وزارة التعليم العالي و البحث العلمي
جامعة آكلي محند اولحاج البويرة
كلية الحقوق والعلوم السياسة
قسم القانون العام

التفتيش الالكتروني بين سلطة التحقيق وحماية الحياة الخاصة

مذكرة لنيل شهادة الماستر في القانون

تخصص: القانون الجنائي والعلوم الجنائية

إعداد الطالبين: **إشراف الأستاذة:**

كمال أشرف صلاح الدين **قريم سكورة**

العزازي هاني

لجنة المناقشة:

الاستاذ(ة): دريدر ملكي .....رئيسا

الأستاذ(ة): قريم سكورة.....مشرفا ومقررا

الأستاذ(ة): بوديسة كريم .....ممتحنا

السنة الجامعية:2026/2025

شكر و عرفان

نتوجه بكامل الشكر والتقدير، لأستاذتنا الفاضلة الدكتورة قريم سكورة لتفضلها بالإشراف على هذا العمل والتي لم تبخل علينا بالمساعدة والتوجيه والنصيحة، نسأل الله ان يمد في عمرها وأن تنفع بعلمها.

كما يمتد شكرنا للأساتذة الافاضل أعضاء لجنة المناقشة على قبولهم مناقشة مذكرتنا

إهداء

إلى أمي الحبيبة، إلى من كان حبها دعائي، وحنانها قوتي، وصبرها نورًا يضيء دربي، إلى من تعجز الكلمات عن وصف فضلها ومكانتها في قلبي. أهديكِ هذا العمل المتواضع عربون محبة وامتنان، وأسأل الله أن يحفظكِ ويديم عليكِ الصحة والسعادة. وإلى أبي العزيز، إلى من علّمني معنى الكفاح والاجتهاد، وكان مثالًا للعطاء والتضحية، إلى من كان سندي وداعمي في كل مراحل حياتي. أهديك هذا الإنجاز تقديرًا لجهودك وعرفانًا بفضلك، راجيًا أن أكون عند حسن ظنك دائمًا.

إلى إخوتي أحبتي رفقاء الدرب.

إلى صديقي وشريكي في هذا العمل،

من شاركني مشوار الإنجاز خطوة بخطوة، وتقاسم معي عناء البحث وجهد العمل، فكان خير رفيق وخير معين. أشكرك على تعاونك وإخلاصك وروحك الطيبة، وأتمنى لك مزيدًا من النجاح والتوفيق في مسيرتك العلمية والعملية. لك مني كل التقدير والاحترام، ودمت صديقًا وأخًا عزيزًا.

إلى عائلتي وكل من ساندني،

أهديكم ثمرة هذا الجهد، شاكرًا لكم دعمكم وتشجيعكم الذي كان له الأثر الكبير في الوصول إلى هذه المرحلة.

كمال اشرف صلاح الدين

إهداء

إلى أمي الغالية، التي احتضنتني بقلبها قبل يديها، وكانت دعاؤها سرّ قوتي ونجاحي أهديكِ هذا العمل بكل حب وامتنان، فأنتِ النور الذي يضيء دربي والروح التي أستمد منها الأمل في كل لحظة، إلى أبي العزيز، الذي علّمني معنى القوة والصبر، وكان سندي في كل خطوة من حياتي أهديك هذا العمل بكل فخر واعتزاز، فأنتَ السند الحقيقي والقدوة التي أستمد منها عزيمتي وإصراري، إلى إخوتي الغاليين، الذين شاركوني لحظات العمر .

وإلى صديقي في العمل،

الذي جمعني به التعاون وصنعت معه روح الفريق أجمل المعاني، الذي لم يكن مجرد زميل، بل كان شريكًا حقيقيًا في النجاح، أقدّر فيك روح التعاون التي تجمعنا، وحسن أخلاقك التي تجعل العمل معك أكثر سهولة وراحة. كنت دائمًا داعمًا في اللحظات الصعبة، ومشجعًا على الاستمرار والتقدم، فشكرًا لك على كل ما قدمته من جهد وإيجابية جعلت بيئة العمل أجمل وأقوى.

إلى عائلتي الكريمة، التي منحتني الانتماء والدعم وكانت لي السند في كل وقت.

إليكم أهدي هذه المذكرة، امتنانًا وحبًا لوجودكم في حياتي.

العزازي هاني

أهم المختصرات:

ج: جزء

د.ب.ن: دون بلد نشر

د.د.ن: دون دار نشر

د.ر.ط: دون رقم الطبعة

د.س.ن: دون سنة نشر

ص.ص: الصفحتان

ص: الصفحة

ع: عدد

م.ق: مجلة قضائية

م.ج: مجلد


مقدمة

مقدمة

أدى التطور المتسارع لتكنولوجيا المعلومات والاتصال إلى إحداث تحولات عميقة في مختلف مجالات الحياة، حيث أصبحت الأنظمة المعلوماتية والشبكات الإلكترونية وسيلة أساسية لحفظ المعلومات وتبادلها ومعالجتها، وقد نتج عن هذا التطور ظهور أنماط جديدة من الجرائم استغلت البيئة الرقمية كوسيلة أو محل للاعتداء، الأمر الذي فرض على المشرع الجزائري تطوير وسائل البحث والتحري والتحقيق لمواكبة هذا النوع من الإجرام المستحدث[1].

ويعد التفتيش الإلكتروني من أبرز الآليات التي استحدثتها السياسة الجنائية الحديثة لمواجهة الجرائم المرتبطة بالأنظمة المعلوماتية، إذ يهدف إلى البحث عن الأدلة الرقمية وضبطها داخل الحواسيب والهواتف الذكية والخوادم وقواعد البيانات وغيرها من الوسائط الإلكترونية، غير أن خصوصية هذا الإجراء تكمن في كونه لا ينصب على أشياء مادية فحسب، وإنما يمتد إلى معطيات ومعلومات شخصية قد تمثل جزءا من الحياة الخاصة للأفراد[2]. ولذلك يثير التفتيش الإلكتروني إشكالية قانونية دقيقة تتمثل في ضرورة الموازنة بين مصلحتين متعارضتين ظاهريا؛ الأولى تتمثل في تمكين سلطات التحقيق من الوصول إلى الأدلة الرقمية اللازمة للكشف عن الجرائم وملاحقة مرتكبيها، والثانية تتعلق بضرورة احترام الحقوق والحريات الأساسية للأفراد، وعلى رأسها الحق في الخصوصية وحماية المعلومات الشخصية وسرية المراسلات والاتصالات الإلكترونية.

وقد أدرك المشرع الجزائري أهمية هذه الموازنة، فسعى إلى توفير حماية دستورية وقانونية للحياة الخاصة والمعطيات ذات الطابع الشخصي، من خلال النصوص الدستورية والقوانين الخاصة بحماية البيانات الشخصية ومكافحة الجرائم المعلوماتية، وفي الوقت نفسه منح سلطات

[1] عبد الرحمان خلفي، الإجراءات الجزائية في التشريع الجزائري والمقارن، دار بلقيس، الجزائر، 2017، ص 112.

[2] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي مصر، 2004، ص 67.

التحقيق صلاحيات تمكنها من مباشرة إجراءات التفتيش الإلكتروني وفق ضوابط وشروط قانونية محددة[1].

ومن هذا المنطلق يكتسي موضوع التفتيش الإلكتروني أهمية بالغة، بالنظر إلى ارتباطه المباشر بفعالية العدالة الجنائية من جهة، وحماية الحقوق والحريات الأساسية من جهة أخرى، الأمر الذي يجعله من المواضيع القانونية المعاصرة الجديرة البحث و تتمثل أهمية دراسة هذا الموضوع في إبراز الطبيعة القانونية للتفتيش الإلكتروني في ظل التطور التكنولوجي مع بيان حدود سلطة التحقيق في مباشرة إجراءات التفتيش الإلكتروني أيضا توضيح الضمانات القانونية المقررة لحماية الحياة الخاصة أثناء التفتيش الإلكتروني و الوقوف على مدى فعالية التشريع الجزائري في تحقيق التوازن بين متطلبات التحقيق الجنائي وحماية الحقوق والحريات.

اما بالنسبة لأهداف الدراسة في هذا الموضوع هو تحديد مفهوم التفتيش الإلكتروني وخصائصه وطبيعته القانونية ودراسة الإطار القانوني المنظم لسلطة التحقيق في هذا المجال

أيضا تحليل الحماية التشريعية المقررة للمعلومات الشخصية مع تقييم الضمانات القانونية المقررة لحماية الحياة الخاصة أثناء مباشرة التفتيش الإلكتروني مع تقديم تصور قانوني يبرز مدى كفاية التنظيم التشريعي الجزائري في هذا المجال.

[1] القانون رقم 18-07 المؤرخ في 10 جوان 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية رقم 34 لسنة 2018، ودستور الجزائر لسنة 2020، المادة 47.

أما بالنسبة لأسباب اختيار الموضوع هو الرغبة الشخصية في دراسة المواضيع القانونية المرتبطة بالتكنولوجيا الحديثة والاهتمام بالإشكالات القانونية التي تثيرها الجرائم الإلكترونية ووسائل مكافحته مع أهمية الموضوع في التكوين الأكاديمي والمهني في مجال القانون الجنائي ، حداثة موضوع التفتيش الإلكتروني وتزايد أهميته العملية كما ان تزايد الاعتماد على الأدلة الرقمية في التحقيقات الجنائي و الحاجة إلى دراسة الضمانات القانونية المقررة لحماية الحياة الخاصة في البيئة الرقمية و الإشارة الى أهمية الوقوف على مدى مواكبة التشريع الجزائري للتطورات التقنية الحديثة.

تجدر الإشارة الى الدراسات السابقة التي تناولت نفس موضوع الدراسة الخاص بمذكرتنا هناك دراسة تناولت التفتيش الإلكتروني كوسيلة من وسائل الإثبات الجنائي في الجرائم المعلوماتية، وركزت على الجوانب الإجرائية المتعلقة بضبط الأدلة الرقمية، دراسة بحثت في الحماية القانونية للبيانات الشخصية في ظل التطور التكنولوجي، واهتمت ببيان الضمانات التشريعية المقررة للخصوصية المعلوماتية، دراسة عالجت جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري، مع التركيز على الجوانب الموضوعية والإجرائية لمكافحتها.

وتتميز هذه الدراسة عن الدراسات السابقة بمحاولة الربط بين سلطة التحقيق في مباشرة التفتيش الإلكتروني وبين متطلبات حماية الحياة الخاصة في إطار رؤية قانونية متكاملة.

اعتمدت هذه الدراسة على:

-المنهج الوصفي لعرض مختلف المفاهيم والنصوص القانونية المرتبطة بالتفتيش الإلكتروني.

-المنهج التحليلي لتحليل الأحكام القانونية والفقهية المتعلقة بالموضوع.

-المنهج المقارن عند الاقتضاء للاستئناس ببعض التشريعات المقارنة وإبراز أوجه التشابه والاختلاف.

تتمحور إشكالية هذه الدراسة حول التساؤل الرئيسي الآتي:

إلى أي مدى وفق المشرع الجزائري في تحقيق التوازن بين مقتضيات التفتيش الإلكتروني باعتباره إجراء ضروريا للكشف عن الجرائم وجمع الأدلة، وبين ضرورة حماية الحياة الخاصة والمعلومات الشخصية للأفراد؟

للإجابة عن الإشكالية المطروحة ومعالجة مختلف جوانب الموضوع، تم تقسيم الدراسة إلى فصلين:

الفصل الأول يتضمن الحماية التشريعية للمعلومات الشخصية في ظل التفتيش الإلكتروني ويتضمن مبحثين: **المبحث الأول** الحماية القانونية للمعلومات الشخصية **المبحث الثاني** التفتيش الالكتروني كاستثناء مشروع على حرمة الحياة الخاصة.

اما الفصل الثاني يتناول التفتيش الإلكتروني بين مقتضيات سلطة التحقيق وضمانات حماية الحياة الخاصة ويتضمن مبحثين **المبحث الأول** الضوابط القانونية للتفتيش الالكتروني **المبحث الثاني** سلطة التحقيق في التفتيش الالكتروني وضمانات حماية الحياة الخاصة.

الفصل الأول

الحماية التشريعية للمعلومات الشخصية في ظل التفتيش الإلكتروني

الفصل الأول

الحماية التشريعية للمعلومات الشخصية في ظل التفتيش الإلكتروني

فرز التطور التكنولوجي المتسارع وانتشار استخدام وسائل الاتصال الحديثة والأنظمة المعلوماتية تحولات عميقة في مجال الإثبات الجنائي، حيث أصبحت الجرائم تُرتكب في بيئة رقمية تعتمد على الوسائل التقنية الحديثة، الأمر الذي استدعى تطوير وسائل البحث والتحري التقليدية لتتلاءم مع طبيعة هذه الجرائم وما تفرزه من أدلة رقمية، ومن بين أهم هذه الوسائل التفتيش الإلكتروني الذي أصبح أداة فعالة بيد سلطات التحقيق للكشف عن الجرائم وجمع الأدلة المخزنة داخل الأنظمة المعلوماتية والأجهزة الإلكترونية.

غير أن مباشرة التفتيش الإلكتروني يثير إشكالية قانونية دقيقة، تتمثل في تعارضه مع الحق في الخصوصية وحماية الحياة الخاصة، لكونه يسمح بالاطلاع على كم هائل من البيانات والمعلومات الشخصية التي تمثل جانبا أساسيا من حرية الفرد وكرامته.

فالتطور التقني الذي سهل تخزين المعلومات وتبادلها إلكترونيا، جعل هذه المعطيات أكثر عرضة للمساس بها سواء من قبل الأفراد أو حتى أثناء مباشرة إجراءات التحقيق الجنائي، لذا فقد تدخل المشرع بوضع منظومة تشريعية تهدف إلى تحقيق التوازن بين مصلحتين متعارضتين ظاهريا؛ تتمثل الأولى في تمكين سلطات التحقيق من ممارسة مهامها في البحث عن الحقيقة وكشف الجرائم، بينما تتمثل الثانية في حماية المعلومات الشخصية وصون الحياة الخاصة من أي اعتداء أو تعسف قد ينجم عن استعمال وسائل التفتيش الحديثة، وقد تجسد ذلك من خلال إقرار حماية قانونية وجزائية للمعلومات الشخصية(المبحث الأول)، وتنظيم التفتيش الإلكتروني من خلال تبيان مفهومه وطبيعته القانونية وحدود مشروعيته باعتباره استثناء يرد على الأصل المتمثل في حماية حرمة الحياة الخاصة(المبحث الثاني).

المبحث الأول: الحماية التشريعية للمعلومات الشخصية

تُعد حرمة الحياة الخاصة حقا دستوريا لا يجوز المساس به إلا بموجب ضرورة يقررها القانون وبأمر قضائي مسبب، وفي ظل الطبيعة "الاختراقية" للتفتيش الإلكتروني، وضع المشرع (لاسيما الجزائري) مجموعة من القواعد القانونية تهدف إلى حماية الفضاء الخاص للأفراد من أي تعسف قد يمارس باسم القانون، وسنحاول في هذا المبحث تفكيك هذه الحماية من خلال عرض المبادئ الدستورية التي تكرس حق الفرد في حماية معلوماته الخاصة، وكذا النصوص القانونية الإجرائية التي تنظم كيفية الموازنة بين حماية الخصوصية وضرورات التحقيق، وذلك عبر المطلبين التاليين: المطلب الأول: الحماية الدستورية للمعلومات الشخصية المطلب الثاني: الحماية الجزائية للمعلومات الشخصية

المطلب الأول: الحماية الدستورية للمعلومات الشخصية

تُعد الحماية الدستورية الأساس الذي تقوم عليه مختلف صور الحماية القانونية للمعلومات الشخصية، إذ حرص المشرع في الدستوري الجزائري على تكريس الحق في الخصوصية وصون الحياة الخاصة للأفراد، بما يضمن حماية بياناتهم ومعلوماتهم من أي مساس غير مشروع، وتظهر هذه الحماية من خلال الاعتراف بالخصوصية المعلوماتية كحق أساسي، إلى جانب إقرار مجموعة من الضمانات الدستورية والقانونية التي تكفل احترام هذا الحق وحمايته، وذلك من خلال فرعين أساسيين:

الفرع الأول: تكريس الحق في الخصوصية المعلوماتية.

الفرع الثاني: الضمانات الدستورية لحماية المعلومات الشخصية.

الفرع الأول: تكريس الحق في الخصوصية المعلوماتية

يُعدّ الحق في صيانة كرامة الإنسان وحماية حياته الخاصة من أبرز الحقوق والحريات التي كرسها الدستور الجزائري، حيث تلتزم الدولة بضمان عدم المساس بحرمة الإنسان، وتحظر

كل أشكال الاعتداء أو المساس بكرامته. كما حرص المؤسس الدستوري على وضع قواعد قانونية تنظم إجراءات التفتيش بما يضمن حماية حرمة المسكن، إذ لا يجوز القيام بأي تفتيش إلا بمقتضى القانون وفي إطار احترامه[1].

ومن جهة أخرى أقرّ الدستور ضمان الحريات الأساسية وحقوق المواطن[2]، حيث نصّ صراحة على عدم جواز انتهاك الحياة الخاصة، مع تأكيد حماية سرية المراسلات والاتصالات بمختلف أشكالها[3]، كما أكد أيضا على حماية شرف المواطن وحرمة حياته الخاصة، وجعل ذلك من الحقوق التي يكفلها القانون[4].

ولم يقتصر المشرع الجزائري على تكريس الحق في الحياة الخاصة باعتباره حقا دستوريا فحسب، بل أضفى عليه طابع الالتزام، إذ يتعين على الأفراد احترام هذا الحق أثناء ممارستهم لحرياتهم، والمحافظة عليه وعدم المساس به، وقد تجسد ذلك من خلال النصوص الدستورية التي توجب ممارسة الحريات في إطار احترام حقوق الغير، لا سيما ما تعلق بالحياة الخاصة[5].

وفي سياق تطور الحماية الدستورية عزّز الدستور الجزائري هذا التوجه بموجب التعديل الدستوري لسنة 2020، وذلك بموجب المادة 47 في فقرتها الرابعة ،[6] ويعكس هذا النص مدى تفاعل المشرع مع التحولات التي فرضها العصر الرقمي من خلال إدراج حماية المعطيات الشخصية ضمن نطاق الحماية الدستورية للخصوصية[7].

---

[1] الجمهورية الجزائرية الديمقراطية الشعبية، دستور 1996 المعدل والمتمم، الجريدة الرسمية، العدد 76، المؤرخ في 8 ديسمبر 1996، المواد المتعلقة بحرمة المسكن والتفتيش.

[2] المادة 40 من الدستور الجزائري لسنة 1996، المعدل والمتمم، المرجع نفسه.

[3] المادة 47 من الدستور الجزائري لسنة 1996، المعدل والمتمم، المرجع نفسه.

[4] المادة 46 من الدستور الجزائري لسنة 1996، المعدل والمتمم، المرجع نفسه.

[5] الجمهورية الجزائرية الديمقراطية الشعبية، دستور 1996 المعدل والمتمم بموجب القانون رقم 16-01 المؤرخ في 06 مارس 2016، الجريدة الرسمية رقم 14، 2016، المادة 63.

[6] تنص المادة 47 من الدستور الجزائري لسنة 1996، المعدل والمتمم، المرجع نفسه على انه: حماية الأشخاص الطبيعيين عند معالجة المعطيات ذات الطابع الشخصي حق أساسي".

[7] عبد الرحمان خلفي، مرجع سابق، ص 112.

كما كرّست المادة 48 من تعديل الدستور ضمان الدولة لعدم انتهاك حرمة المسكن وأكدت على ضرورة حماية كرامة الإنسان من كل أشكال الاعتداء سواء كان ماديًا أو معنويًا، باعتبار ذلك من المقومات الأساسية التي تقوم عليها الدولة، ويُستشف من هذا التوجه حرص المشرع على صون مختلف عناصر الحياة الخاصة والتي تشمل حرمة المسكن وسرية المراسلات والاتصالات الشخصية، باعتبارها مكونات جوهرية لهذا الحق[1].

وقد حافظ المشرع الجزائري عبر مختلف الدساتير المتعاقبة على تكريس جملة من الضمانات الأساسية الرامية إلى حماية الحق في الحياة الخاصة، حيث جاءت هذه النصوص متفقة في مضمونها على تأكيد جملة من المبادئ الجوهرية.

فمن جهة، أقرّ الدستور بأن ممارسة الأفراد لحرياتهم تكون في إطار احترام الحقوق المعترف بها للغير، لا سيما ما تعلق بالشرف وستر الحياة الخاصة، ومن جهة أخرى حمل الدولة مسؤولية حماية كرامة الإنسان وضمان أمنه وسلامته من كل أشكال الاعتداء سواء كانت مادية أو معنوية[2].

كما نص على خضوع كل اعتداء على حقوق المواطن وحرياته لجزاء قانوني، بما يكفل ردع كل مساس بسلامته البدنية أو المعنوية، إضافة إلى ذلك كفل الدستور حق الأفراد في الدفاع عن حقوقهم الأساسية، بما يشمل حماية خصوصياتهم في مختلف صورها.

و أكد الدستور صراحة على عدم جواز انتهاك حرمة الحياة الخاصة للمواطنين، بما في ذلك شرفهم وسرية مراسلاتهم واتصالاتهم الشخصية، باعتبارها من الركائز الأساسية التي تقوم عليها منظومة الحقوق والحريات[3].

---

[1] فاتح قيش، ضوابط ممارسة مهنة الصحافة بين الشريعة الإسلامية والقانون الجزائري، أطروحة مقدمة لنيل شهادة الدكتوراه في العلوم الإسلامية، تخصص: شريعة وقانون، كلية العلوم الإنسانية والاجتماعية، جامعة الجزائر 1، 2014، ص93.

[2] المادة 34، مرجع سابق.

[3] المادة 39 الدستور الجزائري لسنة 1996، المعدل والمتمم، مرجع سابق.

تُكريس حماية حرمة المسكن باعتبارها إحدى أهم صور حماية الحياة الخاصة، حيث لا يجوز تفتيشه إلا بموجب إذن صادر عن الجهات القضائية المختصة، وفي حدود ما يقرره القانون مع مراعاة احترام خصوصيته، ويترتب على ذلك حظر أي مساس به، باستثناء الحالات التي تستدعيها مقتضيات المصلحة العامة، كحالات مكافحة الجريمة ومباشرة إجراءات البحث والتحري والتحقيق وفي هذا الإطار عمل المشرع على تأكيد مبدأ تقييد مباشرتها وفقا لشروط بما يفرض ممارستها في نطاق احترام الحقوق الشخصية والعامة، وعدم تحويل الحق في الخصوصية إلى حق مطلق قد يُستعمل للإضرار بحقوق الغير أو المساس بحرياتهم.

وعليه لا يجوز بأي حال من الأحوال المساس بحرمة الحياة الخاصة دون صدور أمر قضائي مسبب، مع إقرار جزاءات قانونية على كل انتهاك لهذا المبدأ أساسيًا يضمنه القانون وهذا ما يعكس تعزيز المشرع الجزائري للخصوصية في بعدها التقليدي والرقمي على حد سواء.[1]

الفرع الثاني: الضمانات الدستورية لحماية المعلومات الشخصية

لا تقتصر الحماية الدستورية للمعلومات الشخصية على مجرد الاعتراف بالحق في الخصوصية المعلوماتية، وإنما تمتد إلى إقرار جملة من الضمانات الدستورية التي تكفل احترام هذا الحق وتمنع المساس به بصورة تعسفية، وتزداد أهمية هذه الضمانات في ظل التطور التكنولوجي المتسارع وما أفرزه من وسائل حديثة قادرة على جمع البيانات الشخصية وتخزينها ومعالجتها ونقلها في وقت وجيز، الأمر الذي يفرض ضرورة إيجاد توازن بين متطلبات حماية الأمن العام ومكافحة الجريمة من جهة، واحترام الحياة الخاصة للأفراد من جهة أخرى[2].

