقمية[2].

رجوعا إلى القانون الجزائري، نجد أنه اعتمد الأمر بإنتاج وتقديم المعطيات الرقمية؛ بالطريقة نفسها التي انتهجها المشرع الفرنسي. حيث اكتفي بالنص الاتفاقي الصريح الوارد في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 –المصدق عليها سنة 2014–، وفي الوقت نفسه اعتمد بالتشريع الداخلي؛ نهج التطرق الضمني بالنصين الحديث والتقليدي.

فلو ذهبنا إلى أحكام القانون 09–04 السابق بالذكر؛ لوجدنا أن المشرع قد أشار عرضا إلى الأمر بإنتاج وتقديم المعطيات الرقمية، عند تطرقه إلى التزامات مقدمي الخدمات. حيث اعتبر التحفظ العاجل على المعطيات الرقمية المخزنة؛ بمثابة العمل المنجز بغرض وضع هذه المعلومات أساسا تحت تصرف الجهة القضائية التي طلبت هذا التحفظ. ولو أن المعطيات المقصودة بالوضع تحت التصرف بمفهوم القانون 09–04؛ تقتصر على تلك المتعلقة بحركة السير دون المحتوى[3].

يتبين مما طرح أعلاه، أن الجهة القضائية التي طلب التحفظ العاجل على المعطيات الرقمية المخزنة؛ ليست بحاجة فيما بعد لإصدار أمر الإنتاج والتسليم بخصوص المعطيات نفسها بعد التحفظ عليها، نظرا لقول المشرع صراحة؛ على أن التحفظ يكون بغرض الوضع تحت التصرف. ومع ذلك يمكن بالرجوع إلى النص العام لقانون الإجراءات الجزائية، القول بأن المشرع منح الحق للسلطات القضائية القائدة للتحري والتحقيق؛ حتى تتخذ أي إجراء نزيه ومشروع من شأنه المساعدة على السير الحسن لإجراءات التحري والتحقيق[4].

وعلى العموم؛ حاولت بعض الدراسات ذات الصلة بجرائم الوسط الرقمي؛ وضع تعريف مناسب للأمر بإنتاج وتقديم المعطيات الرقمية، كإجراء رقمي حديث. وفي سبيل ذلك، نذكر من عرفه، تحت

---

[1] **أنظر:** - Art 60-1, 77-1-1 et 99-3; code de procédure pénale français, Op.cit.

[2] ويمكن أن نستنتج تعرف "التسخيرة الرقمية-La Réquisition Informatique"، من خلال الدراسات ذات الصلة؛ على أنها: "سلطة منحها القانون للجهة القضائية المختصة، حتى تسخر مقدمي الخدمات الرقمية -وغيرهم ممن لهم علاقة بالوسط الرقمي-؛ بغرض تسليمهم المعطيات الرقمية المخزنة لديهم، التي ستفيد في فك خيوط القضية الجزائية السارية بخصوص جريمة من جرائم الوسط الرقمي كأصل عام، على أن تنجز وفق قواعد وشروط محددة مسبقا بالنص التشريعي والأمر القضائي". **أنظر في ذلك:** - DECHAMPS Frédéric et LAMBILOT Caroline, Op.cit, p 66 et 67.

[3] فعبر المشرع عن ذلك؛ بـ:"...وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 أدناه، تحت تصرف السلطات المذكورة". **أنظر في ذلك:** المادة 1/10؛ قانون رقم 09-04، مرجع سابق.

[4] **أنظر:** المادتان 1/36-4 و1/68؛ أمر رقم 66-155، مرجع سابق.

تسمية إنتاج المعطيات المعلوماتية؛ على أنه: "إجراء يفرضه القانون على مقدم خدمات الإنترنت يلتزم من خلاله بموافاة السلطات المختصة بالبحث والتحقيق بكل المعطيات أو البيانات المعلوماتية المتعلقة بالمشتركين وخدماتهم وغيرها، المتواجدة أصلا تحت سيطرته"[1].

يمكن من خلال كل ما بيناه بخصوص الأمر بإنتاج وتقديم المعطيات الرقمية؛ أن نضع تعريفا له، من خلال الإبقاء على مزايا التعريف المذكور أعلاه، ومحاولة تدعيمه بما نراه مناسبا، سيما وأننا نتحدث عن سلطات قضائية متصلة بالتسخير الإجرائي، الذي لم يحده قانون الإجراءات الجزائية بمعالم معينة. وعليه نقول أنه: "أمر إجرائي يصدر عن وكيل الجمهورية أو قاضي التحقيق على حسب الحالة، بغرض خدمة التحري أو التحقيق، عبر تسخير مقدم خدمة أو أي شخص له علاقة بالمسرح الجرمي الافتراضي، من أجل تسليمهم المعطيات الرقمية المبحوث عنها، التي يم إنتاجها والتحفظ عليها بمعرفتهم".

2. خصائص الأمر بإنتاج وتقديم المعطيات الرقمية: يمكن أن نستشف من التعريف المقدم لإجراء الأمر بإنتاج وتقديم المعطيات الرقمية –وكذا من كل ما بيناه أعلاه وسابقا–؛ أن له العديد من الخصائص الإجرائية، التي تميزه وتعطيه الصفة القضائية الخاصة. حيث يعتبر بمثابة الأمر القضائي، الذي لا يصدر إلا عن قاضٍ مختص –على حسب الحالة–، ولايمكن لضباط الشرطة القضائية إصداره أو تنفيذ محتواه من دون الرجوع إلى القاضي المختص بإصداره.

كما يعتبره البعض على أنه إجراء مرن غير مكلف. الذي لا يتصف بالجبر المتصل بالمشتبه فيه أو المتهم، وإنما يوجه إلى مقدم الخدمة أو أي شخص آخر غير أطراف الدعوى، الذي ينجز ذلك من دون عناء ولا تكلفة نظرا لكون التحفظ على المعطيات في العادة هو إجراء روتيني لدى مقدمي الخدمات خاصةً[2].

كما أنه يوجه إلى شخص أو مقدم خدمة محدد بالذات، الذي يتوجب فيه حسب المادة 25 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 –السابقة بالذكر–؛ أن يكون الحائز أو المسيطر الفعلي على المعطيات المبحوث عنها، التي تحدد بالذات بطريقة لا يمكن أن تسلم مع غيرها من المعطيات؛ إلا في حالة الاستحالة التقنية للفصل بينهما. الأمر الذي يترتب عليه إلى حدٍ ما؛ الحماية الكافية لسرية وحرمة الحياة الخاصة.

مع الإشارة إلى أن الأمر بإنتاج وتقديم المعطيات الرقمية؛ يتصل وفق المادة 25 من الاتفاقية العربية، على العكس من القانون 09-04 سيما المادة 1/10 منه؛ بكل أنواع المعطيات، سواءً المتعلقة بحركة السير أو المتضمنة للمحتوى، وكذا لا فرق بين تلك المتحفظ عليها في إطار ممارسة عمل التحفظ العاجل

[1] **أنظر:** جمال براهيمي، مرجع سابق، ص 108.

[2] **أنظر:** المرجع نفسه، ص 109.

على المعطيات الرقمية المخزنة أو غيرها. فالمهم أن تكون تحت حيازة أو سيطرت الجهة المسخرة. وترى أغلب الدراسات؛ أن المراد من الحيازة والسيطرة؛ أن تكون المعطيات الرقمية المبحوث عنها تحت التصرف الفعلي للجهة المسخرة[1].

ثانيا: إجراءات ممارسة الأمر بإنتاج وتقديم المعطيات الرقمية

لم يتطرق المشرع بالقانون 09-04؛ إلى الإجراءات واجبة الإتباع من أجل ممارسة الأمر بإنتاج وتقديم المعطيات الرقمية، بل اكتفى بالنص الضمني على هذا الإجراء كما بينا سابقا. الأمر الذي نضم بنوع من التفصيل في إطار اتفاقية بودابست والاتفاقية العربية، وكذا من قبل بعض التشريعات المقارنة، سيما الفرنسي منها الذي اعتبر ذلك داخلا في إطار التسخيرة الرقمية. وعلى العموم؛ سنحاول فيما يلي أن نبين إجراءات ممارسة الأمر بإنتاج وتقديم المعطيات الرقمية، في إطار القانون الجزائري عموما، من خلال التطرق إلى سياقه الإجرائي وأطرافه.

1. السياق الإجرائي لممارسة الأمر بإنتاج وتقديم المعطيات الرقمية: يتضح من خلال المفهوم العام لإجراء الأمر بإنتاج وتقديم المعطيات الرقمية، السابق بالذكر؛ أنه إجراء بسياق واسع يتصل بكل المعطيات الرقمية، كما قد يتعلق بأي عمل إجرائي رقمي ومرقمن آخر أو من دون ذلك. إلا أننا بالرجوع إلى القانون الجزائري بصورة خاصة؛ نجد أنه جاء بأحكام اتفاقية وتشريعية متضاربة تخلط السياق الإجرائي عموما.

الثابت من خلال نصوص القانون الجزائري، أن الأمر بإنتاج وتقديم المعطيات الرقمية؛ إجراء لايمكن انجازه إلا في إطار التسخير القضائي. وهو –التسخير القضائي– المعمول به قضائيا سواءً في إطار مرحلة التحري أو إجراءات التحقيق؛ قبل بروز جرائم الوسط الرقمي ومسرحها الجرمي الافتراضي. على غرار التسخير الصادر لمدير شركة يعمل فيها المشتبه فيه؛ حتى يقدم المعلومات ذات الصلة التي تكون تحت حوزته بصفته الجهة المستخدمة.

إلا أن التسخير القضائي نفسه؛ أخذ سياق إجرائي معقد نوعا ما في إطار مكافحة جرائم الوسط الرقمي. حيث يستنتج من مواد القانون الجزائري ذات الصلة؛ أننا قد نكون أمام التسخير القضائي بالمفهوم العام الواسع، كما قد نتعامل مع المفهوم المعاكس القائم على البعد الخاص الضيق. فيمكن وفق ذلك أن يكون للتسخير مفهوما عاما واسعا؛ إذا ما أخذنا بنص الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 –التي صدقت عليها الجزائر سنة 2014–، وأسسنا عليه ممارسة الأمر بإنتاج وتقديم المعطيات الرقمية[2].

---

[1] **أنظر:** جمال براهيمي، مرجع سابق، ص 110.

[2] **أنظر:** المادة 25؛ مرسوم رئاسي رقم 14-252، مرجع سابق.

ونؤسس تكييفنا للأمر بإنتاج وتقديم المعطيات الرقمية الوارد بالاتفاقية العربية، على أنه بمفهوم عام واسع؛ نظرا لسببين اثنين. ينطوي الأول في ورود هذا الأمر؛ كإجراء مستقل عن باقي الإجراءات الرقمية والمرقمنة المقررة بالاتفاقية نفسها، حيث يمكن تصور التسخير المباشر لمقدم الخدمة؛ لينتج ويقدم المعطيات الرقمية، من دون أي إجراء سابق من حيث الطلب[1]. وأما السبب الثاني؛ فيقوم على صفة التعميم الواردة بنص الاتفاقية؛ من حيث نوع المعطيات محل البحث، التي قد تتعلق بالمحتوى كما قد تتصل بمعطيات حركة السير أو الاثنين معا[2].

كما يمكن أن نؤسس للإجراء نفسه على أن له مفهوم خاص ضيق؛ وذلك بالرجوع إلى أحكام القانون 09-04. الذي ربط التسخير المتصل بأمر إنتاج وتقديم المعطيات الرقمية؛ لزاما بعمل التحفظ العاجل على المعطيات الرقمية. بطريقة لايمكن تصور التسخير محل الطرح؛ إلا بخصوص المعطيات محل التحفظ المسبق[3]. وكذلك ورد بالقانون نفسه؛ أن المعطيات محل التحفظ العاجل التي ستكون محلا لممارسة أمر الإنتاج والتقديم؛ تقتصر على معطيات حركة السير فقط دون تلط المتصلة بالمحتوى[4].

2. أطراف الأمر بإنتاج وتقديم المعطيات الرقمية: انطلاقا من التحديد السابق لأجهزة التحري والتحقيق في جرائم الوسط الرقمي، يمكن القول أن أطراف الأمر بإنتاج وتقديم المعطيات الرقمية؛ لا يمكن أن تخرج عن وكيل الجمهورية وقاضي التحقيق –على حسب الحالة– من جهة، ومقدمي خدمات شبكة الاتصال الدولية من جهة أخرى.

إلا أنه بالرجوع إلى القانون 09-04 أولا، والاتفاقية العربية لمكافحة جرائم تقنية المعلومات ثانيا[5]؛ نجد أن القانون 09-04 حصر الجهة المصدرة للأمر في جهاز النيابة العامة، دون التحقيق القضائي بتعبيره "السلطات المكلفة بالتحريات القضائية"، وهو ما نصفه بالسهو في التعبير لا أكثر لكونه إجراء يتصل بالتحري والتحقيق معا. وأما من حيث الجهة محل التسخير التي تنفذ الأمر؛ فرغم حصرها في القانون نفسه؛ بمقدم خدمة الاتصال؛ يمكن القول أنها أوسع مفهوما من ذلك –سيما وفق الاتفاقية العربية–، فيمكن أن تشمل مقدمي خدمات المحتوى وأي شخص يحوز أو يسيطر على المعطيات محل البحث[6].

---

[1] فرغم ورود إجراء الأمر بإنتاج وتقديم المعطيات الرقمية، بالمادة 25 من الاتفاقية، بعد عملي التحفظ العاجل على معطيات المحتوى والمرور الواردين بالمادين 23 و24 على التوالي. إلا أنه لا يوجد ما يوحي في المادة 25؛ أنه لاحق بالضرورة عن التحفظ العاجل. ومنه يصح القول بإمكانية ممارسة أمر إنتاج وتقديم المعطيات؛ بعد التحفظ العاجل أو من دون ذلك.

[2] **أنظر:** المادة 25/1-1 و2؛ مرسوم رئاسي رقم 14-252، مرجع سابق.

[3] الأمر الذي يفهم صراحةً؛ من تعبير المشرع: "...وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 أدناه، تحت تصرف السلطات المذكورة". **أنظر في ذلك:** المادة 1/10؛ قانون 09-04، مرجع سابق.

[4] **أنظر:** المادتان 1/10 و11؛ المرجع نفسه.

[5] **أنظر:** المادة 1/10؛ المرجع نفسه. **وأنظر أيضا:** المادة 25/1-1 و2؛ مرسوم رئاسي رقم 14-252، المرجع نفسه.

[6] حيث قد يحوز صاحب محل مجوهرات مثلا؛ على معطيات رقمية قد تفيد في إثبات جريمة السرقة التقليدية، المتحصل عليها من جراء الكمرات الرقمية المثبتة في المحل.

الفرع الثاني: الأمر بمنع المشتبه فيه من مغادرة التراب الوطني

استحدث المشرع عند تعديله لقانون الإجراءات الجزائية سنة 2015 بالأمر رقم 15-02 السابق بالذكر[1]؛ إجراءً جديدا يمنح لجهاز النيابة العامة ممثلا في وكيل الجمهورية، سلطة منع المشتبه فيه من مغادرة التراب الوطني الجزائري. الأمر الذي يمكن أن يتم اللجوء إليه؛ لمواجهة المشتبه فيه في جرائم الوسط الرقمي، خاصةً وأنها جرائم ذات بعد عالمي قد يشترك في ارتكابها العديد من الأشخاص متعددي الجنسيات، ما يزيد من فرضية مغادرة التراب الوطني للفرار من منطقة إلى أخرى. وعلى العموم سنعمل فيما يلي؛ على دراسة الأمر بمنع المشتبه فيه من مغادرة التراب الوطني من حيث قواعده الإجرائية العامة(أولا)، على أن نتطرق بعد ذلك إلى مواجهة المشتبه فيه الرقمي من خلال الأمر نفسه(ثانيا)[2].

أولا: القواعد الإجرائية العامة لمنع المشتبه فيه من مغادرة التراب الوطني

وضع المشرع عند استحداثه لإجراء الأمر بمنع المشتبه فيه من مغادرة التراب الوطني؛ مجموعة من القواعد الإجرائية التي تعد عامة في هذا الإطار؛ تطبق مبدئيا على الجنايات والجنح بكل أنواعها –رقمية وتقليدية وحديثة غير رقمية-. ولو أننا نستنتج القصور في هذه القواعد –كما سنبين فيما يلي-، التي اكتفت بتقرير الإجراء وإبراز أهم خطوطه العريضة من دون الخوض في التفصيل الواجب، سيما وأنه سيحد من أهم حق من حقوق الإنسان المنطوي على الحق في الحرية –حرية التنقل-. وعلى العموم، يمكن أن نتطرق إلى القواعد العامة لإجراء المنع من مغادرة التراب الوطني؛ من خلال استعراض تعريفه وشروط الأمر به.

1. تعريف منع المشتبه فيه من مغادرة التراب الوطني: جاء المشرع الجزائري محاولةً منه لتحديث أغلب قواعد الإجراءات الجزائية في الفترة الأخيرة؛ بالإجراء محل الطرح، المنطوي على المنع من مغادرة التراب الوطني. الذي أسس له وجعله من صلاحيات جهاز النيابة العامة دون سواها، تستعمله عند الحاجة الإجرائية لذلك.

عالج المشرع إجراء المنع من مغادرة التراب الوطني عموما؛ بموجب مادة واحدة تحت رقم 36مكرر1، تمم بها قانون الإجراءات الجزائية سنة 2015 بالأمر رقم 15-02. التي حاول من خلالها تبيان مضمون هذا الإجراء، مع التطرق –الذي يكاد يكون عرضيا- للشروط الإجرائية والموضوعية ذات الصلة بممارسة هذا الإجراء الحديث[3].

---

[1] **أنظر:** المادة 36مكرر1 مضافة بالمادة 07؛ أمر رقم 15-02، مرجع سابق.

[2] اعتبرنا أمر المنع من مغادرة التراب الوطني؛ من الإجراءات الحديثة في دراستنا، لا لأن له طابع رقمي خاص، وإنما لكونه من الإجراءات العامة، المستحدثة مؤخرا من المشرع. مع تأكيدنا على أن تطبيقه؛ يكون بخصوص الجريمة التقليدية والحديثة الرقمية وغير الرقمية.

[3] الشروط التي سنستعرضها في العنصر الموالي، بعد التعريج على التعريف بأمر المنع من مغادرة التراب الوطني.

يفهم من مضمون المادة 36مكرر1 "ق.إ.ج" السابقة بالذكر، أن المشرع أراد باستحداثه إجراء المنع من مغادرة التراب الوطني؛ الحفاظ على ملابسات الجريمة في إطار مرحلة التحري، مع ضمان عدم فرار المشتبه فيه إلى الخارج من دون عودة. فقد يغادر المشتبه فيه بجناية أو جنحة التراب الوطني من دون رجعة، برغبة الفرار من المسؤولية الجنائية، كما قد يغادره –التراب الوطني– بغرض العبث بملابسات الجريمة أو التأثير على الشهود مثلا، ثم ليرجع بعد ذلك. وهو ما يفهم من تعبير المشرع: "...لضرورة التحريات وبناءً على تقرير مسبب..."[1].

في الحقيقة الأمر بالمنع من مغادرة التراب الوطني؛ رغم كونه حديثا بخصوص إدخاله الصريح ضمن صلاحيات وكيل الجمهورية. إلا أنه كان من الممكن الوصول إلى تحقيق الغرض منه، بالاعتماد على إجراءات تقليدية سارية المفعول من قبل. حيث من صلاحيات وكيل الجمهورية التقليدية –التي لا تزال سارية المفعول حاليا–؛ إصدار أمر الإحضار ضد المشتبه فيه، الذي بمجرد تقديمه يتم استجوابه[2].

وفي حال تبين لوكيل الجمهورية بعد استجوابه للمشتبه فيه؛ وجود دلائل قوية ضده، وضرورة لمنعه من مغادرة التراب الوطني؛ يقوم باتهامه فورا عبر إصدار طلب افتتاحي لإجراء تحقيق، مع الطلب من قاضي التحقيق؛ أن يمنع المتهم من مغادرة التراب الوطني عبر إلزامه بإيداع جواز السفر في إطار الرقابة القضائية –السابقة بالدراسة–، أو يودعه الحبس المؤقت إن توفرت شروطه[3].

لذلك نقول بأن استحداث المشرع لصلاحية الأمر بمنع المشتبه فيه من مغادرة التراب الوطني؛ تعد إجراءً زائدا كما أنه يمس صراحةً بأهم حق من حقوق الإنسان المنطوي على الحق في حرية التنقل[4]، سيما وأنه يصدر عن وكيل الجمهورية الذي سيصبح خصما في الدعوى العمومية بمجرد تحريكها.

كما نقول لمن ينادي بالإضافة الكبيرة التي جاء بها تعديل قانون الإجراءات الجزائية بالأمر رقم 15-02، من حيث أنه غل يد النيابة العامة في مواجهة المشتبه فيه عبر ضمان كرامته وحريته، مؤسسين ذلك بإلغاء سلطة الحبس في الجريمة المتلبس بها واستحداث المثول الفوري[5]. أن المشرع الذي أعطى القليل باليد اليمنى أخذ الكثير بنظيرتها اليسرى، فسلطة الحبس لـــ 08 أيام الملغاة؛ كانت على الأقل لاتُعمل إلا

---

[1] فقد يبين التقرير المحرر من ضابط الشرطة القضائية؛ أسبابا جدية تتصل بمحاولة المشتبه فيه الفرار خارج التراب الوطني، أو المغادرة للمساس بالملابسات أو التأثير على الشهود...الخ. ما يشكل إنتاجا صريحا لضرورة تحري ملحة؛ تدفع وكيل الجمهورية المختص لإصدار أمنع المنع من مغادرة التراب الوطني، ضد المشتبه فيه. **أنظر في ذلك:** المادة 36مكرر1/1؛ أمر رقم 66-155، مرجع سابق.

[2] **أنظر:** المادتان 58 و3/110؛ المرجع نفسه.

[3] **أنظر:** المواد 58 و67 و3/110 و125 مكرر1/1-4 و123؛ المرجع نفسه.

[4] الحق في حرية التنقل المكفول دستوريا -وقبل ذلك دوليا-؛ بموجب المادة 55 من الدستور الجزائري. **أنظر في ذلك:** المادة 55؛ مرسوم رئاسي رقم 96-438، مرجع سابق.

[5] **أنظر:** المادة 16 المضيفة للمادة 339مكرر وما يليها والمادة 26؛ أمر رقم 15-02، مرجع سابق.

في الجناية والجنحة المتلبس بها، وأما سلطة المنع من مغادرة التراب الوطني المستحدثة؛ فتتصل بالجناية والجنحة عموما، سواءً أكانت متلبس بها أم في الحالة العادية[1].

وعلى العموم يمكن القول أن إجراء الأمر بالمنع من مغادرة التراب الوطني، بكل سلبياته وايجابياته؛ أصبح أمرا واقعا يتوجب التعامل معه بحثا وقضاءً، ما يدفع في إطار دراستنا إلى البحث في قواعده العامة، المتصلة بالتعريف به أولا وتبيان شروطه ثانيا. وان كان استعمال المشرع بالنص العربي لعبارة التراب الوطني؛ يعد حسب رأي الباحث في غير محله[2]. حيث إقليم الدولة الجزائرية حسب دستورها الساري؛ لا يقتصر على التراب البري، بل يزيد إلى كل من الإقليم البحري والجوي الذي يعلوا الاثنين[3].

يمكن من خلال ما ذكر بخصوص المضمون العام للإجراء المستحدث من المشرع، المنطوي أساسا على الأمر بمنع المشتبه فيه من مغادرة التراب الوطني؛ أن نضع له تعريفا نبني عليه الشروط الموضوعية والإجرائية التالية بالدراسة عموما، وممارسته في إطار جرائم الوسط الرقمي خاصةً. حيث نقول أنه: "إجراء مستحدث من اختصاص وكيل الجمهورية يمارسه كلما تطلبت ضرورة التحري ذلك، ليأمر بمنع المشتبه فيه –بجناية أو جنحة– الذي توجد ضده دلائل قوية، من مغادرة التراب الوطني لمدة زمنية محددة قانونا".

2. شروط ممارسة الأمر بمنع المشتبه فيه من مغادرة التراب الوطني: يتبين من خلال نص المادة 36مكرر1 "ق.إ.ج" –الوحيدة–؛ أن المشرع قد وضع مجموعة من الشروط، لممارسة أمر المنع من مغادرة التراب الوطني. التي وان نجدها غير كافية من حيث الدقة الإجرائية اللازمة؛ يمكن أن نستنتج منها العديد من الشروط واجبة الإتباع، على غرار ما نعتبرها ذات طبيعة جنائية موضوعية، والأخرى التي تمثل الشق الجنائي الثاني المتصل بالشروط الإجرائية.

أ- **الشروط الموضوعية:** لم يتطرق المشرع الجزائري إلى الشروط الموضوعية ذات الصلة بممارسة أمر المنع من مغادرة التراب الوطني؛ إلا من حيث الذكر العام لنوع الجريمة الجائز في إطارها المنع. حيث فتح المجال بعبارة: "...توجد ضده دلائل ترجح ضلوعه في جناية أو جنحة من مغادرة التراب

---

[1] ولو أنه يمكن القول بمحاولة المشرع الموازنة بين السلطة الملغاة ونظيرتها المستحدثة، من منظور أخف الأضرار على حرية المشتبه فيه. حيث تم تخفيض درجة المساس بالحرية، من خلال التخلي عن الحبس لـ 08 أيام الذي يعدمها تماما –على شاكلة الحبس المؤقت-، واستبداله بالمنع من مغادرة التراب الوطني، الذي يحد منها فقط -على شاكلة التزامات الرقابة القضائية-.

