جامـــعة عمار ثليجي الاغواط

كـلية الحــقوق والعــلوم السـياسية

قسم القانون العام

والموسومة بـــــ:

تأثير تكنولوجيا المعلومات على الأمن الجنائي

مذكـــــــرة تخرج ضمن مقتضيات نيل شهادة الماستر في القانون العام

تخصص: قانون جنائي وعلوم جنائية

إعداد الطالبتين:

جقيدل كوثر

غزال مريم

إشراف الدكتورة :

د.سويدي منال

أعضاء لجنة المناقشة:

د. غريبي يحي	رئيسا
د. سويدي منال	مشرفا ومقررا
د. بلي بلنوار	ممتحنا

السنة الجامعية: 2026/2025

كلمة شكر

الحمد لله الذي علّم الإنسان ما لم يعلم، نشكرُه ونحمدُه
على أنه أعاننا ويسر 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، ونخصُّ
بالذكر الأستاذة المشرفة **سويدي منال**، دون أن ننسى
فضل الدكاترة على ما قدموه لنا طيلة مشوارنا الجامعي

جقبدل كوثر- غزال مريم

مقدمة

مقدمة

شهد العالم خلال العقود الأخيرة تحولاً جذرياً بفعل التطور المتسارع في مجال تكنولوجيا المعلومات والاتصالات، حيث أصبحت الأنظمة الرقمية وشبكات الاتصال الحديثة من أهم الركائز التي تقوم عليها مختلف مجالات الحياة المعاصرة. فقد ساهمت هذه التكنولوجيا في تسهيل تداول المعلومات، وتسريع المعاملات، وتحسين أداء المؤسسات العامة والخاصة، مما جعلها عاملاً أساسياً في تحقيق التنمية الاقتصادية والاجتماعية والإدارية. غير أن هذا التطور لم يقتصر أثره على الجوانب الإيجابية فقط، بل أفرز في المقابل مجموعة من المخاطر والتهديدات الجديدة التي اتخذت طابعاً إلكترونياً، الأمر الذي فرض تحديات غير مسبوقة أمام الأنظمة القانونية والأمنية التقليدية.

لقد أدى الانتقال من البيئة المادية التقليدية إلى البيئة الرقمية إلى تغير طبيعة الجريمة ووسائل ارتكابها، فلم تعد الأفعال الإجرامية مرتبطة بالزمان والمكان أو بالوسائل التقليدية، وإنما أصبحت ترتكب باستخدام الحواسيب والشبكات المعلوماتية والبرمجيات المتطورة. وظهرت بذلك أنماط جديدة من الجرائم، مثل اختراق الأنظمة المعلوماتية، والتلاعب بالبيانات، وسرقة المعلومات، والتجسس الإلكتروني، والاعتداء على الخصوصية الرقمية، وهي جرائم تتميز بخصوصيتها التقنية وصعوبة اكتشافها وإثباتها مقارنة بالجرائم التقليدية. وقد أدى هذا التحول إلى إعادة النظر في مفهوم الأمن الجنائي، الذي لم يعد يقتصر على حماية الأشخاص والممتلكات بالوسائل التقليدية، وإنما أصبح يشمل حماية الأنظمة الرقمية والبيانات والمعلومات باعتبارها من أهم عناصر القوة في العصر الحديث.

ويُعد الأمن الجنائي من المجالات التي تأثرت بشكل مباشر بالتطور التكنولوجي، سواء من حيث طبيعة الجرائم المرتكبة أو من حيث وسائل مكافحتها. فمن جهة، ساهمت تكنولوجيا المعلومات في تطوير أساليب إجرامية أكثر تعقيداً وخطورة، حيث أصبح بإمكان الجاني ارتكاب أفعال تمس مصالح الأفراد والمؤسسات والدول دون الحاجة إلى وجود مادي في مكان الجريمة. ومن جهة أخرى، وفرت التكنولوجيا وسائل حديثة لتعزيز العمل الأمني والقضائي، من خلال استخدام قواعد البيانات الإلكترونية، وتقنيات التحليل الرقمي، وأنظمة المراقبة الذكية، وأساليب التحقيق الجنائي الإلكتروني.

وفي هذا السياق أصبح من الضروري دراسة تأثير تكنولوجيا المعلومات على الأمن الجنائي باعتباره موضوعاً يجمع بين البعد القانوني والتقني والأمني، خاصة في ظل الحاجة إلى تحقيق التوازن بين الاستفادة من التطورات التكنولوجية وضمان حماية المجتمع من المخاطر الناتجة عنها. وقد أدرك المشرع الجزائري أهمية هذا التحول، حيث عمل على تطوير المنظومة القانونية لمواجهة الجرائم المرتبطة بالبيئة الرقمية، سواء من خلال إدراج نصوص خاصة ضمن قانون العقوبات تتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات، أو من خلال سن قوانين خاصة تهدف إلى حماية المعطيات ذات الطابع الشخصي والوثائق الإلكترونية. كما تم تجريم العديد من الأفعال المرتبطة بالدخول غير المشروع إلى الأنظمة المعلوماتية والتلاعب بالبيانات والتعامل غير المشروع في المعطيات الرقمية.

وتبرز أهمية دراسة هذا الموضوع من خلال عدة اعتبارات، أهمها أن الجرائم المعلوماتية أصبحت تمثل تحدياً حقيقياً للأمن الجنائي بسبب طبيعتها العابرة للحدود وصعوبة تحديد مرتكبيها، إضافة إلى تعقيد وسائل إثباتها واعتمادها على أدلة رقمية تحتاج إلى تقنيات خاصة في جمعها وتحليلها. كما تكتسي الدراسة أهمية عملية بالنظر إلى حاجة الأجهزة الأمنية والقضائية إلى تطوير آليات المواجهة القانونية والتقنية لهذه الجرائم، بما يضمن حماية الحقوق والحريات من جهة، وتحقيق فعالية السياسة الجنائية من جهة أخرى.

أما أهداف الدراسة فتتمثل في بيان مفهوم تكنولوجيا المعلومات وارتباطها بالأمن الجنائي، وتحديد مختلف الآثار التي أحدثتها التكنولوجيا على طبيعة الجرائم وأساليب ارتكابها، إضافة إلى تحليل مدى فعالية القواعد القانونية في مواجهة الجرائم المعلوماتية. كما تهدف الدراسة إلى إبراز دور الوسائل التقنية الحديثة في تطوير العمل الأمني والقضائي، والكشف عن أهم الصعوبات التي تواجه سلطات البحث والتحقيق في مجال الجرائم الإلكترونية، مع تقديم مقترحات تهدف إلى تعزيز الحماية الجنائية في البيئة الرقمية.

ويرجع اختيار موضوع الدراسة إلى مجموعة من الأسباب العلمية والعملية، فمن الناحية العلمية يرتبط الاختيار بالأهمية المتزايدة للجرائم الإلكترونية باعتبارها من أبرز الظواهر الإجرامية الحديثة التي تحتاج إلى دراسة قانونية معمقة. أما من الناحية العملية، فيعود سبب الاختيار إلى الانتشار الواسع لاستخدام التكنولوجيا الرقمية وما صاحبه من ظهور اعتداءات إلكترونية تمس أمن الأفراد والمؤسسات والدول، الأمر الذي يجعل البحث في آليات مواجهتها أمراً ضرورياً.

غير أن دراسة هذا الموضوع لا تخلو من صعوبات، أهمها الطبيعة التقنية للجرائم المعلوماتية التي تتطلب الإلمام بجوانب قانونية وتقنية متداخلة، إضافة إلى التطور السريع في مجال التكنولوجيا الذي يجعل النصوص القانونية تواجه صعوبة في مواكبة المستجدات المتلاحقة. كما تبرز صعوبة أخرى تتمثل في محدودية الإحصائيات الدقيقة المتعلقة بحجم الجرائم الإلكترونية، فضلاً عن تعقيد الوصول إلى الأدلة الرقمية والمحافظة على حجيتها القانونية.

وانطلاقاً من أهمية الموضوع والإشكالات المرتبطة به، يمكن طرح الإشكالية الرئيسية التالية:

كيف أثرت تكنولوجيا المعلومات على الأمن الجنائي موضوعيا واجرائيات ومؤسساتيا؟

وللإجابة عن هذه الإشكالية، تم الاعتماد على المنهج الوصفي من خلال وصف ظاهرة الجرائم المعلوماتية وبيان خصائصها ومظاهر تأثير التكنولوجيا على الأمن الجنائي، كما تم الاعتماد على المنهج التحليلي من خلال تحليل النصوص القانونية المنظمة للجرائم الإلكترونية ومدى فعاليتها في توفير الحماية الجنائية اللازمة.

ولتحديد جوانب الدراسة، تم تقسيم الموضوع إلى فصلين أساسيين، حيث تناول الفصل الأول **أثر تكنولوجيا المعلومات في الجانب الموضوعي على الأمن الجنائي**، وتم تقسيمه إلى مبحثين؛ خصص المبحث الأول لدراسة تأثير التكنولوجيا في ظهور الجرائم المعلوماتية وصورها المختلفة، بينما تناول

المبحث الثاني الجرائم المرتبطة بتكنولوجيا المعلومات في القوانين الخاصة، لاسيما الجرائم المتعلقة بالمعطيات الشخصية والوثائق الإلكترونية.

أما الفصل الثاني فقد خصص لدراسة **أثر تكنولوجيا المعلومات في الجانب الإجرائي على الأمن الجنائي،** من خلال تحليل تأثير التكنولوجيا على إجراءات البحث والتحري والتحقيق، ودور الأدلة الرقمية والوسائل التقنية الحديثة في إثبات الجرائم الإلكترونية، مع بيان أهم التحديات التي تواجه الجهات المختصة في هذا المجال.

وبذلك تسعى هذه الدراسة إلى تقديم رؤية شاملة حول التحولات التي أحدثتها تكنولوجيا المعلومات في مجال الأمن الجنائي، وإبراز ضرورة تطوير المنظومة القانونية والمؤسساتية بما يتلاءم مع طبيعة المخاطر الرقمية الجديدة.

الفصل الأول:

اثر تكنولوجيا المعلومات في الجانب الموضوعي على الأمن الجنائي

الفصل الاول: اثر تكنولوجيا المعلومات في الجانب الموضوعي على الأمن الجنائي

أحدثت تكنولوجيا المعلومات والاتصال تحولات عميقة في مختلف مناحي الحياة، إذ أصبحت الأنظمة الرقمية والشبكات المعلوماتية ركيزة أساسية في النشاط الاقتصادي والإداري والاجتماعي. وقد ترتب عن هذا التطور المتسارع ظهور بيئة رقمية جديدة أفرزت أنماطاً مستحدثة من السلوك الإجرامي، تجاوزت في خصائصها وأدواتها الجرائم التقليدية المعروفة، الأمر الذي فرض تحديات غير مسبوقة على منظومة الأمن الجنائي.

فمع اتساع استخدام الوسائط الإلكترونية وتزايد الاعتماد على نظم المعلومات، باتت الجرائم المرتبطة بتكنولوجيا المعلومات تشكل تهديداً حقيقياً للأفراد والمؤسسات والدول، نظراً لما تتسم به من سرعة الانتشار، وصعوبة اكتشاف مرتكبيها، وإمكانية ارتكابها عبر الحدود الجغرافية. وقد استدعى ذلك تدخل المشرع الجزائري من خلال تحديث المنظومة القانونية الجنائية، سواء عبر تعديل أحكام قانون العقوبات أو من خلال استحداث نصوص خاصة تهدف إلى توفير الحماية القانونية للمعطيات والأنظمة والوثائق الإلكترونية.

ويهدف هذا الفصل إلى دراسة أثر تكنولوجيا المعلومات على الجانب الأمني الجنائي من خلال التطرق إلى مختلف صور الجرائم المعلوماتية التي تناولها المشرع الجزائري، سواء تلك التي تمثل امتداداً للجرائم التقليدية باستخدام الوسائط الرقمية، أو الجرائم المستحدثة التي تستهدف الأنظمة المعلوماتية والمعطيات الإلكترونية، وذلك من خلال تقسيم هذا الفصل إلى مبحثين؛ يتناول الأول صور جرائم تكنولوجيا المعلومات في قانون العقوبات، بينما يعالج الثاني صور هذه الجرائم في القوانين الخاصة.

المبحث الاول: صور جرائم تكنولوجيا المعلومات في قانون العقوبات

أمام التطور المتسارع لوسائل تكنولوجيا المعلومات والاتصال، لم يعد قانون العقوبات يقتصر على مواجهة الأفعال الإجرامية التقليدية في صورتها المادية المعتادة، بل أصبح مطالباً بمواكبة التحولات الرقمية التي أفرزت أنماطاً جديدة من الجرائم أو منحت الجرائم التقليدية وسائل أكثر تطوراً وخطورة.

وقد اتجه المشرع الجزائري إلى إدراج العديد من الأحكام المتعلقة بالجرائم المعلوماتية ضمن قانون العقوبات، مستهدفاً بذلك تحقيق الحماية الجنائية للمصالح والأشخاص والأنظمة المعلوماتية من الاعتداءات الإلكترونية المتزايدة. وتجسد هذا التوجه من خلال تجريم بعض الأفعال التي تستخدم تكنولوجيا المعلومات كوسيلة لارتكاب الجريمة، إلى جانب تجريم الأفعال التي تستهدف الأنظمة المعلوماتية ذاتها باعتبارها محلاً للحماية الجنائية.

ويتناول هذا المبحث صور جرائم تكنولوجيا المعلومات الواردة في قانون العقوبات، وذلك من خلال دراسة الجرائم التقليدية المرتكبة بواسطة تكنولوجيا المعلومات، مع التركيز على جريمة القذف الإلكتروني، ثم التطرق إلى الجرائم الواقعة على نظم المعلومات بمختلف صورها.

المطلب الاول: الجرائم التقليدية الواقعة بواسطة تكنولوجيا المعلومات (القذف الإلكتروني نموذجا)

إن جريمة القذف تعد من الجرائم التقليدية المنصوص عليها في اغلب المدونات العقابية أصبحت في الوقت الحالي ومع التطور الكبير في تكنولوجيا المعلومات ووسائل الاتصال تتم بواسطة وسائل مستحدثة منها شبكة الانترنت، حيث عرفها الدكتور حسنين إبراهيم صالح عبيد، هو " إسناد علني عمدي لواقعة محددة تستوجب عقاب أو احتقار من أسندت إليه":وعلى ذلك فان جريمة القذف عن طريق الانترنت هي جريمة يلازم وصفها طبيعة فعل النشر وهي تبدأ وتنتهي بارتكاب هذا الفعل ومن ثم فهي جريمة وقتية. [1]

الفرع الأول: تعريف جريمة القذف على شبكة الانترنت

ظهرت العلاقة بين الانترنت والقانون الجنائي ،عندما ثارت مشكلة تحديد الطبيعة القانونية لجريمة القذف المرتكب عن طريق الانترنت أمام المحاكم الفرنسية بمناسبة قضية اتهم فيها متهم بنشر تعليق يتضمن قذفا في حق شخصية سياسية . وتم تداوله عبر شبكة الانترنت وعند محاكمته دفع بانقضاء الدعوى الجنائية بالتقادم تأسيسا على أن جريمة القذف بطريق الانترنت هي من جرائم النشر التي تنقضي فيها الدعوى بمضي ثلاثة أشهر من تاريخ ارتكاب الجريمة.[2]

و يتجسد الركن المادي لجريمة القذف في اجتماع عدة عناصر وهي:

---

[1] عياط سارة، **جريمة القذف على شبكة الانترنت**، مذكرة مكملة من مقتضيات نيل شهادة الماستر حقوق تخصص القانون الجنائي،جامعة محمد خيضر– بسكرة، الجزائر، 2014/2013،، ص 26

[2] مصطفى محمد موسى،**التحقيق الجنائي في الجرائم الالكترونية** ،الطبعة الأولى، مصر ، 2009،ص 428

أولا – الادعاء بواقعة معينة وإسنادها:

الادعاء: يحمل الادعاء معنى الرواية عن الغير أو ذكر الخبر محتملا الصدق أو الكذب[1].

ومثال ذلك: أن يقال بأن فلان سرق مال المؤسسة فهذا التعبير يكتنف معنى الرواية[2]

الاسناد: يفيد نسبة الامر إلى شخص المقذوف على سبيل التأكيد سواء كانت الوقائع المدعى بها صحيحة أو كاذب، والقذف بالاسناد لا يتحقق بصفة مباشرة فقط إنما يتحقق بكل صور التعبير ولو كان بصفة تشكيكية أو استفهامية أو غامضة[3]، ويكون الاسناد أو الادعاء بأي وسيلة من وسائل التعبير سواء شفاهة أو كتابة أو حتى بالاشارة، كما يتحقق سواء كان سبيل القطع أو الشك بشرط أن يكون لدى العامة من الناس عقيدة بصحة الادعاء أو الاسناد[4].

يستنتج القذف من كل عبارة تتضمن نسبة أمر شائن إلى شخص أو هيئة معينة حتى ولو كانت فحوى العبارات مجازية إذ يمكن اعتبارها قذفا حتى ثبت أن نية القذف اتجهت إلى الحط من الكرامة، بشرط أن يكون الامر المسند إلى المقذوف معينا، محددا يمكن إقامة الدليل عليه بإثباته[5].

وفيما يخص هذا العنصر أنّ المشرع الجزائري يعاقب على الإسناد أو الإدعاء إذا كانت العبارات توحي بأن المتهم يريد بها إسناد واقعة مشينة إلى الشخص المقذوف لذلك لا نعتد بالصيغة أو الأسلوب القولي، فالسلطة التقديرية ترجع لقاضي الموضوع في استنباط العبارات التي تمس بالشرف والاعتبار[6]وهكذا قضى بأن :"الإدعاء أمام بعض الفلاحين بأن الوثائق المحررة من قبل هذا الموثق لا تكتسي أي حجية قانونية ولا قيمة لها من الناحية القانونية وهو الأمر الذي جعلهم يسحبون وثائقهم من ذلك الموثق والتقدم إلى موثق ثاني دلهم عليه المتهم يشكل مساسا بالشرف والاعتبار" قرار في2000/11/07، رقم129058 عن غ ج م ق2 وعليه فان الإدعاء والإسناد الماس بالشرف والاعتبار من عدمه هو مسألة موضوعية ولقاضي الموضوع السلطة التقديرية في ذلك[7].

---

(1) سليمان نعيمة، **المسؤولية الجزائية في جرائم الصحافة المكتوبة**، مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، المدرسة العليا للقضاء، الجزائر،2007–2010،ص.04

(2) كمال بوشليق، **جريمة القذف بين القانون والإعلام(دراسة تحليلية مقارنة مدعمة باجتهاد القضائي للرجال القضاء الإعلام على ضوء قانون العقوبات والإعلام)** ، دون طبعة، دار الهدى للطباعة والنشر والتوزيع، الجزائر، 2010، ص13

(3) أحسن بوسقيعة، **الوجيز في القانون الجزائي الخاص، الجزء الأول، الجرائم ضد الأشخاص ووالجرائم ضد الأموال،** الطبعة الثالثة، دار هومة، الجزائر، 2006، ص190

(4) عياط سارة، المرجع السابق، ص15

(5) علي أحمد رشيدة، **الحق في الإعلام وجنح الصحافة**، بحث لنيل درجة الماجستير في القانون الدولي لحقوق الإنسان كلية الحقوق، جامعة مولود معمري، تيزي وزو، الجزائر،2001–2002، ص 97

(6) كمال بوشليق، المرجع السابق، ص.14

(7) طاهري حسين، **الإعلام والقانون(دراسة مقارنة)**، دون طبعة، دار الهدى للنشر والطباعة، الجزائر،2014، ص 105

1.تعيين الواقعة: يجب أن يصب الإدعاء أو الإسناد على واقعة معينة ومحددة وبهذا الشرط يتميز القذف عن السب لأنه إذا كان خاليا من واقعة معينة فإنه يكون سبا لا قذفا.[1]

لذلك هناك من عرفها أنها حادث إجابي أو سلبي أو مادي أو أدبي يترتب عليه المساس بالشرف والاعتبار.[2]

فإذا كان الإسناد خاليا من واقعة معينة فإنه يكون سبا لا قذفا ومثال ذلك أن يسند الفاعل إلى المجني عليه على أنه سارق أو نصاب أو مرتشي.[3]

لذا لا يشترط في تعيين الواقعة المحددة أن يكون تعيينا حاسما من حيث زمانها ومكانها، فهو أمر متروك لقاضي الموضوع إذ يستوي أن تكون الواقعة المسندة إيجابية كالسرقة أو سلبية كعدم سداد الدين[4].

2.أن يكون من طبيعة تلك الواقعة المساس بالشرف والاعتبار: إن القانون لم يفرق بين الواقعة الماسة بالشرف والواقعة الماسة بالاعتبار وهذا ما هو وارد في نص المادة 696 من قانون العقوبات الجزائري إلا أنه لكل منهما معنى مستقل، فالشرف لا نقصد به قيمة الإنسان في نظر الغير إنما قيمته في تصوره هو كشخص مرتاح الضمير لذا فالفعل الماس بالشرف يعني الفعل المخالف للنزاهة، أما الاعتبار فنقصد به الصورة التي يريد أن يكون عليها الإنسان في نظر غيره وما يمس الاعتبار هو كل ما يمس الإنسان في نظر الغير.[5]

ومسألة الشرف والاعتبار يرجع تقديرها إلى قاضي الموضوع تبعا للظروف المحيطة بالواقعة المسندة مع وجود الاسترشاد بالدلالة العرفية للمتهم وفي هذا السياق قضي أن المساس بالشرف اولاعتبار مسألة موضوعية يرجع تقدي رها لقضاة الموضوع.[6]

وخلاصة لما سبق فإن القانون يراعي أساسا القيم الأخلاقية التي يعتدى عليها وذلك بإدعاء وإسناد وقائع شائنة فيها مساس بالشرف والاعتبار لكن لا يجب التمادي لكي لا نصطدم مع حق معترف به دستوريا وهو حق الشخص في حرية التعبير.[7]

---

(1) عبد الرحيم ريمة ، **جرائم الصحافة**، مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء الجزائر،2007-2010، ص 06

(2) عياط سارة، المرجع السابق، ص.16

(3) أحسن بوسقيعة، المرجع السابق، ص.19

(4) بوريش فواد، **حرية التعبير وجرائم الصحافة**، مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر،2006-2009، ص 33

(5) سليمان نعيمة، المرجع السابق، ص ص 4-5

(6) كمال بوشليق، المرجع السابق، ص.17

(7) المرجع نفسه، ص.18

3.أن تكون الواقعة مسندة لشخص محدد أو لهيئة معينة: يشترط في جريمة القذف تعيين الأشخاص سواء أكانت طبيعية أو معنوية، ولا يستوجب تحديد المجني عليه بذكر اسمه، إنما يكفي أن يكون القذف موجها على صورة يسهل الشخص أو الهيئة محل القذف.[1]

و في هذا السياق ورد بأنه ما دام المتهم أشار في المنشور الذي نشره في صحيفة" لوماتان" إلى مدير مركب أسمدال فإنه بذلك يكون قد قصد الطرف المدني(ل،م) وهو مدير المركب إذ من الممكن تحديده من خلال الإشارة إلى صفته كمدير المركب[2]، إذ يشترط أن يكون المقذوف محدد بغض النظر عن ذكر الاسم بل يكفي أن يفهم من المقال هوية هذا الشخص الموجه إليه أو الهيئة المعنية بالأمر وهذا ما ذهبت إليه المحكمة العليا في إحدى قرارتها ونصت على مبدأ عام فحواه(يعد القذف كل ادعاء بواقعه من شأنها المساس بشرف واعتبار الأشخاص أو إسنادها إليهم ويعاقب على نشر هذا الإدعاء وذلك الإسناد حتى ولو تم ذلك على وجه التشكيك أو إذا قصد به شخص دون ذكر الاسم،لكن كان من الممكن تحديده من عبارات الكتابة موضوع الجريمة.

و المقذوف قد يكون شخصا أو هيئة:

4.الشخص :نقصد به الشخص الطبيعي أو المعنوي، أما يخص الجماعات التي لا تتمتع بالشخصية المعنوية مثل نقابة الأطباء فلا تقوم الجريمة إذا كانت العبارات موجهة ضد المهنة ككل، وبالمقابل يجوز قيام المسوولية المدنية للقاذف اتجاه تلك الجماعة[3]

5.الهيئات النظامية :هي التي تتمتع بوجود شرعي دائم ولقد خولها الدستور قسطا من السلطة والإدارة العمومية ولها الحق في أن تجتمع في جمعية عامة للتداول كالبرلمان مجلس الأمة المجلس الشعبي الوطني مجلس الوزراء مجلس الحكومة المجالس الولائية والبلدية المجلس الأعلى للقضاء المحكمة العليا....إلخ.

-الجيش الوطني الشعبي.

-المجالس والمحاكم القضائية.

5.الهيئات العمومية الأخرى: كالوزارات ومديرية الأمن الوطني، والمديرية العامة للجمارك والمديرية العامة للحماية المدنية، وكل المؤسسات العمومية ذات الطابع الإداري كالجامعات والمعاهد.... إلخ، علاوة على المجالس العليا مثل المجلس الإسلامي الأعلى والمحافظة السامية للأمازغية والمجلس الأعلى للغة العربية والمجلس الوطني الاقتصادي والاجتماعي.

-روساء الدول، رو ساء البعثات الدولية وأعضائها المعتمدين.

---

(1) بوريش فواد،، **حرية التعبير وجرائم الصحافة**، مذكرة لنيل إجازة المدرسة العليا للقضاء الجزائري،الجزائر، 2006-2009، ص.33.

