جامعة باتنة -1- الحاج لخضر
كلية الحقوق والعلوم السياسية
قسم الحقوق

القانون الجزائي والتكنولوجيا الحديثة

مذكرة مكملة لمقتضيات نيل شهادة الماستر في الحقوق
تخصص: قانون جنائي وعلوم جنائية

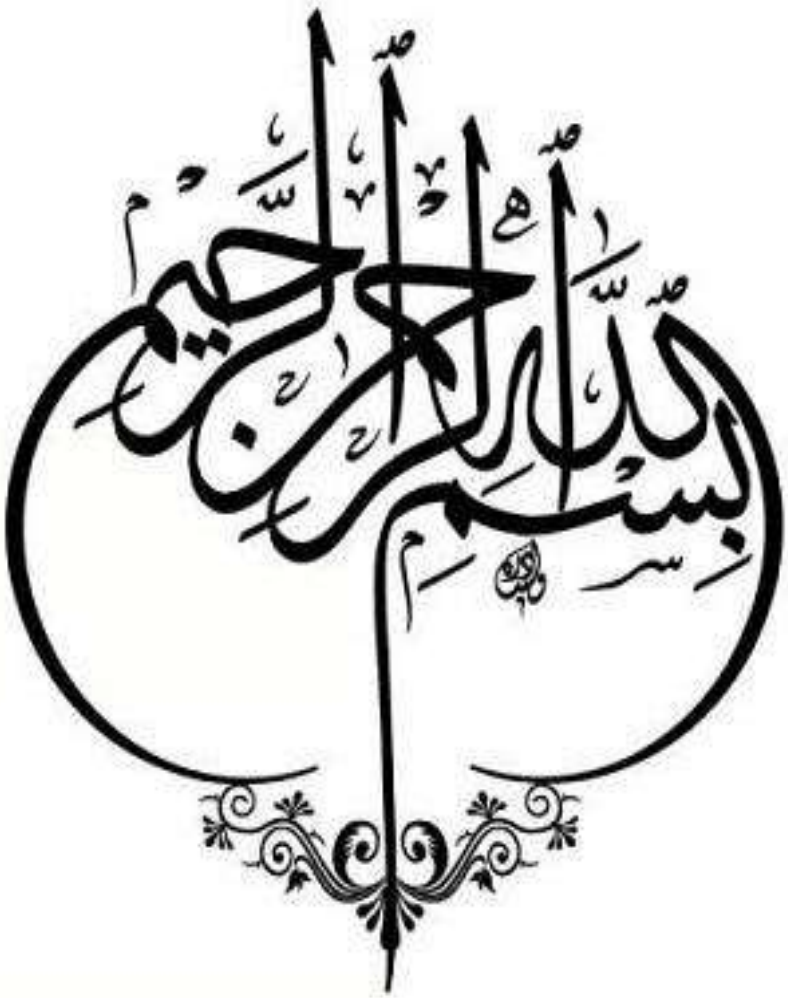
إعداد الطالبين:
رضا مصمودي
علي بزيان

إشراف الأستاذ
بن بوعبد الله نورة

لجنة المناقشة

الاسم واللقب	الرتبة العلمية	المؤسسة الجامعية	الصفة
مخلوفي عبد الوهاب	أستاذ التعليم العالي	جامعة باتنة 1	رئيسا
بن بوعبد الله نورة	أستاذ التعليم العالي	جامعة باتنة 1	مشرفا ومقررا
دريدي وفاء	أستاذ التعليم العالي	جامعة باتنة 1	مناقشا

السنة الجامعية: 2023 - 2024


بسم الله الرحمن الرحيم

شكر وتقدير

– نتقدم بموفور الشكر وأسمى عبارات التقدير للأستاذة الدكتورة **نورة بن بوعبدالله** على قبولها تحمل عبء الاشراف والتأطير والتقرير لمذكرتنا الموسومة ب: " **القانون الجزائي والتكنولوجيا الحديثة**". لا نملك العبارات والكلام للتعبير على مدى امتناننا للأستاذة التي ساهمت في تنشئة فكرنا القانوني والفقهي سيما ما خص العلوم والقانون الجنائيين، فكانت الملهمة.

– شرف عظيم لنا قبول الأستاذ **عبد الوهاب مخلوفي** –عميد كلية الحقوق والعلوم السياسية بجامعة باتنة1– لترأس لجنة مناقشة مذكرة الماستر، هذا الرجل الهادئ والحكيم الذي كان لنا نبراس أضاء طريق تكويننا.

– الشكر الموصول الى الأستاذة الدكتورة **وفاء دريدي** على قبولها مهمة النقاش في لجنة المناقشة لمذكرة الماستر، استاذتنا الفاضلة التي كانت لنا سراج أرشدنا طيلة سنوات الدراسة، لك منا أرقي معاني التقدير.

– شكر خاص الى كل من **منير حملاوي** "الأندلس" والمهندس **لخصر بوراس**، و**بن عبد المؤمن بدرالدين** "دوما".

– شكر موصول لكل من: الأستاذة الدكتورة **وردة بن بوعبدالله**، الأستاذ الدكتور **ميلود بن عبد العزيز**، **الأستاذ الدكتور سمير شعبان**، الدكتورة **لمياء بن دعاس**، الدكتور **أحمد بوراوي**، الدكتور **ياسين بوبشيش**، الدكتور **سامي خطاف**،

دون أن ننسى الدكتور **عمر فلاح**.

إهداء

– لقد خاطبته أمه لحظة وداعه لها في ظلام ليلة من ليالي أواخر شهر أكتوبر 1954، فطلبت منه أن يتزوج حتى ترى أبنائه، اجابها الحكيم قائلا: " سأتزوج بعد استقلال الجزائر ان بقيت حيا، وان استشهدت فإن كل أبناء الجزائر المستقلة أبنائي"

أحد ابنائك: **رضا مصمودي** يهدي هذا العمل المتواضع إلى روحك الطاهرة الزكية.

_ إلى اخي وصديقي الدكتور: رضا مصمودي اهديك هذا العمل المتواضع.

علي بزيان

المقدمة

لطالما ارتبطت الجريمة بوجود الإنسان على الأرض، وتعددت أسبابها والوسائل المستخدمة في تنفيذها. تُعد الجريمة من الأفعال المحظورة شرعاً وقانوناً، وقد أشار الله سبحانه وتعالى إليها في سورة المائدة، حيث قال: "إني أريد أن تبوأ بإثمي وإثمك فتكون من أصحاب النار وذلك جزاء الظالمين (29) فطوعت له نفسه قتل أخيه فقتله فأصبح من الخاسرين (30)"[1].

تختلف هذه الجرائم باختلاف الوسيلة المستخدمة في ارتكابها، حيث أن الوسيلة تحدد نوعية المجرم. ومع حلول القرن الواحد والعشرين، أصبح المجرمون أكثر حنكة، وظهرت جرائم جديدة غيرت الأركان الأساسية أو التقليدية للجريمة، خاصة الركن المادي منها، والوسيلة المستخدمة لتنفيذ الجريمة. ويعود ذلك إلى العامل التكنولوجي المرتبط باستخدام الحاسوب (الكمبيوتر) وتطور شبكة الإنترنت (الشبكة العالمية).

رغم أهمية هذه التقنيات التي سهَّلت مهام الدول والأفراد، إلا أنها انعكست بالسلب عندما استُغِلَّت في عمليات إجرامية تمس بالممتلكات أو الحياة الخاصة للأفراد. ومع تفاقم هذا النوع من الإجرام، سارعت الدول إلى وضع منظومات قانونية وأساليب تقنية لحماية مكتسباتها، وتعد الجزائر من الدول التي وضعت سياسة جزائية محكمة تتماشى مع التطور التكنولوجي العالمي، نظراً للتزايد المستمر في هذا النوع من الجرائم، فقد تم إحصاء 2130 قضية على مستوى مصالح الشرطة القضائية بالمديرية العامة للأمن الوطني في عام 2017، وفقاً لمعطيات نشرتها مجلة الشرطة، هذا من جهة ومن جهة أخرى لا أحد ينكر دور التكنولوجيا الحديثة في تعزيز قواعد القانون الجزائي لاسيما المحاكمة الالكترونية وعصرنة العدالة الجزائية.

[1] سورة المائدة، القراءن الكريم

أهمية الدراسة:

تبرز الأهمية العلمية لهذه الدراسة في تناولها بشكل خاص لموضوع دور التكنولوجيا الحديثة في ظهور جرائم مستحدثة، لاسيما الجريمة الإلكترونية التي تشكل تحدي للقواعد التقليدية للقانون الجزائي نظرا لتزايد نسبة ارتكاب هذه الجريمة المستحدثة في الوسط الاجتماعي عبر مختلف الفئات العمرية، ولتعدد الأضرار التي تنجم عنها، بالإضافة إلى ذلك، تتميز الجريمة الالكترونية بسرعة تنفيذها وبالصعوبات التي تواجهها السلطات في اكتشافها وإثباتها، مما يعزز من الأهمية العلمية للدراسة والبحث في هذا المجال.

وتكتسب هذه الدراسة أهميتها العملية من كونها تتناول دور التكنولوجيا الايجابي في تعزيز قواعد القانون الجزائي خاصة الشق الاجرائي كموضوع "التقاضي الإلكتروني كآلية لعصرنة قطاع العدالة" من خلال دوره الفعّال في مرفق العدالة وتعزيز الخدمة العمومية للمواطنين. يُساهم التقاضي الإلكتروني في تبسيط وتسريع إجراءات التقاضي، ويعزز إمكانية الوصول إلى المعلومات والاطلاع عليها بسهولة، ويساعد في القضاء على التحديات التي يواجهها التقاضي التقليدي المعروف ببطء إجراءاته، مما يضمن حقوق الأفراد بشكل أكثر فعالية.

أهداف الدراسة:

تهدف الدراسة الى التطرق الى الجانب السلبي الذي اوجدته تطورات التكنولوجيات الحديثة من كونها اوجدت نموذجا مستحدثا من الجرائم والمسماة بالجريمة الالكترونية، فوجب التطرق الى تصنيفاتها التشريعية وسبل وآليات مكافحتها وطنيا ودوليا من كونها جريمة تتجاوز حدود الوطنية.

تهدف دراستنا إلى تحليل إجراءات التقاضي الإلكتروني، وتوضيح تطبيقاته وأثره الإيجابي في تعزيز قطاع العدالة. كما نسلط الضوء على مدى الاهتمام بتطوير هذه التقنية على المستوى التشريعي، ونستعرض الإجراءات التي اتخذتها وزارة العدل لتفعيلها في الواقع العملي على نطاق واسع.

أسباب اختيار موضوع الدراسة:

تتبع **الأسباب الموضوعية** التي دفعت إلى اختيار هذا الموضوع بشكل أساسي من قيمته العلمية حيث يحتل الموضوع مكانة بارزة ومهمة في مختلف التشريعات القانونية المقارنة، كما أن الجريمة الالكترونية تعتبر جريمة العصر الحالي، مما يجعل البحث في هذا الموضوع ذا أهمية بالغة، مما أوجب تحويرا جذريا للنصوص القانونية موضوعية كانت او إجرائية، ودفعت الى إعادة هيكلة مرفق العدالة برمته، ودفعت الى عصرنته تماشيا مع المستجدات التي احدثتها التكنولوجيات الحديثة.

أما **الأسباب الذاتية** التي جعلتنا نختار هذا الموضوع ميولنا الشخصي للبحث عن الحلول التي لجأ اليها واضعو القانون الجنائي لمجابهة مشاكل التكنولوجيا الحديثة ولاسيما الجريمة الالكترونية نموذجا في هذه الدراسة وكيف استفاد القانون الجزائي من التكنولوجيا الحديثة في تطوير قواعده.

إشكالية الدراسة:

تتمحور الدراسة حول الإجابة عن الإشكالية التالية:

– كيف أثرت التطورات التكنولوجية الحديثة على طبيعة الجرائم المرتكبة في الجزائر؟ وماهي السبل البديلة والعصرية التي اعتمدها المشرع لتحديث النظام القانوني الجزائري لمواجهتها؟.

وتندرج عن الإشكالية الرئيسية للدراسة بعض التساؤلات الفرعية التي يمكن إيجازها فيما يلي: ماهي الآليات التي اعتمدتها الجزائر في تطبيق نظام المحاكمة الإلكترونية؟ وما الفوائد التي يوفرها هذا النظام، وما التحديات التي تواجهه؟.

المنهج المتبع:

فيما يخص المنهج العلمي المستخدم في هذه الدراسة، نجد أن طبيعة الموضوع الذي بحثناه تتطلب منا تبني المنهج الاستقرائي. هذا يعني القيام بدراسة وتحليل دقيق للنصوص القانونية المتعلقة بتدخلات المشرع في كل من الجوانب الموضوعية والإجرائية. وكذلك استعمل المنهج الوصفي أثناء التطرق للجوانب المفاهيمية العامة.

الدراسات السابقة:

لقد استلهمنا دراستنا للموضوع بالاعتماد على العديد من الاعمال والدراسات السابقة نذكر منها:

- مذكرة الماجستير في القانون للباحث: عبد العزيز بوذراع، **خصوصية الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات**، كلية الحقوق جامعة الجزائر 1، 2011-2012

- مذكرة الماجستير في القانون للباحثة: أمال قارة، **الجريمة المعلوماتية**، كلية الحقوق جامعة بن عكنون، الجزائر 2001.

والفرق بين دراستنا والدراسات السابقة أننا حاولنا التطرق الى تأثير التكنولوجيات الحديثة على تطور قواعد القانون الجزائي، ودورها في تنامي ظاهرة الجرم المستحدث -الجريمة الالكترونية أنموذجا- وكذا مجابهة هذه المنظومة القانونية

موضوعيا واجرائيا لظاهرة تناميه، ثم في دور هاته التكنولوجيات في تعزيز قواعد القانون الجزائي.

صعوبات الدراسة

– أثناء تدرجنا في مسار تصميم وكتابة مذكرتنا، جوبهنا ببعض الصعوبات التي تعد متناسبة مع طبيعة البحث والتنقيب العلميين، والتي نجملها فيما يلي:

– تشعب الدراسة تتطلب المزيد من الوقت لأجل الإحاطة بمختلف جوانبها والهدف استيفاء معالجتها ومناقشتها.

– كثرة النصوص القانونية وصعوبة تحليلها ومناقشتها.

خطة الدراسة:

انطلاقا من الاعتبارات السابقة وللإحاطة الشاملة بالموضوع وتحقيق الأهداف المرجوة منه فقد اعتمدنا على خطة ثنائية وفق تسلسل منهجي متناسق ورد في مقدمة وفصلين يتناول الأول " **دور التكنولوجيات الحديثة في ظهور الجرائم المستحدثة –الجريمة الالكترونية أنموذجا–**" ، أما الفصل الثاني فقد تضمن " **دور التكنولوجيات الحديثة في تعزيز قواعد القانون الجزائي** "، قدمنا في نهاية هاته الدراسة جملة من النتائج والمقترحات ضمناها في خاتمة.

الفصـل الأول

دور التكنولوجيات الحديثة في ظهور الجرائم المستحدثة

-الجريمة الالكترونية أنموذجا-

تمهيد:

أحدثت الثورة المعلوماتية، التي اجتاحت العالم في أواخر القرن العشرين، تحولاً جذرياً في كيفية تفاعلنا، مما جعل المسافات البعيدة تبدو أقرب والعالم كأنه يعيش تحت سقف واحد، هذا التطور التكنولوجي الكبير، مع ذلك، لم يأتِ دون تكلفة، إذ رافقه ظهور جرائم جديدة ومنها الجريمة الالكترونية التي تنتشر بسرعة البرق في كافة أرجاء العالم، مما يستلزم تطوير أساليب جديدة للتعامل مع هذه الظاهرة العابرة للحدود.

ومن ثم، بات من الضروري لكل المعنيين التعمق في دراسة الجريمة الالكترونية بأصنافها المختلفة، وبهذا، يقع على عاتق الباحثين في مجال العلوم القانونية وسائر التخصصات المعرفية مسؤولية تفحص هذه القضية لتحديد مفهومها ، توضيح مكوناتها وخصائصها، والعوامل المسببة لها، وطرق وأدوات التحقيق المتعلقة بها، فضلاً عن إثبات الجريمة وغيرها من الجوانب المتصلة بهذا الموضوع، وللإحاطة بهاته الدراسة سنتناول في المبحث الأول ماهية الجرائم الالكترونية، بينما نتطرق في المبحث الثاني الى جرائم المساس بأنظمة المعالجة الآلية للمعطيات وفقا للقانون 09-04.

المبحث الأول: ماهية الجرائم الالكترونية.

أصبحت الجرائم في مجال المعطيات الرقمية، بمظاهرها وأبعادها المعاصرة، تشكل تهديدًا مباشرًا لا يقتصر فقط على الأفراد والجماعات، بل تمتد آثارها لتشمل الدول بأكملها، هذا التطور دفع العديد من الدول إلى اتخاذ خطوات فعالة نحو مكافحة هذه الجرائم من خلال التوقيع على اتفاقيات دولية مثل اتفاقية بودابست، مما يعكس الجهود الدولية المتزايدة للتصدي لهذا التهديد العابر للحدود.

سنتناول في هذا المبحث ماهية الجرائم الالكترونية، من خلال تحديد مفهومها كمطلب أول ومفهوم مرتكبها أي المجرم الالكتروني كمطلب ثاني.

المطلب الأول : مفهوم الجريمة الالكترونية

لتقديم مفهوم واضح وشامل للجريمة الإلكترونية سنحاول التطرق الى تعريف الجريمة الإلكترونية مع تبيان خصائصها ، ودواقع ارتكابها وتناول المجرم الالكتروني.

الفرع الأول: تعريف الجريمة الالكترونية وخصائصها

ينبغي الإشارة الى غياب وجود تعريف موحّد جامع لمصطلح الجريمة الالكترونية، وفي هذا السياق تباينت التعريفات واستحدث الدارسون لها عددًا ليس بالقليل من التعريفات كلٌّ على حسب الدراسة ، وعليه سنتعرّض فيما يلي الى عرض موجز لتمايز التعريفات حول موضوعنا (أولا)، لنصل بعدها لتبيان خصائصه في (ثانيا).

أولا : تعريف الجريمة الالكترونية

تُعرّف الجريمة، في سياق القانون الجزائي التقليدي، بأنها عمل غير مشروع نابع من إرادة جنائية، ينص القانون لها على عقوبة أو تدبير احترازي[1]، ولئن دراستنا تتمحور حول الجريمة الالكترونية سنتطرق اليها بتعريفها من الناحية الفقهية لتبيان ما استعمله الفقهاء، **وصولا** الى الناحية التشريعية لإلقاء نظرة حول القواعد القانونية في ذات الخصوص.

1 – التعريف الفقهي للجريمة الالكترونية

يُعرف الفقه الفرنسي الجريمة الإلكترونية بأنها الاعتداءات القانونية التي تُرتكب باستخدام التقنيات المعلوماتية، والتي غالبًا ما تهدف إلى تحقيق الربح. ومع ذلك، قد لا تكون دوافع الجريمة الإلكترونية مرتبطة دائمًا بالربح، بل قد تشمل أيضًا الانتقام، السخرية من المنافسين، أو دوافع أخرى[2].

وقد عرفها خبيرا أمريكي: كل فعل إجرامي متعمد أيا كان صلته بالمعلوماتية ينشأ عن خسارة تلحق بالمجنى عليه وكسب يحققه الفاعل[3].

وقد جاء الفقه العربي بعدة تعريفات نذكر منها:

تُعرف الجريمة الإلكترونية بأنها الجريمة التي تُرتكب في الفضاء الافتراضي للحواسيب، حيث يُستخدم الحاسوب كأداة لتنفيذ أركانها[4]، وهي أي فعل أو امتناع متعمد ينبع

---

[1]– محمد نجيب حسني ، **شرح قانون العقوبات القسم الثاني**، دار النهضة العربية، ط6، مصر،1989، ص40.

[2]– محمد عبد الله أبو بكر سلامة، **موسوعة جرائم المعلوماتية**، منشأة المعارف الإسكندرية ،2007، ص 20.

[3]– نقلا عن ممدوح عبد المجيد عبد المطلب، **جرائم استخدام شبكة المعلومات العالمية** – الجريمة عبر الانترنيت–، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنيت، كلية الشريعة والقانون بجامعة الامارات العربية المتحدة ،2000، ص 12.

[4]– سن مظفر الرزو، **القضاء المعلوماتي**، مركز دراسات الوحدة العربية ،الطبعة الأولى ، 2007، ص 31 .

من الاستخدام غير القانوني لتكنولوجيا المعلومات، بهدف الاعتداء على الممتلكات أو الحقوق المعنوية.

أو تُعرَف بأنها فعل أو تقصير متعمد يهدف إلى إلحاق الضرر بمكونات الحاسوب وشبكات الاتصال المرتبطة به، والتي يحميها قانون العقوبات ويقرر لها عقابًا[1].

تُعرَّف بأنها كل فعل يلحق الضرر بالآخرين عبر وسائل إلكترونية مثل الحواسيب، الهواتف المحمولة، شبكات الاتصال الهاتفي، شبكات نقل المعلومات، الإنترنت، أو الاستخدامات غير القانونية للبيانات الحاسوبية الإلكترونية[2].

