جامـــعة عمار ثليجي الاغواط

كـلية الحــقوق والعــلوم السـياسية

قسم الحـــــــــقوق

والموسومة بـــــ:

الضمانات الاجرائية للحماية الحق في الخصوصية للمستهلك وفق القانون 09-04

مذكـــــــرة تخرج ضمن مقتضيات نيل شهادة الماستر

تخصص: قانون أعمال

إعداد الطالبين:

بوقناشة حيدر

زرداب وهيب

إشراف الدكتور :

د.بلحسن حسام الدين لحسن

أعضاء لجنة المناقشة:

د. تيجاني عبد القهار	رئيسا
د. بلحسن حسام الدين لحسن	مشرفا ومقررا
د. بن حليمة بومدين	ممتحنا

السنة الجامعية: 2026/2025

كلمة شكر

الحمد لله الذي علّم الإنسان ما لم يعلم، نشكرُه ونحمدُه
على أنه أعاننا و يسر لنا السبيل حتى
فرغنا بحمده وتوفيقه من إتمام هذا العمل العلمي، الذي
يعدّ ثمرة جهدنا وجهد العديد ممن ساعدونا.
يشرفنا أن نتقدم بالشكر والعرفان إلى كل من مدّ يد
المساعدة وساهم من قريب أو من بعيد في انجازه، و نخُصُّ
بالذكر الأستاذ المشرف **بلحسن حسام الدين لحسن** ، دون
أن ننسى فضل الدكاترة على ما قدموه لنا طيلة مشوارنا
الجامعي

مقدمة

. شهد العالم خلال العقود الأخيرة تطوراً تكنولوجياً متسارعاً أدى إلى إحداث تغيرات عميقة في مختلف مجالات الحياة، خاصة في المجال الاقتصادي والاجتماعي والقانوني، حيث أصبحت تكنولوجيات الإعلام والاتصال جزءاً أساسياً من تعاملات الأفراد اليومية. وقد ساهم الانتشار الواسع للأنظمة المعلوماتية وشبكات الاتصال الإلكترونية في تسهيل الوصول إلى الخدمات وإبرام المعاملات عن بعد، الأمر الذي أدى إلى ظهور نمط جديد من التعاملات يعتمد على البيئة الرقمية.

وفي ظل هذا التحول الرقمي، برز المستهلك الإلكتروني كطرف أساسي في العلاقات الاقتصادية الحديثة، إذ أصبح يعتمد على الوسائط الإلكترونية للحصول على السلع والخدمات وإبرام العقود وتبادل المعلومات الشخصية والمالية. غير أن هذا التطور لم يكن خالياً من المخاطر، حيث أصبحت البيانات والمعطيات الشخصية للمستهلك عرضة للجمع والمعالجة والتخزين والاستغلال بطرق قد تمس بحقه في الخصوصية، خاصة مع تزايد الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال.

ويعد الحق في الخصوصية من الحقوق الأساسية المرتبطة بكرامة الإنسان وحرياته الفردية، فهو يهدف إلى حماية المجال الشخصي للفرد ومنع التدخل غير المشروع في حياته الخاصة أو الاطلاع على أسراره أو استغلال معلوماته الشخصية دون سند قانوني. وقد ازدادت أهمية هذا الحق في البيئة الرقمية نظراً لطبيعة المعلومات المتداولة إلكترونياً وسهولة نسخها ونقلها وانتشارها، مما جعل حماية الخصوصية الرقمية تحدياً قانونياً معاصراً.

وأمام هذه التحولات، تدخل المشرع الجزائري لوضع إطار قانوني خاص لمواجهة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال من خلال القانون رقم 04-09المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، حيث حاول تحقيق التوازن بين ضرورة تمكين السلطات المختصة من وسائل فعالة للكشف عن الجرائم الإلكترونية وجمع الأدلة الرقمية، وبين ضرورة ضمان احترام حقوق الأفراد وحرياتهم الأساسية وعلى رأسها الحق في الخصوصية.

وتبرز أهمية دراسة الضمانات الإجرائية المقررة لحماية خصوصية المستهلك من خلال كون الإجراءات الحديثة للتحري، كالمراقبة الإلكترونية وتفتيش المنظومات المعلوماتية، رغم ضرورتها في مكافحة الجريمة الإلكترونية، قد تشكل في الوقت ذاته مساساً محتملاً

بسرية الاتصالات والمعطيات الشخصية، لذلك كان من الضروري إحاطتها بمجموعة من القيود والضوابط القانونية التي تمنع استعمالها بصورة تعسفية.

تتجلى أهمية الموضوع من الناحية العلمية في كونه يتناول إحدى الإشكالات القانونية الحديثة المرتبطة بالتطور الرقمي، والمتمثلة في كيفية التوفيق بين حماية المستهلك في البيئة الإلكترونية وبين متطلبات مكافحة الجرائم المعلوماتية. فالخصوصية أصبحت من أكثر الحقوق تعرضاً للخطر نتيجة الانتشار الواسع للمعاملات الإلكترونية وتزايد الاعتماد على جمع البيانات الشخصية ومعالجتها.

أما الأهمية العملية فتظهر من خلال دراسة مدى فعالية الضمانات التي أقرها المشرع الجزائري لحماية المستهلك من أي استعمال غير مشروع لمعلوماته الشخصية، خاصة عند اللجوء إلى إجراءات المراقبة الإلكترونية التي تعد من أخطر وسائل البحث والتحري باعتبارها تمكن الجهات المختصة من الوصول إلى بيانات قد تكون ذات طبيعة خاصة.

كما تكتسي الدراسة أهمية خاصة بالنظر إلى أن حماية الخصوصية الرقمية لم تعد مسألة داخلية فقط، بل أصبحت مرتبطة بالتحديات العابرة للحدود التي تفرضها الجرائم الإلكترونية، مما يجعل وجود قواعد إجرائية دقيقة أمراً ضرورياً لتحقيق الأمن المعلوماتي وضمان احترام الحقوق والحريات.

تهدف هذه الدراسة إلى بيان الإطار القانوني للضمانات الإجرائية المقررة لحماية الحق في الخصوصية للمستهلك في البيئة الرقمية، وذلك من خلال تحديد مفهوم هذه الضمانات وبيان مدى كفايتها في مواجهة المخاطر الناتجة عن استعمال التكنولوجيا الحديثة.

كما تهدف إلى تحليل الأحكام التي جاء بها القانون رقم 04-09 المتعلقة بإجراءات مراقبة الاتصالات الإلكترونية وتفتيش المنظومات المعلوماتية، وبيان الشروط والقيود المفروضة على اللجوء إليها، بما يضمن عدم تحولها إلى وسيلة غير مشروعة للمساس بالحياة الخاصة للأفراد.

وتسعى الدراسة كذلك إلى إبراز حدود استعمال المعلومات المتحصل عليها من عمليات المراقبة الإلكترونية، وبيان الحماية القانونية المقررة للمعطيات الشخصية للمستهلك،

إضافة إلى الكشف عن النقائص التي قد تعترض فعالية هذه الحماية واقتراح الحلول المناسبة لتعزيزها.

يرجع اختيار هذا الموضوع إلى حداثته وارتباطه بالتطور التكنولوجي المتسارع الذي فرض تحديات جديدة على قواعد الحماية القانونية التقليدية، خاصة مع توسع استعمال الإنترنت وظهور أشكال جديدة من الاعتداء على البيانات الشخصية للمستهلك.

كما يعود سبب الاختيار إلى أهمية دراسة مدى قدرة التشريع الجزائري على تحقيق التوازن بين متطلبات مكافحة الجرائم الإلكترونية من جهة، وضمان احترام حقوق الأفراد وحرياتهم الأساسية من جهة أخرى، خاصة وأن إجراءات البحث والتحري الحديثة قد تمس مباشرة بسرية الاتصالات والحياة الخاصة.

إضافة إلى ذلك، فإن موضوع حماية خصوصية المستهلك يكتسي أهمية بالنظر إلى الدور المتزايد للمستهلك الإلكتروني في الاقتصاد الرقمي، وحاجته إلى حماية قانونية فعالة تمكنه من استعمال الوسائل الرقمية بثقة وأمان.

واجهت هذه الدراسة مجموعة من الصعوبات، من أهمها حداثة الموضوع وقلة الدراسات المتخصصة التي تناولت بصورة دقيقة العلاقة بين الضمانات الإجرائية في الجرائم الإلكترونية وحماية خصوصية المستهلك.

كما تتمثل إحدى الصعوبات في الطبيعة التقنية للموضوع، إذ يتطلب فهم الإجراءات الإلكترونية الإحاطة ببعض المفاهيم المرتبطة بالتكنولوجيا والأنظمة المعلوماتية، وهو ما يفرض الجمع بين التحليل القانوني والمعرفة التقنية.

بالإضافة إلى ذلك، فإن التطور المستمر في مجال التكنولوجيا يجعل النصوص القانونية بحاجة دائمة إلى التفسير والتقييم حتى تكون قادرة على مواكبة المستجدات الرقمية.

كيف كرس القانون رقم 04-09 ضمانات إجرائية فعالة تكفل حماية الحق في الخصوصية للمستهلك في البيئة الرقمية ؟

اعتمدت هذه الدراسة على المنهج الوصفي من خلال عرض المفاهيم الأساسية المتعلقة بالخصوصية الرقمية والمستهلك الإلكتروني والضمانات الإجرائية المقررة لحمايته، وبيان مختلف الإجراءات القانونية المرتبطة بجمع المعلومات ومراقبة الاتصالات الإلكترونية.

كما تم الاعتماد على المنهج التحليلي من خلال تحليل النصوص القانونية الواردة في القانون رقم 09-04، وبيان مدى فعاليتها في تحقيق الحماية القانونية للخصوصية، مع تقييم النقائص التي قد تحد من تطبيقها واقتراح بعض الآليات لتعزيزها.

لمعالجة موضوع الدراسة تم تقسيمها إلى فصلين أساسيين، حيث تناول الفصل الأول **الضمانات الإجرائية المقررة للمستهلك أثناء جمع المعلومات ومراقبة الاتصالات الإلكترونية**، وتم تقسيمه إلى مبحثين؛ خصص المبحث الأول لدراسة الضمانات القانونية للمستهلك في مجال مراقبة الاتصالات الإلكترونية، من خلال بيان شروط اللجوء إليها والقيود المفروضة عليها، بينما تناول المبحث الثاني الضمانات المتعلقة باستعمال المعلومات المتحصل عليها وحماية المعطيات الشخصية من الاستعمال غير المشروع.

أما الفصل الثاني فقد خصص لدراسة **الضمانات الإجرائية اللاحقة لحماية خصوصية المستهلك وآليات الرقابة والمسؤولية**، من خلال بحث دور الرقابة القضائية والحماية الجزائية والمدنية المقررة عند حدوث تجاوزات تمس بالحق في الخصوصية.

.

الفصل الأول:

الضمانات الإجرائية المقررة للمستهلك أثناء جمع المعلومات ومراقبة الاتصالات الإلكترونية

الفصل الاول: الضمانات الإجرائية المقررة للمستهلك أثناء جمع المعلومات ومراقبة الاتصالات الإلكترونية

أدى التطور المتسارع لتكنولوجيات الإعلام والاتصال إلى إحداث تحول جذري في طبيعة المعاملات والعلاقات الاجتماعية والاقتصادية، حيث أصبح المستهلك يعتمد بصورة متزايدة على الوسائط الإلكترونية في الحصول على الخدمات وإبرام العقود وإجراء مختلف العمليات التجارية. غير أن هذا التحول الرقمي صاحبه ظهور أنماط جديدة من الاعتداءات التي تستهدف البيانات الشخصية والمعلومات الخاصة بالأفراد، الأمر الذي جعل مسألة حماية الحق في الخصوصية في البيئة الرقمية من أهم التحديات القانونية المعاصرة.

ونظراً للطبيعة التقنية المعقدة للجرائم المرتكبة عبر الوسائط الإلكترونية، فقد أصبح من الضروري منح السلطات المختصة وسائل إجرائية حديثة تمكنها من الكشف عن هذه الجرائم وجمع الأدلة الرقمية، ومن أهمها إجراءات مراقبة الاتصالات الإلكترونية. إلا أن هذه الإجراءات، رغم أهميتها في مجال مكافحة الجريمة المعلوماتية، تنطوي في المقابل على إمكانية المساس بسرية الاتصالات والبيانات الشخصية للمستهلكين، باعتبار أن البيئة الرقمية أصبحت فضاءً لتبادل كميات هائلة من المعلومات الخاصة.

وانطلاقاً من هذا التعارض بين مقتضيات مكافحة الجرائم الإلكترونية وضرورة احترام الحريات الفردية، تدخل المشرع الجزائري من خلال القانون رقم 04-09المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، لوضع إطار قانوني ينظم اللجوء إلى إجراءات المراقبة الإلكترونية، ويحدد الحالات التي يجوز فيها استعمالها، كما يفرض مجموعة من القيود والضمانات التي تكفل عدم تجاوز الغرض المشروع منها.

وعليه، سيتم تناول هذا الفصل من خلال دراسة الضمانات القانونية التي تحكم اللجوء إلى المراقبة الإلكترونية، وذلك من خلال مبحثين؛ يتناول المبحث الأول **الضمانات القانونية للمستهلك في مراقبة الاتصالات الإلكترونية**، بينما يخصص المبحث الثاني للضمانات المتعلقة بحماية المعطيات الشخصية للمستهلك الناتجة عن عمليات المراقبة وكيفية تقييد استعمالها.

المبحث الأول: الضمانات القانونية للمستهلك في مراقبة الاتصالات الإلكترونية

تعتبر مراقبة الاتصالات الإلكترونية للمستهلك من أبرز الإجراءات المستحدثة التي أفرزتها التحولات الرقمية في مجال البحث والتحري عن الجرائم، إذ تسمح للجهات المختصة بالوصول إلى معلومات إلكترونية قد تكون ضرورية لكشف الحقيقة وإثبات الجرائم المرتكبة عبر الأنظمة المعلوماتية[1].

غير أن هذا الإجراء يمثل استثناءً على الأصل العام المتمثل في حماية سرية المراسلات والاتصالات واحترام الحياة الخاصة، لذلك فإن مشروعيته ترتبط بضرورة إخضاعه لضوابط قانونية دقيقة تحد من استعماله التعسفي، وتضمن احترام حقوق الأفراد، وعلى رأسهم المستهلك الذي أصبحت بياناته الشخصية معرضة للتداول والمعالجة عبر مختلف المنصات الرقمية.

وقد عمل القانون 04-09على وضع إطار إجرائي خاص للمراقبة الإلكترونية، من خلال تحديد الحالات التي يسمح فيها باللجوء إليها، واشتراط توفر مبررات قانونية وموضوعية تبرر هذا التدخل في الخصوصية. كما أوجب ارتباط هذا الإجراء بضرورات التحقيق وصعوبة الوصول إلى الأدلة بالوسائل التقليدية.

وبناءً على ذلك، سيتم دراسة هذا المبحث من خلال مطلبين؛ يخصص الأول لبيان القيود الموضوعية الواردة على اللجوء إلى المراقبة الإلكترونية، بينما يتناول الثاني الضمانات المتعلقة بحماية المعطيات الناتجة عنها.

المطلب الأول: تقييد اللجوء إلى المراقبة الإلكترونية بحالات محددة قانونًا

تُعد المراقبة الإلكترونية من أخطر الإجراءات التحقيقية المستحدثة التي أفرزتها البيئة الرقمية، نظراً لما تنطوي عليه من إمكانية الاطلاع على مضمون الاتصالات والمعطيات الشخصية للأفراد، وهو ما قد يشكل مساساً مباشراً بالحق في الخصوصية، لاسيما بالنسبة للمستهلك الذي أصبح يعتمد بصورة متزايدة على الوسائط الإلكترونية في إبرام المعاملات واستهلاك الخدمات الرقمية.

[1] أشرف عبد القادر قنديل ،**الإثبات الجنائي في الجريمة الإلكترونية**، دار الجامعة الجديدة، الاسكندرية، 2015، ص 129.

و يعتبر الحق في الحياة الخاصة من الحقوق الدستورية العالمية وثيقة الصلة بالإنسان[1]ولا يمكن تصور حياة الإنسان بدون تحققها وكفالتها .وينصب هذا الحق على كل ما يرغب الإنسان في الاستئثار به واخفائه عن علم الآخرين، ويعتبر الاعتداء على هذا الحق جريمة خطر حيث لا يتطلب حد وث ضرر أو نتيجة معينة من وراء هذا الاعتداء إنما يعاقب القانون على مجرد حدوث ما يهدد أو يمس هذا الحق دون انتظار نتيجة .على اعتبار أن الحياة الخاصة مستودع أسرار الفرد وجزء من كياناتهم وشخصيتهم [2]وقد ذهب بعض الفقه– نتفق معه–إلى أنه يجب ألا نُدخل كل ما يتعلق بالحياة الشخصية في حومة الحياة الخاصة فهناك فرق بينهم[3].

وتجدر الإشارة إلى اختلاف الفقه في تحديد مفهوم متفق عليه للمقصود بالحياة الخاصة .حيث إن هذا المفهوم يختلف من مجتمع للآخر ومن زمن لآخر؛ ويترتب على ذلك أن ما يدخل في نطاق الحياة الخاصة في مجتمع ما قد لا يعتبر كذلك في مجتمع أخر[4]، نتيجة اختلاف القيم الأخلاقية والأعراف ودرجة الثقافة في كل مجتمع عن الآخر .فقد اتجهت التشريعات إلي عدم إيراد تعريف للحق في الحياة الخاصة تاركةً ذلك لاجتهاد الفقه.

ومما لا شك فيه أن التقدم التقني والفني في مجال الاتصالات والتعاملات الإلكترونية واتجاه الحكومات نحو التحول الرقمي في تعاملاتها كان سببًا من الأسباب ذات عظيم الأثر في المساس والتعرض لهذا الحق.

---

[1] .شيماء عبد الغنى عطاالله : تراجع الحق في الخصوصية في مواجهة الاتصالات الإلكترونية، بحث مقدم للمؤتمر العلمي الثاني لكلية القانون الكويتية العالمية" التحديات المستجدة للحق في الخصوصية"، في الفترة 16 – 15 فبراير 2012، طبعة منقحة 2019 ، ص2

[2] عيده بلعباد ، الدليل الرقمي بين حتمية الإثبات الجنائي والحق في الخصوصية المعلوماتية، مجلة أفاق علمية، المركز الجامعي لتامنغست الجزائر ، المجلد 11 العدد 1 السنة 2019 ، ص142

[3] شيماء عبدالغني عطا الله ، تطور الحق في الحياة الخاصة وآثره على دستورية التجريم ومشروعية الدليل في المواد الجنائية، بحث منشور بمجلة روح القوانين، العدد 69 يناير 2015 ، كلية الحقوق جامعة طنطا، طبعة منقحة 2019 ، ص4

[4] أشرف توفيق شمس الدين ، الصحافة والحماية الجنائية للحياة الخاصة "دراسة مقارنة"، دار النهضة العربية، 2007 ، ص33

فبرغم أن الاتصالات الإلكترونية للمستهلك والتحول الرقمي للتعاملات قد سهل التواصل بين الأفراد والحكومات.

وفي هذا الإطار، جاء القانون رقم 09-04[1] المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ليحدد بدقة الحالات التي يجوز فيها اللجوء إلى المراقبة الإلكترونية، كما اشترط أن يكون استعمالها مرتبطاً بضرورات تبررها طبيعة الجريمة أو صعوبة الوصول إلى الأدلة بالوسائل التقليدية.

الفرع الأول: حصر حالات المراقبة الإلكترونية

تُعدّ إجراءات مراقبة الاتصالات الإلكترونية للمستهلك وتفتيش المنظومات المعلوماتية من أخطر وسائل التحري الخاصة التي استحدثها المشرع الجزائري لمواجهة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بالنظر إلى ما تنطوي عليه من مساس مباشر بالحقوق والحريات الأساسية، وعلى رأسها الحق في الخصوصية وسرية المراسلات وحماية المعطيات الشخصية.

