جامعة غليزان
RELIZANE UNIVERSITY

جامعة أحمد زبانة غليـــــزان

كلية الحقـــــوق

قسم القانون العام

محاضرات في مقياس:

" علم الاجرام المعلوماتي "

موجهة لطلبة السنة الثانية ماستر قانون جنائي وعلوم جنائيه

من اعداد وتقديم

د. يوسفي عبدالهادي

أستاذ محاضر أ

لجنة التحكيم

أد/ الجيلالي حسين	جامعة غليزان
د/ عقاب لزرق	جامعة غليزان
أد/ بن لخضر محمد	المركز الجامعي البيض

السنة الجامعية: 2026/2025

مقدمة

أصبحت الجريمة المعلوماتية من أبرز التحديات القانونية والأمنية التي تواجه المجتمعات المعاصرة، نتيجة التطور الهائل في مجال تكنولوجيا المعلومات والاتصال، والاعتماد المتزايد على الأنظمة الرقمية في مختلف القطاعات الحيوية. فقد أفرز هذا التطور أنماطًا إجرامية جديدة تعتمد على الوسائل الإلكترونية، ولم تعد الجرائم تقتصر على الأساليب التقليدية المعروفة، بل انتقلت إلى الفضاء الافتراضي، مستهدفة الأفراد والمؤسسات وحتى الدول.

وتُعد الجريمة المعلوماتية من الجرائم المستحدثة التي تُرتكب باستخدام الحاسوب أو الشبكات المعلوماتية، سواء كان ذلك باعتبار النظام المعلوماتي هدفًا للجريمة، أو وسيلة لارتكابها، وتشمل هذه الجرائم أفعالًا متعددة مثل الدخول غير المشروع إلى الأنظمة، والاعتداء على سلامة البيانات، وسرقة المعلومات، والاحتيال الإلكتروني، وانتهاك الحياة الخاصة، ونشر البرمجيات الضارة، إضافة إلى الجرائم المرتبطة بالمساس بأمن الدولة عبر الوسائط الرقمية.

وتتميز الجريمة المعلوماتية بخصائص تجعل مكافحتها أمرًا معقدًا، من بينها طابعها التقني، وسرعة تنفيذها، وصعوبة اكتشافها وإثباتها، فضلًا عن كونها غالبًا ما تتجاوز الحدود الجغرافية، الأمر الذي يفرض تحديات كبيرة على أجهزة العدالة الجنائية. كما أن مرتكبي هذا النوع من الجرائم غالبًا ما يتمتعون بمهارات تقنية عالية، ما يستدعي وسائل تحقيق خاصة وكفاءات متخصصة.

وإدراكًا لخطورة هذه الجرائم وآثارها السلبية على الأمن الاقتصادي والاجتماعي، أولى المشرّع الجزائري اهتمامًا خاصًا بالجريمة المعلوماتية، حيث سعى إلى مواكبة التطورات التكنولوجية من خلال سنّ نصوص قانونية تهدف إلى الوقاية منها وقمعها. وقد تبنّى المشرّع الجزائري سياسة جنائية حديثة تقوم على تجريم الأفعال التي تمس بالأنظمة المعلوماتية والبيانات الرقمية، مع تشديد العقوبات في الحالات التي تمس بالأمن الوطني أو بالمصالح الحيوية للدولة.

كما حرص المشرّع الجزائري على تعزيز الإطار القانوني المتعلق بحماية المعطيات ذات الطابع الشخصي، وضمان أمن الأنظمة المعلوماتية، إلى جانب تمكين السلطات المختصة من آليات قانونية للتحري والمتابعة، مع احترام الحقوق والحريات الأساسية.

ويعكس هذا التوجه وعي المشرّع الجزائري بخطورة الجريمة المعلوماتية وضرورة التصدي لها من خلال مزيج من التشريع، والتعاون الدولي، والتدابير التقنية.

ويمكن القول إن الجريمة المعلوماتية تمثل تهديدًا حقيقيًا للأمن والاستقرار في المجتمع الرقمي، الأمر الذي يجعل من مكافحتها أولوية تشريعية وأمنية، تتطلب تحديث القوانين باستمرار ومواكبة التطورات التكنولوجية، وهو ما سعى إليه المشرّع الجزائري في إطار سياسته الجنائية الحديثة

المحور الأول: الاطار المفاهيمي للجريمة المعلوماتية

سيتم التطرق من خلال هذا المحور إلى الى مفهوم الجريمة المعلوماتية و تبيان خصائصها وأطرافها

المبحث الأول: مفهوم الجريمة

تعتبر الجريمة المعلوماتية من بين الجرائم التي تعتمد على التقنية المعلوماتية

المطلب الأول: تعريف الجريمة

تعدّدت تعاريف الجريمة المعلوماتية لغياب مصطلح موحّد لها، وذلك بسبب حداثة هذا النوع من الجرائم وتسارع تطور تقنيات المعلومات والاتصال واختلاف الزوايا القانونية والتقنية في دراستها، وقد نتج عن ذلك تعدد التسميات كالجريمة الإلكترونية وجرائم الحاسوب والإنترنت والجرائم السيبرانية، وكلها تشير إلى سلوك إجرامي يُرتكب باستخدام النظم المعلوماتية أو يكون موجّهًا ضدها.

الفرع الأول: التعريف الفقهي للجريمة المعلوماتية

تعددت التعاريف الفقهية الخاصة بالجريمة المعلوماتية وفق الزاوية التي ينظر منا كل اتجاه فقهي

أولا: تعريفات تربط بين الوسيلة التقنية المستخدمة في ارتكاب الجريمة والوصف القانوني الذي يجرّم هذا الفعل.

يذهب أنصار هذا الاتجاه إلى أن الجريمة المعلوماتية تُعد نشاطًا إجراميًا تُستخدم فيه تقنية الحاسب الآلي بصورة مباشرة أو غير مباشرة، سواء كوسيلة لتنفيذ الفعل الإجرامي أو كهدف يقع عليه الاعتداء، ويركّز هذا الاتجاه على الجانب التقني في تعريف الجريمة المعلوماتية، معتبرًا أن الحاسب الآلي يمثل العنصر الجوهري في وقوعها[1].

كما يرى أنصار هذه النظرية بأن الجريمة المعلوماتية هي كل نشاط إجرامي يؤدي فيه نظام الحاسب الألي دورا لإتمامه على أن يكون هذا الدور على قدر من الأهمية و لا يختلف الأمر سواء أكان الحاسب الألي لاتمام النشاط الإجرامي أو كان محلا له[2]

[1] – BROWN S. D. Cameron , Investigating and Prosecuting Cyber Crimes, international journal of cyber criminology, Vol. 9, Issue1, June 2015, p. 57

[2]–حسين طاهري، الجرائم الألكترونية، الطبعة 01، دار الخلدونية، الجزائر،2021،، ص ص 08.09

ثانيا: تعريف الجريمة الالكترونية الذي يرتكز على موضوع الجريمة

لم يركّز أنصار هذا الاتجاه على الوسيلة المستخدمة في الجريمة، بل على موضوع الجريمة نفسه .فالجريمة المعلوماتية ليست مجرد استخدام الحاسب الآلي كأداة، بل هي جريمة تقع على الحاسب الآلي أو داخل نظامه[1]..

وعرفها الفقيه روزبلانت بأنها عبارة" عن نشاط غير مشروع موجه لنسخ أو تغيير أوحذف أو الوصول إلى المعلومات المخزنة داخل الكومبيوتر أو تلك التي يتم تحويلها عن طريقه"[2]

وقد عرّفها أنصار هذا الاتجاه بأنها نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة في الحاسب أو التي تمر عبره .كما عُرفت بأنها غش معلوماتي يشمل كل سلوك غير مشروع يتعلق بالمعلومات المعالجة ونقلها[3].

حيث عرفتها مجموعة من خبراء منظمة التعاون الاقتصادي والتنمية (OECD) على النحو التالي: "كل فعل أو امتناع يؤدي بطريقة مباشرة أو غير مباشرة، عن تدخل التقنية المعلوماتية، إلى الاعتداء على الأموال المادية أو المعنوية". كما عرفتها المنظمة في عام 1983 بقولها: "كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقله[4].

ثالثا: تعريفات تعتمد على السمات الخفية للجريمة المعلوماتية

ويؤكد هذا الاتجاه أن من أبرز سمات هذه الجريمة أنها جريمة خفية تتسم بالسرعة والتطور في وسائل ارتكابها، وهي أقل عنفًا مقارنة بالجرائم التقليدية، كما أنها عابرة للحدود ويصعب إثباتها بسبب قلة الأدلة المادية عليها، بالإضافة إلى سهولة إتلاف هذه الأدلة، ونقص الخبرة العلمية لدى الجهات المختصة بضبطها، وعدم كفاية القوانين القائمة لمعالجتها. ومع ذلك، ينتقد بعض الباحثين هذا التعريف لقصوره، إذ لا يشير بشكل

– [1]د/ عبد الفتاح بيومي حجازي مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، دار الفكر الجامعي، الإسكندرية، 2006، ص20

[2]–مواسة صونية نادية، خصوصية الجريمة المعلوماتية، بحث منشور ضمن مؤلف جماعي تخت عنوان الجريمة الالكترونية، 2019، ص 187.

[3]–فتيحة رصاع، الحماية الجنائية للمعلومات على شبكة الانترنيت، رسالة ماجستير في القانون العام، كلية الحقوق و العلوم السياسة،، جامعة أبو بكر بلقايد، تلمسان، الجزائر،/2012/2011، ص 40.

[4]– ياسمينة بونعارة، الجريمة الإلكترونية، مجلة المعيار، العدد،26 جامعة الأمير عبد القادر للعلوم الإسلامية ، قسنطينة، 2015، ص 276.

واضح إلى وقوع الجريمة المعلوماتية على شبكة الإنترنت في حالات مثل تعطيل الشبكة عن العمل، أو التسبب في بطء سرعتها، أو إتلاف المواقع الإلكترونية[1].

رابعا: تعريف يستند الى صفات المجرم

عرفت وزارة العدل في الولايات المتحدة الأمريكية الجريمة المرتكبة عبر الإنترنت بأنها كل جريمة لفاعلها معرفة فنية بتقنية الحاسبات تمكنه من ارتكابها[2].

كما عرفت على أنها " تلك الجرائم التي تقع على شبكة الأنترنيت أو بواسطتها من قبل شخص ذي معرفة تقنية[3]

ويعتمد هذا الاتجاه في تعريفه للجريمة على معيار شخصي يتمثل في مدى إلمام الجاني بتقنية المعلومات. ومع ذلك، تظهر نقاط القصور في هذا التعريف، إذ أن معرفة الجاني وحدها لا تكفي لتحديد الجريمة الإلكترونية، فقد يتمكن أي شخص عادي، غير متخصص في تقنيات الحاسب الآلي، من ارتكاب جرائم مثل الغش المعلوماتي أو السرقة المعلوماتية، مما يجعل الاعتماد على الجانب الشخصي للفاعل تعريفًا محدودًا وغير شامل لطبيعة الجرائم الإلكترونية[4].

خامسا: الارتكاز على الجانب الموضوعي للجريمة

تبنّت بعض التعريفات الجانب الموضوعي للجريمة المعلوماتية، حيث اعتبرت أن هذه الجريمة لا تعتمد على استخدام الحاسب الآلي باعتباره أداة لارتكاب الجريمة، وإنما تقع هذه الأخيرة على الحاسب الآلي ذاته أو داخل أنظمته، إذ يكون محل الاعتداء هو البيانات أو المعلومات المخزنة فيه أو المعالجة من خلاله، ومن هذه التعريفات أن الجريمة الالكترونية هي " نشاط غير مشروع موجه لنسخ أو تغيير أو حذغ أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو التي تحول عن طريقه"[5]،

---

[1]– د/ عبد الفتاح بيومي حجازي، مرجع سابق، ص 24.

[2]– -محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، دار النهضة العربية، القاهرة، ص.34

[3]–حسين طاهري، كرجع سبق ذكره، ص 09.

[4]– رحيمة نمديلي، "خصوصية الجريمة الالكترونية في القانون االجزائري و القوانين المقارنة"، كتاب أعمال المؤتمر الدولي الرابع عشر: الجرائم الالكترونية، مركز جيل البحث العلمي، طرابلس، لبنان، 24–25 مارس 2017، ص ص: 99.

[5]– مناصرة يوسف جرائم المساس بأنظمة المعالجة الألية للمعطيات، دار الخلدونية، الجزائر،2018، ص 29

وقد عرّفت الجريمة المعلوماتية بأنها نشاط غير مشروع يتمثل في نسخ أو تعديل أو حذف أو إتلاف أو الوصول غير المصرح به إلى المعلومات أو البيانات المخزنة داخل الحاسب الآلي أو تلك التي يتم نقلها أو معالجتها عن طريقه[1].

وفي الاتجاه ذاته عرّفها الأستاذ الخبير الأمريكي دون باركر" كل فعل اجرامي متعمد أي كانت صلته بالمعلوماتية ينشأ عن خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل"[2].

الفرع الثاني: تعريف الجريمة المعلوماتية في القانون الدولي و الوطني

لقد تبنت التشريعات الدولية سواء العالمية أو الاقليمية و الوطنية عدة تعريفات للجريمة المعلوماتية

أولا: تعريف الجريمة المعلوماتية لدى المنظمات الدولية

وقد أولى مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين، المنعقد عام 2000، اهتمامًا خاصًا بمسألة تحديد مفهوم الجريمة الإلكترونية باعتبارها من الجرائم المستحدثة التي فرضها التطور المتسارع في مجال تقنيات المعلومات والاتصال، حيث انطلق المؤتمر من قناعة مفادها أن الجريمة الإلكترونية لا يمكن اختزالها في عنصر واحد، وإنما هي ظاهرة إجرامية مركبة تتداخل فيها عناصر متعددة، تشمل العنصر الشخصي المتمثل في الجاني ومن يسهم معه في ارتكاب الفعل الإجرامي، والعنصر التقني المتمثل في استخدام نظم الحاسب الآلي والشبكات المعلوماتية كوسيلة أو محل للاعتداء، فضلًا عن العنصر المكاني الذي يتمثل في البيئة الإلكترونية بوصفها الإطار الذي تقع فيه الجريمة،[3] ، وعرفها بأنها *كل جريمة يمكن ارتكابها بواسطة نظام حاسوبي، أو شبكة حاسوبية، أو داخل نظام حاسوب، أو في بيئة إلكترونية*[4].

ونظرًا لما تتسم به هذه الجرائم من تطور مستمر وتنوع في الصور والأساليب، وما يترتب على ذلك من صعوبة وضع تعريف قانوني دقيق جامع مانع يحيط بجميع سلوكياتها الإجرامية، ارتأى المؤتمر عدم السعي *إلى صياغة تعريف تقليدي للجريمة الإلكترونية، مكتفيًا بوضع قواعد تأسيسية إرشادية تهدف إلى إبراز*

---

[1]– د/ عبدالقادر القهوجي، الحماية الجنائية لبرامج الحاسب، دار الجامعة الجديدة، مصر، 1997، ص 03.

[2]– مواسة صونية نادية، مرجع سبق ذكره، ص 186.

[3] –CROSS Michael , Scene of the Cybercrime, Second Edition, Syngress Publishing, United Kingdom, 2011, p. 11.

[4]–عبدالسلام محمد المايل، عادل محمد الشربجي، الجريمة الالكترونية في الفضاء الإلكتروني، مجلة أفاق للبحوث و الدراسات، العدد04، 2019، ص 242.

خصائص هذا النوع من الجرائم ورسم حدوده العامة وتمييزه عن الجريمة التقليدية، وذلك تمهيدًا لدراسة مدى كفاية القواعد الجنائية القائمة لمواجهتها، أو الحاجة إلى استحداث قواعد قانونية خاصة بها، سواء على صعيد التجريم أو على صعيد إجراءات الملاحقة والتحقيق أو على صعيد الإثبات الجنائي، وقد تمثلت هذه القواعد الاسترشادية في اعتبار كل جريمة يمكن ارتكابها باستخدام نظام حاسوبي، أو من خلال شبكة معلوماتية، أو يكون محل الاعتداء فيها النظام الحاسوبي ذاته أو البيانات والمعلومات التي يتضمنها، أو تقع داخل بيئة إلكترونية، من قبيل الجرائم الإلكترونية، وهو ما يعكس توجّهًا مرنًا وواسعًا يراعي خصوصية هذا النمط الإجرامي ويواكب التطور التقني المتسارع، أما المجلس الأوروبي ففي تقريره المتعلق بجرائم الحاسوب بأنها كل تغيير غير مشروع في المعطيات أو البيانات أو برامج الحاسوب، أو أي عملية حذف أو نسخ أو إتلاف أو تعديل لها، أو أي تدخل آخر يطال سلامة البيانات أو نظم معالجتها أو نقلها، متى ترتب على هذا التدخل إحداث ضرر اقتصادي أو فقدان حيازة البيانات أو المعلومات من قبل شخص آخر، أو كان القصد من هذا الفعل تحقيق كسب اقتصادي غير مشروع للجاني أو لشخص آخر، ويُظهر هذا التعريف تركيزًا واضحًا على الجانب الموضوعي للجريمة، أي أن الاعتداء يقع مباشرة على البيانات أو البرامج أو نظم الحاسوب نفسها، وليس فقط على الأشخاص أو الممتلكات التقليدية، كما يعكس الطبيعة المتعددة الأبعاد للجريمة الإلكترونية، إذ تتداخل فيها الوسيلة التقنية مع البيئة الإلكترونية التي تقع فيها الجريمة، والنتيجة الاقتصادية أو المادية التي تنشأ عنها، ويؤكد التعريف على أن الجريمة الإلكترونية ليست مجرد استخدام الحاسوب كأداة لارتكاب الجرائم التقليدية، بل تشمل أيضًا أي تدخل في سلامة البيانات أو نظم المعلومات بغرض الإضرار بالغير أو تحقيق منفعة غير مشروعة، ما يجعلها ظاهرة جنائية تتطلب تطوير أطر قانونية خاصة على مستوى التجريم والملاحقة والإثبات، بما يتوافق مع التطور التقني السريع وصعوبة حصر أشكالها وسلوكياتها الإجرامية في تعريف تقليدي جامد[1].

[1]–نهلا عبدالقادر المومني، الجرائم المعلوماتية، دار الثقافة، الاردن، 2008، ص 36.

ثانيا: تعريف الجريمة المعلوماتية في القوانين الوطنية

وعلى مستوى التشريعات المقارنة ، ومنها قانون العقوبات الفرنسي لسنة 1994، الذي ميز بين أنواع من الاعتداء على برامج ومعلومات الحاسب الآلي، وصنف تلك الجرائم في طائفتين ؛ جرائم الاعتداء على برامج ومعلومات الحاسب الآلي، وجرائم الإتلاف التي يكون محلها معطيات الحاسب الآلي[1]

أما بالنسبة للتشريعات العربية[2] فبعضها عرف الجريمة الإلكترونية ومنها التشريع الكويتي، الذي عرفها في المادة الأولى من قانون رقم 63 لسنة2015 بشأن مكافحة جرائم تقنية المعلومات بأن الجريمة المعلوماتية: "كل فعل يرتكب من خلال استخدام الحاسب الآلي أو الشبكة المعلوماتية أو غير ذلك من وسائل تقنية المعلومات بالمخالفة لأحكام هذا القانون.".

وأيضاً عرفها المشرع في المملكة العربية السعودية من خلال نظام مكافحة جرائم المعلوماتية رقم 79 الذي صدر سنة 1428هـ، حيث نصت المادة الأولى في الفقرة الثامنة بأن الجريمة الإلكترونية : "أي فعل يرتكب متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام"

وهناك من اتبع أسلوب الإحالة إلى ما ورد النص علية من جرائم، كالمشرع العماني الذي نص على ذلك في قانون مكافحة جرائم تقنية المعلومات رقم 12 لسنة 2011 في المادة الأولى الفقرة ج على أن: "جرائم تقنية المعلومات: الجرائم المنصوص عليها في هذا القانون."، وهنا يكون المشرع قد التزم نصياً بمبدأ الشرعية الجنائية، لإحالته إلى المواد ذات القانون التي نصت على ما ورد به من جرائم.

والبعض الآخر لم يضع تعريفاً محدداً للجريمة الإلكترونية، تاركاً هذا الأمر للفقه الجنائي كي لا يكن التعريف مقيداً بحقبة زمنية محدده، وإنما مواكبا لتطور تقنية المعلومات ومتغيراً معها ، كالمشرع الإماراتي في القانون رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات، والمشرع الأردني في قانون الجرائم الإلكترونية رقم 27 لسنة ،2015 وهو ما تبناه المشرع الجزائري تاركا تعريف الجريمة المعلوماتية إلى الفقه مواكبا بذلك أي تطورات قد تحدث[3].

المطلب الثاني: طبيعة و خصائص الجريمة المعلوماتية

تُعد الجريمة المعلوماتية من الجرائم المستحدثة التي أفرزها التطور التكنولوجي، إذ ترتبط طبيعتها القانونية باستخدام أنظمة الحاسوب والشبكات في ارتكاب الفعل الجرمي أو توجيهه ضدها. وتمتاز هذه الجريمة بكونها

---

[1]–د / مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية مطابع الشرطة، مصر، ،2000، ص ص 115 وما بعدها

[2]–فيصل عايش عيد المطيري، الوعاء القانوني للدليل التقني في اطار اثبات الجريمة الالكترونية، رسالة مقدمة للحصول على الدكتوراة في الحقوق، جامعة عين شمس، مصر، 2019، ص ص 34،33.

[3]–بعجي عبدالنور، الجريمة الالكترونية بين المفهوم و الخصوصية، بحث مقدم ضمن مؤلف جماعي د/ كوثر مازوني" الجريمة المعلوماتية"، 2012، ص 120.

ذات طابع غير مادي، حيث ينصب الاعتداء فيها على البيانات والمعلومات الرقمية، مما يجعل إثباتها أكثر تعقيدًا مقارنة بالجرائم التقليدية، كما تتسم بطابع عابر للحدود، الأمر الذي يطرح إشكالات قانونية تتعلق بالاختصاص القضائي وتنازع القوانين، فضلًا عن سرعة ارتكابها وصعوبة اكتشاف مرتكبيها، وهو ما يستدعي قواعد قانونية خاصة وآليات فنية متطورة لمواجهتها.