[2] حيث القول بالمنع من مغادرة التراب الوطني؛ يقود بمفهومه الدقيق إلى حرمان المشتبه فيه من استعمال -لأي غرض كان- الإقليمين البحري والجوي للدولة. وعليه كان الأجدر التعبير بـ "الإقليم الوطني" بدلا عن "التراب الوطني"، خاصةً وأن النص نفسه الوارد باللغة الفرنسية؛ يعبر بـ "Territoire" ما يفيد معنى الإقليم وليس التراب، ولو أن دقة التفرقة بين المصطلحين؛ تبرز في اللغة العربية أكثر من نظيرتها الفرنسية. **أنظر في ذلك:** المادة 36مكرر1/1 المضافة بالمادة 07 (النسخة الفرنسية)، أمر رقم 15-02، مرجع سابق.

[3] **أنظر:** المادة 13؛ مرسوم رئاسي رقم 96-438، مرجع سابق.

الوطني"، وهو ما يقود للقول؛ بأن أمر المنع من مغادرة التراب الوطني؛ جائز الإصدار في مواجهة المشتبه فيه بأي جناية أو جنحة –دون المخالفات– مهما كانت درجة خطورتها أو العقوبة المقررة لها[1].

يتبين مما ذكر أعلاه؛ أنه من الممكن قانونا تصور منع أي شخص من مغادرة التراب الوطني، حتى وان كان مشتبها فيه بخصوص جنحة معاقب عليها بالغرامة دون الحبس[2]. وهو ما لا يتقبله المنطق الجنائي السليم، الذي يستبعد في العادة كل الإجراءات القهرية، من المتابعة المتصلة بالجرائم غير المعاقب عليها بعقوبة سالبة للحرية كالحبس والسجن. وأبرز دليل على ذلك؛ التزامات الرقابة القضائية والحبس المؤقت، اللذان لا يمكن اللجوء إليهما إلا بخصوص الجنايات والجنح المعاقب عليها بسلب الحرية[3].

ب– الشروط الإجرائية: بينت المادة 36مكرر/1 "ق.إ.ج" نفسها المذكورة؛ بعض الشروط الإجرائية واجبة الإتباع عند ممارسة أمر المنع من مغادرة التراب الوطني، التي نؤكد على أنها غير كافية من حيث عديد النقاط، سيما أنها لم تقرر البطلان الإجرائي؛ على مخالفة القواعد الإجرائية اللازمة. وعلى العموم بين المشرع في هذا الإطار؛ أن أمر المنع يمارس من خلال مرحلة التحري دون إجراءات التحقيق، وذلك عند تعبيره بـــ: "...لضرورة التحريات..."[4]. ولو أن ذلك يعد منطقيا لكونه قابل للممارسة في إطار إجراءات التحقيق؛ بتسمية أخرى في ضمن التزامات الرقابة القضائية السابقة بالدراسة.

ونظرا لاتصال إجراء المنع من مغادرة التراب الوطني بمرحلة التحري؛ فلا يمكن لغير جهاز النيابة العامة أن يمارسه عبر الأمر به –وكيل الجمهورية بتعبير النص–. كما أنه لا يخاطب إلا المشتبه فيه، الذي تتوفر لدى وكيل الجمهورية معلومات جدية عنه؛ تفيد بضلوعه في جناية أو جنحة. وهو ما عبر عليه النص ضمنا؛ بقوله: "...كل شخص توجد ضده دلائل ترجح ضلوعه في جناية أو جنحة..."[5].

إلا أنه لايمكن لوكيل الجمهورية أن يصدر الأمر بمنع المشتبه فيه من مغادرة التراب الوطني؛ إلا بعد تلقيه تقرير مسبب من ضابط الشرطة القضائية[6]، الذي يشتغل على ملف القضية، وله كل المعطيات المتصلة بموضوعها وأطرافها، سيما المشتبه فيه. الذي قد تصله حوله أخبار تدل على رغبته في مغادرة التراب الوطني، سواءً للفرار أو للمساس بملابسات الجريمة أو التأثير على الشهود أو غير ذلك. ومنه قد تتولد لدى وكيل الجمهورية –الذي له السلطة التقديرية–؛ قناعة بوجود ضرورة إجرائية لإصدار الأمر.

---

[1] **أنظر:** المادة 36مكرر1/1؛ أمر رقم 66-155، مرجع سابق.

[2] كجنحة الإساءة إلى رئيس الجمهورية مثلا. **أنظر في ذلك:** المادة 144مكرر؛ أمر رقم 66-156، مرجع سابق.

[3] **أنظر:** المادتان 124 و125مكرر1؛ أمر رقم 66-155، المرجع نفسه.

[4] **أنظر:** المادة 36مكرر1/1؛ المرجع نفسه.

[5] **أنظر:** المادة والمرجع نفسهما.

[6] وهو ما عبر عنه المشرع بـ: "...لضرورة التحريات، وبناءً على تقرير مسبب من ضابط الشرطة القضائية..." **أنظر في ذلك:** المادة والمرجع نفسهما.

وأما من حيث مدة تنفيذ أمر المنع من مغادرة التراب الوطني؛ فالمشرع ألزم وكيل الجمهورية بمواعيد محددة وفق أصل واستثناء. حيث يصدر الأمر لينفذ خلال مدة 03 أشهر كأقصى حد، ليصبح المشتبه فيه بعد ذلك حرا من حيث التنقل خارج التراب الوطني، إلا إذا ما تم تجديد هذه المدة لـــ 03 أشهر أخرى –لتصبح 06 أشهر في الإجمال–[1]. مع الإشارة لعدم تطرق المشرع لكيفية التجديد، هل بطلب من ضابط الشرطة القضائية، أو من وكيل الجمهورية من تلقاء نفسه، وهل يتطلب ذلك تقرير مسبب إضافي أم من دون الحاجة لذلك...الخ.

وخلافا للأصل المبين أعلاه، جاء المشرع في إطار الفقرة الثالثة من المادة نفسها؛ باستثناء من حيث مواعيد تنفيذ أمر المنع من مغادرة التراب الوطني. حيث جعل الآجال مفتوحة غير محددة بمدة معينة؛ في حال اتصل الأمر بمشتبه فيه بجريمة من جرائم الإرهاب أو الفساد[2]. فيصبح أمر المنع من مغادرة التراب الوطني في هذه الحالة؛ منتهيا عند الانتهاء من كل إجراءات مرحلة التحري[3]، أو بتعبير أدق عند استعمال وكيل الجمهورية لسلطة الملائمة، عبر الحفظ أو الرفع أو التحريك أو إجراء الوساطة[4].

وأخيرا نص المشرع صراحةً، على أن إجراء المنع من مغادرة التراب الوطني؛ يرفع بالأشكال نفسها التي فرض بها. أي عبر أمر رفع يصدر عن وكيل الجمهورية الذي أمر به، سواءً من تلقاء نفسه أو بتقرير مسبب آخر من ضابط الشرطة القضائية نفسه[5]. إلا أن مصطلح الرفع يدل على إنهاء أثر أمر المنع قبل انتهاء آجاله في الحالة العادية، أو في أي لحظة بخصوص المشتبه فيه بجرائم الإرهاب أو المخدرات. مع الإشارة إلى عدم تطرق المشرع إلى حالة انتهاء مرحلة التحري، قبل انتهاء مدة 03 أشهر –أو 06 أشهر– في الحالة العادية[6].

ثانيا: أمر المنع من مغادرة التراب الوطني في مواجهة المشتبه فيه الرقمي

دائما ما تطرقنا من خلال دراستنا؛ إلى القواعد العامة للإجراءات ذات المضمون العام غير المتصل بإجرام معين، على أن نسقطها بعد ذلك على جرائم الوسط الرقمي، لنبين مدى إمكانية القول بأنها من

---

[1] **أنظر:** المادة 36مكرر2/1؛ أمر رقم 66-155، مرجع سابق.

[2] الملاحظ أن المشرع ميز جرائم الإرهاب والفساد عن باقي الجرائم، من حيث فتح مدة سريان أمر المنع من مغادرة التراب الوطني، الأمر الذي يفهم منه أنها جرائم حظيت بمعاملة خاصة. إلا أن الأمر غير المفهوم؛ أن المشرع في أغلب باقي الإجراءات الخاصة؛ يحدد 05 جرائم منها جرائم الإرهاب، وقد يضيف أحيانا جرائم الفساد فنصبح أمام الـ 05 + 01، وفي هذه الحالة الخاصة اكتفي بنوعين فقط من الجرائم الخاصة. فهل هذا دليل على عدم ثبات المشرع على قائمة معينة لجرائم المعاملة الخاصة، أم أن لهذه التفرقة غاية معينة؟

[3] **أنظر:** المادة 36مكرر3/1؛ أمر رقم 66-155، المرجع نفسه.

[4] **أنظر:** المادة 36/1-5؛ المرجع نفسه.

[5] **أنظر:** المادة 36مكرر4/1؛ المرجع نفسه.

[6] ما يدفع للقول بتطبيق الأحكام العامة، التي تفيد بغل يد وكيل الجمهورية من سلطة قهر المشتبه فيه، بعد انتهاء مرحلة التحري، سواءً بالحفظ أو بالاتهام أو بإجراء الوساطة.

الإجراءات المساعدة على التحري والتحقيق في هذه الجرائم الحديثة. وهو ما سنبينه فيما يلي، من خلال محاولة إسقاط القواعد العامة لأمر المنع من مغادرة التراب الوطني –السابقة بالذكر–؛ على جرائم الوسط الرقمي بنوعيها الأساسيين، إن بخصوص تلك الماسة بأنظمة المعالجة الآلية للمعطيات، أو نظيرتها التقليدية المتصلة بالوسط الرقمي.

1. المنع من مغادرة التراب الوطني بمناسبة التحري عن جرائم المساس بأنظمة المعالجة الآلية للمعطيات: تعد جرائم المساس بأنظمة المعالجة الآلية للمعطيات؛ أهم نوعي جرائم الوسط الرقمي، من حيث ارتباطها الوثيق بالإجرام الرقمي الحديث مضمونا وأثرا. هي التي يكيفها المشرع كما بينا سابقا؛ على أنها جنح بسيطة ومشددة على حسب الحالة، مع المعاقبة عليها في مجملها بعقوبات سالبة للحرية وغرامات في الوقت نفسه[1].

ولو رجعنا إلى القواعد العامة المتصلة بأمر المنع من مغادرة التراب الوطني؛ لوجدنا أنها قابلة للتطبيق على المشتبه فيه الرقمي في جرائم المساس هذه. فلوكيل الجمهورية في هذه الحالة بعد أن يتلقى تقريرا مسببا من ضابط الشرطة القضائية؛ أن يأمر بمنع المشتبه فيه من مغادرة التراب الوطني لمدة 03 أشهر قابلة للتجديد مرة واحدة، لتصبح 06 أشهر كأقصى حد.

2. المنع من مغادرة التراب الوطني بمناسبة التحري عن الجريمة التقليدية المتصلة بالوسط الرقمي: زيادةً عن جرائم المساس بأنظمة المعالجة الآلية للمعطيات –جنح–؛ تعتبر الجريمة التقليدية –مخالفات وجنح وجنايات–، القابلة للارتكاب بتسهيل من النطاق الافتراضي للوسط الرقمي؛ من قبيل جرائم الوسط الرقمي الداخلة في دراستنا كما بينا سابقا[2].

إلا أنها غير قابلة في مجملها لأن يكون المشتبه به فيها؛ محلا لأمر المنع من مغادرة التراب الوطني، بل تخضع للشروط العامة السابقة بالذكر، بخصوص التفرقة بين أنواع الجريمة من حيث تكييفها. حيث لا يمكن منع المشتبه فيه الرقمي من مغادرة التراب الوطني في إطار الجريمة التقليدية المتصلة بالوسط الرقمي؛ إلا بخصوص الجنايات والجنح دون المخالفات.

كما تحدد مدة المنع من مغادرة التراب الوطني؛ بـــ 03 أشهر كأصل عام بخصوص الجنايات والجنح التقليدية المتصلة بالوسط الرقمي، التي تكون قابلة للتجديد مرة واحدة بالشروط نفسها لتصبح 06 أشهر كأقصى حد. على أن تكون الآجال مفتوحة إلى غاية الانتهاء من إجراءات مرحلة التحري؛ إذا ما تعلق الأمر بجريمة تقليدية لها تكييف الإرهاب أو الفساد؛ ارتكبت أو سهل ارتكابها عبر النطاق الافتراضي للوسط الرقمي.

---

[1] **أنظر:** المواد من 394مكرر إلى 394مكرر8؛ أمر رقم 66-156، مرجع سابق.

[2] **أنظر:** المادة 1/02-أ؛ قانون رقم 09-04، مرجع سابق.

الفرع الثالث: الأمر بوضع المتهم تحت المراقبة الإلكترونية

بالإضافة إلى كل الأوامر الإجرائية التقليدية والحديثة السابقة بالذكر؛ يعتمد المشرع الجزائري أيضا إجراءً يعتبر حديثا من حيث الورود التشريعي والاتصال الفني، وهو المنطوي على وضع المتهم تحت المراقبة الإلكترونية، وفق شروط وإجراءات معينة فرضتها طبيعة الإجراء نفسه المتعمد من المشرع. الإجراء الذي يمكن تصور ممارسته في مواجهة المتهم في جرائم الوسط الرقمي، وفق المضمون والقواعد نفسها المطبقة بخصوص الجريمة التقليدية والحديثة غير الرقمية. وعليه سنذهب فيما يلي؛ إلى تبيان المفهوم العام لإجراء الوضع تحت المراقبة الإلكترونية(أولا)، على أن نتطرق بعد ذلك إلى الإجراءات القانونية والتقنية المتبعة في سبيل ممارسة ذلك(ثانيا)[1].

أولا: مفهوم الوضع تحت المراقبة الإلكترونية

اكتفى المشرع عند استحداثه لإجراء وضع المتهم تحت المراقبة الإلكترونية؛ بمجرد النص عليه في إطار فقرة واحدة، لا تبين –ولا يمكن أن تبين– القواعد القانونية والتقنية واجبة الإتباع عند ممارسة الامر القاضي به. حيث تم النص على ذلك بموجب المادة 125مكرر1/3 "ق.إ.ج"، التي تتعلق أساسا –المادة عموما– بإجراء الرقابة القضائية السابق بالدراسة. وهو ما دفع بالفقه وكذا السلطة التنفيذية ممثلةً في وزارة العدل؛ إلى التدخل لتبيان العديد من النقاط، التي يمكن من خلالها أن نحدد مفهوم أمر وضع المتهم تحت المراقبة الإلكترونية، سيما من حيث تعريفه وخصائصه.

1. تعريف الوضع تحت المراقبة الإلكترونية: يعد نظام –إجراء– "الوضع تحت المراقبة الإلكترونية –Le placement sous surveillance électronique"[2] عموما؛ أحد أهم الأساليب الحديثة لتنفيذ العقوبة السالبة للحرية قصيرة المدة –السجن بالبيت–، أو لتحقيق أغراض المراقبة القضائية المطبقة على المتهم أثناء مرحلة التحقيق. وهذا عن طريق السماح للمحكوم عليه أو المتهم؛ بالبقاء في الوسط الفتوح خارج المؤسسة العقابية، مع رصد تحركاته وتحديدها في مجال معين، بواسطة جهاز يختلف باختلاف الصورة المتبعة–ما سنراه لاحقا–[3].

---

[1] مع الإشارة إلى أننا نعتبر الأمر بالوضع تحت المراقبة الإلكترونية؛ بمثابة الإجراء الرقمي الحديث، ليس من منطلق أنه متصل بالمسرح الجرمي الافتراضي، وإنما لكونه حديث من حيث النص التشريعي وخاصةً الممارسة القضائية من جهة، وكذلك باعتباره من جهة أخرى؛ على أنه يعمل بالنظام الرقمي الثنائي نفسه المتصل بالوسط الرقمي محل الدراسة.

[2] الذي يسمى بالتسمية ذاتها "pse"، أو بـ "المراقبة الإلكترونية-La surveillance électronique"، أو "السجن في البيت -La prison a domicile"، أو"السوار الإلكتروني-Le bracelet électronique". **أنظر في ذلك:** صفاء أوتاني، "الوضع تحت الرقابة الإلكترونية-السوار الإلكتروني-في السياسة العقابية الفرنسية"، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، مج 25، عدد 01، كلية الحقوق، جامعة دمشق، سوريا، 2009، ص 131.

[3] **أنظر:** كريم مسعودي، "نظام السوار الإلكتروني في ظل السياسة العقابية المعاصرة"، مجلة القانون والأعمال، جامعة الحسن الأول، المملكة المغربية، مقال منشور عبر الموقع الرسمي، تاريخ النشر: 16 نوفمبر 2015، تاريخ التصفح: 29 سبتمبر 2017، الرابط: http://www.droitetentreprise.com.

وفي غياب التعريفات القانونية لإجراء الوضع تحت المراقبة الإلكترونية؛ قدمت العديد من التعريفات الفقهية والرسمية، التي وإن تختلف بحسب الصورة الفنية المتبعة في المراقبة الإلكترونية، تتفق عند الوقوف أمام الغرض الأساس منها، المنطوي على إعمالها كبديل عن عقوبة الحبس أو كضامن لتطبيق تدابير الرقابة القضائية. ولعل أبرز هذه التعريفات؛ نجد أنها: "التزام المحكوم عليه أو المتهم بالإقامة في منزله أو محل إقامته خلال ساعات محددة، بحيث تتم متابعة الشخص الخاضع للمراقبة الإلكترونية"[1].

ومن التعريفات، نجد أيضا من تعتبر إجراء الوضع تحت المراقبة الإلكترونية، من منظور تطبيق العقوبة الجزائية؛ على أنه يمارس في مواجهة المدان، عبر اللجوء إلى وسائل تقنية تعمل وفق تقنيات رقمية. فيعرفونه على أنه: "إلزام المحكوم عليه بالإقامة في مكان سكنه، أو محل إقامته، خلال أوقات محددة، ويتم التأكد من ذلك من خلال متابعته، عن طريق وضع جهاز إرسال على يده يسمح لمركز المراقبة من معرفة ما إذا كان المحكوم عليه موجوداً في المكان والزمان المحددين من قبل الجهة القائمة على التنفيذ، فيعطي الكمبيوتر تقارير عن نتائج الاتصالات"[2].

يتضح من خلال مختلف التعريفات المبينة أعلاه، أن إجراء الوضع تحت المراقبة الإلكترونية؛ يشمل كل من المتهم في إطار إجراءات التحقيق القضائي والمدان نهائيا في آخر مرحلة إجرائية، المنطوية على التنفيذ الجزائي للعقوبة[3]. وهو ما لا يهمنا منه في إطار دراستنا؛ إلا الوضع المتصل بالمتهم عموما والمتهم الرقمي خاصةً، الذي –الإجراء– نص عليه المشرع صراحةً بالمادة 125مكرر3/1 من قانون الإجراءات الجزائية[4].

ومنه يمكن أن نعرف إجراء وضع المتهم تحت المراقبة الإلكترونية –بوصفه أمرا قضائيا–، وفق مضمونه المعتمد من المشرع، الذي جعله لا يمارس إلا بأمر من القاضي المختص، ضد المتهم المعني، الذي هو أصلا تحت الرقابة القضائية؛ على أنه: "أمر إجرائي يصدر عن القاضي المختص، مفاده حمل المتهم للسوار الإلكتروني، الذي يلعب دور الضامن من حيث مراقبته حول مدى تنفيذه لبعض التزامات الرقابة القضائية، المفروضة عليه أصلا".

---

[1] **أنظر:** كريم مسعودي، مرجع سابق.

[2] **أنظر:** فهد يوسف الكساسبة، "دور النظم العقابية الحديثة في الإصلاح والتأهيل-دراسة مقارنة"، مجلة دراسات علوم الشريعة والقانون، كلية الحقوق، الجامعة الأردنية، الأردن، مج 39، عدد 02، 2012، ص 395 و396.

[3] وأما أمر الوضع تحت المراقبة الإلكترونية، الذي يكون محله المدان نهائيا كبديل عن عقوبة الحبس وفق شروط وأحكام وحالات محددة -التي تعد خارج إطار دراستنا-؛ فاستحدثه المشرع ونظمه سنة 2018 عند تعديله لقانون تنظيم السجون وإعادة الإدماج الاجتماعي للمحبوسين. **أنظر في ذلك:** المادة 02 المضيفة للمواد من 150 مكرر إلى 150 مكرر16؛ قانون رقم 18-01، مؤرخ في 30 جانفي 2018، يتمم قانون رقم 05-04، يتضمن قانون تنظيم السجون وإعادة الإدماج الاجتماعي للمحبوسين، (ج ر) عدد 05، صادر بتاريخ 30 جانفي 2018.

[4] **نص المادة:** "يمكن قاضي التحقيق أن يأمر باتخاذ ترتيبات من أجل المراقبة الإلكترونية للتحقق من مدى التزام المتهم بالتدابير المذكورة في 1 و2 و6 و9 و10 أعلاه".

2. خصائص الوضع تحت المراقبة الإلكترونية: يمتاز إجراء –أمر– وضع المتهم تحت المراقبة الإلكترونية في القانون الجزائري؛ بالعديد من الخصائص. التي اكتسبها من خلال طريقة معالجته التشريعية من جهة، والقواعد الإجرائية التي جاء بها التنظيم المفوض تشريعا من جهة أخرى[1]. وعلى العموم يمكن أن نقول؛ أنه إجراء متصل بالرقابة القضائية، الذي يعد جبري بطبيعته، وجد لتحقيق أهداف متباينة، ولا يمكن ممارسته إلا بإتباع طرق تقنية معينة.

أ– إجراء متصل بالرقابة القضائية: يتضح من خلال نص المادة 125مكرر3/1 "ق.إ.ج"، أن المشرع لم يستحدث الوضع تحت المراقبة الإلكترونية؛ كإجراء مستقل بحد ذاته. وإنما لايمكن الأمر به إلا في مواجهة المتهم، الذي سبق وضعه تحت الرقابة القضائية، فتكون المراقبة الإلكترونية بمثابة الضمان والمراقب؛ لتنفيذ الالتزام المفروض على المتهم من قبل القاضي المختص[2].

وعبر المشرع صراحةً على ما ذكر أعلاه، بنصه: "يمكن لقاضي التحقيق أن يأمر باتخاذ ترتيبات من أجل المراقبة الإلكترونية للتحقق من مدى التزام المتهم بالتدابير المذكورة في 1 و2 و6 و9 و10 أعلاه". وهو ما رجعت السلطة التنفيذية لتؤكده، من خلال البطاقة الفنية الصادرة عن وزارة العدل، التي تشرح قواعد عمل الوضع تحت المراقبة الإلكترونية، فاعتبرت أنه من أهم أهداف وايجابيات الاعتماد على هذه المراقبة الحديثة؛ تدعيم الرقابة القضائية وتوسيع نطاقها وضمان احترام المتهم لالتزاماتها[3].

كما يفهم من النصين التشريعي والتنظيمي؛ أن الوضع تحت المراقبة الالكترونية؛ غير جائز إلا في بعض التزامات الرقابة القضائية وليس كلها، وذلك في حدود 05 التزامات من أصل 10 –المذكورة على سبيل المثال أصلا–. وهي عدم مغادرة الحدود الإقليمية المحددة من القاضي المختص، وعدم الذهاب إلى بعض الأماكن المحددة في أمر الرقابة، والامتناع عن رؤية والاجتماع بالأشخاص المحددين في الأمر نفسه، بالإضافة إلى التزام المكوث في الإقامة المحددة بالأمر وعدم مغادرتها إلا بإذن من مصدر الأمر، وأخيرا عدم مغادرة مكان الإقامة إلا بشروط ومواقيت محددة[4].

ب– إجراء بأهداف متباينة: يتبين من خلال مضمون المادة 125مكرر3/1 "ق.إ.ج" المذكورة، أن الهدف الأساس من وراء استحداث المشرع لإجراء الوضع تحت المراقبة الإلكترونية؛ ينطوي على ضمان تنفيذ

---

[1] التفويض الذي نص عليه المشرع صراحةً؛ بقوله: "تحدد كيفيات تطبيق المراقبة الإلكترونية المنصوص عليها في هذه المادة عن طريق التنظيم". **أنظر في ذلك:** المادة 125مكرر5/1؛ أمر رقم 66-155، مرجع سابق.

[2] توجد بعض التشريعات المقارنة، التي تعتمد الوضع تحت المراقبة الالكترونية؛ كإجراء مستقل عن الرقابة القضائية. على غرار المشرع الفرنسي، الذي جعله في المرتبة الثانية بعد الرقابة القضائية وقبل الحبس المؤقت. وان بتحجيم المضمون الوارد بتسمية "الإقامة الجبرية تحت المراقبة الإلكترونية-L'Assignation à résidence avec surveillance électronique". **أنظر في ذلك:** Arts 137 et 142-5; code de procédure pénale français, op.cit.

[3] **أنظر:** وزارة العدل، "بطاقة فنية حول نظام الوضع تحت المراقبة الإلكترونية"، الجزائر، د ت، ص 01.

[4] **أنظر:** المادة 125مكرر3/1؛ أمر رقم 66-155، المرجع نفسه. **وأنظر أيضا:** وزارة العدل، المرجع نفسه، ص 02.

