

خصوصية إجراءات متابعة الجرائم المتصلة
بتكنولوجيا الإعلام والاتصال

السنة الجامعية 2025/2026 ة

شكر وتقدير

الحمدُ والشكرُ لله الذي أعاننا ووفّقنا على إنجاز هذا البحث، والذي نرجو أن يترك أثرًا نافعًا في مجال البحث العلمي، ونسأله تعالى أن يكون خالصًا لوجهه الكريم، وأن ينفع به كلّ من يطّلع عليه.

ولا يسعنا إلا أن نتقدّم بخالص عبارات الشكر والتقدير إلى مشرفنا الدكتور بن قويدر الطاهر الذي تفضّل بالإشراف على هذا العمل، فكان خير عونٍ لنا في إنجازه، ورافقنا بتوجيهاته السديدة وملاحظاته القيّمة في كل مرحلة من مراحل العمل كما نتوجّه بجزيل الشكر إلى كل من أسهم من قريب أو بعيد في دعم هذا العمل المتواضع، سواء بالمشورة أو بالتشجيع أو بتيسير سبل البحث.

الإهداء

الحمد لله وكفى والصلاة على الحبيب المصطفى وأهله ومن وفى أما بعد :

الحمد لله الذي وفقنا لثمين هذه الخطوة في مسيرتنا الدراسية بمذكرتنا هذه

ثمرة الجهد والنجاح بفضلته تعالى مهداة إلى الوالدين الكريمين حفظهما الله

وأدامهما نورا لدربي

لكل العائلة الكريمة الزوجة والأبناء والإخوة

أرجو أن يكون عملنا هذا مخلصا لوجه الله وأن تكون فيه الفائدة

قرقاب الطيب

الإهداء

الحمد لله الذي أنار لنا درب العلم و المعرفة وأعاننا على أداء هذا الواجب

ووفقنا في إنجازه

أقدم هذا العمل المتواضع إلى من اقترن اسمهما باسم رب العالمين والذي

وأمي متعهما الله بالصحة والعافية.

إلى أسرتي إلى أصدقائي إلى كل من دعا لي بالخير

إلى كل هؤلاء أهدي هذا العمل الذي أسأل الله تعالى أن يتقبله خالصا

عويسي حمو ضياء الدين

مقدمة

مقدمة

يشهد العالم المعاصر تحولات تكنولوجية متسارعة لم يسبق لها نظير في تاريخ الحضارة الإنسانية، إذ أفرزت ثورة تكنولوجيا الإعلام والاتصال واقعاً جديداً أعاد رسم ملامح المجتمعات في أبعادها الاقتصادية والاجتماعية والسياسية والقانونية على حدٍ سواء. فلم تعد الشبكات الرقمية مجرد أدوات تقنية لتسهيل التواصل وتبادل المعلومات، بل باتت بنيةً تحتيةً حيوية تُشغل منظومة المجتمع برمتها، من المعاملات المصرفية والإدارية إلى الأنظمة الأمنية والعسكرية، مما جعل الاعتماد عليها وجودياً لا اختياريّاً. وفي ظل هذا التوسع الرقمي المتصاعد، لم يكن بمقدور هذه البيئة الافتراضية أن تظل بمنأى عن ظاهرة الإجرام التي تلازم المجتمعات الإنسانية في كل صورها وأشكالها؛ فسرعان ما وجد الإجرام طريقه إلى هذا الفضاء الجديد، واستغل إمكانياته الهائلة ليفرز جيلاً جديداً من الجرائم التي لم تعرفها المنظومات القانونية الكلاسيكية.

والجريمة الإلكترونية في جوهرها ظاهرة مركّبة تتشابك في تكوينها أبعاد تقنية وقانونية واجتماعية متداخلة، تجعل التعامل معها تعاملاً أحادي البعد قاصراً عن استيعاب حجمها الحقيقي وخطورتها المتصاعدة. فهي من الناحية التقنية تُوظّف أرقى ما أفرزه العقل البشري من ابتكارات رقمية أداةً للاعتداء على الأشخاص والأموال والأنظمة والمعطيات، ومن الناحية القانونية تتحدى الأطر الإجرائية الكلاسيكية في مفاهيمها الراسخة كمفهوم الدليل ومحلّه وطرق جمعه، ومفهوم الاختصاص القضائي في ظل عابرية الفضاء الرقمي للحدود الجغرافية المرسومة. وقد وصف بعض الباحثين هذه الجريمة بأنها "الابن غير الشرعي الذي جاء نتيجة للتزاوج بين ثورة تكنولوجيا المعلومات والعولمة"، وهو توصيف يلتقط بدقة الجانب المزدوج لهذه الظاهرة التي هي في آنٍ معاً ثمرة التقدم ومحنته.

وعلى الصعيد الجزائري، كشفت الإحصاءات الصادرة عن الأجهزة الأمنية المختصة عن منحى تصاعدي لافت في القضايا الإلكترونية المعالجة على مدار السنوات الأخيرة، وهو ما يعكس عمق هذه الظاهرة ورسوخها في الواقع الوطني. وقد أدرك المشرع الجزائري مبكراً

جسامة هذا التحدي فتدخل تشريعياً بخطوات متتالية ومتكاملة؛ إذ أدرج في قانون العقوبات بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 نصوصاً تجريبية خاصة بالمساح بأنظمة المعالجة الآلية للمعطيات، تلتها الخطوة الأهم بصور القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الذي أرسى منظومة إجرائية استثنائية تستجيب لخصوصية هذا النوع من الجرائم. ثم توج هذا المسار بالأمر رقم 21-11 المؤرخ في 25 أوت 2021 الذي استحدث قطباً جزائياً وطنياً مختصاً بهذه الجرائم، فضلاً عن قانون الإجراءات الجزائية الجديد رقم 14-25 الذي جاء بأحكام متطورة في مجال التخصص القضائي وضمانات الشرعية الإجرائية في الفضاء الرقمي.

بيد أن الجهد التشريعي المبذول، على أهميته وعمقه، لا يُغني عن التساؤل الجوهرى حول مدى فعالية هذه المنظومة الإجرائية وقدرتها على تحقيق غايتين متوازيتين يصعب الجمع بينهما في أحيان كثيرة: فعالية المكافحة والردع من جهة، وصون الحقوق والحريات الأساسية التي كفلها الدستور الجزائري في تعديله لسنة 2020 من جهة أخرى. فالإجراءات الاستثنائية كمرقبة الاتصالات الإلكترونية والتفتيش عن بعد والتسرب الإلكتروني تنطوي بطبيعتها على مساح بالحياة الخاصة للأفراد، وهو مساح لا يُقبل قانوناً إلا في الحدود الضيقة التي رسمها المشرع وتحت الرقابة القضائية الصارمة. فهل نجح المشرع الجزائري في تحقيق هذا التوازن الدقيق؟ وما مدى فعالية المنظومة الإجرائية القائمة في مواجهة إجرام رقمي يتجدد باستمرار ويتخطى الحدود بلا توقف؟

أولاً: أهمية الدراسة

تستمد هذه الدراسة أهميتها من تشابك مستويات متعددة تجعل منها إسهاماً أكاديمياً ذا قيمة في أدبيات القانون الجنائي الجزائري. على مستوى الأهمية النظرية، تتناول الدراسة إشكاليات بالغة الدقة تمسّ صميم القانون الجنائي الإجرائي في مفاهيمه الراسخة؛ فهي تُعيد طرح السؤال حول مفهوم الدليل ومحلّه وشروط صحته في بيئة يغيب فيها المادي ويحلّ محلّه الافتراضي، وتستجلي مدى كفاية الإجراءات الجنائية الجزائرية في استيعاب خصائص

الجريمة الرقمية واستجاباتها المتطورة. وهي إشكاليات تتفرد بها الجريمة الإلكترونية دون سائر الجرائم، مما يجعل معالجتها ذات قيمة نظرية خاصة تتعدى مجرد الوصف إلى التحليل والنقد.

أما على مستوى الأهمية العملية، فإن تصاعد حالات الجرائم الإلكترونية في الجزائر يجعل التحليل النقدي للإطار الإجرائي القائم ذا صلة مباشرة بالأداء الميداني للأجهزة الأمنية والقضائية، في ظل تطور أساليب الإجرام الرقمي وتجاوزها المستمر لما أرساه المشرع من أطر. وثمة بُعد ثالث يتعلق بالتوازن الدستوري الدقيق بين ضرورة التصدي الفعال للجريمة الإلكترونية وصون الحقوق والحريات المكفولة دستورياً، وهو توازن يُشكّل الرهان الأعمق الذي تُوجد المنظومة الإجرائية وتعمل في ضوئه.

ثانياً: أهداف الدراسة

تتطوي هذه الدراسة على ثلاثة أهداف متكاملة؛ يتجلى الأول في الاستعراض الوصفي والتحليلي للإطار التشريعي الجزائري المنظم للجرائم المتصلة بتكنولوجيا الإعلام والاتصال، من خلال استقراء النصوص ذات الصلة وبيان الخصوصية الإجرائية التي أرساها المشرع. ويتجلى الثاني في التقييم النقدي لهذه المنظومة الإجرائية بهدف رصد مواطن القصور والثغرات التي تحدّ من فعاليتها الميدانية، سواء على المستوى النصي أو على صعيد التطبيق. أما الهدف الثالث فيتمثل في المساهمة في تغذية النقاش القانوني الأكاديمي بقراءة نقدية موضوعية تستحضر مستجدات المنظومة القانونية الجزائرية بما فيها قانون الإجراءات الجزائية الجديد رقم 14-25.

ثالثاً: المنهج المتبع

اقتضت طبيعة الموضوع وتعدد أبعاده الاستعانة بمناهج بحثية متكاملة؛ فالمنهج التحليلي حاضر في تفكيك النصوص القانونية ذات الصلة واستجلاء مقاصدها وتقييم كفايتها ومدى تكاملها، والمنهج الوصفي لازم في رصد الهياكل المؤسسية وآليات عملها والإجراءات المستحدثة وخصائصها. ويُستعان بالمنهج المقارن في حدوده اللازمة لإضاءة الإطار

الجزائري وتقييمه في ضوء تجارب تشريعية أرسخ باعاً في هذا الميدان، لا بهدف الاستنساخ بل بغرض بناء رؤية نقدية متوازنة.

رابعاً: الدراسات السابقة

لا تنطلق هذه الدراسة من فراغ علمي، بل تستند إلى رصيد أكاديمي متراكم وإن ظلّ غير مُوفٍ لجوانب الموضوع في مجملها. فقد تناولت رسالة نعيم سعيداني المقدّمة لنيل درجة الماجستير سنة 2013 من جامعة الحاج لخضر باتّة تحت عنوان "آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري" الجانب التشغيلي لأجهزة الضبط القضائي دون التعمق الكافي في إشكالية الدليل الرقمي وحجّيته وشروط صحته. وفي سياق أحدث، قدّمت جراد سميرة وقاتل جمال ورقة بحثية منشورة في مجلة الاجتهاد للدراسات القانونية والاقتصادية سنة 2025 تحت عنوان "خصوصية المتابعة الجزائية للجرائم الإلكترونية"، تناولت فيها بالتحليل أهم الآليات الإجرائية الجزائية المستحدثة، وإن بقيت جوانب من الموضوع تستدعي مزيداً من التعمق، لا سيما ما يتعلق بالضمانات الدستورية المحيطة بالإجراءات الاستثنائية ومستجدات قانون الإجراءات الجزائية رقم 14-25. كما اهتمت مذكرات ماستر جامعية عديدة بجوانب محددة من الموضوع غير أنها تبقى جزئية تناول.

وما يُميز هذه الدراسة عن سابقتها محاولة الجمع بين تشريح المنظومة الإجرائية الاستثنائية التي وضعها المشرع الجزائري بما فيها أحكام قانون الإجراءات الجزائية الجديد، وبين التحليل النقدي لضمانات حماية الحقوق والحريات في مواجهة سلطات التحري الرقمي الواسعة الممنوحة للأجهزة المختصة.

انطلاقاً من الفجوة بين تصاعد الظاهرة الإجرامية الرقمية وقصور التحليل الشامل لإطارها الإجرائي في الأدبيات القانونية الجزائرية، تصاغ الإشكالية الرئيسية على النحو الآتي:

إلى أي مدى نجح المشرع الجزائري في بناء منظومة إجرائية فعّالة وخاصة لمتابعة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وفق خصوصية هيكلية وتقنية مستحدثة، مع

صون التوازن المطلوب بين متطلبات فعالية مكافحة ضمانات حماية الحقوق والحريات الأساسية؟

وتتفرع عن هذه الإشكالية تساؤلات فرعية: ما الخصوصية الهيكلية والقضائية للجهات المكلفة بمتابعة الجرائم الإلكترونية؟ وما الأساليب التقنية الخاصة التي استحدثها المشرع للبحث والتحري الرقمي؟ وما القواعد الخاصة التي تحكم التفتيش والحجز في البيئة الرقمية؟ وما القيمة الإثباتية للدليل الرقمي وما الضمانات التي تكفل مشروعية استخدامه؟

خامسا: خطة البحث

في معالجة هذه الإشكالية، اقتضت طبيعة الموضوع تقسيم البحث إلى فصلين رئيسيين ؛ يُخصص الفصل الأول للخصوصية التنظيمية لهيئات المتابعة وآليات التحري الرقمي المستحدثة، من خلال مبحث أول يتناول الخصوصية الهيكلية والقضائية للجهات المكلفة بالمتابعة، ومبحث ثانٍ يُعنى بالأساليب التقنية الخاصة للبحث والتحري الرقمي. أما الفصل الثاني فيُكرّس لخصوصية المعاينة الرقمية وضمانات الشرعية الإجرائية، من حيث خصوصية التفتيش والحجز في البيئة الرقمية في مبحثه الأول، وحجية الدليل الرقمي وضوابط حماية الحريات الفردية في مبحثه الثاني.

الفصل الأول:

الخصوصية التنظيمية لهيئات المتابعة وآليات التحري الرقمي
المستحدثة

يُمثّل هذا الفصل البوابة الأولى لفهم المنظومة الإجرائية الاستثنائية التي أرساها المشرع الجزائري في مواجهة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال؛ إذ لا يكفي في مقاربة هذه الظاهرة الإجرامية المستحدثة الاكتفاء بنصوص التجريم الموضوعية، بل لا بدّ من استجلاء المنظومة الإجرائية الكاملة التي تتكفل بتفعيل هذه النصوص ميدانياً وتحويلها من حبر على ورق إلى آليات ردع وملاحقة فعّالة. وقد انتهج المشرع الجزائري في هذا الإطار مساراً مزدوجاً؛ أولهما بناء هياكل مؤسساتية وقضائية متخصصة قادرة على استيعاب التعقيد التقني الذي تنطوي عليه هذه الجرائم، وثانيهما منح هذه الهياكل أدوات تحرّ استثنائية لم تكن مألوفة في المنظومة الإجرائية الكلاسيكية، تتيح لها رصد الدليل الرقمي وجمعه قبل أن يُمحي أو يُعدّل.