وإدراكًا منه لخطورة هذه الإجراءات الاستثنائية، لم يُطلق المشرع الجزائري يد السلطات المختصة في اللجوء إليها دون ضوابط، وإنما أحاطها بمجموعة من القيود القانونية، من أهمها حصر الحالات التي يجوز فيها اتخاذها على سبيل التحديد، منعًا لأي تعسف أو توسع غير مبرر قد يؤدي إلى انتهاك الحياة الخاصة للأفراد.

وقبل التطرق إلى الحالات التي أجاز فيها القانون اللجوء إلى هذه الإجراءات، يقتضي الأمر التمييز بين مفهومي مراقبة الاتصالات الإلكترونية للمستهلك وتفتيش المنظومات المعلوماتية، باعتبارهما إجراءين مستقلين نص عليهما القانون رقم 04-09المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

أولًا: التمييز بين مراقبة الاتصالات الإلكترونية للمستهلك وتفتيش المنظومات المعلوماتية

نص القانون رقم 04-09على إجراءين أساسيين يمكن للسلطات المختصة اللجوء

[1] القانون رقم 09- 04المؤرخ في 5أغسطس 2009المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها .الجريدة الرسمية للجمهورية الجزائرية، العدد 47

إليهما في إطار مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، يتمثل الأول في مراقبة الاتصالات الإلكترونية، بينما يتمثل الثاني في تفتيش المنظومات المعلوماتية.

غير أن المشرع الجزائري لم يضع تعريفًا دقيقًا لهذين الإجرائين، شأنه في ذلك شأن العديد من التشريعات المقارنة، الأمر الذي يقتضي الرجوع إلى النصوص القانونية ذات الصلة وإلى اجتهادات الفقه لتحديد المقصود بكل منهما.

1.مفهوم مراقبة الاتصالات الإلكترونية

ينصب إجراء المراقبة على الاتصالات الإلكترونية للمستهلك بمختلف صورها وأشكالها، وقد عرفت المادة 2، الفقرة (و)، من القانون رقم 04-09الاتصالات الإلكترونية للمستهلك بأنها: «كل تراسل أو إرسال أو استقبال لعلامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية.[1]

ويستفاد من هذا التعريف أن مفهوم الاتصالات الإلكترونية للمستهلك يشمل جميع أشكال التواصل التي تتم عبر الوسائط الرقمية، سواء تعلق الأمر بالبريد الإلكتروني، أو المحادثات الفورية، أو المكالمات الصوتية والمرئية عبر شبكة الإنترنت، أو الرسائل النصية، أو تبادل الملفات والبيانات الإلكترونية.

وعرف الفقه المقارن الاتصالات الإلكترونية للمستهلك بأنها الاتصالات التي تتم عن طريق أجهزة الحاسب الآلي أو غيرها من الوسائط الإلكترونية، وتتخذ صورًا متعددة، من بينها البريد الإلكتروني(E-mail) ، والمحادثات الفورية(Instant Messaging) ، والمكالمات عبر بروتوكول الإنترنت، وغيرها من وسائل الاتصال الحديثة.

وتبعًا لذلك، فإن الاتصالات الإلكترونية للمستهلك قد تأخذ شكل مراسلات مكتوبة، أو محادثات صوتية، أو صور ومقاطع مرئية، أو بيانات رقمية متبادلة بين شخصين أو أكثر، الأمر الذي يجعلها من أبرز مظاهر الحياة الخاصة للأفراد.

ومن ثم، فإن مراقبة هذه الاتصالات تمثل تدخلاً مباشرًا في نطاق الخصوصية، لما تنطوي عليه من إمكانية الاطلاع على أسرار الأفراد وعلاقاتهم الاجتماعية والمهنية والشخصية.

[1] المادة 02 من القانون 09-04

ويقصد بمراقبة الاتصالات الإلكترونية للمستهلك تجميع محتوى الاتصالات أو تسجيلها أو اعتراضها أو الاطلاع عليها أو الكشف عنها باستعمال وسائل تقنية خاصة، بما يسمح للسلطات المختصة بالحصول على معلومات تفيد في الوقاية من الجرائم أو كشف مرتكبيها.

وقد أغفل المشرع الجزائري تحديد الوسائل التقنية المعتمدة في تنفيذ هذا الإجراء، مكتفيًا بالنص على ضرورة وضع الترتيبات التقنية اللازمة للمراقبة، الأمر الذي دفع الفقه المقارن إلى تحديد أبرز صور المراقبة الإلكترونية، والتي تتمثل فيما يأتي:

- استخدام الوسائل التقنية المخصصة لتسجيل البيانات المتعلقة بالاتصالات، كبيانات المرسل والمتلقي ووقت الاتصال ومدته، فيما يعرف بأنظمة التتبع والمتابعة.
- استخدام تقنيات اعتراض محتوى الرسائل الإلكترونية أو المحادثات الفورية أو المكالمات الرقمية، من خلال وسائل فنية مخصصة للتنصت أو التقاط البيانات.

2.مفهوم تفتيش المنظومات المعلوماتية

إلى جانب مراقبة الاتصالات الإلكترونية، نص القانون رقم 04-09على إجراء آخر أكثر مساسًا بالحياة الخاصة، يتمثل في تفتيش المنظومات المعلوماتية[1].

ويقصد بالمنظومة المعلوماتية كل نظام منفصل أو مجموعة من الأنظمة المترابطة أو المتصلة ببعضها البعض، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذًا لبرنامج محدد.

أما المعطيات المعلوماتية، فهي تمثيل للوقائع أو المعلومات أو المفاهيم في شكل يسمح بمعالجتها داخل منظومة معلوماتية.

ويتمثل تفتيش المنظومات المعلوماتية في تمكين السلطات المختصة من الولوج إلى الأجهزة والأنظمة الإلكترونية والاطلاع على البيانات المخزنة بها أو نسخها أو حجزها متى كانت ضرورية لإثبات الجريمة أو الكشف عن مرتكبيها.

ويكتسي هذا الإجراء خطورة خاصة، لأن الأجهزة الإلكترونية أصبحت تحتوي على

[1] المواد 3 و4 من 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 بتاريخ 16 أوت 2009.

كم هائل من المعلومات الشخصية والمهنية، بما في ذلك الصور والمراسلات والملفات والبيانات البنكية والوثائق الخاصة.

وقد أجازت العديد من التشريعات المقارنة، ومنها التشريع الفرنسي، اللجوء إلى تفتيش الأنظمة المعلوماتية لضبط الأدلة الرقمية المتعلقة بالجرائم المعلوماتية.

وتجدر الإشارة إلى ضرورة التمييز بين تفتيش المنظومات المعلوماتية وبين مجرد دخول ضباط الشرطة القضائية إلى الأماكن العامة التي تحتوي على أجهزة إلكترونية، كنوادي الإنترنت أو المقاهي الإلكترونية.

فوفقًا للقواعد العامة للتفتيش، يجوز لضباط الشرطة القضائية دخول الأماكن العامة دون إذن مسبق، غير أنه لا يجوز لهم فتح الأجهزة المغلقة أو الولوج إلى محتوياتها أو تفتيشها إلا وفق الشروط والضوابط التي يحددها القانون.

ثانيًا: الحالات التي يجوز فيها اللجوء إلى المراقبة الإلكترونية

حرص المشرع الجزائري على حصر حالات اللجوء إلى مراقبة الاتصالات الإلكترونية للمستهلك وتفتيش المنظومات المعلوماتية على سبيل التحديد، بما يضمن عدم التوسع في تطبيقها خارج الأهداف التي شرعت من أجلها.

وقد نص القانون رقم 04-09على الحالات الآتية[1]:

1.الوقاية من جرائم الإرهاب والتخريب والجرائم الماسة بأمن الدولة

أجاز المشرع الجزائري اللجوء إلى إجراءات المراقبة الإلكترونية وتفتيش المنظومات المعلوماتية في مرحلة سابقة على ارتكاب الجريمة، متى تعلق الأمر بالوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة[2].

ويستفاد من ذلك أن هذه الإجراءات ذات طبيعة وقائية، إذ يكفي توفر مؤشرات أو

[1] المادة 04 من القانون 09-04

[2] **القسم الرابع مكرر الجرائم الموصوفة بأفعال إرهابية أو تخريبية** من الامر رقم66-156 مؤرخ في 8 يونيو 1966، ج ر ج ج، عدد يتضمن قانون العقوبات، المعدل والمتمم بالأمر رقم 20-01 المؤرخ في 30 جويلية 2020، المعدل والمتمم للأمر رقم 66-156 المؤرخ في 08 يونيو 1966، المتضمن قانون العقوبات الجزائري، ج ر.ج.ج العدد 44 صادر في 30/07/2020 المعدل والمتمم بالقانون رقم 24-06 مؤرخ في 19 شوال 1445 الموافق ل 2024/02/28 ج.ر عدد 30 الصادرة بتاريخ 2024/04/30

معلومات جدية تفيد باحتمال ارتكاب إحدى هذه الجرائم، دون اشتراط وقوعها فعليًا.

ويرجع ذلك إلى الطبيعة الخطيرة لهذه الجرائم وما قد يترتب عليها من أضرار جسيمة تمس أمن الدولة وسلامة الأشخاص والممتلكات، فضلًا عن اعتماد مرتكبيها في كثير من الأحيان على وسائل الاتصال الحديثة وتقنيات التحكم عن بعد.

2.مواجهة الاعتداءات المحتملة على المنظومات المعلوماتية

يجوز كذلك اللجوء إلى إجراءات المراقبة والتفتيش إذا توفرت معلومات جدية بشأن احتمال وقوع اعتداء على منظومة معلوماتية من شأنه تهديد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني[1].

وتتميز هذه الحالة أيضًا بطابعها الوقائي، إذ تهدف إلى التدخل المبكر لمنع وقوع الجريمة المعلوماتية قبل تحقق نتائجها الضارة.

وتبرز أهمية هذا التدخل الاستباقي بالنظر إلى ما قد تخلفه الهجمات السيبرانية من آثار خطيرة، كتوقف المرافق العامة، أو تعطيل الخدمات الأساسية، أو اختراق قواعد البيانات الحساسة، أو المساس بالبنية التحتية الرقمية للدولة.

3.تنفيذ طلبات المساعدة القضائية الدولية المتبادلة

أجاز المشرع الجزائري اللجوء إلى مراقبة الاتصالات الإلكترونية للمستهلك وتفتيش المنظومات المعلوماتية في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة[2].

ويتعلق الأمر بالجرائم المرتكبة خارج الإقليم الوطني، والتي تستوجب تعاون السلطات الجزائرية مع السلطات الأجنبية المختصة لجمع الأدلة الرقمية أو تعقب مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

---

[1] **القسم السابع مكرر المساس بأنظمة المعالجة الآلية للمعطيات** من نفس الامر

[2] **المادة 111 من الامر** رقم 66-155 المؤرخ في 18 صفر عام 1386، الموافق 08 يونيو 1966 المتضمن قانون الاجراءات الجزائية المعدل والمتمم بالقانون رقم 25-14 مؤرخ في 9 صفر عام 1447 الموافق 3 غشت سنة 2025، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 54، الصادر في 13 شوال 1447 الموافق لـ 19 سبتمبر 2025. في حالة ما إذا كانت الأفعال المجرمة المنسوبة للشخص المعنوي ذات طابع عابر للحدود وكانت جهة قضائية أجنبية قد أخطرت بها، يجوز للنيابة العامة أن تقوم، عن طريق وزارة العدل، بتطبيق الإجراءات المنصوص عليها في هذا الفصل بالتشاور مع الجهة القضائية الأجنبية، في إطار الاتفاقيات الدولية ذات الصلة.

غير أن تنفيذ هذه الإجراءات يظل مشروطًا بوجود اتفاقيات دولية أو تطبيق مبدأ المعاملة بالمثل، مع ضرورة احترام قواعد السيادة الوطنية والضمانات الإجرائية المقررة في التشريع الجزائري.

ويعكس هذا التوجه إدراك المشرع للطبيعة العابرة للحدود التي تتسم بها الجرائم الإلكترونية، والتي تجعل من التعاون الدولي ضرورة حتمية لضمان فعالية مكافحتها.

الفرع الثاني: اشتراط صعوبة الوصول إلى الأدلة بالوسائل العادية

انطلاقًا من كون مراقبة الاتصالات الإلكترونية للمستهلك وتفتيش المنظومات المعلوماتية من الإجراءات الاستثنائية التي تمس بصورة مباشرة الحق في الخصوصية وسرية المراسلات، فقد حرص المشرع الجزائري على عدم إباحة اللجوء إليها إلا في حالات الضرورة التي تقتضيها متطلبات البحث والتحري والتحقيق القضائي.

ويعد اشتراط صعوبة الوصول إلى الأدلة بالوسائل التقليدية من أهم الضمانات القانونية التي تحكم اللجوء إلى هذه الإجراءات، إذ لا يجوز اتخاذها باعتبارها وسيلة أولية أو اعتيادية في البحث عن الأدلة، وإنما كحل استثنائي تفرضه طبيعة الجريمة أو تعقيد ظروف ارتكابها أو عدم كفاية وسائل التحري التقليدية للكشف عن مرتكبيها.

ويستند هذا الشرط إلى مبدأ التناسب بين خطورة الإجراء والغاية المرجوة منه، بما يضمن تحقيق التوازن بين متطلبات مكافحة الجريمة وحماية الحقوق والحريات الأساسية للأفراد.

وفي هذا الإطار، نصت الفقرة الأولى من المادة 4، البند (ج) من القانون رقم 04-09المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، على إمكانية اللجوء إلى مراقبة الاتصالات الإلكترونية للمستهلك أو تفتيش المنظومات المعلوماتية إذا اقتضت ذلك التحريات أو التحقيقات القضائية، وكان من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى هذه الإجراءات الاستثنائية[1]

[1] ثابت دنيازاد، **مراقبة الاتصالات الالكترونية والحق في حرمة الحياة الخاصة في القانون الجزائري**، مجلة العلوم الاجتماعية والإنسانية المجلد 05، العدد01، 2012، ص 209

ويلاحظ أن هذه الحالة تختلف عن الحالات الوقائية التي سبق تناولها، إذ إن اللجوء إلى المراقبة الإلكترونية أو التفتيش المعلوماتي يتم هنا بعد وقوع الجريمة، وخلال مرحلتي جمع الاستدلالات أو التحقيق القضائي، ويكون الهدف الأساسي منه كشف ملابسات الجريمة، وتحديد هوية مرتكبيها، وجمع الأدلة الرقمية اللازمة لإثباتها.

ويعكس هذا التوجه إدراك المشرع للخصوصية التي تتميز بها الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، والتي غالبًا ما ترتكب في بيئة افتراضية يصعب تتبع آثارها بالوسائل التقليدية، كما أن مرتكبيها يستعينون في كثير من الأحيان بتقنيات متطورة لإخفاء هوياتهم أو محو آثار جرائمهم أو تشفير بياناتهم، مما يجعل إجراءات البحث والتحري المعتادة غير كافية للوصول إلى الحقيقة.

ومن ثم، فإن مجرد وجود جريمة معلوماتية لا يكفي لتبرير اللجوء إلى المراقبة الإلكترونية، بل يتعين على الجهة المختصة إثبات تعذر أو صعوبة الحصول على الأدلة بوسائل أخرى أقل مساسًا بالحقوق والحريات.

ويستفاد من صياغة البند (ج) من الفقرة الأولى للمادة 4 أن المشرع اشترط توافر عنصرين متلازمين هما:

- أن تكون هناك تحريات أو تحقيقات قضائية جارية بشأن جريمة تدخل ضمن نطاق تطبيق القانون رقم 09-04.
- أن يثبت وجود صعوبة فعلية في الوصول إلى نتائج تفيد الأبحاث الجارية باستعمال وسائل التحري التقليدية.

غير أن الملاحظ أن المشرع الجزائري لم يحدد على وجه الدقة طبيعة الجرائم المقصودة في هذه الحالة، خلافًا لما فعل في البنود الأخرى من المادة نفسها، التي حصرت اللجوء إلى هذه الإجراءات في جرائم معينة كالإرهاب أو الاعتداءات الماسة بأمن الدولة.

وبناءً على ذلك، يمكن القول إن المراقبة الإلكترونية وتفتيش المنظومات المعلوماتية يجوز اللجوء إليهما في جميع الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، متى توافرت الشروط القانونية اللازمة، وعلى رأسها شرط صعوبة الوصول إلى الأدلة بالوسائل العادية[1]

[1] المادة 4/1/ج من القانون رقم 09-04

ويستند هذا التفسير إلى الغاية التي أنشئ من أجلها القانون رقم 09-04، والمتمثلة في وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الأمر الذي يفيد شمول أحكامه لجميع الجرائم الداخلة في نطاقه الموضوعي.

وتبرز أهمية هذا الشرط بصورة أكبر في الجرائم المنظمة والعابرة للحدود الوطنية، حيث تتسم هذه الجرائم بالتعقيد الفني، واعتماد مرتكبيها على شبكات اتصال متطورة، واستغلالهم للفوارق التشريعية بين الدول، فضلاً عن استخدام وسائل تقنية حديثة كالتشفير وإخفاء الهوية والخوادم الوسيطة، مما يجعل الوصول إلى الأدلة الرقمية بالوسائل التقليدية أمرًا بالغ الصعوبة.

ومن ثم، فإن اشتراط صعوبة الوصول إلى الأدلة بالوسائل العادية يمثل ضمانة أساسية تحول دون التوسع غير المبرر في استخدام وسائل المراقبة الإلكترونية، وتكرس مبدأ الضرورة والتناسب، بما يكفل حماية الحياة الخاصة للأفراد من أي تدخل تعسفي أو غير مشروع.

المطلب الثاني: الرقابة القضائية على إجراءات المراقبة الإلكترونية

لا تقتصر حماية الحق في الخصوصية على مرحلة السماح بإجراء المراقبة الإلكترونية، وإنما تمتد لتشمل مرحلة التعامل مع البيانات التي يتم جمعها أثناء تنفيذ هذا الإجراء. فالمعلومات المتحصلة من مراقبة الاتصالات قد تتضمن معطيات شخصية دقيقة، مما يستوجب إخضاعها لقواعد قانونية تضمن عدم استخدامها أو استغلالها خارج الإطار الذي حدده القانون[1].

ومن هذا المنطلق، أقر المشرع الجزائري مجموعة من الضمانات المرتبطة بتخصيص المعلومات المجمعة للأغراض التي سمح القانون من أجلها بجمعها، كما جرم كل استعمال يؤدي إلى المساس بالحياة الخاصة للأفراد.

وسيتم تناول هذا المطلب من خلال فرعين؛ يخصص الأول لدراسة قاعدة تخصيص المعلومات المجمعة للأغراض القانونية المحددة، بينما يتناول الثاني الحماية الجزائية المقررة ضد المساس بالحياة الخاصة الناتج عن إساءة استعمال المعلومات.

[1] ثابت دنيازاد، مرجع سابق، ص 209

الفرع الأول: اشتراط الإذن الكتابي المسبق من السلطة القضائية

نص القانون**09-04** على أنه لا يجوز إجراء عمليات المراقبة إلا بإذن مكتوب صادر عن السلطة القضائية المختصة[1] دون أن تحدد هذه المادة السلطة القضائية المختصة بمنح الإذن هل يرجع ذلك إلى قاضي التحقيق أو وكيل الجمهورية؟

و هذه الإجراءات يمكن الاستعانة بها من طرف كل من وكيل الجمهورية وقاضي التحقيق اللذين لهما حق إصدار الإذن بمراقبة الاتصالات الالكترونية، وحجتنا في ذلك ما ذكرته **المادة 3** من نفس القانون والتي ذكرت في نصها" :مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات ...ووفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية ."

وبالتالي فهناك إحالة صريحة لما ورد في القواعد العامة في قانوني العقوبات والإجراءات الجزائية في حماية الحق في حرمة الحياة الخاصة .

أما الشروط الشكلية وتتمثل في الإذن القضائي الذي يقصد به: الأمر القضائي الذي يصدره وكيل الجمهورية أو قاضي التحقيق حسب الحالة، باعتبار أن وكيل الجمهورية من يتولى تحريك الدعوى العمومية ومباشرتها وله من الصلاحيات ما يمكنه من إتخاذ أي إجراء يراه مناسبا كذلك قاضي التحقيق تناط به إجراءات التحقيق والتحري وكل إجراء يقوم به قاضي التحقيق يخطر به النيابة العامة. [2]

يجب لممارسة هذا الإجراء حصول ضابط الشرطة القضائية على إذن كتابي من وكيل الجمهورية المختص على أن تنفذ العمليات المأذون بما وتبقى تمارس تحت المراقبة المباشرة لوكيل الجمهورية المختص.