ويلاحظ مما سبق أن التعريفات تختلف بناءً على عدة جوانب؛ بعضها يرتكز على موضوع الجريمة نفسها، في حين تركز تعريفات أخرى على الوسائل المستخدمة في ارتكاب الجريمة. كما توجد تعريفات تأخذ في الاعتبار السمات الشخصية لمرتكب الفعل الإجرامي.

أ- التعريفات التي تستند إلى موضوع الجريمة:

من الضروري أن يكون الفعل المرتكب غير قانوني ويخالف الأنظمة القانونية، مما يترتب عليه إلحاق الضرر بالمجني عليه. تتضمن هذه التعريفات أي سلوك غير مشروع أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو تداولها[3].

ب- التعريفات التي انطلقت من وسيلة ارتكاب الجريمة:

الجريمة عبر الإنترنت لا يمكن ارتكابها دون استخدام الحاسوب، الذي يشكل العنصر الأساسي وليس مجرد طريق ثانوي للمشاركة في الجريمة، بل هو الوسيلة الرئيسية لتنفيذ

[1]- مناصرة يوسف، **جرائم المساس بأنظمة المعالجة الآلية للمعطيات** ، دار الخلدونية للنشر والتوزيع ، الجزائر، 2018 ، ص 32.

[2]- محمد عبد الله أبو بكر سلامة، المرجع السابق، ص 47.

[3]- هدى حامد قشقوش، **جرائم الحاسب الالكتروني**، دار النهضة العربية ،القاهرة ،1992، ص .120

الاعتداء. تُعرّف هذه الجرائم بأنها أي عمل إجرامي يلعب فيه نظام الحاسوب دورًا جوهريًا لإتمامه، سواء كان الحاسوب وسيلة لتنفيذ النشاط الإجرامي أو كان موضوعًا له[1].

ج- التعريفات استنادا لسمات الشخصية لدى مرتكب الفعل:

عُرّف هذا النوع من الجرائم بأنه يتطلب خبرة متخصصة في تطبيقات الحاسب الآلي ونظم المعلومات لارتكابها أو للتحقيق فيها ومقاضاة مرتكبيها[2].

د- التعريفات التي ترتكز على أكثر من معيار لبيان ماهية جريمة الانترنيت:

عرّف الأستاذ "جون كارول" الجريمة الإلكترونية بأنها أي عمل غير قانوني يضر بالأفراد أو الممتلكات، موجه ضدهم ويستخدم التكنولوجيا المتقدمة لنظم المعلومات[3].

ومما سبق تُعرف الجرائم الإلكترونية بأنها أي فعل أو امتناع عن فعل يقوم به شخص ويؤدي إلى الضرر بمكونات الحاسوب أو شبكات الاتصال المحمية قانونًا، ويخضع فاعله للعقاب بموجب القانون.

2 - التعريف التشريعي للجريمة الالكترونية

اختلفت التشريعات العربية وحتى الغربية في اعطاء تعريف للجريمة الإلكترونية نظرا للنمو المتسارع لاستخدام الانترنت، والسبب يعود الى ما يطلق عليه الثورة المعلوماتية ما جبر التشريعات الى التّماشي مع هذه الثورة وضبط سياسة للمعاملات الإلكترونية والجرائم الناتجة عنها.

---

[1]- نائلة عادل محمد فريد بدقورة، **جرائم الحاسب الآلي الاقتصادية (دراسة نظرية مقارنة)**، منشورات المجلس الحقوقية ، الطبعة الأولى، 2005، ص ص 32-33.

[2]- عبد الفتاح مراد، **شرح جرائم للكمبيوتر والانترنيت** ، منشأة المعارف، مصر، 1998، ص 40.

[3]- نقلا عن هشام فريد رستم، **قانون العقوبات ومخاطر تقنية المعلومات** ، مكتبة الآلات الحديثة ، مصر، 1994، ص32.

فقد عرف المشرع السعودي الجريمة الالكترونية بأنها "أي فعل يُرتكب باستخدام الحاسب الآلي أو الشبكة المعلوماتية يُعد مخالفًا لأحكام النظام"[1]. والمشرّع المصري مثلًا ترك تعريف الجريمة الإلكترونية للفقه، فهناك من عرّفها على اساس انها "عمل او امتناع يأتي بأضرار بمكونات الحاسب وشبكات الاتصال الخاصة به التي يحميها قانون العقوبات ويفرض لها عقابا"،[2] أما المشرّع الامريكي وحسب وزارة العدل في الولايات المتحدة الأمريكية فقد عرفت جريمة الكمبيوتر بانها "اي انتهاكات للقانون الجنائي تتضمن المعرفة بتكنولوجيا الكمبيوتر لارتكابها"،[3] وحسب مكتب تقييم التقنية في الولايات المتحدة الأمريكية فجرائم الحاسوب هي تلك الجرائم التي تشترك فيها البيانات الرقمية والبرمجيات بدور أساسي[4].

وبالرجوع للمشرع الجزائري فقد سعى لمواكبة التطورات الحديثة في مجال الجريمة الإلكترونية من خلال إنشاء إطار قانوني مناسب، يتمثل في القانون رقم 09-04 الذي يضع قواعد خاصة بالوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال ومكافحتها. يتميز هذا القانون بتكامله بين الأحكام الجنائية المكملة لقانون الإجراءات الجزائية وبين الأحكام الوقائية التي تهدف إلى الكشف المبكر عن الاعتداءات المحتملة والتدخل الفوري لتحديد مصادرها والتعرف على مرتكبيها، وقد حدد المشرع الجزائري في المادة 2 من القانون رقم 09-04 الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال كتلك الجرائم المتضمنة المساس بأنظمة المعالجة الآلية للمعطيات كما محددة في قانون العقوبات، بالإضافة إلى أية

---

[1]- راجع المادة 8 من النظام السعودي بشأن مكافحة المعلوماتية عام 2007.

[2]- محمد علي العريان، **الجريمة المعلوماتية**، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، 2011، ص56.

[3]- موقع وزارة العدل الامريكية، الاطلاع بتاريخ 2024//04/26م، على الساعة 15.36،
https://www.ojp.gov/ncjrs/virtual-library/abstracts/computer-crimes-

[4]- فاروق سيد الحسين ، **الانترنيت الشبكة العالمية للمعلومات** ، مطابع الهيئة المصرية الهامة للكتاب، القاهرة ،1998 ، ص 293.

جرائم أخرى تُرتكب أو يُسهل ارتكابها باستخدام منظومة معلوماتية أو الاتصالات الإلكترونية[1].

الفرع الثاني: خصائص وتصنيفات الجرائم الالكترونية

للجريمة الالكترونية خصائص تميزها عن الجريمة التقليدية كما لها تصنيفات، وهذا ما سنتعرض إليه في هذا الفرع.

أولا: خصائص الجرائم الالكترونية*

تتميز الجريمة الإلكترونية عن الجريمة التقليدية في عدة أوجه، سواء من حيث الدافع لارتكابها أو في أسلوب تنفيذها ذاته. كما أن لها طابعًا دوليًا يتجاوز حدود الدول الفردية. ومن خصائصها:

1- الجريمة الإلكترونية مستترة:

ترتكب الجريمة الإلكترونية بشكل خفي، دون إدراك المجني عليه لها، ويقوم الجاني بارتكابها من خلال استخدام كمبيوتر متصل بشبكة الإنترنت عن بُعد، ويتطلب من الفاعل أن يمتلك المهارة والمعرفة اللازمة بتقنيات استخدام الكمبيوتر لتنفيذها[1].

---

[1]- راجع المادة 2 من قانون 04/09 المؤرخ في 14 شعبان 1430 هـ الموافق ل 05 غشت 2009 م المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية، عدد 47، سنة 2009.

*- للجريمة الإلكترونية العديد من الخصائص التي لا يمكن عدها ولا حصرها مثل: صعوبة الاحتفاظ الفني بأثرها ان وجد/ تحتاج الى خبرة فنية ويصعب على المحقق التقليدي التعامل معها /سهولة اخفاء معالم الجريمة/ تتسم هذه الجرائم بالغموض حيث يصعب اثباتها والتحقيق فيها /غالبا ما تكون الخسائر الناجمة عنها فادحة/ عدم وجود مفهوم مشترك للجريمة الالكترونية/ قد ترتكب من طرف شخص واحد او بتعاون أكثر من شخص على ارتكابها/ صعوبة الحصول على دليل مادي في مثل هذه الجرائم،

- نورة بن بوعبد الله، **الجريمة الالكترونية (مقاربة مفاهيمية)**، مداخلة ألقيت في الملتقى الوطني حول الجريمة الالكترونية وتداعيات الأمن السيبيراني بين النظرية والواقع، كلية الحقوق والعلوم السياسية، جامعة باتنة1، يوم 11 ماي 2023.

التعرف على مرتكبي الجرائم الالكترونية يُعتبر من الجوانب الأكثر أهمية وتحدياً، نظرًا لسرعة وسهولة فقدان البيانات الإلكترونية التي يُمكن تدميرها، محوها، حذفها، أو تعديلها. هذه العوامل تزيد من صعوبة المهام المنوطة برجال الأمن والمحققين القضائيين.

2- الجريمة الإلكترونية تنفذ عن بعد:

تتميز الجرائم الإلكترونية بطابعها العابر للحدود الجغرافية، حيث يمكن ارتكاب جرائم مثل تبييض الأموال وسرقة المعلومات البنكية وبطاقات الائتمان عبر الإنترنت دون الحاجة للسطو المادي على البنوك. يُمكن للفاعل ارتكاب هذه الجرائم من خلال حساب إلكتروني متصل بشبكة الإنترنت من دولة معينة بينما تظهر نتائج الفعل الإجرامي في دولة أخرى[2].

3- سهولة ارتكاب الجريمة الإلكترونية:

أصبح بمقدور أي شخص لديه معرفة أساسية بكيفية استخدام الحاسوب أن يرتكب جرائم معلوماتية متنوعة عبر شبكة الإنترنت، بفضل توفر البرامج والتطبيقات المجانية التي تسهل هذه الأعمال. هذا التسهيل أدى إلى تعزيز تبادل الخبرات والأفكار بين الجناة عالمياً، مما زاد من مرونة وسهولة التخطيط وتنفيذ هذه الجرائم.

4- **الجريمة الإلكترونية تحدث بدون عنف ولا مقاومة:**

لا يتطلب الجاني المعلوماتي، الذي يرتبط بالضحية، استخدام العنف أو السلاح؛ بل يعتمد على ذكائه ومعرفته بتقنيات الحاسوب والإنترنت. على سبيل المثال، قد يتلقى الضحية

---

[1]- محمد عبد الوهاب سلطان العلماء، **جرائم الانترنيت واحتساب عليها**، المجلة العربية للدراسات الأمنية والتدريب، السنة 18 عدد 36/1424 ، ص 52.

[2]- عبد الله حسين على محمود، **سرقة المعلومات المخزنة في الحاسب الآلي**، مجلة الأمن والقانون، السنة الثانية العدد الأول ، 2004 ، ص 374.

رسالة بريد إلكتروني تحمل فيروسًا يضر الحاسوب فور فتحها، مما يؤدي إلى اختراق الجهاز وسرقة البيانات الحساسة مثل الشفرات والأرقام السرية. لذلك، ينصح دائمًا بتجنب استخدام الحاسوب دون التحقق من خلوه من الفيروسات.

5- صعوبة إثبات الجريمة الإلكترونية:

نظرًا لوقوعها في بيئة افتراضية، تفتقر الجرائم الإلكترونية إلى ترك أي آثار مادية ملموسة، على عكس الجرائم التقليدية التي يمكن إدراكها بالحواس، كما في حالات التزوير للسندات والنقود والطوابع. بينما يمكن للجرائم التقليدية أن تترك أدلة مادية ملحوظة في مسرح الجريمة مثل الشعر، الدم، بصمات الأصابع، وآثار الأقدام. في المقابل، تتميز الجرائم عبر الإنترنت بسهولة إزالة الأدلة ومحوها؛ إذ يمكن القيام بذلك بسرعة فائقة، وربما بضغطة خاطئة على لوحة مفاتيح الحاسوب، مما يجعلها جرائم غير مادية بحتة لا تترك آثارًا مادية تشير إلى وقوعها[1].

6- التفتيش في نطاق هذه البيئة عديم الجدوى:

نظرًا للصعوبات التي تواجهها أثناء التنفيذ بالمقارنة مع الجرائم التقليدية. في جرائم الحاسوب، يركز التفتيش على المكونات المادية للحاسوب وملحقاته وفقًا لقانون الإجراءات الجزائية، بما في ذلك البيانات المخزنة على وسائط مادية مثل الأقراص الممغنطة، الأقراص الصلبة، والأقراص الضوئية[2].

---

[1]- محمد الرشيدي، **العنف في جرائم الانترنيت**، الدار المصرية اللبنانية، مصر، ص 38.

[2]- أسامة أحمد، **جرائم الحاسب الآلي والانترنيت** ، دراسة تحليلية مقارنة، الطبعة الأولى، دار وائل للنشر، عمان الأردن، 2000 ، ص 276.

7 – نقص الخبرة الفنية لدى المحققين:

يشكل نقص الخبرة الفنية لدى المحققين عائقًا كبيرًا أمام إثبات الجرائم المعلوماتية، إذ تتطلب هذه الجرائم خبرة فنية مرتفعة وفهمًا شاملًا لاستخدام الحواسيب والتعامل معها. في بعض الأحيان، قد يكون المحقق نفسه مسؤولًا عن فقدان أو تدمير الأدلة نتيجة لسوء تعامله معها، وذلك بسبب نقص خبرته ومعرفته الفنية اللازمة لاستخراج الأدلة بشكل فعال وسليم[1].

ثانيا: تصنيف الجرائم الالكترونية.

قام مشروع اتفاقية الأوروبية بإدخال تصنيف جديد نسبيًا للجرائم الإلكترونية، متضمنًا أربع فئات مختلفة تغطي أطياف متنوعة من هذه الجرائم. وتم حصرها فيما يلي:

1: تتضمن الجرائم الالكترونية التي تستهدف السرية والسلامة، الأفعال مثل الدخول غير القانوني إلى النظم، وتدمير البيانات، واعتراض النظم، بالإضافة إلى إساءة استخدام الأجهزة لأغراض محظورة قانونيًا.

2: الجرائم التي يرتكبها الأفراد باستخدام الكمبيوتر تشمل التزوير والاحتيال.

3: الجرائم المرتبطة بالمحتوى تشمل تلك الأفعال المرتكبة في مجال الإباحية والمسائل الأخلاقية.

4: الجرائم المتعلقة بانتهاك حقوق الملكية الفكرية والحقوق المجاورة، مثل قرصنة البرمجيات[2].

قام الفقيه "إيلريش سيبر" بتصنيفها إلى ثلاث فئات رئيسية:

---

[1]– محمد السنبري، **التحقيق في جرائم الحاسب الآلي دراسة قانونية مقارنة**، مقدمة أعمال مؤتمر القانون والكمبيوتر والانترنيت الذي عقدته كلية الشريعة والانترنيت بجامعة الإمارات ، 2005.

[2]– الاتفاقية الأوروبية لمكافحة جرائم المعلوماتية ، الجرائم الإلكترونية اتفاقية ببودابست 23/11/ 2001 لمكافحة الجرائم المعلوماتية.

1 – جرائم الحاسب الآلي الاقتصادية تشمل الاحتيال المعلوماتي، التجسس المعلوماتي الإتلاف المعلوماتي، والوصول غير المصرح به إلى نظام الحاسب الآلي.

2– جرائم التعدي على خصوصية الحياة الشخصية.

3– الجرائم التي تستهدف الأمن القومي والسلامة الفردية للأشخاص[1].

يعتبر الفقه الفرنسي أن نشر صور تتعلق بالحياة الخاصة للفرد من دون موافقته الصريحة أو الضمنية يمثل اعتداءً على حقه في الخصوصية.

المطلب الثاني: مفهوم المجرم الالكتروني

قد يكون المجرم الالكتروني شخصا طبيعيا يرتكب الجريمة بنفسه ولحسابه الشخصي، وقد يكون شخصا طبيعيا يقوم بالفعل المجرّم لصالح شخص معنوي (شركة مثلا)، وللمجرم الالكتروني دوافع كثيرة ، وقدا قمنا بذكر أهمها وأكثرها شيوعا كفرع ثاني وقبلها سنتناول تعريف المجرم الالكتروني كفرع أول.

الفرع الأول: تعريف المجرم الإلكتروني

المجرم الالكتروني، في جوهره، ليس سوى فرد من المجتمع يمارس حياته اليومية، وقد يكون مختصًا في مجال الإعلام الآلي، هاوٍ، أو مجرد مستخدم للحاسب الآلي. يواصل هذا الشخص ممارسة وظائفه وحقوقه الاجتماعية والسياسية دون مواجهة عوائق في حياته المهنية، وغالبًا ما يتميز بمستوى عالٍ من الذكاء ويُعتبر شخصًا محترمًا ضمن محيطه[2].

الباحثون متفقون مؤخرًا على أن التصنيف الأمثل لمجرمي الإنترنت يجب أن يعتمد على الأغراض التي من أجلها يتم الاعتداء، وليس بناءً على التكتيكات أو الوسائل المستخدمة في ارتكاب أو تنفيذ الاعتداء.

---

[1]– Emmanuel ZEZ , les noms de domaine de l'internet, Aspets juridiques ,Litee,2000,P50.

[2]– محمد على العريان ، **الجرائم المعلوماتية** ، دار منشأة المعارف ، الإسكندرية 2003 ، ص61.

قام كل من "ديفيد كور"، "كارل سيرغو ويليام"، "وفوشورش" بتقسيم مجرمي الإنترنت إلى ثلاث فئات:- المحترفون.

- المنحرفون.
- الحاقدون.

من التقسيمات الهامة في مجال جرائم الكمبيوتر والإنترنت، التمييز بين الجناة الصغار السن والبالغين الذين يجتمعون لتشكيل تنظيمات إجرامية خطيرة. ومن بين المتسللين إلى الشبكات، نجد المهاجمين أو المخترقين الذين يستهدفون المنظمات والشبكات، بالإضافة إلى المتسللين لنظم الاتصال الاجتماعي والمخترقين الذين يفتقرون إلى الخبرة[1].

أ- <u>المتسلل إلى الشبكة:</u>

هو شخص يتمتع بمهارات عالية في التعامل مع الشبكات، خاصةً شبكة الإنترنت، وهو خبير في اختراق أجهزة الكمبيوتر ونظم الحماية بطريقة غير قانونية، مدفوعًا بالفضول. غالبًا ما يكون غير مؤذٍ، وهو شخص مولع بالتكنولوجيا، يجد متعته في استكشاف تقنيات الكمبيوتر وعمليات البرمجة المتصلة بها. ليس لديه دوافع عدائية أو تخريبية؛ بل ينطلق من رغبة في التحدي وإثبات القدرات. قد منع القانون الفرنسي الاعتداءات على الوسائل التقنية من خلال استخدام أدوات تم تطويرها أو تجهيزها بشكل خاص لهذا الغرض، وذلك بشكل فردي دون اللجوء إلى أي أعمال مساعدة. ويفرض القانون الفرنسي عقوبة تصل إلى غرامة مالية تبلغ 3750 يورو على مرتكبي هذا النوع من الجرائم[2].

---

[1]- David core, Karl Sergu William, Voushorch computer crime d'heillez et Associaés.in 1995,P70 .

[2]- عرب تونس ، **جرائم الكمبيوتر والانترنيت**، منشورات اتحاد المصارف العربية، الطبعة الأولى، 2002، ص268.

ب – صغار السن:

هم شباب مهتمون بعالم المعلوماتية، يقل أعمارهم عن السن القانونية للأهلية، يحفزهم التحدي ورغبة في التغلب على التقنيات الحاسوبية. غايتهم تتمثل في التسلية والمزاح مع الآخرين أحيانًا، ونيتهم لا تتضمن الإضرار بالأشخاص المتضررين من تصرفاتهم[1].

ج – مخترعو النظم والشبكات:

هؤلاء الأشخاص يتخصصون في سرقة البرمجيات والمواقع الإلكترونية، ويتسمون بقدراتهم التدميرية من خلال نشر الفيروسات والتروجانات في المواقع والأنظمة التي ينجحون في اختراقها. يهدفون إلى الحصول على صلاحيات الوصول غير المشروعة للشبكات أو الأنظمة المستهدفة.

ح – الحاقدون:

تتسم هذه الفئة بالسخط، إما على مؤسساتهم أو على شركائهم. دوافعهم لا تقتصر على الربح المادي أو إظهار المهارات التقنية، بل يسعون لإلحاق الضرر بالآخرين من خلال نشر البيانات السرية، استخدامها بشكل ضار، أو حتى مسحها. يحركهم الرغبة في الانتقام والثأر، حيث يستخدمون الفيروسات والبرمجيات الضارة لتعطيل وإتلاف الأنظمة والبيانات[2].