الفرع الأول: الطبيعة القانونية للجريمة المعلوماتية

نتيجة لاعتماد الجريمة الإلكترونية على وسائل وأساليب تقنية ووقوعها في بيئة افتراضية، أصبحت هذه الجريمة من الظواهر المستحدثة التي فرضتها مستجدات العصر والثورة التقنية في أنظمة المعلومات والاتصالات، فهي تتطلب من مرتكبيها درجة معينة من المعرفة التقنية لفهم واستخدام الوسائل الرقمية في تنفيذ أعمالهم الإجرامية، ما يميزها عن الجرائم التقليدية التي تتم في العالم الواقعي وتستند غالبًا إلى أساليب مألوفة. ومن هذا المنطلق، يمكن القول إن الجريمة الإلكترونية اكتسبت طبيعة خاصة تختلف عن الجرائم التقليدية، سواء من حيث البيئة التي تحدث فيها، أو الأساليب المستخدمة، أو المهارات المطلوبة لتنفيذها، مما يجعل مواجهتها تتطلب أدوات وآليات قانونية وتقنية متطورة.

تُعد **المعلوماتية**[1] من المصطلحات التي شاع استخدامها منذ خمسينيات القرن الماضي في مجالات متعددة وسياقات مختلفة، الأمر الذي أدى إلى تنوع مفاهيمها وتعدد دلالاتها في الاستعمال الدارج. ومن الناحية اللغوية، فإن كلمة المعلومات مشتقة من لفظ **العلم**، وتدل بوجه عام على المعرفة التي يمكن نقلها أو اكتسابها أو تداولها بين الأفراد.

وتتميز **الجريمة المعلوماتية** بعدة خصائص تجعلها مختلفة عن باقي الجرائم التقليدية، ومن أبرز هذه الخصائص الطبيعة الخاصة للمعلومات محل الاعتداء.

01-المعلومات ذات طبيعة خاصة: يرى الفقه التقليدي أن للمعلومة طبيعة مميزة، انطلاقاً من الفكرة القائلة بأن القيمة القانونية والاقتصادية لا تُضفى إلا على الأشياء المادية التي تقبل الاستحواذ والاستئثار. وبما أن المعلومات ذات طبيعة معنوية، فإنها . وفقاً لهذا الاتجاه . لا تكون قابلة للاستحواذ إلا في نطاق حقوق الملكية الفكرية.

[1]– بوهرين فتيحة، الجريمة المعلوماتية في التشريع الجزائري، مجلةالحقوق والعلوم الإنسانية المجلد14، العدد: 04 2021،، ص –48 60 ، ص ص 52،53.

وهناك اتجاه على وجوب حماية معلومات الغير عن طريق دعوى المنافسة غير المشروعة استنادا الى حكم محكمة النقض الفرنسية القائل " أن الغاية من دعوى المنافسة غير المشروعة هي تأمين حماية الشخص الذي لا يمكنه أن ينتفع بأي حق استثنائي" ويرى الاستاذ Deboi في وقت مبكر بأن الملكية الفكرية ربما سيأتي يوما ويعترف لصاحب الفكرة لم تحصل على براءة اختراع بالحماية القانونية لأن الفكرة السابقة مستعبدة من مجال الملكية الذهنية[1]

وبناءً على هذا التصور، فإن المعلومات المخزنة التي لا تندرج ضمن المصنفات الأدبية أو الصناعية أو الذهنية لا تُعد من القيم المحمية قانوناً. غير أن هذا الرأي يواجه انتقاداً جوهرياً، إذ يتعارض مع موقف الفقه والقضاء اللذين يعترفان بوجود اعتداء يستوجب العقاب في حالة الاستيلاء غير المشروع على معلومات الغير، حتى وإن لم تكن محمية صراحةً بحقوق ملكية فكرية. ولهذا السبب، تعددت الاتجاهات الفقهية في محاولة تبرير الأساس القانوني للعقاب المترتب على الاعتداء على المعلومات.

02- المعلومات كمجموعة مستحدثة من القيم

ذهب اتجاه فقهي حديث إلى اعتبار المعلومات مجموعة مستحدثة من القيم، ويُعزى الفضل في هذا التصور إلى الفقيهين **Vivant**و، **.Catala**

ويرىCatala أن المعلومة، متى كانت مستقلة عن دعامة مادية معينة، فإنها تكتسب قيمة ذاتية قابلة للاستحواذ، خاصة إذا كانت غير محظورة تجارياً وتُقدَّر قيمتها وفقاً لسعر السوق.

كما يرى أن المعلومة تُعد منتجاً قائماً بذاته، بغض النظر عن الوسيط المادي الذي تحمل عليه أو الجهد المبذول في إنتاجها، وترتبط بمؤلفها بعلاقة قانونية تشبه علاقة المالك بالشيء المملوك، وتقوم بينهما علاقة خاصة يمكن وصفها بعلاقة التبني .وقد استند هذا الاتجاه في إضفاء وصف القيمة على المعلومة إلى حجتين أساسيتين:

-القيمة الاقتصادية للمعلومة

-علاقة التبني القانونية التي تربط المعلومة بمؤلفها.

أما الفقيه vivant فيصف المعلومة بأن قيمة اقتصادية و الثانية وجود علاقة تبني تجمع بينها ومؤلفها مبررا رأيه بالحجتين التاليتين الأولى تتمثل في أنها مستوحاة من بلانيول وريبر وهي فكرة الشيء أو القيمة لها صورة معنوية وإن نوع محل الحق يمكن أن ينتمي إلى قيمة معنوية ذات طابع اقتصادي و لأن تكون جديرة بالحماية القانونية، أما الحجة الثانية يرى هذا الفقيه أن كل الاشياء المملوكة معنوية و التي يعترف بها القانون، وترتكز على الاعتراف بالمعلومة قيمة، عندما تكون من قبيل البراءات أو الرسومات أو النماذج أو حق

[1]-د/ مناصرة يوسف، مرجع سبق ذكره، ص 55.

المؤلف.ولما كانت البرامج عبارة عن معلومات مرتبة ترتيبا معينا بطريقة ألية و لها قيمة اقتصادية في السوق توجب معاملتها معاملة المال[1]

وبذلك، أصبحت المعلومات في ظل هذا الاتجاه الفقهي الحديث محلاً للحماية الجنائية، وأساساً لقيام الجريمة المعلوماتية متى وقع عليها اعتداء غير مشروع، سواء بالاستيلاء أو النسخ أو التداول دون وجه حق.

الفرع الثاني: خصائص الجريمة المعلوماتية

للجريمة المعلوماتية عدة خصائص تميزا عن الجرائم الأخرى التقليدية

أولا: الجريمة الالكترونية جريمة عابرة للحدود

أدى الانتشار الواسع لشبكة الإنترنت إلى إتاحة إمكانية ربط عدد كبير من أجهزة الحاسوب عبر الشبكة العنكبوتية دون التقيد بحدود الزمان والمكان، الأمر الذي سهّل ارتكاب الجرائم الإلكترونية، بحيث قد يكون الجاني في دولة والمجني عليه في دولة أخرى. وهذا ما يبرز الحاجة الملحّة إلى وجود تنظيم قانوني داخلي ودولي متكامل ومتناسق لمكافحة هذا النوع من الجرائم وضبط مرتكبيها والحد من آثارها[2]

إن الطبيعة العابرة للحدود التي تتسم بها الجريمة المعلوماتية أفرزت العديد من الإشكالات القانونية، لا سيما ما يتعلق بتحديد الدولة صاحبة الاختصاص القضائي بنظر هذه الجرائم، وكذلك تحديد القانون الواجب التطبيق، فضلًا عن الصعوبات المرتبطة بإجراءات الملاحقة القضائية.

ومن القضايا التي سلطت الضوء على البعد الدولي للجرائم المعلوماتية، تلك القضية المعروفة باسم مرض نقص المناعة المكتسبة "الإيدز"، حيث تمثلت وقائعها في قيام أحد الأشخاص بتوزيع نسخ يُفترض ظاهريًا أنها تهدف إلى تقديم نصائح تتعلق بهذا المرض، غير أنها كانت في حقيقتها تحتوي على فيروس "حصان طروادة"

وتندرج الجرائم المرتكبة عبر شبكة الإنترنت ضمن نطاق القانون الجنائي الداخلي، غير أنها وبحكم تجاوزها لحدود الدولة الواحدة، تدخل كذلك في إطار دراسات القانون الجنائي الدولي، ومع التزايد المستمر في حجم التجارة الإلكترونية الناتجة عن المبادلات والمراسلات عبر الشبكة، أصبحت هذه الجرائم وثيقة الصلة بالقانون التجاري.

كما أدى ظهور الإنسان المعلوماتي وتشكّل المجتمع الإلكتروني إلى ازدياد المساس بالحقوق والحريات الفردية التي تكفلها القوانين الدستورية، مما يجعلها مرتبطة أيضًا بالقانونين الإداري والدستوري.

---

[1]– د/ مناصرة يوسف، مرجع سبق ذكره، ص 57،58

[2]– عبدالله دعسش العجمي، المشكلات العلمية و القانونية للجرائم الالكترونية، دراسة مقارنة، مذكرة لنيل شهادة الماجستير في القانون العام، جامعة الشرق الأوسط، 2014، ص 20

ثانيا: صعوبة اكتشاف الجريمة المعلوماتية

يرجع ذلك إلى أن الجرائم ذات الطابع التقني تتميز بسهولة ارتكابها من الناحية النظرية، إذ لا تتطلب في الغالب مجهودًا ماديًا أو مواجهة مباشرة مع المجني عليه، كما أن مرتكبيها يستفيدون من الوسائل التقنية المتطورة لإخفاء معالم الجريمة وطمس أدلتها، وتزداد صعوبة تتبع الجناة بسبب اعتماد هذه الجرائم على بيانات رقمية غير مرئية، لا تترك أثرًا ماديًا ملموسًا، وإنما تظهر في شكل تغييرات في الأرقام أو المعطيات المخزنة داخل السجلات والأنظمة الإلكترونية.

ويترتب على ذلك أن اكتشاف الجرائم الإلكترونية يواجه تحديات كبيرة، حيث لا يتم في كثير من الأحيان الانتباه إلى وقوع الجريمة إلا عن طريق المصادفة، أو بعد إجراء تدقيق تقني لاحق، وغالبًا ما يتم ذلك بعد مرور فترة زمنية طويلة على ارتكابها. كما أن هذا التأخر في الاكتشاف يؤدي إلى تعقيد إجراءات التحقيق وجمع الأدلة الرقمية، ويزيد من صعوبة تحديد هوية الجناة ومساءلتهم قانونيًا[1].

ثالثا: ترتكب الجريمة المعلوتية في بيئة رقمية

تُرتكب الجريمة المعلوماتية في إطار البيئة الرقمية، ولا سيما ضمن نظم المعلومات وشبكات الإنترنت، حيث يعتمد الجاني في تنفيذها على وسائل تقنية حديثة. فمرتكب هذا النوع من الجرائم يتعامل أساسًا مع البيانات والمعلومات الرقمية، الأمر الذي يتطلب امتلاكه قدرًا من المعرفة والمهارة التقنية للتعامل مع هذه المعطيات ومعالجتها.

كما قد يقتضي ارتكاب الجريمة الولوج إلى شبكة الإنترنت أو إلى أنظمة معلوماتية محددة، وهو ما يستلزم توافر أجهزة تقنية لدى الجاني، كالحاسوب أو غيره من الوسائط الإلكترونية، فضلًا عن استخدام برامج وأدوات تقنية تساعده على تنفيذ الفعل الإجرامي. وعليه، فإن الطبيعة التقنية لهذه الجرائم تفرض خصوصية مميزة من حيث وسائل ارتكابها وأساليب كشفها وإثباتها[2]

رابعا: ارتكاب الجريمة المعلوماتية عن بعد:

الجريمة المعلوماتية تنفذ عن بعد أي أنها لا ترتكب على مسرح جريمة فعلي، بل ترتكب افتراضيا متجاوزة الحدود الجغرافية للدولة لتصبح عبر وطنية مثل جريمة تبيض الأموال وتحويلها عبر الأنترنت مثل سرقة

---

[1]–سميرة معاشي: "ماهية الجريمة المعلوماتية"، مجلة المنتدى القانوني، العدد 27، كلية الحقوق و العلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائر، أفريل 2010، ص 282.

[2]–رامي عبدالقادر أحمد الطراونة، جرائم تكنولوجيا المعلومات مفهومها وإثباتها، مجلة جامعة الزيتونة الاردنية، للدراسات القانونية، المجلد6 الاصدار 2023. ص 162.

البنوك، وبطاقات الائتمان دون الحاجة إلى السطو الفعلي عل البنك وذلك بارتكابها عن طريق حساب ألي متصل بالانترنت، وقد يكون الفعل الاجرامي في دولة وتحقق النتيجة الإجرامية في دولة أخرى[1].

المبحث الثاني: أطراف الجريمة

للجريمة المعلوماتية طرفين كباقي الجرائم العامة وهما الجاني" المجرم المعلوماتي: و الضحية

المطلب الأول: المجرم المعلوماتي

يعتبر المجرم المعلوماتي مجرم غير تقليدي و يمتاز بعدة خصائص

الفرع الأول :تعريف المجرم المعلوماتي

يُطلق على الجاني في الجريمة المعلوماتية، وفي المجال القانوني، مصطلح "**المجرم المعلوماتي**"، أما في الأوساط الإلكترونية والتقنية فيُطلق عليه خبراء المعلوماتية اسم "**الهاكر**"وهو الشخص الذي يخترق الحاسوب الآلي ويجد متعة في فحص واستكشاف نظم قابلة للبرمجة عن بُعد، ويسعى إلى توسيع معارفه في هذا المجال إلى أقصى حد.

ويختلف هذا المصطلح عن مصطلح "**كراكر**" الذي يُطلق على الفئة التي تمتلك القدرة على الاختراق بهدف التخريب أو الإضرار، كما يوجد من يُعرفون بمصطلح "المخترقين" الذين يكون هدفهم الأساسي إنشاء أدوات برمجية تسمح بالهجوم على أنظمة معلوماتية أو تجاوز نظم الحماية ونشر البرمجيات المدفوعة الثمن بطرق غير مشروعة[2].

والمجرم المعلوماتي هو مجرم متخصص ومحترف في تنفيذ جرائمه المعلوماتية، إذ إن ارتكاب هذا النوع من الجرائم يتطلب القدرة على تجاوز تقنيات حماية أنظمة الحاسوب.

وعلى خلاف المجرم العادي، لا يلجأ المجرم المعلوماتي إلى العنف في تنفيذ جريمته، بل يعتمد في الغالب على الذكاء والمهارة والمعرفة التقنية، ويتمتع بدرجة عالية من الثقافة والخبرة في مجال تكنولوجيا المعلومات[3].

الفرع الثاني : صفات المجرم المعلوماتي

يتميز المجرم المعلوماتي بالصفات التالية

---

[1]– د/ حسين طاهري، مرجع سبق ذكره، ص 16.

[2]– بوخبزة عائشة، الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماجستير في الحقوق، جامعة وهران2013/2012، ص 24.

[3] - رحيمة نمديلي: "خصوصية الجريمة الالكترونية في القانون الجزائري و القوانين المقارنة"، كتاب أعمال المؤتمر الدولي الرابع عشر: الجرائم الالكترونية، مركز جيل البحث العلمي، طرابلس، لبنان، 24،25 مارس 2017، ص 133

أولا: المجرم الالكتروني يتمتع بالخبرة و المهارة والكفاءة

يتمتع المجرم الالكتروني بالكفاءة و الخبرة او المعرفة الكاملة بكافة الظروف المحيطة بالجريمة المزمع ارتكابها، بما في ذلك فرص نجاحها واحتمالات فشلها، وعادةً ما يعمد الجناة إلى التمهيد لجرائمهم من خلال دراسة هذه الظروف بدقة، بهدف تفادي العوامل غير المتوقعة التي قد تؤدي إلى كشف أفعالهم أو ضبطهم.

ويبرز هذا المفهوم بوضوح لدى مجرمي الإنترنت، إذ يكون بمقدورهم تكوين تصور شامل ومسبق عن الجريمة التي ينوون تنفيذها.

كما يتمتع مرتكبو جرائم الإنترنت بمستوى عالٍ من المهارة في استخدام تقنيات الحاسوب والإنترنت، بل إن بعضهم من المتخصصين في مجال معالجة المعلومات آليًا[1].

ويتطلب تنفيذ هذا النوع من الجرائم قدرًا كبيرًا من الكفاءة التقنية، التي قد يكتسبها الجاني من خلال الدراسة الأكاديمية المتخصصة أو عبر الخبرة العملية في مجال تكنولوجيا المعلومات[2].

ويُعد الذكاء كذلك من السمات الجوهرية لمرتكبي الجرائم الإلكترونية، نظرًا لما تتطلبه هذه الجرائم من معرفة تقنية تمكّن الفاعل من الولوج إلى أنظمة الحاسب الآلي، والقدرة على التعديل والتغيير فيها دون اكتشافه

وتشمل هذه الجرائم التلاعب بالبرامج وارتكاب أفعال السرقة والنصب وغيرها من الجرائم التي تستلزم أن يتمتع مرتكبها بدرجة عالية من الذكاء، بما يمكّنه من تنفيذها دون اكتشافه. ويُعد الإجرام عبر الإنترنت إجرامًا يعتمد على القدرات العقلية والذهنية بدرجة أكبر مقارنة بالإجرام التقليدي الذي غالبًا ما يرتبط باستخدام العنف. فمجرم الإنترنت لا يعتمد على القوة المادية، بل يسعى بشغف إلى ابتكار أساليب ووسائل جديدة لا تكون معروفة لغيره، بهدف اختراق الأنظمة والحواجز الأمنية في البيئة الإلكترونية، ومن ثم تحقيق الأهداف الإجرامية التي يسعى إليه.

ثانيا: المجرم المعلوماتي يبرر أفعاله

يسود لدى بعض مرتكبي جرائم الإنترنت اعتقاد مفاده أن الأفعال التي يقومون بها لا تندرج ضمن نطاق الجرائم، أو أنها لا تتسم بعدم الأخلاقية، ولا سيما في الحالات التي يقتصر فيها السلوك على اختراق أنظمة الحاسوب وتجاوز وسائل الحماية المفروضة عليها. ويُميز هؤلاء بين الإضرار بالأشخاص، الذي يعدّونه سلوكًا بالغ اللاأخلاقية، وبين الإضرار بالمؤسسات أو الجهات القادرة اقتصاديًا على تحمّل نتائج تلك الأفعال، الأمر الذي يقلل في نظرهم من جسامة ما يرتكبونه.

---

[1] - طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي،"النظام القانوني لحماية المعلوماتي"، دار الجامعة الجديدة ، مصر، 2009، ص 177.

[2] –MASCALA Corinne, « criminalité et contrat électronique », IN : Le contrat électronique, Travaux de l’association CAPITANT Henri, journées national, Paris, 2000,p 118.

ومع ذلك، لا ينفي هذا التصور وجود فئة من مجرمي الإنترنت الذين يقدمون على ارتكاب هذه الجرائم وهم على علم تام بعدم مشروعيتها وعدم أخلاقيتها، حيث يتسم سلوكهم باتجاه إجرامي واضح وسوء نية بيّن، مع إدراكهم لخطورة أفعالهم وآثارها.

ويبدو أن بعض مرتكبي هذه الجرائم لا يدركون أن سلوكهم يستوجب العقاب، ويُعزى ذلك جزئيًا إلى الاستخدام المتزايد للأنظمة المعلوماتية، الذي أوجد مناخًا نفسيًا يُضعف التمييز بين مفهومي الخير والشر. كما أن غياب الاحتكاك المباشر بين الجاني والمجني عليه يؤدي إلى نوع من التباعد في العلاقة بين الطرفين، مما يسهم في تسهيل ارتكاب الفعل غير المشروع، ويعزز لدى الجاني شعورًا ذاتيًا زائفًا بمشروعية سلوكه.

وفي هذا السياق، يُلاحظ أن بعض العاملين في المؤسسات المختلفة يستخدمون الإنترنت لأغراض شخصية بوصفه سلوكًا شائعًا ومقبولًا اجتماعيًا، دون النظر إليه باعتباره فعلًا إجراميًا. غير أن شيوع هذا السلوك أو ضعف الإحساس بعدم أخلاقيته لدى فئة واسعة من الأفراد لا ينفي الطابع غير المشروع لتلك الأفعال ولا يبررها قانونيًا أو أخلاقيًا [1].

ثالثا: المجرم يخاف من انكشاف أمره

يتسم مرتكبو الجرائم عبر الإنترنت بالخوف الدائم من اكتشاف أفعالهم وافتضاح أمرهم، ورغم أن هذا الشعور يلازم مختلف أنماط المجرمين، إلا أنه يظهر بصورة أوضح لدى مجرمي الإنترنت، نظرًا لما قد يترتب على انكشاف جرائمهم من آثار خطيرة، كالتعرض لاضطرابات مالية أو فقدان الوظيفة والمركز الوظيفي في كثير من الحالات.

كما تسهم طبيعة الأنظمة المعلوماتية ذاتها في تمكين مجرمي الإنترنت من الحفاظ على سرية أفعالهم، إذ إن ما يؤدي غالبًا إلى كشف الجريمة هو تدخل عوامل غير متوقعة أثناء تنفيذها. غير أن الجرائم المرتكبة عبر الإنترنت تتميز بأن أنظمة الحاسوب تؤدي وظائفها في الغالب بصورة آلية ومنتظمة، بحيث لا تختلف المراحل التي تمر بها العمليات من مرة إلى أخرى، الأمر الذي يقلل من احتمالية تدخل متغيرات غير متوقعة، ويساعد على إنجاز الجريمة دون انكشاف، ما دامت جميع خطوات التنفيذ معروفة ومحددة مسبقًا[2].