(2) أحسن بوسقيعة، المرجع السابق، ص. 193

(3) عياط سارة، المرجع السابق، ص.19.

-الرسول" ص" وباقي الأنبياء.

-شعائر الدين الإسلامي .[1]

ثانيا: عنصر العلانية

العلانية هي كل ما يقع تحت نظر الكافة أو يصل إلى سمعهم أو يمكنهم أن يقفوا عليه بمشيئتهم دون عائق [2] وتقوم العلانية على عنصرين هما:

-**العنصر المادي:** ونقصد به السلوك المنتج لحدث نفسي من شأنه إيصال الفكرة أو الشعور أو الإرادة الآثمة للجمهور.

1.العنصر المعنوي : تعتمد إيصال الفكرة أو الشعور أو الإرادة إلى الغير قصد الإذاعة[3]

2.طرق العلانية: إن المشرع الجزائري لم يكن دقيقا في تحديد طرق العلانية والمادة 696 نصت على ذكر النشر وإعادة النشر دون تحديد وسائل النشر وذلك في القانون العقوبات الجزائري، ليستدرك هذا الفراغ بطريقة غير مباشرة حين أشارت نفس المادة إلى الحديث الصياح، التهديد، الكتابة المنشورات، اللافتات والإعلانات ك وسائل لنشر الإدعاء أو إعادة نشره[4]

و عموما تتم العلانية[5] بإحدى الطرق التالية : القول، الكتابة، الصور.

1.القول: وقد يكون:

أ /**الجهر بالقول أو الصياح في محل عمومي** : معنى القول كل ما ينطق به ولو بعبارات مقتضبة أما الصياح كل صوت ولو لم يكن يعبر عن ألفاظ واضحة [6]إذ تتوفر العلانية في هذه الحالة بالجهر بالقول أو الصياح في مكان عمومي بطبيعته كالشوارع والساحات العمومية ولو كان المحل خاليا من الناس، أو في مكان عمومي بالتخصيص أو بالمصادفة كقاعة الجلسات إذا توفر الجمهور والأماكن العمومية بالمصادفة هي التي تكتسب الصفة العامة نتيجة وجود عدد من الأفراد كالمنازل، المحلات التجارية [7]أما الاجتماع فمعناه كل محفل احتشد فيه عدد كبير من الناس لم يدعوا إليه بصفة خاصة ولا حرج على أي

---

[1] سليمان نعيمة، المرجع السابق ،ص ص05-06.

[2] كمال بوشليق، المرجع السابق، ص. 22

[3] نبيل صقر، المرجع السابق، ص105

[4] سليمان نعيمة . المرجع السابق، ص06

[5] المشرع الجزائري لم يذكر العلانية إلا في المادة 296 ق ع كونه اقتبس أحكام القذف من قانون الإعلام الفرنسي المؤرخ في1881/07/29 وأغفل نقل ما نصت عليه المادة 72 منه من طرق العلانية وانتقل مباشرة إلى نقل محتوى المادة 29 التي تقابل نص المادة 296 من قانون العقوبات كالجزائري، بن عيسى كهينة، برانسي سليمة، **جريمة القذف بين قانون وقانون الاعلام**، مذكرة تخرج لنيل شهادة الماستر في الحقوق، تخصص القانون الخاص والعلوم الجنائية، جامعة عبد الرحمان ميرة – بجاية- 2014-2015، ص19

[6] أحسن بوسقيعة، المرجع السابق، ص197

[7] كمال بوشليق، المرجع السابق، ص.23

إنسان من الاشتراك فيه وذلك بغض النظر عن صفة المكان الذي احتشد فيه الجميع ومثال ذلك مراسم الأفراح[1] والقانون لا يشترط حضور المجني عليه وقت القذف إنما يعتد بالأذى الناتج جراء سماع عامة الناس عنه ما يشينه في شرفه واعتباره.[2]

ب /الجهر بالقول والصياح في محل خاص : تتحقق العلانية بالجهر بالقول أو الصياح في هذه الحالة إذا كان من يستطيع سماعه كان في مكان عام [3]فألفاظ القذف التي صدرت من المتهم

وهو داخل المنزل فهي علانية إن أمكن سماعها من طرف المارون في الشارع والعلانية القائمة في هذه الصورة هي احتمال سماع الجمهور لعبارات القذف لذلك لا يشترط السماع الفعلي بل تتوفر العلانية ولو كان المكان العمومي خاليا من الناس [4]

ج /إذاعة القول أو الصياح به بآلية لبث الصوت : يرتكب الجريمة من يوجه عبارات القذف بواسطة جهاز إرسال لاسلكي ويعتبر مكان الجريمة في هذه الحالة محطة الإذاعة أو مكان الإرسال ومن ثمة فإن الإذاعة اللاسلكية تحقق العلانية بالنسبة للكلام أما التلفاز تحقق العلانية بالنسبة للصورة[5]، يسقط طابع العلانية بالنسبة للهاتف النقال والثابت نظرا للطابع السري الذي يكتنفه وهذا ما يعكس كثرة الاعتداءات عل شرف واعتبار الأشخاص.

د-الكتابة : نصت المادة296 العقوبات الجزائري على الكتابة والمنشورت واللافتات والإعلانات، وعليه تتحقق العلانية في حالة التوزيع أو العرض في طريق عام أو مكان عمومي أو إذا بيعت أو عرضت للبيع في أي مكان[6]

2.التوزيع : يتحقق بتوزيع المطبوعات أو المكاتب أو اللافتات إلى عدد من الأفراد بدون تميز فالقضاء الشفوي بفحوي الورقة لعدد من الناس لا يحقق التوزيع والقانون لا يشترط أن يكون التوزيع قد بلغ عدد محددا فيكفي أن يكون المكتوب قد وصل إلى عدد من الناس سواء نسخة أو عدة نسخ[7]

3.التعريض للأنظار : يستوجب وضع الكتابة أو الرسوم أو المطبوعات أو اللافتات في مكان ظاهر فينتفي العرض إذا كانت الكتابة داخل ظرف ولو كان موضوعا في الطريق العام، فيتوفر العرض ولو

---

[1] أحسن بوسقيعة، المرجع السابق، ص198

[2] كمال بوشليق، المرجع السابق، ص.25

[3] بن عيسى كهينة، برانسي سليمة، المرجع السابق، ص 19

[4] عبد الحميد المنشاوي، المرجع السابق،ص19

[5] محمد صبحي نجم، **شرح قانون العقوبات الجزائري " القسم الخاص"** ، بدون طبعة، ديوان المطبوعات الجامعية، الجزائر،2006، ص102

[6] بن عيسى كهينة، برانسي سليمة، المرجع السابق، ص 18

[7] أحسن بوسقيعة، المرجع السابق، ص199

حصل في مكان خاص إذا كانت الكتابة أو الرسم قد عرضت بحيث ترى من المحل العام وكان ذلك قصد الفاعل فلا يشترط أن يكون العرض في مكان عام. [1]

4.البيع أو العرض للبيع: وهو ما اصطلح عليه المشرع الجزائري بالنشر وإعادة النشر وتنطبق هذه الحالة على الكتب، المجلات الجرائد، النشرات، البحوث، الرسوم، الصور.[2]

تتوفر العلانية بشرط إن يكون القصد هو النشر سواء كان المبيع نسخة واحدة أو المشتري كان واحدا واشترى عدة نسخ، أما العرض للبيع فهو طرح الكتابة أو الرسوم للشراء والإعلان عنها بالبيع أو العرض ولو كان ذلك في مكان خاص، كون العلانية لا تستفاد صفة المكان اونما من عملية البيع ذاتها كونها الوسيلة الرئيسية لتداول الكتابة والمطبوعات ونشرها .[3]

5.الصور :إن نشر الصور واعادة نشرها يحقق العلانية ومفهوم الصور واسع إذ يشمل خصوصا الرسوم والكاريكاتور بكافة أنواعه والأفلام السينمائية وكل التركيبات السمعية البصرية[4]

الفرع الثاني :مدى تحقق ركن العلانية عبر الانترنت في التشريع الجزائري

نص المشروع الجزائري على المقصود بجرائم القذف والسب في المادتين296 و 297من قانون العقوبات [5]ولم يحدد المشرع الجزائري هاتين المادتين بدقة ووضوح طرق علانية إذا اكتفت المادة 269 المتعلقة بالقذف، في بداية الأمر بذكر النشر وإعادة النشر دون بيان سندات النشر، وجاء الشطر الأخير للمادة 296 ليستدرك هذا الفراغ ولو بطريقة غير مباشرة، حين أشار للحديث والصياح، والتهديد والكتابة والمنشورات واللافتات والإعلانات كوسائل للنشر الدعاء وإعادة النشر.

وفي هذا يقول الدكتور أحسن بوسقيعة " إن هذا الخلل الوارد في النص 296 من قانون العقوبات الجزائري، راجع إلى سهو المشروع الجزائري عند اقتباس أحكام القذف من قانون الإعلام الفرنسي، إذ أغفل نقل ما نصت عليه المادة 23 من هذا القانون وهي التي عرفت طرق العلنية، وانتقل مباشرة إلى نقل محتوى الفقرة الأولى من المادة 29 التي تقابل نص المادة 296 من قانون العقوبات الجزائري، وفي الوقت الذي أحال فيه المشروع الفرنسي في المواد المتعلقة بالقذف بخصوص الطرق العلنية إلى نص المادة23 ، لا نجد في القانون الجزائري أي حالة مماثلة في المواد المتعلقة بالقذف ، "أما المادة **297** من قانون العقوبات الجزائري المتعلقة بجنحة السب فلم تشر الصراحة إلى العلانية ونرى أن ما قيل بشأن القذف ينطبق على السب،بأن المشروع الجزائري عندما اقتبس أحكام السب من الفقرة الثانية المادة 29 من قانون الإعلام الفرنسي، أغفل ما نصت عليه المادة 23 من هذا القانون، وانتقل مباشرة إلى نقل

---

[1] بن عيسى كهينة، برانسي سليمة، المرجع السابق، ص 18

[2] كمال بوشليق، المرجع السابق، ص27

[3] احسن بوسقيعة، المرجع السابق، ص200

[4] كمال بوشليق، المرجع السابق، ص29

[5] عياط سارة، المرجع السابق، ص 40

محتوى الفقرة الثانية من المادة 21 التي تقابل المادة 297 من قانون العقوبات الجزائري، في الوقت الذي أحال فيه المشرع الفرنسي في المواد المتعلقة بالسب بخصوص الطرق العلنية من المادة 23 من قانون الإعلام، لا نجد في المواد المتعلقة بالسب في قانون العقوبات الجزائري أي إحالة مماثلة، واذا كان المشرع الجزائري لم يشر الصراحة إلى علانية في نص المادة 297 من قانون العقوبات[1]

كان تعديل قانون العقوبات الجزائري بموجب القانون رقم **01-09 لسنة 2001** فرصة لتدارك هذا السهو واعادة انسجام قانون العقوبات، غير أن المشرع ضيع هذه الفرصة، حين ترك نص المادتين296 و 297على حالها، بل زاد الأمر تعقيدا وذلك لأمرين:

الأول : عندما نص على جزاء المقرر للقذف الموجه إلى رئيس الجمهورية، وإلى الهيئات والمؤسسات العمومية للقسم الخاص بالإهانة، بدل التنصيص عليه في القسم الخاص بالقذف وهو مكانه الطبيعي.

الثاني:عندما خص القذف الموجه إلى رئيس الجمهورية والهيئات المذكورة بالطرق العلانية المميزة، وهي كتابة ورسوم، وأية آلية لبث الصوت أو الصورة، أو أية وسيلة الكترونية أو معلوماتية أو إعلامية، وكأننا بذلك أمام وضعية تختلف فيها الطرق العلنية باختلاف الجهة الموجهة إليها القذف[2]

كما أن المشرع الجزائري ضيع فرصة أخرى لتدارك هذا السهو بمناسبة تعديله لقانون العقوبات بموجب القانون رقم06-23 [3]، أما القضاء الجزائري فقد فك هذا الغموض والالتباس الوارد في المواد 296 و 297من قانون العقوبات الجزائري استنادا إلى سلطته في تفسير النصوص العقابية، حين قضى بضرورة توافر أركانها وخاصة ركن العلانية لقيام جريمة القذف، حيث قضت المحكمة العليا بأن إدانة المتهم بجنحة القذف دون توافر أركانها وخاصة ركن العلانية يعد خرقا للقانون، ولقاضي الموضوع سلطة تقدير الوقائع المادية حسبما يراها وعللا ضوئها يحم بتوافر العلانية أو بانتفائها.

تتحقق العلانية في جرائم القذف والسب طبقا لنصوص قانون العقوبات الجزائري بالقول أو الكتابة، أما الفعل أو الإيماء فلا نجد له أية إشارة في قانون العقوبات الجزائري.

ولما كانت العلانية في جرائم القذف والسب تتحقق بالقول أو الكتابة، وكانت العبارات الواردة في المواد296 و 297من قانون العقوبات الجزائري لا تشترط أن يتم لقول أو الكتابة بوسيلة معينة، حيث أنها جاءت من المرونة بما يسمح بانطباقها على الانترنت، لذا يمكننا القول بانطباق أحكام القذف والسب الواردة في المواد213 و 217من قانون العقوبات الجزائري، على أفعال القذف والسب التي تتم بطريق الانترنت.

---

[1] عياط سارة، المرجع السابق، ص 41

[2] المرجع_ نفسه، ص 41

[3] المؤرخ في 20 ديسمبر 2006

إلا أنه يجدر بالمشرع الجزائري أن يعدل المادتين296 و 297من قانون العقوبات لفك الغموض المتعلق بركن العلانية، كما يجب تعديلها لتكون صياغتها واضحة ومحددة بشأن انطباقها على جرائم القذف السب المرتكبة بواسطة الأجهزة المستحدثة بفعل التقدم التكنولوجي وتطور تقنية المعلومات وخاصة الانترنت على النحو الذي وردت به جريمة الإهانة والقذف والسب الموجه إلى رئيس الجمهورية في المادة 144مكرر وذلك حتى يتوافق نص المادتين296 و 297مع مقتضيات مبدأ الشرعية المنصوص عليه في المادة الأولى من قانون العقوبات حيث أن مبدأ الشرعية يقتضي أن تصاغ نصوص التجريم والعقاب بطريقة واضحة محددة كافية لا لبس فيها[1].

المطلب الثاني: الجرائم الواقعة على نظام المعلومات

مع التعديل الأخير الذي أُدخل على قانون العقوبات الجزائري بموجب القانون رقم 24-06، حاول المشرّع مواجهة بعض صور الاعتداءات الحديثة التي أصبحت تستهدف المصالح العليا للدولة في ظل التطور المتسارع لاستخدام الوسائط الرقمية ومنصات التواصل الاجتماعي، وفي هذا الإطار، تم استحداث المادتين 63 مكرر و63 مكرر 1 اللتين تجرّمان الأفعال المرتبطة بتسريب أو نشر أو إتاحة معلومات أو وثائق ذات طابع سري تمس بالأمن الوطني أو الدفاع الوطني أو الاقتصاد الوطني، متى ارتكبت لفائدة دولة أجنبية أو أحد عملائها، أو عندما يكون الهدف منها الإضرار بالمصالح الحيوية للدولة أو التأثير على استقرار مؤسساتها .[2]

ويكتسي هذا التعديل أهمية خاصة بالنظر إلى التحول الذي عرفته طبيعة التهديدات الموجهة ضد الدول، إذ لم تعد المعلومات السرية عرضة للاختراق بالوسائل التقليدية فقط، بل أصبحت البيئة الرقمية مجالًا خصبًا لتسريب البيانات الحساسة ونشرها على نطاق واسع، بما قد يؤدي إلى إلحاق أضرار جسيمة بالأمن القومي وبالثقة في مؤسسات الدولة. لذلك جاء تدخل المشرّع بهدف توسيع دائرة الحماية الجنائية لتشمل الأفعال المرتكبة عبر شبكات التواصل الاجتماعي والوسائط الإلكترونية باعتبارها أدوات حديثة قد تستعمل في تنفيذ أنشطة تجسسية أو تخريبية.

غير أن الملاحظ على هذا التنظيم أن المشرّع الجزائري لم يتجه إلى إنشاء جريمة مستقلة خاصة بالمساس بالبيانات الرقمية السرية، رغم خصوصية هذه البيانات واختلاف طبيعتها عن الوثائق التقليدية. فقد تم إدراج هذه الأفعال ضمن الإطار العام للجرائم الماسة بأمن الدولة، ولا سيما جرائم التجسس والإفشاء غير المشروع للمعلومات السرية، كما يتضح من خلال صياغة المادة 63 مكرر التي ركزت على طبيعة المعلومات أو الوثائق محل الاعتداء والغاية من تسريبها أكثر من تركيزها على الوسيلة الرقمية المستخدمة في ارتكاب الفعل.

---

[1] عياط سارة، المرجع السابق، ص 42

[2] هاشمي رشيدة، ملياني عبد الوهاب، **المواجهة التشريعية لجريمة التجسس الالكتروني في ظل القانون24-06**، مجلة الفكر القانوني والسياسي، المجلد09، العدد01، 2025، ص546.

وعليه، فإن الحماية الجنائية التي أقرها القانون 24-06 تظل مرتبطة بالتصور التقليدي لجريمة التجسس، رغم أن البيئة الرقمية أفرزت أنماطًا جديدة من الاعتداءات تختلف من حيث الوسائل والخطورة والآثار عن الجرائم الكلاسيكية. فالمساس بالبيانات الرقمية لا يقتصر فقط على إفشاء وثيقة سرية، وإنما قد يشمل اختراق قواعد البيانات، أو نسخ المعلومات الإلكترونية، أو نقلها عبر شبكات الاتصال، أو استغلالها بطرق تقنية معقدة، وهي صور لم يعالجها المشرّع الجزائري كجرائم قائمة بذاتها.

لذلك يتم الرجوع إلى المواد من 394 مكرر إلى 394 مكرر 8 الواردة في قانون العقوبات الجزائري رقم 15-04، والمعدلة بموجب القوانين 06-23، 16-02، و24-06[1]، وتشكل هذه المواد الإطار القانوني العام للجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، والمعروفة بالجرائم المعلوماتية.

نظرًا لعدم قيام المشرع بالنص على جريمة التجسس الإلكتروني بشكل منفصل، فإن هذا النوع من الجرائم يتم تصنيفه ضمن الجرائم المعلوماتية التي تخضع للتنظيم القانوني في المواد ذات الصلة، والتي سنناقشها بتفصيل أدناه.

نظرًا لعدم قيام المشرع بالنص على جريمة التجسس الإلكتروني بشكل منفصل، فإن هذا النوع من الجرائم يتم تصنيفه ضمن الجرائم المعلوماتية التي تخضع للتنظيم القانوني في المواد ذات الصلة، والتي سنناقشها بتفصيل أدناه.

الفرع الاول: جريمة الدخول أو البقاء عن طريق الغش

تُعتبر جريمة الدخول أو الاستمرار غير المشروع في نظام المعالجة الآلية للمعطيات الحجر الأساس للعديد من الجرائم الإلكترونية، بما في ذلك جريمة التجسس الإلكتروني، إذ تُعد هذه الأفعال خطوة تمهيدية لارتكاب جرائم أشد خطورة.[2]

أولا: الركن المادي للجريمة

من خلال استقراء نص المادة 394 مكرر من قانون العقوبات الجزائري، نجد أن الركن المادي للجريمة يتكون من عنصرين: الدخول أو البقاء عن طريق الغش إلى نظام المعالجة الآلية للمعطيات.

الدخول في هذا السياق لا يُقصد به الولوج المادي إلى المكان الذي يحتوي على الحاسوب، وإنما يعني الوصول إلى النظام المعلوماتي نفسه باستخدام تقنيات حديثة[3]، ويمكن أن يتم ذلك بطرق متعددة،

---

[1] 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

[2] بوبرقيق عبد الرحيم، **مفهوم انظمة المعالجة الالية في الجرائم المحددة في المواد 394 مكرر الى 394 مكرر 02 من قانون العقوبات الجزائري**، مجلة الدراسات والبحوث القانوني، المجلد 04، العدد01، جوان، 2019، ص 356.

[3] رابحي عزيزة، طاهري محمد بشار، **العنصر المفترض في جريمة الدخول أو البقاء غير المصرح به للنظام المعلوماتي**، المجلة الجزائري للدراسات والتاريخية والقانونية، العددين 01و02، جانفي- جوان، 2016، ص 262

كالاتصال المباشر بالنظام أو اعتراض الاتصالات بطرق غير مشروعة، ويُعتبر هذا الدخول غير مشروع إذا حدث من دون إذن من صاحب النظام أو خالف الشروط التي وضعها مالك النظام أو الشخص المُخوَّل بالتحكم فيه.[1]

وقد استخدم المشرّع الجزائري في الفقرة الأولى من المادة 394 مكرر من قانون العقوبات عبارة "**كل من يدخل أو يبقى عن طريق الغش**"...، وهي عبارة تدل على اشتراط عدم مشروعية الولوج إلى النظام المعلوماتي، أي أن الدخول لا يشكل جريمة إلا إذا تم دون ترخيص أو خارج نطاق الصلاحيات الممنوحة للشخص. ويُفهم من ذلك أن المشرّع ركّز على عنصر **الدخول غير المشروع** باعتباره الركن المادي الأساسي للجريمة، سواء تعلق الأمر بالدخول إلى منظومة معلوماتية كاملة أو إلى جزء منها، متى تم ذلك باستعمال وسائل احتيالية أو دون وجود سند قانوني يسمح بالوصول إليها.

وفي هذا السياق، فإن دخول جهاز حكومي أو نظام معلوماتي تابع لإحدى الهيئات العمومية لا يعد فعلاً مجرّمًا إذا كان قائمًا على رضا الجهة المالكة للنظام، سواء كان هذا الرضا صريحًا من خلال منح صلاحيات الدخول، أو ضمنيًا من خلال طبيعة المهام الوظيفية للأشخاص المخولين بالوصول إلى الشبكة أو الأجهزة المرتبطة بها. غير أن هذا الترخيص يظل محددًا بحدود الصلاحيات الممنوحة، إذ يتحول الفعل إلى اعتداء غير مشروع متى تجاوز المستخدم نطاق الإذن الممنوح له أو استعمل صلاحياته للوصول إلى بيانات أو أنظمة غير مخولة له.. [2]

أما **البقاء غير المشروع** فيُقصد به استمرار الفاعل في الوجود داخل النظام المعلوماتي دون أن يكون له الحق في ذلك، سواء كان دخوله الأولي إلى النظام مشروعًا ثم تجاوز حدود الترخيص الممنوح له، أو كان دخوله منذ البداية غير مشروع. ويتحقق هذا الفعل عندما يرفض الشخص مغادرة النظام بعد انتهاء مدة السماح له بالدخول، أو عندما يستمر في استخدامه خارج نطاق الصلاحيات المخولة له، كأن يقوم موظف بالاطلاع على ملفات أو أنظمة لا تدخل ضمن اختصاصه الوظيفي رغم تمتعه أصلًا بحق الولوج إلى الشبكة. [3]

ومن أجل قيام جريمة الدخول أو البقاء غير المشروع في النظام المعلوماتي، لا يشترط تحقق ضرر فعلي أو حصول الجاني على البيانات المخزنة داخل النظام، إذ يكفي مجرد تمكنه من الوصول إلى النظام أو الاستمرار فيه بغير حق حتى تكتمل الجريمة. ولذلك تعد هذه الجريمة من **الجرائم الشكلية** التي تقوم بمجرد ارتكاب السلوك المجرّم، باعتبار أن المشرّع يهدف إلى حماية أمن وسلامة الأنظمة

---

[1] بن مكي نجاة، **السياسة الجنائية لمكافحة الجرا ئم المعلوماتية**، دار الخلدونية، الجزائر،2017 ، ص 179، 180.

[2] رابح وهيبة، **الجريمة المعلوماتية في التشريع الإجرائي الجزائري**، مجلة الباحث للدراسات الأكاديمية، العدد الرابع، ديسمبر2014 ، ص321

[3] عبد الفتاح بيومي الحجازي، **مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي(دراسة قانونية متعمقة في القانون المعلوماتي)**، دار الكتب القانونية، مصر،2007 ، ص 360، 361.

المعلوماتية قبل تحقق أي اعتداء لاحق على محتوياتها أو بياناتها، وهو ما يعكس الطابع الوقائي للتجريم في مجال الجرائم المعلوماتية.[1]

وبناءً على ذلك، يتمثل السلوك الإجرامي في جريمة التجسس الإلكتروني في قيام الجاني بالولوج غير المشروع إلى الأنظمة المعلوماتية التابعة للجهات الحكومية أو مراقبتها أو اعتراض البيانات المتداولة فيها باستعمال وسائل وتقنيات إلكترونية متطورة، بهدف الوصول إلى معلومات أو معطيات ذات طبيعة حساسة تمس بمصالح الدولة. ولا يقتصر محل هذه المعلومات على المجال العسكري أو الدفاعي فقط، بل يمتد ليشمل مختلف المجالات الحيوية، كالمجال الأمني والسياسي والاقتصادي والعلمي والمالي، متى كانت هذه البيانات من شأنها التأثير في أمن الدولة أو مصالحها العليا.