بعض التزامات الرقابة القضائية، التي سبق فرضها على المتهم. إلا أن الحقيقة غير ذلك، فبالإضافة إلى ضمان تنفيذ التزامات الرقابة القضائية، يعزز إجراء وضع المتهم تحت المراقبة الإلكترونية؛ حقوق الإنسان والحريات الفردية، من خلال احترام قرينة البراءة ومبادئ المحاكمة العادلة، عبر الحد الجزئي من حرية المتهم بدلا من إعدامها كليا عبر اللجوء إلى الحبس المؤقت[1].

كما يهدف الوضع تحت المراقبة الإلكترونية؛ إلى التقليل من حالة العود عبر الوقاية منها، من خلال إبعاد المتهم عن إمكانية الاختلاط مع معتادي الإجراء داخل المؤسسات العقابية[2]. ويسعى من ناحية أخرى إلى ضمان استقرار حياة المتهم، من خلال احتفاظه بحياته العادية المتصلة بالعمل والدراسة والعائلة...الخ، ما يكون سببا مباشرا في تفادي صعوبة إعادة الإدماج الاجتماعي والمهني للمتهم الخارج من الحبس المؤقت، سيما لو حضي بالبراءة[3].

زيادةً على ما ذكر، يهدف الوضع تحت المراقبة الإلكترونية؛ إلى ضمان السير الحسن لإجراءات التحقيق السارية، عبر ضمان المراقبة عن بعد تنفيذا لالتزامات الرقابة القضائية. بالإضافة إلى المساعدة على حسن سير المؤسسات العقابية، عبر تفادي الاكتظاظ الذي يعد ظاهرة صعبة المواجهة بالإجراءات التقليدية، وفي الوقت نفسه يقلل من الإنفاق العام على المؤسسات نفسها[4].

إلا أنه رغم كل هذه الأهداف المذكورة؛ التي تعزز من مكانة إجراء الوضع تحت المراقبة الإلكترونية، في المنظومة الإجرائية الجزائية؛ نجد أن له الكثير من المخالب، التي تجعله محلا للنقد الفقهي. على غرار القول بصعوبة تقبله من الرأي العام، ومساسه المباشر بحرية وحرمة الحياة الخاصة للمتهم، وبمبدأ المساواة، فضلا عن كونه مثالا حيا للحرية الافتراضية ذات الكثير من الآثار الجانبية[5].

ج- إجراء بطابع جبري: يقوم إجراء الوضع تحت المراقبة الإلكترونية في القانون الجزائري، عكس أغلب التشريعات المقارنة -سيما الفرنسي منها-؛ على الطابع الجبري غير الرضائي. حيث إذا ما رأي القاضي المختص؛ بضرورته لضمان تنفيذ إجراءات الرقابة القضائية؛ يأمر به بغض النظر عن تقبله من

---

[1] **أنظر:** وزارة العدل، مرجع سابق، ص 01. **وأنظر أيضا:** ساهر إبراهيم الوليد، "مراقبة المتهم إلكترونيا كوسيلة للحد من مساوئ الحبس الاحتياطي-دراسة تحليلية"، مجلة الجامعة الإسلامية للدراسات الإسلامية، كلية الحقوق، جامعة غزة، فلسطين، مج 21، عدد 01، 2013، ص 673.

[2] **أنظر:** وزارة العدل، المرجع نفسه، ص 01. **وأنظر أيضا:** صادق ضريفي، "المراقبة الجنائية الإلكترونية كآلية بديلة للحبس الاحتياطي"، ورقة عمل مقدمة في إطار الملتقى الوطني الثالث الموسوم بتطورات النظم الإجرائية الجزائرية في ضوء التعديلات الإجرائية الأخيرة والتعديل الدستوري لسنة 2016، كلية الحقوق والعلوم السياسية، جامعة أكلي محند أولحاج، البويرة، الجزائر، 23 و24 ماي 2017، ص 07.

[3] **أنظر:** وزارة العدل، المرجع نفسه، ص 01. **وأنظر أيضا:** ساهر إبراهيم الوليد، المرجع نفسه، ص 676.

[4] **أنظر:** وزارة العدل، المرجع نفسه، ص 01. **وأنظر أيضا:** صفاء أوتاني، مرجع سابق، ص 152 و153.

[5] **أنظر:** صفاء أوتاني، المرجع نفسه، ص 155 و156 و158. **وأنظر أيضا:** كريم مسعودي، مرجع سابق. **وأنظر كذلك:** صادق ضريفي، المرجع نفسه، ص 07 و08.

المتهم أو رفضه. مع التأكيد على أنه يأخذ حكم الرقابة القضائية –لأنه ضامن لها فقط–، من حيث استبداله بالحبس المؤقت في حالة عدم التزام المتهم به[1].

وعلى النقيض من ذلك، يعتبر الوضع تحت المراقبة الإلكترونية من الإجراءات الرضائية في التشريع الفرنسي –وأغلب التشريعات المقارنة–. حيث يمكن للمتهم أو المحكوم عليه الذي تتوفر فيه الشروط اللازمة لذلك؛ أن يطلبه من الجهة القضائية المختصة، كما لا يمكن لهذه الأخيرة؛ أن تفرضه على المعني في حالة رفضه له[2].

د– إجراء بطابع قانوني تقني: يعد الوضع تحت المراقبة الإلكترونية؛ بمثابة الإجراء القانوني القائم على الأبعاد التقنية. وذلك لعدم إمكانية العمل به من الجهات القضائية المختصة؛ إلا بوجود نص قانوني يجيز ذلك أولا، وباستعمال معدات تقنية إلكترونية ثانيا. حيث يتيح النص القانوني؛ استعمال أجهزة تقنية متطورة، على غرار أجهزة الإرسال والاستقبال الرقمية، التي تختلف حسب الصورة المعتمدة[3].

ثانيا: ممارسة الأمر بوضع المتهم تحت المراقبة الإلكترونية

لممارسة الأمر بوضع المتهم تحت المراقبة الالكترونية؛ يتوجب إتباع العديد من القواعد الإجرائية مزدوجة الطبيعة، الدائرة بين القانونية والتقنية. التي لا فرق في إطارها بين المتهم في الجريمة التقليدية ونظيره في جرائم الوسط الرقمي، سيما وأنه إجراء تابع للرقابة القضائية، التي تطرقنا لها سابقا وبينا أنها جائزة التطبيق على المتهم الرقمي، وان طالبنا بضرورة التحديث في طبيعة الالتزامات المفروضة، حتى تتماشى مع الطابع الافتراضي المعقد للوسط الرقمي. وعلى العموم لايمكن تصور ممارسة أمر وضع المتهم تحت المراقبة الإلكترونية؛ إلا عبر إجراءات تتبع عند إصداره وأخرى تعمل بمناسبة تنفيذه.

1. إجراءات إصدار الأمر بوضع المتهم تحت المراقبة الإلكترونية: لايمكن قانونا ممارسة إجراء وضع المتهم تحت المراقبة الإلكترونية؛ إلا بعد صدور الأمر القضائي المقرر لها، وهو الذي يلي بالضرورة صدور أمر الرقابة القضائية. حيث إذا ما كان المتهم الرقمي –حتى غيره–؛ محلا لالتزام من التزامات الرقابة القضائية الواردة في البنود رقم 1 و2 و6 و9 و10 –سابقة الذكر–، من المادة 125مكرر2/1؛ ورأى القاضي الآمر بها، بضرورة متابعة حسن تنفيذها بطريقة فعالة؛ يأمر بالتبعية أن يوضع المتهم نفسه تحت المراقبة الإلكترونية وفق إجراءات التنفيذ التالية بالدراسة[4].

---

[1] **أنظر:** المادتان 123مكرر و125مكرر1؛ أمر رقم 66-155، مرجع سابق.

[2] **أنظر:** كريم صياد، "فعالية نظام المراقبة الإلكترونية في تنفيذ عقوبة الحبس المؤقت"، مداخلة مقدمة في إطار الملتقى الوطني الثالث الموسوم بتطورات النظم الإجرائية الجزائرية في ضوء التعديلات الإجرائية الأخيرة والتعديل الدستوري لسنة 2016، كلية الحقوق والعلوم السياسية، جامعة البويرة، الجزائر، 23 و24 ماي 2017، ص 04.

[3] **أنظر:** المرجع نفسه، ص 03.

[4] **أنظر:** المادة 123مكرر والمادة 125مكرر2/1 و3؛ أمر رقم 66-155، المرجع نفسه.

وفي الإطار نفسه؛ تتمثل أطراف أمر الوضع تحت المراقبة الإلكترونية؛ في المتهم بجناية أو جنحة معاقب عليها بعقوبة سالبة للحرية، محل تنفيذ التزامات الرقابة القضائية المذكورة، وكذا الجهة المكلفة بوضع الجهاز وضمان المراقبة، المتمثلة حسب وزارة العدل؛ في المكتب المختص المتواجد على مستوى المحاكم والمجالس القضائية، بالإضافة إلى مصالح الشرطة القضائية. على ألا يصدر القرار إلا عن القاضي المختص، المنطوي على قاضي التحقيق وغرفة الاتهام بمناسبة ممارسة إجراءات التحقيق الابتدائي، أو قاضي الحكم في الحالة العادية وكذا حالة المثول الفوري بمناسبة ممارسة التحقيق النهائي وتأجيل المحاكمة[1].

2. إجراءات تنفيذ الأمر بوضع المتهم تحت المراقبة الإلكترونية: تقوم عملية تنفيذ أمر وضع المتهم تحت المراقبة الإلكترونية؛ على إجراءات تقنية أكثر منها قانونية. حيث بمجرد صدور أمر الوضع؛ يلتزم المكتب المختص المتواجد على مستوى الجهة القضائية المعنية أولا؛ بتثبيت السوار الإلكتروني على كاحل المتهم –مع إمكانية تثبيته على مستوى معصم اليد–، ومصالح الشرطة القضائية المختصة؛ بضمان المراقبة المستمرة وتسيير السوار الإلكتروني المثبت[2].

وتمارس إجراءات تثبيت السوار الإلكتروني وتسييره المبينة أعلاه؛ وفق العديد من القواعد التقنية الفرعية المحددة بالتفصيل من طرف وزارة العدل. الذي –التفصيل– يفهم منه أن القضاء الجزائري يكتفي بالمراقبة الإلكترونية المتحركة دون الثابتة من جهة، ولا يعير من جهة أخرى؛ أي أهمية لطبيعة التقنية المستعملة عند انجاز هذه المراقبة المتنقلة[3]. وذلك رغم التباين المقارن التقني والتشريعي –الكبيرين–، حول التقنيات المستعملة نصا وتطبيقا[4].

---

[1] **أنظر:** وزارة العدل، مرجع سابق، ص 01 و02. **وأنتظر أيضا:** المواد 125مكرر1 و125مكرر2/3 و339مكرر6؛ أمر رقم 66-155، مرجع سابق.

[2] **أنظر:** وزارة العدل، المرجع نفسه، ص 02.

[3] فتقنيا يتم التفرقة بين ثلاثة صور من المراقبة الإلكترونية، حيث تقوم الأولى على طريقة البث المتواصل، وتتأسس الثانية على التحقيق التدقيقي -النداء التليفوني-، وأما الثالثة والأخيرة؛ فتنجز عن طريق الأقمار الصناعية -المراقبة بالساتل-. **أنظر في ذلك:** كريم صياد، مرجع سابق، ص 04.

[4] فلو ضربنا مثالا بالقانون الفرنسي؛ لوجدنا أنه يعتمد كل من المراقبة الإلكترونية "الثابتة-Statique" و"المتحركة-Mobile" معا. حيث تقوم المراقبة الثابتة؛ على ربط الاتصال بين السوار الإلكتروني المثبت في معصم أو كاحل المتهم، والهاتف الثابت المتواجد بمحل إقامته غير المتصل بالإنترنت. وتنجز الثانية عن طريق استعمال ثلاثة أجهزة أساسية، المتمثلة في السوار الإلكتروني المثبت في معصم أو أسفل قدم المعني، وجهاز استقبال محمول يوضع حول وسطه، مع تثبيت جهازا آخرا في محل إقامته. على ألا تعمل هذه الأجهزة الثلاث بطريقة جماعية، فإما يكون الاتصال بين السوار الإلكتروني والجهاز المثبت حول وسط الشخص عبر تقنية الـ "GPS"، أو بين السوار الإلكتروني نفسه والجهاز المثبت في محل إقامة الشخص نفسه، بواسطة تقنية "GSM". **أنظر في ذلك:**

- Arts de 723-7 a 723-14; code de procédure pénale français, op.cit. **et:** Ministère de la justice Française, "Le placement sous surveillance électronique", 27 juillet 2016. Disponible sur le Lien: http://www.justice.gouv.fr. **et:** Ministère de la justice Française, Circulaire de la DACG, n° CRIM 08-05/E3, du 28 janvier 2008, relative au placement sous surveillance électronique mobile, bulletin officiel du Ministère de la justice, France. Disponible sur le Lien: http://www.justice.gouv.fr, p p 03-05.

وعلى العموم تباشر عملية الوضع تحت المراقبة الإلكترونية؛ عبر أول إجراء المنطوي على وضع السوار الإلكتروني على مستوى كاحل المتهم –أو معصمه–، طيلة فترة المراقبة المحددة بالأمر الصادر عن القاضي المختص. السوار الذي له العديد من السمات والخصائص الأساسية، على غرار كونه مقاوم للماء والحرارة والرطوبة والغبار والاهتزازات والذبذبات والصدمات، وكذلك مقاوم للتمزق والقطع والفتح في حالة الربط، بالإضافة إلى كونه مقاوما للأشعة فوق البنفسجية وقوة الضغط، مع كونه قابلا للشحن الكهربائي –باستعمال الشاحن الخاص به–، ويحتوي على عازل مصنوع من القماش يفصله عن بشرة المتهم، ما يستبعد أعراض الحساسية[1].

ويتكون السوار الإلكتروني –الحامل للخصائص المبينة أعلاه–؛ من جزأين أساسيين. يقوم الأول منهما على تكنولوجيا الاتصال –شريحة "GSM" مثلا–، المدمجة مع نظام تتبع المواقع الجغرافية الذي يعمل عبر الاستعانة بالعديد من الطرق الفنية، سيما تقنيات "GPRS, LBS, GPS". ويتصل الجزء الثاني بتقنية الشحن الإلكتروني –الكهربائي–، المتمثلة في البطارية الواردة مع السوار. مع الإشارة إلى أن فتح هذا السوار الإلكتروني؛ لا يتم كأصل عام إلا آليا –أوتوماتيكيا–، وعبر الاستعانة بمفتاح معد خصيصا لهذا الغرض[2].

وبعد أن يثبت السوار الإلكتروني وفق التقنيات المبينة أعلاه على كاحل أو معصم المتهم؛ يصبح يعمل بطريقة فنية حُدِدَتْ معالمها بالبطاقة الفنية الصادرة وزارة العدل. حيث يبث السوار ذبذبات أو إشارات إلكترونية، تتصل مباشرة بمصالح الشرطة القضائية العاملة عن بد على تلقي وتسيير المراقبة محل الانجاز. بالإضافة إلى تمتعه –السوار– بخاصية تقنية تمكنه من تحديد مكان تواجد حامله وتوقيت ذلك، والإنذار الفوري من إزالته في حال تم ذلك[3].

وعلى العموم يتم الاستعانة عند تنفيذ أمر الوضع تحت المراقبة الإلكترونية، لغرض تسيير المتهم محل أمر الوضع؛ بواسطة برنامج رقمي –منظومة إعلام آلي–، يربط بين المواقيت والمواقع الجغرافية المعينة في الأمر القاضي بالمراقبة من جهة، والتحركات الفعلية للمتهم عبر تحديد مواقع تواجده بعد التنقلات التي يقوم بها من جهة أخرى. مع التأكيد على ضرورة استعانة مكتب مراقبة تنفيذ أمر الوضع تحت المراقبة الإلكترونية؛ بلوحة تحكم معلوماتية –رقمية– تسمح بتتبع ومراقبة مختلف تحركات المتهم حامل السوار الإلكتروني[4].

---

[1] **أنظر:** وزارة العدل، مرجع سابق، ص 02.

[2] **أنظر:** المرجع والصفحة نفسهما.

[3] **أنظر:** المرجع والصفحة نفسهما.

[4] **أنظر:** المرجع نفسه، ص 03.

كخلاصة للباب الثاني من الدراسة، يمكن القول أن المشرع الجزائري –وقبله الاتفاقي والمقارن–؛ قد سلم بخصوصية مواجهة جرائم الوسط الرقمي، بشقيها الموضوعي والإجرائي. حيث ولج موضوعيا ليجرم العديد من السلوكيات الرقمية والمرقمنة، بالاعتماد على العديد من القواعد الجنائية الحديثة، التي تتناسب مع المسرح الجرمي الافتراضي.

كما عمل المشرع بعد ذلك؛ على تحيين القواعد الإجرائية لتتناسب مع خصوصية الوسط الرقمي، بعد الولوج الموضوعي من حيث التجريم والعقاب. الأمر الذي أدى إلى إفراز الإطار الإجرائي العام المبين في الباب الأول، سيما من حيث التحيين في القواعد المتصلة بالأجهزة التقليدية الممارسة للتحري والتحقيق، سواءً بخصوص قواعد اختصاصها، أو الحث على ضرورة الاستعانة بمن لهم الخبرة الكافية في الوسط الرقمي. أو عبر إنشاء أجهزة حديثة متخصصة في مواجهة جرائم الوسط الرقمي، التي تعمل بنظام الفريق المتكامل، بالإضافة إلى الحث على ضرورة التعاون القضائي الدولي في هذا الإطار.

وفق سلم تدرجي إجرائي منطقي، توجب بعد ما ذكر أعلاه؛ النظر إلى المواجهة الإجرائية لجرائم الوسط الرقمي عبر التحري والتحقيق فيها؛ بالنظرة الرقمية الحديثة التي تغير لا محال من الإجراءات محل الممارسة، المنطوية على الأعمال والأذون والأوامر الإجرائية، المؤدية للوصول إلى الدليل الجنائي المظهر للحقيقة بخصوص الجرائم المرتكبة.

وعليه أصبحت الإجراءات الحديثة؛ تتأسس حول دليل جنائي من نوع حديث متمثل في الدليل الرقمي، الذي له ماهية حديثة تضفي عليه الكثير من الخصوصية، سيما وأن له حجية قانونية وقضائية في القانون وأمام القضاء الجزائريين. وهو الدليل –الجنائي الرقمي–؛ الذي أخلط المفهوم المعروف للإطار الإجرائي الخاص المتصل بالتحري والتحقيق في الجريمة عموما، ما دفعنا لإعادة توزيع الوسائل الإجرائية المؤدية إلى استخراجه بطريقة تتناسب مع خصوصيته الحديثة، فقلنا أنها جوهرية ومساعدة.

ورأينا أن الوسائل الجوهرية لاستخراج الدليل الجنائي الرقمي؛ تنطوي على المعاينة والتفتيش المرقمنين، وأبعادهما التقنية المنطوية، على ضرورة الاستعانة بالدعم التقني من مساعدة وخبرة، وكذا الحجز المرقمن المترتب عن كل ذلك.

وفي الوقت نفسه؛ كيفنا باقي الإجراءات؛ على أنها مساعدة لنظيرتها الجوهرية المذكورة. وهي المتمثلة في الإجراءات التقليدية، على غرار أعمال التنصت والتسرب وسماع واستجواب الأشخاص أولا، وإذن التوقيف للنظر وأمر الوضع تحت الرقابة القضائية، والإيداع في الحبس المؤقت ثانيا. بالإضافة إلى الإجراءات الحديثة الرقمية وغيرها، المنطوية على أعمل مراقبة الاتصالات الإلكترونية، والتحفظ العاجل على المعطيات الرقمية المخزنة وتحديد هوية المشتبه فيه، وكذا أمر إنتاج وتقديم المعطيات الرقمية، والأمر بالمنع من مغادرة التراب الوطني، وأخيرا الأمر بالوضع تحت المراقبة الإلكترونية.

الخـــاتـــمـــــــــــــة

يتبين من خلال دراسة إجراءات التحري والتحقيق في جرائم الوسط الرقمي؛ أنه موضوع من الأهمية بمكان، إن بالنظرة المجتمعية العامة أو القانونية الضيقة، سيما إذا ما رجعنا إلى ما بدئنا به الدراسة –في مقدمتها–، من خلال القول أنه موضوع قد أسال الكثير من الحبر، وان يبقى ذلك في إطار الدراسات السابقة، التي تجاوزها الواقع الرقمي سريع التطور.

فعمل الباحثين الأكاديميين وكذا المؤسسات الرسمية المختصة، كما بينا في متن الدراسة، على البحث المستمر والمتكرر في الموضوع؛ يؤكد أهميته التي لها وجه آخر، منطوي على كونها الدافع الأساس للوصول إلى العديد من النتائج القانونية بعد دراسة الموضوع، ومنه الوقوف عند كم وكيف لا بأس به من حيث التوصيات واجبة الإتباع، للوصول إلى المواجهة المرجوة لجرائم الوسط الرقمي، من خلال الوقاية والمكافحة معا.

وربطا بين النقاط الثلاث الأساسية في موضوع الدراسة، المنطوية على البعد الرقمي الحديث من جهة، والنص القانوني الساري المفعول –سيما القانون الجزائي الجزائري– من جهة ثانية، والدراسات الفقهية الجزائية من جهة أخرى، في إطار مقاربة بحثية قانونية تقوم على التحليل والنقد والتركيب القانونيين؛ يمكن القول أننا توصلنا في دراستنا هذه، إلى الإجابة عن أغلب الأسئلة المطروحة في إشكالية البحث ومشكلته عموماً.

فحاولنا من خلال الدراسة؛ التطرق إلى كل الجوانب القانونية، التي تتصل بصفة مباشرة أو غير مباشرة؛ بالتحري والتحقيق في جرائم الوسط الرقمي. باحثين من خلال ذلك الإجابة عن مضمون إشكالية الموضوع، التي تدور حول تحديد القواعد الإجرائية واجبة الإعمال –في القانون الجزائري– عند مواجهة جرائم الوسط الرقمي، عبر التحري والتحقيق فيها.

كما ذهبنا من خلال بحثنا هذا؛ إلى السعي وراء تحديد الطبيعة القانونية، المتصلة بهذه الإجراءات واجبة الإعمال للتحري والتحقيق في جرائم الوسط الرقمي. ومدى تكيفها مع المبادئ الإجرائية العامة، المعمول بها كإطار عام عند مواجهة الجريمة التقليدية المعهودة، التي تتصل بالوسط المادي الملموس، من خلال العمل على مكافحتها.

ويمكن القول أننا بعد التطرق إلى الإجراءات المعمول بها في التحري والتحقيق، محل الدراسة تحديدا وقياسا بنظيرتها التقليدية؛ توصلنا إلى الوقوف على تحديد العديد من النقائص الإجرائية النصية، واجبة التدارك، قبل أن تصبح بمثابة الثغرة المسهلة لفشل إجراءات التحري والتحقيق، ومنه إفلات الجناة وزيادة نسبة الجريمة في الوسط الرقمي، التي هي أصلا مرتفعة للعديد من الأسباب، تتمحور أغلبها حول الإشكالات الإجرائية، كقلة الاكتشاف والمتابعة.

وزيادة إلى ما ذكر؛ فإننا توصلنا إلى معالجة إشكالية الإجراءات المعمول بها تحديدا وطبيعة ونقصا، من خلال التطرق العرضي للإجراءات النافذة؛ في بعض التشريعات المقارنة –التي تعد رائدة في هذا المجال– من جهة، والاتفاقيات الدولية الإقليمية والعالمية –المصدق عليها من الجزائر والرائدة– من جهة أخرى. ومنه الفصل في كون الإشكالات التي تواجه المشرع الجزائري؛ هي لنقص فيه، أم للاستحالة الفعلية التي تواجه غيره على مستوى العالم.

وعلى العموم؛ يمكن القول أننا توصلنا بعد البحث المعمق في موضوع الدراسة، الموسوم بإجراءات التحري والتحقيق في جرائم الوسط الرقمي؛ إلى العديد من النتائج المتصلة بالإشكالات المبينة أعلاه وسابقا –وغيرها–، التي أسسنا عليها مجموعة من التوصيات، المعبرة عن رأي الباحث القائم بعد الدراسة والتحليل والنقد.

فتوصلنا من خلال دراسة موضوع البحث في إطار نتائجها –الدراسة–؛ إلى أن الخصوصية التي تكتنف الوسط الرقمي، هي أكبر بكثير مما يتصوره الكثير ومما طرح للدراسة القانونية من قبل. حيث لا تتصل الجريمة الحديثة؛ إلا بالنطاق الافتراضي الذي تحدثه عناصر الوسط الرقمي، دون هذه الأخيرة كماديات ملموسة. كما أن هذه العناصر لا تخرج في كل الأحوال عن عنصرين أساسين، تتفرع عنهما العديد من العناصر الأخرى، وهما المتمثلين في جهاز الإعلام الآلي وشبكة الاتصال الدولية.

وعليه المسرح الجرمي الذي تمارس فيه إجراءات التحري والتحقيق؛ ينحصر في النطاق الافتراضي المذكور أعلاه. وهو الذي له قسمين أساسيين، يتمثل الأول في "الويب السطحي–Surface Web" ويتصل الثاني بالويب العميق–Deep Web". حيث يعد التحري والتحقيق في الأول "الويب السطحي"؛ ممكنا في الكثير من الأحيان، بينما يدور ذلك بخصوص الثاني "الويب العميق"؛ بين الإمكانية النسبية في الأصل، والاستحالة المطلقة إذا ما تعلق الأمر بجزئه الخفي المسمى بـــ "الويب المظلم–Dark Web".