خ – المجرمون المنظمون المحترفون:

ينشطون هؤلاء المجرمون ضمن أطر الجريمة المنظمة، مستخدمين التقنيات الحاسوبية لتحقيق منافع مادية بطرق غير قانونية. يتمتعون بخبرة واسعة ومعرفة فنية متقدمة، مما يجعلهم أكثر خطورة من المجرمين التقنيين الآخرين. نشاطهم يتنوع بحسب الجريمة، من

---

[1]– Peter Greinsbosky,electronic crime upper.sadal.River N5 Pearsons,Prentrie,Hall–2007,P13.

[2] –B.Strenling they Haker. Crak ouv, Lawend electronic Fouinter, London,Viking,1993,P3.

التجسس الصناعي واختراق أنظمة المنافسين، إلى العمل لحساب منظمات إرهابية أو سياسية أو حتى دول، مما يجعلهم فاعلين رئيسيين في ساحات النزاعات التقنية العالمية.

د – مجرمون ذو معتقدات وأفكار خاصة:

تتميز هذه المجموعة بامتلاكها لأيديولوجيا محددة قد تكون سياسية، دينية، أو اجتماعية، تهدف إلى لفت الانتباه لوجهات نظرها ومطالبها. يتجلى هذا في اعتداءاتهم على أنظمة الحاسوب الحكومية، التي تعتبر ركيزة أساسية في إدارة الشؤون الدولية، وخصوصاً في المجالات الحساسة مثل الأمن العسكري والمفاعلات النووية. هذه الاعتداءات تهدف للتأثير وإحداث ضرر في المصالح الوطنية الحيوية.

ذ – مخترعو الشبكات في النظم قليلو الخبرة:

هؤلاء هم الأفراد الذين يستفيدون من المعلومات والبرامج التي يطورها الهاكرز، مستخدمين إياها في التنفيذ دون القدرة على اكتشاف الثغرات أو تطوير الأدوات بأنفسهم. بدلاً من ذلك، يقتصر دورهم على تطبيق هذه الأدوات المعدة مسبقًا[1].

ر – المتسلل إلى نظم الاتصال الهاتفي:

هو الفرد الذي يخترق شبكات الهاتف أو أنظمة الاتصالات الأخرى المؤمنة بهدف استكشاف طريقة عملها ومعرفة خصائصها[2].

الفرع الثاني: دوافع ارتكاب الجريمة:

بعد مناقشة تصنيفات المجرمين الإلكترونيين، نتوقف هنا لاستعراض الدوافع التي تحفزهم على ارتكاب جرائمهم، ومن بين هذه الدوافع نذكر:

---

[1]- حسن دوواد طاهر، **جرائم نظم المعلومات** ، أكاديمية نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى ، 2000 ، ص 58.

[2]– حسن دوواد طاهر، المرجع السابق ، ص 58.

1 – دافع التحدي:

يظهر المجرم المعلوماتي مهاراته التقنية والمعرفة المعلوماتية، مما يدفعه نحو الجريمة دون وعي كامل بتصرفاته، باستخدام مهارات إجرامية تقنية في التنفيذ، يهدف إلى اختراق الجدران الأمنية للنظم المعلوماتية ليبرهن على وجود عدة ثغرات أمنية، وليس الربح هو دافعه الأساسي، بل إثبات قدراته في المجال التكنولوجي.

2 – دافع الربح:

الدافع نحو تحقيق الربح المادي والإغراء المالي يأتي من جماعات العصابات المنظمة أو المؤسسات المتنافسة أو حتى الحكومات المتصارعة، التي تستهدف الحصول على معلومات عسكرية، سياسية، اقتصادية أو بيانات حكومية حساسة.

3– دافع إيديولوجي:

تتحفز هذه الفئة من المجرمين الإلكترونيين للدفاع عن أو نشر أو دعم تبني الآراء، الأفكار الدينية أو الأيديولوجية. وقد يقودهم الشغف تجاه هذه الأفكار إلى التورط في أعمال عنف إجرامي ضد المعارضين لها، باستخدام أساليب الجريمة الإلكترونية بمختلف أشكالها وأنواعها.

4 –دافع التسلية:

الفضول والرغبة في استكشاف المجهول يغري الشباب بالغوص في عالم الحرب المعلوماتية، ويجذبهم لما تحتويه من تقنيات ومعلومات وخصائص تقنية متقدمة. هذه الرغبة تدفعهم للسعي وراء المزيد من المعرفة، وتنقيب في أعماق الأنظمة والمواقع ومحركات البحث وقواعد البيانات، مما يشبع فضولهم ورغبتهم في التحدي واستكشاف التقنيات الجديدة[1].

[1]– محمد سامي الشواء ، **ثورة المعلومات انعكاساتها على قانون العقوبات**، دار النهضة العربية ، مصر، 1998، ص ص 52.53.

5 –دافع الانتقام والتأثر:

قد تتجمع الضغائن والأحقاد الدفينة وتطفو على سطح التقنية، حيث يستغل البعض خبراتهم التقنية في التخريب وتدمير ما لدى الآخرين. فمن جراء التسريح التعسفي من العمل، قد يسعى البعض، ممن يملكون معرفة كافية بأنظمة الشركة أو المصرف الذي تم فصلهم منه، إلى إلحاق خسائر مالية كبيرة بهذه المؤسسات من خلال تدمير النظام المعلوماتي لها، أو السماح لجهات خارجية بالدخول وممارسة أعمال تخريبية، أو حتى استغلال النظام لإضحاك العموم وجني الأرباح[1].

المبحث الثاني: مواجهة الجريمة الالكترونية في التشريع الجزائري

في ظل التطور التكنولوجي المتسارع، برزت الحاجة الملحة لتطوير التشريعات الجزائية، خاصة في مواجهة الجرائم التي تستهدف المعطيات الرقمية، هذا التطور يتطلب تحقيق توازن بين تطور أنماط الجرائم الرقمية وفعالية الأساليب القانونية المستخدمة لمكافحتها. المشرع الجزائري، في هذا الإطار، يدرس فعالية الأنظمة والقوانين الحالية في مواجهة هذا النوع من الجرائم، مستكشفًا المجالات التي تعاني من نقص أو قصور لتطوير تشريعات جديدة تكفل تحقيق أعلى درجات الفعالية في مكافحة هذه الجرائم.

عكست جملة القوانين الصادرة في الجزائر مثل القانون رقم 09-04 والقانون 15-04، إلى جانب التعديلات التي أُدخلت على قانون العقوبات بموجب القانون 04-15، جدية المشرع في مكافحة الجرائم الالكترونية، هذه القوانين شملت تحديدًا استحداث جرائم ضمن القسم السابع المعنون ب"المساس بأنظمة المعالجة الآلية للمعطيات"، مما يبرز أهمية وضرورة

[1]– نعيم مغبغب ، **مخاطر المعلوماتية** ، المخاطر على الحياة الخاصة وحمايتها" دراسة في القانون المقارن ، منشورات الحلبي ،1998 ، ص ص 211-212

التعامل القانوني مع هذه الجرائم من خلال القواعد الموضوعية المتعلقة بالتجريم والجزاء نظرًا لتأثيرها الكبير على الأمن الرقمي والمعلوماتي (المطلب الأول)، كما أكد على متابعة مرتكبي هذه الجرائم وذلك بأساليب البحث و التحري و الاختصاص القضائي أو ما اصطلحنا عليه بالقواعد الاجرائية لمواجهة الجريمة الالكنرونية(المطلب الثاني) .

المطلب الأول: القواعد الموضوعية لمواجهة الجريمة الالكترونية في التشريع الجزائري

اهتم المشرع الجزائري بمواجهة الجريمة الالكترونية وذلك بسن قوانين تخص مكافحة هذه الجريمة للتصدي لها وردعها، وفي هذا المطلب سنتطرق الى صور الجريمة الالكترونية أو ما أطلق عليه قانونا بمصطلح الجرائم الماسة بأنظمة المعالجة الألية للمعطيات، العقوبات المقررة لها .

الفرع الأول: صور الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات

تتمثل هذه الجرائم في عدة صور نذكر منها مع تبيان البنيان القانوني لها:

أولا: <u>جريمة الدخول أو البقاء بغش:</u>

<u>1- الركن الشرعي:</u>

يفرض المشرع الجزائري عقوبات على الدخول والبقاء غير المصرح بهما وفقًا للمادة 394 مكرر من القانون العقوبات.

تعتبر جرائم الدخول أو البقاء في الأنظمة المعلوماتية عبر الغش من الأشكال المبسطة لجرائم المعالجة الآلية للمعطيات، حيث تتحقق هذه الجرائم عندما يتم "الدخول" أو "البقاء" غير المشروعين في نظام معلوماتي.

احتدم الجدل الفقهي حول تجريم الدخول والبقاء غير المصرح بهما في الأنظمة المعلوماتية، حيث يرى بعض الفقهاء أن هذه الأفعال قد تعكس مجرد تمرين تقني أو استعراض للمهارات الذهنية للفرد الذي يقوم بها، ولا ينبغي أن تُعتبر جرائم تستوجب العقوبة.

يدعم التيار الثاني تجريم الدخول والبقاء غير المصرح بهما في المنظومات المعلوماتية، حتى في حال 2عدم وجود نية لارتكاب جرائم لاحقة. يستندون في موقفهم إلى الأضرار المادية الناجمة عن هذه الأفعال، إذ يوجد أكثر من 100 ألف خبير استشاري في المجال المعلوماتي يعملون بأكثر من 20 ألف شركة حول العالم، حيث بلغ إجمالي النفقات التي أنفقتها هذه الشركات على خدمات الاستشارات المعلوماتية ما يقرب من 4.5 مليون دولار لضمان أمن المعاملات الإلكترونية.

2- الركن المادي: يتشكل الركن المادي في جريمة الدخول والبقاء غير المصرح بهما من صورتين: صورة بسيطة وصورة مشددة.

أ- فعل الدخول: يشمل الولوج إلى نظام المعالجة الآلية للمعطيات بشكل معنوي، وهدفه توجيه هجمات إلى النظام المعلوماتي بهدف الإضرار بسلامته أو التعدي على قدرته على أداء وظائفه بصورة غير مشروعة، وذلك من خلال استخدام برامج متطورة يديرها أفراد ذوو خبرة تقنية. الدخول يمكن أن يكون مباشرًا أو غير مباشر، ولا تعد هذه الأفعال جريمة عند استخدام الجاني لأجهزة مثل القرص، التلفاز، الكمبيوتر الشخصي، أو البطاقات الممغنطة، أو حتى عند إدخال رمز سري لحماية برنامج معين[1].

[1]- أمال قارة، **الجريمة المعلوماتية**، مذكرة ماجستير، تخصص قانون جنائي ، كلية الحقوق جامعة بن عكنون، الجزائر 2001، ص 42

ب- فعل البقاء:

نعني بالتواجد داخل نظام المعالجة الآلية للمعطيات من دون إرادة مالك الموقع أو النظام، وهذه الجريمة تشمل وجهين: الوجه الإيجابي الذي يتعلق بالفعل الإيجابي للبقاء داخل النظام، والوجه السلبي الذي يرتبط بفعل سلبي يتمثل في رفض الجاني مغادرة النظام. يختلف الفقهاء حول تحديد متى تنتهي جريمة الدخول ومتى تبدأ جريمة البقاء؛ حيث يرى الاتجاه الأول أن جريمة الدخول تتحقق بمجرد دخول الجاني إلى النظام ويتبع ذلك استمراره لفترة محددة يبدأ بعدها التأطير لجريمة البقاء، وتنتهي هذه الجريمة بانتهاء حالة البقاء. بينما يرى الاتجاه الثاني أن تلك الفترة تبدأ من اللحظة التي يدرك فيها الجاني أن وجوده داخل النظام يُعد غير قانوني[1].

الرأي الأرجح يقضي بأن جريمة البقاء تبدأ من اللحظة التي يدرك فيها الجاني أنه لا يملك الحق في الدخول أو البقاء داخل النظام. فإذا ولج الجاني النظام واستمر في البقاء دون مغادرة، تعتبر هذه جريمة دخول. أما إذا بدأ الجاني في التنقل داخل النظام بعد الدخول، فتُعد جريمة بقاء تبدأ من تلك اللحظة التي يدرك فيها أن وجوده داخل النظام غير قانوني.

3- الركن المعنوي:

الركن المعنوي يلعب دوراً محورياً في إثبات جريمة الدخول والبقاء غير المصرح بهما، ولتحقق هذا الركن يجب أن يتوفر في الجاني القصد العام الذي يشمل العلم والإرادة. العلم يتطلب أن يكون الجاني على دراية بأنه يقوم بالتجول داخل نظام آلي للمعطيات بدون الحق القانوني لذلك. أما الإرادة، فتعني أن يكون لدى الجاني نية صريحة في الاستمرار في

[1]-حمد حماد مرهج الهيئي، **جرائم الحاسوب(ماهيتها موضوعها أهم صورها والصعوبات التي تواجهها)**، دراسة تحليلية واقع الاعتداءات التي يتعرض لها الحاسوب وموقف التشريعات الجنائية منها، دار المناهج للنشر والتوزيع، الأردن 2006، ص 44.

استخدام النظام وعدم قطع الاتصال، على الرغم من علمه بأن وجوده داخل النظام غير مشروع.

تعتبر هذه الجريمة من الجرائم العمدية، حيث يجب على الجاني، لإثبات عدم وجود علاقة سببية بين سلوكه الإجرامي—سواء الدخول أو البقاء غير المشروع—والنتيجة الإجرامية، أن يبرهن على أن التغيير أو مسح المعطيات كان نتيجة قوة قاهرة أو حدث مفاجئ. بثبوت ذلك، يعتبر السلوك الإجرامي معدومًا وبالتالي ينتفي القصد الجنائي[1].

ثانيا- جريمة المساس بسلامة المعطيات:

1- الركن الشرعي: تنصه عليه المادة394 مكرر 01 من قانون العقوبات بموجب الأمر 04-15.

2- الركن المادي: تقع جريمة المساس بسلامة المعطيات عندما يتم إظهار أحد السلوكيات الثلاثة: إدخال، تعديل، أو إزالة المعطيات. سيتم فيما يلي تفصيل وشرح كل سلوك بمفرده.

- **الإدخال:** يتضمن الإدخال إضافة بيانات جديدة إلى دعامة موجودة سلفاً، بغض النظر عن حالتها، سواء كانت فارغة أو تحتوي بيانات مسبقة. على سبيل المثال، لو أن طالباً قام بتغيير درجاته المسجلة على النظام الإلكتروني للجامعة، من خلال الادعاء بأنه الطالب الذي حصل على المركز الأول في شهادة البكالوريا لعام 2008، مستبدلًا بياناته ببيانات الطالب الأول. يثبت الجرم كذلك من خلال إدخال برامج ضارة مثل فيروسات أو حصان طروادة، التي تقوم بدمج بيانات مبتكرة ضمن النظام[2].

---

[1]- محمد امين الرومي، **جرائم الكمبيوتر والانترنت**، دار المطبوعات الجامعية، مصر 2004، ص 106.

[2]- عبد العزيز بوذراع، **خصوصية الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات**، مذكرة الماجستير في القانون، كلية الحقوق جامعة الجزائر 1، 2011-2012 ، ص 66.

- **الإزالة:** يتمثل في إزالة أو حذف جزء من المعطيات المسجلة على دعامة تخزين ضمن نظام معلوماتي، أو تدمير تلك الدعامة بشكل يؤدي إلى فقدان المعطيات. يشمل ذلك أيضًا نقل أو إعادة تخزين جزء من المعطيات إلى منطقة مختلفة ضمن الذاكرة، وهو ما يؤدي إلى تغيير في ترتيب أو سلامة البيانات الأصلية[1].

- **التعديل:** يتمثل هذا السلوك في تغيير المعطيات داخل نظام معلوماتي بإستبدالها بأخرى، حيث ينفذ ذلك عبر استخدام برامج خارجية تؤثر في المعطيات إما بمحوها كليًا أو جزئيًا أو بتعديلها. تتضمن الأدوات المستخدمة في هذه العملية القنبلة المعلوماتية للمعطيات، برنامج الممحاة، وأنواع مختلفة من الفيروسات التي تتلاعب في سلامة ودقة البيانات[2].

3-الركن المعنوي: الركن المعنوي في هذه الجريمة العمدية يعتمد على القصد الجنائي العام، ويشمل العلم والإرادة؛ يتطلب أن تكون إرادة الجاني متجهة عمداً نحو الإدخال، المحو، أو التعديل، مع العلم بأن تصرفاته غير مشروعة وتشكل اعتداءً على حقوق صاحب المعطيات أو من يملك السيطرة عليها. على الرغم من ذلك، الضرر الناتج عن الفعل الإجرامي يعتبر نتيجة للجريمة لكنه ليس شرطاً ضرورياً لإثبات وقوع الجريمة نفسها.

ثالثا- جريمة تخريب أو تعطيل نظام التشغيل:

1- الركن الشرعي: تنصه عليه المادة394 مكرر في فقرتها الثالثة من قانون العقوبات بموجب الأمر 04-15.

يُلاحظ أن المشرع الجزائري قد أدرج جريمة التدخل في سلامة المعطيات ضمن نطاق جرائم الدخول والبقاء بغش، رغم كونها مستقلة بذاتها. لذا، يُرى ضرورة توفير نص خاص

[1]- سفيان سوبر، **جرائم المعلوماتية**، مذكرة الماجستير في العلوم الجنائية وعلم الإجرام، جامعة أبو بكر بلقايد، تلمسان،2010-2011 ، ص 94.

[2]- أمال قارة، المرجع السابق، ص 53

لتنظيمها بشكل مفصل، مشابهًا للمنهج الذي تبنته اتفاقية بودابست في مادتها الخامسة. تنص الاتفاقية على أن كل دولة طرف يجب أن تتخذ الإجراءات التشريعية والتدابير اللازمة لتجريم الأفعال التالية، إذا ما ارتُكبت عمداً ودون حق: الإعاقة الخطيرة لعمل نظام الكومبيوتر من خلال إدخال، إرسال، تعديل، حذف، تغيير، أو تدمير البيانات المعلوماتية[1].

2- الركن المادي: يتجلى الركن المادي لجريمة تخريب أو تعطيل نظام التشغيل في استخدام أساليب مختلفة تشمل تخريب الجهاز عبر استعمال الفيروسات أو القنابل المنطقية، تغيير الرقم السري، أو إتلاف برنامج الدخول. وتؤدي هذه الأفعال إلى انقطاع كلي أو جزئي في عمل النظام، مما يحول دون الاستفادة من النظام المعلوماتي بشكل مطلق. وهو ما سيتم شرحه فيما يلي:

- **الإعاقة أو العرقلة:** تشمل الأفعال التي تعيق النظام، بشكل كامل أو جزئي، من أداء وظائفه وتشمل أيضًا البرامج المرتبطة بهذا النظام. قد تكون هذه العوائق مادية، مثل تخريب أو تعطيل أجهزة الحاسوب أو شبكات الاتصال، أو معنوية، مثل إدخال الفيروسات إلى النظام أو تغيير كلمات المرور.

- **الإخلال:** يشير إلى جميع الأفعال التي تؤثر سلبًا على أداء النظام المعلوماتي، حيث تضعف هذه التصرفات النظام بتقليل سرعته أو بتعطيل قدرته على أداء الوظائف التي برمج لها.

3- الركن المعنوي: تُعد جريمة تعطيل أو إفساد نظام المعالجة من الجرائم العمدية التي يظهر فيها الركن المعنوي كقصد جنائي يتضمن علم الفاعل وإرادته. يتطلب الأمر أن تتجه الإرادة صراحةً نحو العرقلة أو التعطيل وكذلك الإفساد. كما ينبغي أن يكون الفاعل على

[1] المادة 05 من اتفاقية بودابست الخاصة بالإجرام المعلوماتي. السالفة الذكر.

وعي بأن فعله الإجرامي سيؤدي إلى تعطيل أو إفساد نظام المعالجة الآلي للمعطيات. ومن الضروري أيضًا أن يعي الجاني أن ما سيقوم به يتم بدون موافقة صاحب الحق في التحكم في ذلك النظام.

رابعا- جريمة إساءة استخدام الأجهزة:

1- الركن الشرعي: تنصه عليه المادة394 مكرر2 في فقرتها الثالثة من قانون العقوبات بموجب الأمر 04-15. يتضح أن اتفاقية بودابست قد عالجت هذه الجريمة تحت مسمى "إساءة استخدام الأجهزة" وفقًا للمادة السادسة.

2- الركن المادي: من خلال تحليلنا للمادة 394 مكرر 2، نستنتج أن تحقق الركن المادي يتضح في الأفعال المحددة بشكل حصري، والتي يمكن تقسيمها إلى صورتين:

-**التعامل في معطيات صالحة الارتكاب الجريمة:** وهي الأعمال المنصوص عليها في الفقرة الأولى للمادة 394 مكرر 2. (تصميم معطيات، البحث، التجميع، التوفير، النشر، الاتجار)

-**التعامل في معطيات متحصل عليها من الجريمة:** وهي الأعمال المنصوص عليها في الفقرة الثانية للمادة 394 مكرر 2. (الحيازة، الافشاء، الاستعمال)

3- الركن المعنوي: جريمة إساءة استخدام الأجهزة تُصنف ضمن الجرائم العمدية، حيث يتميز الركن المعنوي فيها بوجود عنصري العلم والإرادة.