وتتميز هذه الجريمة بطابعها الخاص من حيث عدم اشتراط تحقق النتيجة الإجرامية المتمثلة في الحصول الفعلي على المعلومات السرية، إذ يكفي أن يثبت أن الجاني قام بأفعال تهدف إلى الوصول إلى هذه البيانات أو جمعها من خلال اختراق النظام أو التجسس عليه. فمجرد الدخول غير المشروع بقصد الاستيلاء على المعلومات أو مراقبتها يُعد كافيًا لقيام الجريمة، باعتبار أن المشرّع يتدخل في هذه الحالة لحماية سرية البيانات وأمن الأنظمة المعلوماتية قبل تحقق الضرر، نظرًا لما قد يترتب على تسريب هذه المعلومات من تهديد مباشر للأمن الوطني واستقرار مؤسسات الدولة.. [2]

ثانيا: الركن المعنوي للجريمة

من خلال تحليل نص المادة 394 مكرر والمادة 394 مكرر 01 من قانون العقوبات الجزائري، يتضح أن المشرع قد عالج جرائم متعلقة بأنظمة المعلومات والمعطيات الرقمية، مقسماً هذه الجرائم إلى نوعين رئيسيين: جريمة الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات، وجريمة التلاعب بمعطيات الحاسب الآلي. فيما يلي تحليل لمكونات وأركان كل من هاتين الجريمتين:[3]

هذه الجريمة تُعد من الجرائم العمدية، حيث يتطلب تحققها توافر القصد الجنائي العام المكون من عنصرين: العلم والإرادة.

– عنصر العلم: يعني إدراك الجاني بطبيعة الفعل المتمثل في الدخول أو البقاء بشكل غير مشروع داخل النظام المعلوماتي، وإذا كان هناك جهل بحقيقة النظام أو إذا حدث الدخول نتيجة خطأ أو اعتقاد خاطئ بأن الدخول مصرح به، فإن القصد الجنائي ينتفي، ومع ذلك، إذا علم الشخص بعد ذلك بعدم شرعية دخوله واستمر في البقاء داخل النظام، يتحقق القصد الجنائي وتنشأ الجريمة منذ لحظة العلم.[4]

---

[1] بن مكي نجاة، المرجع السابق، ص 180-184.

[2] الطيبي البركه، **الحماية الجنائية لنظام المعالجة الآلية للمعطيات دراسة مقارنة**، رسالة مقدمة لاستكمال متطلبات الحصول على شهادة دكتوراه الطور الثالث تخصص قانون جنائي، جامعة أحمد دراية، ادرار، 2020-2021، ص155.

[3] هاشمي رشيدة، ملياني عبد الوهاب، مرجع سابق، ص 547.

[4] بن مكي نجاة، المرجع السابق، ص 182-185

– عنصر الإرادة: يجب أن تتوفر لدى الجاني الإرادة لتجاوز القانون والقيام بالفعل الإجرامي، الإرادة هنا تتركز على السلوك غير المشروع، أي قرار الدخول أو البقاء داخل النظام دون تفويض. [1]

من الجدير بالذكر أن هذه الجريمة تصنف ضمن الجرائم الشكلية؛ إذ لا يشترط لقيامها حدوث نتيجة مادية معينة سوى مجرد القيام بالسلوك الإجرامي ذاته. [2]

الفرع الثاني: جريمة التلاعب بمعطيات الحاسب الالي

نصت المادة 394 مكرر 01 من قانون العقوبات الجزائري على تجريم كافة أشكال التلاعب العمدي بالمعطيات الرقمية، سواء بإدخال معلومات كاذبة، حذف معلومات صحيحة، أو تعديل المعطيات بطريقة غير مشروعة، ولتحقق هذه الجريمة يكفي ارتكاب أي فعل من تلك الأفعال دون الحاجة إلى اجتماعها معاً. [3]

أولا: الركن المادي للجريمة:

يتمثل الركن المادي في الأفعال الإجرامية المحددة وهي:

1. الإدخال: إدراج أو تغيير معطيات موجودة في النظام، كإضافة بيانات زائفة أو برامج ضارة بهدف إلحاق الضرر. يُعتبر الفعل جريمة بغض النظر عما إذا كان مرتكبها لديه تفويض بالدخول للنظام واستغل هذا التفويض، أو لم يكن لديه تفويض أصلاً. [4]

2.المحو أو الازالة: ويتحقق بفقدان البيانات المخزنة عبر الحذف أو النقل إلى أماكن غير متاحة[5]، يمكن تنفيذ هذا الفعل عبر استخدام برمجيات خبيثة مثل الفيروسات أو البرمجيات الضارة كفيروسات الديدان أو "حصان طروادة".[6]

3.التعديل: إدخال تغييرات غير مشروعة على البيانات الرقمية لتبديلها أو استبدالها بمعطيات أخرى، مما يؤدي إلى تغيير النتائج المرجوة من النظام. يتم ذلك عادة باستخدام أدوات تخريبية مثل "القنابل المعلوماتية" أو الفيروسات التي تشل الأداء النظامي. [7]

---

[1] بن مكي نجاة، المرجع نفسه، ص183 .

[2] هاشمي رشيدة، ملياني عبد الوهاب، المرجع السابق، ص 547.

[3] بن مكي نجاة، المرجع السابق، ص 187، 188.

[4] جدي نسيمة، **جرائم المساس بأنظمة المعالجة الالية للمعطيات**، مذكرة ماجستير في القانون الجنائي، كلية الحقوق، جامعة وهرا ن،2014 – 2013 ، ص 64.

[5] امال قارة، **الحماية الجزائية للمعلوماتية في التشريع الجزائري**، دار هومة،2007 ، الجزائر، ص122.

[6] عبد الفتاح بيومي الحجازي، المرجع السابق، ص 387.

[7] حديدان سفيان، **الدخول أو البقاء عن طريق الغش في نظام المعالجة الآلية للمعطيات**، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد الثامن، المجلد الثاني، ديسمبر، 2017، ص301.

ثانيا: الركن المعنوي للجريمة:

جريمة التلاعب بالمعطيات تُصنف أيضاً ضمن الجرائم العمدية التي تتطلب توافر القصد الجنائي العام بعنصريه الرئيسيين:

– العلم: إدراك الجاني أن فعله غير مشروع وأن هدفه يتمثل بالتلاعب واستغلال البيانات الرقمية دون وجه حق.[1]

– الإرادة: تعني توجيه نية الجاني للقيام بالسلوك الجرمي كإدخال معلومات كاذبة أو حذف بيانات أو تعديلها للانتقاص من حقوق الآخرين أو إحداث ضرر معين. [2]

الخلاصة أن كلا الجريمتين، رغم اختلاف نوع السلوك الإجرامي فيهما، تشتركان في كون القصد الجنائي والإرادة الواعية هما الركيزتان الأساسيتان لقيامهما قانونياً، يعكس التجريم في المواد 394 مكرر و394 مكرر 01 سعي المشرع لحماية أنظمة المعلومات والمعطيات الرقمية باعتبارها دعامة أساسية في الحياة المعاصرة، وللحفاظ على حقوق الأفراد والمؤسسات ضد الاعتداءات الرقمية التي أضحت شائعة في العصر الحديث.

الفرع الثالث: جريمة التعامل في معطيات غير مشروعة

جريمة التعامل بالمعطيات غير المشروعة، المنصوص عليها في المادة 394 مكرر 02 من قانون العقوبات الجزائري، تُعد من أخطر الجرائم التي تهدد أمن المعلومات، يتمثل السلوك الإجرامي المرتبط بها في صورتين رئيسيتين: الأولى هي التعامل مع معطيات يمكن أن تُستخدم في ارتكاب جريمة، والثانية تتعلق بالتعامل مع معطيات ناتجة عن جريمة سابقة، ويهدف التجريم في هذه الحالات إلى الحيلولة دون وقوع الجرائم واستغلال المعلومات المسروقة. [3]

الركن المادي للجريمة يتفرع إلى قسمين رئيسيين سيتم شرح كل منهما على النحو التالي:

أولا: جريمة التعامل في معطيات صالحة لارتكاب جريمة

الفقرة الأولى من المادة 394 مكرر 02 من قانون العقوبات الجزائري تُجرّم التعامل بالمعطيات الصالحة لارتكاب جرم، تشمل هذه الجرائم أفعالًا محددة كالتصميم، البحث، التجميع، التوفير، النشر، والاتجار بالمعلومات أو البيانات القادرة على استخداماتها الإجرامية ضد أنظمة المعالجة الآلية للمعطيات، يكفي توافر أيٍّ من هذه الممارسات لقيام الجريمة، دون اشتراط اجتماعها جميعًا، وفيما يلي شرح لكل فعل على حدة: [4]

---

[1] هاشمي رشيدة، ملياني عبد الوهاب، المرجع السابق، ص547.

[2] جدي نسيمة، المرجع السابق، ص 68، 69.

[3] را بحي عزيزة، **الاسرار المعلوماتية وحمايتها الجزائية**، أطروحة مقدمة لنيل شهادة دكتوراه علوم في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان، 2017–2018، ص 170.

[4] بن مكي نجاة، المرجع السابق، ص 194، 195.

– **التصميم:** يشير إلى الجهود الموجهة نحو إنشاء أو تطوير أدوات وبرامج للتسهيل من ارتكاب الجرائم المتعلقة بأنظمة معالجة البيانات الآلية، قد يشمل ذلك تصميم الفيروسات أو أدوات الاختراق أو برامج التجسس، وهي أعمال غالبًا ما يقوم بها متخصصون مثل المبرمجين أو مهندسي الأمن السيبراني الذين يوظفون خبراتهم بشكل غير مشروع.[1]

– **البحث:** لا يقتصر مفهوم البحث هنا على مجرد الاطلاع أو السعي للمعرفة، بل يمتد إلى التحري عن الوسائل والأساليب لتطوير المعطيات الإجرامية وتجهيزها للاستخدام في جرائم مثل تصميم أدوات التجسس.[2]

– **التجميع:** يتضمن جمع وترتيب البيانات والمعلومات التي يمكن توظيفها بطريقة غير قانونية للدخول إلى أنظمة المعلومات أو العبث بها. [3]

– **التوفير:** يشمل جميع الأفعال التي تهدف إلى إتاحة أو تسهيل وصول طرف ثالث إلى معطيات قد تُستخدم بطريقة غير مشروعة لاختراق أنظمة المعالجة البيانات الآلية أو التلاعب بها، مما يوسّع نطاق الخطر.[4]

– **النشر:** يعني توفير المعلومات التي تخدم الأغراض الإجرامية لجمهور أوسع، مما يزيد خطر استغلالها، يعد هذا الفعل بالغ الخطورة بسبب احتمالية تفاقم نشر البيانات بشكل واسع.[5]

– **الاتجار:** يتمثل ذلك في بيع أو شراء أو تبادل المعطيات الصالحة لتنفيذ الجرائم، وهو فعل يختلف عن مفهوم التوفير، إذ يكون الاتجار عادةً بمقابل مادي.[6]

التشديد على هذه العناصر يأتي انطلاقًا من ضرورة حماية نظم المعلومات وضمان سلامتها من كافة أشكال الاستغلال الإجرامي.[7]

ثانيا: التعامل في معطيات متحصل عليها من ارتكاب جريمة

تقع هذه الجريمة عند القيام بأحد الأفعال المنصوص عليها في الفقرة الثانية من المادة 394 مكرر 2 من قانون العقوبات الجزائري، والتي تتمثل في حيازة، إفشاء، نشر أو استعمال معطيات تم التحصل عليها بطرق غير قانونية، عبر ارتكاب أي من الجرائم المرتبطة بأنظمة المعالجة الآلية للمعطيات، فيما يلي سنتناول هذه الأفعال بالتفصيل: [8]

---

[1] هاشمي رشيدة، ملياني عبد الوهاب، المرجع السابق، ص 550.

[2] بن مكي نجاة، المرجع السابق، ص 194، 195.

[3] هاشمي رشيدة، ملياني عبد الوهاب، المرجع السابق، ص 550.

[4] بن مكي نجاة، المرجع السابق، ص 194، 195.

[5] هاشمي رشيدة، ملياني عبد الوهاب، المرجع السابق، ص 550.

[6] بن مكي نجاة، المرجع السابق، ص 194، 195.

[7] هاشمي رشيدة، ملياني عبد الوهاب، المرجع السابق، ص550.

[8] بن مكي نجاة، المرجع السابق، ص198، 199.

-**الحيازة:** تعني السيطرة الفعلية على معطيات تم التحصل عليها بأساليب غير قانونية نتيجة التعدي على أنظمة المعالجة الآلية للمعطيات، مثل الحصول على معطيات من عملية تجسس، تتيح هذه السيطرة الحق في التصرف في تلك المعطيات بأي شكل كان، سواء بالتعديل أو النقل أو حتى التدمير، وبالتالي، يكفي مجرد حيازة هذه المعطيات لتُعتَبر جريمة مستقلة بحد ذاتها.[1]

-**الافشاء:** يشير إلى نقل المعطيات التي حصل عليها الشخص بطريقة غير شرعية – كتلك المحصلة من خلال التجسس – إلى طرف آخر، ومن المهم الإشارة إلى أن مرتكب فعل الإفشاء ليس بالضرورة ملزمًا قانونيًا بكتمان هذه المعطيات، وقد يكون هو نفسه قد حصل عليها بوسيلة غير قانونية. [2]

-**النشر:** يشمل النشر أي تصرف يسعى إلى إتاحة المعطيات الصالحة لارتكاب جرائم للآخرين، سواء كان ذلك بشكل مجاني أو مقابل مادي، ولم تقيّد المادة 394 مكرر 2 طريقة النشر بوسيلة معينة، فذلك يتضمن الوسائل التقليدية كالكتابة والوسائل الحديثة كالإنترنت أو الأقراص المضغوطة.[3]

-**الاستعمال:** يُقصد به أي استخدام للمعطيات التي تم الحصول عليها بطريقة غير قانونية، بغض النظر عن هدف الاستخدام أو عدد المرات التي تُستخدم فيها، حتى لو كان الاستخدام لمرة واحدة فقط – كما في حالة شركة تستغل بيانات سرية تم الحصول عليها عبر التجسس على شركة منافسة – فإنه يعد انتهاكًا.[4]

تُعد جريمة التعامل في معطيات غير مشروعَة من الجرائم العمدية التي تتطلب وجود القصد الجنائي العام بعنصريه: العلم والإرادة، ويتطلب القانون أن يكون الجاني على علم بأن المعطيات التي يتعامل بها غير مشروعة أو تم الحصول عليها من خلال جرائم موجهة ضد أنظمة المعالجة الآلية، وإذا كان الجاني يفتقد العلم بأحد عناصر الجريمة المكونة، ينتفي القصد الجنائي، علاوة على ذلك، لا يكفي أن يكون الجاني مُلمًّا بعناصر الجريمة وحسب، بل يجب أن تنصرف إرادته بوضوح إلى ارتكاب الأفعال المجرّمة المذكورة.[5]

لا تكتمل الصورة الأولى لجريمة التعامل في معطيات صالحة لارتكاب جريمة بمجرد توافر القصد الجنائي العام فقط؛ بل يتوجب أيضًا وجود القصد الجنائي الخاص، والذي يعني اتجاه علم وإرادة الجاني إلى وقائع معينة تتجاوز مجرد أركان الجريمة الشكلية، بهدف استخدام تلك المعطيات بشكل مُعدّ لارتكاب جريمة مثل التجسس الإلكتروني.[6]

---

[1] هاشمي رشيدة، ملياني عبد الوهاب، المرجع السابق، ص551..

[2] بن مكي نجاة، المرجع السابق، ص198، 199.

[3] هاشمي رشيدة، ملياني عبد الوهاب، المرجع السابق، ص551..

[4] بن مكي نجاة، المرجع السابق، ص198، 199.

[5] هاشمي رشيدة، ملياني عبد الوهاب، المرجع السابق، ص551..

[6] بن مكي نجاة، المرجع السابق، ص 201 202

أما بالنسبة للصورة الثانية من الجريمة – وهي التعامل في معطيات تم الحصول عليها من ارتكاب جريمة – فإن توافر القصد الجنائي العام بعنصريه العلم والإرادة فقط يكون كافيًا لإثباتها، على سبيل المثال: إذا قام شخص ما بجمع معلومات عن نظام حماية معين لشركة بقصد اختراقه، فإنه بذلك يكون قد ارتكب الصورة الأولى للجريمة، وذلك لتوافر القصد الجنائي الخاص لأنه ينوي استخدام تلك المعلومات في تنفيذ الجريمة، بينما إذا اشترى شخص قاعدة بيانات تحتوي على معلومات شخصية مع علمه بإمكانية استخدامها في ارتكاب جرائم ولكن دون أن يحدد كيفية استخدامها، فإنه يكون قد ارتكب الصورة الثانية للجريمة، حيث يكفي هنا وجود القصد الجنائي العام لإثباتها.[1]

الفرع الرابع: اعتراض البيانات الشخصية لأغراض اجرامية

يمثل اعتراض البيانات الشخصية أحد أخطر مظاهر الاعتداء في البيئة الرقمية، لما ينطوي عليه من آثار نفسية واجتماعية وقانونية جسيمة، فنتيجة الكم الهائل من البيانات المتداولة عبر مواقع التواصل الاجتماعي، أصبحت هذه المنصات فضاءً مفتوحًا للاطلاع غير المشروع على المعلومات الشخصية، في كثير من الأحيان دون احترام خصوصية أصحابها أو إرادتهم.

لم تعرف معظم التشريعات العقابية فعل التهديد، وترك أمر ذلك لفقهاء القانون الجنائي الذين ع رفوا هذا السلوك بتعريفات عديدة تتفق في مضمونها على أن التهديد هو "كل قول أو كتابة من شأنه إلقاء الرعب والخوف في قلب الشخص المهدد من ارتكاب الجاني للجريمة ضد النفس أو المال أو إفشاء أو نسبة أمور مخدشة للشرف، وقد يحمله التهديد تحت تأثير ذلك الخوف إلى إجابة الجاني إلى ما ابتغى متى اصطحب التهديد بطلب.[2]

ويمكن تعريفه بأنه محاول للإكراه وسلب الإرادة والحرية وإيقاع الأذى الجسدي أو المعنوي على الضحايا عن طريق وسائل يتفنن الجاني في استخدامها لتحقيق جرائمه الأخلاقية أو المادية أو كليهما معاً.[3]

أما التهديد الإلكتروني "الابتزاز" فهو مصطلح مكون من كلمتين "الابتزاز" ويكاد أن يجمع على معناها اللغوي بأنه: "الحصول على المال أو المنافع من شخص تحت التهديد بفضح أسراره أو غير ذلك"، والكلمة الثانية "الإلكتروني" أي حصول فعل التهديد باستعمال وسائل ووسائط الكترونية. ولا يعني

---

[1] هاشمي رشيدة، ملياني عبد الوهاب، المرجع السابق، ص551..

[2] ساره محمد حنش، **المسؤولية الجزائية عن التهديد عبر الوسائل الإلكترونية دراسة مقارنة**، مذكرة الماجستير في القانون العام، جامعة الشرق الأوسط، 2020،، ص 20

[3] بن حميد صالح، **الابتزاز (المفهوم والواقع) –** ورقة بحثية مقدمة في ندوة الابتزاز المفهوم، الأسباب، العلاج، 7 – 8 مارس 2011 : جامعة الملك سعود، المملكة العربية السعودية، ص، ص 14.

هذا عدم حصول الابتزاز بوسائل أخرى مثل الاتصالات الهاتفية والرسائل والبرقيات الورقية أو عن طريق الفاكس وغيرها من الوسائل الأخرى[1]

ويُستغل هذا الوضع من قبل بعض الأطراف في أغراض الابتزاز أو التشهير أو الاختراق، من خلال الولوج غير المصرح به قانونًا إلى أنظمة المعالجة الآلية للبيانات باستخدام وسائل تقنية مختلفة، كالتجسس الرقمي أو اعتراض الاتصالات أو سرقة الحسابات[2]، وتؤدي هذه الأفعال إلى استغلال المعطيات الشخصية للإضرار بسمعة الأفراد، أو الضغط عليهم، أو تحقيق مكاسب غير مشروعة، وهو ما يجعلها من أخطر الجرائم المعلوماتية التي تستهدف الحق في الخصوصية والكرامة الإنسانية.

وعليه، يتضح أن مظاهر تهديد الخصوصية المعلوماتية في البيئة الرقمية تتعدد وتتنوع، غير أنها تشترك جميعًا في كونها تمسّ جوهر الحق في حماية البيانات الشخصية، وتفرض على المشرّع ضرورة إقرار قواعد قانونية فعالة توازن بين متطلبات التطور التكنولوجي وضرورة صون الحقوق والحريات الأساسية للأفراد.

---

[1] يونس محمد غانم، **الابتزاز الإلكتروني" دراسة من وجهة نظر قانونية**"، ضمن مؤلف :الابتزاز الالكتروني جريمة العصر الحديث، إصدار :وزارة الداخلية العراقية، بغداد :دار الكتب والوثائق،2019، ص 05

[2] الدهبي خدوجة، **حق الخصوصية في مواجهة الاعتداءات الالكترونية دراسة مقارنة**، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة أحمد دراية، أدرار، المجلد 01، ع 08، ديسمبر، 2017، ص 11 .

المبحث الثاني: صور جرائم تكنولوجيا المعلومات في القوانين الخاصة

إدراكاً من المشرع الجزائري لخصوصية الجرائم المرتبطة بالبيئة الرقمية وتعقيداتها التقنية، لم يقتصر التنظيم القانوني لها على الأحكام العامة الواردة في قانون العقوبات، بل عززه بجملة من القوانين الخاصة التي تهدف إلى توفير حماية جنائية متخصصة لمجالات معينة تفرضها متطلبات التحول الرقمي.

وتأتي هذه القوانين استجابةً للتطورات المتلاحقة في مجال استخدام التكنولوجيا، وما يرافقها من مخاطر تمس بالحقوق والحريات الأساسية، خاصة ما يتعلق بحماية المعطيات ذات الطابع الشخصي وتأمين الوثائق الإدارية الإلكترونية من مختلف أشكال التزوير أو الاستعمال غير المشروع.

وعليه، سيتم في هذا المبحث دراسة أبرز صور جرائم تكنولوجيا المعلومات المنصوص عليها في القوانين الخاصة، وذلك من خلال التطرق إلى الجرائم الماسة بالمعطيات ذات الطابع الشخصي، ثم الجرائم الماسة بالوثائق الإدارية الإلكترونية

المطلب الاول: الجرائم الماسة بالمعطيات ذات الطابع الشخصي

أدى التطور المتسارع لتكنولوجيات الإعلام والاتصال والاعتماد المتزايد على الأنظمة الرقمية وقواعد البيانات الإلكترونية إلى بروز مخاطر جديدة تهدد الحياة الخاصة للأفراد وتمس بحقوقهم الأساسية المرتبطة بحماية معطياتهم الشخصية، الأمر الذي دفع المشرع الجزائري إلى إرساء منظومة قانونية خاصة بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، من خلال القانون رقم 18-07 المعدل والمتمم بالقانون 25-11. [1]

ولم يكتف المشرع بوضع القواعد التنظيمية المتعلقة بمشروعية المعالجة وضمانات حماية المعطيات الشخصية، بل دعمها بجملة من النصوص الجزائية الرامية إلى ردع كل أشكال الاعتداء على المعطيات ذات الطابع الشخصي أو إساءة استعمالها، سواء تعلق الأمر بالمعالجة غير المشروعة أو بالإفشاء غير القانوني أو الإهمال في تأمين البيانات أو الإخلال بالالتزامات المفروضة على المسؤول عن المعالجة ومقدمي الخدمات.[2]

وتكتسي هذه الجرائم أهمية بالغة بالنظر إلى طبيعتها التقنية وخطورتها على الحياة الخاصة للأشخاص، إذ قد تؤدي إلى انتهاك السرية الرقمية واستغلال المعطيات الشخصية لأغراض غير مشروعة، بما ينعكس سلبًا على الحقوق والحريات الفردية. وعليه، سيتم التطرق في هذا المطلب إلى

---

[1] القانون رقم 25-11 مؤرخ في 28 محرم عام 1447 الموافق لـ 24 يوليو سنة 2025 معدل ومتمم للقانون 18-07 المؤرخ في 10 يونيو سنة2018 ، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية، العدد48 ، الصادرة بتاريخ 2025/07/24

[2] بن حاجة أحمد، **القانون 18-07 المعدل والمتمم كآلية لحماية المعطيات ذات الطابع الشخصي**، مجلة المعيار، المجلد 16، العدد02، 2025، ص 469

الجرائم المرتبطة بالمعالجة غير المشروعة للمعطيات، ثم الجرائم المتعلقة بالإفشاء والإهمال والإخلال بالأمن المعلوماتي.

الفرع الأول: الجرائم المرتبطة بالمعالجة غير المشروعة للمعطيات

الأصل أن تتم معالجة المعطيات الشخصية وفقا لمقتضيات القانون، ولا يطرح أي إشكال بخصوص مسؤولية المعالج، ولكن القانون لا يقف عند هذا الافتراض الحسن بل يضع الضوابط وفي حالة الإخلال بها يستتبع مسائلة المعالج أو أي شخص أخر تسهل له وظيفته استخدام المعطيات بطريقة غير مشروعة، أو تمكين غير المؤهلين منها.

وبالرجوع إلى القانون 07/18 نجد بأن الإخلال بضوابط المعالجة الآلية للمعطيات الشخصية يتخذ عدة صور كلها تشكل جرائم ماسة بنظام هذه المعالجة[1]، فقد يتحقق الإخلال بهذه الضوابط عند القيام بجمع المعطيات الشخصية من خلال استعمال وسائل تدليسيه أو غير نزيهة، أو الاستغلال غير المشروع للمعطيات الشخصية، أو من خلال جمع معطيات حساسة تتعلق بالوضعية الجزائية للشخص المعني، أو في حالة مخالفة الشروط المسبقة للمعالجة، أو من خلال إخلال الملتزم بالمعالجة بالتزاماته القانونية.