وعلى العموم يعد النطاق الافتراضي للوسط الرقمي المذكور أعلاه؛ بمثابة مسرح الجريمة الحديث، الذي يمتاز بالكثير من الخصوصية المذكورة في متن الدراسة. مع التأكيد على أنه معرض للتعديل والتحيين والتطوير في أي وقت، وكلما وجدت تقنيات جديدة تضاف إلى عنصريه الأساسيين، المنطويين على جهاز الإعلام الآلي، وشبكة الاتصال الدولية ومن في حكمهما.

كما أننا توصلنا من خلال دراستنا هذه؛ إلا أن الجريمة المتصلة بالمسرح الجرمي الافتراضي عموما؛ لها طابع خاص والكثير من الخصوصية أيضا. حيث تطرق إليها المشرع الجزائري عبر النظرة الحديثة اللازمة –موضوعيا–، التي جعلته يعتمد ما نسميه بمبدأ الشرعية العام أو الشامل. من خلال تأكيده بالمادة 1/02–أ من القانون 09–04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها –المذكور–؛ على أن جرائم الوسط الرقمي هي نوعان، جرائم المساس بأنظمة

المعالجة الآلية للمعطيات أولا، وثانيا الجريمة التقليدية التي ترتكب عبر النطاق الافتراضي للوسط الرقمي أو يكون المسهل لارتكابها.

وعليه نستنتج أن المشرع الجزائري يأخذ بمنطق التمييز، عبر التفرقة بين الجريمة الرقمية المنطوية على جرائم المساس، غير المسبوق التعامل مع مثلها. والجريمة المرقمنة، المنطوية على السلوكيات المجرمة بالنص التقليدي المعمول به من قبل، التي أصبح من الممكن تصور ارتكابها؛ في النطاق الافتراضي للوسط الرقمي أو بمساعدته.

وأما بخصوص إجراءات التحري والتحقيق في جرائم الوسط الرقمي، التي تعد محور الدراسة، فتبين لنا من خلال البحث فيها؛ أنها كانت في البداية تتصف بالعجز الإجرائي التام والكامل، إن من حيث الأجهزة الممارسة لها أو الأعمال والأوامر والأذون محل الممارسة من هذه الأجهزة. إلا أن المشرع الجزائري بداية من سنة 2004؛ حاول العمل على التعديل والتتميم المستمرين للإجراءات الجزائية، سيما من خلال القانون 09-04 المذكور. الأمر الذي نقول فيه بصفة عامة؛ أنه مس بالأجهزة والأعمال بالطريقة السلسة نوعا ما.

فمن حيث أجهزة التحري والتحقيق في جرائم الوسط الرقمي؛ يتبين أن المشرع الجزائري قد لامس المقبول إلى أبعد الحدود، من خلال العمل المزدوج على التدريب الرقمي للأشخاص من جهة، وإنشاء أجهزة أخرى حديثة متخصصة في مواجهة جرائم الوسط الرقمي من جهة أخرى. مع التأكيد على فتح المجال قانونا وواقعا أمام التعاون الدولي اللازم في مثل هكذا جرائم، انطلاقا من عالمية المسرح الجرمي الافتراضي أصلا والجرائم المتصلة به بالتبعية.

وأما بخصوص ممارسة إجراءات التحري والتحقيق في جرائم الوسط الرقمي؛ فنستنتج أنها تتمحور حول ما يسمى بالدليل الرقمي الجنائي. الذي يقوم على الأحكام والقواعد الفنية أكثر من نظيرتها القانونية النصية. وعليه نقول أن المشرع الجزائري؛ أحسن التصرف عندما لم يتطرق له بنصوص قانونية تضبطه، وتركه للقضاء الذي يتعامل معه؛ في إطار القواعد العامة المتصلة بنظام الإثبات الحر، سيما من حيث متطلبات الصحة القضائية حتى تقوم الحجية من عدمها.

إلا أن أجهزة التحري والتحقيق في جرائم الوسط الرقمي؛ تتخذ في سبيل وصولها إلى الدليل الرقمي الجنائي؛ العديد من الأعمال والأذونات والأوامر المقننة قانونا. التي تبين لنا بعد الدراسة المعمقة لموضوع الدراسة، أنها تتمثل وفق النصوص الإجرائية السارية المفعول؛ في الأعمال الجوهرية والأخرى المساعدة. حيث الطبيعة الافتراضية المعقدة للنطاق الافتراضي للوسط الرقمي؛ رفعت من عملي المعاينة والتفتيش –حسب الباحث–، إلى درجة الأعمال الجوهرية. فلا يمكن مهما كان عند مواجهة أي جريمة رقمية أو مرقمنة؛ الاستغناء عن أحد هذين الإجراءين.

وزيادةً عن الأعمال الجوهرية المذكورة، يمكن لأجهزة التحري والتحقيق؛ أن تباشر أعمالا أخرى مساعدة، التي قد تكون تقليدية كما قد تكون حديثة رقمية أو غيرها، أو قد تكون أيضا مدخلة في أحد الأعمال الجوهرية كالمعاينة أو التفتيش. فنقول أنه يمكن أن نواجه جرائم الوسط الرقمي ببعض الأعمال التقليدية –ليس الكل–، دون أن نقول أننا نواجه عجزا رقميا بالرجوع إلى الإجراءات التقليدية. ومن أبرز هذه الإجراءات؛ نجد التنصت والتسرب من جهة وسماع الأشخاص واستجوابهم. بالإضافة إلى توقيف المشتبه فيه للنظر ووضع المتهم تحت الرقابة القضائية أو الحبس المؤقت.

كما نستنتج في إطار الإجراءات المساعدة ذات الطابع الرقمي الحديث؛ أن المشرع قد واكب التطور المقارن والدولي بهذا الخصوص –إلى حد ما–. من حيث تقريره لعمل مراقبة الاتصالات الالكترونية بالمادة 03 وما يليها من القانون 09–04 المذكور، الذي يختلف تماماً عن عمل التنصت الهاتفي الحامل للطابع التقليدي. كما يعد عمل التحفظ العاجل عن المعطيات الرقمية المخزنة، والأمر بإنتاجها وتقديمها؛ من الإجراءات النافذة في القانون الجزائري، لكونها مقررة بالاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، المصدق عليها من الجزائر سنة 2014.

مع التأكيد على إمكانية مواجهة جرائم الوسط الرقمي؛ عبر العمل ببعض الإجراءات الحديثة غير الرقمية، المستحدثة من المشرع الجزائري مؤخرا، وذلك على الرغم من ورودها عامة، تخص الجريمة بشكل عام دون تخصيص. والتي تتمثل أساسا؛ في الأمر بمنع المشتبه فيه من مغادرة التراب الوطني، الذي يمارس أثناء مرحلة التحري، والأمر بوضع المتهم تحت المراقبة الالكترونية، الذي يختص به قاضي التحقيق؛ أثناء مباشرة إجراءات التحقيق القضائي الابتدائي.

إلا أن نتائج دراستنا هذه لا تقتصر على الجوانب الايجابية؛ بل توصلنا إلى العديد من السلبيات، التي تعتري النصوص القانونية –الجزائرية– عموما. حيث تبين لنا أن المشرع لا يعتمد على تسمية واحدة مستقرة لجرائم الوسط الرقمي، فتارة يسميها بالجريمة الالكترونية و/أو المعلوماتية، وتارة أخرى يسميها بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، كما يستعمل مصطلحات أخرى لها علاقة بالوسط الرقمي على غرار "السيبرانية" و"الرقمية والمرقمنة".

كما أن المشرع في المادة 02 –التعريفية– من القانون 09–04 المذكور سابقا؛ يذهب إلى اعتبار الجريمة المرتكبة عبر الهاتف التقليدي والفاكس والتيليكس...الخ؛ من جرائم الوسط الرقمي. الأمر الذي يعد مجانبا للصواب منطقا وقانونا، فالخصوصية كما بينا في بحثنا هذا؛ خلقها النطاق الافتراضي العامل بالرقمية الثنائية، والذي لا ينتج –النطاق الافتراضي–؛ إلا بالتفاعل مع جهاز الإعلام الآلي و/أو شبكة الاتصال الدولية –أو من في حكمهما– دونا سواهم. وأما الهاتف ومن في حكمه؛ فهي أجهزة تماثلية ظهرت منذ القدم، ولم تغير من الطابع التقليدي للجريمة.

ورجوعا إلى الأجهزة الممارسة للتحري والتحقيق في جرائم الوسط الرقمي؛ نجد أنه رغم اعتبارها كافية من ناحية التأسيس والوجود –كما بينا سابقا–؛ إلا أنها تعتبر متداخلة من حيث الاختصاصات والمهام. فللهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاتصال ومكافحتها مثلا؛ اختصاصات واسعة في المواجهة –خاصة من حيث الوقاية–، إلا أنها تتداخل في مهامها مع الشرطة القضائية الخاصة، على غرار مركز الوقاية من جرائم الإعلام والجرائم المعلوماتية ومكافحتها التابع للدرك الوطني.

وأما بخصوص الأعمال والأوامر والأذون الإجرائية؛ فنجد أن المشرع لم يحسن التعامل مع جرائم الوسط الرقمي بخصوص تفرقته بين الرقمية والمرقمنة. حيث في العديد من الإجراءات –كالتوقيف للنظر مثلا–؛ يعامل الجريمة الرقمية –جرائم المساس بأنظمة المعالجة الآلية للمعطيات– معاملة خاصة، دون نظيرتها المرقمنة –الجريمة التقليدية المتصلة بالوسط الرقمي–، وذلك رغم وحدت مسرح الجريمة الافتراضي بينها.

هذا بالإضافة إلى تعامل المشرع التمييزي بين التفتيش والمعاينة المرقمنين. حيث تطرق إلى التفتيش بأحكام حديثة في إطار المادة 05 من القانون 09-04 المذكور، التي تنظمه بقواعد خاصة تمنع الرجوع إلى أحكام قانون الإجراءات الجزائية إلا عند الحاجة أو الإحالة. في حين لم يعرج أبدا على المعاينة، رغم كونها من الأعمال الجوهرية –كما بينا سابقا–، ما يدفع للتعامل معها بالإجراءات التقليدية التي تعد غير مجدية في الكثير من الأحيان.

مع التأكيد على أن المشرع لم يتطرق أيضا؛ إلى أحد الأعمال المساعدة الضرورية في الكثير من الأحيان، عند ممارسة عملي التفتيش و المعاينة. وهو العمل المتمثل في تحديد هوية المشتبه فيه، سواءً عن طريق استعمال البروتوكول "TCP-IP" أو من دونه، وذلك رغم كونه الوسيلة الأساس المستعملة في هذا الصدد، من أغلب الأجهزة العالمية والمقارنة المختصة بمواجهة جرائم الوسط الرقمي.

وزيادةً على ما ذكر تعد من أبرز نتائج بحثنا هذا؛ أن القانون الجزائري فتح المجال لأجهزة التحري والتحقيق –الهيئة الوطنية خاصةً–، من أجل ممارسة التعاون الدولي لمواجهة جرائم الوسط الرقمي نظرا لعالمية هذه الجرائم. الأمر الذي رغم كونه مفيدا وربما الحل الوحيد في الكثير من الأحيان؛ إلا أن له العديد من السلبيات، سيما نظرا لمساس ذلك بسيادة الدولة الجزائرية.

أيضا تنطوي الأعمال الإجرائية الممارسة من طرف أجهزة التحري والتحقيق في جرائم الوسط الرقمي؛ على سلبية أخرى قد يكون لها الأثر البالغ على الحقوق والحريات. حيث مكنت المواد 03 و04 و05 من القانون 09-04 السابق الذكر؛ الهيئة الوطنية وحتى غيرها؛ من ممارسة مراقبة الاتصالات الالكترونية والتفتيش والحجز المرقمنين، لغرض الوقاية من بعض جرائم الوسط الرقمي وحتى غيرها من الجرائم التقليدية الخطيرة، وذلك لمجرد الشك أو نظرا لاحتمال الوقوع.

يتضح من خلال النتائج السابقة المقدمة، سيما ذات الأثر السلبي منها، أنه لموضوع إجراءات التحري والتحقيق في جرائم الوسط الرقمي؛ العديد من النقاط القانونية، واجبة المراجعة –مع التأكيد على ايجابية البعض منها–، حتى نصل إلى المواجهة الإجرائية المرجوة، التي نصبوا إليها. وعليه نوصي في إطار دراستنا الأكاديمية هذه؛ بضرورة التدخل التشريعي، من أجل التعامل مع النصوص سارية المفعول، وذلك عبر التعديل والتتميم المدروسين، بغرض تفادي السلبيات المذكورة سابقا وغيرها. الأمر الذي قد يكون إما عبر التدخل الفوري بالتعديل والإضافة، أو بالتدخل على حسب الحاجة بعد الترقب المستمر، كما قد يتوجب على المشرع أن يتخذ الموقف السلبي، من بعض التعديلات محل المناداة بها من قبل البعض.

فمن حيث التدخل الفوري للتعديل والإضافة؛ نجد أنه يتوجب على المشرع الجزائري التدخل الفوري، من أجل إيجاد تسمية موحدة لجرائم الوسط الرقمي، توحد النظرة القانونية والتحليلات الفقهية، سيما وأن ذلك يعد ممكنا وفق الطرح الذي قدمناه في المتن، من خلال تفضيل تسمية جرائم الوسط الرقمي، التي نحبذها للأسباب والتأسيس المذكورين.

كما ننادي بالتدخل الفوري للمشرع؛ حتى يضع نصوصا تقنن ما سميناها بالوقاية الرقمية. التي تعد من أنجع الحلول الفنية، لمواجهة جرائم الوسط الرقمي، عبر الوقاية منها قبل مكافحتها. سيما وأن المشرع أبان صراحةً عن نيته للعمل على الوقاية من جرائم الوسط الرقمي، من خلال استحداثه لإجراءات جزائية وقائية على غير المألوف، بالمادة 03 وما يليها من القانون 09–04 المذكور. مع التأكيد على إتباع الأساليب المذكورة في دراستنا، وكل أسلوب حديث يظهر مع تطور النطاق الافتراضي للوسط الرقمي.

بالإضافة إلى العمل على تحيين المادة 03 وما يليها من القانون 09–04 المذكورة، من خلال وضع ضمانات إجرائية، تكون كفيلة لأن تحمي الحقوق والحريات العامة، في صورة حرمة الحياة الخاصة، التي تنتهك عند ممارسة الدور الوقائي، لمجرد الشك أو الاحتمال. الأمر الذي نقترح فيه؛ أن تمارس هذه الإجراءات بمعرفة قاضٍ مختص، يكون مشبعا بثقافة حقوق الإنسان، على شاكلة قاضي الحريات في القانون الفرنسي، الذي لا يختص إلا؛ بالفصل في مسألة وضع المتهم رهن الحبس المؤقت من عدمه.

كما نوصي في إطار بحثنا هذا؛ بضرورة تدخل المشرع من أجل توحيد الإجراءات المعمول بها في مواجهة جرائم الوسط الرقمي، إلا ما تطلبته الضرورة الإجرائية والعملية. فمن غير المعقول أن تفتح مواعيد التفتيش في مواجهة جريمة الدخول عن طريق الغش –كجريمة رقمية–، وتترك مقيدة بالمواعيد التقليدية بخصوص جريمة القتل عن طريق الآلة –كجريمة مرقمنة–، رغم وحدة الوسط المستعمل لارتكاب الجريمة من جهة، وخطورة الجريمة المرقمنة عن الرقمية في هذه الحالة من جهة أخرى.

وزيادةً على ما ذكر؛ نوصي بضرورة التدخل الفوري من المشرع؛ بغرض إيجاد آلية حقيقية تسمح بالتشريع وفق إجراءات سريعة لا تأخذ الكثير من الوقت، من أجل مواكبة التطور الديناميكي السريع

للمسرح الجرمي الافتراضي. كأن يسمح لرئيس الجمهورية أن يشرع بالأوامر، في مواجهة جرائم الوسط الرقمي ذات الخصوصية المعقدة فائقة السرعة من حيث التطور. أو أن ينظر لها بمنظور الجرائم الاقتصادية، التي للتنظيم فيها دور كبير بالموازاة مع التشريع.

وأما في إطار المواجهة الخاصة؛ فنتطرق إلى "الويب المظلم–Dark Web" على وجه الخصوص. حيث نوصي بضرورة وضع خطة خاصة متكاملة، تسمح بمواجهته بالخصوصية التي تتناسب مع طبيعته الاستثنائية. حيث نؤكد على ضرورة العمل الوقائي عبر إتباع النهج الإماراتي، الذي ذهب بالمادة 09 من قانون مكافحة جرائم تقنية المعلومات لسنة 2012 المعدل والمتمم –المذكور–، إلى تجريم استعمال العناوين الشبكية الوهمية، من منطلق أنها قرينة على الإجرام. إلا أننا نوصي على إضافة شرط الترخيص المسبق، حتى لا نحرم من يريد المحافظة على خصوصيته المشروعة من ذلك. فنقول بضرورة التدخل التشريعي؛ لتجريم النطاقات الشبكية المشفرة والوهمية، المستعملة من دون ترخيص مسبق.

كما أننا نتجه في هذا الإطار إلى القول؛ بضرورة العمل بنظام البرامج الرقمية الوقائية، كبرنامج "Memex"، الذي طورته وزارة الدفاع الأمريكية سنة 2014، من أجل أن يمسح آليا كل إعلان يتعلق بالاتجار بالأشخاص على مواقع "الويب المظلم–Dark Web" وغيره، حتى لا يتمكن ناشره من استغلال الأشخاص، سيما الأطفال. على أن يكون البرنامج المستعمل، من تطوير كفاءات جزائرية تحفظ السرية وسيادة الدولة. وفي الوقت نفسه؛ نوصي بإمكانية العمل بنظام التسرب من قبل أجهزة التحري والتحقيق، لمكافحة جرائم هذا النطاق الشبكي الخاص، وفق الطرح المبين في متن الدراسة.

وفي النحو نفسه المتصل بضرورة التدخل الفوري للمشرع؛ نوصي بالتدخل من أجل إما بإنشاء مركز علمي مستقل يختص بدراسة الإجرام في الوسط الرقمي موضوعيا وإجرائيا، أو بتفعيل دور الهيئة الوطنية، من خلال نصوص جديدة تجعلها بمثابة القطب العلمي أيضا في هذا المجال. ومنها نتطرق إلى التدخل على حسب الحاجة بعد الترقب المستمر، من خلال ترقب المركز أو الهيئة للتطورات المستمرة في الوسط الرقمي، وإخطار الهيئة التشريعية من أجل وضع الإجراءات المناسبة في الوقت المناسب.

كما أننا نؤكد على ضرورة تفادي المشرع؛ لفكرة القانون الخاص بمكافحة جرائم الوسط الرقمي، الذي يضم الشقين الموضوعي والإجرائي معاً، وفق ما ينادي به البعض. وهذا لأننا نرى بأن جمع جرائم الوسط الرقمي في قانون خاص مستقل، ما هو إلا تكرار لنصوص قانون العقوبات، الذي يضم أصلا جرائم الوسط الرقمي بقسميها، الرقمية والمرقمنة. مع القول بالإبقاء على القانون 09–04، بعد تعديله إلى جانب قانون الإجراءات الجزائية؛ لتفادي النقائص الإجرائية المذكورة.

هذا هو كلام الختام، الذي نقول فيه بعد تقديم أهم النتائج والتوصيات القانونية؛ أننا حاولنا والكمال لله، أننا ابتغينا؛ أن نفيد ونستفيد. فان أصبنا فمن عند الله، وان أخطئنا فمن عند أنفسنا.

قائـــــمـــــــــة
المـراجـــــع

أولا: المـــــــــراجع باللغـــــــة العربيـــــــــــة

1. الكتـــــــــــــــب:

أ- الكتب العامة:

أ-1/ أبو عامر محمد زكي، الإجراءات الجنائية، منشأة المعارف، الإسكندرية، مصر، د س ن.

أ-2/ أحسن بوسقيعة، الوجيز في القانون الجزائي العام، الطبعة الثانية عشر، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2013.

أ-3/ .....، الوجيز في القانون الجزائي الخاص، الطبعة الخامسة، الجزء الأول، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2013.

أ-4/ .....، التحقيق القضائي، الطبعة العاشرة، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2013.

أ-5/ جمال سايس، الاجتهاد الجزائري في مادة الجنح والمخالفات، منشورات كليك، الجزء الأول، الجزائر، 2014.

أ-6/ .....، الاجتهاد الجزائري في مادة الجنح والمخالفات، منشورات كليك، الجزء الثاني، الجزائر، 2014.

أ-7/ .....، الاجتهاد الجزائري في مادة الجنح والمخالفات، منشورات كليك، الجزء الرابع، الجزائر، 2014.

أ-8/ جمال نجيمي، قانون الإجراءات الجزائية الجزائري على ضوء الاجتهاد القضائي، الطبعة الأولى، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2015.

أ-9/ حسين طاهري، الوجيز في شرح قانون الإجراءات الجزائية، الطبعة الثالثة، دار الخلدونية للنشر والتوزيع، الجزائر، 2005.

أ-10/ مجمع اللغة العربية، المعجم الوسيط، الطبعة الرابعة، مكتبة الشرق الدولية، القاهرة، مصر، 2004.

أ-**11**/ محمد حزيط، مذكرات في قانون الإجراءات الجزائية الجزائري، الطبعة السادسة، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2011.

أ-**12**/ محمد مروان، نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري، ديوان المطبوعات الجامعية، الجزائر، 1999.

أ-**13**/ محمد سويلم، الإدارة في القرن الحادي والعشرين، دون دار نشر، القاهرة، مصر، 1997.

أ-**14**/ محمود نجيب حسني، شرح قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، مصر، 1988.

أ-**15**/ .....، شرح قانون العقوبات-القسم الخاص، دار النهضة العربية، القاهرة، مصر، 1992.

أ-**16**/ منصور رحماني، الوجيز في القانون الجنائي العام، دار العلوم للطباعة والنشر والتوزيع، الجزائر، 2006.

أ-**17**/ عاشور محمد أنور، الموسوعة في التحقيق الجنائي العلمي، الطبعة الثانية، عالم الكتب، القاهرة، مصر، د س ن.

أ-**18**/ عبد الله أوهايبية، شرح قانون العقوبات الجزائري، المؤسسة الوطنية للفنون المطبعية، الجزائر، 2011.

أ-**19**/ .....، شرح قانون الإجراءات الجزائية الجزائري، الطبعة الرابعة، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2013.

أ-**20**/ عبد الرزاق السنهوري، الوسيط في شرح القانون المدني-نظرية الالتزام بوجه عام-الإثبات وآثار الالتزام، الجزء الثاني، دار النهضة العربية، القاهرة، مصر، 1968.

أ-**21**/ فضيل العيش، شرح قانون الإجراءات الجزائية بين النظري والتطبيقي، مطبعة البدر، الجزائر، د س ن.

أ-**22**/ شريف أحمد الطباخ، البحث الجنائي والأدلة الجنائية في ضوء القضاء والفقه، دار الفكر الجامعي، الإسكندرية، مصر، 2017.

ب- الكتب المتخصصة:

ب-1/ أحمد إبراهيم مصطفى سليمان، الإرهاب والجريمة المنظمة، دار الطلائع للنشر والتوزيع، القاهرة، مصر، 2006.

ب-2/ أيمن عبد الحفيظ، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، الطبعة الأولى، دار النهضة العربية للنشر والتوزيع، القاهرة، مصر، 2005.

ب-3/ أيمن عبد الله فكري، جرائم نظم المعلومات، دراسة مقارنة، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، 2007.

ب-4/ أمير فرج يوسف، الجرائم المعلوماتية على شبكة الإنترنت، دار المطبوعات الجامعية للنشر، الإسكندرية، مصر، 2008.

ب-5/ .....، الإثبات الجنائي للجريمة الالكترونية والاختصاص القضائي لها، مكتبة الوفاء القانونية، الإسكندرية، مصر، 2016.

ب-6/ أروى يحيى عبد الرحمن الإرياني، أساسيات تحليل وتصميم نظم المعلومات، شعاع للنشر والتوزيع، حلب، سوريا، 2008.

ب-7/ جبريل بن حسن العريشي ومحمد حسن الشلهوب، أمن المعلومات، الطبعة الأولى، دار المنهجية للنشر والتوزيع، عمان، الأردن، 2016.

ب-8/ جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيات الحديثة، الطبعة الثانية، دار النهضة العربية، القاهرة، مصر، 2012.

ب-9/ هلالي عبد الله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية-دراسة مقارنة، الطبعة الثانية، دار النهضة العربية، القاهرة، مصر، 2008.

ب-10/ حازم محمد حنفي، الدليل الالكتروني ودوره في المجال الجنائي، دار النهضة العربية، القاهرة، مصر، 2017.

ب-11/ حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت-دراسة مقارنة، دار النهضة العربية، القاهرة، مصر، 2009.

ب-12/ حسن طاهر داود، جرائم نظم المعلومات، مطابع أكاديمية نايف العربية للعلوم الأمنية، الرياض، السعودية، 2000.

ب-13/ يوسف حسن يوسف، الجرائم الدولية للإنترنت، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، مصر، 2011.

ب-14/ لحسن ناني، التحقيق في الجرائم المتصلة بتكنولوجية المعلوماتية، الطبعة الأولى، دار النشر الجامعي الجديد، الجزائر، 2017.

ب-15/ محمد الأمين البشري، التحقيق في الجرائم المستحدثة، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، 2004.

ب-16/ محمد أمين الشوابكة، جرائم الحاسوب والإنترنات-الجريمة المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2009.

ب-17/ محمد حماد مرهج الهيتي، جرائم الحاسوب، الطبعة الأولى، دار المناهج للنشر والتوزيع، عمان، الأردن، 2006.