وتتمثل أولى هذه الضمانات في تكريس مبدأ حرمة الحياة الخاصة، إذ نص المؤسس الدستوري الجزائري على عدم جواز انتهاك الحياة الخاصة للأشخاص، واعتبرها من الحقوق الأساسية المكفولة دستوريا ويشمل مفهوم الحياة الخاصة مختلف الجوانب المرتبطة بشخصية

[1] المادة 46 من الدستور الجزائري لعام 1996 المعدل والمتمم، مرجع سابق.

[2] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، مرجع سابق، ص45.

الفرد، بما في ذلك بياناته الشخصية ومعلوماته العائلية والصحية والمالية، الأمر الذي يجعل حماية هذه المعطيات امتداداً طبيعياً للحماية المقررة للحياة الخاصة.[1]

كما حرص الدستور على ضمان سرية المراسلات والاتصالات بمختلف أشكالها حيث أكد أن سرية المراسلات والاتصالات الخاصة مضمونة ولا يجوز المساس بها إلا بأمر معلل صادر عن السلطة القضائية المختصة وفي الحالات التي يحددها القانون[2]. وتكتسي هذه الحماية أهمية خاصة في البيئة الرقمية، حيث أصبحت غالبية المعلومات الشخصية متداولة عبر وسائل الاتصال الإلكترونية وشبكات الإنترنت، مما يجعل حماية المراسلات الإلكترونية جزءاً لا يتجزأ من حماية المعلومات الشخصية.

ومن الضمانات الدستورية المهمة كذلك حماية حرمة المسكن باعتباره المجال الذي تتجسد فيه الحياة الخاصة للفرد بصورة واضحة وقد أقر الدستور عدم جواز انتهاك حرمة المسكن أو إجراء أي تفتيش داخله إلا وفق الشروط والإجراءات التي يحددها القانون، وتزداد أهمية هذه الحماية في مجال التفتيش الإلكتروني بالنظر إلى احتواء المساكن على أجهزة الحاسوب والهواتف الذكية والوسائط الإلكترونية التي تختزن كما هائلا من البيانات الشخصية والمعلومات الخاصة[3].

وإلى جانب ذلك كرس الدستور مبدأ خضوع كل تقييد للحقوق والحريات للشرعية القانونية والرقابة القضائية، فلا يجوز المساس بالحقوق الأساسية للأفراد إلا بناء على نص قانوني يحدد الحالات والإجراءات والضمانات اللازمة لذلك[4]. ويُعد هذا المبدأ ضمانة أساسية للحيلولة دون التعسف في استعمال سلطات التفتيش أو المراقبة الإلكترونية، لاسيما عندما يتعلق الأمر بالوصول إلى البيانات الشخصية المخزنة في الأنظمة المعلوماتية.

---

[1] المادة 47 الفقرة 3 من دستور 2020.

[2] المادة 47 من دستور 2020.

[3] صالح بوزاية، الحماية الجنائية للحق في السر والحق في الحياة الخاصة في التشريع الجزائري، مذكرة ماجستير، كلية الحقوق، جامعة 20 اوت 1955، سكيكدة، 2011-2012، ص 74.

[4] المادة 34 من دستور 2020.

كما أقر الدستور حق الأفراد في اللجوء إلى القضاء للدفاع عن حقوقهم وحرياتهم الأساسية، بما في ذلك الحقوق المرتبطة بالحياة الخاصة وحماية البيانات الشخصية. وتبرز أهمية هذه الضمانة في تمكين الأفراد من مواجهة أي اعتداء يقع على معلوماتهم الشخصية والمطالبة بإزالة آثاره والحصول على التعويض المناسب عند الاقتضاء[1].

وفي إطار مواكبة التطورات الرقمية، عزز المؤسس الدستوري الحماية الدستورية للمعلومات الشخصية من خلال النص صراحة في المادة 47 من دستور 2020 على أن حماية الأشخاص الطبيعيين عند معالجة المعطيات ذات الطابع الشخصي حق أساسي[2]. ويُعد هذا المقتضى من أبرز المستجدات الدستورية إذ نقل حماية البيانات الشخصية من نطاق الحماية الضمنية المستمدة من الحق في الحياة الخاصة إلى نطاق الحماية الدستورية المباشرة، بما يعكس إدراك المشرع لأهمية المعطيات الشخصية في المجتمع الرقمي المعاصر.

ويتضح من خلال هذه الضمانات أن الدستور الجزائري لم يكتفِ بتقرير الحق في الخصوصية المعلوماتية، بل أحاطه بمنظومة متكاملة من الضمانات الدستورية الرامية إلى حماية المعلومات الشخصية من مختلف صور الاعتداء، سواء تعلق الأمر بالمساس بالحياة الخاصة أو سرية المراسلات أو حرمة المسكن أو معالجة البيانات الشخصية بطرق غير مشروعة، وهو ما يشكل الأساس الذي تقوم عليه مختلف صور الحماية القانونية والجزائية المقررة لهذه المعلومات.[3]

المطلب الثاني: الحماية الجزائية للمعلومات الشخصية

[1] فريد روانج، ضمانات حرمة الحياة الخاصة أثناء إجراءات مراقبة الاتصالات الإلكترونية، مجلة الأبحاث القانونية والسياسية، جامعة سطيف 2، المجلد 02، العدد 02، سنة 2020، ص 7.

[2] المادة 4/47 من دستور 2020.

[3] محمد أمين أحمد الشوابكة، الجرائم المعلوماتية، (دراسة مقارنة)، دار الثقافة للنشر والتوزيع، عمان (الأردن)، ط1، 2011، ص 112.

تُعد الحماية الجزائية للمعلومات الشخصية من أبرز الآليات القانونية التي أقرها المشرع الجزائري لضمان احترام الحياة الخاصة وصون سرية البيانات ذات الطابع الشخصي، وذلك من خلال تجريم مختلف الأفعال التي تمس بالمعلومات الشخصية أو تؤدي إلى إفشائها أو معالجتها بغير وجه مشروع، ولم يقتصر دور القانون على إقرار الحق في الخصوصية فحسب، بل عززه بجملة من النصوص العقابية والضمانات الإجرائية الرامية إلى توفير حماية فعالة للأفراد في البيئة الرقمية [1].

وهذا ما سنوضحه من الخلال الفرعين التاليين:

الفرع الأول: الحماية الجزائية للمعلومات الشخصية في قانون العقوبات الجزائري.

الفرع الثاني: الحماية الجزائية للمعلومات الشخصية في القوانين الخاصة.

الفرع الأول: الحماية الجزائية للمعلومات الشخصية في قانون العقوبات الجزائري

على الرغم أن قانون العقوبات الجزائري لم يضع تنظيما خاصا ومتكاملا لحماية البيانات الشخصية في صورها الحديثة، إلا أن أحكامه تضمنت عدداً من النصوص التي يمكن الاستناد إليها لتوفير حماية جنائية لهذه البيانات، سواء من خلال القواعد التقليدية المتعلقة بحماية الأسرار، أو من خلال النصوص المستحدثة الخاصة بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

أولا: الحماية من خلال تجريم إفشاء الأسرار:

أخضع المشرع الجزائري بعض فئات الأشخاص الذين تقتضي طبيعة وظائفهم أو مهنهم الاطلاع على أسرار الغير لالتزام قانوني بالمحافظة على سريتها، حيث نصت المادة 301 [2]من قانون العقوبات على معاقبة كل من يفشي سرا أؤتمن عليه بحكم مهنته أو وظيفته في

[1] أحمد فتحي سرور، الحماية الدستورية للحقوق والحريات، مطابع الشروق، القاهرة، 2000، ص 731.

[2] المادة 301 من امر رقم 66-156 مؤرخ في 18 صفر 1386، الموافق ل 8 يونيو 1966، يتضمن قانون العقوبات المعدل والمتمم، الجريدة الرسمية العدد 48، الصادرة بتاريخ 11 يونيو 1966.

غير الأحوال التي يجيزها أو يفرضها القانون، ويستند هذا التجريم إلى فكرة حماية الثقة المشروعة التي يضعها الأفراد في الأشخاص الذين يطلعون على معلوماتهم الخاصة بحكم وظائفهم أو مهنهم.

غير أن التطور التكنولوجي واتساع نطاق تداول البيانات الشخصية عبر الأنظمة المعلوماتية أظهر محدودية هذه الحماية التقليدية، إذ ان نطاقها يظل مقصورا على الأسرار المهنية أو الوظيفية، في حين أن البيانات الشخصية المعالجة إلكترونيا قد لا تندرج دائما ضمن مفهوم السر المهني، الأمر الذي دفع جانبا من الفقه إلى التشكيك في قدرة هذه النصوص على توفير حماية فعالة لمختلف صور البيانات الشخصية المتداولة في البيئة الرقمية[1]

ثانيا: الحماية من خلال تجريم المساس بأنظمة المعالجة الآلية للمعطيات

وعياً منه بالمخاطر التي أفرزتها الثورة الرقمية، عمد المشرع الجزائري إلى تدعيم الحماية الجنائية للمعطيات الإلكترونية من خلال استحداث أحكام خاصة بالجرائم المعلوماتية ضمن قانون العقوبات، وفي هذا الإطار جرمت المواد من 374 مكرر الى 394 مكرر7 الأفعال الماسة بأنظمة المعالجة الالية للمعطيات المتعلقة بالدخول او البقاء غير المشروع الى النظم المعلوماتية و تصميم أو تجميع أو توفير أو نشر أو الاتجار في معطيات معلوماتية يمكن استخدامها في ارتكاب الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، كما جرمت حيازة تلك المعطيات أو إفشاءها أو استقبالها أو نشرها متى تم ذلك بطريق الغش.

وتتجلى أهمية هذه النصوص في كونها توفر حماية للبيانات الشخصية المخزنة أو المعالجة أو المتداولة إلكترونيا، باعتبارها جزءا من المعطيات التي تستهدفها الجرائم المعلوماتية، غير أن هذه الحماية تظل محدودة النطاق، لكونها تنصرف أساساً إلى بعض صور الاعتداء المرتبطة بالإفشاء أو النشر أو التداول غير المشروع للمعطيات، دون أن تشمل جميع الأفعال التي قد تمس بالبيانات الشخصية في مراحل جمعها أو معالجتها أو استغلالها.

[1] محمد امين أحمد شوابكة، مرجع سابق، ص104.

أولا: الدخول غير المشروع إلى النظام المعلوماتي

يقصد بالدخول غير المشروع كل ولوج أو اتصال يتم بنظام المعالجة الآلية للمعطيات دون ترخيص قانوني أو خارج حدود الترخيص الممنوح، ويستوي في ذلك أن يتم الدخول بصورة مباشرة عبر التعامل المادي مع الجهاز المعلوماتي، أو بصورة غير مباشرة عن طريق شبكات الاتصال الحديثة والإنترنت ولم يقيد المشرع الجزائري وسائل ارتكاب هذا الفعل، مما يجعل الجريمة قائمة مهما كانت الوسيلة المستعملة للوصول غير المشروع إلى النظام؛ سواء باستعمال كلمات المرور الخاصة بالغير أو من خلال برامج وتقنيات الاختراق المختلفة[1].

ويمتد نطاق الحماية القانونية ليشمل مختلف صور الدخول غير المشروع بغض النظر عن الحدود الجغرافية أو المكانية، إذ يمكن أن يتحقق الاختراق من أي مكان متصل بالشبكة المعلوماتية، وفي هذا السياق أكدت محكمة استئناف باريس في قرارها الصادر بتاريخ 5 أفريل 1994 أن مفهوم الدخول غير المشروع يستوعب جميع أشكال الولوج غير القانوني إلى أنظمة المعالجة الآلية للمعطيات، ولو تم ذلك عن بُعد بواسطة حاسب آلي متصل بالنظام المستهدف[2].

كما لا يشترط أن ينصب الدخول على كامل النظام المعلوماتي، او أن يرد على جزء منه، وهو ما يستفاد من نص المادة 394 مكرر التي تتحدث عن دخول "كل أو جزء من منظومة". وعليه، فإن الولوج إلى برنامج معين أو قاعدة بيانات محددة أو جزء من مكونات النظام يكفي لقيام الجريمة متى كان هذا الجزء داخلاً في نطاق المنظومة المعلوماتية محل الحماية.[3]

---

[1] أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي (الحماية الجنائية للحاسب الآلي)، دراسة مقارنة، رسالة دكتوراه، قسم القانون الجنائي، كلية الحقوق، جامعة طنطا، مصر، 2000، ص 304.

[2] محكمة استئناف باريس، قرار بتاريخ 5 أفريل 1994، القضاء الفرنسي.

[3]. Raymond Gassin, informatique (fraude informatique), répertoire pénal, Dalloz, octobre1995, n°108, p18.

وتكمن أهمية هذا التجريم في حماية المعلومات الشخصية المخزنة داخل الأنظمة المعلوماتية من خطر الوصول غير المصرح به، إذ إن مجرد تمكين الجاني من الولوج إلى النظام قد يتيح له الاطلاع على البيانات الشخصية أو نسخها أو تعديلها أو استغلالها بصورة غير مشروعة. ولهذا تعد جريمة الدخول غير المشروع من الجرائم الشكلية التي تتحقق بمجرد حصول الولوج غير المصرح به دون اشتراط وقوع ضرر فعلي بالبيانات أو بالنظام المعلوماتي[1].

ثانياً: البقاء غير المشروع داخل النظام المعلوماتي:

إلى جانب تجريم الدخول غير المشروع، جرم المشرع الجزائري فعل البقاء غير المشروع داخل النظام المعلوماتي، وهو السلوك الذي يتحقق عندما يستمر الشخص في التواجد داخل النظام رغم انتفاء السند القانوني الذي يبرر وجوده، وتبرز أهمية هذه الصورة في الحالات التي يكون فيها الدخول الأول مشروعا أو عرضيا، ثم يتحول لاحقا إلى وجود غير مشروع بسبب تجاوز حدود الترخيص أو استمرار الاتصال بالنظام رغم العلم بعدم أحقيته في ذلك.[2]

وقد كرست التشريعات المقارنة القاء غير المشروع في النظم المعلوماتية حيث عاقب القانون الفرنسي على البقاء داخل نظام المعالجة الآلية للمعطيات بعد الدخول إليه بطريق الخطأ متى استمر الشخص في التواجد داخله رغم علمه بعدم أحقيته في ذلك، كما اعتبرت محكمة النقض الفرنسية أن الاستمرار في استعمال وسائل الدخول إلى قاعدة البيانات بعد انتهاء مدة الترخيص الممنوح يشكل صورة من صور البقاء غير المشروع المعاقب عليه قانوناً[3].

وتتجلى أهمية تجريم هذا السلوك في توفير حماية فعالة للمعلومات الشخصية، لأن استمرار الجاني داخل النظام المعلوماتي يمكن أن يمكنه من الوصول إلى كم كبير من البيانات

[1] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، مرجع سابق، ص 314.

[2] محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، الطبعة الثانية، القاهرة، 1998، ص206.

[3] . Cass Crim., 3 octobre 2007, pourvoi n ° 07-81045, disponible sur le site, https://www.legifrance.gouv.fr visiter le 20/05/2026 à 11:30.

الشخصية المخزنة أو المعالجة داخله، وهو ما يزيد من احتمالات الاعتداء عليها أو استغلالها بطرق غير مشروعة[1].

ثالثاً: الجزاء المقرر لحماية الأنظمة المعلوماتية الحاضنة للمعلومات الشخصية:

أحاط المشرع الجزائري جرائم الدخول والبقاء غير المشروع داخل الأنظمة المعلوماتية بجملة من الجزاءات الجنائية الرامية إلى توفير حماية فعالة للبيانات والمعطيات المخزنة داخلها، حيث قررت المادة 394 مكرر من قانون العقوبات عقوبة الحبس من ثلاثة أشهر إلى سنة وغرامة مالية من 50.000 دج إلى 100.000 دج[2].

كما دعم المشرع هذه الحماية بعقوبات تكميلية نصت عليها المادة 394 مكرر 6، تتمثل في مصادرة الأجهزة والبرامج والوسائل المستعملة في ارتكاب الجريمة، فضلاً عن غلق المواقع أو أماكن الاستغلال التي استخدمت في النشاط الإجرامي متى توافرت الشروط القانونية لذلك، مع المحافظة على حقوق الغير حسن النية[3].

رابعاً: تجريم الأعمال التحضيرية والشروع

لم يقتصر المشرع على معاقبة الجريمة التامة، بل وسع نطاق الحماية الجزائية ليشمل المراحل السابقة على تنفيذها، إدراكاً منه لخطورة الجرائم المعلوماتية وما قد يترتب عليها من تهديد للمعلومات الشخصية.[4] ولهذا جرم الأعمال التحضيرية المتعلقة بالإعداد لارتكاب الجرائم

---

[1] علي عبد القادر القهوجي، الحماية الجنائية للمعطيات المعالجة آلياً، مجلة الشريعة والقانون، تصدر عن جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، المجلد الثاني، الطبعة الثالثة، 2004، ص 601.

[2] المادة 394 مكرر من امر رقم 66-156، يتضمن قانون العقوبات المعدل والمتمم، مرجع سابق.

[3] المادة 394 مكرر 6 من امر رقم 66-156، يتضمن قانون العقوبات المعدل والمتمم، مرجع نفسه.

[4] . Jean Devése, atteintes aux systèmes de traitement automatisé de données, Juris Classeur, pénal, article (323 1 à 323-7) ,2, 1997, p 16, n°75.

الماسة بأنظمة المعالجة الآلية للمعطيات متى تجسدت في أفعال مادية ملموسة، وذلك بموجب المادة 394 مكرر 5 من قانون العقوبات.[1]

كما سوى المشرع بين الجريمة التامة والشروع فيها من حيث العقاب بموجب المادة 394 مكرر 7، بما يعكس رغبته في توفير حماية استباقية للأنظمة المعلوماتية وما تحتويه من معلومات شخصية، وردع مختلف صور الاعتداء عليها قبل تحقق النتيجة الإجرامية بصورة كاملة .[2]

الفرع الثاني: الحماية الجزائية للمعلومات الشخصية في القوانين الخاصة

أمام قصور القواعد التقليدية عن استيعاب مختلف المخاطر التي تهدد البيانات الشخصية في البيئة الرقمية، اتجه المشرع الجزائري إلى تبني نصوص خاصة ترمي إلى إرساء حماية قانونية أكثر فعالية للمعطيات ذات الطابع الشخصي، وذلك من خلال إخضاع عمليات جمعها ومعالجتها وتخزينها ونقلها لجملة من الضوابط القانونية التي يؤدي الإخلال بها إلى قيام المسؤولية الجزائية.

1 -القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي:

يشكل هذا القانون الإطار التشريعي الأساسي لحماية البيانات الشخصية في الجزائر، إذ جاء استجابة للتطورات التقنية المتسارعة وما ترتب عنها من مخاطر متزايدة على الخصوصية المعلوماتية للأفراد، وقد كرس المشرع من خلاله مجموعة من المبادئ الجوهرية التي تحكم معالجة المعطيات ذات الطابع الشخصي في مقدمتها مبدأ رضا الشخص المعني بالمعالجة، ومبدأ مشروعية المعالجة، ومبدأ تحديد الغرض منها، ومبدأ دقة البيانات وتحيينها،

[1] المادة 394 مكرر 5 من امر رقم 66-156، يتضمن قانون العقوبات المعدل والمتمم، مرجع سابق.

[2] المادة 394 مكرر 7 من امر رقم 66-156، يتضمن قانون العقوبات المعدل والمتمم، المرجع نفسه.

فضلاً عن ضرورة الاحتفاظ بها خلال المدة اللازمة فقط لتحقيق الأهداف التي جُمعت من أجلها[1].

ولتعزيز فعالية هذه الحماية، ألزم المشرع المسؤول عن المعالجة باحترام مجموعة من الإجراءات والالتزامات القانونية، من بينها التصريح المسبق لدى السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي وفقاً للمادة 14 من القانون، كما أخضع بعض عمليات المعالجة لنظام الترخيص المسبق بموجب المادة 17 متى كانت من شأنها المساس بالحياة الخاصة للأفراد أو تعريض حقوقهم وحرياتهم للخطر، بما يجعل مخالفة هذه الضوابط أساساً للمساءلة الجزائية[2].

2 -القانون رقم 88-09 المتعلق بالأرشيف الوطني:

امتدت الحماية الجزائية للمعلومات الشخصية إلى المجال الأرشيفي، حيث حرص المشرع على تحقيق التوازن بين حق المجتمع في الاطلاع على الوثائق التاريخية وضرورة احترام الحياة الخاصة للأفراد، ولهذا الغرض قيد الاطلاع على بعض الوثائق التي تتضمن معلومات ذات صلة بالحياة الخاصة، فنصت المادة 10 من قانون الأرشيف الوطني على عدم جواز الاطلاع على بعض المعلومات القضائية إلا بعد انقضاء مدة خمسين سنة من غلق المل[3] .

كما أولى المشرع عناية خاصة للمعطيات الطبية بالنظر إلى حساسيتها، ومنع الكشف عنها قبل مرور مائة سنة من تاريخ ميلاد الشخص المعني بها[4]، وهو ما يعكس حرصه على

---

[1] القانون رقم 18-07 المؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية، العدد 34، الصادرة بتاريخ 12 يونيو 2018.

[2] المادتان 14 و17 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، المرجع نفسه.

[3] القانون رقم 88-09 المؤرخ في 7 جمادى الثانية عام 1408 الموافق 26 يناير سنة 1988، المتعلق بالأرشيف الوطني، الجريدة الرسمية للجمهورية الجزائرية، العدد 4، الصادرة بتاريخ 27 يناير 1988.

[4] المادة 10 من القانون رقم 88-09، مرجع نفسه.

توفير حماية ممتدة زمنياً للبيانات المرتبطة بالحياة الخاصة. كما عزز هذه الحماية من خلال المادة 67 التي تحظر نقل بعض الوثائق والمحفوظات المتعلقة بالحياة الخاصة للأفراد خارج الإطار الذي يحدده القانون.[1]

[1] المادة 67 من القانون رقم 88-09 المتعلق بالأرشيف الوطني، المرجع نفسه.

المبحث الثاني: التفتيش الالكتروني كاستثناء مشروع على حرمة الحياة الخاصة

أدى التطور المتسارع في تكنولوجيا المعلومات والاتصال إلى ظهور أنماط جديدة من الجرائم التي ترتكب عبر الوسائط الإلكترونية، الأمر الذي فرض على التشريعات الحديثة مواكبة هذه التحولات من خلال إقرار آليات قانونية حديثة تمكن السلطات المختصة من كشف هذه الجرائم وملاحقة مرتكبيها،[1] ومن بين أهم هذه الآليات التفتيش الإلكتروني الذي يعد وسيلة إجرائية تهدف إلى البحث عن الأدلة الرقمية داخل الأنظمة المعلوماتية ووسائط التخزين المختلفة،[2] وعليه يقتضي الأمر الوقوف على مفهوم التفتيش الإلكتروني وتحديد الإطار القانوني، وهو ما سيتم التطرق إليه في هذا المبحث من خلال مطلبين، المطلب الأول وهو تعريف التفتيش الالكتروني والمطلب الثاني الطبيعة القانونية للتفتيش الالكتروني.

المطلب الأول: تعريف التفتيش الالكتروني

التفتيش الإلكتروني من الموضوعات الحديثة التي أفرزها التطور التكنولوجي في مجال تكنولوجيا المعلومات، وقد ارتبط بظهور استخدام الوسائط الرقمية في المجال الجنائي، مما استدعى ضبط مفهومه، ونظرًا لخصوصية البيئة الرقمية، فإنه يثير عدة إشكالات تتعلق بتحديد مفهومه وحدوده ومدى توافقه مع القواعد العامة للتفيش التقليدي ، إضافة إلى علاقته بحماية الحق في الخصوصية، وهو ما يبرز أهمية تعريفه، وهذا ما سنتطرق اليه من خلال الفرع الأول الذي سنتناول فيه مقصود التفتيش الالكتروني، والفرع الثاني الذي سنوضح فيه خصائص التفتيش الالكتروني.

---

[1] أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص: الجرائم ضد الأشخاص، الجرائم ضد الأموال، بعض الجرائم الخاصة، ج1، دار هومة للنشر والتوزيع، الجزائر، 2022، ص 214.

[2] عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، الاسكندرية، مصر، 2006، ص 133.