وتتجلى خطورة هذين المسارين معاً في أنهما يُحدثان قطيعةً نوعية مع منطق الإجراءات الجنائية التقليدية؛ فالهياكل المستحدثة لا تعمل وفق الأطر الاختصاصية الإقليمية المعهودة، بل تمتد صلاحياتها عابرة الحدود الجغرافية متى تعلق الأمر بالمصالح الاستراتيجية للدولة الجزائرية. والأدوات التقنية الممنوحة لأجهزة التحري تتيح اختراق الاتصالات الخاصة ومراقبة الفضاء الرقمي، وهو ما كان يُعدّ انتهاكاً صريحاً لمبدأ سرية المراسلات في المنظومة الكلاسيكية. ولا يجوز إغفال هذه الخطورة المزدوجة حين تُناقش فعالية هذه المنظومة، إذ ينبغي دائماً استحضار الرهان المحوري المتمثل في الموازنة بين اقتضاءات الأمن الرقمي ومتطلبات صون الحقوق الدستورية للأفراد.

وعلى هذا الأساس يُقسم هذا الفصل إلى مبحثين متكاملين؛ يتناول **المبحث الأول** الخصوصية الهيكلية والقضائية للجهات المكلفة بمتابعة الجرائم الإلكترونية، فيما يُعنى **المبحث الثاني** بالأساليب التقنية الخاصة للبحث والتحري الرقمي المستحدثة في التشريع الجزائري.

المبحث الأول: الخصوصية الهيكلية والقضائية للجهات المكلفة بالمتابعة

لا يمكن الحديث عن فعالية إجرائية في مواجهة الجريمة الإلكترونية دون تحديد دقيق للجهات المؤهلة قانوناً وتقنياً للتعامل معها. فالمشرع الجزائري أدرك أن الأجهزة القضائية والأمنية التقليدية، مهما بلغت من كفاءة في ميادينها المعهودة، تظل عاجزة عن مواجهة جرائم تختبئ خلف شاشات حاسوبية وتنتقل عبر ألياف ضوئية وتترك أثراً رقمياً لا تُقرأ إلا بأدوات تقنية متخصصة. لذلك أثر المشرع التدخل لإرساء منظومة هيكلية متكاملة تضم هيئات تقنية متخصصة وأقطاباً قضائية ذات اختصاص موسّع يتجاوز القيود الإقليمية الكلاسيكية. غير أن هذا التدخل لا يصحّ دراسة دون استيعاب وعاء التجريم الرقمي الذي يُشكّل الأساس الذي تقوم عليه هذه المنظومة الهيكلية. ويتناول هذا المبحث في مطلبه الأول وعاء التجريم الرقمي ومبدأ الامتداد الاختصاصي، ثم في مطلبه الثاني الهيئات المتخصصة والأقطاب القضائية المختصة¹.

المطلب الأول: وعاء التجريم الرقمي وامتداده المكاني الحامي للمصالح الاستراتيجية

يُشكّل تحديد النطاق المفاهيمي للجريمة التكنولوجية وتعيين المجال الاختصاصي للمحاكم الجزائرية في مواجهتها ركيزتين لا غنى عنهما لأي منظومة إجرائية متماسكة. إذ لا قيمة لهياكل مؤسساتية مهما بلغت من تخصص وكفاءة إذا لم يكن وعاء التجريم محدداً بدقة كافية، ولا قيمة لاختصاص قضائي إذا ظل مقيداً بحدود إقليمية لا تعرفها الجريمة الإلكترونية ولا تُقيدها. وقد أدرك المشرع الجزائري هذه الحقيقة فعالج المسألتين معاً في إطار تشريعي متسق.

¹ محمد حزيق، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، دار هومة للطباعة والنشر والتوزيع، الجزائر، الطبعة الثانية، 2018، ص 133-154.

الفرع الأول: تحديد مفهوم الجريمة التكنولوجية ونطاق المتابعة الإجرائية

أولاً: المفهوم التشريعي وفق القانون 04-09

آثر المشرع الجزائري في القانون رقم 04-09 المؤرخ في 05 أوت 2009 اعتماداً منهجية تعريفية وظيفية تقوم على الوصف الموضوعي بدلاً من التعريف المجرد المنفصل عن الواقع التطبيقي، وهو مسلك يتسق مع منطق التشريع الجنائي الذي يُفضّل الدقة التحديدية على العموميات الفضفاضة التي تُفتح لتأويلات متعارضة. فقد نصّت الفقرة (أ) من المادة الثانية من هذا القانون على أن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال هي: "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية".¹

ويتضمن هذا التعريف التشريعي في حقيقته معياراً مزدوجاً جامعاً بين المحل الجرمي ووسيلة الارتكاب في آنٍ معاً؛ فالطائفة الأولى تضم الجرائم التي تستهدف مباشرة أنظمة المعالجة الآلية للمعطيات وما تحويه من بيانات، وهي الجرائم المدرجة في المواد من 394 مكرر إلى 394 مكرر 7 من قانون العقوبات. أما الطائفة الثانية فتشمل سائر الجرائم التي تتخذ من الفضاء الرقمي أداةً لارتكابها دون أن يكون النظام المعلوماتي هدفاً في حد ذاته، كجرائم النصب والاحتيال الإلكتروني وجرائم الابتزاز والتشهير عبر الإنترنت. وهذا التوسيع مقصود ومحسوب، إذ يُعالج حالة التطور المستمر لأساليب الإجرام الرقمي التي لا يمكن حصرها مسبقاً في قائمة مغلقة دون المساس بفعالية التجريم.

¹ القانون رقم 04-09 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، المادة 2 الفقرة أ.

ثانياً: مفهوم نظام المعالجة الآلية للمعطيات

كما عرّفت المادة الثانية من القانون ذاته "الاتصالات الإلكترونية" في فقرتها (ج) بأنها "أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية". وقد استكمل المشرع هذا البناء المفاهيمي في قانون العقوبات بموجب القانون رقم 15-04، إذ عرّف "نظام المعالجة الآلية للمعطيات" بأنه كل مجموعة أجهزة مترابطة تقوم بمعالجة آلية للمعطيات، وهو تعريف يكتسي طابعاً وظيفياً مرناً يشمل الحواسيب الشخصية والشبكات المحلية والخوادم البعيدة والهواتف الذكية على حدّ سواء. وهذه المرونة المفاهيمية ضرورة تقنية في ظل تطور أشكال الأجهزة الرقمية وتعددتها وتجديدها المستمر.¹

ثالثاً: الأثر الإجرائي للتعريف التشريعي

لا يقتصر أثر هذا التعريف على الجانب الموضوعي بل يمتد إلى الجانب الإجرائي امتداداً مباشراً؛ إذ يُحدد نطاق تطبيق الإجراءات الاستثنائية كمراقبة الاتصالات الإلكترونية والتفتيش عن بعد وسائر الأدوات التقنية التي منحها المشرع لأجهزة التحري، فهذه الأدوات لا تُستعمل إلا في الجرائم الداخلة ضمن وعاء التجريم الذي حدده القانون 04-09. كما يُحدد نطاق اختصاص الهيئات المؤسسية المستحدثة والأقطاب القضائية المتخصصة، فلا يجوز لهذه الهيئات مباشرة اختصاصاتها إلا في الجرائم المحددة بموجب هذا الوعاء التجريمي، تحت طائلة البطلان الإجرائي المقرر قانوناً.

¹ القانون رقم 15-04 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات، الجريدة الرسمية، العدد 71.

الفرع الثاني: مبدأ الامتداد الاختصاصي العابر للحدود

أولاً: إشكالية الاختصاص الإقليمي في مواجهة الجريمة الإلكترونية

تُشكّل إشكالية الاختصاص القضائي أحد أعقد التحديات التي تُقرزها الجريمة الإلكترونية على المنظومة القانونية الكلاسيكية؛ إذ يقوم القانون الجنائي التقليدي في تحديد الاختصاص على مبدأ الإقليمية الذي يربط الاختصاص القضائي بمكان ارتكاب الجريمة أو مكان إقامة المتهم. وهذا المبدأ، المنطقي في مواجهة جرائم مادية تقع في مكان محدد وتخلّف آثاراً ملموسة في إقليم بعينه، يبدو مُربكاً وقاصراً حين يُواجه بجريمة إلكترونية يكون فيها الجاني في دولة ما والضحية في دولة أخرى والخادم الذي حُزنت فيه الأدلة في دولة ثالثة، وتمتد آثارها إلى دول رابعة وخامسة في اللحظة ذاتها. هذا الواقع يجعل تطبيق مبدأ الإقليمية الصارم مدعاةً للتهرب من العقاب لا ضماناً للعدالة.

ثانياً: الحل التشريعي الجزائري: الامتداد الاختصاصي الاستراتيجي

تدخّل المشرع الجزائري للخروج من هذا المأزق بصياغة تشريعية استراتيجية تحمي المصالح الجوهرية للدولة بصرف النظر عن مكان ارتكاب الجريمة. فقد نصّت المادة 15 من القانون 04-09 على منح المحاكم الجزائرية اختصاصاً بمتابعة الجرائم التكنولوجية المرتكبة خارج الإقليم الوطني، حتى ولو كان مرتكبها أجنبياً غير مقيم في الجزائر، متى استهدفت هذه الجرائم مؤسسات الدولة الجزائرية أو أجهزة الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني.¹

وهذا الامتداد الاختصاصي الاستراتيجي يقوم على معيار المصلحة المحمية لا معيار الإقليمية، وهو مسلك تشريعي يتسق مع الواقع الجيوسياسي الراهن الذي تُشكّل فيه البنية

¹ القانون رقم 04-09، المرجع السابق، المادة 15.

التحتية الرقمية للدولة هدفاً استراتيجياً تسعى القوى المعادية إلى اختراقه والتأثير فيه من بُعد. فحماية منظومة الدفاع الوطني وأنظمة المؤسسات العامة والاقتصاد الوطني من الاختراق الرقمي باتت مسألة سيادة بالمعنى الكامل للكلمة، ولا يجوز تركها رهينةً لمصادفات الإقليمية وتعقيدات التسليم والإنابة القضائية الدولية.

ثالثاً: الأسس القانونية المعززة لهذا الامتداد

يستند هذا الامتداد الاختصاصي إلى منطق قانوني متسق مع المبادئ الراسخة في القانون الدولي الجنائي؛ فمبدأ الشخصية الإيجابية وإن أجاز للدول ملاحقة رعاياها عن الجرائم المرتكبة في الخارج، فإن المشرع الجزائري ذهب أبعد من ذلك ليُجيز الملاحقة حتى ضد الأجانب متى مسّت جرائمهم مصالح الدولة الجزائرية الجوهرية. وهو تشريع يُجسد مبدأ الشخصية السلبية الموسّع، المعمول به في كثير من التشريعات المقارنة عند تعلق الأمر بالجرائم ذات التأثير على الأمن القومي. ويتكامل هذا الامتداد مع المادة 37 من قانون الإجراءات الجزائية التي وسّعت الاختصاص الإقليمي لوكيل الجمهورية في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات لتمتد إلى دوائر اختصاص محاكم أخرى.¹

رابعاً: الإشكاليات العملية لمبدأ الامتداد الاختصاصي

على الرغم من أهمية هذا الامتداد الاختصاصي من حيث المبدأ، تبرز في تطبيقه إشكاليات عملية جسيمة لا يمكن إغفالها. فالتحقيق في جريمة إلكترونية مرتكبة من الخارج يستلزم جمع أدلة رقمية مخزنة في دول أجنبية، وهو ما يصطدم بسيادة هذه الدول وقوانين حماية البيانات المعمول بها فيها. كما أن القبض على مرتكب جريمة إلكترونية موجود خارج الإقليم الجزائري يستلزم تفعيل آليات التسليم والتعاون القضائي الدولي، وهي آليات بالغة البطء

¹ القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون الإجراءات الجزائية، الجريدة الرسمية، العدد 84، المادة 37.

قياساً بسرعة الجريمة الإلكترونية وسهولة محو آثارها. وهذه الإشكاليات تُقضي إلى فجوة عملية بين الاختصاص المُقرّر نصاً والقدرة الفعلية على ممارسته، وهي فجوة تستدعي الاهتمام التشريعي والمؤسّساتي في المرحلة القادمة.

المطلب الثاني: الهيئات المتخصصة والأقطاب القضائية في التحري الرقمي والمتابعة

يُشكّل التنظيم المؤسّساتي الوجه التطبيقي للمنظومة التشريعية؛ إذ لا قيمة عملية لأي نص مهما بلغت دقته ما لم يُسند به بناء مؤسّساتي قادر على تجسيده ميدانياً. وقد حرص المشرع الجزائري على إرساء منظومة هيكلية متعددة المستويات تجمع بين الهيئة الوطنية المتخصصة ذات الطابع التقني والأقطاب القضائية ذات الاختصاص القضائي الخاص، في تكامل هيكلي يسعى إلى الجمع بين التخصص التقني والسلطة القضائية¹.

الفرع الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها

أولاً: الأساس القانوني وتطور التنظيم

أنشأ المشرع الجزائري بموجب المادة الثالثة عشرة من القانون 09-04 الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، لتُشكّل الدرع التقني الأول في منظومة مكافحة الإجرام الرقمي. وقد حدّد المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر 2015 تشكيلتها وتنظيمها وكيفيات سيرها، قبل أن يأتي المرسوم الرئاسي رقم 20-183 المؤرخ في 13 جويلية 2020 ليعيد تنظيمها في ضوء التحديات المستجدة، مُقرّراً

¹ عبد الفتاح بيومي حجازي، الدليل الجنائي الرقمي وجرائم الإنترنت، دار الفكر الجامعي، الإسكندرية، 2008، ص

مجلس توجيه تحدد المادة السابعة منه مهامه في توجيه عمل الهيئة والإشراف عليها ومراقبتها، والمداولة حول الاستراتيجية الوطنية للوقاية من الجرائم المعلوماتية.¹

وتتشكل الهيئة من لجنة مديرة ومديرية عامة ومديرية للمراقبة الوقائية واليقظة الإلكترونية ومديرية التنسيق التقني ومركز العمليات التقنية وملحقات جهوية. ويُعكس هذا التنظيم الهيكلي المتشعب إدراكاً واضحاً لضرورة التخصص الوظيفي داخل الهيئة ذاتها، إذ تتكفل كل وحدة بجانب محدد من عمل مكافحة الرقمية.