ب-18/ محمد طارق عبد الرؤوف الخن، جريمة الاحتيال عبر الإنترنت، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2011.

ب-19/ محمد كمال شاهين، الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي-دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، مصر، 2018.

ب-20/ محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت دراسة مقارنة، دار النهضة العربية للنشر، القاهرة، مصر، 2005.

ب-21/ محمود أمحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2005.

ب-22/ محمود محمد محمود جابر، الأحكام الإجرائية للجرائم الناشئة عن استخدام الهواتف النقالة، الكتاب الثاني، دار الكتب والوثائق القومية، القاهرة، مصر، 2018.

ب-23/ محمود عبد الحميد عبد المطلب، البحث والتحقيق الجنائي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة، مصر، 2007.

ب-24/ منال هلال المزاهرة، تكنولوجيات الاتصال والمعلومات، الطبعة الأولى، دار المسيرة للطباعة والنشر والتوزيع، عمان، الأردن، 2014.

ب-25/ منير محمد الجنبيهى وممدوح محمد الجنبيهى، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتهما، دار الفكر الجامعي للطباعة والنشر، الإسكندرية، مصر، 2006.

ب-26/ مصطفى علي خلف، الضوابط الإجرائية لجرائم التقنية الحديثة-دراسة مقارنة، نادي القضاة، القاهرة، مصر، 2016.

ب-27/ م.ش.بلعيد، مدخل إلى هندسة الكمبيوتر، دار الصفحات الزرقاء العالمية، الجزائر، د س ن.

ب-28/ نجاة بن مكي، السياسة الجنائية لمكافحة جرائم المعلوماتية، دار الخلدونية للنشر والتوزيع، الجزائر، 2017.

ب-29/ نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2010.

ب-30/ سامي جلال فقي حسين، الأدلة المتحصلة من الحاسب الآلي وحجيتها في الإثبات الجنائي، دار الكتب القانونية، القاهرة، مصر، 2011.

ب-31/ عبد الله بن عبد العزيز الموسى، مقدمة في الحاسب الآلي والإنترنت، الطبعة السادسة، مؤسسة شبكة البيانات، المملكة العربية السعودية، 2010.

ب-32/ عبد الله سيف الكيتوب، الأحكام الإجرائية لجريمة الاحتيال المعلوماتي، دار النهضة العربية، القاهرة، مصر، 2013.

ب-33/ عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والإنترنت، منشورات الحلبي الحقوقية، بيروت، لبنان، 2007.

ب-34/ عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة، مصر2006.

ب-35/ .....، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت-دراسة متعمقة في جرائم الحاسب الآلي والإنترنت، بهجات للطباعة والتجليد، القاهرة، مصر، 2009.

ب-**36/** علي حسن الطوالبة، التفتيش الجنائي على نظم الحاسوب والإنترنت-دراسة مقارنة، عالم الكتب الحديث، اربط، الأردن، 2004.

ب-37/ علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المكتب الجامعي الحديث، الإسكندرية، مصر، 2012.

ب-38/ عماد الدين وادي وحنان أوشن، الإثبات الجنائي والوسائل العلمية الحديثة، دار الخلدونية للنشر والتوزيع، الجزائر، 2015.

ب-39/ عمرو عيسى القي، الجرائم المعلوماتية-جرائم الحاسب الآلي والإنترنت في مصر والدول العربية، المكتب الجامعي الحديث، الإسكندرية، مصر، 2006.

ب-**40/** عمر محمود أبو بكر يونس، الجرائم الناشئة عن استخدام الإنترت-الأحكام الموضوعية والجوانب الإجرائية، دار النهضة العربية، القاهرة، مصر، 2004.

ب-41/ عمر محمد بن يونس، الاتفاقية الأوروبية حول الجريمة الافتراضية – المذكرة التفسيرية، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، 2005.

ب-**42/** ضياء علي أحمد النعمان، الغش المعلوماتي-الظاهرة والتطبيقات، المطبعة الوطنية، الرباط، المملكة المغربية، 2011.

2. المقالات العلميـــــة:

أ- إبراهيم بختي، "الإنترنت في الجزائر"، مجلة الباحث، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة ورقلة، الجزائر، عدد 01، 2002، ص ص 26-35.

ب- إيهاب عبد الرحيم علي، "أمن المعلومات الصحية"، مجلة التقدم العلمـــي، مؤسســـة الكويـــت للتقـــدم العلمي، الكويت، عدد 99، أكتوبر 2017، ص ص 20-26.

ج- إمام حسنين خليل، "التعاون القضائي الدولي لمواجهة الجريمة المنظمة-دراسة مقارنة"، مجلة رؤى إستراتيجية، مركز الإمارات للدراسات والبحوث الإستراتيجية، أبو ظبي، الإمارات العربية المتحدة، عدد 09، جانفي 2015، ص ص 08-41.

د- أسامة بن غانم العبيدي، "التفتيش عن الدليل في الجرائم المعلوماتية"، المجلة العربية للدراسات الأمنية والتدريب، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، مج 29، عدد 58، نوفمبر-ديسمبر 2013، ص ص 85-132.

ه- مروة أديب محمد الجوهري، "الحاسوب والإعجاز العددي في القران الكريم"، مجلة كلية العلوم الإسلامية، جامعة الموصل، العراق، مج 08، عدد 1/15، 2014، ص ص 295-346.

و- محروس نصار غايب، "الجريمة المعلوماتية"، مجلة التقني، هيئة التعليم التقني، العراق، مجلد 24، عدد 09، 2011، ص ص 100-123.

ز- ساهر إبراهيم الوليد، "مراقبة المتهم الكترونيا كوسيلة للحد من مساوئ الحبس الاحتياطي-دراسة تحليلية"، مجلة الجامعة الإسلامية للدراسات الإسلامية، كلية الحقوق، جامعة غزة، فلسطين، مج 21، عدد 01، 2013، ص ص 661-695.

ح- سليم مزيود، "الجرائم المعلوماتية واقعها في الجزائر وآليات مكافحتها"، المجلة الجزائرية للاقتصاد والمالية، مخبر الاقتصاد الكلي والمالية الدولية، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة يحي فارس بالمدية، الجزائر، عدد 01، أفريل 2014، ص ص 94-107.

ط- عادل يوسف عبد النبي الشكري، "الجريمة المعلوماتية وأزمة الشرعية الجزائية"، مجلة مركز دراسات الكوفة، جامعة الكوفة، العراق، مج 01، عدد 07، 2008، ص ص 111-132.

ي- فاطمة زهرة بوعناد، "مكافحة الجريمة الالكترونية في التشريع الجزائري"، مجلة النـــدوة للدراســـات القانونية، قسنطينة، الجزائر، عدد 01، 2013، ص ص 63-74.

ك- فهد يوسف الكساسبة، "دور النظم العقابية الحديثة في الإصلاح والتأهيل-دراسة مقارنة"، مجلة دراسات علوم الشريعة والقانون، كلية الحقوق، الجامعة الأردنيـــة، الأردن، مـــج 39، عـــدد 02، 2012، ص ص 387-402.

ل- صفاء أوتاني، "الوضع تحت الرقابة الالكترونية-السوار الالكتروني-في السياسة العقابيـــة الفرنســـية"، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، مج 25، عدد 01، كلية الحقوق، جامعة دمشق، ســـوريا، 2009، ص ص 129-162.

3. أعمال المؤتمرات والملتقيات العلمية:

أ- أبو المعالي محمد عيسى، "الحاجة إلى تحديث آليات التعاون الدولي في مجال مكافحة الجريمة المعلوماتية"، ورقة عمل مقدمة إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، ليبيا، 28 أكتوبر 2009.

ب- أحمد بن عبد الرحمن البعادي، "دعاوى الجرائم الالكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول"، ورقة عمل مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا بالدول العربية، الخرطوم، السودان، 23-25 سبتمبر 2012.

ج- أمقران طيبي، "المنع من السفر بين الإطلاق والتقييد"، ورقة عمل مقدمة وفق متطلبات المشاركة في الملتقى الوطني الثالث بعنوان تطورات النظم الإجرائية الجزائية في ضوء التعديلات الإجرائية الأخيرة والتعديل الدستوري لسنة 2016، كلية الحقوق والعلوم السياسية، جامعة أكلي محند أولحاج، البويرة، الجزائر، 23 و24 ماي 2017.

د- إيهاب ماهر السنباطي، "الجرائم الالكترونية(الجرائم السيبيرية): قضية جديدة أم فئة مختلفة؟ التناغم القانوني هو السبيل الوحيد!"، ورقة عمل مقدمة إلى الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية، 19 و20 جوان 2007.

ه- وردة شرف الدين، "المساعدة القضائية الدولية في مجال مكافحة جرائم الاتجار بالأشخاص والمرتكبة بواسطة تقنية المعلومات-وفقاً للاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، ورقة عمل مقدمة إلى المؤتمر الدولي الثاني حول جريمة الاتجار بالبشر-الأشكال الجديدة والتحديات الراهنة، مخبر الدولة والإجرام المنظم، كلية الحقوق والعلوم السياسية، جامعة البويرة، الجزائر، 16 و17 أفريل 2018.

و- يونس عرب، "جرائم الكمبيوتر والانترنت"، ورقة عمل مقدمة إلى مؤتمر الأمن العربي، أبو ظبـــي، الإمارات العربية المتحدة، 10-12 فيفري 2002.

ز- يونس عرب، "صور الجرائم الإلكترونية واتجاهات تبويبها"، ورقة عمل مقدمة إلى ورشة عمـــــل تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية، مسقط، سلطنة عمان، 02-04 أفريل 2006.

ح- كريم صياد، "فعالية نظام المراقبة الالكترونية في تنفيذ عقوبة الحبس المؤقت"، مداخلة مقدمة في إطار الملتقى الوطني الثالث الموسوم بتطورات النظم الإجرائية الجزائرية في ضوء التعديلات الإجرائية الأخيرة والتعديل الدستوري لسنة 2016، كلية الحقوق والعلوم السياسية، جامعة البويرة، الجزائر، 23 و24 ماي 2017.

ط- محمد طارق الخن، "جرائم المعلوماتية (الأحكام الموضوعية و الإجرائية)"، ورقة عمل مقدمة إلى ورشة عمل حول التشريعات الالكترونية السيبرانية وآلية تطبيقها، دمشق، سوريا، فيفري 2015.

ي- منى الأشقر جبور، "الأمن السيبراني: التحديات ومستلزمات المواجهة"، ورقة عمل مقدمة إلى اللقاء السنوي الأول للمتخصصين في أمن وسلامة الفضاء السيبراتني، المركز العربي للبحوث القانونية والعربية، جامعة الدول العربية، بيروت، لبنان، 27 و28 أوت 2012.

ك- مفتاح بوبكر المطردي، "الجريمة الالكترونية والتغلب على تحدياتها"، ورقة عمل مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية، الخرطوم، السودان، 23-25 سبتمبر 2012.

ل- علي زغيب، "أفضل الممارسات الأمنية لمزودي خدمات الإنترنت"، أعمال مؤتمر الأمن السيبراني والدفاع السيبراني، الجامعة اللبنانية والوكالة الجامعية للفرنكوفونية AUF، لبنان، د ت.

م- عمر عبد العزيز موسى الدبور، "آليات تفعيل الحماية والوقاية من الجرائم الالكترونية"، أعمال المؤتمر الدولي الرابع عشر حول الجرائم الالكترونية، طرابلس، لبنان، 24 و25 مارس 2017.

ن- فضيلة عاقلي، "الجريمة الالكترونية وإجراءات مواجهتها من خلال التشريع الجزائري"، أعمال المؤتمر الدولي الرابع عشر حول الجرائم الالكترونية، طرابلس، لبنان، 24 و25 مارس 2017.

س- صادق ضريفي، "المراقبة الجنائية الالكترونية كآلية بديلة للحبس الاحتياطي"، ورقة عمل مقدمة في إطار الملتقى الوطني الثالث الموسوم بتطورات النظم الإجرائية الجزائرية في ضوء التعديلات الإجرائية الأخيرة والتعديل الدستوري لسنة 2016، كلية الحقوق والعلوم السياسية، جامعة أكلي محند أولحاج، البويرة، الجزائر، 23 و24 ماي 2017.

ع- رحيمة ندميلي، "خصوصية الجريمة الالكترونية في القانون الجزائري والقوانين المقارنة"، أعمال المؤتمر الدولي الرابع عشر حول الجرائم الالكترونية، طرابلس، لبنان، 24 و25 مارس 2017.

ف- ذياب موسى البداينية، "الجرائم الإلكترونية: المفهوم والأسباب"، ورقة عمل مقدمة إلى الملتقى العلمي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، عمان، المملكة الأردنية الهاشمية، 02-04 سبتمبر 2014.

4. الأطروحات والرسائل والمذكرات العلمية:

أ- أطروحات الدكتوراه:

أ-1/ جمال براهيمي، (التحقيق الجنائي في الجرائم الالكترونية)، أطروحة لنيل درجة دكتوراه علوم، تخصص القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، الجزائر، 2018.

أ-2/ وردة شرف الدين، (الإثبات الجنائي بالأدلة الالكترونية-دراسة مقارنة)، أطروحة لنيل درجة الدكتوراه في الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر، 2017.

أ-3/ حسين ربيعي، (آليات البحث والتحقيق في الجرائم المعلوماتية)، أطروحة لنيل شهادة دكتوراه علوم في قانون العقوبات والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة 1، الجزائر، 2016.

أ-4/ كريمة خطاب، (قرينة البراءة)، أطروحة لنيل شهادة دكتوراه علوم فرع قانون، كلية الحقوق، جامعة الجزائر 1، الجزائر، 2015.

أ-5/ مليكة بهلول، (دور الشرطة العلمية والتقنية في الكشف عن الجريمة)، رسالة لنيل شهادة الدكتوراه، طلية الحقوق، جامعة الجزائر 1، الجزائر، 2013.

أ-6/ مليكة عطوي، (الحماية القانونية لحقوق الملكية الفكرية على شبكة الإنترنت)، أطروحة لنيل درجة الدكتوراه في علوم الإعلام والاتصال، كلية العلوم والاتصال، كلية العلوم السياسية والإعلام، جامعة دالي إبراهيم، الجزائر، 2010.

أ-7/ ناصر إبراهيم محمد زكي، (سلطة القاضي الجنائي في تقدير الأدلة-دراسة مقارنة)، رسالة دكتوراه، كلية الشريعة والقانون، جامعة الأزهر، القاهرة، مصر، 1987.

أ-8/ نشادي عبد الرحمان، (الجرائم المعلوماتية ووسائل الاتصال الحديثة)، أطروحة لنيل شهادة الدكتوراه في علوم الإعلام والاتصال، كلية علوم الإعلام والاتصال، جامعة الجزائر 3، الجزائر، 2017.

أ-9/ سالم محمد سليمان الأوجلي، (أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوطنية -دراسة مقارنة)، رسالة لنيل شهادة الدكتوراه، كلية الحقوق، جامعة عين شمس، القاهرة، مصر، 1997.

أ-**10**/ غازي عبد الرحمن هيان الرشيد، (الحماية القانونية من جرائم المعلوماتية-الحاسب والإنترنت)، أطروحة لنيل درجة الدكتوراه في القانون، كلية الحقوق، الجامعة الإسلامية، لبنان، 2004.

ب- رسائل ومذكرات الماجستير:

ب-1/ أسامة محمد أحمد سليمان، (ضمانات المتهم في مرحلتي الاستدلال والتحقيق الابتدائي)، رسالة لنيل درجة الماجستير في القانون، كلية الدراسات العليا، الجامعة الأردنية، المملكة الأردنية الهاشمية، 1997.

ب-2/ بهاء فهمي الكبجي، (مدى توافق أحكام جرائم أنظمة المعلومات في القانون الأردني مع الأحكام العامة للجريمة)، رسالة لنيل درجة الماجستير في القانون العام، كلية الحقوق، جامعة الشرق الأوسط، الأردن، 2013.

ب-3/ حاسين فنور، (المنظمة الدولية للشرطة الجنائية والجريمة المنظمة)، مذكرة لنيل شهادة الماجستير في القانون الدولي والعلاقات الدولية، كلية الحقوق، جامعة الجزائر 1، الجزائر، 2013.

ب-4/ يوسف صغير، (الجريمة المرتكبة عبر الإنترنت)، مذكرة لنيل شهادة الماجستير في القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 2013.

ب-5/ يحي محمود عيشان، (الصعوبات التي تواجه التنسيق والتعاون الدولي في مكافحة جرائم الحاسب الآلي والإنترنت-دراسة مقارنة)، رسالة لنيل درجة الماجستير في القانون العام، كلية الدراسات القانونية العليا، جامعة عمان العربية للدراسات العليا، عمان، الأردن، 2008.

ب-6/ مليكة عطوي، (الإنترنت والملكية الفكرية)، مذكرة لنيل شهادة الماجستير في علوم الإعلام والاتصال، كلية العلوم والاتصال، جامعة الجزائر 3، الجزائر، 2004.

ب-7/ مروان بن مرزوق الروقي، (القصد الجنائي في الجرائم المعلوماتية-دراسة تأصيلية مقارنة)، رسالة لنيل درجة الماجستير في العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، 2011.

ب-8/ نسيم دردور، (جرائم المعلوماتية على ضوء القانون الجزائري والمقارن)، مذكرة لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة منتوري، قسنطينة، الجزائر، 2013.

ب-9/ نعيم سعيداني، (آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري)، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية تخصص علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، الجزائر 2013.

ب–**10**/ سهيل الخييلي، (مدى إلزامية التعاون القضائي الدولي في المجال الجنائي–دراسة مقارنة)، رسالة لنيل شهادة الماجستير في القانون العام، كلية الدراسات القانونية العليا، جامعة عمان العربية للدراسات العليا، الأردن، 2006.

ب–11/ عبد اللطيف معتوق، (الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن)، مذكرة مكملة لنيل شهادة الماجستير في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، الجزائر، 2012.

ب–12/ عبد الله بن عبد العزيز بن عبد الله الخثعمي، (التفتيش في الجرائم المعلوماتية في النظام السعودي–دراسة تطبيقية)، رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير في العدالة الجنائية، كلية الدراسات العليا، قسم العدالة الجنائية، تخصص السياسة الجنائية، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، 2011.

ب–13/ عبد الفتاح ولد باباه، (الركن المعنوي في الجرائم المعلوماتية في النظام السعـــودي–دراسة تأصيلية)، رسالة لنيل درجة الماجستير في العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، 2013.

ب–14/ فافة لحمر، (إجراءات تسليم المجرمين في التشريع الجزائري على ضوء الاتفاقيات الدولية)، مذكرة لنيل شهادة الماجستير في القانون، كلية الحقوق والعلوم السياسية، جامعة وهران، الجزائر، 2014.

ب–15/ فتيحة رصاع، (الحماية الجنائية للمعلومات على شبكة الإنترنت)، مذكرة لنيل شهادة ماجستير في القانون العام، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، الجزائر، 2012.

5. النصوص القانونية:

أ– النصوص القانونية الدولية:

أ–**1**/ النظام الأساسي لمجلس وزراء الداخلية العرب، معتمد في الدورة العادية الثامنة والسبعون لمجلس جامعة الدول العربية، القاهرة، مصر، 23 سبتمبر 1982.

أ–**2**/ اتفاقية الأمم المتحدة لمكافحة الاتجار غير المشروع بالمخدرات والمؤثرات العقلية، الموافق عليها في فيينا بتاريخ 20 ديسمبر 1988، والمصدق عليها بتحفظ بموجب، مرسوم رئاسي رقم 95–41، مؤرخ في 28 جانفي 1995، (ج ر) عدد 07، صادر بتاريخ 15 فيفري 1995.

أ-**3**/ اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، المعتمدة من قبل الجمعية العامة للأمم المتحدة بنيويورك يوم 31 أكتوبر 2003، والمصدق عليها بتحفظ بموجب، مرسوم رئاسي رقم 02-55، مؤرخ في 05 فيفري 2002،(ج ر)، عدد 09، صادر بتاريخ 10 فيفري 2002.

أ-**4**/ اتفاقية الأمم المتحدة لمكافحة الفساد، المعتمدة من قبل الجمعية العامة للأمم المتحدة بنيويورك يوم 31 أكتوبر 2003، والمصدق عليها بتحفظ بموجب، مرسوم رئاسي رقم 04-128، مؤرخ في 19 أفريل 2004، (ج ر) عدد 26، صادر بتاريخ 25 أفريل 2004.

أ-**5**/ المعاهدة المتعلقة بالتعاون القضائي في المجال الجزائي بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وحكومة الولايات المتحدة الأمريكية، الموقعة بالجزائر بتاريخ 07 أفريل 2010، والمصدق عليها بموجب، مرسوم رئاسي رقم 11-184، مؤرخ في 03 ماي 2011،(ج ر) عدد 30، صادر بتاريخ 01 جوان 2011.

أ-**6**/ الاتفاقية العربية لمكافحة الفساد، المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، والمصدق عليها بموجب، مرسوم رئاسي رقم 14-249، مؤرخ في 08 سبتمبر 2014،(ج ر) عدد 54، صادر بتاريخ 21 سبتمبر 2014.

أ-**7**/ الاتفاقية العربية لمكافحة غسل الأموال وتمويل الإرهاب، المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، والمصدق عليها بموجب، مرسوم رئاسي رقم 14-250، مؤرخ في 08 سبتمبر 2014، (ج ر) عدد 55، صادر بتاريخ 23 سبتمبر 2014.

أ-**8**/ الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية، المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، والمصدق عليها بموجب، مرسوم رئاسي رقم 14-251، مؤرخ في 08 سبتمبر 2014،(ج ر) عدد 56، صادر بتاريخ 25 سبتمبر 2014.

أ-**9**/ الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21 ديسبر 2010، والمصدق عليها بموجب، مرسوم رئاسي رقم 14-252، مؤرخ في 08 سبتمبر 2014،(ج ر) عدد 57، صادر بتاريخ 28 سبتمبر 2014.

أ-**10**/ اتفاقية التعاون القانوني والقضائي في المجال الجزائي بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وحكومة دولة الكويت، الموقعة بالجزائر بتاريخ 12 أكتوبر 2010، والمصدق عليها بموجب، مرسوم رئاسي رقم 15-255، مؤرخ في 05 أكتوبر 2015،(ج ر) عدد 53، صادر بتاريخ 08 أكتوبر 2015.

أ-**11**/ النظام الأساسي لآلية الاتحاد الإفريقي للتعاون الشرطي "أفريبول"، معتمد في الدورة العادية الثامنة والعشرون لمؤتمر الاتحاد الإفريقي، أديس أبابا، إثيوبيا، 30 جانفي 2017.

أ-**12**/ الاتفاقية المتعلقة بالتعاون القضائي في المجال الجزائي بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وحكومة الجمهورية الفرنسية، الموقعة بباريس بتاريخ 05 أكتوبر 2016، والمصدق عليها بموجب، مرسوم رئاسي رقم 18-73، مؤرخ في 25 فيفري 2018،(ج ر) عدد 13، صادر بتاريخ 28 فيفري 2018.

ب- النصوص القانونية الوطنية:

ب-1/ النص الدستوري:

- مرسوم رئاسي رقم 96-438، مؤرخ في 07 ديسمبر 1996، يتعلق بإصدار نص تعديل الدستور الجزائري، (ج ر) عدد 76، صادر بتاريخ 08 ديسمبر 1996. معدل ومتمم سيما بقانون رقم 16-01، مؤرخ في 06 مارس 2016، (ج ر) عدد 14، صادر بتاريخ 07 مارس 2016.

ب-2/ النصوص التشريعية:

ب-2-1/ أمر رقم 66-155، مؤرخ في 08 جوان 1966، يتضمن قانون الإجراءات الجزائية، (ج ر) عدد 49، صادر بتاريخ 11 جوان 1966، معدل ومتمم.

ب-2-2/ أمر رقم 66-156، مؤرخ في 08 جوان 1966، يتضمن قانون العقوبات، (ج ر) عدد 49، صادر بتاريخ 11 جوان 1966، معدل ومتمم.

ب-2-3/ أمر رقم 68-10، مؤرخ في 23 جانفي 1968، يعدل ويتمم أمر رقم 66-155، يتضمن قانون الإجراءات الجزائية، (ج ر) عدد 09، صادر بتاريخ 30 جانفي 1968.

ب-2-4/ أمر رقم 71-28، مؤرخ في 22 أفريل 1971، يتضمن قانون القضاء العسكري، (ج ر) عدد 38، صادر بتاريخ 11 ماي 1971، معدل ومتمم.

ب-2-5/ أمر رقم 75-58، مؤرخ في 26 سبتمبر 1975، يتضمن القانون المدني، (ج ر) عدد 78، صادر بتاريخ 30 سبتمبر 1975، معدل ومتمم.

ب-2-6/ قانون رقم 82-03، مؤرخ في 13 فيفري 1982، يعدل ويتمم أمر رقم 66-155، يتضمن قانون الإجراءات الجزائية، (ج ر) عدد 07، صادر بتاريخ 16 فيفري 1982.

ب-2-7/ قانون رقم 85-02، مؤرخ في 26 جانفي 1985، يعدل ويتمم أمر رقم 66-155، يتضمن قانون الإجراءات الجزائية، (ج ر) عدد 05، صادر بتاريخ 27 جانفي 1985.

ب-2-8/ قانون رقم 86-08، مؤرخ في 04 مارس 1986، يعدل ويتمم أمر رقم 66-155، يتضمن قانون الإجراءات الجزائية، (ج ر) عدد 10، صادر بتاريخ 05 مارس 1986.

