جامعة محمد لمين دباغين – سطيف 2-

كلية الحقوق والعلوم السياسية

قسم الحقوق

محاضرات في مقياس الوقاية من الجرائم الإلكترونية

مطبوعة مقدمة لطلبة سنة ثانية ماستر

تخصص: إدارة إلكترونية وخدمات رقمية

د/ بطيحي نسمة

الموسم الجامعي: 2022/2021

مقدمة:

تعتبر أجهزة الحاسب الآلي وشبكات الإتصال من الإختراعات الهامة في تاريخ البشرية، وقد اتسع استخدامها ليشمل جميع المجالات الحياتية وكافة شرائح المجتمع، سواء كان ذلك في الدول المتقدمة أو النامية. وعلى الرغم من منافعها التي لا حصر لها، إلا أنها ساعدت في الوقت ذاته على انتشار أنواع جديدة من الجرائم، تُسمى بـ «جرائم تقنية المعلومات» أو «الجرائم الإلكترونية»، كما كان لها دور في ظهور نوع جديد من المجرمين بخصائص متميزة عَمَا أَلِفنَاهُ لدى المجرمين التقليديين.

وتعرف الجريمة الإلكترونية على أنها ذلك النشاط الإجرامي الذي يلجأ فيه الجاني إلى استخدام تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة، كأداة أو هدف لتحقيق الفعل الإجرامي المقصود[1].

والجرائم الإلكترونية على نوعان، (الأول) يتمثل في الجرائم الموجهة ضد جهاز الحاسب الآلي وأنظمة الإتصال، وهي الجرائم التي تعرف فقها بالجرائم المعلوماتية البحتة، كجريمة الدخول غير المشروع والتلاعب بالمعطيات ونشر الفيروسات، و(الثاني) يتمثل في الجرائم التي تكون فيها أنظمة الحاسب الآلي مجرد وسيلة في ارتكاب جرائم تقليدية، كالإحتيال لتحويل مبالغ مالية، السحب من الأرصدة في البنوك والمصارف أو التحويل من حساب إلى آخر، سرقة حقوق الملكية الفكرية والإستغلال الجنسي للأطفال، التجسس والتنصت على الأفراد ونحوها.

وقد أفرزت الجريمة الإلكترونية تحديات بارزة على الصعيد القانوني، لاسيما منه ما يتعلق بالقانون الجنائي، ذلك أن خصوصية هذه الجريمة وطبيعتها، التي يغلب عليها الطابع اللامادي، جعل من الصعب التعامل معها باللجوء إلى النصوص الجنائية التقليدية، مع ما قد يمثله ذلك من مساس بمبدأ شرعية الجرائم والعقوبات، ومبدأي التفسير الضيق للنصوص الجنائية وحظر القياس، كل هذه القيود دفعت المشرعين في الدول المختلفة إلى سن نصوص تجريمية جديدة تتوافق مع هذا النشاط الإجرامي الجديد.

---

[1] محمد الأمين البشـــرى، **التحقيق في الجرائم المســـتحدثة**، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004، ص 88.

لا تقتصر الصعوبات التي تطرحها الجريمة الإلكترونية على القوانين الجنائية الموضوعية فقط (قوانين التجريم والعقاب)، بل تمتد لتشمل القوانين الجنائية الإجرائية أيضا، هذه الأخيرة التي صِيغَت نصوصها لتكون أكثر انسجاما مع الجرائم التقليدية المعهودة، حيث أن الجهات الأمنية والقضائية تعودت على التعامل مع جرائم ترتكب في عالم مادي ملموس، كما يكون من اليسير البحث والتحقيق في شأنها، كونها تتضمن عناصر مرئية ملموسة تُدركُ بالحواس، كالبصمات أو قطرات من الدم أو آلة حادة ونحوها، بخلاف الجرائم الإلكترونية، التي تُقترف وتُنسَجُ خيوطها في مسرح افتراضي يختلف تماما عن مسرح الجريمة في حُلَتِهِ التقليدية، كما لا يُخلف مرتكبها أي آثار مادية تُذكر، الأمر الذي يجعل الهيئات الأمنية والقضائية عاجزة مُكَبَلَةَ الأيدي أمام هذه الوقائع غير المألوفة.

إن الوضع قد يزداد تأزما وتعقيدا بالنسبة للجهات الأمنية والقضائية، فيما لو تجاوزت آثار الجريمة الإلكترونية حدود الإقليم الوطني؛ إذ تصعب حينها مسألة إثباتها ونسبتها لمرتكبها، بسبب الإصطدام بمبدأ سيادة الدول ومبادئ الإختصاص القضائي المتعارف عليها.

وعلى إثر هذه العقبات والمشاكل القانونية التي طرحتها الجريمة الإلكترونية، كان من اللازم البحث عن آليات وطرق جديدة في الوقاية من هذه الجرائم ومكافحتها، بالشكل الذي يساعد في المحافظة على الدليل الرقمي وتعقب أثر المجرمين وتقديمهم للعدالة.

ويشمل المقرر ثلاث فصول رئيسة، تتمثل في:

فصل أول: إطار مفاهيمي حول إجراءات الوقاية من الجرائم الإلكترونية

فصل ثاني: إجراءات الوقاية من الجرائم الإلكترونية وضمانات المتهم

فصل ثالث: الآليات المؤسسات الوطنية وأحكام الإختصاص القضائي والتعاون الدولي في مجال الجريمة الإلكترونية

الفصل الأول

إطار مفاهيمي حول إجراءات الوقاية من الجرائم الإلكترونية ومكافحتها

أثارت الجريمة الإلكترونية العديد من المشاكل القانونية، الشيء الذي دفع تشريعات مختلف الدول إلى التدخل بوضع تنظيم قانوني يخصها، ليس فقط من خلال تجريمها وتقرير عقوبات لها، بل أيضا بوضع إجراءات خاصة في متابعتها جزائيا.

ندرس من خلال هذا المبحث **مشروعية الإجراءات الجزائية الخاصة بالجريمة الإلكترونية** في (المبحث الأول)، ثم **مجال تطبيق الإجراءات المحددة في القانون رقم 09-04** في (المبحث الثاني)، و**تصنيف الإجراءات الخاصة بالجريمة الإلكترونية** في (المبحث الثالث).

المبحث الأول: مشروعية الإجراءات الجزائية الخاصة بالجريمة الإلكترونية

عادة ما يتم التحري والتحقيق في جميع الجرائم باتخاذ إجراءات مُمَاثِلَة، غير أن اختلاف طرق ووسائل ارتكاب الجريمة والتوجه المتصاعد نحو اعتماد أدوات التكنولوجيا الحديثة، جعل مختلف التشريعات تعتمد تدابير وإجراءات خاصة لمواجهة الجريمة الإلكترونية وملاحقة مرتكبيها.

نتناول في (المطلب الأول) **خصـــوصـــية الجريمة الإلكترونية**، ثم في (المطلب الثاني) **الجدل الفقهي بشـــأن مشـــروعية الإجراءات الخاصـــة بالجريمة الإلكترونية**، وفي (المطلب الثالث) **حالات اللجوء إلى الإجراءات الخاصة بالجريمة الإلكترونية وضوابط استخدامها**.

المطلب الأول: خصوصية الجريمة الإلكترونية

إن تفرد الجريمة الإلكترونية بمميزات تختلف عما عهدناه في الجرائم الأخرى، دفع إلى التفكير بإجراءات جديدة تتناسب مع هذه الجريمة. نشرح ذلك من خلال التطرق إلى خصوصية الجريمة الإلكترونية، من حيث كونها **جريمة عابرة للحدود** (الفرع الأول)، أضف إلى أنها **تتجرد من الطبيعة المادية الملموسة** (الفرع الثاني).

الفرع الأول: البعد الدولي للجريمة الإلكترونية

تعد الجريمة الإلكترونية عابرة للحدود، كونها – غالبا – ما ترتكب في أماكن مختلفة من العالم باستخدام تقنيات حديثة، ما يؤدي إلى توزيع أركانها على عدة دول؛ إذ من المحتمل أن

ترتكب الجريمة في إقليم دولة معينة وتتحقق النتيجة الإجرامية في دولة أخرى، كمن يقوم بإرسال برنامج فيروسي من جهاز إلكتروني في دولة معينة إلى جهاز آخر في دولة ثانية مرورا بجهاز آخر في دولة ثالثة، وهنا تنشأ مشكلة البحث عن الأدلة الجنائية خارج دائرة إختصاص الدولة التي سُجِلَ فيها البلاغ وتم فيها تحريك الإجراءات الجنائية، كما تطرح أيضا مشاكل فحص البيانات في مراكز معلومات تابعة لدول أخرى، الأمر الذي يتطلب خضوع إجراءات التحقيق للقوانين السارية المفعول في تلك الدولة[1].

إن القوانين الجنائية السارية في الوقت الحالي وفي معظم دول العالم تأخذ بالطابع الإقليمي (مبدأ الإقليمية)، وهذا الأمر ليس بالمرونة الكافية لمواكبة حركة المعلوماتية والإتصالات التي غزت مختلف مناطق العالم، فمكان ارتكاب الجريمة لم يعد يلازم وقوع الفعل المادي أو أحد عناصره، كما هو عليه الحال بالنسبة للجرائم التقليدية، حتى أن البعض اتجه إلى حد نزع الصفة المادية عن هذا الفعل، على أساس ارتباط الجريمة الإلكترونية بالعالم الإفتراضي وكون التقنيات المستخدمة في ارتكابها لا تترك آثارا مادية ملموسة[2].

الفرع الثاني: الطابع غير المادي للجريمة الإلكترونية

تتميز الجريمة الإلكترونية بطابعها غير المادي، فهي تقع في بيئة افتراضية عبر نبضات وذبذبات إلكترونية رقمية غير مرئية، تُمحَى آثارها بمجرد نقرة بسيطة على لوحة المفاتيح وفي وقت وجيز قد يكون جزءا من الثانية، الأمر الذي يجعل أمر اكتشافها وإثباتها في غاية الصعوبة، لاسيما مع نقص الخبرة في أوساط رجال الضبطية القضائية وجهات التحقيق، فهي لا تترك شهودا يمكن الإستدلال بأقولهم ولا بصمات أو أدلة مادية بالإمكان تحليلها أو فحصها[3].

إن طابعها الخاص لا يقتصر على طريقة ارتكابها، بل حتى في الوسيلة المستعملة لذلك، فهي (أي الوسيلة المستعملة) تتسم بالطابع التقني الذي يضفي عليها جانبا كبيرا من التعقيد،

---

[1] محمد الأمين البشرى، المرجع السابق، ص 1.

[2] براهيمي جمال، **التحقيق الجنائي في الجرائم الإلكترونية**، أطروحة دكتوراه في العلوم، تخصص قانون، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2018، ص 188.

[3] بشـــان عبد النور، الجوانب الموضـــوعية لمعالجة الجريمة المعلوماتية، أطروحة دكتوراه، تخصـــص القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر 1، السنة الجامعية: 2017 – 2018، ص. ص (64 – 65).

حيث يعمد المجرم الإلكتروني إلى توظيف قدراته الفنية العالية ومعارفه الواسعة في مجال الإعلام الآلي والتكنولوجيا الحديثة في سبيل تحقيق جرمه، بالشكل الذي يحول دون اكتشاف أمره، فهذه الجريمة ترتكب بأسلوب هادئ ناعم عكس الجرائم التقليدية التي يغلب عليها العنف والقوة، فالواقع يؤكد لنا أن معظم هذه الجرائم الإلكترونية يتم اكتشافها بمحض الصدفة[1].

المطلب الثاني: الجدل الفقهي حول مشروعية إجراءات التحري والتحقيق الخاصة بالجريمة الإلكترونية

يُقصد بأساليب التحري والتحقيق الخاصة تلك العمليات والإجراءات والتقنيات التي تستعملها الجهات المختصة، تحت مراقبة وإشراف السلطة القضائية، بهدف البحث والتحري والتحقيق في الجرائم الخطيرة وجمع الأدلة عنها والكشف عن مرتكبيها، ويتم ذلك دون علم ورضا الأشخاص المعنيين[2]. ويعد من قبيل الإجراءات الخاصة في مجال الجرائم الإلكترونية التفتيش الإلكتروني، مراقبة الإتصالات الإلكترونية، التسرب الإلكتروني.

ويعتبر استخدام أساليب تحري وتحقيق خاصة بالجريمة الإلكترونية من المسائل الشائكة التي أثارت الجدل حول مشروعيتها، فهناك من رفض اللجوء إليها (الفرع الأول)، وهناك من أيد استخدامها (الفرع الثاني).

الفرع الأول: الإتجاه الرافض لاستخدام الإجراءات الخاصة بالجريمة الإلكترونية

ذهب رأي فقهي إلى رفض استخدام أساليب التحري والتحقيق الخاصة بالجريمة الإلكترونية، على أساس أنها، من جهة، وسائل غير مضمونة، لأنها لا تعكس دائما الحقيقة، نظرا لإمكانية تغيير أو حذف أي مقاطع أو صور عن بعضها البعض، أو على العكس من ذلك تركيبها بشكل يغير الحقيقة، وينطبق هذا القول على الصوت والصورة.

---

[1] بشان عبد النور، المرجع السابق، ص 66.

[2] شرف الدين وردة، **مشروعية أساليب التحري الخاصة في مكافحة الجريمة المعلوماتية** –في التشريع الجزائري –، مجلة المفكر، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، العدد 15، جوان 2017، ص 540.

كما أنها من جهة ثانية، تعد وسائل غير مشروعة، من باب أن نصوص الدستور تقضي بأنه لا يجوز انتهاك حرمة حياة المواطن الخاصة وسرية المراسلات والإتصالات الخاصة، وكذلك تعاقب نصوص قانون العقوبات على المساس بحرمة الحياة الخاصة للمواطن.

الفرع الثاني: الإتجاه المؤيد لاستخدام الإجراءات الخاصة بالجريمة الإلكترونية

ذهب اتجاه آخر إلى أنه لابأس من استخدام الإجراءات الجزائية الخاصة بالجريمة الإلكترونية ترجيحا للمصلحة العامة، التي تقتضي استخدام وسائل ناجعة وفعالة تتناسب مع التغيرات والمنحى الخطير لمستوى الإجرام الحديث، الذي تعد الجريمة الإلكترونية أحد أشكاله، خاصة وأن المجرم بحد ذاته قد غير من أساليب وطرق تنفيذ جريمته، فمن غير المنطقي مثلا أن تلجأ الجماعات الإرهابية إلى التطبيقات الحديثة كالميسنجر والفيبر وشبكات التواصل الاجتماعي من أجل تجنيد الشباب في الجماعات الإرهابية المتطرفة ونقول نحن بأن وضع هذه الوسائل تحت المراقبة لغرض تقفي أثر هذه الجرائم أمر غير مشروع، إذ لابد من أن تتماشى وتتطور أساليب التحري والتحقيق عن الجرائم مع واقع الإجرام الحديث[1].

بين هذا الرأي وذاك، ذهبت مختلف التشريعات إلى الأخذ بالرأي الثاني، حيث تسود الآن موجة في مختلف دول العالم لإصلاح التشريعات الجنائية، لاسيما الإجرائية منها، لكي تساير التطورات والتغيرات المتسارعة في جرائم تقنية المعلومات، وهو الأمر الذي سار على نهجه المشرع الجزائري، من خلال سنه للقانون رقم 09-04 المؤرخ في5 أوت 2009 والمتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال[2].

---

[1] فيما يخص الجدل الفقهي حول مشروعية هذه الأساليب، لاسيما منه ما يتعلق باعتراض المراسلات وتسجيل الأصوات والمراقبة الإلكترونية. راجع، شرف الدين وردة، المرجع السابق، ص. ص (552 -553).

[2] القانون رقم 09-04 المؤرخ في5 أوت 2009 والمتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، (ج. ر: عدد 47، بتاريخ 16 غشت 2009، ص5).

- وقد جاء في الأعمال التحضيرية لهذا القانون، أن الدافع إلى سن هذا النص يعود في المقام الأول إلى ما يشهده العالم من تطور غير مسبوق في مجال المعلوماتية والإتصال، الأمر الذي أدى إلى زيادة استخدام التقنيات التكنولوجية الحديثة من طرف الأشخاص الطبيعية والمعنوية على حد سواء في جميع المجالات، كما أن هذا التطور أدى إلى بروز مجال جديد للإتصال يتمثل في العالم الإفتراضي، الذي يتم من خلاله نقل المعلومات الرقمية وتُجرَى بواسطته جميع أشكال المعاملات والخدمات الإلكترونية، بالطريقة التي جعلت من غير الممكن على السلطات العامة التحكم فيه بطرق الرقابة التقليدية. راجع:

المطلب الثالث: حالات اللجوء إلى الإجراءات الخاصة بالجريمة الإلكترونية وضوابط استخدامها

جاء في المادة 15 من اتفاقية بودابست أنه لابد على الدول الأطراف عند تطبيق النصوص الإجرائية المتعلقة بالتحقيق في الجرائم الإلكترونية وجمع أدلتها بالخضوع إلى الشروط والضمانات المتعلقة بحقوق الإنسان والحريات العامة، كذلك أكد المشرع الجزائري على أن إجراءات التحري والتحقيق الخاصة بالجريمة الإلكترونية لا تُتَخذ إلا في حالات معينة، وبناء على شروط وضوابط معينة.

نتناول في (الفرع الأول) **حالات اللجوء على الإجراءات الخاصة بالجريمة الإلكترونية**، ثم **ضوابط استخدام الإجراءات الخاصة بالجريمة الإلكترونية في** (الفرع الثاني).

الفرع الأول: حالات اللجوء إلى الإجراءات الخاصة بالجريمة الإلكترونية

ورد في المادة الثالثة (3) من القانون رقم 09-04 أنه: ((مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والإتصالات يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الإتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية))

يُفهم من نص المادة أعلاه، أن المشرع الجزائري قيد مشروعية الإجراءات الخطيرة (إجراءي المراقبة الإلكترونية والتفتيش الإلكتروني) بحالات الضرورة التي تتطلبها عملية التحري والتحقيق في الجرائم الإلكترونية، وتتمثل هذه الحالات فـي:

أولا: بصفة أساسية في الجرائم الإلكترونية الخطيرة

ويتعلق الأمر بصفة خاصة فيما لو امتد أثر الجرائم الإلكترونية ليهدد النظام العام والأمن الوطنيين، كالجريمة الإرهابية مثلا، وَكَيْ لا يتم تفويت الفرصة أمام الجهات الأمنية والقضائية في تحصيل المعلومات التي تساعد في مجريات التحقيق. وقد أكد المشرع الجزائري هذا الأمر،

مجلس الأمة، **الجريدة الرسمية للمداولات**، الفترة التشريعية الثانية، السنة السادسة، الدورة الربيعية، 2009، العدد 6، ص. ص (3 – 4).

حينما سمح في المادة الرابعة (4) من القانون رقم 09-04 بمراقبة الاتصالات الإلكترونية للمتهم، غير أنه قيد اتخاذ هذا الإجراء بحالات معينة.

ثانيا: بصفة احتياطية في الجرائم الإلكترونية العادية

سمح المشرع الجزائري للجهات المختصة باللجوء إلى إجراءي التفتيش الإلكتروني وإجراء المراقبة الإلكترونية، على الرغم من خطورتهما على الحريات العامة وخصوصيات الأفراد، في غير الجرائم الإلكترونية الخطيرة، عندما تتطلب عملية التحري والتحقيق اللجوء إليهما، ويتحقق ذلك في الحالات التي تكون فيها وسائل الإثبات العادية غير كافية في نسبة التهمة إلى المتهم، فعندما يكون اللجوء مثلا إلى المعاينة أو شهادة الشهود أو الإستجواب أو المواجهة غير كاف في فهم ملابسات الجريمة والتعرف على مرتكب الجريمة، أي بمفهوم المخالفة أنه ليس هناك داع للمخاطرة بإجراء الرقابة الإلكترونية أو التفتيش الإلكتروني في حالة كفاية الطرق التقليدية العادية.

الفرع الثاني: ضوابط استخدام الإجراءات الخاصة بالجريمة الإلكترونية

يعد إجراءي التفتيش الإلكتروني والرقابة الإلكترونية من الإجراءات الخطيرة على الحريات الفردية، فالمحقق الذي يقوم بتفتيش النظام المعلوماتي أو قواعد بياناته مثلا قد يتجاوز النظام المعلوماتي للمتهم إلى أنظمة أخرى متصلة به، وهو الشيء الذي قد يؤدي إلى الإطلاع على ملفات ومعلومات سرية تتعلق بأشخاص لا علاقة لهم بالجريمة، ولذلك فإن هذه الإجراءات لا تُتَخذ إلا بمراعاة ضوابط قانونية، وعدم التقيد بهذه الضوابط ينجم عنه عدم صحة الدليل المستخلص منها ومن ثمة بطلانه.

وقد قام المشرع الجزائري بوضع أحكام دقيقة ومفصلة تتعلق بهذه الإجراءات الخاصة، سواء في قانون الإجراءات الجزائية أو في القانون رقم 09-04 المتعلق بالوقاية من الجرائم الإلكترونية، وعلى القائمين بالتحري والتحقيق الإلتزام بها، كتحديده للسلطة القضائية التي تأذن باتخاذ هذه الإجراءات، تحديد مدة القيام بها، نطاق الجرائم التي تُتَخَذ بشأنها، ضرورة الحفاظ على السر المهني، العقوبات الجزائية والتأديبية التي يتعرض لها مُنَفِذُوا هذا الإجراء على فرض مخالفتهم للإجراءات القانونية ونحوها[1].

[1] شرف الدين وردة، المرجع السابق، ص 555.

المبحث الثاني: مجال تطبيق الإجراءات المحددة في القانون رقم09-04

إن الأحكام الإجرائية الخاصة التي جاء بها القانون رقم 09-04 تتعلق بالجريمة الإلكترونية، وهو ما أكده المشرع الجزائري في المادة الأولى (1) من ذات القانون، التي تنص على أنه: ((يهدف هذا القانون إلى وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها)).

والحقيقة، أنه ليس هناك تعريف دقيق وجامع بشأن الجريمة الإلكترونية، فهناك اتجاه فقهي يركز في تعريفه للجريمة الإلكترونية على أداة ارتكاب الجريمة، ويتجه إلى القول أن السلوك الإجرامي يعد من قبيل الجرائم الإلكترونية إذا استخدم النظام المعلوماتي كوسيلة رئيسية في اقترافه، واتجاه آخر ركز في تعريفه لهذه الجريمة على محلها، بالقول أنها ذلك الفعل الإجرامي الذي يستهدف من خلاله الجاني المعطيات المعلوماتية، حيث يلجأ إلى نسخها أو تعديلها أو حذفها أو الوصول إلى المعلومات المخزنة في النظام المعلوماتي. في حين ذهب اتجاه ثالث إلى اعتماد معيار شخصي محض في تعريفه للجريمة الإلكترونية، حيث ذهبوا إلى القول أن الجريمة الإلكترونية هي ذلك الفعل الذي يكون فيه الجاني مُلِما بتقنية المعلومات ونظم الحاسب الآلي[1].

لذلك وجد المشرع الجزائري نفسه مضطرا إلى التدخل بتحديد مفهوم الجريمة الإلكترونية التي تسري عليها الأحكام الإجرائية الخاصة التي جاءت بالقانون رقم 09-04، وقد كان ذلك تحديدا في المادة الثانية (2) من ذات القانون (المطلب الأول)، غير أن ما ينبغي التأكيد عليه أن بعضا من الأحكام التي جاء بها القانون رقم 09-04 لا يمكن تطبيقها إلا بصدد جرائم إلكترونية محددة (المطلب الثاني).

المطلب الأول: الجرائم الإلكترونية بمفهوم القانون رقم 09-04

إن الإجراءات النوعية المحددة في القانون رقم 09-04 المتعلق بالوقاية من الجرائم الإلكترونية ومكافحتها مقررة لمقتضيات التحري والتحقيق في الجرائم الإلكترونية بمفهوم هذا

[1] يعيش تمام شوقي، الجريمة المعلوماتية، (دراسة تاصيلية مقارنة)، الطبعة الأولى، مطبعة الرمال، الوادي، الجزائر، 2019، ص. ص (18 – 22).

القانون. ويقصد بالجرائم الإلكترونية[1]، على حسب ما جاء بالمادة الثانية بند(أ) من القانون رقم 09-04: ((جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية)).

وقد شمل هذا التعريف ثلاث أصناف من الجرائم، تدخل كلها في مفهوم الجريمة الإلكترونية بمفهومها الإجرائي، وهي:

الفرع الأول: جرائم المساس بأنظمة المعالجة الآلية للمعطيات

وهي الجرائم التي نظم المشرع الجزائري أحكامها في القسم السابع مكرر في قانون العقوبات، والتي يطلق عليها فقها بـ (الجرائم المعلوماتية البحتة)، في هذا النوع من الجرائم يكون النظام المعلوماتي في حد ذاته هدفا للمجرم، وتتمثل في:

- جريمة الدخول أو البقاء داخل النظام المعلوماتي، التي عاقب عليها المشرع الجزائري في المادة 394 مكرر من ق ع، وتعد أهم جريمة إلكترونية، على أساس أن الدخول إلى النظام المعلوماتي يكون عادة هو الخطوة الأساسية والأولى في ارتكاب باقي الجرائم الإلكترونية؛

- جرائم المساس بمعطيات النظام المعلوماتي، التي جرمها المشرع الجزائري في المادة 394 مكرر1 من ق ع، وهي تلك الجرائم التي تطال المعطيات المعلوماتية، ويكون من شأنها إحداث تغيير في وضعية النظام المعلوماتي (إما بالإدخال، التعديل أو الإزالة)، ومن ثمة الإضرار به؛

- جريمة إساءة استخدام معطيات النظام المعلوماتي، وقد جرمها المشرع الجزائري في المادة 394 مكرر2 من ق ع، كفعل تصميم البرامج الخبيثة وحيازة كلمات المرور وأدوات القرصنة.

الفرع الثاني: الجرائم التي ترتكب بواسطة منظومة معلوماتية

هي الجرائم التي تستغل الأنظمة المعلوماتية فيها كأدة لارتكاب جرائم تقليدية، بحيث لا تقع الجريمة على جهاز الحاسب الآلي ذاته، أو برامجه ونظمه، ولكنها ترتكب من خلال الإستعانة

[1] استعمل المشرع الجزائري مصطلح **الجرائم المتصلة بتكنولوجيا الإعلام والإتصال** للتعبير عن الجرائم الإلكترونية، والأدق هو عبارة (الجرائم المتصلة بتكنولوجيا المعلوماتية والإتصال).