رابعا: المجرم الالكتروني اجتماعي

تُعد هذه السمة امتدادًا لخاصيتي التخطيط والتنظيم، إذ ينشأ التكيف الاجتماعي عادةً داخل جماعات تجمع أفرادها خصائص مشتركة. فعلى سبيل المثال، تتقارب أفكار مجموعات من ذوي المهارات المتقدمة في مجال تكنولوجيا المعلومات، الأمر الذي يؤدي إلى نشوء علاقات وروابط فيما بينهم تسهم في تسهيل ارتكاب الجرائم الإلكترونية. ولا تقتصر هذه الروابط على النطاق المحلي فحسب، بل قد تتجاوز ذلك لتأخذ طابعًا دوليًا، حيث

---

[1]–نهلا عبد القدر المومني، المرجع السابق، ص78

[2]– المرجع نفسه ، ص 79.

تتلاقى تلك الجماعات على أفكار ومنهجيات مشتركة في توظيف المعرفة والتقدم العلمي لأغراض غير مشروعة، ويُعد عقد المؤتمرات واللقاءات الدولية بين هذه المجموعات دليلاً على وجود مثل هذه الروابط العابرة للحدود.

وعلاوة على ذلك، يتميز مجرمو الإنترنت في الغالب بقدرتهم على التكيف الاجتماعي، إذ يكونون أشخاصًا اجتماعيين قادرين على الاندماج في محيطهم دون الدخول في حالة عداء مع المجتمع الذي ينتمون إليه. بل إنهم غالبًا ما يظهرون توافقًا وتصالحًا مع بيئتهم الاجتماعية، مستندين إلى ما يتمتعون به من مستوى عالٍ من الذكاء. غير أن خطورتهم الإجرامية قد تتفاقم كلما ازداد هذا التكيف الاجتماعي مقترنًا بتوافر النزعة الإجرامية لديهم[1].

الفرع الثاني: المجني عليه " الضحية"

ينقسم ضحيا الجريمة المعلوماتية الى عنصرين الشخص الطبيعي و المؤسسات على اختلاف أنواعها

أولا: الأشخاص الطبيعيون

يعتبر الأشخاص الطبيعيون من أكثر الفئات تضررًا من الجرائم الإلكترونية، ويعود ذلك إلى الانتشار الواسع لاستخدام شبكة الإنترنت وتزايد أعداد المنخرطين فيها. ولم يعد نطاق الجرائم المرتكبة عبر الإنترنت محصورًا في المجالات المالية أو العسكرية، بل اتسع ليشمل الأفراد، حيث يتعرض العديد منهم لجرائم الاحتيال والسرقة والإتلاف بمختلف صورها. وتُعد البيئة الإلكترونية مجالًا ملائمًا لارتكاب هذه الأفعال، نظرًا لما تحتويه من كميات هائلة من البيانات والمعلومات السرية المتعلقة بالأشخاص، سواء كانوا أفرادًا عاديين أو يشغلون مناصب معينة، والتي تصبح عرضة للاستغلال من قبل من يمتلك القدرة على اختراق أنظمة المعلومات.

وتأتي جرائم الإتلاف باستخدام الفيروسات في مقدمة الجرائم التي تستهدف الأشخاص الطبيعيين، ولا سيما من خلال البريد الإلكتروني الذي يُعد من أبرز الوسائل التي يستغلها القراصنة للنفاذ إلى أجهزة المستخدمين. كما تُعد سرقة بيانات وأرقام بطاقات الائتمان من الجرائم الشائعة التي يتعرض لها الأفراد في الفضاء الإلكتروني[2].

ثانيا: المؤسسات

أدى التطور المتسارع في تكنولوجيا المعلومات إلى ظهور التجارة الإلكترونية، التي أسهمت في تسهيل الاتصال بين أطراف المعاملات التجارية وتقليل الاعتماد على الإجراءات الورقية والبشرية، فضلا عن سرعة تبادل البيانات وخفض تكاليف التشغيل وتوسيع نطاق الأسواق. ونتيجة لذلك، اتجهت العديد من الشركات والمؤسسات المالية والاقتصادية إلى استخدام شبكة الإنترنت والاستفادة من مزاياها في مجال الأعمال.

---

[1]– - تركي بن عبد الرحمن المويشر، بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته، أطروحة مقدمة استكمالا لمتطلبات الحصول على درجة دكتوراه الفلسفة الأمنية، كلية الدراسات العليا بجامعة نايف العربية للعلوم الأمنية،الرياض، 200، ص120.

[2]– - محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة للنشر، الإسكندرية، ،2001 ص95.

غير أن هذا التحول أفرز مخاطر جديدة تمثلت في تهديد الأنظمة الشبكية التي تدير أنشطة المصارف وأسواق المال، مما قد يؤدي إلى اضطراب المعاملات التجارية وتعطيل الأنشطة الاقتصادية جزئيًا أو كليًا. ولم تقتصر ثورة المعلومات على المجال المدني، بل امتدت إلى المجال العسكري وأسهمت في ظهور ما يُعرف بحرب المعلومات، التي تستهدف الأهداف العسكرية والسياسية للدول، وأصبحت المعلومات في هذا الإطار تمثل السلاح الرئيسي في الصراعات الحديثة، الأمر الذي استدعى تطوير استراتيجيات هجومية ودفاعية تعتمد على نظم المعلومات وشبكات الحاسوب والأقمار الصناعية، كما دفع ذلك الدول إلى تكثيف أنشطة التجسس الإلكتروني للحصول على معلومات استراتيجية عن خصومها، وفي ظل الاعتماد شبه المطلق على الشبكات المعلوماتية في عالم المال والأعمال، أصبحت المؤسسات المالية والاقتصادية أهدافًا مغرية للجرائم الإلكترونية، لما قد يترتب على اختراقها من آثار سلبية خطيرة تمس الثقة والاستقرار في النظام الاقتصادي العالمي[1].

[1]–صغير يوسف، الجريمة المرتكبة عبر الانترنيت، مذكرة لنيل شهادة الماجستير في الحقوق، تخصص القانون الدولي للأعمال ، كلية الحقوق و العلوم السياسية، جامعة مولود معمري تيزي وزو، السنة الجامعية، 2012/2023، ص ص 22 وما بعدها.

المحور الثاني: مكافحة الجريمة المعلوماتية في التشريع الجزائري

المبحث الأول : أركان وأصناف الجريمة المعلوماتية بصفة عامة

للجريمة المعلوماتية أركان وهما الأركان التقليدية للجريمة لمعلوماتية، كما توجد لها عدة أصناف

المطلب الأول:أركان الجريمة المعلوماتية

تتميز الجرائم الإلكترونية بأنها تقع في الفضاء الافتراضي، ما يمنحها سمات خاصة تختلف عن الجرائم التقليدية في العالم المادي، ومع ذلك، فإنها لا تنفصل عن المبادئ العامة للجريمة.

الفرع الأول: الركن الشرعي

الركن الشرعي للجريمة يشير إلى الصفة القانونية للفعل، أي وجود نص قانوني يجرم الفعل ويحدد العقوبة المترتبة عليه في وقت ارتكابه، ويُعد هذا الركن أساسياً لضمان شرعية العقوبة ومنع محاكمة الأفراد عن أفعال لم يكن القانون قد جرمها وقت ارتكابها، وهو ما يعكس مبدأ عدم رجعية القانون الجنائي .وبالتالي، لا يجوز مساءلة شخص عن فعل ارتكبه قبل صدور نص التجريم أو بعد إلغاء هذا النص، كما لا يجوز توسيع نطاق التجريم ليشمل أفعالا لم ينص القانون على تجريمها، حتى لو كانت مشابهة من حيث الدوافع أو النتائج أو الوسائل المستخدمة لأفعال أخرى مجرمة. ويُلزم القضاة بالتفسير الحرفي للنصوص الجزائية، والالتزام بمضامينها دون تجاوز أو تأويل مفرط.

ويتحقق الركن الشرعي من خلال ركنين أساسيين: الأول مطابقة الفعل للنص القانوني، أي أن يكون الفعل المرتكب ضمن الأفعال التي يجرمها القانون ويحدد لها العقوبة بوضوح، بما يمنع الاستدلال على التجريم بالقياس أو التشابه فقط، والثاني عدم وجود سبب يبيح الفعل، أي ألا يكون هناك مبرر قانوني مشروع مثل الدفاع عن النفس أو حالة الضرورة، مما يبرر ارتكاب الفعل دون أن يكون جريمة. وتؤكد الاجتهادات القضائية العليا، مثل تطبيق نظرية العقوبة المبررة، على أن العقوبة المقررة يجب أن تتوافق مع النص المطبق لضمان العدالة ومنع التجاوزات في التجريم.

وبهذا الشكل، يمثل الركن الشرعي صمام أمان القانون الجنائي، حيث يحدد حدود التجريم ويمنع التعسف في تطبيق العقوبات، كما يضمن أن تكون العقوبات مستندة إلى نصوص واضحة ومعلنة، ما يعزز الثقة بالنظام القانوني ويحقق مبدأ سيادة القانون[1].

الفرع الثاني: الركن المعنوي

يقوم الركن المعنوي للجريمة الإلكترونية على وجود إرادة جرمية لدى الفاعل، تُوجَّه نحو ارتكاب فعل غير مشروع ينص القانون على تجريمه، مثل انتحال شخصية مزود خدمات الإنترنت أو سرقة أرقام البطاقات

[1]– بلعليات إبراهيم، أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري، دار الخلدونية، الجزائر، 2007، ص.18.

الائتمانية، وتكتسب إرادة الجاني صفة الجريمة من خلال النتيجة الضارة المترتبة على أفعاله حيث يكون الجاني عالمًا بالآثار الضارة التي قد تنشأ عن سلوكه غير المشروع.

ويختلف طبيعة الركن المعنوي بين الجرائم المعلوماتية حسب نوعها، ففي جريمة الدخول غير المصرح به إلى نظام الحاسب الآلي، يُشترط وجود قصد جنائي عام، ويعني ذلك أن يكون الجاني عالمًا بأن الدخول غير المصرح به إلى النظام يشكل جريمة، نظرًا لحماية المشرع لجهاز الحاسب وبياناته ومحتوياته من معلومات وبرامج، وبالتالي، فإن الدخول بالخطأ أو عن طريق السهو يُنفي شرط القصد الجنائي، بشرط مغادرة الفاعل للنظام فور اكتشافه للدخول غير المشروع، اذ تتطلب توفر القصد الجنائي الذي يضمره الجاني في نفسه[1] أما في جريمة تخريب أو تعطيل نظام التشغيل ، فهي جريمة عمدية تتطلب وجود قصد جنائي محدد، في أن تتجه إرادة الجاني إلى فعل عرقلة أو تعطيل أو إفساد كما يكون له العلم أن نشاطه يؤدي إلى تعطيل أو إفساد نظام المعالجة الألية للمعطيات، وأن يعلم أن ذلك يتم دون موافقة صاحب الحق في السيطرة على النظام[2]

الفرع الثالث: الركن المادي

يقصد بالركن المادي للجريمة ذلك المظهر الخارجي الملموس للسلوك الإجرامي الصادر عن إنسان يتمتع بالإدراك والاختيار، والذي يترتب عليه مساس بحق أو مصلحة يحميها الدستور والقانون.

ويُعد هذا الركن الأساس الواقعي لقيام الجريمة، إذ لا يمكن تصور جريمة دون فعل مادي يعبر عن الإرادة الإجرامية في صورة قابلة للإثبات.

وقد ذهب جانب من الفقه الجنائي إلى أن الركن المادي يتكون من ثلاثة عناصر مترابطة، هي :السلوك الإجرامي، والنتيجة الإجرامية، والعلاقة السببية التي تربط بينهما، بحيث لا يكتمل هذا الركن إلا بتوافر هذه العناصر مجتمع[3].

أولا: السلوك الإجرامي

يتمثل السلوك الإجرامي في نشاط إرادي يصدر عن الجاني، وقد يأخذ صورة الفعل الإيجابي عندما يقوم الجاني بسلوك فعلي يهدف إلى إحداث نتيجة معينة، كما قد يتمثل في **الامتناع أو السلوك السلبي** عندما يحجم الجاني عن أداء واجب يفرضه القانون، وفي نطاق الجرائم المعلوماتية، يتجلى هذا السلوك بنوعيه الإيجابي والسلبي، غير أنه يتسم بخصوصية ناتجة عن التطور التقني المتسارع، إذ انتقل السلوك الإجرامي من صور تقليدية بسيطة إلى أفعال رقمية معقدة، تعتمد على وسائل تقنية متطورة وقدرات ذهنية عالية لدى الفاعل، الأمر الذي أفرز صعوبات عملية وقانونية في إثبات هذا السلوك وتحديد معالمه.

---

[1]–حسن طاهري، مرجع سبق ذكرخ، ص 125

[2]– المرجع نفسه، ص 139.

[3]– بلعليات إبراهيم، مرجع سبق ذكره، ص 18

ثانيًا: النتيجة الإجرامية

تتمثل النتيجة الإجرامية في الأثر الضار الذي يترتب على السلوك الإجرامي، ويُقصد بها التغيير المادي أو المعنوي الذي يصيب الحق أو المصلحة محل الحماية القانونية. ولا يُعتد في هذا السياق إلا بالنتيجة التي اعتبرها المشرع جوهرية ورتب عليها التجريم والعقاب، بصرف النظر عن النتائج العرضية أو غير المقصودة التي قد تترتب على الفعل.

ثالثًا: العلاقة السببية بين السلوك والنتيجة

تعبر العلاقة السببية عن الصلة المباشرة التي تربط بين السلوك الإجرامي والنتيجة المترتبة عليه، بحيث يُثبت أن هذه النتيجة ما كانت لتتحقق لولا ارتكاب الفعل محل التجريم، وتكتسب هذه الرابطة أهمية بالغة في إسناد المسؤولية الجنائية إلى الجاني، إذ يشترط لقيامها أن يكون الفعل هو السبب المباشر أو الفعال في حدوث النتيجة، دون تدخل سبب أجنبي يقطع هذه العلاقة.

وبذلك، يشكل الركن المادي في الجرائم الإلكترونية الإطار الواقعي الذي تُبنى عليه المسؤولية الجنائية، مع مراعاة الخصوصية التقنية التي تميز هذا النوع من الجرائم عن الجرائم التقليدية.

المطلب الثاني: أصناف الجريمة المعلوماتية

للجريمة المعلوماتية عدة أصناف

الفرع الأول: الجريمة الإلكترونية كجريمة أموال

يصنف الفقه الجريمة الإلكترونية ضمن جرائم الأموال، وذلك باعتبار أن محلها غالباً هو المال، أو أي شيء يقوّم بالمال، سواء كان مادياً أو معنوياً، مثل السرقة أو الاحتيال أو خيانة الأمانة، وتكون الجريمة الإلكترونية من هذا النوع عندما **يكون** محتوى الحاسب الآلي ذا قيمة مالية**.**

ويمكن تمييز نوعين من معطيات الحاسب الآلي:

أولا: المعطيات المادية :وهي الأجزاء الظاهرة والملموسة، مثل الشاشة وأسلاك التوصيل، وعادةً لا تُعد سرقتها جريمة إلكترونية، بل تبقى ضمن **الجرائم التقليدية** إذا تم الاعتداء عليها بأساليب تقليدية.

ثانيا: المعطيات المعنوية :وهي الأجزاء ذات القيمة المالية غير المادية، وتنقسم إلى:

01-مفردات تقنية إلكترونية، مثل البيانات، المعلومات، الرموز، الصور، أو برامج الحاسب الآلي.

02-معطيات شبكات تقنية المعلومات، التي تربط بين أطراف مختلفة لضمان انسياب المعلومات.

وبناءً على ذلك، تُعتبر الجريمة الإلكترونية جريمة أموال إذا:

-كانت الجريمة واقعة على المعطيات التقنية المعنوية، أو **تم** استخدامها كوسيلة لإيقاع جرائم أموال، مثل السرقة أو الاحتيال أو إساءة الائتمان، فتُسمى عندئذ جرائم السرقة الإلكترونية أو جرائم الاحتيال الإلكتروني.

كانت الأنظمة التقنية أو الحاسب الآلي هي نفسها محل الجريمة، مثل الدخول غير المصرح به على الشبكات، أو التلاعب بالبيانات والمعلومات، أو نسخها أو حجب الوصول إليها، أو سائر السلوكيات غير المشروعة التي تستهدف وسائل الاتصالات.

على سبيل المثال، في عام 1989، أصدرت محكمة النقض الفرنسية حُكماً مهماً في قضية **Bourquin** حيث قام موظفان في مطبعة بنسخ 47 قرصاً ممغنطاً يحتوي على بيانات ومعلومات سرية تخص عملاء المؤسسة بهدف إنشاء مؤسسة منافسة، مستخدمين معدات المطبعة نفسها. وأيدت محكمة النقض إدانة المتهمين بسرقة المحتوى المعلوماتي للبيانات، مما شكل خطوة هامة في الاعتراف بالسرقة الإلكترونية للمعلومات كممارسة جرمية حقيقية[1].

وأفاد مركز الجريمة الإلكترونية التابع لمكتب التحقيقات الفيدرالي "FBI" في تقريره السنوي بتلقي 207,492 شكوى، وكانت الغالبية العظمى منها تتعلق بالاحتيال عبر الإنترنت، حيث بلغ إجمالي الأموال المفقودة من قبل مقدمي الشكاوى 1,984,400,000دولار، وتشير السوابق القضائية في الولايات المتحدة إلى أن المدعين العامين المتخصصين في الجرائم الإلكترونية يركزون على تحديد أوجه الدخول غير المصرح به، سواء تم الدخول إلى أنظمة المعالجة الإلكترونية للبيانات بدون تصريح أو بما يتجاوز حدود التصريح المسموح به، وذلك لإثبات الاتهام بدقة وفقاً لكل حالة[2].

الفرع الثاني: الجريمة الإلكترونية كجرائم أشخاص

إلى جانب الجرائم الإلكترونية ذات الطابع المالي، **توجد** جرائم إلكترونية تتعلق بالأشخاص، حيث يكون المعتدى عليه شخصياً ويشمل حقه في سلامة جسده وكرامته وحياته الخاصة .ومن أبرز أشكال هذه الجرائم **:** الإيذاء، السب والقذف والتحقير الإلكتروني، التهديد الإلكتروني، وإفشاء المعلومات الشخصية**.**

.

ونصت القوانين الكويتية على غرار ذلك، حيث جرم أي اعتداء على الحياة الخاصة للأشخاص، أو على عرضهم وكرامتهم وسمعتهم، أو أي فعل خادش للآداب العامة، مع تشديد العقوبة إذا اقترنت الجريمة الإلكترونية بناقصي الأهلية.

وتوضح السوابق العملية طبيعة هذه الجرائم الإلكترونية:

---

[1] VIVANT Michel, Le droit de L'Internet et de la société de l'information ،Larcier, Paris, 2001, p. 21.

[2] – MARSHALL H. Prosecuting Computer Crimes, Legal Education Executive Office, USA, p. 8.

–قضية الحاخام **Kaye David** في فرجينيا، الذي أجرى محادثة جنسية مع صبي يبلغ من العمر 13 عامًا وأرسل له صورًا خليعة عبر الإنترنت، حيث صدر ضده حكم بالسجن لمدة ست سنوات ونصف بعد القبض عليه وتقديمه للمحاكمة[1].

الفرع الثالث: الجريمة الإلكترونية كجرائم مخلة بأمن الدولة

تُصنَّف بعض الجرائم الإلكترونية ضمن الجرائم المخلة بأمن الدولة وبالثقة العامة، باعتبارها من أخطر الصور التي يمكن أن تتخذها الجريمة في العصر الحديث، فمع التطور المتسارع للتكنولوجيا وتشعب وسائلها، أصبحت الوسائل التقنية أداة فعّالة لارتكاب جرائم تمس أمن الدولة واستقرارها، ولكن بأساليب إلكترونية مستحدثة تختلف عن الأساليب التقليدية من حيث الخطورة والتأثير.

ومن أبرز هذه الجرائم جرائم التجسس التقني والإرهاب الإلكتروني، حيث تُستغل الأنظمة المعلوماتية ووسائل الاتصال الحديثة لإحداث أضرار جسيمة تطال البنية التحتية للدولة، أو تهدد أمنها السياسي والاقتصادي والعسكري. وتمتاز هذه الجرائم بقدرتها على إحداث آثار واسعة النطاق تفوق في كثير من الأحيان ما يمكن تحقيقه بالوسائل الإجرامية التقليدية، مما يجعلها تمثل تحديًا حقيقيًا لأمن الدول ويتطلب مواجهتها تشريعات وتقنيات متطورة تتناسب مع طبيعتها الخاصة[2].

لقد أسهم التطور الكبير في تقنيات أنظمة المعلومات وانتشار شبكة الإنترنت في ظهور مواقع إلكترونية معادية، يُوجَّه بعضها ضد سياسة دولة معينة أو ضد عقيدة أو مذهب محدد، وذلك من خلال نشر الأخبار الكاذبة والمعلومات المضللة أو المنشورات التحريضية التي من شأنها تهديد أمن الدولة وزعزعة استقرارها. ويتم تداول هذه المحتويات عبر مواقع الإنترنت المختلفة، والقوائم البريدية، والمدونات الإلكترونية، مما يزيد من سرعة انتشارها واتساع نطاق تأثيرها، ويجعلها أحد أخطر مظاهر الجرائم الإلكترونية المخلة بأمن الدولة في العصر الرقمي.