ثانياً: المهام الجوهرية للهيئة

تضطلع الهيئة وفقاً للمادة الرابعة عشرة من القانون 09-04 بمهام محورية متعددة لا يمكن اختزالها في دور إداري بحت، بل تمتد لتشمل الجانبين الوقائي والتحري معاً. فعلى صعيد الوقاية، تضطلع الهيئة بتنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على المستوى الوطني، وهي مهمة تقتضي رصدًا مستمرًا لمستجدات الإجرام الرقمي واستشرافاً لأساليبه المتطورة. وعلى صعيد دعم أجهزة العدالة، تضطلع الهيئة بمساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال التحريات وإنجاز الخبرات التكنولوجية، وهو ما يُكرّس دورها كرافد تقني للسلطة القضائية لا كجهاز مستقل عنها.²

وتُضاف إلى هذه المهام مهمة تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية، وهي مهمة بالغة الأهمية تُجسّد دور الهيئة في ضمان سلامة الدليل الرقمي قبل تقديمه أمام القضاء. ثم تبادل المعلومات مع

¹ المرسوم الرئاسي رقم 20-183 المؤرخ في 13 جويلية 2020 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 40، المادة 7.

² القانون رقم 09-04، المرجع السابق، المادة 14 الفقرتان أ وب.

نظيراتها في الخارج قصد التعرف على مرتكبي الجرائم الإلكترونية وتحديد مكان تواجدهم، وهو ما يُجعل منها بوابة التعاون الدولي التقني في هذا الميدان.

ثالثاً: نطاق الرقابة على عمل الهيئة

تخضع الهيئة لنوعين متكاملين من الرقابة يُشكّلان ضماناً جوهرياً ضد التجاوز في استخدام صلاحياتها التقنية الواسعة؛ أولهما رقابة السلطة التنفيذية من خلال رفع تقارير دورية إلى الجهات المختصة، وثانيهما الرقابة القضائية التي تُمثّل الضمانة الأساسية، إذ تمارس السلطة القضائية الاختصاص الحصري في مراقبة الاتصالات الإلكترونية تحت إشراف قاضٍ مختص. وهذا التوازن بين التخصص التقني للهيئة والرقابة القضائية عليها يُجسّد الحرص التشريعي على الجمع بين الفعالية الأمنية وصون ضمانات الشرعية الإجرائية.

غير أن الممارسة الميدانية تكشف عن إشكالية حقيقية تتعلق بمدى فعالية هذه الرقابة القضائية على عمل هيئة ذات طابع تقني بالغ التخصص والتعقيد، إذ يجد القاضي نفسه في مواجهة تقارير وخبرات تقنية يصعب عليه تقييمها بصورة مستقلة في غياب تكوين تقني كافٍ. وهو ما يجعل الرقابة القضائية أحياناً رقابةً شكليةً تُطغي عليها الثقة في التقرير التقني دون نقد موضوعي مستقل.

الفرع الثاني: الأجهزة الأمنية المتخصصة في الضبط القضائي الرقمي

أولاً: المعهد الوطني للأدلة الجنائية وعلم الإجرام

أنشئ المعهد الوطني للأدلة الجنائية وعلم الإجرام بالمرسوم رقم 04-183 المؤرخ في 26 جوان 2004، وهو مؤسسة عمومية ذات طابع إداري تحت الوصاية المباشرة لوزير الدفاع الوطني. ويضم المعهد دائرة للإعلام الآلي والإلكترونيك مكلفة بمعالجة وتحليل وتقديم كل

دليل رقمي للعدالة، وتتفرع إلى ثلاثة مخابر متخصصة: مخبر الإعلام الآلي المتخصص في تحليل الحوامل الرقمية، ومخبر الفيديو المختص بإعادة بناء مسرح الجريمة ومقارنة الصور، ومخبر الصوت. وقد شهدت القضايا المعالجة من قبل هذه المؤسسة نمواً لافتاً يُعكس تصاعد الإجرام الرقمي في الواقع الجزائري، إذ انتقلت من 18 قضية سنة 2009 إلى 240 قضية سنة 2015، أي نمواً يفوق 13 ضعفاً في ست سنوات.¹

ثانياً: المصلحة المركزية لمكافحة الجريمة المعلوماتية

أنشئت هذه المصلحة التابعة لمديرية الأمن الوطني سنة 2010، وهي الذراع التشغيلية للشرطة القضائية في مواجهة الإجرام الرقمي. وتوزعت خلاياها على مستوى الولايات في ثماني خلايا بالشرق وثمانى بالوسط وست بالغرب وواحدة بالجنوب، مما يُعكس محاولة اللامركزية الجغرافية في مواجهة ظاهرة لا تعرف الحدود الجغرافية. غير أن هذا التوزيع يكشف في الوقت ذاته عن عدم تكافؤ في الحضور الجغرافي لهذه الخلايا، إذ تتمركز أغلبها في المناطق الحضرية الكبرى فيما يظل التغطية في المناطق الداخلية والجنوبية محدودة.²

الفرع الثالث: الأقطاب القضائية المتخصصة وآفاق التخصص القضائي

أولاً: المسار التشريعي لإرساء التخصص القضائي

أدرك المشرع الجزائري مبكراً أن القضاء العادي بتكوينه القانوني المعهود وأدواته الإجرائية الكلاسيكية لا يستطيع وحده مواجهة قضايا بالغة التعقيد التقني كالجرائم الإلكترونية. فتدخل بموجب القانون رقم 04-14 المؤرخ في 10 نوفمبر 2004 باستحداث "القطب الجزائري

¹ حكار، أيمن، وبدير، يحيى. الجرائم المتصلة بتكنولوجيات الإعلام والاتصال. مذكرة ماستر، جامعة بلحاج بوشعيب عين تموشنت، 2022-2023، ص 47.

² رفعي، سمير. البحث والتحري عن الجريمة الإلكترونية. مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة 20 أوت 1955 سكيكدة، 2017، ص 52.

المتخصص"، ونظّم المرسوم التنفيذي رقم 06-348 المؤرخ في 05 أكتوبر 2006 المعدّل بالمرسوم رقم 16-267 المؤرخ في 17 أكتوبر 2016 هذا التوسع، محدداً أربعة أقطاب قضائية جهوية على مستوى محاكم الجزائر العاصمة وقسنطينة وورقلة ووهران، تختص بالنظر في الجرائم الإلكترونية على امتداد دوائر اختصاص المجالس القضائية التابعة لها.¹

ثانياً: القطب الجزائي الوطني: قفزة نوعية في التخصص القضائي

جاءت الخطوة الأكثر أهمية في مسار التخصص القضائي بصدور الأمر رقم 21-11 المؤرخ في 25 أوت 2021 المعدل والمتمم لقانون الإجراءات الجزائية، الذي استحدث "القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال" على مستوى محكمة الجزائر العاصمة، ومنحه اختصاصاً يمتد على كامل التراب الوطني في طائفة محددة من أشد الجرائم الإلكترونية خطورةً وتعقيداً. وقد عرّفت المادة 211 مكرر 22 الجرائم الداخلة في اختصاص هذا القطب بأنها تلك التي يمكن ارتكابها باستعمال أنظمة المعلومات أو أنظمة الاتصالات الإلكترونية أو بأي وسيلة أخرى في البيئة الرقمية.²

وتتضمن الجرائم الداخلة صراحةً في اختصاص هذا القطب بموجب المادة 211 مكرر 24: الجرائم الماسة بأمن الدولة والدفاع الوطني عبر الفضاء الرقمي، وجرائم نشر الأخبار الكاذبة والتحريض على الفتنة عبر الوسائل الإلكترونية، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات الخاصة بالإدارات والهيئات العامة، فضلاً عن جرائم التمييز وخطاب الكراهية الإلكتروني.

¹ المرسوم التنفيذي رقم 06-348 المؤرخ في 05 أكتوبر 2006 المعدل بالمرسوم رقم 16-267 المؤرخ في 17 أكتوبر 2016، الجريدة الرسمية، العدد 62.

² الأمر رقم 21-11 المؤرخ في 25 أوت 2021 المعدل والمتمم للأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، العدد 65، المادة 211 مكرر 22.

ثالثاً: مستجدات قانون الإجراءات الجزائية الجديد رقم 14-25

يُعدّ قانون الإجراءات الجزائية الجديد رقم 14-25 مرحلةً جديدةً ونقلةً نوعيةً في مسار تطوير المنظومة الإجرائية الجزائية في مواجهة الجرائم الإلكترونية؛ إذ جاء بأحكام متطورة تنظم الأقطاب القضائية المتخصصة سواء منها الوطنية أو المحلية، مع ضبط دقيق لآجال وإجراءات التلبس الرقمي الذي يطرح إشكالية تحديدية خاصة، إذ كيف يتسنى الحديث عن "حالة تلبس" في جريمة ترتكب في الفضاء الرقمي وتنتهي في أجزاء من الثانية. كما نظم هذا القانون إجراءات التوقيف للنظر في القضايا الإلكترونية بما يضمن فاعلية الملاحقة الأمنية دون المساس بضمانات المتهم الدستورية.¹

ويتكامل هذا القانون مع المنظومة التشريعية السابقة ليُشكّل إطاراً إجرائياً أكثر اكتمالاً وأشدّ تخصصاً في مواجهة الإجرام الرقمي، وإن كانت التساؤلات تبقى مشروعةً حول مدى الرقابة الفعلية التي تُمارسها الأقطاب القضائية على الأدوات الاستثنائية الممنوحة لأجهزة التحري، لا سيما في ظل الفجوة التقنية بين كفاءة الأجهزة الأمنية وكفاءة القاضي في تقييم أعمالها.

¹ جراد، سميرة، وقتال، جمال. "خصوصية المتابعة الجزائية للجرائم الإلكترونية". مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد 14، العدد 01، 2025، ص 38.

المبحث الثاني: الأساليب التقنية الخاصة للبحث والتحري الرقمي

إذا كان المبحث الأول قد تناول الخصوصية الهيكلية للجهات المكلفة بمتابعة الجرائم الإلكترونية، فإن هذا المبحث ينزل إلى مستوى أعمق ليتناول الخصوصية الإجرائية المتمثلة في الأساليب التقنية المستحدثة التي منحها المشرع لهذه الجهات. وهذه الأساليب تُمثل القطيعة الأكثر وضوحاً مع منطق الإجراءات الجنائية الكلاسيكية؛ فهي تُجيز صراحةً ما كان يُعدّ انتهاكاً لمبادئ راسخة كمبدأ سرية المراسلات وحرمة الحياة الخاصة، وتُضفي مشروعيةً استثنائيةً على ما كان يُعدّ تجسّساً محظوراً.

إن المشرع حين أباح مراقبة الاتصالات الإلكترونية واعتراض المراسلات الرقمية لم يفعل ذلك استهواءً بالصلاحيات الاستثنائية، بل كاستجابة ضرورية لواقع تقني فرض ذاته بقوة؛ إذ إن جمع الدليل الرقمي في قضايا الإجرام الإلكتروني يستحيل في كثير من الأحيان دون الاستعانة بهذه الأساليب التقنية الاستثنائية. ومن هنا تبرز أهمية الضمانات المصاحبة لهذه الأساليب وضرورة إحاطتها بسياج قضائي يكفل عدم توظيفها خارج نطاقها المشروع. يتناول هذا المبحث في مطلبه الأول آليات المراقبة الإلكترونية واعتراض المراسلات الرقمية، وفي مطلبه الثاني التزامات مقدمي الخدمات ودورهم في دعم التحريات¹.

المطلب الأول: آليات المراقبة الإلكترونية واعتراض المراسلات الرقمية في حينها

الفرع الأول: الشرعية الإجرائية للمراقبة التقنية

أولاً: الأساس الدستوري وإشكالية التوازن

¹ محمد حزيط، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، دار هومة للطباعة والنشر والتوزيع، الجزائر، الطبعة الثانية، 2018، ص 164-175.

قبل الخوض في تفاصيل المراقبة الإلكترونية المُجازة قانوناً، لا بدّ من استحضار الأساس الدستوري الذي ينظم التوتر الجوهرى بين ضرورة المراقبة وحرمة الحياة الخاصة. فقد نصّت المادة 47 من التعديل الدستوري الجزائري لسنة 2020 على أن "سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة، ولا تقيد لممارسة هذا الحق إلا بأمر قضائي محدد المدة وطبقاً للأشكال المنصوص عليها في القانون". وهذا النص الدستوري يُرسي ثلاثة شروط جوهرية لمشروعية أي قيد على سرية المراسلات: أن يصدر بأمر قضائي، وأن يكون محدداً في المدة، وأن يكون وفق الأشكال المنصوص عليها قانوناً. وهي شروط لا يجوز للمشرع العادي أن يتجاوزها مهما كانت حجج الضرورة الأمنية.

ثانياً: نص المادة الثالثة من القانون 04-09 والإطار التشريعي للمراقبة

في إطار هذا التأطير الدستوري، نصّت المادة الثالثة من القانون 04-09 على إمكانية "وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها"، وذلك لمقتضيات حماية النظام العام أو مستلزمات التحريات القضائية الجارية. وعبرة "في حينها" دالة ومحددة، إذ تُشير إلى المراقبة الآنية اللحظية لمحتوى الاتصالات فور حدوثها، وليس الاطلاع اللاحق على بيانات محفوظة مسبقاً، مما يُعطي هذه الأداة قوةً تحريريةً استثنائية لا تستوعبها الإجراءات الكلاسيكية.¹

وتُجيز هذه المادة المراقبة في سياقين: الأول سياق وقائي يتعلق بحماية النظام العام حتى قبل فتح تحقيق قضائي، والثاني سياق إجرائي مرتبط بمستلزمات تحريات قضائية جارية. وهذا التمييز مهم من حيث الضمانات المصاحبة، إذ يرتبط السياق الوقائي بسلطة إدارية ذات طابع أمني بينما يخضع السياق الإجرائي لرقابة قضائية أشد صرامة.

¹ القانون رقم 04-09، المرجع السابق، المادة 3.