تُعدّ المعالجة المشروعة للمعطيات ذات الطابع الشخصي من أهم الضمانات القانونية التي أقرها المشرع لحماية الحياة الخاصة للأفراد، لذلك أحاطها بمجموعة من الشروط والإجراءات التي يجب احترامها عند جمع المعطيات أو استعمالها أو تخزينها أو نقلها، وأمام تزايد مخاطر الاستغلال غير المشروع للبيانات الشخصية، جرم المشرع الجزائري مختلف صور المعالجة غير القانونية التي تتم خارج الضوابط المحددة قانونًا، سواء تعلقت بانعدام الأساس القانوني للمعالجة، أو مخالفة مبدأ الغائية، أو معالجة المعطيات الحساسة دون ترخيص أو موافقة، أو السماح لغير المؤهلين بالوصول إلى المعطيات الشخصية.[2]

وتبرز من خلال المواد من 54 إلى 60 إرادة المشرع في إرساء حماية جزائية فعالة للمعطيات الشخصية، من خلال تجريم الأفعال التي تشكل اعتداءً على خصوصية الأفراد أو إخلالًا بمبادئ المعالجة المشروعة.

---

[1] طباش عز الدين، **الحماية الجزائية للمعطيات الشخصية في التشريع الجزائري، دراسة في ظل قانون 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي**، المجلة الأكاديمية للبحث القانوني، جامعة بجاية، العدد 2، 2018، ص 39.

[2] إبراهيم محمد القاسمي، **جرائم الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات الإلكترونية (وفقا للمرسوم بقانون اتحادي رقم 05 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات وتعديلاته)**، أطروحة مقدمة لاستكمال متطلبات الحصول على درجة الماجستير في القانون العام، جامعة الإمارات العربية المتحدة، كلية القانون، نوفمبر 2018، ص 24.

أولا: جريمة خرق مبادئ المعالجة المشروعة

جرّم المشرع الجزائري كل إخلال بأحكام المادة 2 من القانون المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، حيث نصت المادة 54 على معاقبة كل من يخرق المبادئ الأساسية المنظمة للمعالجة بالحبس وغرامة مالية[1]

وتتمثل خطورة هذه الجريمة في كونها تمس الأساس الذي تقوم عليه حماية المعطيات الشخصية، لأن احترام مبادئ المشروعية والنزاهة والشفافية والغائية والتناسبية يُعدّ شرطًا جوهريًا لصحة أي معالجة. وبالتالي فإن أي معالجة تتم خارج هذا الإطار القانوني تشكل مساسًا مباشرًا بالحياة الخاصة للأفراد وتهديدًا لحقوقهم الرقمية.[2]

كما تتجسد هذه الجريمة في كل سلوك يؤدي إلى معالجة المعطيات دون احترام القواعد القانونية المحددة مسبقًا، سواء تعلق الأمر بجمع البيانات بطريقة غير مشروعة أو استعمالها في أغراض مخالفة لما جُمعت من أجله أو الاحتفاظ بها دون مبرر قانوني. ويُلاحظ أن المشرع شدد العقوبة بالنظر إلى جسامة الضرر الذي قد ينجم عن هذه الأفعال في البيئة الرقمية الحديثة.

ثانيا: جريمة المعالجة دون موافقة أو رغم اعتراض الشخص المعني

أقر المشرع مبدأ الموافقة الصريحة باعتباره أساسًا لمشروعية معالجة المعطيات الشخصية، ولذلك عاقب بموجب المادة 55 كل من قام بمعالجة معطيات ذات طابع شخصي خرقًا لأحكام المادة 7 من القانون[3]،وتتحقق هذه الجريمة متى تمت معالجة المعطيات دون الحصول على رضا الشخص المعني أو دون توفر سند قانوني يبرر المعالجة، وهو ما يشكل انتهاكًا لحرية الفرد في التحكم في بياناته الشخصية. كما تتجسد الجريمة كذلك في حالة استمرار المعالجة رغم اعتراض الشخص المعني، خاصة إذا كانت المعالجة تستهدف الإشهار التجاري أو كانت أسباب الاعتراض مشروعة.[4]

وتكمن أهمية هذه الحماية في تعزيز حق الأفراد في تقرير مصير معطياتهم الشخصية ومنع استغلالها في الأغراض التسويقية أو التجارية دون إرادتهم، وهو ما ينسجم مع المبادئ الحديثة لحماية الخصوصية الرقمية.[5]

---

[1] المادة 54 من القانون 25-11.

[2] العيداني محمد، يوسف زروق، **حماية المعطيات لشخصية في الجزائر على ضوء القانون رقم 07/18 (المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي)**، مجلة معالم للدراسات القانونية والسياسية، المركز الجامعي تندوف، العدد5، ديسمبر 2018، ص 122.

[3] المادة 55 من القانون 25-11.

[4] طباش عز الدين، المرجع السابق، ص 33.

[5] العيداني محمد، يوسف زروق، المرجع السابق، ص 122.

ثالثا: جريمة المعالجة دون تصريح أو ترخيص قانوني

ألزم المشرع المسؤول عن المعالجة باحترام إجراءات التصريح أو الترخيص المسبق في بعض أنواع المعالجة، لما تثيره من مخاطر على حقوق الأشخاص المعنيين، ولذلك نصت المادة 56 على معاقبة كل من ينجز أو يأمر بإنجاز معالجة معطيات ذات طابع شخصي دون احترام الشروط القانونية المتعلقة بالتصريح أو الترخيص.

كما تشمل الجريمة كذلك الإدلاء بتصريحات كاذبة أمام السلطة المختصة أو مواصلة نشاط المعالجة رغم سحب وصل التصريح أو الترخيص الممنوح، وهو ما يعكس حرص المشرع على ضمان الرقابة القانونية والإدارية على عمليات المعالجة.[1] .

ويُعدّ التصريح والترخيص من الآليات الوقائية الأساسية التي تسمح للسلطة الوطنية بمراقبة مدى احترام المعالجة للضمانات القانونية، لذلك فإن تجاوز هذه الإجراءات يُعتبر اعتداءً على النظام القانوني لحماية المعطيات الشخصية

رابعا: جريمة معالجة المعطيات الحساسة دون موافقة

تُعتبر المعطيات الحساسة من أخطر أنواع المعطيات الشخصية، لارتباطها بالجوانب الحميمة للشخص كالأصل العرقي أو الآراء السياسية أو المعتقدات الدينية أو البيانات الصحية والبيومترية، لذلك أخضعها المشرع لحماية مشددة.[2]

وفي هذا الإطار، نصت المادة 57 على معاقبة كل من يقوم بمعالجة المعطيات الحساسة دون الموافقة الصريحة للشخص المعني، وفي غير الحالات المسموح بها قانونًا.[3].، وتبرز خطورة هذه الجريمة في كون المعطيات الحساسة قد تُستعمل في التمييز أو الابتزاز أو المساس بكرامة الأشخاص وحرياتهم الأساسية، الأمر الذي يبرر تشديد العقوبات المقررة بشأنها.

خامسا: جريمة تحويل الغاية من المعالجة

كرّس المشرع مبدأ الغائية باعتباره من أهم مبادئ حماية المعطيات الشخصية، ومن ثم جرم كل استعمال للمعطيات في أغراض غير تلك المصرح بها أو المرخص لها.[4]

وقد نصت المادة 58 على معاقبة كل من ينجز أو يستعمل معالجة معطيات لأغراض مخالفة للغرض المحدد قانونًا[5]، وتتحقق هذه الجريمة عندما يقوم المسؤول عن المعالجة بإعادة استعمال البيانات

---

[1] المادة 56 من القانون 25-11.

[2] طباش عز الدين، المرجع السابق، ص 42.

[3] المادة 57 من القانون 25-11.

[4] حزام فتيحة، **الضمانات القانونية لمعالجة المعطيات ذات الطابع الشخصي، دراسة على ضوء القانون رقم 07/18**، مجلة الإجتهاد للدراسات القانونية والاقتصادية، المجلد 8، العدد4 لسنة 2019، ص 285.

[5] المادة 58 من القانون 25-11.

الشخصية في أهداف جديدة لم يُعلم بها الشخص المعني، كتحويل بيانات الزبائن لأغراض إشهارية أو تجارية دون موافقتهم، وهو ما يشكل مساسًا بثقة الأفراد وبمبدأ الشفافية.[1]

سادسا: جريمة الجمع التدليسي أو غير المشروع للمعطيات

حرص المشرع على ضمان نزاهة وسائل جمع المعطيات الشخصية، ولذلك جرم كل جمع يتم بطرق تدليسية أو غير مشروعة أو تفتقر إلى الشفافية.

فنصت المادة 59 على معاقبة كل من يجمع معطيات ذات طابع شخصي بطريقة تدليسية أو غير نزيهة أو غير مشروعة[2]، وتتحقق هذه الجريمة في الحالات التي يتم فيها الحصول على البيانات عن طريق الخداع أو انتحال الصفة أو استعمال وسائل تقنية غير مشروعة، أو جمع المعلومات دون إعلام الشخص المعني بحقيقة الغرض من المعالجة، وهو ما يشكل اعتداءً مباشرًا على حرية الأفراد وحقهم في الخصوصية.[3]

سابعا: جريمة السماح لغير المؤهلين بالولوج إلى المعطيات

ألزم المشرع المسؤول عن المعالجة باتخاذ التدابير الأمنية الكفيلة بحماية المعطيات الشخصية من الوصول غير المشروع، ولذلك جرم السماح لأشخاص غير مؤهلين بالولوج إلى هذه المعطيات.

وقد نصت المادة 60 على معاقبة كل من يسمح لأشخاص غير مؤهلين بالوصول إلى المعطيات ذات الطابع الشخصي[4]، وتتجسد هذه الجريمة في كل إخلال بواجب السرية أو التقصير في تأمين نظم المعلومات، بما يؤدي إلى كشف البيانات الشخصية أو تمكين الغير من الاطلاع عليها دون سند قانوني، وهو ما قد يترتب عنه أضرار جسيمة تمس الأشخاص المعنيين.

الفرع الثاني: الجرائم المتعلقة بالإفشاء والإهمال والإخلال بالأمن المعلوماتي

إلى جانب تجريم المعالجة غير المشروعة للمعطيات الشخصية، حرص المشرع الجزائري على توفير حماية جزائية للمعطيات ضد مختلف صور الإفشاء غير القانوني والإهمال والإخلال بالتدابير الأمنية، باعتبار أن الخطر لا يقتصر فقط على جمع المعطيات أو استعمالها بصورة غير مشروعة، وإنما يمتد كذلك إلى سوء تأمينها أو تسريبها أو تمكين الغير من الوصول إليها .

وفي ظل تزايد الهجمات السيبرانية والاختراقات المعلوماتية، أصبحت حماية المعطيات الشخصية تقتضي فرض التزامات دقيقة على المسؤولين عن المعالجة ومقدمي الخدمات، مع تقرير عقوبات جزائية ضد كل إخلال بواجبات السرية والأمن والإبلاغ عن الانتهاكات. ولهذا خصص المشرع المواد من 61 إلى 69 لتجريم الأفعال التي تمس أمن المعطيات الشخصية وسريتها وسلامة معالجتها.

---

[1] حزام فتيحة، المرجع السابق، ص 287.

[2] المادة 59 من القانون 25-11.

[3] حزام فتيحة، المرجع السابق، ص 290،291.

[4] المادة 60 من القانون 25-11.

أولا: جريمة عرقلة عمل السلطة الوطنية

نصت المادة 61 على معاقبة كل من يعرقل عمل السلطة الوطنية المكلفة بحماية المعطيات الشخصية، سواء بالاعتراض على عمليات التحقق أو رفض تقديم الوثائق والمعلومات المطلوبة أو تقديم معلومات غير مطابقة للحقيقة.[1]

وتُعدّ هذه الجريمة من الجرائم الماسة بحسن سير الرقابة الإدارية، لأن السلطة الوطنية تضطلع بدور أساسي في مراقبة مدى احترام أحكام القانون، وبالتالي فإن عرقلة مهامها من شأنه أن يضعف فعالية الحماية القانونية للمعطيات الشخصية.[2]

ثانيا: جريمة إفشاء المعلومات المحمية قانونا

ألزم المشرع الأشخاص المكلفين بمعالجة المعطيات أو الاطلاع عليها بواجب السرية المهنية، ولذلك عاقب كل من يفشي معلومات محمية بموجب القانون بالعقوبات المنصوص عليها في المادة 301 من قانون العقوبات.[3]

وتتحقق هذه الجريمة بمجرد كشف أو نقل أو إفشاء المعطيات المحمية إلى الغير دون سند قانوني، لما في ذلك من مساس خطير بخصوصية الأشخاص وثقتهم في الأنظمة المعلوماتية.

ثالثا: الجرائم المرتبطة بالإخلال بالأمن المعلوماتي وحقوق الأشخاص

تشمل هذه الجرائم الولوج غير المشروع إلى السجل الوطني للمعطيات الشخصية، ورفض تمكين الشخص المعني من حقوقه المتعلقة بالإعلام أو التصحيح أو الاعتراض، والاحتفاظ بالمعطيات بعد انتهاء المدة القانونية، وعدم الإبلاغ عن انتهاكات المعطيات الشخصية.[4]

وقد جرم المشرع هذه الأفعال بالنظر إلى ارتباطها المباشر بضمانات حماية المعطيات الشخصية واحترام حقوق الأفراد في مواجهة المسؤول عن المعالجة. كما تهدف هذه النصوص إلى تعزيز مبدأ الشفافية وإلزام الهيئات والمؤسسات باتخاذ تدابير فعالة لتأمين البيانات.[5]

رابعا: جريمة نقل المعطيات إلى الخارج بطريقة غير مشروعة

أخضع المشرع نقل المعطيات الشخصية إلى دولة أجنبية لشروط وضمانات قانونية محددة، حمايةً للمعطيات من الاستغلال في دول لا توفر مستوى كافيًا من الحماية.

---

[1] المادة 61 من القانون 25-11.

[2] العيداني محمد، يوسف زروق، المرجع السابق، ص 123.

[3] المادة 62 من القانون 25-11.

[4] المواد 63 إلى 66 من القانون 25-11.

[5] بلحسن ريم، بولباري أحمد، **الحق في خصوصية المعطيات الشخصية في التشريع الجزائري، دراسة في ظل القانون رقم18-07**، مجلة العلوم القانونية والاجتماعية، جامعة زيان عاشور بالجلفة الجزائر، المجلد05 ، العدد 03 سبتمبر 2020، ص241

ولهذا نصت المادة 67 على معاقبة كل من ينقل معطيات ذات طابع شخصي نحو دولة أجنبية خرقًا للأحكام القانونية[1]، وتبرز أهمية هذه الجريمة في ظل الطابع العابر للحدود للمعالجة الإلكترونية، حيث قد يؤدي النقل غير المشروع للمعطيات إلى فقدان السيطرة عليها وتعريضها للاستغلال أو التسريب.

خامسا: جريمة حفظ المعطيات المتعلقة بالجرائم والإدانات خارج الحالات القانونية

جرّم المشرع حفظ المعطيات المتعلقة بالجرائم أو الإدانات أو التدابير الأمنية خارج الحالات التي يجيزها القانون، بالنظر إلى حساسية هذه البيانات وخطورة استعمالها.[2]

فنصت المادة 68 على معاقبة كل من يقوم بوضع أو حفظ هذه المعطيات في الذاكرة الآلية بصفة غير قانونية، لما قد يشكله ذلك من تهديد لقرينة البراءة ولمستقبل الأشخاص المعنيين وحقوقهم الاجتماعية والمهنية.[3]

سادسا: جريمة تسريب المعطيات والإهمال في حمايتها

تُعدّ هذه الجريمة من أخطر الجرائم المرتبطة بحماية المعطيات الشخصية، لأنها تشمل حالات الإهمال أو التقصير في تأمين المعطيات بما يؤدي إلى تسريبها أو استغلالها بصورة تعسفية أو تدليسية.

وقد نصت المادة 69 على معاقبة كل مسؤول عن المعالجة أو معالج من الباطن أو شخص مكلف بمعالجة المعطيات يتسبب أو يسهل، ولو عن إهمال، الاستعمال التعسفي أو التدليسي للمعطيات أو إيصالها إلى غير المؤهلين لذلك[4]، وتكمن أهمية هذا النص في تكريس المسؤولية الجزائية عن الإهمال المعلوماتي، بما يعكس اتجاه المشرع نحو إلزام مختلف المتدخلين في مجال معالجة المعطيات باتخاذ تدابير تقنية وتنظيمية صارمة لحماية البيانات الشخصية من الاختراق أو التسريب أو سوء الاستعمال.[5]

---

[1] المادة 67 من القانون 25-11.

[2] حنصالي صابرينة، **حماية المعطيات ذات الطابع الشخصي للمتعاقد الالكتروني : نحو تحقيق الأمن السيبراني**، المجلة الجزائرية للعلوم القانونية والسياسية، كلية الحقوق، جامعة الجزائر 01، المجلد 59، العدد 02، جوان 2022، ص 273 .

[3] المادة 68 من القانون 25-11.

[4] المادة 69 من القانون 25-11.

[5] مباركية مفيدة، **الحماية الجنائية للحق في الخصوصية الرقمية في القانون الجزائري**، مجلة الشريعة والاقتصاد جامعة قسنطينة، الجزائر، العدد 13، 2018 ص 463

المطلب الثاني : الجرائم الماسة بالوثائق الادارية الالكترونية

عمد المشرع الجزائري، على غرار العديد من مشرعي دول أخرى إلى إضفاء حماية أكبر على المعلومات والوثائق الإدارية، بتجريم مختلف السلوكيات الواقعة عليها التي تشكل انتهاكا لخصوصيتها وخصوصية ما تحمله من معطيات.[1]

بالنسبة للجرائم التي يمكن تقع على المعلومات والوثائق الإدارية، بعضها ينطلق من الركن المفترض بالنظر إلى صفة مرتكبها الذي يكون موظفا أو مؤتمنا عليها، والبعض الآخر يقوم متى ارتكب الفعل المجرم لذاته.

الفرع الاول: الجرائم الواقعة من الموظف أو المؤتمن على المعلومات والوثائق الإدارية

في الكثير من الحالات يعهد لشخص معين بسبب انتمائه لوظيفة معينة أو ائتمانه عليها الحق في الاطلاع على وثائق ومعلومات معينة ما كان له هذا الحق لولا ذلك، فيكون ملزما بالمحافظة عليها وعدم البوح بما هو موجود فيها في غير ما ألزمه القانون، غير أن الموظف أو المؤتمن قد يحيد عن واجب الحفاظ على المعلومات المتوصل إليها بسبب الوظيفة أو المهنة فيكون بذلك قد ارتكب فعلا مجرما يستوجب العقاب[2]

اولا: جرائم نشر أو إفشاء الوثائق أو المعلومات الإدارية من الموظف أو المؤتمن:

تحظى المعلومات والوثائق الإدارية بحماية جزائية، تزداد أهميتها إذا تعلق الاعتداء بنشر أو إفشاء ما ورد فيها من قبل موظف أو شخص مؤتمن عليها، فالتجريم هنا يستند على صفة مرتكب الفعل المجرم، وتتخذ الاعتداءات في هذه الحالة عدة صور شريطة أن تتعلق بالمعلومات والوثائق المصنفة، التي يقصد بها :" أي مكتوب ورقي أو إلكتروني أو رسم أو مخطط أو خريطة أو صورة أو شريط صوتي أو سمعي بصري أو أي سند مادي أو إلكتروني آخر كانت محل تدابير ترمي إلى منع نشرها أو تقييد الاطلاع عليها[3]

في هذا السياق، جرم المشرع الجزائري فعل قيام الموظف العمومي بنشر أو إفشاء أو اطلاع الغير أو السماح له بأخذ صورة من المعلومات أو الوثائق المصنفة " توزيع محدود"[4] والتي يقصد بها ..

---

[1] عباسي محمد حبيب، **الحماية الجزائية للمعلومات والوثائق الادارية من خلال الأمر 21-09، مجلة** القانون والعلوم السياسية، المجلد 09، العدد01، 2023، ص415.

[2] المرجع نفسه، ص 415.

[3] انظر المطة 03 من المادة 03 من الامر 21-09 مؤرخ في 27 شوال عام 1442 الموافق 8 يونيو سنة 2021 ، يتعلق بحماية المعلومات والوثائق الإدارية ، ج.ر.ج.ج، ع 45 ، الصادرة بتاريخ 28 شوال عام 1442 الموافق 9 يونيو سنة 2021 ،

[4] انظر المادة 28 من الامر 21-09

الوثائق التي يؤدي إنشاؤها إلى المساس بمصالح الدولة ولا يجوز الاطلاع عليها إلا من قبل الأشخاص المؤهلين بحكم الوظيفة أو المهنة" [1]

كما جرم المشرع نفس الفعل[2]، إذا كانت المعلومة أو الوثيقة المعتدى عليها مصنفة" واجب الكتمان"، والذي يتضمن الوثائق التي يلحق إنشاؤها ضررا أكيدا بمصالح الحكومة أو الوزارات أو الإدارات أو إحدى الهيئات العمومية"، أو كانت مصنفة تحت نظام "سري" والذي يتضمن الوثائق التي يلحق إفشاؤها ضررا خطيرا بمصالح الدولة"[3]، أو نظام "سري جدا" المتضمن ... الوثائق التي يلحق إفشاؤها خطرا بالأمن الوطني الداخلي والخارجي.[4]

وذهب المشرع الجزائري إلى أبعد من ذلك، عندما جرم فعل إفشاء أو نشر أو إطلاع الغير على معلومات أو وثائق مصنفة أو سمح له بأخذ صور منها، حتى في حالة ارتكاب هذا الفعل بدون قصد جنائي، أي نتيجة عدم مراعاة الموظف العمومي للأحكام التشريعية و/أو التنظيمية أو القواعد الاحترازية المرتبطة بطبيعة مهامه أو وظائفه . [5]

ثانيا: جريمة قيام الموظف أو المؤتمن بإفشاء السر الوظيفي

لا شك أن المركز الوظيفي للموظف الناتج عن العلاقة التنظيمية التي تربطه بالإدارة يفرض عليه الالتزام بواجب التحفظ، الذي من بين أهم مظاهره عدم إفشاء السر الذي توصل إليه بسبب الوظيفة أو بمناسبتها [6] ويتعلق هذا الالتزام بالنسبة للموظف بفترة ممارسة مهامه ويستمر المدة عشر سنوات بعد انتهاء العلاقة المهنية مهما كان السبب.[7]

ولا يقتصر الالتزام بعدم إفشاء السر الوظيفي على الموظف العمومي فحسب، وإنما يسري هذا الالتزام على كل شخص تحصل على معلومات أو بيانات تدخل ضمن السرية الوظيفية بحكم مهنته أو وضعيته القانونية.[8]

في مجال الحماية الجزائية للسر الوظيفي، نجد بأن تحريم فعل إفشاء هذا السر يستقي أحكامه من خلال الأمر رقم 21-09، المتعلق بحماية المعلومات والوثائق الإدارية، إلا أن المشرع استثنى من تطبيق أحكام هذا الأمر على أسرار الدفاع والأسرار الطبية وأحال في ذلك إلى تطبيق أحكام قانون

((1)) انظر المطة 04 من المادة 06 من الامر 21-09

((2)) انظر المادة 29 من الامر 21-09

((3)) انظر المطة 02 من المادة 29 من الامر 21-09

((4)) انظر المطة 01 من المادة 29 من الامر 21-09

((5)) انظر المادة 30 من الامر 21-09

((6)) عبدلي حمزة، **المسؤولية الجزائية عن افشاء اسرار الوظيفة العمومية**، اطروحة دكتوراه، تخصص: قانون اداري، جامع بن يوسف بن خدة، جامعة الجزائر، 2019-2020، ص 109

((7)) انظر المادة 14 من الامر 21-09

((8)) عباسي محمد حبيب، المراجع السابق، ص 416

العقوبات [1]فمن خلال استقرار أحكام هذا الأمر يتضح أن المشرع جرم فعل إفشاء السر الوظيفي، كما يضاف إلى مقتضيات الحماية الجزائية لهذه المعلومات والوثائق. [2]

والمعلوم أن الدولة بمؤسساتها المختلفة تحتاج إلى إضفاء السرية على بعض أوجه نشاطاتها المختلفة، وهي بذلك تحرص على كتمان ما يصدر عنها من قرارات أو إجراءات أو معلومات قد يؤدي الإفشاء بها إلى الإضرار بأمنها أو بمصالحها.[3]

وغالبا ما تكون حيازة السر الوظيفي بحكم تواجد الشخص في وضعية قانونية سمحت له بالحصول عليه، وبالتالي فإن إفشاءه يعد إهدارا للثقة الموضوعة في شخصه، وقد وسع المشرع في النطاق الشخصي لتجريم فعل إفشاء السر الوظيفي من خلال الأمر ،21-09 المتعلق بحماية المعلومات والوثائق الإدارية، إذ اعتبر أن الجريمة قائمة في حالة قيام كل شخص مؤتمن بحكم الواقع أو المهنة أو الوظيفة الدائمة أو المؤقتة على أسرار أدلي بها إليه وأفشاها في غير الحالات التي يوجب أو يرخص القانون بالتبليغ عنها.[4]

الفرع الثاني: التجريم الذاتي للاعتداءات الواقعة على المعلومات والوثائق الإدارية

إلى جانب التجريم الذي يستند على صفة مرتكبي الفعل الذي يشكل تعديا على المعلومات والوثائق الإدارية، يجرم القانون بعد الأفعال الواقعة عليها بصرف النظر عن مرتكبيها، يستوي يكون الفعل صادرا عن موظف أو مؤمن أو عن غيرهما.[5]

تقسم الجرائم التي تلحق بالمعلومات والوثائق الإدارية التي تستند على السلوك الإجرامي لذاته إلى نوعين؛ جرائم تقليدية وجرائم إلكترونية على النحو الآتي:

أولا: الجرائم التقليدية الواقعة على المعلومات والوثائق الإدارية

تتخذ الجرائم الواقعة على المعلومات والوثائق الإدارية في حالاتها التقليدية عدة صور بعضها يتعلق بتمكين الغير من معرفة محتواها والاطلاع عليه، والبعض الآخر يرتبط بالاستحواذ عليها أو إتلافها أو تغييرها.[6]

1.الجرائم التقليدية المتعلقة بتمكين الغير من المعلومات والوثائق الإدارية: عمد المشرع الجزائري إلى تحرم بعض الأفعال التي تتضمن تمكين الغير من الاطلاع على المعلومات والوثائق الإدارية أو إفشاء ما فيها، إذا ما تم هذا الفعل في غير الأحوال التي يجيز فيها القانون القيام بذلك من بين التي تدخل ضمن

((1)) انظر المادة 49 من الامر 21-09.