الفرع الرابع : الجريمة الالكترونية قد تتخذ طابعا اقتصاديا

إضافة إلى ما سبق، تتخذ بعض الجرائم **الإلكترونية** طابعاً اقتصادياً، إذ أصبح القطاع الاقتصادي، سواء العام أو الخاص، ميداناً رئيسياً لارتكاب الجرائم الإلكترونية. فقد ارتبطت التقنية في العديد من الحالات أكثر بالجوانب الاقتصادية منها بالأمنية، وتعد السلوكيات التقنية التي تشكل أطر التجريم في المجال الاقتصادي .هي الأكثر شيوعاً وانتشاراً

---

[1] –CHRIS Hansen, To Catch a Predator Protecting Your Kids from Online Enemies Already in Your Home, USA : Plume, 2007, p. 27

[2] – منير محمد الجنبيهي، وممدوح محمد الجنبيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2004، ص –86

وعند وصف جريمة ما بأنها جريمة اقتصادية، يُفهم من ذلك أن كل سلوك غير مشروع يمس بقيمة اقتصادية عامة أو خاصة، سواء كان متعلقاً بالمال كوحدة اقتصادية أو أثر على الأنظمة المالية بشكل مباشر. كما تُعرف الجريمة الاقتصادية بأنها:

"كل فعل أو امتناع يعاقب عليه القانون ويخالف السياسة الاقتصادية للدولة"[1]

ويؤكد هذا المفهوم ما جاء **في** مؤتمر الأمم المتحدة لمنع الجريمة ومعاملة المجرمين المنعقد بالقاهرة عام 1995، حيث تم التأكيد على أن الجريمة الإلكترونية قد تتخذ أشكالاً اقتصادية تؤثر على الأنشطة المالية والتجارية للدولة والشركات والأفراد، مما يستلزم سن تشريعات خاصة وأساليب رقابية وتقنية لمواجهة هذه التهديدات الاقتصادية الرقمية[2].

وتُعد الجريمة الإلكترونية جريمة اقتصادية متى استُخدمت تقنيات نظم المعلومات والاتصالات على نحو متزايد لارتكاب سلوكيات اقتصادية غير مشروعة، أو لتنفيذ صفقات اقتصادية محظورة، أو للتلاعب بالبيانات والمعلومات الاقتصادية ذات الأثر المباشر والكبير على الاقتصاد الوطني.

المبحث الثاني : مكافحة الجريمة المعلوماتية في قانون العقوبات

يتجسّد هذا التوجّه التشريعي من خلال تناول مختلف صور الجرائم المعلوماتية التي أحاطها المشرّع الجزائري بالحماية الجزائية.

المطلب الأول: جرائم المساس بأنظمة المعالجة الألية لممعطيات

أقرّ المشرّع الجزائري، بموجب تعديل قانون العقوبات سنة 2004، استحداث قسم سابع مكرّر خُصّص للجرائم الماسّة بأنظمة المعالجة الآلية للمعطيات، وتضمّن المواد من 394 مكرّر إلى 394 مكرّر 7[3].

وقد تم تعزيز هذا الإطار التشريعي سنة 2016 بإضافة المادة 394 مكرّر 8 المتعلقة بمقدّمي خدمات الإنترنت. وتمثّل هذه الجرائم النواة الأساسية لدراسة الجريمة المعلوماتية في التشريع الجزائري وفي إطار المقارنة مع الاتفاقيات الدولية. وتنصب الحماية الجنائية فيها أساسًا على الجانب المعنوي للنظام المعلوماتي، والمتمثل في المعطيات والبرامج، أما الاعتداءات التي تطال الجانب المادي للأجهزة، فتظل خاضعة لأحكام الجرائم التقليدية كالسرقة والإتلاف.

---

[1]– عبود السراج، قانون العقوبات الاقتصادية، جامعة دمشق، الطبعة السابعة، دمشق، ،1998 ص 10.

[2]– أعمال مؤتمر الأمم المتحدة لمنع الجريمة ومعاملة المجرمين حول تحديات الجريمة عبر الوطنية المنعقد في القاهرة العام ١٩٩

[3]–القانون رقم 04–15 المؤرخ في 10 نوفمبر 2004، المنشور **في** الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية عدد 71، والذي يعدّل ويتمّم الأمر رقم 66–156 المؤرخ في 8 جوان 1966، المتضمن قانون العقوبات

الفرع الأول: جريمتي الدخول والبقاء غير المصرح بهما

كرّس المشرّع الجزائري من خلال المادة 394مكرر من قانون العقوبات حماية جزائية خاصة للنظم المعلوماتية، وذلك بتجريم فعلي الدخول غير المشروع والبقاء غير المصرّح به داخل منظومة المعالجة الآلية للمعطيات. ويُعد هذا التجريم تجسيدًا للتوجه الوقائي للسياسة الجنائية الحديثة، التي لم تعد تشترط تحقق الضرر الفعلي، بل تكتفي بمجرد تعريض النظام المعلوماتي للخطر، لما ينطوي عليه من تهديد لأمن المعلومات وسريتها وسلامتها.

ويقوم الركن المادي في هذه الجريمة على سلوك إجرامي محدد يتمثل في الولوج أو الاستمرار داخل النظام المعلوماتي دون سند قانوني، سواء تعلّق الأمر بالنظام ككل أو بأحد أجزائه، وهو ما أكده المشرّع صراحة بعبارة :"*كل أو جزء من منظومة للمعالجة الآلية للمعطيات*"

أولا: الدخول غير المشروع إلى النظام المعلوماتي:

تنص المادة 394مكرّر من قانون العقوبات الجزائري على أنه:"*يعاقب بالحبس من ثلاث 3 أشهر الى سنة وبغرامة من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقى، عن طريق الغش، في كل أو جزء من منظومة للمعالجة الآلية للمعطيات*"

ومن خلال هذا النص، يتبيّن أن المشرّع الجزائري قد أقرّ بتجريم فعلي الدخول والبقاء غير المشروع داخل النظام المعلوماتي، باعتبارهما من الجرائم المعلوماتية المستقلة التي تقوم على ركنين أساسيين :ركن مادي وركن معنوي، سيتم تناول كل منهما على حدى[1]

01-الركن المادي لجريمة الدخول أو البقاء غير المشروع

يتحقق الركن المادي لهذه الجريمة من خلال سلوك إجرامي يتمثل في الدخول إلى النظام المعلوماتي أو الاستمرار في التواجد داخله دون وجه حق .ويكفي لقيام هذا الركن تحقق أحد السلوكين دون اشتراط اجتماعهما، وذلك وفقًا لما يُستفاد من صياغة المادة 394 مكرّر من قانون العقوبات.

ولغرض الإحاطة الدقيقة بمضمون هذا الركن، سيتم التمييز بين صورتي السلوك الإجرامي، مع بيان العلاقة القائمة بينهما.

[1]-بطيحي نسيمة، جريمة الدخول أو البقاء غير المشروع إلى النظام المعلوماتي، مجلة الفقه القانوني و السياسي، المجلد01، العدد01، 2019، ص 78.

أ: الصورة الأولى للسلوك الإجرامي " الدخول إلى النظام المعلوماتي"

يُقصد بالدخول إلى النظام المعلوماتي كل ولوج غير مشروع إلى منظومة المعالجة الآلية للمعطيات، سواء تم ذلك بصورة مادية أو معنوية. فالدخول لا يقتصر على التواجد المادي أمام أجهزة الحاسوب، بل يتحقق كذلك عبر الوسائط التقنية عن بُعد، كالدخول من خلال شبكة الإنترنت أو الشبكات الداخلية، وهو ما يجعل البعد المكاني غير ذي أهمية في قيام الجريمة[1].

ويتحقق فعل الدخول متى قام الجاني بالنفاذ إلى النظام دون ترخيص، أو بتجاوز حدود الإذن الممنوح له، سواء من حيث المدة أو الغاية أو نطاق الصلاحيات. ولا يشترط المشرّع الجزائري تحديد الوسائل التي يتم بها الدخول، مما يفيد أن أي وسيلة تقنية تُستعمل للوصول غير المشروع إلى النظام تُعد كافية لقيام الجريمة، كاستعمال كلمات مرور حقيقية تم الحصول عليها بطرق غير مشروعة، أو استخدام برامج أو معدات خارجية، أو استغلال ثغرات أمنية.

كما يستوي في ذلك أن يكون الدخول مباشرًا أو غير مباشر، إذ قد يقوم الجاني بالولوج مباشرة إلى النظام المعلوماتي، أو يدخل إليه عن طريق الاتصال بجهاز وسيط متصل بالنظام، كالدخول عبر خوادم الشبكة أو من خلال الاتصال بالإنترنت. وقد أكّد القضاء المقارن هذا المفهوم الواسع للدخول، معتبرًا أن الاختراق غير القانوني يتحقق بمجرد النفاذ إلى نظام المعالجة الآلية للمعطيات، ولو تم ذلك عن بُعد.

ولا يُشترط لقيام الركن المادي أن ينصب الدخول على كامل النظام المعلوماتي، بل يكفي الولوج إلى جزء منه، وهو ما صرّحت به المادة 394 مكرّر من قانون العقوبات بقولها :*"كل أو جزء من منظومة للمعالجة الآلية للمعطيات"* ، ويشمل ذلك الدخول إلى أحد مكونات النظام أو إلى قاعدة بيانات معينة أو إلى ملف أو برنامج محدد داخل النظام[2].

غير أن الدخول إلى جزء من النظام لا يندرج ضمن دائرة التجريم إلا إذا كان هذا الجزء يُعد عنصرًا من عناصر النظام المعلوماتي المحمي قانونًا، أما إذا تعلق الاعتداء بجزء مستقل لا يُشكّل نظامًا قائمًا بذاته، فقد يندرج الفعل ضمن الجرائم التقليدية، كجرائم الاعتداء على الملكية الفكرية أو حقوق المؤلف، وفقًا للنصوص الخاصة بذلك.

[1]–حمودي ناصر، الحماية الجنائية لنظم المعالجة الألية للمعطيات في التشريع الجزائري، المجلة الاكاديمية للبحث القانوني، المجلد 14، العدد02، 2016، ص74.

[2] –Raymond Gassin, informatique "fraude informatique", répertoire pénal,Dalloz, octobre1995, p17

وتُعد جريمة الدخول غير المشروع جريمة شكلية، إذ تتحقق بمجرد تحقق فعل الدخول دون اشتراط حصول الجاني على المعطيات أو إحداث ضرر بها. فالعبرة هنا ليست بالمساس الفعلي بالبيانات، وإنما بانتهاك حرمة النظام المعلوماتي ذاته، لما يمثله ذلك من تهديد لأمنه وسلامته[1].

ولا يُعتد في هذا السياق بالدافع أو الغاية من الدخول، كما لا يُشترط أن يترتب عنه ضرر فعلي، إذ يكفي مجرد السلوك المتمثل في الولوج غير المشروع. كما لا يُعد الدخول في حد ذاته فعلاً من أفعال النسخ أو النقل أو الاطلاع المشروع، ما لم يكن مقرونًا بسلوك آخر مجرّم بنص خاص.

وبذلك يتضح أن المشرّع الجزائري قد اعتمد مفهومًا واسعًا لفعل الدخول، قصد توفير حماية شاملة للنظم المعلوماتية، وجعل هذا الفعل المدخل الأساسي لباقي صور الجرائم المعلوماتية، وعلى رأسها جرائم التلاعب بالمعطيات أو تخريب الأنظمة.

ثانيا: البقاء غير المشروع داخل النظام المعلوماتي:

يُعدّ البقاء غير المشروع داخل النظام المعلوماتي صورة متميزة من صور السلوك الإجرامي في مجال الجرائم المعلوماتية، وقد حظي هذا الفعل باهتمام خاص في الاتفاقيات الدولية، وعلى رأسها اتفاقية بودابست، كما تبنّته عدة تشريعات مقارنة كالتشريع الفرنسي والسوري والأردني والكويتي.

ويقصد بالبقاء غير المشروع استمرار الشخص في التواجد داخل نظام المعالجة الآلية للمعطيات دون سند قانوني يبرّر هذا التواجد، سواء كان الدخول في بدايته غير مشروع، أو كان مشروعًا ثم زالت أسبابه أو تم تجاوز حدوده[2].

وتبرز أهمية تجريم هذا السلوك في الحالات التي لا يتحقق فيها الدخول غير المشروع ابتداءً، وإنما يتم الولوج إلى النظام بصورة مشروعة، كالدخول المصرّح به مؤقتًا، أو الدخول الناتج عن خطأ أو إهمال من صاحب النظام، ثم يستغل الجاني هذا الوضع ليستمر داخل النظام رغم انتفاء الإذن أو مخالفته لشروط الترخيص، ففي مثل هذه الحالات، يتحقق الاعتداء الجنائي من خلال عنصر الاستمرار داخل النظام، لا من خلال فعل الدخول ذاته.

ويتحقق الركن المادي لجريمة البقاء غير المشروع بمجرد استمرار الجاني داخل النظام المعلوماتي خارج الإطار المسموح به، سواء من حيث الزمن أو الغاية أو نطاق الصلاحيات. ومن صور ذلك: بقاء المستخدم

---

[1]– IBID.P 19.

[2]–عاسية زروق، الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري، ضمن مؤلف جماعي كوثر مازوني، الجريمة المعلوماتية، منشورات الخلدونية، 2022، ص 14

متصلًا بالنظام بعد انتهاء مدة الترخيص، أو الاستمرار في استخدامه لأغراض غير تلك التي خُوّل من أجلها، أو تجاهل أمر صريح بقطع الاتصال والخروج من النظام.

كما يدخل ضمن هذا المفهوم بقاء الشخص داخل النظام خارج أوقات العمل أو خارج الإطار الوظيفي المحدد له، متى كان ذلك دون موافقة صاحب النظام. ويزداد الأمر خطورة إذا استُغل هذا البقاء للوصول إلى معطيات أو وظائف غير مصرح بها، وهو ما يبرّر تدخل المشرّع بالتجريم حمايةً لسلامة النظام وأمنه.

أما في التشريع الجزائري، فقد جاء نص المادة 394 مكرّر من قانون العقوبات بصيغة عامة، حيث جمع بين فعلي الدخول والبقاء غير المشروعين دون تفصيل دقيق لحالات البقاء، غير أن هذه العمومية تُفسَّر على نحو يسمح بإدراج البقاء داخل النظام بعد زوال سبب الدخول المشروع ضمن نطاق التجريم، سواء تعلق الأمر بانتهاء الترخيص الزمني، أو بتجاوز حدود الصلاحيات الممنوحة من قبل مالك النظام.

ويُستفاد من ذلك أن الولوج المشروع إلى النظام المعلوماتي لا يمنح صاحبه حقًا مطلقًا في التواجد داخله، بل يظل مقيدًا بالشروط والحدود التي رسمها صاحب النظام، فإذا خالف الجاني هذه الشروط، تحوّل وجوده داخل النظام إلى وجود غير مشروع، وقامت بذلك مسؤوليته الجنائية عن فعل البقاء غير المشروع.

وخلاصة القول، إن جريمة البقاء غير المشروع تمثل اعتداءً مستقلًا عن جريمة الدخول غير المشروع، وتقوم على عنصر الاستمرار داخل النظام دون سند قانوني، بما يعكس حرص المشرّع على توفير حماية شاملة للنظم المعلوماتية، ليس فقط من الاختراقات المباشرة، وإنما أيضًا من إساءة استعمال حقوق الولوج الممنوحة، حمايةً لسلامة الأنظمة والمعطيات التي تحتويها الجزاء الجنائي المقرر لجريمة الدخول أو البقاء غير المشروع داخل النظام المعلوماتي تُعدّ جريمة الدخول أو البقاء غير المشروع داخل النظام المعلوماتي من الجرائم ذات الطابع الشكلي، إذ يكفي لقيامها تحقق السلوك الإجرامي المتمثل في الولوج أو الاستمرار داخل النظام دون سند قانوني، دون اشتراط تحقق نتيجة ضارة. غير أنّ المشرّع الجزائري، إدراكًا لخطورة هذه الأفعال، قد أحاطها بنظام عقابي متكامل يقوم على التدرّج والتشديد بحسب جسامة الفعل والآثار المترتبة عنه.

و لقد أقرّ المشرّع الجزائري بموجب المادة 394 مكرّر من قانون العقوبات عقوبة الحبس والغرامة لكل من يدخل أو يبقى داخل نظام المعالجة الآلية للمعطيات بطريقة غير مشروعة، ويعكس هذا التوجه رغبة المشرّع في توفير حماية فعالة للأنظمة المعلوماتية، بالنظر إلى ما تمثله من قيمة اقتصادية وأمنية متزايدة.

ولم يقتصر الجزاء على العقوبات الأصلية، بل امتد إلى عقوبات تكميلية ذات طابع تقني، تتلاءم مع خصوصية الجريمة المعلوماتية، إذ خوّل المشرّع للقضاء سلطة مصادرة الأجهزة والبرمجيات ووسائل الاتصال المستعملة في ارتكاب الجريمة، فضلاً عن غلق المواقع أو أماكن الاستغلال التي استُخدمت في تنفيذها، متى ثبت علم مالكها بالفعل الإجرامي، وهو ما نصت عليه المادة 394 مكرر 6[1].

ثالثا: الشروع والاتفاق الجنائي

وسّع المشرّع من نطاق التجريم ليشمل الشروع في جريمة الدخول أو البقاء غير المشروع، حيث ساوى بين الجريمة التامة ومحاولة ارتكابها من حيث العقوبة، تأسيسًا على ما ينطوي عليه الشروع من خطورة حقيقية على أمن النظام المعلوماتي[2]، كما جرم الاتفاق الجنائي متى انصب على الإعداد لارتكاب هذه الجريمة، ولو لم تتحقق النتيجة النهائية، وذلك متى تجسّد الاتفاق في أفعال مادية ملموسة.

ويهدف هذا التوجه إلى التصدي المبكر للجرائم المعلوماتية، خاصة تلك التي تُرتكب في إطار جماعي أو منظم، بما يعزز سياسة الردع الاستباقي ويحدّ من انتشار هذا النوع من الجرائم التقنية[3].

رابعا: المسؤولية الجزائية للشخص المعنوي

وانسجامًا مع التطور الحديث في السياسة الجنائية، أقرّ المشرّع الجزائري مسؤولية الشخص المعنوي عن جريمة الدخول أو البقاء غير المشروع، متى ارتُكبت لحسابه أو باسمه. وفي هذه الحالة، تُفرض على الشخص المعنوي غرامة مالية مشددة قد تصل إلى خمسة أضعاف الغرامة المقررة للشخص الطبيعي، دون الإخلال بحق القاضي في توقيع العقوبات التكميلية الملائمة، وهو ما يعكس إدراك المشرّع للدور المتنامي الذي تلعبه المؤسسات في المجال المعلوماتي[4].

خامسا: الظروف المشددة للعقوبة

شدّد المشرّع الجزائري العقوبة إذا اقترن الدخول أو البقاء غير المشروع بنتائج تمس سلامة النظام أو المعطيات، باعتبار أن الضرر في هذه الحالة يتجاوز مجرد التهديد إلى المساس الفعلي. ومن أبرز هذه الظروف حذف المعطيات أو تغييرها، بما يؤدي إلى الإخلال بتكاملها أو مصداقيتها.

---

[1]– نسيمة بطحي، مرجع سبق ذكره، ص 81

[2]المادة 394 مكرر 07من القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، المعدل و المتمم المتضمن قانون العقوبات، مرجع سابق

[3] Jean Devése, atteintes aux systèmes de traitement automatisé de données, Jurisclasseur, pénal, article 323-1 à 323-7,2, 1997.p 16.

[4]– المادة 394 مكرر 04 م07من القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، المعدل و المتمم المتضمن قانون العقوبات، مرجع سابق

كما تُضاعف العقوبة إذا أسفر الفعل الإجرامي عن تخريب نظام اشتغال النظام المعلوماتي، سواء عن طريق تعطيله، أو إدخال برامج خبيثة، أو إحداث خلل يمنع استغلاله كليًا أو جزئيًا، ويُنظر إلى هذه الأفعال على في الاعتداء العمدي على المعطيات الداخلية للنظام، بينما تتجسد الثانية في الاعتداء العمدي على المعطيات الخارجية المرتبطة بالنظام أنها اعتداء جسيم يحوّل الجريمة من جريمة خطر إلى جريمة ضرر.

ويبلغ التشديد أقصاه إذا استهدف الاعتداء أنظمة أو معطيات تتعلق بالدفاع الوطني أو بالهيئات والمؤسسات الخاضعة للقانون العام[1]، لما يشكله ذلك من مساس مباشر بأمن الدولة واستقرارها، الأمر الذي يبرر مضاعفة العقوبة المقررة قانونًا.

الفرع الثاني: السياسة الجنائية لتجريم الاعتداءات على أنظمة المعالجة الآلية للمعطيات في التشريع الجزائري

يُقصد بالاعتداء في هذا السياق كل سلوك غير مشروع يُوجَّه إلى أنظمة المعالجة الآلية للمعطيات، ويكون من شأنه إلحاق الضرر بالبيانات المعلوماتية أو بوظائف النظام ذاته، سواء تم ذلك من خلال المساس بسرية المعطيات، أو الإخلال بسلامة محتواها وتكاملها، أو عبر تعطيل كفاءة الأنظمة وقدرتها التشغيلية، بما يؤدي إلى عرقلة أدائها لوظيفتها على نحو طبيعي وسليم.

وغالبًا ما يتحقق الاعتداء على معطيات النظام في مرحلة لاحقة لولوج النظام والبقاء داخله دون وجه حق، الأمر الذي يجعل هذا الاعتداء يتخذ صورتين أساسيتين.

أولا: جريمة الاعتداء العمدي على المعطيات الداخلية للنظام

يتمثل محل النشاط الإجرامي في جريمة الاعتداء العمدي على المعطيات الداخلية للنظام في المعطيات أو البيانات التي تتم معالجتها آليًا داخل نظام معلوماتي معيّن، حيث تفقد هذه المعطيات صورتها التقليدية لتتحول إلى رموز وإشارات إلكترونية قابلة للتخزين والمعالجة والاسترجاع بواسطة الوسائل التقنية، ولا ينصرف الاعتداء في هذا الإطار إلى المعلومات في مضمونها الذهني أو المعرفي، وإنما إلى شكلها التقني باعتبارها عنصرًا رقميًا مدمجًا داخل النظام المعلوماتي[2].

ويقتصر نطاق هذه الجريمة على المعطيات الموجودة داخل نظام المعالجة الآلية ذاته، أي تلك المخزنة في وسائطه الداخلية أو المرتبطة مباشرة بوظائفه التشغيلية، دون أن يمتد إلى المعطيات الخارجية أو المتبادلة مع

---

[1]– المادة 394 مكرر 03 من القانون رقم 04–15 المؤرخ في 10 نوفمبر 2004، المعدل و المتمم المتضمن قانون العقوبات، مرجع سابق

[2]–أمال قارة، الجريمة المعلوماتية، مذكرة لنيل شهادة الماجستير في الحقوق، تخصص قانون عام، كلية الحقوق، جامعة الجزائر، 2002، ص 120.