الفرع الأول: المقصود بالتفتيش الالكتروني

يُعدّ التفتيش من أهم إجراءات التحقيق الابتدائي، باعتباره وسيلة قانونية تهدف إلى البحث عن الأدلة وضبطها بما يساهم في كشف الحقيقة وإثبات الجريمة ونسبتها إلى مرتكبها، وقد ارتبط مفهوم التفتيش تقليديًا بالأماكن المادية والمحلات الملموسة، غير أن التطور التكنولوجي المتسارع وظهور الجرائم المعلوماتية أفرزا صورا جديدة من الأدلة ذات الطبيعة الرقمية، الأمر الذي فرض ضرورة توسيع نطاق هذا الإجراء ليتلاءم مع البيئة الرقمية.

وفي هذا السياق ظهر ما يُعرف بالتفتيش الإلكتروني، باعتباره امتدادا للتفتيش التقليدي، غير انه يتميز بخصوصية تقنية وقانونية تفرضها طبيعة المعطيات الرقمية والأنظمة المعلوماتية[1]. وقد استدعى ذلك إعادة النظر في المفهوم التقليدي للتفتيش، من خلال اعتماد مصطلحات أكثر دقة وانسجاما مع البيئة الرقمية، كالدخول أو الولوج أو النفاذ إلى الأنظمة المعلوماتية، بعدما لم يعد التفتيش مقتصرا على المحل المادي، بل أصبح يشمل البيانات الرقمية والمعطيات الرقمية المخزنة أو المتداولة داخل الأنظمة المعلوماتية.

ورغم هذا التطور، فإن أغلب التشريعات، ومن بينها التشريع الجزائري، لم تتجه إلى وضع تعريف قانوني صريح للتفتيش الالكتروني، تاركة هذه المهمة للفقه والاجتهاد القضائي، وفي هذا الإطار عرف الفقه التفتيش بأنه: «إجراء من إجراءات التحقيق تباشره سلطة مختصة قانونا، ويهدف إلى البحث عن أدلة مادية لجناية أو جنحة ثابتة الوقوع داخل محل خاص يتمتع بالحماية القانونية، وذلك بغض النظر عن إرادة صاحبه».[2]

غير أن هذا التعريف، وإن كان قد أصاب في اعتباره التفتيش إجراء قضائيا يرد على محل يتمتع بالحماية القانونية، إلا أنه لم يعد كافيا لاستيعاب خصوصية الجرائم المعلوماتي،

[1] خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت، دار الثقافة للنشر والتوزيع، الطبعة الأولى، سنة 2011، ص151.

[2] حمداش شمس الدين، البشير بن مبروك، "القواعد الجرائية المقررة لتفتيش المنظومة المعلوماتية في القانون الجزائري"، مجلة صوت القانون، المجل د09، العدد 02، سنة 2023، ص100.

لكونه حصر محل التفتيش في الأدلة المادية فقط، في حين أنّ الدليل في المجال المعلوماتي غالبا ما يكون ذا طبيعة معنوية يتمثل في بيانات ومعلومات مخزنة داخل الدعائم والأنظمة الرقمية.

ويُعد التفتيش الإلكتروني من أخطر إجراءات التحقيق، لما قد يترتب عليه من مساس بحقوق الأفراد وحرياتهم الأساسية، خاصة الحق في الخصوصية وحرمة الحياة الخاصة وسرية المعطيات الشخصية، وهي حقوق كفلتها الدساتير والتشريعات الوطنية والدولية بالحماية. لذلك لا يجوز اللجوء إلى هذا الإجراء إلا في الحدود التي تقتضيها مصلحة التحقيق، وبالقدر اللازم لجمع الأدلة والتحقيق، مع إخضاعه لجملة من الضوابط والإجراءات القانونية التي تكفل تحقيق التوازن بين مقتضيات البحث والتحري من جهة، وضمان حماية الحقوق والحريات الفردية من جهة أخرى.[1]

وفي هذا الإطار، أجاز المشرّع الجزائري في المادة 5 من القانون 04/09[2] المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على جواز قيام السلطات القضائية المختصة، وكذا ضباط الشرطة القضائية، بالدخول بغرض التفتيش إلى منظومة معلوماتية أو منظومة لتخزين المعطيات، والاطلاع على البيانات المخزنة بها، كما أجاز النص أن يتم هذا التفتيش سواء في مكان ارتكاب الجريمة أو عن بعد، وهو ما يعكس تطور مفهوم التفتيش ليتلاءم مع البيئة الرقمية وخصوصياتها.

يُقصد بالتفتيش عن بعد ذلك الإجراء الذي تباشره الجهة المختصة قانونا، سواء كان ضابط الشرطة القضائية أو قاضي التحقيق من مقر عمله، باستخدام وسائل وبرامج معلوماتية متخصصة عبر البيئة الرقمية، بما يتيح له البحث عن أدلة الجريمة دون الحاجة إلى الانتقال المادي إلى مكان وجود محل التفتيش.

---

[1] زيدان زيبحة، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة، الجزائر، 2011، ص130.

[2] القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، الصادر سنة 2009.

ويُعد هذا الإجراء صورة مستحدثة من صور التفتيش، حيث يتم تنفيذه داخل بيئة معلوماتية، ويستهدف الولوج إلى الأنظمة أو وسائل تخزين المعطيات، قصد ضبط الأدلة الرقمية المخزنة بها، وهو بذلك يختلف عن التفتيش التقليدي من حيث وسيلته ومجاله، دون أن يخرج عن طبيعته كإجراء من إجراءات التحقيق التي تخضع لضوابط قانونية محددة.

كما يقوم التفتيش عن بعد على فكرة البحث أو الاطلاع الدقيق على محل يتمتع بحماية قانونية خاصة، باعتباره مستودعا لأسرار صاحبه سواء تعلق الأمر بجهاز حاسوب أو شبكة معلوماتية، وهو ما يفرض ضرورة مراعاة الضمانات القانونية الكفيلة بحماية الحياة الخاصة والمعطيات الشخص.[1]

ويتميز هذا النوع من التفتيش بسرعة الوصول إلى البيانات، لكنه يثير في المقابل إشكالات قانونية معقدة، أبرزها مسألة الاختصاص القضائي عندما تكون البيانات خارج الإقليم الوطني، وهو ما يمس بمبدأ السيادة الرقمية للدولة[2].

كما يطرح هذا النوع من التفتيش خطر المساس بالبيانات الشخصية غير المرتبطة بالجريمة، نظرًا لاتساع نطاق المعطيات الرقمية، مما يستدعي ضرورة حصر التفتيش في نطاق محدد بدقة مسبقة[3].

ومن الناحية القانونية، يتطلب هذا الإجراء إذنًا قضائيًا صريحًا ومحددًا، مع رقابة صارمة على التنفيذ، لضمان عدم تحوله إلى وسيلة للاطلاع العشوائي على المعطيات الشخصية للأفراد[4].

---

[1] علي حسن محمد الطوالبة، التفتيش الجنائي عن نظم الحاسوب والأنترنيت، الطبعة الأولى، عالم الكتب الحديث، الاردن، 2004، ص442.

[2] أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، ج2، دار هومة، 2019، ص340.

[3] علي حسن الطوالبة، مرجع سابق، ص233.

[4] مرجع نفسه، ص235.

كما أن الاتجاه الحديث في الفقه الجنائي يدعو إلى وضع إطار تشريعي خاص بهذا النوع من التفتيش، نظرًا لخصوصيته التقنية وعدم كفاية القواعد التقليدية لضبطه

الفرع الثاني: خصائص التفتيش الالكتروني

يُعد التفتيش الإلكتروني صورة مستحدثة من إجراءات التحقيق، أفرزها تطور البيئة الرقمية وخصوصية الجرائم المعلوماتية، وبالنظر لاختلافه عن التفتيش التقليدي من حيث المحل والوسيلة، فإنه يتميز بجملة من الخصائص التي تعكس طبيعته التقنية وتطرح تحديات قانونية خاصة، وعليه يقتضي الأمر الوقوف على أهم هذه الخصائص لبيان مميزاته وحدود ممارسته.

أولا: خصائص التفتيش الالكتروني من حيث الابعاد القانونية:

بالنظر لخصوصية التفتيش الواقع على المنظومة المعلوماتية وتعقيده يستلزم الأمر توضيح خصائص ومميزاته وتحديد أبعاده وأنظمته القانونية

1- الجبر والاكراه:

يعد التفتيش الإلكتروني من الإجراءات التي تباشر بقوة القانون، ويتضمن قدرا من الجبر والإكراه المشروع الواقع على المتهم، وقد تقتضي الضرورة القانونية إخضاع الأجهزة الإلكترونية أو الشبكات المعلوماتية للتفتيش دون اشتراط الحصول على موافقة مسبقة من صاحبها، بل قد يتم ذلك رغما عن إرادته متى استوفت العملية للشروط والضوابط القانونية المقررة بما يضمن مشروعية الإجراء وحماية الحقوق والحريات.[1]

غير أن هذه الحرمة قد تقيّد بموجب سلطة الجبر والإكراه التي تمارسها النيابة العامة، وفق ما يقره القانون تحقيقا للتوازن بين حرية الأفراد الشخصية من جهة، وحق المجتمع في

[1] سعاد راضي حسين، "الإجراءات الجزائية في تفتيش محل الجرائم الإلكترونية"، مجلة الشرق الأوسط للدراسات القانونية والفقهية، المجلد 04، ع04، 2024، جامعة ذي قار، العراق، ص125.

العقاب وصون مصالحه التي قد تتعرض للانتهاك بفعل جرائم المعلوماتية من جهة أخرى، حيث يتم التفتيش في هذه الحالة استنادا إلى القانون وضمن ضمانات إجرائية محددة.

أما إذا تم التفتيش برضا الشخص المعني، فإننا نكون بصدد حالة تنازل عن الحماية القانونية المقررة له وهو ما يفقد الإجراء أحد أهم خصائصه وهي صفة الجبر والإكراه.

وبناء على ذلك لا يجوز للمتهم الدفع ببطلان التفتيش في هذه الحالة، لكونه لم يتحقق أصلًا بالمعنى القانوني للإجراء.[1]

2 – البحث عن الدليل الرقمي:

يعد البحث عن الدليل الرقمي من أبرز خصائص التفتيش الالكتروني، إذ لا يمكن إدانة المتهم بجريمة معينة دون دليل يثبت ارتكابها، ويتميز التفتيش في المنظومة المعلوماتية بطابعه الإلكتروني الخاص، إذ يتناول بيانات ذات طبيعة رقمية محفوظة داخل وسائط تخزين رقمية، مثل الأقراص الصلبة، والهواتف الذكية، والحواسيب، إضافة إلى الشبكات المعلوماتية، ويختلف هذا النوع من التفتيش عن التفتيش التقليدي، كونه يتعلق بمحتوى غير مادي وذي طبيعة خاصة يتمثل في المعلومات والبيانات الرقمية.

وتتسم هذه البيانات بقابلية عالية للتغيير أو الإتلاف أو الحذف خلال فترات زمنية وجيزة جدا، مما يجعل عملية تتبعها أو استرجاعها أكثر صعوبة وتعقيدا، ويستدعي ذلك اعتماد تقنيات وأساليب تحقيق متطورة تتناسب مع خصوصية البيئة الرقمية.[2]

ويُلاحظ أن التفتيش في صورته الرقمية يستلزم قواعد إجرائية تتلاءم مع طبيعته الخاصة، نظرا لعدم إمكانية تطبيق القواعد الإجرائية التقليدية عليه بشكل مباشر، خاصة فيما يتعلق

2 سامي جلال فقي، التفتيش في الجرائم الإلكترونية دراسة تحليلية، الطبعة الاولى، دار الكتب القانونية، القاهرة، 2012، ص5.

[2] حمداش شمس الدين، البشير بن مبروك، مرجع سابق، ص 100

بمساسه بحرية المتهم وخصوصية البيانات الإلكترونية، الأمر الذي يقتضي وضع إطار قانوني أكثر دقة وصرامة يراعي خصوصية الدليل الإلكتروني وطبيعته غير المادية. [1]

3- المساس بحق الأشخاص في السر:

ينطوي التفتيش الالكتروني خاصة في الجرائم المعلوماتية على مساس مباشر بحرية المتهم الشخصية وبسرية بياناته ومعلوماته الرقمية، سواء كانت مخزنة على جهاز الحاسوب، أو محفوظة داخل برامج خاصة، أو متداولة عبر البريد الإلكتروني، أو متاحة على شبكة الإنترنت، ويُعزى ذلك إلى أن الجريمة المعلوماتية تقوم أساسا على كل فعل ينطوي على استخدام وسائل تقنية المعلومات أو النظام المعلوماتية أو شبكة معلوماتية، بصورة غير مشروعة، وبما يخالف أحكام القانون.

وعلى الرغم من أن التفتيش الالكتروني يعد قيدا على حرمة المساكن وسرية المعلومات الشخصية، حيث يمتد إلى تفتيش الأماكن المادية بحثا عن الأدلة الرقمية داخل الأجهزة المعلوماتية الموجودة فيها، كما يمكن يتخذ طابعا أكثر تطورا وتعقيدا، يتمثل في التفتيش عن بعد من خلال اختراق الشبكات المعلوماتية والحواسيب والبريد الإلكتروني، ويُطلق على هذا النوع من الإجراءات مصطلح "التفتيش على الخط"، ويباشر وفق تقنيات وأساليب تحقيق جنائي فني متخصصة، من قبل أشخاص ذوي خبرة في معالجة البيانات والأنظمة المعلوماتية.[2]

ثانيا: خصائص التفتيش الالكتروني من حيث الاسس القانونية:

1 -من حيث وسائل التفتيش الالكتروني

يمتاز التفتيش الإلكتروني بكونه وسيلة للبحث عن المعنوية للجريمة وضبطها، بما يسهم في الوصول إلى الحقيقة وإثبات الوقائع الجنائية، ويقوم هذا النوع من التفتيش على

2 محمد راشد أحمد الظنحاني، التفتيش في الجرائم الإلكترونية، دار النهضة العلمية للنشر والتوزيع، الطبعة الأولى، 2017، ص36.

1 رضا هميسي، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، العدد 5، جوان 2012، ص16.

توظيف تقنيات المعلومات، أي كل وسيلة مادية أو غير مادية، أو مجموعة من الوسائل المترابطة أو غير المترابطة، المخصصة لتخزين المعلومات وتنظيمها وترتيبها واسترجاعها ومعالجتها وتطويرها وتبادلها، وفقا للأوامر والتعليمات المبرمجة داخلها.[1]

ويشمل ذلك مختلف المدخلات والمخرجات المرتبطة بالنظام المعلوماتي أو بالشبكة المعلوماتية، سواء كانت سلكية أو لاسلكية، بما يتيح الإحاطة بمختلف البيانات المتداولة داخل هذه الأنظمة، والتي قد تكون محلًا أو وسيلة لارتكاب الجريمة الإلكترونية أو لإثباتها.[2]

2- من حيث مجال التفتيش الالكتروني:

ينصب التفتيش الإلكتروني من حيث خصوصياته على الوظائف المعلوماتية المرتبطة بالنظم والشبكات المعلوماتية، حيث تعد الشبكة المعلوماتية ارتباطا بين أكثر من وسيلة تقنية للمعلومات بغرض الحصول عليها وتبادلها، بما في ذلك الشبكات الخاصة والعامة، والشبكة العالمية "الإنترنت"، إضافة إلى المواقع الإلكترونية باعتبارها فضاءات لإتاحة البيانات أو معالجتها أو تداولها على الشبكة المعلوماتية، وذلك بهدف الكشف عن الأدلة المادية والمعنوية للجريمة وضبطها[3].

وفي هذا السياق، سعى المشرع من خلال القانون رقم 04/09 إلى تحديد الأبعاد التي ينصب عليها التفتيش الإلكتروني، وذلك عبر تقديم بعض المفاهيم الاصطلاحية، حيث نصت المادة 02 منه على أنه: "يقصد في مفهوم هذا القانون ما يلي: الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وهي جرائم المساس بالأنظمة المعالجة الآلية للمعطيات المحددة في قانون

2 طارق ابراهيم الدسوقي عطية، الموسوعة الأمنية: الامن المعلوماتي، النظام القانوني لحماية المعلوماتية، دار الجامعة الجديدة، الإسكندرية، مصر، 2015، ص240.

[2] مرجع نفسه، ص 240.

[3] امال عبد الرحيم عثمان، شرح قانون الإجراءات الجنائية، الهيئة المصرية العامة للكتاب، القاهرة، الطبعة الثانية، 1991، ص62.

العقوبات، وأي جريمة أخرى تُرتكب أو يسهَل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.

المطلب الثاني: الطبيعة القانونية للتفتيش الالكتروني وانواعه.

يعد التفتيش الإلكتروني من الإجراءات الحديثة التي استحدثها التطور التكنولوجي وانتشار استخدام الأنظمة المعلوماتية في مختلف مجالات الحياة، ونظرا لخصوصيته فقد أثار هذا الإجراء العديد من النقاشات الفقهية حول تكييفه القانوني وطبيعته، ولفهم الإطار القانوني الذي يحيط بهذا الإجراء، يجدر الوقوف على طبيعته القانونية (الفرع الأول)، كما يستدعي الأمر بيان أنواعه التي يمكن أن يتخذها في المجال الرقمي (الفرع الثاني).

الفرع الأول: الطبيعة القانونية للتفتيش الالكتروني.

انقسم الفقه في تحديده للطبيعة القانونية للتفتيش الى أربعة اتجاهات واستند كل اتجاه على معيار معين، وهو ما نبينه فيما يلي:

الاتجاه الأول: ويستند أصحاب هذا الاتجاه في تحديدهم للطبيعة القانونية للتفتيش إلى المعيار الوظيفي المتمثل في الغاية منه؛ إذ يرى هذا التيار أن جوهر الإجراء يكمن في الحصول على الأدلة الجرمية وضبطها، والعمل على كشف الحقيقة من خلال إزالة حالة الغموض التي قد تحيط بالواقعة، تمهيدا لترجيح نسبتها إلى شخص معين، ويبرز ذلك بوضوح في مجال الجرائم المعلوماتية من خلال إجراءات ضبط البرامج غير المشروعة المخزنة على جهاز الحاسوب الخاص بالمتهم، وتقديمها كدليل اتهام مادي وقانوني ضده أمام الجهة القضائية المختصة[1].

[1] كيحول عبد القادر، التفتيش الالكتروني كإجراء للتحقيق في الجرائم المعلوماتية، مذكرة ماستر، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة، الجزائر، 2019، ص18.

الاتجاه الثاني: يربط أنصار هذا الاتجاه التكييف القانوني للتفتيش بالمرحلة الإجرائية التي تمر بها الدعوى العمومية؛ فوفقا لهذا الطرح يكتسب التفتيش طبيعته من وقت اتخاذه، فإذا بوشر في مرحلة البحث والتحري التي تسبق تحريك الدعوى العمومية، فإنه يصنف ضمن أعمال الاستدلال، أما في حال مباشرته بعد تحريك الدعوى العمومية ودخولها مرحلة التحقيق الابتدائي، فإنه يكتسب حينئذ صفة إجراء من إجراءات التحقيق[1].

غير أن هذا الاتجاه يصطدم بصعوبات عملية في فضاء الجرائم المعلوماتية؛ نظرا لما تفرضه بعض الإجراءات الإجرائية، كالتنصت أو التجسس الرقمي، من ضرورة قصوى للسرعة في تحري الأدلة وضبطها قبل تلاشيها، وهو الأمر الذي قد يستدعي تخويل جهات الضبط القضائي صلاحيات أوسع لمباشرة التفتيش في الحالات الطارئة والملحة، دون انتظار الإجراءات الروتينية لتحريك الدعوى الجزائية [2].

الاتجاه الثالث: يرتكز هذا الاتجاه في تحديد الطبيعة القانونية للتفتيش على صفة الجهة القائمة بالإجراء؛ إذ يذهب أنصاره إلى أن التفتيش لا يكتسب صفة «إجراء التحقيق» إلا إذا باشرته سلطة التحقيق المختصة قانونا دون غيرها، وبمفهوم المخالفة فإن قيام أي جهة أخرى بهذا الإجراء يخرجه من نطاق أعمال التحقيق غير أن هذا الرأي واجه انتقادات فقهية، تأسيسا على أن المشرع الإجرائي قد لا يعتد دائما بصفة القائم بالإجراء لتكييف طبيعته؛ إذ يطرح التساؤل حول كيفية وصف التفتيش بأنه من أعمال التحقيق حينما يباشره الضبطية القضائية، ولاسيما في حالات التلبس بالجرائم أو بناء على ندب قضائي صريح[3].

ويرد هذا الاتجاه على هذا النقد بالتأكيد على أن مأمور الضبطية القضائية حينما يباشر إجراء التفتيش في حالتي التلبس والندب القضائي، فإنه يمارس في الواقع صلاحيات تحقيق أصيلة لا أعمال استدلالية؛ إذ يمنحه القانون في هذه الظروف الاستثنائية مكنة اتخاذ إجراءات

---

[1] علي حسن محمد الطوالبة، مرجع سابق، ص13.

[2] مرجع نفسه، ص 14.

[3] غازي عبد الرحمن هيان الرشيد، الحماية القانونية من جرائم المعلوماتية (الحاسب والانترنت)، أطروحة دكتوراه في القانون، كلية الحقوق، الجامعة الإسلامية في لبنان، بيروت، لبنان، 2004، ص 546.

تخضع لقواعد وضوابط قانونية صارمة لا تترتب عليه عادة في سياق وظائفه الضبطية الاعتيادية وبناء عليه فإن المشرع يضفي على الضبطية القضائية في هذه الحالات صفة سلطة التحقيق، مما يجعل من إجراءاتهم ومنها التفتيش الإلكتروني من أعمال التحقيق[1].

الاتجاه الرابع: يتبنى هذا الاتجاه رؤية توفيقية تجمع بين المعايير السابقة، حيث يرى أن الطبيعة القانونية للتفتيش تتحدد بالاستناد إلى المعايير الثلاثة مجتمعة؛ وبناء عليه، يكتسب التفتيش صفة «عمل من أعمال التحقيق» متى باشرته السلطة المختصة بالتحقيق، عقب افتتاح إجراءاته رسميا، وبقصد الكشف عن الحقيقة الجنائية[2].

ويبدو جلياً أن المشرع الجزائري قد مال إلى تبني هذا المعيار المختلط؛ إذ كرّس التفتيش كإجراء من إجراءات التحقيق الابتدائي وأسنده كأصل عام إلى سلطة قضائية ممثلة في قاضي التحقيق (معيار الجهة المنفذة)، على أن يتم في مرحلة التحقيق (معيار التوقيت)[3]. ومع ذلك، أجاز المشرع لضباط الشرطة القضائية ممارسة هذا الإجراء استثناءً في حالتين محددتين: حالة التلبس بالجناية أو الجنحة (طبقاً لأحكام المواد من 44 إلى 47 من قانون الإجراءات الجزائية)، وحالة التفتيش خارج حالات التلبس شريطة الحصول على الرضا والكتابة بخط يد الشخص المعني (طبقاً للمادة 64 مكرر من ذات القانون)[4].

وفي سياق التفتيش المعلوماتي، لم يحد المشرع الجزائري عن هذه الضوابط الحمائية؛ حيث نصت المادة الخامسة من القانون رقم 09-04 (المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها) على جواز دخول الأماكن بغرض التفتيش والولوج إلى المنظومات المعلوماتية أو منظومات التخزين الرقمية وكافة المعطيات

[1] رؤوف عبيد، مبادئ الإجراءات الجنائية في القانون المصري، الطبعة السادسة عشر، دار الجيل للطباعة، الفجالة، مصر، القاهرة، 1985، ص278.

[2] سامي جلال فقي حسين، مرجع سابق، ص 96.

[3] رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الالية للمعطيات في التشريع الجزائري والمقارن، مذكرة ماجستير، كلية الحقوق، قسم القانون الجزائري، جامعة دمشق سوريا 2010، ص311.

[4] المادة 64 مكرر من قانون الإجراءات الجزائية (المستحدثة بموجب الامر رقم15-02 المؤرخ في23 يوليو2015).