ثالثاً: الضمانة الجوهرية: الإذن القضائي المسبق

لضمان ألا تتحول المراقبة الإلكترونية إلى أداة للتجسس الاعتباطي على المواطنين، أحاطها المشرع بضمانة جوهرية تتمثل في الإذن القضائي المسبق. فقد منحت المادة الرابعة من القانون 04-09 النائب العام لدى مجلس قضاء الجزائر صلاحية منح ضباط الهيئة الوطنية إذناً كتابياً ومسبباً للمراقبة، وحددت مدة هذا الإذن بستة أشهر قابلة للتجديد بناءً على تقرير تقني مسبب.¹ وهذا الاشتراط يُجسّد ما أراده الدستور من "أمر قضائي محدد المدة"، ويجعل المراقبة الإلكترونية رهينة دائماً بوجود سلطة قضائية تُراقب تنفيذها وتُقيده بحدود زمنية وموضوعية واضحة.

غير أن التساؤل يبقى مشروعاً حول مدى فعالية هذه الرقابة القضائية في الواقع؛ فالنائب العام يمنح الإذن بناءً على تقرير تقني قدّمه ضباط الهيئة، ومن الناحية العملية قد يكون من العسير عليه تقييم هذا التقرير بصورة نقدية مستقلة تبعاً لمستوى تكوينه التقني. وهو ما يجعل الرقابة القضائية على هذه المرحلة رهينة، إلى حدّ ما، بالثقة في الأجهزة التقنية المقدّمة للتقارير.

الفرع الثاني: الحالات الحصرية للجوء للمراقبة الإلكترونية

أولاً: القائمة الحصرية وأهمية التحديد

أدرك المشرع الجزائري خطورة إطلاق صلاحية المراقبة الإلكترونية دون تحديد الحالات المبررة لها، إذ من شأن الإطلاق أن يُحوّل هذه الأداة الاستثنائية إلى وسيلة مراقبة شاملة لا تستهدف المجرمين وحدهم. لذلك حدّدت المادة الرابعة من القانون 04-09 أربع حالات

¹ القانون رقم 04-09، المرجع السابق، المادة 4.

حصرية لا يجوز اللجوء إلى المراقبة الإلكترونية خارجها، وهذا التحديد الحصري يُجسّد مبدأ التناسب بين الإجراء الاستثنائي ومبرراته الموضوعية.

ثانياً: تفصيل الحالات الحصرية

الحالة الأولى هي الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة. وهذه الحالة الأشد دلالةً على الطابع الاستثنائي للمراقبة، إذ تُجيزها حتى في مرحلة الوقاية قبل وقوع الجريمة متى توافرت مؤشرات على احتمال ارتكابها. والحالة الثانية هي توافر معلومات عن احتمال اعتداء على منظومة معلوماتية يُهدد النظام العام أو الدفاع الوطني أو الاقتصاد الوطني، وهي حالة تكشف عن القلق المشروع من استهداف البنية التحتية الرقمية للدولة. والحالة الثالثة هي مقتضيات التحريات والتحقيقات القضائية الجارية حين يتعذر الوصول إلى نتيجة دون اللجوء إلى المراقبة الإلكترونية، وهذا الاشتراط الأخير يُجسّد معيار الضرورة ويشترط استنفاد الوسائل البديلة قبل اللجوء إلى المراقبة. والحالة الرابعة هي تنفيذ طلبات المساعدة القضائية الدولية المتبادلة، وهي حالة تعكس البُعد الدولي في مكافحة الجريمة الإلكترونية العابرة للحدود.¹

ثالثاً: اعتراض المراسلات السلوكية واللاسلكية بموجب قانون الإجراءات الجزائية

استكمل المشرع المنظومة الإجرائية للمراقبة بموجب القانون رقم 06-22 المعدل لقانون الإجراءات الجزائية، إذ استحدث الفصل الرابع من الباب الثاني من الكتاب الأول بعنوان "اعتراض المراسلات وتسجيل الأصوات والنقاط الصور" ضمن المواد من 65 مكرر إلى 65 مكرر 10. وعرّفت المادة 65 مكرر 5 اعتراض المراسلات بأنه اعتراض أو تسجيل أو نسخ المراسلات التي تتم عبر قنوات أو وسائل الاتصال السلوكية أو اللاسلكية، وأجازت هذا

¹ القانون رقم 09-04، المرجع السابق، المادة 4 الفقرات 1-4.

الإجراء لقاضي التحقيق في جرائم محددة بمدة أقصاها أربعة أشهر قابلة للتجديد مرة واحدة فقط.¹

ولا يفوت الملاحظ الدقيق التمييز بين نظامين إجرائيين متوازيين: نظام المراقبة المقرر في القانون 04-09 المعلق على إذن النائب العام لمدة ستة أشهر، ونظام اعتراض المراسلات المقرر في قانون الإجراءات الجزائية المنوط بقاضي التحقيق بمدة أربعة أشهر فقط. وهذا التوازي التشريعي يُفرز تساؤلاً حول مدى التنسيق بين النظامين وإمكانية الجمع بينهما في القضية الواحدة، وهو ما يستدعي تنظيمًا تشريعيًا أكثر وضوحاً وتماسكاً.

الفرع الثالث: الأثر الجزائي على المساس بالحياة الخاصة

أولاً: عقوبة المراقبة غير المرخصة

لضمان عدم توظيف المراقبة الإلكترونية خارج إطارها القانوني المشروع، حرص المشرع على تجريم المراقبة غير المرخصة والمساس غير المبرر بالحياة الخاصة، وأفضى ذلك إلى تقرير عقوبات رادعة تبال كل من يلجأ إلى هذه الأدوات التقنية الاستثنائية دون الاستناد إلى إذن قضائي مشروع. وقد أكدت المادة الرابعة من القانون 04-09 تحديداً أن المراقبة التي تتم خارج الحالات الحصرية المنصوص عليها والشروط المقررة تُعرض أصحابها لعقوبات المساس بالحياة الخاصة المنصوص عليها في التشريع المعمول به.

ثانياً: إشكالية ضمان الفعلية في التطبيق

يُطرح تساؤل جوهري حول مدى احترام هذه القيود الحصرية في الممارسة الفعلية؛ إذ كثيراً ما تجد الأجهزة الأمنية نفسها في مواجهة ضغط التحقيق والحاجة إلى معلومات عاجلة تدفعها

¹ القانون رقم 06-22، المرجع السابق، المادة 65 مكرر 5.

إلى اللجوء إلى أدوات المراقبة قبل استكمال الإجراءات الشكلية لاستصدار الإذن القضائي. وهو ما يُشكّل مساساً بمبدأ الشرعية الإجرائية التي هي ضمانة دستورية لا يجوز المساس بها بحجة الضرورة الأمنية. ويتكامل هذا الإشكال مع غياب آلية إجرائية واضحة لمراقبة ما تم استخدامه فعلاً من أدوات المراقبة ومدى تطابقه مع نطاق الإذن القضائي الممنوح.

المطلب الثاني: التزامات مقدمي الخدمات وضبط المعطيات المتعلقة بحركة السير

الفرع الأول: إلزامية مساعدة العدالة وكتمان السرية

أولاً: الأساس القانوني لإلزام مقدمي الخدمات

أدرك المشرع الجزائري أن الأجهزة الأمنية والقضائية مهما امتلكت من أدوات تقنية متطورة تظل عاجزة عن الوصول إلى بيانات مخزنة لدى مزودي خدمات الإنترنت والاتصالات دون تعاون هؤلاء الآخرين. ذلك أن الشركات المزودة للخدمات الرقمية تحتفظ بكميات هائلة من البيانات تتعلق بحركة الاتصالات ومحتواها وبيانات المستخدمين، وهي بيانات تُشكّل مادةً أساسية لا غنى عنها في التحريات القضائية المتعلقة بالجرائم الإلكترونية. لذلك أسبغ المشرع على هذا التعاون طابعاً إلزامياً لا اختيارياً.

فقد فرضت المادة العاشرة من القانون 04-09 على مقدمي الخدمات التزاماً قانونياً صريحاً بتقديم المساعدة للسلطات المكلفة بالتحريات لجمع وتسجيل محتوى الاتصالات في حينها، مع الإبقاء على محتوى تلك الاتصالات طبقاً للشروط المقررة. وهذا الالتزام يُحوّل مقدمي الخدمات من كيانات تجارية محايدة إلى شركاء إجرائيين في منظومة مكافحة الجريمة الإلكترونية، وهو تحوّل له دلالاته القانونية والعملية البالغة.¹

¹ القانون رقم 04-09، المرجع السابق، المادة 10.

ثانياً: اشتراط كتمان السرية التامة

بالتوازي مع هذا الالتزام بالتعاون، فرض المشرع على مقدمي الخدمات التزاماً مقابل بكتمان السرية التامة على عمليات المراقبة التي يُساعدون في تنفيذها، وذلك تحت طائلة عقوبات إفشاء أسرار التحقيق. وهذا الاشتراط له وجهان متكاملان: الأول حماية سرية التحريات وضمنان عدم إخطار المشتبه فيهم بأنهم يخضعون للمراقبة، والثاني حماية خصوصية سائر المستخدمين الذين لا يخضعون للتحري ولا مبرر لكشف بياناتهم.

غير أن هذا الالتزام بالسرية يُفرز بدوره إشكالية قانونية دقيقة؛ إذ كيف يُوفَّق بين حق مزود الخدمة في إخطار عملائه بأن بياناتهم شاركها مع الجهات الأمنية، وهو حق قد يُكرّسه قانون حماية البيانات الشخصية، وبين الالتزام بالسرية الذي يفرضه قانون مكافحة الجرائم الإلكترونية؟ هذا التعارض لم يُعالجه المشرع الجزائري بصورة صريحة حتى الآن.

ثالثاً: نطاق الالتزام بالتعاون وحدوده

يمتد التزام مقدمي الخدمات بالتعاون ليشمل توفير البيانات التقنية اللازمة كعناوين IP والبيانات الوصفية لعمليات الاتصال ومعلومات التسجيل لدى الخدمة، فضلاً عن تمكين الأجهزة المختصة من الوصول إلى محتوى الاتصالات في الحالات المرخصة قضائياً. غير أن المشرع لم يُحدد الحد الأدنى والحد الأقصى لهذا التعاون بصورة تفصيلية كافية، مما يفتح باباً للنزاع بين الأجهزة الأمنية ومقدمي الخدمات حول نطاق البيانات الواجب تقديمها وأشكال التعاون المطلوب¹.

¹ عبد الفتاح بيومي حجازي، النظام القانوني لحماية الحكومة الإلكترونية: الكتاب الثاني، الحماية الجنائية والأمنية للمعلومات، دار الفكر الجامعي، الإسكندرية، 2008، ص 472-486.

الفرع الثاني: حفظ بيانات حركة السير والمسؤولية الجزائية

أولاً: الالتزام بالحفظ مدة سنة

تُشكّل بيانات حركة السير (Traffic Data) مادةً تحريريةً ثمينة لا غنى عنها في التحقيق بالجرائم الإلكترونية؛ إذ تُتيح معرفة من اتصل بمن ومتى وكم مدةً وعبر أي وسيلة وانطلاقاً من أي موقع جغرافي، دون الاطلاع على مضمون الاتصال ذاته. لذلك ألزمت المادة الحادية عشرة من القانون 04-09 مقدمي الخدمات ومقدمي خدمة الإنترنت بحفظ المعطيات التي تسمح بالتعرف على المستعملين والاتصالات لمدة سنة واحدة ابتداءً من تاريخ التسجيل.¹

وقد أُنيط بمقدمي الخدمات أيضاً التدخلُ الفوري لسحب أو حجب المحتويات المخالفة للقانون حين يطلب ذلك منهم السلطة القضائية المختصة، مما يُعطيهم دوراً إجرائياً نشطاً في مكافحة المحتوى الرقمي غير المشروع. وهو دور يتجاوز المساعدة السلبية بتقديم المعلومات إلى التدخل الإيجابي في إزالة المحتوى المجرم.

ثانياً: المسؤولية الجزائية عن عرقلة التحريات

حرص المشرع الجزائري على إسناد هذه الالتزامات بمنظومة جزائية رادعة؛ إذ جرّمت المادة الثانية عشرة من القانون 04-09 امتناع مقدمي الخدمات عن التعاون مع السلطات، وقرّرت عقوبة الحبس من ستة أشهر إلى خمس سنوات فضلاً عن الغرامة المالية، وذلك متى أدى هذا الامتناع إلى عرقلة حسن سير التحريات القضائية. وقد جعل المشرع هذه العقوبة

¹ القانون رقم 04-09، المرجع السابق، المادة 11.

مشروطةً بإثبات وجود أثر سلبي على التحريات، وهو اشتراط منطقي يُتجنب به التوسع في التجريم.¹

ثالثاً: إشكاليات تطبيقية في الالتزام بالحفظ

رغم وضوح النص التشريعي القاضي بحفظ البيانات مدة سنة، تبرز في التطبيق إشكاليات عملية لا يمكن إغفالها. فمقدمو الخدمات الأجانب العاملون في الفضاء الرقمي الجزائري، كشركات التواصل الاجتماعي العالمية الكبرى، يرفضون في الغالب الامتثال للأوامر القضائية الجزائرية المطالبة بتقديم بيانات المستخدمين، محتجّين بالتعارض مع قوانين حماية البيانات المعمول بها في دول مقارّها. وهذا الواقع يُفرز فجوةً عملية خطيرة في منظومة مكافحة الجريمة الإلكترونية، إذ تجد الأجهزة الجزائرية نفسها عاجزةً عن الحصول على بيانات مخزنة على خوادم أجنبية رغم وجود قرار قضائي يأمر بذلك.

¹ القانون رقم 09-04، المرجع السابق، المادة 12.

خلاصة الفصل الأول

يُفْضِي استعراض هذا الفصل إلى جملة من الاستنتاجات الجوهرية التي تُلقِي ضوءاً كاشفاً على طبيعة المنظومة الإجرائية الجزائرية في مواجهة الجرائم الإلكترونية وحدود فعاليتها.

على صعيد الإطار المفاهيمي والاختصاصي، اعتمد المشرع الجزائري معياراً مزدوجاً في تحديد وعاء التجريم الرقمي يجمع بين المحل الجرمي ووسيلة الارتكاب، وهو مسلك يُوسّع نطاق الحماية الجنائية ويجعلها قابلةً للتطور مع تجدد الإجرام الرقمي. وعلى صعيد الاختصاص، تجاوز المشرع قيود الإقليمية الكلاسيكية بإرساء مبدأ الامتداد الاختصاصي الاستراتيجي، مما منح المحاكم الجزائرية سلطةً تمتد إلى خارج الإقليم متى تعلق الأمر بالمصالح الجوهرية للدولة.