تتوجه إرادة الجاني نحو تنفيذ الأفعال المحددة في المادة 394 مكرر 2، ضمن فقرتيها الأولى والثانية، بحيث تشمل الفقرة الأولى أفعال التصميم، البحث، التجميع، التوفير، النشر، والاتجار، بينما تتضمن الفقرة الثانية الحيازة، الإفشاء، والاستخدام.

يتطلب أيضًا أن يكون الجاني مدركًا أن فعله سيؤدي إلى ارتكاب جرائم تضر بأنظمة المعالجة الآلية للمعطيات، مع الشرط أن يكون مصحوبًا بنية الإضرار بالغير. وتتحقق الجريمة بمجرد امتلاك برامج أو استخدام أي وسيلة قد تؤدي إلى ارتكاب هذه الجريمة.

الفرع الثاني: العقوبات المقررة على مرتكبي الجريمة الالكترونية في قانون العقوبات الجزائري

تخضع الجريمة الإلكترونية كغيرها من الجرائم لمبدأ الشرعية بمعنى وجود نصوص قانونية تجرم الافعال وتقرر لها عقوبات سواء كان مرتكب الجريمة شخص طبيعي شخص معنوي .

أولا-العقوبات المقررة على الشخص الطبيعي

في الواقع، تتفاوت العقوبات بين الجرائم المختلفة، لكنها تتقاسم عدة قواعد وخصائص مشتركة. اللافت أن العقوبات في هذا السياق جاءت مخففة نسبياً مقارنةً بالتشديد الملحوظ في قوانين أخرى، مما يشكل مخالفة للاتفاقية العربية لمكافحة جرائم تقنية المعلومات التي تدعو إلى تغليظ العقوبات على هذه الأنواع من الجرائم.

نورد في الجدول أدناه العقوبات المقررة لشخص الطبيعي عن جرائم المساس بأنظمة المعالجة الآلية للمعطيات وفقا لقانون العقوبات الجزائري:

نوع الجريمة	العقوبة المقررة	المادة القانونية
جريمة الدخول أو البقاء بغش في منظومة المعالجة الالية للمعطيات	من 6 أشهر الى سنتين وبغرامة مالية من60.000 دج الى 200,000 دج	394 مكرر فقرة 1
جريمة تخريب نظام اشتغال المنظومة	من سنة الى3 سنوات وبغرامة مالية من100.000 دج الى 300,000 دج	394 مكرر فقرة 2
جريمة ادخال بطريق الغش معطيات او ازالها او عدل فيها في نظام المعالجة الالية للمعطيات	من سنة الى3 سنوات وبغرامة مالية من500.000 دج الى 2.000,000 دج	394 مكرر1
جريمة المساس بسلامة المعطيات	من سنة الى5 سنوات وبغرامة مالية من1.000.000 دج الى 5.000,000 دج	394 مكرر2
جمعية أشرار الاعلام الآلي	عقوبة جريمة تكوين جمعية أشرار المقررة وفقا لقانون العقوبات	394 مكرر5
جريمة الشروع	عقوبة جريمة تكوين جمعية أشرار المقررة وفقا لقانون العقوبات	394 مكرر7
مخالفة الالتزامات خاصة مقدمي خدمة الانترنت بالرغم من الاعذار	من سنة الى3 سنوات وبغرامة مالية من500.000 دج الى 2.000,000 دج	394 مكرر8

الجدول من اعداد الطالبين

- تتشارك جرائم التعدي على أنظمة المعالجة الآلية للمعطيات في مجموعة من القواعد المتعلقة بالجزاءات منها :

أ – مضاعفة العقوبة:

بناءً على المادة 394 مكرر 3 من قانون العقوبات، تتم مضاعفة العقوبات على الجرائم التي تستهدف أنظمة المعالجة الآلية للمعطيات، خاصة إذا كانت هذه الجرائم موجهة ضد الدفاع الوطني أو ضد الهيئات والمؤسسات العامة، مع الحفاظ على إمكانية تطبيق عقوبات أشد في حال الضرورة.

ب – المصادرة:

تحدد المادة 394 مكرر6 من قانون العقوبات إجراءات مصادرة البرامج والأدوات المستعملة في الجريمة، بالإضافة إلى إغلاق المواقع الإلكترونية التي تستضيف النشاط الإجرامي. كما يمكن إغلاق المكان الذي استُخدم لارتكاب الجريمة، إذا ثبت علم مرتكب الجريمة بذلك.

ثانيا: العقوبات المقررة على الشخص المعنوي

حسب المادة 394 مكرر 4 من قانون العقوبات الجزائري بأن الشخص المعنوي الذي يرتكب أيا من الجرائم المذكورة في هذا الباب يخضع لغرامة تساوي خمسة أضعاف الحد الأقصى للغرامة المفروضة على الأشخاص الطبيعيين.

تتضاعف العقوبات في هذا الصدد وتشدد نظراً لخطورتها ومساسها بأمن الدولة كالإرهاب الالكتروني والتجسس الالكتروني وغيرها، اما العقوبات الأشد نجدها في المواد من 77 الى 86 من قانون العقوبات الجزائري المتعلقة بالجرائم الماسة بأمن الدولة ومؤسساتها او الوحدة الوطنية والسلامة الترابية.

فيما يخص العقوبات المطبقة على الشخص المعنوي في مواد الجنايات والجنح يمكن الرجوع للمادة 18 مكرر من قانون العقوبات الجزائري اين تساوي الغرامة من مرة الى خمس مرات الحد الاقصى لغرامة الشخص الطبيعي مع امكانية الحل او الغلق او الاقصاء من الصفقات

العمومية وغيرها، والمادة 51 مكرر من ذات القانون اذ مسائلة الشخص المعنوي لا تمنع من مسائلة الشخص الطبيعي كفاعل أصلي او شريك في الجرم.

المطلب الثاني: القواعد الاجرائية لمواجهة الجريمة الالكترونية في التشريع الجزائري

نظرًا للتحديات التي تواجه التعامل مع الجرائم الالكترونية في إطار النصوص الإجرائية التقليدية، وما يرتبط بها من تأثيرات على مبدأ الشرعية الجزائية والتفسير المحدود للنص الجزائي ومنع القياس، خاصة أن محور الجريمة يتمثل في مجموعة من البيانات التي تعد في الواقع مجرد تذبذبات إلكترونية، يسهُل على الجاني تنفيذ عمليات إجرامية دون ترك أثر يذكر. إضافة إلى ذلك، فإن مدة ارتكاب هذه الأعمال الإجرامية قد لا تتجاوز بضع ثوانٍ، مما يزيد من صعوبة كشفها وإثباتها.

لذا، بدأ المشرع الجزائري منذ بداية الألفية الثانية في تطوير النصوص القانونية لمجابهة تحديات الجرائم الإلكترونية. هذه الجهود تهدف إلى تأمين دليل قاطع يُدين المجرمين الإلكترونيين، وقد تضمنت التعديلات القانونية نصوصًا عقابية تغطي جميع أنواع الجرائم التي تؤثر على أنظمة المعالجة الآلية للمعطيات.

من الناحية الإجرائية، تضمنت بعض المواد في قانون الإجراءات الجزائية تعديلات تخص الجرائم التي تستهدف أنظمة المعالجة الآلية للمعطيات. في هذا السياق، قررنا أن نتناول أولاً أساليب البحث والتحري في جرائم المساس بأنظمة المعالجة الآلية للمعطيات كمطلب أول، ثم نتطرق في المطلب الثاني إلى الأساليب المؤسساتية لمواجهتها، و التعاون الدولي كوسيلة للحد منها.

الفرع الأول: أساليب البحث والتحري في جرائم المساس بأنظمة المعالجة الآلية للمعطيات.

وضع المشرع الجزائري آليات قانونية محددة للتصدي للجرائم التي تؤثر على أنظمة المعالجة الآلية للمعطيات. تتجلى أولى هذه الإجراءات في الأساليب الإجرائية، التي تشكل المرحلة الأولى في عملية جمع الدليل الإلكتروني. أو كما تعرف بأساليب التحري أو جمع التحريات عمومًا بأنها الإجراءات المستخدمة للحصول على المعلومات من مصادرها، معبرةً عن الحدود الشكلية التي توجهها. هذه الحدود الشكلية ضرورية لضمان أن تحقق التحريات تأثيرها المطلوب في التفاعل مع الحدود الموضوعية وتجنب أي إبطال لنتائجها[1].

أيضًا، هناك نوعان من الطرق المستخدمة في إجراءات التحري؛ بعضها تقليدي والبعض الآخر خاص.

أولا: إجراءات التحري الكلاسيكية

بعض إجراءات التحقيق في الجرائم الإلكترونية تشكل مصادر رئيسية للأدلة، مثل المعاينة والتفتيش، بالإضافة إلى الضبط والخبرة. هذه الإجراءات لا تخضع لترتيب محدد وإنما يقرر المحقق بدء ما يجده مناسبًا بناءً على وقائع الجريمة المعروضة أمامه. المحقق، المخول قانونًا باستخدام جميع الإجراءات القانونية والأدوات المشروعة، يسعى لكشف غموض الجرائم، ضبط مرتكبيها، وتقديمهم للمحاكمة[2].

[1]– لوجاني نور الدين، **أساليب البحث والتحري الخاصة وإجراءاتها**، مداخلة في يوم دراسي حول علاقة النيابة العامة بالشرطة القضائية احترام حقوق الإنسان ومكافحة الجريمة، المديرية العامة للأمن الوطني، أمن ولاية ايليزي يوم 12 ديسمبر 2007، ص03.

[2]– خالد ممدوح إبراهيم، **فن التحقيق الجنائي في الجرائم الالكترونية**، ط1، دار الفكر الجامعي الإسكندرية، 2009، ص 87.

1- المعاينة:

عند بحث الطرق الإجرائية لمواجهة الجرائم التي تؤثر على أنظمة المعالجة الآلية للمعطيات، ينبغي أولًا توضيح مفهوم المعاينة، والتي تعني مشاهدة الموقع أو الشخص أو الشيء بصريًا لتقييم حالته والحكم عليه بهدف كشف الحقيقة، أو تتمثل في انتقال مأمور الضبط القضائي إلى مكان وقوع الجريمة للبدء في التحقيق وتحديد كافة العناصر الموجودة هناك من أشخاص وأشياء التي تساهم في توضيح تفاصيل الجريمة[1].

كذلك يلعب الزمن دورًا حاسمًا في معاينة مسرح الجريمة، إذ يمكن أن يؤثر تأخير الوقت منذ وقوع الجريمة على صلاحية الدليل الإلكتروني، بل قد يؤدي إلى فقدانه أو تغييره. لذا، تعد سرعة الانتقال إلى مكان الجريمة ضرورية لضمان عدم ضياع الدليل. هذا المبدأ مُعتمد في المادة 42 من قانون الإجراءات الجزائية الجزائري[2].

تظهر أهمية المعاينة أيضًا في توفير صورة شاملة عن مسرح الجريمة، مما يمكن الشرطة القضائية والقضاة من تكوين فكرة مبدئية حول مجريات الجريمة واستخلاص بعض التفاصيل من الأدلة التي تم جمعها[3].

قد حدد المشرع الجزائري عقوبات جنائية لكل من يقوم بتغيير أو تعديل المعلومات المخزنة في الحاسوب قبل أن تقوم سلطة التحقيق بإجراء المعاينة، وفقًا لما ورد في المادة 43 من قانون الإجراءات الجزائية. ومع ذلك، يُستثنى من هذا الحظر الحالات التي تتطلب فيها

---

[1]- محمد زكي أبو عامر، **الإجراءات الجنائية**، دار الجامعة الجديد ، الاسكندرية، مصر، 2008، ص 123.

[2]-عمرو حسين عباس، **أدلة الإثبات الجنائي والجرائم الالكترونية (المعلوماتية)**، بحث مقدم إلى مؤتمر الإقليمي 02 حول تحديات تطبيق الملكية الفكرية في الوطن العربي، خلال فترة 27-26-04 سنة 2008، جامعة الدول العربية، ص 16.

[3]- عبد الفتاح بيومي حجازي، **مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت**، ط1، دار الفكر الجامعي 180 مصر، 2006 ص 180.

التغييرات أو إزالة الأشياء لأسباب تتعلق بالسلامة والصحة العامة، أو عندما تكون ضرورية لمعالجة المجني عليهم.

2 –التفتيش:

يُعرف التفتيش بأنه عملية بحث بوليسية أو قضائية تهدف للعثور على عناصر دليلية في قضية ما، وبموجب قواعد قانونية خاصة، يمكن تنفيذه في المسكن الخاص لأي شخص أو في أي مكان آخر قد يحتوي على أشياء يُعتقد أن اكتشافها سيساهم في كشف الحقيقة[1].

يهدف التفتيش إلى تجميع جميع الأدلة في مكان وقوع الجريمة، ولذلك يُعرف قانونًا بأنه استقصاء لجمع كل ما هو مادي في موقع الجريمة بهدف البحث عن الأشياء المرتبطة بالحادثة، وذلك أثناء جمع الاستدلالات أو أثناء إجراء تحقيق بشأنها. لم يقدم المشرع الجزائري تعريفًا خاصًا للتفتيش، بل اعتبره إجراءً يندرج ضمن مراحل التحقيق[2].

تُظهر المادة 44 من قانون الإجراءات الجزائية أن المشرع الجزائري قد أعطى أهمية خاصة للتفتيش، خصوصًا عندما يكون المكان محل التفتيش خاصًا مثل منزل أو مسكن. ومع ذلك، فإن هذا الإجراء محكوم بضوابط محددة موضحة في المادة 64 من نفس القانون. لكن في حالة الجرائم التي تؤثر على أنظمة المعالجة الآلية للمعطيات، يجوز إجراء التفتيش في أي وقت، سواء نهارًا أو ليلاً، وهذا ما تؤكده المادة 47 من نفس القانون.

فالهدف من خضوع بيانات الحاسوب للتفتيش هو الحصول على دليل يكشف معالم الجريمة.

---

[1]– بكري يوسف بكري، **التفتيش عن المعلومات في رسائل التقنية الحديثة**، دار الفكر الجامعي، الإسكندرية ط1، 2011، ص 58.

[2]– محمد حزيط، **قاضي التحقيق في النظام القضائي الجزائري**، دار هومة، الجزائر، ط 2، 2009، ص 91.

تطرح مسألة التفتيش الذي يتجاوز الحدود الجغرافية الوطنية تحديات معينة، خاصة إذا كان حاسوب المتهم متصلاً بحاسوب يقع خارج الدولة. في هذا السياق، توفر اتفاقية بودابست الإطار القانوني لمثل هذه الحالات في مادتها 19، حيث تجيز إجراء التفتيش عبر الحدود[1].

أما المشرع الجزائري، فقد أدرج إمكانية إجراء التفتيش عن بُعد ضمن المادة 05 من قانون 09-04، شريطة إبلاغ السلطة القضائية المختصة مسبقًا. قام المشرع الجزائري بتنظيم التفتيش من خلال مجموعة من القواعد الموضوعية والشكلية، وذلك في إطار الالتزام بحماية الحريات الشخصية.

وفقًا للمادة 45 من قانون الإجراءات الجزائية الجزائري، نص المشرع على أن التفتيش في مسكن الشخص المشتبه في مشاركته بارتكاب جناية يجب أن يتم بحضوره. إذا كان حضوره غير ممكن في وقت إجراء التفتيش، يُطلب منه بواسطة ضابط الشرطة القضائية تعيين ممثل عنه. في حال رفضه تعيين ممثل أو كان فارًا، يستدعي ضابط الشرطة القضائية شاهدين من غير الموظفين الخاضعين لسلطته لحضور العملية.

ومع ذلك، استثنى المشرع الجزائري الجرائم التي تستهدف أنظمة المعالجة الآلية للمعطيات من هذه القاعدة، كما هو موضح في الفقرة الثالثة من المادة 47 من نفس القانون.

3- الضبط في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات:

يُعرف الضبط بأنه عملية استيلاء أو السيطرة على الأدلة المرتبطة بجريمة مؤكدة الوقوع، حيث يُسهم هذا الدليل بشكل خاص في الكشف عن حقيقة الجريمة وتحديد مرتكبيها.

[1] المادة 19 من اتفاقية بودابست الخاصة بالإجرام المعلوماتي، السالفة الذكر.

علاوة على ذلك، يُحفظ هذا الدليل في أحراز مختومة ليُقدم لاحقًا أمام الجهة القضائية المختصة كدليل إدانة.

من التعريف نستنتج أن الضبط في الجرائم الإلكترونية يتم على المعطيات. وقد أثار هذا الموضوع جدلًا فقهيًا حول طبيعة هذه المعطيات لكونها غير مادية، مما يطرح السؤال: كيف يُمكن تنفيذ الضبط على معطيات غير ملموسة؟.

يذهب الفريق الأول إلى القول بأنه لا يمكن ضبط بيانات الحاسوب نظرًا لعدم وجود شكل مادي لها، إلا عبر تحويلها إلى شكل ملموس. ويستندون في حجتهم إلى أن النصوص القانونية المتعلقة بالضبط تطبق عادةً على الأشياء المادية الملموسة، هذا من ناحية.

من ناحية أخرى، يرى الفريق الثاني أن المعطيات المعالجة آليًا، التي تتخذ شكل ذبذبات إلكترونية أو موجات كهرومغناطيسية، يمكن تسجيلها والاحتفاظ بها على وسائط مادية، ويمكن أيضًا إرسالها، نشرها، استقبالها، وإعادة إنتاجها. وعليه، فإن حضورها المرئي يعتبر دليلاً لا يمكن تجاهله.

لذا، توضح المادة 19 في فقرتها الثالثة من اتفاقية بودابست المعنية بجرائم المعلوماتية، وتسوي الخلاف الفقهي بنصها على منح السلطات المختصة الصلاحية لضبط أو تأمين بيانات الكمبيوتر، وفقًا لما هو مذكور في الفقرتين 1 و2 من نفس المادة.

4- الخبرة

تُعد الولايات المتحدة الأمريكية رائدة في هذا المجال، حيث طورت أجهزة متخصصة لإجراء الخبرات التقنية على شبكة الإنترنت.

إن التطور في الجرائم الحديثة، والذي برز من خلال هذه الجريمة، جعل من الخبرة إجراءً ذو وزن وأهمية كبيرة، حيث تقدم أدلة مادية أو معنوية لجهات التحقيق والسلطات القضائية وكل الجهات المعنية بالدعوى الجزائية. لذلك، أعار المشرع الجزائري اهتمامًا بالغًا لتأطير أعمال الخبرة في المواد من 143 إلى 156 من قانون الإجراءات الجزائية، معتبرًا إياها إجراءً هامًا للبحث عن الأدلة. ونصت المادة 143 على أنه: "يمكن لجهات التحقيق أو الحكم، عندما تعرض لها مسألة ذات طابع فني، أن تأمر بندب خبير إما بناءً على طلب النيابة العامة أو من تلقاء نفسها أو بناءً على طلب الخصوم"[1].

كما تكمن أهمية الخبرة في القدرة على التعامل مع مسائل مادية أو فنية يصعب على المحقق البحث فيها، ولا يمكن جمع الأدلة بطرق أخرى للإثبات في مجال الجريمة الالكترونية، وتتجلى أهمية الخبرة في مجال الضبط، حيث أنه عند مواجهة صعوبة في الحصول على الدليل خلال مرحلة التحقيق، بسبب عدم توفر التخصص المطلوب للتعامل مع الجوانب التكنولوجية المستخدمة في الجريمة، قد يتعرض الدليل للتلف أو الإزالة.

نظرًا لأهمية الخبرة في مجال التحقيق وجمع الأدلة في الجرائم المعلوماتية، أولى المشرع الجزائري اهتمامًا كبيرًا لهذا الجانب في النصوص القانونية. فقد أشير إلى ذلك في المادة الخامسة، الفقرة الأخيرة، من قانون 09-04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها. تنص المادة على أنه يمكن للسلطة المكلفة بتفتيش الأنظمة المعلوماتية الاستعانة بأي شخص لديه خبرة في عمل النظام المعلوماتي المعني أو في التدابير المتخذة لحماية البيانات التي يحتويها، بهدف مساعدتها وتزويدها بالمعلومات الضرورية لإنجاز مهمتها.

[1]- خالد ممدوح إبراهيم، المرجع السابق، ص 299.

ثانيا: إجراءات التحري المستحدثة

استحدث المشرع الجزائري قواعد إجرائية جديدة بموجب قانون 06-22 المعدل والمتمم لقانون الإجراءات الجزائية، والذي شمل إجراءات التسرب واعتراض المراسلات. بالإضافة إلى ذلك، أضاف قانون 09-04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، إجراءات جديدة تتضمن المراقبة الإلكترونية وحفظ المعطيات المتعلقة بحركة السير.

1- التسرب:

يُعتبر التسرب في الإطار الأمني إجراءً مخططًا له بعناية، يهدف إلى التغلغل في وسط تنظيم إجرامي من أجل الاطلاع على أدق تفاصيله وأسراره، بما يتوافق مع تطلعات الجهات المختصة ولخدمة المصلحة العامة[1]، من الناحية القانونية، فقد أشار إليه المشرع في المواد من 65 مكرر 11 الى 65 مكرر 18.