أنظمة أخرى. ويُعزى ذلك إلى الطبيعة الخاصة للحماية الجنائية التي أقرّها المشرّع، والتي تهدف أساسًا إلى ضمان سلامة النظام المعلوماتي من الداخل وحماية موثوقية البيانات التي يحتويها.

وتُدرس هذه الجريمة من خلال تحليل ركنيها الأساسيين: الركن المادي والركن المعنوي، باعتبارهما الإطار القانوني الذي يُبنى عليه التجريم والعقاب.

01- الركن المادي لجريمة الاعتداء العمدي على المعطيات الداخلية للنظام

يتجسد الركن المادي لهذه الجريمة في صدور سلوك إجرامي إيجابي من شأنه المساس بالمعطيات الداخلية للنظام، وقد حدّد المشرّع الجزائري صور هذا السلوك على سبيل الحصر، وذلك في المادة 394 مكرر 3 من قانون العقوبات، حيث تتمثل هذه الصور في :**فعل الإدخال، وفعل المحو، وفعل التعديل.**

ويلاحظ أن المشرّع لم يشترط اجتماع هذه الأفعال لقيام الجريمة، بل اكتفى بتحقق أي صورة منها بشكل مستقل، متى ترتب عنها المساس بالمعطيات الداخلية للنظام، وهو ما يعكس اتساع نطاق الحماية الجنائية وتكيّفها مع الطبيعة التقنية للجرائم المعلوماتية.

أ-فعل الإدخال: يُقصد بفعل الإدخال كل نشاط غير مشروع يقوم به الجاني ويؤدي إلى إضافة معطيات أو بيانات جديدة إلى الدعامة التقنية المخصصة لتخزين المعلومات المعالجة آليًا داخل النظام .ويستوي في ذلك أن تكون المعطيات المضافة وهمية لا أساس لها من الصحة، أو أن تكون معطيات حقيقية أُدخلت إلى جانب بيانات قائمة سلفًا، متى كان من شأن هذا الإدخال الإضرار بسلامة البيانات أو التشويش على صحتها أو إرباك وظائف النظام.ولا يُشترط لتحقق هذه الصورة من صور الاعتداء أن يترتب عنها ضرر فعلي، بل يكفي أن يكون الفعل من شأنه تعريض المعطيات للخطر أو المساس بمصداقيتها، وذلك انسجامًا مع الطابع الوقائي للتجريم في مجال الجرائم المعلوماتية، كما لا يُعتدّ بالوسيلة المستعملة في الإدخال، سواء تمت عبر برامج خبيثة، أو أوامر تقنية، أو استغلال صلاحيات ممنوحة على نحو غير مشروع، ما دام الأثر الإجرامي قد تحقق داخل النظام.، ويُعد فعل الإدخال من أخطر صور الاعتداء، لما له من تأثير مباشر على الثقة في البيانات المعلوماتية، إذ قد يؤدي إلى اتخاذ قرارات خاطئة أو إحداث اضطراب في سير المرفق أو النشاط الذي يعتمد على هذ ه المعطيات[1].

و غالبًا ما تُرتكب جريمة إدخال المعطيات غير المشروعة من قبل أشخاص يتمتعون بمكانة وظيفية تمكّنهم من النفاذ المشروع إلى الأنظمة المعلوماتية، وعلى رأسهم المسؤولون عن الأقسام المعلوماتية أو المالية داخل المؤسسات، ولا سيما أولئك الذين تُسند إليهم مهام المحاسبة ومعالجة المعاملات المالية. إذ يضعهم هذا الموقع

[1]-آمنة امحمدي بوزينة، خصوصية قواعد التجريم عن الاعتداء على أنظمة المعالجة الآلية للمعطيات في إطار التشريع الجزائري، *مجلة ببليوفيليا لدراسات المكتبات والمعلومات*، جامعة العربي التبسي، تبسة، الجزائر، العدد 4، ص. 88.

الوظيفي في وضع مميّز يسهّل عليهم التلاعب بالمعطيات الرقمية واستغلال النظام المعلوماتي لتحقيق أغراض غير مشروعة، مستفيدين من الثقة الممنوحة لهم وصعوبة اكتشاف أفعالهم في كثير من الأحيان.

ويتجسد هذا السلوك الإجرامي، على سبيل المثال، في إساءة استعمال الوسائل الإلكترونية المرتبطة بالمعاملات البنكية، كأن يقوم الحائز الشرعي لبطاقة السحب الممغنطة باستخدام رقمه السري للدخول إلى أجهزة الصرف الآلي، ثم إجراء عمليات سحب تتجاوز الرصيد الحقيقي المتوفر في حسابه. كما يتحقق الفعل ذاته في حالة الاستعمال غير المشروع لبطاقات الائتمان، عندما يتجاوز حاملها الحد الائتماني المسموح به عن طريق إدخال بيانات أو أوامر غير مطابقة للوضع المالي الحقيقي.

وتتخذ جريمة إدخال المعطيات المصطنعة صورًا عملية أخرى داخل المؤسسات، من بينها قيام المسؤول المعلوماتي بإضافة أسماء مستخدمين وهميين إلى قواعد البيانات، أو الإبقاء عمدًا على حسابات مستخدمين غادروا مناصبهم الوظيفية، بما يسمح بتوجيه العمليات أو الاستفادة من الموارد المالية بطرق غير مشروعة.

كما يتحقق فعل الإدخال كذلك في كل حالة يتم فيها إدراج برامج أو تعليمات إلكترونية دخيلة على النظام، كإدخال فيروسات أو برمجيات خبيثة، من شأنها توليد معطيات جديدة أو تعديل البيانات القائمة، بما يؤدي إلى الإخلال بسلامة النظام المعلوماتي ووظائفه[1].

ب- فعل المحو

يُقصد بفعل المحو كل سلوك إجرامي يترتب عليه إعدام أو إزالة المعطيات المخزنة داخل نظام المعالجة الآلية للمعطيات، سواء تم ذلك بشكل كلي أو جزئي، متى كان من شأنه المساس بسلامة البيانات أو تعطيل الوظيفة الطبيعية للنظام. ولا يقتصر المحو على الشطب المباشر للمعلومات، بل يشمل كذلك كل تصرف يؤدي إلى فقدان المعطيات لقيمتها أو قابليتها للاستعمال.

ويتخذ فعل المحو صورًا متعددة، من بينها إزالة جزء من البيانات المسجلة على الدعامة الإلكترونية، أو إتلافها تقنيًا عبر تعطيل وسائط التخزين أو تحطيمها، كما يتحقق أيضًا بنقل المعطيات من موضعها الأصلي إلى مكان آخر دون ترخيص، أو تخزينها بطريقة تؤدي إلى حرمان النظام أو مستعمله الشرعي من الوصول إليها أو الاستفادة منها.

ولا يُشترط في تحقق فعل المحو استعمال وسيلة تقنية معيّنة، إذ قد يتم باستخدام أوامر برمجية مباشرة، أو عن طريق برامج خبيثة، أو باستغلال صلاحيات الدخول المخوّلة للجاني على نحو غير مشروع، كما لا يُشترط أن يكون المحو نهائيًا أو غير قابل للاسترجاع، بل يكفي أن يؤدي الفعل إلى إحداث اضطراب فعلي أو محتمل في سلامة المعطيات أو في انتظام عمل النظام.

---

[1]- عبد الفتاح بيومي حجازي، مرجع سابق، ص .70.

ويُعد فعل المحو من أخطر صور الاعتداء على المعطيات الداخلية للنظام، لما يترتب عليه من نتائج جسيمة، خاصة عندما يتعلق الأمر ببيانات حيوية ذات طابع مالي أو إداري أو أمني، إذ قد يؤدي إلى شلل جزئي أو كلي في نشاط المؤسسة أو المساس بحقوق الغير ومصالحهم المشروعة.

قد يتحقق فعل المحو من خلال نقل جزء من المعطيات من مواقعها الأصلية إلى مناطق مخصصة للذاكرة أو إلى مساحات تخزين معزولة، بما يؤدي إلى تعطيل إمكانية الوصول إليها أو استغلالها، وهو ما يعادل من حيث الأثر القانوني إزالة البيانات أو إفناءها. ويُلاحظ في هذا السياق أن المحو يُعدّ عملية لاحقة منطقيًا وزمنيًا على إدخال المعطيات، إذ يفترض وجودًا سابقًا للبيانات داخل النظام، فلا يتصور قيام فعل المحو في غياب معطيات سبق إدخالها أو معالجتها آليًا.

ويملك الأشخاص المكلّفون قانونًا بحفظ البيانات وإدارتها قدرة تقنية تمكّنهم، في حال إساءة استعمال صلاحياتهم، من إتلاف أو القضاء على المعلومات المخزنة داخل النظام المعلوماتي، سواء عبر محوها كليًا أو جزئيًا، أو من خلال التلاعب بوسائط التخزين التي تحتويها. وقد يتم هذا السلوك الإجرامي بأساليب تقنية متعددة، من بينها العبث بالشرائط أو الأقراص الممغنطة، أو تعطيل قواعد البيانات، أو إفساد بنيتها الداخلية على نحو يجعل المعطيات غير قابلة للاستعمال.

ويستلزم تحقق فعل المحو، من الناحية الواقعية، وجود معطيات خاضعة للمعالجة الآلية، إذ يستحيل تصور محو بيانات غير موجودة أصلًا داخل النظام، كما يفترض هذا الفعل قيام الجاني بعملية دخول إلى النظام المعلوماتي، سواء كان هذا الدخول مشروعًا في الأصل ثم تم تجاوزه باستعمال الصلاحيات الممنوحة على نحو غير مشروع، أو كان دخولًا غير مصرح به تم تحقيقه عن طريق الاختراق أو التحايل التقني.

وعليه، فإن فعل المحو يرتبط ارتباطًا وثيقًا بمسألة النفاذ إلى النظام والبقاء داخله، وهو ما يجعله من أخطر صور الاعتداء على المعطيات الداخلية، لكونه يجمع بين إساءة استعمال الحق في الولوج أو انتهاكه أصلا، وبين النتيجة المتمثلة في إعدام أو تعطيل البيانات محل الحماية الجنائية[1].

ج- فعل التعديل: يُقصد بفعل التعديل في سياق الجرائم المعلوماتية كل عمل يُحدث تغييرًا مقصودًا في المعطيات المخزنة داخل النظام المعلوماتي، بحيث يتم استبدال البيانات الأصلية أو تعديلها أو إدخال بيانات جديدة غير صحيحة. ويمكن أن يتم ذلك مباشرة على المعطيات أو عن طريق التلاعب بالبرامج، أي تعديل طريقة عملها أو تزويدها بمعطيات تؤدي إلى نتائج مخالفة لما صُممت من أجل[2].

---

[1]- مولاي ملياني دلال، إشكالية الإثبات في جرائم الإنترنت في التشريع الجزائري، أطروحة لنيل الدكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة تلمسان، 2018/2017، ص 122.

[2]- عبد الفتاح بيومي حجازي، مرجع سابق، ص .386.

ويُعتبر فعل التعديل من الأفعال التي تهدد سلامة النظام المعلوماتي وأمان البيانات، إذ أن أي تغيير غير مشروع قد يُحدث نتائج خطيرة مثل فقدان المعلومات، تعطيل العمليات، أو التلاعب في المعاملات الإلكترونية، وهو ما يشكل تهديدًا مباشرًا للأمن المعلوماتي للأفراد والمؤسسات على حد سواء.

ويتحقق فعل التعديل عادة باستخدام أدوات برمجية متخصصة منها[1] برامج محو البيانات أو برامج الإتلاف : تُستخدم لمحو المعطيات كليًا أو جزئيًا، وهو ما يؤدي إلى فقدان المعلومات المهمة أو تعطيل العمليات، الفيروسات والبرمجيات الخبيثة :من أبرزها:فيروس حصان طروادة :يتميز بقدرته على التسلل إلى النظام دون اكتشافه، ويتيح للمهاجم التحكم في المعطيات أو تعديلها حسب هدفه، فيروس الدودة :(Worm) برنامج قادر على الانتشار الذاتي داخل النظام الشبكي وتعطيل الحواسيب، مما يتيح التلاعب بالبيانات على نطاق واسع، القنابل المعلوماتية الموجهة للبيانات :برمجيات أو أدوات تقنية تهدف خصيصًا إلى تغيير المعطيات أو تعديل نتائج العمليات الحسابية في النظام[2].

وتُظهر هذه الوسائل مدى التعقيد التقني للأدلة الرقمية، مما يجعل التثبت من وقوع الجريمة وتحليل آثارها تحديًا أمام القضاء، ويتطلب خبرة تقنية متخصصة.

أما آثار فعل التعديل ينتج عن فعل التعديل آثار قانونية ومادية خطيرة على النظام المعلوماتي:

التغيير في نتائج العمليات الحسابية أو الإلكترونية، مثل التلاعب في الحسابات البنكية أو البيانات الحكومية.

إلحاق ضرر بالمعطيات الأصلية سواء بشكل كلي أو جزئي، ما يؤدي إلى فقدان الثقة في نظم المعلومات.

تعطيل النظام المعلوماتي، خصوصًا عند استخدام الفيروسات أو الديدان، ما قد يوقف العمليات بشكل كامل ويؤثر على سير الأعمال أو الخدمات الإلكترونية.

ويشترط لقيام الركن المعنوي في جريمة الاعتداء على المعطيات المعلوماتية توافر القصد الجنائي العام المتمثل في العلم والإرادة، إلى جانب نية الغش التي تعكس الطابع غير المشروع للسلوك الإجرامي. غير أن اشتراط نية الغش لا يعني بالضرورة وجوب توافر قصد إلحاق الضرر بالغير، إذ إن المشرّع لا يجعل من تحقق الضرر عنصرًا لازمًا لقيام الجريمة.

وتتحقق الجريمة متى أقدم الجاني، عن علم وإرادة، على أحد الأفعال المجرّمة المتمثلة في إدخال المعطيات أو محوها أو تعديلها داخل النظام المعلوماتي، وهو مدرك تمامًا لعدم مشروعية فعله، وعالم بأن هذا السلوك يتجاوز الصلاحيات المخولة له قانونًا أو تعاقديًا. ويكفي في هذا الإطار أن يتجه قصد الفاعل إلى ارتكاب الفعل ذاته مع علمه بحظره، دون حاجة إلى إثبات نيته في إحداث نتيجة ضارة معينة.

---

[1]– عبد الفتاح بيومي حجازي، مرجع سابق، ص .388.

[2]–حسن طاهري، مرجع سبق ذكره، ص75.

أما الضرر، ورغم أنه قد يتحقق فعليًا كنتيجة طبيعية للنشاط الإجرامي، فإنه لا يُعد عنصرًا مكوّنًا للجريمة، ولا يشترط لقيامها. فالجريمة تقوم وتكتمل أركانها بمجرد المساس غير المشروع بسلامة المعطيات، باعتبار أن المصلحة القانونية المحمية تتمثل أساسًا في حماية الثقة في الأنظمة المعلوماتية وضمان سلامة البيانات، وليس فقط في تفادي الضرر المادي أو المعنوي اللاحق بالغير[1].

وعليه، فإن جريمة الاعتداء على المعطيات تُصنّف ضمن الجرائم الشكلية التي يُعاقب عليها لمجرد تحقق السلوك الإجرامي المقرون بالعلم بعدم المشروعية، بصرف النظر عن النتائج المترتبة عنه، الأمر الذي يعكس توجه المشرّع نحو توفير حماية وقائية متقدمة للمنظومة المعلوماتية.

ثانيا: جريمة الاعتداء على المعطيات الخارجية للنظام

يقصد بالمعطيات الخارجية لنظام المعالجة تلك البيانات والمعلومات التي تُستخدم كمدخلات لتحقيق نتائج محددة ضمن النظام المعلوماتي، بحيث تساهم هذه المعطيات مباشرة في العمليات الحسابية أو المنطقية التي يقوم بها النظام، وتمثل الركيزة الأساسية لفعالية المعالجة الآلية للبيانات[2]،

01- الركن المادي للجريمة

يُستفاد من مضمون المادة 394 مكرر من قانون العقوبات الجزائري أن المشرّع قد حدّد الركن المادي لهذه الجريمة **في** صورتين أساسيتين.

أ-الصورة الأولى: التعامل في المعطيات غير المشروعة تتمثل هذه الصورة في كل سلوك ينصب على التعامل غير المشروع في المعطيات، حيث قررت المادة 394 مكرر 2 فقرة 01 من قانون لعقوبات السالف اذكر على معاقبة كل من يقوم، عن *قصد* أو بطريق الغش، بأحد الأفعال المتمثلة في تصميم، أو البحث عن، أو تجميع، أو توفير، أو نشر، أو الاتجار في معطيات تكون مخزنة أو معالجة أو مرسلة بواسطة منظومة معلوماتية، متى كانت هذه المعطيات صالحة أو قابلة للاستعمال في ارتكاب الجرائم المنصوص عليها في هذا القسم من قانون العقوبات.

ويكفي لقيام النشاط الإجرامي أن يأتي الجاني أحد هذه الأفعال دون اشتراط تحقق نتيجة معينة، إذ ينصب محل الجريمة على المعطيات ذاتها، بغض النظر عن شكلها أو وسيط تخزينها، سواء كانت محفوظة على

---

[1]- نسيمة جدي، جرائم المساس بأنظمة المعالجة الألية للمعطيات، رسالة ماجستير في القانون الجنائي، كلية الحقوق، جامعة وهران، 2014/2013، ص 69.

[2]- جمال براهيمي: "مكافحة الجرائم الالكترونية في التشريع الج ازئري"، المجلة النقدية، جامعة مولود معمري، تيزي وزو، الجزائر، المجلد 88، العدد 20، نوفمبر 2016.، ص135.

أشرطة أو أقراص رقمية، أو كانت محل معالجة آلية، أو تم إرسالها عبر شبكة معلوماتية، ما دامت قابلة لأن تُستعمل كوسيلة لارتكاب الجرائم المقررة في القسم السابع مكرر من قانون العقوبات[1].

وعليه، فإن مجرد التعامل في هذه المعطيات على النحو الذي حدده النص القانوني يُعد كافيًا لقيام الركن المادي للجريمة، دون حاجة لإثبات استعمالها الفعلي في ارتكاب الجريمة محل الحماية التشريعية.

ويقصد بالتصميم كل عمل يهدف إلى إنشاء أو ابتكار معطيات أو أدوات معلوماتية قابلة للاستخدام في ارتكاب الجريمة، مثل إعداد الفيروسات، والبرمجيات الخبيثة، وبرامج الاختراق والقرصنة، وغالبًا ما يصدر هذا السلوك عن أشخاص يمتلكون خبرات تقنية متقدمة، كمهندسي البرمجيات أو المختصين في الإعلام الآلي.

أما البحث فينصرف إلى كل نشاط يرمي إلى التنقيب أو التحري عن المعطيات والمعلومات التي يمكن توظيفها في ارتكاب الجريمة، سواء تم ذلك عبر الشبكات المعلوماتية أو من خلال قواعد البيانات المختلفة.

ويقصد بالتجميع جمع عدد من المعلومات أو المعطيات ذات الصلة، وربطها ببعضها البعض، وإعدادها بطريقة تجعلها صالحة للاستعمال الإجرامي، مع وضعها في متناول الغير.

في حين يعني التوفير إتاحة هذه المعطيات وعرضها للغير بأي وسيلة كانت، بما يسمح بالوصول إليها أو الحصول عليها.

أما النشر فيتمثل في بث أو إذاعة المعطيات محل الجريمة، وتمكين عدد غير محدد من الأشخاص من الاطلاع عليها عبر مختلف وسائل النشر الإلكترونية أو الرقمية.

ويقصد بالاتجار كل تعامل يقوم على تقديم المعطيات مقابل عوض، سواء كان هذا العوض ماديًا أو عينيًا أو في صورة خدمات، وذلك بقصد استخدامها في أغراض غير مشروعة.

ب–الصورة الثانية: التعامل في معطيات متحصلة من جريمة

تتمثل الصورة الثانية من الركن المادي في جريمة التعامل في معطيات صالحة لارتكاب الجريمة، حيث قررت الفقرة الثانية من المادة 394 مكرر 02 من قانون العقوبات الجزائري تجريم كل سلوك ينصب على حيازة أو إفشاء أو نشر أو استعمال، لأي غرض كان، للمعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم[2].

ويُعد كل واحد من هذه الأفعال نشاطًا إجراميًا مستقلاً، تقوم به الجريمة متى توافر القصد الجنائي، بغض النظر عن الغاية التي توخاها الجاني من التعامل في هذه المعطيات، الأمر الذي يعكس تشدد المشرّع في حماية المعطيات ومنع إعادة توظيفها في أنشطة غير مشروعة

---

[1]– مختارية بوزيدي: "ماهية الجريمة الالكترونية"، الملتقى الوطني حول: آليات مكافحة الجرائم الالكترونية في التشريع الجزائري مركز جيل البحث العلمي، الجزائر 01 مارس ،2017 ص 18.

[2]– قسمية محمد، وخضري، حمزة. مكافحة الجرائم الماسة بنظام المعالجة الآلية للمعلومات في القانون الجزائري، *مجلة صوت القانون*، جامعة خميس مليانة، الجزائر، المجلد 27، العدد 20، نوفمبر 2020، ص ص 140 ومابعدها.

يقصد ب**الحيازة** خضوع المعطيات المتحصلة من إحدى الجرائم المعلوماتية لسيطرة الجاني الفعلية، بحيث تدخل ضمن نطاق إشرافه وتحكمه المباشر، ولا تقوم الحيازة إلا إذا اقترنت بعنصر العلم، إذ يستحيل تصور حيازة قانونية أو غير قانونية لمعلومات يجهل الشخص طبيعتها أو وجودها، ذلك أن السيطرة المجردة دون إدراك لا تكفي لقيام هذا الوصف.

أما الإفشاء فيتمثل في كل تصرف يؤدي إلى نقل أو تسريب المعطيات التي تم الحصول عليها بطرق غير مشروعة إلى الغير، سواء تم ذلك بصورة مباشرة أو غير مباشرة، وبأي وسيلة كانت، مما يترتب عليه توسيع دائرة الاطلاع غير المشروع على هذه المعلومات.