ب-2-9/ قانون رقم 90-24، مؤرخ في 18 أوت 1990، يعدل ويتمم أمر رقم 66-155، يتضمن قانون الإجراءات الجزائية، (ج ر) عدد 36، صادر بتاريخ 22 أوت 1990.

ب-2-10/ أمر رقم 95-10، مؤرخ في 25 فيفري 1995، يعدل ويتمم أمر رقم 66-155، يتضمن قانون الإجراءات الجزائية، (ج ر) عدد 17، صادر بتاريخ 29 مارس 1995(استدراك).

ب-2-11/ قانون رقم 2000-03، مؤرخ في 05 أوت 2000، يتضمن القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، (ج ر) عدد 48، صادر بتاريخ 06 أوت 2000. (ملغى)

ب-2-12/ قانون رقم 01-09، مؤرخ في 26 جوان 2001، يعدل ويتمم أمر رقم 66-156، يتضمن قانون العقوبات، (ج ر) عدد 34، صادر بتاريخ 27 جوان 2001.

ب-2-13/ أمر رقم 03-03، مؤرخ في 19 جويلية 2003، يتعلق بالمنافسة، (ج ر)، عدد 43، صادر بتاريخ 20 جويلية 2003، معدل ومتمم.

ب-2-14/ قانون رقم 04-14، مؤرخ في 10 نوفمبر 2004، يعدل ويتمم أمر رقم 66-155، يتضمن قانون الإجراءات الجزائية، (ج ر)، عدد 71، صادر بتاريخ 10 نوفمبر 2004.

ب-2-15/ قانون رقم 04-15، مؤرخ في 10 نوفمبر 2004، يعدل ويتمم أمر رقم 66-156، يتضمن قانون العقوبات، (ج ر) عدد 71، صادر بتاريخ 10 نوفمبر 2004.

ب-2-16/ قانون رقم 09-04، مؤرخ في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، (ج ر) عدد 47، صادر بتاريخ 06 أوت 2009.

ب-2-17/ قانون رقم 13-07، مؤرخ في 29 أكتوبر 2013، يتضمن تنظيم مهنة المحاماة، (ج ر) عدد 55، صادر بتاريخ 30 أكتوبر 2013.

ب-2-18/ أمر رقم 15-02، مؤرخ في 23 يوليو 2015، يعدل ويتمم أمر رقم 66-155، يتضمن قانون الإجراءات الجزائية، (ج ر) عدد 40، صادر بتاريخ 23 يوليو 2015.

ب-2-19/ قانون رقم 15-12، مؤرخ في 15 جوان 2015، يتعلق بحماية الطفل، (ج ر) عدد 39، صادر بتاريخ 19 جوان 2015.

ب-2-20/ قانون رقم 16-02، مؤرخ في 19 جوان 2016، يعدل ويتمم أمر رقم 66-156، يتضمن قانون العقوبات، (ج ر)، عدد 37، صادر بتاريخ 22 جوان 2016.

ب-2-21/ قانون رقم 17-07، مؤرخ في 27 مارس 2017، يعدل ويتمم أمر رقم 66-155، يتضمن قانون الإجراءات الجزائية، (ج ر) عدد 20، صادر بتاريخ 29 مارس 2017.

ب-2-22/ قانون رقم 17-11، مؤرخ في 27 ديسمبر 2017، يتضمن قانون المالية لسنة 2018، (ج ر) عدد 76، صادر بتاريخ 28 ديسمبر 2017.

ب-2-23/ قانون رقم 18-01، مؤرخ في 30 جانفي 2018، يتمم قانون رقم 05-04، يتضمن قانون تنظيم السجون وإعادة الإدماج الاجتماعي للمحبوسين، (ج ر) عدد 05، صادر بتاريخ 30 جانفي 2018.

ب-2-24/ قانون رقم 18-04، مؤرخ في 10 ماي 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، (ج ر) عدد 27، صادر بتاريخ 13 ماي 2018.

ب-2-25/ قانون رقم 18-05، مؤرخ في 10 ماي 2018، يتعلق بالتجارة الإلكترونية، (ج ر) عدد 28، صادر بتاريخ 16 ماي 2018.

ب-2-26/ قانون رقم 18-07، مؤرخ في 10 جوان 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، (ج ر) عدد 34، صادر بتاريخ 10 جوان 2018.

ب-3/ النصوص التنظيمية:

ب-3-1/ مرسوم رقم 82-368، مؤرخ في 20 نوفمبر 1982، يتضمن مهام المديرية العسكرية للأمن العسكري، (ج ر) عدد 48، صادر بتاريخ 30 نوفمبر 1982.

ب-3-2/ مرسوم رئاسي رقم 04-183، مؤرخ في 26 جوان 2004، يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، (ج ر) عدد 41، صادر بتاريخ 27 جوان 2004.

ب-3-3/ مرسوم رئاسي رقم 04-432، مؤرخ في 29 ديسمبر 2004، يتضمن إنشاء المعهد الوطني للبحث في علم التحقيق الجنائي، (ج ر) عدد 84، صادر بتاريخ 29 ديسمبر 2004.

ب-3-4/ مرسوم رئاسي رقم 08-52، مؤرخ في 09 فيفري 2008، يتضمن إحداث مصلحة مركزية للشرطة القضائية للمصالح العسكرية للأمن التابعة لوزارة الدفاع الوطني ويحدد مهامها، (ج ر) عدد 08، صادر بتاريخ 13 فيفري 2008.

ب-3-5/ مرسوم رئاسي رقم 13-309، مؤرخ في 08 سبتمبر 2013، يلغي مرسوم رئاسي رقم 08-52، يتضمن إحداث مصلحة مركزية للشرطة القضائية للمصالح العسكرية للأمن التابعة لوزارة الدفاع الوطني ويحدد مهامها، (ج ر) عدد 45، صادر بتاريخ 18 سبتمبر 2013.

ب-3-6/ مرسوم رئاسي رقم 14-183، مؤرخ في 11 جوان 2014، يتضمن التحقيق القضائي لمديرية الأمن الداخلي بدائرة الاستعلام والأمن ومهامها وتنظيمها، (ج ر) عدد 32، صادر بتاريخ 12 جوان 2014.

ب-3-7/ مرسوم رئاسي رقم 15-261، مؤرخ 08 أكتوبر 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما، (ج ر) عدد 53، صادر بتاريخ 08 أكتوبر 2015.

ب-3-8/ مرسوم تنفيذي رقم 96-265، مؤرخ في 03 أوت 1996، يتضمن إنشاء سلك الحرس البلدي ويحدد مهامه وتنظيمه، (ج ر) عدد 47، صادر بتاريخ 07 أوت 1996.

ب-3-9/ مرسوم تنفيذي رقم 98-257، مؤرخ في 25 أوت 1998، يضبط شروط وكيفيات إقامة خدمات "أنترنات" واستغلالها، (ج ر) عدد 63، صادر بتاريخ 26 أوت 1998. معدل ومتمم بمرسوم تنفيذي 2000-307، مؤرخ في 14 أكتوبر 2000، (ج ر) عدد 60، صادر بتاريخ 15 أكتوبر 2000.

ب-3-10/ مرسوم تنفيذي رقم 06-348، مؤرخ في 05 أكتوبر 2006، يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، (ج ر) عدد 63، صادر بتاريخ 08 أكتوبر 2006، معدل بمرسوم تنفيذي رقم 16-267، مؤرخ في 17 أكتوبر 2016، (ج ر) عدد 62، صادر بتاريخ 23 أكتوبر 2016.

ب-3-11/ مرسوم تنفيذي رقم 17-324، مؤرخ في 08 نوفمبر 2017، يتضمن شروط وكيفيات تعيين المساعدين المتخصصين لدى النيابة العامة وقانونهم الأساسي ونظام تعويضاتهم، (ج ر) عدد 67، صادر بتاريخ 15 نوفمبر 2017.

ب-3-12/ قرار وزاري مشترك، مؤرخ في 17 ديسمبر 2017، يحدد التنظيم الداخلي لهياكل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، (ج ر) عدد 14، صادر بتاريخ 04 مارس 2018.

ب-3-13/ قرار وزارة العدل، مؤرخ في 07 مارس 2018، يحدد قائمة التخصصات التي يعين فيها المساعدون المتخصصون والجهات القضائية المعنية، (ج ر) عدد 22، صادر بتاريخ 18 أفريل 2018.

ج- النصوص القانونية المقارنة:

ج-1/ قانون رقم 2002-02، مؤرخ في 12 فيفري 2002، يتعلق بالمعاملات والتجارة الإلكترونية لإمارة دبي، الإمارات العربية المتحدة.

ج-2/ مرسوم بقانون اتحادي رقم 2012-05، مؤرخ في 13 أوت 2012، يتعلق بمكافحة جرائم تقنية المعلومات، الإمارات العربية المتحدة، معدل ومتمم.

ج-3/ قانون رقم 2015-27، مؤرخ في 04 ماي 2015، يتعلق بالجريمة الالكترونية، الأردن.

6. التقارير والمقالات الإعلامية والبحوث المؤسساتية والأعمال الاسترشادية:

أ- إبراهيم الوسلاتي ومن معه، "دليل تطبيقي للانابات القضائية الدولية في المادة الجزائية"، وزارة العدل، تونس، 2015، متوفر عبر الرابط:
https://www.idlo.int/sites/default/files/pdfs/highlights/Tunisia%20%20Guide%20to%20Letters%20Rogatory.pdf.

ب- أحمد جواد ربيعي ومن معه – عن الأمين العام للإنتربول، "منظمة التفاهم المبرمة بين الإنتربول ومجلس وزراء الداخلية العرب تبقى أساسا للتعاون بين المنظمتين"، مجلة أصداء الأمانة، الأمانة العامة لمجلس وزراء الداخلية العرب، ضفاف البحيرة، تونس، عدد 41، مارس 2017. متوفر عبر الرابط: http://www.aim-council.org.

ج- الإنتربول، "الجريمة السيبيرية"، مشاريع شرطية تركز على المستقبل، د ت. متوفر عبر الرابط: https://www.interpol.int/.../UFS_CYBER_Brochure_feb17_AR_03.

د- أنيل كورانا وبدر العلماء، "الثورة الصناعية الرابعة: بناء المؤسسات الصناعية الرقمية"، وثيقة معلومات، شركة برايس ووترهاوس كوبرز(في دبليو سي) بالتعاون مع القمة العالمية للصناعة والتصنيع(GMIS) وبمبادرة من منظمة الأمم المتحدة للتنمية الصناعية(اليونيدو) ووزارة الاقتصاد في دولة الإمارات العربية المتحدة، 2016. متوفر عبر الرابط:
https://www.pwc.com/gx/en/industries/industry-4.0.html.

ه- وزارة العدل، "بطاقة فنية حول نظام الوضع تحت المراقبة الإلكترونية"، الجزائر، د ت.

و- وحيد تاجي –مكتب الموقع الالكتروني، "الأفريبول يحتضن اجتماعات العمل حـــول دليـــل العـــرائض والأدلة الرقمية"، مجلة الشرطة، المديرية العامة للأمن الوطني، الجزائر، عدد 140، مارس 2018.

ز- لجنة الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، "برنامج تعزيز حكم القانون في بعض الـــدول العربية-مشروع تحديث النيابيات العامة"، برنامج الأمم المتحدة للتنمية، المملكة المغربية، 2007.

ح- مجلس أوربا، "التقرير التفسيري لاتفاقية الجريمة الالكترونية"، بودابست، هنغاريا، 2001. متوفر عبر الرابط: https://rm.coe.int/explanatory-report-budapest-convention-in-arabic/1680739174.

ط- مصطفاوي عبد القادر- رئيس المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيـــات الإعـــلام والاتصال، "جهود استباقية للأمن الوطني لتحقيق الأمن المعلوماتي والامتياز في الأداء"، مجلة الشـــرطة، المديرية العامة للأمن الوطني، الجزائر، عدد 129، ديسمبر 2015.

ي- مقررات وتوصيات مؤتمر ريو دي جانيرو بشأن جرائم الكمبيوتر، مؤتمر الأمم المتحدة الخامس عشر للجمعية الدولية لقانون العقوبات، ريو دي جانيرو، البرازيل ، 04-09 أكتوبر 1994. متوفر عبر الرابط: http://www.f-law.net/law/threads/1080.

ك- مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها للدرك الوطني، "الجريمة المعلوماتية ودور الدرك الوطني"، الجزائر، د ت.

ل- .....، "حالات ملموسة"، الجزائر، د ت.

م- مركز هردو لدعم التعبير الرقمي، "الجريمة الالكترونية وحجية الدليل الرقمي في الإثبات الجنائي"، تقرير، القاهرة، مصر، 2014.

ن- عبد الله بن سعيد أبو داسر، إثبات الدعوى الجنائية-دراسة مقارنة، بحث في إطار برنامج الدكتوراه، قسم السياسة الشرعية، جامعة الإمام محمد بن سعود الإسلامية، الرياض، المملكة العربية السعودية، 2011.

س- علي حسن الطوالبة، "التعاون الدولي في مجال مكافحة الجرائم الالكترونية"، مركز الإعلام الأمني، وزارة الداخلية، مملكة البحرين، د ت. متوفر عبر الرابط:
https://www.policemc.gov.bh/research/cyber-economic-and-criminal-crimes/.

ع- فريق الخبراء المعني بالجريمة السيبرانية، "مشروع المواضيع المطروحة للنظر في إطار دراسة شاملة بشأن تأثير الجريمة السيبرانية وتدابير التصدي لها"، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، منظمة الأمم المتحدة، فيينا، النمسا، 21 جانفي 2011. متوفر عبر الرابط:
http://www.unodc.org/unodc/fr/cybercrime/index.html.

ف- فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، "دراسة شاملة عن مشكلة الجريمة السيبرانية والتدابير التي تتخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدي لها"،

مكتب الأمم المتحدة المعني بالمخدرات والجريمة، منظمة الأمم المتحدة، فيينا، النمسا، 28 فيفري 2013. متوفر عبر الرابط: https://www.unodc.org/unodc/en/cybercrime/index.html.

ص- قرار هافانا بشأن الجرائم ذات الصلة بالكمبيوتر، مؤتمر الأمـــم المتحدة الثـــامن لمنـــع الجريمة ومعاملة السجناء، هافانا، كوبا، 1990. متوفر عبر الرابط: http://faculty.mu.edu.sa/nalthobaiti/crime.

7. المحاضرات المطبوعـــــــــة:

أ- دلال محمد بخيت، (مهارات الحاسب CPIT-100)، محاضرات في إطار الحصول على الرخصة الدولية لقيادة الحسب الآلي "ICDL"، المحاضرة الأولى، كلية الحاسبات وتقنية المعلومات، جامعة الملك عبد العزيز، المملكة العربية السعودية، د ت. متوفر عبر الرابط:
http://www.kau.edu.sa/Files/0010566/Subjects.ppt/المحاضرة%20الأولى.

ب- ناصر حمودي، (القانون الجنائي العام: الأحكام العامة لقانون العقوبات والنظرية العامة للجريمة)، محاضرات السنة الثانية حقوق، معهد الحقوق، المركز الجامعي العقيد آكلي محند أولحاج، البويرة، الجزائر، 2010.

ج- .....، (قانون الإجراءات الجزائية الجزائري)، محاضرات السنة الثانية حقوق، معهد الحقوق، المركز الجامعي العقيد آكلي محند أولحاج، البويرة، الجزائر، 2010.

د- ناصر حمودي، (قضاء التحقيق في قانون الإجراءات الجزائية الجزائري-دراسة تحليلية نقدية)، مطبوعة مقدمة لطلبة الماستر، كلية الحقوق والعلوم السياسية، جامعة العقيد آكلي محند أولحاج، البويرة، الجزائر، 2012.

8. مواقع شبكة الاتصال الدولية:

أ- المعجم الوسيط-قاموس اللغة العربية المعاصر-قاموس عربي عربي-قاموس رقمي، "تعريف ومعنى تنصت"، د ت ن، تاريخ التصفح: 29 نوفمبر 2018، الرابط:
https://www.almaany.com/ar/dict/ar-ar/تنصت/.

ب- أحمد عبد العزيز، "شرطة أبوظبي تشكل فرقاً متخصصة لمكافحة الجرائم الإلكترونية"، تاريخ النشر: 13 فيفري 2012، تاريخ التصفح: 06 مارس 2018. الرابط:
http://www.alittihad.ae/details.php?id=15105&y=2012.

ج- أحمد عبد القادر، "إنترنت الأقمار الصناعية وإنترنت الكابلات البحرية لا يتعارضان ولكن يتكاملان"، تاريخ النشر: 11 أفريل 2009، تاريخ التصفح: 25 نوفمبر 2017، الرابط:
https://aitnews.com/2009/02/11/9709.

د- ايفا الشوفي، "كيف تحارب التكنولوجيا الاتجار بالبشر؟"، تاريخ النشر: 17 أوت 2017، تاريخ التصفح: 09 فيفري 2018، الرابط: http://www.al-akhbar.com/node/281825.

ه- الموقع الرسمي لوزارة البريد والمواصلات السلكية واللاسلكية والتكنولوجيات والرقمنة، الجزائر، د ت ن، تاريخ التصفح: 02 أفريل 2018، الرابط: https://www.mpttn.gov.dz.

و- الموقع الرسمي للأمن الوطني الجزائري، "اختتام اجتماعات عمل أفريبول – أوروماد شرطة IV حول–دليل العرائض والأدلة الرقمية"، د ت ن، تاريخ التصفح: 06 مارس 2018، الرابط: http://www.algeriepolice.dz.

ز- الموقع الرسمي للأمن الوطني الجزائري، "الاجتماع الأول لآلية التعاون الشرطي الإفريقي أفريبول"، تاريخ نشر: 14 ماي 2017، تاريخ التصفح: 05 ماي 2018، الرابط: http://www.algeriepolice.dz.

ح- المعاني الجامع، "معجم كلمات رقمي"، د ت ن، تاريخ التصفح: 19 نوفمبر 2017. الرابط: https://www.almaany.com/ar/dict/ar-ar/وسط/.

ط- الناشط الجزائري، "ألمانيا سلمت 6 دول عربية منها الجزائر معدات وتجهيزات لمراقبة الإنترنت"، تاريخ النشر: 03 جويلية 2013، تاريخ التصفح: 23 فيفري 2018، الرابط: http://dzactiviste.info.

ي- العربية.نت، "جنون الـ"البيتكوين" يقترب من عتبة 10 آلاف دولار"، تاريخ النشر: 27 نوفمبر 2017، تاريخ التصفح: 27 نوفمبر 2017، الرابط: https://www.alarabiya.net/ar/aswaq/financial-markets/2017/11/27/جنون-بيتكوين-المتواصل-يقترب-بها-من-عتبة-10000-دولار.html.

ك- أسماء سعد الدين، "الفرق بين الثورة الصناعية الأولى والثانية"، تاريخ النشر: 10 أوت 2015، تاريخ التصفح: 19 نوفمبر 2017. الرابط: http://www.almrsal.com/post/262428.

ل- ب. حكيم، "الجزائر تؤمن شبكة الإنترنت عبر الكابل البحري من اسبانيا"، تاريخ النشر: 05 جانفي 2017، تاريخ التصفح: 10 أكتوبر 2017، الرابط: http://www.eco-algeria.com/content/الجزائر-تؤمن-شبكة-الانترنت-عبر-الكابل-البحري-الجديد-من-اسبانيا.

م- جريدة البلاد، "كابل الانترنت المتضرر.. اتصالات الجزائر تصدر بينا توضيحيا حول عملية تصليحه"، تاريخ النشر: 14 أفريل 2017، تاريخ التصفح: 10 أكتوبر 2017، الرابط: http://www.elbilad.net/article/detail?titre=كابل-الانترنت-المتضرر-إتصالات-الجزائر-تصدر-بيانا-توضيحيا-حول-عملية-إصلاحه&id=69124.

ن- هاني سمير علي، "ما لا تعرف عن الإنترنت الخفي Deep Web"، تاريخ النشر: 03 جويلية 2015، تاريخ التصفح: 05 جانفي 2017، الرابط: http://www.arageek.com/tech/2015/07/03/what-you-do-not-know-about-.

س- هزار بحبوح، "تحدي الحوت الأزرق...لعبة لانتحار المراهقين"، تاريخ النشـــر: 31 مـــاي 2017، تاريخ التصفح: 03 جانفي 2017، الرابط:
https://raseef22.com/life/2017/05/31/تحدي-الحوت-الأزرق-لعبة-تؤدي-لانتحار-ا/.

ع- ويكيبيديا، "جيل رابع(اتصالات لا سلكية)"، تاريخ النشر-آخر تعديل-: 24 سبتمبر 2017، تاريخ التصفح: 04 أكتوبر 2017، الرابط: https://ar.wikipedia.org/wiki/جيل_رابع_(اتصالات_لاسلكية).

ف- وليد عاكوم، "التحقيق في جرائم الحاسوب"، د ت ن، تاريخ التصفح: 25 جانفي 2017، الرابط: http// :ArabLawInfo.com.

ص- حسين بن سعيد الغافري، "التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الإنترنت"، شبكة قوانين الشرق، د ت ن، تاريخ التصفح: 01 مارس 2018، الرابط: http://www.eastlaws.com.

ق- كريم مسعودي، "نظام السوار الالكتروني في ظل السياسية العقابية المعاصرة"، مجلة القانون والأعمال، جامعة الحسن الأول، المملكة المغربية، مقال منشور عبر الموقع الرسمي، تاريخ النشر: 16 نوفمبر 2015، تاريخ التصفح: 29 سبتمبر 2017، الرابط: http://www.droitetentreprise.com.

ر- مدونة التوظيف في الجزائر، "إعلان عن توظيف في الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها أفريل 2017"، تاريخ النشر: 12 أفريل 2017، تاريخ التصفح: 23 مارس 2018، الرابط: http://www.dzemploi.org/2017/04/2017_92.html.

ش- موقع علم تعلم، "كل شئ عن الإنترنت المظلم dark web والنت العميق .. deep web بالتفصيل"، د ت ن، تاريخ التصفح: 06 جانفي 2017، الرابط:
http://www.ta3allamdz.com/2015/11/dark-web-deep-we.html.

ت- محمد الغضبان، "العالم الخفي! ما هو الديب ويب؟ وكيف تدخل إليه؟"، د ت ن، تاريخ التصـــفح: 08 جانفي 2017، الرابط:
http://www.netaawy.com/2016/08/What-is-the-deeb-web-and-how-to-access.

ث- ممدوح عبد الحميد عبد المطلب، "استخدام بروتوكول TCP/IP في بحث وتحقيق الجرائم على الكمبيوتر"، مقال رقمي، د ت ن، تاريخ التصفح: 10 أكتوبر 2017، الرابط:http:// ArabLawInfo.com.

خ- م. روابح، "الإنترنت متوفرة عبر الساتل للمواطنين قريبا"، تاريخ النشر: 17 أفريـــل 2015، تـــاريخ التصفح: 20 نوفمبر 2017، الرابط: https://www.echoroukonline.com/ara/articles/240116.html.

ذ - نواف القبيسي، "السعودية مقرا إقليميا لـــ «الإنتربول» بالشرق الأوسط"، تاريخ النشر: 13 أفريل 2018، تاريخ التصفح: 10 ماي 2018، الرابط:
https://thenewkhalij.news/سياسة/السعودية-مقرا-إقليميا-لـ«الإنتربول»-بالشرق-الأوسط/.

ض – سيد أحمد بورمانة – المدير العام للمعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني ببوشاوي، "حوار لـــ ديكانيوز: نطمح لتوسيع دائرة الاعتمـــاد بإدراج طـــرق تحليلية لفائدة مخابر أخرى"، تاريخ النشر: 08 ديسمبر 2014، تاريخ التصفح: 24 أفريل 2018، الرابط:
HTTP://AR.DKNEWS-DZ.COM/INDEX.PHP/NATION/ACTUALITE/25768-2014-12-08-17-29-20.

ظ– خبـــر 24، "the bad rabbi أخطر مجرمي الديب ويب"، تاريخ النشر: 23 جويلية 2017، تاريخ التصفح: 17 فيفري 2018، الرابط: https://www.youtube.com/watch?v=aDCMULEgPdA.

ثانيا: المراجع باللغة الأجنبية (فرنسية وانجليزية)

1. OUVRAGES:

A- ANDRE Lucas et DEVEZE Jean, Le Droit de L'Informatique et de L'Internet, PUF, Paris, France, 2001.

B- ARPAGIAN Nicolas, la Cybersécurité, Imprimé par ITCIS, Algérie, 2014.

C- AZZOUZI Ali, La Cybercriminalité au Maroc, Imprimé par Bishops Solution, Casablanca, Maroc, 2010.

D- DECHAMPS Frédéric et LAMBILOT Caroline, Cybercriminalité-Etat des lieux, Imprimé par Anthemis, Limal, Belgique, 2016.

E- GARE Thierry et GINESTET Catherine, Droit Pénal Procédure Pénal, Dalloz, France, 2012.

F- LALITTE Eric, Apprenez le fonctionnement des réseaux TCP/IP, 3eme édition, Imprimé par Eyrolles, Paris, France, 2016.

G- QUEMENER Myriam, Le Droit Face à La Disruption Numérique, Imprimé par Gualino éditeur, Paris, France, 2018.

2. ARTICLES SCIENTIFIQUES:

A- CHAVENT-LECLERE Anne-Sophie, "Droit pénal de l'internet", Revue Pénitentiaire, Numéro 1, France, Janvier-Mars 2017, p p 209-221.

B- DELAHAYE Jean-Paul, "Le Bitcoin, Première Crypto-Monnaie", Bulletin de la société informatique de France, Numéro 4, France, 2014, p p 67-104.