((2)) عباسي محمد حبيب، مرجع سابق، 416.

((3))المرجع نفسه، ص 416.

((4)) انظر المادة 31 من الامر 21-09

((5)) عباسي محمد حبيب، المرجع السابق، ص 416

((6))المرجع نفسه، ص417.

هذا المجال تحريم نشر محاضر و/أو أوراق التحريات والتحقيق القضائي أو إفشاء محتواها أو تمكين من لا صفة له حيازتها.[1]

وقد أحسن المشرع فعلا عندما اعتبر أن الجريمة قائمة في هذه الحالة بغض النظر عن صفة مرتكبها، سواء كان قد تحصل على هذه المحاضر أو الأوراق بسبب وظيفته أو مهنته، أو من باب الصدفة فقط، ليكون بذلك قد جسد خصوصية أن التحريات والتحقيقات تمتاز بالسرية. جرم المشرع الجزائري في نفس الاتجاه، فعل اطلاع الغير بمقابل على معلومة أو وثيقة مصنفة أو يسر لغيره ذلك، مهما كانت طبيعة المقابل المتحصل عليه.[2]

2. الجرائم التقليدية المتعلقة بالاستحواذ على المعلومات والوثائق الإدارية أو التعدي عليها: تتعلق المعلومات والوثائق الإدارية بالدولة أو بمؤسساتها، وهو ما يعني عدم جواز الاستحواذ عليها بدون وجه حق أو إتلافها أو طمس ما فيها، استجابة لهذه الخاصية جرم المشرع الجزائري فعل حيازة وثيقة مصنفة دون أن يكون مؤهلا لذلك ولم يقم بتسليمها. كما أنه يعد مرتكبا لجريمة إضافية إذا ما قام بإفشاء مضمونها.[3]

إضافة إلى ذلك، يجرم القانون الجزائري بعض الأفعال التي تتعلق بالاستحواذ على الوثائق الإدارية والتعدي عليها إذا ما أرتكبت من غير الفاعلين أو الشركاء، وتتمثل هذه الأفعال فيما يلي:

1- إخفاء الوثيقة المصنفة أو الأشياء أو الأدوات التي استعملت أو كانت ستستعمل في ارتكاب الجرائم المنصوص عليها في هذا الأمر أو الأشياء أو المواد أو الأموال المتحصلة منها مع علمه بذلك،

2 إتلاف أو اختلاس أو إخفاء أو تزييف عمدا وثيقة عمومية أو خاصة من شأنها تسهيل البحث عن الجرائم المنصوص عليها في هذا الأمر ومعاقبة مرتكبيها.[4]

يلاحظ من خلال هذا التجريم أن الجريمة المرتكبة وإن كانت جريمة مستقلة إلا أنها جريمة لاحقة لجريمة أخرى مرتكبة، بدليل استعمال المشرع لعبارة ارتكاب إحدى هذه الأفعال من غير الفاعلين أو الشركاء، بمعنى آخر أنها جريمة تستند إلى جريمة أخرى وتقوم على باعث يتمثل في طمس الحقيقة عن الجريمة الأولى المرتكبة.[5]

ثانيا: والوثائق الإدارية محل اعتداءات تتم بواسطة استعمال التكنولوجيات الحديثة

الأمر الذي زاد من حدة الأضرار الماسة بها، يجعل محتواها مادة سائغة للجميع، وقد حاول المشرع الجزائري تجنب مثل هذه الاعتداءات تجريم مختلف السلوكات التي تقع على المعلومات والوثائق

((1)) انظر المادة 32 من الامر 21-09.

((2)) انظر المادة 33 من الامر 21-09.

((3)) انظر المادة 35 من الامر 21-09.

((4)) انظر المادة 36 من الامر 21-09.

((5)) عباسي محمد حبيب، المرجع السابق، ص417

الإدارية باستعمال الوسائل الإلكترونية، وهو ما يضمن عدم إفلات مرتكب مثل هذه الأفعال من المتابعة الجزائية والعقاب، سواء كان محترفا أو هاويا.

في هذا السياق، جرم القانون الجزائري فعل الدخول دون ترخيص إلى منظومة معلوماتية أو موقع إلكتروني أو شبكة إلكترونية أو استعمال أي وسيلة أخرى من وسائل تكنولوجيات الإعلام والاتصال للسلطات المعنية، بقصد الحصول بغير وجه حق على معلومات أو وثائق مصلة .[1]

كذلك، اعتبر المشرع الجزائري أن إنشاء أو إدارة أو الإشراف على موقع أو حساب إلكتروني أو برنامج معلوماتي يستعمل لنشر المعلومات أو الوثائق المصنفة أو محتواها، كليا أو جزئيا، جريمة معاقب عليها، وأيضا فعل نشر هذه المعلومات والوثائق، كليا أو جزئيا، على شبكة إلكترونية أو بإحدى وسائل تكنولوجيات الإعلام.[2]

من جهة أخرى، تعد جريمة في نظر القانوني الجزائري قيام شخص عمدا بنشر أو بث، عن طريق الاتصالات الإلكترونية أو منظومة معلوماتية، معلومة أو وثيقة مصنفة بغرض المساس بالنظام العام أو السكينة العامة.[3]

((1)) انظر المادة 37 من الامر 21-09.

((2)) انظر المادة 38 من الامر 21-09.

((3)) عباسي محمد حبيب، المرجع السابق، ص418.

خلاصة

تناول الفصل الأول أثر التطور التكنولوجي على الجانب الموضوعي للأمن الجنائي، من خلال بيان التحولات التي أحدثتها تكنولوجيا المعلومات في طبيعة السلوك الإجرامي وفي المصالح القانونية محل الحماية. فقد أدى الانتشار الواسع لاستخدام الأنظمة المعلوماتية وشبكات الاتصال إلى ظهور نمط جديد من الجرائم يختلف عن الجرائم التقليدية من حيث الوسائل المستعملة، وطبيعة محل الجريمة، وطرق ارتكابها، الأمر الذي فرض ضرورة إعادة النظر في السياسة الجنائية لمواجهة هذه الظاهرة المستحدثة.

وقد تبين من خلال دراسة هذا الفصل أن تكنولوجيا المعلومات لم تقتصر آثارها على تطوير وسائل ارتكاب الجرائم، بل ساهمت أيضاً في توسيع نطاق المصالح التي تستوجب الحماية الجنائية، حيث أصبحت الأنظمة المعلوماتية والبيانات الرقمية من العناصر الأساسية التي تستهدفها الأفعال الإجرامية. فقد ظهرت جرائم تمس سلامة الأنظمة المعلوماتية، من بينها جريمة الدخول أو البقاء غير المشروع في أنظمة المعالجة الآلية للمعطيات، وجريمة التلاعب بالبيانات، والتعامل غير المشروع في المعطيات الرقمية، وهي أفعال جرمها المشرع الجزائري ضمن أحكام قانون العقوبات بهدف حماية الأمن المعلوماتي.

كما أظهرت الدراسة أن خطورة الجرائم المعلوماتية لا تكمن فقط في الوسيلة التقنية المستخدمة، وإنما في طبيعتها الخاصة التي تجعل ارتكابها ممكناً دون التقيد بالحدود الجغرافية، مع صعوبة تحديد هوية الجاني وإثبات العلاقة بينه وبين الفعل المرتكب، كما أن بعض هذه الجرائم تقوم بمجرد ارتكاب السلوك الإجرامي دون اشتراط تحقق نتيجة مادية، وهو ما يعكس الطابع الوقائي للتجريم في مجال حماية الأنظمة والبيانات الرقمية.

ومن جهة أخرى، تبين أن المشرع الجزائري لم يكتف بالنصوص العامة الواردة في قانون العقوبات، وإنما دعمها بقوانين خاصة تهدف إلى حماية مجالات محددة فرضتها البيئة الرقمية، لاسيما حماية المعطيات ذات الطابع الشخصي والوثائق الإلكترونية. وقد ساهم هذا التنظيم في تعزيز الحماية الجنائية، غير أنه لا يزال بحاجة إلى مزيد من التطوير لمواكبة التحولات التقنية المتسارعة، خاصة فيما يتعلق بالجرائم المستحدثة التي لم تعد تقتصر على الصور التقليدية للاعتداء الإلكتروني.

وعليه، يمكن القول إن الجانب الموضوعي للأمن الجنائي أصبح مرتبطاً بشكل وثيق بمدى قدرة التشريع الجنائي على استيعاب التطورات التكنولوجية، من خلال وضع نصوص دقيقة ومرنة في آن واحد، تحقق الحماية الفعالة للمصالح الرقمية دون المساس بالحقوق والحريات الأساسية.

الفصل الثاني:

اثر تكنولوجيا المعلومات في الجانب الاجرائي والمؤسساتي على الأمن الجنائي

الفصل الثاني: اثر تكنولوجيا المعلومات في الجانب الاجرائي والمؤسساتي على الأمن الجنائي

لم يقتصر تأثير تكنولوجيا المعلومات على استحداث أنماط جديدة من الجرائم فحسب، بل امتد ليشمل مختلف آليات مواجهة الظاهرة الإجرامية، سواء على المستوى الإجرائي أو المؤسساتي. فقد أفرزت الجرائم المعلوماتية تحديات عملية وقانونية دفعت السلطات العامة إلى تطوير وسائل البحث والتحري، وتحديث إجراءات التقاضي بما يتلاءم مع خصوصية البيئة الرقمية.

وفي هذا السياق، شهدت السياسة الجنائية المعاصرة توجهاً متزايداً نحو توظيف الوسائل التكنولوجية في مراحل الدعوى العمومية، بدءاً من جمع الأدلة الرقمية وتتبع الأنشطة الإجرامية إلكترونياً، وصولاً إلى اعتماد أنظمة التقاضي الإلكتروني التي تسهم في تحسين فعالية العدالة وتسريع الإجراءات.

ومن جهة أخرى، استلزم التصدي للجرائم الإلكترونية استحداث هياكل ومؤسسات متخصصة تتولى التنسيق والوقاية والمكافحة، بما يضمن تعزيز الأمن السيبراني وحماية الأنظمة المعلوماتية والمعطيات الرقمية.

وعليه، يتناول هذا الفصل أثر تكنولوجيا المعلومات على الأمن الجنائي من زاويتين أساسيتين؛ تتمثل الأولى في الأثر الإجرائي لتكنولوجيا المعلومات، بينما تتمثل الثانية في الأثر المؤسساتي من خلال دراسة الهيئات والهياكل المستحدثة لمواجهة الجرائم الإلكترونية.

المبحث الاول: اثر تكنولوجيا المعلومات الاجرائي على الامن الجنائي

أدت الطبيعة الخاصة للجرائم المعلوماتية، وما تتميز به من سرعة في التنفيذ وإمكانية إخفاء آثارها الرقمية، إلى فرض تحديات جديدة أمام أجهزة العدالة الجنائية، الأمر الذي استوجب إعادة النظر في الوسائل الإجرائية التقليدية وتطويرها بما يتلاءم مع البيئة الرقمية.

وقد تجسد هذا التطور في اعتماد أساليب حديثة للبحث والتحري، من بينها الترصد الإلكتروني وتقنيات المراقبة الرقمية، فضلاً عن إدماج الوسائط الإلكترونية في مختلف مراحل المحاكمة من خلال اعتماد نظم التقاضي الإلكتروني.

ومن هذا المنطلق، يتناول هذا المبحث أثر تكنولوجيا المعلومات على الإجراءات الجنائية، من خلال دراسة دور الترصد الإلكتروني في مرحلة البحث والتحري، ثم بيان انعكاسات التقاضي الإلكتروني على سير العدالة الجنائية.

المطلب الاول: في مرحلة البحث والتحري(الترصد الالكتروني)

استثناءً عن القاعدة العامة التي تقتضي حماية الحق في الحياة الخاصة وصون سرية المراسلات والاتصالات، أقر المشرع الجزائري، على غرار مختلف التشريعات المقارنة، نظام التحريات الخاصة لمواجهة الجرائم الخطيرة والمعقدة، ومن بينها جرائم الفساد، وذلك من خلال استحداث إجراء الترصد الإلكتروني باعتباره وسيلة فعالة للكشف عن هذه الجرائم وجمع الأدلة المتعلقة بها .[1]

وقد كرس المشرع هذا التوجه بموجب المادة 56 من القانون رقم 06-01 المتعلق بالوقاية من الفساد ومكافحته، التي أحالت إلى أحكام قانون الإجراءات الجزائية المتعلقة بأساليب التحري الخاصة، بما يسمح باللجوء إلى الوسائل التقنية الحديثة في البحث والتحري عن جرائم الفساد. [2]

ورغم الأهمية البالغة لهذا الإجراء، إلا أن المشرع الجزائري لم يضع تعريفاً صريحاً لمصطلح "الترصد الإلكتروني"، سواء في قانون الوقاية من الفساد ومكافحته أو في قانون الإجراءات الجزائية بمختلف تعديلاته، غير أنه حدد الوسائل التقنية التي يتم من خلالها، والمتمثلة أساساً في اعتراض

---

[1] الوارد ذكرها في المواد من 65 مكرر5 الى المادة 65 مكرر 10 الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق لـ : 8 يونيو سنة 1966 المتضمن قانون الإجراءات الجزائية, المعدل والمتمم بالأمر 20-04 المؤرخ في 2020/08/30، الجريدة الرسمية للجمهورية الجزائرية، العدد51، بتاريخ 2020/08/30

[2] سعاد بنور، **الأقطاب الجزائية المتخصصة بين الاستراتيجية الوطنية والتعاون القضائي الدولي لمكافحة جرائم الفساد**، مجلة أبحاث قانونية وسياسية، العدد التاسع /ديسمبر2019، ص 61

المراسلات السلكية واللاسلكية، وتسجيل الأصوات، والتقاط الصور، والمنصوص عليها في المواد 114 إلى 118 من قانون الإجراءات الجزائية المعدل والمتمم بموجب القانون رقم 25-14[1].

ويُقصد بالترصد الإلكتروني مجموع الإجراءات التقنية التي تسمح للسلطات القضائية المختصة بمراقبة وتتبع الاتصالات والمحادثات والتصرفات ذات الصلة بالجريمة، وذلك من خلال وسائل تقنية حديثة، بهدف جمع الأدلة وإظهار الحقيقة، مع مراعاة الضمانات القانونية المقررة لحماية الحقوق والحريات الفردية.

ولما كان الترصد الإلكتروني ينطوي على مساس مباشر بالحق الدستوري في الحياة الخاصة وحرمة المراسلات، فقد أحاطه المشرع بجملة من الشروط والضوابط القانونية التي تكفل تحقيق التوازن بين مقتضيات المصلحة العامة في مكافحة الفساد وضمان احترام الحقوق الأساسية للأفراد. [2]

وعليه، سيتم التطرق إلى مفهوم الترصد الإلكتروني وصوره القانونية (الفرع الأول)، ثم بيان الشروط والضوابط القانونية المنظمة له (الفرع الثاني)

الفرع الأول: مفهوم الترصد الإلكتروني وصوره القانونية

يُعد الترصد الإلكتروني من أبرز وسائل التحري الخاصة التي استحدثها المشرع الجزائري لمواجهة جرائم الفساد، بالنظر إلى ما تتميز به هذه الجرائم من طابع خفي وتعقيد في وسائل ارتكابها، الأمر الذي يجعل وسائل التحري التقليدية عاجزة في كثير من الأحيان عن كشفها وإثباتها.

أولاً: مفهوم الترصد الإلكتروني

لم يورد المشرع الجزائري تعريفاً محدداً للترصد الإلكتروني، إلا أن استقراء أحكام المادة 56 من قانون الوقاية من الفساد ومكافحته، إلى جانب المواد 114 إلى 118 من قانون الإجراءات الجزائية، يسمح باستخلاص مفهومه باعتباره مجموعة من الإجراءات التقنية التي تهدف إلى مراقبة وتتبع الأشخاص المشتبه في ارتكابهم جرائم الفساد، من خلال اعتراض مراسلاتهم وتسجيل أصواتهم والتقاط صورهم، دون علمهم، وبإذن من السلطة القضائية المختصة.

ويتضح من هذا المفهوم أن الترصد الإلكتروني يتميز بمجموعة من الخصائص، فهو إجراء استثنائي يرد على مبدأ حرمة الحياة الخاصة، كما أنه إجراء سري يتم دون علم الأشخاص المعنيين به، فضلاً عن كونه وسيلة تقنية حديثة تخضع لإشراف ورقابة قضائية مباشرة.

---

[1] القانون 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] عبد الله أوهابية، **شرح قانون الإجراءات الجزائية، التحري والتحقيق**، ط2، دار هومة،2011، ص 345.

كما يُعد الترصد الإلكتروني وسيلة إجرائية تهدف إلى جمع الأدلة والكشف عن الحقيقة، وليس غاية في حد ذاته، الأمر الذي يقتضي حصر نطاق تطبيقه في الجرائم التي تتسم بالخطورة والتعقيد، ومن بينها جرائم الفساد. .[1]

ثانياً: صور الترصد الإلكتروني

استناداً إلى أحكام المواد 114 إلى 118 من قانون الإجراءات الجزائية، يتخذ الترصد الإلكتروني عدة صور، تتمثل فيما يلي:

1.اعتراض المراسلات السلكية واللاسلكية

يقصد باعتراض المراسلات تتبع المحادثات والمكالمات والرسائل التي تتم عبر وسائل الاتصال المختلفة، سواء كانت سلكية أو لاسلكية، بما في ذلك الهاتف النقال والبريد الإلكتروني والرسائل النصية ومختلف تطبيقات الاتصال الحديثة.

ويفيد اعتراض المراسلات تارة التصنت خفية على المحادثات الجارية، وتارة أخرى تسجيل هذه المحادثات دون علم أصحابها، بهدف جمع الأدلة المتعلقة بجرائم الفساد والكشف عن مرتكبيها.

وتتم هذه العمليات بناءً على إذن قضائي يسمح بوضع الترتيبات التقنية اللازمة لاعتراض المراسلات ومراقبتها، دون اشتراط موافقة الأشخاص المعنيين بها.

2.تسجيل الأصوات

يقصد بتسجيل الأصوات التقاط وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص، سواء كانوا متواجدين في أماكن عامة أو خاصة.

ويُعد هذا الإجراء من أخطر وسائل الترصد الإلكتروني بالنظر إلى مساسه المباشر بحرمة الحياة الخاصة، الأمر الذي دفع المشرع إلى إخضاعه لرقابة قضائية صارمة، ضماناً لعدم التعسف في استعماله.[2]

وتكمن أهمية تسجيل الأصوات في كونه يسمح بالكشف عن الاتفاقات السرية والمحادثات المتعلقة بارتكاب جرائم الفساد، والتي غالباً ما تتم بعيداً عن أعين السلطات المختصة.

---

[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] جميلة خلفي ،**مبادئ الشرعية الإجرائية للمحاكمة الجزائية دراسة قانونية وفق القانون 17-07**، مذكرة لإستكمال متطلبات شهادة ماستر أكاديمي حقوق تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة غرداية ،2017-2018، ص 10

3.التقاط الصور والتسجيل السمعي البصري

يشمل هذا الإجراء التقاط صور لشخص أو عدة أشخاص يتواجدون في أماكن خاصة أو عامة، كما يشمل التسجيلات السمعية البصرية التي تساعد على توثيق الوقائع الإجرامية.

وقد أجازت المادة 114 من قانون الإجراءات الجزائية، في سبيل تنفيذ هذه الترتيبات التقنية، الدخول إلى السكن ولو خارج المواعيد المحددة قانوناً، ودون علم الأشخاص الذين لهم حق على هذا السكن، شريطة أن يتم ذلك بإذن من السلطة القضائية المختصة وتحت إشرافها المباشر.

الفرع الثاني: الشروط والضوابط القانونية للترصد الإلكتروني

نظراً لما ينطوي عليه الترصد الإلكتروني من مساس بالحريات الفردية المكفولة دستورياً، فقد أحاطه المشرع الجزائري بجملة من الشروط الشكلية والموضوعية التي تضمن مشروعية اللجوء إليه.

أولاً: الشروط الشكلية للترصد الإلكتروني

1.ضرورة الحصول على إذن قضائي مسبق

اشترط المشرع الجزائري، بموجب المادة 114 من قانون الإجراءات الجزائية، ضرورة حصول ضابط الشرطة القضائية على إذن كتابي مسبق من السلطة القضائية المختصة قبل مباشرة إجراءات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور.

ففي مرحلة البحث والتحري، يصدر الإذن من وكيل الجمهورية المختص، باعتباره الجهة التي تتولى تحريك الدعوى العمومية ومباشرتها، وتتم العمليات المأذون بها تحت رقابته المباشرة.[1]

أما في حالة فتح تحقيق قضائي، فإن العمليات المذكورة تتم بناءً على إذن يصدره قاضي التحقيق وتحت إشرافه المباشر، وهو ما أكدته الفقرة الثانية من المادة 114 من قانون الإجراءات الجزائية.

ويلاحظ أن المشرع الجزائري خالف في ذلك المشرع الفرنسي، الذي قصر سلطة إصدار الإذن باعتراض المراسلات السلكية واللاسلكية على قاضي التحقيق دون وكيل الجمهورية.

2.البيانات الجوهرية للإذن القضائي

يشترط لصحة الإذن القضائي أن يتضمن مجموعة من البيانات الجوهرية، تتمثل في تحديد الأماكن المقصودة بوضع الترتيبات التقنية الخاصة باعتراض المراسلات وتسجيل الأصوات والتقاط الصور.

كما يجب أن يكون الإذن مؤرخاً ومحدداً المدة وموقعاً عليه من مصدره، مع ضرورة بيان اليوم والشهر والسنة والساعة والدقيقة التي صدر فيها.

وتكمن أهمية تحديد تاريخ وساعة إصدار الإذن في إمكانية احتساب مدة تنفيذ الإجراء ومراقبة مدى احترام الآجال القانونية المحددة له.

---

[1] المادة 114 من القانون 25-14.

ويترتب على إغفال أي بيان من هذه البيانات الجوهرية بطلان الإجراء وما يترتب عنه من آثار قانونية.

3.تحرير محضر بالعمليات المنجزة

طبقاً لأحكام المادة 118 من القانون رقم 25-14، يلتزم ضابط الشرطة القضائية بتحرير محضر يتضمن جميع العمليات المنجزة المتعلقة باعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسجيل السمعي البصري.[1]

ويجب أن يتضمن المحضر وصفاً دقيقاً للترتيبات التقنية المستعملة، إلى جانب تاريخ وساعة بداية ونهاية العمليات المنجزة.

كما تُودع هذه المحاضر ضمن ملف القضية، ويقوم ضابط الشرطة القضائية بوصف أو نسخ المراسلات والصور والمحادثات المسجلة التي تفيد في إظهار الحقيقة وإرفاقها بالملف.

وإذا كانت المحادثات أو المراسلات قد تمت بلغة أجنبية، فإنها تُنسخ وتُترجم عند الاقتضاء بمساعدة مترجم يتم تسخيره لهذا الغرض.

ثانياً: الشروط الموضوعية للترصد الإلكتروني

1. قصر الإجراء على جرائم الفساد والجرائم المحددة قانوناً

لا يجوز اللجوء إلى الترصد الإلكتروني إلا في الجرائم التي أجاز القانون بشأنها استعمال أساليب التحري الخاصة، ومن بينها جرائم الفساد المنصوص عليها في المادة 56 من قانون الوقاية من الفساد ومكافحته. ويبرر هذا التقييد الطبيعة الاستثنائية لهذا الإجراء، وضرورة عدم التوسع في تطبيقه حمايةً للحريات الفردية.

2.تنفيذ الإجراء تحت الإشراف القضائي المباشر

يشترط المشرع أن تتم جميع عمليات الترصد الإلكتروني تحت الإشراف المباشر لوكيل الجمهورية أو قاضي التحقيق، بحسب الحالة، ضماناً لشرعية الإجراءات واحترام حقوق الأفراد.

ويهدف هذا الإشراف القضائي إلى منع أي تعسف محتمل في استعمال وسائل التحري الخاصة، والتأكد من اقتصارها على الأهداف التي أُقرت من أجلها.