وبخصوص **النشر**، فقد اتجه المشرّع إلى تضييق نطاق الأشخاص الذين يجوز لهم الوصول إلى المعطيات المتحصلة من الجرائم المعلوماتية، فجرّم كل فعل من شأنه إتاحة هذه المعلومات أو بثّها لجمهور غير محدد، ويُعد هذا السلوك الفعل المشترك الوحيد بين صورتي جريمة التعامل في المعطيات غير المشروعة وجريمة التعامل في المعطيات المتحصلة من جريمة.

أما الاستعمال فيُعد أخطر صور التعامل في المعطيات غير المشروعة، إذ لا يقتصر على مجرد الحيازة أو الإفشاء أو النشر، بل يتعدى ذلك إلى توظيف هذه المعطيات فعليًا لتحقيق أغراض غير مشروعة. وتتجلى خطورة هذا السلوك بوجه خاص في المجال الاقتصادي، كما هو الحال عند لجوء إحدى الشركات إلى استغلال معطيات سرية تخص شركة منافسة لها، بما يمس بمبدأ المنافسة المشروعة ويخل بالتوازن الاقتصاد[1].

ثانيا: الركن المعنوي

يُستفاد من مضمون المادة 394 مكرر 02 من قانون العقوبات الجزائري أن جريمة الاعتداء العمدي على المعطيات الخارجية للنظام المعلوماتي تُعد من الجرائم العمدية، التي يشترط لقيامها توافر القصد الجنائي العام لدى الجاني، ويتجلى هذا القصد من خلال استعمال المشرّع لعبارتي "عمداً" و"عن طريق الغش"، بما يدل على ضرورة توافر عنصري العلم والإرادة.

ويقتضي ذلك أن يكون الجاني على علم بطبيعة المعطيات التي يتعامل معها، وأن يُدرك عدم مشروعية هذا التعامل، فضلًا عن علمه بأن سلوكه من شأنه المساس بالمصلحة القانونية محل الحماية. كما يجب أن تتجه إرادته الحرة إلى ارتكاب الفعل المجرّم رغم إدراكه لما ينطوي عليه من مخالفة للقانون.

ولا يُشترط لقيام هذه الجريمة توافر قصد خاص يتمثل في نية إحداث ضرر معين، إذ يكفي أن يثبت علم الفاعل بعدم مشروعية المعطيات أو بإمكان استخدامها في ارتكاب جرائم أخرى، أو كونها متحصلة من جريمة

[1]–عباس كريمة، جرائم المساس بأنظمة المعالجة الألية للمعطيات، مجلة البيان للدراسات القانونية و السياسية، العدد04، ديسمبر 2017، ص 127.

سابقة. فمتى تحقق هذا العلم واقترنت به الإرادة، انعقد الركن المعنوي للجريمة، بغض النظر عن النتائج التي قد تترتب فعليًا عن هذا السلوك.
وعليه، فإن القصد الجنائي العام يُعد كافيًا لقيام جريمة الاعتداء على المعطيات الخارجية للنظام، الأمر الذي يعكس توجه المشرّع نحو توفير حماية وقائية موسعة للمعطيات والأنظمة المعلوماتية، دون تعليق التجريم على تحقق ضرر فعلي.

يشترط لقيام الركن المعنوي في جريمة التعامل في المعطيات غير المشروعة أن يكون الفاعل على علم بالطبيعة غير القانونية للمعلومات التي يتعامل معها، وأن يُدرك أن هذا السلوك من شأنه المساس بالمصلحة القانونية محل الحماية. ويتحقق هذا العلم سواء تعلق الأمر بالصورة الأولى للجريمة، حيث تكون المعطيات قابلة للاستعمال في ارتكاب جرائم معلوماتية، أو بالصورة الثانية، عندما ينصب التعامل على معطيات متحصلة من إحدى جرائم الاعتداء على نظام المعالجة الآلية للمعطيات، بما يؤدي إلى مضاعفة أو تفاقم الأضرار المترتبة عن الجريمة الأصلية.
ولا يقتصر الأمر على مجرد إدراك الفاعل لوجود المعطيات، بل يتعين أن يكون عالمًا بعدم مشروعيتها، سواء لكونها وسيلة محتملة لارتكاب جريمة، أو لأنها ناتجة عن نشاط إجرامي سابق. فإذا ثبت هذا العلم، واتجهت إرادة الجاني الحرة إلى التعامل في هذه المعطيات رغم ذلك، انعقدت الجريمة وتحققت أركانها القانونية دون حاجة لإثبات نية خاصة.
أما من حيث القصد الجنائي الخاص، فإن جريمة التعامل في معطيات متحصلة من جريمة لا تستلزم توافره، ذلك أن الصفة غير المشروعة لهذه المعطيات تكون قائمة وثابتة بذاتها، مما يجعل القصد الجنائي العام كافيًا لقيام الجريمة، ولا يُسأل الفاعل عن غاية معينة أو هدف خاص من وراء هذا التعامل.
ومن جهة أخرى، لم يضع المشرّع الجزائري نصًا خاصًا يُجرّم صراحة الاعتداء العمدي على السير العادي لنظام المعالجة الآلية للمعطيات، غير أن هذا الاعتداء قد يتخذ عدة صور عملية، من أهمها التعطيل، الذي قد يصيب العناصر المادية للنظام، كتحطيم وسائط التخزين أو قطع شبكات الاتصال، أو يمتد إلى العناصر المنطقية، كالبرامج والمعطيات، وذلك باستخدام فيروسات أو برمجيات خبيثة تؤدي إلى شلّ عمل النظام كليًا أو جزئيًا[1].

[1]– يوسف دلاندة ،قانون العقوبات، دار هومة للطباعة والنشر والتوزيع ،2006، ص 276.

المبحث الثالث : مواجهة الجريمة المعلوماتية القانون رقم 04/09

أمام التطور المتسارع لتكنولوجيات الإعلام والاتصال، وما أفرزه من أنماط إجرامية جديدة لم تكن القواعد القانونية التقليدية كافية لمواجهتها، تدخل المشرّع الجزائري من خلال استحداث إطار قانوني خاص يهدف إلى تدارك النقائص التشريعية السابقة. وفي هذا السياق صدر القانون 09–04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[1]، والذي جاء مكملاً ومصححاً لما ورد في قانون 15/04. ويُلاحظ أن هذا القانون قد أحدث تحولاً جوهرياً في تحديد مفهوم الجريمة المعلوماتية، إذ لم يعد يقتصر على الجرائم التي تمس مباشرة أنظمة المعالجة الآلية للمعطيات، وإنما اعتمد مفهوماً موسعاً يأخذ بعين الاعتبار مختلف صور الاستعمال غير المشروع للوسائط التكنولوجية الحديثة، فقد عرّفت **المادة 02** من القانون الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بأنها الجرائم التي تمس بأنظمة المعالجة الآلية للمعطيات، إضافة إلى كل جريمة أخرى تُرتكب أو يُسهَّل ارتكابها بواسطة منظومة معلوماتية أو نظام للاتصالات الإلكترونية.
ومن خلال هذا التعريف، يتضح أن المشرّع الجزائري قد انتقل من مفهوم تقني ضيق للجريمة المعلوماتية إلى مفهوم قانوني شامل، يمتد ليشمل ليس فقط الجرائم الواقعة على الأنظمة المعلوماتية ذاتها، وإنما كذلك الجرائم التي تُستخدم فيها هذه الأنظمة كوسيلة أو أداة لتنفيذ السلوك الإجرامي. ويشمل ذلك مختلف وسائل الاتصال الحديثة، سواء كانت شبكات الإنترنت أو أنظمة الاتصال الإلكترونية أو الهواتف النقالة والثابتة.

وعليه، فإن كل جريمة يكون النظام المعلوماتي محلاً لها، أو وسيلة لارتكابها، أو عاملاً مسهلاً في تنفيذها، تُعدّ جريمة متصلة بتكنولوجيات الإعلام والاتصال. ويعكس هذا التوسيع إرادة المشرّع في مواكبة المستجدات التقنية، وضمان حماية فعالة للمصالح الفردية والجماعية من المخاطر المتزايدة للجرائم الإلكترونية.
إلى جانب ذلك، لم يقتصر القانون 09–04 على الجانب الموضوعي فقط، بل تضمّن أيضاً أحكاماً إجرائية خاصة تهدف إلى تعزيز فعالية المتابعة الجزائية في هذا النوع من الجرائم، حيث جمع بين القواعد الإجرائية الواردة في قانون الإجراءات الجزائية، وبين آليات وقائية حديثة تسمح بالكشف المبكر عن الاعتداءات المعلوماتية المحتملة، والتدخل السريع لتحديد مصادرها، والحد من آثارها أو منع وقوعها متى أمكن ذلك.

[1]– قانون رقم 09 – 04 مؤرّخ في 5 أوت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية رقم 47، المؤرخة في 16 أوت 2009.

المطلب الأول: **توسّع المفهوم القانوني للجريمة المعلوماتية ليشمل الجرائم التقليدية المرتكبة عبر الوسائل الإلكترونية في ظل القانون رقم 09-04**

قبل صدور القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، كان مفهوم الجريمة المعلوماتية في النظام العقابي الجزائري مفهوماً ضيقاً ومحدوداً، إذ كان يقتصر حصراً على الأفعال التي تمس بأنظمة المعالجة الآلية للمعطيات، سواء تعلّق الأمر بالاعتداء على سلامة البيانات أو البرامج أو الأنظمة المعلوماتية ذاتها.

غير أن التطور المتسارع لتكنولوجيات الإعلام والاتصال، وما رافقه من توسّع في صور الإجرام المرتكب عبر الوسائط الإلكترونية، فرض على المشرع الجزائري إعادة النظر في هذا المفهوم الضيق. ولهذا الغرض، تبنّى المشرع بموجب القانون رقم 09-04 تعريفاً موسعاً للجريمة الإلكترونية، بحيث لم يعد يقتصر على الجرائم الواقعة مباشرة على الأنظمة المعلوماتية، وإنما امتد ليشمل كل جريمة تُرتكب أو يُسهَّل ارتكابها بواسطة منظومة معلوماتية أو نظام للاتصالات الإلكترونية، بما في ذلك وسائل الاتصال المختلفة كالهاتف الثابت والهاتف النقال وشبكات الاتصال الحديثة[1].

الفرع الأول: أصناف الجريمة المعلوماتية وفق القانون 04/09

وبناءً على هذا التوسّع التشريعي، يمكن تصنيف الجرائم المعلوماتية وفقاً لما جاء في القانون رقم 09-04 إلى ثلاثة أصناف رئيسية، وهي

الفرع الأول: **الجرائم الواقعة على أنظمة المعالجة الآلية للمعطيات**

وهي تلك التي يكون النظام المعلوماتي ذاته محلاً للاعتداء، كالدخول غير المشروع، أو الإتلاف، أو التعديل غير المرخص للبيانات والأنظمة.

الفرع الثاني: جرائم الوسيلة المعلوماتية

وهي الجرائم التي يُستخدم فيها النظام المعلوماتي كوسيلة أو أداة لتنفيذ الجريمة، دون أن يكون هو محل الاعتداء المباشر، كجرائم الاحتيال أو التزوير المرتكبة باستعمال الحاسوب.

[1]-بعجي عبدالنور، مرجع سبق ذكره، ص 121.

الفرع الثالث: جرائم الاتصال الإلكتروني

وهي الجرائم التي يتم تنفيذها عن طريق وسائل الاتصالات الإلكترونية، كشبكات الهاتف أو الإنترنت، مثل جرائم الابتزاز أو التشهير أو المساس بالحياة الخاصة عبر وسائل الاتصال الحديثة.

ومن خلال هذا التصنيف، يمكن استخلاص جملة من الملاحظات الأساسية أبرزها:

-أن المشرع الجزائري **اعتمد** معيار موضوع الجريمة لتحديد مفهوم الجريمة المعلوماتية، حيث اشترط أن يقع الاعتداء على نظام معلوماتي في الجرائم التي سمّاها صراحة بجرائم المساس بأنظمة المعالجة الآلية للمعطيات، ونظّمها في قانون العقوبات من المادة 394 مكرر إلى المادة 394 مكرر 07، ثم فتح المجال على مصراعيه ليشمل أي جريمة أخرى تُرتكب أو يُسهَّل ارتكابها بواسطة منظومة معلوماتية أو نظام للاتصالات الإلكترونية بموجب القانون رقم 09-04.

-أن المشرع لم يحدّد بدقة درجة أو مدى الدور الذي تلعبه المنظومة المعلوماتية أو نظام الاتصالات الإلكترونية في ارتكاب الجريمة، إذ يكفي – حسب النص – أن تكون الجريمة قد ارتُكبت أو سُهِّل ارتكابها بواسطة هذه الوسائل، وهو ما يؤدي إلى إدخال عدد كبير جداً من الجرائم ضمن نطاق الجرائم الإلكترونية، حتى تلك التي يكون فيها للتقنية المعلوماتية دور ثانوي أو عرضي.

كما أن المشرع لم يبيّن على نحو دقيق صور السلوك الإجرامي الذي يمكن أن يُرتكب أو يُسهَّل ارتكابه بواسطة منظومة معلوماتية أو نظام للاتصالات الإلكترونية، الأمر الذي أدى إلى توسّع كبير في دائرة التجريم، وأثار إشكالات فقهية وقضائية تتعلق بحدود مفهوم الجريمة الإلكترونية.

وبناءً على ما سبق، نرى أن التعريف الأقرب إلى الدقة والصواب للجريمة المعلوماتية يتمثل في اعتبارها: كل اعتداء موجّه ضد النظام المعلوماتي ذاته، أو كل اعتداء يُرتكب باستخدام النظام المعلوماتي أو وسائل الاتصالات الإلكترونية، شريطة أن يكون لهذه الوسائل دور أساسي وجوهري في تحقق السلوك الإجرامي ونتيجته، لا مجرد دور ثانوي أو عرضي.

بدايةً، يُلاحظ من خلال استقراء النصوص القانونية المنظمة للإجراءات الجزائية وجود تباين في النظام الإجرائي المطبق على جرائم المساس بأنظمة المعالجة الآلية للمعطيات من جهة، وجرائم تكنولوجيات الإعلام والاتصال من جهة أخرى. إذ تخضع الجرائم الأولى لكل من القواعد العامة الواردة في قانون الإجراءات الجزائية، إضافة إلى الإجراءات الخاصة المنصوص عليها في القانون رقم 09-04، في حين لا تمتد هذه الإجراءات الخاصة إلى جرائم تكنولوجيات الإعلام والاتصال بصفة عامة.

ويُعزى ذلك إلى أن قانون الإجراءات الجزائية عند تنظيمه لهذه الآليات الإجرائية قد أشار صراحة إلى جرائم المساس بأنظمة المعالجة الآلية للمعطيات دون غيرها، وهو أمر مفهوم بالنظر إلى أن النصوص التي تضمنت هذه الإجراءات صدرت قبل ظهور التنظيم التشريعي الخاص بجرائم تكنولوجيات الإعلام والاتصال، رغم التعديلات اللاحقة التي عرفها قانون الإجراءات الجزائية دون أن تشمل إخضاع هذه الجرائم لنفس النظام الإجرائي الخاص.

المطلب الثاني: الاجراءات التي أقرها القانون رقم 04/09

وفيما يتعلق بالإجراءات الخاصة التي أقرها القانون رقم 09-04، فقد تضمن هذا الأخير جملة من الآليات الإجرائية الرامية إلى الوقاية من الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال ومكافحتها، ويمكن إجمالها فيما يلي:

الفرع الأول: مراقبة الاتصالات الإلكترونية

خول القانون رقم 09-04 للسلطات المختصة إمكانية اللجوء إلى المراقبة الإلكترونية للاتصالات، وذلك لدواعي النظام العام أو لمقتضيات التحريات والتحقيقات القضائية، ضمن حالات محددة على سبيل الحصر. وتشمل هذه الحالات الوقاية من الجرائم الموصوفة بالإرهاب أو التخريب أو تلك الماسة بأمن الدولة، وكذا في حال توفر معلومات جدية عن احتمال وقوع اعتداء على منظومة معلوماتية من شأنه المساس بالنظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، إضافة إلى الحالات التي تستدعيها ضرورات البحث والتحقيق القضائي، أو في إطار التعاون الدولي القضائي[1]

وتتسم هذه المراقبة بطابعين أساسيين؛ طابع وقائي يُتخذ قبل وقوع الجريمة بهدف تفاديها، وطابع تحقيقي يُمارس بعد ارتكاب الجريمة عندما تقتضي متطلبات البحث ذلك. ونظراً لما ينطوي عليه هذا الإجراء من مساس بسرية وحرمة المراسلات، فقد أحاطه المشرع بجملة من الضمانات، أهمها حصر الحالات المبيحة له، وإخضاعه لرقابة السلطة القضائية، وتحديد نطاق استعمال المعطيات المتحصل عليها، فضلاً عن تجريم إفشاء المعلومات ذات الطابع الشخصي الناتجة عن المراقبة الإلكترونية.

ويقصد بالمراقبة الإلكترونية للاتصالات استخدام الوسائل التقنية اللازمة لتجميع وتسجيل محتوى الاتصالات بمختلف أشكالها، سواء عبر شبكة الإنترنت أو الهاتف أو غيرها من وسائل الاتصال الإلكترونية، على أن يتم هذا الإجراء أثناء إجراء الاتصال ذاته، أما الاطلاع اللاحق على هذه المعطيات فلا يعد مراقبة، وإنما يندرج ضمن إجراءات التفتيش.

---

[1]-اسماعيل بن يحي، التعريف بمراقبة الاتصالات الالكترونية كإجراء من اجراءات جمع الأدلة في الجريمة الالكترونية، مجلة صوت القانون ، المجلد 08، العدد 03، 2022، ص 1071،1070

الفرع الثاني: تفتيش المنظومة المعلوماتية

أجاز القانون رقم 09- 04 من خلال المادة 05 منه للسلطات القضائية المختصة وضباط الشرطة القضائية القيام بتفتيش المنظومات المعلوماتية أو جزء منها، وكذا المعطيات المخزنة فيها أو في منظومات التخزين المعلوماتية، وذلك في نفس الحالات التي تبرر اللجوء إلى المراقبة الإلكترونية، وقد استثنى المشرع هذه العمليات من بعض القواعد الإجرائية التقليدية للتفتيش المنصوص عليها في قانون الإجراءات الجزائية، مع الإبقاء على شرط الإذن القضائي، كما أجاز، في حالات الجرائم الإرهابية أو التخريبية أو الماسة بأمن الدولة، توسيع نطاق التفتيش إلى منظومات معلوماتية أخرى غير مشمولة بالإذن متى وجدت أسباب جدية للاعتقاد بأن المعطيات محل البحث مخزنة فيها، مع إعلام الجهة القضائية المختصة، وإمكانية طلب المساعدة القضائية الدولية إذا كانت هذه المنظومات موجودة خارج الإقليم الوطني[1].

الفرع الثالث: حجز المعطيات المعلوماتية

تُختتم عملية التفتيش بحجز المعطيات المعلوماتية التي من شأنها المساهمة في كشف الجريمة وتحديد مرتكبيها، ويجوز أن يشمل الحجز كامل المنظومة المعلوماتية أو جزءاً منها فقط، إما عن طريق نسخ المعطيات على دعامات مادية، أو بوضعها تحت الإحراز والختم وفق الإجراءات القانونية. وفي حال تعذر ذلك لأسباب تقنية، يمكن اتخاذ تدابير بديلة تتمثل في منع الوصول إلى المعطيات أو تقييد استعمالها، مع اتخاذ كل الوسائل الكفيلة بحمايتها من الإتلاف أو التغيير إلى حين اتخاذ الإجراءات اللازمة لاستخراج الدليل[2].

المبحث الرابع: مواجهة الجريمة المعلوماتية وفق 07/18[3] المتعلق بالمعطيات الشخصية

لقد تنبّه المشرّع الجزائري إلى المخاطر المتزايدة التي باتت تهدد المعطيات ذات الطابع الشخصي، فسارع إلى إصدار قانون خاص يهدف إلى توفير حماية كافية للحياة الخاصة للأشخاص الطبيعيين. وقد أفرد هذا القانون بابًا كاملًا للأحكام الجزائية، يمتد من المادة 54 إلى المادة 74، بيّن من خلاله مختلف الجرائم التي يمكن أن تمسّ بالمعطيات الشخصية، إلى جانب العقوبات المقررة لردع مرتكبيها.

المطلب الأول : الجرائم المرتبطة بعدم احترام الشروط الشكلية للمعالجة

---

[1] – ليندا بن طالب، التفتيش في الجريمة المعلوماتية، مجلة العلوم القانونية و السياسية، المجلد 08، العدد02، 2017، ص ص 490 وما بعدها

[2] –فلاح عبدالقادر، حجز وحفظ المعطيات في الجريمة الالكترونية، مجلة صوت القانون، المجلد 08، العدد01، 2021، ص ص 179 وما بعدها

[3] – القانون رقم 18–07 مؤرخ في 25 رمضان عام 1439 هـ، الموافق لـ 10 يونيو 2018، ويتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية رقم 34 الصادرة بتاريخ 10 يونيو2018.

الفرع الأول: جريمة معاجلة المعطيات الشخصية دون موافقة أو رغم اعتراض الشخص المعني

أخضع القانون رقم 18- 07 من خلال المادة 07 و 36 منه عملية معالجة المعطيات الشخصية لضرورة الحصول على رضا صريح من الشخص المعني، كما خوّله حق الاعتراض متى وُجدت أسباب مشروعة لذلك، ويؤدي تجاوز هذا الشرط، سواء بإجراء المعالجة دون موافقة أو بالاستمرار فيها رغم الاعتراض، إلى قيام الجريمة المنصوص عليها قانونًا.

وتشتد الحماية إذا تعلق الأمر بالمعطيات الحساسة وفق المادة 18 من القانون 07/18 ، إذ يُحظر أصلا معالجتها، ولا يُستثنى من ذلك إلا حالة الموافقة الصريحة من الشخص المعني، وبالتالي فإن مباشرة معالجة هذا النوع من المعطيات دون موافقته يُعد فعلا مجرّمًا بذاته.