C- ROUSSELET-MAGRI Alexandre, "Les Perquisitions «informatiques» à l'épreuve du principe de souveraineté dans un contexte de mondialisation du stockage de données-étude comparée en droit français et États-Unien", Revue de science criminelle et de droit comparé, Numéro 4, France, Octobre-Décembre 2017, p p 659-676.

3. THESES ET MEMOIRES SCIENTIFIQUES:

A- BOOS Romain, (La lutte contre la cybercriminalité au regard de l'action des états), Thèse de doctorat, Droit privé et sciences criminelles, faculté de droit et sciences économiques et gestion de Nancy, Université de Lorraine, France, 2016.

B- BOUNNEFILLE Vincent, (Les Darknets: Extrémités D'un Réseau Aumbiant), Mémoire Master 1, Département Arts Plastiques, Université de Paris 8 Saint-Denis Vincennes, France, 2015.

C- THI Thuy Linh Phi, (La détention provisoire-Etude de droit comparé droit français et droit vietnamien), Thèse de doctorat, Ecole doctorale de droit, faculté de droit et de sciences politique, Université Montesquieu, Bordeaux IV, France, 2012.

4. CONVENTIONS INTERNATIONALES ET TEXTES JURIDIQUES:

A- Conventions internationales:

A-1/ Convention sur la cybercriminalité- Budapest, Convention Européenne (Internationale), Conseil de l'Europe, 2001. Disponible sur le Lien: http://www.coe.int/fr/web/conventions.

A-2/ Décision (UE) N° 2002/187/JAI, du 28 février 2002, Instituant Eurojust afin de renforcer la lutte contre les formes graves de criminalité, Conseil de l'Union européenne, Journal officiel de l'Union européenne, du 06 mars 2002. amendée par la décision du Conseil, N° 2003/659/JAI, du 18 juin 2003, (J O U E) du 29 septembre 2003. Et par; la décision du Conseil, N° 2009/426/JAI, du 16 décembre 2008, (J O U E) du 04 juin 2009. Disponible sur le Lien: http://www.eurojust.europa.eu/Pages/languages/fr.aspx.

A-3/ Règlement (UE) N° 2016/794, du 11 mai 2016, Relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol), Parlement Européen et Conseil de l'Union européenne, (J O U E) du 24 mai 2016. Disponible sur le Lien: https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0794.

A-4/ Résolution N° 16, GA-2017-86-RES-16, Coopération avec le mécanisme africain de coopération policière (Afripol), Assemblée générale de l'Interpol, 86ème session, Beijing, Chine, du 26 au 29 septembre 2017. Disponible sur le Lien: https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2017/Le-President-Xi-Jinping-ouvre-l-Assemblee-generale-dINTERPOL.

A-5/ Statut de L'O.I.P.C - Interpol, Version consolidée au 2017. Disponible sur le Lien: https://www.interpol.int/fr/Internet.

B- Textes juridiques:

B-1/ Code pénale français, Partie législative, Version consolidée au 17 septembre 2017. Disponible sur le Lien: https://www.legifrance.gouv.fr.

B-2/ Code de procédure pénale français, Partie législative, Version consolidée au 17 septembre 2017. Disponible sur le Lien: https://www.legifrance.gouv.fr.

B-3/ Code de commerce français, Version consolidée au 3 mars 2018. Disponible sur le Lien: https://www.legifrance.gouv.fr.

B-4/ Code des postes et des communications électroniques français, Version consolidée au 01 janvier 2019. Disponible sur le Lien: https://www.legifrance.gouv.fr.

5. RAPPORTS ET RECHERCHES SCIENTIFIQUES:

A- AHOUTY Charlotte, "Quels Mécanismes de coopération policière pour faire face à la cybercriminalité dans l'espace francophone ?", ORS Interpol BR Abidjan, Côte d'Ivoire, 08-10 février 2016. Disponible sur le Lien: https://www.interpol.int/fr.

B- BENSOUSSAN Alain et LEPAGE Agathe et QUEMENER Myriam, "Loyauté de la preuve et nouvelles technologies: entre exigences processuelles et efficacité répressive", Cycle de conférences 2013, La Cour de cassation, paris, France, 2013.

C- BOISSERIE Daniel, "Sécurités gendarmerie nationale", Avis fait au nom de la commission de la défense et des forces armées sur le projet de loi de finances pour 2016, N° 3115, Assemblée Nationale, France, 08 octobre 2015. Disponible sur le Lien: http://www.assemblee-nationale.fr/index.asp.

D- BRETON Thierry, "Chantier sur la lutte contre la cybercriminalité", Rapport remis a Monsieur le Ministre de l'Intérieur, de la Sécurité Intérieure, France, 25 février 2005. Disponible sur le Lien: http://www.ladocumentationfrancaise.fr/rapports-publics/054000263/index.shtml.

E- Centre de Prévention et de lutte Contre la Criminalité Informatique et la Cybercriminalité de la Gendarmerie Nationale, "Exécution des commissions rogatoires internationales-Exemples d'affaires traitées par les unités de la gendarmerie nationale et la sureté nationale se rapportant aux infractions liées aux TIC", Algérie, s d.

F- Centre de Prévention et de lutte Contre la Criminalité Informatique et la Cybercriminalité de la Gendarmerie Nationale, "Bilan d'activité du Centre Au titre de l'année 2016", Algérie, s d.

G- Centre de Prévention et de lutte Contre la Criminalité Informatique et la Cybercriminalité de la Gendarmerie Nationale, "Bilan d'activité du Centre Au titre de l'année 2017", Algérie, s d.

H- Convention sur la cybercriminalité- Budapest, "Rapport explicatif", Conseil de l'Europe, 2001. Disponible sur le Lien: http://www.coe.int/fr/web/conventions.

I- Comité de la Convention Cybercriminalité, "Les Attaques DDOS", Note d'Orientation: 05, Conseil de l'Europe, Strasbourg-France, 2013. Disponible sur le Lien: http://www.coe.int/fr/web/conventions.

J- Comité de la Convention Cybercriminalité, "Les Spams", Note d'Orientation: 08, Conseil de l'Europe, Strasbourg-France, 2014. Disponible sur le Lien: http://www.coe.int/fr/web/conventions.

K- DAVADIE Philippe, "La Théorie du Darknet", Chaire De Cyberdéfense Et Cybersecuritè, France, 2015. Disponible sur le Lien: http://www.chaire-cyber.fr/#&panel1-2.

L- DIGIMIND, "Découvrir et Exploiter le Web Invisible pour la Veille Stratégique", La Société Digimind-Social Media Monitoring d'e-réputation et de Veille Stratégique, New-York, USA, 2006. Disponible sur le Lien: http://www.digimind.com/fr/.

M- Eurojust, "Rapport annuel 2016 d'Eurojust", La Haye, Pays-Bas, 2017. Disponible sur le Lien: http://www.eurojust.europa.eu/doclibrary/corporate/Pages/annual-reports.aspx.

N- GATTOLIN André, "Europol et Eurojust: perspectives d'avenir", Rapport d'information fait au nom de la commission des affaires européennes, N° 477, Assemblée Nationale, France, 17 Avril 2014. Disponible sur le Lien: https://www.senat.fr/rap/r13-477/r13-4771.pdf.

O- Groupe de Travail Interministériel Sur la Lutte Contre la Cybercriminalité, "Protéger les Internautes", Rapport sur la Cybercriminalité, Europol, 2014. Disponible sur le Lien: https://www.europol.europa.eu.

P- Internet crime complaint center, "2016 Internet Crime Report", USA, u d. Available on Link: https://pdf.ic3.gov/2016_IC3Report.pdf.

Q- Internet crime complaint center, "IC3-Brochure", USA, u d. Available on Link: https://www.ic3.gov/media/IC3-Brochure.pdf.

R- LegiGlobe, "Cybercriminalité (br, cn, es, us, nl, uk)", Projet de développement du Réseau Francophone de Diffusion du Droit-Droit comparé, paris, France, 2013. Disponible sur le Lien: http://legiglobe.rf2d.org/cybercriminalite-2/2013/09/05/.

S- Logistique Seine-Normandie et La Région Haute-Normandie, "Les nouveaux Usages d'Internet et de L'informatique au Service de Votre Entreprise", France, s d. Disponible sur le Lien: https://www.logistique-seine-normandie.com/accueil.html.

T- Ministère de la justice Française, Circulaire de la DACG, n° CRIM 08-05/E3, du 28 janvier 2008, relative au placement sous surveillance électronique mobile, bulletin officiel du Ministère de la justice, France. Disponible sur le Lien: http://www.justice.gouv.fr.

U- Ministère de la justice Française, "Le placement sous surveillance électronique", 27 juillet 2016. Disponible sur le Lien: http://www.justice.gouv.fr.

6. COURS UNIVRSITAIRES:

- CARIOU Eric, (Historique et Architecture Générale des Ordinateurs), Cours 4, Université de Pau et des Pays de l'Adour UFR Sciences Pau-Département Informatique, France, s d. Disponible sur le Lien: http://famouspdf.com/search?q=Historique+et+Architecture+Générale+des+Ordinateurs.

7. SITES D'INTERNET:

A- CAMPBELL Chris, Accédez au dark Web en 5 minutes ou moins, s d p, Date d'Accès: 07 janvier 2017. Lien: http:// libredagir.fr/accedez-dark-web-5-minutes-ou-moins.

B- COEFFE Thomas, Chiffres Internet – 2017, Blog du Modérateur, Date de Publication: 01 Avril 2017, Date d'Accès: 31 novembre 2017. Lien: https://www.blogdumoderateur.com/chiffres-internet/.

C- JOAO FERNANDES Silva, "Le Dark Web: ombre et lumière", date de publication: 02 novembre 2016, date Date d'Accès: 06 janvier 2017. Lien: http://www.cafebabel.fr/style-de-vie/article/le-dark-web-ombre-et lumiere.html.

D- Larousse-Encyclopédie en Ligne, Internet, s d p, Date d'Accès: 30 novembre 2017. Lien: http://www.larousse.fr/encyclopedie/divers/Internet/125060.

E- Official website of the Internet Crime Complaint Center, File a complaint-IC3.gov-I accept, n p d, Date of Access: 01 May 2018, Link: https://www.ic3.gov/default.aspx.

F- Official website of Europol, Partners and agreements-Member States, n p d, Date of Access: 02 May 2018, Link: https://www.europol.europa.eu/partners-agreements/member-states.

G- Official website of Europol, Partners and agreements-Operational agreements, n p d, Date of Access: 02 May 2018, Link: https://www.europol.europa.eu/partners-agreements/operational-agreements#.

H- Official website of Europol, About Europol-European cybecrime centre "EC3", n p d, Date of Access: 02 May 2018, Link: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

I- Site officiel d'Eurojust, Bienvenue sur le site d'Eurojust, s d p, Date d'Accès: 05 mai 2018, Lien: http://www.eurojust.europa.eu/Pages/languages/fr.aspx.

J- Site officiel de la police nationale française, Organisation-Direction centrale de la police judiciaire-Sous-direction de lutte contre la cybercriminalité, Date de Publication: 19 janvier 2015, Date d'Accès: 09 mai 2018, Lien: https://www.police-nationale.interieur.gouv.fr

K- Site officiel de l'Interpol, Criminilaté-Cybercriminalité-Operations-Simda botnet, Date de Publication: 13 Avril 2015, Date d'Accès: 01 mai 2018, Lien: https://www.interpol.int/fr/Centre-des-médias/Nouvelles/2015/N2015-038/.

L- Site officiel de l'Interpol, Pays membres-Afrique-Algérie, Date de Publication: 2018, Date d'Accès: 30 Avril 2018, Lien: https://www.interpol.int/fr/Pays-membres/Monde.

M- Site officiel de la Gendarmerie nationale française, Accueil-Zooms-Cybercriminalité, s d p, Date d'Accès: 10 mai 2018, Lien: https://www.gendarmerie.interieur.gouv.fr/Zooms/Cybercriminalite.

الفهـــــــــــــرس

المضمـــــــــــــــــــــون	الصفحة
بسملـــــــــة – إهـــــــــداء – شـــــــكر – قائمـــــة المختصـــــرات	/
مـــقـــدمـــــــــــــــة	06
الباب الأول **الإطار العام لإجراءات التحري والتحقيق في جرائم الوسط الرقمي**	17
الفصل الأول: خصوصية إجراءات التحري والتحقيق في جرائم الوسط الرقمي	20
المبحث الأول: جرائم الوسط الرقمي ومسرحها الافتراضي الحديث	22
المطلب الأول: الوسط الرقمي الافتراضي كمسرح جرمي حديث	22
الفرع الأول: مفهوم الوسط الرقمي	23
أولا: نشأة وتطور الوسط الرقمي	23
ثانيا: تعريف الوسط الرقمي 1. تعريف "الوسط" و"الرقمية"، 2. تعريف "الوسط الرقمي".	24
ثالثا: خصائص الوسط الرقمي 1. تركيب وتكامل ماديات الوسط الرقمي، 2. افتراضية الوسط الرقمي.	26
الفرع الثاني: عناصر الوسط الرقمي المحدثة للمسرح الجرمي الافتراضي	28
أولا: جهاز الإعلام الآلي 1. مفهوم جهاز الإعلام الآلي، 2. أنواع جهاز الإعلام الآلي.	28
ثانيا: شبكة الاتصال الدولية 1. مفهوم شبكة الاتصال الدولية، 2. نظام عمل شبكة الاتصال الدولية.	33

الفرع الثالث: نطاق الوسط الرقمي الافتراضي كمسرح للجريمة	**38**
أولا: النطاق الافتراضي المتصل بجهاز الإعلام الآلي 1. أنظمة المعلومات الرقمية، 2. المعلومات الرقمية.	**38**
ثانيا: النطاق الافتراضي المتصل بشبكة الاتصال الدولية 1. النطاق الافتراضي العام لشبكة الاتصال الدولية، 2. النطاق الافتراضي الخاص لشبكة الاتصال الدولية.	**41**
المطلب الثاني: جرائم الوسط الرقمي	**46**
الفرع الأول: مفهوم جرائم الوسط الرقمي	**46**
أولا: نشأة وتطور الظاهرة الإجرامية في الوسط الرقمي	**46**
ثانيا: تعريف جرائم الوسط الرقمي 1. التعريف الضيق لجرائم الوسط الرقمي، 2. التعريف الواسع لجرائم الوسط الرقمي، 3. تعريف المشرع الجزائري لجرائم الوسط الرقمي.	**48**
ثالثا: خصائص جرائم الوسط الرقمي 1. عدم الاتفاق على إطار عام لجرائم الوسط الرقمي، 2. الطبيعة المزدوجة لأثر السلوك الافتراضي في جرائم الوسط الرقمي، 3. عالمية جرائم الوسط الرقمي، 4. التطور الديناميكي المستمر لجرائم الوسط الرقمي.	**52**
الفرع الثاني: الأركان العامة لجرائم الوسط الرقمي	**54**
أولا: الركن الشرعي لجرائم الوسط الرقمي 1. الإطار التقليدي لمبدأ الشرعية الجنائية، 2. مبدأ الشرعية الجنائية في جرائم الوسط الرقمي.	**55**
ثانيا: الركن المادي لجرائم الوسط الرقمي 1. الإطار التقليدي للركن المادي للجريمة، 2. الركن المادي في جرائم الوسط الرقمي.	**58**
ثالثا: الركن المعنوي لجرائم الوسط الرقمي 1. الإطار التقليدي للركن المعنوي للجريمة، 2. الركن المعنوي في جرائم الوسط الرقمي.	**60**
الفرع الثالث: تقسيمات جرائم الوسط الرقمي	**62**
أولا: التقسيمات المختلفة لجرائم الوسط الرقمي	**63**

1. المحاولات الأولى لتقسيم جرائم الوسط الرقمي، 2. تقسيم اتفاقية بودابست لجرائم الوسط الرقمي.	
ثانيا: تقسيم المشرع الجزائري لجرائم الوسط الرقمي 1. جرائم المساس بأنظمة المعالجة الآلية للمعطيات، 2. الجرائم التقليدية التي يكون النطاق الافتراضي للوسط الرقمي وسيلتها أو المسهل لارتكابها.	**66**
المبحث الثاني: إجراءات التحري والتحقيق في مواجهة المسرح الجرمي الافتراضي	**69**
المطلب الأول: عجز إجراءات التحري والتحقيق التقليدية عن مواجهة المسرح الجرمي الافتراضي	**69**
الفرع الأول: المفهوم التقليدي لإجراءات التحري والتحقيق	**70**
أولا: المفهوم التقليدي لإجراءات التحري 1. تعريف إجراءات التحري كمرحلة إجرائية، 2. مميزات إجراءات التحري كمرحلة إجرائية.	**70**
ثانيا: المفهوم التقليدي لإجراءات التحقيق 1. تعريف إجراءات التحقيق، 2. مميزات إجراءات التحقيق، 3. التمييز بين إجراءات التحقيق ومرحلة التحري.	**74**
الفرع الثاني: مظاهر عجز إجراءات التحري والتحقيق التقليدية عن مواجهة المسرح الجرمي الافتراضي	**80**
أولا: مظاهر العجز المتصلة بأجهزة التحري والتحقيق التقليدية	**80**
ثانيا: مظاهر العجز المتصلة بأعمال التحري والتحقيق التقليدية 1. صعوبة اكتشاف الجريمة في المسرح الافتراضي، 2. صعوبة إثبات الجريمة في المسرح الافتراضي.	**82**
المطلب الثاني: التوجه نحو إجراءات مستحدثة لمواجهة المسرح الجرمي الافتراضي	**87**
الفرع الأول: حتمية الاعتماد على إجراءات الوقاية الرقمية	**88**
أولا: مفهوم الوقاية الرقمية 1. تعريف الوقاية الرقمية، 2. خصائص الوقاية الرقمية كصورة من صور الأمن الرقمي.	**88**
ثانيا: مراحل الوقاية الرقمية	**92**

1. مرحلة تحديد المعلومة الهامة، 2. مرحلة تحليل المخاطر الإجرامية، 3. مرحلة التقييم واختيار الوسيلة الوقائية.	
ثالثا: وسائل الوقاية الرقمية 1. جدران الحماية (الجدران النارية)، 2. التحقق من الهوية، 3. مضادات الفيروسات، 4. التوقيع الرقمي، 5. تحديد نطاق الاستخدام، 6. التعامل مع المعطيات الحساسة والأجهزة الحاملة لها، 7. المراقبة المرئية.	**94**
الفرع الثاني: حتمية تحيين إجراءات التحري والتحقيق	**99**
أولا: تحيين الإجراءات المتصلة بأجهزة التحري والتحقيق 1. التدريب الرقمي لأعضاء أجهزة التحري والتحقيق، 2. إنشاء أجهزة تحري وتحقيق متخصصة في مواجهة جرائم الوسط الرقمي.	**100**
ثانيا: تحيين الإجراءات المتصلة بأعمال التحري والتحقيق 1. تحديث الأعمال الإجرائية التقليدية، 2. إضافة أعمال إجرائية حديثة.	**106**
الفصل الثاني: أجهزة التحري والتحقيق في جرائم الوسط الرقمي	**110**
المبحث الأول: الأجهزة الوطنية المختصة بالتحري والتحقيق في جرائم الوسط الرقمي	**112**
المطلب الأول: الأجهزة الرئيسية المختصة بالتحري والتحقيق في جرائم الوسط الرقمي	**112**
الفرع الأول: الأجهزة القضائية القائدة للتحري والتحقيق في جرائم الوسط الرقمي	**113**
أولا: جهاز النيابة العامة القائد لمرحلة التحري عن جرائم الوسط الرقمي 1. الأحكام العامة لجهاز النيابة العامة، 2. قواعد اختصاص جهاز النيابة العامة في إطار جرائم الوسط الرقمي.	**113**
ثانيا: جهاز قضاء التحقيق القائد لإجراءات التحقيق في جرائم الوسط الرقمي 1. الأحكام العامة لجهاز قضاء التحقيق، 2. قواعد اختصاص جهاز قضاء التحقيق في إطار جرائم الوسط الرقمي.	**117**
الفرع الثاني: الأجهزة الشرطية المباشرة للتحري والتحقيق في جرائم الوسط الرقمي	**121**

أولا: الجهاز الشرطي العام المباشر للتحري والتحقيق في جرائم الوسط الرقمي 1. الأحكام العامة للجهاز الشرطي العام، 2. قواعد اختصاص الجهاز الشرطي العام في إطار جرائم الوسط الرقمي.	**121**
ثانيا: الأجهزة الشرطية الخاصة المباشرة للتحري والتحقيق في جرائم الوسط الرقمي 1. الأجهزة الشرطية الخاصة التابعة للأمن الوطني، 2. الأجهزة الشرطية الخاصة التابعة للدرك الوطني، 3. الجهاز الشرطي الخاص التابع للمصالح العسكرية للأمن.	**126**
المطلب الثاني: الأجهزة الوطنية المساعدة على التحري والتحقيق في جرائم الوسط الرقمي	**132**
الفرع الأول: الهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام والاتصال ومكافحتها	**132**
أولا: التعريف بالهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام والاتصال ومكافحتها	**132**
ثانيا: تشكيلة الهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام والاتصال ومكافحتها 1. الهياكل العامة للهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام والاتصال ومكافحتها، 2. الهياكل الفنية للهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام والاتصال ومكافحتها، 3. الهياكل الفرعية للهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام والاتصال ومكافحتها.	**134**
ثالثا: مهام الهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام والاتصال ومكافحتها 1. تحديد مهام الهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام والاتصال ومكافحتها، 2. طريقة سير الهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام والاتصال ومكافحتها.	**139**
الفرع الثاني: الأجهزة التقنية المساعدة على التحري والتحقيق في جرائم الوسط الرقمي	**142**
أولا: الأجهزة الأمنية ذات الطابع التقني المساعد على التحري والتحقيق في جرائم الوسط الرقمي 1. المخابر التقنية التابعة للأمن الوطني، 2. المخبر التقني التابع للدرك الوطني.	**142**
ثانيا: الأجهزة المدنية ذات الطابع التقني المساعد على التحري والتحقيق في جرائم الوسط الرقمي 1. مقدمو الخدمات، 2. خبراء الوسط الرقمي.	**146**
المبحث الثاني: الأجهزة الأجنبية المتعاونة على التحري والتحقيق في جرائم الوسط الرقمي	**151**

المطلب الأول: التعاون الدولي على التحري والتحقيق في جرائم الوسط الرقمي	**151**
الفرع الأول: ماهية التعاون الدولي على التحري والتحقيق في جرائم الوسط الرقمي	**152**
أولا: مفهوم التعاون الدولي على التحري والتحقيق في جرائم الوسط الرقمي 1. تعريف التعاون الدولي على التحري والتحقيق في جرائم الوسط الرقمي، 2. خصائص التعاون الدولي على التحري والتحقيق في جرائم الوسط الرقمي.	**152**
ثانيا: إجراءات التعاون الدولي على التحري والتحقيق في جرائم الوسط الرقمي 1. الإجراءات العامة للتعاون الدولي على التحري والتحقيق في جرائم الوسط الرقمي، 2. الإجراءات الخاصة للتعاون الدولي على التحري والتحقيق في جرائم الوسط الرقمي.	**159**
الفرع الثاني: اعتماد القانون الجزائري للتعاون الدولي على التحري والتحقيق في جرائم الوسط الرقمي	**165**
أولا: مصادر القانون الجزائري المتصلة بالتعاون على التحري والتحقيق في جرائم الوسط الرقمي 1. المصادر الدولية الاتفاقية، 2. المصادر الوطنية الوضعية.	**165**
ثانيا: إجراءات القانون الجزائري الخاصة بالتعاون على التحري والتحقيق في جرائم الوسط الرقمي 1. مبادئ إجراءات القانون الجزائري الخاصة بالتعاون الدولي على التحري والتحقيق في جرائم الوسط الرقمي، 2. تفعيل إجراءات القانون الجزائري الخاصة بالتعاون الدولي على التحري والتحقيق في جرائم الوسط الرقمي، 3. صور إجراءات القانون الجزائري الخاصة بالتعاون الدولي على التحري والتحقيق في جرائم الوسط الرقمي.	**169**
المطلب الثاني: نماذج الأجهزة الأجنبية المتعاونة على التحري والتحقيق في جرائم الوسط الرقمي	**173**
الفرع الأول: الأجهزة الدولية المتعاونة على التحري والتحقيق في جرائم الوسط الرقمي	**173**
أولا: الأجهزة العالمية المتعاونة على التحري والتحقيق في جرائم الوسط الرقمي 1. منظمة الشرطة الجنائية الدولية "الإنتربول–Interpol"، 2. مركز شكاوى جرائم الإنترنت "IC3".	**174**
ثانيا: الأجهزة الأوروبية المتعاونة على التحري والتحقيق في جرائم الوسط الرقمي 1. وكالة الاتحاد الأوروبي للتعاون في مجال إنفاذ القانون "الأوروبول–Europol"،	**178**