وفي حالة تحقيق قضائي، تتم العمليات المذكورة بناءا على إذن قاضي التحقيق وتحت مراقبته المباشرة وهذا ما بينته المطة الثانية من المادة 114 من قي إج، وهنا نلاحظ أن المشرع الوطني إختلف عن المشرع الفرنسي الذي خول لقاضي التحقيق إصدار قرار بإعتراض المراسلات السلكية واللاسلكية، ولم يمنح ذلك لوكيل الجمهورية.

[1] الفقرة 2 من **المادة**4 من القانون 09-04

[2] عبد الله أوهايبة، **شرح قانون الإجراءات الجزائية، التحري والتحقيق**، ط2، دار هومة،2011، ص 345.

ويشترط في الإذن أن يحتوي على تحديد الأماكن المقصودة لوضع الترتيبات العملية إعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور، ويكون مؤرخا ومحدد المدة وموقعا عليه من مصدره، وذلك بأن يذكر فيه اليوم والشهر والسنة والساعة والدقيقة التي صدر فيها، فتحديد التاريخ مهم جدا فمن خلاله يتم حساب المدة التي يجب فيها تنفيذ عملية الإعتراض خلالها، إذا فالمقصود من البيانات الجوهرية في الإذن التي يترتب على إغفالها البطلان .[1]

وطبقا لمقتضيات نص المادة 118 من القانون 25-14 يحرر محضر بالعمليات التي تمت من إعتراض للرسائل وتسجيل للأصوات، وعن الترتيبات التقنية والتقاط الصور والتسجيل الصوتي أو السمعي البصري، وأن يتضمن المحضر تاريخ وساعة بداية ونهاية تلك العمليات.[2]

إيداع المحضر في ملف القضية، يصف فيه ضابط الشرطة القضائية أو ينسخ فيه المراسلات والصور والمحادثات المسجلة والمفيدة في إظهار الحقيقة كمرفقات تودع بالملف، وإذا كانت المكالمات قد تمت باللغة الأجنبية تنسخ وتترجم عند الإقتضاء بمساعدة مترجم يسخر لهذا الغرض.

لا يكون لهذه المحاضر قوة الإثبات، إلا إذا كانت صحيحة في الشكل طبقا لنص المادة 214 من قانون الاجراءات الجزائية، والأدلة الواردة بما لها حجية نسبية ما لم يقدم ما يخالفها، على خلاف الأدلة الواردة بالمحاضر المنصوص عليها في المادة 16 و20 من قانون الاجراءات الجزائية[3]، كما يستشف من أحكام نص المواد 114 من القانون 25-14 نجد أن صفة القائم بالعمليات التقنية هو ضابط الشرطة القضائية، ويجوز لوكيل الجمهورية أو ضابط الشرطة القضائية المتاب أن يسخر كل عون مؤهل لدى مصلحة أو وحدة عمومية أو خاصة مكلفة بالمواصلات السلكية واللاسلكية للتكفل بالجوانب التقنية للعمليات المذكورة في المادة 114.

---

[1] فوزي لواقي، **التحقيق في جرائم المخدرات على ضوء أساليب التحري الخاصة**، رسالة ماجيستير فرع القانون الجنائي، كلية الحقوق جامعة الجزائر 1، 2014/2015، ص 52

[2] عبد الله أوهابية، **شرح قانون الإجراءات الجزائية الجزائري**، المرجع السابق، ص 280

[3] نصر الدين مروك، **محاضرات في الإثبات الجنائي، النظرية العامة للإنبات الجنائي**، ج 1، دار هومة، الجزائر، سنة 2003، ص 358.

وما يؤكد ذلك أيضا أن اللجوء إلى عمليات المراقبة تدعو إليه في بعض الحالات المنصوص عليها في **المادة 4** الوقاية من وقوع بعض الجرائم ولمقتضيات التحريات وهذا يكون أثناء مباشرة التحقيق الأولي أي بمناسبة مرحلة الاستدلالات، وهذه المرحلة لا يتصل بها قاضي التحقيق ولا يمكن القيام بأي إجراء ما لم يطلب منه فتح التحقيق بواسطة طلب افتتاحي من طرف وكيل الجمهورية أو شكوى مصحوبة بادعاء مدني .

وفي الحالتين يوجه الإذن إلى ضابط الشرطة القضائية المختص محليا سواء بصفته مأذون له من طرف وكيل الجمهورية أو منابا من قاضي التحقيق بوضع الترتيبات التقنية لمراقبة الاتصالات الإلكترونية للمستهلك وتسجيل محتواها .هذا الضابط بإمكانه أن يستعين بمقدمي الخدمات[1]الذين ألزمهم **القانون09-04** بموجب نص **المادة 10** منه على وجوب تقديم المساعدات للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات التي يتعين عليهم حفظها[2]

لكن الملاحظ أن المشرع الجزائري نص على حالة خاصة في **القانون0-04** بموجب المادة 4 فقرة 3 أنه إذا تعلق الأمر بمنح الإذن بمراقبة الاتصالات الإلكترونية للمستهلك في حالة الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، فإن النائب العام لدى مجلس قضاء الجزائر هو الذي يختص بمنح إذن لمدة 6 أشهر لضباط الشرطة القضائية المنتمين للهيئة المنصوص عليها في **المادة 13** من هذا القانون[3]

[1] يقصد بمقدمي الخدمات في مفهوم القانون09-04 وفقا لما نصت عليه المادة 2 بند)د (هم – :كل كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام

–أي كيان أخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها .

[2] المادة 11 من القانون 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

[3] في إطار القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال تقرر إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال على أن تحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم الذي لم يصدر بعد، لكن وفقا لما ذكره المشرع الجزائري في نص المادة 4 فقرة 3 من هذا القانون فإنه سوف يكون ضمن تشكيلتها ضباط للشرطة القضائية .

الفرع الثاني: تحديد مدة المراقبة وإمكانية تجديدها وفق ضوابط قانونية

تُعد مسألة تحديد مدة المراقبة الإلكترونية من أهم الضمانات الإجرائية التي أقرّتها التشريعات الحديثة للحد من مخاطر التوسع في استعمال التقنيات الحديثة للتحري، باعتبار أن هذا الإجراء يمثل استثناءً على الأصل العام المتمثل في احترام حرمة الحياة الخاصة وسرية الاتصالات، فكلما امتدت مدة المراقبة الإلكترونية زمنياً، ازدادت إمكانية الاطلاع على عدد أكبر من المعطيات الشخصية للأفراد، الأمر الذي قد يؤدي إلى تحول الإجراء من وسيلة استثنائية لجمع الأدلة إلى وسيلة دائمة لمتابعة الأشخاص والتدخل في حياتهم الخاصة.

وقد تبنى المشرع الجزائري هذا الاتجاه من خلال القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[1] ، حيث نظم مدة الإذن بالمراقبة الإلكترونية في بعض الحالات، وربطها برقابة السلطة القضائية، غير أن تنظيمه لهذه المسألة يثير بعض الملاحظات المتعلقة بمدى كفاية الضمانات المقررة لحماية الحق في الخصوصية .

وعليه، سيتم تناول هذا الفرع من خلال العناصر الآتية:

أولا: تحديد مدة المراقبة الإلكترونية كضمانة لحماية الخصوصية الرقمية

يشكل تحديد مدة المراقبة الإلكترونية أحد أهم القيود الزمنية التي تحكم مشروعية هذا الإجراء، إذ إن السلطة المخولة بمباشرة المراقبة لا يمكن أن تبقى مفتوحة زمنياً دون حدود، لأن ذلك يؤدي إلى إهدار مبدأ الشرعية الإجرائية ويشكل تهديداً مباشراً للحق في الخصوصية.

فالأصل أن الاتصالات الإلكترونية للمستهلك تدخل ضمن نطاق الحياة الخاصة للفرد، سواء تعلق الأمر بالمراسلات الإلكترونية أو بيانات الاتصال أو مختلف المعطيات التي يتم تبادلها عبر الأنظمة المعلوماتية، وبالتالي فإن إخضاعها للمراقبة يجب أن يكون مؤقتاً ومرتبطاً بضرورة إجرائية محددة.

[1] المادة 4 من القانون رقم 09-04

وقد أكد المشرع الجزائري هذا المبدأ من خلال المادة 4 من القانون 09-04، حيث اشترط أن تتم عمليات المراقبة الإلكترونية في الحالات التي حددها القانون وبعد الحصول على إذن مكتوب من السلطة القضائية المختصة.[1]

كما نص على أن الإذن الممنوح لضباط الشرطة القضائية التابعين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، في حالة الجرائم الإرهابية أو الجرائم الماسة بأمن الدولة، يكون لمدة ستة (06) أشهر قابلة للتجديد.[2]

1. الطبيعة الاستثنائية لتحديد مدة المراقبة الإلكترونية

إن تحديد مدة المراقبة لا يمثل مجرد إجراء شكلي، وإنما يعد ضمانة جوهرية تمنع استمرار تدخل السلطات في خصوصية الأفراد دون مبرر قانوني.

فإذا كان المشرع قد سمح بمراقبة الاتصالات الإلكترونية للمستهلك لمواجهة بعض الجرائم الخطيرة، فإن ذلك لا يعني تعليق الحق في الخصوصية طوال فترة البحث، وإنما يجب أن يكون هذا التدخل محدوداً بالمدة التي تقتضيها الضرورة.

ويستند هذا التوجه إلى قاعدة مفادها أن الإجراءات المقيدة للحريات يجب أن تكون مؤقتة، لأن استمرارها لفترة طويلة قد يؤدي إلى جمع معلومات لا ترتبط بالجريمة محل البحث، مما يوسع من نطاق التدخل في الحياة الخاصة.

كما أن المستهلك الإلكتروني أصبح يحتفظ عبر الوسائط الرقمية بكمية كبيرة من البيانات الشخصية، مثل بيانات الشراء الإلكتروني، والمراسلات، والمعلومات المالية، وبالتالي فإن إطالة مدة المراقبة قد تؤدي إلى كشف جوانب متعددة من حياته الخاصة لا علاقة لها بالجريمة محل التحقيق.

2. مدة الستة أشهر في الجرائم الإرهابية والجرائم الماسة بأمن الدولة

بالرجوع إلى المادة 4 من القانون 09-04، نجد أن المشرع حدد مدة الإذن بالمراقبة الإلكترونية بستة أشهر قابلة للتجديد عندما يتعلق الأمر بالوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.[3]

---

[1] المادة 4 من القانون رقم 09-04

[2] الفقرة الثالثة من المادة 4 من القانون رقم 09-04.

[3] الفقرة الثالثة من المادة 4 من القانون رقم 09-04.

ويبرر المشرع هذا التنظيم الخاص بخطورة هذه الجرائم، باعتبارها جرائم ذات طبيعة منظمة ومعقدة، وقد تمتد عمليات البحث والتحري بشأنها لفترات طويلة بسبب اعتماد مرتكبيها على وسائل تقنية متطورة وشبكات اتصال عابرة للحدود.

غير أن اعتماد مدة ستة أشهر قابلة للتجديد دون تحديد عدد مرات التجديد يثير إشكالية تتعلق بمدى كفاية الحماية المقررة للحق في الخصوصية، إذ قد يؤدي ذلك عملياً إلى استمرار المراقبة لفترات طويلة، خاصة إذا لم تكن هناك رقابة فعلية على أسباب التجديد.

ثانيا: ضوابط تجديد مدة المراقبة الإلكترونية وحدود سلطة الجهات المختصة

لا يعني السماح بتجديد مدة المراقبة الإلكترونية منح السلطة المختصة إمكانية تمديدها بصورة تلقائية، وإنما يجب أن يكون التجديد قائماً على أسباب موضوعية وجدية تبرر استمرار التدخل في الحياة الخاصة.

فالتجديد يفترض أن تكون هناك ضرورة مستمرة مرتبطة بالتحقيق، كوجود مؤشرات جديدة أو احتمال الوصول إلى أدلة مهمة أو استمرار الخطر الذي يبرر الإجراء.

1. ضرورة قيام أسباب جدية لتبرير التجديد

إن استمرار المراقبة الإلكترونية بعد انتهاء مدتها الأصلية يجب ألا يكون قائماً على مجرد الرغبة في مواصلة جمع المعلومات، وإنما يتعين أن يستند إلى عناصر واقعية تثبت أن استمرار الإجراء ضروري.

فإذا تبين أن المراقبة لم تحقق الغرض المطلوب منها، أو لم تعد هناك حاجة إليها، فإن استمرارها يصبح غير مشروع، لأنه يتحول من وسيلة لكشف الجريمة إلى تدخل غير مبرر في خصوصية الأفراد.

ومن ثم، كان من الأفضل أن يحدد المشرع الجزائري عدد مرات التجديد أو يضع حداً أقصى لمدة المراقبة، حتى لا تبقى الحرية الفردية مرتبطة بتقدير غير محدود للجهات القائمة على التحقيق[1].

[1] الفقرة 02 من المادة 119 من القانون 25-14

2. ضرورة ارتباط التجديد بمبدأ التناسب

يقتضي مبدأ التناسب أن يكون استمرار المراقبة متوافقاً مع خطورة الجريمة والنتائج المرجوة منها، فلا يجوز تمديد إجراء يمس الخصوصية إذا كان بالإمكان تحقيق أهداف التحقيق بوسائل أقل مساساً بالحقوق والحريات.

وعليه، فإن تجديد الإذن يجب أن يخضع لتقييم دوري يبين مدى فائدة استمرار المراقبة، ومدى ارتباط المعلومات التي يتم جمعها بالجريمة محل البحث.

ويعتبر هذا الأمر أكثر أهمية في مجال حماية المستهلك، لأن استمرار مراقبة الاتصالات قد يؤدي إلى جمع بيانات تتجاوز نطاق المعاملة أو النشاط الإجرامي محل التحقيق.

ثالثا: موقف المشرع الجزائري من مدة المراقبة في باقي الحالات ومدى كفاية الحماية القانونية

يثير تنظيم المادة 4 من القانون 04-09ملاحظة مهمة، تتمثل في أن المشرع حدد مدة المراقبة صراحة بالنسبة للحالة المتعلقة بالإرهاب والجرائم الماسة بأمن الدولة، لكنه لم يحدد مدة واضحة لباقي الحالات المنصوص عليها في المادة نفسها.

وهنا يطرح التساؤل حول ما إذا كان عدم تحديد مدة زمنية يعني إمكانية استمرار المراقبة دون حد معين.

والإجابة بالنفي، لأن القول بإطلاق مدة المراقبة يتعارض مع المبادئ الدستورية المتعلقة بحماية الحياة الخاصة وسرية الاتصالات، كما يتعارض مع طبيعة الإجراءات الاستثنائية التي يجب أن تبقى مؤقتة ومحددة.

1. الرجوع إلى القواعد العامة في قانون الإجراءات الجزائية: في حالة عدم وجود نص خاص يحدد مدة المراقبة في بعض الحالات، يمكن الرجوع إلى القواعد العامة المتعلقة بإجراءات التسرب والمراقبة الخاصة في قانون الإجراءات الجزائية.

وقد حدد المشرع الجزائري في المادة 116 من قانون الإجراءات الجزائية مدة بعض الإجراءات الخاصة بأربعة أشهر قابلة للتجديد وفق شروط محددة، عندما تقتضي ذلك ضرورات البحث والتحري والتحقيق.[1]

[1] المادة 116من قانون الإجراءات الجزائية الجزائري

ويستفاد من ذلك أن المراقبة الإلكترونية، باعتبارها إجراءً ماساً بالخصوصية، ينبغي ألا تمتد إلا في حدود الضرورة وبصفة مؤقتة.

2. ضرورة إنهاء المراقبة بزوال أسبابها: إن استمرار المراقبة الإلكترونية مرتبط بوجود الحاجة التي بررت اتخاذها، فإذا زالت هذه الحاجة أو لم تعد تحقق فائدة في كشف الحقيقة، وجب إنهاؤها فوراً.

فالمعيار الأساسي ليس مدة التحقيق فقط، وإنما مدى جدوى الإجراء وضرورته، لأن حماية الخصوصية تقتضي إنهاء أي تدخل لم تعد تبرره أسباب قانونية[1].

اتجه المشرع الفرنسي بدوره إلى تقييد إجراءات مراقبة الاتصالات بمدة زمنية محددة، حيث جعل مدة هذه الإجراءات محدودة بأربعة أشهر قابلة للتجديد وفق شروط وضوابط معينة، بما يحقق نوعاً من التوازن بين متطلبات التحقيق الجنائي وحماية الحريات الفردية.

ويلاحظ أن التشريع الفرنسي كان أكثر دقة من التشريع الجزائري في ضبط مسألة التجديد، من خلال ربطه بشروط محددة وعدم ترك المجال مفتوحاً أمام تمديد غير محدود.

يتضح أن تحديد مدة المراقبة الإلكترونية يمثل ضمانة أساسية لحماية الحق في الخصوصية، باعتبار أن طول مدة هذا الإجراء يزيد من احتمالات المساس بالمعطيات الشخصية للأفراد. وقد حاول المشرع الجزائري من خلال القانون 04-09وضع إطار زمني لهذا الإجراء، غير أن تنظيمه بقي بحاجة إلى مزيد من الدقة، خاصة فيما يتعلق بعدد مرات التجديد ومدد المراقبة في بعض الحالات الأخرى.

وعليه، فإن تعزيز حماية الخصوصية الرقمية يقتضي وضع سقف زمني واضح لجميع حالات المراقبة الإلكترونية، وربط أي تمديد بضرورة جدية تخضع لرقابة قضائية فعالة.

[1] المادة 09 من القانون 09-04

المبحث الثاني: الضمانات الإجرائية المتعلقة باستعمال المعلومات المتحصل عليها

إن الحصول على المعلومات بواسطة إجراءات المراقبة الإلكترونية لا يمثل نهاية المسار الإجرائي، بل تبرز بعد ذلك أهمية مرحلة استعمال هذه البيانات وتحديد الجهات المخولة بالاستفادة منها والحدود القانونية لذلك، فالمعلومات الرقمية تتميز بطابعها الخاص، إذ قد تكشف عن جوانب شخصية مرتبطة بحياة الفرد أو نشاطه الإلكتروني، مما يجعل أي استعمال غير مشروع لها اعتداءً على الحق في الخصوصية[1].

ولهذا تبنى المشرع الجزائري مبدأ تقييد استعمال المعلومات المتحصل عليها، حيث منع توظيفها إلا في الحدود الضرورية للتحريات والتحقيقات القضائية، كما فرض التزاماً بالسرية على مقدمي الخدمات والأشخاص المتدخلين في تنفيذ الإجراءات التقنية.

وعليه سيتم دراسة هذا المبحث من خلال مطلبين؛ يتناول الأول حدود استعمال المعلومات في المجال القضائي، بينما يخصص الثاني لضمان حماية سرية هذه المعلومات ومنع إفشائها.

المطلب الأول: ضمانات حماية المعطيات الشخصية أثناء المراقبة

تثير إجراءات مراقبة الاتصالات الإلكترونية للمستهلك وتفتيش المنظومات المعلوماتية إشكالات قانونية دقيقة تتعلق بمدى توافقها مع الحق في حماية المعطيات الشخصية وحرمة الحياة الخاصة، باعتبار أن هذه الإجراءات تتيح للسلطات المختصة الاطلاع على قدر كبير من البيانات والمعلومات ذات الطابع الشخصي، والتي قد تشمل المراسلات الخاصة، والبيانات التعريفية، والمعاملات الإلكترونية، وغيرها من المعطيات المرتبطة بالحياة الشخصية للأفراد.

ومن هذا المنطلق، حرص المشرع الجزائري على إقرار جملة من الضمانات القانونية الكفيلة بتحقيق التوازن بين متطلبات مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال من جهة، وضمان احترام الحقوق والحريات الأساسية للأفراد من جهة أخرى.