يقصد بالتسرب قيام ضباط أو أعوان الشرطة القضائية، تحت إشراف ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة من خلال إيهامهم بأنه شريك لهم أو مشارك في الجريمة. يُسمح لضباط أو أعوان الشرطة القضائية في هذا السياق باستخدام هوية مستعارة، وارتكاب الأفعال الضرورية المذكورة في المادة 65 مكرر 14 عند الحاجة. ولا يجوز تحت طائلة البطلان، أن تشكل هذه الأفعال تحريضا على ارتكاب جرائم، وضع المشرع الجزائري مجموعة من القواعد الشكلية والموضوعية لإجراء التسرب، وتتمثل في:

[1]- نعيم سعداني، **آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري**، مذكرة الماجستير في العلوم القانونية، بجامعة الحاج لخضر، باتنة 2012/2013 ص 175.

أ- القواعد الشكلية للتسرب:

كأول إجراء شكلي يقيد عملية التسرب هو الحصول على الإذن، وهذا ما نصت عليه المادة 65 مكرر 11 من قانون الإجراءات الجزائية: "يجوز لوكيل الجمهورية أو لقاضي التحقيق، بعد إخطار وكيل الجمهورية، أن يأذن تحت رقابته، حسب الحالة، بمباشرة عملية التسرب".

ب- القواعد الموضوعية للتسرب:

تتمثل القواعد الموضوعية لإجراء التسرب في قاعدتين:

- **أولها:** تتعلق القاعدة الأولى بتحديد نوع الجريمة، حيث يجب أن تندرج ضمن الجرائم المنصوص عليها في المادة 65 مكرر 5 على سبيل الحصر، مثل "جرائم المخدرات، أو الجريمة المنظمة العابرة للحدود الوطنية، أو الجرائم التي تستهدف أنظمة المعالجة الآلية للمعطيات".

- **ثانيها:** يتعلق الإذن بعملية التسرب، حيث يجب أن يكون مسببًا. وقد نصت على ذلك المادة 65 مكرر 15: "يجب أن يكون الإذن الصادر تطبيقًا للمادة 65 مكرر 11 أعلاه مكتوبًا ومسببًا".

حدد المشرع مدة سريان عملية التسرب بأربعة أشهر قابلة للتمديد، مع إمكانية إيقافها قبل انتهاء هذه المدة إذا دعت الضرورة لذلك. كما استثنى المشرع الحالة التي يواجه فيها المتسرب صعوبة في الانسحاب من الشبكة، حيث يمكنه البقاء لمدة قد تصل إلى ضعف المدة القانونية[1].

[1]- نورة بن بوعبد الله، **الجريمة الالكترونية (مقاربة مفاهيمية)**، المرجع السابق.

2-اعتراض المراسلات وتسجيل الأصوات والتقاط الصور:

يعني اعتراض المراسلات التعقب السري والمستمر للمشتبه به قبل وبعد ارتكابه الجريمة، ومن ثم القبض عليه أثناء قيامه بالفعل الإجرامي. كما يُعرف بأنه إجراء تحقيقي يتم بشكل خفي ويخترق خصوصية الأحاديث، ويُعد أداة مهمة في يد الضبطية القضائية، ويتم عبر وسائل سلكية ولاسلكية فقط[1].

حدد المشرع الجزائري في المادة 65 مكرر 5 من قانون الإجراءات الجزائية نوع المراسلات التي يمكن اعتراضها، وتشمل الاتصالات السلكية واللاسلكية، مستثنيًا الرسائل المكتوبة، مثل الخطابات الخطية التي تُرسل عبر البريد.

كما نجد أن المشرع الجزائري قد قيد هذا الإجراء بشروط قانونية حرصًا على حماية حقوق الأفراد، وتتجلى هذه الشروط في:

- يجب أن يكون هناك تصريح خطي ومبرر من قبل وكيل الجمهورية أو قاضي التحقيق، استنادًا إلى المادة 05 من قانون الإجراءات الجزائية.

- فرضت المادة 65 مكرر 09 من نفس القانون على ضابط الشرطة القضائية واجب تحرير محضر لكل إجراء يتعلق بعمليات اعتراض وتسجيل المراسلات، بالإضافة إلى عمليات تركيب الأجهزة التقنية والقبض وتثبيت وتسجيل الأصوات أو الصور. يجب أن يتضمن المحضر توثيق تاريخ ووقت بدء هذه العمليات وانتهائها.

- كذلك نصت المادة 65 مكرر 07 على أن مدة اعتراض المراسلات لا تتعدى أربعة أشهر، ويمكن تجديدها وفقاً لاحتياجات التحقيق.

[1]- ياسر الأمير فاروق، **مراقبة الأحاديث الخاصة في الإجراءات الجزائية**، دار المطبوعات الجامعية، جامعة القاهرة. 2009 ص150.

3 – المراقبة الإلكترونية:

تُعرف المراقبة الإلكترونية بأنها العمل الذي يقوم به المراقب بِاستخدام التقنية الإلكترونية لجمع المعطيات والمعلومات عن المشتبه فيه سواء كان شخصا أو مكانا أو شيئا حسب طبيعته مرتبط بالزمن لتحقيق غرض أمني او أي غرض آخر، وفقاً لطبيعة الحالة وارتباطها بالوقت، بهدف تحقيق غاية أمنية أو غيرها من الأغراض.[1]

يسمح بتطبيق المراقبة الإلكترونية في الحالات التي حددها المشرع الجزائري في المادة 04 من قانون 09-04، والتي تشمل:

– اتخاذ التدابير الوقائية ضد الأفعال المعرّفة كجرائم إرهابية، تخريبية، أو تلك التي تمس بأمن الدولة.

– في حالة وجود معلومات تشير إلى احتمال وقوع هجوم على منظومة معلوماتية بما يُعرض النظام العام، الدفاع الوطني، مؤسسات الدولة، أو الاقتصاد الوطني للخطر.

– لأغراض التحريات والتحقيقات القضائية، عندما يصعب التوصل إلى نتائج فعالة للأبحاث الجارية دون استخدام المراقبة الإلكترونية.

– ضمن سياق تلبية طلبات المساعدة القضائية الدولية المتبادلة.

فرض المشرع الجزائري قيودًا على إجراء المراقبة الإلكترونية، موضحة في قانون 09-04 الذي يختص بالقواعد الخاصة للوقاية من الجرائم المرتبطة بتكنولوجيا المعلومات والاتصال ومكافحتها، والتي تتمثل في:

[1]- نورة بن بوعبد الله، **أثر التحول الرقمي على إجراءات المتابعة الجزائية** ، مداخلة ألقيت في الملتقى الوطني حول الأثر التحول الرقمي على المنظومتين القانونية والقضائية، كلية الحقوق والعلوم السياسية، جامعة الجلفة، يوم 25 أفريل 2024.

- ضرورة الحصول على إذن كتابي من السلطة القضائية المختصة.

- إصدار الإذن من قبل النائب العام لدى مجلس قضاء الجزائر العاصمة.

- ينفذ ضباط الشرطة القضائية العائدون للهيئة المذكورة في المادة 13 من القانون رقم 09-04 عملية المراقبة، حيث تكون مدة الإذن ستة أشهر، وهي قابلة للتجديد.

4 - حفظ المعطيات المتعلقة بحركة السير:

حدد المشروع الجزائري في المادة 02، فقرة هـ من قانون 09-04 المعطيات المتعلقة بحركة السير بأنها تشمل أي بيانات تتعلق بالاتصال عبر منظومة معلوماتية تولدها النظام، كجزء من سلسلة الاتصالات، وتوضح مصدر الاتصال ووجهته، والمسار المتبع، وزمن وتاريخ وحجم ومدة الاتصال، بالإضافة إلى نوع الخدمة المستخدمة.

أدرج المشرع الجزائري في المادة 11 من نفس القانون تعريفاً لإجراء حفظ المعطيات المتعلقة بحركة السير، ملزمًا مقدمي الخدمات بالاحتفاظ بالتالي:

- البيانات التي تمكن من تحديد هوية مستخدمي الخدمة.

- البيانات المرتبطة بالأجهزة الطرفية المستخدمة في الاتصال.

- المواصفات التقنية، بالإضافة إلى تاريخ ووقت ومدة كل اتصال.

- البيانات المتعلقة بالخدمات التكميلية المطلوبة أو المستخدمة ومقدمي تلك الخدمات.

- البيانات التي تمكن من تحديد المستقبِل أو المستقبِلين للاتصال، وكذلك عناوين المواقع التي تم الاطلاع عليها.

الفرع الثاني: الاطار المؤسساتي والتعاون الدولي لتصدي للجرائم الإلكترونية في التشريع الجزائري

اتخذت مكافحة الجريمة الالكترونية شكلاً جديدًا يتمثل في إنشاء مؤسسات وطنية (الفرع الأول)، واللجوء الى التعاون الدولي باعتبار أغلبها جرائم عابرة للحدود(الفرع الثاني).

أولا: الاطار المؤسساتي لمواجهة الجرائم الإلكترونية في التشريع الجزائري

نتناول في هذا الفرع الهيئة الوطنية للوقاية من الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال ومكافحتها، والهيئة القضائية الجزائية المتخصصة ، بالإضافة إلى المعهد الوطني للأدلة الجنائية وعلم الإجرام.

1-<u>الهيئة الوطنية للوقاية من جرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته:</u>

حددت المادة 13 من قانون09-04 تأسيس الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال. تُعرف هذه الهيئة كسلطة إدارية مستقلة ذات شخصية معنوية واستقلال مالي. أما عن مهام هذه الهيئة، فهي تشمل مهمتين رئيسيتين[1]:

أ- <u>العمل على الوقاية من الجرائم التي تستهدف أنظمة المعالجة الآلية للمعطيات</u>:

تتمثل في رفع مستوى الوعي لدى مستخدمي تكنولوجيات الإعلام والاتصال بشأن المخاطر التي قد يتعرضون لها كضحايا أثناء تصفحهم أو استخدامهم لهذه التكنولوجيات.

[1] المادة 02 من المرسوم الرئاسي رقم 15 - 261 المتعلق بتحديد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 53، في 08/10/2015.

من بين أبرز هذه الجرائم التجسس على الاتصالات والرسائل الإلكترونية، التلاعب بحسابات العملاء، أو استخدام بطاقات انتمائهم بشكل غير قانوني.

ب – مكافحة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات:

عُرفت من خلال المادة 14 من قانون رقم 09-04 التي جاء فيها:

– تنظيم وتنسيق الأنشطة الخاصة بالوقاية من الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال ومكافحتها.

– تقديم الدعم للسلطات القضائية ومصالح الشرطة القضائية في التحقيقات المتعلقة بالجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال، وذلك من خلال جمع المعلومات وإجراء الخبرات القضائية.

– تبادل المعلومات مع الهيئات المماثلة في الخارج بهدف تجميع كافة البيانات الضرورية لتحديد هوية مرتكبي الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال ومعرفة أماكن تواجدهم.

2- الأقطاب الجزائية المتخصصة

ظهرت فكرة الأقطاب الجزائية المتخصصة كمبادرة حديثة في عام 2004، وذلك بتعديل قانون الإجراءات الجزائية من خلال القانون رقم 04-14 المؤرخ في 10 نوفمبر 2004، الذي أدخل إمكانية توسيع الاختصاص المحلي لوكيل الجمهورية وقاضي التحقيق. هذا التعديل مثل نقطة انطلاق لتطور الجوانب الإجرائية في عمل الأقطاب الجزائية المتخصصة.

نص المرسوم التنفيذي رقم 06-348 المؤرخ في 5 أكتوبر 2006 على توسيع اختصاص محاكم إضافية، ويرتبط هذا التوسع بـ:

- القطب الجزائي المتخصص بمحكمة سيدي أمحمد بالجزائر ويتولى هذا القطب قضايا إقليم الوسط.

- القطب الجزائي المتخصص بمحكمة قسنطينة ويتولى هذا القطب قضايا إقليم الشرق.

- القطب الجزائي المتخصص بمحكمة وهران ويتولى هذا القطب قضايا إقليم الغرب.

- القطب الجزائي المتخصص بمحكمة ورقلة ويتولى هذا القطب قضايا إقليم الجنوب[1]

أذن المشرع الجزائري بتوسيع نطاق الأقطاب الجزائية المتخصصة عند التعامل مع الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات. نظرًا للموارد المادية والبشرية المطلوبة لتأسيس هذه المحاكم، لجأ المشرع الجزائري إلى مفهوم الأقطاب المتخصصة[2].

إضافة إلى ذلك فان التعبير عن هذه الأقطاب الجزائية المتخصصة تم تكريسه على المستوى الميداني من طرف وزير العدل، والجدير بالذكر أن قضاة هذه المحاكم قد تلقوا تدريبًا خاصًا، بدأ عند توقيع وزارة العدل اتفاقية تمويل مشروع إصلاح العدالة مع الاتحاد الأوروبي. وقد ركزت هذه الاتفاقية على تأهيل إطارات العدالة. بناءً على ذلك، بادرت وزارة العدل بإرسال دفعات من القضاة إلى الخارج، بالإضافة إلى تنظيم العديد من الملتقيات في الجزائر.

[1]- حملاوي الدراجي ،**الأقطاب الجزائية المتخصصة**، مذكرة الماستر تخصص قانون جنائي، جامعة محمد بوضياف مسيلة، 2014-2015، ص26.

[2]- مريم احمد مسعود، **آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال في ضوء قانون رقم 09-04**، مذكرة الماجستير، جامعة قاصدي مرباح كلية الحقوق والعلوم السياسية سنة 2012 ، 2013 ص 49 .

3- المعهد الوطني للأدلة الجنائية وعلم الإجرام:

يعتبر المعهد الوطني للأدلة الجنائية وعلم الإجرام في بوشاوي، الجزائر العاصمة، مؤسسة عمومية ذات طابع إداري تحت الإشراف المباشر لوزير الدفاع الوطني. يتألف المعهد من إحدى عشرة دائرة متخصصة في مجالات متنوعة، تساهم كل منها في التدريب والتعليم وإجراء الخبرات والفحوص العلمية ضمن إطار التحريات الأولية والتحقيقات القضائية، بهدف جمع الأدلة التي تمكن من تحديد هوية مرتكبي الجنايات والجنح.

ثانيا: دور التعاون الدولي في مواجهة الجريمة الالكترونية.

تختلف أشكال التعاون الدولي في مجال مكافحة الجريمة الإلكترونية، وتشمل بشكل رئيسي التعاون الأمني الدولي، التعاون القضائي الدولي.

1: التعاون الأمني الدولي لمكافحة الجرائم الالكترونية:

يُعد التعاون الأمني واحدًا من الأساليب الرئيسية لمكافحة الجرائم الإلكترونية، إذ يمكّن الدول من تتبع المجرمين عبر الحدود الوطنية. تتيح أجهزة التعاون الأمني للدول التعاون المشترك للحد من هذه الجرائم وتتبع الجناة.

أ- **تعريف التعاون الأمني:** التعاون الأمني الدولي، بمفهومه الشامل، يغطي مجالات متعددة بما في ذلك الشرطي، القانوني، والقضائي. يعكس هذا التنوع حاجة تحقيق الأمن إلى تطبيق إجراءات من هذه المجالات المتكاملة. التعاون الأمني لا يقتصر فقط على ملاحقة الأشخاص المطلوبين للعدالة، بل يتسع نطاقه ليشمل مكافحة الجريمة من خلال الأساليب

الوقائية والقمعية، مع التأكيد على حماية حقوق المتهمين والضحايا، واحترام حقوق الدول وسيادتها[1].

التعاون الدولي الأمني يمثل واحدًا من أبرز أشكال التعاون الدولي في مجال مكافحة الجريمة بشكل عام، والجرائم الإلكترونية بشكل خاص. في هذا الإطار، تلعب المنظمة الدولية للشرطة الجنائية (الإنتربول) دورًا محوريًا في تعزيز أسس هذا التعاون وتطويره.

ب- أهميته:

يشكل التعاون الأمني الدولي أداة رئيسية لمنع وتقليل هذه الجرائم. التحقيقات في الجرائم بشكل عام، والجرائم الإلكترونية بشكل خاص، تبرز أهمية هذا التعاون، حيث من الصعب على دولة واحدة بمفردها القضاء على الجرائم العابرة للحدود. أجهزة الأمن الوطنية تواجه تحديات في تعقب وملاحقة المجرمين خارج حدودها، مما يؤكد الحاجة إلى تعاون دولي فعال[2].

ملاحقة مرتكبي هذه الجرائم وتقديمهم للعدالة يتطلب إجراء تحريات تتجاوز حدود الدولة التي وقعت فيها الجريمة، أو على الأقل جزء منها. من بين هذه الإجراءات، تفتيش مواقع الإنترنت الأجنبية، ضبط الأقراص الصلبة، وتفتيش أنظمة الحاسوب.

ج- التعاون الأمني وجهود المنظمة الدولية للشرطة الجنائية:

يعتبر الإنتربول أكبر منظمة شرطية دولية تأسست عام 1923 في فيينا، النمسا، ويقع مقرها الرئيسي حاليًا في مدينة ليون، فرنسا. وفقاً لدستور الإنتربول، تتألف المنظمة من

---

[1]- عادل عبد العال ابراهيم، **خراشي اشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها**، كلية الشريعة والقانون، القاهرة ، ص 1. الاطلاع بتاريخ 2024//04/26م، على الساعة 22.25 .
https://jfslt.journals.ekb.eg/article_14124_9940c95e1f087a055130abff802ddbd8.pdf،

[2]- جميل عبد الباقي الصغير، **الجوانب الاجرائية المتعلقة بالأنترنت**، دار النهضة العربية، القاهرة ، 2001، ص 72.

عدة هياكل أساسية تشمل: الجمعية العامة، اللجنة التنفيذية، الأمانة العامة، المكاتب المركزية الوطنية، المستشارين، ولجنة ضبط ملفات الإنتربول.

تعتمد طريقة العمل داخل المنظمة الدولية للشرطة الجنائية (الإنتربول) على تبادل المعلومات بين أعضاء الشرطة الدولية حول المجرمين الدوليين، ويتعاون الأعضاء في مكافحة الجرائم الدولية مثل التهريب، والتجارة غير المشروعة في الأسلحة، والجرائم الإلكترونية. في السنوات الأخيرة، ركز الإنتربول بشكل أساسي على الجريمة المنظمة والأنشطة المتعلقة بها مثل غسل الأموال، كما يحتفظ أعضاء المنظمة بسجلات تفصيلية للجرائم الدولية[1].

شرطة الإنتربول تُعد منظمة عالمية متخصصة في مكافحة الجرائم الدولية العابرة للحدود، بما في ذلك الجرائم الإلكترونية. هذا ما أكدته نتائج الدورة رقم 77 للجمعية العامة لمنظمة الإنتربول، حيث دعا الأمين العام، سيد بونالد نوبل، جميع الحكومات والدول إلى دعم وتطوير أنظمة تبادل المعلومات بشأن المشتبه بهم ومكافحة كافة أشكال الإرهاب، بما في ذلك الإرهاب المعلوماتي. وقد نجحت المنظمة في الأعوام الأخيرة في تعزيز مكانتها كواحدة من أكثر الأسماء التي يخشاها المجرمون عالميًا[2].

2- التعاون القضائي الدولي

تعد المساعدة القضائية المتبادلة في المسائل الجنائية، المعروفة أيضًا بالتعاون القضائي الدولي، من أهم وأكثر الأساليب فعالية في التعاون الدولي لمكافحة الجريمة، هذا النوع من التعاون يلعب دورًا حيويًا في تعقب مرتكبي الجرائم، ملاحقتهم، القبض عليهم، ومحاكمتهم، وأخيرًا إنزال العقاب بهم، وتُعرف المساعدة القضائية الدولية بأنها مجموعة من

[1]- عادل عبد العال ابراهيم خراشي، المرجع السابق، ص ص 195 و 196.

[2]- جميل عبد الباقي صغير، **الجوانب الاجرائية للجرائم المتعلقة بالأنترنت**، دار النهضة العربية، مصر، 2002، ص 127.

الإجراءات القضائية التي تنفذها دولة بغرض تسهيل عملية المحاكمة في دولة أخرى تتعلق بإحدى الجرائم[1].

وقد أورد المشرع الجزائري في القانون رقم 09-04، وتحديداً في المادة 16 منه، مبدأ المساعدة القضائية الدولية المتبادلة. يُعتبر أنه خلال التحريات والتحقيقات القضائية لمعاينة الجرائم الإلكترونية، يمكن للسلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الإلكترونية المتعلقة بالجريمة، ترتبط الجزائر بعدة معاهدات واتفاقيات ثنائية في مجال التعاون القضائي، والتي تشمل أحكاماً خاصة بتسليم المجرمين، يتخذ التعاون الدولي القضائي في مكافحة الجريمة عدة أشكال، منها **تبادل المعلومات:** يعرف تبادل المعلومات بأنه تقديم المعلومات والوثائق التي تطلبها سلطة قضائية أجنبية بخصوص جريمة معينة، شاملة الاتهامات الموجهة لرعاياها في الخارج والإجراءات المتخذة ضدهم. بالإضافة إلى ذلك، يشمل تبادل المعلومات أيضاً السوابق القضائية للجناة، مما يمكن الجهات القضائية من معرفة الماضي الجنائي للأفراد بدقة. هذا المبدأ متضمن في العديد من الاتفاقيات الوطنية والدولية، التي تعد من أهم الأدوات في هذا المجال[2].