وعلى صعيد الهياكل المؤسسية، أظهر المشرع وعياً تدريجياً متصاعداً بضرورة التخصص المؤسسي، تجسّد في إنشاء الهيئة الوطنية وتوسيع دورها، وفي إرساء الأقطاب القضائية الجهوية والوطنية التي بلغت ذروتها بالقطب الجزائي الوطني. غير أن ثمة فجوة تظل قائمة بين الكفاءة التقنية لهذه الهياكل والرقابة القضائية الفعلية عليها.

أما على صعيد أساليب التحري الرقمي، فقد استحدث المشرع أدوات استثنائية بالغة الفاعلية كمراقبة الاتصالات وإلزام مقدمي الخدمات بالتعاون والحفظ، وأحاطها بضمانات هامة في مقدمتها الإذن القضائي المسبق والتحديد الحصري للحالات المجيزة للمراقبة. بيد أن التساؤل يظل مشروعاً حول مدى فعالية هذه الضمانات في مواجهة الضغوط الأمنية الميدانية وشح التكوين التقني لدى السلطات القضائية المراقبة، وهو ما يقود تلقائياً إلى استجلاء خصوصية التفتيش والحجز في البيئة الرقمية وضمانات الشرعية الإجرائية في الفصل الثاني.

الفصل الثاني:

خصوصية المعاينة الرقمية وضمانات الشرعية الإجرائية

إذا كان الفصل الأول قد أرسى الأطر التشريعية والموضوعية للجرائم المتصلة بتكنولوجيا الإعلام والاتصال في المنظومة القانونية الجزائرية، فإن الفصل الثاني ينتقل إلى ما هو أكثر دقة وحساسية في آنٍ واحد؛ ذلك الإطار الإجرائي الذي يُحكم التوازن الصعب بين متطلبات الكشف عن الجريمة الإلكترونية وصون الحقوق الدستورية المكفولة للأفراد. فالبينة الرقمية بما تنطوي عليه من خصائص تقنية فريدة كاللامادية والسرعة الفائقة في الانتشار والتعقيد التشفيري وعبور الحدود الوطنية، جعلت أدوات التحري والإثبات التقليدية عاجزةً بمفردها عن مواجهة هذا النوع من الإجرام. وفي مواجهة هذا التحدي المزدوج، لم يكتفِ المشرع الجزائري بتكثيف الآليات القائمة، بل منح المحققين صلاحيات واسعة النطاق في التفتيش الرقمي والحجز الإلكتروني ومراقبة الاتصالات، وهي صلاحيات تفرض بالمقابل ضرورة وضع ضوابط صارمة تحمي الفرد من التعسف الرقمي وتضمن مبدأ الشرعية الإجرائية الذي لا يقبل المساومة.

ومن هنا تنبثق إشكالية هذا الفصل في صورتها الجوهرية: كيف وازن المشرع الجزائري بين منح سلطات التحقيق الأدوات الإجرائية اللازمة للكشف الفعال عن الجرائم الإلكترونية من جهة، وصون الحرية الشخصية وحرمة الحياة الخاصة والضمانات الدستورية من التوظيف التعسفي لهذه الأدوات من جهة ثانية؟

ولمعالجة هذه الإشكالية، يُقسّم هذا الفصل إلى مبحثين متكاملين: يُعالج المبحث الأول خصوصية التفتيش والحجز في البيئة الرقمية، بما يستلزمه ذلك من بيان الأحكام الاستثنائية التي استحدثها القانون رقم 09-04 وما ترتب عليها من آليات إجرائية متميزة. في حين يُكرّس المبحث الثاني لبيان حجية الدليل الرقمي وضوابط حماية الحريات الفردية، بما في ذلك القيود المفروضة على استعمال المعلومات المتحصل عليها وشروط التعاون الدولي والجزاءات الإجرائية المترتبة على انتهاك الشرعية.

المبحث الأول: خصوصية التفتيش والحجز في البيئة الرقمية

يُشكّل التفتيش والحجز في الجرائم الإلكترونية إشكاليةً إجرائيةً بالغة الأهمية، ليس فحسب لأنها يمسّان حقوقاً دستورية راسخة كحرمة المسكن وسرية الاتصالات وحماية البيانات الشخصية، بل أيضاً لأن ميدان تطبيقهما تحوّل جذرياً. فالتفتيش في الجرائم التقليدية ينصبّ على أماكن مادية محددة يمكن ضبطها جغرافياً، وعلى أشياء مادية يمكن حيازتها ونقلها والاحتفاظ بها. أما في البيئة الرقمية، فإن مسرح الجريمة لا جدران له ولا حدود مرئية؛ إنه شبكة من الأنظمة المترابطة والبيانات المخزنة في فضاء افتراضي قد يمتد عبر قارات. وعليه، فإن التفتيش الإلكتروني والحجز الرقمي يتطلبان أحكاماً استثنائية لم يعرفها القانون الكلاسيكي،¹ وهو ما تنبّه إليه المشرع الجزائري بالنص عليها في إطار القانون رقم 09-04 المؤرخ في 05 أغسطس 2009.

وفي هذا المبحث، نعالج في مطلب أول الأحكام الاستثنائية لتفتيش المنظومات المعلوماتية والشبكات، ثم ننتقل في مطلب ثانٍ إلى آليات الحجز الرقمي للبيانات ومنع الوصول إليها.

المطلب الأول: الأحكام الاستثنائية لتفتيش المنظومات المعلوماتية والشبكات

تبرز خصوصية التفتيش الرقمي بوضوح حين نستحضر مقارنةً دقيقة مع نظيره التقليدي؛ ففي التفتيش المادي تكون الحدود الجغرافية للعملية محددةً سلفاً بما يضمن ضبطها رقابياً. أما في التفتيش الرقمي، فإن الأدلة المطلوبة قد تكون مبعثرةً على أنظمة متعددة ومتصلة ببعضها البعض، ومن ثمة فإن التفتيش في منظومة واحدة قد يقود حتماً وتلقائياً إلى منظومات أخرى. هذا الواقع التقني هو ما استوجب من المشرع استحداث أحكام استثنائية

¹ عبد الفتاح بيومي حجازي، الدليل الجنائي الرقمي وجرائم الإنترنت، دار الفكر الجامعي، الإسكندرية، 2007، ص

تنظّم هذا النوع المستحدث من الإجراءات، محتفظةً في الوقت ذاته بالضمانات الجوهرية اللازمة لمنع التعسف.

الفرع الأول: التفتيش الافتراضي ولو عن بعد

أولاً: النص التشريعي وسياقه

أجازت المادة الخامسة الفقرة (أ) من القانون رقم 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها للسلطات القضائية وضباط الشرطة القضائية أن يدخلوا، بغرض التفتيش، إلى منظومة معلوماتية أو جزء منها، وكذا إلى المعطيات المخزنة فيها. والجديد البارز في هذا النص أنه أجاز ذلك "ولو عن بعد"، أي أن التفتيش لا يشترط الحضور الجسدي في مكان الجهاز محل التفتيش، بل يمكن أن يتم عبر الشبكة وعن طريق الاتصال عن بُعد بالمنظومة المستهدفة.¹

ثانياً: المبرر القانوني والتقني

لم تأت هذه الإجازة من فراغ؛ إذ تفرضها بالضرورة طبيعة البيئة الرقمية التي تتسم بالتوزع والتشبيك. فالمجرم الإلكتروني نادراً ما يخزّن معطياته على جهاز واحد في مكان واحد؛ بل يوزّعها على خوادم متعددة وقد تكون موزّعة بين دول مختلفة. ومن ثمة فإن اشتراط الحضور الجسدي التقليدي كان سيفرغ إجراء التفتيش من مضمونه ويُعيق الكشف عن الجريمة. وقد أشار الفقيه الجزائري سليمان بارش إلى أن القانون رقم 04-09 جاء بمقاربة جديدة تركز

¹ القانون رقم 04-09 المؤرخ في 05 أغسطس 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، الصادرة بتاريخ 16 أغسطس 2009، المادة 5.

على "التكيف مع الواقع التقني للجريمة الإلكترونية بدلاً من محاولة إخضاعها إكراهاً لإجراءات صيغت لواقع مغاير".¹

ثالثاً: الإشكاليات التي يُثيرها التفتيش عن بُعد

بيد أن التفتيش عن بُعد يُثير في المقابل جملةً من الإشكاليات القانونية الدقيقة. أولها إشكالية الاختصاص الإقليمي؛ فإذا كانت المنظومة المُفتَّشة عن بُعد مستضافةً على خادم في دولة أجنبية، هل يملك الضابط الجزائري ولاية قانونية للتفتيش فيها؟ وهذا ما سيأتي الجواب عنه في سياق معالجة التعاون القضائي الدولي. وثانيها إشكالية توثيق الدليل المستخرج عن بُعد وإثبات عدم التلاعب به خلال عملية النقل الشبكي، وهو ما يستدعي تقنيات تشفير وتجزئة متطورة تضمن سلامة البيانات. وثالثها إشكالية أن التفتيش عن بُعد لا يترك أثراً مادياً ملموساً، مما يجعل رقابة القضاء عليه أكثر صعوبةً من التفتيش التقليدي، وهو ما يدفع إلى التشديد في اشتراط الإذن القضائي المسبق والمسبب.²

الفرع الثاني: تمديد التفتيش السريع وتسخير ذوي الدراية

أولاً: آلية تمديد التفتيش السريع

أقرّت المادة الخامسة الفقرة الثانية من القانون رقم 09-04 آليةً فريدةً من نوعها في المنظومة الإجرائية الجزائرية، وهي ما يمكن تسميته بـ"تمديد التفتيش السريع". وتقوم هذه الآلية على أنه إذا تبين لضابط الشرطة القضائية أثناء تفتيشه لمنظومة معلوماتية أن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى يمكن الوصول إليها بصفة

¹ سليمان بارش، شرح قانون الإجراءات الجزائية الجزائري، دار الهدى، عين مليلة، الجزائر، الطبعة الرابعة، 2013، ص 342.

² عمر زودة، الاختصاص القضائي في الجرائم المعلوماتية، مجلة الحقوق والعلوم السياسية، جامعة خنشلة، العدد 12، 2020، ص 87.

مشروعة من المنظومة الأولى، جاز له تمديد التفتيش بسرعة إلى تلك المنظومة الثانية، بشرط إعلام السلطة القضائية المختصة بذلك مسبقاً.¹

والمسوّغ التقني لهذه الآلية واضح؛ إذ كثيراً ما تكون منظومات الكمبيوتر في المؤسسات أو الشبكات الخاصة مترابطة بحيث يُتيح الدخول إلى إحداها الوصول إلى الأخرى. وفي غياب هذه الآلية، كان المحقق مضطراً للتوقف عند حدود المنظومة الأولى وانتظار إذن جديد للمنظومة الثانية، وهو ما قد يُتيح الفرصة للجنة لمسح الأدلة أو إتلافها عن بُعد. وقد وازن المشرع بين متطلبات الفعالية واعتبارات الضمان بأن جعل التمديد مشروطاً بالإعلام المسبق للسلطة القضائية، لا بانتظار الإذن، مما يُبقي على الرقابة دون أن يُعيق التدخل السريع.

ثانياً: التمييز بين الإعلام المسبق والإذن المسبق

يُلاحظ أن المشرع اشترط "الإعلام المسبق" لا "الإذن المسبق"، وهو تمييز ذو أهمية إجرائية بالغة. فالإعلام المسبق يعني أن ضابط الشرطة القضائية يُبادر إلى التمديد ويُخطر السلطة القضائية في الوقت ذاته أو قبله مباشرة، دون أن ينتظر موافقتها. في حين أن الإذن المسبق كان سيعني ضرورة الانتظار حتى يصدر القرار القضائي، مما قد يُضيع الدليل. غير أن هذا الاختيار التشريعي لا يعني إطلاق يد ضابط الشرطة القضائية بلا قيد؛ فالسلطة القضائية المُعلّمة تملك الحق في إيقاف التمديد أو وضع قيود عليه أو ترتيب بطلان الإجراء إذا ثبت تجاوزه الغرض المحدد.²

ثالثاً: تسخير ذوي الدراية الفنية

¹ القانون رقم 09-04، المادة 5 الفقرة 2، المرجع السابق.

² بشير سعد زغلول، النظرية العامة للإثبات الجنائي في الجرائم المعلوماتية، مجلة المفكر، جامعة محمد خيضر بسكرة، العدد 18، 2018، ص 112.

نصّت المادة الخامسة الفقرة الرابعة من القانون ذاته على منح ضابط الشرطة القضائية سلطة تسخير أي شخص لديه دراية فنية بآلية عمل المنظومة المعلوماتية أو بتقنيات فك التشفير المطبقة عليها، لتقديم المساعدة التقنية اللازمة لاستخراج البيانات وإنجاز عملية التفتيش. وتبرز أهمية هذا الحكم في مواجهة ما بات يُعرف بـ"التشفير الكامل (Full Encryption)" الذي أصبح سمةً شائعةً في الأجهزة الإلكترونية، مما يجعل محتوياتها غير مقروء دون مفتاح التشفير. وقد تناول هذه المسألة الباحث زواوي محند آكلي بالتحليل في سياق دراسته للإجراءات الجزائية في مواجهة الجريمة المعلوماتية.¹

رابعاً: الإشكالية الدستورية المتعلقة بتسخير المتهم

تُقرز آلية تسخير ذوي الدراية إشكاليةً دستوريةً بالغة الحساسية حين يكون المُسَخَّر هو المتهم ذاته؛ إذ قد يكون الجاني هو الوحيد الذي يعرف مفتاح تشفير جهازه. وفي هذه الحالة، فإن إجباره على الإفصاح عن هذا المفتاح يُشكّل إكراهاً على تجريم ذاته، وهو ما يتعارض مع الحق في الصمت وقرينة البراءة المكرّستين في الدستور الجزائري لعام 2020 وفي قانون الإجراءات الجزائية المعدّل بالقانون رقم 14-25. وقد ظلّ المشرع الجزائري صامتاً حتى الآن حيال هذه الإشكالية دون أن يُقدم حسمًا تشريعيًا واضحاً، في حين أن المقارنة تكشف عن نقاشات فقهية وقضائية حادة في هذا الصدد؛ ففي فرنسا ذهب المجلس الدستوري إلى جواز إلزام الشخص بتسليم مفتاح التشفير شريطة ألا يكون ذلك دليلاً مباشراً على إدانته، في حين اعتبر بعض الفقه الأنجلوساكسوني ذلك انتهاكاً صريحاً لحق عدم تجريم النفس المكرّس في التعديل الخامس للدستور الأمريكي.²

¹ زواوي محند آكلي، الإجراءات الجزائية في مواجهة الجريمة المعلوماتية في الجزائر، مذكرة ماجستير، كلية الحقوق،

جامعة مولود معمري تيزي وزو، 2012، ص 78.