[1] ميسون خلف الحمداني وآخر، **الدليل الرقمي وعلاقته بالمساس بالحق في الخصوصية المعلوماتية أثناء إثبات الجريمة**، جامعة النهرين كلية الحقوق، العراق، 2016 ، ص7

وقد تجسدت هذه الضمانات أساسا في مبدأ تخصيص المعلومات المجمعة للأغراض التي حددها القانون، وتجريم كل صور المساس بالحياة الخاصة الناتجة عن إساءة استعمال هذه المعلومات.

الفرع الأول: تخصيص المعلومات المجمعة للأغراض المحددة قانونًا

يقصد بمبدأ تخصيص المعلومات المجمعة للأغراض المحددة قانونًا عدم جواز جمع البيانات والمعطيات الشخصية أو معالجتها أو الاحتفاظ بها أو استغلالها إلا لتحقيق الأهداف المشروعة التي رخص بها القانون، وفي الحدود الضرورية واللازمة للكشف عن الجرائم والتحري بشأنها.

ويعد هذا المبدأ من أهم الضمانات القانونية لحماية المعطيات الشخصية أثناء تنفيذ إجراءات المراقبة الإلكترونية، لأنه يمنع السلطات المختصة من توسيع نطاق استخدام المعلومات المتحصل عليها أو توظيفها في غير الغرض الذي جُمعت من أجله.

وفي هذا الإطار، نصت الفقرة الرابعة من المادة 4 من القانون رقم 04-09المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على ضرورة احترام مبدأ تخصيص المعلومات، بحيث لا يجوز استعمال المعطيات المتحصل عليها إلا في إطار الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والكشف عنها والتحقيق فيها[1].

ويترتب على هذا المبدأ عدة نتائج قانونية، أهمها:

- حظر جمع البيانات التي لا ترتبط مباشرة بالجريمة محل البحث أو التحقيق.
- عدم جواز استخدام المعلومات المتحصل عليها لأغراض إدارية أو تجارية أو سياسية أو شخصية.
- الاقتصار على جمع القدر اللازم من المعلومات دون تجاوز مبدأ التناسب بين الإجراء المتخذ والغاية المرجوة منه.
- منع الاحتفاظ بالبيانات لمدة تتجاوز المدة اللازمة للتحقيق أو المتابعة القضائية.

[1] المادة 4/4 من 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 بتاريخ 16 أوت 2009.

- إلزام الجهات المختصة باتخاذ التدابير الفنية والتنظيمية الكفيلة بمنع الوصول غير المشروع إلى المعلومات المجمعة.

كما يرتبط هذا المبدأ ارتباطًا وثيقًا بمبدأ الشرعية الإجرائية، إذ لا يمكن للسلطات العامة مباشرة إجراءات المراقبة أو استغلال نتائجها إلا في الحدود التي رسمها القانون وتحت رقابة السلطة القضائية المختصة، ضمانًا لعدم تحول هذه الإجراءات الاستثنائية إلى وسيلة للمساس غير المبرر بالحقوق الأساسية للأفراد.

الفرع الثاني: تجريم المساس بالحياة الخاصة الناتج عن إساءة استعمال المعلومات

إذا كان المشرع الجزائري قد أجاز للسلطات المختصة اللجوء إلى إجراءات مراقبة الاتصالات الإلكترونية للمستهلك وتفتيش المنظومات المعلوماتية باعتبارها وسائل استثنائية لمكافحة الجرائم الإلكترونية، فإنه في المقابل أقر حماية جزائية للحياة الخاصة من خلال تجريم كل صور إساءة استعمال المعلومات المتحصل عليها بمناسبة تنفيذ هذه الإجراءات.

ويتحقق المساس بالحياة الخاصة عندما يتم استخدام البيانات والمعلومات الشخصية التي جُمعت بصورة مشروعة في غير الأغراض التي حددها القانون، أو عندما يتم إفشاؤها أو تداولها أو تمكين الغير من الاطلاع عليها دون سند قانوني.

وتتخذ إساءة استعمال المعلومات صورًا متعددة، من بينها نشر المراسلات الخاصة، أو تسريب البيانات الشخصية، أو الاحتفاظ بالمعلومات لمدة غير مبررة، أو استخدامها للإضرار بسمعة الأشخاص أو ابتزازهم أو التأثير على حياتهم المهنية أو الاجتماعية.

ولمواجهة هذه المخاطر، أكدت الفقرة الرابعة من المادة 4 من القانون رقم 04-09على ضرورة قصر استعمال المعلومات المتحصل عليها على الأهداف التي حددها القانون، بما يشكل ضمانة أساسية لحماية الحياة الخاصة للأفراد[1].

وإلى جانب الأحكام الخاصة الواردة في القانون رقم 09-04، كرس قانون العقوبات الجزائري حماية جزائية للحياة الخاصة من خلال تجريم الأفعال التي تنطوي على انتهاك

[1] المادة 4/4 من 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 بتاريخ 16 أوت 2009.

خصوصية الأفراد، لا سيما تلك المتعلقة بالتقاط أو تسجيل أو نقل أو إفشاء الأقوال أو الصور أو المعطيات الشخصية دون رضا أصحابها أو دون ترخيص قانوني.

وقد أورد المشرع الجزائري فيما يتعلق بالموضوع المواد من 303 مكرر إلى 303 مكرر 3 من قانون العقوبات بموجب "القانون رقم 23-06 المؤرخ في 20 ديسمبر سنة 2006"، حيث نص في المادة 303 مكرر على انه:" يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 50.000 دج إلى 300.000 دج. كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأية تقنية كانت وذلك:

بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص، بغير إذن صاحبها أو رضاه."[1]

أما المادة 303 مكرر 1 ، فنصت على انه يعاقب بالعقوبات المنصوص في المادة السابقة كل من احتفظ أو وضع أو سمح بان توضع في متناول الجمهور أو الغير أو استخدم بأية وسيلة كانت التسجيلات أو الصور أو الوثائق المتحصل عليها بواسطة أحد الأفعال المنصوص عليها في المادة 303 مكرر من هذا القانون." من خلال المادة 303 مكر رفق 2 من ق ع ج ، ومقارنتها بالمادة 226-1 فقرة 2 من ق ع ف والمادة 309 مكرر فقرة ب من ق ع م السالفتي الذكر، يتضح أن جنحة الحصول على صورة الشخص دون موافقة صاحبها أو رضاه.[2]

وتكتسي هذه الحماية أهمية خاصة في البيئة الرقمية، بالنظر إلى سهولة نسخ المعلومات وتخزينها ونقلها ونشرها عبر الوسائط الإلكترونية، وما يترتب على ذلك من تضاعف مخاطر الاعتداء على الخصوصية.

كما أن مساءلة مرتكبي هذه الأفعال لا تقتصر على المسؤولية الجزائية فحسب، بل قد تمتد إلى المسؤولية المدنية لجبر الأضرار التي تلحق بالأشخاص المتضررين، فضلاً عن المسؤولية التأديبية بالنسبة للأعوان والموظفين العموميين الذين يثبت إخلالهم بواجب المحافظة على سرية المعلومات.

[1] العاقب عيسى، **حماية حق الانسان في صورته**، دراسات قانونية، دورية فصلية تصدر عن مركز البحوث والاستشارات والخدمات التعليمية ، الجزائر، جانفي 2013 ، ، ص 170

[2] نفس المرجع، ص 171

ومن ثم، فإن تجريم المساس بالحياة الخاصة الناتج عن إساءة استعمال المعلومات يشكل آلية قانونية أساسية لضمان فعالية الحماية المقررة للمعطيات الشخصية، وتحقيق التوازن بين ضرورات الأمن ومكافحة الجريمة من جهة، واحترام الحقوق والحريات الفردية من جهة أخرى.

المطلب الثاني: تقييد استعمال المعلومات المتحصل عليها

حرص المشرع الجزائري، عند إقراره لإجراءات مراقبة الاتصالات الإلكترونية للمستهلك وتفتيش المنظومات المعلوماتية، على وضع ضوابط قانونية تكفل عدم الانحراف باستعمال المعلومات والبيانات المتحصل عليها من هذه الإجراءات الاستثنائية. فبالرغم من أهميتها في الكشف عن الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال وجمع الأدلة المتعلقة بها، إلا أن خطورتها تكمن في إمكانية المساس بحرمة الحياة الخاصة وسرية المعطيات الشخصية، الأمر الذي استوجب تقييد استعمالها وحصره في الحدود التي رسمها القانون، مع فرض التزام صارم بالمحافظة على سريتها وعدم إفشائها إلا في الحالات التي يجيزها القانون.

الفرع الأول: حصر استعمال المعلومات في أغراض التحري والتحقيق

ألزم المشرع الجزائري الجهات المختصة بعدم استعمال المعلومات والبيانات المتحصل عليها من إجراءات مراقبة الاتصالات الإلكترونية للمستهلك وتفتيش المنظومات المعلوماتية إلا في الحدود التي اقتضتها ضرورة البحث والتحري والتحقيق القضائي. ويهدف هذا القيد إلى منع توظيف المعطيات المجموعة لأغراض أخرى لا تمت بصلة إلى الجريمة محل المتابعة، سواء تعلق الأمر باستغلالها لتحقيق مصالح شخصية أو مهنية أو استخدامها في قضايا أخرى خارج الإطار القانوني المحدد[1].

وقد نصت المادة 9 من القانون رقم 04-09المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على أن المعلومات المتحصل عليها بمناسبة تنفيذ هذه الإجراءات لا يجوز استعمالها إلا للأغراض التي رخصت من

[1] المادة 9 من القانون رقم 09-04

أجلها، وهو ما يعكس حرص المشرع على تحقيق التوازن بين متطلبات الكشف عن الجرائم وضمان احترام الحقوق والحريات الأساسية للأفراد، وعلى رأسها الحق في الخصوصية[1].

وتبرز أهمية هذا القيد في الحد من مخاطر التعسف في استعمال السلطة، إذ يترتب على مخالفة هذا الالتزام إمكانية مساءلة القائمين على تنفيذ هذه الإجراءات، فضلا عن إمكانية استبعاد الأدلة المتحصل عليها إذا ثبت استخدامها خارج النطاق الذي حدده القانون.

الفرع الثاني: حماية سرية المعلومات المتحصل عليها

إلى جانب تقييد استعمال المعلومات، أوجب المشرع الجزائري المحافظة على سرية البيانات والمعطيات التي يتم الحصول عليها بمناسبة تنفيذ إجراءات مراقبة الاتصالات الإلكترونية للمستهلك وتفتيش المنظومات المعلوماتية، وذلك بالنظر إلى طبيعتها الحساسة وما قد يترتب على كشفها أو تداولها من مساس بالحياة الخاصة للأفراد أو الإضرار بمصالحهم المشروعة.

لقد بدا سر المهنة كواجب أخلاقي تمليه قواعد الأخلاق والشرف والأمانة، وجزاء الإخلال به سيتوجب محاسبة الفرد أدبيا، شانه في ذلك شان الالتزامات الأخرى، واقتصر الأمر على بعض الطوائف التقليدية من المهن كالطب والمحاماة وأعمال رجال الدين من الكهنة، إلا أنه إزاء تطور الدولة واتساع نشاطها في مجالات الحياة وازدياد واجباتها، فقد وجد مبدأ سر المهنة له تطبيقات كثيرة في أعمال كالقضاء والوظيفة العامة والمصارف وغيرها وشعور الأفراد بضرورة الجزاء المادي ضمانا لحقوقهم.

السر في اللغة هو ما تكتمه وتخفيه ويشتمل على كل قول أو فعل ينبغي أن يبقى مكتوما[2]

لم يرد في القانون تعريف لسر المهنة مما يتعين على الفقهاء وضع تعريف له لان تحديد السر مسالة تختلف باختلاف الزمان والمكان والأشخاص وطبيعة الوقائع والأحداث، فقد يكون أمرا ما سرا في زمان ولا يكون سرا في زمان آخر، وقد يكون سرا في مكان آخر

[1] المادة 9 من 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 بتاريخ 16 أوت 2009.

[2] بولرباح نويجم ، مسؤولية الضبطية القضائية عن إفشاء السر المهنية مذكرة ضمن متطلبات نيل شهادة الماستر حقوق تخصص إدارة ومالية، جامعة زيان عاشور بالجلفة ، 2016-2017، ص22

ولا يكون سرا في مكان آخر، وقد يكون سرا بالنسبة للأشخاص ولا يكون بالنسبة لأشخاص آخرين.

و هناك من يرى أن القانون لم يبين معنى السر ولا هو بمستطيع ذلك ويجب أن يرجع في ذلك إلى العرف وإلى طريق كل حادثة على انفراد وبهذا قضت محكمة النقض المصرية وعرفت موسوعة دالوز السر بأنه كل ما يعني إفشاؤه بسمعة مودعة أو كرامته واعتراض بعض الفقهاء على ذلك بالقول: " إن السر قد يكون مشرفا لمن يريد كتمانه ومع ذلك يعتبر سرا "، ولأهمية تعريف السر المهني سنتعرض له بالمفهوم اللغوي والمفهوم الاصطلاحي[1].

وقد جرم المشرع الجزائري على غرار معظم التشريعات الفرنسي والأردني واللبناني، إفشاء السر المهني، وذلك في القسم الخامس من الفصل الأول من الباب الثاني، تحت عنوان الاعتداء على شرف واعتبار الأشخاص وعلى حياتهم الخاصة وإفشاء الأسرار.

يعاقب بالحبس من شهر إلى ستة أشهر وبغرامة :« تنص المادة 301 من قانون العقوبات من 20.000 إلى 100.000 دج الأطباء والجراحون والصيادلة والقابلات وجميع المؤتمنين بحكم الواقع أو المهنة أو الوظيفة الدائمة أو المؤقتة على أسرار أدلي بها إليهم وأفشوها ...». في غير الحالات التي يوجب عليهم فيها القانون إفشاءها ويصرح لهم بذلك من خلال هذا النص، نجذ أن المشرع الجزائري اعتبر إفشاء السر المهني جنحة معاقب عليها، سواء ارتكبها شخص طبيعي أو شخص معنوي، ومهما تكن طبيعة الوظيفة التي يمارسها الشخص، دائمة كانت أو مؤقتة، وسواء كان الإفشاء كتابة أو شفاهة.

لكن سمح المشرع في حالات محددة إفشاء الأسرار التي تحصلوا عليها بمناسبة ممارستهم لمهنتهم إذا كان من شأن هذا الإفشاء حماية مصلحة أولى بالحماية.

اما في قانون الإجراءات الجزائية فيجد يجد السر المهني أساسه أيضا في قانون الإجراءات الجزائية والذي نص على ضرورة التزام المهني بالسر وعدم إفشاءه، سواء فيما يتعلق بإجراءات التحقيق أو التفتيش.

[1] سليمان علي حمادي الحلبوسي، **المسؤولية المدنية الناشئة عن إفشاء السر المهني(دراسة قانونية)**، بيروت، لبنان، ص 18

حيث تكون إجراءات التحري والتحقيق تنص المادة 19 من قانون الإجراءات الجزائية سرية، ما لم ينص القانون على خلاف ذلك، ودون إضرار بحقوق الدفاع.

كل شخص يساهم في هذه الإجراءات ملزم بكتمان السر المهني بالشروط المبينة في قانون العقوبات وتحت طائلة العقوبات المنصوص عليها فيه[1]

نستنتج من هذه المادة، أنه يمنع الإدلاء بإجراءات التحري التي تجرى من طرف كل الأشخاص المساهمين فيها، لأنها تعد سرية ويجب أن تبقى في طي الكتمان، لأن إفشاؤها يمس بكرامة واعتبار المعنيين بها.[2]

والهدف من ذلك هو العمل على حسن سير هذه الإجراءات وكل مفش لها يعاقب طبقا لنص المادة 301 من قانون العقوبات، ويحرص القانون أيضا، على ضرورة التزام القائمين بإجراءات التفتيش بمراعاة الأشخاص المؤتمنين على السر المهني أثناء تأديتهم لمهامهم، وذلك بعدم تفتيش الأشياء التي تحتوي على معلومات سرية وعدم الإطلاع عليها، غير أنه يجب عند تفتيش أماكن يشغلها شخص ملزم وهذا ما جاءت به المادة 76 في فقرتها الرابعة من قانون الاجراءات الجزائية والتي تنص بكتمان السر المهني أن تتخذ مقدما جميع التدابير اللازمة لضمان احترام ذلك السر [3]كما تنص المادة 77 من نفس القانون [4]على معاقبة كل من أفشى مستندا ناتجا من التفتيش أو أطلع عليه شخصا لا صفة له قانونا في الإطلاع عليه، وذلك بغير إذن من المتهم أو من الموقع على ذلك المستند أو من ذوي حقوقه أو من المرسل إليه ما لم تدع ضرورات التحقيق إلى غير ذلك.

---

[1] المادة 19 من القانون 25-14

[2] ما ديو نصيرة، **افشاء السر المهني بين الاباحة والتجريم** ، مذكرة لنيل شهادة الماجستير في القانون، فرع : "قانون المسؤولية المهنية"، جامعة مولود معمري – تيزي وزو ، 2010، ، ص 39

[3] الفقرة الرابعة من المادة 76 من الامر25-14:" غير أنه يجب عند تفتيش أماكن يشغلها شخص ملزم قانونا بكتمان السر المهني أن تتخذ مقدما جميع التدابير اللازمة لضمان إحترام ذلك السر .

تغلق الأشياء أو المستندات المحجوزة ويختم عليها، إذا أمكن ذلك، فإذا تعذرت الكتابة عليها فإنها توضع في وعاء أو كيس يضع عليه ضابط الشرطة القضائية شريطا من الورق ويختم عليه بختمه .

[4] المادة 77 من نفس القانون:" يعاقب بالحبس من شهرين (2) إلى سنتين (2) وبغرامة تتراوح بين 50.000 دج إلى 150.000 دج، كل من أفشى مستندا ناتجا من التفتيش أو أطلع عليه شخصا لا صفة له قانونا في الاطلاع عليه وذلك بغير إذن من المتهم أو من ذوي حقوقه أو من الموقع على هذا المستند أو من المرسل إليه ما لم تستدع ضرورات التحقيق غير ذلك.

وتضيف المادة 161 من نفس القانون على معاقبة كل من أفشى أو أذاع مستندا متحصلا من تفتيش شخص، لا صفة له قانونا في الإطلاع عليه[1].

فطبقا لهذه النصوص لا يحق للمهني إفشاء سر إجراءات التحقيق، لأن للسر المهني طابعين؛ طابع حقوق الدفاع الرامية إلى المحافظة على سرية الأمانة المصرح للمحامي بصفته تلك وطابع النظام العام المستوجب احترامه تفاديا للمتابعة الجزائية المنصوص عليها في قانون العقوبات

وفي هذا الإطار، نصت الفقرة الثانية من المادة 10 من القانون رقم 04-09على التزام الأشخاص المكلفين بتنفيذ هذه الإجراءات، وكل من يطلع بحكم وظيفته أو مهامه على المعلومات المتحصل عليها، بالمحافظة على سريتها وعدم إفشائها أو استغلالها خارج الحدود التي يسمح بها القانون[2].

ويهدف هذا الالتزام إلى تعزيز الثقة في الإجراءات القانونية المتخذة لمكافحة الجرائم الإلكترونية، وضمان عدم تحول وسائل التحري الخاصة إلى أداة لانتهاك الخصوصية أو المساس بالحقوق الأساسية للأفراد. كما يشكل واجب المحافظة على السر المهني ضمانة أساسية لحماية المعطيات الشخصية ومنع تداولها أو تسريبها بطرق غير مشروعة.

ويترتب على الإخلال بهذا الواجب قيام المسؤولية القانونية، سواء كانت جزائية أو تأديبية، وفقا للأحكام العامة المتعلقة بإفشاء السر المهني وانتهاك سرية المعلومات.

[1] المادة 161 من نفس القانون:" دون الإخلال بالعقوبات الأشد المنصوص عليها في التشريع الساري المفعول، يعاقب بالحبس من شهرين (2) إلى سنتين (2) وبغرامة من 20.000 دج إلى 200.000 دج، كل من أفشى أو أذاع مستندا متحصلا من تفتيش إلى شخص لاصفة له قانونا في الاطّلاع عليه وكان ذلك بغير إذن من المتهم أو من خلفه أو الموقع بإمضائه على المستند أو الشخص المرسل إليه وكذلك كل من استعمل ما وصل إلى علمه منه، ما لم يكن ذلك من ضرورات التحقيق القضائي.