به كوسيلة في تنفيذها، كعمليات الإستيلاء على الأموال التي تتم من خلال تحويلات إلكترونية غير مشروعة عبر البنوك أو الإستيلاء على أرقام بطاقات الإئتمان.

الفرع الثالث: الجرائم التي يسهل ارتكابها بواسطة منظومة معلوماتية

يتعلق الأمر هنا بالجرائم التي لا تمثل فيها الأداة المعلوماتية سِوَى أداة مُسهلة في ارتكابها، أي بمعنى أن الإجراءات المحددة بالقانون رقم 09-04 تُعد في هذه الحالة وسيلة في جمع الدليل الذي يثبت وقوع الجريمة ونِسبتها إلى مرتكبها. ففي جريمة القتل مثلا، يمكن للجهات القضائية المختصة أن تطلب من مزودي خدمة الأنترنت الإحتفاظ بمعطيات حركة السير التي تمكن من التعرف على معلومات تتعلق باتصالات معينة (مصدر الإتصال ومُنتهَاهُ) التي أُجريت خلال فترة محددة، وهو الأمر الذي قد يكون مفيدا في تحديد هوية الجناة، فجريمة القتل هي جريمة عادية، وبالإمكان اللجوء إلى بعض الإجراءات المحددة بالقانون رقم 09-04، (عملية حفظ معطيات حركة السير كما في المثال) لتحصيل الدليل الإلكتروني.

بذلك، نخلص إلى القول أن:

- التعريف الذي جاء به المشرع الجزائري فيما يخص الجريمة الإلكترونية، **تعريف واسع** يشمل أي جريمة تستهدف النظام المعلوماتي، ويكون هذا الأخير إما هدفا لها أو وسيلة في ارتكابها (الصنف الأول والثاني)، وتكون في هذه الحالة الإجراءات المحددة بالقانون رقم 09-04 هي الوسيلة الأفضل في تحصيل الدليل الذي يثبتها، كونها من ذات الطبيعة (الطبيعة التقنية) التي ارتكبت بها، كما يشمل التعريف أيضا أي جريمة عادية يكون من المفيد اللجوء إلى الإجراءات المحددة بالقانون رقم 09-04 لتحصيل الدليل الجنائي الذي يثبتها(الصنف الثالث).

- أن التعريف الذي جاء به المشرع الجزائري ينبغي أن **يُحمل مَحْمَلا ضيقا**، يقتصر على القانون رقم 09-04، بدليل أن المشرع الجزائري نص في المادة الثانية (2) من ذات القانون أنه: ((يقصد بمفهوم هذا القانون ...)).

المطلب الثاني: تضييق مجال تطبيق بعض الإجراءات الواردة في القانون رقم 09-04

إن المفهوم الذي جاء به المشرع الجزائري فيما يخص الجريمة الإلكترونية مفهوم واسع جدا، الأمر الذي يؤدي إلى بَسْطْ تطبيق الإجراءات المحددة بالقانون رقم 09-04، على أي

جريمة جنائية، يمكن أن يكون اللجوء فيها إلى هذه الإجراءات مُساعدا للجهات الأمنية والقضائية في تحصيل الدليل الذي يُثْبِتُها.

بالمقابل، فإن بعضا من الإجراءات المحددة بالقانون رقم 09-04، من الخطورة بمكان، لذلك فإنه لا يمكن بأي حال من الأحوال السماح باتخاذها بصدد أي جريمة جنائية، لذلك أكد المشرع الجزائري، في المادة الرابعة (4) من القانون رقم 09-04 على حالات اللجوء إلى إجراء الرقابة الإلكترونية للمحادثات الشفوية، فهذا الإجراء خطير جدا على الحريات الفردية ويمثل خرقا لسرية الإتصالات الإلكترونية المكفول دستوريا، لذلك لا يسمح باتخاذه في جميع الجرائم الإلكترونية بالمفهوم الوارد بالمادة الثانية (2) من القانون رقم 09-04 أعلاه، فهو لا يُتَخذ – إجمالا – إلا في الجرائم الإلكترونية الخطيرة (الجرائم الإرهابية والتخريبية والجرائم الماسة بالأمن الوطني).

المبحث الثالث: أنواع الإجراءات الجزائية الخاصة بالجرائم الإلكترونية

يُقسم الفقه عادة الإجراءات الجزائية المتعلقة بالجريمة الإلكترونية إلى قسمين؛ **الإجراءات الجزائية الحديثة الخاصة بالجريمة الإلكترونية**، نتناولها في (المطلب الأول)، و**الإجراءات الجزائية التقليدية الخاصة بالجريمة الإلكترونية**، نخصص لها (المطلب الثاني).

المطلب الأول: الإجراءات الجزائية الحديثة الخاصة بالجريمة الإلكترونية

تبنت التشريعات المختلفة إجراءات حديثة مستقلة وقائمة بذاتها ليس لها مثيل في القوانين الإجرائية التقليدية، وتختلف هذه الإجراءات على حسب طبيعة البيانات الإلكترونية في البيئة الرقمية؛ ما إذا كانت بيانات ساكنة أو متحركة. وتقسم الإجراءات الحديثة المتعلقة بالجريمة الإلكترونية إلى **إجراءات متعلقة بالبيانات الساكنة** (الفرع الأول)، **وإجراءات تخص البيانات المتحركة** (الفرع الثاني).

الفرع الأول: الإجراءات الجزائية المتعلقة بالبيانات الإلكترونية الساكنة

تتمثل الإجراءات الخاصة بالبيانات الساكنة في **إجراء التحفظ العاجل على هذه البيانات(أولا)، والأمر بتقديم بيانات إلكترونية متعلقة بالمشترك(ثانيا).**

أولا: إجراء التحفظ العاجل على البيانات المخزنة

يقصد بالتحفظ العاجل على البيانات قيام السلطة المختصة بتوجيه أمر إلى مزودي خدمة الأنترنت بالتحفظ على البيانات التي لديهم، ريثما يتم القيام بإجراءات قانونية أخرى كالتفتيش مثلا، فالهدف من هذا الإجراء إذا هو الإحتفاظ بالبيانات قبل محوها أو شطبها، سواء من طرف المتهم أو مزود الخدمة، فمثلا قد يصل إلى علم رجال الشرطة القضائية وجود صور دعارة للأطفال في اليوم الأول، ويقومون بإجراءات طلب الحصول على إذن بالتفتيش في اليوم الثاني، ويحصلون على الإذن في اليوم الثالث، وبعدها يصل إلى علمهم أن مزود خدمة الأنترنت قام بشطب هذه البيانات، فهنا تظهر أهمية هذا الإجراء في كونه إجراء مؤقتا يحول دون محو البيانات في التحقيقات القضائية الطويلة نسبيا[1].

ثانيا: الأمر بتقديم بيانات إلكترونية تتعلق بالمشترك

تلزم التشريعات المختلفة مزودي خدمة الأنترنت بتقديم ما بحوزتهم من بيانات تتعلق بالمشتركين، وقد ورد ذلك في المادة العاشرة (10) من القانون رقم 09-04 المتعلق بالوقاية من الجرائم الإلكترونية، التي ألزم من خلالها المشرع الجزائري مزود خدمة الأنترنت بالتعاون مع السلطات القضائية وتزويدهم بالمعلومات الخاصة بهوية مستخدمي شبكة الأنترنت، ومن شأن هذه المعلومات أن تفيد الجهات القضائية المختصة في التعرف على هوية الجناة.

الفرع الثاني: الإجراءات الجزائية المتعلقة بالبيانات الإلكترونية المتحركة

تتعلق الإجراءات المتعلقة بالبيانات المتحركة في إجراء اعتراض الإتصالات الإلكترونية الخاصة، ويقصد بهذا الإجراء مراقبة الإتصالات الإلكترونية أثناء بثها أي في الزمن الفعلي لنقلها بين أطراف الإتصال.

وقد حدد المشرع الجزائري أحكام هذا الإجراء في المادة الرابعة (4) من القانون رقم 09-04 المتعلق بالوقاية من الجرائم الإلكترونية.

[1] عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، (دراسة مقارنة)، رسالة ماجستير، كلية الحقوق، جامعة الإسكندرية، 2009، ص. ص (100-101).

المطلب الثاني: الإجراءات الجزائية التقليدية الخاصة بالجريمة الإلكترونية

تقسم الإجراءات التقليدية إلى إجراءات مادية وهي المعاينة والتفتيش وحجز الأشياء، وإجراءات شخصية، وتتمثل في التسرب، الشهادة والخبرة واستجواب المتهم. وتستخدم هذه الإجراءات التقليدية بصفة عامة في التحري والتحقيق في جميع الجرائم، بما فيها الجرائم الإلكترونية، غير أن بعضا من هذه الإجراءات قد تكون بحاجة إلى تطوير فيما يخص الجريمة الإلكترونية، لكي تتناسب مع طبيعتها الخاصة.

من أجل ذلك، عمل المشرع الجزائري على إضافة مجموعة من الأحكام الإجرائية إلى بعض الإجراءات التقليدية، هذه الأحكام المُضافة تعتبر أكثر انسجاما مع طبيعة الجريمة الإلكترونية، سواء كان ذلك في القانون رقم 09-04 أو في قانون الإجراءات الجزائية.

الفرع الأول: بالنسبة للأحكام الإجرائية العامة في القانون رقم 09-04

لم يكتف المشرع الجزائري وغيره من التشريعات المقارنة، بالأحكام المتعلقة بالتفتيش والحجز التي جاءت في قانون الإجراءات الجزائية، بل وضع أحكاما خاصة تتعلق بالتفتيش الإلكتروني والحجز الإلكتروني، كون أن الجريمة الإلكترونية تقع في محيط افتراضي غير مرئي، الأمر الذي يجعل بعض أحكام التفتيش والحجز التقليدي غير منسجمة مع طبيعة هذه الجريمة.

الفرع الثاني: بالنسبة للأحكام الإجرائية العامة في قانون الإجراءات الجزائية

تجسدت خصوصية الجريمة الإلكترونية من حيث الأحكام الإجرائية التي تطبق عليها في قانون الإجراءات الجزائية، نذكر من بينها:

أولا: الإجراءات الخاصة بالإختصاص بالنسبة للقضاء الجزائي والضبطية القضائية

نميز بين اختصاص القضاء الجزائي واختصاص الشرطة القضائية.

1) أحكام الإختصاص بالنسبة للقضاء الجزائي:

الأصل أن الإختصاص الإقليمي للمحكمة يتحدد بالمكان الذي تقع فيه الجريمة أو مكان القبض على الشخص محل المتابعة أو بمحل إقامته، سواء بالنسبة لوكيل الجمهورية (المادة 37-1 من ق إ ج)، أو قاضي التحقيق (المادة 40-1 من ق إ ج)، أو قاضي الحكم (المادة

329 من ق إ ج). إلا أن المشرع الجزائري، ولغرض تسهيل عمل الجهاز القضائي، استحدث في مجال الإختصاص ما يُسمى بـ (الأقطاب المتخصصة) أو (المحاكم ذات الإختصاص الموسع)، بموجب القانون رقم 04-14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون الإجراءات الجزائية، لمكافحة بعض الجرائم الخطيرة[1]، ومن بينها جرائم المعالجة الآلية للمعطيات، المجرمة في القسم السابع مكرر من ق ع.

لاحقا قام المشرع الجزائري باستحداث قطب جزائي مستقل خاص بالجرائم الإلكترونية، بموجب الأمر رقم 21-11 المؤرخ في 2021/8/25[2].

2) أحكام الإختصاص بالنسبة للشرطة القضائية:

ينعقد اختصاص ضباط الشرطة القضائية في الجرائم العادية في الدائرة الإقليمية التي يباشرون فيها مهامهم المعتادة، وضابط هذا الإختصاص يكون بمكان ارتكاب الجريمة أو إقامة أحد المشتبه فيهم أو بمكان القبض عليه، لكن المشرع الجزائري وسع في المادة 16 من ق إ ج الإختصاص الإقليمي لرجال الضبطية القضائية إلى كافة التراب الوطني في بحث ومعاينة الأنواع الستة للجرائم الخطيرة، التي من بينها جرائم المعالجة الآلية للمعطيات.

ثانيا: الإجراءات الجزائية المستحدثة في مواجهة الجرائم الخطيرة

تسمى هذه الإجراءات عادة بـ "أساليب التحري الخاصة"، وقد استحدثها المشرع الجزائري على إثر تعديله لقانون الإجراءات الجزائية، بموجب القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المعدل لقانون الإجراءات الجزائية[3]، تماشيا مع التطور المتسارع الذي تعرفه الجريمة في مجتمعنا، وفي إطار المكافحة الإجرائية لهذا النوع من الإجرام.

---

[1] القانون رقم 04 – 14 المؤرخ في 10 نوفمبر 2004، يُعدِل ويتمم الأمر رقم 66 – 155، المتضـــمن قانون الإجراءات الجزائية، (ج ر: عدد 71، بتاريخ 10 نوفمبر 2004، ص4).

_ يتعلق الأمر بجرائم المخدرات والإرهاب وتبييض الأموال وجرائم الصـرف، بالإضـافة إلى جرائم الفسـاد التي أُضِـيفت إلى القائمة بموجب قانون الوقاية من الفساد ومكافحته، عند تعديله بالأمر رقم 05-10 بتاريخ 26 غشت 2010.

[2] الأمر رقم 21 – 11 المؤرخ في 25 غشـــت 2021، يُتمم الأمر رقم 66 – 155 المؤرخ في 8 يونيو 1966 المتضمن قانون الإجراءات الجزائية. (ج ر: عدد 65، بتاريخ 26 غشت 2021، ص 7).

[3] القانون رقم 06-22 المؤرخ في 20 ديسـمبر 2006، المعدل والمتمم للأمر 155/66 المتضـمن قانون الإجراءات الجزائية. (ج ر: 84، بتاريخ 24 ديسمبر 2006، ص 4).

وتتمثل في ثلاث صور، هـي:

1) مراقبة الأشخاص والأشياء والأموال: (المادة 16 مكرر من ق إج)

يقصد بهذا الإجراء وضع شخص أو وسائل نقل أو أماكن أو مواد تحت رقابة سرية ودورية بغرض الحصول على معلومات لها علاقة بالشخص المشتبه فيه أو بأمواله أو بالنشاط الذي يقوم به. وهي عبارة عن عملية أمنية يقوم بها ضباط الشرطة القضائية عبر كامل التراب الوطني بهدف البحث والتحري المباشر على الأشخاص الذين يوجد ضدهم مبرر مقبول أو أكثر يحمل على الإشتباه في ارتكاب أو محاولة ارتكاب إحدى الجرائم الخطيرة أو نقل أشياء أو أموال أو متحصلات من ارتكاب هذه الجرائم أو قد تستعمل في ارتكابها[1].

2) اعتراض المراسلات وتسجيل الأصوات والتقاط الصور:

يقصد **باعتراض المراسلات** عملية مراقبة سرية المراسلات السلكية واللاسلكية في إطار البحث والتحري عن الجريمة وجمع الأدلة أو المعلومات حول الأشخاص المشتبه في ارتكابهم للجريمة أو مشاركتهم فيها[2]. ويطلق على هذا الإجراء تسميات أخرى في الفقه كمصطلح التنصت الهاتفي (écoutes téléphoniques) واعتراض المكالمات الهاتفية (interception des conversations téléphoniques)[3].

ويقصد **بتسجيل الأصوات** مراقبة المحادثات الشفوية التي يتحدث بها الأشخاص بصفة سرية أو خاصة، وفي مكان عام أو خاص، عن طريق التقاطها أو نقلها أو تسجيلها. أو أنه الإستماع خلسة للأحاديث دون علم صاحبها، بواسطة أجهزة إلكترونية[4].

كما يقصد **بالتقاط الصور** القيام بالتصوير الخفي لشخص أو عدة أشخاص يتواجدون في مكان خاص، كوضع ميكروفون في منزل المتهم أو مكتبه أو سيارته أو أي مكان يتردد عليه

---

[1] عبد الرحمان خلفي، **الإجراءات الجزائية في التشريع الجزائري والمقارن**، الطبعة الرابعة، دار بلقيس، الجزائر 2019، ص. ص(9 – 99).

[2] المرجع نفسه، ص 100.

[3] روابح فريد، **الأســاليب الإجرائية الخاصــة للتحري والتحقيق في الجريمة المنظمة**، أطروحة دكتوراه، القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة بن يوسف بن خدة، الجزائر 1، 2016، ص 302.

[4] المرجع نفسه، ص. ص (273 – 274).

المشتبه فيه وحتى باستعمال التلفون المحمول الذي باستطاعته تسجيل الصوت والصورة على نحو مُتَنَاهٍ في الدقة[1].

3) التسرب:

عرفت المادة 65 مكرر12 من ق إ ج التسرب على أنه (قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بايهامهم أنه فاعل معهم أو شريك لهم أو خاف)، فهو إذا عملية أمنية تسمح لضابط الشرطة القضائية بالتوغل داخل جماعة إجرامية بالشكل الذي يجعله يتقرب إليهم وذلك لغرض مراقبة تحركات أفراد هذه الجماعة قبل أو خلال قيامهم بالعمل الإجرامي[2].

ويمكن تصور عملية التسرب في الجرائم الإلكترونية في دخول ضابط أو عون الشرطة القضائية إلى البيئة الإفتراضية ومشاركته في محادثات غرف الدردشة أو انخراطه في مجموعات أو نوادي الهاكر مستخدما في ذلك أسماء وهيئات مستعارة، ظاهرا فيها بمظهر يوحي بأنه واحد من أعضاء المجموعة، قصد استدراجهم والكشف عن أفعالهم الإجرامية[3].

ثالثا: بين ما جاء به المشرع الجزائري من أحكام إجرائية خاصة بالجريمة الإلكترونية في قانون الإجراءات الجزائية والقانون رقم 09-04 المتعلق بالوقاية من الجرائم الإلكترونية، لابد من **إبداء الملاحظات التالية:**

1) إن ما جاء به المشرع الجزائري من أحكام بموجب القانون رقم 09-04 هي **أحكام مكملة** لما هو مقرر في قانون الإجراءات الجزائية، وجاءت لغرض سد الفراغ القانوني الموجود في قانون الإجراءات الجزائية، هذا الأخير الذي تعد أحكامه أكثر انسجاما مع الأشياء المادية دون الأشياء المعنوية كالمعلومات. ووجود القانون رقم 09-04 الخاص بالجرائم الإلكترونية ليس معناه استبعاد قانون الإجراءات الجزائية تماما من مجال تطبيق الجرائم الإلكترونية، بالشكل الذي يكون فيه لدينا

---

[1] عبد الرحمان خلفي، المرجع السابق، ص 101.

[2] المرجع نفسه، ص 104.

[3] عبير بعقيقي، **الإثبات في الجرائم المعلوماتية على ضوء القانون 09-04**، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمى لخضر، الوادي، الجزائر، المجلد 9، العدد2، جوان 2018، ص 43.

قانون إجرائي متعلق بالجرائم التقليدية وقانون إجرائي خاص بالجريمة الإلكترونية، حيث يطبق كلا منهما جنبا إلى جنب في علاقة تكاملية ذات هدف واحد هو مكافحة الجرائم الإلكترونية[1].

2) أن خطورة الجريمة الإلكترونية وما ينجر عنها من نتائج وخيمة، خاصة فيما لو استغلت الأنظمة المعلوماتية كوسيلة للمساس بأمن الدولة واستقرارها، دفع المشرع الجزائري إلى الترخيص باتخاذ **بعض الإجراءات كتدابير وقائية** من شأنها توفير المعلومات الأولية عن الجرائم الإلكترونية قبل وقوعها، كإجراء الرقابة الإلكترونية وإجراء التفتيش الإلكتروني، حيث جاء في المادة الأولى (1) من القانون رقم 09-04 أنه: ((يهدف هذا القانون إلى وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها)).

الفصل الثاني

إجراءات الوقاية من الجرائم الإلكترونية وضمانات المتهم فيها

أصبحت الإجراءات التقليدية للتحري والتحقيق غير كافية لمواجهة الجرائم الخطيرة والمعقدة كالجرائم الإلكترونية، كونها إجراءات لا تتوافق مع مسرح الجريمة الإلكتروني ومع فطنة ودهاء ما أصبح يُعرف بالمجرم المعلوماتي، الأمر الذي جعل المشرعين في الدول المختلفة، بما في ذلك المشرع الجزائري، يَضعون إجراءات جديدة تتوافق مع طبيعة الجريمة الإلكترونية، كالتسرب الإلكتروني، التفتيش الإلكتروني، وأيضا المراقبة الإلكترونية.

غير أن ما تُسبِبُه هذه الإجراءات الحديثة من إعتداء صارخ على خصوصيات الأفراد وسرية إتصالاتهم ومراسلاتهم وبياناتهم الشخصية، خاصة وأنها تقوم على التنصت والمراقبة السرية دون علم المعني ودون رضائه، دفع التشريعات المختلفة إلى تقييد استعمال هذه الإجراءات بشروط وضوابط معينة، كي لا يُساء استخدامها في غير أغراضها المشروعة التي وُجِدت لأجلها.

---

[1] في ذات السياق، توصل مشروع توصيات وقرارات المؤتمر الدولي الثامن عشر التحضيري للقانون الجنائي سنة 2008، في القسم الثالث الذي يحمل عنوان (التدابير الإجرائية الخاصة واحترام حقوق الإنسان)، أنه في حالات كثيرة تكون النصوص الإجرائية العادية كافية لمواجهة النشاطات الإجرامية الحديثة، أي بمعنى أنه لا يمكن الإستهانة بنجاعة الإجراءات التقليدية، كما أن التشريعات لم تستغن عنها بل قامت بتعزيزها من خلال توسيع نطاقها بما يتلاءم وطبيعة الإجرام الحديث وخصوصيته. روابح فريد، المرجع السابق، ص 99.

نعالج من خلال (المبحث الأول) **إجراء الرقابة الإلكترونية وضمانات المتهم فيه**، ثم **إجراء التفتيش الإلكتروني** في (المبحث الثاني)، و**إجراء الحجز الإلكتروني** في (المبحث الثالث)، وفي (المبحث الرابع) نبحث في **التزامات مقدمي خدمات الأنترنت**.

المبحث الأول: مراقبة الإتصالات الإلكترونية

تبنى المشرع الجزائري إجراء المراقبة الإلكترونية للإتصالات، بموجب القانون رقم 09 – 04 المؤرخ في 5 أوت 2009، المتعلق بالوقاية من الجرائم الإلكترونية، وكانت اتفاقية بودابست قد أوصت في المادة 21 منها الدول الأعضاء في الإتفاقية بضرورة اعتماد هذا الإجراء في التحري والتحقيق عن الجرائم، بعد أن ثبتت فعاليته في الكشف عن الجرائم وتحديد هوية المتورطين فيها.

لتحديد أحكام إجراء الرقابة الإلكترونية، نتناول في (المطلب الأول) **تعريف إجراء الرقابة الإلكترونية للإتصالات**، ثم **حالات السماح باتخاذ إجراء الرقابة الإلكترونية** في (المطلب الثاني)، ثم **ضوابط اتخاذ إجراء الرقابة الإلكترونية** في (المطلب الثالث).

المطلب الأول: تعريف المراقبة الإلكترونية للإتصالات ووسائله (cyber-surveillance)

يتمحور إجراء الرقابة الإلكترونية حول الإتصالات الإلكترونية. **نعرف في** (الفرع الأول) **الإتصالات الإلكترونية**، ثم نوضح **المقصود بإجراء مراقبة الإتصالات الإلكترونية** في (الفرع الثاني)، **والعلاقة بينه وبين إجراء اعتراض المراسلات السلكية واللاسلكية في (الفرع الثالث)**، ونحدد في (الفرع الرابع) **وسائل اتخاذ هذا الإجراء**.

الفرع الأول: تعريف الإتصالات الإلكترونية

عرف المشرع الجزائري الإتصالات الإلكترونية في المادة الثانية بند (و) من القانون رقم 09-04 على أنها، ((أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور

أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية))[1]، كما عرفها في القانون رقم 18-04 المؤرخ في 10 ماي 2018، الذي يحدد القواعد العامة المتعلقة بالبريد والإتصالات الإلكترونية[2]، أنها ((كل إرسال أو تراسل أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو بيانات أو معلومات مهما كانت طبيعتها، عبر الأسلاك أو الألياف البصرية أو بطريقة كهرومغناطيسية)).

وعليه تشمل الإتصالات الإلكترونية: اتصالات الهاتف الثابت، الهاتف النقال، الإتصالات التي تتم عبر شبكة الأنترنت، من خلال التطبيقات الحديثة (ماسنجر، فايبر، سكايب، ...)، كما تأخذ الإتصالات الإلكترونية شكل مراسلات مكتوبة أو محادثات شفوية أو صور ملتقطة[3].

الفرع الثاني: تعريف مراقبة الإتصالات الإلكترونية

يُسمى إجراء مراقبة الإتصالات الإلكترونية عند البعض بـ (اعتراض المراسلات الإلكترونية)[4]، ويعرف على أنه إدخال تدابير تقنية ممغنطة في خط أحد المشتركين لتسجيل المكالمات عن طريق البحث عن مصدر الإتصال من خلال عنوان (IP) في جهاز الحاسب الآلي الذي يجري منه الإتصال بالموقع[5]، أو أنها عملية الإستماع لمضمون أسلاك أو أية اتصالات شفوية عن طريق استخدام جهاز إلكتروني أو أي جهاز آخر[6].

---

[1] وقد كان المشرع يضيف إلى هذا التعريف عبارة (بما في ذلك وسائل الهاتف الثابت والنقال)، بموجب المادة الخامسة (5) من المرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر 2015، (الملغى) الذي يحدد تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال. جر: (عدد 53، بتاريخ 8 أكتوبر 2015، ص 16).

[2] ج. ر: (عدد 27، لسنة 2018، ص 3).

[3] ثابت دنيا زاد، مراقبة الإتصـــالات الإلكترونية والحق في حرمة الحياة الخاصـــة في القانون الجزائري، مجلة العلوم الإجتماعية والإنسانية، تصدر عن جامعة تبسة، الجزائر، العدد السادس، ديسمبر 2012، ص 207.

[4] بوعناد فاطمة زهرة، مكافحة الجريمة الإلكترونية في التشـريع الجزائري، مجلة الندوة للدراسـات القانونية، العدد الأول، 2013، ص 72.