² عبد العزيز سعد، الإجراءات الجزائية في التشريع الجزائري، ديوان المطبوعات الجامعية، الجزائر، الطبعة الثانية، 2019، ص 198.

المطلب الثاني: الحجز الرقمي للبيانات وآليات منع الوصول إليها

يُمثل الحجز في الجرائم الإلكترونية أحد أكثر الإجراءات إبداعاً في المنظومة الإجرائية الجزائرية؛ إذ أقرز القانون رقم 04-09 شكلاً جديداً من الحجز لم يعرفه التشريع التقليدي، وهو الحجز بالنسخ أو ما يُعرف بـ"الحجز المعنوي" الذي ينصبّ على البيانات لا على الدعامة المادية. كما استحدثت آليات لمنع الوصول إلى البيانات غير المشروعة بصرف النظر عن مكان تخزينها.

الفرع الأول: الحجز بالنسخ وتشكيل الأحرار المعنوية

أولاً: آلية الحجز بالنسخ

جاءت المادة السادسة من القانون رقم 04-09 بحكم استثنائي ذي طابع تقني، إذ نصّت على أنه إذا اكتشف المحقق بيانات إلكترونية مفيدة للكشف عن الجريمة ولم يكن من الضروري حجز الجهاز كاملاً، يُجرى نسخ المعطيات الإلكترونية وتوضع في أحرار، مع التزام المحقق فنياً بالسهر على سلامة المعطيات وعدم المساس بمحتواها الأصلي.¹ وهذا الحكم يكرّس مبدأً إجرائياً مستحدثاً يمكن تسميته بـ"الفصل بين الدليل ودعامته"، بمعنى أن المشرع قبل بأن يكون الحجز وارداً على البيانات ذاتها دون الاستيلاء على الجهاز المادي الذي تحويها.

ثانياً: المبررات العملية للحجز بالنسخ

لهذا الخيار التشريعي مبرراته العملية الوجيهة؛ إذ إن حجز الأجهزة الإلكترونية بالكامل في المؤسسات أو الشركات قد يُسبّب أضراراً جسيمة لأصحابها الذين لا علاقة لهم بالجريمة

¹ القانون رقم 04-09، المادة 6، المرجع السابق.

المحقق فيها. فإذا أُغلقت شركة ذات استخدام قانوني لأن أحد أجهزتها يحتوي على دليل إلكتروني، كان في ذلك ضرر غير مبرر بحقوق أطراف ثالثة. والحجز بالنسخ يُحقق الغرض الإجرائي ذاته بالاستحواذ على الدليل دون إلحاق هذا الضرر. وهو ما أشار إليه الفقيه الفرنسي Mikaël Benillouche في دراسته المقارنة لإجراءات الحجز الإلكتروني حين قرّر أن "الأثر الجانبي للحجز الرقمي على الأطراف البريئة يُشكّل أحد أبرز التحديات التي تواجه التشريعات الإجرائية الحديثة".¹

ثالثاً: الضمانات التقنية لسلامة النسخة المحجوزة

التزام المحقق بـ"السهر على سلامة المعطيات وعدم المساس بمحتواها الأصلي" يُفضي من الناحية التقنية إلى اشتراط جملة من الممارسات المهنية المتعارف عليها في علم الجريمة الرقمية الشرعية: (Digital Forensics) أولها استخدام موانع الكتابة (Write Blockers) التي تحول دون أي تعديل على البيانات الأصلية أثناء النسخ. وثانيها إنشاء نسخة طبق الأصل على المستوى الثنائي (Bit-by-Bit Image) تكون مطابقة تماماً للأصل. وثالثها توليد القيمة التجزئية (Hash Value) للبيانات قبل النسخ وبعده، لإثبات عدم حدوث أي تعديل. ورابعها توثيق كامل مراحل عملية النسخ في محضر تقني مفصّل يتضمن هوية كل شخص تعامل مع الدليل، وهو ما يُعرف بسلسلة الحفظ (Chain of Custody).²

¹ Mikaël Benillouche, *La saisie de données informatiques en droit français: problèmes et perspectives*, Revue de Science Criminelle et de Droit Pénal Comparé, n° 2, 2011, p. 267.

² نبيل صقر، الدليل العملي للبحث والتحري في الجرائم المعلوماتية، دار الهدى، عين مليلة، الجزائر، 2014، ص 134.

الفرع الثاني: الحجز التقني لمنع الوصول إلى البيانات غير المشروعة

أولاً: آليات منع الوصول عند استحالة النسخ

أضافت المادة السابعة من القانون رقم 04-09 حكماً تكميلياً يُعالج الحالات التي يتعذر فيها نسخ البيانات لأسباب تقنية كالتشفير القوي أو ضخامة الحجم أو الحماية التقنية المعقدة؛ إذ أجازت في هذه الحالات استعمال التقنيات المناسبة لمنع الوصول إلى تلك البيانات. وهذا الإجراء يُشكّل في حقيقته شكلاً من أشكال "الحجز السلبي" الذي لا يستولي فيه المحقق على البيانات لكنه يمنع الآخرين من الوصول إليها، وهو ما يُوفّر حمايةً للدليل الرقمي ريثما تُرفع العوائق التقنية التي تحول دون الاستحواذ عليه.

ثانياً: المصادرة التقنية الآنية للمحتوى المجرّم

ذهب المشرع في المادة الثامنة من القانون رقم 04-09 إلى أبعد من ذلك بشأن المعطيات ذات المحتوى المجرّم قانوناً؛ إذ منح السلطة الحق في اتخاذ إجراءات تقنية فورية تُمنع بموجبها الاطلاع على تلك البيانات كلياً. وهذا الحكم يُجسّد ما يمكن وصفه بـ"المصادرة التقنية المعاصرة" التي تُنجز آنياً عبر التقنيات المعلوماتية، كحجب المواقع الإلكترونية التي تحتوي على محتوى يُشكّل جريمة وفقاً للقانون 04-09. وهذا الإجراء يُثير بدوره تساؤلات جدية حول مدى الرقابة القضائية عليه ومدى احترامه لمبدأ التناسب بين الإجراء والغرض منه؛ إذ قد تؤدي المصادرة التقنية الفورية إلى إخفاء دليل يمكن أن يكون نافعاً للدفاع، وهو ما يستدعي أن يُحاط بضمانات قضائية واضحة.¹

¹ القانون رقم 04-09، المادتان 7 و8، المرجع السابق.

ثالثاً: إلزام مقدمي الخدمات بالتعاون

ولضمان فعالية آليات الحجز والمنع على شبكة الإنترنت، أقرت المادة السادسة من القانون رقم 04-09 التزاماً صريحاً على مقدمي خدمات الإنترنت والمنصات الرقمية بالتعاون مع السلطات القضائية وتمكينها من البيانات اللازمة للتحقيق. وقد تعزز هذا الالتزام بصدور المرسوم التنفيذي رقم 97-09 المؤرخ في 22 فيفري 2009 الذي نظم شروط الاعتماد والتشغيل لمقدمي خدمات الإنترنت وحدد التزاماتهم في مجال حفظ السجلات والتعاون مع السلطات.¹ ويبقى في هذا الإطار تساؤل جوهري حول وضع مقدمي الخدمات الأجانب كشركات جوجل وميتا ومايكروسوفت التي تستضيف كميات هائلة من البيانات ذات الصلة بالجرائم الإلكترونية الجزائرية، ولا تخضع بالضرورة للقانون الجزائري ولا تلتزم بالاستجابة لطلباته مباشرةً دون المرور بقنوات التعاون القضائي الدولي.

¹ المرسوم التنفيذي رقم 97-09 المؤرخ في 22 فبراير 2009 المحدد لشروط وكيفيات منح الاعتماد للمتعاملين الذين يقدمون خدمات الاتصالات الإلكترونية عبر الأنترنت وعبر شبكة الاتصالات الراديوية، الجريدة الرسمية للجمهورية الجزائرية، العدد 14، 2009.

المبحث الثاني: حجية الدليل الرقمي وضوابط حماية الحريات الفردية

إذا كان المبحث الأول قد انصبَّ على الجانب الإجرائي التقني للتفتيش والحجز، فإن هذا المبحث ينتقل إلى المستوى الأعمق والأكثر حساسيةً، وهو إشكالية القيمة الإثباتية للدليل الرقمي أمام القضاء الجزائي، والضوابط التي وضعها المشرع لحماية الحريات الفردية من التوظيف التعسفي للتحقيقات الرقمية. وهنا يظهر التوترُ الجوهرى في صميم السياسة الجنائية الإجرائية؛ فمن جهة يُريد المشرع أن يجعل الدليل الرقمي أداةً فعّالةً في كشف الجريمة الإلكترونية وإدانة مرتكبيها، ومن جهة أخرى يُدرك أن الاعتراف بهذا الدليل بلا قيود قد يُفضي إلى مخاطر جسيمة تمسّ الحقوق الدستورية المكفولة للأفراد.

يُعالج هذا المبحث في مطلب أول القيمة الإثباتية للدليل الرقمي وحدود استعماله، ثم في مطلب ثانٍ ضوابط التعاون الدولي والجزاءات الإجرائية المترتبة على انتهاك الشرعية.

المطلب الأول: القيمة الإثباتية للدليل الرقمي وحدود استعماله

تُعَدُّ مسألة القيمة الإثباتية للدليل الرقمي إحدى أبرز المعضلات التي يواجهها قضاء الموضوع في عصر التقنية؛ فهذا الدليل يجمع بين ثنائية من التناقض الظاهر: من جهة يتمتع بدقة تقنية لا تُضاهيها أدلة أخرى كثيرة حين يُجمع بالأساليب العلمية الصحيحة، ومن جهة أخرى يُشكّل سهولة تعديله وتزويره دون ترك أثر ظاهر تحدياً جوهرياً لقناعة القاضي.

الفرع الأول: حجية الدليل الرقمي في المنظومة القانونية الجزائرية

أولاً: المسار التشريعي للاعتراف بالدليل الرقمي

لم يعرف التشريع الجزائري الاعتراف الصريح بحجية الدليل الرقمي إلا بصورة تدريجية؛ فقد خطا القانون المدني خطوته الأولى بموجب المادة 323 مكرر من القانون المدني المستحدثة

بالقانون رقم 05-10 التي أقرت بالكتابة الإلكترونية وسيلةً للإثبات. ثم جاء القانون رقم 09-04 ليُرسي في المادة الثامنة عشرة منه مبدأ التكافؤ بين المحررات الإلكترونية والمحررات الورقية في الحجية، إذ نصّت صراحةً على أن "المحررات المتحصل عليها من منظومة معلوماتية لها نفس القوة الثبوتية المخولة للمحررات المكتوبة". وقد عزّز هذا التوجه قانون الإجراءات الجزائية المعدّل بموجب الأمر رقم 21-11 الذي أكدّ صراحةً قبول الدليل الرقمي وسيلةً للإثبات الجنائي.¹

ثانياً: الدليل الرقمي بوصفه خاضعاً للسلطة التقديرية للقاضي

يُقرر الفقه والقانون الجزائري أن الدليل الرقمي لا يرتب قناعةً مطلقةً لدى القاضي ولا يلزمه بنتيجة محددة، بل يخضع لسلطته التقديرية في تقييمه شأنه شأن سائر الأدلة. وهذا الموقف يُجسّد الانحياز المبدئي للنظام الجزائري نحو الاقتناع القضائي الحر بوصفه الأساس في الإثبات الجنائي، وهو ما يُعبّر عنه الفقه الفرنسي بمبدأ "la liberté de la preuve" الذي أخذ به المشرع الجزائري. بيد أن هذا التقدير الحر لا يعني التقدير التعسفي؛ فثمة معايير موضوعية تحكم تقييم الدليل الرقمي ينبغي مراعاتها، في مقدمتها صحة الحصول عليه وسلامته التقنية وثبوت صلته بالواقعة المحقّق فيها.²

ثالثاً: السياق الحمائي للدليل الرقمي المتعلق بالبيانات الشخصية

أحاط المشرع الجزائري الدليل الرقمي المتعلق بالبيانات الشخصية بسياج من السرية، وذلك تطبيقاً لأحكام القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة

¹ القانون رقم 09-04، المادة 18، المرجع السابق؛ الأمر رقم 21-11 المؤرخ في 25 أغسطس 2021 المتضمن تعديل وتتميم الأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية، العدد 65، 2021.

² عبد الرحمن خلفي، قانون الإجراءات الجزائية في ضوء الممارسة القضائية، مكتبة الرشاد، الجزائر، 2018، ص 223.

البيانات ذات الطابع الشخصي. فليس كل بيان رقمي يُستخرج من جهاز يصلح دليلاً في الإثبات؛ فالبيانات الصحية والسياسية والدينية والجنسية تتمتع بحماية مشددة لا تُتاح إلا في الحدود الضيقة التي يقرها القانون، مع اشتراط الإذن القضائي المسبق.¹

الفرع الثاني: تقييد الاستعمال الشخصي للمعلومات المتحصل عليها

أولاً: النص التشريعي وأثره

وضعت المادة التاسعة من القانون رقم 04-09 قيداً صارماً بعبارة قاطعة لا تحتمل التأويل، مفادها أنه تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، لا يجوز استعمال المعلومات المتحصل عليها عبر عمليات المراقبة إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية.² وهذا النص يُجسّد تطبيقاً مبدأ التخصيص الإجرائي؛ أي أن كل دليل يُجمع لغرض إجرائي محدد لا يجوز توظيفه في غير هذا الغرض. فالمعلومات التي تجمعها الشرطة خلال تحرياتها في جريمة إلكترونية معينة لا يجوز توظيفها في متابعة صاحبها على أفعال أخرى لا صلة لها بالتحقيق الجاري، وذلك حماية من خطر الرقابة الشاملة التي قد تُحوّل أدوات التحري الجنائي إلى أدوات مراقبة شاملة للأفراد.

ثانياً: التكامل مع الضمانات الدستورية

تتكامل هذه القيود مع المنظومة الضامنة التي يوفرها الدستور الجزائري لعام 2020 وقانون الإجراءات الجزائية المعدّل بالقانون رقم 14-25. فمبدأ قرينة البراءة المكرّس في المادة 37 من الدستور يُفرض احتراماً مشدداً في سياق الأدلة الرقمية؛ إذ لا يجوز أن يُعكّس هذا المبدأ

¹ القانون رقم 07-18 المؤرخ في 10 يونيو 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات

ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية، العدد 34، 2018.