[2] المادة 2/10 من 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 بتاريخ 16 أوت 2009.

خلاصة

من خلال دراسة الضمانات الإجرائية المقررة للمستهلك أثناء جمع المعلومات ومراقبة الاتصالات الإلكترونية يتضح أن التطور التكنولوجي فرض على المشرع الجزائري ضرورة إيجاد آليات قانونية جديدة لمواجهة الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال، غير أن استعمال هذه الآليات يثير إشكالية أساسية تتمثل في احتمال تعارضها مع الحق في الخصوصية وسرية الاتصالات.

وقد تبين أن المشرع الجزائري من خلال القانون رقم 04-09 حاول تحقيق نوع من التوازن بين متطلبات البحث والتحري في الجرائم الإلكترونية وبين ضرورة حماية الحقوق والحريات الفردية، وذلك من خلال إخضاع إجراءات مراقبة الاتصالات الإلكترونية وتفتيش المنظومات المعلوماتية لجملة من القيود القانونية. فقد تم حصر اللجوء إلى هذه الإجراءات في حالات محددة ترتبط بالوقاية من الجرائم الخطيرة أو كشف الجرائم المعلوماتية عندما يصعب الوصول إلى الأدلة بالوسائل التقليدية.

كما أن هذه الإجراءات لم تترك للسلطات المختصة بصورة مطلقة، بل أخضعها المشرع لضوابط إجرائية تهدف إلى الحد من التعسف، من بينها ضرورة الحصول على إذن قضائي مسبق، وتحديد نطاق استعمال المعلومات المتحصل عليها، وربط الإجراء بالغاية التي شرع من أجلها. ويعد ذلك ضمانة مهمة للحفاظ على خصوصية المستهلك باعتبار أن بياناته الإلكترونية أصبحت تمثل جزءاً من حياته الخاصة.

وقد أظهرت الدراسة أن حماية الخصوصية لا تقتصر فقط على مرحلة جمع المعلومات، وإنما تمتد إلى مرحلة استعمالها، حيث ألزم المشرع الجهات المختصة بعدم توظيف المعطيات المتحصّل عليها إلا في إطار التحريات والتحقيقات القانونية، مع تجريم كل استعمال غير مشروع لها قد يؤدي إلى المساس بالحياة الخاصة للأفراد.

الفصل الثاني:

الضمانات الإجرائية المقررة للمستهلك أثناء التفتيش والحجز الإلكتروني

الفصل الثاني: الضمانات الإجرائية المقررة للمستهلك أثناء التفتيش والحجز الإلكتروني

إذا كان الفصل الأول قد تناول الضمانات المرتبطة بالمراقبة الإلكترونية وجمع المعلومات الرقمية، فإن حماية الخصوصية لا تكتمل إلا بدراسة الإجراءات اللاحقة التي تتمثل أساساً في التفتيش الإلكتروني وحجز المعطيات المعلوماتية. فهذه الإجراءات تعد من أكثر التدابير تأثيراً على حرمة الحياة الخاصة، لأنها تمكن السلطات من الوصول إلى محتويات الأنظمة المعلوماتية والبيانات المخزنة داخلها.

وقد أدرك المشرع الجزائري خطورة هذه الإجراءات، لذلك وضع مجموعة من القواعد التي تنظم كيفية مباشرتها، وتحدد نطاق تدخل السلطات المختصة، مع فرض التزامات تهدف إلى المحافظة على سلامة البيانات وعدم المساس بمحتواها إلا في الحدود التي تقتضيها ضرورة التحقيق.

وسيتم تناول هذا الفصل من خلال مبحثين؛ يخصص المبحث الأول للضمانات المتعلقة بإجراءات التفتيش الإلكتروني، بينما يتناول المبحث الثاني الضمانات المرتبطة بالحجز الإلكتروني وحماية المعطيات بعد ضبطها.

الفصل الثاني: الضمانات الإجرائية المقررة للمستهلك أثناء التفتيش والحجز الإلكتروني

المبحث الأول: الضمانات المتعلقة بالتفتيش الإلكتروني

إن خصوصية التفتيش الإلكتروني تختلف عن التفتيش التقليدي، إذ لا ينصب فقط على مكان مادي محدد، وإنما قد يمتد إلى فضاءات رقمية تحتوي على كميات كبيرة من المعلومات الشخصية والخاصة، مثل المراسلات الإلكترونية، الملفات الشخصية، بيانات الاتصال، والمعاملات الرقمية للمستهلك. وهو ما يجعل هذا الإجراء من أكثر الإجراءات الجزائية مساساً بالحق في الخصوصية، خاصة في ظل إمكانية الاطلاع على بيانات لا ترتبط مباشرة بالجريمة محل البحث.

ومن هذا المنطلق، لم يجعل المشرع الجزائري التفتيش الإلكتروني إجراءً مطلقاً، وإنما أحاطه بجملة من الضمانات القانونية التي تهدف إلى تحقيق التوازن بين ضرورة تمكين الجهات المختصة من الوصول إلى الأدلة الرقمية، وبين حماية حرمة الحياة الخاصة للأفراد. وقد نظم القانون رقم 04-09المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها أحكام التفتيش الإلكتروني، من خلال تحديد الجهات المختصة بمباشرته، وضبط نطاق امتداده إلى الأنظمة المعلوماتية الأخرى المرتبطة بالنظام محل التفتيش.[1]

وعليه، سيتم تناول هذا المبحث من خلال دراسة الرقابة القانونية المفروضة على إجراءات التفتيش الإلكتروني، وذلك من خلال مطلبين؛ يخصص الأول لبيان خضوع التفتيش الإلكتروني للسلطة القضائية وضباط الشرطة القضائية المختصين، بينما يتناول الثاني تنظيم التفتيش الممتد إلى الأنظمة المعلوماتية الأخرى.

المطلب الأول: الرقابة القانونية على إجراءات التفتيش الإلكتروني

يُعتبر التفتيش الإلكتروني من الإجراءات التي تثير إشكالية التوفيق بين متطلبات مكافحة الجرائم المعلوماتية وبين ضمان احترام الحقوق والحريات الأساسية، إذ إن تنفيذه قد يؤدي إلى الاطلاع على محتويات رقمية ذات طابع شخصي لا تقتصر على المعلومات المرتبطة بالجريمة فقط.

[1] القانون رقم 09-04

ولهذا فإن إخضاع التفتيش الإلكتروني للرقابة القانونية يعد من أهم الضمانات الإجرائية التي تحول دون التعسف في استعمال السلطة، حيث لا يجوز لأي جهة القيام بهذا الإجراء إلا في إطار الصلاحيات التي منحها القانون، وتحت إشراف الجهات المؤهلة قانوناً.

وقد حرص المشرع الجزائري من خلال القانون 04-09على تحديد الأشخاص المخولين بإجراء التفتيش الإلكتروني، كما نظم كيفية امتداده إلى أنظمة معلوماتية أخرى عندما تكون هناك علاقة بين النظام محل التفتيش ونظام آخر يحتوي على أدلة رقمية ذات صلة بالجريمة.[1]

وبناءً على ذلك، سيتم تقسيم هذا المطلب إلى فرعين:

الفرع الأول: خضوع التفتيش للسلطة القضائية وضباط الشرطة القضائية المختصين

يُعد إخضاع التفتيش الإلكتروني للسلطة القضائية أحد أهم مظاهر الشرعية الإجرائية، باعتبار أن هذا الإجراء ينطوي على مساس مباشر بسرية البيانات والمعلومات المخزنة في الأنظمة المعلوماتية. فالتفتيش الإلكتروني لا يتعلق فقط بالبحث عن أشياء مادية، وإنما قد يؤدي إلى كشف جوانب دقيقة من الحياة الخاصة للأفراد، مما يستوجب أن يكون تحت رقابة جهة تتمتع بالحياد والاستقلال.

وانطلاقاً من ذلك، لم يمنح المشرع الجزائري صلاحية إجراء التفتيش الإلكتروني لأي شخص، وإنما قصرها على الجهات التي حددها القانون، وفي مقدمتها ضباط الشرطة القضائية المختصون، مع ضرورة احترام القواعد العامة المنظمة للتفتيش في قانون الإجراءات الجزائية.

وقد نصت المادة 5 الفقرة الأولى من القانون 04-09على إمكانية قيام ضباط الشرطة القضائية، بعد الحصول على إذن من السلطة القضائية المختصة، بالدخول إلى الأنظمة المعلوماتية أو البيانات المخزنة بها بغرض البحث عن الأدلة المرتبطة بالجرائم المعلوماتية.[2]

وعليه، سيتم تناول هذا الفرع من خلال العناصر التالية:

[1] المادة 5 من القانون رقم 09-04.

[2] الفقرة الأولى من المادة 5 من القانون رقم 09-04.

أولا: دور السلطة القضائية في الإذن بالتفتيش الإلكتروني

يشكل الإذن القضائي ضمانة أساسية لحماية الحقوق والحريات أثناء تنفيذ التفتيش الإلكتروني، لأنه يمنع لجوء الجهات المكلفة بالبحث والتحري إلى هذا الإجراء بصورة تلقائية أو تعسفية[1].

فالسلطة القضائية باعتبارها الحامية للحقوق والحريات تتولى تقدير مدى توفر الشروط القانونية التي تبرر إجراء التفتيش، ومدى ارتباطه بضرورة البحث عن الأدلة المتعلقة بالجريمة.

ويكتسي هذا الأمر أهمية خاصة في المجال الإلكتروني، لأن النظام المعلوماتي الواحد قد يحتوي على معلومات متعددة لا ترتبط بالجريمة محل البحث، مثل الصور الشخصية، المراسلات الخاصة، البيانات المالية أو معلومات المستهلك المتعلقة بمعاملاته الإلكترونية.

ومن ثم، فإن تدخل القاضي قبل مباشرة التفتيش يسمح بالتأكد من وجود مبررات جدية لاتخاذ هذا الإجراء، ويضمن عدم تحول البحث عن الأدلة الرقمية إلى وسيلة للاطلاع غير المشروع على الحياة الخاصة للأفراد.

ثانيا: اختصاص ضباط الشرطة القضائية في تنفيذ إجراءات التفتيش الإلكتروني

إذا كانت السلطة القضائية تضطلع بدور الرقابة والإذن، فإن تنفيذ التفتيش الإلكتروني يندرج ضمن اختصاص ضباط الشرطة القضائية الذين يمتلكون الصفة القانونية والخبرة التقنية اللازمة لمباشرة هذا النوع من الإجراءات.

غير أن تدخل ضباط الشرطة القضائية لا يعني منحهم سلطة مطلقة في التعامل مع البيانات الرقمية، وإنما يتعين عليهم الالتزام بحدود الإذن القضائي، فلا يجوز لهم البحث إلا عن المعلومات المرتبطة بالجريمة محل التحقيق.

كما يجب عليهم احترام سلامة المعطيات الرقمية، لأن أي تعديل أو حذف أو تغيير في محتوى البيانات قد يؤثر على حجيتها كدليل أمام القضاء.

[1] الفقرة الاخيرة من المادة 04 من القانون 09-04.

وتظهر أهمية هذا القيد بالنسبة للمستهلك الإلكتروني، لأن جهازه أو حسابه الرقمي قد يحتوي على بيانات شخصية عديدة، وبالتالي فإن أي تجاوز في نطاق التفتيش قد يؤدي إلى انتهاك مباشر لخصوصيته.

ثالثا: أهمية الرقابة القضائية في حماية خصوصية المستهلك الإلكتروني

تزداد أهمية الرقابة القضائية في مجال التفتيش الإلكتروني بالنظر إلى الطبيعة الخاصة للبيانات الرقمية، حيث إن المعلومات المخزنة إلكترونياً يمكن أن تكشف عن تفاصيل واسعة من حياة الشخص.

فالمستهلك عند استخدامه للمنصات الرقمية يترك آثاراً إلكترونية تتضمن بيانات الهوية، عمليات الشراء، وسائل الدفع، سجل الاتصالات وغيرها، وهي معلومات تدخل ضمن نطاق الخصوصية.

ولهذا فإن إخضاع التفتيش الإلكتروني لرقابة القضاء يمثل ضمانة تمنع التوسع غير المشروع في الوصول إلى هذه البيانات، ويحقق التوازن بين متطلبات الإثبات الجنائي وحماية الحقوق الفردية[1].

الفرع الثاني: تنظيم التفتيش الممتد إلى الأنظمة المعلوماتية الأخرى

تتميز الجرائم الإلكترونية بطبيعتها العابرة للحدود التقنية، حيث قد لا تكون الأدلة الرقمية محفوظة داخل النظام المعلوماتي محل التفتيش، بل قد تكون موجودة في نظام آخر مرتبط به، سواء داخل الدولة أو خارجها. وهذا الأمر يفرض إمكانية امتداد التفتيش الإلكتروني إلى أنظمة معلوماتية أخرى، غير أن هذا الامتداد قد يؤدي إلى توسيع نطاق التدخل في خصوصية الأفراد.

ولهذا وضع المشرع الجزائري ضوابط خاصة لهذا النوع من التفتيش، حيث أجاز الوصول إلى الأنظمة المعلوماتية المرتبطة بالنظام محل التفتيش متى كانت البيانات المطلوبة متاحة من خلاله، مع ضرورة احترام الشروط القانونية المتعلقة بمشروعية الإجراء.

[1] شيماء عبد الغنى عطاالله، مرجع سابق، ص 07.

وقد نصت المادة 5 الفقرة الثانية من القانون 04-09على إمكانية تمديد التفتيش إلى نظام معلوماتي آخر إذا كانت هناك أسباب تدعو إلى الاعتقاد بأن البيانات المتعلقة بالجريمة موجودة فيه، وكان الوصول إليها ممكناً من خلال النظام الأول.[1]

أولاً: مبررات امتداد التفتيش إلى الأنظمة المعلوماتية الأخرى

يرجع السماح بامتداد التفتيش الإلكتروني إلى طبيعة البيئة الرقمية التي لا ترتبط فيها البيانات دائماً بجهاز واحد، فقد يتم تخزين المعلومات في خوادم بعيدة أو حسابات إلكترونية مرتبطة بالنظام محل التفتيش.

ولهذا فإن قصر التفتيش على النظام الأصلي قد يؤدي إلى عدم الوصول إلى الأدلة الرقمية، مما يعرقل عملية الكشف عن الجرائم الإلكترونية[2].

غير أن هذا الامتداد يجب أن يبقى مرتبطاً بوجود علاقة مباشرة بين النظام الثاني والجريمة محل البحث، حتى لا يتحول إلى وسيلة للوصول العشوائي إلى بيانات الأشخاص.

ثانياً: ضرورة احترام نطاق الامتداد المعلوماتي

رغم أهمية هذا الإجراء في كشف الجرائم الإلكترونية، إلا أن امتداده يجب ألا يؤدي إلى تجاوز حدود الضرورة، لأن الوصول إلى أنظمة أخرى قد يكشف بيانات إضافية لا علاقة لها بالجريمة.

ولهذا يجب أن يقتصر البحث على البيانات المرتبطة بالواقعة الإجرامية، مع احترام مبدأ التناسب بين الهدف من التفتيش وحجم المعلومات التي يتم الوصول إليها.

ثالثاً: حماية خصوصية المستهلك عند امتداد التفتيش الإلكتروني

يمثل امتداد التفتيش إلى أنظمة أخرى خطورة خاصة بالنسبة للمستهلك الإلكتروني، لأن الخدمات الرقمية الحديثة تعتمد غالباً على التخزين السحابي وربط الحسابات الإلكترونية بعدة منصات.

ومن ثم فإن أي توسع غير منضبط في هذا الإجراء قد يؤدي إلى الاطلاع على بيانات شخصية وتجارية لا علاقة لها بالجريمة.

---

[1] الفقرة الثانية من المادة 5 من القانون رقم 09-04.

[2] المادة 05 من القانون 09-04

وعليه، فإن احترام الضوابط القانونية للامتداد المعلوماتي يعد شرطاً أساسياً لضمان فعالية التفتيش الإلكتروني دون التضحية بالحق في الخصوصية.

يتضح أن المشرع الجزائري حاول إحاطة التفتيش الإلكتروني بمجموعة من الضمانات الإجرائية، من خلال إخضاعه لرقابة السلطة القضائية وقصر تنفيذه على ضباط الشرطة القضائية المختصين، إضافة إلى تنظيم حالات امتداده إلى الأنظمة المعلوماتية الأخرى.

غير أن خصوصية البيئة الرقمية تفرض ضرورة تفسير هذه الإجراءات في نطاق ضيق، بما يضمن عدم تحول التفتيش الإلكتروني من وسيلة مشروعة لجمع الأدلة إلى أداة تؤدي إلى انتهاك خصوصية المستهلك وبياناته الشخصية.

المطلب الثاني: ضمانات حماية الخصوصية أثناء التفتيش

يمثل التفتيش الإلكتروني أحد أكثر الإجراءات الجزائية ارتباطاً بمسألة حماية الخصوصية، نظراً لما يسمح به من إمكانية الوصول إلى محتويات الأنظمة المعلوماتية والاطلاع على كميات هائلة من البيانات المخزنة رقمياً. فبخلاف التفتيش التقليدي الذي ينصب عادةً على أشياء مادية محددة، فإن التفتيش الإلكتروني قد يكشف عن معلومات شخصية واسعة تشمل المراسلات الخاصة، الصور، البيانات المالية، الملفات المهنية، وسجل التعاملات الإلكترونية للأفراد، وهو ما قد يؤدي إلى تجاوز نطاق البحث عن الدليل الجنائي إلى المساس بالحياة الخاصة[1].

وتزداد خطورة هذا الإجراء عندما تتعلق البيانات محل البحث بأنظمة معلوماتية مرتبطة بشبكات خارج الإقليم الوطني أو عندما تتطلب عملية استخراجها الاستعانة بأشخاص ذوي خبرة تقنية، إذ إن طبيعة البيئة الرقمية قد تفرض تدخل أطراف متعددة قادرة على الوصول إلى معلومات ذات طابع شخصي.

ولهذا حرص المشرع الجزائري، من خلال القانون رقم 04-09المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، على إحاطة

[1] مبدر لويس، **أثر التطور التكنولوجي على الحريات العامة**، رسالة دكتوراه، جامعة القاهرة،منشأة المعارف، دون سنة للنشر، مصر، ص 262.

التفتيش الإلكتروني بمجموعة من الضمانات التي تحد من مخاطر المساس بالخصوصية، حيث نظم مسألة الوصول إلى البيانات الموجودة خارج الإقليم الوطني، كما قيد الاستعانة بالخبراء بالقدر الذي تقتضيه ضرورة البحث والتحري.[1]

وعليه، سيتم تناول هذا المطلب من خلال فرعين:

الفرع الأول: تقييد الوصول إلى المعطيات الموجودة خارج الإقليم الوطني

أدى الطابع العابر للحدود الذي تتميز به الأنظمة المعلوماتية الحديثة إلى ظهور إشكالية جديدة تتمثل في إمكانية وجود الأدلة الرقمية خارج الإقليم الوطني، رغم ارتباطها بنظام معلوماتي موجود داخل الدولة، فقد يتم تخزين البيانات المتعلقة بجريمة إلكترونية في خوادم موجودة بدولة أجنبية، أو في منصات تعتمد تقنيات الحوسبة السحابية، الأمر الذي يجعل الوصول إليها يتجاوز الحدود الإقليمية التقليدية.

وبالرغم من أهمية هذا الإجراء في مكافحة الجرائم الإلكترونية، إلا أنه يثير إشكالات مرتبطة بالسيادة الوطنية وحماية خصوصية الأفراد، لأن الوصول إلى بيانات موجودة خارج الإقليم قد يؤدي إلى الاطلاع على معلومات شخصية لا ترتبط بالضرورة بالجريمة محل البحث.

ولهذا لم يجعل المشرع الجزائري هذا الامتداد مفتوحاً، وإنما أخضعه لضوابط محددة تهدف إلى ضمان أن يكون الوصول إلى البيانات الخارجية مرتبطاً بضرورة البحث عن الأدلة، دون أن يتحول إلى وسيلة للتوسع في الاطلاع على المعطيات الشخصية.