-على المستوى الشرعي الوطني، تنص المادة 17 من قانون 04/09 على أن الدولة الجزائرية تلبي طلبات المساعدة القضائية الدولية التي تهدف إلى تبادل المعلومات، وذلك ضمن إطار الاتفاقيات الدولية ذات الصلة ومبدأ المعاملة بالمثل.

[1]- جميل عبد الباقي صغير، المرجع السابق، ص 10.

[2]- محمد الفاضل، **التعاون الدولي في مكافحة الإجرام**، دار الكتب الجامعية، الاسكندرية، 1967 ص 352.

خلاصة الفصل الأول

ختامًا لهذا الفصل، توصلنا إلى أن الجرائم التي تمس المنظومة المعلوماتية تُعتبر حديثة بالنسبة للتشريع الجزائري ، ولاحظنا وجود عدة تسميات لها أطلقت عليها ، والمشرع الجزائري بموجب قانون رقم 04-15، أطلق عليها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات. هذه الجرائم تتخذ أشكالًا متعددة وتتميز بأنها عابرة للحدود، وقام بتدريج العقوبات من التبسيط إلى التشديد.

كما لاحظنا أن هناك تشابهًا في إجراءات التحري وجمع الأدلة بين الجرائم التقليدية والجرائم المعلوماتية، حيث تشمل هذه الإجراءات المعاينة والتفتيش والضبط، بالإضافة إلى الخبرة. ومع اعتماد المشرع لقانون 09-04، تم تحديد مجموعة من الإجراءات الجديدة المتعلقة بجريمة المعلوماتية، مثل مراقبة الاتصالات الإلكترونية وحفظ المعطيات، سعى المشرع الجزائري إلى تعزيز الآليات القانونية لمكافحة الجرائم بواسطة الأساليب المؤسساتية مثل هيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها. إلا أن دورها لم يتجسد على الأرض بشكل فعّال. ففي الفترة الأخيرة، لاحظنا تزايد هذا النوع من الجرائم بينما بقي دور هذه الهيئة غير ملموس وغير مفعّل، بالإضافة إلى ذلك، فإن فكرة الأقطاب الجزائية المتخصصة، التي أنشأت بموجب قانون 04-14، هي فكرة جيدة وخطوة فعالة في مكافحة الجريمة. يجب أيضًا التقدير للدور الفعّال الذي يقوم به المعهد الوطني للأدلة الجنائية وعلم الجريمة، حيث يُسهّل عملية البحث ويُسهم في كشف معالم الجريمة والمجرمين الإلكترونيين.

ونتيجة للتطورات التكنولوجية وبروز أشكال جديدة من الجرائم الإلكترونية التي تزايد حجمها على المستويات الوطنية والإقليمية والعالمية، فقد أصبح التعاون الدولي ضرورة ملحة لمكافحتها.

الفصل الثاني

دور التكنولوجيات الحديثة في تعزيز قواعد القانون الجزائي

تمهيد:

تمثلت جزئية من جهود عصرنة القضاء في تبني التكنولوجيا المتقدمة، خاصة تكنولوجيات المعلومات والاتصالات، لتحديث مرفق العدالة وضمان الشفافية والإدارة الفعّالة. هذا السعي يهدف إلى توفير عدالة سهلة الوصول للمواطنين وتقديم خدمات قضائية عامة بطريقة إلكترونية ومعاصرة تلبي احتياجاتهم، تم تنفيذ العديد من المشاريع بهدف تحقيق عدالة معاصرة تلبي المعايير الدولية، خاصةً في مجال تسهيل وصول جميع فئات المجتمع إلى القضاء، تبسيط وتحسين الإجراءات القضائية، وتطوير أساليب الإدارة والتسيير القضائي، وكذلك تعزيز وتطوير الخدمات القضائية المقدمة عن بعد للمواطنين والمتقاضين ومساعدي العدالة. (الخدمات الالكترونية متاح على الموقع الالكتروني الرسمي لوزارة العدل)
من بين هاته المشاريع نذكر القانون رقم 15-03 الصادر سنة 2015 المتعلق بعصرنة العدالة، والقانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين.

تتجه هذه الإجراءات نحو تعزيز مصداقية القضاء وبناء ثقة المواطنين به، وكذلك عصرنة العدالة وتدعيم الهياكل القضائية بأدوات حديثة، تعتبر رقمنة مرفق العدالة من الركائز الأساسية لإصلاح وعصرنة النظام القضائي.

وللإحاطة بموضوعنا نتناول في المبحث الأول الآليات المستحدثة لسير الدعوى العمومية، بينما نتطرق في المبحث الثاني الى نظام المحاكمة الالكترونية وفقا لأحكام قانون عصرنة العدالة 15-03.

المبحث الأول: الآليات المستحدثة لسير الدعوى القضائية

في إطار الجهود المتواصلة التي تبذلها الدولة الجزائرية لرقمنة قطاع الإدارة، من خلال إنشاء قاعدة بيانات خاصة بالحالة المدنية والتحول إلى الوثائق البيومترية، فقد أولى المشرع الجزائري اهتماماً خاصاً بقطاع العدالة، مسترشداً بالتشريعات المقارنة في سعيه لتطوير وعصرنة هذا القطاع، وقد تم ذلك من خلال ملائمة القوانين مع معطيات العولمة

وإدخال تكنولوجيا المعلومات في إدارة العدالة، ونتيجة لذلك فقد أثرت التكنولوجيا الحديثة في تعزيز قواعد القانون الجزائي من خلال استحداث آليات لسير الدعوى، من خلال عصرنة العمل القضائي والخدمات القضائية (المطلب الأول) و الشكوى الالكترونية(المطلب الثاني).

المطلب الأول: عصرنة العمل القضائي والخدمات القضائية

في إطار جهود عصرنة العدالة، تم تطوير مجموعة من الأنظمة المعلوماتية والآليات الرقمية الرامية إلى إنشاء منظومة إلكترونية شاملة تسهل تنفيذ المحاكمة الإلكترونية، هذه الأنظمة تشمل نظام التسيير والمتابعة الآلية للملف القضائي، والنظام الآلي لصحيفة السوابق القضائية ، ونظام التسيير والمتابعة الآلية لشريحة المحبوسين ، كل هذه الأنظمة تهدف إلى تسهيل وتبسيط الإجراءات القضائية وتحسين إدارة المعلومات القضائية، مما يعزز من كفاءة العملية القضائية ويضمن سرعة الفصل في القضايا.

الفرع الأول: انشاء نظام التسيير والمتابعة الآلية للملف القضائي:

نظام التسيير والمتابعة الآلية للملف القضائي هو برنامج معلوماتي تم تطويره في إطار الجهود المبذولة لإصلاح وعصرنة العدالة. يعمل هذا النظام على رقمنة الملفات القضائية، سواء كانت مدنية، جزائية، أو إدارية، ويتابعها آليًا منذ بداية دخولها إلى الهيئات القضائية بمختلف درجاتها، بما في ذلك المحاكم، المجالس القضائية، المحكمة العليا، والمحاكم الإدارية، حتى صدور الحكم أو القرار. كما يقدم هذا النظام مجموعة متنوعة من الخدمات القضائية، مثل الشباك الإلكتروني، متابعة الملف القضائي، وخدمة التبليغ بالرسائل القصيرة، مما يساهم في تعزيز كفاءة وفعالية الإجراءات القضائية.

أولا: الشباك الالكتروني:

تم تطوير نظام التسيير والمتابعة الآلية للملف القضائي في جميع الجهات القضائية، وهو يتيح للمواطنين والمحامين الاطلاع على مسار الملف القضائي بشكل فوري وآلي، دون الحاجة إلى التنقل إلى مكاتب أمناء الضبط. هذا النظام يُمكِّن أيضًا من تسجيل العرائض وطلب وسحب الوثائق الضرورية كالأحكام والقرارات في وقت قياسي. بالإضافة إلى ذلك، يسمح النظام بتسجيل الطعون بالنقض عن بُعد للقضايا المطروحة أمام المحكمة العليا ويعمل على دعم ذوي الاحتياجات الخاصة من خلال تخصيص فضاء خاص لهم، مما يعزز الوصولية ويسهم في تحقيق العدالة الشاملة.

ثانيا: مآل الملف القضائي:

في عام 2010، تم استحداث نافذة إلكترونية تمكّن المتقاضي أو وكيله المحامي من متابعة مآل قضيته، سواء تم حفظ الملف، أو كانت القضية قيد المداولة، مؤجلة، أو تم الفصل فيها، بالإضافة إلى إمكانية متابعة استماع الأطراف. يتم الوصول إلى هذه المعلومات من خلال الحصول على اسم مستخدم وكلمة مرور تصدر من الجهة القضائية المسؤولة عن القضية. الهدف من هذا التطور هو تقريب العدالة من المواطن والتقليل من عبء التنقل إلى الجهات القضائية، مما يسهل على الأفراد التفاعل مع النظام القضائي بكفاءة وفعالية أكبر.

ثالثا: خدمة التبليغ عبر رسالة قصيرة:

هذه التقنية الجديدة توفر للمتقاضين إمكانية تتبع مآل قضاياهم من خلال استقبال رسائل نصية قصيرة عبر الهاتف المحمول. كما تمكّن المحاكم من إرسال الاستدعاءات وتبليغ المتقاضين إلكترونياً، مما يغني عن الحاجة لإرسالها عبر البريد العادي. هذه الخدمة

تساهم في تبسيط الإجراءات الإدارية، توفير النفقات المتعلقة بالتبليغ، وتسهيل وصول المعلومات القضائية إلى المتقاضين في وقت قياسي، مما يعزز من كفاءة وفعالية النظام القضائي.

الفرع الثاني: النظام الآلي لصحيفة السوابق العدلية

يعتبر النظام الآلي لصحيفة السوابق القضائية عنصرًا أساسيًا في عملية رقمنة قطاع العدالة، حيث يوفر خدمة عمومية هامة تتمثل في إصدار صحيفة السوابق القضائية رقم 03 للمواطنين والصحيفة رقم 02 للإدارات العمومية. هذا النظام يتم تنظيمه وإدارته من قبل المركز الوطني لصحيفة السوابق القضائية، ويعزز الشفافية والكفاءة في توفير الوثائق القضائية الرسمية للأفراد والهيئات الحكومية، مما يسهل إجراءات متعددة تتطلب التحقق من الخلفية القضائية للأشخاص.[1]

تم ربط النظام الآلي لصحيفة السوابق القضائية آليًا بجميع الهيئات القضائية عبر البلاد، مما يتيح للمواطن الحصول على صحيفة السوابق القضائية من أي محكمة داخل الدولة، بغض النظر عن مكان ميلاده. هذا التكامل يسهل إجراءات الحصول على الوثائق القضائية اللازمة، ويعزز من الكفاءة والفعالية في توزيع الخدمات القضائية، مما يساهم في تسريع الإجراءات وتحسين الوصول للمواطنين إلى حقوقهم القانونية بشكل عادل وموحد على مستوى الدولة.

تم توسيع نطاق النظام الآلي لصحيفة السوابق القضائية ليشمل المواطنين المولودين في الخارج، مما يتيح لهم إمكانية سحب هذه الوثيقة من أي جهة قضائية داخل الدولة. هذا

[1]- بواشري أمينة و سالم بركاهم، **الاصلاح الاداري في الجزائر عرض تجربة مرفق العدالة 2017/1999** ، المجلة العلمية، المجلد 06، العدد 11، جانفي 2018، ص. 220

التطوير يسهل الوصول الشامل للخدمات القضائية ويدعم الاندماج القانوني للمواطنين في الخارج.

بالإضافة إلى ذلك، يقدم النظام ميزة المعالجة الآلية لملفات رد الاعتبار بقوة القانون. هذا يعني أن الأشخاص الذين استفادوا من رد الاعتبار تلقائيًا، وفقًا للقانون، يمكنهم استخراج صحيفة سوابق قضائية خالية من أي سجلات سابقة في التاريخ المحدد بالقانون دون الحاجة إلى تقديم طلب شخصي. هذه الوظيفة تعزز من كفاءة النظام وتقدم راحة كبيرة للمستفيدين من رد الاعتبار[1].

الفرع الثالث: انشاء نظام التسيير والمتابعة الآلية لشريحة المحبوسين

يعد هذا النظام حيويًا لأنه يدير ويتابع ملف كل محبوس منذ لحظة دخوله المؤسسة العقابية حتى خروجه منها. يوفر النظام رصدًا شاملاً لمسار كل محبوس، بدءًا من أسباب وظروف الحبس، مرورًا بسلوك الفرد وتطوره أثناء فترة الحبس، وانتهاءً بإجراءات إطلاق سراحه.

هذه المتابعة المفصلة تسهل على الإدارات المعنية تقييم الحالات بدقة واتخاذ القرارات المناسبة بناءً على سلوك وتطور كل فرد، مما يساعد في تعزيز فعالية البرامج الإصلاحية وضمان التعامل العادل والمنصف مع المحبوسين. كما يتكفل هذا النظام ب:

- إعداد برامج فردية لإعادة التربية وإعادة الإدماج الاجتماعي.
- إعطاء إحصائيات دقيقة وموثوقة حول أهم التحولات لمختلف شرائح المساجين.

[1]- بواشري أمينة و سالم بركاهم، المرجع السابق، ص. 220

- الحصول على بطاقة خاصة لكل مسجون يمكن الاعتماد عليها في حالة استفادة هذا الأخير من الإفراج المشروط أو اتخاذ أي إجراء آخر من طرف قاضي تنفيذ العقوبات والاطلاع الفوري على وضعية المحبوس.

- إعداد وتسيير ومراقبة برامج المكافأة على حسن السيرة التي جاء بها الإصلاح وهي ترمي إلى تحفيز الاستفادة من إجراءات الإفراج المشروط والحرية النصفية وأعمال الورشات.

المطلب الثاني: الشكوى الالكترونية

منذ إصدار القانون رقم 15-03 الذي يعنى بعصرنة العدالة، قام قطاع العدالة بتنفيذ العديد من المشاريع الهادفة إلى تطوير استخدام تكنولوجيا الإعلام والاتصال والانتقال نحو البيئة الرقمية. هذه المبادرات تأتي في إطار سعي القطاع لتحقيق عدالة تلبي المعايير الدولية، خصوصًا في مجال تسهيل الوصول إلى القضاء لجميع فئات المجتمع، وتبسيط وتحسين الإجراءات القضائية .بالإضافة إلى ذلك، تمت ترقية أساليب التسيير القضائي والإداري، وتطوير الخدمات القضائية المقدمة عن بُعد، مما يُعزز الفائدة للمواطن المتقاضي ومساعدي العدالة.

الفرع الأول: مفهوم الشكوى الالكترونية

في إطار جهود تحسين خدمات منظومة العدالة وعصرنتها، ومواكبة للتحديات التي فرضها انتشار وباء كورونا، أطلقت وزارة العدل بتاريخ 28 جويلية 2020 منصة إلكترونية جديدة. تهدف هذه المنصة إلى تمكين الأفراد من تقديم الشكاوى أو العرائض عن بُعد، بما يُغنيهم عن الحاجة للتوجه مباشرة إلى المؤسسات القضائية، وذلك في إطار تسهيل الوصول إلى الخدمات القضائية وضمان استمراريتها في ظل الظروف الصحية الراهنة.

تُعد هذه الخدمة إحدى آخر المنجزات التي تم تحقيقها حتى الآن في إطار مشروع عصرنة منظومة العدالة، وقد تم إتاحتها للمواطنين مما يُميزها ببساطة الإجراءات وسهولة الاستخدام. لمن يرغب في تقديم شكوى، يتوجب عليه الدخول إلى الأرضية الإلكترونية المُعدة خصيصًا لهذا الغرض، والتي تُعرف بالنيابة الإلكترونية المتاحة عبر البوابة الإلكترونية لوزارة العدل، يجب على المستخدم ملء استمارة تسجيل الشكوى أو العريضة عن بُعد بتزويدها بمعلوماته الشخصية الكاملة مثل الهوية، عنوان الإقامة، رقم الهاتف المحمول، بالإضافة إلى تحديد نوع الشكوى أو العريضة وإدخال محتواها.

الفرع الثاني: سير الشكوى الالكترونية

بعد ايداع شكوى او عريضة على مستوى مصالح وكيل الجمهورية الكترونيا المخصصة لهذا الغرض والمتاحة عبر وزارة العدل، والتي تحول هذه الشكوى بصفة ألية إلى النيابة العامة لإتخاد الإجراء المناسب ، بعد تصرف ممثل النيابة في الشكوى، يتم إعلام المعني بمآلها والإجراءات المتخذة أو المطلوب اتخاذها، وذلك عبر أرضية النيابة الإلكترونية، وكذا عبر رسالة نصية قصيرة (SMS) و/أو بريده الإلكتروني[1].

دون الحاجة للحضور الشخصي للمعني أمام المحكمة، مما يساهم في التخلص من الكم الهائل من الشكاوى الورقية التي كانت تتلقاها النيابة العامة، كما بتيح هذا النظام إمكانية استلام الشكوى من أي مكان عبر الانترنت، على خلاف ماكان عليه سابقا، وفي جميع أيام الأسبوع ليلا ونهارا، دون الولوج الى اروقة المحاكم، وبالتالي تحقيق العدالة بين المواطنين بأقصر الطرق، رفع عبء التنقل عن المواطنين، خاصة في ظل الأزمة الصحية التي

[1]- نورة بن بوعبد الله، **أثر التحول الرقمي على إجراءات المتابعة الجزائية**، المرجع السابق.

عاشتها البلاد بعد تفشي وباء كوفيد،19 والمشرع الجزائري ادخل هذا النظام الجديد حيز التنفيذ بتاريخ 28 جويلية 2020- كما سبق وذكرنا-.[1]

وفي هذا الإطار، قامت مديرية الشؤون القضائية والقانونية بوزارة العدل بمراسلة الاتحاد الوطني لمنظمات المحامين بتاريخ 05 نوفمبر 2020، بهدف تحديث قاعدة البيانات الخاصة بالمحامين في تطبيق تسيير مهن الأعوان القضائيين، الهدف من ذلك هو ربط هذه البيانات بالنظام الآلي للتقاضي الإلكتروني. تجسيد هذا الإجراء في الواقع يُمثل تطوراً نوعياً في مسار التقاضي الإلكتروني، ما يُعد تحولاً جذرياً مقارنة بالإجراءات السابقة التي كانت تقتصر على عمليات بسيطة مثل نسخ القرارات وتسجيلها على الأجهزة الإلكترونية.

المبحث الثاني: نظام المحاكمة الالكترونية وفقا لأحكام قانون عصرنة العدالة 15-03

يشهد العالم اليوم ثورة معلوماتية هائلة تُحدث تأثيرًا عميقًا على مختلف جوانب الحياة الاجتماعية والاقتصادية والعلمية، هذه الثورة تُجسدت في تحولات واضحة كرقمنة وثائق الحالة المدنية، التعليم الإلكتروني، والتجارة الإلكترونية، وقد امتد تأثيرها إلى السلطة القضائية. على الرغم من الفوائد التي يوفرها نظام التقاضي الإلكتروني مثل سرعة الفصل في الدعاوى المدنية ومعالجة مشكلات التأخير في الفصل بالخصومات المدنية من خلال تسهيل إجراءات التقاضي ومواكبة التطورات المعاصرة، إلا أن تطبيق المحاكم الإلكترونية يظل يطرح إشكاليات معينة، خصوصًا فيما يتعلق بالتأثير على حقوق الأفراد إذا لم يتم تنفيذه بالشكل الأمثل[2].

[1]- نورة بن بوعبد الله، **أثر التحول الرقمي على إجراءات المتابعة الجزائية**، المرجع السابق.

[2]– أشرف جودة محمد محمود، **المحاكم الإلكترونية في ضوء الواقع الإجرائي المعاصر**، مجلة الشريعة والقانون، العدد 35 ،الجزء 3، 2020 ، ص. 17.

ولتحقيق هذه الأهداف، أصدر المشرع القانون رقم15-03 المتعلق بعصرنة العدالة، كما تم تعديل قانون الإجراءات الجزائية بإدراج المادة 441 مكرر بموجب الأمر رقم 20-04 لتتوافق مع نظام المحاكمة عن بعد. في هذا البحث، سنستعرض مفهوم المحاكمة الالكترونية تماشيا مع مقتضيات قانون عصرنة العدالة 15-03 بشكل مفصل (المطلب الأول)، ، ثم دراسة تقنية المحادثة المرئية عن بُعد في التشريع الجزائري (المطلب الثاني).

المطلب الأول: مفهوم المحاكمة الالكترونية

يُعرف التقاضي من خلال المحكمة الإلكترونية بأنه هيكل تقني معلوماتي يسمح للمتقاضين بتسجيل دعاواهم وتقديم أدلتهم، وكذلك حضور جلسات المحاكمة عبر وسائل الاتصال الإلكتروني، مما يُمهد الطريق لإصدار الأحكام وتنفيذها. هذا النظام يُمكن القضاة من الاتصال بالمتخاصمين وإدارة إجراءات التقاضي دون الحاجة لحضورهم الشخصي. يتيح النظام للقضاة والأطراف المعنية إمكانية الوصول السريع والشفاف إلى المعلومات، متابعة الدعاوى، تسجيل الطلبات، إعلان أوراق المرافعات، والتواصل مع موظفي وقضاة المحاكم إلكترونيًا دون الحاجة إلى الحضور الشخصي.