[5] روابح فريد، المرجع السابق، ص 308.

[6] بن بادة عبد الحليم، المراقبة الإلكترونية كإجراء لاســـتخلاص الدليل الإلكتروني، (بين الحق في الخصـــوصـــية ومشـــروعية الدليل الإلكتروني)، المجلة الأكاديمية للبحث القانوني، تصـــدر عن جامعة عبد الرحمان ميرة، بجاية، المجلد 10، العدد3، 2019، ص 391.

وقد استعمل المشرع الجزائري مصطلح (المراقبة) وليس (التنصت)، فالأول أوسع وأشمل من الثاني، فالمراقبة تشمل التنصت من جهة والتسجيل من جهة ثانية. ويقصد بالتسجيل حفظ الأحاديث على الأشرطة المخصصة لذلك حتى يكون بالإمكان لاحقا إعادة سماعها[1].

ما يميز المراقبة أيضا أنها تتم خِلسة وخُفية دون علم صاحب الحديث أو الإتصال ودون رضاه، وتتيح بذلك سماع وتسجيل أدق أسرار الإنسان، سواء كانت هذه الأسرار تتعلق بالشخص المعني بالمراقبة أو الأشخاص الذين يتحدث معهم. بذلك تعتبر هذه الإتصالات اعتداء وقيد خطيرا على حرية وسرية الحديث باعتباره حق من الحقوق اللصيقة بشخصية الإنسان، كما ينجم عن مراقبته أن يصبح الفرد خائفا مترددا في ممارسة حقه في الحديث عبر وسائل الإتصال، ففرض المراقبة قد يكشف عن أدق أسرار حياة الشخص دون علمه، كما أنه لا يفرق بين المحادثات التي لها صلة بالجريمة موضوع التحري أو غيرها من المحادثات[2].

وتُجرى المراقبة بواسطة إحدى الوسائل التقنية الحديثة، وفي الوقت الحالي يتم مراقبة المراسلات التي تقع من خلال وعبر البريد الإلكتروني، عبر تطبيق الفيسبوك، أو تطبيق الماسنجر، أو الفايبر والسكايب وغيرها من برامج التواصل الإلكتروني[3].

يقصد أيضا بهذا الإجراء مراقبة الإتصالات الإلكترونية أثناء بثها، وليس الحصول على اتصالات إلكترونية مخزنة، من هنا يختلف إجراء المراقبة الإلكترونية عن إجراء التفتيش الإلكتروني، فالمراقبة الإلكترونية ترد على البيانات الإلكترونية المتحركة، التي تتمثل هنا في الإتصالات الإلكترونية لحظة إجرائها، دون تلك التي انتهت وخُزِنت، بيد أن التفتيش يرد فقط

---

[1] روابح فريد، المرجع السابق، ص 282.

– حتى يكون التسجيل منتجا لآثاره القانونية يجب أن يكون من الناحية التقنية واضحا يرسم صورة كاملة لحقيقة الحديث من بدايته إلى نهايته بشكل يسمح للقاضي أن يستخلص منه دليل إدانة أو براءة. وتطبيقا لذلك يجب ألا يكون التسجيل مشوشا أو يحتوي على كلام غير واضح أو عبارات غير مسموعة أو متداخلة أو مطموسة أو كانت لا تبين هوية الأشخاص المتحدثين أو احتوت على فراغات صوتية أو تضمنت أصواتا غير عادية. روابح فريد، المرجع نفسه، ص 282.

[2] روابح فريد، المرجع نفسه، ص 301.

[3] بن بادة عبد الحليم، المرجع السابق، ص 391.

على البيانات الإلكترونية الساكنة أو المخزنة، التي تتجسد هنا في الإتصالات التي تم إجراؤها وتخزينها[1].

الفرع الثالث: العلاقة بين إجراء المراقبة الإلكترونية وإجراء اعتراض المراسلات السلكية واللاسلكية

استحدث المشرع الجزائري إجراء اعتراض المراسلات السلكية واللاسلكية بموجب القانون رقم 06 – 22 المؤرخ في 20 سبتمبر 2006 المعدل لقانون الإجراءات الجزائية، الذي أضاف الفصل الرابع تحت عنوان ((اعتراض المراسلات وتسجيل الأصوات والتقاط الصور))، وكثيرا ما يُطرح التساؤل حول العلاقة بين إجراء الرقابة الإلكترونية للإتصالات واعتراض المراسلات السلكية واللاسلكية؟

لابد من التأكيد أولا أن كلا من الإجراءين يندرجان ضمن فكرة واحدة هي المراقبة[2]، وقد اتجه جانب من الشراح إلى القول بأن إجراء اعتراض المراسلات السلكية واللاسلكية يقتصر على التنصت التليفوني أي مراقبة المكالمات الهاتفية فقط، ما يعني بدوره أن إجراء الرقابة الإلكترونية للإتصالات يرتبط بالإتصالات التي تتم عبر نظام الحاسب الآلي فقط، وهذا الإعتقاد يَجُرُ إلى أن الإجراءين مُنفَصِلَينِ ولكل مِنهما مجاله الخاص، غير أن اتجاه آخرا يذهب إلى القول أن كلا من الإجراءين يرتبطان بموضوع واحد هو الإتصال، إلا أن مراقبة الإتصالات الإلكترونية أوسع في دلالتها من إجراء اعتراض الإتصالات السلكية واللاسلكية، بحيث تشمل (أي المراقبة

---

[1] بوعناد فاطمة زهرة، المرجع السابق، ص 72.

[2] المراقبة بمفهومها الواسع تشمل ثلاثة أشكال وأنواع، هي: **مراقبة الأحاديث الخاصة (تسجيل الأصوات)**، وتسمى بالتنصت المباشر، وتقوم على مراقبة الأحاديث الخاصة والسرية للأشخاص، أو نوع خاص من استراق السمع للأحاديث خلسة ودون علم صاحبها، بواسطة أجهزة إلكترونية؛ **مراقبة الإتصالات**، من خلال اعتراض المراسلات السلكية واللاسلكية (التنصت الهاتفي)، وكذا اعتراض المراسلات الإلكترونية التي تتم عبر الأنترنت؛ **المراقبة البصرية**، وتتمثل في التصوير الخفي من خلال التقاط أو تثبيت أو بث أو تسجيل صور الأشخاص في الأماكن الخاصة. روابح فريد، المرجع السابق، ص 273.

الإلكترونية) اعتراض جميع الإتصالات، سواء تلك التي تتم عبر الهاتف الثابت والهاتف المحمول أو تلك التي تقع عبر شبكة الأنترنت، من خلال التطبيقات الحديثة[1].

الفرع الرابع: وسائل وتقنيات المراقبة الإلكترونية للإتصالات

لم يحدد المشرع الجزائري وسائل المراقبة الإلكترونية، حيث اكتفى بالإشارة في المادة الثالثة (3) من القانون رقم 09-04 إلى أنه يتوجب وضع الترتيبات التقنية الخاصة بمراقبة الإتصالات الإلكترونية، وحسنا فعل المشرع حينما تجنب تحديد جهاز معين بذاته، حتى يكون بالإمكان مسايرة التطور العلمي في هذا المجال[2].

ويعد من أشكال المراقبة الإلكترونية اللجوء إلى:

- استخدام وسائل فنية كقلم التسجيل أو ما يسمى بالفخ والمتابعة، في هذه الحالة يتم تسجيل أسماء المتراسلين مع متهم معين أي مع بريده الإلكتروني أو مع من يقوم بالمحادثة الفورية معه.
- استخدام وسائل التصنت والإعتراض على محتوى الرسائل الإلكترونية أو المحادثة الفورية الإلكترونية[3].

ولكي تقوم الجهات الأمنية بمراقبة الإتصالات الإلكترونية فإنها تحتاج إلى مساعدة هيئات متخصصة، في هذا الإطار نشير إلى الدور الهام الذي تلعبه الهيئة الوطنية للوقاية من الجرائم الإلكترونية، ممثلة في مديرية المراقبة الإلكترونية واليقظة الإلكترونية، التي يعد من مهامها تنفيذ عمليات مراقبة الإتصالات الإلكترونية وتزويد السلطات القضائية ومصالح الشرطة القضائية،

---

[1] نادية سلامي، آليات مكافحة التجسس الإلكتروني، أطروحة دكتوراه، علوم، تخصص: القانون الجنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي، تبسة، الجزائر، السنة الجامعية: 2018 – 2019، ص. ص 245 – 248).

_ كان المشرع الجزائري يعرف الإتصالات الإلكترونية، في المادة الخامسة، من المرسوم الرئاسي رقم 15 – 261 المؤرخ 8 أكتوبر 2015، (الملغى)، أنها: ((كل تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات أيا كانت طبيعتها عن طريق أي وسيلة إلكترونية، **بما في ذلك وسائل الهاتف الثابت والنقال**)).

[2] وقد استعمل المشرع الجزائري ذات العبارة (الترتيبات التقنية) في المادة 65 مكرر5 من ق إ ج، التي تنص على إجراء اعتراض المراسلات وتسجيل الأصوات والتقاط الأصوات، كذلك فعل في المادة 303 مكرر من ق ع، التي عبرت عن جرائم التنصت الماسة بحرمة الحياة الخاصة بعبارة (بأية تقنية كانت).

[3] ثابت دنيا زاد، المرجع السابق، ص. ص (207 – 208).

تلقائيا أو بناء على طلبها، بالمعلومات اللازمة، كقيامها مثلا بمراقبة ورصد وتسجيل إتصالات أشخاص أو جماعات مشبوهة، تجتمع أو تحضر وتجهز للقيام بعمليات إرهابية، وتحديد مصدرها ومسارها، ومثل هذه المعلومات قد تساعد رجال الشرطة القضائية والسلطة القضائية في اتخاذ الإجراءات المناسبة من أجل الوقاية من الجرائم الإلكترونية ومكافحتها والقبض على مرتكبيها[1].

المطلب الثاني: حالات السماح بمراقبة الإتصالات الإلكترونية

تنص المادة الرابعة (4) من القانون 09-04 أنه: (يمكن القيام بعمليات المراقبة المنصوص عليها في المادة الثالثة (3) أعلاه في الحالات الآتية:

أ – للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

ب – في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الإقتصاد الوطني.

ج – لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.

د –في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة).

من خلال ما جاء بالمادة الرابعة (4) أعلاه، يتضح أن المشرع الجزائري قد حدد حصرا الحالات التي يمكن اللجوء فيها لإجراء المراقبة الإلكترونية للإتصالات، نوجزها في ثلاث فروع متتالية:

الفرع الأول: اتخاذ الرقابة الإلكترونية للإتصالات كإجراء وقائي

سمح المشرع الجزائري باتخاذ إجراء الرقابة الإلكترونية للإتصالات كإجراء وقائي بالنسبة لعدد من الجرائم الخطيرة، ألا وهي الجرائم الإرهابية والتخريبية والجرائم الماسة بالأمن الوطني، بالنظر لما يميز هذا النوع من الجرائم من خطورة بالغة على أمن الدولة وحياة الأفراد وممتلكاتهم،

[1] شنتير خضرة، الآليات القانونية لمكافحة الجريمة الإلكترونية، (دراسة مقارنة)، أطروحة دكتوراه، (ل م د)، تخصص القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة أحمد درارية، أدرار، السنة الجامعية 2021/2020، ص 167.

فإذا تعلق الأمر مثلا بالجرائم الإرهابية التي تستهدف المدنيين فلا يمكن الحديث حينها عن حقوق الإنسان[1]، أضف إلى ذلك أن تنفيذ هذه الجرائم يتم في كثير من الأحيان بواسطة أجهزة اتصالات أو تحكم عن بعد[2].

وقد أجاز المشرع الجزائري اتخاذه حتى قبل ارتكاب هذه الجرائم، وهو ما تؤكده عبارة (الوقاية)، التي جاءت بالبند (أ)، فالوقاية تسبق عملية البدء في التنفيذ وتسبق حتى عملية التحضير للجريمة[3].

رخص المشرع الجزائري أيضا باتخاذ إجراء الرقابة الإلكترونية للإتصالات باعتباره يندرج ضمن الإجراءات الوقائية لحماية مجموعة من المصالح والهيئات، لاسيما مع السياسة التي اعتمدتها البلاد في عصرنة كافة القطاعات وذلك بالإعتماد المتزايد على أنظمة المعلومات، فحساسية هذه القطاعات كالدفاع الوطني مثلا تقتضي المراقبة السابقة، لما لها من تأثير على كيان الدولة ككل في حال المساس بها[4].

الفرع الثاني: اتخاذ إجراء الرقابة الإلكترونية لمقتضيات التحري والتحقيق

أجاز المشرع الجزائري اتخاذ إجراء الرقابة الإلكترونية للإتصالات لمقتضيات التحريات الأولية والتحقيقات القضائية، وفي هذه الحالة يكون اللجوء إلى المراقبة الإلكترونية بعد ارتكاب الجريمة، خلال مرحلتي جمع الإستدلالات والتحقيق القضائي، لغرض التوصل إلى معرفة مرتكبي الجريمة في حالة عدم جدوى الإجراءات التقليدية في الوصول إلى الحقيقة[5].

نُنَوِه إلى أن البند (ج) من المادة الرابعة (4) من القانون رقم 09-04 لم يحدد بالضبط نوع الجرائم المقصودة، ما يعني إمكانية اتخاذ هذا الإجراء في كافة جرائم القانون العام، وبصدد كل

---

[1] جبار فطيمة، مراقبة الإتصالات الإلكترونية بين الحظر والإباحة في التشريع الجزائري، مجلة الدراسات القانونية المقارنة، يصدرها مخبر البحث (القانون الخاص المقارن)، جامعة حسيبة بن بوعلي الشلف الجزائر، العدد الثالث، ديسمبر 2016، ص. ص (17 – 18).

[2] ثابت دنيا زاد، المرجع السابق، ص 210.

[3] جبار فطيمة، المرجع نفسه، ص. ص (17 – 18).

[4] المرجع نفسه، ص 18.

[5] ثابت دنيا زاد، المرجع نفسه، ص 210.

قضية مستعصية صغيرة كانت أو كبيرة، وهو ما يؤدي بدوره إلى تعميم استخدام هذه الآلية دون حد[1].

الفرع الثالث: اتخاذ إجراء الرقابة الإلكترونية في إطار التعاون الدولي

يمكن اتخاذ إجراء الرقابة الإلكترونية للإتصالات في إطار تنفيذ المساعدات القضائية الدولية المتبادلة، وتدخل هذه الحالة في إطار التعاون الدولي للحد من الجرائم العابرة للحدود، كما لو طلبت دولة معينة من الجزائر مراقبة الإتصالات الإلكترونية لأشخاص مقيمين في الجزائر يُحتمل اشتراكهم في عمل إجرامي بالخارج مس بالدولة الأجنبية، فهنا يجوز للسلطات القضائية مراقبة اتصالات هؤلاء الأشخاص في إطار المعاملة بالمثل[2].

المطلب الثالث: ضوابط اتخاذ إجراء المراقبة الإلكترونية

قيد المشرع الجزائري إجراء المراقبة الإلكترونية بمجموعة من الضوابط الهامة، نوضح هذه الضوابط فيما يلي:

الفرع الأول: ضرورة الحصول على إذن مسبق من الجهة القضائية المختصة

يعتبر وضع هذا الإجراء، الذي يمس بالحريات الفردية والحياة الخاصة للأفراد، تحت يد القضاء المستقل ضمانة حقيقية، على أساس أن القاضي يهدف إلى الموازنة بين مقتضيات التحقيق وإلزامية حماية الأفراد المشتبه فيهم، فمجرد الإشتباه لا يجعل من الفرد مجرما وهذا ما يندرج بضمانات المحاكمة العادلة[3].

نقوم بتحديد **الجهة المختصة بإصدار الإذن بالمراقبة(أولا)**، ثم **مدة الإذن بالمراقبة(ثانيا)**.

أولا: الجهة المختصة بإصدار الإذن بالمراقبة

---

[1] امحمدي بوزينة آمنة، إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية، (دراسة تحليلية لأحكام قانون الإجراءات الجزائية وقانون الوقاية من جرائم الإعلام)، أعمال الملتقى الوطني (آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري)، الجزائر: 29 مارس 2017، المنظم من طرف مركز جيل البحث العلمي، 2017، ص 74.

[2] فطيمة جبار، المرجع السابق، ص 18؛ دنيا ثابت زاد، المرجع السابق، ص 211.

[3] امحمدي بوزينة آمنة، المرجع نفسه، ص75.

جاء في المادة الرابعة (4) فقرة 2 من القانون 09-04 أنه: (لا يجوز إجراء عمليات المراقبة، إلا بإذن مكتوب من السلطات القضائية المختصة)، بذلك يقوم وكيل الجمهورية بإصدار الإذن بمراقبة الإتصالات الإلكترونية أثناء مرحلة التحريات الأولية، في حين يقوم قاضي التحقيق بإصدار هذا الإذن أثناء مرحلة التحقيقات القضائية[1].

وإذا تعلق الأمر بالأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، فإن النائب العام لدى مجلس قضاء الجزائر هو الذي يختص بمنح إذن المراقبة لضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحته.

ويتعين على القضاء قبل إصدار الإذن بالمراقبة تقدير مدى توافر حالة من الحالات الواردة على سبيل الحصر في الفقرة الأولى من المادة الرابعة (4) السابقة الذكر، منعا للتعسف من أي جهة أخرى، ويبطل أي إجراء يتم دون الحصول على الإذن، ما يؤدي إلى بطلان الدليل المستمد منه وبالتالي جميع الإجراءات التي بُنِيَت عليه[2].

ثانيا: مدة الإذن بالمراقبة

حددت المادة الثالثة(3) من القانون 09-04 مدة الإذن الذي يمنحه النائب العام لدى مجلس قضاء الجزائر لضباط الشرطة القضائية بشأن وضع الترتيبات التقنية للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة لمدة 6 أشهر قابلة للتجديد.

ولم يحدد المشرع الجزائري عدد مرات التجديد، ولعل ذلك يرجع إلى خطورة هذا النوع من الإجرام الذي يمس بأمن الدولة بالدرجة الأولى، ولكون هذا النوع من الإجرام هو إجرام منظم وعابر للحدود الوطنية في كثير من الأحيان، حيث لا يتم الكشف عنه بسهولة، الأمر الذي يتطلب اتخاذ التحريات خلال مدة زمنية معينة، يتم خلالها الكشف عن حقيقة الجرم والتوصل إلى عناصر هذه التنظيمات المنتشرة عبر العديد من المواقع والأقاليم[3]، لكن كان من الأجدر على

---

[1] ثابت دنيا زاد، المرجع السابق، ص 213.

[2] مرزوقي كريمة، المرجع السابق، ص 1373.

[3] ثابت دنيا زاد، المرجع السابق، ص 221.

المشرع الجزائري أن يحدد عدد المرات التي يسمح فيها بالتحديد والتي لا يمكن أن تستمر لسنوات، فإذا لم تجد هذه الإجراءات نفعا في الوصول إلى الحقيقة يتعين الإبتعاد عنها[1].

وبالنسبة لباقي الحالات المنصوص عليها في المادة الثالثة (3) من القانون رقم 09-04، فإنه يتم الرجوع إلى القواعد العامة في قانون الإجراءات الجزائية، وهي تقديم إذن من قبل قاضي التحقيق أو وكيل الجمهورية كل حسب اختصاصه بهدف اعتراض المراسلات مع تحديد العناصر المهمة في الإذن ويسلم مكتوبا لمدة أربعة أشهر قابلة للتجديد عند الضرورة، حسب المادة 65 مكرر 7 من ق إ ج[2].

الفرع الثاني: الإلتزام بالسرية أثناء مراقبة الإتصالات الإلكترونية

يكون الموظفون القائمون على عمليات المراقبة الإلكترونية قادرون على الإطلاع على معلومات ذات طابع مجرم وأخرى ذات طابع شخصي، وفي كلتا الحالتين يكون هؤلاء مطالبين باحترام السر المهني، وعليه جرم المشرع الجزائري كل محاولة من قبل هؤلاء الموظفين نحو استغلال عمليات المراقبة لأغراض شخصية أو كل تجاوز لحدود المراقبة الإلكترونية نحو انتهاك حرمة الحياة الشخصية للأفراد أيا كان السبب[3].

الفرع الثالث: حدود استعمال المعطيات المتحصل عليها

أكد المشرع الجزائري أنه لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة إلا في تجميع وتسجيل معطيات ذات صلة بالحالات الواردة على سبيل الحصر في المادة الرابعة (4) من القانون 09-04، فيما يخص الأفعال الإرهابية وفي الحدود الضرورية للتحريات أو التحقيقات القضائية، ما يعني تجريم كل استعمال لها خارج هذا الإطار[4].

---

[1] ثابت دنيا زاد، المرجع السابق، ص 221.

[2] جبار فطيمة، المرجع السابق، ص 19.

[3] امحمدي بوزينة آمنة، المرجع السابق، ص 76.

[4] المرجع نفسه، ص. ص (75-76).

المبحث الثاني: التفتيش الإلكتروني (perquisition informatique)

التفتيش إجراء يستهدف البحث عن عناصر الجريمة في وعاء السر الخاص بالمتهم، سواء كان منزلا أو نظام حاسوب، وقد سمح المشرع باتخاذه على الرغم مما يحتويه من تعرض لحرمة الحياة الخاصة للأفراد تغليبا للمصلحة العامة، غير أنه قيده في الوقت ذاته بشروط وضوابط معينة.

نتطرق، من خلال هذا المبحث، إلى **تعريف التفتيش الإلكتروني وتمييزه عن التفتيش التقليدي** في (المطلب الأول)، ثم **ضوابطه** في (المطلب الثاني).

المطلب الأول: مفهوم إجراء التفتيش الإلكتروني

يعتبر إجراء التفتيش الإلكتروني من الإجراءات الهامة، التي استحدثها المشرع الجزائري بموجب المادة الخامسة (5) من القانون رقم 09 – 04، نقوم بتوضيح المقصود بهذا الإجراء الجديد، **من خلال تعريفه** (الفرع الأول)، ثم **نميزه عن التفتيش التقليدي** (الفرع الثاني).

الفرع الأول: تعريف التفتيش الإلكتروني

يُعرف التفتيش بوجه عام أنه إجراء من إجراءات التحقيق، يستهدف البحث عن الحقيقة في مستودع السر[1]، ويعتبر من الإجراءات الهامة في التحقيق؛ إذ غالبا ما يُسفر عن أدلة تفيد في كشف ملابسات الجريمة.

ويُعرف التفتيش الإلكتروني (أو كما يسميه البعض بالولوج إلى النظم المعلوماتية)[2]، على أنه إجراء يسمح بجمع الأدلة المخزنة أو المسجلة بشكل إلكتروني، كما يستهدف ضبط أدلة

---

[1] عبد الله أو هايبية، تفتيش المساكن في القانون الجزائري، المجلة الجزائرية للعلوم القانونية والإقتصادية والسياسية، تصدر عن معهد الحقوق والعلوم الإدارية، جامعة الجزائر، الجزء 36، العدد2، 1998، ص 70.

[2] شنتير خضرة، المرجع السابق، ص 71.

_ استعمل المشرع الجزائري في المادة الخامسة (5) من القانون رقم 09 – 04، عبارة **(تفتيش المنظومة المعلوماتية)**، وكذا عبارة **(الدخول بغرض التفتيش)** للتعبير عن هذا الإجراء الجديد، أي أنه آثر المزاوجة بين المصطلحات التقنية الجديدة، مع عدم التخلي عن المُسميات الإجرائية التقليدية، فالمصطلحات الجديدة تُمثل تجسيدا لتطور المفاهيم الإجرائية تأثرا بالبيئة الرقمية، أما عن المصطلحات التقليدية، فهي تُعبر عن تطابق التفتيش الإلكتروني مع نظيره التقليدي، من ناحية أن كلاهما في جوهرهما عبارة عن بحث وتنقيب في مستودع السر، بحثا عن عناصر الجريمة. لهوى رابح، الشرعية الإجرائية للأدلة

الجريمة مثل البرامج غير المشروعة والملفات المخزنة في الحواسيب، والمعطيات المعلوماتية والإتصالات الإلكترونية[1]. أو أنه اطلاع استثنائي لجهة التحقيق، يستهدف معلومات مخزنة ذات حُرمَة، بُغية البحث عن أدلة الجريمة وكل ما يُفيد في إظهار الحقيقة[2].

الفرع الثاني: تمييز التفتيش الإلكتروني عن التفتيش التقليدي

يشترك التفتيش الإلكتروني مع التفتيش التقليدي، في أن كلا منهما يهدف إلى جمع الأدلة التي تؤدي إلى الكشف عن الحقيقة والوصول إلى دليل حاسم في التحقيق؛ إذ لا يُمكن إدانة شخص دون دليل، كما يعتبر كل منهما قيدا على حرمة وحصانة الشخص ومساسا لحقه في سرية حياته الخاصة.

غير أن التفتيش الإلكتروني يختلف عن التفتيش في شكله التقليدي في العديد من الجوانب، نوجزها في النقاط التالية:

من جهة أولى، يتطلب التفتيش الإلكتروني من القائم بعملية التفتيش استخدام أساليب ووسائل تقنية فريدة من نوعها، فهو خلاف التفتيش التقليدي لا يحتاج في الكثير من الحالات الإنتقال إلى منازل الأشخاص المشتبه في ارتكابهم للجريمة، فقد يتم عن بُعد، وهو ما يُعرف بالتفتيش على الخط (perquisition en ligne).

من جهة ثانية، وترتيبا على ما تقدم، يعتبر التفتيش الإلكتروني عملية معقدة ومتشابكة، تتطلب بأن يكون الشخص الذي يقوم بها على دراية واسعة وكفاءة عالية في البحث عن المعلومة، وفي معالجة المعطيات وتحليلها وفك رموزها.

ومن جهة ثالثة، يتفرد التفتيش الإلكتروني بطابعه اللامادي، فهو يستهدف البحث عن برامج وبيانات إلكترونية ليس لها أي كيان مادي ملموس، كذلك الذي تحوزه الأشياء المادية التي يتركز

المعلوماتية المستمدة من التفتيش، أطروحة دكتوراه، تخصص: علوم جنائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة باتنة 1، السنة الجامعية: 2021/2020، ص 79.

[1] رضا هميسي، تفتيش المنظومة المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، تصدر عن كلية الحقوق والعلوم السياسية، جامعة الوادي، الجزائر، عدد 5، جوان 2012، ص 161.