الفرع الثاني:جريمة انجاز معالجة للمعطيات الشخصية دون الحصول على تصريح أو ترخيص

أوجب القانون إخضاع بعض عمليات المعالجة لإجراء مسبق يتمثل في التصريح أو الحصول على ترخيص من الجهة المختصة، وهي السلطة الوطنية لحماية المعطيات الشخصية

وعليه، فإن الشروع في المعالجة دون استكمال هذا الإجراء يشكل جريمة قائمة الأركان.

ويمتد التجريم كذلك إلى حالات الإدلاء بتصريحات غير صحيحة، أو مواصلة النشاط رغم سحب وصل التصريح أو إلغاء الترخيص الممنوح، لما في ذلك من تحايل على الرقابة القانونية[1].

ثانيًا: الجرائم المتعلقة باجراءات الحماية والتعاون مع السلطة الوطنية

01- جريمة عدم الالتزام بسلامة وسرية المعالجة للمعطيات الشخصية

حمّل المشرّع المسؤول عن المعالجة التزامًا صريحًا بضمان أمن المعطيات وسريتها، من خلال اتخاذ تدابير تقنية وتنظيمية فعالة تحول دون إتلافها أو ضياعها أو تسريبها أو الولوج غير المشروع إليها. وتشمل هذه التدابير، على سبيل المثال، أنظمة التشفير، كلمات المرور، وبرامج الحماية المعلوماتية.

كما ألزمه، في حال إسناد المعالجة إلى متعهد من الباطن، باختيار جهة تتوفر على ضمانات كافية في مجال الأمن المعلوماتي، مع تنظيم العلاقة بعقد رسمي يحدد الالتزامات بدقة. وأي تقصير في هذه الجوانب يعرّض المسؤول للمتابعة الجزائية[2].

---

[1]- المادة 56 من القانون 07/18 المتعلق بحماية المعطيات ذات الطابع الشخصي.

[2]- المواد38،65، 39 من القانون 07/18

02- جريمة عرقلة عمل السلطة وعدم الإبلاغ عن الانتهاكات

حرص المشرّع على تمكين السلطة الوطنية لحماية المعطيات الشخصية من أداء مهامها الرقابية، فجرّم كل سلوك من شأنه عرقلة عملها. ويتجسد ذلك في منع أعضائها من القيام بعمليات التفتيش والمعاينة، سواء بوسائل مادية كمنع الدخول إلى المقرات، أو بوسائل تقنية مثل الامتناع عن تسليم كلمات المرور أو تعطيل الأنظمة المعلوماتية.

كما يشمل التجريم رفض تزويدها بالوثائق والمعلومات الضرورية، أو تقديم بيانات غير مطابقة للحقيقة، أو إخفاء المستندات ذات الصلة.

ومن جهة أخرى، ألزم القانون مقدمي الخدمات بإخطار السلطة الوطنية، بل وحتى الشخص المعني، بكل خرق يمس المعطيات الشخصية، كحالات الإتلاف أو الضياع أو الإفشاء أو الولوج غير المشروع.

ويُعد الامتناع عن هذا الإبلاغ سلوكًا مجرّمًا لما له من أثر مباشر على حقوق الأفراد وحرياتهم.

وبذلك يتضح أن المشرّع لم يكتفِ بتجريم الأفعال الماسة بجوهر المعالجة، بل وسّع نطاق الحماية ليشمل الإجراءات الوقائية وآليات الرقابة، تكريسًا لحماية فعالة للمعطيات ذات الطابع الشخصي[1].

المطلب الثاني: الجرائم املتعلقة بالقواعد الموضوعية للمعاجلة

الفرع الأول: جرائم الجمع غير المشروع للمعطيات الشخصية

أولا: جمع المعطيات بوسائل غير مشروعة

يُعدّ استعمال الطرق التدليسية أو غير النزيهة أو المخالفة للقانون في جمع المعطيات ذات الطابع الشخصي فعلًا مجرّمًا، والمقصود بعملية الجمع هو الحصول على المعلومات وتنظيمها تمهيدًا لاستعمالها لاحقًا، سواء تم ذلك بأساليب تقليدية كالسجلات الورقية، أو عبر أنظمة معلوماتية ووسائط إلكترونية. فالعبرة ليست بوسيلة الجمع، بل بمدى مشروعية الأسلوب المعتمد[2].

ثانيا: جمع المعطيات المتعلقة بالوضعية الجزائية للشخص

جرّم القانون تخزين أو إدراج البيانات المرتبطة بالسوابق القضائية أو الإدانات أو تدابير الأمن الخاصة بالشخص في ذاكرة معلوماتية، ما لم يكن ذلك من اختصاص الجهات المخوّلة قانونًا. وتتحقق الجريمة بمجرد وضع هذه البيانات أو الاحتفاظ بها، حتى ولو لم تُستعمل فعليًا.

---

[1]- المواد43،63،61 من القانون 07/18

[2]- المادة 59 من القانون 07/18

ويُقصد بـ"الوضع" إدراج هذه المعلومات ضمن نظام معلوماتي أيًا كان الغرض الأصلي منه، في حين يعني "الحفظ" إبقاءها مسجلة بحيث يمكن الرجوع إليها في أي وقت، ويأتي هذا التشدد نظرًا لحساسية المعطيات المرتبطة بالماضي الجزائي للأفراد وما قد يترتب على تداولها من مساس بسمعتهم وحقوقهم[1].

الفرع الثاني: جرائم الاستغلال غير المشروع للمعطيات الشخصية

يتحقق هذا النوع من الجرائم عند الانحراف عن الغاية أو الشروط التي أُجيزت من أجلها المعالجة، ومن أبرز صورها:

استعمال المعطيات أو معالجتها لأغراض مغايرة للغرض المصرّح به أو المرخّص له، في مخالفة لمبدأ تحديد الهدف من المعالجة.

الاحتفاظ بالمعطيات لمدة تتجاوز الفترة المحددة قانونًا أو المعلن عنها، بما يشكل خرقًا لمبدأ تحديد مدة الحفظ.

تمكين أشخاص غير مخوّلين من الولوج إلى المعطيات الشخصية.

استعمال المعطيات بشكل تعسفي أو تدليسي، أو إفشاؤها لجهات غير مؤهلة.

نقل المعطيات إلى دولة أجنبية دون استيفاء الشروط القانونية، والمتمثلة في الحصول على ترخيص من السلطة الوطنية لحماية المعطيات الشخصية، والتأكد من أن الدولة المستقبِلة توفر مستوى كافيًا من الحماية للخصوصية والحقوق الأساسية.

ويتضح من ذلك أن المشرّع أحاط المعالجة بسياج قانوني متكامل، لا يقتصر على مرحلة ما قبل المعالجة، بل يمتد ليشمل كيفية تنفيذها وحدود استغلال نتائجها، ضمانًا لصون الحياة الخاصة وتعزيزًا لحماية المعطيات ذات الطابع الشخصي[2].

---

[1]– المادة 68 من القانون 07/18

[2]– المادة 14 و 65 من القانون 07/18

المحور الثالث: المواجهة الوقائية للجريمة المعلوماتية

نتطرق من خلال هذا المحور على هيئتين رئيستين الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال و السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي

المبحث الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

من خلال استقراء الأحكام القانونية المنظمة لها، يتضح أن الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال تُصنَّف ضمن الهيئات العمومية ذات الطابع الإداري، وهو ما يدل على أن المشرّع لم يتجه إلى اعتبارها سلطة إدارية مستقلة بالمعنى الدقيق لهذا الوصف، خلافًا لما هو معمول به بالنسبة لبعض الهيئات الأخرى، على غرار الهيئة الوطنية للوقاية من الفساد ومكافحته.

ويُلاحظ هذا التوجه التشريعي رغم استعمال المشرّع، في مناسبات مختلفة، لمصطلحي «سلطة» و«هيئة» عند الإشارة إلى هذه الجهة، وهو ما قد يثير نوعًا من الغموض أو الاضطراب المفاهيمي في تحديد طبيعتها القانونية.

غير أن هذا التداخل في المصطلحات لا يغيّر من الحقيقة القانونية الجوهرية، والمتمثلة في أن المشرّع لم يُدرج الهيئة ضمن فئة السلطات الإدارية المستقلة، وإنما أبقاها ضمن إطار المؤسسات العمومية الإدارية الخاضعة للتنظيم العام للإدارة.

وعليه، فإن العبرة لا تكون بالتسمية المستعملة، بقدر ما تكون بالمركز القانوني الذي خوله لها المشرّع والاختصاصات التي أسندها إليها ضمن المنظومة القانونية القائمة.

حتى تتمكن الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال من أداء مهامها على الوجه الأمثل وتحقيق الفعالية المنشودة، كان من الضروري أن يحيط بها المشرّع بجهاز إداري يتولى تسيير شؤونها وتنفيذ اختصاصاتها. ولهذا الغرض، أقرّ القانون مجموعة من الآليات التنظيمية والقانونية التي من شأنها ضمان حسن سير الهيئة وتمكينها من الاضطلاع بالمهام المسندة إليها.

المطلب الأول: أجهزة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال" مجلس التوجيه"

وفي هذا الإطار، نصّ المشرّع على أن تتكون الهيئة من جهازين أساسيين، هما **مجلس التوجيه** و**المديرية العامة**، ونركز على مجلس التوجيه الذي له دور مهم في هذا الإطار

ويُعهد إليه مهمة رسم التوجهات العامة لنشاط الهيئة والإشراف على أعمالها، بينما تتولى المديرية العامة الجوانب التنفيذية والإدارية، ويرأس مجلس التوجيه الوزير المكلف بالدفاع الوطني أو من يمثله، ويضم في

عضويته ممثلين عن عدد من القطاعات الوزارية، من بينها وزارة الدفاع الوطني، ووزارة العدل، ووزارة الداخلية، والوزارة المكلفة بالبريد والمواصلات السلكية واللاسلكية[1].

غير أن وجود هذا النوع من الهيئات لا يعني انفصالها عن السياسة العامة للدولة أو عملها بمعزل عن الأهداف الكبرى التي تسعى السلطة العمومية إلى تحقيقها، إذ إن الغاية من إنشائها تتمثل أساسًا في تجسيد السياسات العمومية للدولة في مجالات محددة. ومن ثمّ، فإن تمكين هذه الهيئات من قدر من الاستقلالية لا يعدو أن يكون وسيلة وظيفية تهدف إلى تعزيز فعاليتها وتسريع وتيرة أدائها، وليس غاية في حد ذاته.

كما زُوِّدت الهيئة بأمانة عامة توضع تحت سلطة وزارة الدفاع الوطني، الأمر الذي يعكس بوضوح طبيعة الارتباط العضوي بينها وبين هذه الوزارة. ويتولى مجلس التوجيه، في هذا السياق، جملة من الصلاحيات، من أبرزها دراسة واعتماد الاستراتيجيات العامة للهيئة، وبحث سبل تطوير التعاون مع المؤسسات والهيئات الوطنية المعنية بمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، إلى جانب التقييم الدوري لمستوى التهديدات في هذا المجال، قصد تحديد أولويات العمل والآليات الواجب اعتمادها.

كما تشمل صلاحيات مجلس التوجيه اقتراح الأنشطة ذات الصلة بالبحث والتقييم الميداني المباشر في مجال الجرائم المعلوماتية، والمصادقة على برامج عمل الهيئة، ودراسة التقارير السنوية، وإبداء الرأي في المسائل المرتبطة بمهامها، فضلاً عن المساهمة في وضع وتحديث المعايير القانونية ذات الصلة بمجال اختصاصها، ودراسة مشاريع النصوص المتعلقة بالهيئة.

وقد حدّد المشرّع كيفية سير مجلس التوجيه بموجب قرار صادر عن الوزير المكلف بالدفاع الوطني، وهو ما يكشف بوضوح عن هيمنة هذه الوزارة على آليات تسيير الهيئة. ويترتب على ذلك أن الهيئة تظل خاضعة لوصاية وزارة الدفاع الوطني، الأمر الذي يحول دون اعتبارها هيئة مستقلة استقلالًا فعليًا.

ويُقصد بالاستقلالية، في هذا السياق، عدم خضوع الهيئة لأي رقابة تسلسلية أو وصاية إدارية من قبل السلطة التنفيذية، سواء تعلّق الأمر بهيئات تتمتع بالشخصية المعنوية أم لا، ذلك أن الشخصية المعنوية في حد ذاتها لا تُعد معيارًا حاسمًا لقياس درجة الاستقلال، وإنما يُستدل على ذلك من خلال طبيعة العلاقة التي تربط الهيئة بالسلطة الوصية وحدود تدخلها في تسيير شؤونها[2].

---

[1]– المرسوم الرئاسي رقم 19–172 المؤرخ في 06 يونيو 2019، المتضمن تحديد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وتنظيمها وكيفيات سيرها، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 37، الصادر بتاريخ 09 يونيو 2019

[2] –ZOUAIMIA Rachid, Les autorités administratives indépendantes et la régulation économique en Algérie, édition distribution HOUMA, Alger, 2005,p25

يقتضي تمكين الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال من أداء المهام المسندة إليها بفعالية، توفير إطار تنظيمي واضح يقوم على توزيع دقيق للاختصاصات وضمان حسن التسيير الإداري. ولهذا الغرض، أقرّ المشرّع بنية تنظيمية تسمح للهيئة بالاضطلاع بوظائفها وفق أسس قانونية محددة.
وفي هذا الإطار، نصّ المرسوم الرئاسي رقم 19-172 على أن تتكون الهيئة من هيئتين أساسيتين، هما مجلس التوجيه والمديرية العامة، ويتولى مجلس التوجيه رسم التوجهات العامة لسياسة الهيئة ومتابعة تنفيذها، بينما تُناط بالمديرية العامة المهام التنفيذية والإدارية اليومية، ويرأس مجلس التوجيه الوزير المكلف بالدفاع الوطني أو من يمثله، ويضم في عضويته ممثلين عن قطاعات وزارية أساسية، تشمل وزارة الدفاع الوطني، ووزارة العدل، ووزارة الداخلية، والوزارة المكلفة بالبريد والمواصلات السلكية واللاسلكية[1].
ولا يُفهم من هذا التنظيم أن الهيئة تتمتع باستقلال تام عن الدولة، إذ إن هذه الأخيرة تعمل في إطار السياسة العامة وتُسهم في تنفيذها في مجال الوقاية من الجرائم المعلوماتية. فغاية المشرّع من إنشاء الهيئة لا تتمثل في عزلها عن السلطة التنفيذية، وإنما في توفير جهاز متخصص قادر على ترجمة توجهات الدولة إلى إجراءات عملية وفعّالة. ومن هذا المنطلق، فإن منحها هامشًا من الاستقلالية يهدف أساسًا إلى تمكينها من العمل بكفاءة وسرعة، دون أن يعني ذلك خروجها عن الإطار العام للسياسات العمومية.
كما أُلحقت الهيئة بأمانة عامة توضع تحت إشراف وزارة الدفاع الوطني، وهو ما يعكس استمرار العلاقة التنظيمية بينها وبين هذه الوزارة. ويضطلع مجلس التوجيه، في هذا السياق، بعدد من الصلاحيات، من بينها اعتماد الاستراتيجيات العامة للهيئة، ودراسة آليات التعاون والتنسيق مع الهيئات والمؤسسات الوطنية المختصة، إضافة إلى التقييم الدوري لمستوى المخاطر والتهديدات المرتبطة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بما يسمح بتحديد الأولويات وضبط برامج العمل.
وتشمل مهام مجلس التوجيه كذلك اقتراح الأنشطة ذات الطابع البحثي والتقييمي في مجال الجرائم المعلوماتية، والمصادقة على برامج عمل الهيئة، ودراسة التقارير السنوية، وإبداء الرأي في المسائل المرتبطة باختصاصاتها، فضلاً عن المساهمة في تطوير المعايير القانونية المنظمة لمجال تدخلها، ودراسة مشاريع النصوص المتعلقة بها.
وقد خوّل المشرّع الوزير المكلف بالدفاع الوطني صلاحية تحديد كيفية سير مجلس التوجيه بموجب قرار تنظيمي، وهو ما يدل على خضوع الهيئة لإشراف مباشر من هذه الوزارة. ويترتب على ذلك أن الهيئة لا يمكن اعتبارها سلطة إدارية مستقلة استقلالا كاملا ، بالنظر إلى ارتباطها الهيكلي والوظيفي بوزارة الدفاع الوطني.
ويُقصد بالاستقلالية الإدارية، في هذا السياق، عدم خضوع الهيئة لأي رقابة تسلسلية أو وصاية إدارية من قبل السلطة التنفيذية، سواء كانت تتمتع بالشخصية المعنوية أم لا، ذلك أن الشخصية المعنوية لا تشكّل معيارًا

[1]– المادة 05 **من** المرسوم الرئاسي رقم 19-172 المؤرخ في 06 يونيو 2019 السابق

كافيًا لتحديد درجة الاستقلال، وإنما يُستدل على ذلك من خلال مدى تدخل السلطة الوصية في تسيير شؤون الهيئة وتوجيه نشاطها[1].

المطلب الثاني: آليات تدخل الهيئة في الوقاية من الجرائم الإلكترونية

الفرع الأول: مهام الهيئة

تعمل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال تحت إشراف وزارة الدفاع الوطني، وتتمثل مهامها الأساسية فيما يلي:

السهر على حسن سير الهيئة وتنظيم عملها الداخلي.

إعداد مشروع ميزانيتها ومتابعة تنفيذها.

تنسيق ومراقبة نشاطات الهياكل التابعة لها.

تنشيط وتنسيق عمليات الوقاية من الجرائم الإلكترونية.

تبادل المعلومات والخبرات على المستويين الوطني والدولي.

إعداد التقارير السنوية المتعلقة بنشاطها[2].

ويلاحظ أن المشرّع لم يمنح الهيئة صلاحيات قضائية مستقلة، بل حصر تدخلها في إطار الجرائم التي تمس أمن الدولة، كالإرهاب، التجسس، المساس بأنظمة المعالجة الآلية للمعطيات ذات الطابع السيادي، دون أن يشمل باقي الجرائم الإلكترونية ذات الطابع العادي.

و يبرز الطابع الأمني لتدخل الهيئة من خلال النصوص القانونية أن دور الهيئة يتركز أساسًا في الجرائم الإلكترونية المرتبطة بالإرهاب وأمن الدولة، وهو ما يفسر خضوعها لوصاية وزارة الدفاع الوطني. كما أن تدخلها يتم غالبًا بطلب من السلطات القضائية أو الأمنية المختصة، خاصة في الحالات التي تستدعي استعمال وسائل التحري الخاصة.

وقد خوّلها المشرّع دعم الجهات القضائية والأمنية عبر تقديم الخبرة التقنية، وجمع وتحليل المعطيات الرقمية، والمساهمة في الكشف عن الجرائم ذات الخطورة البالغة[3].

---

[1]– المادة 05 من المرسوم الرئاسي رقم 19–172 المؤرخ في 06 يونيو 2019 مرجع سابق ذكره

[2]- المادة 09 المرجع نفسه

[3] المادة 11 من **المرسوم الرئاسي** رقم 19–172 المؤرخ في 06 يونيو 2019

الفرع الثاني: مباشرة إجراءات التحري بإذن قضائي

حرص المشرّع على حماية الحريات الفردية، فنص صراحة على أن أي إجراء يمس الحياة الخاصة، كاعتراض الاتصالات أو تسجيل المحادثات، لا يجوز إلا بناءً على إذن مسبق ومسبب من الجهة القضائية المختصة

. غير أنّه عندما يتعلق الأمر بالوقاية من الأفعال الموصوفة بالإرهابية أو التخريبية، أو بالجرائم الماسّة بأمن الدولة، فإن الاختصاص بمنح الإذن بالمباشرة في إجراءات المراقبة الإلكترونية ووضع الترتيبات التقنية اللازمة، وكذا تجديد مدتها، ينعقد للنائب العام لدى مجلس قضاء الجزائر العاصمة، باعتباره الجهة المخوّلة قانونًا في مثل هذه الحالات ذات الطابع الخطير[1]

ويشترط في هذا الإذن أن يحدد بدقة:
نوع الجريمة محل التحقيق.
طبيعة الوسائل التقنية المستعملة.
أماكن وضع الأجهزة.
مدة الإجراء، والتي تكون محددة وقابلة للتجديد وفق ضوابط قانونية.
كما لا يجوز استعمال الإذن الصادر في جريمة معينة للتحقيق في جريمة أخرى إلا بإذن جديد[2].

سرية إجراءات التحري وحماية المعطيات الشخصية

تُعد السرية من المبادئ الأساسية التي تحكم مرحلة التحري، حيث يلتزم كل من يشارك في هذه الإجراءات باحترام السر المهني، ويُمنع إفشاء أي معلومة تتعلق بالتحقيق أو بالأشخاص المعنيين به.
كما ألزم المشرّع السلطات المختصة بعدم الاحتفاظ بالمعطيات غير المؤكدة أو غير المفيدة للتحقيق، حمايةً لسمعة الأفراد وقرينة البراءة، ومنعًا لأي تعسف قد يمس حقوقهم الأساسية[3].

---

[1]– المادة 04 من القانون 04/09 السابق الذكر

[2]– المرجع نفسه

[3]– المادة 65 مكرر09 من الامر رقم 155/66 متمم بموجب المادة 14 من القانون رقم 22/06 المؤرخ في 20 ديسمبر 2006 يعدل و يتمم الأمر رقم 155/66 مؤرخ في 08 جوان 1966 يتضمن قانون الاجراءات الجزائية، جريدة رسمية عدد 84 صادرة بتاريخ 24 ديسمبر 2006 المعدل و المتمم

المبحث الثاني: السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي

المطلب الأول: الإطار القانوني والطبيعة التنظيمية للسلطة الوطنية

الفرع الأول: تشكيلة الهيئة :

أنشأ المشرّع الجزائري بموجب القانون رقم 07/18 المؤرخ في 10 جوان 2018 السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي باعتبارها سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي والإداري، وتوضع لدى رئيس الجمهورية، ويكون مقرها الرسمي بالجزائر العاصمة[1].