نظرًا لحداثة مصطلح "المحكمة الرقمية أو الالكترونية"، من الضروري أولًا تحديد تعريف المحاكمة الالكترونية **(الفرع الأول)**، ثم استعراض خصائص ومميزات المحاكم الإلكترونية **(فرع ثاني)**.

الفرع الأول: تعريف المحاكمة الالكترونية

تُعد المحاكم الرقمية أو الإلكترونية نتاجاً بارزاً لثورة الاتصالات وتكنولوجيا المعلومات، وهي تُظهر كيف يمكن استغلال التقنيات الرقمية لتطوير إدارة العدالة. تُجسد هذه المحاكم مفهوم "التقاضي الإلكتروني" أو "التقاضي عن بُعد، على الرغم من أن المشرع

الجزائري لم يُقدم تعريفاً محدداً للمحاكمة الإلكترونية ضمن قانون عصرنة العدالة رقم 15-03، فقد ترك هذا الأمر للفقه فعرّفت بأنّها "تقنية سمعية بصرية تتم باستعمال البث المباشر صوتا وصورة بين المحاكم على اختلاف درجاتها واختصاصاتها والمؤسسات العقابية في إطار قانوني مضبوط وذلك من أجل استجواب متهم أو شاهد أو طرف مدني أو خبير يتعذر تواجدهم بالمحكمة بسبب وضعيتهم الجزائية المتمثلة في الحبس أو لدواعي أخرى كاستحالة التنقل إلى مقر المحكمة التي تباشر بها المحاكمة"[1].

تمثل المحاكم الإلكترونية تحولاً جوهرياً في إدارة الأعمال القضائية، بفضل تكاملها مع التكنولوجيات الرقمية وأنظمة المعلومات. تُعزز هذه المحاكم من كفاءة التسيير الإداري من خلال تحويل البيانات إلى معلومات قابلة للتداول اليومي بسهولة. النظام الإلكتروني يتفوق على النظام التقليدي بميزاته المتعددة مثل سرعة الاتصالات والقدرة على نقل الوثائق والمستندات بين الأطراف المعنية بشكل فعال، ما يسهم في تقليل الوقت والجهد المبذولين من قبل القاضي والمتقاضين[2].

مع ذلك، فإن هذا التعريف قد حصر المحاكمة الرقمية في جانب واحد يتعلق بنقل المستندات إلكترونيًا إلى القاضي، بينما يشمل نظام التقاضي الإلكتروني، بالإضافة إلى نقل السندات والوثائق إلكترونيًا، استخدام تقنيات المحادثة عن بُعد في الإجراءات القضائية. كما يتضمن النظام وجود منظومة معلوماتية مركزية تعزز من فعاليته، ولا يُغفل عن أهمية نظام التصديق الإلكتروني الذي تضمنته المادة الأولى من قانون 15-03

لذا، ذهب بعض الفقهاء إلى تعريف التقاضي الإلكتروني على أنه سلطة الهيئة القضائية المتخصصة للفصل إلكترونيًا في النزاعات المعروضة أمامها، من خلال استخدام شبكة

---

[1]- نورة بن بوعبد الله، **أثر التحول الرقمي على إجراءات المتابعة الجزائية**، المرجع السابق.

[2]– أمير فرج يوسف، **المحاكم الإلكترونية المعلوماتية والتقاضي الإلكتروني**، المكتب العربي الحديث، الإسكندرية، 2014، ص31.

الإنترنت والاعتماد على أنظمة إلكترونية وآليات تقنية متطورة .يهدف هذا النظام إلى تسريع عملية الفصل في الخصومات وتسهيل الإجراءات القضائية للمتخاصمين[1].

من التحليل السابق، يظهر بوضوح أن المحاكمة الإلكترونية تستلزم أولاً إنشاء شبكة اتصالات مؤمنة تربط المحاكم، المجالس القضائية، المحكمة العليا، ومحكمة التنازع. وفي المرحلة الثانية، تتطلب العملية رقمنة الوثائق والملفات الورقية لتسهيل الوصول السريع إلى المعلومات واسترجاعها بفعالية، فضلاً عن تمكين الربط الفعّال بين هذه الوثائق.

الفرع الثاني: خصائص المحكمة الإلكترونية ومميزات التقاضي الالكتروني

تطبيق تقنية التقاضي الإلكتروني بالشكل الأمثل في الإدارة القضائية يؤدي إلى نتائج إيجابية من حيث سرعة إنجاز المعاملات والقضايا، ويساهم في توحيد وتبسيط إجراءات العمل القضائي. كما يعزز من أمن المعلومات من خلال حفظها بشكل آمن وتمكين الوصول إليها للأشخاص المصرح لهم فقط، بالإضافة إلى ضمان جودة العمل ومواكبة التطورات التقنية المستمرة.

ومع ذلك، فإن نجاح تقنية التقاضي الإلكتروني مرتبط بشكل وثيق بالعناية بالعناصر الأخرى التي تؤثر في تقديم الخدمات القضائية. هذه العناصر تشمل تطوير التقنية نفسها، تعزيز الموارد البشرية المؤهلة، وتحسين إجراءات العمل القضائي، والتي جميعها تلعب دورًا حاسمًا في تعظيم الفوائد المرجوة من النظام الإلكتروني.

تطبيق نظام المحكمة الالكترونية يسهم بفعالية في تحقيق العدالة، إذ يوفر للمتقاضين إمكانية المشاركة في الإجراءات القضائية دون الحاجة إلى تحمل عناء التنقل إلى مقر

[1]– أسعد فاضل منديل، **التقاضي عن بعد**، مجلة الكوفة للعلوم القانونية والسياسية، مجلد 1 ، العدد 21 ، 2014 ، ص. 101.

المحكمة. هذا التحول يعزز من سهولة الوصول إلى الخدمات القضائية ويقلل العبء اللوجستي على المتقاضين، مما يساعد في تسريع عملية تحقيق العدالة ويجعلها أكثر كفاءة.

يحمل التقاضي الإلكتروني مجموعة من الميزات الإيجابية التي شجعت الدول على تبنيه بنشاط، مثل تحقيق السرعة في الفصل في الدعاوى وتبسيط الإجراءات القضائية، هذه الميزات تسهم في تحسين كفاءة النظام القضائي، وتقليل الأعباء المترتبة على الجهات القضائية والمتقاضين على حد سواء، مما يعزز من فعالية العدالة ويسرع من عملية تحقيقها.

تم تحديد النطاق الاجرائي للمحادثة المرئية عن بعد في العمل القضائي الجزائي، بموجب القانون15_03المتعلق بعصرنة قطاع العدالة، حيث أجاز اللجوء إليها في إجراءات المحاكمة الجزائية وتشمل مرحلة التحقيق الابتدائي و المحاكمة، و هو ما نصت عليه المادة14 والمادة 15 من القانون 15-03 ، و في ظل انتشار جائحة كورونا و إعمالا لمبدأ الآجال المعقولة وحفاظا على الأمن و الصحة العمومية، تم إصدار الأمر20_04 في31 أوت2020، المتضمن تعديل قانون الإجراءات الجزائية ، الذي نص على تعميم استخدام تقنية المحادثة المرئية عن بعد في مرحلة التحقيق و المحاكمة الجزائية المادة 441 مكرر 2و7 من الأمر 20 – 04 المشار اليه سابقا.[1]

المطلب الثاني : تقنية المحادثة المرئية عن بُعد في الإجراءات القضائية

تم تكريس استخدام تقنية المحادثة المرئية عن بُعد في الإجراءات القضائية بموجب القانون رقم 15-03 المتعلق بعصرنة العدالة. المشرع الجزائري اعتبر استخدام هذه التقنية أمراً جوازياً، يمكن للقاضي أن يلجأ إليه بناءً على مقتضيات حسن سير العدالة أو للحفاظ على الأمن أو الصحة العمومية، كما شهدنا خلال جائحة كورونا، أو في حالات الكوارث

[1]- نورة بن بوعبد الله، **أثر التحول الرقمي على إجراءات المتابعة الجزائية**، المرجع السابق.

الطبيعية، أو لضمان احترام مبدأ المهل الزمنية المعقولة. يمكن الاستعانة بتقنية المحادثة المرئية عن بُعد في مرحلة البحث والتحري (الفرع الأول) ومرحلة التحقيق الابتدائي (الفرع الثاني) وأيضاً خلال المحاكمة (الفرع الثالث)، مما يساهم في تسهيل وتعزيز فعالية الإجراءات القضائية.

الفرع الأول: استعمال تقنية المحادثة المرئية عن بعد خلال مرحلة البحث والتحري

أجاز الأمر 20-04 المشار اليه اعلاه من خلال نص المادة 141 مكرر1 لوكيل الجمهورية اللجوء الى استعمال المحادثة المرئية عن بعد في حالة تمديد التوقيف للنظر، وكذا في حالة القبض على المتهم خارج دائرة اختصاص قاضي التحقيق الذي أصدر الأمر بالقبض، وبذلك اصبح بإمكانه تمديد التوقيف للنظر دون أن يمثل أمامه المشتبه به ماديا بل عن طريق المثول الافتراضي، خلافا للقاعدة العامة التي تقتضي اقتياد المشتبه فيه امام وكيل الجمهورية عند تمديد مده التوقيف للنظر. [1]

الفرع الثاني: استعمال تقنية المحادثة المرئية عن بعد خلال مرحلة التحقيق الابتدائي

تعد مرحلة التحقيق تُعد جزءًا أساسيًا وتحضيريًا في العملية القضائية، حيث تُعنى بجمع وتقييم الأدلة المتعلقة بالدعوى قبل إحالتها إلى المحكمة. هذه المرحلة تتيح للمحكمة فحص وتقييم مختلف الأدلة التي تم جمعها والتي تثبت ارتكاب الجرم وتنسيبه للمتهم، مما يمهد لفهم عميق وشامل لعناصر الدعوى قبل الشروع في الفصل فيها[2].

خلال مرحلة التحقيق، يُمنح المتهم مجموعة من الضمانات القانونية التي تحمي حقوقه وحريته من أي تعسف أو انتهاك قد ينجم عن إجراءات التحقيق. هذه الضمانات تشمل

---

[1]- نورة بن بوعبد الله، **أثر التحول الرقمي على إجراءات المتابعة الجزائية**، المرجع السابق.

[2]– محمد شاكر سلطان، **ضمانات المتهم أثناء مرحلة التحريات الأولية والتحقيق الابتدائي**، مذكرة ماجستير في القانون تخصص علم الإجرام والعقاب. كلية الحقوق والعلوم السياسية، جامعة العقيد الحاج لخضر باتنة. 2013، ص. 108

بشكل خاص حق الدفاع، الذي يضمن للمتهم الحق في أن يكون ممثلاً بمحامٍ يدافع عنه ويشارك في جميع مراحل التحقيق، بالإضافة إلى الحق في سرية إجراءات التحقيق، التي تهدف إلى ضمان ألا يتم الإفصاح عن تفاصيل القضية للعامة، مما يحمي المتهم من التأثيرات السلبية التي قد تنجم عن التشهير أو الإدانة المسبقة.

مع استخدام تقنية المحادثة المرئية عن بُعد، تتعزز هذه الضمانات بتوفير وسيلة يمكن من خلالها إجراء استجوابات ومناقشات دون الحاجة لنقل المتهم، مما يساهم في الحفاظ على سلامته وكرامته أثناء التحقيق.

بفضل استخدام تقنية المحادثة المرئية عن بُعد في مرحلة التحقيق بالنظام القضائي الجزائري، أصبح بإمكان قاضي التحقيق استجواب المتهمين باستخدام هذه التقنية من المحكمة الأقرب لمكان إقامة الشخص المطلوب تلقي تصريحاته، وذلك بحضور وكيل الجمهورية المختص إقليميًا وأمين الضبط. خلال عملية الاستجواب، يجب على قاضي التحقيق أن يضمن حضور محامي المتهم، حيث يتم استدعاء المحامي إما بكتاب موصى عليه يرسل إليه قبل موعد الاستجواب بيومين على الأقل، أو شفاهةً، ويتم تثبيت ذلك في المحضر.

كذلك، يحق لمحامي المتهم أن يحضر رفقة موكله في مكان الاستماع إليه و/أو أمام جهة التحقيق المختصة، مما يكفل حقوق الدفاع ويضمن سير العملية القضائية وفقًا للمعايير القانونية المطلوبة لحماية حقوق المتهمين.

لضمان مبدأ سرية إجراءات التحقيق وتعزيز الثقة في استخدام نظام المحادثة المرئية عن بعد، أكد المشرع الجزائري على وجوب توفير الوسائل الكفيلة بضمان سرية الإرسال وأمانته خلال استخدام هذه التقنية، يشمل ذلك تسجيل التصريحات على دعامة إلكترونية موثوقة

تضمن حفظ المعلومات بأمان وحمايتها من التلف أو التعديل الغير مصرح به. هذه الإجراءات تساهم في الحفاظ على النزاهة العملية وتعزز من فعالية النظام القضائي في التعامل مع البيانات الحساسة بطريقة آمنة ومحمية[1].

الفرع الثاني: استعمال تقنية المحادثة المرئية عن بعد خلال المحاكمة

تعتبر مرحلة المحاكمة المرحلة الأساسية والحاسمة في الدعوى العمومية، حيث يتم فيها تحديد مصير المتهم، سواء بالبراءة أو الإدانة. استخدام تقنية المحادثة المرئية عن بُعد في المحاكمات الجزائية يلعب دورًا مهمًا، خاصة في ظل الظروف الصحية الراهنة المتعلقة بجائحة فيروس كورونا، هذه التقنية تمكّن من إجراء الجلسات دون الحاجة لحضور الجمهور في قاعة المحكمة، مما يدعم جهود الحفاظ على الصحة العامة من خلال التقيد بالبروتوكولات الصحية المفروضة، بما في ذلك التباعد الجسدي، كما حددته منظمة الصحة العالمية[2]، هذا التكيف التقني ليس فقط يحافظ على الصحة وسلامة الجميع، بل يضمن أيضاً استمرارية العملية القضائية بكفاءة وفعالية، مما يمكن القضاة وجميع الأطراف المعنية من تنفيذ واجباتهم دون تأخير أو إعاقة، ويسمح بتحقيق العدالة حتى في أوقات الأزمات.

يكفل القانون الجزائري حقوق وحريات الشخص الموقوف بما في ذلك الحق في اختيار نوع المحاكمة التي يفضلها، سواء كانت محاكمة عن بُعد باستخدام المحادثة المرئية أو محاكمة تقليدية في قاعة المحكمة. هذا يمنح المتهم فرصة للمشاركة بفعالية في العملية القضائية بالشكل الذي يراه مناسبًا ومريحًا له.

---

[1]– المادة 441 مكرر من قانون الإجراءات الجزائية المعدل والمتمم.

[2]– خليل الله فليغة ويزيد بوجليط، **المحاكمة عن بعد: سرعة الإجراءات أم إهدار للضمانات**، مجلة العلوم القانونية والسياسية المجلد 12، العدد 1، أفريل 2021، ص897

جهة الحكم لديها السلطة لاستخدام تقنية المحادثة المرئية عن بُعد من تلقاء نفسها، أو يمكن أن يتم هذا بناءً على طلب من النيابة العامة أو أحد الخصوم أو ممثليهم القانونيين. هذا النهج يضمن مرونة في النظام القضائي ويسمح بتلبية احتياجات جميع الأطراف المعنية، مع مراعاة متطلبات كل حالة بشكل فردي، وفي الوقت نفسه يحافظ على الكفاءة والفعالية في تنفيذ العدالة، خاصة في ظروف تستدعي الحد من التجمعات أو في حالات الطوارئ الصحية[1].

ان استخدام تقنية المحادثة عن بُعد، عندما يتم تنفيذه وفقًا للشروط والوسائل المناسبة، يضمن حماية حقوق الخصوم وبالأخص الطرف المتهم، حيث يعتبر المتهم حاضرًا إلكترونيًا في الجلسة، ويتم ذلك بعد استطلاع رأي النيابة العامة وإعلام باقي الخصوم باللجوء إلى هذه التقنية لإجراء المحاكمة[2].

منح المشرع الجزائري للقاضي الصلاحية لمواصلة استخدام تقنية المحاكمة عن بُعد حتى في حال رفض النيابة العامة أو أحد الخصوم لهذه التقنية، متى ما رأى القاضي أن الاعتراض المُقدم غير جدي أو لا يستند إلى أسس قوية. هذا يبرز الجهود المبذولة لضمان استمرارية العملية القضائية وتحقيق العدالة بكفاءة وفعالية، حتى في الظروف التي قد تحول دون الحضور الفعلي للأطراف في قاعة المحكمة.

أما عن تنظيم المحاكمات عن بُعد في الجزائر بدأ بالفعل يأخذ زخمًا كبيرًا منذ الحدث الرائد في محكمة القليعة بتاريخ 7 أكتوبر 2015– سبق الاشارة اليه–، وهذا يعد مؤشرًا على التقدم في استخدام التقنيات الحديثة في النظام القضائي. تبع ذلك أول محاكمة دولية تمت بتقنية المحاكمة عن بُعد في 11 يوليو 2016، حيث تم الاستماع إلى شاهد من مجلس

[1]– المادة 441 مكرر 7 من قانون الإجراءات الجزائية المعدل والمتمم.

[2]– المادة 441 مكرر 7 من قانون الإجراءات الجزائية المعدل والمتمم.

قضاء "نانتير" في فرنسا من قبل مجلس قضاء المسيلة، مما يدل على القدرة العالية على التعامل مع الشهادات الدولية دون الحاجة لتنقلات دولية معقدة.

وقد طالبت هيئات الدفاع و بشكل متزايد الاستفادة من تقنية المحادثة عن بُعد، خاصة في حالات السجناء الذين يتم محاكمتهم ويكونون متهمين في قضايا أخرى أو مطلوبين كشهود في قضايا تتعلق بآخرين، هذه التقنية تُعتبر حلاً فعالاً للمشاكل المتعلقة بالتأخير والتأجيل في الجلسات، خاصة مع الإجراءات الجديدة التي تمنع الحبس الاحتياطي إلا للضرورة القصوى، وبذلك تخفف العبء عن القضاة وتسرع من إجراءات العدالة بشكل عام[1].

[1]– بواشري أمينة وسالم بركاهم، المرجع السابق، ص. 225.

خلاصة الفصل الثاني

تُعد عصرنة قطاع العدالة في الجزائر ضرورة ملحة ومطلبًا أساسيًا، خاصة في ظل التغيرات الدولية والتزامات الجزائر بالاتفاقيات والمعاهدات الدولية المعنية بحماية حقوق الإنسان ومكافحة الفساد، هذا التوجه نحو تحديث قطاع العدالة يُعد من ثمار التحولات الدولية ويتجلى في تبني استراتيجية رقمية للإدارة الإلكترونية للقطاع تتضمن سلسلة من المراحل الإصلاحية.

في إطار تحقيق مشروع الإدارة الإلكترونية، اعتمد المشرع الجزائري التقاضي الإلكتروني، مُعززًا رقمنة جميع القطاعات منذ عام 2015، ومؤسسًا لهذا التوجه بالأساس القانوني المُتمثل في القانون رقم 15 – 03 الخاص بعصرنة العدالة. ومع تفشي جائحة كورونا، تأكدت الحاجة الماسة والأهمية الكبرى لتفعيل هذه التقنية، الأمر الذي عُزز بتعديل قانون العقوبات وفق الأمر 20 – 04، بدأت مراحل إصلاح قطاع العدالة بإنشاء الأسس اللازمة لعملية العصرنة، وذلك من خلال إطلاق بوابة إلكترونية للتفاعل والإعلام مع العموم، وتطوير إطار قانوني وتشريعي يدعم التسيير الرقمي، بالإضافة إلى تأسيس الهياكل التنظيمية التي تتماشى مع النهج الجديد في الإدارة الإدارية للقطاع، متجاوزةً بذلك الأساليب التقليدية.

تتمثل محطات العصرنة التي أعقبت سلسلة الإصلاحات في تطوير الخدمات العمومية بأسلوب حديث، وذلك من خلال إطلاق عملية السوار الإلكتروني، الإمضاء الإلكتروني، وإتاحة استخراج الوثائق القضائية، الجنسية، والسوابق العدلية إلكترونياً. كما تشمل العصرنة تبني المحاكمة عن بُعد، إنشاء قاعدة بيانات ونظام إدارة تقني خاص بالقطاع، وتطوير شبكات الاتصال الداخلية بين المحاكم القضائية، المؤسسات العقابية، والإدارة المركزية ومؤسساتها الإدارية. هذه التحديثات تساهم في تسريع العمليات الإدارية وتقديم خدمات عمومية بمعايير عالية من الجودة والكفاءة.

الخاتمة

أفرزت دراستنا لموضوع القانون الجزائي والتكنولوجيا الحديثة جملة من النتائج والمقترحات نوردها فيما يلي:

أولا: النتائج

– بسبب حداثة الجريمة الإلكترونية، لم يتم بعد التوصل إلى إجماع فقهي حول تعريف موحد لهذا النوع من الجرائم.