[2] لهوى رابح، المرجع السابق، ص 79.

عليها التفتيش التقليدي. كما أن أوعية التخزين التي تتضمن المحتوى المعلوماتي المجرم لا تعترف بحيز جغرافي معين، ما يُصَعِب بدوره عملية إثباتها ونسبتها لمرتكبها، لسهولة التخلص من الأدلة من خلال محوها أو إتلافها أو التلاعب بالبيانات في وقت وجيز[1].

المطلب الثاني: ضوابط إجراء التفتيش الإلكتروني

أدرك المشرع الجزائري أنه لابد من إخضاع إجراء التفتيش الإلكتروني لأحكام مستقلة تتلاءم مع طبيعته الخاصة، حيث سن في المادة الخامسة (5) من القانون رقم 09-04، أحكاما موضوعية وأخرى شكلية تعالج هذا الأمر.

نتناول **الضوابط الموضوعية** في (الفرع الأول)، يليها **الضوابط الشكلية** في (الفرع الثاني).

الفرع الأول: الضوابط الموضوعية للتفتيش الإلكتروني

تتمثل الضوابط الموضوعية للتفتيش الإلكتروني (أولا) **بضرورة وجود سبب يبرر اللجوء للتفتيش الإلكتروني**، بالإضافة إلى **الأحكام الخاصة بالمحل الذي ينصب عليه** (ثانيا).

أولا: وجود سبب للتفتيش الإلكتروني

يعتبر عنصر السبب ضمانة قانونية لصحة ومشروعية إجراء التفتيش بوجه عام، يتحقق بوقوع جريمة ما يتم بموجبها توجيه الإتهام إلى الشخص أو الأشخاص المراد تفتيشهم بناء على أدلة أو قرائن قوية تفيد تورطهم في هذه الجريمة، عملا بمبدأ الشرعية الجزائية القاضي بـ (أن لا جريمة ولا عقوبة إلا بنص)؛ إذ دون وقوع جريمة وتوجيه اتهام إلى شخص أو أشخاص معينين وفقا لأدلة كافية يكون التفتيش باطلا لانتفاء السبب الذي يبرره[2].

غير أن المشرع الجزائري خرج عن هذه القاعدة في المادة الخامسة (5) فقرة أولى من القانون رقم 09 – 04، التي تنص أنه (يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية، في إطار قانون الإجراءات الجزائية **وفي الحالات المنصوص عليها في المادة 4 أعلاه**، ....)، وبالرجوع إلى الحالات المحددة بالمادة الرابعة (4) من القانون 09-04 نجد أن المشرع الجزائري قد وسع من مجال اتخاذ هذا الإجراء، حيث أجاز لجهات التحقيق اللجوء إلى

---

[1] راجع في هذا الخصوص، هميسي رضا، المرجع نفسه، ص. ص (161 – 162).

[2] براهيمي جمال، المرجع السابق، ص 31.

تفتيش الأنظمة المعلوماتية في مراحل سابقة على وقوع الجرائم، أي باعتباره إجراء وقائيا، كما سمح بإجرائه في حالة توفر معلومات عن احتمال وقوع جرائم معينة ذكرتها المادة الرابعة (4) من القانون رقم 09-04، التي من بينها الإعتداء على منظومة معلوماتية على النحو الذي من شأنه المساس بالنظام العام.

ثانيا: محل التفتيش الإلكتروني

يشمل مسرح الجريمة الإلكترونية شقين اثنين، (الأول) مسرح تقليدي مادي، يقع خارج نظام الحاسب الآلي، في المكان المادي المتواجد فيه، حيث من الممكن أن يترك الجاني آثار مادية ملموسة، كوسائط التخزين الإلكترونية مثلا، و(الثاني) مسرح افتراضي غير مادي، يتمثل في البيانات الإلكترونية، التي تتواجد داخل الحاسب، في ذاكرة الأقراص الصلبة[1]، وعليه قد ينصب التفتيش على المكونات المادية (hardware) للنظام أو المكونات المعنوية له (software) وكذا شبكات الإتصال، ويختلف الحكم القانوني على حسب طبيعة المحل الذي ينصب عليه التفتيش الإلكتروني.

نوضح في **نقطة أولى** أحكام التفتيش الذي يطال المكونات المادية للنظام، وفي **نقطة ثانية** أحكام التفتيش الذي يقع على المكونات المعنوية له، في حين ندرس في **نقطة ثالثة** التفتيش الذي ينصب على شبكات الإتصال:

1) تفتيش المكونات المادية للنظام:

يقصد بالمكونات المادية للنظام المعلوماتية الأشياء الملموسة من أجزائه وأدواته، التي تعمل بطريقة متكاملة لآداء مهمة معينة، تتمثل في معالجة البيانات بطريقة آلية، كوحدات الإدخال والإخراج ووحدة المعالجة المركزية. وإذا ورد التفتيش الإلكتروني على المكونات المادية للنظام، فإنه في هذه الحالة يكون قد انصب على أشياء مادية ملموسة لا تختلف – البَتَة –عن الأشياء التي يرد عليها التفتيش العادي، وعلى الرغم من ذلك إلا أن المشرع الجزائري خرج عن القواعد المتعارف عليها بشأن تفتيش الأشياء المادية؛ إذ نجده أفرغ التفتيش من كل الضمانات والشروط

[1] بوعناد فاطمة الزهراء، المرجع السابق، ص 68.

القانونية، لاسيما ما يتعلق بالوقت القانوني للتفتيش، الأشخاص المطلوب حضورهم عملية التفتيش[1].

بذلك ميز المشرع الجزائري الجريمة الإلكترونية عن غيرها من الجرائم العادية، حتى لو كان التفتيش هنا يتعلق بأشياء مادية، وذلك يرجع إلى اقتناعه بخطورة هذه الجريمة، على النحو الذي يكون من اللازم معاملتها بطريقة متميزة ومتشددة عن غيرها من الجرائم[2].

2) تفتيش المكونات المعنوية للنظام:

يقصد بالمكونات المعنوية للنظام برامجه وبياناته، ويعتبر التفتيش الإلكتروني في هذه الحالة في غاية الخطورة على خصوصيات الأفراد، لأن البرامج والملفات عادة ما تكون متداخلة، فالبعض منها قد يتعلق بالمتهم والبعض الآخر قد يخص أشخاصا آخرين[3]، كما أن هذه الملفات قد تحتوي على بيانات مجرمة تشكل موضوعا للدليل الجنائي، وقد تتضمن أيضا ملفات بريئة لا علاقة لها بالجريمة[4].

لذلك عرفت فكرة تفتيش المكونات المعنوية للنظام كالبرامج والمعطيات جدلا واسعا بين مؤيد للفكرة ومنكر لها، فالرأي الرافض للفكرة يرجع ذلك إلى الطبيعة غير المادية للمعطيات والبرامج، ما يجعلها تتنافى مع الهدف الذي يسعى إليه التفتيش بمفهومه التقليدي، الذي يتحرى ويبحث عن الأدلة المادية، في حين يذهب الرأي المؤيد للفكرة إلى القول أن هذه البرامج عبارة عن نبضات أو ذبذبات إلكترونية أو موجات كهرومغناطيسية، وهي قابلة للتسجيل والتخزين والتحميل على وسائط ودعائم مادية، كالأشرطة والأقراص والأسطوانات، لذلك فمن الممكن إخضاعها لقواعد التفتيش التقليدي[5].

---

[1] راجع المواد 45، 47 من قانون الإجراءات الجزائية.

[2] يزيد بوحليط، **تفتيش المنظومة المعلوماتية وحجز المعطيات في التشـــريع الجزائري**، مجلة التواصـــل في التجارة والإقتصاد والقانون، عدد 48، ديسمبر 2016، ص84.

[3] مصـطفى عبد الباقي، التحقيق في الجريمة الإلكترونية وإثباتها في فلسـطين (دراسـة مقارنة)، مجلة دراسـات، علوم الشريعة والقانون، المجلد 45، عدد4، ملحق 2، 2018، ص 290.

[4] لهوى رابح، المرجع السابق، ص 750.

[5] علي عدنان الفيل، إجراءات التحقيق الإبتدائي في الجريمة المعلوماتية، (دراسة مقارنة)، مجلة الحقوق، المجلد الثامن، ص. ص (460 – 461).

وقد حسم المشرع الجزائري موقفه بشأن هذا الجدل، حيث جاء في المادة الخامسة (5) من القانون رقم 09-04 أنه: (يجوز للسلطات القضائية ... الدخول، بغرض التفتيش، ولو عن بعد، إلى: أ – منظومة معلوماتية **أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها...)**، بذلك أقر المشرع الجزائري أنه يمكن تفتيش المنظومة المعلوماتية ككل أو جزء منها، بما في ذلك البرامج والمعطيات المخزنة.

وإن كان المشرع الجزائري أقر بجواز تفتيش الملفات الإلكترونية، إلا أنه لم يُقَدِم لنا حلا فيما يخص نطاق هذا التفتيش، وما إذا كان التفتيش عاما يشمل كافة الملفات المتواجدة داخل نظام الحاسب الآلي للمتهم، أم أنه يكون محددا بجزء معين منها فقط؟

وجدت هذه الإشكالية خلافا فقهيا وقضائيا كبيرا في الدول الغربية الأكثر تطورا في المجال الإلكتروني، حيث اتجه رأي – وهو موقف القضاء الأمريكي – إلى أن كل ملف في النظام يعتبر حاوية مغلقة ويقتضي إذنا خاصا بالتفتيش، فمثلا إذا كانت التهمة حيازة صور أو فيديوهات جنسية لأطفال على جهاز الحاسب الآلي للمتهم، فيجب حصر نطاق التفتيش في الملفات والبرامج المخصصة للصور والفيديوهات دون غيرها. ويرجع سبب تبني هذا الموقف إلى أن الحاسب الآلي يمكن أن يحتوي على ملفات تخص الحياة الخاصة لصاحبها ولا علاقة لها بالجريمة، وفتح جهات التحقيق لهذه الملفات يعد تعديا على الخصوصية[1].

في حين اتجه رأي آخر إلى أنه يكفي الحصول على الإذن بتفتيش النظام المعلوماتي للمتهم، حتى يكون من حق جهات التحقيق تفتيش ما يحتويه النظام من بيانات وبرامج، دون قيد أو تخصيص، وحجتهم في ذلك أن الأجهزة الإلكترونية بمختلف أنواعها تعد مجالا حيويا وضخما لتخزين مئات الآلاف من الملفات والبيانات، ومن غير المعقول إصدار إذن بالتفتيش على كل ملف من هذه الملفات[2].

3) تفتيش شبكات الإتصال المعلوماتي (التفتيش عن بُعد):

أصبح من السهل، بوجود أنظمة الحاسب الآلي، توزيع المعلومات التي تحتوي أدلة الجريمة عبر شبكات حاسوبية في أماكن كثيرة بعيدة عن الموقع المادي للتفتيش، ويثير إخضاع شبكات

[1] مصطفى عبد الباقي، المرجع السابق، ص 290.

[2] براهيمي جمال، المرجع نفسه، ص39.

الإتصال التي تربط بين أجهزة الحاسب الآلي بعضها ببعض لإجراء التفتيش مشاكل قانونية تتعلق بالإختصاص القضائي، حيث يطرح التساؤل حول مدى جواز امتداد التفتيش إلى الأنظمة المعلوماتية المتصلة بالنظام المأذون بتفتيشه، إذا كانت متواجدة في دوائر اختصاص مختلفة، أو كانت موجودة خارج القطر الوطني؟

وعليه يمكن أن نتصور هنا حالتين:

ح1/ اتصال حاسب المتهم بحاسب آخر موجود في مكان آخر داخل الدولة

جاء في المادة الخامسة (5) فقرة 2 من القانون 09-04 أنه إذا كانت المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى، ويمكن الولوج إليها انطلاقا من المنظومة الأولى، فإنه يجوز تفتيش هذه المنظومة بسرعة دون استصدار إذن قضائي، أي أنه يكفي فقط إعلام السلطة القضائية المختصة بذلك.

فانتظار الحصول على الإذن من السلطات المختصة قد يأخذ بعض الوقت، الأمر الذي قد يؤدي إلى تلاشي الدليل واندثاره في وقت قياسي، كأن يقوم المشتبه فيه بمحوه وإتلافه مثلا؛ إذ يكفي الضغط على مكان معين لإنهاء وجود المعلومة ومن ثمة تضمحل عناصر الإثبات، وهو ما يشكل صعوبة في إيجاد دليل حاسم، وعليه فاستصدار إذن قضائي في مثل هذه الحالات لا طائل منه[1].

ح 2/ اتصال حاسب المتهم بحاسب موجود في مكان آخر خارج الوطن

تواجه سلطات التحقيق في هذه الحالة مشكلة تتمثل في مدى جواز تمديدها إجراءات التفتيش إلى خارج الإقليم الجغرافي للدولة، وهو ما يسمى بـ (التفتيش العابر للحدود). وقد اتفق الفقه أنه لا يجوز لسلطات التحقيق التابعة لدولة ما اللجوء إلى التفتيش الإلكتروني العابر للحدود لاسترجاع البيانات المخزنة في الخارج، إلا في إطار اتفاقات تعاون خاصة ثنائية أو جماعية تجيز وتنظم هذا التمديد، أو في إطار الإنابة القضائية المتبادلة أو على الأقل بعد الحصول على الإذن

[1] رضا هميسي، المرجع السابق، ص 93.

الصريح من الدولة الأجنبية، وفي ظل غياب هذه الإتفاقيات يعد اتخاذ هذا الإجراء انتهاكا واختراقا فعليا لمبدأ السيادة، كما يعتبر من قبيل التجسس الإلكتروني الذي يمس الأمن القومي لأية دولة[1].

وقد جاء في المادة الخامسة (5) في فقرتها الثالثة (3) من القانون رقم 09-04 أنه: (إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للإتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل)، بذلك لم يسمح المشرع الجزائري للسلطات القضائية المختصة وضباط الشرطة القضائية بتوسيع نطاق التفتيش الإلكتروني ليشمل المعطيات المخزنة في منظومة معلوماتية تقع خارج القطر الوطني، إلا في إطار المساعدة القضائية المتبادلة وفي نطاق الإتفاقيات الدولية المبرمة في مجال ملاحقة مقترفي الجرائم الإلكترونية[2].

الفرع الثاني: الضوابط الشكلية لإجراء التفتيش الإلكتروني

يتطلب القانون شـــروطا شـــكلية معينة لابد من توافرها عند القيام بإجراء التفتيش؛ تتعلق بالجهة المختصـــة باتخاذه، والميعاد القانوني المقرر لذلك. نتناول (أولا) **الســـلطة المختصـــة بالتفتيش الإلكتروني**، ثم (ثانيا) **الميعاد القانوني لتنفيذه**، و(ثالثا) **الإلتزام بتحرير محضـــر التفتيش**.

أولا: السلطة المختصة بالتفتيش الإلكتروني

يتم القيام بالتفتيش من طرف الأشخاص الذين يحددهم القانون ويعطيهم صلاحية القيام بإجرائه، وقد نصت المادة الخامسة (5) من القانون 09-04 على أنه: (يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية ... الدخول، بغرض التفتيش ...)، وعليه خول المشرع

---

[1] شنتير خضرة، المرجع السابق، ص99.

[2] براهيمي جمال، المرجع السابق، ص 28.

- في هذا الإطار، جاء في المادة 16 في فقرتها الأولى من القانون رقم 09-04 أنه: (في إطار التحريات أو التحقيقات القضائية الجارية لمعاية الجرائم المشمولة بهذا القانون وكشف مرتكبيها، يمكن السلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني).

الجزائري صلاحية القيام بالتفتيش إلى السلطات القضائية، المتمثلة في النيابة العامة أو قاضي التحقيق وكذا ضباط الشرطة القضائية.

وعلى أساس الخصوصية التي تميز الجرائم الإلكترونية، من حيث أنها معقدة ومتشابكة، الأمر الذي يقتضي معرفة كيفية التعامل مع الأجهزة والبرامج الإلكترونية، لذلك فطلب المساعدة من أهل الإختصاص تعد ضرورة ملحة تقتضيها ظروف الحال. تطبيقا لذلك، سمح المشرع الجزائري، في المادة الخامسة في فقرتها الرابعة من القانون رقم 09-04، للسلطات المكلفة بالتفتيش بـ (تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاح مهمتها). وتتمثل مهمة الشخص الخبير في تقديم التوضيحات الكافية حول كيفية تشغيل هذه الأنظمة وطريقة النفاذ إليها أو إلى المعطيات المخزنة أو المعالجة أو المنقولة في شكل يمكن فهمه وإدراكه[1]. ويمكن هنا للسلطة المختصة بالتفتيش أن تطلب المساعدة من الهيئة الوطنية للوقاية من الجرائم الإلكترونية، بما لها من خبراء وكفاءات متخصصة، حيث يعد من مهام الهيئة، حسب ما ورد بالمادة 14 من القانون رقم 09 – 04، مساعدة السلطة القضائية ومصالح الشرطة القضائية في التحريات التي تجريها.

وكان المشرع الجزائري قد حدد في المادة الخامسة (5) من القانون رقم 09 – 04 السلطة المختصة بالتفتيش الإلكتروني، ومن يقدم لها العون فيما تحتاجه لتنفيذه، غير أنه لم يتطرق إلى مسألة في غاية الأهمية، تتعلق بالإذن بالتفتيش الإلكتروني، فإذا كان من يقوم بعملية التفتيش هي السلطة القضائية، فليس هناك إشكال، أما إذا كان من يقوم بالتفتيش هم رجال الضبطية القضائية، فهنا يطرح التساؤل حول ما إذا كان بإمكانهم القيام بذلك تلقائيا دون الحاجة لاستصدار الإذن بالتفتيش، أم أنه من الضروري اتخاذ هذا الإجراء بناء على إذن من السلطة القضائية؟

[1] رضا هميسي، المرجع السابق، ص 172.

وفي الفرض الذي يحصل فيه رجال الضبطية القضائية على الإذن بتفتيش منزل المتهم، أو سيارته مثلا، فهل يجوز لهم حينئذ الولوج إلى كل ما يصادفهم من أجهزة إلكترونية متواجدة بالمنزل للبحث عن أدلة إثبات الجريمة؟

يتجه البعض إلى أن الإذن بالتفتيش للأنظمة المعلوماتية يُستخلص ضمنا، من المادة الخامسة من القانون رقم 09-04، التي جاء فيها: (يجوز تمديد التفتيش بسرعة إلى هذه المنظومة بعد إعلام السلطة القضائية المختصة بذلك مسبقا)، ويفهم من ذلك أنه يجب على رجال الضبطية القضائية الحصول أولا على إذن مُسبق بالتفتيش للمنظومة المعلوماتية وفي حال تمديد عملية التفتيش إلى أنظمة أخرى متصلة بالنظام المعلوماتي للمتهم، فإنه يكفي في ذلك إعلام السلطة المختصة[1].

وتبعا لما تقدم، فإنه يجب على رجال الضبطية القضائية الحصول على إذن مستقل بتفتيش المنظومة المعلوماتية للمتهم، ولا يكون الإذن العام بتفتيش منزل المتهم كافيا لتفتيش نظام الحاسب الآلي المتواجد فيه.

ثانيا: الميعاد الزمني لإجراء التفتيش الإلكتروني

يعد فرض قيود زمنية للقيام باجراء التفتيش ضمانة إجرائية مهمة لحماية الحريات والحقوق العامة للأفراد. لذلك لم يسمح المشرع الجزائري – كقاعدة عامة –، بمقتضى المادة 47 من ق إ ج، بتفتيش المنازل وما في حكمها إلا في الوقت المحصور بين الساعة الخامسة (5) صباحا والثامنة مساء(8)[2].

غير أن المشرع الجزائري أقر حالات استثنائية يجوز فيها الخروج عن هذا الميعاد القانوني؛ بأن يتم إجراء التفتيش في أي ساعة من ساعات النهار والليل، وتعد الجرائم الإلكترونية من ضمن الحالات التي خصها المشرع الجزائري بالإستثناء، حيث جاء في الفقرة الثالثة (3) من المادة 47 من ق إ ج أنه (عندما يتعلق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الوطنية **أو الجرائم**

---

[1] خابت أمال، دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها في مواجهة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، المجلة الدولية للبحوث القانونية والسياسية، تصدر عن كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر، الوادي، الجزائر، المجلد 5، العدد3، ديسمبر 2021، ص 472.

[2] تنص المادة 47 من ق إ ج على أنه: (لا يجوز البدء في تفتيش المساكن أو معاينتها قبل الساعة الخامسة صباحا، ولا بعد الساعة الثامنة مساءا).

الماسة بالمعالجة الآلية للمعطيات ... فإنه يجوز إجراء التفتيش .. في كل محل سكني **في كل ساعة من ساعات النهار أو الليل** وذلك بناء على إذن مسبق من وكيل الجمهورية).

ويرجع السبب في استثناء المشرع الجزائري الجرائم الإلكترونية من شرط الميعاد القانوني، من جهة، إلى الطبيعة المتميزة لهذه الجريمة، حيث أن أدلة الإثبات فيها غير ملموسة وسهلة المحو والإتلاف والتعديل، ومراعاة الميعاد القانوني المقرر وفقا للمبدأ العام الذي جاءت به المادة 47 في فقرتها الأولى من ق إ ج قد يكون سببا في ضياع الأدلة ومن ثمة إعاقة سير عملية التحقيق، خاصة إذا وصل إلى علم المشتبه فيه أمر وجود التفتيش، حينها يكون من السهل عليه مسح الدليل أو التعديل فيه، لذلك ترك المشرع مسألة تقدير إجراء التفتيش للجهة القائمة بالتحقيق، لتتخير الوقت المناسب لذلك في أي وقت من أوقات النهار والليل دون قيد[1].

ومن جهة أخرى – وهو الأهم–أنه ليس لهذا الشرط أهمية تُذكر مع وجود تقنية التفتيش عن بُعد، الذي يمكن إجراؤه في أي وقت ومن أي مكان في العالم، مع العلم أن تحديد الوقت قد يختلف من دولة إلى أخرى، فالوقت الذي يكون نهارا في دولة معينة مثل كندا قد يكون ليلا في دولة أخرى مثل الجزائر[2].

إلى جانب استثناء المشرع الجزائري الجرائم الإلكترونية من شرط التقيد بالميعاد القانوني المقرر بالمادة 47 من ق إ ج، خص المشرع هذه الجرائم أيضا باستثناء آخر، بموجب الفقرة الأخيرة من المادة 45 من ق إ ج، التي تعفي الجهة المكلفة بالتفتيش من الإلتزام المقرر بذات المادة في فقرتها الأولى[3]؛ الذي مفاده وجوب حضور المتهم أو من ينوبه أو شاهدين عند الإقتضاء مجريات التفتيش، وذلك اعتبارا لخصوصية الجرائم الإلكترونية وما تتطلبه من إضفاء نوع من السرية أثناء جمع الدليل التقني فيها.

---

[1] رضا هميسي، المرجع السابق، ص 173.

[2] براهيمي جمال، المرجع السابق، ص 42.

[3] تنص المادة 45 في فقرتها الأولى من ق إ ج أنه: (إذا وقع التفتيش في مسكن شخص يشتبه أنه ساهم في ارتكاب جناية فيجب أن يحصل التفتيش بحضوره، وإذا تعذر عليه الحضور وقت إجراء التفتيش، فإن ضابط الشرطة القضائية ملزم بأن يكلفه بتعيين ممثل له، وإذا امتنع عن ذلك أو كان هاربا استدعى ضابط الشرطة القضائية لحضور تلك العملية شاهدين من غير الموظفين الخاضعين لسلطته).

ثالثا: تحرير محضر بإجراء التفتيش

لما كان التفتيش عملا من أعمال التحقيق، فإنه يتوجب تدوينه، ويكون ذلك بإعداد محضر يثبت فيه كل الإجراءات والخطوات المتخذة أثناء عملية التفتيش وما أسفر عنه من أدلة. ويجب أن يتضمن المحضر وصف العملية من بدايتها إلى نهايتها وكذا جرد الأشياء وضبطها التي تم حجزها أثناء عملية التفتيش، تاريخ تحريره وتوقيع محرره[1].

المبحث الثالث: الحجز الإلكتروني (saisir informatique)

يسعى القائم بالتفتيش إلى تحديد مكان البيانات المخزنة في المنظومة المعلوماتية التي تفيد في مجريات التحقيق، ويتم ضبطها بعد ذلك لتكون دليلا في إثبات الجريمة ونسبتها لمرتكبها. وعليه يعد ضبط الأدلة أو ما عبر عنه المشرع الجزائري بـ (حجز المعطيات المعلوماتية) النتيجة الطبيعية التي ينتهي إليها إجراء التفتيش الإلكتروني والأثر المباشر الذي ينتج عنه. ويقصد بالحجز الإلكتروني استخدام البرامج المهمة لغرض الوصول للبيانات المراد ضبطها إلى جانب وضع اليد على تلك الدعائم المادية[2].

نتناول فيما يلي **إجراءات وطرق تنفيذ الحجز الإلكتروني** في (الفرع الأول)، يليها نحدد **التزامات القائم بالحجز** في (الفرع الثاني).

الفرع الأول: إجراءات وطرق تنفيذ الحجز الإلكتروني

قد يقع الحجز الإلكتروني على أشياء مادية، كما قد يرد على أشياء معنوية تفيد في إظهار الحقيقة. ففي الفرض الذي يقع الحجز الإلكتروني على أشياء مادية كأجهزة الحاسوب ولواحقه وأجهزة التخزين وأجهزة الإرسال، يتم العمل بأحكام التفتيش التقليدي؛ إذ جاء في المادة 84 من ق إ ج، أنه لابد من جرد هذه الأشياء وتحرير محضر عنها وإرفاقه بملف الإجراءات، كما ينبغي على القائم بالتفتيش والحجز أن يحافظ على هذه الأجهزة بالحالة التي كانت عليها[3].

---

[1] هميسي رضا، المرجع السابق، ص. ص (169-170)؛ براهيمي جمال، المرجع السابق، ص 44.

[2] شنتير خضرة، المرجع السابق، ص 101.

[3] رضا هميسي، المرجع نفسه، ص 174.