المخزنة فيها، من قِبل السلطات القضائية المختصة وضباط الشرطة القضائية، وذلك ضمن الأطر الإجرائية المحددة قانوناً والتي تستوجب إخطار النيابة أو قاضي التحقيق بحسب الأحوال[1].

وعليه، فإن اختصاص تنفيذ التفتيش في البيئة الرقمية للبحث عن الأدلة لا ينعقد حصراً لقاضي التحقيق، بل يمتد لضباط الشرطة القضائية المؤهلين بموجب أذونات قضائية مسبقة وضمن ضوابط الحرمة الخاصة. غير أنه يجب الفصل بدقة بين إجراء التفتيش الإلكتروني للمنظومات (المادة 5 من ذات القانون)، وبين إجراء مراقبة الاتصالات الإلكترونية وتسجيلها وتجميع معطياتها وحجزها (المادة 4 من القانون 09-04)؛ إذ أن هذا الأخير يُعد استثناءً شديد الخطورة يمس سرية المراسلات، ولذلك حصره المشرع تحت السلطة والإشراف المباشر للقاضي المختص، وتتولى تنفيذه جهات فنية متخصصة كالهيئة الوطنية للوقاية من الجرائم المعلوماتية ومكافحتها لضمان التوازن بين مقتضيات الفعالية الجنائية وحماية الحق في الخصوصية الرقمية[2].

الفرع الثاني: أنواع التفتيش الإلكتروني.

يعد التفتيش الإلكتروني من الإجراءات المستحدثة التي فرضتها التطورات المتسارعة في مجال تكنولوجيات الإعلام والاتصال، وقد سعى المشرع الجزائري إلى تنظيمه بموجب القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. ومن خلال استقراء أحكام المادتين 4 و5 من هذا القانون، يتضح أن التفتيش الإلكتروني لا يقتصر على وظيفته التقليدية في البحث عن الأدلة وإثبات

[1] قريم سكورة، المواجهة الإجرائية للجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة ماستر في القانون، تخصص: قانون جنائي وعلوم جنائية، قسم القانون العام، كلية الحقوق والعلوم السياسية، جامعة اكلي محند اولحاج-البويرة، 2015، ص52.

[2] المادة 4 من القانون رقم 09-04، مرجع سابق، وربطا بالضوابط الدستورية، ينبغي مراعاة المادتين 47 و48 من الدستور اللتين تجعلان من حظر انتهاك حرمة الحياة الخاصة وسرية المراسلات أصلا عاما لا يجوز الاستثناء منه الا بضمانات قضائية مشددة.

الجرائم، وإنما يمتد ليؤدي دورًا وقائيًا يهدف إلى حماية المصالح الأساسية للدولة من الأخطار المحتملة المرتبطة بالفضاء الرقمي، وهو ما يبرر التمييز بين التفتيش الإلكتروني الوقائي والتفتيش الإلكتروني كإجراء من إجراءات التحقيق.

أولًا: التفتيش الإلكتروني الوقائي.

الأصل في التفتيش، باعتباره إجراء ماسا بحرمة الحياة الخاصة، أن يتم في إطار دعوى جزائية قائمة أو تحقيق قضائي يهدف إلى الكشف عن جريمة وقعت بالفعل، غير أن خصوصية الجرائم المعلوماتية وما تنطوي عليه من مخاطر جسيمة على أمن الدولة وسلامة أنظمتها المعلوماتية دفعت المشرّع الجزائري إلى إقرار صورة استثنائية من التفتيش الإلكتروني تمارس قبل وقوع الجريمة بغرض الوقاية منها ومنع آثارها المحتملة[1].

ويستند هذا النوع من التفتيش إلى مقتضيات المادة الرابعة التي احالتنا اليها المادة من القانون رقم 09-04 التي أجازت اللجوء إلى التفتيش الالكتروني في حالات محددة على سبيل الحصر، تتمثل في الوقاية من الجرائم الإرهابية والتخريبية والجرائم الماسة بأمن الدولة، أو عند توفر معلومات جدية تفيد باحتمال وقوع اعتداء على منظومة معلوماتية من شأنه تهديد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني[2].

وتتولى ممارسة هذه المهمة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، التي أعيد تنظيمها بموجب المرسوم الرئاسي رقم 21-439 المؤرخ في 7 نوفمبر 2021، حيث نصت المادة الرابعة منه على تكليف الهيئة بضمان التفتيش الالكتروني الوقائي قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والجرائم الماسة بأمن الدولة تحت سلطة القاضي المختص[3]. ويستفاد من هذا النص أن المشرّع

[1] عبد القادر عميمر، التحديات القانونية لإثبات الجريمة المعلوماتية، دار الجامعة الجديدة، الإسكندرية، ص 118.

[2] المادة 4 من القانون رقم 09-04، مرجع سابق.

[3] المادة 4 من المرسوم الرئاسي رقم 21-439 المؤرخ في 7 نوفمبر 2021 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

لم يترك سلطة التفتيش الوقائي مطلقة، وإنما أخضعها للرقابة القضائية ضمانا للتوازن بين مقتضيات الأمن وحماية الحقوق والحريات الأساسية للأفراد.

ثانيًا: التفتيش الإلكتروني كإجراء من إجراءات التحقيق

يُقصد بالتفتيش الإلكتروني التحقيقي ذلك الإجراء الذي تباشره السلطات القضائية المختصة بعد وقوع الجريمة أو عند وجود دلائل جدية على ارتكابها، بهدف البحث عن الأدلة الرقمية وضبطها بما يساعد على كشف الحقيقة وتحديد المسؤولية الجزائية، ويعد هذا النوع امتدادا للتفتيش القضائي التقليدي، غير أن محله لم يعد يقتصر على الأماكن المادية وإنما يشمل الأنظمة المعلوماتية والشبكات وقواعد البيانات ووسائط التخزين الإلكترونية بمختلف أنواعها[1].

وقد أجاز المشرع الجزائري اللجوء إلى هذا الإجراء بموجب المادة الخامسة من القانون رقم 09-04، التي نصت على إمكانية استعمال التفتيش الإلكتروني لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى هذه الوسائل التقنية، ويُفهم من ذلك أن المراقبة أو التفتيش الإلكتروني لا يشكل إجراءً أصليا، وإنما وسيلة استثنائية تبررها الضرورة العملية عندما تعجز وسائل التحري التقليدية عن الوصول إلى الأدلة المطلوبة[2].

ويشمل التفتيش الإلكتروني التحقيقي صورتين أساسيتين: التفتيش المباشر والتفتيش الإلكتروني عن بعد، فالتفتيش المباشر يتم من خلال فحص الأجهزة والوسائط الإلكترونية الموجودة تحت يد جهة التحقيق، كالحواسيب والهواتف الذكية والأقراص الصلبة ووسائط التخزين المختلفة، أما التفتيش الإلكتروني عن بعد فيتم عبر النفاذ إلى منظومة معلوماتية أو

[1] عبد الله أوهايبية، شرح قانون الإجراءات الجزائية: الجزء الأول، الدعوى الناشئة عن الجريمة والبحث والتحري والاستدلال، ط1، بيت الافكار، الجزائر، 2022، ص 401.

[2] المادة 5 من القانون رقم 09-04، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها مرجع السابق.

أكثر بواسطة وسائل الاتصال الإلكترونية دون الانتقال المادي إلى مكان وجودها، وذلك بناءً على إذن قضائي وفي الحدود التي يقررها القانون[1].

وقد كرس المشرّع هذه الصورة الحديثة من التفتيش عندما أجاز امتداد عمليات البحث إلى أنظمة معلوماتية أخرى مرتبطة بالنظام محل التفتيش «ولو عن بُعد»، وهو ما يسمح للمحققين بتتبع الأدلة الرقمية أينما وجدت داخل البيئة المعلوماتية المترابطة، شريطة احترام مبدأ المشروعية وضمانات حماية الحياة الخاصة وعدم تجاوز نطاق الإذن القضائي[2].

وتزداد أهمية التفتيش الإلكتروني، لاسيما عن بعد في ظل اعتماد الجماعات الإجرامية على شبكات الاتصال الحديثة في التخطيط للجرائم وتنسيق تنفيذها وإخفاء آثارها، حيث أصبحت شبكة الإنترنت وسيلة فعالة لتبادل المعلومات والبيانات والاتصالات بين الجناة دون التقيد بالحدود الجغرافية. ومن ثم فإن الوصول إلى الأدلة الرقمية في مثل هذه الجرائم يصبح في كثير من الأحيان متعذرا دون اللجوء إلى تقنيات التفتيش والمراقبة الإلكترونية التي تتيح تتبع النشاط الإجرامي وكشف مرتكبيه بصورة أكثر فعالية[3].

[1] عبد القادر عميمر، مرجع سابق، ص 126.

[2] فطيمة جبار، مراقبة الاتصالات الإلكترونية بين الحظر والإباحة في التشريع الجزائري، مجلة الدراسات القانونية، ص15.

[3] عبد القادر عميمر، مرجع سابق، ص 132.

الفصل الثاني:

التفتيش الالكتروني بين مقتضيات التحقيق وضمانات حماية الحياة الخاصة

الفصل الثاني:

التفتيش الالكتروني بين مقتضيات التحقيق وضمانات حماية الحياة الخاصة

بعد أن تناولنا في الفصل الأول الحماية التشريعية المقررة للمعلومات الشخصية في ظل التفتيش الإلكتروني، من خلال بيان مختلف الآليات الدستورية والجزائية التي تكفل صون الحياة الخاصة، وكذا إبراز مفهوم التفتيش الإلكتروني وطبيعته القانونية وأنواعه باعتباره استثناءً مشروعا يجيز المساس ببعض مظاهر الخصوصية خدمةً لمقتضيات العدالة الجنائية، تبرز الحاجة إلى دراسة الأحكام الإجرائية التي تحكم ممارسة هذا الإجراء وحدود السلطة المخولة للجهات القائمة عليه.

فالتفتيش الإلكتروني لا يثير الإشكال على مستوى مشروعية وجوده فحسب، وإنما يمتد إلى كيفية ممارسته والضوابط القانونية الواجب احترامها أثناء تنفيذه، بالنظر إلى ما ينطوي عليه من قدرة على الولوج إلى المعطيات الرقمية والبيانات الشخصية المخزنة داخل الأنظمة المعلوماتية، ومن ثم فإن فعالية هذا الإجراء في مكافحة الجرائم المعلوماتية تظل مرتبطة بمدى احترام الشروط القانونية المنظمة له، وبوجود ضمانات كفيلة بمنع التعسف في استعمال سلطات التحقيق والمحافظة على التوازن بين متطلبات البحث عن الحقيقة وحماية الحياة الخاصة للأفراد.

وقد سعى المشرع الجزائري على غرار التشريعات المقارنة إلى إحاطة التفتيش الإلكتروني بجملة من الشروط الموضوعية والشكلية التي تضفي عليه المشروعية القانونية، كما أخضع ممارسته لرقابة قضائية وضمانات إجرائية متعددة تهدف إلى الحد من المساس غير المشروع بالحقوق والحريات الأساسية، ويكتسي هذا التوازن أهمية خاصة في البيئة الرقمية التي تتسم بسهولة الوصول إلى البيانات واتساع نطاق المعلومات التي يمكن الاطلاع عليها أثناء عملية التفتيش.

وعليه، سيتم التطرق في هذا الفصل إلى الضوابط القانونية للتفتيش الإلكتروني في المبحث الأول، ثم دراسة سلطة التحقيق في مباشرته والضمانات القانونية المقررة لحماية الحياة الخاصة أثناء ممارسته في المبحث الثاني.

المبحث الأول: الضوابط القانونية للتفتيش الالكتروني

يُعد التفتيش الإلكتروني من الإجراءات التحقيقية الحديثة التي فرضتها طبيعة الجرائم المرتبطة بالبيئة الرقمية، إذ أصبح وسيلة أساسية للكشف عن الأدلة الإلكترونية وجمعها بما يساهم في الوصول إلى الحقيقة وإثبات الجرائم. غير أن خطورة هذا الإجراء وما قد يترتب عليه من مساس بالحياة الخاصة والبيانات الشخصية للأفراد استوجب إخضاعه لجملة من الضوابط القانونية التي تكفل مشروعيته وتحد من أي تعسف قد يطال الحقوق والحريات المكفولة قانونًا.

ومن هذا المنطلق، حرص المشرّع على تنظيم التفتيش الإلكتروني من خلال وضع شروط وضوابط تحكم مباشرته، سواء تعلق الأمر بالشروط الموضوعية المرتبطة بمبررات اللجوء إليه ونطاقه القانوني، أو بالشروط الشكلية المتعلقة بالإجراءات الواجب اتباعها عند إصداره وتنفيذه. وعليه، سيتم التطرق في هذا المبحث إلى الشروط الموضوعية للتفتيش الإلكتروني (المطلب الأول)، ثم دراسة الشروط الشكلية للتفتيش الإلكتروني (المطلب الثاني).

المطلب الأول: الشروط الموضوعية للتفتيش الإلكتروني

لا يعد التفتيش الإلكتروني إجراء مطلقا تمارسه سلطات التحقيق دون ضوابط، بل يخضع لجملة من الشروط الموضوعية التي تكفل مشروعيته وتضمن سلامة نتائجه في مجال البحث عن الأدلة الرقمية وضبطها[1]، وتكتسي هذه الشروط أهمية بالغة بالنظر إلى ما ينطوي عليه التفتيش الإلكتروني من مساس محتمل بالحق في الخصوصية وسرية البيانات والمعطيات

[1] لمصارة منال، إجراءات التفتيش الإلكتروني في التشريع الجزائري، رسالة ماجستير في القانون العام، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 2012، ص 15.

الشخصية المخزنة داخل الأنظمة المعلوماتية، الأمر الذي يقتضي إخضاعه لضوابط دقيقة توازن بين مصلحة المجتمع في مكافحة الجريمة المعلوماتية ومصلحة الأفراد في حماية حقوقهم وحرياتهم الأساسية[1]، ومن ثم فإن مشروعية التفتيش الإلكتروني لا تتحقق إلا بتوافر أسباب قانونية تبرر اتخاذه، وانصبابه على محل مشروع يمكن أن يحتوي على أدلة أو معطيات مرتبطة بالجريمة محل البحث والتحقيق، وعليه سيتم تناول هذه الشروط من خلال فرعين أساسيين، يُخصص الأول لبيان سبب التفتيش الإلكتروني، بينما يعنى الفرع الثاني بتحديد محل هذا التفتيش ونطاقه.

الفرع الأول: سبب التفتيش الإلكتروني.

يهدف التفتيش الإلكتروني أساسا إلى البحث عن الأدلة الرقمية واستخراجها وضبطها وحفظها وفقا للأوضاع القانونية المقررة، بما يسمح بالكشف عن الحقيقة وتمكين سلطة التحقيق من بناء قناعتها القضائية على أسس موضوعية وقانونية سليمة[2]. ويعد هذا الإجراء من أخطر إجراءات التحقيق الجنائي نظرا لقدرته على النفاذ إلى البيانات والمعلومات المخزنة داخل الأنظمة المعلوماتية، ولذلك لا يجوز اللجوء إليه إلا إذا استند إلى سبب جدي ومشروع يبرر المساس المؤقت بحرمة الحياة الخاصة في سبيل تحقيق العدالة الجنائية[3]. ويقتضي ذلك أن تكون هناك جريمة معينة محل بحث أو تحقيق، وأن تنسب هذه الجريمة إلى شخص محدد، فضلا عن وجود دلائل أو قرائن قوية تشير إلى احتمال العثور على أدلة رقمية ذات صلة بالوقائع الإجرامية داخل الأجهزة أو الأنظمة المراد تفتيشها[4]. وعلى هذا الأساس يقوم سبب التفتيش الإلكتروني على مجموعة من المبررات القانونية والواقعية التي تجعل اللجوء إليه ضرورة تفرضها متطلبات البحث والتحقيق الجنائي.

---

[1] جباري عمار، التفتيش الإلكتروني (دراسة مقارنة)، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2015، ص 34.

[2] براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2011، ص 42.

[3] عبد الفتاح بيومي الحجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، مرجع سابق، ص 88.

[4] لمصارة منال، مرجع سابق، ص 22.

1 –وقوع جريمة إلكترونية

يعد وقوع الجريمة الشرط الأساسي الذي يبرر مباشرة إجراءات التفتيش الإلكتروني، إذ لا يتصور قانونا إجراء تفتيش بشأن واقعة لا تشكل جريمة أو لم يجرمها القانون أصلا[1]. فالتفتيش باعتباره إجراء من إجراءات التحقيق لا يتخذ إلا للكشف عن حقيقة جريمة وقعت بالفعل والبحث عن الأدلة المتعلقة بها، ومن ثم يكون التفتيش الذي يجري استنادا إلى مجرد الشكوك أو الافتراضات المجردة أو النوايا المستقبلية عديم الأساس القانوني ومعرضا للبطلان وهذا كقاعدة عامة[2]. لذلك استقر الفقه الجنائي على أن سبب التفتيش يجب أن يرتبط بواقعة إجرامية محددة تشكل اعتداءً على مصلحة يحميها القانون، وأن يكون الغرض منه جمع أدلة تثبت وقوعها أو تكشف عن مرتكبيها[3].

غير أن خصوصية الجرائم المعلوماتية وما تنطوي عليه من مخاطر جسيمة على الأنظمة المعلوماتية وأمن الدولة دفعت المشرع الجزائري إلى تبني توجه أكثر مرونة مقارنة بالقواعد التقليدية، إذ يتضح من خلال أحكام المادتين 04 و05 من القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها أنه أجاز اتخاذ بعض إجراءات المراقبة والتفتيش الإلكتروني في إطار وقائي يسبق وقوع الجريمة متى تعلق الأمر بجرائم خطيرة أو توفرت معلومات جدية تفيد بوجود خطر يهدد النظام العام أو أمن الدولة أو سلامة المنظومات المعلوماتية[4]، ويعد هذا الاستثناء مرتبطا بطبيعة الجرائم المعلوماتية التي

---

[1] علي حسن محمد طوالبة، مرجع سابق، ص 105.

[2] جمال نجيمي، قانون الإجراءات الجزائية الجزائري على ضوء الاجتهاد القضائي، الجزء الأول، الطبعة الثالثة، دار هومة، الجزائر، 2018، ص 114.

[3] نبيلة هبة هروال، الجوانب الإجرائية للجرائم الإلكترونية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، 2014، ص 53.

[4] المادتان 04 و05 من القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها (الجريدة الرسمية الجزائرية، العدد 47، الصادرة بتاريخ 16 أوت 2009).

تتميز بسرعة التنفيذ وسهولة محو آثارها وصعوبة تدارك نتائجها بعد وقوعها، الأمر الذي يقتضي أحيانًا التدخل المسبق للحيلولة دون إتمام النشاط الإجرامي أو الحد من آثاره المحتملة[1].

2 –توجيه التهمة لشخص وإسنادها إليه

لا يكفي لسلامة التفتيش الإلكتروني مجرد وقوع الجريمة، وإنما يتعين كذلك أن تتجه الشبهة إلى شخص معين تُنسب إليه الواقعة الإجرامية استنادًا إلى مؤشرات وأدلة أولية تبرر اتخاذ إجراءات التحقيق في مواجهته[2]. فالتفتيش لا يُمارس بصورة عشوائية أو على سبيل التحري العام عن الجرائم، وإنما يجب أن يكون موجها نحو شخص تتوافر بشأنه دلائل جدية تدعو إلى الاعتقاد بارتباطه بالفعل الإجرامي، سواء بوصفه فاعلًا أصليًا أو شريكًا أو مساهمًا فيه بأي صورة من صور المساهمة الجنائية.

وتكمن أهمية هذا الشرط في كونه يشكل ضمانة أساسية لحماية الأفراد من التعسف في استعمال سلطات التحقيق، إذ يمنع إخضاع الأشخاص للتفتيش لمجرد الشك أو الاشتباه غير المؤسس[3]. كما أن اشتراط وجود علاقة محتملة بين الشخص والجريمة ينسجم مع مبدأ الشرعية الإجرائية الذي يفرض أن تكون جميع إجراءات التحقيق قائمة على أسباب جدية ومبررات موضوعية يمكن التحقق منها[4].

وتطبيقا لذلك أوجب المشرع الجزائري على قاضي التحقيق عند مباشرته إجراءات التحقيق القضائي تحديد الشخص المنسوب إليه الفعل الإجرامي وبيان صفته القانونية في الدعوى، سواء كان فاعلا أصليا أم شريكا، وإذا تعذر تحديد هوية مرتكب الجريمة أو بقي مجهولا رغم

---

[1] رشيدة بوكر، مرجع سابق، ص 76.

[2] عز الدين عثماني، "إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية"، مجلة المحكمة العليا الجزائرية، قسم الوثائق القضائية، العدد الرابع، الجزائر، ص 19.

[3] سعيد محمد، الجرائم الإلكترونية وآليات الحصول على دليل فيها، الطبعة الأولى، دار الكتب القانونية، مصر، 2016، ص 94.

[4] عبد القادر عميمر، مرجع سابق، ص 40.

التحريات المنجزة، جاز لقاضي التحقيق إصدار أمر بألا وجه للمتابعة أو حفظ الملف إلى حين ظهور عناصر جديدة تسمح بتحديد المسؤول عن الواقعة محل التحقيق.

3 –توفر أمارات وقرائن قوية تدل على وجود أدلة تكشف الجريمة

لا ينهض سبب التفتيش الإلكتروني بمجرد وقوع الجريمة وإسنادها إلى شخص معين، بل يجب أن تدعم ذلك قرائن وأمارات جدية ترجح وجود أدلة أو معطيات رقمية يمكن العثور عليها داخل الأجهزة أو الأنظمة المعلوماتية المراد تفتيشها[1]، فالغرض من التفتيش ليس مجرد الاطلاع على محتويات الأنظمة المعلوماتية أو المساس بحرمة البيانات الشخصية، وإنما البحث عن عناصر إثبات من شأنها المساهمة في كشف الحقيقة وإثبات الوقائع الإجرامية أو نفيها.

وتتمثل هذه الأمارات في كل مؤشر موضوعي من شأنه أن يربط بين الجريمة المرتكبة وبين وسيلة إلكترونية معينة، كوجود مراسلات إلكترونية مشبوهة، أو سجلات اتصال رقمية، أو معلومات تقنية تفيد باستخدام جهاز محدد في ارتكاب الجريمة، أو وجود بيانات يُحتمل أن تكون متحصلة من النشاط الإجرامي أو مرتبطة به، كما قد تتمثل في تقارير الخبرة الفنية أو محاضر التحريات أو تصريحات الشهود أو الضحايا التي تشير إلى استعمال نظام معلوماتي معين في تنفيذ الجريمة أو إخفاء آثارها[2].

ويكتسي هذا الشرط أهمية خاصة في مجال الجرائم المعلوماتية نظرا للطبيعة غير المادية للدليل الإلكتروني وسهولة تعديله أو إتلافه أو نقله بين الأنظمة المختلفة، الأمر الذي يفرض على سلطات التحقيق الاستناد إلى مؤشرات جدية قبل الإذن بالتفتيش[3]، كما يضمن هذا الشرط عدم تحول التفتيش الإلكتروني إلى وسيلة استكشاف عامة أو بحث غير محدد في البيانات

[1] ليندا بن طالب، الدليل الإلكتروني ودوره في الإثبات الجنائي، أطروحة دكتوراه في القانون الجنائي، كلية الحقوق، جامعة جيلالي ليابس، سيدي بلعباس، الجزائر، 2019، ص 67.

[2] المرجع نفسه، ص 73.

[3] يوسف مناصرة، الدليل الإلكتروني في القانون الجزائي: الطريق إلى تحول أدلة الإثبات في المادة الجزائية – دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، مصر، 2021، ص 118.

الخاصة للأفراد، بل يبقى مقصورا على الحالات التي توجد فيها أسباب واقعية وقانونية قوية تبرر الاعتقاد بأن الأجهزة أو الأنظمة محل التفتيش تحتوي على أدلة أو معلومات تفيد في كشف الحقيقة وتحقيق العدالة الجنائية[1].

الفرع الثاني: محل التفتيش الالكتروني

أولا: محل التفتيش الالكتروني.