ويهدف هذا التنظيم إلى ضمان حياد السلطة وفعاليتها في أداء مهامها، بعيدًا عن أي تبعية إدارية مباشرة قد تؤثر على استقلال قراراتها، خاصة بالنظر إلى حساسية مجال حماية الحياة الخاصة والمعطيات الشخصية.
وتتكون السلطة الوطنية من ستة عشر عضوًا، يتم تعيينهم بموجب مرسوم رئاسي لمدة خمس 05 سنوات قابلة للتجديد، ويتم اختيارهم بناءً على كفاءاتهم القانونية أو التقنية في مجال معالجة المعطيات ذات الطابع الشخصي.
ويُراعى في تشكيلها التعدد والتوازن، إذ تضم[2]:
-شخصيات مختصة يعيّنها رئيس الجمهورية، من بينهم رئيس السلطة.
-قضاة من المحكمة العليا ومجلس الدولة يقترحهم المجلس الأعلى للقضاء.
-ممثلين عن غرفتي البرلمان.
-ممثلين عن المجلس الوطني لحقوق الإنسان وعدد من الوزارات ذات الصلة، كالدفاع، العدل، الداخلية، الصحة، الشؤون الخارجية، والعمل والاتصال والرقمنة.
كما يمكن للسلطة الاستعانة بخبراء أو مختصين عند الحاجة، إضافة إلى أمانة تنفيذية يشرف عليها أمين تنفيذي يساعده طاقم إداري وتقني.

الفرع الثاني: سير عمل السلطة وضمانات الحياد والنزاهة

يؤدي أعضاء السلطة الوطنية، قبل مباشرة مهامهم، اليمين القانونية أمام مجلس قضاء الجزائر، كما يتمتعون بحماية الدولة ضد أي تهديد أو إساءة قد تطالهم بسبب أو أثناء تأدية وظائفهم.

---

[1] المادة 22 من القانون 07/18 السابق ذكره

[2]– المادة 23 من القانون 07/18 السابق ذكره

ويُكرّس المشرّع مبدأ الاستقلال الوظيفي لأعضاء السلطة، حيث لا يخضعون للتدرج الإداري ولا يتلقون تعليمات من أي جهة حكومية، كما لا يجوز عزلهم تعسفيًا. وفي المقابل، فرض القانون قيودًا صارمة لتفادي تضارب المصالح، إذ يُمنع على الأعضاء ممارسة أي نشاط أو امتلاك مصالح في المؤسسات العاملة في مجال الاتصالات أو معالجة المعطيات.

كما يلتزم الأعضاء والمستخدمون بالمحافظة على سرية المعطيات والمعلومات التي يطلعون عليها، حتى بعد انتهاء مهامهم، مع منح السلطة حق الولوج إلى المعطيات المعالجة والوثائق المرتبطة بها دون التذرع بالسر المهني في مواجهتها.

وتعد السلطة تقريرًا سنويًا عن نشاطها ترفعه إلى رئيس الجمهورية، تكريسًا لمبدأ الشفافية والمساءلة[1].

المطلب الثاني مهام السلطة الوطنية في حماية الحق في الخصوصية

تضطلع السلطة الوطنية بدور محوري في حماية حرمة الحياة الخاصة من خلال رقابة سابقة ولاحقة على عمليات معالجة المعطيات ذات الطابع الشخصي.

الفرع الأول: الرقابة المسبقة على المعالجة

تمسك السلطة سجلًا وطنيًا خاصًا تُقيّد فيه جميع التصريحات والتراخيص المتعلقة بمعالجة المعطيات الشخصية، ويلتزم كل مسؤول عن المعالجة بالحصول على تصريح أو ترخيص مسبق قبل الشروع في أي عملية معالجة.

ويتم إيداع التصريح إما ورقيًا أو إلكترونيًا، وتسلم السلطة وصلاً خلال أجل لا يتجاوز 48 ساعة، يسمح للمسؤول ببدء المعالجة تحت مسؤوليته[2].

ويجب أن يتضمن التصريح معلومات دقيقة تتعلق بهوية المسؤول عن المعالجة، طبيعة المعطيات، الغرض من المعالجة، فئات الأشخاص المعنيين، الجهات المرسلة إليها المعطيات، مدة الاحتفاظ بها، والتدابير الأمنية المعتمدة.

كما يفرض القانون إخطار السلطة بأي تعديل أو حذف يطرأ على المعالجة، وفي حالة التنازل عن ملف المعطيات، يلتزم المتنازل له بإعادة إجراءات التصريح[3].

---

[1]– المادة 25 من القانون 07/18 السابق ذكره

[2]– المادة 13 و المادة 25 من القانون 07/18

[3]– المادة 14 من القانون رقم 07/18

الفرع الثاني: الترخيص بمعالجة المعطيات الحساسة ونقلها إلى الخارج

تُعد المعطيات الحساسة من أكثر المعطيات ارتباطًا بالحقوق والحريات الأساسية، لذلك لا يُرخّص بمعالجتها إلا في حالات استثنائية تتعلق بالمصلحة العامة، أو بموافقة صريحة من الشخص المعني، أو لضرورات قانونية محددة.

كما منح القانون السلطة الوطنية صلاحية الترخيص بنقل المعطيات الشخصية إلى دول أجنبية، شريطة أن توفر تلك الدول مستوى كافيًا من الحماية، وألا يشكل النقل خطرًا على الأمن العمومي أو المصالح الحيوية للدولة.

وفي حالات استثنائية، يجوز النقل حتى في غياب هذه الشروط، كحالات الضرورة القصوى، أو التعاون القضائي الدولي، أو تنفيذ اتفاقيات دولية تكون الجزائر طرفًا فيه[1].

الفرع الثالث: الرقابة اللاحقة وسلطات الردع

تمارس السلطة الوطنية بعد المعالجة رقابة فعالة تشمل:

تلقي الشكاوى والطعون والاحتجاجات[2].

توعية المسؤولين والأشخاص المعنيين بحقوقهم وواجباتهم[3].

الأمر بتعديل أو توقيف أو إتلاف المعطيات المخالفة للقانون[4].

إصدار آراء وتوصيات واقتراح إصلاحات تشريعية[5].

فرض جزاءات إدارية، مثل الإنذار، سحب الترخيص مؤقتًا أو نهائيًا، وفرض غرامات مالية[6].

وتكون قرارات السلطة قابلة للطعن أمام مجلس الدولة، ضمانًا لحق التقاضي[7].

وفي حال معاينة وقائع ذات طابع جزائي، تلتزم السلطة بإخطار النيابة العامة فورًا، ما يعكس دورها التكميلي للسلطة القضائية[8].

---

[1]– المادة 25 فقرة 01 و 05 من القانون 07/18

[2] المادة 04/25 من القانون 07/18

[3]– المادة 25/ 03 من القانون 07/18

[4]– المادة7/25 من القانون 07/18

[5]– المادة 25 فقرة 05 من نفس القانون

[6]– المادة 25 فقرة 11 من القانون 07/18

[7]– المادة 46 فقرة 02 من القانون 07/18

[8]–المادة 51 من القانون 07/18

خاتمة

في الختام، تولي الجزائر أهمية بالغة لمكافحة الجريمة المعلوماتية، إدراكًا منها لخطورة هذا النوع من الجرائم على الأمن الوطني والاقتصادي والاجتماعي. فقد أصبحت الجرائم الإلكترونية تشكل تهديدًا متزايدًا مع توسع استخدام تكنولوجيات الإعلام والاتصال، الأمر الذي دفع الدولة الجزائرية إلى تبني إستراتيجية شاملة تقوم على الجوانب القانونية والتقنية والتوعوية من أجل التصدي لها بفعالية.

على الصعيد القانوني، عملت الجزائر على سنّ وتحيين مجموعة من القوانين التي تجرّم الأفعال المرتبطة بالمساس بالأنظمة المعلوماتية، والاحتيال الإلكتروني، وانتهاك المعطيات الشخصية، ونشر المحتوى غير المشروع عبر الإنترنت. وقد ساهم هذا الإطار التشريعي في توفير أساس قانوني يسمح للسلطات المختصة بمتابعة مرتكبي الجرائم المعلوماتية ومعاقبتهم وفقًا للقانون، بما يضمن حماية الحقوق الرقمية للأفراد والمؤسسات.

أما على المستوى الأمني والتقني، فقد أنشأت الجزائر هياكل متخصصة ووحدات أمنية مختصة في الجرائم السيبرانية، تعمل على رصد التهديدات الإلكترونية، والتحقيق في القضايا المتعلقة بالاختراق والابتزاز الإلكتروني، وحماية الشبكات والأنظمة الحساسة. كما تم تعزيز قدرات هذه الوحدات من خلال التكوين المستمر وتزويدها بالتجهيزات الحديثة لمواكبة التطور المتسارع لأساليب الجريمة المعلوماتية.

وقد أدركت الجزائر مبكرًا خطورة الجريمة المعلوماتية، فعملت على وضع إطار قانوني يجرّم مختلف الأفعال المرتبطة بالمساس بالأنظمة المعلوماتية، والاحتيال الإلكتروني، وانتهاك المعطيات الشخصية، بما يضمن حماية الحقوق الرقمية وملاحقة الجناة. كما عززت الدولة جهودها الأمنية من خلال إنشاء وحدات متخصصة في مكافحة الجرائم السيبرانية، وتطوير قدراتها التقنية والبشرية لمواكبة التطور السريع في أساليب الجريمة الإلكترونية.

إلى جانب ذلك، أولت الجزائر أهمية كبيرة للوقاية، من خلال نشر الوعي المجتمعي بثقافة الأمن المعلوماتي، وتحسيس المواطنين بمخاطر الاستخدام غير الآمن للإنترنت ووسائل التواصل الاجتماعي. كما ساهمت المؤسسات التربوية والإعلامية في ترسيخ السلوك الرقمي المسؤول، خاصة لدى فئة الشباب.

وإيمانًا منها بأن الجريمة المعلوماتية ظاهرة عابرة للحدود، حرصت الجزائر على تعزيز التعاون الدولي والإقليمي، عبر تبادل الخبرات والمعلومات والمشاركة في الجهود المشتركة لمكافحة هذا النوع من الجرائم.

وعليه، فإن مكافحة الجريمة المعلوماتية في الجزائر تُعدّ مسؤولية جماعية تتقاسمها الدولة والمجتمع والأفراد. ومن خلال تضافر الجهود القانونية والأمنية والتوعوية، تسعى الجزائر إلى بناء فضاء رقمي آمن ومستقر، يواكب التحول الرقمي، ويساهم في حماية المجتمع ودعم مسار التنمية الوطنية.

وفي المجال الوقائي، ركزت الجزائر على نشر الوعي بأهمية الأمن المعلوماتي، من خلال حملات تحسيسية وبرامج توعوية تستهدف مختلف فئات المجتمع، خاصة الشباب، حول مخاطر الاستعمال السيئ للإنترنت ووسائل التواصل الاجتماعي. كما ساهمت المؤسسات التربوية والإعلامية في ترسيخ ثقافة الاستخدام الآمن والمسؤول للتكنولوجيا.

إضافة إلى ذلك، تدرك الجزائر أن الجريمة المعلوماتية ظاهرة عابرة للحدود، لذا عملت على تعزيز التعاون الدولي والإقليمي في هذا المجال، من خلال تبادل المعلومات والخبرات، والمشاركة في الاتفاقيات والجهود المشتركة الرامية إلى مكافحة الجرائم الإلكترونية.

وعليه، فإن مكافحة الجريمة المعلوماتية في الجزائر تمثل أولوية وطنية تتطلب تضافر جهود الدولة والمجتمع معًا. ومن خلال تطوير التشريعات، وتعزيز القدرات التقنية، ونشر الوعي الرقمي، تسعى الجزائر إلى بناء فضاء إلكتروني آمن يواكب متطلبات العصر الرقمي، ويضمن حماية الأفراد والمؤسسات، ويدعم مسار التنمية الوطنية.

قائمة المراجع

المراجع

الكتب

– بلعليات إبراهيم، أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري، دار الخلدونية، الجزائر، 2007.

– عبدالقادر القهوجي، الحماية الجنائية لبرامج الحاسب، دار الجامعة الجديدة، مصر، 1997.

– عبود السراج، قانون العقوبات الاقتصادية، جامعة دمشق، الطبعة السابعة، دمشق، ،1998 .

-محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة للنشر، الإسكندرية، ،2001.

– مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية مطابع الشرطة، مصر، ،2000.

– مناصرة يوسف جرائم المساس بأنظمة المعالجة الألية للمعطيات، دار الخلدونية، الجزائر،2018.

– يوسف دلاندة ،قانون العقوبات، دار هومة للطباعة والنشر والتوزيع، الجزائر،،2006.

–حسين طاهري، الجرائم الألكترونية، الطبعة 01، دار الخلدونية، الجزائر،2021.

–رحيمة نمديلي: "خصوصية الجريمة الالكترونية في القانون الجزائري و القوانين المقارنة"، كتاب أعمال المؤتمر الدولي الرابع عشر: الجرائم الالكترونية، مركز جيل البحث العلمي، طرابلس، لبنان، 24،25 مارس 2017.

-طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي،"النظام القانوني لحماية المعلوماتي"، دار الجامعة الجديدة ، مصر، ،2009 .

–عبد الفتاح بيومي حجازي مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، دار الفكر الجامعي، الإسكندرية، 2006.

–محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، دار النهضة العربية، القاهرة.

–منير محمد الجنبيهي، وممدوح محمد الجنبيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، ،2004 .

–نهلا عبدالقادر المومني، الجرائم المعلوماتية، دار الثقافة، الاردن، 2008.

أطاريح الدكتوراة و مذكرات الماجستير

– تركي بن عبد الرحمن المويشر، بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته، أطروحة مقدمة استكمالا لمتطلبات الحصول على درجة دكتوراه الفلسفة الأمنية، كلية الدراسات العليا بجامعة نايف العربية للعلوم الأمنية،الرياض، 2000.

– مولاي ملياني دلال، إشكالية الإثبات في جرائم الإنترنت في التشريع الجزائري، أطروحة لنيل الدكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة تلمسان، 2018/2017.

–فيصل عايش عيد المطيري، الوعاء القانوني للدليل التقني في اطار اثبات الجريمة الالكترونية، رسالة مقدمة للحصول على الدكتوراة في الحقوق، جامعة عين شمس، مصر، 2019.

–أمال قارة، الجريمة المعلوماتية، مذكرة لنيل شهادة الماجستير في الحقوق، تخصص قانون عام، كلية الحقوق، جامعة الجزائر، 2002.

–بوخبزة عائشة، الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماجستير في الحقوق، جامعة وهران2013/2012.

–صغير يوسف، الجريمة المرتكبة عبر الانترنيت، مذكرة لنيل شهادة الماجستير في الحقوق، تخصص القانون الدولي للأعمال ، كلية الحقوق و العلوم السياسية، جامعة مولود معمري تيزي وزو، السنة الجامعية، 2012/2023.

–عبدالله دعسش العجمي، المشكلات العلمية و القانونية للجرائم الالكترونية، دراسة مقارنة، مذكرة لنيل شهادة الماجستير في القانون العام، جامعة الشرق الأوسط، 2014.

–فتيحة رصاع، الحماية الجنائية للمعلومات على شبكة الانترنيت، رسالة ماجستير في القانون العام، كلية الحقوق و العلوم السياسة،، جامعة أبو بكر بلقايد، تلمسان، الجزائر،/2012/2011.

– نسيمة جدي، جرائم المساس بأنظمة المعالجة الألية للمعطيات، رسالة ماجستير في القانون الجنائي، كلية الحقوق، جامعة وهران، 2014/2013.

المقالات

–اسماعيل بن يحي، التعريف بمراقبة الاتصالات الالكترونية كإجراء من اجراءات جمع الأدلة في الجريمة الالكترونية، مجلة صوت القانون ، المجلد 08، العدد 03، 2022.

–آمنة امحمدي بوزينة، خصوصية قواعد التجريم عن الاعتداء على أنظمة المعالجة الآلية للمعطيات في إطار التشريع الجزائري، *مجلة ببليوفيليا لدراسات المكتبات والمعلومات*، جامعة العربي التبسي، تبسة، الجزائر، العدد 4.

–بطيحي نسيمة، جريمة الدخول أو البقاء غير المشروع إلى النظام المعلوماتي، مجلة الفقه القانوني و السياسي، المجلد01، العدد01، 2019.

–بعجي عبدالنور، الجريمة الالكترونية بين المفهوم و الخصوصية، بحث مقدم ضمن مؤلف جماعي د/ كوثر مازوني" الجريمة المعلوماتية"، 2012.
–بوهرين فتيحة، الجريمة المعلوماتية في التشريع الجزائري، مجلةالحقوق والعلوم الإنسانية المجلد14، العـدد: 04 2021،،
–جمال براهيمي: "مكافحة الجرائم الالكترونية في التشريع الج ازئري"، المجلة النقدية، جامعة مولود معمري، تيزي وزو، الجزائر، المجلد ،88 العدد ،20 نوفمبر ،2016.
–حمودي ناصر، الحماية الجنائية لنظم المعالجة الألية للمعطيات في التشريع الجزائري، المجلة الاكاديمية للبحث القانوني، المجلد 14، العدد02، 2016.
–رامي عبدالقادر أحمد الطراونة، جرائم تكنولوجيا المعلومات مفهومها وإثباتها، مجلة جامعة الزيتونة الاردنية، للدراسات القانونية، المجلد6 الاصدار 2023.
–سميرة معاشي: "ماهية الجريمة المعلوماتية"، مجلة المنتدى القانوني، العدد ،27 كلية الحقوق و العلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائر، أفريل 2010.
–عاسية زروق، الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري، ضمن مؤلف جماعي كوثر مازوني، الجريمة المعلوماتية، منشورات الخلدونية، 2022.
–عباس كريمة، جرائم المساس بأنظمة المعالجة الألية للمعطيات، مجلة البيان للدراسات القانونية و السياسية، العدد04، ديسمبر 2017.
–عبدالسلام محمد المايل، عادل محمد الشربجي، الجريمة الالكترونية في الفضاء الإلكتروني، مجلة أفاق للبحوث و الدراسات، العدد04، 2019، ص 242.
–فلاح عبدالقادر، حجز وحفظ المعطيات في الجريمة الالكترونية، مجلة صوت القانون، المجلد 08، العدد01، 2021.
–قسمية محمد، وخضري، حمزة، مكافحة الجرائم الماسة بنظام المعالجة الآلية للمعلومات في القانون الجزائري، *مجلة صوت القانون*، جامعة خميس مليانة، الجزائر، المجلد 27، العدد 20، نوفمبر 2020.
–ليندا بن طالب، التفتيش في الجريمة المعلوماتية، مجلة العلوم القانونية و السياسية، المجلد 08، العدد02، 2017.
–مختارية بوزيدي: "ماهية الجريمة الالكترونية"، الملتقى الوطني حول: آليات مكافحة الجرائم الالكترونية في التشريع الجزائري مركز جيل البحث العلمي، الجزائر 01 مارس ،2017 .
–مواسة صونية نادية، خصوصية الجريمة المعلوماتية، بحث منشور ضمن مؤلف جماعي تحت عنوان الجريمة الالكترونية، دار الخلدونية، الجزائر 2012.

–ياسمينة بونعارة، الجريمة الإلكترونية، مجلة المعيار، العدد،26 جامعة الأمير عبد القادر للعلوم الإسلامية ، قسنطينة، 2015.

القوانين

–القانون رقم 04–15 المؤرخ في 10 نوفمبر 2004، المنشور **في** الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية عدد 71، والذي يعدّل ويتمّم الأمر رقم 66–156 المؤرخ في 8 جوان 1966، المتضمن قانون العقوبات.

–قانون رقم 09 – 04 مؤرّخ في 5 أوت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية رقم 47، المؤرخة في 16 أوت 2009.

–القانون رقم 18–07 مؤرخ في 25 رمضان عام 1439 هـ، الموافق لـ 10 يونيو 2018، ويتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية رقم 34 الصادرة بتاريخ 10 يونيو2018.

– المرسوم الرئاسي رقم 19–172 المؤرخ في 06 يونيو 2019، المتضمن تحديد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وتنظيمها وكيفيات سيرها، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 37، الصادر بتاريخ 09 يونيو 2019

– الامر رقم 155/66 متمم بموجب المادة 14 من القانون رقم 22/06 المؤرخ في 20 ديسمبر 2006 يعدل و يتمم الأمر رقم 155/66 مؤرخ في 08 جوان 1966 يتضمن قانون الاجراءات الجزائية، جريدة رسمية عدد 84 صادرة بتاريخ 24 ديسمبر 2006 المعدل و المتمم.

أعمال الأمم المتحدة

– أعمال مؤتمر الأمم المتحدة لمنع الجريمة ومعاملة المجرمين حول تحديات الجريمة عبر الوطنية المنعقد في القاهرة العام 1990

المراجع باللغة الأجنبية

− BROWN S. D. Cameron , Investigating and Prosecuting Cyber Crimes, international journal of cyber criminology, Vol. 9, Issue1, June 2015, p. 57

− CROSS Michael , Scene of the Cybercrime, Second Edition, Syngress Publishing, United Kingdom, 2011.

−MASCALA Corinne, « criminalité et contrat électronique », IN : Le contrat électronique, Travaux de l’association CAPITANT Henri, journées national, Paris, 2000.

¯ VIVANT Michel, Le droit de L'Internet et de la société de l'information ،Larcier, Paris, 2001.

− MARSHALL H. Prosecuting Computer Crimes, Legal Education Executive Office, USA, p. 8.

−CHRIS Hansen, To Catch a Predator Protecting Your Kids from Online Enemies Already in Your Home, USA : Plume, 2007, p. 27

−Raymond Gassin, informatique "fraude informatique", répertoire pénal,Dalloz, octobre1995, p17

−Jean Devése, atteintes aux systèmes de traitement automatisé de données, Jurisclasseur, pénal, article 323-1 à 323-7,2, 1997.p 16.

−ZOUAIMIA Rachid, Les autorités administratives indépendantes et la régulation économique en Algérie, édition distribution HOUMA, Alger, 2005.

الفهرس

الفهرس