أما وإن تعلق الأمر بالبيانات المعالجة والمخزنة في النظم المعلوماتية، فإنه يتم حجزها بطريقتين؛ إما من خلال **عمل نسخة من المعطيات الإلكترونية**، أو **عن طريق منع الوصول إلى تلك المعطيات**، نشرح ذلك فيما يلي:

أولا: الحجز عن طريق نسخ المعطيات الإلكترونية

جاء في المادة السادسة (6) من القانون رقم 09-04 أنه: (عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية)

ويتم اللجوء إلى عملية النسخ عندما يكون من غير الضروري حجز كل المنظومة المعلوماتية، حيث يعمل القائم بالتفتيش على نسخ وحفظ المعطيات الإلكترونية في دعامات تخزين إلكترونية، كالأقراص المضغوطة أو المتحركة، الأشرطة المغناطيسية، القرص الصلب والقرص المرن وغيرها؛ ذلك أنه من غير الممكن التعامل مع المعطيات، التي هي عبارة عن نبضات أو ذبذبات إلكترونية أو إشارات ممغنطة، إلا بعد نسخها على دعامات أو وسائط. وقد قصد المشرع الجزائري إدراج عبارة (دعامات تخزين إلكترونية) وهي عبارة واسعة من شأنها احتواء ما قد يظهر ويُستجد من تقنيات تخزين جديدة بناء على التطورات التقنية المذهلة في مجال صناعة الحواسيب وملحقاتها[1].

وتمتد عملية النسخ أيضا إلى المعطيات اللازمة لفهم المعطيات محل التفتيش، حيث أنه من المحتمل أن هذه الأخيرة لا تقرأ مباشرة إلا بتدخل وسائل معينة ومعطيات أخرى[2].

ثانيا: الحجز عن طريق منع الوصول للمعطيات الإلكترونية

تتضمن هذه الطريقة تدابير جديدة استُحدِثت خِصِيصا لضبط الأدلة الجنائية الرقمية، في الفرض الذي يستحيل فيه نسخ المعطيات الإلكترونية لأسباب تقنية؛ قد تتعلق مثلا بالمنظومة

[1] يزيد بوحليط، المرجع السابق، ص 91.

[2] هميسي رضا، المرجع السابق، ص 176.

المعلوماتية كاستحالة الدخول لوجود كلمة السر أو بسبب وجود نظام حماية من الصعب اختراقه، كما قد يرتبط المانع من النسخ بعملية نسخ المعطيات ذاتها بسبب التطور الدائم في هذه التقنيات وما يتطلبه ذلك من توفير الوسائل التقنية اللازمة[1].

في هذا الإطار جاء في المادة السابعة (7) من القانون رقم 09-04 أنه (إذا استحال إجراء الحجز وفقا لما هو منصوص عليه في المادة 6 أعلاه، لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، أو إلى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة)، بذلك منح المشرع للسلطة المكلفة بالتفتيش استعمال ما يكون مناسبا من تقنيات وتدابير حماية فنية كتقنيات التشفير والترميز، وبرامج منع الكتابة ونحوها[2]. والهدف من هذا الإجراء هو الحفاظ على الأدلة في محيطها الإلكتروني وعدم تمكين المجرم من الوصول إلى المعطيات الإلكترونية ومن ثمة طمسها أو تدميرها أو تعديلها أو إخفاء معالمها[3].

كما أعطت المادة الثامنة (8) من القانون رقم 09-04[4] أهمية كبيرة للمعطيات ذات المحتوى المجرم؛ بأن أكدت على اتخاذ ما يلزم من تدابير لمنع الإطلاع عليها، لاسيما من خلال تكليف أي شخص مؤهل لاتخاذ الوسائل التقنية المناسبة[5]، ويلاحظ أن المشرع هنا قد أشار إلى دور الخبرة الفنية في التحقيق في شأن الجرائم الإلكترونية، الذي أصبح ضرورة لا غنى، في سبيل المحافظة على المعطيات الإلكترونية ذات المحتوى المجرم، فإذا تعذر على القائم بالتفتيش أن يقوم باتخاذ التدابير المناسبة للحفاظ على المعطيات بنفسه يمكنه أن يستعين بأهل الخبرة من ذوي الإختصاص، ذلك أن إساءة التعامل مع هذه المعطيات أحيانا، مِمَن ليس له دراية كافية

---

[1] يزيد بوحليط، المرجع السابق، ص 91.

[2] براهيمي جمال، المرجع السابق، ص 48.

[3] هميسي رضا، المرجع السابق، ص. ص (176 – 177).

[4] تنص المادة الثامنة (8) من القانون رقم 09 -04 أنه: (يمكن السلطة التي تباشر التحقيق أن تأمر باتخاذ الإجراءات اللازمة لمنع الإطلاع على المعطيات التي يُشكل محتواها جريمة، لاسيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك).

[5] نشير إلى أن ذلك يعد خروجا عما أقرته المادة 84 من ق إ ج، التي اشارت إلى أنه إذا أسفر التفتيش على مستندات فإنه يحق فقط لقاضي التحقيق أو ضابط الشرطة القضائية المناب الحق في الإطلاع عليها قبل ضبطها.

بنظم المعلومات وبرامجها، قد يؤدي إلى ضياع الدليل الرقمي[1]، وبإمكان الجهة القائمة بالتفتيش أن تستعين بالهيئة الوطنية للوقاية من الجرائم الإلكترونية.

بالإضافة إلى إجراءات الحجز بنوعيه نصت المادة 394 مكرر 6 من ق ع على تدابير أخرى، كمصادرة الأجهزة والبرامج والوسائل المستخدمة وإغلاق المواقع الإلكترونية التي تكون محلا للجريمة، كالمنع من الوصول إلى المواقع الإباحية أو المواقع الإرهابية التي تدعو إلى الأفكار المضللة وتوضح كيفيات صنع القنابل.

الفرع الثاني: التزامات القائم بالحجز الإلكتروني

يتعين على القائم بالحجز أن **يتحرى سلامة المعطيات ويتخذ ما يراه مناسبا من تدابير في سبيل تحقيق ذلك** (أولا)، كما عليه أيضا أن يقتصر في **ضبط المعطيات الإلكترونية على ما يراه كافيا في كشف الحقيقة** (ثانيا).

أولا: تقيد القائم بالحجز بالتزام المحافظة على سلامة المعطيات

تحتاج عملية الضبط والتحريز، بالنظر للطبيعة الخاصة للأشياء محل التفتيش الإلكتروني، إلى اتخاذ إجراءات خاصة لحمايتها فنيا ومنع العبث بها، لذلك ألزمت المادة السادسة في فقرتها الثانية من القانون رقم 09-04 القائم بالتفتيش والحجز أن يحافظ على سلامة المعطيات المحجوزة، حيث نصت أنه (يجب في كل الأحوال على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية).

فالتهاون في توفير ما يلزم من التدابير لضمان سلامة المعطيات قد ينجر عنه ضياع الدليل الرقمي، ففي قضية تدور وقائعها في قيام إحدى الشركات الأمريكية بالإبلاغ عن قيام أحد الأشخاص بوضع قنبلة منطقية في النظام المعلوماتي الخاص بالشركة، وعند التحقيق في الأمر اتضح أن الشركة وقبل إبلاغ السلطات المختصة كانت قد استدعت خبيرا للتأكد من الأمر وإزالة القنبلة المنطقية، وكان الخبير قد نجح في إزالة القنبلة، غير أنه اتضح لاحقا أنه بإزالة القنبلة تم إتلاف الدليل الرقمي الذي يؤكد وجود الجريمة، كما حدث أيضا بإحدى دوائر الشرطة في الولايات الأمريكية المتحدة أن طلبت جهات التحقيق من الشركة التوقف عن تشغيل نظامها المعلوماتي

[1] بوعناد فاطمة الزهراء، المرجع السابق، ص 71.

بهدف وضعه تحت المراقبة لغرض كشف مرتكب الجريمة ونتيجة لذلك أُتلف ما كان قد سلم من ملفات وبرامج[1].

في سياق ذو صلة، أشارت الفقرة الثالثة من المادة 19 من اتفاقية بودابست إلى بعض التدابير الخاصة بتحريز المعطيات الإلكترونية محل الضبط، التي من شأنها أن تضمن سلامة المعطيات الإلكترونية، نذكر منها مثلا:

– أخذ نسخ إحتياطية من دعائم البيانات والمعطيات المضبوطة والعمل عليها لتجنب المساس بالدليل الأصلي؛

– تأمين البرامج المعلوماتية المضبوطة فنيا قبل تشغيلها؛

– الأخذ في الإعتبار ظروف الحرارة والرطوبة المناسبة في أماكن تخزين الأقراص والأشرطة الممغنطة المحرزة، مع تفادي تعريضها للأضواء أو لأي سائل من السوائل.

وبحسب مفهوم الفقرة الثالثة من المادة السادسة (6) من القانون رقم 09-04، لا يعد من قبيل المساس بسلامة المعطيات الإلكترونية، لجوء القائم بالتفتيش لتشكيل المعطيات المحجوزة أو إعادة تشكيلها بهدف جعلها قابلة للإستغلال، وذلك باستعمال الوسائل التقنية اللازمة، بشرط ألا يؤدي ذلك إلى المساس بمحتوى المعطيات الإلكترونية، كأن يؤدي مثلا إلى تعديل مضمونها أو محو جزء منها أو تعطيل جزء آخر[2].

ثانيا: تقيد القائم بالحجز بحدود ما تتطلبه مقتضيات التحقيق

أشارت المادة 84 من ق إ ج بضرورة ألا تتعدى عملية الضبط تحصيل ما ينفع من الأشياء والوثائق النافعة في إظهار الحقيقة، وتأكيدا لذلك جاء في المادة التاسعة (9) من القانون رقم 09-04 أنه لا يجوز استعمال المعلومات المتحصل عليها إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية.

ومن الصعوبات التي تطرح في هذا السياق، أنه أحيانا يكون من غير الممكن عزل المعطيات الإلكترونية الهامة في إثبات الجريمة عن المنظومة المعلوماتية التي تحتويها، مِمَا يقود

---

[1] شنتير خضرة، المرجع السابق، ص. ص (110 -111).

[2] رضا هميسي، المرجع السابق، ص 176.

بالضرورة القائم بالحجز إلى ضبط المنظومة بأكملها لمدة معينة، وهو الأمر الذي قد يكلف أصحاب المشاريع خسائر طائلة، لذلك يتعين على القائم بالحجز تحري نوعا من المرونة أثناء عملية الحجز، بإعمال ما يعرف بمبدأ التناسب، لغرض إقامة التوازن بين مصلحتين؛ من جهة مصلحة الدولة في الكشف عن الحقيقة ومن جهة أخرى مصلحة صاحب النظام في تسيير أعماله وعدم ضياع فرص الربح في المشاريع الإقتصادية. ويقصد بمبدأ التناسب اقتصار إجراء الضبط على الأدلة الضرورية التي تفيد في التحقيق دون أن ينجر على ذلك تعطيل كل العمل بالنظام والشبكات المتصلة به. ومن التطبيقات القضائية فيما يخص مبدأ التناسب ما قضت به المحكمة الألمانية الفدرالية بإلغاء قرار الضبط الذي انصب على 220 قرص بالإضافة إلى الوحدة المركزية لمخالفته مبدأ التناسب[1].

المبحث الرابع: التزامات مقدمي خدمة الأنترنت

تسمح شبكة الأنترنت بتبادل المعلومات بغض النظر عن البعد المكاني والإختلاف الزماني من دولة لأخرى، ويتطلب الدخول إلى هذه الشبكة تدخل وسيط يطلق عليه مزود خدمة الأنترنت. ويقوم هذا الأخير بربط مستخدم الأنترنت بالمواقع أو بربطه مع غيره من المستخدمين، فمثلا الرسالة البريدية التي يبعث بها شخص إلى آخر تمر حتما على مزود الخدمة.

نتناول في (المطلب الأول) **تعريف مقدم خدمة الأنترنت وأصنافهم**، ثم نفصل في (المطلب الثاني) في **التزاماته**.

المطلب الأول: تعريف مزودي خدمة الأنترنت وأصنافهم

نحدد **تعريف مزودي خدمة الأنترنت** (الفرع الأول)، ثم **أصنافهم** (الفرع الثاني).

الفرع الأول: تعريف مزودي خدمة الأنترنت

عرف المشرع الجزائري في البند (د) من المادة الثانية (2) من القانون رقم 09-04 ما سماه بمقدم الخدمة **(fournisseur de service)** أنه: (1 – أي كيان عام أو خاص يقدم لمستعملي خدماته، القدرة على الإتصال بواسطة منظومة معلوماتية و/ أو نظام اتصالات.

[1] براهيمي جمال، المرجع السابق، ص 54؛ شنتير خضرة، المرجع السابق، ص 109.

2 –وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الإتصال المذكورة أو لمستعمليها).

وقد حدد المشرع الجزائري مزودي خدمات الأنترنت، على حسب الدور المنوط بهم، فمن خلال عبارة (أي كيان عام أو خاص يقدم لمستعملي خدماته، القدرة على الإتصال بواسطة منظومة معلوماتية و/ أو نظام اتصالات)، التي وردت بالمادة الثانية – أعلاه –من القانون رقم 09-04، يتضح الدور الذي يقوم به مزودو الخدمات الذين يقومون بتوفير الوسائل الفنية اللازمة لربط شبكات الإتصال وتمكين العملاء من الوصول إلى المادة المعلوماتية المَبْثُوثَة عبر الأنترنت، كناقل المعلومات ومتعهد خدمة الدخول، كما استعمل المشرع الجزائري في المادة الثانية (2) أعلاه من ذات القانون عبارة (وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الإتصال المذكورة أو لمستعمليها) ويتضح من خلال هذه العبارة الدور الذي يقوم به مقدموا الخدمات الذين يوفرون خدمة معالجة أو تخزين المعطيات المعلوماتية كمتعهدوا خدمة الإيواء (fournisseur d'hébergement).

الملاحظ على هذا التعريف أيضا أنه أقرب إلى التصنيف منه إلى التعريف، وذلك أمر منطقي، حيث من الصعب إيجاد تعريف جامع ومانع يحتوي جميع ما يندرج ضمن مزودي خدمة الأنترنت، فمع التطورات المتسارعة في ميدان تكنولوجيا المعلومات يكون من الصعب حصر كافة الأشخاص الوسطاء في شبكة الأنترنت.

الفرع الثاني: أصناف مزودي خدمة الانترنت

قام المشرع الجزائري، من خلال المادة الثانية من القانون رقم 09 – 04، بتصنيف مزودي خدمة الأنترنت، على أساس نوع الخدمة التي تقع على عاتقهم؛ ما إذا كانت خدمة اتصال، أو خدمة تخزين، أو خدمة معالجة للبيانات. نتطرق فيما يلي إلى أهم مقدمي الخدمات الوسيطة في الأنترنت:

أولا: ناقل المعلومات

ناقل المعلومات(transmetteur) هو كل شخص طبيعي أو معنوي، يلتزم بموجب عقد نقل المعلومات الذي يربطه بعملائه، بتقديم الوسائل الفنية الضرورية لعملية النقل المادي للمضمون

المعلوماتي[1]، وعادة ما تقوم بهذه العملية الهيئات العامة للإتصال في الدولة، فاتصالات الجزائر مثلا هي التي تقوم بدور ناقل المعلومات في الجزائر، وتوجد إلى جانبها بعض الشبكات الخاصة كمقدم الخدمة موبيليس ونجمة[2].

ثانيا: متعهد خدمة الدخول

متعهد خدمة الدخول هو من يقوم بتزويد مستخدمي الشبكة بالوسائل والأجهزة التقنية الضرورية التي تمكنهم من الدخول إلى شبكة الأنترنت، ومن هذه الوسائل مثلا المودام (modem)[3]. ومن أمثلة مقدمي خدمات الوصول في الجزائر، (DJAWEB)، (FAWRI) في القطاع العام، و(ASSILA BOX)، (EEPAD) في القطاع الخاص[4].

ثالثا: متعهد خدمة الإيواء

متعهد الإيواء هو كل شخص طبيعي أو معنوي يتولى تخزين البيانات والمعلومات التي يبثها أصحاب المواقع الإلكترونية على حاسباته الآلية المرتبطة بصفة دائمة بشبكة الأنترنت، بالشكل الذي يُمكِن أصحاب هذه المواقع من إِطْلاَعِ الجمهور على مضمونها المعلوماتي على مدار الساعة[5].

ويعد متعهد الإيواء بمثابة المؤجر لمكان على الشبكة؛ إذ يعرض إيواء الصفحات (Web site) على حاسباته الخادمة مقابل أجر، ويكون للمستأجر الحرية في إنشاء ما يريد من صور أو نصوص أو تنظيم مؤتمرات أو حلقات نقاشية أو إنشاء روابط معلوماتية مع مواقع أخرى[6].

---

[1] أحمد قاســم فرح، النظام القانوني لمقدمي خدمات الأنترنت، (دراســة تحليلية مقارنة)، المنارة، المجلد 13، العدد 9، 2007. المرجع السابق، ص 329.

[2] عكو فاطمة الزهراء، المســؤولية المدنية لمقدمي الخدمة الوســيطة في الأنترنت، رســالة دكتوراه، قانون خاص، كلية الحقوق، جامعة الجزائر1، السنة الجامعية 2016/2015، ص 27.

[3] عبد المهدي كاظم ناصر، المسؤولية المدنية لوسطاء الأنترنت، مجلة القادسية للقانون والعلوم السياسية، كلية القانون، جامعة القادسية، العراق، المجلد الثاني، العدد الثاني، 2009، ص 231.

[4] عكو فاطمة الزهراء، المسؤولية المدنية لمقدمي الخدمة ....، المرجع السابق، ص 26.

[5] أحمد قاسم فرح، المرجع نفسه، ص. ص (324 – 325).

[6] عبد المهدي كاظم ناصر، المرجع نفسه، ص. ص (229 – 228).

المطلب الثاني: التزامات مقدمي خدمات الأنترنت

يتمثل دور مقدم خدمة الأنترنت في تمكين المستخدم من الدخول إلى الشبكة والإطلاع عما يبحث عنه، الأمر الذي يمكنه من معرفة جميع الخطوات التي يتبعها المستخدم وكذا المواقع التي زارها والمعلومات التي قام بتخزينها وجميع الإتصالات التي أجراها، لذلك قد يكون لدى مقدم خدمة الأنترنت من المعلومات ما من شأنه أن يساعد جهات التحقيق والتحري في الوصول إلى المعلومات التي تفيد في كشف الحقيقة عن الجريمة الإلكترونية وشخص مرتكبها.

على هذا الأساس، قيد المشرع الجزائري مقدم خدمة الأنترنت بمجموعة من الإلتزامات، **منها ما يتعلق بمعطيات المرور** (الفرع الأول) ومنها ما **يخص المعطيات المرتبطة بالمحتوى غير المشروع** (الفرع الثاني).

الفرع الأول: الإلتزامات المتعلقة بمعطيات المرور

وضع المشرع الجزائري على عاتق مقدم خدمة الأنترنت في المادة 10 من القانون رقم 09-04 التزامات لها علاقة بمعطيات السير، تتمثل في **ضرورة حفظها، وكذا الإلتزام بسريتها**(أولا)، كما أوجب عليه أيضا ضرورة **التعاون مع جهات البحث والتحري المختصة من خلال وضع هذه المعطيات تحت تصرف هذه الأخيرة** (ثانيا).

أولا: الإلتزام المتعلق بحفظ معطيات السير

يلتزم مزود خدمة الأنترنت بحفظ معطيات حركة السير، نحاول أن نتعرف على هذا الإلتزام من خلال تعريف الحفظ، ومحله المتمثل في معطيات حركة السير(1)، ثم نوضح التمييز بين حفظ معطيات حركة السير والحفظ العاجل لمعطيات حركة السير (2)، ثم المدة القانونية المقررة لحفظها (3).

1) تعريف عملية الحفظ ومحلها:

يُقصد بعملية الحفظ قيام مزود خدمة الأنترنت بتجميع المعطيات الإلكترونية التي يتم من خلالها التعرف على هوية مستعملي الخدمة، ومن ثمة حفظها في أرشيف وفق ترتيب معين، يُمَكِن جهات التحقيق لاحقا من استغلالها لمقتضيات التحقيق[1].

وتنصب عملية الحفظ على معطيات المرور (données relatives au traffic)، أو كما سماها المشرع الجزائري بالمعطيات المتعلقة بحركة السير، وعرفها في البند (ه) من المادة الثانية (2) من القانون رقم 09-04 على أنها: (أي معطيات متعلقة بالإتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حركة اتصالات، توضح مصدر الإتصال، والوجهة المرسل إليها، والطريق الذي يسلكه، ووقت وتاريخ وحجم ومدة الإتصال ونوع الخدمة).

وقد أخذ المشرع هذا التعريف من البند (د) من المادة الأولى من اتفاقية بودابست، وكان التقرير التوضيحي للإتفاقية قد وضح بأن المعطيات المتعلقة بالمرور هي طائفة من البيانات الإلكترونية التي تخضع لنظام قانوني معين، وتنشأ هذه البيانات عن طريق أجهزة الحاسب في سلسلة من الإتصالات، من أجل توجيه الإتصال من منبعه أو أصله إلى مكان وصوله، وعلى ذلك فهي ملحقات الإتصال في حد ذاته.

إذا فالمعطيات الخاصة بحركة السير هي الملحقات الخارجية الخاصة بالإتصال، المرتبطة بتحديد الهوية (المرسل والمرسل إليه)، أو الإتصال (مدة ونوع وحجم الخدمة ...)[2]، ولا علاقة لها بفحوى الإتصال أو مضمونه.

وقد حددت المادة 11 من القانون رقم 09-04 المعطيات التي لابد من حفظها، وهي:

أ – المعطيات التي تسمح بالتعرف على مستعملي الخدمة؛
ب – المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للإتصال؛
ج – الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال؛
د – المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها؛

[1] براهيمي جمال، المرجع السابق، ص 101.
[2] عكو فاطمة الزهراء، المسؤولية المدنية لمقدمي الخدمة ...، المرجع السابق، ص 161.

هـ – المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الإتصال (كأرقام الهاتف مثلا أو عناوين بروتوكول الأنترنت) وكذا عناوين المواقع المطلع عليها.

بالنسبة لنشاطات الهاتف يقوم المتعامل بحفظ المعطيات المذكورة في الفقرة (أ) من هذه المادة وكذا تلك التي تسمح بالتعرف على مصدر الإتصال وتحديد مكانه.

2) التمييز بين حفظ معطيات حركة السير والحفظ العاجل للبيانات:

يجب عدم الخلط بين إجراء حفظ معطيات حركة السير، الذي نصت عليه المادة 10 من القانون رقم 09 – 04، أو كما يسمى عند البعض بـــ (الحفظ الشامل للبيانات) وبين إجراء آخر لم ينص عليه المشرع الجزائري ولم يحدد أحكامه، في الوقت الذي نصت عليه تشريعات أخرى، وهو إجراء (الحفظ العاجل لبيانات حركة السير) أو (إجراء التجميد السريع لبيانات حركة السير).

ويقصد بإجراء الحفظ العاجل لمعطيات حركة السير، صدور أمر قضائي من سلطة التحقيق المختصة إلى مزود خدمة الأنترنت، يتضمن إلزامه بحفظ البيانات المخزنة لديه، وحمايتها من كل ما يؤدي إلى إتلافها، أو تجريدها من صفتها أو حالتها الراهنة، وذلك لفترة معينة. ويعد هذا الإجراء ذو طابع وقائي، يتم اللجوء إليه خلال فترة التحقيقات القضائية الطويلة نسبيا، تجنبا لحذف البيانات ذات الصلة بالجريمة[1].

وعليه، يهدف كلا من الإجراءين إلى الحيلولة دون حذف البيانات التي لها علاقة بالجريمة، من مُنطلق أن الأدلة الرقمية تتميز بسرعة اندثارها وتلاشيها، فعنصر الوقت عامل مُهم في السير الحسن لإجراءات التحقيق في الجرائم الإلكترونية، غير أنهما يختلفان من ناحية أن إجراء حفظ معطيات حركة السير، الذي جاءت أحكامه بالمادتين 10 و11 من القانون رقم 09 – 04، هو التزام عام يتعلق بحفظ مزود خدمة الأنترنت لبيانات حركة السير لجميع المستخدمين، دون استثناء، لمدة معينة، بُغية استغلالها مستقبلا لمقتضيات التحقيق، مع التأكيد على أن ما يقوم به مزود الخدمة هو مجرد تخزين لا غير، حيث لا يقع على عاتقه واجب حماية هذه المعطيات من التلف والتغيير، في حين أن إجراء الحفظ

[1] لهوى رابح، المرجع السابق، ص 120.

العاجل لمعطيات الســـير، هو إلزام مزود خدمة الأنترنت، بناء على قرار قضـــائي، ولمدة معينة، بحفظ البيانات المتصـلة بالأشـخاص المشـتبه فيهم فقط، التي كان قد سـبق لمزود خدمة الأنترنت أن قام بتخزينها وتجميعها، بحكم مهامه العادية[1]، والعمل على حمايتها من كل ما يعرضها لخطر التغيير أو التجريد من صفتها أو حالتها الراهنة[2].

3) المدة القانونية المقررة لعملية الحفظ:

قيد المشرع الجزائري عملية الحفظ بمدة معينة، حيث جاء في المادة 11 فقرة 3 من القانون 09-04 أنه: (تحدد مدة حفظ المعطيات المذكورة في هذه المادة بسنة واحدة ابتداء من تاريخ التسجيل).

كما يقع على عاتق مقدمي الخدمات أيضا المحافظة على سرية عملية الحفظ، وعليهم كتمان المعلومات التي قاموا بجمعها بناء على طلب من المحققين، وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق[3].

ولم تحدد المادة أعلاه مصير المعطيات التي تم الإحتفاظ بها بعد المدة القانونية المقررة لحفظها، غير أنه يُفهم منها أنه يتعين على مزود خدمة الأنترنت فور انتهاء هذه المدة إزالة كل المعطيات التي تم تخزينها أو على الأقل وضع الترتيبات التقنية التي تضمن عدم إمكانية الإطلاع عليها، حفاظا على سريتها وخصوصيتها، وإلا تعرض لعقوبات إدارية وأخرى جزائية قد تصل إلى عقوبات سالبة للحرية[4]. بل أنه عندما يؤدي إخلاله بالإلتزامات المذكورة إلى عرقلة حسن سير التحريات القضائية، فإن ذلك يعرضه للعقوبة المحددة في نص المادة 11 من القانون رقم 09-04.