2. وحدة التعاون القضائي الأوروبي "الأوروجست–Eurojust".	
ثالثا: الأجهزة الإفريقية والعربية المتعاونة على التحري والتحقيق في جرائم الوسط الرقمي 1. آلية الاتحاد الإفريقي للتعاون الشرطي "الأفريبول–Afripol"، 2. المكتب العربي للشرطة الجنائية.	**181**
الفرع الثاني: الأجهزة المقارنة المتعاونة على التحري والتحقيق في جرائم الوسط الرقمي	**184**
أولا: الأجهزة الفرنسية المتعاونة على التحري والتحقيق في جرائم الوسط الرقمي 1. الإطار التنظيمي للأجهزة الفرنسية المختصة بالتحري والتحقيق في جرائم الوسط الرقمي، 2. مظاهر تعاون الأجهزة الفرنسية المختصة بالتحري والتحقيق في جرائم الوسط الرقمي مع نظيرتها الجزائرية.	**184**
ثانيا: الأجهزة الأمريكية (و.م.أ) المتعاونة على التحري والتحقيق في جرائم الوسط الرقمي 1. الإطار التنظيمي للأجهزة الأمريكية (و.م.أ) المختصة بالتحري والتحقيق في جرائم الوسط الرقمي، 2. مظاهر تعاون الأجهزة الأمريكية (و.م.أ) المختصة بالتحري والتحقيق في جرائم الوسط الرقمي مع نظيرتها الجزائرية.	**188**
الباب الثاني **مباشرة إجراءات التحري والتحقيق في جرائم الوسط الرقمي**	**192**
الفصل الأول: الإجراءات الأساسية للتحري والتحقيق في جرائم الوسط الرقمي	**195**
المبحث الأول: الدليل الرقمي محور التحري والتحقيق في جرائم الوسط الرقمي	**197**
المطلب الأول: ماهية الدليل الرقمي الجنائي	**197**
الفرع الأول: مفهوم الدليل الرقمي الجنائي	**198**
أولا: تعريف الدليل الرقمي الجنائي 1. التعريف العام للدليل الجنائي، 2. التعريف الخاص للدليل الرقمي الجنائي.	**198**

ثانيا: مميزات الدليل الرقمي الجنائي 1. ميزة الازدواجية في الطبيعة، 2. ميزة البعد العلمي التكنولوجي، 3. ميزة التنوع والتطور الديناميكي، 4. ميزة التحصين الآلي من الزوال، 5. ميزة المحدد الدقيق لأطراف الجريمة وتحركاتهم الرقمية.	**203**
الفرع الثاني: البعد التقني للدليل الرقمي الجنائي	**209**
أولا: البعد التقني العام للدليل الرقمي الجنائي 1. أقسام الدليل الرقمي الجنائي، 2. مصادر الدليل الرقمي الجنائي.	**210**
ثانيا: البعد التقني الخاص للدليل الرقمي الجنائي 1. المنطقة الأولى، 2. المنطقة الثانية، 3. المنطقة الثالثة، 4. المنطقة الرابعة.	**215**
المطلب الثاني: حجية الدليل الرقمي في الإثبات الجنائي	**217**
الفرع الأول: حجية الدليل الرقمي في أنظمة الإثبات الجنائي المختلفة	**217**
أولا: حجية الدليل الرقمي في نظام الإثبات الجنائي الحر 1. مفهوم الإثبات الجنائي المقيد، 2. الدليل الرقمي ونظام الإثبات الجنائي المقيد.	**217**
ثانيا: حجية الدليل الرقمي في نظام الإثبات الجنائي المقيد 1. مفهوم الإثبات الجنائي الحر، 2. الدليل الرقمي ونظام الإثبات الجنائي الحر.	**220**
ثالثا: حجية الدليل الرقمي في نظام الإثبات الجنائي المختلط 1. مفهوم الإثبات الجنائي المختلط، 2. الدليل الرقمي ونظام الإثبات الجنائي المختلط.	**222**
الفرع الثاني: حجية الدليل الرقمي أمام القضاء الجنائي	**224**
أولا: المتطلبات القضائية لصحة الدليل الرقمي الجنائي 1. مشروعية الدليل الرقمي، 2. نزاهة الدليل الرقمي، 3. علاقة الدليل الرقمي بموضوع الجريمة،	**224**

4. يقينية الدليل الرقمي،	
5. مناقشة الدليل الرقمي.	
ثانيا: نماذج عن تعامل القضاء المقارن مع الدليل الرقمي الجنائي	**227**
1. نماذج عن تعامل القضاء الفرنسي مع الدليل الرقمي الجنائي،	
2. نماذج عن تعامل القضاء الأمريكي –و.م.أ– مع الدليل الرقمي الجنائي.	
الفرع الثالث: حجية الدليل الرقمي الجنائي في القانون والقضاء الجزائريين	**230**
أولا: حجية الدليل الرقمي الجنائي في القانون الجزائري	**230**
1. الاعتماد القانوني الصريح لنظام الإثبات الجنائي الحر،	
2. الاعتماد القانوني الضمني للدليل الرقمي في الإثبات الجنائي.	
ثانيا: حجية الدليل الرقمي الجنائي أمام القضاء الجزائري	**234**
1. التكريس القضائي لنظام الإثبات الجنائي الحر،	
2. العمل القضائي بالدليل الرقمي في الإثبات الجنائي،	
المبحث الثاني: الأعمال الجوهرية لاستخراج الدليل الرقمي الجنائي	**237**
المطلب الأول: المعاينة والتفتيش أساس استخراج الدليل الرقمي الجنائي	**237**
الفرع الأول: المعاينة في جرائم الوسط الرقمي	**238**
أولا: مفهوم المعاينة في جرائم الوسط الرقمي	**238**
1. تعريف المعاينة في جرائم الوسط الرقمي،	
2. الطبيعة القانونية للمعاينة في جرائم الوسط الرقمي،	
3. أهمية المعاينة في جرائم الوسط الرقمي.	
ثانيا: خصوصية المعاينة في جرائم الوسط الرقمي	**241**
1. محل المعاينة في جرائم الوسط الرقمي،	
2. القواعد الإجرائية والفنية للمعاينة في جرائم الوسط الرقمي،	
3. معوقات انجاز المعاينة في جرائم الوسط الرقمي.	
الفرع الثاني: التفتيش في جرائم الوسط الرقمي	**246**
أولا: مفهوم التفتيش في جرائم الوسط الرقمي	**246**
1. تعريف التفتيش في جرائم الوسط الرقمي،	
2. الطبيعة القانونية للتفتيش في جرائم الوسط الرقمي،	
3. أهمية التفتيش في جرائم الوسط الرقمي.	
ثانيا: خصوصية التفتيش في جرائم الوسط الرقمي	**250**
1. محل التفتيش في جرائم الوسط الرقمي،	
2. القواعد الإجرائية للتفتيش في جرائم الوسط الرقمي،	

3. القواعد الفنية للتفتيش في جرائم الوسط الرقمي.	
المطلب الثاني: أبعاد المعاينة والتفتيش في جرائم الوسط الرقمي	**260**
الفرع الأول: الدعم التقني لانجاز المعاينة والتفتيش في جرائم الوسط الرقمي	**260**
أولا: الدعم التقني المقدم من المساعدين المتخصصين أثناء مرحلة التحري 1. ماهية الدعم التقني المقدم من المساعدين المتخصصين أثناء مرحلة التحري، 2. القواعد الفنية للدعم التقني المقدم من المساعدين المتخصصين أثناء مرحلة التحري.	**260**
ثانيا: الدعم التقني المقدم من الخبراء أثناء إجراءات التحقيق 1. ماهية الدعم التقني المقدم من الخبراء أثناء إجراءات التحقيق، 2. القواعد الفنية للدعم التقني المقدم من الخبراء أثناء إجراءات التحقيق.	**264**
الفرع الثاني: الحجز المترتب عن المعاينة والتفتيش في جرائم الوسط الرقمي	**270**
أولا: مفهوم الحجز المترتب عن المعاينة والتفتيش في جرائم الوسط الرقمي 1. تعريف الحجز المترتب عن المعاينة والتفتيش في جرائم الوسط الرقمي، 2. طبيعة الحجز المترتب عن المعاينة والتفتيش في جرائم الوسط الرقمي، 3. أهمية الحجز المترتب عن المعاينة والتفتيش في جرائم الوسط الرقمي.	**271**
ثانيا: خصوصية الحجز المترتب عن المعاينة والتفتيش في جرائم الوسط الرقمي 1. محل الحجز المترتب عن المعاينة والتفتيش في جرائم الوسط الرقمي، 2. القواعد الإجرائية للحجز المترتب عن المعاينة والتفتيش في جرائم الوسط الرقمي، 3. القواعد الفنية للحجز المترتب عن المعاينة والتفتيش في جرائم الوسط الرقمي.	**275**
الفصل الثاني: الإجراءات المساعدة على التحري والتحقيق في جرائم الوسط الرقمي	**279**
المبحث الأول: الإجراءات التقليدية المساعدة على التحري والتحقيق في جرائم الوسط الرقمي	**281**
المطلب الأول: الأعمال التقليدية المساعدة على التحري والتحقيق في جرائم الوسط الرقمي	**281**
الفرع الأول: أعمال التنصت والتسرب المساعدة على التحري والتحقيق في جرائم الوسط الرقمي	**282**
أولا: التنصت المساعد على التحري والتحقيق في جرائم الوسط الرقمي 1. تعريف التنصت المساعد على التحري والتحقيق في جرائم الوسط الرقمي، 2. جرائم الوسط الرقمي الجائز التنصت بخصوص ممارسة التحري والتحقيق فيها،	**282**

3. إجراءات اللجوء إلى التنصت المساعد على التحري والتحقيق في جرائم الوسط الرقمي.	
ثانيا: التسرب المساعد على التحري والتحقيق في جرائم الوسط الرقمي 1. تعريف التسرب المساعد على التحري والتحقيق في جرائم الوسط الرقمي، 2. جرائم الوسط الرقمي الجائز التسرب بخصوص ممارسة التحري والتحقيق فيها، 3. إجراءات اللجوء إلى التسرب المساعد على التحري والتحقيق في جرائم الوسط الرقمي.	**286**
الفرع الثاني: أعمال السماع والاستجواب المساعدة على التحري والتحقيق في جرائم الوسط الرقمي	**291**
أولا: السماع المساعد على التحري والتحقيق في جرائم الوسط الرقمي 1. القواعد الإجرائية العامة للسماع الممارس للتحري والتحقيق في الجريمة، 2. الوجه الرقمي الحديث للسماع المساعد على التحري والتحقيق في جرائم الوسط الرقمي.	**291**
ثانيا: الاستجواب المساعد على التحقيق في جرائم الوسط الرقمي 1. القواعد الإجرائية العامة للاستجواب الممارس للتحقيق في الجريمة، 2. الوجه الرقمي الحديث للاستجواب المساعد على التحقيق في جرائم الوسط الرقمي.	**297**
المطلب الثاني: الأذون والأوامر التقليدية المساعدة على التحري والتحقيق في جرائم الوسط الرقمي	**301**
الفرع الأول: الإذن بتوقيف المشتبه فيه للنظر المساعد على التحري عن جرائم الوسط الرقمي	**301**
أولا: القواعد الإجرائية العامة للتوقيف للنظر 1. مفهوم التوقيف للنظر، 2. مدة تنفيذ إذن التوقيف للنظر، 3. ضمانات الموقوف للنظر.	**301**
ثانيا: خصوصية التوقيف للنظر المساعد على التحري عن جرائم الوسط الرقمي 1. خصوصية التوقيف للنظر في مواجهة جرائم المساس بأنظمة المعالجة الآلية للمعطيات، 2. خصوصية التوقيف للنظر في مواجهة الجريمة التقليدية المتصلة بالوسط الرقمي.	**306**
الفرع الثاني: الأمر بوضع المتهم تحت الرقابة القضائية المساعد على التحقيق في جرائم الوسط الرقمي	**308**
أولا: القواعد الإجرائية العامة للوضع تحت الرقابة القضائية 1. مفهوم الوضع تحت الرقابة القضائية، 2. الالتزامات التي يفرضها أمر الوضع تحت الرقابة القضائية، 3. إجراءات إصدار وتنفيذ أمر الوضع تحت الرقابة القضائية.	**308**

ثانيا: ممارسة أمر الوضع تحت الرقابة القضائية كمساعد على التحقيق في جرائم الوسط الرقمي 1. إمكانية اللجوء إجرائيا إلى الوضع تحت الرقابة القضائية في مواجهة جرائم الوسط الرقمي، 2. معوقات نجاعة الوضع تحت الرقابة القضائية كمساعد على التحقيق في جرائم الوسط الرقمي.	**312**
الفرع الثالث: الأمر بإيداع المتهم في الحبس المؤقت المساعد على التحقيق في جرائم الوسط الرقمي	**315**
أولا: القواعد الإجرائية العامة للإيداع في الحبس المؤقت 1. مفهوم الإيداع في الحبس المؤقت، 2. مبررات إصدار أمر الإيداع في الحبس المؤقت، 3. مدة الحبس المؤقت المحددة بأمر الإيداع.	**315**
ثانيا: ممارسة أمر الإيداع في الحبس المؤقت كمساعد على التحقيق في جرائم الوسط الرقمي 1. إمكانية اللجوء إجرائيا إلى الإيداع في الحبس المؤقت بخصوص جرائم الوسط الرقمي، 2. مدد الحبس المؤقت في جرائم الوسط الرقمي.	**319**
المبحث الثاني: الإجراءات الحديثة المساعدة على التحري والتحقيق في جرائم الوسط الرقمي	**321**
المطلب الأول: الأعمال الحديثة المساعدة على التحري والتحقيق في جرائم الوسط الرقمي	**321**
الفرع الأول: مراقبة الاتصالات الإلكترونية	**322**
أولا: مفهوم مراقبة الاتصالات الإلكترونية 1. تعريف مراقبة الاتصالات الإلكترونية، 2. مميزات مراقبة الاتصالات الإلكترونية، 3. تمييز مراقبة الاتصالات الإلكترونية عما يشابهها.	**322**
ثانيا: شروط ممارسة مراقبة الاتصالات الإلكترونية 1. الشروط العامة للممارسة مراقبة الاتصالات الإلكترونية، 2. الشروط الخاصة للممارسة مراقبة الاتصالات الإلكترونية.	**328**
الفرع الثاني: التحفظ العاجل على المعطيات الرقمية المخزنة	**330**
أولا: مفهوم التحفظ العاجل على المعطيات الرقمية المخزنة 1. تعرف التحفظ العاجل على المعطيات الرقمية المخزنة، 2. نتائج التحفظ العاجل على المعطيات الرقمية المخزنة.	**331**

ثانيا: أنواع المعطيات الرقمية المخزنة محل التحفظ العاجل 1. التحفظ العاجل على المعطيات المخزنة المتعلقة بالمحتوى، 2. التحفظ العاجل على المعطيات المخزنة المتعلقة بحركة السير.	**336**
الفرع الثالث: تحديد هوية المشتبه فيه الرقمي	**339**
أولا: التحديد الرقمي لهوية المشتبه فيه عبر تتبع بروتوكول الـــ "TCP-IP" 1. المضمون التقني لبرتوكول الـــ "TCP-IP"، 2. الاعتماد الإجرائي على برتوكول الـــ "TCP-IP" لتحديد هوية المشتبه فيه.	**339**
ثانيا: التحديد الرقمي لهوية المشتبه فيه من دون تتبع بروتوكول الـــ "TCP-IP" 1. التحديد الرقمي لهوية المشتبه فيه عبر تتبع بطاقات الهاتف المحمول، 2. التحديد الرقمي لهوية المشتبه فيه عبر الاستنتاج المتصل بالأعمال الرقمية الأخرى، 3. التحديد الرقمي لهوية المشتبه فيه عبر الاستنتاج المتصل بالأعمال التقليدية الأخرى.	**344**
المطلب الثاني: الأوامر الحديثة المساعدة على التحري والتحقيق في جرائم الوسط الرقمي	**346**
الفرع الأول: الأمر بإنتاج وتقديم المعطيات الرقمية	**346**
أولا: مفهوم الأمر بإنتاج وتقديم المعطيات الرقمية 1. تعريف الأمر بإنتاج وتقديم المعطيات الرقمية، 2. خصائص الأمر بإنتاج وتقديم المعطيات الرقمية.	**346**
ثانيا: إجراءات ممارسة الأمر بإنتاج وتقديم المعطيات الرقمية 1. السياق الإجرائي لممارسة الأمر بإنتاج وتقديم المعطيات الرقمية، 2. أطراف الأمر بإنتاج وتقديم المعطيات الرقمية.	**350**
الفرع الثاني: الأمر بمنع المشتبه فيه من مغادرة التراب الوطني	**352**
أولا: القواعد الإجرائية العامة لمنع المشتبه فيه من مغادرة التراب الوطني 1. تعريف منع المشتبه فيه من مغادرة التراب الوطني، 2. شروط ممارسة الأمر بمنع المشتبه فيه من مغادرة التراب الوطني.	**352**
ثانيا: أمر المنع من مغادرة التراب الوطني في مواجهة المشتبه فيه الرقمي 1. المنع من مغادرة التراب الوطني بمناسبة التحري عن جرائم المساس بأنظمة المعالجة الآلية للمعطيات، 2. المنع من مغادرة التراب الوطني بمناسبة التحري عن الجريمة التقليدية المتصلة بالوسط الرقمي.	**356**
الفرع الثالث: الأمر بوضع المتهم تحت المراقبة الإلكترونية	**358**
أولا: مفهوم الوضع تحت المراقبة الإلكترونية 1. تعريف الوضع تحت المراقبة الإلكترونية،	**358**

2. خصائص الوضع تحت المراقبة الإلكترونية.	
ثانيا: ممارسة الأمر بوضع المتهم تحت المراقبة الإلكترونية 1. إجراءات إصدار أمر وضع المتهم تحت المراقبة الإلكترونية، 2. إجراءات تنفيذ أمر وضع المتهم تحت المراقبة الإلكترونية.	**362**
الخاتمـــــــــــــــة	**366**
قائمـــة المـــــــراجـــع	**374**
الفهـــــــــــــــرس	**401**
ملخـــــص (عربي – فرنسي – انجليزي)	**416**

ملـخـــــــــــص

(عربي - فرنسي - انجليزي)

ملخـــــــــص

يبدوا لأول وهلة أنه للنطاق الافتراضي الذي خلقته عناصر الوسط الرقمي –جهاز الإعلام الآلي وشبكة الاتصال الدولية–؛ الأثر الايجابي المفيد للأشخاص خاصة والمجتمع عموما. حيث أصبح من الممكن للمتفاعل مع هذه العناصر؛ أن يلج إلى نطاقها الافتراضي، فيفيد ويستفيد إلى أبعد الحدود الممكنة. إلا أن هذا الولوج السهل والسلس؛ أنتج مع مرور الوقت أثرا سلبيا، تجاوز في أخطاره ومضاره كل حدود المعقول والمسموح ظاهراً ومضموناً.

ومع تزايد الأخطار والأضرار الناتجة عن تفاعل الأشخاص –طبيعية ومعنوية– مع عناصر الوسط الرقمي؛ كان لزاما على المشرع أن يلج إلى هذا الوسط، ليجرم ويعاقب فيه، السلوكيات واجبة التجريم بعد محاولة تحديدها، انطلاقا من الأثر السلبي الذي تحدثه. الأمر الذي لم يكن بالسهولة المتصلة بالجريمة التقليدية، بل صاحب هذا الولوج والتحديد؛ الكثير من التعقيدات، المنبثقة أصلا من الخصوصية الفنية المعقدة للوسط الرقمي، التي انبثقت بدورها على الإجرام المتصل بها، فاكتسب الكثير من الخصوصية الحديثة هو الآخر.

إلا أن هذا الولوج التجريمي من المشرع إلى الوسط الرقمي، بكل خصوصياته وتعقيداته القانونية ذات المرجعية الفنية الحديثة؛ جعل من التدخل التشريعي الإجرائي أمرا لازما، سيما وأن هذا الأخير –الشق الإجرائي–؛ يتبع بالضرورة نضيره الموضوعي، من حيث الطبيعة في التكوين والمواجهة، انطلاقا من القاعدة الإجرائية الجوهرية التي مفادها؛ أن دور النص الإجرائي عموما، يبدأ بعد انتهاء دور النص الموضوعي، الذي من المفروض أنه وضع قبله.

وفي السياق نفسه المذكور أعلاه؛ واجه المشرع النطاق الافتراضي للوسط الرقمي، كمسرح جرمي حديث له الكثير من الخصوصية الفنية الحديثة. الأمر الذي أسس لبروز خصوصية إجرائية غير مألوفة التعامل، سيما من حيث إجراءات التحري والتحقيق، التي ظهرت بشكل حديث مغاير، إن بخصوص إطارها العام بما في ذلك الأجهزة الرئيسية والمساعدة والمتعاونة، أو الأعمال الإجرائية الممارسة من طرف هذه الأجهزة.

ومن خلال الولوج الإجرائي المذكور، أصبحت تُوَاجَهُ جرائم الوسط الرقمي؛ بالعديد من الأحكام الإجرائية ذات الصلة بالتحري والتحقيق، التي توصلنا بخصوص مباشرتها؛ أنها تتمحور حول الدليل الرقمي الجنائي؛ الذي تستخرجه الأجهزة المختصة، بعد مباشرة أعمال جوهرية وإجراءات مساعدة –أعمال وأذون وأوامر– تقليدية وحديثة. التي خلصنا بخصوصها –إجراءات التحري والتحقيق في جرائم الوسط الرقمي السارية–، في إطار النتائج والتوصيات؛ أن لها العديد من الايجابيات واجبة التعزيز، كما لها العديد من السلبيات أيضا، التي من الضروري تفاديها بالطرق الموصى بها.

Résumé

Il semble au premier abord que le champ virtuel créé par les éléments de cyber espace, l'ordinateur et l'internet, ont un impact utile positif pour les personnes en particulier et pour la société en général. En conséquence, il est probablement devenu possible pour les personnes possédant ces éléments d'avoir accès à leur champ virtuel afin d'en bénéficier et d'en tirer le meilleur parti possible. Mais cet accès facile et sans heurt a eu un impact négatif au fil du temps, dépassant toutes les limites.

Face aux dangers et dommages croissants causés par le champ virtuel créé par les éléments de cyberespace, le législateur était obligé d'accéder à ce domaine afin de prendre des décisions concrêtes concernant tous les comportements à incriminer, et leurs sanctions, se fait en fonction de l'impact négatif provoqué. ce n'était pas si facile "par rapport au infraction traditionnel", Par conséquent, cet accès en particulier a entraîné de nombreuses complications liées à la complicité du cyber espace, et en même temps le crime numérique lié a ce dernier.

Cependant, cette intrusion criminelle du législateur au domaine virtuel, avec toutes ses particularités et complexités juridiques de la référence technique moderne, rendait nécessaire une intervention législative procédurale, d'autant plus que cette dernière "partie procédurale" suit obligatoirement le coté objectif, concernant la nature, la composition et la confrontation, Partant de la règle de procédure fondamentale, le rôle du texte de procédure en général commence après l'achèvement du rôle du texte de fond, qui aurait dû être placé avant lui.

Dans le même contexte que celui mentionné ci-dessus, le législateur a affronté le champ virtuel du cyber espace, en tant que scène criminelle moderne dotée d'une grande confidentialité. Ce qui a favorisé le processus de privatisation procédurale non fondée. En ce qui concerne les procédures d'investigation et d'enquête, qui ont été mises en évidence dans un cadre différent "moderne", en général y compris les principaux organes d'assistance et de coopération, et en particulier les actions en matière de procédure menées par ces organes.

Grâce à cet accès procédural, la cybercriminalité est maintenant confrontée à de nombreuses dispositions procédurales liées à l'investigation et l'enquête, à laquelle nous sommes parvenus en ce qui concerne leur ouverture, selon lesquelles ils sont centrées sur la preuve numérique. Ce qui est accordé par les services compétents, après des directives principales et des procédures d'assistance "directives, Permis et ordonnances" peuvent être traditionnels ou récents. que nous avons conclus "les procédures d'investigation et d'enquête sur la cybercriminalité en vigueur", dans le cadre des conclusions et recommandations, indiquant que de nombreux éléments positifs doivent être renforcés, ainsi que de nombreux éléments négatifs, sont nécessaires pour éviter de la manière recommandée.

Abstract

It seems for the first glance that the virtual field created by cyber espace's elements, the computer and the internet, The positive useful impact for persons especially and for the society in general. As a result, it became probably possible for the reactor with these elements to get access to their virtual fields so as they could benefit and get benifited from it to an extreme possible limits. But that easy smooth access produced a negative impact over the time, which overrusing all limits.

With the increasing dangers and damage caused by persons "physical and mental" reactions with cyber espace's elements, it was compulsory for the legislator to access that field, in order to make implement decisions about criminilization and punishments, after discussing and selecting. Based on the negative ampact that it creates, it was not that easily connected to the traditional crime. Consequently, that access in particular carried a lot of complications based on the complicated privacy of cyber espace, and at the same time, cybercriminality linked by it.

However, this criminal access from the legislator to the virtual field, with all its particularities and legal complexities of modern technical reference, made procedural legislative intervention necessary, especially since the latter "procedural part" necessarily follows its objective counterpart, in terms of nature in the composition and confrontation. Proceeding from the fundamental rule of procedure, that the role of the procedural text in general, begins after the end of the role of the substantive text, which should have been placed before it.

In the same context mentioned above, the legislator faced the virtual Field of the cyber espace, as a modern criminal scene with a lot of modern privacy. Which established to prove the unfounded procedural privatization dealing. Especially, in terms of investigation procedures, which has been shown up in a different wai either its general framework, including the main assistive and cooperative bodies, or the procedural actions practised by these bodies.

Through this procedural access, the crimes of the cyber espace's are now confronted with many of the procedural provisions related to the investigation, which we have reached regarding their initiation, that they are centered on the digital evidence. Which is granted by the competent services, after direct substantive work and assistance. Framework, Permits and orders "traditional and recent" that we have concluded "the procedures for the investigation of cybercriminality in force", in terms of the findings and recommendations that they have many positives to be strengthened, as well as many negatives, which are necessary to avoid in the recommended ways.