اشترط المشرع الجزائري لصحة التفتيش أن يكون مسببا، باعتباره إجراء من إجراءات البحث والتحقيق ويهدف إلى البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها بمكان أو شخص يتمتع بالحرمة، فلا تفتيش إلا بمقتضى القانون[2].

والغرض من محل الجريمة هو الحصول على الدليل وحجزه وفقا للمقتضيات القانونية[3] وهذا ما تؤكده المادة 06 من القانون رقم 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها [4].

1-تحديد محل التفتيش في البيئة التقنية.

بالنظر إلى حداثة الجرائم المعلوماتية واتصالها بأنظمة تكنولوجية معقدة من حيث الأساليب والأدوات المستعملة في تنفيذها، الأمر الذي استدعى تغيير أسلوب عمل أجهزة البحث والتحقيق، إذ فرض عليه التعامل مع جريمة مسرحها غير معتاد يقع في عالم افتراضي،

---

[1] جباري عمار، مرجع سابق، ص 50.

[2] علي حسن محمد الطوالبة، مرجع سابق، ص46.

[3] جمال نجيمي، قانون الإجراءات الجزائية الجزائري على ضوء الاجتهاد القضائي، الجزء الأول، دار هومة، الجزائر، ط3، سنة 2017، ص 98.

[4] تنص المادة 06 القانون رقم 09- 04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، مرجع سابق، "عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبها 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 احراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية".

وفي بيئة تقنية تتطلب مهارات وقدرات وتقنيات خاصة قد لا تتوفر معظم هذه الأجهزة ما فرض عليها اعتماد فرق متخصصة ومكونة في مجال تقنيات المعلوماتيات ورصدها لمكافحة هذه الجرائم[1].

وعليه محل التفتيش يشمل كل ملف من الملفات المخزنة المنظومة المعلوماتية حتى وإن كان الإجراء يحدث مساسا بالحريات الشخصية لذا أحاطته التشريعات بضمانات، والهدف منها تحقيق الموازنة بين مصلحة المجتمع في العقاب وبين حقوق الأفراد وحرياتهم، لذا أجاز خرق الخصوصية من خلال العمليات التفتيشية[2].

تجدر الإشارة إلى أنه نظرا للطبيعة الفنية للدليل الإلكتروني، أجاز المشرع الجزائري للسلطات المكلفة بالتفتيش بموجب المادة 5 من القانون 09-04 [3] تفتيش كل المنظومة المعلوماتية وكل منظومة تخزين المعلومات وكذا كل المعلومات المخزنة فيها، دون حصرها في المعلومات ذات المحتوى المجرم، وكذلك تسخير شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو التدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات لإنجاح مهمتها[4]

2-الأشخاص والمساكن كمحل للتفتيش في النظام المعلوماتي.

يساهم تفتيش الأشخاص في الاطلاع على المستودع الذي يحتفظ بسر الجريمة، فالشخص المراد تفتيشه لديه أو لدى غيره أدوات استخدمت في جريمة من جرائم الاعتداء على نظم المعالجة الآلية أو أشياء متحصلة أو مستندات أو دعامات تفيد في كشف الحقيقة[5] .

---

[1] يوسف مناصرة، مرجع سابق، ص97.

[2] عبد القادر عميمر، المرجع السابق، ص106.

[3] القانون رقم 09- 04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مرجع سابق.

[4] جباري عمار، مرجع سابق، ص21.

[5] علي حسن محمد الطوالبة، مرجع سابق، ص47.

وعلى هذا الأساس تتعدد المحال ولا تكون قائمة بذاتها بل تكون موضوعة في مكان ما كالمسكن أو المكتب أو تكون صحبة مالكها أو حائزها، قد يكون من المالك أو مستخدمي الكمبيوتر أو من خبراء البرامج سواء كانت برامج نظام أو تطبيقات، وقد يكون من المحللين أو من مهندسي الصيانة والاتصالات أو من مديري النظم المعلوماتية، أو أي أشخاص آخرين قد تكون بحوزتهم معدات وأجهزة معلوماتية أو أجهزة حاسب آلي محمولة متصلة بجهاز المخدم، وأمتعته التي كانت في حوزته، حتى وإن كان مستقلا بها باعتبارها من توابعه[1].

3 –تقنيات تفتيش محل الجريمة المرتبط بالأشخاص والمساكن.

إن إجراء التفتيش في الجريمة المعلوماتية يحتاج إلى تقنيات خاصة تختلف عن حالات التفتيش التقليدية، لأن تفتيش نظم المعلومات ليست سهلة وتتطلب دراية ومعرفة بملفات الأجهزة وأماكن

إخفاء المعلومات فيها لأنه يسهل إتلافها كليا أو جزئيا، كما يصعب تحديد مكان الدليل[2]، يلاحظ أنه في الحالات التي يجوز فيها لضابط الشرط القضائية القيام بإجراء التفتيش والضبط فإن مشروعية هذا الإجراء تتوقف على محل ارتكاب الجريمة ومدى تبعيته للمجني عليه[3].

ويقوم المفتش في إطار البحث عن الجرائم المعلوماتية بمجموعة وفقا لطرق تتماشى والطبيعة الخاصة للتفتيش الالكتروني نلخصها فيما يلي:

3-1 –محل تفتيش النظام المعلوماتي الخاص بالمتهم.

تنصب إجراءات التفتيش حول محل ارتكاب الجريمة المرتبط بالنظام المعلوماتي الخاص بالمتهم وغالبا جرائم الحاسب الآلي الذي يعد نافذة يطل على عالم الإنترنت، والشبكة التي تشمل في مكوناتها الخادم والمزود الآلي، ويجدر الإشارة هنا إلى أن مثل هذا المحل لا يكون

[1] جباري عمار، مرجع سابق، ص22.

[2] رشيدة بوكر، مرجع سابق، ص208.

[3] عز الدين عثماني، مرجع سابق، ص60.

قائما بذاته، وإنما يشمله مكان أو عقار ما أو يكون صحبة مالكه أو حائزه ولذلك وجب على ضابط الشرطة القضائية عند استصداره إذن التفتيش أن يحدد محل ذلك الإجراء تحديدا دقيقا وكذلك الغرض منه و هذا ما يصعب تطبيقه في النظم المعلوماتية لصعوبة تحديدها وذلك عكس المحل في التفتيش التقليدي[1].

وعليه يحدد التفتيش الإلكتروني دقة الإجراءات فمن خلاله يتم نقل البرنامج الداخلي من الوسائط المتعددة وبذلك يتم الحصول على دليل ارتكاب الجريمة، وهذا ما يتم في جرائم النسخ والتقليد حيث يتم ضبط الوسائط المتعددة المحملة بالبرامج المنسوخة والأجهزة المستخدمة في ذلك[2].

3-2 محل تفتيش النظام المعلوماتي غير الخاص بالمتهم.

تتعدد الوسائط الإلكترونية وأنظمتها المختلفة المرتبطة بالجرائم التي ترتكب باستخدام الشبكات بحيث يتم ارتكاب الجريمة من أي جهاز من أجهزة الحاسبات الآلية الأخرى المتصلة بالحاسب الذي ارتكبت في نظامه الجريمة المعلوماتية، فهذا الفرض يؤكد فإن إجراءات التفتيش والضبط تتطلب الدخول في نظام معلوماتي لشخص آخر[3].

المطلب الثاني: الضوابط الشكلية للتفتيش الإلكتروني

لا يقتصر التفتيش الإلكتروني على توافر الشروط الموضوعية المتعلقة بمشروعيته، بل يستلزم كذلك احترام مجموعة من الضوابط الشكلية التي أقرها المشرع ضمانا لصحة هذا الإجراء وحماية للحقوق والحريات الفردية، فالتفتيش باعتباره من أخطر إجراءات التحقيق لما ينطوي عليه من مساس بحرمة الحياة الخاصة وسرية المعطيات، يجب أن يتم وفق لضوابط

[1] عبد الفتاح بيومي الحجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، مرجع سابق، ص 378.

[2] سعيد محمد، مرجع سابق، ص 53.

[3] نبيلة هبة هروال، مرجع سابق، ص228.

قانونية شكلية دقيقة تكفل التوازن بين مصلحة المجتمع في كشف الحقيقة والصدي للجريمة، وبين حق الأفراد في صون حرياتهم وعدم التعرض لأي تعسف من قبل السلطات المختصة.

وتتمثل هذه الضوابط الشكلية في مجموعة من الإجراءات التي يتعين مراعاتها أثناء تنفيذ التفتيش الإلكتروني، كإجراء التفتيش بحضور الأشخاص الذين يعينهم القانون (الفرع الأول)، والتقيد بالأوقات المحددة قانونا لتنفيذ هذا الإجراء (الفرع الثاني)، إضافة إلى تحرير محضر يثبت كافة الإجراءات المتخذة أثناء التفتيش (الفرع الثالث)، وذلك بما يضمن مشروعية التفتيش وسلامة الأدلة المستخلصة منه.

الفرع الأول: إجراء التفتيش بحضور أشخاص يعينهم القانون

تقتضي أغلب التشريعات الإجرائية عند مباشرة عملية التفتيش، ضرورة حضور أشخاص معينين قانونا أثناء تنفيذ هذا الإجراء، ويتمثل ذلك أساسا في حضور المتهم، أو من ينوب عنه عند تعذر حضوره، وفي حالة تعذر الأمرين معا يتم الاستعانة بشاهدين. ويعد هذا الحضور من الضمانات الجوهرية التي يترتب على مخالفتها بطلان إجراء التفتيش، تجسيدًا لمبدأ الحضور أثناء تفتيش المساكن،[1] وذلك وفقًا لما نصت عليه المادة 76 من قانون الإجراءات الجزائية[2] ويهدف هذا الإجراء إلى تكريس حماية حرمة الحياة الخاصة وضمان نزاهة وشفافية عمليات التفتيش.

إلا أن المشرع الجزائري لم يجعل هذا المبدأ مطلق التطبيق، بل أورد عليه استثناء يراعي خصوصية الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال، بالنظر إلى ما تتميز به من طبيعة تقنية خاصة وسرعة إمكانية إخفاء أو إتلاف الأدلة الرقمية المتعلقة بها. ولهذا السبب، نصت الفقرة الأخيرة من المادة76 من قانون الإجراءات الجزائية على جواز مباشرة ضباط

[1] رضا هميسي، مرجع سابق، ص172.

[2] المادة 76 من القانون 14/25 مؤرخ في 9 صفر 1447 الموافق 3 غشت 2025، يتضمن قانون الاجراءات الجزائية، الجريدة الرسمية العدد 54 الصادرة ب 13 اوت 2025.

الشرطة القضائية لإجراءات التفتيش دون التقيد بشرط حضور المتهم أو من يمثله أو حتى الشاهدين، متى تعلق الأمر بهذا النوع من الجرائم.[1]

ويجد هذا الاستثناء مبرره في الطابع الخاص للجرائم الإلكترونية، التي تتسم بسرعة زوال أدلتها وإمكانية محوها أو تعديلها في وقت وجيز، الأمر الذي يفرض على السلطات المختصة التحرك بسرعة وفعالية مع الحفاظ على عنصر المباغتة والسرية لضمان نجاح التحقيق. ومن ثم، فإن الإذن بالتفتيش في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال يمنح الجهات المختصة إمكانية مباشرة هذا الإجراء وفق آليات استثنائية تتلاءم مع طبيعة هذه الجرائم ومتطلبات إثباتها.

أ. الإذن بالتفتيش:

يقصد بالإذن بالتفتيش ذلك الترخيص القانوني الصادر عن السلطة القضائية المختصة، والمتمثلة في قاضي التحقيق أو وكيل الجمهورية، والذي يمنح لضباط الشرطة القضائية، سواء تعلق الأمر بشخص أو بمكان معين، وذلك في إطار البحث والتحري عن جريمة محددة وجمع الأدلة اللازمة لإظهار الحقيقة، ويهدف هذا الإذن إلى تمكين السلطات المختصة من مباشرة إجراءات التفتيش بصفة سريعة وفعالة، لا سيما في الحالات التي يخشى فيها من ضياع الأدلة أو إتلافها، أو عندما يتعذر على قاضي التحقيق مباشرة إجراءات التفتيش بنفسه[2].

ويلاحظ أن إذن التفتيش الواقع على نظم الحاسوب وشبكات الإنترنت تتميز بخصوصية تختلف عن التفتيش التقليدي، وذلك بالنظر إلى الطبيعة التقنية الدقيقة للأجهزة والبرامج محل التفتيش، ومن ثم يتعين على الجهات المختصة مراعاة جملة من التدابير والتحريات الفنية لضمان سلامة الإجراء وفعاليته وتتمثل ذلك فيما يلي:

[1] رجاء أمدور، خصوصية التحقيق في مواجهة الجرائم المعلوماتية؛ أطروحة مقدمة لنيل شهادة الدكتوراه، تخصص القانون الخاص، كلية الحقوق وعلوم السياسية، جامعة محمد البشير الابراهيمي، برج بوعريريج، الجزائر ،2021، ص146.

[2] راجع المادة 75 من الامر 14/25 يتضمن قانون الإجراءات الجزائية، مرجع سابق.

– تحديد طبيعة النظام المعلوماتي المراد تفتيشه بدقة، سواء تعلق الأمر بالحواسيب أو الشبكات أو الوسائط الإلكترونية المختلفة.

– الإعداد المحكم لعملية التفتيش من خلال إجراء تقييم شامل للوضع التقني، بما يضمن عدم ضياع أو إفلات الأدلة الرقمية محل البحث.

– اتخاذ الاحتياطات الفنية اللازمة لمواجهة إمكانية دخول المشتبه فيه عن بُعد إلى النظام المعلوماتي عبر وسائل الاتصال المختلفة، بما قد يؤدي إلى إخفاء أو إتلاف الدليل الإلكتروني.

– التحكم الدقيق في عملية الولوج إلى الأجهزة والأنظمة المعلوماتية أثناء التفتيش، مع الحرص على المحافظة على سلامة الدليل الرقمي وعدم العبث به أو إتلافه، والاستعانة بوسائل التصوير والتوثيق لإثبات مختلف مراحل وإجراءات التفتيش الإلكتروني[1].

استنادا الة المادة 75 قانون الإجراءات الجزائية يتعين أن يكون الإذن مكتوبا وموقعا من الجهة القضائية التي أصدرته، مع ضرورة إظهاره للمعني بالأمر قبل مباشرة التنفيذ ويجب كذلك أن يتضمن بيانات دقيقة تتعلق بهوية الشخص محل التفتيش أو العنوان المحدد للمكان المراد تفتيشه، إضافة إلى بيان الجريمة موضوع التفتيش بصورة واضحة، وذلك ضمانا لاحترام الحقوق والحريات الفردية، وتفاديًا لأي تعسف أو تجاوز في استعمال السلطة.[2]

الفرع الثاني: احترام الميقات الزمني لإجراء التفتيش :

يعد فرض القيود الزمنية على إجراء التفتيش من أهم الضمانات القانونية التي تهدف إلى الحد من التعسف في استعمال سلطة التفتيش، لما يحققه من توازن بين مقتضيات المصلحة العامة وضرورة احترام الحياة الخاصة للأفراد، وفي هذا الإطار حرص المشرع الجزائري على تنظيم الأوقات التي يجوز خلالها القيام بالتفتيش الالكتروني، حيث استنادا الى المادة 78من

[1] علي حسين محمد الطوالبة، المرجع السابق، ص 59.

[2] حمداش شمس الدين، البشير بن مبروك، مرجع سابق، ص 106.

قانون الإجراءات الجزائية[1] فانه لا يجوز البدء في التفتيش قبل الساعة الخامسة (5) صباحا ولا بعد الساعة الثامنة (8) ليلا و هذا ما ينطبق أيضا على التفتيش الالكتروني و هذا اومن خلال هذا النص يتضح أن المشرّع الجزائري جعل استنادا الى المادة 5 من القانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها.[2]

وعليه وفقا لما تقدم فان التفتيش الالكتروني مقيدا بمدة زمنية محددة كأصل عام، مع إقرار بعض الاستثناءات التي تبرر الخروج عن هذه القاعدة متى اقتضت الضرورة ذلك، فنظرا لخصوصية التفتيش الإلكتروني، فإن عامل الوقت يكتسي أهمية بالغة، خاصة في ظل سهولة وسرعة إتلاف أو محو المعطيات المعلوماتية التي قد تشكل دليلا أساسيا في التحقيق، فالدليل الإلكتروني يتميز بطبيعته القابلة للتغيير أو الإزالة في وقت وجيز، الأمر الذي يجعل من السرعة في مباشرة إجراءات التفتيش ضرورة ملحة لضمان الحفاظ على الأدلة الرقمية لذلك فإن مجرد تسرب علم المتهم بقيام السلطات المختصة باتخاذ إجراءات التفتيش قد يدفعه إلى السعي لمحو أو إتلاف جزء من المعطيات المعلوماتية أو كلها، بهدف عرقلة سير التحقيق والتخلص من الأدلة التي يمكن أن تدينه.

تجسيدا لهذا التوجه منحت الفقرة الثالثة من المادة 78 من قانون الإجراءات الجزائية الجزائري صلاحية إجراء التفتيش في العديد من الجرائم المحددة على سبيل الحصر ومن بينها الجرائم المتصلة بتكنولوجيات العلام والاتصال في أي وقت، نهارا أو ليلا، ويشترط المشرع لاستخدام هذا الحق استصدار إذن مسبق من وكيل الجمهورية المختص، وهو ما يبرز الطبيعة الاستثنائية للجرائم المعلوماتية التي تستوجب سرعة التدخل ومرونة الإجراءات للحفاظ على الدليل الرقمي وحمايته من التلاشي أو العبث.

[1] المادة 78 من القانون 14/25 يتضمن قانون الإجراءات الجزائية، مرجع سابق.

[2] المادة 5 من القانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، مرجع سابق.

الفرع الثالث: تحرير محضر لإجراءات التفتيش

يستوجب لصحة التفتيش الالكتروني وجوب تحرير محضر إجراءات فور الانتهاء من التنفيذ، يوثق تسلسلا زمنيا وموضوعيا لكافة ما عاينه القائم بالتفتيش من وقائع، وما اتخذه من قرارات، وما أسفرت عنه العملية من نتائج. ويظل هذا الالتزام قائماً كضمانة جوهرية بغض النظر عن النتيجة؛ سواء أفضى التفتيش إلى ضبط أدلة مادية (نتيجة إيجابية) أو لم يسفر عن شيء (نتيجة سلبية)..[1]

تتمحور الغاية الجوهرية من هذا التوثيق حول تمكين الرقابة القضائية من بسط سلطتها على مشروعية إجراءات التفتيش الالكتروني؛ ضمانا لسلامة الأدلة المستمدة منها من جهة، وصونا للحريات الفردية من جهة أخرى.

وبناءً عليه فإن أي إخلال بجوهرية هذا الإجراء يستتبع البطلان الذي يمتد بالضرورة ليقوض القيمة القانونية للدليل المتحصل منه (قاعدة ما بُني على باطل فهو باطل).

ومع أن التشريعات الجنائية – كأصل عام – لم تقيد محضر التفتيش بقالب شكلي جامد، إلا أنها استوجبت توافر بيانات جوهرية تمليها القواعد العامة لضمان صحته وحجيته؛ وفي مقدمتها: تدوينه باللغة الرسمية، إثبات تاريخ ومكان الإجراء بدقة، بيان صفة القائم بالتفتيش، وتوقيع المحرر وكافة الأطراف المشاركة أو الحاضرة في مسرح التفتيش. [2]

كما يجب أن يتضمن كافة الإجراءات التي اتخذت من بداية الى نهاية التفتيش وتدوين كافة الملاحظات المتعلقة بإجراء التفتيش، وما تم اتخاذه من إجراءات اثناء مباشرة التفتيش ويختم المحضر باسم القائم بالتفتيش وتوقيعه، باعتباره مسؤول عن صحة ما ورد فيه من البيانات[3].

---

[1] سامي حسني، النظرية العامة للتفتيش في القانون المصري والمقارن، جار النهضة، القاهرة,1973, ص277.

[2] مرجع نفسه، ص288.

[3] مولاي ملياني دلال، التفتيش في جرائم تكنولوجيات الإعلام والاتصال، مجلة القانون والعلوم السياسية، المجلد، 02، العدد 01، كلية الحقوق والعلوم السياسية، جامعة الدكتور مولاي الطاهر، سعيدة، الجزائر،2016، ص 302.

وعلاوة على ما سبق يلتزم محرر المحضر بسرد وقائع التفتيش سردا مفصلا وشاملا، يبدأ من لحظة الانتقال إلى مسرح الإجراء وينتهي بتمام التنفيذ؛ بحيث يشتمل على وصف دقيق للمكان (سواء كان مسكناً أو محلاً تجارياً) إذا كان النظام المعلوماتي موجود في مسكن معين وتحديد هوية الأشخاص الخاضعين للتفتيش. ويجب أن يوثق المحضر كافة العقبات المادية أو القانونية التي واجهت القائم بالتفتيش، كحالات المقاومة أو الامتناع عن فتح الأبواب، وما تلاها من إجراءات قانونية لاقتضاء نفاذ الإذن (مثل الاستعانة بالقوة العامة).

وتتجلى الأهمية القانونية لهذا السرد في كونه يمثل شهادة رسمية لمحرره، يُسأل عنها بصفته الوظيفية؛ لذا فإن تذييل المحضر بتوقيعه وبيان صفته لا يعد مجرد إجراء شكلي، بل هو إقرار بمسؤوليته الكاملة عن صحة البيانات المدوّنة، وضمانة لعدم دحضها إلا بسلوك طريق الطعن بالتزوير[1].

[1] حطاب كمال، خصوصية التفتيش في البيئة الإلكترونية، مجلة البحوث في الحقوق والعلوم السياسية، المجلد 09، عدد01، كلية الحقوق والعلوم السياسية، جامعة ابن خلدون،2023، ص603.

المبحث الثاني: سلطة التحقيق وضمانات حماية الحياة الخاصة في التفتيش الإلكتروني.

أدى التطور التكنولوجي المتسارع وازدياد الاعتماد على الوسائط الرقمية في مختلف مجالات الحياة إلى بروز أنماط جديدة من الجرائم المرتبطة بالأنظمة المعلوماتية والشبكات الإلكترونية، وهو ما فرض على سلطات التحقيق الجنائي تطوير وسائلها الإجرائية لمواكبة هذا التحول، فلم يعد البحث عن الأدلة مقتصرا على الأماكن المادية التقليدية، بل امتد إلى الفضاء الرقمي بما يحتويه من بيانات معلوماتية ومعطيات شخصية ورسائل واتصالات ذات طبيعة خاصة، الأمر الذي أفرز ما يعرف بالتفتيش الإلكتروني باعتباره من أخطر إجراءات التحقيق الحديثة وأكثرها مساسا بالحياة الخاصة للأفراد.

ويتميز التفتيش الإلكتروني بخصوصية قانونية وتقنية تجعله يختلف عن التفتيش التقليدي، بالنظر إلى طبيعة الدليل الرقمي القابل للتعديل أو الإخفاء أو الإتلاف بسهولة، فضلا عن اتساع نطاق المعطيات التي يمكن الوصول إليها أثناء عملية التفتيش، لذلك كان لزاما على المشرّع وضع إطار قانوني يحدد سلطة التحقيق في مباشرة هذا الإجراء، ويضبط الجهات المختصة به وحدود ممارسته، مع إخضاعه لجملة من الضمانات التي تكفل احترام الحقوق والحريات الأساسية، وعلى رأسها الحق في الخصوصية وسرية المعطيات الشخصية والاتصالات الإلكترونية.

وقد حاول المشرّع الجزائري من خلال قواعد قانون الإجراءات الجزائية والقوانين الخاصة بمكافحة الجرائم المعلوماتية، تحقيق التوازن بين متطلبات مكافحة الجريمة الإلكترونية وضرورة حماية الحياة الخاصة، وذلك عبر إخضاع التفتيش الإلكتروني لرقابة قضائية وضمانات إجرائية دقيقة تحد من التعسف في استعمال سلطة التحقيق. وتبرز أهمية هذه الضمانات في ظل اتساع صلاحيات الجهات المكلفة بالتحقيق، وما قد ينجرّ عن سوء استعمالها من انتهاكات خطيرة تمسّ بحرمة الحياة الخاصة الرقمية للأفراد.