وقد نصت المادة 5 الفقرة الثالثة من القانون 04-09على إمكانية الوصول إلى البيانات الموجودة خارج الإقليم الوطني إذا كانت متاحة من خلال النظام المعلوماتي محل التفتيش، وذلك مع مراعاة القواعد المتعلقة بالتعاون الدولي.[2]

[1] القانون رقم 09-04 القانون رقم 09-04

[2] الفقرة الثالثة من المادة 5 من القانون رقم 09-04.

أولاً: الأساس القانوني للوصول إلى البيانات الموجودة خارج الإقليم الوطني

يقوم السماح بالوصول إلى البيانات الموجودة خارج الإقليم الوطني على فكرة أساسية تتمثل في أن طبيعة الجريمة الإلكترونية لا تتقيد بالحدود الجغرافية، إذ يمكن أن تكون الأدلة الرقمية موزعة بين عدة أنظمة أو خوادم مختلفة.

ومن ثم، فإن فعالية البحث والتحري تقتضي تمكين السلطات المختصة من الوصول إلى هذه البيانات عندما تكون مرتبطة بالنظام المعلوماتي محل التفتيش.

غير أن هذا الاختصاص لا يعني منح السلطات الوطنية صلاحية مطلقة للوصول إلى أي بيانات موجودة خارج الإقليم، وإنما يجب أن يكون ذلك في حدود ما يسمح به القانون، وأن تكون هناك علاقة مباشرة بين البيانات المطلوبة والجريمة محل التحقيق.

وبالتالي فإن المشرع حاول تحقيق توازن بين متطلبات مكافحة الجريمة الإلكترونية من جهة، واحترام سيادة الدول وحقوق الأفراد من جهة أخرى.

ثانياً: شرط ارتباط البيانات الخارجية بالنظام المعلوماتي محل التفتيش

يشترط المشرع أن تكون البيانات الموجودة خارج الإقليم متاحة من خلال النظام المعلوماتي محل التفتيش، أي أن يكون هناك ارتباط تقني وقانوني بين النظامين[1].

ويهدف هذا الشرط إلى منع قيام السلطات بالبحث العشوائي عن البيانات الموجودة في أنظمة أجنبية، لأن الأصل هو احترام الحدود الإقليمية وعدم ممارسة اختصاص خارج نطاق السلطة الوطنية إلا في الحالات التي يسمح بها القانون.

كما أن اشتراط هذا الارتباط يضمن أن يكون تدخل السلطات محدوداً بالبيانات الضرورية للتحقيق، فلا يمتد إلى معلومات أخرى لا علاقة لها بالجريمة.

ثالثاً: حماية خصوصية المستهلك عند الوصول إلى البيانات الخارجية

تظهر أهمية هذا القيد بالنسبة للمستهلك الإلكتروني، باعتبار أن العديد من الخدمات الرقمية تعتمد على تخزين البيانات في خوادم خارج الدولة، مثل خدمات التجارة الإلكترونية، الدفع الإلكتروني، والتخزين السحابي.

[1] المادة 05 من القانون 09-04.

فقد تحتوي هذه الأنظمة على معلومات شخصية دقيقة تتعلق بالمستهلك، مثل بيانات الهوية، الحسابات المالية، أو سجل العمليات الإلكترونية.

ولهذا فإن أي وصول غير منضبط إلى هذه البيانات قد يؤدي إلى انتهاك خطير للخصوصية، مما يفرض ضرورة احترام مبدأ التناسب وقصر الاطلاع على البيانات ذات الصلة بالجريمة فقط.

الفرع الثاني: الاستعانة بالخبراء في حدود ما تقتضيه إجراءات البحث

تتميز الأدلة الرقمية بطبيعتها التقنية المعقدة، مما يجعل التعامل معها يتطلب أحياناً الاستعانة بأشخاص متخصصين في مجال الإعلام الآلي والأمن السيبراني، بهدف استخراج البيانات وتحليلها والمحافظة على سلامتها التقنية.

غير أن تدخل الخبراء في إجراءات التفتيش الإلكتروني قد يشكل بدوره خطراً على الخصوصية، لأن الخبير بحكم عمله قد يطلع على معلومات شخصية أو سرية موجودة داخل النظام المعلوماتي محل التفتيش.

ولهذا فإن الاستعانة بالخبراء يجب ألا تكون وسيلة لتوسيع دائرة الاطلاع على البيانات، وإنما تظل مرتبطة بالضرورة التقنية التي يفرضها البحث عن الأدلة الرقمية.

وقد نصت المادة 5 الفقرة الرابعة من القانون 04-09على إمكانية الاستعانة بالخبراء لمساعدة ضباط الشرطة القضائية أثناء تنفيذ إجراءات التفتيش الإلكتروني، وذلك في الحدود التي تقتضيها عملية البحث والتحري.[1]

أولاً: ضرورة الاستعانة بالخبرة التقنية في مجال التفتيش الإلكتروني

إن الطبيعة التقنية للأنظمة المعلوماتية تجعل عملية البحث عن الأدلة الرقمية مختلفة عن التفتيش التقليدي، إذ تحتاج إلى معرفة متخصصة تمكن من الوصول إلى البيانات دون إتلافها أو تغيير محتواها.

فالخبير التقني يمكن أن يساهم في:

- استخراج الملفات المحذوفة .
- تحليل البيانات الرقمية .

[1] الفقرة الرابعة من المادة 5 من القانون رقم 09-04.

- تحديد مصدر المعلومات .
- المحافظة على سلامة الدليل الإلكتروني .

وتكتسي هذه المساعدة أهمية كبيرة لضمان حجية الدليل الرقمي أمام القضاء.

ثانياً: تقييد تدخل الخبير بمبدأ الضرورة

رغم أهمية دور الخبراء، فإن تدخلهم يجب أن يبقى محصوراً في الحدود التي تقتضيها إجراءات البحث، فلا يجوز أن يتحول دورهم إلى فرصة للاطلاع الواسع على محتويات النظام المعلوماتي.

فالأصل أن مهمة الخبير تقتصر على الجانب التقني، وليس له الحق في استعمال أو نسخ أو نشر المعلومات التي يطلع عليها أثناء أداء مهمته.

ومن ثم، فإن احترام مبدأ الضرورة يشكل ضمانة أساسية لحماية البيانات الشخصية للمستهلك، خاصة عندما تتضمن الأنظمة الإلكترونية معلومات تتعلق بحياته الخاصة أو معاملاته المالية.

ثالثاً: التزام الخبراء بالمحافظة على سرية البيانات

إن طبيعة المعلومات التي قد يطلع عليها الخبير أثناء التفتيش الإلكتروني تفرض إخضاعه لالتزام قانوني وأخلاقي بالمحافظة على السرية[1].

فإفشاء المعلومات التي يتم الاطلاع عليها أثناء تنفيذ المهمة أو استعمالها لأغراض شخصية يمثل اعتداءً على الخصوصية ويترتب عليه قيام المسؤولية القانونية.

وتزداد أهمية هذا الالتزام في المجال الإلكتروني، لأن تسريب البيانات الرقمية قد يؤدي إلى أضرار واسعة النطاق، بالنظر إلى سرعة انتشار المعلومات عبر الشبكات الإلكترونية.

يتضح أن المشرع الجزائري حاول من خلال المادة 5 من القانون 04-09وضع مجموعة من الضوابط التي تحكم التفتيش الإلكتروني بما يضمن عدم تحوله إلى وسيلة لانتهاك الخصوصية، حيث قيد الوصول إلى البيانات الموجودة خارج الإقليم الوطني

[1] المادة 10 من القانون 09-04

بضرورة ارتباطها بالنظام محل التفتيش، كما نظم الاستعانة بالخبراء وجعلها مرتبطة فقط بالحاجة التقنية التي تفرضها إجراءات البحث.

غير أن التطور المستمر للبيئة الرقمية يفرض تعزيز هذه الضمانات من خلال وضع قواعد أكثر تفصيلاً تحدد حدود الوصول إلى البيانات العابرة للحدود، وتنظم مسؤولية الخبراء والمتدخلين في معالجة الأدلة الرقمية، بما يحقق حماية أكثر فعالية للحق في الخصوصية للمستهلك الإلكتروني.

المبحث الثاني: الضمانات المتعلقة بالحجز الإلكتروني وحفظ المعطيات

يُعد الحجز الإلكتروني من أهم الإجراءات المستحدثة التي فرضتها الطبيعة الخاصة للجريمة المعلوماتية، إذ لم تعد الأدلة الجنائية تقتصر على الأشياء المادية التقليدية، وإنما أصبحت البيانات الرقمية بمختلف صورها تمثل عنصراً أساسياً في إثبات الجرائم وكشف مرتكبيها. وتشمل هذه البيانات الملفات الإلكترونية، الرسائل الرقمية، سجلات الدخول والاتصال، البرامج، وقواعد البيانات المخزنة داخل الأنظمة المعلوماتية.

غير أن خصوصية الدليل الإلكتروني تكمن في قابليته السريعة للتغيير أو النسخ أو الإتلاف، مما يجعل عملية حجزه تختلف عن الحجز التقليدي، إذ لا يتعلق الأمر فقط بضبط الشيء المادي، وإنما يتطلب اتخاذ تدابير تقنية دقيقة تهدف إلى المحافظة على سلامة البيانات وضمان عدم تعديلها أو العبث بمحتواها. كما أن عملية الحجز قد تؤدي إلى الاطلاع على معلومات شخصية لا ترتبط مباشرة بالجريمة، الأمر الذي يجعلها من الإجراءات التي قد تمس بشكل مباشر بالحق في الخصوصية.

وانطلاقاً من ذلك، حرص المشرع الجزائري من خلال القانون رقم 04-09المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، على وضع مجموعة من الضمانات التي تحكم مرحلة حجز المعطيات المعلوماتية، سواء أثناء عملية الضبط والنسخ، أو خلال مرحلة حفظ هذه البيانات بعد حجزها، وذلك بهدف تحقيق التوازن بين ضرورة الحصول على الدليل الرقمي ومتطلبات حماية الحياة الخاصة للأفراد.

وقد نظم المشرع هذه الضمانات ضمن القانون 09-04[1]، حيث حدد كيفية نسخ المعطيات الضرورية للتحقيق، وفرض المحافظة على سلامتها، كما وضع قيوداً على الوصول إليها أو تداولها بعد الحجز.

وعليه، سيتم تناول هذا المبحث من خلال مطلبين: **الأول** :الضمانات المقررة أثناء حجز المعطيات المعلوماتية و **الثاني** :الضمانات المقررة لحماية المعطيات بعد الحجز .

[1] ضمن المواد 6 و7 و8 من القانون 09-04،

المطلب الأول: الضمانات المقررة أثناء حجز المعطيات المعلوماتية

تمثل مرحلة حجز المعطيات المعلوماتية مرحلة دقيقة ضمن إجراءات البحث والتحقيق في الجرائم الإلكترونية، باعتبار أنها تتعلق بالتعامل مع دليل غير مادي يتميز بخصوصية تقنية تجعله قابلاً للتغيير أو النسخ أو المحو خلال فترة وجيزة.

فإذا كان الهدف الأساسي من الحجز هو تمكين الجهات المختصة من الاحتفاظ بالأدلة التي تساعد في كشف الحقيقة، فإن ذلك لا يعني منحها سلطة مطلقة في الاستيلاء على جميع البيانات الموجودة داخل النظام المعلوماتي، لأن هذا الأمر قد يؤدي إلى المساس بكمية كبيرة من المعلومات الخاصة التي لا علاقة لها بالجريمة محل البحث.

ولهذا أخضع المشرع الجزائري عملية الحجز الإلكتروني لمجموعة من الضوابط، أهمها الاقتصار على نسخ المعطيات الضرورية للتحقيق، والمحافظة على سلامة البيانات المحجوزة وعدم إجراء أي تعديل أو تغيير عليها، باعتبار أن سلامة الدليل الرقمي تعد شرطاً أساسياً لقبوله أمام القضاء.

وقد نصت المادة 6 من القانون 04-09على كيفية التعامل مع المعطيات المعلوماتية أثناء الحجز، حيث أجازت نسخ البيانات الضرورية للتحقيق، مع إلزام الجهات القائمة على الحجز باتخاذ التدابير اللازمة للمحافظة على سلامتها.[1]

وسيتم تناول هذا المطلب من خلال فرعين:

الفرع الأول: الاقتصار على نسخ المعطيات الضرورية للتحقيق

يعتبر مبدأ الاقتصار على نسخ المعطيات الضرورية للتحقيق من أهم الضمانات التي أقرها المشرع لحماية الخصوصية أثناء عملية الحجز الإلكتروني، لأنه يمنع التوسع في ضبط البيانات الرقمية بما يتجاوز الهدف الإجرائي المحدد.

فالنظام المعلوماتي محل الحجز قد يحتوي على عدد كبير من الملفات والبيانات الشخصية التي لا ترتبط بالجريمة موضوع البحث، مثل الصور الخاصة، المراسلات الشخصية، البيانات البنكية، أو المعلومات المتعلقة بنشاط المستهلك الإلكتروني، وبالتالي فإن نسخ جميع محتويات النظام قد يشكل تدخلاً غير مبرر في الحياة الخاصة.

[1] المادة 6 من القانون رقم 09-04.

ولهذا اعتمد المشرع الجزائري مبدأ الضرورة، حيث قيد عملية النسخ بالبيانات التي تكون لها علاقة مباشرة بالتحقيق.

وقد نصت المادة 6 الفقرة الأولى من القانون 04-09على أنه عندما تكون المعطيات محل البحث موجودة داخل نظام معلوماتي، يتم نسخها وحجزها وفق الإجراءات المحددة قانوناً، وذلك في الحدود التي تقتضيها ضرورة التحقيق.[1]

أولاً: مبدأ الضرورة في تحديد نطاق المعطيات المحجوزة

يقوم هذا المبدأ على قاعدة مفادها أن الحجز الإلكتروني لا يجب أن ينصب إلا على البيانات التي يكون لها ارتباط مباشر بالجريمة محل التحقيق[2].

فإذا كان الهدف من الإجراء هو البحث عن دليل رقمي معين، فلا يجوز للجهات القائمة بالحجز نسخ بيانات أخرى لا علاقة لها بالواقعة الإجرامية، لأن ذلك يؤدي إلى توسيع نطاق التدخل في خصوصية الأفراد.

ويكتسي هذا المبدأ أهمية خاصة بالنسبة للمستهلك الإلكتروني، باعتبار أن الأجهزة والأنظمة المعلوماتية أصبحت تحتوي على كم هائل من البيانات الشخصية التي تعكس مختلف جوانب حياته اليومية.

وعليه، فإن اقتصار الحجز على البيانات الضرورية يمثل وسيلة لتحقيق التوازن بين فعالية التحقيق وحماية الخصوصية.

ثانياً: منع تحويل الحجز الإلكتروني إلى وسيلة لجمع المعلومات الشخصية

إن الخطورة الأساسية التي قد تنتج عن الحجز الإلكتروني تتمثل في إمكانية استخدامه لجمع معلومات تتجاوز نطاق البحث عن الدليل.

فنسخ كامل محتويات جهاز إلكتروني أو حساب رقمي قد يؤدي إلى الحصول على معلومات شخصية لا علاقة لها بالجريمة، وهو ما يتعارض مع مبدأ التناسب.

ولهذا فإن احترام حدود الحجز يقتضي تحديد البيانات المطلوبة مسبقاً، وعدم الاحتفاظ إلا بما يخدم أغراض التحقيق.

---

[1] الفقرة الأولى من المادة 6 من القانون رقم 09-04.

[2] المادة 06 من القانون 09-04

الفرع الثاني: المحافظة على سلامة المعطيات وعدم المساس بمحتواها

تتميز الأدلة الرقمية بخصوصية تجعل المحافظة على سلامتها أمراً ضرورياً، إذ إن أي تغيير بسيط في محتوى البيانات أو طريقة استخراجها قد يؤدي إلى فقدان قيمتها الإثباتية أمام القضاء.

كما أن التعامل غير السليم مع البيانات المحجوزة قد يؤدي إلى تعديل معلومات شخصية أو حذفها أو كشفها لأشخاص غير مخولين، مما يشكل اعتداءً على خصوصية أصحابها.

ولهذا ألزم المشرع الجهات القائمة على الحجز باتخاذ التدابير التقنية اللازمة لضمان سلامة المعطيات وعدم المساس بمحتواها.

وقد نصت المادة 6 الفقرتان الثانية والثالثة من القانون 04-09على ضرورة اتخاذ الإجراءات المناسبة للمحافظة على سلامة البيانات المحجوزة وضمان عدم تغييرها أو إتلافها.[1]

أولاً: ضمان سلامة الدليل الإلكتروني

تُعد سلامة الدليل الإلكتروني من أهم الضمانات الإجرائية التي تحكم عملية الحجز المعلوماتي، باعتبار أن الدليل الرقمي يختلف عن الدليل التقليدي من حيث طبيعته التقنية وقابليته للتغيير أو النسخ أو الحذف دون ترك آثار مادية واضحة. لذلك فإن مجرد ضبط المعطيات المعلوماتية لا يكفي لضمان حجيتها أمام القضاء، وإنما يتعين المحافظة عليها في حالتها الأصلية منذ لحظة اكتشافها وحجزها إلى غاية عرضها على الجهات القضائية المختصة.

ويقصد بسلامة الدليل الإلكتروني **المحافظة على الحالة الأصلية للبيانات الرقمية وعدم إدخال أي تعديل أو تغيير عليها منذ لحظة ضبطها، بما يضمن بقاء محتواها مطابقاً لما كان عليه وقت الحجز** .ويهدف هذا المبدأ إلى ضمان الثقة في الدليل الإلكتروني باعتباره وسيلة إثبات، إذ إن أي تغيير يطرأ على البيانات، ولو كان بسيطاً، قد يؤدي إلى التشكيك في مصدرها أو محتواها أو مدى حجيتها أمام القضاء.

[1] الفقرتان الثانية والثالثة من المادة 6 من القانون رقم 09-04.

وقد أولى المشرع الجزائري أهمية خاصة لهذه الضمانة من خلال المادة 6 من القانون رقم 09-04، حيث ألزم الجهات القائمة على الحجز الإلكتروني باتخاذ التدابير اللازمة للمحافظة على سلامة المعطيات المعلوماتية وعدم المساس بمحتواها أثناء عمليات النسخ أو الحفظ.[1]

1.منع تعديل البيانات الأصلية

يُعد منع تعديل البيانات الأصلية من أهم مظاهر حماية الدليل الإلكتروني، إذ إن أي تغيير يطرأ على محتوى المعطيات المحجوزة قد يفقدها قيمتها الإثباتية ويثير الشك حول مدى صحتها ومصداقيتها.

فالبيانات الرقمية تختلف عن الأشياء المادية التقليدية، لأنها قابلة للتعديل بسرعة ودون ترك آثار واضحة في كثير من الأحيان، سواء تعلق الأمر بتغيير محتوى ملف إلكتروني، أو حذف جزء من البيانات، أو إعادة ترتيب المعلومات المخزنة داخل النظام المعلوماتي[2].

ولهذا يجب أن تتم عملية الحجز بطريقة تضمن عدم التعامل المباشر مع النسخة الأصلية للبيانات، وإنما يتم عادة إنشاء نسخة مطابقة لها تسمى **نسخة جنائية أو نسخة طبق الأصل** يتم العمل عليها خلال مراحل التحليل والفحص، مع المحافظة على البيانات الأصلية في حالتها الأولى.

ويكتسي هذا الإجراء أهمية خاصة بالنسبة لحماية خصوصية المستهلك الإلكتروني، لأن الأجهزة الرقمية قد تحتوي على معلومات شخصية عديدة، وأي تعديل أو عبث بهذه البيانات قد يؤدي إلى تغيير مضمونها أو الكشف عن معلومات لم تكن محل بحث أصلاً.

ومن ثم، فإن المحافظة على الأصل الرقمي للبيانات تمثل ضمانة مزدوجة، فهي تحمي من جهة قيمة الدليل أمام القضاء، وتحمي من جهة أخرى حقوق الأشخاص الذين تتعلق بهم هذه البيانات.