² القانون رقم 04-09، المادة 9، المرجع السابق.

بجعل الفرد مُلزماً بإثبات براءته مما ظهر في تاريخ تصفّحه أو مراسلاته الرقمية. كما يقتضي حق الدفاع المكفول في المادة 37 مكرر من الدستور منح المتهم ومحاميه إمكانية الطعن في الدليل الرقمي والتحقق من صحة شروط الحصول عليه والنقاش في قيمته التقنية.¹

ثالثاً: تقييم الإطار الحمائي

يبدو الإطار الحمائي الذي رسمه القانون 09-04 ومعه الدستور وقانون الإجراءات الجزائية متكاملًا من الناحية النصية، غير أن التحدي الحقيقي يكمن في التطبيق. إذ تكشف الممارسة القضائية عن فجوة واسعة بين النص ومقتضياته والتطبيق الفعلي؛ فالقضاة لا يملكون في الغالب الخلفية التقنية التي تُمكنهم من التحقق الفعلي من شروط صحة الدليل الرقمي، وكثيراً ما يكتفون بما يُقدّمه خبير الجهة القضائية دون تقييم نقدي حقيقي. وهذا ما أفضى إلى وضع دقيق يشترك فيه الدور الفعلي لقاضي الموضوع مع الخبير التقني بشكل يُثير تساؤلات جدية حول مدى الاستقلالية الفعلية للسلطة القضائية في تقييم الدليل الرقمي.²

المطلب الثاني: ضوابط التعاون الدولي وبطلان الإجراءات المخالفة للشرعية

تتجاوز الجريمة الإلكترونية بطبيعتها التكنولوجية حدود الإقليم الوطني، مما يجعل مبدأ السيادة الإقليمية التقليدي في الإجراءات الجزائية عاجزاً عن مواجهتها منفرداً. وقد أفرز هذا الواقع التقني ضرورة التعاون الدولي، غير أن هذا التعاون يُثير بدوره تساؤلات دقيقة حول حدوده وضوابطه وما يترتب على تجاوزه من بطلان إجرائي.

¹ الدستور الجزائري المعدّل لعام 2020، المادتان 37 و37 مكرر؛ القانون العضوي رقم 14-25 المؤرخ في 25 ديسمبر 2014 المتضمن تعديل وتتميم الأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية، العدد 74، 2014.

² جلول شيتور، مبادئ الإجراءات الجزائية في القانون الجزائري، ديوان المطبوعات الجامعية، الجزائر، الطبعة الثالثة، 2016، ص 315.

الفرع الأول: آليات التعاون الدولي في إطار القانون 04-09

أولاً: الإطار التشريعي للتعاون الدولي

رسمت المادة الخامسة الفقرة الثالثة من القانون رقم 04-09 حدود التفتيش الدولي بوضوح تام؛ إذ حظرت الحصول على البيانات المخزنة خارج الإقليم الوطني بصورة مباشرة، وأُجِبت اتباع مسار التعاون الدولي المنظم وفق الاتفاقيات الدولية ومبدأ المعاملة بالمثل. وقد جاءت المادتان 16 و17 من القانون ذاته لتسهّل قبول طلبات المساعدة المتبادلة المستعجلة لجمع الأدلة الإلكترونية، بما فيها إمكانية تبادل الطلبات عبر وسائل الاتصال السريعة كالبريد الإلكتروني، شريطة توافر الضمانات الأمنية التقنية الكافية للتحقق من هوية مُرسل الطلب وصحة مضمونه.¹

ثانياً: الموقف من الاتفاقيات الدولية للجريمة السيبرانية

يُلاحظ أن الجزائر لم تنضم بعد إلى اتفاقية بودابست للجريمة السيبرانية لعام 2001 التي تُمثّل الإطار المرجعي الدولي الأبرز في هذا الميدان بعضوية تتجاوز ستين دولة. كما أن اتفاقية مالابو الأفريقية للأمن السيبراني لعام 2014 التي وقّعها الجزائر لم تصادق عليها بعد، مما يُبقيها خارج آليات التعاون المُسرّعة التي تُتيحها هذه الاتفاقية. ويترتب على ذلك أن التعاون الدولي الجزائري في مجال الجريمة الإلكترونية يسير عبر المسارات الثنائية التقليدية وهي مسارات بالغة البطء مقارنةً بسرعة الجريمة الإلكترونية ذاتها وسهولة إتلاف أدلتها.²

¹ القانون رقم 04-09، المواد 5 الفقرة 3، 16 و17، المرجع السابق.

² Sofiane Dobbi et Souria Yessad, *Les infractions liées aux technologies de l'information et de la communication en droit algérien*, Revue Algérienne des Sciences Juridiques, Politiques et Économiques, Vol. 57, n°3, 2020, p. 412.

ثالثاً: إشكالية الوصول المباشر إلى البيانات المخزنة في الخارج

يبرز في هذا السياق تحدّي إجرائي عملي بالغ الدقة، وهو ما يُعرّف بـ"الوصول الانفرادي عبر الحدود (Unilateral Transborder Access)"; أي قيام سلطات دولة ما بالوصول إلى بيانات مخزنة على خوادم في دولة أجنبية دون الحصول على موافقة هذه الدولة. ويُقسّم القانون 04-09 هذه الحالة إلى صورتين: الأولى مسموح بها وهي الوصول إلى البيانات المتاحة للعموم بصرف النظر عن مكان تخزينها. والثانية محظورة وهي الوصول غير المأذون إلى البيانات غير العامة دون الحصول على إذن الدولة المضيفة أو إذن قضائي جزائري مسبق، وما تحمله هذه الصورة من مساس بالسيادة الوطنية للدولة الأجنبية.¹

الفرع الثاني: البطلان الإجرائي جزاءً على انتهاك الشرعية الرقمية

أولاً: الحد الإجرائي الفاصل في المادة 18 من القانون 04-09

وضعت المادة الثامنة عشرة من القانون رقم 04-09 خطأً أحمر صريحاً في مواجهة الإجراءات المخالفة للسيادة الوطنية أو النظام العام؛ إذ رتّبت صراحةً رفض تنفيذ طلبات المساعدة الدولية التي يكون من شأنها المساس بالسيادة الوطنية أو النظام العام. وقد ارتبط هذا الحكم بالقواعد الصارمة لقانون الإجراءات الجزائية المعدّل بالقانون رقم 14-25 لتُفرز معاً منظومة واضحة للبطلان الإجرائي.²

ثانياً: شروط صحة الإجراء الرقمي تحت طائلة البطلان

يستخلص من الربط بين نصوص القانون رقم 04-09 والقانون رقم 14-25 أن صحة الإجراء الرقمي تستلزم توافر أربعة شروط جوهرية، يُفضي انتفاء أي منها إلى البطلان:

¹ القانون رقم 04-09، المادة 5 الفقرة 3، المرجع السابق.

² القانون رقم 04-09، المادة 18؛ القانون العضوي رقم 14-25، المرجع السابق.

الشرط الأول هو الإذن القضائي الكتابي المسبق والمسبب، إذ لا يُقبل شفهيّاً ولا لاحقاً بعد انجاز الإجراء. والشرط الثاني هو أن تتوافق حدود الإجراء مع الغرض الذي أُذن فيه؛ فالإذن بتفتيش بريد إلكتروني لا يُجيز تمديده إلى ملفات على القرص الصلب. والشرط الثالث هو صون حرمة الحياة الخاصة بأن لا يتجاوز الإجراء ما هو ضروري لأغراض التحري. والشرط الرابع هو احترام إجراءات التوثيق التقني والحفاظ على سلامة الدليل. وانتفاء أي من هذه الشروط يُفضي إلى بطلان الدليل الرقمي المستمدّ وما تفرّع عنه من إجراءات.¹

ثالثاً: طبيعة البطلان: المطلق أم النسبي؟

تُثير الإشكالية التشريعية المتعلقة بطبيعة البطلان الإجرائي نقاشاً فقهيّاً جوهريّاً؛ فالبطلان المطلق يسري بقوة القانون بصرف النظر عن تمسك الخصوم به ولو لم يدفع به أحد، في حين أن البطلان النسبي لا يُعمل به إلا بطلبٍ من الخصم المتضرر. والراجح في الفقه الجزائري أن بطلان الإجراء الرقمي الواقع في مخالفة صريحة لاشتراط الإذن القضائي هو بطلان مطلق من حيث إنه يمس النظام العام الإجرائي في جوهره ويتعلق بمبادئ دستورية راسخة، وهو ما يعني أن القاضي يملك الحكم به من تلقاء نفسه دون أن ينتظر دفْعاً من أطراف الخصومة. وقد ذهب الأستاذ عبد الرحمن خلفي إلى أن "البطلان المرتبط بالحقوق الدستورية المكفولة يأخذ في النظام الإجرائي الجزائري طابع البطلان المطلق الذي يسري بقوة القانون".²

¹ علي شملال، الجريمة المعلوماتية في التشريع الجزائري: دراسة تحليلية مقارنة، مجلة الاجتهاد للدراسات القانونية

والاقتصادية، جامعة تامنغست، المجلد 9، العدد 2، 2020، ص 74.

² عبد الرحمن خلفي، المرجع السابق، ص 287.

رابعاً: الأثر الانعكاسي للبطلان على الأدلة المترتبة

يُثير بطلان الإجراء الرقمي تساؤلاً إضافياً حول مصير الأدلة التي استُخلصت منه. وتُقرّر نظرية "ثمرة الشجرة المسمومة" (Fruit of the Poisonous Tree) "المعروفة في القانون الأمريكي أن البطلان يمتد ليشمل جميع الأدلة التي كان الدليل الملقى سبباً في الحصول عليها. وقد نحا قانون الإجراءات الجزائية الجزائري بتعديلاته الأخيرة منحى قريباً من هذه النظرية دون أن يُقررها صراحةً بنص صريح، إذ يميل الاجتهاد القضائي نحو إعمال الأثر الانعكاسي للبطلان لا سيما حين يكون الإجراء الملقى قد استُخدم أساساً لإجراءات لاحقة ذات صلة مباشرة به.¹

¹ أحمد غاي، إجراءات المتابعة الجزائية في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، مجلة العلوم القانونية والسياسية، جامعة الوادي، العدد 22، 2021، ص 198.

خلاصة الفصل الثاني

أبرز هذا الفصل البعد الإجرائي التقني لمواجهة الجريمة الإلكترونية في التشريع الجزائري، من خلال رصد الأحكام الاستثنائية التي استحدثها القانون رقم 09-04 وما تلاه من تعديلات.

فعلى صعيد التفتيش والحجز، تبين أن المشرع الجزائري منح السلطات القضائية وضباط الشرطة القضائية آليات استثنائية بالغة الفعالية، في مقدمتها التفتيش الافتراضي عن بُعد وآلية تمديد التفتيش السريع وتسخير ذوي الدراية الفنية. وفيما يتعلق بالحجز، كرّس المشرع مفهوم الحجز بالنسخ وتشكيل الأحرار المعنوية التي تُجسّد مبدأ "الفصل بين الدليل ودعامته"، إلى جانب آليات منع الوصول إلى البيانات غير المشروعة.

وعلى صعيد الإثبات وحماية الحريات، كرّس المشرع حجية الدليل الرقمي مع إخضاعه للسلطة التقديرية للقاضي، وفرض قيوداً صارمة على توظيف المعلومات المتحصل عليها خارج نطاق التحري، معزراً ذلك بالضمانات الدستورية المتعلقة بقرينة البراءة وحقوق الدفاع. أما على صعيد التعاون الدولي، فقد وضع المشرع حداً فاصلاً واضحاً يُحظر تجاوزه هو السيادة الوطنية والنظام العام، مرتباً على مخالفته البطلان المطلق للإجراءات والأدلة.

وتبقى المعادلة الصعبة هي كيفية الموازنة في التطبيق الفعلي بين هذه الصلاحيات الواسعة الممنوحة للتحقيق وبين الضمانات الدستورية للأفراد، لا سيما في ظل محدودية التكوين التقني للأطراف الإجرائية وقصور آليات التعاون الدولي مقارنةً بحجم التحديات المطروحة.

خاتمة

الخاتمة

تقف هذه الدراسة عند نهاية مسار تحليلي طويل ومتشعب، استهدف الكشف عن الملامح الحقيقية للمنظومة الإجرائية الجزائية في مواجهة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، تلك المنظومة التي نشأت في سياق استثنائي وتطورت تحت ضغط واقع إجرامي متجدد لا يمنح المشرع ترف التأمل الهادئ. وقد انطلقت الدراسة من إشكالية محورية تتمحور حول مدى نجاح المشرع الجزائري في بناء منظومة إجرائية فعّالة وخاصة لمتابعة هذه الجرائم، وذلك مع صون التوازن المطلوب بين متطلبات فعالية المكافحة من جهة وضمانات حماية الحقوق والحريات الأساسية من جهة أخرى. وفي ضوء ما أسفر عنه الفصلان من تحليل ونقد، يمكن بلوغ جملة من النتائج والتوصيات الجوهرية.

أولاً: النتائج

على صعيد الإطار المفاهيمي والاختصاصي، أسس المشرع الجزائري منظومته الإجرائية على معيار مزدوج في تحديد وعاء التجريم الرقمي يجمع بين المحل الجرمي ووسيلة الارتكاب، وهو مسلك يُوسّع نطاق الحماية الجنائية ويجعلها قابلةً للتطور مع تجدد أساليب الإجرام الرقمي. وفي ما يخص الاختصاص القضائي، تجاوز المشرع قيود الإقليمية الكلاسيكية بإرساء مبدأ الامتداد الاختصاصي الاستراتيجي المقرر في المادة 15 من القانون رقم 04-09، وهو مبدأ يمنح المحاكم الجزائرية صلاحية ملاحقة الجرائم الإلكترونية المرتكبة خارج الإقليم متى مسّت المصالح الجوهرية للدولة. غير أن ثمة فجوةً عملية واضحة بين هذا الامتداد المُقرّر نصاً والقدرة الفعلية على ممارسته، في ظل بطء آليات التعاون الدولي مقارنةً بسرعة الجريمة الإلكترونية وسهولة إتلاف أدلتها.