وعليه، يقتضي دراسة هذا المبحث التطرق أولا إلى نطاق سلطة التحقيق في التفتيش الإلكتروني وحدودها، من خلال بيان الجهات المختصة وإجراءات التفتيش الإلكتروني (المطلب الأول)، ثم دراسة الضمانات القانونية المقررة لحماية الحياة الخاصة أثناء ممارسة هذه السلطة، سواء من خلال الضمانات الإجرائية المقيدة لسلطة التحقيق أو من خلال الرقابة القضائية باعتبارها ضمانة أساسية لمشروعية إجراءات التفتيش الإلكتروني (المطلب الثاني).

المطلب الأول: نطاق سلطة التحقيق في التفتيش الالكتروني وحدودها.

في ظل التحول الرقمي المتسارع الذي مس مختلف مجالات الحياة، لم يعد التفتيش في المجال الجنائي يقتصر على صورته التقليدية المرتبطة بالمحلات المادية، بل امتد ليشمل الفضاء المعلوماتي بما يثيره من إشكالات قانونية وتقنية معقدة تتعلق بحماية الحياة الخاصة وضمان فعالية التحقيق الجنائي في آن واحد، ومن هذا المنطلق يكتسي موضوع نطاق سلطة التحقيق في التفتيش الإلكتروني وحدودها أهمية بالغة، باعتباره الإطار الذي يحدد من جهة الجهات المختصة بمباشرة هذا الإجراء، سواء كانت السلطة الأصلية المتمثلة في قاضي التحقيق أو السلطات الاستثنائية كالإنابة القضائية والتسخير الفني، ومن جهة أخرى يضبط مختلف المراحل والإجراءات التقنية والقانونية التي تحكم عملية التفتيش الإلكتروني من بدايتها إلى غاية استغلال نتائجها أمام القضاء.

وعليه، سيتم تناول هذا المطلب من خلال فرعين أساسيين، يتمثل الفرع الأول في: الجهات المختصة بالتفتيش الإلكتروني، بينما يتناول الفرع الثاني: إجراءات التفتيش الإلكتروني، وذلك قصد إبراز الإطار القانوني والإجرائي الذي يحكم ممارسة هذا الاختصاص وحدوده في التشريع الجزائري.

الفرع الأول: الجهات المختصة بالتفتيش الالكتروني.

يعد التفتيش الإلكتروني من أخطر إجراءات التحقيق الجنائي في العصر الحديث، بالنظر إلى ما ينطوي عليه من مساس مباشر بحرمة الحياة الخاصة في بعدها الرقمي، والتي

لم تعد تقتصر على المسكن المادي، بل امتدت لتشمل الفضاء المعلوماتي بما يحتويه من بيانات شخصية ومراسلات إلكترونية وملفات رقمية ذات طابع حساس، وقد فرض هذا التحول على المشرع الجزائري ضرورة وضع إطار قانوني دقيق يحدد الجهات المختصة بمباشرة هذا الإجراء، ويضبط شروطه، بما يحقق التوازن بين فعالية البحث الجنائي وحماية الحقوق والحريات الأساسية[1].

وعليه، فإن تحديد الجهات المختصة بالتفتيش الإلكتروني يقتضي التمييز بين السلطة الأصلية التي تملك هذا الاختصاص ابتداء، والسلطات الاستثنائية التي تمارسه في إطار الإنابة أو التسخير بنوعيه القضائي والفني.

أولًا: السلطة الأصلية في إجراء التفتيش الإلكتروني.

يعتبر قاضي التحقيق الجهة القضائية المختصة الاصلية بإصدار أوامر التفتيش الإلكتروني، باعتباره صاحب الولاية العامة في إدارة مرحلة التحقيق الابتدائي، والمخول قانونا بجمع الأدلة، بما في ذلك الأدلة الرقمية التي أصبحت تحتل مكانة مركزية في الإثبات الجنائي، لا سيما في الجرائم المعلوماتية[2].

ويستند هذا الاختصاص إلى مبدأ الشرعية الإجرائية، الذي يفرض أن يكون كل إجراء ماسّ بالحياة الخاصة قائمًا على نص قانوني وتحت رقابة قضائية مستقلة، وهو ما يشكل ضمانة أساسية للحد من التعسف، خاصة بالنظر إلى حساسية البيانات الرقمية وقدرتها على كشف أدق تفاصيل الحياة الشخصية للأفراد[3]. ويضاف إلى مبدأ الشرعية الإجرائية مبدأ الرقابة القضائية الفعلية، الذي لا يقتصر على مجرد إصدار الإذن بالتفتيش، بل يمتد ليشمل متابعة تنفيذ الإجراء والتأكد من احترام حدوده الموضوعية والزمنية. ويكتسي هذا البعد أهمية خاصة

[1] أحسن بوسقيعة، التحقيق القضائي في قانون الإجراءات الجزائية الجزائري، دار هومة، الجزائر، ط5، 2017، ص 45.

[2] عبد الله اوهايبية، مرجع سابق، ص80.

[3] دستور الجمهورية الجزائرية لسنة 2020، المادة 47.

في التفتيش الإلكتروني، بالنظر إلى سهولة تجاوز نطاق الإذن، سواء من خلال الاطلاع على بيانات غير معنية بالتحقيق، أو من خلال التوسع في تحليل محتوى الأجهزة المضبوطة[1].

كما يثير التفتيش الإلكتروني إشكالية تحديد نطاق الإذن القضائي، خاصة في الحالات التي تكون فيها البيانات مترابطة داخل أنظمة معلوماتية معقدة. لذلك، يذهب الفقه إلى ضرورة أن يكون إذن التفتيش محددًا قدر الإمكان، سواء من حيث نوع البيانات أو الفترة الزمنية أو طبيعة النظام المعلوماتي محل الفحص، وذلك تفاديًا لتحوله إلى تفتيش شامل يمس بالحياة الخاصة بشكل غير مبرر[2].

كما يستمد قاضي التحقيق سلطته من أحكام قانون الإجراءات الجزائية، التي تخوّله اتخاذ جميع الإجراءات اللازمة لكشف الحقيقة، بما في ذلك إصدار أوامر التفتيش التي يمكن أن تنصب على الأنظمة المعلوماتية والوسائط الرقمية، في ظل التطور التكنولوجي[3].

ويمتد نطاق التفتيش الإلكتروني ليشمل ليس فقط الأجهزة المادية كالحواسيب والهواتف الذكية، بل كذلك البيانات المخزنة عن بُعد، كالمعطيات الموجودة على الخوادم أو ضمن خدمات الحوسبة السحابية، وهو ما يعكس اتساع مفهوم محل التفتيش ليشمل الفضاء الرقمي في حد ذاته. ويطرح امتداد التفتيش إلى البيانات المخزنة عن بُعد إشكالات قانونية تتعلق بمسألة الاختصاص الإقليمي، خاصة عندما تكون الخوادم خارج الإقليم الوطني. ففي هذه الحالة، يتعين التوفيق بين متطلبات التحقيق الجنائي ومبدأ سيادة الدول، وهو ما قد يقتضي اللجوء إلى آليات التعاون القضائي الدولي، أو الاتفاقيات الدولية ذات الصلة بالجرائم المعلوماتية[4].

---

[1] أحسن بوسقيعة، مرجع سابق، ص45.

[2] رشيدة بوكر، مرجع سابق، ص 154.

[3] الأمر رقم 66-155 المؤرخ في 08 جوان 1966، المتضمن قانون الإجراءات الجزائية، المعدل والمتمم، المواد 29 وما يليها.

[4] عبد القادر عدو، الإثبات الجنائي في المواد المعلوماتية، دار بلقيس، الجزائر، 2018، ص120.

غير أن ممارسة هذه السلطة تبقى مقيدة بضوابط قانونية دقيقة، تتمثل أساسًا في ضرورة تحديد نطاق التفتيش، واحترام مبدأ التناسب، وعدم المساس ببيانات لا علاقة لها بموضوع التحقيق، فضلاً عن توثيق جميع الإجراءات في محاضر رسمية تضمن سلامة الدليل الرقمي وقابليته للإثبات أمام القضاء[1].

ثانيًا: السلطات الاستثنائية في إجراء التفتيش الإلكتروني.

رغم أن الاختصاص الأصيل في التفتيش الإلكتروني ينعقد لقاضي التحقيق، إلا أن المشرّع الجزائري أجاز، على سبيل الاستثناء، ممارسته من قبل جهات أخرى، في إطار الإنابة القضائية أو التسخير، وذلك لمواجهة الطبيعة التقنية والعملية المعقدة لهذا النوع من التفتيش[2].

1 .الإنابة القضائية.

تعد الإنابة القضائية وسيلة قانونية تخول لقاضي التحقيق تفويض بعض اختصاصاته إلى قاضٍ آخر أو إلى أحد ضباط الشرطة القضائية، للقيام بإجراءات محددة، من بينها التفتيش الإلكتروني، خاصة في الحالات التي تتطلب سرعة التدخل أو خبرة ميدانية[3].

وتكتسي هذه الآلية أهمية خاصة في المجال الرقمي، نظرا لسهولة إتلاف الأدلة الإلكترونية أو تغييرها، مما يستدعي التدخل الفوري للحفاظ عليها، غير أن ضابط الشرطة القضائية المنتدب يظل ملزما بحدود الإنابة، ويترتب على تجاوزها بطلان الإجراء لمخالفته مبدأ الشرعية. ولا يقتصر دور الإنابة القضائية على مجرد تنفيذ إجراء التفتيش، بل قد يشمل أيضًا اتخاذ تدابير تحفظية عاجلة، كمنع الولوج إلى النظام المعلوماتي أو تجميد الحسابات الرقمية، وذلك بهدف الحفاظ على الأدلة من الضياع أو التلاعب. غير أن هذه الصلاحيات

[1] الطيب بلولة، إجراءات البحث والتحري في الجرائم الإلكترونية، دار الخلدونية، الجزائر، 2019، ص62.

[2] المادة 234 من القانون 14/25 يتضمن قانون الإجراءات الجزائية ، مرجع سابق.

[3] أحسن بوسقيعة، مرجع سابق، ص 112.

تظل مقيدة بضرورة الرجوع إلى قاضي التحقيق في أقرب الآجال، تكريسًا لمبدأ الرقابة القضائية[1].

2 .التسخير القضائي والفني.

يُعدّ التسخير من أهم الآليات التي يعتمد عليها التفتيش الإلكتروني، نظرا لما يتطلبه من كفاءات تقنية متخصصة. ويشمل هذا التسخير نوعين متكاملين: التسخير القضائي والتسخير الفني.

أ. التسخير القضائي:

يقصد به استعانة السلطة القضائية بأشخاص ذوي صفة أو خبرة معينة، كضباط الشرطة القضائية أو أعوان مختصين، للمساهمة في تنفيذ إجراءات التفتيش، خاصة في الجوانب المرتبطة بحجز الأجهزة أو التعامل الأولي مع الأدلة الرقمية[2].

ب. التسخير الفني:

أما التسخير الفني، فيمثل الامتداد التقني للتسخير القضائي، ويقصد به الاستعانة بخبراء مختصين في مجال الإعلام الآلي والأمن السيبراني، أو بمؤسسات تقنية مثل مزودي خدمات الإنترنت وشركات الاتصالات، وذلك للقيام بالعمليات التقنية المعقدة التي يتطلبها التفتيش الإلكتروني. ويُلاحظ في هذا السياق أن التسخير الفني لا يقتصر على الخبراء الأفراد، بل قد يمتد إلى أشخاص معنويين، كالشركات المتخصصة في الأمن المعلوماتي أو المؤسسات المقدمة للخدمات الرقمية، وهو ما يعكس الطابع المؤسسي المتزايد للتحقيقات الجنائية في البيئة الرقمية[3].

[1] محمد محدة، الشرطة القضائية ودورها في الإثبات الجنائي، دار هومة، الجزائر، 2012، ص74.

[2] نفس المرجع، ص 80.

[3] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، مرجع سابق، ص 210.

ويشمل هذا النوع من التسخير مهام متعددة، من أبرزها: استخراج البيانات الرقمية، استرجاع المعطيات المحذوفة، فك التشفير، تحليل الأنظمة المعلوماتية، وتتبع الأنشطة الرقمية، وهي عمليات ضرورية لضمان فعالية التحقيق والوصول إلى أدلة رقمية ذات قيمة إثباتية. كما تبرز أهمية التسخير الفني في ضمان ما يُعرف بـ سلامة الدليل الرقمي (Digital Integrity)، وذلك من خلال احترام المعايير التقنية المعتمدة في جمع الأدلة، كعدم تغيير البيانات الأصلية، وتوثيق جميع مراحل التعامل معها، وهو ما يعزز حجيتها أمام القضاء ويحد من إمكانية الطعن فيها[1].

كما قد يمتد هذا التسخير إلى إلزام مزودي الخدمات بتقديم البيانات أو سجلات الاتصال، في إطار احترام القواعد القانونية المنظمة لذلك[2].

غير أن اللجوء إلى التسخير لاسيما الفني منه، يظل خاضعا لرقابة قانونية صارمة تفرض تحديد مهمة الخبير بدقة، وعدم تجاوز نطاق التسخير، واحترام سرية التحقيق، مع إمكانية مساءلته في حال الإخلال بالتزاماته، ويهدف ذلك إلى منع أي مساس غير مشروع بالحياة الخاصة الرقمية التي تظل محل حماية دستورية وقانونية، ويضاف إلى ذلك أن تدخل الخبراء التقنيين يطرح إشكالية مدى حجية أعمالهم، حيث يميز الفقه بين الدور الفني البحت للخبير الذي يقتصر على تقديم المعطيات التقنية وبين سلطة التقدير التي تبقى حكرا على القاضي مما يكرس مبدأ حرية القاضي في تكوين اقتناعه انطلاقا من مختلف عناصر الإثبات[3].

وقد ذهب جانب من الفقه إلى اعتبار التسخير الفني أحد أبرز مظاهر تطور التحقيق الجنائي في البيئة الرقمية لما يوفره من فعالية في كشف الجرائم، غير أنه يستوجب في المقابل تعزيز الضمانات القانونية حفاظا على التوازن بين متطلبات الأمن وحقوق الأفراد[4].

---

[1] محمد حزيط، الجرائم المعلوماتية وأدلة الإثبات الرقمية، دار هومة، الجزائر، 2015، ص133.

[2] المادة 5 من القانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، مرجع سابق.

[3] عبد القادر عدو، حماية الحياة الخاصة في البيئة الرقمية، دار بلقيس، الجزائر، 2020، ص57.

[4] المرجع نفسه، ص81.

ومن زاوية أخرى، يظهر تنظيم الجهات المختصة بالتفتيش الإلكتروني أن المشرع الجزائري يتجه نحو تبني نموذج التحقيق متعدد التخصصات، الذي يجمع بين الخبرة القانونية والتقنية، في مواجهة الجرائم المعلوماتية التي تتسم بالتعقيد والتطور المستمر. غير أن نجاح هذا النموذج يظل مرتبطًا بمدى التنسيق بين مختلف المتدخلين، وضمان تكوينهم المستمر في المجال الرقمي[1].

الفرع الثاني: مراحل التفتيش الإلكتروني.

يعد التفتيش الإلكتروني من الإجراءات الجزائية المستحدثة التي فرضها التطور التكنولوجي، حيث لم يعد التفتيش يقتصر على المحل المادي التقليدي، بل امتد ليشمل المعطيات الرقمية المخزنة داخل الأنظمة المعلوماتية والشبكات وقواعد البيانات، ويتميز هذا الإجراء بخصوصية تقنية وقانونية في ان واحد، إذ يتعامل مع أدلة غير مادية قابلة للتغيير أو الإتلاف أو الإخفاء في أي لحظة، وهو ما يفرض اعتماد إجراءات دقيقة ومترابطة تضمن تحقيق التوازن بين فعالية التحقيق الجنائي وحماية الحقوق والحريات الأساسية[2].

وتقوم إجراءات التفتيش الإلكتروني على سلسلة من المراحل المتكاملة، تبدأ بالتحضير التقني، ثم الولوج إلى النظام المعلوماتي، فالبحث والتنقيب، ثم تثبيت وجمع الدليل الرقمي، لتصل في صورتها الحديثة إلى التفتيش الإلكتروني عن بُعد، مع مرحلة أخيرة تتمثل في تحليل واستغلال الدليل الرقمي قضائيًا[3]. ويُلاحظ أن هذا التدرج ليس شكليًا، بل هو تدرج وظيفي يهدف إلى تقليل مخاطر العبث بالمعطيات الرقمية وضمان سلامة الدليل من الناحية الفنية والقانونية.

[1] أحسن بوسقيعة، التحقيق القضائي، مرجع سابق، ص342.

[2] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، مرجع سابق، ص 45.

[3] أحسن بوسقيعة، التحقيق القضائي، مرجع سابق، ص312.

أولًا: المرحلة التحضيرية للتفتيش الإلكتروني.

تعد المرحلة التحضيرية الأساس الذي تبنى عليه باقي إجراءات التفتيش الإلكتروني، حيث يتم فيها تحديد نطاق العملية بدقة، من خلال تحديد الأجهزة أو الحسابات أو الأنظمة المعلوماتية المستهدفة وذلك من اجل منع التوسع غير المبرر في جمع البيانات، وضمان احترام مبدأ التناسب بين خطورة الجريمة ونطاق الإجراء[1].

كما تكتسي هذه المرحلة أهمية خاصة في الجرائم المعلوماتية المعقدة حيث قد تكون الأدلة موزعة عبر عدة أجهزة أو منصات حسابية، مما يستوجب إعداد خطة تقنية مسبقة تعتمد على تحليل البنية الرقمية للهدف قبل التنفيذ.

وتشمل هذه المرحلة كذلك دراسة البنية التقنية للنظام المعلوماتي محل التفتيش، من حيث طبيعة الحماية المعتمدة عليه، سواء كانت تشفيرا أو كلمات مرور أو أنظمة تحقق متعددة، ويؤدي هذا التقييم دورا أساسيا في تحديد الوسائل التقنية المناسبة للدخول إلى النظام دون الإضرار بالبيانات الأصلية[2].

كما أن تطور تقنيات الحماية الرقمية خاصة التشفير المتقدم (End-to-End Encryptions)، جعل من هذه المرحلة أكثر تعقيدا إذ لم يعد الوصول إلى البيانات مجرد مسألة تقنية بل أصبح يتطلب أحيانا تعاونا قضائيا دوليا أو تسخير خبرات متخصصة عالية المستوى.

وتقتضي هذه المرحلة أيضا اتخاذ تدابير احترازية مسبقة نظرا لاحتمال تعرض البيانات للحذف أو التعديل عن بعد فور اكتشاف عملية التفتيش، مما يستوجب أحيانا عزل النظام عن

[1] رشيدة بوكر، مرجع سابق، ص122.

[2] عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، مرجع سابق، ص 89.

الشبكة أو تأمينه تقنيا قبل الشروع في التنفيذ[1]، ويعرف هذا الإجراء في المجال التقني بـ"عزل البيئة الرقمية(Digital Isolation) "، وهو إجراء وقائي أساسي للحفاظ على سلامة الأدلة.

ثانيًا: مرحلة الولوج إلى النظام المعلوماتي.

تمثل هذه المرحلة نقطة الانطلاق الفعلية للتفتيش الإلكتروني، حيث يتم الدخول إلى النظام المعلوماتي محل البحث سواء بشكل مباشر عبر الأجهزة المحجوزة أو بشكل غير مباشر عبر الشبكات أو الحسابات الرقمية.

ويعد هذا الولوج من أكثر المراحل حساسية نظرا لكون أي تدخل غير مضبوط قد يؤدي إلى تغيير البيانات أو إتلافها، مما يؤثر على حجيتها القانونية، لذلك يتم التعامل مع هذه المرحلة وفق ضوابط تقنية دقيقة تضمن الحفاظ على سلامة الدليل الرقمي[2].

ومن الناحية العملية يتم اللجوء إلى تقنيات النسخ المؤقت أو التشغيل في بيئة معزولة (Sandbox Environment)لضمان عدم المساس بالبيانات الأصلية أثناء عملية الولوج، وهو ما يعكس تطور أساليب العمل الجنائي الرقمي.

كما قد يواجه المحققون خلال هذه المرحلة عوائق تقنية تتمثل في أنظمة التشفير أو كلمات المرور أو الحماية السحابية، مما يستدعي اللجوء إلى وسائل تقنية متخصصة أو إلى الخبرة الفنية، في إطار ما يسمح به القانون من تسخير للخبراء[3].

ويلاحظ أن المشرع الجزائري من خلال قانون الإجراءات الجزائية، وإن لم يفصل بشكل دقيق في التقنيات الرقمية إلا أنه أرسى قواعد عامة تسمح بالاستعانة بالخبرة كلما تطلب الأمر ذلك، وهو ما يفتح المجال لتكييف الإجراءات مع التطور التكنولوجي.

---

[1] أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، مرجع سابق، ص318.

[2] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، مرجع سابق، ص67.

[3] علي حسن محمد طوالبة، شرح قانون الإجراءات الجزائية، مرجع سابق، ص214.

ويخضع هذا الإجراء من حيث المشروعية إلى القواعد العامة للتفتيش والحجز المنصوص عليها في قانون الإجراءات الجزائية الجزائري، بما يضمن عدم المساس بالحقوق الدستورية للأفراد دون سند قانوني[1]، خاصة الحق في الخصوصية وسرية الاتصالات.

ثالثًا: مرحلة البحث والتنقيب عن الأدلة الرقمية.

تعد هذه المرحلة جوهر التفتيش الإلكتروني حيث يتم فيها فحص النظام المعلوماتي بحثا عن الأدلة الرقمية ذات الصلة بالجريمة، ويشمل ذلك تحليل الملفات الرقمية، الوثائق، الصور، مقاطع الفيديو، الرسائل الإلكترونية، سجلات النظام، وسجلات التصفح.

ولا يقتصر البحث على البيانات الظاهرة فقط بل يمتد ليشمل البيانات المخفية والمحذوفة، والتي يمكن استرجاعها باستخدام تقنيات جنائية متقدمة، مما يعزز من فعالية هذا الإجراء مقارنة بالتفتيش التقليدي[2].

ويعد علم الأدلة الرقمية (Digital Forensics) من أهم العلوم المساندة في هذه المرحلة، حيث يتيح تقنيات متقدمة لاستعادة البيانات وتحليلها وربطها بسلوك المستخدمين داخل النظام المعلوماتي.

كما يتم في هذه المرحلة تحليل البيانات الوصفية(Metadata) ، التي تكشف معلومات دقيقة حول تاريخ إنشاء الملفات وتعديلها ومصدرها، وهو ما يسمح بإعادة بناء التسلسل الزمني للأحداث المرتبطة بالجريمة[3].

وتكتسي هذه البيانات أهمية خاصة في الإثبات الجنائي لأنها غالبا ما تكون غير قابلة للتلاعب المباشر مقارنة بمحتوى الملفات نفسه، مما يجعلها عنصرا قويا في تكوين القناعة القضائية.

---

[1] علي حسن محمد طوالبة، مرجع سابق، ص220.

[2] عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، مرجع سابق، ص134.

[3] رشيدة بوكر، مرجع سابق، ص156.

وتتميز هذه المرحلة بكونها تتطلب دقة تقنية عالية مما يجعل الاستعانة بالخبرة الفنية أمرا ضروريا في العديد من الحالات لضمان الفهم الصحيح للبيانات المستخرجة وتحليلها بشكل علمي سليم[1].

رابعًا: مرحلة تثبيت وجمع الدليل الرقمي.

بعد عملية البحث يتم الانتقال إلى مرحلة تثبيت الدليل الرقمي، وهي مرحلة محورية تهدف إلى ضمان إمكانية استخدامه أمام القضاء دون الطعن في صحته أو سلامته.

ويتم ذلك من خلال إنشاء نسخ جنائية مطابقة للأصل(Forensic Imaging) ، بحيث يتم التعامل مع النسخة بدل البيانات الأصلية حفاظا عليها من أي تعديل أو تلف[2].