---

[1] المادة 6 من القانون رقم 09-04

[2] سعيد بن علي بن تركي الجلعود، **الدليل الرقمي وأثره في الإثبات دراسة فقهية تطبيقية مقارنة بالنظام السعودي**، مجلة العلوم الشرعية، جامعة القصيم، المجلد 17 ، العدد03 ، الجزء الأول، سنة 2024 ، ص06

2.استخدام وسائل تقنية موثوقة في نسخ المعطيات

إن عملية نسخ البيانات المعلوماتية لا تعد مجرد عملية تقنية بسيطة، وإنما تمثل إجراءً دقيقاً يجب أن يتم وفق وسائل تضمن مطابقة النسخة للبيانات الأصلية.

ولهذا يتعين استعمال أدوات وبرامج تقنية متخصصة تسمح باستخراج البيانات دون التأثير على محتواها، مع إمكانية التأكد لاحقاً من أن النسخة المستخرجة لم يطرأ عليها أي تعديل منذ إنشائها.[1]

وتكمن أهمية هذه الوسائل في ضمان ما يعرف بـ **سلامة السلسلة الرقمية للدليل،** أي التأكد من أن البيانات التي يتم تقديمها أمام القضاء هي نفسها التي تم ضبطها أثناء عملية الحجز.

كما أن الاعتماد على وسائل تقنية موثوقة يمنع حدوث أخطاء قد تكون ناتجة عن عمليات النسخ العادية، مثل فقدان بعض الملفات، أو تغيير خصائصها، أو التأثير على تاريخ إنشائها أو تعديلها، وهي عناصر قد تكون مهمة في إثبات الجريمة الإلكترونية.
وعليه، فإن استخدام الوسائل التقنية المناسبة يعد شرطاً أساسياً للحفاظ على القيمة القانونية للدليل الإلكتروني.[2]

3.الحفاظ على تسلسل عملية الحجز الإلكتروني

يقصد بتسلسل عملية الحجز الإلكتروني المحافظة على جميع المراحل التي مر بها الدليل منذ اكتشافه إلى غاية تقديمه أمام القضاء، وذلك من خلال تسجيل كل عملية تمت عليه، وتحديد الأشخاص الذين تعاملوا معه، وتاريخ ووقت كل إجراء تم اتخاذه.

ويعرف هذا الإجراء في المجال الجنائي بمفهوم سلسلة الحيازة أو سلسلة المحافظة على الدليل، ويهدف إلى إثبات أن الدليل لم يتعرض لأي تغيير أو تدخل غير مشروع أثناء انتقاله بين مختلف الجهات المكلفة بالبحث والتحقيق.

وتزداد أهمية هذا المبدأ في البيئة الرقمية بسبب سهولة نسخ البيانات وانتقالها بين عدة أجهزة أو أنظمة، مما يجعل توثيق مراحل التعامل معها أمراً ضرورياً لإثبات سلامتها.

---

[1] طرشي نورة، **مكافحة الجريمة المعلوماتية**، مذكرة من أجل الحصول على شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر 1، 2011-2012، ص 131.

[2] المادة07 من القانون 09-04

فإذا لم يتم تحديد كيفية ضبط البيانات والأشخاص الذين قاموا بمعالجتها، فقد يثار أمام القضاء دفع يتعلق بإمكانية تغيير الدليل أو التلاعب به، مما يؤثر على قوته الإثباتية.

4.توثيق جميع الإجراءات المتعلقة بالتعامل مع الدليل الرقمي

يشكل توثيق إجراءات التعامل مع الدليل الإلكتروني ضمانة أساسية لإثبات مشروعية عملية الحجز وسلامتها، إذ يجب تسجيل مختلف العمليات التي تمت على البيانات منذ لحظة ضبطها.

ويشمل ذلك بيان:

- تاريخ ومكان إجراء الحجز .
- الجهة التي قامت به .
- طبيعة الأجهزة أو الأنظمة التي تم استخراج البيانات منها .
- الوسائل التقنية المستخدمة في النسخ والتحليل .
- الأشخاص الذين اطلعوا على البيانات أو تعاملوا معها .

ويهدف هذا التوثيق إلى تحقيق الرقابة على مراحل التعامل مع الدليل الإلكتروني، ومنع أي استخدام غير مشروع له، كما يسمح للقاضي بتقييم مدى احترام الإجراءات القانونية المتعلقة بالحجز.

كما يمثل التوثيق وسيلة لحماية حقوق المستهلك، لأنه يضمن أن البيانات الشخصية التي تم ضبطها لم تستخدم إلا في الحدود التي يسمح بها القانون، وأنها لم تتعرض للكشف أو الاستغلال خارج نطاق التحقيق.

5.أثر سلامة الدليل الإلكتروني في تعزيز الثقة القضائية

إن احترام قواعد سلامة الدليل الإلكتروني يؤدي دوراً أساسياً في تعزيز ثقة القضاء في الأدلة الرقمية، لأن القاضي لا ينظر فقط إلى مضمون الدليل، وإنما يهتم كذلك بالطريقة التي تم الحصول عليه وحفظه بها[1].

[1] مراد بن عيسى، **حجية الدليل الرقمي في المادة الجزائية**، أطروحة دكتوراه، كلية الحق وق، جامعة الجزائر، 2019، ص 38

فالدليل الإلكتروني لا تكون له قيمة إثباتية إلا إذا ثبتت مشروعية الحصول عليه وسلامة المحافظة عليه منذ لحظة ضبطه إلى غاية تقديمه أمام المحكمة.

ومن هنا، فإن ضمان سلامة المعطيات لا يخدم فقط مصلحة التحقيق الجنائي، وإنما يحقق كذلك حماية للحقوق والحريات، لأنه يمنع استعمال بيانات الأشخاص أو تعديلها بصورة قد تؤثر على مركزهم القانوني.

وبذلك يتضح أن سلامة الدليل الإلكتروني تمثل حلقة أساسية في تحقيق التوازن بين متطلبات مكافحة الجرائم المعلوماتية وبين ضرورة احترام الحق في الخصوصية، خاصة بالنسبة للمستهلك الذي أصبحت بياناته الشخصية جزءاً من الأدلة الرقمية المحتمل جمعها أثناء إجراءات البحث والتحقيق.

ثانياً: حماية البيانات من التغيير أو الإتلاف

إن أي تدخل غير مشروع في البيانات المحجوزة قد يؤدي إلى فقدان قيمتها القانونية، كما قد يشكل اعتداءً على حقوق أصحابها.[1]

ولهذا يجب أن تتم عملية التعامل مع البيانات وفق إجراءات تقنية دقيقة، بحيث يقتصر دور الجهات المختصة على استخراج المعلومات الضرورية دون تعديل محتواها.

المطلب الثاني: الضمانات المقررة لحماية المعطيات بعد الحجز

لا تنتهي حماية الخصوصية بمجرد الانتهاء من عملية الحجز الإلكتروني، بل تمتد إلى المرحلة اللاحقة المتعلقة بحفظ البيانات المحجوزة والتعامل معها.

فالمعطيات التي يتم ضبطها أثناء التحقيق قد تتضمن معلومات شخصية حساسة، ولذلك فإن مجرد الاحتفاظ بها يفرض ضرورة وضع قيود على الأشخاص الذين يمكنهم الوصول إليها، وعلى كيفية استخدامها أو تداولها.

ولهذا وضع المشرع الجزائري مجموعة من الضمانات اللاحقة للحجز، تهدف إلى منع الوصول غير المشروع إلى البيانات المحجوزة، ومنع الاطلاع على المعطيات ذات المحتوى غير المشروع أو تداولها خارج الإطار القانوني، وسيتم تناول هذا المطلب من خلال فرعين:

[1] المادة 05 من القانون 09-04

الفرع الأول: منع الوصول غير المشروع إلى المعطيات المحجوزة

إن حفظ المعطيات المحجوزة يمثل مرحلة لا تقل أهمية عن مرحلة ضبطها، لأن البيانات الرقمية قد تبقى عرضة للخطر حتى بعد وضع اليد عليها من طرف السلطات المختصة.

ولهذا فإن حماية الخصوصية تقتضي ضمان عدم وصول الأشخاص غير المؤهلين إلى هذه البيانات، سواء كانوا من خارج الجهات المكلفة بالتحقيق أو حتى من داخلها إذا لم تكن لهم صفة أو ضرورة للاطلاع عليها.

وقد نصت المادة 7 من القانون 04-09على ضرورة اتخاذ التدابير اللازمة لمنع الوصول غير المشروع إلى المعطيات المحجوزة.[1]

أولاً: قصر الاطلاع على الجهات المخولة قانوناً

يجب أن يكون الوصول إلى البيانات المحجوزة مقتصراً على الأشخاص الذين تقتضي طبيعة مهامهم الاطلاع عليها.

فليس لكل موظف أو متدخل في إجراءات التحقيق الحق في الوصول إلى محتوى البيانات الرقمية، وإنما يحدد ذلك وفق الصفة القانونية والحاجة العملية.

ثانياً: حماية المستهلك من تسرب بياناته الشخصية

تكمن أهمية هذا القيد في حماية المستهلك الإلكتروني من مخاطر تسرب بياناته الخاصة، لأن الكشف غير المشروع عن المعلومات الرقمية قد يؤدي إلى أضرار مادية ومعنوية خطيرة.

الفرع الثاني: منع الاطلاع على المعطيات ذات المحتوى المجرّم وتقييد تداولها

تتميز المعطيات المعلوماتية الناتجة عن عمليات الحجز الإلكتروني بخصوصية كبيرة، إذ قد لا تقتصر فقط على البيانات التقنية المرتبطة بالجريمة محل البحث، وإنما قد تشمل أيضاً محتويات رقمية ذات طبيعة حساسة، من بينها صور أو تسجيلات أو مراسلات إلكترونية أو ملفات تتضمن معلومات شخصية أو أسراراً خاصة بالأفراد. وقد تكون هذه

[1] المادة 06من القانون رقم 09-04.

البيانات إما ذات صلة مباشرة بالجريمة المرتكبة، أو أنها تكشف عن عناصر إضافية يمكن أن تساعد الجهات القضائية في الوصول إلى الحقيقة[1].

غير أن اكتشاف هذه المعطيات لا يؤدي إلى اعتبارها مباحة التداول أو متاحة للاطلاع بشكل مطلق، لأن الغاية من الحجز الإلكتروني تتمثل في جمع الأدلة والمحافظة عليها، وليس في كشف مضمونها أو نشرها خارج الإطار الذي حدده القانون. فالمعطيات ذات المحتوى المجرّم، رغم أهميتها في المجال الإثباتي، تبقى محمية بمجموعة من المبادئ القانونية، وعلى رأسها احترام الحياة الخاصة، وسرية التحقيق، وحماية البيانات الشخصية للأفراد.

وتزداد أهمية هذه الحماية في البيئة الرقمية بالنظر إلى سهولة نسخ المعلومات وإعادة نشرها، إذ إن تسريب ملف إلكتروني واحد قد يؤدي إلى انتشاره على نطاق واسع خلال فترة زمنية قصيرة، مما قد يتسبب في أضرار جسيمة يصعب تداركها لاحقاً، سواء بالنسبة للأشخاص المعنيين بالبيانات أو بالنسبة للضحايا المحتملين للجريمة.

وانطلاقاً من ذلك، تدخل المشرع الجزائري لتنظيم كيفية التعامل مع هذه البيانات، حيث نصت المادة 8 من القانون رقم 04-09المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على ضرورة إخضاع المعطيات ذات المحتوى المجرّم لضوابط خاصة تمنع استعمالها أو تداولها خارج الحدود التي يقتضيها البحث والتحقيق.[2]

ويهدف هذا التنظيم إلى تحقيق التوازن بين مصلحتين أساسيتين؛ تتمثل الأولى في تمكين السلطات القضائية من الاستفادة من هذه البيانات باعتبارها أدلة ضرورية لإثبات الجرائم، بينما تتمثل الثانية في حماية خصوصية الأفراد ومنع تحول الإجراءات الجزائية إلى وسيلة لانتهاك حقوقهم الأساسية.

وعليه، سيتم تناول هذا الفرع من خلال عنصرين:

[1] المادة 08 من القانون 09-04

[2] المادة 8 من القانون رقم 09-04

أولاً: تقييد تداول المعطيات ذات المحتوى المجرّم

إن طبيعة المعطيات ذات المحتوى المجرّم تفرض إخضاعها لنظام قانوني خاص، إذ لا يمكن التعامل معها باعتبارها مجرد معلومات عادية، بل باعتبارها بيانات ذات قيمة إثباتية من جهة، وذات خطورة محتملة على الحقوق والحريات من جهة أخرى.

فقد تتضمن هذه المعطيات معلومات تكشف عن هوية أشخاص معينين، أو تفاصيل من حياتهم الخاصة، أو وقائع مرتبطة بسلوكيات مجرّمة، وبالتالي فإن السماح بتداولها بصورة غير منظمة قد يؤدي إلى المساس بكرامة الأشخاص وسمعتهم، وربما إلى إحداث أضرار أكبر من تلك الناتجة عن الجريمة الأصلية.

ولهذا فإن القاعدة الأساسية التي تحكم التعامل مع هذه البيانات تتمثل في **مبدأ تخصيص الاستعمال**، أي أن استعمالها يجب أن يكون مرتبطاً فقط بالهدف الذي تم من أجله الحصول عليها، وهو خدمة إجراءات البحث والتحقيق وإثبات الجرائم، ولا يجوز استخدامها لأي أغراض أخرى.

وقد جاء تدخل المشرع الجزائري في هذا المجال انسجاماً مع ضرورة حماية سرية الإجراءات الجزائية، حيث جعل استعمال المعطيات المحجوزة مقيداً بالإطار القانوني المحدد لها، بما يمنع تحولها إلى وسيلة للاطلاع غير المشروع أو النشر غير المبرر.[2]

1.اقتصار استعمال المعطيات المجرّمة على الجهات المختصة قانوناً

تعتبر قاعدة قصر الاطلاع على المعطيات ذات المحتوى المجرّم على الجهات المختصة من أهم الضمانات التي تحمي الخصوصية أثناء مرحلة ما بعد الحجز الإلكتروني، لأن مجرد ضبط هذه البيانات لا يمنح الحق في الاطلاع عليها لكل من له علاقة بإجراءات التحقيق.

فالأصل أن الوصول إلى هذه المعطيات يكون من اختصاص الجهات التي منحها القانون سلطة التعامل معها، وفي مقدمتها ضباط الشرطة القضائية المختصون، وقضاة التحقيق، والجهات القضائية المختصة بالفصل في القضية، إضافة إلى الخبراء الذين تتم الاستعانة بهم في حدود المهام التقنية المسندة إليهم[1].

[1] المادة 09 من القانون 09-04

ويستند هذا القيد إلى فكرة أساسية مفادها أن المعطيات الرقمية المحجوزة ليست ملكاً للجهة القائمة على الحجز، وإنما هي وسيلة إثبات وضعت تحت تصرف العدالة لتحقيق غاية محددة، وهي كشف الحقيقة بشأن الجريمة.

وعليه، فإن أي اطلاع من طرف أشخاص لا تتوافر فيهم الصفة القانونية أو دون وجود ضرورة إجرائية يعتبر خروجاً عن الغرض المشروع من الحجز، وقد يشكل اعتداءً على الحق في الخصوصية.

كما تبرز أهمية هذا القيد في حماية المستهلك الإلكتروني، إذ إن الأنظمة المعلوماتية التي يستعملها المستهلك قد تحتوي على معلومات شخصية ومالية حساسة، مثل بيانات الدفع الإلكتروني، سجل المشتريات، أو المراسلات الخاصة، وبالتالي فإن قصر الاطلاع عليها يمثل ضمانة لمنع استغلال هذه المعلومات خارج نطاق التحقيق.

2.منع نشر المعطيات ذات المحتوى المجرّم أو استخدامها خارج الغرض القضائي

إن الطابع الإجرامي للبيانات المحجوزة لا يؤدي إلى فقدانها للحماية القانونية، إذ تبقى هذه البيانات خاضعة لمبدأ السرية، ولا يجوز نشرها أو تداولها لمجرد كونها مرتبطة بجريمة.

فقد تحتوي الملفات الرقمية المحجوزة على معلومات تتعلق بأشخاص ضحايا أو شهود أو حتى أشخاص وردت أسماؤهم أو بياناتهم عرضاً أثناء البحث، وبالتالي فإن نشر هذه المعلومات قد يؤدي إلى المساس بحقوقهم الأساسية.

كما أن نشر المحتوى المجرّم قد يؤدي إلى نتائج عكسية، بحيث تتحول عملية مكافحة الجريمة إلى وسيلة لإعادة إنتاج الضرر، خصوصاً في الجرائم التي تمس الحياة الخاصة أو السمعة أو الاعتبار الشخصي.

ولهذا يجب أن يبقى استعمال هذه المعطيات محصوراً في الغرض القضائي، أي استخدامها كوسيلة لإثبات الجريمة أمام الجهات المختصة، دون السماح بتداولها إعلامياً أو اجتماعياً أو استعمالها لتحقيق أغراض شخصية[1].

[1] المادة 09 من القانون 09-04

ويكتسي هذا الأمر أهمية خاصة في مجال الجرائم الإلكترونية، لأن طبيعة الشبكات الرقمية تجعل انتشار المعلومات سريعاً وغير قابل للسيطرة الكاملة، مما يفرض تشديد القيود على تداول البيانات المحجوزة.

3.حماية المستهلك الإلكتروني من مخاطر تسريب البيانات المحجوزة

أصبح المستهلك الإلكتروني في البيئة الرقمية ينتج كماً كبيراً من البيانات أثناء استعماله للمنصات الإلكترونية، سواء تعلق الأمر بالتجارة الإلكترونية أو الخدمات البنكية أو التواصل الرقمي.

وقد تتضمن هذه البيانات معلومات شخصية ومالية يمكن أن تكشف عن جوانب دقيقة من حياته الخاصة، ولذلك فإن إخضاعها للحماية أثناء إجراءات الحجز يعد أمراً ضرورياً[1].

فإذا تم تداول هذه البيانات خارج الإطار القانوني، فقد يتعرض المستهلك لأضرار متعددة، مثل سرقة هويته الرقمية، أو استعمال معلوماته المالية بصورة غير مشروعة، أو المساس بسمعته الشخصية والمهنية.

ومن ثم، فإن تقييد تداول المعطيات ذات المحتوى المجرّم لا يمثل فقط ضمانة إجرائية في مجال التحقيق الجنائي، وإنما يعد أيضاً وسيلة لحماية الثقة في البيئة الرقمية وتشجيع الأفراد على استخدام الخدمات الإلكترونية بأمان.

ثانياً: التوازن بين متطلبات الإثبات الجنائي وحماية الخصوصية

تفرض الجرائم الإلكترونية الحديثة على السلطات القضائية الاعتماد بشكل متزايد على الأدلة الرقمية، باعتبار أن النشاط الإجرامي في البيئة الإلكترونية يترك آثاراً معلوماتية قد تكون الوسيلة الوحيدة لإثبات وقوع الجريمة أو تحديد مرتكبيها.

فأصبحت أجهزة الأمن أمام معادلة صعبة وهي تحقيق الأمن والكشف عن الج ا رئم وجمع أدلة ثبوتها وفي المقابل قد تعرض البيانات والمعلومات الشخصية للمجني عليه والجاني أحيانًا للمساس والتهديد والكشف عنها .فحماية خصوصية البيانات الشخصية يعد

[1] المادة 10 من القانون 09-04

من أكبر التحديات التي تواجه الدول في عصر التحول الرقمي والفضاء الإلكتروني وخصوصًا أن بعض الدول قد تسعى إلى خرق خصوصيات البيانات

الشخصية للأف ا رد بدعوى المحافظة على الأمن القومي للدولة، غير أن جمع هذه الأدلة والتعامل معها قد يؤدي إلى الاطلاع على بيانات شخصية لا ترتبط دائماً بالفعل الإجرامي، مما يثير إشكالية تحقيق التوازن بين ضرورة مكافحة الجريمة واحترام الحقوق الفردية[1].

ولهذا فإن حماية الخصوصية لا تعني منع استعمال الأدلة الرقمية، وإنما تعني إخضاع استعمالها لضوابط قانونية تضمن عدم تجاوز حدود الضرورة.

1.حماية مصلحة العدالة في الوصول إلى الحقيقة

لا يمكن إنكار الدور المهم الذي تلعبه المعطيات الرقمية في الكشف عن الجرائم الإلكترونية، إذ أصبحت العديد من الجرائم تعتمد على الوسائط التقنية، مما يجعل الدليل التقليدي غير كافٍ لإثباتها.