3.الجهة المختصة بتنفيذ العمليات التقنية

يستفاد من أحكام المادة 114 من قانون الإجراءات الجزائية أن تنفيذ العمليات التقنية المتعلقة بالترصد الإلكتروني يندرج ضمن اختصاص ضباط الشرطة القضائية.[2]

---

[1] المادة 118 من القانون رقم 25-14

[2] المادة 114 من القانون رقم 25-14

كما يجوز لوكيل الجمهورية أو لضابط الشرطة القضائية المنتدب أن يسخر كل عون مؤهل تابع لمصلحة أو وحدة عمومية أو خاصة مكلفة بالمواصلات السلكية واللاسلكية، قصد التكفل بالجوانب التقنية للعمليات المنصوص عليها قانوناً.

4.حجية المحاضر الناتجة عن الترصد الإلكتروني

لا تكون للمحاضر المحررة بشأن عمليات الترصد الإلكتروني قوة في الإثبات إلا إذا استوفت جميع الشروط الشكلية والموضوعية التي يتطلبها القانون.

وطبقاً لأحكام المادة 214 من قانون الإجراءات الجزائية، فإن الأدلة الواردة بهذه المحاضر تتمتع بحجية نسبية، بحيث يجوز إثبات عكس ما ورد فيها.

ويختلف ذلك عن المحاضر المنصوص عليها في المادتين 16 و20 من قانون الإجراءات الجزائية، التي منحها المشرع قوة إثبات خاصة في الحدود التي رسمها القانون.

المطلب الثاني: في مرحلة المحاكمة (التقاضي الالكتروني)

أدى التطور التكنولوجي المتسارع إلى تغييرات جوهرية مست مختلف الميادين، بما فيها قطاع العدالة، الأمر الذي فرض على المنظومة القضائية ضرورة التكيف مع هذه التحولات من خلال إدماج الوسائل الرقمية ضمن إجراءات التقاضي، وفي هذا الإطار، ظهر مفهوم" التقاضي الإلكتروني "كخيار عصري يهدف إلى تبسيط إجراءات التقاضي، وتسريع وتيرة الفصل في النزاعات. [1]

يعد التقاضي الإلكتروني نقلة نوعية في قطاع العدالة، إذ يمثل انتقالا من الإجراءات الورقية التقليدية إلى نظام رقمي متطور، يعتمد على تكنولوجيا المعلومات والاتصال في جميع مراحل التقاضي. انطلاقا مما سبق، يقتضي الأمر في(الفرع الأول)التطرق لمفهوم التقاضي الإلكتروني، وفي(الفرع الثاني)تحديد الاطار القانوني للتقاضي الإلكتروني في الجزائر.

الفرع الأول: مفهوم التقاضي الإلكتروني

يعد التقاضي الإلكتروني من المفاهيم الحديثة التي جاءت استجابة للتطور الرقمي الذي يشهده العالم، حيث يقصد به استعمال الوسائل التكنولوجية الحديثة، وعلى رأسها الإنترنت، في مباشرة إجراءات التقاضي أمام الجهات القضائية. ويهدف هذا النمط الجديد من التقاضي إلى تجاوز الإشكالات التقليدية المرتبطة بالبطء، والتكدس، والتعقيد، من خلال اعتماد أدوات رقمية تمكن من تسجيل الدعاوى، وتبادل المذكرات، وحضور الجلسات عن بعد، وبناء على ما سبق، سنتناول في هذا الفرع تعريف التقاضي الإلكتروني في اولا، ثم ننتقل إلى بيان خصائصه في ثانيا.

---

[1] غربي صورية، **نظام التقاضي الالكتروني في القانون الجزائري**، المجلة النقدية للقانون والعلوم السياسية كلية الحقوق والعلوم السياسية – جامعة تيزي وزو، الجزائر، المجلد 18، العدد01، 2023، ص167.

الفصل الثاني: اثر تكنولوجيا المعلومات في الجانب الاجرائي والمؤسساتي على الأمن الجنائي

اولا: تعريف التقاضي الإلكتروني

لقد عرف بعض الفقهاء التقاضي الإلكتروني بعدة تعاريف، من أبرزها:

التقاضي الالكتروني هو عبارة عن نظام قضائي تقني معلوماتي جديد، يتيح للمتداعين تسجيل دعواهم وتقديم أدلتهم وحضور جلسات المحاكمة تمهيدا للوصول إلى الحكم وتنفيذه من خلال وسائل الاتصال الالكترونية ب واسطة أجهزة الحاسوب المرتبطة بشبكة الانترنت وعبر البريد الالكتروني .

كما عرف القاضي حازم محمد الشرعة التقاضي الإلكتروني بأنه: " سلطة لمجموعة متخصصة من القضاة النظاميين بنظر في الدعوى ومباشرة الاجراءات القضائية بوسائل إلكترونية مستحدثة، ضمن نظام أو أنظمة قضائية معلوماتية متكاملة الأطراف والوسائل، تعتمد منهج تقنية شبكة الربط الدولية (الإنترنت) وبرامج الملفات الحاسوبية الإلكترونية بنظر في الدعاوى والفصل بها وتنفيذ الأحكام بغية الوصول لفصل سريع في الدعاوى والتسهيل على المتقاضين.[1]

فالتقاضي الإلكتروني يمثل نمطا حديثا من أنماط التقاضي يقوم على إعادة هيكلة شاملة للعملية القضائية التقليدية، وذلك من خلال توظيف الوسائل الرقمية والتقنيات القانونية الحديثة. وتشمل هذه الوسائل مجموعة من الأدوات البرمجية المتقدمة، مثل آلية مراجعة المستندات إلكترونيا، ومنصات تسوية المنازعات عبر الإنترنت.[2]

يهدف هذا التحول الرقمي إلى تعزيز كفاءة الأداء القضائي، من حيث السرعة والدقة وتيسير الوصول إلى العدالة تجدر الإشارة إلى أن المشرع الجزائري لم يدرج ضمن نصوصه التشريعية تعريفا قانونيا لمفهوم التقاضي الإلكتروني، ما يعكس غياب إطار قانوني واضح ينظم هذا الشكل المستحدث من التقاضي. إذ يعد التقاضي الإلكتروني وسيلة حديثة تمكن القضاة من الفصل في المنازعات الإدارية باستخدام تقنيات رقمية بديلة عن الإجراءات الورقية التقليدية. ويتم ذلك من خلال أنظمة معلوماتية تستخدم في تسجيل العرائض، وتبادل المذكرات، ومتابعة إجراءات سير الدعوى إلكترونيا.[3]

ومن الفقه الجزائري من عرفه على أنه استخدام وسائل تقنية للاتصال المرئية والسمعية الإلكترونية في مباشره الدعوى القضائية وحتى الفصل في المنازعات القضائية عن بعد وعيه من خلال التعاريف السابقة يمكننا اقتراح تعريف له وهو أن التقاضي الالكتروني نظام قضائي حكمي مقابل للنظام

---

[1] حايطي فاطمة، هروال نبيلة هبة، **نظام التقاضي الالكتروني بين تحسين جودة العمل القضائي وتحديات الفضاء الرقمي**، مجلة الدراسات القانونية المقارنة، المجلد7 ، العدد الأول، كلية الحقوق والعلوم السياسية، جامعة حسيبة بن بوعلي الشلف، الجزائر،2021 ، ص138

[2] بوخنوفة شهيناز، **التقاضي الإلكتروني في القضاء الإداري الجزائري**، مذكرة ماستر في الحقوق، تخصص :قانون عام، جامعة محمد الصديق بن يحي جيجل- الجرزائر، 2024-2025، ص 09

[3] المرجع نفسه، ص 10

القضائي التقليدي يعمل إلكترونيا ويطبق فيه إجراءات التقاضي والمحاكمة باستعمال وسائل ومعدات الكترونية وبشرية بغرض تسهيل وتسريع التقاضي. [1]

ثانيا: خصائص التقاضي الإلكتروني

يمثل التقاضي الإلكتروني تحولا كبيرا في النظام القضائي، حيث يعتمد على استخدام التكنولوجيا لتسهيل الإجراءات القضائية، مما يعزز الكفاءة والسرعة ويساهم في تقريب العدالة من المواطن في هذا الفرع، سنستعرض خصائص التقاضي الإلكترونية، ويتميز نظام التقاضي الإلكتروني بعدة سمات تميّزه عن الأساليب التقليدية في التقاضي، ومن أبرز هذه الخصائص ما يلي:

1. الانتقال من النظام الورقي إلى النظام الرقمي

يتميز القضاء الرقمي على اعتماد الوسائل التكنولوجية الحديثة في مختلف مراحل الخصومة القضائية، ابتداء من تسجيل الدعوى إلكترونيا، مرورا بتبليغ أطراف النزاع، وعقد الجلسات عن بعد، وصولا إلى تنفيذ الأحكام دون الحاجة إلى التعامل بالوثائق الورقية، ويتم تبادل المستندات والمذكرات بين الخصوم بشكل إلكتروني بالكامل، ويحقق هدف العدالة الرقمية الرامية إلى إنشاء بيئة قضائية خالية من التعاملات الورقية، أي تجسيد مبدأ تقريب العدالة من المواطن.[2]

لذلك نجد، بأن الدعائم الإلكترونية سوف تحل محل الدعائم الورقية بحيث يصبح المحرر الإلكتروني هو السند القانوني الذي يمكن طرفي النزاع من اعتماده.[3]

كرس المشرع الجزائري، من خلال التعديل الأخير لقانون الإجراءات المدنية والإدارية، اعتماد الوسائل الإلكترونية في التقاضي، وذلك بهدف مواكبة التطورات التكنولوجية وتحقيق النجاعة القضائية. إذ أتاح للأطراف إمكانية رفع الدعوى أمام القضاء الإداري عبر الوسائط الإلكترونية، مما يعكس تحولا من النظام الكلاسيكي نحو نظام التقاضي الإلكتروني في رفع الدعوى الإدراية .[4]

2. سرعة تطبيق الإجراءات القضائية

من أهداف التحول الرقمي إنجاز المعاملات، ويتحقق بتوفر عامل السرعة في رفع الدعوى والبت فيها، حيث يوفر القضاء الإلكتروني على المحامين عناء التنقل إلى مقرات الجهات القضائية، لرفع

---

[1] بكايس سمية، **التقاضي الالكتروني ومدى فعاليته في النظام القضائي الجزائري**، مجلة البصائر للدراسات القانونية والاقتصادية، المجلد03، العدد01، 2021، ص 112.

[2] رشا علي الدين، **أمل ماهر جبر، محمد مجدي قاسم، أحمد الحسنين كرم الدين، علا ماهر جبر، منى عماد الدين الشيمي، ندى ضيف السيد لبيب،** " **رقمنة القضاء "التجارب العربية**" "، مجله البحوث القانونية والاقتصادية، جامعة المنصورة، عدد 23، 2024، ص ص 122 – 121 .

[3] المرجع نفسه، ص 122 .

[4] عبد الكريم بوخالفة، " **نحو قضاء إداري إلكتروني في الجزائر** "، مجلة دفاتر السياسية والقانون، جامعة ورقلة، المجلد 15، العدد 2، الجزائر، 2023، ص 130 .

الدعوى واستكمال باقي الإجراءات القضائية فمن خلال القيام بخطوات بسيطة عبر تطبيق إلكتروني يتم رفع الدعوى واستلام وتبادل الوثائق والمستندات المتعلقة بالدعوى على مدار اليوم وطوال أيام الأسبوع دون الحاجة للذهاب للمحكمة، كما يمكن هذا النظام القضاة من الاطلاع على الدعوى والمستندات المرفقة في أي وقت.

إن تطبيق نظام التقاضي الإلكتروني يساعد في حل مشكلة تأخر الفصل في القضايا، وتقليل مشاكل ازدحام الجمهور في المحاكم، مما يؤدي بشكل عام إلى ارتفاع مستوى الخدمات المقدمة لأطراف الدعوى، والارتقاء بمستوى مرفق القضاء [1]

3. تسليم المستندات والمذكرات إلكترونيا

اتاحت شبكة الإنترنت إمكانية تسليم بعض الرسائل والمستندات ومذكرات إلكترونيا أي التسليم المعنوي للوثائق Download، مثل الكتب، الأبحاث والتقارير الإلكترونية، إلى جانب بعض الخدمات مثل الإستشارات القانونية .[2]

يطلق على تسليم الوثائق إلكترونيا عبر الإنترنت بالتسليم المعنوي أو التنزيل عن بعد والمقصود منه استقبال أو نقل أو تنزيل أحد البرامج أو البيانات عبر الإنترنت الخاص للمستخدم، إذ يمكن نقل المستندات والملفات على الخط دون اللجوء إلى العالم الخارج، ويعتبر تسليم الإلكتروني للمستندات والمذكرات من الآليات المستحدثة التي كرستها الرقمنة في سبيل تيسير العمل القضائي، حيث يسمح هذا النمط من تقديم الوثائق مباشرة، دون الحاجة للحضور المادي إلى مقر الجهة القضائية. وهو ما يساهم في تقليص الآجال، وضمان سرعة الفصل في المنازعات، لاسيما في ظل ارتفاع عدد القضايا المطروحة أمام الجهات القضائية.[3]

4. وجود الوسيط الإلكتروني

إن من أهم خصائص التقاضي الإداري الإلكتروني عدم الحضور الشخصي للمتقاضين واستخدام وسائط إلكترونية تسمح لهم بالحضور عبر نوافذ وشاشات إلكترونية دون الحاجة للقاء الأطراف والقضاة في المحكمة، والوسيط الإلكتروني هو عبارة عن أجهزة حواسيب متصلة بشبكة الإنترنت تتم من خلالها

---

[1] مريم محمد الشامسي، **نظام التقاضي عن بعد وفقا لقانون الإجراءات المدنية الإماراتي**، مذكرة مقدمة لنيل درجة الماجستير في القانون، تخصص قانون خاص، كلية القانون، جامعة الامارات العربية المتحدة، 2022، ص 11 .

[2] بوخنوفة شهيناز، مرجع سابق، ص 12

[3] يوسف مباركة، حنان عكوش، " **التقاضي الإلكتروني في الجزائر** "، مجلة الحقوق والعلوم الإنسانية، جامعة عمار ثليجي أغواط، المجلد 15، العدد 1، الجزائر، 2022، ص 547 .

عملية التقاضي الإلكتروني في المادة الإدارية، وهو ما يعني الحضور الافتراضي للمتقاضين لتحقيق السرعة والتقليل من الجهد والأعباء.[1]

الفرع الثاني: الاطار القانوني للتقاضي الالكتروني

يمثل التقاضي الإلكتروني إحدى أبرز صور تحديث المرفق القضائي في ظل التحول الرقمي الذي يشهده قطاع العدالة، حيث أصبح توظيف الوسائط التكنولوجية في إدارة الدعوى القضائية وتبادل العرائض والمذكرات وعقد الجلسات عن بعد ضرورة عملية تهدف إلى تسريع الفصل في المنازعات، تقليص الآجال، تعزيز الشفافية، وتكريس مبدأ الوصول إلى العدالة. وقد تبنّى المشرّع الجزائري هذا التوجه من خلال إدراج أحكام قانونية صريحة تؤسس للإطار التنظيمي للتقاضي الإلكتروني، سواء في المجال الجزائي أو المدني والإداري، ضمن مقاربة تشريعية تهدف إلى عصرنة المنظومة القضائية وضمان فعاليتها.

وفي هذا السياق، يتجلى الإطار القانوني للتقاضي الإلكتروني من خلال النصوص التالية حيث نتطرق في اولا الى القانون 25-03 المتعلق بعصرنة قطاع العدالة، ثم القانون 20-04 المعدل والمتمم لقانون الإجراءات الجزائية في ثانيا، وفي ثالثا القانون 22-13 المعدل والمتمم لقانون الاجراءات المدنية والادارية.

اولا: في القانون 15-03 المتعلق بعصرنة قطاع العدالة

لقد تبنى المشرع الجزائري نظام التقاضي الالكتروني من خلال القانون رقم 15-03[2] المتعلق بعصرنة قطاع العدالة، والذي يحتوي على 19 مادة موزعه على5 فصول يتضمن الفصل الأول الأحكام العامة والهدف من وضع القانون، بحيث ينص الفصل الثاني منه على المنظومة المعلوماتية المركزية لوزارة العدل والإشهاد على صحة الوثائق الإلكترونية، وعلى التصديق الالكتروني للوثائق والمحررات .أما الفصل الثالث فنظم عملية إرسال الوثائق والإجراءات القضائية بالطريقة الالكترونية، وبالنسبة للفصل الرابع نظم شروط واجراءات استعمال المحادثات المرئية عن بعد ويختص الفصل الأخير بالأحكام الجزائية المسلطة على المخالفين لهذا القانون، فالمادة 09 منه نصت بصراحة أن الجزائر اعتمدت فعليا على التقاضي الالكتروني من خلال التبليغ الالكتروني وارسال المحررات القضائية الالكترونية، هذا

---

[1] وردة حميزي، فايزة دحموش، " **التقاضي الإداري الإلكتروني في الجزائر** "، مجلة الاجتهاد القضائي، جامعة محمد خيضر بسكرة، مجلد 15، عدد 2، 2023 الجزائر،، ص 248

[2] القانون رقم15-03 المتعلق بعصرنة العدالة، المؤرخ في 01 فبراير 2015 ،ج ر.ج ج العدد6 ، الصادر في 10 فبراير. 2015

وبالإضافة لقانون عصرنه العدالة تم تعديل قانون الإجراءات الجزائية بموجب الأمر رقم 15-02 [1]والذي نص على جواز سماع الشهود والخبراء عن طريق الوسائل التقنية والمحادثات المرئية عن بعد.

ثانيا: في القانون 20-04 المعدل والمتمم لقانون الإجراءات الجزائية

قام المشرع الجزائري بتعديل قانون الإجراءات الجزائية بالأمر رقم20-04، حيث نص المشرع على إمكانية استجواب وسماع الأطراف عن طريق المحادثة المرئية عن بعد مع مراعاة احترام الحقوق والقواعد المنصوص عليها في قانون الإجراءات الجزائية، أين ربط المشرع استعمال هذه التقنية بشروط سرية الإرسال وأمانته، وضرورة تسجيل التصريحات على دعامة تضمن سلامتها، وتدوينها كاملة وحرفيا على محضر يوقع من طرف القاضي المكلف وأمين الضبط. [2]

كما أتاح المشرع الجزائري إمكانية الاستماع لشهادة الشهود والأطراف المدنية وحتى الخبراء بواسطة المحادثة المرئية عن بعد، من طرف جهة الحكم، بمقر المحكمة الأقرب من مكان الشخص المطلوب تلقي تصريحاته وبحضور وكيل الجمهورية المختص إقليميا وأمين الضبط[3]، بل يمكن استعمال هذه التقنية للاستماع للمتهم المحبوس في المؤسسة العقابية بموافقته طبعا وموافقة النيابة العامة على ذلك.[4]

وقد سعى المشرع إلى تحقيق نظام التقاضي الالكتروني من خلال إصدار أمر20-04 المتضمن تعديل قانون الإجراءات الجزائية الصادر سنة2020 ، وذلك لأسباب دعت إليها مقتضيات حسن سير العدالة والحفاظ على الأمن والصحة العمومية أو أثناء الكوارث الطبيعية، وبالخصوص ما يم ر به العالم من أزمة صحية جراء تفشي فيروس كورونا المستجد، وما ترتب عنه من تعطيل سير مختلف مرافق ومؤسسات الدولة ومنها قطاع العدالة..[5]

---

[1] الأمر رقم 15-02 المؤرخ 23 جويلية2015 ، يعدل ويتمم الأمر رقم 515 - 66 المؤرخ في 8 جوان 1966 المتضمن قانون الإجراءات الجزائية ،ج ر.ج ج العدد 4 الصادر بتاريخ 23 جويلية. 2015

[2] المادة 14 من القانون 15-03

[3] المادة 16 من القانون رقم15-03

[4] المادة 15 من القانون رقم15-03

[5] بن عزوز أحمد، **نظام المحاكمة الالكترونية وفقا لأحكام قانون عصرنة العدالة15-03**، مجلة البصائر للدراسات القانونية والاقتصادية، عدد خاص، كلية الحقوق، جامعة بلحاج بوشعيب، عين تموشنت، الجزائر، ديسمبر2021 ، ص ص 64 – 63

ثالثا: في القانون 22-13 المعدل والمتمم لقانون الاجراءات المدنية والادارية

يرتكز التقاضي الإلكتروني الإداري، وفق اً لأحكام القانون رقم 22 - 13[1] المعدل والمتمم لقانون الإجراءات المدنية والإدارية، في الجزائر على تحديث وتطوير منظومة القضاء الإداري، بما يتماشى مع التوجه نحو عصرنة العدالة وتبنى التقاضي الإلكتروني كآلية حديثة لتعزيز فعالية وسرعة الفصل في المنازعات الإدارية.

لقد تبنى المشرع الجزائري نظام التقاضي الإلكتروني الإداري بموجب التعديل الذي أدخل على قانون الإجراءات المدنية والإدارية بموجب القانون رقم 22 - 13 لسنة 2022، وذلك تماشي اً مع أحكام القانون رقم 15 - 03 المتعلق بعصرنة العدالة. وقد ك رست المادة 815 مكررة من هذا القانون إمكانية رفع الدعوى الإدارية بوسائل إلكترونية، مما يعد خطوة هامة نحو تبسيط الإجراءات القضائية الإدارية[2]

[1] القانون 22-13 مؤرخ في 13 ذي الحجة عام 1443 الموافق لـ 12 يوليو 2022 يعدل ويتمم القانون 08-09 المؤرخ في 18 صفر 1429 الموافق 25 فبراير 2008 المتضمن قانون الإجراءات المدنية والإدارية الجزائري، الجريدة الرسمية العدد 48 مؤرخة في 17 يوليو 2022

[2] بوخنوفة شهيناز، مرجع سابق، ص 30-31

المبحث الثاني: اثر تكنولوجيا المعلومات على الجانب المؤسساتي للامن الجنائي

إن مواجهة الجرائم الإلكترونية لا تقتصر على تطوير النصوص القانونية والإجراءات القضائية فحسب، بل تقتضي أيضاً إنشاء منظومة مؤسساتية متخصصة قادرة على مجابهة التهديدات السيبرانية المتزايدة، وتوفير الحماية اللازمة للأنظمة المعلوماتية والبنى التحتية الرقمية.

وفي هذا الإطار، عمل المشرع الجزائري على استحداث هيئات وأجهزة متخصصة تضطلع بمهام الوقاية والكشف والتنسيق ومكافحة الجرائم الإلكترونية، بما يحقق التكامل بين مختلف الفاعلين في مجال الأمن السيبراني.

وعليه، يخصص هذا المبحث لدراسة أهم الآليات المؤسساتية المستحدثة في مجال الأمن الجنائي الرقمي، وذلك من خلال التطرق إلى الهيئة الوطنية لمكافحة الجرائم الإلكترونية، ثم هيكل أمن الأنظمة المعلوماتية وحماية المعطيات المستحدث بموجب المرسوم الرئاسي رقم 26-07.

المطلب الاول: الهيئة الوطنية لمكافحة الجرائم الالكترونية

تقوم هيئات الدولة الجزائرية المختصة تجاه الجرائم الالكترونية باتخاذ مجموعة من الإجراءات بموجب مقتضيات معينة تتمثل أساسا في حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية وفقا لقواعد قانون الإجراءات الجزائية مع وضع ترتيبات لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية .

تتم الاستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي إجراءات تحفظية بناءا على الاتفاقيات الدولية ذات الصلة والاتفاقيات الثنائية وحسب مبدأ المعاملة بالمثل بينما يتم رفض طلبات المساعدة الدولية إذا كان من شانها المساس بالسيادة الوطنية أو النظام العام، يطبق إجراء عمليات المراقبة في هذه الحالات حصرا بموجب إذن مكتوب من السلطة القضائية المختصة[1]

الفرع الاول: تشكيلة وتنظيم وسير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها

تعتبر الهيئة لبنة جديدة في إطار مسار الإصلاحات التي تنتهجها الجزائر مؤخرا ذات الطابع القانوني والأمني والسياسي لتعزيز دولة القانون والتأكيد على سيدته في كل الأحوال وإصلاح العدالة، تعد الهيئة بمثابة سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي يوجد مقرها بالجزائر

[1] المواد من 03 إلى 15 من القانون رقم 09-04 المؤرخ في 5 غشت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ،صادر بالجريدة الرسمية للجمهورية الجزائرية، العدد 47، 16 غشت 2009، ص ص 06-08.

وضعت لدى الوزير المكلف بالعدل تم إنشاؤها بموجب لمرسوم الرئاسي الموقع من قبل رئيس الجمهورية رقم 15-261.

أولا:المهام الموكلة إلى الهيئة

تمارس الهيئة العديد من المهام والمسؤوليات في ظل احترام الأحكام التشريعية تتمثل أساسا في:

- اقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.
- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها
- مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال من خلال جمع المعلومات والتزويد بها ومن خلال الخبرات القضائية.
- ضمان المراقبة والوقاية للاتصالات الالكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة تحت سلطة القاضي المختص
- تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من اجل استعمالها في الإجراءات القضائية [12].
- العمل على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها قصد جمع المعلومات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم.[1]
- تطوير التعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال.
- المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيا الإعلام والاتصال .
- المساهمة في تحديث المعايير القانونية في مجال اختصاصها .[2]

ثانيا: تشكيلة الهيئة وتنظيمها

تضم الهيئة من حيث تشكيلتها لجنة مديرة، مديرية عامة، مديرية للمراقبة الوقائية واليقظة الالكترونية، مديرية للتنسيق التقني، مركز للعمليات التقنية، ملحقات جهوية .