على صعيد الهياكل المؤسسية، أظهر المشرع الجزائري وعياً تدريجياً متصاعداً بضرورة التخصص المؤسسي، تجسّد في إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتطوير هياكلها بموجب المرسوم الرئاسي رقم 20-183، وفي إرساء الأقطاب القضائية الجهوية التي بلغت ذروتها باستحداث القطب الجزائري الوطني بموجب الأمر رقم 21-11. بيد أن إشكالية هيكلية حقيقية تظل قائمة، وهي الفجوة بين الكفاءة التقنية لهذه الهياكل والرقابة القضائية الفعلية عليها، إذ يجد القاضي نفسه في مواجهة تقارير خبرة بالغة التعقيد التقني يصعب عليه تقييمها بصورة نقدية مستقلة دون تكوين تقني متخصص، مما يُفرغ الرقابة القضائية أحياناً من مضمونها الحقيقي ويُحيلها إلى مجرد مصادقة شكلية على ما تنتهي إليه الأجهزة الأمنية والخبرات التقنية.

على صعيد أساليب التحري الرقمي، استحدث المشرع أدوات استثنائية بالغة الفاعلية كمرقبة الاتصالات الإلكترونية وآلية التفتيش الافتراضي عن بُعد وتمديد التفتيش السريع وإلزام مقدمي الخدمات بالتعاون والحفظ، وأحاطها بضمانات هامة في مقدمتها الإذن القضائي الكتابي المسبق والمسبّب والتحديد الحصري للحالات المجيزة للمراقبة. بيد أن التساؤل يظل مشروعاً وملحاً حول مدى فعالية هذه الضمانات في مواجهة الضغوط الأمنية الميدانية، لا سيما أن الممارسة تكشف أحياناً عن تقديم الاعتبارات الأمنية العاجلة على حساب الشرعية الإجرائية الواجبة، وهو ما يُشكّل مساساً بمبدأ راسخ لا يقبل المقايضة.

على صعيد الإثبات والدليل الرقمي، كرّس المشرع الجزائري حجية الدليل الرقمي بصورة تدريجية بدءاً من المادة 323 مكرر من القانون المدني المستحدثة بالقانون رقم 05-10، مروراً بمبدأ التكافؤ المقرر في المادة 18 من القانون رقم 09-04، وانتهاءً بأحكام الأمر رقم 21-11 المعدّل لقانون الإجراءات الجزائية. وقد أحاط المشرع هذا الدليل بضمانات جوهرية تتعلق بشروط صحة الحصول عليه وسلامة حفظه وتقييد توظيفه خارج نطاق التحري

الجاري، معززاً ذلك بالضمانات الدستورية المكرّسة في التعديل الدستوري لعام 2020، غير أن الفجوة بين هذه الضمانات النصية ومقتضيات التطبيق الفعلي تبقى قائمة ولافتة في ظل ضعف التكوين التقني لدى الأطراف الإجرائية.

على صعيد التعاون الدولي، يعاني الإطار الجزائري من إشكالية هيكلية مُركّبة تتمثل في عدم انضمام الجزائر إلى اتفاقية بودابست للجريمة السيبرانية لعام 2001، وعدم مصادقتها على اتفاقية مالابو الأفريقية لعام 2014، مما يُبقي مسارات التعاون الدولي رهينةً بالآليات الثنائية التقليدية البالغة البطء. وفي ظل هذا القصور، يُصبح الامتداد الاختصاصي المقرر في القانون 04-09 مجرد حكم نظري لا تسنده آليات تعاون دولية فعّالة تُمكن من تجسيده على أرض الواقع.

ثانياً: الإقتراحات

انطلاقاً من النتائج المستخلصة، ومن منطلق الحرص على الارتقاء بالمنظومة الإجرائية الجزائرية إلى مستوى التحديات المطروحة، تُقدّم هذه الدراسة جملةً من الاقتراحات التي تراها جديرة بالاعتبار.

تبدو الحاجة ملحةً إلى إرساء برامج تكوين تقني متخصص ومستمر لفائدة القضاة المنتدبين للنظر في القضايا الإلكترونية وأعضاء النيابة العامة المكلفين بالإشراف على التحريات الرقمية، وذلك لردم الفجوة التقنية التي تُضعف الرقابة القضائية الفعلية على أعمال الهيئة الوطنية وسائر الأجهزة المتخصصة. فالرقابة القضائية المجدية تقتضي قاضياً قادراً على فهم التقنية ونقد الخبرة والمساءلة المستقلة لا مجرد التوقيع على التقارير.

يستوجب كذلك التفكير الجاد في الانضمام إلى اتفاقية بودابست للجريمة السيبرانية أو على الأقل المصادقة على اتفاقية مالابو الأفريقية، بوصفهما مسارين ضروريين لتجاوز القصور

الذريع في آليات التعاون الدولي الراهنة. فالجريمة الإلكترونية العابرة للحدود لا تُواجه بأدوات وطنية مهما بلغت من تطور، بل تستلزم بالضرورة شبكة تعاون دولية واسعة تُتيح تبادل الأدلة بسرعة وفعالية تتناسب مع طبيعة هذا الإجرام.

ومن الأهمية بمكان كذلك تعزيز المنظومة التشريعية بنصوص صريحة تُحسم الإشكاليات التفسيرية التي كشفت عنها الدراسة، ولا سيما إشكالية إلزام المتهم بتسليم مفتاح تشفير جهازه وما ينطوي عليه ذلك من تعارض مع الحق في الصمت وقرينة البراءة، وإشكالية الأثر الانعكاسي للبطلان الإجرائي على الأدلة المترتبة. فاستمرار الصمت التشريعي حيال هذه المسائل يُبقيها مصدر اضطراب في الاجتهاد القضائي ومدعاة للطعون الإجرائية المتكررة.

يُضاف إلى ذلك ضرورة العمل الدبلوماسي على إبرام اتفاقيات ثنائية مع الدول التي تُقيم فيها كبرى شركات التكنولوجيا العالمية، بهدف تنظيم الإطار القانوني لطلبات الحصول على البيانات المخزنة على خوادمها، إذ إن الفراغ القائم في هذا الشأن يُشكّل ثغرة استراتيجية في منظومة مكافحة الجريمة الإلكترونية لا يمكن سدّها بالنصوص الوطنية وحدها.

قائمة المصادر والمراجع

قائمة المصادر والمراجع

أولاً: النصوص القانونية

1. الدستور الجزائري المعدل سنة 2020.
2. الأمر رقم 66-155 المؤرخ في 08 جوان 1966 المتضمن قانون الإجراءات الجزائية، المعدل والمتمم.
3. الأمر رقم 66-156 المؤرخ في 08 جوان 1966 المتضمن قانون العقوبات، المعدل والمتمم.
4. القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات، الجريدة الرسمية، العدد 71.
5. القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون الإجراءات الجزائية، الجريدة الرسمية، العدد 84.
6. القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47.
7. القانون العضوي رقم 14-25 المؤرخ في 25 ديسمبر 2014 المتضمن تعديل وتتميم الأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، العدد 74.
8. القانون رقم 18-07 المؤرخ في 10 جوان 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية، العدد 34.
9. الأمر رقم 21-11 المؤرخ في 25 أوت 2021 المعدل والمتمم للأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، العدد 65.

ثانياً: المراسيم التنظيمية

1. المرسوم التنفيذي رقم 06-348 المؤرخ في 05 أكتوبر 2006 المحدد لتنظيم المصالح التقنية والعلمية للشرطة القضائية، المعدل والمتمم بالمرسوم التنفيذي رقم 16-267 المؤرخ في 17 أكتوبر 2016.
2. المرسوم التنفيذي رقم 09-97 المؤرخ في 22 فبراير 2009 المحدد لشروط وكيفيات منح الاعتماد للمتعاملين الذين يقدمون خدمات الاتصالات الإلكترونية عبر الإنترنت وعبر شبكة الاتصالات الراديوية.
3. المرسوم الرئاسي رقم 20-183 المؤرخ في 13 جويلية 2020 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 40.

ثالثاً: الكتب

1. بارش، سليمان. شرح قانون الإجراءات الجزائية الجزائري. الطبعة الرابعة، دار الهدى، عين مليلة، الجزائر، 2013.
2. بيومي حجازي، عبد الفتاح. الدليل الجنائي الرقمي وجرائم الإنترنت. دار الفكر الجامعي، الإسكندرية، 2008.
3. بيومي حجازي، عبد الفتاح. النظام القانوني لحماية الحكومة الإلكترونية: الكتاب الثاني، الحماية الجنائية والأمنية للمعلومات. دار الفكر الجامعي، الإسكندرية، 2008.
4. خلفي، عبد الرحمن. قانون الإجراءات الجزائية في ضوء الممارسة القضائية. مكتبة الرشاد، الجزائر، 2018.
5. حزيط، محمد. الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات. الطبعة الثانية، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2018.
6. سعد، عبد العزيز. الإجراءات الجزائية في التشريع الجزائري. الطبعة الثانية، ديوان المطبوعات الجامعية، الجزائر، 2019.

7. شيتور، جلول. مبادئ الإجراءات الجزائية في القانون الجزائري. الطبعة الثالثة، ديوان المطبوعات الجامعية، الجزائر، 2016.
8. صقر، نبيل. الدليل العملي للبحث والتحري في الجرائم المعلوماتية. دار الهدى، عين مليلة، الجزائر، 2014.

رابعاً: الرسائل والمذكرات الجامعية

1. حكار، أيمن، وبدير، يحي. الجرائم المتصلة بتكنولوجيات الإعلام والاتصال. مذكرة ماستر، جامعة بلحاج بوشعيب، عين تموشنت، 2022-2023.
2. رفعي، سمير. البحث والتحري عن الجريمة الإلكترونية. مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة 20 أوت 1955، سكيكدة، 2017.
3. زاوي محند آكلي. الإجراءات الجزائية في مواجهة الجريمة المعلوماتية في الجزائر. مذكرة ماجستير، كلية الحقوق، جامعة مولود معمري، تيزي وزو، 2012.

خامساً: المقالات والدوريات العلمية

1. أحمد غاي. "إجراءات المتابعة الجزائية في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات". مجلة العلوم القانونية والسياسية، جامعة الوادي، العدد 22، 2021.
2. بشير سعد زغلول. "النظرية العامة للإثبات الجنائي في الجرائم المعلوماتية". مجلة المفكر، جامعة محمد خيضر بسكرة، العدد 18، 2018.
3. جراد، سميرة، وقتال، جمال. "خصوصية المتابعة الجزائية للجرائم الإلكترونية". مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد 14، العدد 01، 2025.
4. شملال، علي. "الجريمة المعلوماتية في التشريع الجزائري: دراسة تحليلية مقارنة". مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد 9، العدد 2، 2020.
5. عمر زودة. "الاختصاص القضائي في الجرائم المعلوماتية". مجلة الحقوق والعلوم السياسية، العدد 12، 2020.

سادساً: المراجع الأجنبية

1. Benillouche, Mikaël. "La saisie de données informatiques en droit français : problèmes et perspectives." Revue de Science Criminelle et de Droit Pénal Comparé, n° 2, 2011.
2. Dobbi, Sofiane, et Souria Yessad. "Les infractions liées aux technologies de l'information et de la communication en droit algérien." Revue Algérienne des Sciences Juridiques, Politiques et Économiques, vol. 57, n° 3, 2020.

فهرس المحتويات

فهرس المحتويات

الصفحة	المحتوى
	شكر وتقدير
	الإهداء
1	مقدمة
الفصل الأول: الخصوصية التنظيمية لهيئات المتابعة وآليات التحري الرقمي المستحدثة	
7	تمهيد
8	المبحث الأول: الخصوصية الهيكلية والقضائية للجهات المكلفة بالمتابعة
9	المطلب الأول: وعاء التجريم الرقمي وامتداده المكاني الحامي للمصالح الاستراتيجية
11	الفرع الأول: تحديد مفهوم الجريمة التكنولوجية ونطاق المتابعة الإجرائية
13	الفرع الثاني: مبدأ الامتداد الاختصاصي العابر للحدود
13	المطلب الثاني: الهيئات المتخصصة والأقطاب القضائية في التحري الرقمي والمتابعة
13	الفرع الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها
15	الفرع الثاني: الأجهزة الأمنية المتخصصة في الضبط القضائي الرقمي
16	الفرع الثالث: الأقطاب القضائية المتخصصة وآفاق التخصص القضائي
19	المبحث الثاني: الأساليب التقنية الخاصة للبحث والتحري الرقمي
19	المطلب الأول: آليات المراقبة الإلكترونية واعتراض المراسلات الرقمية في حينها
19	الفرع الأول: الشرعية الإجرائية للمراقبة التقنية
21	الفرع الثاني: الحالات الحصرية للجوء للمراقبة الإلكترونية
23	الفرع الثالث: الأثر الجزائي على المساس بالحياة الخاصة
24	المطلب الثاني: التزامات مقدمي الخدمات وضبط المعطيات المتعلقة بحركة السير
24	الفرع الأول: إلزامية مساعدة العدالة وكتمان السرية
26	الفرع الثاني: حفظ بيانات حركة السير والمسؤولية الجزائية

28	خلاصة الفصل الأول
	الفصل الثاني: خصوصية المعاينة الرقمية وضمانات الشرعية الإجرائية
30	تمهيد
31	المبحث الأول: خصوصية التفتيش والحجز في البيئة الرقمية
31	المطلب الأول: الأحكام الاستثنائية لتفتيش المنظومات المعلوماتية والشبكات
32	الفرع الأول: التفتيش الافتراضي ولو عن بعد
33	الفرع الثاني: تمديد التفتيش السريع وتسخير ذوي الدراية
36	المطلب الثاني: الحجز الرقمي للبيانات وآليات منع الوصول إليها
36	الفرع الأول: الحجز بالنسخ وتشكيل الأحراز المعنوية
38	الفرع الثاني: الحجز التقني لمنع الوصول إلى البيانات غير المشروعة
40	المبحث الثاني: حجية الدليل الرقمي وضوابط حماية الحريات الفردية
40	المطلب الأول: القيمة الإثباتية للدليل الرقمي وحدود استعماله
40	الفرع الأول: حجية الدليل الرقمي في المنظومة القانونية الجزائرية
42	الفرع الثاني: تقييد الاستعمال الشخصي للمعلومات المتحصل عليها
43	المطلب الثاني: ضوابط التعاون الدولي وبطلان الإجراءات المخالفة للشرعية
44	الفرع الأول: آليات التعاون الدولي في إطار القانون 04-09
45	الفرع الثاني: البطلان الإجرائي جزاءً على انتهاك الشرعية الرقمية
48	خلاصة الفصل الثاني
50	خاتمة
55	قائمة المصادر والمراجع
60	فهرس المحتويات