كما يتم اعتماد تقنيات التحقق من سلامة البيانات مثل البصمة الرقمية(Hash Value) ، التي تسمح بكشف أي تغيير قد يطرأ على الدليل بعد استخراجه، مما يعزز من حجيته القانونية[3].

وتعد هذه التقنية من أهم ضمانات العدالة الرقمية، لأنها توفر معيارًا علميًا دقيقًا لإثبات أن الدليل لم يتعرض لأي تعديل منذ لحظة استخراجه.

ويتم كذلك توثيق جميع العمليات التي تمت على الدليل ضمن ما يعرف بسلسلة الحيازة (Chain of Custody)، التي تضمن تتبع مسار الدليل منذ لحظة جمعه إلى غاية تقديمه أمام القضاء[4].

ويعتبر هذا التوثيق شرطا جوهريا لقبول الدليل الرقمي أمام الجهات القضائية، إذ يضمن الشفافية ويمنع الطعن في سلامة الإجراءات.

---

[1] أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، مرجع سابق، ص331.

[2] عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، مرجع سابق، ص 101.

[3] المرجع نفسه، ص105.

[4] رشيدة بوكر، مرجع سابق، ص172.

خامسًا: تحليل واستغلال الدليل الرقمي.

يعد تحليل واستغلال الدليل الرقمي المرحلة النهائية في إجراءات التفتيش الإلكتروني، حيث يتم فيها تحليل البيانات المستخرجة وربطها بوقائع الجريمة، ويهدف هذا التحليل إلى تحويل المعطيات الرقمية إلى أدلة قانونية قابلة للاعتماد أمام القضاء.

ويتم في هذه المرحلة استخدام أدوات تحليل رقمية متقدمة لمعالجة كميات كبيرة من البيانات واستخراج العلاقات والأنماط الرقمية التي قد تكون ذات دلالة إثباتية.

كما يتم تفسير النتائج في ضوء القواعد القانونية المعمول بها، من أجل تحديد مدى حجيتها ومدى إمكانية اعتمادها في الإثبات الجنائي، مما يجعل هذه المرحلة حلقة وصل بين الجانب التقني والجانب القانوني[1].

ويضاف إلى ذلك أن التحليل قد يشمل تقنيات الذكاء الاصطناعي في بعض الأنظمة الحديثة، مما يفتح نقاشا فقهيا حول مدى حجية النتائج الآلية في الإثبات الجنائي، وحدود الاعتماد على الخوارزميات في تكوين القناعة القضائية[2].

المطلب الثاني: الضمانات القانونية لحماية الحياة الخاصة أثناء ممارسة سلطة التحقيق

إن الطبيعة الاستثنائية لإجراء التفتيش الإلكتروني وما يرافقه من قدرة على النفاذ إلى أدق تفاصيل الحياة الخاصة والمعطيات الرقمية للأفراد، جعلت منه إجراء يقع على خط التماس مع الحقوق والحريات الأساسية المكرسة دستوريا وأمام هذا الواقع التقني المعقد، لم يكتفِ المشرع الجزائري بالقواعد التقليدية للتفتيش، بل استحدث منظومة متكاملة من الضمانات تهدف

[1] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، مرجع سابق، ص 150.

[2] رشيدة بوكر، مرجع سابق، ص190.

إلى سد الثغرات التي قد تفرزها البيئة الرقمية، وذلك بغية كبح جماح سلطات التحقيق ومنعها من الانحراف بالإجراء عن غايته المنشودة في كشف الحقيقة.

وتتجسد هذه المنظومة في محورين متكاملين؛ يمثل الأول الضمانات الإجرائية التي تفرض قيوداً شكلية وموضوعية صارمة على عملية التفتيش منذ لحظة التفكير فيه وحتى تمام تنفيذه، بينما يمثل المحور الثاني الرقابة القضائية الفعالة التي تعد صمام الأمان والحصن المنيع لضمان مشروعية تلك الإجراءات وعدم تحولها إلى وسيلة للاعتداء التعسفي على الحرمات. وبناءً على ذلك، سنقوم بدراسة هذه الضمانات من خلال تقسيم هذا المطلب إلى فرعين: نخصص الفرع الأول لتسليط الضوء على الضمانات الإجرائية المقيّدة لسلطة التحقيق، في حين نتناول في الفرع الثاني دور الرقابة القضائية في حماية الحياة الخاصة للمواطنين.

الفرع الأول: الضمانات الإجرائية المقيدة لسلطة التحقيق

يثير التفتيش الإلكتروني إشكالات قانونية وإجرائية معقدة بالنظر إلى طبيعته الخاصة وارتباطه المباشر بالحق في الخصوصية الرقمية، إذ لم تعد الحياة الخاصة تقتصر على المسكن التقليدي أو المراسلات الورقية، بل أصبحت تشمل المعطيات الإلكترونية والرسائل الرقمية والحسابات الشخصية وقواعد البيانات المخزنة داخل الأنظمة المعلوماتية[1]، وقد أدى التطور الهائل في وسائل الاتصال والتكنولوجيا الحديثة إلى اتساع نطاق الجرائم المعلوماتية، الأمر الذي دفع المشرع الجزائري إلى استحداث قواعد قانونية وإجرائية خاصة تمكن سلطات التحقيق من مكافحة هذا النوع من الجرائم، مع ضرورة وضع ضمانات تحد من تعسف السلطة وتحافظ على الحقوق والحريات الأساسية للأفراد[2].

ويعد التفتيش الإلكتروني من أخطر إجراءات التحقيق الجنائي، لأنه يسمح للسلطات المختصة بالولوج إلى نظم معلوماتية قد تحتوي على كم هائل من البيانات الشخصية والأسرار

[1] علي حسن محمد الطوالبة، مرجع سابق، ص10.

[2] علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المكتب الجامعي الحديث، 2012، ص39.

المهنية والمعطيات الخاصة، وهو ما يجعل أي استعمال غير مشروع لهذا الإجراء يشكل انتهاكًا صارخًا للحياة الخاصة[1]، لذلك حرص المشرع على تقييد سلطة التحقيق بمجموعة من الضمانات الإجرائية التي تهدف إلى تحقيق التوازن بين مصلحة المجتمع في مكافحة الجريمة من جهة، وضرورة حماية الحقوق الفردية من جهة أخرى.

وتستند هذه الضمانات أساسا إلى مبدأ الشرعية الإجرائية، الذي يقتضي أن تكون جميع إجراءات التحقيق، ومنها التفتيش الإلكتروني، خاضعة للقانون وممارسة في الحدود التي يرسمها[2]: فلا يجوز للسلطة المختصة مباشرة أي تفتيش خارج الحالات التي يجيزها القانون، أو دون احترام الشروط الشكلية والموضوعية المحددة قانونا، وإلا تعرّض الإجراء للبطلان واستُبعد الدليل المستخلص منه.

ويعتبر الإذن القضائي المسبق من أهم الضمانات الإجرائية المقيدة لسلطة التحقيق في مجال التفتيش الإلكتروني، لأن هذا الإجراء ينطوي على مساس مباشر بالحياة الخاصة وحرمة البيانات الإلكترونية. ولهذا نصّ الدستور الجزائري على حماية الحياة الخاصة وسرية المراسلات والاتصالات، ومنع المساس بها إلا بأمر صادر عن السلطة القضائية المختصة ومعلل قانونًا[3]. كما أكد قانون الإجراءات الجزائية ضرورة صدور إذن بالتفتيش من الجهة القضائية المختصة، مع تحديد محل التفتيش وسببه والغرض منه بصورة دقيقة[4].

ويكتسي التسبيب القضائي أهمية خاصة في مجال التفتيش الإلكتروني، لأن طبيعة البيانات الرقمية تسمح بالوصول إلى معلومات واسعة تتجاوز في كثير من الأحيان نطاق الجريمة محل التحقيق، ولذلك يجب أن يكون الإذن القضائي واضحًا ومحددًا من حيث

[1] أحسن بوسقيعة، التحقيق القضائي، مرجع سابق، ص83.

[2] يوسف دلاّندة، قانون الإجراءات الجزائية، دار هومة، الجزائر، 2001، ص46.

[3] المادة 47 والمادة 48 من الدستور الجزائري المعدل.

[4] المواد 44 إلى 47 من قانون الإجراءات الجزائية الجزائري.

الأشخاص والأجهزة والبيانات المراد تفتيشها، منعا لأي توسع تعسفي في الإجراء[1]. فكلما كان الإذن عاما أو غامضا، زادت احتمالات المساس غير المشروع بالحياة الخاصة.

ومن أهم الضمانات كذلك ضرورة احترام مبدأ التناسب بين إجراء التفتيش وخطورة الجريمة محل البحث، فلا يجوز اللجوء إلى وسائل تفتيش واسعة تمس بحقوق الأفراد وحرياتهم إذا كانت الجريمة بسيطة أو إذا كان بالإمكان الحصول على الدليل بوسائل أقل مساسًا بالحياة الخاصة[2]. ويُعدّ هذا المبدأ من المبادئ الأساسية التي تحكم الإجراءات الجزائية الحديثة، خاصة في مجال الجرائم المعلوماتية التي تتميز بحساسية المعطيات المتداولة داخلها.

كما يلتزم القائمون بالتفتيش الإلكتروني باحترام نطاق الإذن القضائي وعدم تجاوزه، بحيث يقتصر التفتيش على البيانات والمعطيات المرتبطة مباشرة بالجريمة موضوع التحقيق، دون الامتداد إلى بيانات أخرى لا علاقة لها بالفعل الإجرامي[3]. ويعتبر هذا القيد ضروريا لأن الأنظمة المعلوماتية الحديثة تحتوي غالبًا على بيانات شخصية ومهنية وعائلية ومالية شديدة الخصوصية، وهو ما يجعل أي توسع غير مبرر في التفتيش اعتداءً على الحق في الخصوصية الرقمية.

وقد كرس المشرع الجزائري هذا القيد من خلال المادة 05 من القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، حيث أجاز تمديد التفتيش إلى منظومة معلوماتية أخرى فقط إذا وُجدت أسباب تدعو للاعتقاد بأن البيانات محل البحث مخزنة فيها، مع ضرورة إعلام السلطة القضائية المختصة مسبقا بذلك[4]. ويتضح من هذا النص أن المشرع لم يمنح سلطات التحقيق حرية

---

[1] رضا هميسي، مرجع سابق، ص162.

[2] عبد الله احمد هلالي، تفتيش نظم الحاسب الالي وضمانات المتهم المعلوماتي، دار النهضة العربية، القاهرة، ص180.

[3] علي حسن محمد الطوالبة، المرجع السابق، ص59.

[4] المادة 05 من القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مرجع سابق.

مطلقة في الولوج إلى الأنظمة المعلوماتية، وإنما أخضع ذلك لرقابة قضائية وضوابط قانونية دقيقة.

ومن الضمانات المهمة أيضا احترام سرية المعطيات والبيانات التي يتم الاطلاع عليها أثناء التفتيش الإلكتروني، لأن القائمين بالتفتيش قد يطلعون بحكم مهامهم على معلومات تمسّ الحياة الخاصة للأفراد أو أسرارهم المهنية أو التجارية. ولهذا فإن استعمال هذه البيانات خارج إطار التحقيق أو إفشاءها يُعدّ خرقًا للواجب القانوني ولمبدأ حماية الخصوصية[1].

وتزداد أهمية هذه الضمانة في ظل الطبيعة التقنية للجرائم المعلوماتية، حيث يمكن للجهات المختصة أثناء التفتيش الوصول إلى الحسابات البنكية والرسائل الإلكترونية والصور والملفات الشخصية والمعطيات الطبية وغيرها من البيانات ذات الطابع الحساس. ولذلك فإن احترام مبدأ السرية يُعدّ من أهم القيود المفروضة على سلطة التحقيق أثناء مباشرة التفتيش الإلكتروني[2].

كما يلتزم القائمون بالتفتيش بالمحافظة على سلامة الدليل الإلكتروني وعدم تغييره أو إتلافه أثناء عملية الفحص والمعاينة التقنية، لأن الدليل الرقمي يتميز بسهولة التعديل أو المحو أو النقل في وقت قصير[3]، ولهذا تفرض القواعد الإجرائية الحديثة ضرورة توثيق جميع مراحل التفتيش الإلكتروني، مع بيان الوسائل التقنية المستعملة وكيفية استخراج البيانات والمحافظة عليها لضمان حجيتها أمام القضاء.

ومن الضمانات الإجرائية الجوهرية كذلك الاستعانة بالخبرة الفنية أثناء تنفيذ التفتيش الإلكتروني، لأن هذا النوع من التفتيش يتطلب معرفة تقنية متخصصة بطبيعة الأنظمة المعلوماتية وطرق استخراج الأدلة الرقمية[4]، ولذلك أجاز المشرع للسلطات المختصة الاستعانة

---

[1] محمد عبد الله أبو بكر سلامة، موسوعة جرائم المعلوماتية: جرائم الكمبيوتر والانترنت، المكتب العربي الحديث، القاهرة، الطبعة الأولى، 2006، ص214.

[2] خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2009، ص177.

[3] عبد الله أحمد هلالي، حجية المخرجات الكمبيوترية في الإثبات الجنائي، دار النهضة العربية، القاهرة، 1997، ص46.

[4] علي عدنان الفيل، مرجع سابق، ص39.

بأشخاص ذوي كفاءة تقنية لمساعدتها أثناء التفتيش، خاصة عندما يتعلق الأمر بأنظمة معقدة أو بيانات مشفرة يصعب التعامل معها بالوسائل التقليدية[1].

وتكمن أهمية الخبرة التقنية في ضمان تنفيذ التفتيش بصورة قانونية وفنية سليمة، وتفادي ضياع الأدلة أو العبث بها أثناء الفحص، كما تساعد الجهات القضائية على فهم الجوانب التقنية المرتبطة بالجريمة المعلوماتية. ولهذا أصبح التعاون بين المحققين والخبراء التقنيين من أهم متطلبات التحقيق الحديث في الجرائم الإلكترونية[2].

ومن الضمانات الأساسية أيضا ضرورة احترام حقوق الدفاع أثناء التفتيش الإلكتروني، وذلك من خلال تمكين الشخص المعني بالإجراء من معرفة سبب التفتيش والطعن في مشروعيته متى كان ذلك ممكنا قانونيا[3]. كما يحق له التمسك ببطلان التفتيش إذا تم خارج الحدود التي رسمها القانون أو في غياب الضمانات الشكلية المقررة.

وفي السياق ذاته يعد حضور الشخص المعني بالتفتيش أو من يمثله ضمانة مهمة لتحقيق الشفافية ومنع التعسف، إلا أن المشرع أجاز في بعض الحالات الاستثنائية مباشرة التفتيش دون حضوره خاصة إذا تعلق الأمر بجرائم معلوماتية التي يخشى فيها ضياع الأدلة أو إتلافها بسرعة[4]. ويبرر ذلك بخصوصية الدليل الإلكتروني الذي يمكن محوه أو تعديله عن بعد في ثوانٍ معدودة.

كما تخضع إجراءات التفتيش الإلكتروني لرقابة القضاء، باعتبارها أهم ضمانة لحماية الحياة الخاصة في مواجهة سلطة التحقيق، حيث يملك القاضي مراقبة مدى احترام الضوابط

[1] المادة 05 فقرة 04 من القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مرجع سابق.

[2] هبة هروال نبيلة، مرجع سابق، ص87.

[3] المادة 76 من القانون 14/25 يتضمن قانون الإجراءات الجزائية الجزائري، مرجع سابق.

[4] أحسن بوسقيعة، مرجع سابق، ص85.

القانونية أثناء تنفيذ التفتيش، كما يمكنه استبعاد الأدلة المتحصّل عليها بطريقة غير مشروعة[1]. ويُعتبر هذا المبدأ تجسيدًا لفكرة سمو الشرعية الإجرائية وخضوع السلطة العامة للقانون.

وقد أكدت المحكمة العليا الجزائرية على ضرورة احترام الإجراءات القانونية المتعلقة بالتفتيش، معتبرة أن مخالفة القواعد الجوهرية المنظمة له تؤدي إلى بطلان الإجراء وما يترتب عنه من آثار[2]، ويظهر ذلك حرص القضاء الجزائري على حماية الحقوق والحريات الأساسية وعدم التضحية بها بحجة مكافحة الجريمة المعلوماتية.

وعليه، يتبين أن المشرع الجزائري حاول إرساء منظومة من الضمانات الإجرائية التي تهدف إلى الحد من خطورة التفتيش الإلكتروني وضمان عدم تحوله إلى وسيلة للمساس التعسفي بالحياة الخاصة، غير أن فعالية هذه الضمانات تبقى مرتبطة بمدى احترام السلطات المختصة لها عمليا، وبمدى تكوين القائمين بالتحقيق في المجال التقني والقانوني، بما يضمن تحقيق التوازن بين متطلبات الأمن الرقمي وحماية الحقوق والحريات الفردية.

الفرع الثاني: الرقابة القضائية ودورها في حماية الحياة الخاصة.

تعد الرقابة القضائية من أهم الآليات القانونية التي اعتمدها المشرع لحماية الحياة الخاصة أثناء مباشرة إجراءات التفتيش الإلكتروني، باعتبار أن هذا النوع من التفتيش ينطوي على مساس مباشر بالمعطيات الشخصية والاتصالات الإلكترونية والبيانات الرقمية المخزنة داخل الأنظمة المعلوماتية[3]، فالتطور التكنولوجي الذي رافق ظهور الجرائم المعلوماتية أدى إلى توسع صلاحيات سلطات البحث والتحقيق، الأمر الذي استوجب إخضاع هذه الصلاحيات

[1] يوسف دلاّندة، المرجع السابق، ص52.

[2] قرار المحكمة العليا، الغرفة الجنائية، رقم 165609، بتاريخ 1997/07/30، المجلة القضائية، العدد الثاني، 1997، ص250.

[3] علي حسن محمد الطوالبة، مرجع سابق، ص13.

لرقابة قضائية فعالة تحول دون التعسف في استعمالها وتحافظ على التوازن بين مقتضيات مكافحة الجريمة وضمان احترام الحقوق والحريات الفردية[1].

وتكمن أهمية الرقابة القضائية في كونها تمثل ضمانة أساسية لحماية مبدأ الشرعية الإجرائية، إذ لا يجوز مباشرة التفتيش الإلكتروني أو اتخاذ أي إجراء يمس بالحياة الخاصة إلا تحت إشراف السلطة القضائية ووفق الضوابط التي يحددها القانون[2]، ولذلك فإن القضاء لا يقتصر دوره على إصدار الأوامر المتعلقة بالتفتيش بل يمتد إلى مراقبة مشروعية الإجراءات المتخذة ومدى احترامها للحدود القانونية المقررة.

وقد حرص الدستور الجزائري على تكريس هذه الحماية من خلال التأكيد على أن المساس بحرمة الحياة الخاصة وسرية المراسلات لا يكون إلا بأمر صادر عن السلطة القضائية المختصة[3]، ويُستفاد من ذلك أن الرقابة القضائية تعد شرطا جوهريا لمشروعية إجراءات التفتيش الإلكتروني، وأن أي تدخل خارج هذا الإطار يُعتبر انتهاكا للحقوق الدستورية المقررة للأفراد.

وتظهر الرقابة القضائية بصورة واضحة منذ المرحلة الأولى لإجراءات التفتيش الإلكتروني، حيث يتعين على سلطات التحقيق الحصول على إذن قضائي مسبق قبل مباشرة التفتيش، يتضمن تحديد طبيعة الجريمة والأجهزة أو الأنظمة المعلوماتية محل التفتيش والغاية منه[4]. ويهدف هذا الإذن إلى منع سلطات التحقيق من التوسع غير المشروع في استعمال صلاحياتها، خاصة أن البيئة الرقمية تسمح بالوصول إلى بيانات واسعة قد لا تكون لها علاقة مباشرة بالجريمة محل التحقيق.

كما تبرز الرقابة القضائية من خلال سلطة قاضي التحقيق في تقدير مدى ضرورة اللجوء إلى التفتيش الإلكتروني، إذ لا يجوز إصدار الإذن إلا إذا وُجدت دلائل كافية تبرر اتخاذ هذا

---

[1] علي عدنان الفيل ، مرجع سابق، ص39.

[2] يوسف دلاّندة، مرجع سابق، ص46.

[3] المادة 47 و48 من الدستور الجزائري، مرجع سابق.

[4] المواد من75الى79 من القانون 14/25 المتضمن قانون الإجراءات الجزائية، مرجع سابق.

الإجراء[1]، ويعد هذا القيد من أهم الضمانات التي تحول دون استعمال التفتيش الإلكتروني بصورة تعسفية أو لمجرد الشكوك العامة غير المؤسسة قانونا.

ويمارس القضاء كذلك رقابة على نطاق التفتيش الإلكتروني وحدوده، حيث يلتزم المحققون بعدم تجاوز البيانات أو الأنظمة المحددة في الإذن القضائي[2]، فإذا تجاوزت سلطات التحقيق حدود الإذن أو قامت بالاطلاع على بيانات لا علاقة لها بالجريمة، أمكن الدفع ببطلان الإجراء لوقوعه مخالفا لمبدأ الشرعية الإجرائية.

ويكتسي هذا الأمر أهمية خاصة في البيئة الرقمية لأن التفتيش الإلكتروني قد يسمح بالاطلاع على صور شخصية أو مراسلات خاصة أو بيانات مالية وصحية ومهنية، وهو ما يجعل الرقابة القضائية ضرورية لمنع المساس غير المشروع بالحياة الخاصة[3]، لذلك فإن القضاء يعتبر الحصن الأساسي الذي يضمن عدم تحول التفتيش الإلكتروني إلى وسيلة للمراقبة الشاملة أو الاعتداء على الحرية الفردية.

ومن صور الرقابة القضائية أيضا مراقبة مدى احترام مبدأ التناسب بين إجراء التفتيش وخطورة الجريمة محل التحقيق، فلا يجوز أن تكون إجراءات التفتيش مبالغًا فيها مقارنة بالفعل الإجرامي المرتكب[4]. ويقتضي ذلك أن يوازن القاضي بين مصلحة المجتمع في كشف الحقيقة ومصلحة الفرد في حماية حياته الخاصة، بحيث لا يتم التضحية بالحقوق الأساسية إلا في الحدود الضرورية التي تقتضيها العدالة الجنائية.

كما تمتد الرقابة القضائية إلى مرحلة تنفيذ التفتيش الإلكتروني، حيث يخضع القائمون بالتفتيش لإشراف السلطة القضائية المختصة، ويتعين عليهم الالتزام بالقواعد القانونية المتعلقة

---

[1] أحسن بوسقيعة، التحقيق القضائي، مرجع سابق، ص83.

[2] رضا هميسي، مرجع سابق، ص159.

[3] خالد ممدوح إبراهيم، مرجع سابق، ص177.

[4] عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، ص112.

بحفظ الأدلة الرقمية وسلامتها وعدم العبث بها[1]. ويهدف هذا الإشراف إلى ضمان نزاهة الإجراءات والمحافظة على حجية الدليل الإلكتروني أمام القضاء.

ويُعدّ توثيق إجراءات التفتيش الإلكتروني من أهم مظاهر الرقابة القضائية، إذ يجب إثبات جميع الخطوات المتخذة أثناء التفتيش في محاضر رسمية تتضمن وصف الأجهزة والبيانات المضبوطة والوسائل التقنية المستعملة[2]. وتكمن أهمية هذا التوثيق في تمكين القضاء من مراقبة مدى احترام القواعد القانونية والفنية أثناء تنفيذ التفتيش.

كما يملك القضاء سلطة استبعاد الأدلة الإلكترونية المتحصّل عليها بطرق غير مشروعة، تطبيقًا لمبدأ بطلان الإجراءات المخالفة للقانون[3]. فإذا تم التفتيش دون إذن قضائي، أو تم خارج الحدود القانونية، أو ترتب عنه انتهاك غير مشروع للحياة الخاصة، فإن الدليل المستخلص منه يفقد حجيته القانونية ولا يجوز الاعتماد عليه في الإدانة.