---

[1] المادة 14 من القانون رقم 09-04 المؤرخ في 5 غشت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مرجع سابق، ص 08.

[2] المواد 2 و3 من المرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية العدد 53، 8 أكتوبر 2015، ص ص 16-17

ا- **اللجنة المديرة :** يرأس اللجنة الوزير المكلف بالعدل تتشكل من الأعضاء التالية الوزير المكلف بالداخلية، الوزير المكلف بالبريد وتكنولوجيات الإعلام والاتصال، قائد الدرك الوطني، المدير العام للأمن الوطني، ممثل عن رئاسة الجمهورية، ممثل عن وزارة الدفاع الوطني، قاضيان من المحكمة العليا.

تمارس اللجنة المديرة وتكلف بالقيام بالمهام التالية توجيه عمل الهيئة والإشراف عليه ومراقبته بالإضافة لدراسة كل مسالة تخضع لمجال اختصاص الهيئة لا سيما فيما يتعلق بتوفر اللجوء للمراقبة الوقائية للاتصالات الالكترونية وضبط برنامج عمل الهيئة وتحديد شروط وكيفيات تنفيذه . قيام اللجنة بشكل دوري بتقييم حالة الخطر في مجال الإرهاب والتخريب والمساس بأمن الدولة للتمكن من تحديد مشتملات عمليات المراقبة الواجب القيام بها والأهداف المنشودة بدقة كما تتولى عملية اقتراح كل نشاط يتصل بالبحث وتقييم الأعمال المباشرة في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ناهيك عن دراسة مشروع النظام الداخلي للهيئة وميزانيتها والموافقة عليه دون إغفال دراستها للتقرير السنوي لنشاطات الهيئة والمصادقة عليه وإبداء رأيها في كل مسالة تتصل بمهام الهيئة مع تقديم كل اقتراح مفيد يتصل بمجال اختصاص الهيئة .[1]

ب- **المديرية العامة :** يتولى إدارتها مدير عام يعين بموجب مرسوم رئاسي وتنهى مهامه بنفس الطريقة حيث يمتلك المدير العام العديد من الصلاحيات حتى يتمكن من القيام بمهامه على أكمل وجه تتمثل أهمها في العمل على حسن سير الهيئة الوطنية عن طريق ضمان تنفيذ برنامج عملها وتنشيط نشاطات هياكل الهيئة وتنسيقها ومتابعتها ومراقبتها وقيامه بتحضير اجتماعات اللجنة المديرة، بالإضافة لقيامه بتمثيل الهيئة لدى السلطات والمؤسسات الوطنية والدولية ولدى القضاء وفي جميع أعمال الحياة المدنية ناهيك عن ممارسة السلطة السلمية على مستخدمي الهيئة والعمل على احترام قواعد حماية السر في الهيئة والقيام بإجراءات التأهيل وأداء اليمين فيما يخص المستخدمين المعنيين في الهيئة مع إعداد التقرير السنوي لنشاطات الهيئة وعرضه على اللجنة المديرة للمصادقة عليه كما يعمل على ضمان التسيير الإداري والمالي للهيئة.

ج- **مديرية المراقبة والوقاية واليقظة الالكترونية :** يتم تعيين مديرها بموجب مرسوم رئاسي موقع من رئيس الجمهورية كما يتم إنهاء مهامه بموجب نفس الطريقة . تتكفل مديرية المراقبة بالقيام بالعديد من المهام لضمان فعالية الهيئة نذكر منها على وجه الخصوص القيام بتنفيذ عمليات المراقبة والوقاية للاتصالات الالكترونية من اجل الكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بناءا على رخصة مكتوبة تمنح من السلطة القضائية وتتم تحت مراقبتها، وإرسال المعلومات المحصل عليها من خلال القيام بالمراقبة الوقائية إلى السلطات القضائية ومصالح الشرطة القضائية المختصة بالإضافة لتنفيذ

[1] المادة 06 من المرسوم الرئاسي رقم 15-261، مرجع سابق، ص 17

طلبات المساعدة القضائية الأجنبية في مجال تدخل الهيئة وجمع المعطيات المفيدة في تحديد مكان تواجد مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والتعرف عليهم . [1]

تتولى أيضا مهمة جمع ومركزة واستغلال كل المعلومات التي تسمح بالكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها والعمل على تنظيم أو المشاركة في عمليات التوعية حول كيفية استعمال تكنولوجيات الإعلام والاتصال وحول المخاطر المتصلة بها ناهيك عن تنفيذ التوجيهات المقدمة إليها من قبل اللجنة المديرة وتزويد السلطات القضائية ومصالح الشرطة القضائية تلقائيا أو بناءا على طلبها بالمعلومات والمعطيات المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال مع وضع مركز العمليات التقنية والملحقات الجهوية قيد الخدمة والسهر على حسن سيره والحفاظ على الحالة الجيدة لمنشاته وتجهيزاته ووسائله التقنية مع ضرورة تطبيق قواعد الحفاظ على السر في نشاطاتها الممارسة .[2]

د- مديرية التنسيق التقني : يتم تعيين مدير المديرية وإنهاء مهامه بموجب مرسوم رئاسي صادر عن رئيس الجمهورية، تتولى بدورها مهام عديدة لكفالة أداء الهيئة بكافة فروعها وأجهزتها واجباتها وتحقيق الغرض من إنشائها حيث تتولى المديرية ممارسة المهام المتمثلة في انجاز الخبرات القضائية في مجال اختصاص الهيئة وتكوين قاعدة معطيات تحليلية للإجرام المتصل بتكنولوجيات الإعلام والاتصال واستغلالها وإعداد الإحصائيات الوطنية المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال بالإضافة للقيام بمبادرة منها أو بناءا على طلب اللجنة المديرة بكل دراسة أو تحليل أو تقييم يتعلق بصلاحياتها مع ضمان تسيير منظومة الإعلام للهيئة وإدارتها .

هـ- مركز العمليات التقنية : يتم تزويده بالمنشات والتجهيزات والوسائل المادية وبالمستخدمين التقنيين الضروريين لتنفيذ العمليات التقنية لمراقبة الاتصالات الالكترونية يتبع المركز مديرية المراقبة الوقائية واليقظة الالكترونية حيث يتم تشغيله من طرفها .

و- **الملحقات الجهوية** يتم تشغيلها من طرف مديرية المراقبة والوقاية واليقظة الالكترونية التي تكون تابعة لها [3]

---

[1] المواد 9- 18 من المرسوم الرئاسي رقم 15-261، مرجع سابق، ص ص 17-18

[2] المواد 9- 18 من مرسوم رئاسي رقم 21- 439 يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

[3] بوزيرة سهيلة، **الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا ت الاعلام والاتصال بين سرية المعطيات الشخصية الالكترونية ومكافحة الجرائم الاالكترونية**، المجلة النقدية للقانون والعلوم السياسية، المجلد 17، العدد02، 2022، ص 567

الفرع الثاني: كيفية سير وممارسة الهيئة لمهامها ومساهمتها في تقليص الإجرام الالكتروني عامة والإرهاب الالكتروني بالخصوص.

تجتمع الهيئة بناءا على استدعاء من رئيسها أو بناءا على طلب احد أعضائها إذ تقوم بإعداد نظامها الداخلي والمصادقة عليه حيث يتم تزويدها بقضاة وضباط وأعوان للشرطة القضائية من المصالح العسكرية للاستعلام والأمن والدرك الوطني يتم تحديد عددهم بموجب قرارات مشتركة بين وزير العدل والدفاع والداخلية كما تزود بمستخدمي الدعم التقني والإداري ضمن مستخدمي المصالح العسكرية للاستعلام والأمن والدرك الوطني كما يمكن لها الاستعانة بأي خبير أو أي شخص يمكن تعيينه في أعمالها شرط التزامهم بالسر المهني وواجب التحفظ وخضوعهم لإجراءات التأهيل .

في إطار الوقاية من الأفعال الموصوفة بجرائم الإرهاب او التخريب والمساس بأمن الدولة تكلف الهيئة بمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية تحت سلطة قاض مختص يتم ذلك بوضع وحدة مراقبة واحدة أو أكثر تزود بالوسائل والتجهيزات التقنية الضرورية تتكون الوحدة من مستخدمين تقنيين يعملون تحت إدارة ومراقبة قاض يساعده ضابط من الشرطة القضائية أو أكثر ينتمي إلى الهيئة .

لا يمكن أن يشارك في عملية مراقبة الاتصالات الالكترونية إلا أعضاء الوحدة أو الوحدات التي أوكلت لها السلطة القضائية هذه المهمة كما يتخذ مسئول الوحدة أثناء سير العملية كل التدابير اللازمة بالاتصال مع المسئولين المعنيين في الهيئة من اجل ضمان سرية العملية وحماية المعلومات المستقاة من المراقبة .

يتم حفظ المعلومات المستقاة أثناء عملية المراقبة خلال حيازتها من الهيئة بالإضافة لتسجيل الاتصالات الالكترونية التي تكون موضوع مراقبة وتحرر وفق الشروط والأشكال المنصوص عليها قانون خاصة في إطار قانون الإجراءات الجزائية إذ تسلم التسجيلات والمحررات إلى السلطات القضائية ومصالح الشرطة القضائية المختصة حيث تحتفظ دون سواها بهذه المعطيات أثناء المدة القانونية المنصوص عليها في التشريع . إذ يجب عدم استخدام المعطيات والمعلومات التي تستلمها أو تجمعها الهيئة لأية أغراض أخرى غير تلك المتعلقة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها .[1]

في إطار ممارستهم لوظائفهم أو بمناسبتها يمكن أن يقوم القضاة وضباط الشرطة القضائية التابعين للهيئة طبقا للتشريعات المعمول بها بتفتيش أي مكان أو هيكل أو جهاز بلغ إلى علمهم انه يحوز أو يستعمل وسائل وتجهيزات موجهة لمراقبة الاتصالات الالكترونية . من جهة أخرى في حال معاينة

[1] المواد من 19- 26 من مرسوم رئاسي رقم 21- 439 يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

أفعال يمكن وصفها جزائيا تخطر الهيئة النائب العام المختص للقيام بالمتابعات المحتملة إذ يمكن في هذا الصدد أن تطلب الهيئة مساعدة موظفين مختصين من الوزارات المعنية في مجالات تكنولوجيات الإعلام والاتصال حيث يتم رفع تقارير فصلية عن نشاطات الهيئة من قبل رئيس اللجنة المديرة للهيئة إلى رئيس الجمهورية.

في إطار ضمان قيام موظفو الهيئة بمهامهم في أحسن الظروف يستفيد مستخدمو الهيئة من حماية الدولة من التهديدات أو الضغوط أو الاهانات مهما تكن طبيعتها التي قد يتعرضون لها بسبب أو بمناسبة قيامهم بمهامهم باستثناء الحالات السابقة لا يمكن أن يتم استيراد أو اقتناء أو حيازة أو استعمال وسائل وتجهيزات تقنية لمراقبة الاتصالات الالكترونية إلا الهيئة أو عند الاقتضاء سلطة ضبط الاتصالات السلكية واللاسلكية أو المؤسسة العمومية المكلفة بشبكات الاتصالات .[1]

المطلب الثاني: هيكل أمن الأنظمة المعلوماتية وحماية المعطيات المستحدث بالمرسوم الرئاسي 26-07

جاء المرسوم الرئاسي رقم 26-07 ليكرّس توجهًا تشريعيًا حديثًا يرمي إلى تعزيز الأمن السيبراني داخل المؤسسات والإدارات العمومية، وذلك من خلال **إلزامية إنشاء هيكل متخصص** يتولى مهام أمن الأنظمة المعلوماتية وحماية المعطيات.

فقد نصت **المادة 2** [2]صراحة على إلزام جميع المؤسسات والإدارات والهيئات العمومية بإنشاء هذا الهيكل، مع التأكيد على ضرورة **استقلاليته عن الهيكل المكلف بالأنظمة المعلوماتية**، وهو ما يعكس رغبة المشرّع في تجنب تضارب المصالح وضمان فعالية الرقابة.

كما أقرّ المرسوم إلحاق هذا الهيكل مباشرة بـ **المسؤول الأول للمؤسسة**، مما يمنحه مكانة تنظيمية رفيعة ويعزز من قدرته على اتخاذ القرارات الاستراتيجية والتنسيق مع مختلف المصالح، بما يضمن فعالية تنفيذ سياسات الأمن المعلوماتي.

1. الطابع الدائم والشامل لمهام الهيكل: أكدت **المادة 3** [3]على أن مهام الهيكل ذات طابع **دائم ومستمر وفي جميع الظروف**، وهو ما يدل على أن الأمن السيبراني لم يعد مجرد إجراء ظرفي، بل أصبح وظيفة استراتيجية مستمرة تواكب تطور التهديدات الرقمية.

---

[1] المواد من 30-32 من مرسوم رئاسي رقم 21- 439 يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

[2] انظر المادة 02 من المرسوم الرئاسي رقم26-07 مؤرخ في 7 جانفي 2026 يتضمن إنشاء هيكل مسؤول عن أمن الأنظمة المعلوماتية وحماية المعطيات في المؤسسات والإدارات والهيئات العمومية، وتحديد مهامه وتنظيمه وسيره، ج.ر العدد04 الصادرة بتاريخ2023/01/18.

[3] انظر المادة 03 من المرسوم الرئاسي رقم26-07 .

كما ألزمت نفس المادة بتوفير الموارد البشرية والوسائل المادية والتقنية اللازمة، مع مراعاة خصوصيات كل مؤسسة، وهو ما يعكس اعتماد مقاربة **مرنة ومتكيفة** حسب طبيعة الأنظمة المعلوماتية ودرجة حساسيتها.

2. تحديد دقيق لمهام الهيكل (مقاربة وقائية ورقابية): تُبرز المادة 4 من المرسوم الرئاسي 26-07[1] من خلال تحديدها الدقيق لمهام الهيكل اعتماد المشرّع على مقاربة مزدوجة تقوم على الجمع بين الوقاية والرقابة والتدخل، بما يعكس تصورًا متكاملاً لتعزيز الأمن السيبراني داخل المؤسسة. ففي الجانب الاستراتيجي، أُنيط بالهيكل إعداد سياسة أمن الأنظمة المعلوماتية وضمان تنفيذها بما يتوافق مع التوجهات الوطنية ذات الصلة، إلى جانب تبني منهجية حديثة قائمة على إدارة المخاطر من خلال إعداد خريطة شاملة للمخاطر والسهر على تنفيذ خطط المعالجة والتصحيح.

أما على المستوى العملياتي، فتشمل مهام الهيكل الجوانب التقنية المرتبطة بتسيير حلول الأمن السيبراني وتعزيز المرونة السيبرانية، إلى جانب المهام الرقابية من خلال إجراء عمليات التدقيق والمراقبة بالتنسيق مع الجهات المختصة، فضلاً عن الدور الوقائي القائم على اليقظة المستمرة. كما يمتد اختصاصه إلى التبليغ الفوري عن الحوادث السيبرانية، وضمان الامتثال للأطر القانونية المتعلقة بحماية المعطيات ذات الطابع الشخصي، بالإضافة إلى ترسيخ ثقافة الأمن المعلوماتي عبر التكوين والتحسيس. ويعكس هذا التنوع في المهام تبني المشرّع لرؤية شمولية تدمج الأبعاد التقنية والقانونية والبشرية في منظومة الأمن السيبراني.

3. تعزيز التنسيق المؤسساتي (الداخلي والخارجي): تُبيّن المادة 5 من المرسوم الرئاسي 26-07[2]، الإطار المنظّم للعلاقات الوظيفية للهيكل، حيث ألزمت مسؤولَه بإرساء تنسيق متعدد المستويات يضمن انسجام الجهود وتكاملها داخل المؤسسة وخارجها. فعلى الصعيد الداخلي، يمتد هذا التنسيق ليشمل المسؤول الأول للمؤسسة في ما يتعلق بالتوجيهات الاستراتيجية وتعزيز الوعي بالمخاطر، كما يشمل الهيكل المكلف بالأنظمة المعلوماتية بهدف تحقيق التكامل الوظيفي، خاصة في إدارة الحوادث وتطوير الأنظمة. ويشمل كذلك مصلحة الصفقات العمومية لإدماج متطلبات الأمن السيبراني ضمن العقود، وهيكل الأمن الداخلي لضمان حماية المستخدمين والتجهيزات، إضافة إلى التنسيق مع الهيئات التابعة بما يحقق انسجام السياسات على المستوى القطاعي.

أما على الصعيد الخارجي، فيتجسد هذا التنسيق من خلال التعاون مع مختلف الجهات المختصة، وعلى رأسها وكالة أمن الأنظمة المعلوماتية، والسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، فضلاً عن باقي الهيئات ذات الصلة، ويعكس هذا التنظيم توجه المشرّع نحو تكريس مبدأ

((1)) انظر المادة 04 من المرسوم الرئاسي رقم26-07 .

((2)) انظر المادة 05 من المرسوم الرئاسي رقم26-07 .

الحوكمة التشاركية في مجال الأمن السيبراني، من خلال تجاوز المقاربة المنعزلة واعتماد آليات تعاون وتكامل مؤسساتي تضمن فعالية أكبر في مواجهة التهديدات السيبرانية.

4. هيكلة تنظيمية مرنة ومتكيفة: تُحدّد المادة 6 مكوّنات الهيكل من خلال ضبط خمسة مناصب أساسية تُشكّل الإطار التنظيمي لوظيفته، حيث تضم مسؤول الهيكل، ومكلفًا بالعمليات واليقظة، ومكلفًا بالتدقيق وتسيير المخاطر، ومكلفًا بحماية المعطيات ذات الطابع الشخصي، إضافة إلى مكلف بالتحسيس والتكوين. ويعكس هذا التوزيع الوظيفي تنوع الأدوار داخل الهيكل، بما يضمن تغطية مختلف أبعاد الأمن السيبراني، سواء التقنية أو التنظيمية أو القانونية أو التحسيسية.

ومن جهة أخرى، أقرّت المادة إمكانية دمج بعض هذه المناصب وفقًا لحجم المؤسسة ودرجة حساسية أنظمتها المعلوماتية، وهو ما يدل على تبنّي المشرّع لمرونة تنظيمية تراعي الفوارق بين الهيئات الإدارية، ويسمح هذا التوجه بتكييف الهيكل مع الإمكانيات المتاحة والاحتياجات الفعلية، دون الإخلال بمتطلبات الفعالية في ضمان أمن الأنظمة المعلوماتية.[1]

كما أكدت المادتان 7 و8 على إخضاع تنظيم وتصنيف مناصب الهيكل لمجموعة من المعايير الموضوعية، وفي مقدمتها حجم المؤسسة وطبيعة وتصنيف أنظمتها المعلوماتية. ويهدف هذا التوجه إلى ضمان توزيع عقلاني للموارد البشرية والوظائف، بما يتلاءم مع احتياجات كل مؤسسة ومستوى تعقيد بنيتها الرقمية. [2]

ويُبرز هذا التنظيم الطابع الوظيفي الذي اعتمده المشرّع، حيث لم يتم الاكتفاء بوضع هيكل جامد، بل تم ربطه بعوامل واقعية تسمح بتكييفه وفق خصوصيات كل جهة. ومن شأن ذلك تعزيز فعالية الهيكل في أداء مهامه، من خلال تحقيق التوازن بين متطلبات الأمن السيبراني والإمكانيات التنظيمية المتاحة.

5. آليات التوظيف والتكوين كضمان لفعالية الهيكل: نصّت المادتان 10 و11 على جملة من الآليات العملية الكفيلة بتفعيل الهيكل وضمان جاهزيته، حيث اعتمد المشرّع على ثلاثة مسارات أساسية تتمثل في إعادة التوزيع الداخلي للموارد البشرية، واللجوء إلى النقل أو الانتداب، إضافة إلى التوظيف الخارجي. ويُبرز هذا التنوع في آليات الاستقطاب حرص المشرّع على توفير المرونة اللازمة لتغطية احتياجات الهيكل، مع إعطاء الأولوية للكفاءات المؤهلة، بما يعكس توجّهًا واضحًا نحو تثمين الخبرات المتخصصة في مجال الأمن السيبراني.

كما أقرّ المرسوم إلزامية الخضوع لتكوين تحضيري يتم بالتنسيق مع الجهات المختصة، وهو ما يعزز من جاهزية المستخدمين ويرفع من مستوى كفاءتهم المهنية. ويساهم هذا التكوين في تمكين الموارد

((1)) انظر المادة 06 من المرسوم الرئاسي رقم26-07 .

((2)) انظر المادتان (07، 08) من المرسوم الرئاسي رقم26-07 .

البشرية من مواكبة التطورات التقنية والتشريعية المتسارعة، بما يضمن أداءً فعّالًا ومتجددًا لمهام الهيكل في بيئة رقمية دائمة التغير.[1]

6. الطابع الإلزامي والتوسعي لأحكام المرسوم: تُبرز المادة 12 من المرسوم الرئاسي رقم 26-07 اتساع نطاق تطبيقه ليشمل حتى الهيئات والمؤسسات التي لم تُذكر صراحة ضمن أحكامه، وهو ما يعكس إرادة المشرّع في إضفاء طابع شمولي وإلزامي على هذا التنظيم. فبدل حصر تطبيق المرسوم في فئات محددة، تم تبني مقاربة مرنة تضمن خضوع مختلف الكيانات العمومية، مهما كانت طبيعتها أو تسميتها، لالتزامات الأمن السيبراني، ويؤكد ذلك أن حماية الأنظمة المعلوماتية لم تعد مسألة قطاعية، بل أصبحت التزامًا عامًا يشمل كامل البنية الإدارية للدولة، بما يضمن توحيد المعايير وتعزيز مستوى الحماية على الصعيد الوطني..[2]

أما المادة 13، فقد أحالت إلى إمكانية إصدار تعليمات وتدابير تطبيقية، وهو ما يمنح هذا النص بعدًا ديناميكيًا يسمح له بمواكبة التطورات التكنولوجية والمخاطر السيبرانية المتجددة. فبدل الجمود التشريعي، أتاح المشرّع إمكانية تكييف أحكام المرسوم عبر نصوص تنظيمية أو توجيهات عملية تصدر عن الجهات المختصة، بما يضمن مرونة التطبيق وفعاليته. وتكمن أهمية هذه الآلية في تمكين الإدارة من الاستجابة السريعة للتهديدات الرقمية، دون الحاجة إلى تعديل النص الأصلي في كل مرة، وهو ما يعزز النجاعة القانونية والتنظيمية..[3]

وفي المجمل، يكرّس المرسوم الرئاسي رقم 26-07 تحولًا نوعيًا في مقاربة الإدارة الجزائرية لموضوع الأمن السيبراني، من خلال إرساء هيكل مؤسساتي متخصص ومستقل، واعتماد مقاربة شاملة تجمع بين الوقاية والرقابة والتنظيم، فضلًا عن تعزيز التنسيق بين مختلف الفاعلين والاستثمار في الموارد البشرية والتكوين، ويعكس هذا التوجه إدراك الدولة لأهمية الأمن الرقمي كركيزة أساسية في إنجاح مسار التحول الرقمي، وضمان حماية المعطيات ذات الطابع الشخصي، بما يعزز الثقة في الإدارة الإلكترونية ويرسّخ مبادئ الحوكمة الحديثة.

---

[1] انظر المادتان (10، 11) من المرسوم الرئاسي رقم26-07 .

[2] انظر المادة 12 من المرسوم الرئاسي رقم26-07 .

[3] انظر المادة 13 من المرسوم الرئاسي رقم26-07 .

خلاصة

تناول الفصل الثاني أثر تكنولوجيا المعلومات على الجانب الإجرائي للأمن الجنائي، من خلال دراسة التحولات التي مست إجراءات البحث والتحري والتحقيق والإثبات الجنائي نتيجة ظهور الجرائم الإلكترونية. فقد فرضت الطبيعة التقنية لهذه الجرائم ضرورة تطوير أساليب العمل الأمني والقضائي، والانتقال من وسائل التحقيق التقليدية إلى وسائل تعتمد على الخبرة التقنية والتحليل الرقمي.

وقد أظهرت الدراسة أن التكنولوجيا الحديثة ساهمت في تطوير قدرات أجهزة الأمن والقضاء، من خلال استخدام الأنظمة المعلوماتية وقواعد البيانات الإلكترونية وتقنيات التتبع والتحليل الرقمي، مما ساعد على كشف بعض الجرائم المعقدة وتحديد مسار النشاط الإجرامي. غير أن هذه الوسائل تطرح في المقابل تحديات قانونية وعملية، خاصة فيما يتعلق بضمان احترام الحريات الفردية وحماية الحق في الخصوصية. كما تبين أن الدليل الرقمي أصبح يمثل محوراً أساسياً في إثبات الجرائم المعلوماتية، نظراً لاعتماد هذه الجرائم على البيانات الإلكترونية والآثار الرقمية التي يتركها الجاني أثناء ارتكاب الفعل الإجرامي، إلا أن خصوصية هذا الدليل تفرض ضرورة احترام مجموعة من الشروط المتعلقة بجمعه وحفظه وتحليله، حتى يحافظ على قيمته القانونية أمام الجهات القضائية.