---

[1] فمثلا الرسالة البريدية التي يقوم مزود خدمة الأنترنت باستقبالها من المرسل، فإنها تستقر في حالة تخزين لدى مزود خدمة الأنترنت، وتكون حينئذ النسخة من الإتصال في هذه الحالة مخزنة، وتتواجد كإجراء مؤقت في انتظار إرسالها من مقدم خدمة الأنترنت إلى شخص المرسل إليه، وبمجرد وصول الرسالة إلى المرسل إليه، تكون حينها هذه الأخيرة قد وصلت إلى وِجهتها الأخيرة، وهنا يكون موقف مزود خدمة الأنترنت يتراوح بين إما القيام بمسح الرسالة أو القيام بحفظها.

[2] لهوى رابح، المرجع السابق، ص123.

[3] عكو فاطمة الزهراء، المسؤولية المدنية لمقدمي الخدمة ...، المرجع السابق، ص 158.

[4] براهيمي جمال، المرجع السابق، ص 105.

ثانيا: الإلتزام بوضع معطيات السير تحت تصرف القائمين بالتحقيق

يعد هذا الإجراء عملية مكملة لإجراء حفظ معطيات المرور، السابق الإشارة إليه، حيث جاء في المادة 10 من القانون رقم 09-04 التي تنص أنه: (في إطار تطبيق أحكام القانون يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية .... وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 أدناه، تحت تصرف السلطات المذكورة ...). بذلك تتمكن سلطات البحث والتحقيق من التعرف على منبع الإتصال ومُنتَهَاه، وهي معلومات قد تساعد في التعرف على هوية الأشخاص المتورطين في الجرائم الإلكترونية وكذا الكشف عن فحوى اتصالاتهم[1].

الفرع الثاني: الإلتزامات المتعلقة بمعطيات المحتوى

ألزم المشرع الجزائري مقدم خدمة الأنترنت باتخاذ التدابير التحفظية التي من شأنها وقف بث النشاط غير المشروع، حيث يلتزم بسحبه في الفرض الذي يصل إليه العلم بوجوده(أولا)، أو وضع الترتيبات التقنية التي تؤدي إلى حصره ومنع وصول الجمهور إليه(ثانيا).

أولا: الإلتزام بسحب المحتوى غير المشروع

ألزمت المادة 12 بند (أ) من القانون رقم 09-04 مقدمي خدمات الأنترنت بالتدخل الفوري لسحب المحتوى المعلوماتي غير المشروع، أو منع الوصول إليه، بمجرد العلم بذلك.

لفهم هذا الإلتزام نتطرق في نقطة أولى إلى **المقصود بالمحتوى غير المشروع**، ثم في نقطة ثانية إلى **إجراءات سحب المحتوى المعلوماتي غير المشروع**.

1) المقصود بالمحتوى المعلوماتي غير المشروع:

يقصد بالمحتوى المعلوماتي غير المشروع كافة الأفعال غير المقبولة التي يقوم بها شخص أو مجموعة من الأشخاص، عن عمد أو إهمال، في البيئة الرقمية، وتلحق الضرر بشخص معين أو عدة أشخاص. وقد يتضمن المحتوى الإلكتروني غير المشروع ما يدخله في دائرة التجريم

[1] براهيمي جمال، المرجع السابق، ص 108.

كاحتوائه على عبارات السب أو القذف مثلا، أو نشر صور جنسية عبر صفحات الويب، أو التحريض على العنصرية والكراهية، كما قد يشمل المحتوى غير المشروع تعديا على حقوق الآخرين أو أمرا يضر بهم، كالتعدي على حقوق الملكية الفكرية. ويمكن القول عموما أن الإعتداءات التي يتضمنها المحتوى الإلكتروني غير المشروع هي نفسها – بالتقريب –التي تقع في العالم الحقيقي[1].

2) إجراءات سحب المحتوى المعلوماتي غير المشروع:

لا يعتبر مزود خدمة الأنترنت مسؤولا عن المحتوى المعلوماتي غير المشروع الذي يتكفل بنقله أو التي يُؤْوِيه، إلا إذا كان على علم به، سواء بطريقة مباشرة أو غير مباشرة، وفقا لما أشارت إليه المادة 12 من القانون رقم 09 – 04، ولكن ما هو العلم المطلوب لقيام مسؤوليته، ومن هي الجهة المخول لها قانونا تحديد عدم مشروعية المحتوى المعلوماتي ومن ثمة المطالبة بسحبه أو وقف بثه؟

لم يحدد المشرع الجزائري هذه المسائل في المادة 12 من القانون رقم 09 – 04، والمعمول به لدى تشريعات الدول المقارنة، أن العلم المعتد به قانونا هو العلم المؤكد (لا المفترض) بالطبيعة غير المشروعة للمحتوى الإلكتروني، الذي يتأتى من خلال التبليغ، فالعلم مقترن إذا بالتبليغ، خاصة إذا لم تكن صفة عدم المشروعية ظاهرة بالشكل الكافي. ففي فرنسا مثلا، يُعطي القانون الفرنسي المتعلق بـ "الثقة في الإقتصاد الرقمي" الحق في تبليغ مزود خدمة الأنترنت بوقف المضمون الإلكتروني غير المشروع للسلطة القضائية وللشخص المتضرِّر من بثِّه. ويمكن أن تقوم مسؤولية مقدم خدمة الأنترنت عن المحتوى غير المشروع دون تبليغه به، أي أن علمه بوجوده يكون مفترضاً، عندما تكون صفة عدم مشروعية المضمون ظاهرة بما يكفي، والمعيار هنا موضوعي[2].

---

[1] بن عزة أحمد حمزة، **المسـؤولية القانونية لمتعاملي الأنترنت**، (دراسـة مقارنة)، أطروحة دكتوراه علوم، قانون إعلام، كلية الحقوق والعلوم السياسية، جامعة جيلالي اليابس، سيدي بلعباس، السنة الجامعية 2019/2018، ص. ص (84 – 85).

[2] أحمد قاسم فرح، المرجع السابق، ص 371.

وإن لم تحدد المادة 12 من القانون 09-04 الإجراءات التي ينبغي اتباعها، من حيث صاحب الحق في طلب سحب المحتوى غير المشروع والجهة التي يُلجأ إليها بهذا الطلب، إلا أن المادة 394 مكرر 8 من ق ع، التي أضافها المشرع الجزائري بموجب القانون رقم 16-02 المعدل والمتمم لقانون العقوبات[1]، جاءت بقواعد جديدة في هذه المسألة، في الفرض الذي يحمل المحتوى غير المشروع في طياته صفة التجريم، وما يُفهم من نص المادة 394 مكرر 8 من ق ع أن علم مقدم خدمة الأنترنت بالصفة الجرمية للمضمون الإلكتروني يتم من خلال إخطاره بذلك بموجب قرار قضائي من الجهات القضائية أو بناء على إعذار من الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها. كما أن ذات المادة أدرجت الإخلال بهذا الإلتزام تحت طائلة التجريم، الأمر الذي يجعل مقدمي خدمة الأنترنت في وضعية قانونية تسمح للجهات القضائية إثارة مسؤوليتهم الجزائية عن سلبيتهم اتجاه المضامين ذات المحتوى المجرم[2].

ثانيا: الإلتزام بوضع الترتيبات التقنية لمنع وصول الجمهور للمحتوى غير المشروع

فرضت المادة 12 في بندها (ب) من القانون رقم 09-04 على مزودي خدمة الأنترنت وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة وإخبار المشتركين لديهم بوجودها.

ويلاحظ على هذا الإلتزام أنه ما هو إلا إعادة لما هو محدد بالمادة 14 فقرة أخيرة من المرسوم التنفيذي رقم 98 – 257 الذي يضبط شروط وكيفيات إقامة خدمات "أنترنت" واستغلالها، التي نصت على ضرورة (اتخاذ الإجراءات اللازمة لتأمين حراسة دائمة لمضمون الموزعات المفتوحة لمشتركيه، قصد منع النفاذ إلى الموزعات التي تحتوي معلومات تتعارض مع النظام العام).

---

[1] القانون رقم 16-02 المؤرخ 19 يونيو 2016، المعدل والمتمم لقانون العقوبات (ج ر: عدد 37، لسنة 2016، ص 4).

[2] عكو فاطمة الزهراء، ملاحظات حول التزامات مزود الوصول إلى الأنترنت لوقف نشر المحتوى غير المشروع بعد إضافة المادة 394 مكرر 8 من ق ع في القانون رقم 16 – 02، مجلة الحقوق والعلوم السياسية، تصدر عن كلية الحقوق والعلوم السياسية، جامعة الجيلالي اليابس سيدي بلعباس، الجزائر، العدد 13، 2017، ص. ص (55-57).

في هذا المجال قامت اتصالات الجزائر عام 2013 باطلاق برنامج " في أمان" الخاص بخدمة المراقبة الأبوية، الذي يهدف إلى تمكين الأولياء من مراقبة أطفالهم وحمايتهم من مخاطر الأنترنت. "في أمان" برنامج يتم بموجبه تصفية وحجب جميع المواقع التي يعتبرها الأولياء خطرا على أبنائهم، كما يمكن تحديد جداول يومية لتوقيت استعمال الأنترنت.

الفصل الثالث

الآليات المؤسساتية الوطنية والتعاون الدولي لمواجهة الجريمة الإلكترونية

إن الطبيعة التقنية المعقدة للجريمة الإلكترونية دفعت المشـرع الجزائري إلى إنشـاء هيئات متخصـصـة، بهدف تحقيق الفعالية في مواجهتها، سـواء كانت هذه الهيئات المتخصـصـة على مستوى الجهاز القضـائي بحد ذاته، والذي تجسد من خلال استحداث المشرع الجزائري للقطب الجزائي المتعلق بالجرائم الإلكترونية (المبحث الأول). كما أنشأ المشرع الجزائري قبل ذلك هيئة مُســـاعدة للجهاز القضـــائي تمثل في الهيئة الوطنية للوقاية من الجرائم الإلكترونية (المبحث الثاني).

من جهة ثانية، فإن الطبيعة الدولية والعابرة للحدود لهذه الجرائم، لفت الإنتباه إلى ضـرورة تعزيز التعاون الدولي وتطويره في هذا المجال (المبحث الثالث).

المبحث الأول: الجهات القضائية المختصة بالجرائم الإلكترونية

توجه المشـرع الجزائري نحو التخصـص القضـائي في المادة الجزائية بموجب القانون رقم 04 – 14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون الإجراءات الجزائية[1]، الذي أنشاء الجهات القضـائية الجزائية ذات الإختصـاص الموسـع، التي يؤول إليها الإختصـاص في عدد من الجرائم الخطيرة، وتُعد جرائم المعالجة الآلية للمعطيات من بينها، غير أن ما تتســم به الجريمة الإلكترونية من تعقيدات تقنية بالغة دفعت المشـرع الجزائري مُؤخرا إلى اسـتحداث جهة

[1] القانون رقم 04 – 14 المؤرخ في 10 نوفمبر 2004، يُعدِل ويتمم الأمر رقم 66 – 155، المتضـــمن قانون الإجراءات الجزائية، (ج ر: عدد 71، بتاريخ 10 نوفمبر 2004، ص4).

قضائية وطنية متخصصة بالجرائم الإلكترونية تُسمى بالقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، بموجب الأمر رقم 21 – 11 المؤرخ في 25 أوت 2021.[1]

نتناول **قواعد اختصاص القطب الجزائي المختص بالجرائم الإلكترونية** في (المطلب الأول)، ثم **قواعد اتصال ملف القضية بهذا القطب** في (المطلب الثاني).

المطلب الأول: قواعد اختصاص القطب الجزائي المختص بالجرائم الإلكترونية

أخضع المشرع الجزائري القطب الجزائي المتخصص في مكافحة الجرائم الإلكترونية لقواعد إجرائية خاصة، فيما يتعلق بالإختصاص المحلي أو النوعي.

نتناول **قواعد الإختصاص المحلي للقطب** (الفرع الأول)، ثم **قواعد الإختصاص النوعي للقطب** (الفرع الثاني).

الفرع الأول: الإختصاص المحلي للقطب الجزائي المختص بالجرائم الإلكترونية:

تقتضي القواعد العامة في قانون الإجراءات الجزائية أن الإختصاص الإقليمي للمحكمة يتحدد بالمكان الذي تقع فيه الجريمة أو مكان القبض على الشخص محل المتابعة أو محل أقامته، سواء كان ذلك بالنسبة لوكيل الجمهورية أو قاضي التحقيق أو قاضي الحكم.

وقد خرج المشرع الجزائري عن هذه القاعدة بخصوص الجرائم الإلكترونية، حيث جاء في المادة 211 مكرر23 من ق إ ج أنه: ((يمارس وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، وكذا قاضي التحقيق، ورئيس ذات القطب صلاحياتهم في كامل الإقليم الوطني))

ولعل لخروج المشرع الجزائري عن قواعد الإختصاص المحلي المتعارف عليها ما يبرره؛ إذ تتميز الجريمة الإلكترونية بتوزع عناصر الركن المادي المكون لها عبر كامل التراب الوطني، بل وقد يتعدى الحدود الإقليمية للدولة، الأمر الذي يجعل التمسك بالمعايير التقليدية للإختصاص عقبة أمام السيطرة على هذا النوع من الجرائم ومكافحته.

---

[1] الأمر رقم 21 – 11 المؤرخ في 25 غشت 2021، يُتمم الأمر رقم 66 – 155 المؤرخ في 8 يونيو 1966 المتضمن قانون الإجراءات الجزائية. (ج ر: عدد 65، بتاريخ 26 غشت 2021، ص 7).

ولا يُعتبر القطب الجزائي المتخصص بالجرائم الإلكترونية جهة قضائية قائمة بذاتها في إطار هيكل التنظيم القضائي الجزائري، إنما ينشأ على مستوى محكمة مقر مجلس قضاء الجزائر، وتكون مستقلة عن أقسامها، وهو ما أكده المشرع الجزائري في المادة 211 مكرر 22 من ق إ ج[1]. كما يخضع القطب لنفس القواعد الإجرائية العامة[2].

الفرع الثاني: الإختصاص النوعي للقطب الجزائي المختص بالجرائم الإلكترونية

يختص القطب الجديد وفقا لما جاء بالمادة 211 مكرر 22 من ق إ ج بالجرائم المتصلة بتكنولوجيا الإعلام والإتصال (1)، وفق أحكام تفصيلية وردت في المادتين 211 مكرر 24، 211 مكرر25 من ق إ ج (2).

أولا: مجال اختصاص القطب الجزائي الجديد

جاء في المادة 211 مكرر 22 (فقرة أولى) من ق إ ج أنه: ((يُنشأ على مستوى محكمة مقر مجلس قضاء الجزائر قطب جزائي وطني متخصص في المتابعة والتحقيق في الجرائم المتصلة بتكنولوجيا الإعلام والإتصال والجرائم المرتبطة بها ...))

يتبين من خلال هذه المادة أن هذا القطب الجديد يختص بالنظر في جرائم محددة، هي الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، وقد عرف المشرع الجزائري (الجرائم المتصلة بتكنولوجيا الإعلام والإتصال) في المادة 211 مكرر 22 من ق إ ج أنها: ((أي جريمة ترتكب ويسهل ارتكابها باستعمال منظومة معلوماتية أو نظام للإتصالات الإلكترونية أو أي وسيلة أخرى أو آلية ذات صلة بتكنولوجيا الإعلام والإتصال)).

ومن خلال نص المادة أعلاه، يتبين ما يلي:

---

[1] تنص المادة 211 مكرر 22 من ق إ ج أنه: ((ينشأ على مستوى محكمة مقر مجلس قضاء الجزائر قطب جزائي وطني متخصص في المتابعة والتحقيق في الجرائم المتصلة بتكنولوجيا الإعلام والإتصال والجرائم المرتبطة بها)).

[2] تنص المادة 40 مكرر من ق إ ج أنه: ((تطبق قواعد هذا القانون المتعلقة بالدعوى العمومية والتحقيق والمحاكمة أمام الجهات القضائية التي تم توسيع اختصاصها المحلي طبقا للمواد 37 و40 و329 من هذا القانون مع مراعاة أحكام المواد من 40 مكرر1 إلى 40 مكرر5 أدناه)).

– نطاق اختصـــاص هذا القطب الجديد واســـع جدا، حيث يمتد ليشـــمل كل جريمة وقعت على النظم المعلوماتية أو أي جريمة ارتكبت أو ســـهل ارتكابها باســـتعمال تكنولوجيا المعلوماتية والإتصـــالات، الحالية منها والمسـتقبلية[1]، أي أن هذا التعريف جاء مرنا أخذ من خلاله المشـرع الجزائري في الحسـبان ما يفرزه التطور التكنولوجي الهائل من الإختراعات الإلكترونية من أجهزة جديدة تظهر كل يوم.

– لم يدرج المشـرع الجزائري صـراحة جرائم المعالجة الآلية للمعطيات في صُـلب هذا التعريف، كما فعل في المادة الثانية (2) من القانون رقم 09-04، إلا أنه يمكن أن تندرج ضـــمن عبارة ((... أي جريمة ترتكب أو يســـهل ارتكابها باســـتعمال منظومة معلوماتية)) التي جاءت بالمادة 211 مكرر 22 من ق إ ج[2]. ولكن بنوع من التفصيل الذي سوف يأتي بيانه لاحقا.

يتحدد أيضـــا الإختصـــاص النوعي للقطب الجزائي الجديد على حســـب نوع الجريمة الإلكترونية المرتكبة، وينبغي هنا التمييز بين مراحل المتابعة الجزائية التالية:

- **خلال مرحلتي البحث والتحري والتحقيق:** يختص وكيل الجمهورية وكذا قاضـــي التحقيق على مســـتوى القطب الجزائي الجديد بالمتابعة والتحقيق في كافة الجرائم الإلكترونية بالمفهوم الســـابق، جنايات كانت أو جنح، أو الجرائم المرتبطة بها، وهو ما جاءت به المادة 211 مكرر 22 (فقرة أولى) من ق إ ج.
- **خلال مرحلة المحاكمة:** يختص قاضـــي الحكم لدى القطب الجزائي الجديد، خلافا لوكيل الجمهورية وقاضـــي التحقيق، بالنظر فقط في الجرائم الإلكترونية بالمفهوم السـابق، ذات وصـف جنحة، وهو ما نصـت عليه المادة 211 مكرر 22 فقرة 2 من ق إ ج. وتخضـع الجنايات التي

[1] بوقرة جمال الدين، عنان جمال الدين، القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، مجلة الأستاذ الباحث لدراسات القانونية والسياسية، جامعة محمد بوضياف بالمسيلة، الجزائر، المجلد 7، العدد1، جوان 2022، ص 1674.

[2] شريفة سوماتي، القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال كآلية جديدة ضمن الجهاز القضائي المتخصص، مجلة الدراسات القانونية، تصدر عن جامعة يحي فارس بالمدية، الجزائر، المجلد 8، العدد2، جوان 2022، ص 491.

تم التحري والتحقيق بشـــأنها من طرف القطب الجديد لاختصـــاص محكمة الجنايات الإبتدائية لمجلس قضاء الجزائر[1].

ثانيا: الأحكام التفصيلية المتعلقة بالإختصاص النوعي للقطب

لا تدخل جميع الجرائم الإلكترونية بمفهومها الســـابق ضـــمن نطاق اختصـــاص القطب الجزائي الجديد، بل أن اختصـــاص هذا القطب في بعض الحالات **يكون حصـــريا مانعا (1)**، وفي حالات أخرى يكون **اختصاصا مُشتركا مع الجهات القضائية الأخرى(2)**.

1) الإختصاص الحصري للقطب الجزائي المتخصص بالجرائم الإلكترونية:

يقصـد بالإختصـاص الحصـري هو الإختصـاص الذي ينفرد القطب بممارسـته، دون أن تشـــترك معه أي جهة قضـــائية جزائية أخرى، مهما كان نوعها، ســـواء كانت عادية أو قطب جزائي[2].

وقد منح المشرع الجزائري هذا الإختصاص الحصري للقطب الجديد في حالتين، هما:

(أ) الحالة الأولى (الجرائم الواردة بالمادة 211 مكرر 24 من ق إ ج والجرائم المرتبطة بها):

حددت المادة 211 مكرر 24 من ق إ ج الجرائم التي يختص بها القطب حصريا، وهـي:

- الجرائم التي تمس بأمن الدولة والدفاع الوطني؛
- جرائم نشـر وترويج أخبار كاذبة بين الجمهور من شـأنها المسـاس بالأمن أو السـكينة العامة أو استقرار المجتمع[3]؛
- جرائم نشـر وترويج أنباء مغرضـة تمس بالنظام والأمن العموميين ذات الطابع المنظم أو العابر للحدود الوطنية؛
- جرائم المساس بأنظمة المعالجة الآلية للمعطيات المتعلقة بالإدارات والمؤسسات العمومية؛

---

[1] بوقرة جمال الدين، عنان جمال الدين، المرجع نفسه، ص. ص(1684، 1685).

[2] شريفة سوماتي، المرجع السابق، ص 493.

[3] المجرمة بموجب القانون رقم 20-06 المؤرخ في 28 أفريل 2020 المعدل والمتمم لقانون العقوبات (ج ر: عدد 25، بتاريخ 29 أفريل 2020، ص 10).

- جرائم الإتجار بالأشخاص أو بالأعضاء البشرية أو تهريب المهاجرين؛
- جرائم التمييز وخطاب الكراهية[1].

ويشترط لانعقاد الإختصاص الحصري للقطب توفر الشروط التالية:

- أن يتعلق الأمر بالجرائم المذكورة بالمادة 211 مكرر 24 من ق إ ج على سبيل الحصر، أو الجرائم المرتبطة بها[2]. وتتميز هذه الجرائم بخطورتها على الأمن والنظام العموميين، لاسيما لو استخدمت الأداة المعلوماتية في ارتكابها.
- أن ترتكب هذه الجرائم بإيعاز تكنولوجيا المعلوماتية والإتصالات: بدليل أن المشرع الجزائري نص في المادة 211 مكرر 24 من ق إ ج أنه: ((... يختص وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال وقاضي التحقيق ورئيس ذات القطب حصريا بالمتابعة والتحقيق والحكم في الجرائم **المتصلة بتكنولوجيا الإعلام والإتصال المذكورة أدناه ...**))، وبالتالي يُستثنى من نطاق اختصاص هذا القطب هذه الجرائم في حال ما إذا تم ارتكابها بالطرق التقليدية[3].

(ب) الحالة الثانية (<u>الجرائم الإلكترونية الأكثر تعقيدا والجرائم المرتبطة بها</u>):

يختص القطب الجزائي الجديد دون سواه بمعالجة الجرائم المتصلة بتكنولوجيا المعلوماتية والإتصالات الأكثر تعقيدا والجرائم المرتبطة بها، وقد عرفت المادة 211 مكرر 25 من ق إ ج الجريمة الإلكترونية الأكثر تعقيدا على أنها: ((الجريمة التي بالنظر إلى تعدد الفاعلين أو الشركاء، أو المتضررين، أو بسبب اتساع الرقعة الجغرافية لمكان ارتكاب الجريمة، أو جسامة آثارها، أو الأضرار المترتبة عليها، أو لطابعها المنظم، أو العابرة للحدود الوطنية، أو لمساسها بالنظام والأمن العموميين، تتطلب استعمال وسائل تَحَرٍ خاصة، أو خبرة فنية متخصصة، أو اللجوء إلى تعاون قضائي دولي)).

---

[1] المجرمة بموجب القانون رقم 20-05 المؤرخ في 28 أفريل 2020 المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما (ج ر: عدد 25، بتاريخ 29 أفريل 2020، ص 4).

[2] لمعرفة حالات الإرتباط بين الجرائم راجع المادة 188 من ق إ ج.

[3] شريفة سوماتي، المرجع السابق، ص 494.

ويرجع السبب في ذلك إلى أن خصوصية هذه الجرائم الجديدة تجعل من أجهزة التحقيق التقليدية عاجزة عن البحث والتحري والتحقيق بشأنها وضبط الدليل والوصول إلى مرتكبيها، لذلك أعطى المشرع الإختصاص الحصري لهذا القطب الجديد، نظرا لما يتمتع به من وسائل مُستحدثة تُساعده في التعامل مع هذه الجرائم[1].

2) الإختصاص المشترك للقطب الجزائي المتخصص بالجرائم الإلكترونية:

تنص المادة 211 مكرر 27 فقرة أولى من ق إ ج أنه: ((دون الإخلال بأحكام المادتين 211 مكرر 24 و211 مكرر 25 أعلاه، يمارس وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، وكذا قاضي التحقيق ورئيس ذات القطب اختصاصا مشتركا مع الإختصاص الناتج عن تطبيق المواد 37 و40 و329 من هذا القانون بالنسبة للجرائم المتصلة بتكنولوجيا الإعلام والإتصال والجرائم المرتبطة بها)).

إذا يتمتع القطب الجزائي الجديد عند معالجته لبقية الجرائم المتصلة بتكنولوجيا المعلوماتية والإتصال والجرائم المرتبطة بها، التي تخرج من نطاق اختصاصه الحصري المحدد بنصوص المواد 211 مكرر 24، 211 مكرر 25 من ق إ ج، باختصاص مشترك مع باقي الجهات القضائية الأخرى المختصة إقليميا مع تَمَتُّعِهِ بأفضلية معالجتها.

وفي هذا الفرض، يتمتع وكيل الجمهورية لدى القطب الجزائي الجديد بسلطة تقديرية في المطالبة بالملف أو عدم المطالبة به، بعد أخذ رأي النائب العام لدى مجلس قضاء الجزائر.

المطلب الثاني: قواعد اتصال القطب بملف القضية

تختلف قواعد اتصال القطب بالملف على حسب ما إذا كان اختصاص القطب حصريا أو مشتركا، نشرح ذلك كما يلي:

الفرع الأول: في حال الإختصاص الحصري للقطب الجزائي الجديد

إذا كانت الجريمة المرتكبة من الجرائم التي ينعقد فيها الإختصاص حصريا للقطب الجزائي المتخصص في الجرائم الالكترونية، فإنه يتعين تحويل ملف القضية وجوبا إلى القطب

[1] بوقرة جمال الدين، عنان جمال الدين، المرجع السابق، 1686.

الجديد، وفي هذه الحالة تطبق القواعد الإجرائية المحددة بالمواد من 211 مكرر19 إلى 211 مكرر21 من ق إ ج[1].