– مع ظهور أنماط جديدة من مرتكبي الجرائم، لم يعد الدافع وراء الجرائم التقليدية مقتصرًا على الأسباب القديمة فحسب، بل ظهرت دوافع معاصرة تشمل، بجانب تحقيق الكسب المادي والانتقام، أيضًا إثبات التفوق العلمي والدعاية والتسلية.

– المجرم الالكتروني يختلف عن المجرم التقليدي؛ فهو شخص يتمتع بمعرفة علمية وكفاءة عالية، ويتسم بقدرات عقلية وذهنية تمكنه من تجنب العقاب.

– يفتقر المشرع الجزائري إلى الأدوات الكفيلة بمواجهة الآثار الجسيمة التي تنجم عن جرائم الاعتداء على أنظمة المعالجة الآلية للبيانات، سواء على مستوى النصوص التشريعية أو فيما يتعلق بطبيعة الكوادر والأجهزة المتخصصة. لذا، يُعتبر ضروريًا أن يسارع إلى اعتماد سياسة شاملة ومدروسة تهدف إلى مواجهة جميع التحديات التي تطرحها هذه الجريمة، مع التأكيد على أهمية الوقوف بحزم أمام التحديات التي تفرضها.

– بالنظر إلى الخصائص الفريدة للجريمة الجريمة الإلكترونية، وطابع بيئتها غير الملموس، تواجه السلطات شبه القضائية والقضائية تحديات كبيرة في كشف الجرائم وجمع الأدلة المتعلقة بها. على الرغم من النجاح النسبي للدول في تطبيق الأساليب الإجرائية التقليدية مثل المعاينة، التفتيش، والضبط، مع تعديل بعض الخصوصيات والشروط لتتناسب مع طبيعة الجريمة المعلوماتية، فإن هناك صعوبات تظل قائمة. تتمثل هذه الصعوبات بشكل أساسي في قلة الآثار المادية التي تتركها هذه الجرائم

وكثرة الأشخاص الذين قد يترددون على مكان الجريمة بين وقت ارتكابها ووقت اكتشافها، مما يعقد عملية الكشف عنها.

– مبدأ التعاون الدولي يُعتبر من المبادئ القانونية الدولية الرئيسية في العالم المعاصر، خاصة في مجال مكافحة الجريمة. لقد برزت أهمية هذا المبدأ مع تنوع وتعقيد التطورات التي شهدتها طرق وأساليب ارتكاب الجرائم الإلكترونية، لكن الحدود الإقليمية تشكل عائقًا أمام التعاون الدولي في مجال مكافحة الجريمة الإلكترونية، مما يؤدي إلى تسهيل إفلات مرتكبي هذه الجرائم من العقاب، وبالتالي يزيد من تشجيعهم على ارتكاب المزيد منها.

– تُعتبر المحاكمة الإلكترونية مستقبل قطاع العدالة، وقد أدت جائحة كورونا والتدابير الاحترازية التي فرضتها إلى تعطيل قطاع العدالة والعديد من القطاعات الإدارية الأخرى، مما بيّن بشكل كبير ضرورة تبني نظام المحاكمة الرقمية. السعي نحو تطوير هذا النظام وتطبيقه أصبح أمرًا حيويًا، بل ومن الضروري توسيع نطاق استخدامه نظرًا لما يوفره من توفير الوقت وتبسيط إجراءات التقاضي.

– على الرغم من التعديلات التي أدخلتها الجزائر في مجال مكافحة الجريمة الالكترونية وفي تطوير وعصرنة مرفق العدالة، فإن النصوص القانونية الحالية لا تزال غير كافية لمواكبة التطور المتسارع في الاحتراف الإجرامي المعلوماتي.

ثانيا: المقترحات

من خلال النتائج المتوصل اليها نقترح مايلي:

– تكييف إجراءات التفتيش مع طبيعة الجريمة الالكترونية التي تختلف عن الجريمة التقليدية.

– في مجالات التحري والتحقيق، والمحاكمة لابد من التخصص العلمي والوظيفي في جرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات وتطبيقات الحاسوب، بالإضافة إلى الجرائم المتعلقة بها.

– كما يُقترح النظر في إدراج موضوعات تتعلق بجرائم الإنترنت ضمن مناهج التحقيق الجنائي في كليات الحقوق ومعاهد التدريب الشرطي.

– تعزيز الوعي الرقمي بين المستخدمين حول كيفية حماية بياناتهم الشخصية. يشمل ذلك عدم الاحتفاظ ببيانات شخصية أو مالية على الأجهزة، الامتناع عن نشر معلومات شخصية، وعدم مشاركة كلمات السر، يُمكن أيضًا دمج هذه المفاهيم ضمن المناهج الدراسية لتعميق الفهم والوعي.

وفي الأخير على الرغم من أن وزارة العدل قد أطلقت العديد من الخدمات وأتاحتها عبر الإنترنت، إلا أن العديد من المواطنين لا يزالون غير مدركين لوجود هذه الخدمات ويستمرون في زيارة الجهات القضائية للحصول عليها، لذلك، نقترح القيام بحملات توعوية وإرشادية لتعريف المواطنين بهذه الخدمات الإلكترونية وتشجيعهم على استخدامها.

قائمة المصادر والمراجع

أولا المصادر:

سورة المائدة، القراءن الكريم_

- **1/ الأوامر:**

– الأمر رقم 03 –05 مؤرخ في 19 جمادى الأولى عام 1424 الموافق 19 يوليو سنة 2003، يتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية العدد 44 بتاريخ 232 جمادى الأولى 1424 الموافق 23 يوليو 2003.

– الأمر رقم 15 –02 مؤرخ في 7 شوال عام 1436 الموافق 23 يوليو سنة 2015 يعدل ويتمم الأمر رقم 66 – 155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية.

– الأمر رقم 20 –04 مؤرخ في 11 محرم عام 1442 الموافق 30 غشت سنة 2020 يعدل ويتمم الأمر رقم 66– 155 المؤرخ في 18 صفر عام 1386 الموافق 8 يناير سنة 1966 والمتضمن قانون الإجراءات الجزائية.

-2/ القوانين:

– القانون رقم 04–14 المؤرخ في 27 رمضان عام 1425 الموافق 10 نوفمبر سنة 2004 الموافق 10 نوفمبر سنة 2004 المعدل والمتمم للأمر رقم 66–155 المتضمن قانون الإجراءات الجزائية.

–القانون رقم 04 – 15 مؤرخ في 27 رمضان عام 1425 الموافق 10 نوفمبر سنة 2004، يعدل ويتمم الامر رقم 66 – 156 المؤرخ في 18 صفر عام 1386 الموافق8 يونيو سنة 1966 والمتضمن قانون العقوبات القسم السابع مكرر: المساس بأنظمة المعالجة الآلية المعطيات.

– القانون رقم 06 – 22 مؤرخ في 29 ذي القعدة عام 1427 الموافق 20 ديسمبر سنة 2006 ، يعدل ويتمم الأمر رقم 66 – 155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية الفصل الرابع: في اعتراض المراسلات وتسجيل الاصوات والتقاط الصور.

- القانون رقم 15- 03 مؤرخ في 11 ربيع الثاني عام 1436 الموافق أول فبراير سنة 2015 يتعلق بعصرنة العدالة.

- القانون رقم 15-04: مؤرخ في 11 ربيع الثاني 1436 الموافق أول فبراير سنة 2015 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين.

3/ المراسيم:

- المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد53 .
- المرسوم الرئاسي رقم 19-172 مؤرخ في 06-06-2019 يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنلوجيا الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها، ، الجريدة الرسمية، العدد 37.
- المرسوم الرئاسي رقم 04-183 المؤرخ في8 جمادى الأولى 1425ه الموافق 26 يونيو2004، المتضمن احداث المعهد الوطني للأدلة الجنائية وعلم الاجرام للدرك الوطني وتحديد قانونه الأساسي، الجريدة الرسمية، العدد41 بتاريخ 27 يونيو 2004.

ثانيا: المراجع باللغة العربية

1-الكتب:

- أسامة أحمد ، جرائم الحاسب الآلي والانترنيت ، دراسة تحليلية مقارنة، الطبعة الأولى، دار وائل للنشر، عمان الأردن، 2000 .
- أمير فرج يوسف، المحاكم الإلكترونية المعلوماتية والتقاضي الإلكتروني، المكتب العربي الحديث، الإسكندرية، 2014.
- بكري يوسف بكري، التفتيش عن المعلومات في رسائل التقنية الحديثة، دار الفكر الجامعي، الإسكندرية ط1، 2011.

قائمة المصادر والمراجع

- حسن دوواد طاهر، جرائم نظم المعلومات ، أأكاديمية نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى ، 2000 .
- محمد الفاضل، التعاون الدولي في مكافحة الإجرام، دار الكتب الجامعية، الاسكندرية، 1967 .
- محمد امين الرومي، جرائم الكمبيوتر والانترنت، دار المطبوعات الجامعية، مصر 2004.
- مناصرة يوسف ،جرائم المساس بأنظمة المعالجة الآلية للمعطيات ، دار الخلدونية للنشر والتوزيع ، الجزائر، 2018 .
- جميل عبد الباقي الصغير، الجوانب الاجرائية المتعلقة بالأنترنت، دار النهضة العربية، القاهرة ، 2001.
- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، ط1، دار الفكر الجامعي الإسكندرية، 2009.
- عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت، ط1، دار الفكر الجامعي 180 مصر، 2006 .
- عبد الفتاح مراد ، شرح جرائم للكمبيوتر والانترنيت ، منشأة المعارف، مصر، 1998.
- عرب تونس ، جرائم الكمبيوتر والانترنيت، منشورات اتحاد المصارف العربية، الطبعة الأولى، 2002.
- فاروق سيد الحسين ، الانترنيت الشبكة العالمية للمعلومات، مطابع الهيئة المصرية الهامة للكتاب، القاهرة ،1998 .
- محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، دار هومة، الجزائر، ط 2، 2009.

قائمة المصادر والمراجع

- محمد حماد مرهج الهيئي، جرائم الحاسوب(ماهيتها موضوعها أهم صورها والصعوبات التي تواجهها)، دراسة تحليلية واقع الاعتداءات التي يتعرض لها الحاسوب وموقف التشريعات الجنائية منها، دار المناهج للنشر والتوزيع، الأردن 2006.
- محمد زكي أبو عامر، الإجراءات الجنائية، دار الجامعة الجديد ، الاسكندرية، مصر، 2008.
- محمد سامي الشواء ، ثورة المعلومات انعكاساتها على قانون العقوبات دار النهضة العربية ، مصر، 1998.
- سن مظفر الرزو، القضاء المعلوماتي، مركز دراسات الوحدة العربية ،الطبعة الأولى، 2007.
- محمد الرشيدي، العنف في جرائم الانترنيت، الدار المصرية اللبنانية، مصر، 2004.
- محمد عبد الله أبو بكر سلامة، موسوعة جرائم المعلوماتية، منشأة المعارف الإسكندرية ،2007.
- محمد على العريان ، الجرائم المعلوماتية ، دار منشأة المعارف ، الإسكندرية 2003.
- محمد علي العريان، الجريمة المعلوماتية، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، 2011.
- محمد نجيب حسني، شرح قانون العقوبات القسم الثاني، دار النهضة العربية، ط6، مصر،1989.
- نائلة عادل محمد فريد بدقورة ،جرائم الحاسب الآلي الاقتصادية (دراسة نظرية مقارنة)، منشورات المجلس الحقوقية ، الطبعة الأولى، 2005.
- نعيم مغبغب، مخاطر المعلوماتية، المخاطر على الحياة الخاصة وحمايتها" دراسة في القانون المقارن ، منشورات الحلبي الحقوقية ، لبنان، 1998 .
- هدى حامد قشقوش، جرائم الحاسب الالكتروني، دار النهضة العربية ،القاهرة ،1992.

- هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات ، مكتبة الآلات الحديثة، مصر، 1994.

2- المقالات العلمية:

- أشرف جودة محمد محمود، المحاكم الإلكترونية في ضوء الواقع الإجرائي المعاصر، مجلة الشريعة والقانون، العدد 35 ،الجزء 3، 2020.

- أسعد فاضل منديل، التقاضي عن بعد، مجلة الكوفة للعلوم القانونية والسياسية، مجلد 1 ، العدد 21، 2014.

- بواشري أمينة وسالم بركاهم، الاصلاح الاداري في الجزائر عرض تجربة مرفق العدالة 1999/2017 ، المجلة العلمية ،الجزائر 3، العدد11، جانفي 2018.

- خليل الله فليغة و يزيد بوجليط، المحاكمة عن بعد: سرعة الإجراءات أم إهدار للضمانات، مجلة العلوم القانونية والسياسية المجلد 12، العدد 1، أفريل 2021.

- عادل عبد العال ابراهيم، خراشي اشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، كلية الشريعة والقانون، القاهرة .

- عبد الله حسين على محمود، سرقة المعلومات المخزنة في الحاسب الآلي، مجلة الأمن والقانون، السنة الثانية العدد الأول ، 2004 - محمد عبد الوهاب سلطان العلماء، جرائم الانترنيت واحتساب عليها، المجلة العربية للدراسات الأمنية والتدريب، السنة 18 عدد 36/1424 .

3_ الرسائل الجامعية:

أ_مذكرات الماجيستير

- أمال قارة، الجريمة المعلوماتية، مذكرة ماجستير، تخصص قانون جنائي ، كلية الحقوق جامعة بن عكنون، الجزائر 2001.
- سفيان سوبر، جرائم المعلوماتية، مذكرة الماجستير في العلوم الجنائية وعلم الإجرام، جامعة أبو بكر بلقايد، تلمسان،2010- 2011 .

- عبد العزيز بوذراع، خصوصية الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، مذكرة الماجستير في القانون، كلية الحقوق جامعة الجزائر 1، 2011-2012 .
- محمد شاكر سلطان، ضمانات المتهم أثناء مرحلة التحريات الأولية والتحقيق الابتدائي، مذكرة ماجستير في القانون تخصص علم الإجرام والعقاب. كلية الحقوق والعلوم السياسية، جامعة العقيد الحاج لخضر باتنة. 2013.
- مريم احمد مسعود، آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال في ضوء قانون رقم 09-04، مذكرة الماجستير، جامعة قاصدي مرباح كلية الحقوق والعلوم السياسية سنة 2012 - 2013 .
- نعيم سعداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة الماجستير في العلوم القانونية، بجامعة الحاج لخضر، باتنة 2012-2013 .

ب- مذكرات الماستر

- حملاوي الدراجي ،الأقطاب الجزائية المتخصصة، مذكرة الماستر تخصص قانون جنائي، جامعة محمد بوضياف مسيلة، 2014-.2015

4_ التظاهرات والملتقيات العلمية:

- محمد السنبري، التحقيق في جرائم الحاسب الآلي دراسة قانونية مقارنة، أعمال مؤتمر القانون والكمبيوتر والانترنيت الذي عقدته كلية الشريعة والانترنيت بجامعة الإمارات ، 2005.

- عمرو حسين عباس، أدلة الإثبات الجنائي والجرائم الالكترونية (المعلوماتية) بحث مقدم إلى المؤتمر الإقليمي 02 حول تحديات تطبيق الملكية الفكرية في الوطن العربي، خلال فترة 27-26-04 سنة 2008، جامعة الدول العربية.

- لوجاني نور الدين، أساليب البحث والتحري الخاصة وإجراءاتها، مداخلة في يوم دراسي حول علاقة النيابة العامة بالشرطة القضائية احترام حقوق الإنسان ومكافحة الجريمة، المديرية العامة للأمن الوطني، أمن ولاية ايليزي يوم 12 ديسمبر 2007.

– ممدوح عبد المجيد عبد المطلب، جرائم استخدام شبكة المعلومات العالمية – الجريمة عبر الانترنيت–، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنيت، كلية الشريعة والقانون بجامعة الامارات العربية المتحدة ،2000.

– نورة بن بوعبد الله ، الجريمة الالكترونية (مقاربة مفاهيمية)، مداخلة ألقيت في الملتقى الوطني حول الجريمة الالكترونية وتداعيات الأمن السيبيراني بين النظرية والواقع، كلية الحقوق والعلوم السياسية، جامعة باتنة1، يوم 11 ماي 2023.

– نورة بن بوعبد الله، أثر التحول الرقمي على إجراءات المتابعة الجزائية ، مداخلة ألقيت في الملتقى الوطني حول الأثر التحول الرقمي على المنظومتين القانونية والقضائية، كلية الحقوق والعلوم السياسية، جامعة الجلفة، يوم 25 أفريل 2024.

5_ المراجع الالكترونية

–ياسر الأمير فاروق، مراقبة الأحاديث الخاصة في الإجراءات الجزائية، دار المطبوعات الجامعية، جامعة القاهرة. 2009 ، بتاريخ 2024//04/26، على الساعة 22.26 ،https://jfslt.journals.ekb.eg/article_14124_9940c95e1f087a055130abff802ddbd8.pdf

–موقع وزارة العدل الامريكية، الاطلاع بتاريخ 2024//04/26، على الساعة 15.36، https://www.ojp.gov/ncjrs/virtual-library/abstracts/computer-crimes-7

ثانيا: المراجع الأجنبية

- B.Strenling they Haker. Crak ouv, Lawend electronic Fouinter, London,Viking,1993.
- David core, Karl Sergu William, Voushorch computer crime d'heillez et Associaés.in 1995.
- Emmanuel ZEZ , les noms de domaine de l'internet, Aspets juridiques ,Litee,2000.
- Peter Greinsbosky, electronic crime upper.sadal.River N5 Pearsons,Prentrie,Hall-2007.

فهرس المحتويات

فهرس المحتويات

شكر وتقدير .....

إهداء .....

المقدمة 1

الفصل الأول دور التكنولوجيات الحديثة في ظهور الجرائم المستحدثة – الجريمة الالكترونية أنموجا6

المبحث الأول: ماهية الجرائم الالكترونية..... 8

المطلب الأول : مفهوم الجريمة الالكترونية..... 8

المطلب الثاني: مفهوم المجرم الالكتروني..... 17

المبحث الثاني: مواجهة الجريمة الالكترونية في التشريع الجزائري 22

المطلب الأول: القواعد الموضوعية لمواجهة الجريمة الالكترونية في التشريع الجزائري 23

المطلب الثاني: القواعد الاجرائية لمواجهة الجريمة الالكترونية في التشريع الجزائري 33

خلاصة الفصل الأول..... 52

الفصل الثاني دور التكنولوجيات الحديثة في تعزيز قواعد القانون الجزائي..... 53

المبحث الأول: الآليات المستحدثة لسير الدعوى القضائية 54

المطلب الأول: عصرنة العمل القضائي والخدمات القضائية 55

المطلب الثاني: الشكوى الالكترونية..... 59

المبحث الثاني: نظام المحاكمة الالكترونية وفقا لأحكام قانون عصرنة العدالة 15-03..... 61

المطلب الأول: مفهوم المحاكمة الالكترونية..... 62

المطلب الثاني : تقنية المحادثة المرئية عن بُعد في الإجراءات القضائية 65

خلاصة الفصل الثاني 71

الخاتمة..... 78

فهرس المحتويات

قائمة المصادر والمراجع..... 74

فهرس المحتويات 81

الملخص:..... 87

الملخص:

تعد الجرائم الالكترونية من بين الجرائم الأكثر خطورة وتعقيداً، وقد أدت الثورة الرقمية التي كانت نتاج للتطور التكنولوجي إلى ظهور جرائم جديدة تستهدف برامج الكمبيوتر وتلحق الضرر بأنظمتها المعلوماتية، وعلى ضوء ذلك، سعى المشرع الجزائري لمواكبة التطورات في مكافحة الجرائم الالكترونية من خلال تعديل قانون العقوبات، وذلك بموجب القانون رقم 04-15 الذي أدخل بعض الجرائم الجديدة ضمن القسم السابع، الذي يحمل عنوان "المساس بأنظمة المعالجة الآلية للمعطيات"، وحاول استثمار التكنولوجيا الحديثة في تعزيز قواعد القانون الجزائي، من خلال عصرنة قطاع العدالة فظهرت ملامح تأثيره على الاجراءات السابقة على تحريك الدعوى العمومية من خلال إقرار الشكوى الالكترونية، واستعمال تقنية المحادثة المرئية في أداء العمل القضائي في المواد الجزائية .

الكلمات المفتاحية: القانون الجزائي، الجرائم الالكترونية، تكنولوجيا حديثة.

Summary:

Cybercrimes are considered among the most dangerous and complex crimes, having arisen as a result of advances in technology and technical methods. The information revolution has led to the emergence of new crimes targeting The Algerian legislator has sought to keep pace with developments in combating cybercrimes by amending the penal code, according to Law No. 04-15, which introduced some new crimes under Section Seven, titled "Interference with Automated Data Processing Systems, and tried to invest modern technology in strengthening the rules of criminal law, by modernizing the justice sector, thus clarifying the features of its impact on the procedures prior to initiating public lawsuits by approving the electronic complaint, and using video chat technology in performing judicial work in criminal matters.

Keywords: Criminal law, cybercrimes, modern technology