وقد كشفت الدراسة كذلك أن مرحلة البحث والتحقيق في الجرائم الإلكترونية تواجه مجموعة من الصعوبات، من أبرزها سرعة اختفاء الأدلة الرقمية، وإمكانية تغييرها أو إتلافها، إضافة إلى تعقيد تحديد مصدر الهجمات الإلكترونية خاصة عندما تكون مرتكبة عبر شبكات عابرة للحدود، لذلك أصبح التعاون بين الجهات الأمنية والقضائية والمؤسسات التقنية أمراً ضرورياً لتعزيز فعالية المواجهة الجنائية.

وبناءً عليه، فإن نجاح السياسة الجنائية في مواجهة الجرائم الإلكترونية لا يتوقف فقط على وجود نصوص قانونية تجرم الأفعال غير المشروعة، وإنما يتطلب أيضاً تطوير البنية التقنية للأجهزة المختصة، وتعزيز التكوين المتخصص، ووضع آليات إجرائية تتلاءم مع خصوصية البيئة الرقمية، بما يحقق التوازن بين فعالية العدالة الجنائية واحترام الحقوق الأساسية للأفراد.

خاتمة

خاتمة

خاتمة

أصبح التطور المتسارع في مجال تكنولوجيا المعلومات أحد أبرز التحولات التي أثرت بصورة عميقة في مختلف جوانب الحياة المعاصرة، حيث لم يعد الاعتماد على الأنظمة الرقمية مقتصراً على المجالات الاقتصادية والإدارية فقط، بل امتد ليشمل المجال الأمني والقضائي، مما أدى إلى إعادة تشكيل مفهوم الأمن الجنائي ومهامه. فقد ساهمت التكنولوجيا الحديثة في تطوير وسائل الوقاية والكشف عن الجرائم، وتوفير أدوات أكثر فعالية لملاحقة الجناة، غير أنها في المقابل أوجدت بيئة جديدة لظهور أنماط إجرامية مستحدثة تتميز بالتعقيد والسرعة وصعوبة الإثبات.

ومن خلال دراسة موضوع **تأثير تكنولوجيا المعلومات على الأمن الجنائي**، يتضح أن العلاقة بين التكنولوجيا والجريمة أصبحت علاقة مزدوجة؛ فهي من جهة تمثل وسيلة متطورة لتعزيز قدرات أجهزة إنفاذ القانون وتطوير آليات البحث والتحقيق والإثبات، ومن جهة أخرى أصبحت أداة تستعمل في ارتكاب جرائم خطيرة تمس الأفراد والمؤسسات وحتى أمن الدول. فقد أدى الانتشار الواسع للأنظمة المعلوماتية وشبكات الاتصال إلى ظهور جرائم تستهدف البيانات الرقمية والأنظمة المعلوماتية، مثل الاختراق غير المشروع، والتلاعب بالمعطيات، وسرقة المعلومات، والتجسس الإلكتروني، والاعتداء على الخصوصية الرقمية. وقد تدخل المشرع الجزائري لمواجهة هذه الأفعال من خلال تجريم الاعتداءات الواقعة على أنظمة المعالجة الآلية للمعطيات ووضع إطار قانوني خاص للجرائم المعلوماتية.

وقد توصلت الدراسة إلى مجموعة من النتائج الأساسية، من أهمها أن تكنولوجيا المعلومات أحدثت تحولاً جوهرياً في مفهوم الأمن الجنائي، فلم يعد هذا الأخير يقتصر على مكافحة الجرائم التقليدية، وإنما أصبح يشمل حماية البيئة الرقمية باعتبارها مجالاً جديداً للمصالح القانونية الجديرة بالحماية. كما تبين أن الجرائم المعلوماتية تتميز بخصوصية تجعل مواجهتها أكثر صعوبة، بسبب اعتمادها على وسائل تقنية متطورة، وسرعة تنفيذها، وإمكانية ارتكابها من خارج الحدود الإقليمية للدولة، فضلاً عن صعوبة تحديد هوية مرتكبيها.

كما أظهرت الدراسة أن المشرع الجزائري بذل جهوداً معتبرة في مجال مكافحة الجرائم الإلكترونية، سواء من خلال تعديل قانون العقوبات وإدراج نصوص خاصة بالمساس بأنظمة المعالجة الآلية للمعطيات، أو من خلال وضع قواعد قانونية لحماية المعطيات ذات الطابع الشخصي والوثائق الإلكترونية. إلا أن هذه الحماية تبقى بحاجة إلى التطوير المستمر بالنظر إلى التطور السريع للتكنولوجيا وظهور أساليب إجرامية جديدة تتجاوز أحياناً نطاق النصوص القانونية القائمة.

ومن النتائج المهمة كذلك أن الجانب الإجرائي للأمن الجنائي عرف تحولاً كبيراً بفعل التكنولوجيا، حيث أصبح التحقيق الجنائي يعتمد بصورة متزايدة على الوسائل الرقمية والأدلة الإلكترونية. وقد أصبح الدليل الرقمي عنصراً أساسياً في إثبات الجرائم المعلوماتية، غير أن فعاليته ترتبط بمدى احترام القواعد الفنية والقانونية المتعلقة بجمعه وحفظه وتحليله، بما يضمن سلامته وعدم تعرضه للتغيير أو التلاعب.

خاتمة

كما كشفت الدراسة أن مواجهة الجرائم الإلكترونية لا يمكن أن تتحقق بالاعتماد على الجانب العقابي وحده، وإنما تتطلب سياسة جنائية متكاملة تجمع بين التجريم والعقاب من جهة، والوقاية والتوعية والتكوين والتعاون التقني من جهة أخرى. فالتطور التكنولوجي يفرض على الدولة تطوير قدراتها المؤسساتية وتعزيز التنسيق بين مختلف الجهات الأمنية والقضائية والتقنية.

ورغم أهمية الجهود المبذولة، فقد أظهرت الدراسة وجود مجموعة من النقائص التي تحد من فعالية الحماية الجنائية، من أبرزها عدم قدرة بعض النصوص القانونية على مواكبة التطورات التقنية المتسارعة، خاصة الجرائم المرتبطة بالذكاء الاصطناعي، والحوسبة السحابية، والهجمات الإلكترونية المعقدة. كما يلاحظ وجود حاجة إلى مزيد من التخصص في مجال التحقيق الرقمي، سواء بالنسبة لأفراد الشرطة القضائية أو القضاة، إضافة إلى محدودية الإمكانيات التقنية المتاحة لبعض الجهات المكلفة بمكافحة الجرائم الإلكترونية.

كما تتمثل إحدى النقائص في الطبيعة العابرة للحدود للجرائم المعلوماتية، إذ قد يكون الفاعل في دولة، والخادم الإلكتروني في دولة أخرى، والضحية في دولة ثالثة، مما يجعل التعاون الدولي ضرورة حتمية وليس مجرد خيار. لذلك فإن فعالية المواجهة الجنائية تتطلب تعزيز الاتفاقيات الدولية وتبادل الخبرات والمعلومات بين الدول لملاحقة مرتكبي الجرائم الإلكترونية.

وبناءً على النتائج المتوصل إليها، يمكن تقديم مجموعة من الاقتراحات، تتمثل أساساً في:

– ضرورة تحديث التشريعات الجنائية المتعلقة بالجرائم الإلكترونية بصورة مستمرة، بما يضمن استيعاب التطورات التقنية الجديدة وتحديد الأفعال المجرمة بدقة أكبر

–تعزيز التكوين المتخصص للقضاة وأفراد الضبطية القضائية في مجال الأمن السيبراني والتحقيق الرقمي، وإنشاء وحدات تقنية متخصصة قادرة على التعامل مع الأدلة الإلكترونية بكفاءة عالية.

– بتطوير البنية التقنية لمؤسسات العدالة والأمن، واعتماد أنظمة حديثة لحماية المعلومات والبيانات، إضافة إلى تعزيز التعاون بين الدولة والقطاع الخاص، خاصة المؤسسات المتخصصة في التكنولوجيا والاتصالات

–نشر ثقافة الأمن الرقمي لدى مستخدمي التكنولوجيا، باعتبار أن الوقاية والتوعية تمثلان خط الدفاع الأول في مواجهة الجرائم الإلكترونية.

وفي الأخير، يمكن القول إن تأثير تكنولوجيا المعلومات على الأمن الجنائي يمثل ظاهرة مركبة تجمع بين فرص التطوير ومخاطر الاستغلال الإجرامي، الأمر الذي يجعل تحقيق الأمن في البيئة الرقمية رهيناً بمدى قدرة المنظومة القانونية والمؤسساتية على التكيف مع التحولات التكنولوجية. ومن ثم فإن بناء أمن جنائي فعال في العصر الرقمي يتطلب رؤية متكاملة تقوم على تحديث التشريع، وتطوير القدرات التقنية، وتعزيز التعاون، بما يضمن حماية المجتمع ومواكبة متطلبات العصر الرقمي.

المصادر

والمراجع

المصادر والمراجع

القوانين والاوامر

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
3. القانون رقم15-03 المتعلق بعصرنة العدالة، المؤرخ في 01 فبراير 2015 ،ج ر.ج ج العدد6 ، الصادر في 10 فبراير. 2015
4. الأمر رقم 15-02 المؤرخ 23 جويلية 2015 ، يعدل ويتمم الأمر رقم 515 - 66 المؤرخ في 8 جوان 1966المتضمن قانون الإجراءات الجزائية ،ج ر.ج ج العدد 4 الصادر بتاريخ 23 جويلية. 2015
5. الامر 21-09 مؤرخ في 27 شوال عام 1442 الموافق 8 يونيو سنة 2021 ، يتعلق بحماية المعلومات والوثائق الإدارية ، ج.ر.ج.ج، ع 45 ، الصادرة بتاريخ 28 شوال عام 1442 الموافق 9 يونيو سنة 2021،
6. القانون رقم 25-11 مؤرخ في 28 محرم عام 1447 الموافق لـ 24 يوليو سنة 2025 معدل ومتمم للقانون 18-07 المؤرخ في 10 يونيو سنة2018 ، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية، العدد48 ، الصادرة بتاريخ 2025/07/24
7. القانون 22-13 مؤرخ في 13 ذي الحجة عام 1443 الموافق لـ 12 يوليو 2022 يعدل ويتمم القانون 08-09 المؤرخ في 18 صفر 1429 الموافق 25 فبراير 2008 المتضمن قانون الإجراءات المدنية والإدارية الجزائري، الجريدة الرسمية العدد 48 مؤرخة في 17 يوليو 2022

المراسيم

1. المرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية العدد 53، 8 أكتوبر 2015، ص ص 16-17
2. المرسوم الرئاسي رقم26-07 مؤرخ في 7 جانفي 2026 يتضمن إنشاء هيكل مسؤول عن أمن الأنظمة المعلوماتية وحماية المعطيات في المؤسسات والإدارات والهيئات العمومية، وتحديد مهامه وتنظيمه وسيره، ج.ر العدد04 الصادرة بتاريخ2023/01/18.

المصادر والمراجع

الكتب

1. أحسن بوسقيعة، **الوجيز في القانون الجزائي الخاص، الجزء الأول، الجرائم ضد الأشخاص ووالجرائم ضد الأموال**، الطبعة الثالثة، دار هومة، الجزائر، 2006
2. امال قارة، **الحماية الجزائية للمعلوماتية في التشريع الجزائري**، دار هومة،2007 ، الجزائر
3. بن مكي نجاة، **السياسة الجنائية لمكافحة الجرا ئم المعلوماتية**، دار الخلدونية، الجزائر،2017
4. طاهري حسين، **الإعلام والقانون(دراسة مقارنة)**، دون طبعة، دار الهدى للنشر والطباعة، الجزائر،2014
5. عبد الفتاح بيومي الحجازي، **مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي(دراسة قانونية متعمقة في القانون المعلوماتي)**، دار الكتب القانونية، مصر،2007
6. عبد الله أوهابية، **شرح قانون الإجراءات الجزائية، التحري والتحقيق**، ط2، دار هومة،2011
7. كمال بوشليق، **جريمة القذف بين القانون والإعلام(دراسة تحليلية مقارنة مدعمة باجتهاد القضائي للرجال القضاء الإعلام على ضوء قانون العقوبات والإعلام)** ، دون طبعة، دار الهدى للطباعة والنشر والتوزيع، الجزائر، 2010
8. محمد صبحي نجم، **شرح قانون العقوبات الجزائري " القسم الخاص"** ، بدون طبعة، ديوان المطبوعات الجامعية، الجزائر،2006
9. مصطفى محمد موسى،**التحقيق الجنائي في الجرائم الالكترونية** ،الطبعة الأولى، مصر ، 2009
10. يونس محمد غانم، **الابتزاز الإلكتروني" دراسة من وجهة نظر قانونية"**، ضمن مؤلف :الابتزاز الالكتروني جريمة العصر الحديث، إصدار :وزارة الداخلية العراقية، بغداد :دار الكتب والوثائق،2019

المقالات والمداخلات

1. بكايس سمية، **التقاضي الالكتروني ومدى فعاليته في النظام القضائي الجزائري**، مجلة البصائر للدراسات القانونية والاقتصادية، المجلد03، العدد01، 2021
2. بلحسن ريم، بولباري أحمد، **الحق في خصوصية المعطيات الشخصية في التشريع الجزائري، دراسة في ظل القانون رقم18-07**، مجلة العلوم القانونية والاجتماعية، جامعة زيان عاشور بالجلفة الجزائر، المجلد 05، العدد 03 سبتمبر2020
3. بن حاجة أحمد، **القانون 18-07 المعدل والمتمم كآلية لحماية المعطيات ذات الطابع الشخصي**، مجلة المعيار، المجلد 16، العدد02، 2025
4. بن حميد صالح، **الابتزاز (المفهوم والواقع) –** ورقة بحثية مقدمة في ندوة الابتزاز المفهوم، الأسباب، العلاج، 7 – 8 مارس 2011 : جامعة الملك سعود، المملكة العربية السعودية

5. بن عزوز أحمد، **نظام المحاكمة الالكترونية وفقا لأحكام قانون عصرنة العدالة15-03**، مجلة البصائر للدراسات القانونية والاقتصادية، عدد خاص، كلية الحقوق، جامعة بلحاج بوشعيب، عين تموشنت، الجزائر، ديسمبر 2021

6. بوبرقيق عبد الرحيم، **مفهوم انظمة المعالجة الالية في الجرائم المحددة في المواد 394 مكرر الى 394 مكرر 02 من قانون العقوبات الجزائري**، مجلة الدراسات والبحوث القانوني، المجلد 04، العدد01، جوان، 2019

7. بوزيرة سهيلة، **الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا ت الاعلام والاتصال بين سرية المعطيات الشخصية الالكترونية ومكافحة الجرائم الاالكترونية**، المجلة النقدية للقانون والعلوم السياسية، المجلد 17، العدد02، 2022

8. حايطي فاطمة، هروال نبيلة هبة، **نظام التقاضي الالكتروني بين تحسين جودة العمل القضائي وتحديات الفضاء الرقمي**، مجلة الدراسات القانونية المقارنة، المجلد7 ، العدد الأول، كلية الحقوق والعلوم السياسية، جامعة حسيبة بن بوعلي الشلف، الجزائر،2021

9. حديدان سفيان، **الدخول أو البقاء عن طريق الغش في نظام المعالجة الآلية للمعطيات**، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد الثامن، المجلد الثاني، ديسمبر، 2017،

10. حزام فتيحة، **الضمانات القانونية لمعالجة المعطيات ذات الطابع الشخصي، دراسة على ضوء القانون رقم 07/18**، مجلة الإجتهاد للدراسات القانونية والاقتصادية، المجلد 8، العدد4 لسنة 2019

11. حنصالي صابرينة، **حماية المعطيات ذات الطابع الشخصي للمتعاقد الالكتروني : نحو تحقيق الأمن السيبراني**، المجلة الجزائرية للعلوم القانونية والسياسية، كلية الحقوق، جامعة الجزائر 01، المجلد 59، العدد 02، جوان 2022

12. الدهبي خدوجة، **حق الخصوصية في مواجهة الاعتداءات الالكترونية دراسة مقارنة**، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة أحمد دراية، أدرار، المجلد 01، ع 08، ديسمبر، 2017

13. رابح وهيبة، **الجريمة المعلوماتية في التشريع الإجرائي الجزائري**، مجلة الباحث للدراسات الأكاديمية، العدد الرابع، ديسمبر 2014

14. رابحي عزيزة، طاهري محمد بشار، **العنصر المفترض في جريمة الدخول أو البقاء غير المصرح به للنظام المعلوماتي**، المجلة الجزائري للدراسات والتاريخية والقانونية، العددين 01و02، جانفي- جوان، 2016

15. رشا علي الدين، **أمل ماهر جبر، محمد مجدي قاسم، أحمد الحسنين كرم الدين، علا ماهر جبر، منى عماد الدين الشيمي، ندى ضيف السيد لبيب، " رقمنة القضاء "التجارب العربية**" "، مجله البحوث القانونية والاقتصادية، جامعة المنصورة، عدد 23، 2024

16. سعاد بنور، **الأقطاب الجزائية المتخصصة بين الاستراتيجية الوطنية والتعاون القضائي الدولي لمكافحة جرائم الفساد**، مجلة أبحاث قانونية وسياسية، العدد التاسع /ديسمبر 2019
17. طباش عز الدين، **الحماية الجزائية للمعطيات الشخصية في التشريع الجزائري، دراسة في ظل قانون 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي**، المجلة الأكاديمية للبحث القانوني، جامعة بجاية، العدد 2، 2018،
18. عباسي محمد حبيب، **الحماية الجزائية للمعلومات والوثائق الادارية من خلال الأمر 21-09**، مجلة القانون والعلوم السياسية، المجلد 09، العدد01، 2023.
19. عبد الكريم بوخالفة، " **نحو قضاء إداري إلكتروني في الجزائر** "، مجلة دفاتر السياسية والقانون، جامعة ورقلة، المجلد 15، العدد 2، الجزائر، 2023،
20. العيداني محمد، يوسف زروق، **حماية المعطيات لشخصية في الجزائر على ضوء القانون رقم 07/18 (المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي)**، مجلة معالم للدراسات القانونية والسياسية، المركز الجامعي تندوف، العدد5، ديسمبر 2018
21. غربي صورية، **نظام التقاضي الالكتروني في القانون الجزائري**، المجلة النقدية للقانون والعلوم السياسية كلية الحقوق والعلوم السياسية – جامعة تيزي وزو، الجزائر، المجلد 18، العدد01، 2023
22. مباركية مفيدة، **الحماية الجنائية للحق في الخصوصية الرقمية في القانون الجزائري**، مجلة الشريعة والاقتصاد جامعة قسنطينة، الجزائر، العدد 13، 2018
23. هاشمي رشيدة، ملياني عبد الوهاب، **المواجهة التشريعية لجريمة التجسس الالكتروني في ظل القانون24-06**، مجلة الفكر القانوني والسياسي، المجلد09، العدد01، 2025
24. وردة حميزي، فايزة دحموش، " **التقاضي الإداري الإلكتروني في الجزائر** "، مجلة الاجتهاد القضائي، جامعة محمد خيضر بسكرة، مجلد 15، عدد 2، 2023 الجزائر،
25. يوسف مباركة، حنان عكوش، " **التقاضي الإلكتروني في الجزائر** "، مجلة الحقوق والعلوم الإنسانية، جامعة عمار ثليجي أغواط، المجلد 15، العدد 1، الجزائر، 2022

المذكرات

1. إبراهيم محمد القاسمي، **جرائم الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات الإلكترونية (وفقا للمرسوم بقانون اتحادي رقم 05 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات وتعديلاته)**، أطروحة مقدمة لاستكمال متطلبات الحصول على درجة الماجستير في القانون العام، جامعة الإمارات العربية المتحدة، كلية القانون، نوفمبر 2018
2. بن عيسى كهينة، برانسي سليمة، **جريمة القذف بين قانون وقانون الاعلام**، مذكرة تخرج لنيل شهادة الماستر في الحقوق، تخصص القانون الخاص والعلوم الجنائية، جامعة عبد الرحمان ميرة – بجاية– 2015-2014

3. بوخنوفة شهيناز، **التقاضي الإلكتروني في القضاء الإداري الجزائري**، مذكرة ماستر في الحقوق، تخصص :قانون عام، جامعة محمد الصديق بن يحي جيجل- الجزائر، 2024-2025
4. بوريش فواد، **حرية التعبير وجرائم الصحافة**، مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر،2006-2009
5. جدي نسيمة، **جرائم المساس بأنظمة المعالجة الالية للمعطيات**، مذكرة ماجستير في القانون الجنائي، كلية الحقوق، جامعة وهرا ن،2014 - 2013
6. جميلة خلفي ،**مبادئ الشرعية الإجرائية للمحاكمة الجزائية دراسة قانونية وفق القانون 17-07**، مذكرة لإستكمال متطلبات شهادة ماستر أكاديمي حقوق تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة غرداية ،2017-2018
7. را بحي عزيزة، **الاسرار المعلوماتية وحمايتها الجزائية**، أطروحة مقدمة لنيل شهادة دكتوراه علوم في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان، 2017-2018
8. ساره محمد حنش، **المسؤولية الجزائية عن التهديد عبر الوسائل الإلكترونية دراسة مقارنة**، مذكرة الماجستير في القانون العام، جامعة الشرق الأوسط، 2020،
9. سليمان نعيمة، **المسؤولية الجزائية في جرائم الصحافة المكتوبة**، مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، المدرسة العليا للقضاء، الجزائر،2007-2010
10. الطيبي البركه، **الحماية الجنائية لنظام المعالجة الآلية للمعطيات دراسة مقارنة**، رسالة مقدمة لاستكمال متطلبات الحصول على شهادة دكتوراه الطور الثالث تخصص قانون جنائي، جامعة أحمد دراية، ادرار، 2020-2021
11. عبد الرحيم ريمة ، **جرائم الصحافة**، مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء الجزائر،2007-2010
12. عبدلي حمزة، **المسؤولية الجزائية عن افشاء اسرار الوظيفة العمومية**، اطروحة دكتوراه، تخصص: قانون اداري، جامع بن يوسف بن خدة، جامعة الجزائر، 2019-2020
13. علي أحمد رشيدة، **الحق في الإعلام وجنح الصحافة**، بحث لنيل درجة الماجستير في القانون الدولي لحقوق الإنسان كلية الحقوق، جامعة مولود معمري، ت زي وزو،2001-2002
14. عياط سارة، **جريمة القذف على شبكة الانترنت**، مذكرة مكملة من مقتضيات نيل شهادة الماستر حقوق تخصص القانون الجنائي،جامعة محمد خيضر- بسكرة-2014/2013،
15. فوزي لواقي، **التحقيق في جرائم المخدرات على ضوء أساليب التحري الخاصة**، رسالة ماجيستير فرع القانون الجنائي، كلية الحقوق جامعة الجزائر 1، 2014/2015

16. مريم محمد الشامسي، **نظام التقاضي عن بعد وفقا لقانون الإجراءات المدنية الإماراتي**، مذكرة مقدمة لنيل درجة الماجستير في القانون، تخصص قانون خاص، كلية القانون، جامعة الامارات العربية المتحدة، 2022

الفهرس

الفهرس

ملخص

ملخص

تهدف هذه الدراسة إلى تحليل تأثير تكنولوجيا المعلومات على الأمن الجنائي، من خلال بيان التحولات التي أحدثتها البيئة الرقمية في طبيعة الجريمة ووسائل مكافحتها. فقد أدى التطور التكنولوجي إلى ظهور أنماط جديدة من الجرائم تمس الأنظمة المعلوماتية والبيانات الرقمية والخصوصية الإلكترونية، الأمر الذي فرض تحديات جديدة أمام المشرع والجهات الأمنية والقضائية. وقد تناولت الدراسة الجانب الموضوعي من خلال تحليل الجرائم المعلوماتية وصورها المختلفة، كما تناولت الجانب الإجرائي من خلال إبراز دور التكنولوجيا في تطوير إجراءات البحث والتحقيق والإثبات الجنائي.

وقد توصلت الدراسة إلى أن تكنولوجيا المعلومات تمثل عاملاً مزدوج التأثير على الأمن الجنائي، فهي من جهة ساهمت في تطوير وسائل مكافحة الجريمة وتعزيز فعالية التحقيقات، ومن جهة أخرى أوجدت مخاطر إجرامية جديدة تتميز بالتعقيد وصعوبة الإثبات. كما تبين أن فعالية المواجهة الجنائية للجرائم الإلكترونية تتطلب تطوير النصوص القانونية، وتعزيز التكوين المتخصص، وتوفير الوسائل التقنية الحديثة، إضافة إلى دعم التعاون الدولي ونشر الوعي بالأمن الرقمي.

الكلمات المفتاحية: تكنولوجيا المعلومات – الأمن الجنائي – الجرائم الإلكترونية.

Abstract

This study aims to analyze the impact of information technology on criminal security, by demonstrating the transformations brought about by the digital environment in the nature of crime and the means of combating it. Technological development has led to the emergence of new types of crimes affecting information systems, digital data, and electronic privacy, which has imposed new challenges before the legislator, security and judicial authorities. The study addressed the objective aspect by analyzing information crimes and their various forms. It also addressed the procedural aspect by highlighting the role of technology in developing criminal research, investigation, and proof procedures.

The study concluded that information technology represents a dual factor that has a double impact on criminal security. On the one hand, it has contributed to developing means of combating crime and enhancing the effectiveness of investigations, and on the other hand, it has created new criminal risks that are characterized by complexity and difficulty of proof. It has also been shown that the effectiveness of criminal confrontation with cybercrimes requires developing legal texts, enhancing specialized training, and providing modern technical means, in addition to supporting international cooperation and spreading awareness of digital security.

Keywords: information technology - criminal security - cybercrime