وعلى هذا الأســاس، يتعين إرســال التقارير الإخبارية وإجراءات التحقيق من طرف رجال الشرطة القضائية مباشرة إلى وكيل الجمهورية لدى القطب ويتلقى رجال الشرطة القضائية حينئذ التعليمات منه مباشرة، وإذا تبين لوكيل الجمهورية أن الوقائع التي تم تبليغه بها لا تدخل ضمن اختصــاصــه، عملا بالمادتين 211 مكرر24، 211 مكرر25 من ق إ ج فإنه يصــدر مقررا بالتخلي لصالح وكيل الجمهورية المختص إقليميا.

وذات الأمر ينطبق على قاضي التحقيق، فإذا ما اتضح له أن الوقائع التي تم إخطاره بها لا تندرج ضمن اختصاصه يصدر أمرا بعدم اختصاصه.

الفرع الثاني: في حال الإختصاص المشترك مع الجهات القضائية الأخرى

إذا كانت الجريمة المرتكبة من الجرائم الإلكترونية التي يمارس فيها القطب الجزائي الجديد اختصاصا مشتركا مع غيره من الجهات القضائية الجزائية الأخرى، فإنه في هذه الحالة نميز بين ما إذا كان هذا الاختصاص المشترك مع باقي الجهات القضائية المختصة محليا (أولا)، أو مع الأقطاب الجزائية المتخصصة الأخرى (ثانيا).

أولا: الإختصاص المشترك مع الجهات القضائية المختصة محليا

يتصل القطب المتخصص بالجرائم الإلكترونية بالملف وفقا للقواعد الإجرائية التي جاءت بالمواد 211 مكرر 4 إلى 211 مكرر 15 من ق إ ج[2]، التي حددت طريقة طلب الملف وإجراء التخلي عنه:

1) طلب الملف:

توجب المادة 211 مكرر6 من ق إج على وكلاء الجمهورية لدى الجهة القضــائية المختصــة إقليميا الإرسال الفوري وبكل الطرق نسخا من التقارير الإخبارية وإجراءات التحقيق

---

[1] تنص المادة 211 مكرر 26 من ق إ ج أنه: ((تطبق على الإختصاص الحصري للقطب الجزائي الوطني لمكافحة الجرائم المتصــلة بتكنولوجيا الإعلام والإتصــال، المنصــوص عليه في المادتين 211 مكرر24 و211 مكرر25 أعلاه، الإجراءات المنصوص عليها في المواد 211 مكرر19 إلى 211 مكرر21 من هذا القانون)).

[2] تنص المادة 211 مكرر 27 فقرة ثانية من ق إ ج أنه: ((تطبق، في هذه الحالة، الإجراءات المنصــوص عليها في المواد 211 مكرر 4 إلى 211 مكرر15 من هذا القانون ...)).

المنجزة من طرف الشرطة القضائية الى وكيل الجمهورية لدى القطب الجزائي الخاص بالجريمة الإلكترونية.

يطلع وكيل الجمهورية لدى القطب على هذه التقارير، حيث تبقى له السلطة التقديرية في المطالبة بملف الإجراءات، سواء على مستوى التحريات الأولية أو المتابعة أو التحقيق القضائي، متى تبين له أن الجريمة تدخل ضمن مجال اختصاصه، وذلك بعد أخذ رأي النائب العام لدى مجلس قضاء الجزائر، الذي يخضع لسلطته السلمية.

2) التخلي عن الملف:

بعد وصول إلتماسات وكيل الجمهورية لدى القطب المتخصص في الجرائم الإلكترونية إلى وكيل الجمهورية المختص إقليميا يصدر هذا الأخير مقررا بالتخلي لصالح نظيره بالقطب الجزائي، وهذا خلال مرحلتي التحريات الأولية والمتابعة.

أما إذا كانت القضية على مُستوى قاضي التحقيق المختص إقليميا، فيحول له وكيل الجمهورية المختص إقليميا التماسات وكيل الجمهورية لدى القطب، ويصدر قاضي التحقيق المختص إقليميا حينئذ أمرا بالتخلي لصالح القطب.

ثانيا: الإختصاص المشترك مع الأقطاب الجزائية المتخصصة الأخرى

نُمَيز بين ما إذا كانت المطالبة بالملف من طرف القطب الجزائي الخاص بالجريمة الإلكترونية تمت بالموازاة مع الأقطاب الجزائية ذات الإختصاص الموسع (1)، أو مع القطب الجزائي الإقتصادي والمالي ومحكمة مجلس قضاء الجزائر (2):

1) الإختصاص المشترك مع الأقطاب الجزائية ذات الإختصاص الموسع:

إذا تزامنت المطالبة بالملف من قبل وكيل الجمهورية لدى القطب المختص بالجرائم الإلكترونية مع المطالبة به من طرف وكيل الجمهورية لدى الجهات القضائية ذات الإختصاص الإقليمي الموسع، فإن الإختصاص يؤول وجوبا إلى وكيل الجمهورية لدى القطب المختص بالجرائم الإلكترونية[1].

[1] راجع المادة 211 مكرر 11 من ق إ ج.

ويتم في هذه الحالة التخلي عن الملف، سـواء خلال مرحلة التحريات الأولية أو المتابعة أو التحقيق القضائي، لصالح وكيل الجمهورية لدى القطب الخاص بالجرائم الإلكترونية. ويُرسل له ملف الإجراءات كاملا.

2) الإختصاص المشترك مع القطب الإقتصادي والمالي أو محكمة مقر مجلس قضاء الجزائر:

إذا تزامن اختصاص القطب الجزائي الخاص بالجريمة الإلكترونية مع اختصاص القطب الإقتصادي والمالي الموجود مقره على مستوى محكمة مقر مجلس قضاء الجزائر فإن الإختصاص يؤول وجوبا إلى القطب الإقتصادي والمالي[1].

وفي هذه الحالة لابد عل القطب الجزائي الخاص بالجرائم الإلكترونية التخلي عن الملف لصالح القطب الإقتصادي والمالي، سواء كان ذلك خلال مرحلة التحريات الأولية، المتابعة أو التحقيق القضائي، ويرسل له ملف الإجراءات كاملا.

وفي حال تزامن اختصاص القطب الجزائي الخاص بالجرائم الإلكترونية مع اختصاص محكمة مقر مجلس قضاء الجزائر، فإن الإختصاص يؤول وجوبا لمحكمة مقر مجلس قضاء الجزائر[2].

المبحث الثاني: الجهاز المساعد للجهاز القضائي في مجال الجرائم الإلكترونية

قام المشرع الجزائري بموجب القانون رقم 09 – 04 بإنشاء جهاز مُساعد للجهاز القضائي، يُسمى بالهيئة الوطنية للوقاية من الجرائم الإلكترونية، يقوم بِمَدِ يَدِ العون للهياكل القضائية في إطار مكافحة الجرائم الإلكترونية. ندرس من خلال هذا المطلب **مبررات استحداث الهيئة وتشكيلتها وكيفية سيرها** (المطلب الأول)، **ثم دور الهيئة في مجال الوقاية من الجرائم الإلكترونية ومكافحتها** (المطلب الثاني).

المطلب الأول: مبررات إنشاء الهيئة وتشكيلتها وكيفية سيرها

[1] المادة 211 مكرر 28 من ق إ ج.

[2] المادة 211 مكرر 29 من ق إ ج.

نتناول في (الفرع الأول) **مبررات إنشاء الهيئة الوطنية للوقاية من الجرائم الإلكترونية،** ثم في (الفرع الثاني) **تشكيلة الهيئة وكيفية سيرها.**

الفرع الأول: مبررات إنشاء الهيئة الوطنية للوقاية من الجرائم الإلكترونية

أكدت الإتفاقية العربية لمكافحة جرائم تقنية المعلومات على أهمية وجود هيئات متخصصة تعمل على مساعدة الجهاز القضائي في مكافحة الجرائم الإلكترونية، حيث جاء في المادة 43 منها أنه: (تكفل كل دولة طرف، وفقا للمبادئ الأساسية لنظامها القانوني، وجود جهاز متخصص ومُتفرِغ على مَدَارِ الساعة لضمان المساعدة الفورية، لغايات التحقيق أو الإجراءات المتعلقة بجرائم تقنية المعلومات أو لجمع الأدلة بشكلها الإلكتروني، في جريمة معينة ...)

من هذا المنطلق، أسست مختلف الدول هيئات ومصالح ووحدات في سبيل مكافحة الجرائم الإلكترونية، وتضم هذه الهيئات مجموعة من الموارد البشرية والإمكانيات المادية والتقنية، التي تسهل عملية البحث عن مرتكبي الجرائم الإلكترونية، وتمكن من القبض عليهم، وتسليمهم للجهات القضائية المختصة. في هذا السياق قامت الجزائر بإنشاء بعض الأجهزة والوحدات المتخصصة في الجرائم الإلكترونية على مستوى هياكل الأمن والدرك الوطني[1]، لتقوم بعدها من خلال القانون رقم 09 – 04، بإنشاء الهيئة الوطنية للوقاية من الجرائم الإلكترونية.

واستحداث المشرع الجزائري لهذه الهيئة له أهميته القصوى من ناحيتين:

من جهة، تضمن الهيئة الوطنية للوقاية من الجرائم الإلكترونية، بما لها من إمكانيات مادية وتقنية وخبراء متخصصين في هذا المجال، تحقيق الفعالية في مواجهة الجرائم الإلكترونية، ومد يد العون للجهاز القضائي، والجهاز الأمني كالشرطة والدرك، الذي قد يجد صعوبة في التعامل مع هذه الجريمة، بحكم ما يميزها من تعقيدات تقنية، من الصعب فهمها من غير ذوي الإختصاص.

من جهة ثانية، سمح المشرع الجزائري للجهات الأمنية والقضائية من خلال القانون رقم 09 – 04 باتخاذ مجموعة من الإجراءات الخطيرة، كمراقبة الإتصالات الإلكترونية والهاتفية

[1] أنشأت الجزائر عدت وحدات خاصة بمكافحة الجريمة الإلكترونية، على مستوى جهاز الشرطة والدرك. من أجل أكثر تفصيل انظر، شنتير خضرة، المرجع السابق، ص. ص (191 – 204).

وتفتيش الأنظمة المعلوماتية وحجزها، مع ما قد تؤدي إليه ذلك، إما عن قصد أو غير قصد، من مساس بحرمة الحياة الخاصة للأشخاص وأمن اتصالاتهم وبياناتهم الشخصية، المالية والصحية والإجتماعية، لذلك كان من الضروري إنشاء هيئة تعمل كجهاز رقابي في مجال الجرائم الإلكترونية، وحتى تضمن الحق الدستوري المقرر لكل مواطن في حرمة حياته ومراسلاته وتحول دون المساس به بحجة مكافحة الجرائم.

الفرع الثاني: تشكيلة الهيئة وكيفية سيرها

استحدث المشرع الجزائري ما سماه بـــــــ (الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصـــال ومكافحتها) في الفصـــل الخامس من القانون رقم 09-04، حيث نصـــت المادة 13 منه أنه: (تنشـــأ هيئة وطنية للوقاية من الجرائم المتصـــلة بتكنولوجيا الإعلام والإتصـــال ومكافحته... تحدد تشـكيلة الهيئة وتنظيمها وكيفيات سـيرها عن طريق التنظيم)، وقد حدد المرســـوم الرئاســـي رقم 21 – 439 المؤرخ في 7 نوفمبر 2021 تنظيم الهيئة وكيفية سيرها[1].

بالرجوع إلى المادتين الثانية (2) والثالثة (3) من المرسـوم الرئاسـي رقم 21 – 439 تعد الهيئة الوطنية للوقاية من الجرائم الإلكترونية سـلطة إدارسـة مسـتقلة تتمتع بالشـخصـية المعنوية والإستقلال المالي، توضـع تحت سلطة رئيس الجمهورية. ويحدد مقر الهيئة بالجزائر العاصـمة، ويمكن نقله إلى أي مكان آخر من التراب الوطني، بموجب مرسوم رئاسي.

---

[1] المرسوم الرئاسي رقم 21 – 439 المؤرخ في 7 نوفمبر 2021 يتظمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها. (ج ر: عدد 86، بتاريخ 11 نوفمبر 2021، ص 5).

قام المشرع الجزائري بتنظيم الهيئة الوطنية للوقاية من الجرائم الإلكترونية من خلال العديد من المراسيم:

- المرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر 2015، الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصـــلة بتكنولوجيا الإعلام والإتصـــال ومكافحتها. (ج ر: العدد 53، بتاريخ 8 أكتوبر 2015، ص 16)؛
- المرسوم الرئاسي رقم 19-172 المؤرخ في 6 يونيو 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال وتنظيمها وكيفية سيرها، (ج ر: عدد 37، الصادرة في 9 يونيو 2019)؛
- المرسوم الرئاسي رقم 183/20 المؤرخ في 13 يوليو 2020 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتهما، (ج ر: عدد 40، المؤرخ في 18 يوليو 2020).

وتتكون الهيئة، وفقا للمادة 5 من المرسوم الرئاسي رقم 21 –439، من **مجلس توجيه** (أولا) و**مديرية عامة** (ثانيا):

أولا: مجلس توجيه

يضم مجلس التوجيه، على حسب المادة السادسة (6) من المرسوم الرئاسي رقم 21 –439، مجموعة من الأعضاء: الأمين العام لوزارة الشؤون الخارجية والجالية الوطنية بالخارج، الأمين العام لوزارة الداخلية والجماعات المحلية والتهيئة العمرانية، الأمين العام لوزارة العدل، الأمين العام لوزارة البريد والمواصلات السلكية واللاسلكية، قائد الدرك الوطني، المدير العام للأمن الداخلي، المدير المركزي لأمن الجيش لأركان الجيش الوطني الشعبي، المدير العام للأمن الوطني، رئيس مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة لأركان الجيش الوطني الشعبي، ممثل عن رئاسة الجمهورية يعينه رئيس الجمهورية.

يترأس مجلس التوجيه الأمين العام لرئاسة الجمهورية.

يتولى المدير العام للهيئة أمانة مجلس التوجيه.

يقوم مجلس التوجيه، وفقا للمادة السابعة (7) من المرسوم الرئاسي رقم 21–439، لاسيما بـ:

توجيه عمل الهيئة والإشراف عليه ومراقبته؛ دراسة كل مسألة تخضع لمجال اختصاص الهيئة، لاسيما فيما يتعلق بتوفر شروط اللجوء للمراقبة الوقائية للإتصالات الإلكترونية المنصوص عليها في المادة 4 من القانون رقم 09–04؛ المداولة حول الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها؛ المداولة حول مسائل التطوير والتعاون والمؤسسات والهيئات الوطنية والأجنبية المعنية بالجرائم المتصلة بتكنولوجيا الإعلام والإتصال؛ القيام دوريا بتقييم حالة التهديد في جرائم المتصلة بتكنولوجيا الإعلام والإتصال للتمكن من تحديد مضامين العمليات الواجب القيام بها والأهداف المنشودة؛ اقتراح كل نشاط يتصل بالبحث وتقييم الأعمال المباشرة في مجال الوقاية من هذه الجرائم؛ إعداد نظامها الداخلي والمصادقة عليه؛ الموافقة على برنامج الهيئة؛ دراسة التقرير السنوي لنشاطات

الهيئة والمصادقة عليه؛ دراسة مشروع الميزانية للهيئة والموافقة عليه؛ إبداء رأيه في كل مسألة تتصل بمهام الهيئة؛ تقديم كل اقتراح يتصل بمجال اختصاص الهيئة.

يجتمع مجلس التوجيه، وفقا للمادة 8 من المرسوم الرئاسي رقم 21-439، مرة واحدة في السنة، في دورة عادية، بناء على استدعاء من رئيسه، كما يمكنه أيضا الإجتماع في دورة غير عادية، كلما كان ذلك ضروريا، بناء على استدعاء من رئيسه أو بطلب من أحد أعضائه أو من المدير العام للهيئة.

ثانيا: المديرية العامة

تضم المديرية العامة، وفقا للمادة 11 من المرسوم الرئاسي رقم 21-439:

- مديرية للمراقبة الوقائية واليقضة الإلكترونية؛
- مديرية للإدارة والوسائل؛
- مصلحة للدراسات والتلخيص؛
- مصلحة للتعاون واليقظة التكنولوجية.
- ملحقات جهوية.

يدير المديرية العامة مدير عام يعين بموجب مرسوم رئاسي، وتُنهَى مهامه حسب نفس الأشكال.

وبالتالي فالهيئة الوطنية للوقاية من الجرائم الإلكترونية، تتكون من تشكيلة إدارية وأخرى تقنية:

بالنسبة **لتشكيلة الهيئة الإدارية**، تتمثل في مجلس التوجيه وكذا المديرية العامة[1]، وتمارس هذه الأخيرة مهام الأمانة العامة لمجلس التوجيه، كما تقوم بالعمل الإداري، من خلال السهر على السير الحسن للهيئة؛ إعداد مشروع ميزانية الهيئة وعرضه على مجلس التوجيه للموافقة

[1] تعتبر المديرية العامة المحرك الفعلي لهذه الهيئة، حيث تلعب **دور مزدوج**؛ إذ تمارس مهام الأمانة العامة لمجلس التوجيه، بالإضافة إلى أنها تمارس العمليات التقنية، من خلال مديرية المراقبة الوقائية واليقضة الإلكترونية، كما تقوم بالعمل الإداري.

عليه؛ إعداد وتنفيذ برنامج عمل الهيئة بعد الموافقة عليه من طرف مجلس التوجيه، ضمان التسيير الإداري والمالي للهيئة، دراسة مشروع الميزانية وتقديم تقارير خاصة بنشاط الهيئة؛ تبادل المعلومات مع مثيلاتها في الخارج بغرض تجميع كل المعطيات المتعلقة بتحديد مكان وهوية مرتكبي الجرائم الإلكترونية. والهيئة الإدارية بهذا الشكل لا تقوم بالإجراءات الخاصة بالوقاية من الجرائم الإلكترونية.

فيما يخص **تشكيلة الهيئة التقنية**، فهي المكلفة بإنجاز المهام التقنية المتعلقة بالوقاية من الجرائم الإلكترونية، لاسيما مديرية المراقبة الوقائية واليقظة الإلكترونية، والملحقات الجهوية.

الفرع الثاني: دور الهيئة في مجال مكافحة الجرائم الإلكترونية والوقاية منها

تقوم الهيئة، من خلال مديرية المراقبة الوقائية واليقظة الإلكترونية، وتحت رقابة السلطة القضائية، بدورين، (الأول) وقائي أي رقابي، بصدد جرائم الإرهاب أو التخريب والمساس بأمن الدولة، و(الثاني) دور مُساعد للهيئات القضائية بالنسبة للجرائم الإلكترونية الأخرى:

أولا: الدور الوقائي للهيئة الوطنية لمكافحة الجرائم الإلكترونية

جاء في المادة 25 من المرسوم الرئاسي رقم 21 – 439 أنه: ((قصد الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو التي تمس بأمن الدولة ومكافحتها، تكلف الهيئة حصريا، في مجال اختصاصها، بمراقبة الإتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها داخل منظومة معلوماتية تحت سلطة قاض لدى الهيئة، وفقا للأحكام المنصوص عليها في المادة 4 من القانون رقم 09 – 04 ... على أن تخضع إجراءات التفتيش والحجز لأحكام قانون الإجراءات الجزائية))

إذا يُستنتج من هذه المادة أن للمراقبة الإلكترونية طابعا وقائيا وآخر حصري، إذا كان الأمر يتعلق بالجرائم الإرهابية أو التخريبية أو الماسة بأمن الدولة. ويُقصد الطابع الوقائي للمراقبة الإلكترونية إمكانية اتخاذ هذا الإجراء دون حدوث أي جريمة، من خلال العمل على مراقبة ورصد تحركات واتصالات الأشخاص أو الجماعات المشبوهة، التي تحضر أو تجتمع للقيام بعمليات إرهابية أو تخريبية أو الجرائم الماسة بأمن الدولة، بغرض تفادي حدوثها، وذلك عن طريق إخطار السلطات القضائية المختصة، أو في حالة توفر معلومات عن احتمال اعتداء

على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الإقتصاد الوطني[1].

ويعني الطابع الحصري لها، أن للهيئة دون سواها الإختصاص في وضع التقنيات اللازمة لتجميع وتسجيل محتوى الإتصالات الإلكترونية، بما في ذلك تلك التي تتم عبر شبكة الأنترنت.

في هذا الصدد، يتبادر إلى الأذهان أنه طالما أن إجراء الرقابة الإلكترونية قد يُتخذ للوقاية من الجرائم الخطيرة، أي قبل حدوث الجريمة، من يُقرِر وجوب التدخل للقيام بإجراء المراقبة الوقائية؟

جاء في المادة الرابعة (4) من القانون رقم 09 – 04 أنه يجب صدور إذن مكتوب من السلطة القضائية المختصة للقيام بإجراء المراقبة الإلكترونية الوقائية، لكن متى يُقدم هذا الإذن وبناء على ماذا، خاصة إذا علمنا أنه لا وجود للجريمة؟

تنص المادة 7 من المرسوم الرئاسي رقم 21 –439 أن مجلس التوجيه يكلف بـــ ((... القيام بتقييم حالة التهديد في مجال الجرائم المتصلة بتكنولوجيا الإعلام والإتصال للتمكن من تحديد مضامين العمليات الواجب القيام بها والأهداف المنشودة بدقة))، إذا مجلس التوجيه هو من يقرر وجود حالات التهديد، ويتم بعدها إخطار السلطة القضائية، مُمَثلة في النائب العام لدى مجلس قضاء الجزائر، ويقوم هذا الأخير بناء على إذن مكتوب بالسماح باتخاذ هذا الإجراء[2].

ثانيا: الدور المساعد للهيئة الوطنية للوقاية من الجرائم الإلكترونية

تقوم الهيئة، من خلال مديرية المراقبة الوقائية واليقظة الإلكترونية، أيضا بدور مُساعد في مجال مكافحة الجرائم الإلكترونية، إن كان ذلك على المستوى الداخلي أو الدولي:

على المستوى الداخلي، جاء في المادة 14 من القانون رقم 09 – 04 أنه من مهام الهيئة مساعدة السلطات القضائية في التحريات التي تجريها في شأن الجرائم الإلكترونية، بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية، بما في ذلك القيام بإجراءي التفتيش

[1] حابت أمال، المرجع السابق، ص 468.

[2] المرجع نفسه، ص469.

والمراقبة القضائية، وذلك خروجا عن الأصل العام الذي يقتضي أن هذه الإجراءات تضطلع بها السلطة القضائية أو ضباط الشرطة القضائية.

تتكفل الهيئة أيضـــا، **على المســـتوى الدولي**، على تبادل المعلومات مع نظيراتها في الخارج، قصـــد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم الإلكترونية وتحديد مكان تواجدهم. وبذلك تكون هذه الهيئة همزة وصـــل مهمة جدا في تطوير تبادل المعلومات والتعاون الدولي، خاصـــة عندما يتعلق الأمر بتنفيذ طلبات المســـاعدة الصـــادرة عن البلدان الأجنبية[1].

ولأجل كل ذلك، تضـــع مديرية المراقبة واليقظة الإلكترونية التجهيزات والوســـائل والأجهزة التقنية الضـــرورية لتنفيذ مهامها على مســـتوى المنشـــآت القاعدية للمتعاملين ومقدمي الخدمات، الذين هم ملزمين بحكم القانون على تقديم المســـاعدات الضـــرورية لها للقيام بتنفيذ مهامها على أكمل وجه[2]، حيث يمكن للهيئة أن تطلب من أي جهاز أو مؤســـســـة أو مصـــلحة كل وثيقة أو معلومة تراها ضرورية لإنجاز مهامها[3].

المبحث الثالث: الإختصاص القضائي والتعاون القضائي الدوليين للجرائم الإلكترونية العابرة للحدود

تعتبر الجرائم الإلكترونية العابرة للحدود من أكثر الجرائم إثارة للجدل فيما يخص المسائل المتعلقة بتنازع الإختصاص القضائي بين الدول (المطلب الأول)، وهو الأمر الذي يجعل التعاون القضائي الدولي في مُقدِمة الآليات الأكثر فعالية في مكافحة هذه الجرائم (المطلب الثاني).

المطلب الأول: الإختصاص القضائي الدولي في الجرائم الإلكترونية العابرة للحدود

تُعَدُ المسائل المرتبطة الإختصاص القضائي على المستوى الداخلي أكثر سهولة من تلك المتعلقة بها على المستوى الدولي، حيث يقتصر التنازع القضائي الداخلي على تحديد الجهة القضائية المختصة فحسب، دون القانون الواجب التطبيق، لخضوع كامل الإقليم الوطني لقانون

---

[1] المادة 14 من المرسوم الرئاسي رقم 21 – 439.

[2] المادة 15 من المرسوم الرئاسي رقم 21–439.

[3] المادة 24 من المرسوم الرئاسي رقم 21–439.

عقابي واحد، إلا أن التنازع القضائي بين الدول لاسيما فيما يتعلق بالجرائم الإلكترونية العابرة للحدود يطرح التساؤل حول الأمرين معا[1]؛ القانون الواجب التطبيق من جهة (الفرع الأول)، والجهة القضائية المختصة (الفرع الثاني).

الفرع الأول: القانون الواجب التطبيق على الجرائم الإلكترونية العابرة للحدود

لحل مشكلة القانون الواجب التطبيق على الجرائم الإلكترونية العابرة للحدود تُطبق المبادئ ذاتها المعمول بها في الجرائم العادية الأخرى، ويأتي في مقدمتها مبدأ الإقليمية، يتم تكملته بالمبادئ الإحتياطية الأخرى، التي تتمثل في مبدأي الشخصية والعينية.

نتناول **المبدأ الأصلي الأَوْلَى بالتطبيق على الجرائم الإلكترونية** (أولا)، ثم **المبادئ الإحتياطية المكملة له**(ثانيا).

أولا: المبدأ الأصلي (مبدأ إقليمية النص الجنائي)

يُقصد بمبدأ الإقليمية تطبيق التشريع الجنائي الوطني على جميع الجرائم المرتكبة على إقليم الدولة، بغض النظر عن جنسية الجاني أو المجني عليه، أو المصلحة التي أهدرتها الجريمة[2]. ووفقا للتشريع الجزائري تُعد الجريمة مُرتكبة داخل الإقليم الوطني بمجرد أن يقع أحد العناصر المكونة للركن المادي لها في الجزائر[3]، كمثال على ذلك يطبق القانون الوطني على الصور الإباحية أو العبارات التي تحث على الكراهية المنتشرة والمتداولة عبر شبكة الأنترنت، بغض النظر عن الدولة التي صدرت عنها هذه الصور أو العبارات، طالما أنه بإمكان المستخدم الدخول إليها في الإقليم الوطني[4].