فالمعلومات المستخرجة من الأنظمة المعلوماتية قد تساعد في:

- تحديد هوية مرتكبي الجرائم .
- الكشف عن طرق ارتكاب الأفعال الإجرامية .
- إثبات العلاقة بين المتهم والجريمة .
- تتبع العمليات الإلكترونية المشبوهة .

ومن ثم فإن السماح باستعمال هذه البيانات في الحدود التي يقررها القانون يعد ضرورة لضمان فعالية العدالة الجنائية.

غير أن هذه الضرورة لا تعني إطلاق سلطة الجهات المكلفة بالتحقيق، وإنما يجب أن يبقى استعمال البيانات مرتبطاً بالهدف الإجرائي المحدد، وتحت رقابة الجهات القضائية المختصة.

[1] طارق جمعه السيد راشد ، **الحماية القانونية لخصوصية البيانات الشخصية في العصر الرقمي (دراسة مقارنة)**، مجلة القانون والاقتصاد –ملحق خاص العدد(الثاني والتسعون)، كلية الحقوق جامعة القاهرة، 2019 ، ص. 205

2.حماية حق الفرد في الخصوصية

في مقابل أهمية الدليل الإلكتروني، يبقى الحق في الخصوصية من الحقوق الأساسية التي يجب احترامها خلال جميع مراحل الإجراءات الجزائية.

فالبيانات التي يتم ضبطها أثناء الحجز قد تتضمن معلومات لا علاقة لها بالجريمة، وقد تخص أشخاصاً غير معنيين مباشرة بالتحقيق، ولذلك فإن التعامل معها يجب أن يتم بحذر شديد.

وتتحقق حماية الخصوصية من خلال مجموعة من الضمانات، أهمها:

- تحديد الأشخاص المخولين بالاطلاع على البيانات .
- منع نسخ أو نشر المعطيات دون ضرورة قانونية .
- قصر استعمال البيانات على أغراض التحقيق .
- المحافظة على سرية المعلومات المحجوزة .

وتساهم هذه الضمانات في منع تحول الحجز الإلكتروني إلى وسيلة لمراقبة الأفراد أو جمع معلومات شخصية لا ترتبط بالجريمة[1].

3.تكريس مبدأ التناسب بين متطلبات التحقيق وحقوق الأفراد

يعد مبدأ التناسب من المبادئ الأساسية التي تحكم الإجراءات الماسة بالخصوصية، ومقتضاه أن يكون التدخل في حقوق الأفراد بالقدر الضروري فقط لتحقيق الهدف المشروع.

فلا يجوز أن تمتد عملية الاطلاع أو استعمال المعطيات المحجوزة إلى معلومات تفوق ما تحتاجه إجراءات التحقيق، لأن ذلك يشكل تجاوزاً للغرض الذي شرع من أجله الإجراء.

وبالتالي، فإن استخدام المعطيات ذات المحتوى المجرّم يجب أن يخضع دائماً لمعادلة دقيقة تراعي:

- خطورة الجريمة المرتكبة .
- أهمية البيانات في إثباتها .

[1] فاطمة مرتيز ، **المراقبة الإلكترونية كإجراء استدلالي في مواجهة الحق في الخصوصية**، مجلة الحقيقة، العدد الثامن والثلاثون، جامعة أدرار، 2016 ، ص278

- مدى تأثير استعمالها على خصوصية الأشخاص .

ومن خلال هذا التوازن يمكن تحقيق فعالية العدالة الجنائية دون التضحية بالحريات الفردية.

يتضح أن تنظيم المشرع الجزائري للمعطيات ذات المحتوى المجرّم في المادة 8 من القانون 04-09يعكس حرصه على عدم إطلاق استعمال البيانات المحجوزة، وإنما إخضاعها لقيود تهدف إلى حماية الخصوصية وضمان احترام الحقوق الفردية.

فالدليل الإلكتروني، رغم أهميته في كشف الجرائم الحديثة، لا يمكن أن يكون مبرراً لانتهاك الحياة الخاصة أو نشر معلومات شخصية خارج الإطار القضائي، ولذلك فإن تقييد تداول هذه المعطيات يمثل ضمانة أساسية لتحقيق التوازن بين متطلبات الإثبات الجنائي من جهة، وحماية خصوصية المستهلك الإلكتروني وحقوقه الرقمية من جهة أخرى.

خلاصة

تناول الفصل الثاني مختلف الضمانات اللاحقة التي تهدف إلى تعزيز حماية الحق في الخصوصية للمستهلك بعد تنفيذ الإجراءات الإلكترونية، حيث تبين أن فعالية الحماية القانونية لا تتحقق فقط بالسماح باتخاذ إجراءات المراقبة والتحري، وإنما تتطلب أيضاً فرض رقابة صارمة على كيفية التعامل مع المعلومات والبيانات التي يتم الحصول عليها.

وقد تم التأكيد على أن البيانات الشخصية للمستهلك تمثل عنصراً جوهرياً في حياته الخاصة، الأمر الذي يستوجب حمايتها من أي استعمال غير مشروع أو إفشاء غير مبرر.

ولهذا اعتمد المشرع الجزائري مجموعة من المبادئ، أهمها مبدأ تخصيص المعلومات للغرض الذي جمعت من أجله، وعدم جواز استعمالها خارج الإطار القانوني المحدد.

كما أن الحماية الجزائية تشكل وسيلة أساسية لضمان احترام الخصوصية، من خلال معاقبة الأفعال التي تؤدي إلى كشف أو نشر أو استغلال المعلومات الشخصية بطرق غير مشروعة، فالمساس بالخصوصية في البيئة الرقمية قد يؤدي إلى أضرار خطيرة بالنظر إلى سرعة انتشار المعلومات وصعوبة السيطرة عليها بعد تداولها.

ورغم أهمية هذه الضمانات، فإن الدراسة كشفت وجود بعض النقائص، خاصة ما يتعلق بالحاجة إلى تعزيز الرقابة القضائية وتحديد بعض الإجراءات بصورة أكثر دقة، بما يضمن عدم توسع السلطات في استعمال الوسائل التقنية الحديثة على حساب الحريات الفردية.

الخاتمة

الخاتمة

أدى التطور المتسارع في مجال تكنولوجيات الإعلام والاتصال إلى تغيير طبيعة العلاقات بين الأفراد والمؤسسات، وأصبح العالم الرقمي فضاءً أساسياً لممارسة مختلف الأنشطة الاقتصادية والاجتماعية. وقد نتج عن هذا التحول ظهور تحديات قانونية جديدة تمس بصورة مباشرة الحقوق الأساسية للأفراد، وعلى رأسها الحق في الخصوصية وحماية البيانات الشخصية، خاصة بالنسبة للمستهلك الذي أصبح يتعامل يومياً مع المنصات الإلكترونية ويقدم العديد من المعلومات ذات الطابع الشخصي.

وقد حاول المشرع الجزائري مواجهة هذه التحديات من خلال وضع إطار قانوني خاص بمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، حيث جاء القانون رقم 04-09 بمجموعة من القواعد التي تنظم إجراءات البحث والتحري الإلكترونية، وتحدد شروط اللجوء إلى مراقبة الاتصالات الإلكترونية وتفتيش الأنظمة المعلوماتية.

وقد خلصت الدراسة إلى:

- أدرك المشرع الجزائري خطورة هذه الإجراءات على الحريات الفردية، لذلك لم يجعل استعمالها مطلقاً، بل ربطها بمجموعة من القيود، أهمها ضرورة وجود مبررات قانونية، وارتباط الإجراء بضرورات التحقيق، وصعوبة الوصول إلى الأدلة بالوسائل العادية، إضافة إلى اشتراط الرقابة القضائية.
- حماية خصوصية المستهلك الإلكتروني لا تتحقق فقط من خلال منع الاعتداء على البيانات الشخصية، وإنما تتطلب أيضاً تنظيم كيفية جمع هذه البيانات ومعالجتها والاحتفاظ بها. ولهذا فإن مبدأ تخصيص المعلومات وعدم استعمالها إلا للأغراض المحددة قانوناً يعد من أهم الضمانات التي تمنع الانحراف باستعمال السلطة.
- شكل القانون 04-09 خطوة إيجابية في مجال حماية الخصوصية الرقمية، باعتباره وفر إطاراً قانونياً يسمح بمواجهة الجرائم الإلكترونية مع المحافظة على الحقوق الأساسية للأفراد. كما أكد على ضرورة إخضاع الإجراءات التقنية الحديثة لضوابط قانونية تحول دون تحولها إلى وسائل للتدخل غير المشروع في الحياة الخاصة.

خاتمة

غير أن الدراسة كشفت في المقابل عن بعض النقائص، من أبرزها عدم كفاية بعض الأحكام المتعلقة بالتنظيم الدقيق لمدة بعض إجراءات المراقبة الإلكترونية، مما قد يثير مخاوف من استمرار هذه الإجراءات لفترات طويلة دون تحديد واضح للحدود الزمنية. كما أن التطور المستمر للتكنولوجيا يفرض ضرورة مراجعة النصوص القانونية بشكل دوري حتى تبقى مواكبة للمخاطر الرقمية الحديثة.

وبناءً على ذلك، يمكن تقديم مجموعة من الاقتراحات تتمثل أساساً في:

- ضرورة تعزيز الرقابة القضائية على إجراءات المراقبة الإلكترونية
- وضع ضوابط أكثر دقة بشأن مدة استعمال هذه الإجراءات وتجديدها.
- تطوير آليات حماية البيانات الشخصية للمستهلك الإلكتروني.
- بتدعيم الوعي القانوني لدى المستهلكين حول مخاطر مشاركة بياناتهم عبر الوسائط الرقمية
- تشجيع المؤسسات والجهات المعنية على اعتماد أنظمة تقنية أكثر أمناً لحماية المعلومات الشخصية، بما يحقق التوازن بين متطلبات الأمن الرقمي وضمان احترام الحقوق والحريات.

المصادر

والمراجع

المصادر والمراجع

الاوامر

1. **الامر** رقم 66-155 المؤرخ في 18 صفر عام 1386، الموافق 08 يونيو 1966 المتضمن قانون الاجراءات الجزائية المعدل والمتمم بالقانون رقم 25-14 مؤرخ في 9 صفر عام 1447 الموافق 3 غشت سنة 2025، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 54، الصادر في 13 شوال 1447 الموافق لـ 19 سبتمبر 2025.
2. الامر رقم66-156 مؤرخ في 8 يونيو 1966، ج ر ج ج، عدد يتضمن قانون العقوبات، المعدل والمتمم بالأمر رقم 20-01 المؤرخ في 30 جويلية 2020، المعدل والمتمم للأمر رقم 66-156 المؤرخ في 08 يونيو 1966، المتضمن قانون العقوبات الجزائري، ج ر.ج.ج العدد 44 صادر في 30/07/2020 المعدل والمتمم بالقانون رقم 24-06 مؤرخ في 19 شوال 1445 الموافق ل 2024/02/28 ج.ر عدد 30 الصادرة بتاريخ 2024/04/30

القوانين

1. القانون رقم 09- 04المؤرخ في 5أغسطس 2009المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها .الجريدة الرسمية للجمهورية الجزائرية، العدد 47

الكتب

1. أشرف توفيق شمس الدين ، الصحافة والحماية الجنائية للحياة الخاصة "دراسة مقارنة"، دار النهضة العربية،2007
2. أشرف عبد القادر قنديل ،**الإثبات الجنائي في الجريمة الإلكترونية**، دار الجامعة الجديدة، الاسكندرية، 2015
3. سليمان علي حمادي الحلبوسي، **المسؤولية المدنية الناشئة عن إفشاء السر المهني (دراسة قانونية)**، بيروت، لبنان
4. عبد الله أوهابية، **شرح قانون الإجراءات الجزائية، التحري والتحقيق**، ط2، دار هومة،2011
5. نصر الدين مروك، **محاضرات في الإثبات الجنائي، النظرية العامة للإنبات الجنائي**، ج 1، دار هومة، الجزائر، سنة 2003

المقالات

1. ثابت دنيازاد، **مراقبة الاتصالات الالكترونية والحق في حرمة الحياة الخاصة في القانون الجزائري**، مجلة العلوم الاجتماعية والإنسانية المجلد 05، العدد01، 2012
2. سعيد بن علي بن تركي الجلعود، **الدليل الرقمي وأثره في الإثبات دراسة فقهية تطبيقية مقارنة بالنظام السعودي**، مجلة العلوم الشرعية، جامعة القصيم، المجلد 17 ، العدد03 ، الجزء الأول، سنة2024
3. شيماء عبد الغنى عطاالله : تراجع الحق في الخصوصية في مواجهة الاتصالات الإلكترونية، بحث مقدم للمؤتمر العلمي الثاني لكلية القانون الكويتية العالمية" التحديات المستجدة للحق في الخصوصية"، في الفترة 16 – 15 فبراير 2012 ، طبعة منقحة2019
4. شيماء عبدالغني عطا الله ، تطور الحق في الحياة الخاصة وآثره على دستورية التجريم ومشروعية الدليل في الموا الجنائية، بحث منشور بمجلة روح القوانين، العدد 69 يناير 2015، كلية الحقوق جامعة طنطا، طبعة منقحة2019
5. طارق جمعه السيد راشد ، **الحماية القانونية لخصوصية البيانات الشخصية في العصر الرقمي (دراسة مقارنة)**، مجلة القانون والاقتصاد –ملحق خاص العدد(الثاني والتسعون) ، كلية الحقوق جامعة القاهرة،2019
6. العاقب عيسى، **حماية حق الانسان في صورته**، دراسات قانونية، دورية فصلية تصدر عن مركز البحوث والاستشارات والخدمات التعليمية ، الجزائر، جانفي2013
7. عيده بلعباد ، الدليل الرقمي بين حتمية الإثبات الجنائي والحق في الخصوصية المعلوماتية، مجلة أفاق علمية، المركز الجامعي لتامنغست الجزائر ، المجلد 11 العدد 1 السنة 2019
8. فاطمة مرتيز ، **المراقبة الإلكترونية كإجراء استدلالي في مواجهة الحق في الخصوصية**، مجلة الحقيقة، العدد الثامن والثلاثون، جامعة أدرار، 2016

الاطروحات

1. مراد بن عيسى، **حجية الدليل الرقمي في المادة الجزائية**، أطروحة دكتوراه، كلية الحقوق، جامعة الجزائر.

مذكرات الماجستير

1. طرشي نورة، **مكافحة الجريمة المعلوماتية**، مذكرة من أجل الحصول على شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر 1، 2011-2012
2. فوزي لواقي، **التحقيق في جرائم المخدرات على ضوء أساليب التحري الخاصة**، رسالة ماجيستير فرع القانون الجنائي، كلية الحقوق جامعة الجزائر 1، 2014/2015
3. ما ديو نصيرة، **افشاء السر المهني بين الاباحة والتجريم** ، مذكرة لنيل شهادة الماجستير في القانون، فرع : "قانون المسؤولية المهنية"، جامعة مولود معمري – تيزي وزو ، 2010
4. ميسون خلف الحمداني وآخر، **الدليل الرقمي وعلاقته بالمساس بالحق في الخصوصية المعلوماتية أثناء إثبات الجريمة**، جامعة النهرين كلية الحقوق، العراق، 2016

مذكرات الماستر

1. بولرباح نويجم ، مسؤولية الضبطية القضائية عن إفشاء السر المهنية مذكرة ضمن متطلبات نيل شهادة الماستر حقوق تخصص إدارة ومالية، جامعة زيان عاشور بالجلفة ، 2016-2017

الفهرس

مقدمة 1

الفصل الأول: الضمانات الإجرائية المقررة للمستهلك أثناء جمع المعلومات ومراقبة الاتصالات الإلكترونية

المبحث الأول: الضمانات القانونية للمستهلك في مراقبة الاتصالات الإلكترونية 7

المطلب الأول: تقييد اللجوء إلى المراقبة الإلكترونية بحالات محددة قانونًا 7

الفرع الأول: حصر حالات المراقبة الإلكترونية 9

الفرع الثاني: اشتراط صعوبة الوصول إلى الأدلة بالوسائل العادية 14

المطلب الثاني: الرقابة القضائية على إجراءات المراقبة الإلكترونية 16

الفرع الأول: اشتراط الإذن الكتابي المسبق من السلطة القضائية 17

الفرع الثاني: تحديد مدة المراقبة وإمكانية تجديدها وفق ضوابط قانونية 20

المبحث الثاني: الضمانات الإجرائية المتعلقة باستعمال المعلومات المتحصل عليها .. 25

المطلب الأول: ضمانات حماية المعطيات الشخصية أثناء المراقبة 25

الفرع الأول: تخصيص المعلومات المجمعة للأغراض المحددة قانونًا 26

الفرع الثاني: تجريم المساس بالحياة الخاصة الناتج عن إساءة استعمال المعلومات. 27

المطلب الثاني: تقييد استعمال المعلومات المتحصل عليها 29

الفرع الأول: حصر استعمال المعلومات في أغراض التحري والتحقيق 29

الفرع الثاني: حماية سرية المعلومات المتحصل عليها 30

الفصل الثاني: الضمانات الإجرائية المقررة للمستهلك أثناء التفتيش والحجز الإلكتروني

المبحث الأول: الضمانات المتعلقة بالتفتيش الإلكتروني 37

المطلب الأول: الرقابة القانونية على إجراءات التفتيش الإلكتروني 37

الفرع الأول: خضوع التفتيش للسلطة القضائية وضباط الشرطة القضائية المختصين 38

المطلب الثاني: ضمانات حماية الخصوصية أثناء التفتيش 42

الفرع الأول: تقييد الوصول إلى المعطيات الموجودة خارج الإقليم الوطني 43

الفرع الثاني: الاستعانة بالخبراء في حدود ما تقتضيه إجراءات البحث 45

المبحث الثاني: الضمانات المتعلقة بالحجز الإلكتروني وحفظ المعطيات 48

المطلب الأول: الضمانات المقررة أثناء حجز المعطيات المعلوماتية..... 49
الفرع الأول: الاقتصار على نسخ المعطيات الضرورية للتحقيق..... 49
الفرع الثاني: المحافظة على سلامة المعطيات وعدم المساس بمحتواها 51
المطلب الثاني: الضمانات المقررة لحماية المعطيات بعد الحجز 55
الفرع الأول: منع الوصول غير المشروع إلى المعطيات المحجوزة 56
خلاصة..... 64
الخاتمة..... 66

ملخص

تناولت هذه الدراسة موضوع الضمانات الإجرائية لحماية الحق في الخصوصية للمستهلك وفق القانون رقم 04-09، باعتباره من المواضيع الحديثة التي فرضتها التحولات الرقمية وانتشار المعاملات الإلكترونية. وقد تم التركيز على مدى قدرة التشريع الجزائري على حماية المستهلك من مخاطر المساس ببياناته الشخصية، خاصة في ظل اعتماد السلطات المختصة على إجراءات تقنية حديثة لمواجهة الجرائم الإلكترونية.

وقد توصلت الدراسة إلى أن المشرع الجزائري وضع مجموعة من الضمانات القانونية والإجرائية التي تهدف إلى تحقيق التوازن بين مكافحة الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال وبين حماية الحياة الخاصة للأفراد. إلا أن هذه الحماية تحتاج إلى مزيد من التطوير من خلال تعزيز الرقابة القضائية وتحديث القواعد القانونية بما يتلاءم مع التطور المستمر للبيئة الرقمية.

الكلمات المفتاحية: الخصوصية الرقمية – المستهلك الإلكتروني – الضمانات الإجرائية

Abstract

This study addresses the procedural safeguards for protecting the consumer's right to privacy under Law No. 04-09, a topic that has emerged in response to digital transformation and the proliferation of electronic transactions. The study focuses on the extent to which Algerian legislation can protect consumers from the risks of compromising their personal data, particularly given the reliance of competent authorities on modern technological procedures to combat cybercrime.

The study concludes that the Algerian legislator has established a set of legal and procedural safeguards aimed at achieving a balance between combating crimes related to information and communication technologies and protecting individuals' privacy. However, this protection requires further development through enhanced judicial oversight and the modernization of legal rules to keep pace with the continuous evolution of the digital environment.

Keywords: Digital Privacy – Electronic Consumer – Procedural Safeguards