وقد أكد القضاء الجزائري على أهمية احترام الضمانات القانونية المتعلقة بالتفتيش، حيث اعتبرت المحكمة العليا أن مخالفة الإجراءات الجوهرية المنظمة للتفتيش تؤدي إلى بطلان الإجراء وما يترتب عنه من آثار[4]. ويُظهر هذا الاتجاه القضائي حرص القضاء على حماية الحقوق والحريات الأساسية وعدم السماح بتبرير انتهاكها تحت ذريعة مكافحة الجريمة.

ومن جهة أخرى، تساهم الرقابة القضائية في حماية مبدأ سرية المعطيات الشخصية أثناء التفتيش الإلكتروني، إذ يراقب القاضي كيفية التعامل مع البيانات المضبوطة ومدى احترام خصوصية الأفراد[5]. فالمعطيات الإلكترونية قد تتضمن معلومات شخصية دقيقة لا يجوز تداولها أو استعمالها خارج نطاق التحقيق القضائي.

---

[1] عبد الله أحمد هلالي، مرجع سابق، ص48.

[2] علي عدنان الفيل، مرجع سابق، ص51.

[3] يوسف دلاّندة، المرجع السابق، ص52.

[4] قرار المحكمة العليا، الغرفة الجنائية، رقم 165609، بتاريخ 1997/07/30، المجلة القضائية، العدد الثاني، 1997، ص250.

[5] محمد عبد الله أبو بكر سلامة، مرجع سابق، ص214.

وتزداد أهمية هذه الرقابة مع تطور تقنيات التخزين السحابي والشبكات العابرة للحدود، حيث أصبحت البيانات الإلكترونية تنتقل بسهولة بين الدول وتخزن أحيانا خارج الإقليم الوطني، الأمر الذي يطرح صعوبات قانونية تتعلق بالاختصاص القضائي وحماية الخصوصية الرقمية[1]. ولهذا أصبح التعاون القضائي الدولي من الوسائل الأساسية لضمان مشروعية إجراءات التفتيش الإلكتروني واحترام الحقوق الأساسية للأفراد.

كما تلعب الرقابة القضائية دورا مهما في حماية حقوق الدفاع إذ تتيح للمتهم أو دفاعه الطعن في مشروعية التفتيش الإلكتروني وطلب إبطال الإجراءات المخالفة للقانون[2]. ويعتبر هذا الحق من أهم مظاهر المحاكمة العادلة، لأنه يسمح بمراقبة شرعية الأدلة الرقمية ومدى احترام الضمانات الإجرائية أثناء الحصول عليها.

ولا تقتصر الرقابة القضائية على القضاء الوطني فقط، بل أصبحت الاتفاقيات الدولية المتعلقة بحقوق الإنسان تؤكد بدورها ضرورة إخضاع إجراءات التفتيش الإلكتروني لرقابة قضائية فعالة، حمايةً للحياة الخاصة ومنعًا للتعسف في استعمال الوسائل التقنية الحديثة[3]. ويظهر ذلك أن حماية الخصوصية الرقمية أصبحت من المبادئ الأساسية المعترف بها دوليا في مواجهة التطور المتسارع لوسائل المراقبة الإلكترونية.

كما أن الرقابة القضائية تساهم في تعزيز الثقة في العدالة الجنائية الرقمية، لأن خضوع إجراءات التفتيش لرقابة مستقلة ومحايدة يضمن احترام القانون ويمنع إساءة استعمال السلطة[4].

وعليه يتضح أن الرقابة القضائية تمثل ضمانة جوهرية لحماية الحياة الخاصة أثناء ممارسة سلطة التحقيق في مجال التفتيش الإلكتروني، إذ تفرض حدودا قانونية على سلطات البحث والتحقيق وتمنعها من التوسع التعسفي في المساس بالبيانات والمعطيات الشخصية،

---

[1] عبد الله أحمد هلالي، اتفاقية بودابست لمكافحة جرائم المعلوماتية، دار النهضة العربية، 2007، ص76.

[2] المادة 80 من القانون 14/25 يتضمن الإجراءات الجزائية الجزائري، مرجع سابق.

[3] Roger Merle et André Vitu, Traité de droit criminel, Tome 2, Cujas, Paris, 1989, p.57.

[4] هبة هروال نبيلة، مرجع سابق، ص87.

كما تساهم في تكريس مبدأ الشرعية الإجرائية وضمان التوازن بين فعالية مكافحة الجريمة المعلوماتية واحترام الحقوق والحريات الفردية، وهو ما يجعلها حجر الأساس في مشروعية التفتيش الإلكتروني في التشريع الجزائري.

خاتمة

خاتمة

وفي ختام هذه الدراسة يمكن القول ان الثورة الرقمية المعاصرة قد فرضت إعادة نظر جذرية في النظرية العامة للإجراءات الجنائية، فلم تعد الجريمة محصورة في أبعادها المادية أو الحدود الجغرافية التقليدية، بل اتخذت من الفضاء المعلوماتي مسرحا افتراضيا لها، الأمر الذي حتم على المشرع الجزائري الاستجابة الفورية لاستحداث آليات إجرائية جديدة، يتصدرها "التفتيش الإلكتروني.

باعتبار ان التفتيش الالكتروني بطبيعته يقع على خط التماس المباشر مع "الحق في حرمة الحياة الخاصة الرقمية"، وهو حق متجذر في صلب المبادئ الدستورية المصونة، ومن خلال استقراء التوازن التشريعي بين أحكام قانون الإجراءات الجزائية (لا سيما مستجدات القانون رقم 24-15) والقوانين ذات الصلة، وعلى رأسها القانون رقم 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، بالتكامل مع القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، تتبلور لدينا النتائج والتوصيات الاستشرافية الآتية:

أولاً: النتائج المستخلصة:

- عن قصور المعايير الإجرائية الكلاسيكية للتفتيش المستندة إلى ثنائية (المكان المادية/المنقول الملموس) عن استيعاب الطبيعة الفنية للدليل الرقمي، الذي يتميز بالافتراضية، وسرعة المحو، والتدفق العابر للحدود الوطنية عبر الحوسبة السحابية.

التكريس التشريعي للصلاحيات التوسعية: كشف التحليل القانوني لأحكام القانون رقم 09-04 وقانون الإجراءات الجزائية عن منحى تشريعي يتسم بالتوسع في تخويل ضباط الشرطة القضائية وجهات التحقيق سلطات واسعة لولوج الأنظمة المعلوماتية واعتراض المراسلات الرقمية، وهو ما يفرض تهديدا كامنا للحقوق اللصيقة بالشخصية في غياب كوابح قانونية دقيقة.

– يحسب للمشرع الجزائري مواكبته الحثيثة للمستجدات التقنية ومأسسته للضبط الرقمي، سعيًا لإحداث الموازنة الصعبة بين مقتضيات الفعالية الإجرائية في مكافحة الإجرام المعلوماتي والالتزامات الدستورية الحمائية للحريات الفردية وسرية المراسلات.

– رغما عن السياج الحمائي الذي فرضه القانون رقم 18–07 لمعالجة المعطيات الشخصية، إلا أن الاستثناءات التشريعية الممنوحة لاعتبارات الأمن القومي ومصلحة التحقيق القضائي جاءت بصيغ فضفاضة، مما يؤدي عملياً إلى رجحان كفة مصلحة التحقيق على حساب سرية المعطيات الشخصية للأفراد.

ثانياً: التوصيات المقترحة:

تتويجا للمخرجات المستخلصة، نتقدم بنصيب من المقترحات الرامية إلى تجويد الصياغة التشريعية وضبط الممارسة العملية:

– إفراد نص تشريعي صريح وجامع ضمن قانون الإجراءات الجزائية يحدد المفهوم الإجرائي لـ "التفتيش الإلكتروني"، ويرسم بدقة حدوده الموضوعية، وشروطه الفنية، والخط الفاصل بين البيانات الخاضعة للضبط والأسرار اللصيقة بالحياة الخاصة للمتهم أو الغير..

–تفعيل الحماية القضائية المسبقة عبر اشتراط صدور إذن مكتوب ومسبب تسبيباً سائغاً من الجهة القضائية المختصة، يحدد الحسابات أو الوسائط الرقمية المستهدفة على وجه الدقة؛ قطعا للطريق أمام "التفتيش الاستكشافي العشوائي "المقوض لخصوصيات الأفراد دون مسوغ قاطع.

– النص صراحة وبألفاظ حاسمة على بطلان أي إجراء من إجراءات التفتيش أو الاعتراض الإلكتروني يتم بالمخالفة للضمانات الدستورية والقانونية، واعتبار هذا البطلان من النظام العام الذي تقضي به المحكمة تلقائياً وتجوز إثارته في أية مرحلة كانت عليها الدعوى.

– تكثيف البرامج التكوينية والتدريبية المتخصصة للقضاة ومساعديهم من ضباط الشرطة القضائية في الشق الفني والمعلوماتي، لضمان ممارسة هذه المكنات الصلاحية باحترافية تحول

دون الانحراف بالسلطة، أو الإتلاف العمدي للأدلة الرقمية، أو الاختراق غير المبرر للحياة الخاصة للمواطنين.

قائمة المراجع

أولاً: المصادر:

1. الدستور:

دستور الجمهورية الجزائرية الديمقراطية الشعبية لسنة 2020 (الجريدة الرسمية رقم 82، المؤرخة في 30 ديسمبر 2020) المعدل والمتمم.

2.النصوص التشريعية:

- الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 جوان سنة 1966 المتضمن قانون الإجراءات الجزائية، ملغى.
- الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 جوان سنة 1966 المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 49، الصادر بتاريخ 11 جوان 1966، المعدل والمتمم.
- القانون رقم 88-09 المؤرخ في 7 جمادى الثانية عام 1408 الموافق 26 يناير سنة 1988، المتعلق بالأرشيف الوطني الجريدة الرسمية رقم 4، لسنة 1988.
- القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 أوت سنة 2009، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الجريدة الرسمية رقم 47، لسنة 2009.
- القانون رقم 18-07 المؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي الجريدة الرسمية رقم 34، لسنة 2018.
- القانون رقم 25-14 أو الأمر رقم 25-14 المتضمن قانون الإجراءات الجزائية الجريدة الرسمية رقم 54، لسنة 2025.

3.**النصوص التنظيمية:**

1.المرسوم الرئاسية رقم 21-439 المؤرخ في 2 ربيع الثاني عام 1443 الموافق 7 نوفمبر سنة 2021، المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

ثانياً: المراجع باللغة العربية .

1.**الكتب:**

1. أحسن بوسقيعة، التحقيق القضائي في قانون الإجراءات الجزائية الجزائري، دار هومة للنشر والتوزيع، الطبعة الخامسة، الجزائر، 2017.

2. أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص: الجرائم ضد الأشخاص، الجرائم ضد الأموال، بعض الجرائم الخاصة (جزءان)، دار هومة للنشر والتوزيع، الجزائر، 2022/2019.

3. أحمد فتحي سرور، الحماية الدستورية للحقوق والحريات، مطابع الشروق، مصر، 2000.

4. آمال عبد الرحيم عثمان، شرح قانون الإجراءات الجنائية، الهيئة المصرية العامة للكتاب، الطبعة الثانية، مصر، 1991.

5. براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، دار الثقافة للنشر والتوزيع، الأردن، 2011.

6. جباري عمار، التفتيش الإلكتروني (دراسة مقارنة)، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2015.

7. جمال نجيمي، قانون الإجراءات الجزائية الجزائري على ضوء الاجتهاد القضائي (الجزء الأول)، دار هومة، الجزائر، الطبعة الثالثة، 2018.

8. خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، الطبعة الأولى، الأردن، 2011.

9. خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، مصر، 2009.

10. رؤوف عبيد، مبادئ الإجراءات الجنائية في القانون المصري، دار الجيل للطباعة، الطبعة السادسة عشر، مصر، 1985.

11. زبيدة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، الجزائر، 2011.

12. سامي جلال فقي حسين، التفتيش في الجرائم الإلكترونية: دراسة تحليلية، دار الكتب القانونية، الطبعة الأولى، مصر، 2012.

13. سامي حسني، النظرية العامة للتفتيش في القانون المصري والمقارن، دار النهضة العربية، مصر، 1973.

14. سعيد محمد، الجرائم الإلكترونية وآليات الحصول على دليل فيها، دار الكتب القانونية، الطبعة الأولى، مصر، 2016.

15. طارق إبراهيم الدسوقي عطية، الموسوعة الأمنية: الأمن المعلوماتي، النظام القانوني لحماية المعلوماتية، دار الجامعة الجديدة، مصر، 2015.

16. الطيب بلولة، إجراءات البحث والتحري في الجرائم الإلكترونية، دار الخلدونية، الجزائر، 2019.

17. عادل بن العينين، الضمانات القضائية لحماية حقوق الإنسان في المادة الجنائية، دار الكتاب الحديث، مصر، 2013.

18. عبد الرحمان خلفي، الإجراءات الجزائية في التشريع الجزائري والمقارن، دار بلقيس، الجزائر، 2017.

19. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، مصر، 2004.

20. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، مصر، 2006.

21. عبد القادر عدو، الإثبات الجنائي في المواد المعلوماتية، دار بلقيس، الجزائر، 2018.

22. عبد القادر عدو، حماية الحياة الخاصة في البيئة الرقمية، دار بلقيس، الجزائر، 2020.

23. عبد القادر عميمر، التحديات القانونية لإثبات الجريمة المعلوماتية، دار الجامعة الجديدة، مصر، 2014.

24. عبد الله أحمد هلالي، اتفاقية بودابست لمكافحة جرائم المعلوماتية، دار النهضة العربية، مصر، 2007.

25. عبد الله أحمد هلالي، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية، مصر، 2001.

26. عبد الله أحمد هلالي، حجية المخرجات الكمبيوترية في الإثبات الجنائي (دراسة مقارنة)، دار النهضة العربية، مصر، 1997.

27. عبد الله أوهايبية، شرح قانون الإجراءات الجزائية (الجزء الأول)، بيت الأفكار، الطبعة الأولى، الجزائر، 2022.

28. علي حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي (الحماية الجنائية للحاسب الآلي)، دار الجامعة الجديدة، مصر، 2003.

29. علي حسن محمد الطوالبة، التفتيش الجنائي عن نظم الحاسوب والإنترنت، عالم الكتب الحديث، الطبعة الأولى، الأردن، 2004.

30. علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المكتب الجامعي الحديث، مصر، 2012.

31. محمد أمين أحمد الشوابكة، الجرائم المعلوماتية (دراسة مقارنة)، دار الثقافة للنشر والتوزيع، الطبعة الأولى، الأردن، 2011.

-نبيلة هبه هروال، الجوانب الإجرائية للجرائم الإلكترونية، دار الفكر الجامعي، الطبعة الأولى، مصر، 2014.

32. محمد حزيط، الجرائم المعلوماتية وأدلة الإثبات الرقمية، دار هومة، الجزائر، 2015.

33. محمد راشد أحمد الظنحاني، التفتيش في الجرائم الإلكترونية، دار النهضة العلمية للنشر والتوزيع، الطبعة الأولى، مصر، 2017.

34. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، الطبعة الثانية، مصر، 1998.

35. محمد عبد الله أبو بكر سلامة، موسوعة جرائم المعلوماتية: جرائم الكمبيوتر والإنترنت، المكتب العربي الحديث، الطبعة الأولى، مصر، 2006.

36. محمد محدة، الشرطة القضائية ودورها في الإثبات الجنائي، دار هومة، الجزائر، 2012.

37. يوسف دلاندة، قانون الإجراءات الجزائية، دار هومة، الجزائر، 2001.

38. يوسف مناصرة، الدليل الإلكتروني في القانون الجزائي: الطريق إلى تحول أدلة الإثبات في المادة الجزائية (دراسة مقارنة)، دار الجامعة الجديدة، مصر، 2021.

2. الأطروحات والرسائل الجامعية :

اطروحات دكتوراه

1. رجاء أومدور، خصوصية التحقيق في مواجهة الجرائم المعلوماتية، أطروحة دكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعريريج، الجزائر، 2021.
2. غازي عبد الرحمن هيان الرشيد، الحماية القانونية من جرائم المعلوماتية (الحاسب والإنترنت)، أطروحة دكتوراه في القانون، كلية الحقوق، الجامعة الإسلامية في لبنان، بيروت، 2004.
3. ليندا بن طالب، الدليل الإلكتروني ودوره في الإثبات الجنائي، أطروحة دكتوراه في القانون الجنائي، كلية الحقوق، جامعة جيلالي ليابس–سيدي بلعباس، الجزائر، 2019.فاتح قيش، ضوابط ممارسة مهنة الصحافة بين الشريعة الإسلامية والقانون

الجزائري، أطروحة دكتوراه في العلوم الإسلامية (شريعة وقانون)، كلية العلوم الإنسانية والاجتماعية، جامعة الجزائر 1، 2014.

مذكرات الماجستير

1. بوكر رشيدة، جرائم الاعتداء على نظم المعالجة الآلية للمعطيات في التشريع الجزائري والمقارن، مذكرة ماجستير، كلية الحقوق، جامعة دمشق، سوريا، 2010.
2. صالح بوزاية، الحماية الجنائية للحق في السر والحق في الحياة الخاصة في التشريع الجزائري، مذكرة ماجستير، كلية الحقوق، جامعة 20 أوت 1955–سكيكدة، الجزائر، 2011–2012.
3. لمصارة منال، إجراءات التفتيش الإلكتروني في التشريع الجزائري، رسالة ماجستير في القانون العام، كلية الحقوق والعلوم السياسية، جامعة مولود معمري–تيزي وزو، الجزائر، 2012.

مذكرات الماستر

1. قريم سكورة، المواجهة الإجرائية للجريمة المعلوماتية في التشريع الجزائري، مذكرة ماستر، تخصص: قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة آكلي محند أولحاج–البويرة، الجزائر، 2015.
2. كيحول عبد القادر، التفتيش الإلكتروني كإجراء للتحقيق في الجرائم المعلوماتية، مذكرة ماستر، تخصص: القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور–الجلفة، الجزائر، 2019.

3 المقالات:

1. حطاب كمال، "خصوصية التفتيش في البيئة الإلكترونية"، مجلة البحوث في الحقوق والعلوم السياسية، المجلد 09، العدد 01، الجزائر، 2023.
2. حمداش شمس الدين، البشير بن مبروك، "القواعد الإجرائية المقررة لتفتيش المنظومة المعلوماتية في القانون الجزائري"، مجلة صوت القانون، المجلد 09، العدد 02، الجزائر، 2023.

3. رضا هميسي، "تفتيش المنظومات المعلوماتية في القانون الجزائري"، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، العدد 5، جوان 2012.
4. سعاد راضي حسين، "الإجراءات الجزائية في تفتيش محل الجرائم الإلكترونية"، مجلة الشرق الأوسط للدراسات القانونية والفقهية، المجلد 04، العدد 04، جامعة ذي قار، العراق، 2024.
5. عز الدين عثماني، "إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية"، مجلة المحكمة العليا الجزائرية، قسم الوثائق القضائية، العدد الرابع، الجزائر.
6. علي عبد القادر القهوجي، "الحماية الجنائية للمعطيات المعالجة آلياً"، مجلة الشريعة والقانون، تصدر عن جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، المجلد الثاني، الطبعة الثالثة، 2004.
7. فريد روانج، "ضمانات حرمة الحياة الخاصة أثناء إجراءات مراقبة الاتصالات الإلكترونية"، مجلة الأبحاث القانونية والسياسية، جامعة سطيف 2، المجلد 02، العدد 02، الجزائر، 2020.
8. فطيمة جبار، "مراقبة الاتصالات الإلكترونية بين الحظر والإباحة في التشريع الجزائري"، مجلة الدراسات القانونية، الجزائر.
9. مولاي ملياني دلال، "التفتيش في جرائم تكنولوجيات الإعلام والاتصال"، مجلة القانون والعلوم السياسية، المجلد 02، العدد 01، كلية الحقوق والعلوم السياسية، جامعة الدكتور مولاي الطاهر–سعيدة، الجزائر، 2016.

ثالثاً: الاجتهادات القضائية (الأحكام والقرارات):

1. المحكمة العليا الجزائرية، الغرفة الجنائية، القرار رقم 165609 الصادر بتاريخ 1997/07/30، المجلة القضائية، العدد الثاني، 1997.

2.محكمة استئناف باريس، قرار صادر بتاريخ 5 أفريل 1994، القضاء الفرنسي.

رابعاً: المراجع باللغة الأجنبية :

1. Cass. Crim., 3 octobre 2007, pourvoi n° 07-81045, disponible sur le site: Légifrance.
2. Jean Devése, "Atteintes aux systèmes de traitement automatisé de données", Juris-Classeur Pénal, articles 323-1 à 323-7, fascicule 2, 1997.
3. Raymond Gassin, "Informatique (fraude informatique)", Répertoire de droit pénal, Dalloz, octobre 1995.
4. Roger Merle et André Vitu, Traité de droit criminel, Tome 2, Éditions Cujas, Paris, 1989.

الفهرس

ملخص الدراسة

ملخص المذكرة

تتناول هذه المذكرة التفتيش الإلكتروني كإجراء تحقيقي حديث فرضه التطور التكنولوجي لمكافحة الجرائم المعلوماتية وجمع الأدلة الرقمية، مع ما يثيره من إشكال يتعلق بالتوازن بين فعالية التحقيق وحماية الحياة الخاصة وسرية المعطيات.

ويخضع هذا الإجراء لضوابط موضوعية (وجود جريمة أو شبهات جدية، توجيه الاشتباه، قرائن قوية، وتحديد النطاق) وضوابط شكلية (الإذن القضائي، احترام الوقت القانوني، حضور المقرر قانونًا، وتحرير محاضر دقيقة).

وتخلص الدراسة إلى أن سلطة التحقيق تبقى مقيدة بمبدأي الشرعية والتناسب وتخضع لرقابة قضائية، كما أن المشرع الجزائري سعى إلى تحقيق توازن بين مكافحة الجريمة الإلكترونية وحماية الخصوصية عبر إطار قانوني خاص ودعم تقني.

وفي النهاية، يظل التفتيش الإلكتروني ضرورة في مواجهة الجريمة الرقمية، بشرط احترام الضمانات القانونية التي تكفل مشروعيته.

Summary

This study examines electronic search as a modern investigative measure driven by technological development to combat cybercrime and collect digital evidence, while raising concerns about balancing the effectiveness of criminal investigations with the protection of privacy and personal data confidentiality.

Electronic search is subject to substantive conditions, including the existence of a crime or serious suspicion, the identification of the person concerned, the presence of strong indications of digital evidence, and the precise definition of the scope of the search. It is also governed by formal requirements such as prior judicial authorization, compliance with legal time limits, the presence of legally designated persons, and the preparation of detailed official reports.

The study concludes that the powers of investigative authorities are limited by the principles of legality and proportionality and remain subject to judicial oversight. It also highlights the efforts of the Algerian legislator to balance the fight against cybercrime with the protection of privacy through a specific legal framework and the use of technical expertise.

Ultimately, electronic search has become a necessary tool in combating cybercrime, provided that the legal safeguards ensuring its legitimacy and the protection of individual rights are respected.

Résumé

Cette étude traite de la perquisition électronique comme mesure d'enquête moderne imposée par le développement technologique afin de lutter contre la criminalité informatique et de collecter des preuves numériques, tout en soulevant la question de l'équilibre entre l'efficacité de l'enquête et la protection de la vie privée ainsi que de la confidentialité des données.

Cette mesure est soumise à des conditions de fond (existence d'une infraction ou de fortes suspicions, identification de la personne concernée, indices sérieux et délimitation du champ de la perquisition) et à des conditions de forme (autorisation judiciaire, respect des horaires légaux, présence des personnes prévues par la loi et rédaction de procès-verbaux précis).

L'étude conclut que le pouvoir des autorités d'enquête est encadré par les principes de légalité et de proportionnalité et soumis au contrôle du juge. Le législateur algérien a ainsi cherché à concilier la lutte contre la cybercriminalité et la protection de la vie privée à travers un cadre juridique spécifique et le recours aux techniques d'investigation.

En définitive, la perquisition électronique demeure une nécessité contre la criminalité numérique, sous réserve du respect des garanties juridiques assurant sa légitimité.