---

[1] صفاء حسن نصيف، التحديات الإجرائية المتصلة بالجرائم المعلوماتية، مجلة العلوم القانونية والسياسية، كلية القانون والعلوم السياسية، جامعة ديالي، العراق، المجلد الخامس، العدد الثاني، 2016، ص274.

[2] عبد الله أوهايبية، شرح قانون العقوبات الجزائري، (القسم العام)، دار موفم للنشر، الجزائر، 2009، ص 131.

– تنص المادة 2 من ق ع: ((يطبق قانون العقوبات على كافة الجرائم التي ترتكب في أراضي الجمهورية...)).

[3] راجع المادة 586 من ق إ ج.

[4] عادل عبد العال إبراهيم خرشي، إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعة الجديدة، مصر، 2015، ص 278 – 279.

ثانيا: المبادئ الإحتياطية

تعطي التشريعات المختلفة الأولوية لمبدأ الإقليمية؛ بالنظر لأهميته العملية، فحيث ترتكب الجريمة، يكون من اليسير تحصيل أدلة الإثبات المتعلقة بها، غير أن ارتكاب الجريمة في العالم الإفتراضي، جعلها غير مرتبطة بحيز مكاني أو رقعة جغرافية محددة، ما دفع البعض إلى نزع الصفة المادية عن الجرائم الإلكترونية[1]، وتبعا لذلك ازدادت أهمية المبادئ الأخرى، المتمثلة في:

1) مبدأ الشخصية:

يُقصد بمبدأ الشخصية تطبيق القانون الجنائي للدولة على كل من يحمل جنسيتها، إذا ارتكب جريمته خارج الإقليم الوطني[2].

2) مبدأ العينية:

يعني مبدأ العينية سريان التشريع الجنائي الوطني على الجريمة التي تقع خارج الدولة، المرتكبة من طرف أجنبي، إذا كانت مُخلة بالمصالح الأساسية للدولة. وتحرص الدول من خلال هذا المبدأ على فرض الحماية على مصالحها الحيوية المعتدى عليها في الخارج، لاسيما وأن الدولة الأجنبية المرتكب على أراضيها الجرم لا تهتم عادة بهذه الجرائم[3].

وجاء النص على مبدأ العينية في المادة 588 من ق إ ج، إلا أن المشرع الجزائري أعاد التأكيد عليه بشأن الجرائم الإلكترونية في المادة 15 من القانون رقم 09 – 05 التي تنص أنه: ((زيادة على قواعد الإختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيا الإعلام والإتصال المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإسترتيجية للإقتصاد الوطني)).

الفرع الثاني: الجهة القضائية المختصة في حال تنازع الإختصاص بين الدول

---

[1] سـعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجسـتير، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، السنة الجامعية 2012 – 2013، ص 99 – 100.

[2] عبد الله أو هايبية، شرح قانون العقوبات الجزائري...، المرجع السابق، ص 148.

[3] المرجع نفسه، ص 154.

قد يُقدِمُ أجنبي على ارتكاب جريمة إلكترونية في إقليم دولة معينة، فهنا تخضع هذه الجريمة لاختصاص الدولة التي ارتكبت على إقليمها الجريمة وفقا لمبدأ الإقليمية، وذات الجريمة تخضع لاختصاص الدولة التابع لها هذا الأجنبي وفقا لمبدأ الشخصية، وقد تكون هذه الجريمة من الجرائم التي تهدد أمن وسلامة دولة ثالثة، فتكون هذه الأخيرة أيضا مختصة بالنظر في هذه القضية على أساس مبدأ العينية[1].

والسؤال الذي يطرح نفسه هنا، من هي الجهة القضائية التي يؤول إليها الإختصاص في مثل هذه الحالات؟

في هذا الشأن نصت المادة 30 فقرة 3 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات أنه: ((إذا ادعت أكثر من دولة طرف بالإختصاص القضائي لجريمة منصوص عليها في هذه الإتفاقية فيقدم طلب الدولة التي أخلت الجريمة بأمنها أو مصالحها ثم الدولة التي وقعت الجريمة في إقليمها ثم الدولة التي يكون الشخص المطلوب من رعاياها وإذا اتحدت الظروف فتقدم الدولة الأسبق في طلب التسليم)).

من خلال هذا النص يتضح أن الأولوية في الإختصاص القضائي بين الدول، تتحدد أولا وفقا لمعيار **المصلحة المعتدى عليها**، وقد لَقِيَ هذا المعيار تأييد الفقه أيضا، غير أنهم ذهبوا إلى التمييز بناء على المعيار ذاته، بين ما إذا كانت المصلحة المهدورة تهم الجماعة الدولية بِرُمَتِها، وهنا ينعقد الإختصاص لأي دولة يُضبط الجاني على أراضيها، وتُجسِدُ هذه الحالة ما يُعرف بمبدأ الإختصاص العالمي أو الشامل[2]، أما وإن مَسَتِ الجريمة الإلكترونية مصالح دولة بعينها دون غيرها أو مست مصالحها الحيوية، كالهجمات الإلكترونية التي تَطالُ المواقع الحكومية الحساسة، فهنا يؤول الإختصاص إلى تلك الدولة، وهذه الحالة تجسد لنا مبدأ العينية[3].

ولعل إجماع الفقه وتأييد المواثيق الدولية على إعطاء الأولوية عند تنازع الإختصاص لقضاء الدولة التي أضرت الجريمة الإلكترونية بأمنها ومصالحها، هو الذي دفع المشرع الجزائري

---

[1] عادل عبد العال إبراهيم خراشي، المرجع السابق، ص 240.

[2] يقصد بالإختصاص القضائي الشامل تطبيق القانون الجنائي الوطني على كل مجرم تم القبض عليه داخل الإقليم الوطني، بغض النظر عن مكان ارتكاب الجريمة، أو جنسية مرتكبها. عبد الله أو هايبية، شرح قانون العقوبات....، المرجع السابق، ص 157.

[3] صفاء حسن نصيف، المرجع السابق، ص 279؛ يعيش شوقي تمام، المرجع السابق، ص. ص (39 – 41).

إلى التأكيد مُجددا على مبدأ العينية، وتكريسه في مجال الجرائم الإلكترونية، في المادة 15 من القانون رقم 09 – 04، على الرغم من أن القواعد العامة في قانون الإجراءات الجزائية تُقِرُه.

أما في حال لم تضر الجريمة الإلكترونية بمصالح دولة بعينها، فإنه يمكن في هذه الحالة الإحتكام إلى مبدأ الإقليمية، أي تطبيق قانون الدولة التي وقعت فيها الجريمة، ثم قانون الدولة التي يحمل الجاني جنسيتها.

المطلب الثاني: التعاون القضائي الدولي في الجرائم الإلكترونية العابرة للحدود

يُعد التعاون القضائي الدولي أحد أهم الوسائل في مكافحة الجرائم العابرة للحدود، التي تُعد الجريمة الإلكترونية من بينها. ويُعرف التعاون القضائي الدولي على أنه كل إجراء قضائي تقوم به دولة معينة يكون من شـــأنه تســـهيل عملية المحاكمة في دولة أخرى بصـــدد جريمة من الجرائم[1].

نُوَضـــح في (الفرع الأول) **صـــور التعاون القضـــائي الدولي** ثم ندرس في (الفرع الثاني) **أحكامه التي تناولها القانون رقم 09 -04.**

الفرع الأول: صور التعاون القضائي الدولي

تتمثل صور التعاون القضائي الدولي فـي:

أولا: نظام تبادل المعلومات

قد يكون لدولتين الإختصـــاص في ذات الجريمة، غير أن إحداهما لا ترغب في مباشـــرة التحقيق بشـــأنها، وتتطوع بتزويد الدولة الأخرى التي يُجرى فيها التحقيق بالبيانات والمعلومات التي تم تحصـــيلها فيما يخص الجريمة والمجرم، ويتم ذلك وِفقا لنظام يُســـمَى بنظام تبادل المعلومات.

ويُقصد بتبادل المعلومات أن تتكفل دولة معينة بتقديم البيانات والوثائق والمواد الإستدلالية التي بحوزتها إلى دولة أخرى وهي بصـدد النظر في جريمة معينة، كالقيام مثلا بتسـليم الوثائق

[1] عادل عبد العال إبراهيم خرشي، المرجع السابق، ص 202.

الخاصة بالسوابق القضائية للجناة، التي تسمح بالتعرف على الماضي الجنائي للأفراد، بُغية تحديد الأحكام المتعلقة بالعود ووقف تنفيذ العقوبة وغيرها من الإجراءات[1].

ثانيا: نظام نقل الإجراءات

يُقصد بنقل الإجراءات قيام إحدى الدول، بناء على اتفاقية، باتخاذ الإجراءات الجنائية بشأن جريمة ارتكبت في إقليم دولة أخرى، ولمصلحة هذه الدولة بناء على اتفاقية، وذلك إذا توافرت شروط معينة أهمها:

- أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والمطلوب منها؛
- أن تكون الإجراءات المطلوب اتخاذها مقررة في قانون الدولة المطلوب منها عن ذات الجريمة؛
- أن يكون الإجراء المطلوب اتخاذه يؤدي إلى الوصول إلى الحقيقة، كأن تكون أدلة الجريمة موجودة بالدولة المطلوب منها[2].

ثالثا: الإنابة القضائية الدولية

يقصد بالإنابة القضائية الدولية طلب اتخاذ إجراء قضائي من إجراءات الدعوى الجنائية، تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها، لأهميته للفصل في مسألة معروضة على السلطة القضائية في الدول الطالبة، ويتعذر عليها القيام به بنفسها[3].

وتتطلب الإنابة القضائية الدولية إرسال الملف المتعلق بالدعوى الجنائية ومرفقاته من مستندات ووثائق ومحاضر التحقيق التي أُجرِيَت بمعرفة السلطة القضائية في الدولة المطلوب فيها اتخاذ بعض إجراءات التحقيق، وهي على هذا النحو تُشبه كثيرا الإنابة القضائية الداخلية[4].

تطبيقا لذلك أجاز المشرع الجزائري في المادة الرابعة (4) من القانون رقم 09 – 04 للسلطات القضائية الجزائية مراقبة الإتصالات الإلكترونية لأشخاص مقيمين بالجزائر يُحتمل تورطهم في عمل إجرامي مس بمصالح الدولة الأجنبية، في إطار المعاملة بالمثل.

---

[1] فريد ناشف، آليات التعاون الدولي في مكافحة الجرائم الإلكترونية، مجلة البحوث في الحقوق والعلوم السياسية، تصدر عن كلية الحقوق والعلوم السياسية، جامعة تيارت، الجزائر، المجلد 8، العدد1، 2022، ص 440.

[2] عادل عبد العال إبراهيم خرشي، المرجع السابق، ص 106 – 107.

[3] المرجع نفسه، ص209.

[4] المرجع نفسه، ص 212.

الفرع الثاني: الأحكام الخاصة بالتعاون القضائي الدولي في مجال الجرائم الإلكترونية

يُمكِن إيجاز الأحكام المتعلقة بالتعاون القضـــائي الدولي في مجال الجرائم الإلكترونية في النقاط التالية:

أولا: الإتفاقيات الدولية هي وحدها التي من الممكن أن تنبع منها الإلتزامات بين الدول، ومن دون الإتفاقيات الدولية وخارج الشروط التي تنص عليها، لا يمكن للدولة أن تعتمد على مساعدة الدولة المطلوب منها، وهو ما تؤكده المادة 17 من القانون رقم 09 – 04؛

ثانيا: أشار المشرع الجزائري في المادة 16 فقرة 1 من القانون رقم 09 – 04 إلى إمكانية تقديم المساعدة للدول المختلفة في إطار التحريات والتحقيق القضائي، لغرض جمع الدليل الإلكتروني الذي يثبت الجريمة الإلكترونية، ولكن السـؤال المطروح هنا: من هي السـلطة المختصـة في الجزائر التي تتكفل بتقديم المساعدة لنظيراتها في الخارج؟

إن من المهام الأساسية للهيئة الوطنية للوقاية من الجرائم الإلكترونية، التي تتشكل من خبراء مختصـين في هذا المجال، السـهر على تنفيذ طلبات المسـاعدة الصـادرة عن الدول الأجنبية وتطوير تبادل المعلومات والتعاون على المسـتوى الدولي في مجال اختصـاصـها في إطار الإتفاقيات التي توقعها الجزائر، وقد أكد هذا الأمر البند (ج) من المادة 14 من القانون رقم 09 – 04 التي حددت مهام الهيئة؛

ثالثا: بالنظر إلى أن المساعدة القضائية الدولية، بما في ذلك تبادل المعلومات، تتم في الغالب وِفق الطرق التقليدية البطيئة القائمة على نقل الوثائق الخطية والمختومة عبر القنوات الديبلوماسية أو أنظمة إرسال البريد القديمة، لذلك أكد المشرع الجزائري في المادة 16 فقرة 2 من القانون رقم 09 – 04 على أنه في حالة الطوارئ والإستعجال، كما هو الحال عادة بالنسبة للتحقيق في الجرائم الإلكترونية، يُمكن إرسال طلبات المعلومات عن طريق وسائل الإتصال السريعة، بما في ذلك أجهزة الفاكس أو البريد الإلكتروني، وذلك بقدر ما توفره هذه الوسائل من شروط أمن كافية للتأكد من صحتها؛

رابعا: فيما يخص القيود الواردة على طلبات المساعدة القضائية الدولية

نصـت المادة 18 فقرة أولى من القانون رقم 09 – 04 أن طلبات المسـاعدة القضـائية الدولية لا يمكن قبولها، فيما لو كان من شـأنها المسـاس بالسـيادة الوطنية أو النظام العام. وهذه مسـألة متروكة للسـلطة التقديرية للدولة (ممثلة في وزارة العدل عادة وفقا للإتفاقيات الثنائية الدولية) التي لها واسع النظر في تنفيذ أو عدم تنفيذ هذه الطلبات[1].

كما أشارت الفقرة الثانية من ذات المادة أن طلبات المساعدة القضائية الدولية يمكن أن تُقيَد بشـرط المحافظة على سـرية المعلومات المبلغة أو بشـرط عدم اسـتعمالها في غير ما هو مُوضح في الطلب.

خاتمة:

تتميز الجرائم الإلكترونية بمميزات فريدة من نوعها، فهي من جهة ذات طبيعة غير مادية، كما أنها ذات طبيعة عالمية، كون أن آثارها قد تتخطى الحدود الجغرافية لأكثر من دولة. وهذا الأمر طرح تحديات إجرائية جديدة تتعلق بمدى فعالية إجراءات التحري والتحقيق التقليدية في مواجهة هذه الجريمة والمجرم الذي يقترفها، ومدى الحاجة تبعا لذلك لإجراءات جديدة تتناسـب مع طبيعة هذه الجريمة.

وعلى إثر هذه التحديات الجديدة، وتماشـيا مع زيادة مُعدَلات الجرائم الإلكترونية المرتكبة يوما بعد يوم في الجزائر، تدخل المشـرع الجزائري، على غرار غيره من التشـريعات، بسـن إجراءات جزائية جديدة، تجسدت بشكل أساسي في وضـع قانون إجرائي مستقل يتضـمن أحكام إجرائيـة جديـدة تتعلق بـالجرائم الإلكترونيـة، هو القـانون رقم 09 – 04 المتعلق بـالوقـايـة من الجرائم الإلكترونية، كما أضاف المشرع نصوص جديدة في صلب قانون الإجراءات الجزائية.

أخذ المشـرع الجزائري أيضـا بعين الإعتبار الطبيعة التقنية للبيئة الرقمية التي تُرتكب فيها الجريمة الإلكترونية، وكذا مهارة وذكاء المجرم الإلكتروني، وتجلى ذلك من خلال اسـتحداث هياكل جديدة، إن كان ذلك على مسـتوى على الجهاز القضـائي، باسـتحداث القطب الوطني الخاص بالجريمة الإلكترونية مؤخرا، أو خارج الجهاز القضائي، من خلال إنشاء المشرع للهيئة الوطنية للوقاية من الجرائم الإلكترونية، وهي – أي الهيئة – بما لها من إمكانيات بشـرية وتقنية

[1] حابت أمال، المرجع السابق، ص 477.

عالية المســتوى، قد تســاهم إلى حد كبير في تحقيق الفعالية المرجوة في التعامل مع هذا النوع الجديد من الجرائم.

إن الطبيعة العابرة للحدود التي تَطبع الجرائم الإلكترونية في أغلب الحالات، جعلت من الآليات الداخلية المستحدثة على مستوى التشريعات الوطنية، سواء من حيث الإجراءات أو الهياكل، غير كافية عموما في مواجهة هكذا جرائم، الأمر الذي يجعل من التعاون الدولي، بمختلف آشكاله الأمنية والقضائية، في مجال الجرائم الإلكترونية أكثر من ضرورة، فإحساس المجرم بأنه لن يكون في مأمن من الملاحقة أينما وُجِدَ وارتحل، يُعد عاملا مُهما في إدخال الخوف والرعب في قلوب أؤلئك المجرمين، الشيء الذي قد يقلل من ارتكاب الجرائم الإلكترونية ويساهم في الحد منها.

تم بعون الله وتوفيقه

قائمة المصادر والمراجع:

أولا: المصادر (القوانين)

1. الأمر رقم 21 – 11 المؤرخ في 25 غشت 2021، يُتمم الأمر رقم 66 – 155 المؤرخ في 8 يونيو 1966 المتضمن قانون الإجراءات الجزائية. (ج ر: عدد 65، بتاريخ 26 غشت 2021، ص 7).
2. القانون رقم 16–02 المؤرخ 19 يونيو 2016، المعدل والمتمم لقانون العقوبات.
3. القانون رقم 09–04 المؤرخ في5 أوت 2009 والمتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، (ج. ر: عدد 47، بتاريخ 16 غشت 2009، ص5).
4. القانون رقم 06–22 المؤرخ في 20 ديسمبر 2006، المعدل والمتمم للأمر 155/66 المتضمن قانون الإجراءات الجزائية. (ج ر: 84، بتاريخ 24 ديسمبر 2006، ص 4).

ثانيا: المراجع

الكتب:

1. عادل عبد العال إبراهيم خرشي، إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعة الجديدة، مصر، 2015.
2. عبد الرحمان خلفي، الإجراءات الجزائية في التشريع الجزائري والمقارن، الطبعة الرابعة، دار بلقيس، الجزائر 2019.
3. عبد الله أوهايبية، شرح قانون الاجراءات الجزائية الجزائري، (التحري والتحقيق)، دار هومة، الطبعة الثانية، 2011.
4. عبد الله أوهايبية، شرح قانون العقوبات الجزائري، (القسم العام)، دار موفم للنشر، الجزائر، 2009.
5. محمد الأمين البشرى، التحقيق في الجرائم المستحدثة، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004.
6. يعيش تمام شوقي، الجريمة المعلوماتية، (دراسة تاصيلية مقارنة)، الطبعة الأولى، مطبعة الرمال، الوادي، الجزائر، 2019.

المجلات:

.1

2. أحمد قاسم فرح، النظام القانوني لمقدمي خدمات الأنترنت، (دراسة تحليلية مقارنة)، المنارة، المجلد 13، العدد 9، 2007.

3. بن بادة عبد الحليم، المراقبة الإلكترونية كإجراء لاستخلاص الدليل الإلكتروني، (بين الحق في الخصوصية ومشروعية الدليل الإلكتروني)، المجلة الأكاديمية للبحث القانوني، تصدر عن جامعة عبد الرحمان ميرة، بجاية، المجلد 10، العدد3، 2019.

4. بوعناد فاطمة الزهراء، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة الندوة للدراسات القانونية، العدد الأول، 2013،

5. بوقرة جمال الدين، عنان جمال الدين، القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، مجلة الأستاذ الباحث لدراسات القانونية والسياسية، جامعة محمد بوضياف بالمسيلة، الجزائر، المجلد 7، العدد1، جوان 2022.

6. ثابت دنيا زاد، مراقبة الإتصالات الإلكترونية والحق في حرمة الحياة الخاصة في القانون الجزائري، مجلة العلوم الإجتماعية والإنسانية، تصدر عن جامعة تبسة، الجزائر، العدد السادس، ديسمبر 2012.

7. جبار فطيمة، مراقبة الإتصالات الإلكترونية بين الحظر والإباحة في التشريع الجزائري، مجلة الدراسات القانونية المقارنة، يصدرها مخبر البحث (القانون الخاص المقارن)، جامعة حسيبة بن بوعلي الشلف الجزائر، العدد الثالث، ديسمبر 2016.

8. حابت أمال، دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها في مواجهة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، المجلة الدولية للبحوث القانونية والسياسية، تصدر عن كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر، الوادي، الجزائر، المجلد 5، العدد3، ديسمبر 2021.

9. رضا هميسي، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، تصدر عن كلية الحقوق والعلوم السياسية، جامعة الوادي، الجزائر، العدد 5، جوان 2012.

10. شرف الدين وردة، مشروعية أساليب التحري الخاصة في مكافحة الجريمة المعلوماتية – في التشريع الجزائري –، مجلة المفكر، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، العدد 15، جوان 2017.

11. شريفة سوماتي، القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال كآلية جديدة ضمن الجهاز القضائي المتخصص، مجلة الدراسات القانونية، المجلد 8، العدد2، جوان 2022.

12. صفاء حسن نصيف، التحديات الإجرائية المتصلة بالجرائم المعلوماتية، مجلة العلوم القانونية والسياسية، كلية القانون والعلوم السياسية، جامعة ديالي، العراق، المجلد الخامس، العدد الثاني، 2016.

13. عادل عبد العال إبراهيم خرشي، إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعة الجديدة، مصر، 2015.

14. عبد الله أو هايبية، تفتيش المساكن في القانون الجزائري، المجلة الجزائرية للعلوم القانونية والإقتصادية والسياسية، تصدر عن معهد الحقوق والعلوم الإدارية، جامعة الجزائر، الجزء 36، العدد2، 1998.

15. عبد المهدي كاظم ناصر، المسؤولية المدنية لوسطاء الأنترنت، مجلة القادسية للقانون والعلوم السياسية، كلية القانون، جامعة القادسية، العراق، المجلد الثاني، العدد الثاني، 2009.

16. عبير بعقيقي، **الإثبات في الجرائم المعلوماتية على ضوء القانون 09-04**، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمى لخضر، الوادي، الجزائر، المجلد 9، العدد2، جوان 2018.

17. عكو فاطمة الزهراء، ملاحظات حول التزامات مزود الوصول إلى الأنترنت لوقف نشر المحتوى غير المشروع بعد إضافة المادة 394 مكرر8 من ق ع في القانون رقم 16 – 02، مجلة الحقوق والعلوم السياسية، تصدر عن كلية الحقوق والعلوم السياسية، جامعة الجيلالي اليابسن سيدي بلعباس، الجزائر، العدد 13، 2017.

18. فريد ناشف، آليات التعاون الدولي في مكافحة الجرائم الإلكترونية، مجلة البحوث في الحقوق والعلوم السياسية، تصدر عن كلية الحقوق والعلوم السياسية، جامعة تيارت، الجزائر، المجلد 8، العدد1، 2022.

19. مصطفى عبد الباقي، التحقيق في الجريمة الإلكترونية وإثباتها في فلسطين، (دراسة مقارنة)، مجلة دراسات، علوم الشريعة والقانون، المجلد 45، عدد4، ملحق2، 2018.
20. يزيد بوحليط، تفتيش المنظومة المعلوماتية وحجز المعطيات في التشريع الجزائري، مجلة التواصل في التجارة والإقتصاد والقانون، تصدر عن جامعة باجي مختار، عنابة، عدد 48، ديسمبر 2016.

الرسائل الجامعية:

رسائل الدكتوراه:

1. براهيمي جمال، **التحقيق الجنائي في الجرائم الإلكترونية**، أطروحة لنيل شهادة دكتوراه في العلوم، تخصص قانون، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2018.
2. بشان عبد النور، الجوانب الموضوعية لمعالجة الجريمة المعلوماتية، أطروحة دكتوراه، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر 1، السنة الجامعية 2017 – 2018.
3. بن عزة محمد حمزة، **المسؤولية القانونية لمتعاملي الأنترنت**، (دراسة مقارنة)، أطروحة دكتوراه علوم، قانون إعلام، كلية الحقوق والعلوم السياسية، جامعة جيلالي اليابس، سيدي بلعباس، السنة الجامعية 2019/2018.
4. روابح فريد، **الأساليب الإجرائية الخاصة للتحري والتحقيق في الجريمة المنظمة**، أطروحة دكتوراه، القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة بن يوسف بن خدة، الجزائر1، 2016.
5. شنتير خضرة، **الآليات القانونية لمكافحة الجريمة الإلكترونية**، (دراسة مقارنة،)، أطروحة دكتوراه، (ل م د)، تخصص القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة أحمد درارية، أدرار، السنة الجامعية 2021/2020.
6. عكو فاطمة الزهرة، **المسؤولية المدنية لمقدمي الخدمة الوسيطة في الأنترنت**، رسالة دكتوراه، قانون خاص، كلية الحقوق، جامعة الجزائر1، السنة الجامعية 2016/2015.

7. لهوى رابح، الشرعية الإجرائية للأدلة المعلوماتية المستمدة من التفتيش، أطروحة دكتوراه، تخصص: علوم جنائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة باتنة 1، السنة الجامعية: 2021/2020.

8. مولاي ملياني دلال، إشكالية الإثبات في جرائم الأنترنت في التشريع الجزائري، قسم القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، السنة الجامعية: 2018/2017.

9. نادية سلامي، آليات مكافحة التجسس الإلكتروني، أطروحة دكتوراه، علوم، تخصص: القانون الجنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي، تبسة، الجزائر، السنة الجامعية: 2018 – 2019.

مذكرات الماجستير:

1. سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجستير، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، السنة الجامعية 2012 – 2013.

2. عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، (دراسة مقارنة)، رسالة ماجستير، كلية الحقوق، جامعة الإسكندرية، 2009.

أشغال الملتقيات:

امحمدي بوزينة آمنة، إجراءات التحري الخاصـــة في مجال مكافحة الجرائم المعلوماتية، (دراســـة تحليلية لأحكام قانون الإجراءات الجزائية وقانون الوقاية من جرائم الإعلام)، أعمال الملتقى الوطني (آليات مكافحة الجرائم الإلكترونية في التشــريع الجزائري)، الجزائر: 29 مارس 2017، المنظم من طرف مركز جيل البحث العلمي، 2017.

الفهرس: