المركز الجامعي صالحي أحمد بالنعامة

معهد الحقوق

قسم القانون العام

مذكرة تخرج لنيل شهادة الماستر

تخصص قانون جنائي والعلوم الجنائية

الجريمة المعلوماتية وسبل مواجهتها على المستويين الوطني والدولي

إعداد الطلبة

- بويش عمر
- فردي سارة

تحت إشراف

د/ عثماني رضوان

لجنة المناقشة

د_ حشيفة المجدوب	أستاذ محاضر قسم أ	رئيسا
د- عثماني رضوان	أستاذ محاضر قسم ب	مشرفا ومقررا
د- بن حبيبة إيمان	أستاذ محاضر قسم ب	مناقشا

السنة الجامعية: 2023-2024

المركز الجامعي صالحي أحمد بالنعامة

معهد الحقوق

قسم القانون العام

مذكرة تخرج لنيل شهادة الماستر

تخصص قانون جنائي والعلوم الجنائية

الجريمة المعلوماتية وسبل مواجهتها على المستويين الوطني والدولي

إعداد الطلبة

بويش عمر

فاردي سارة

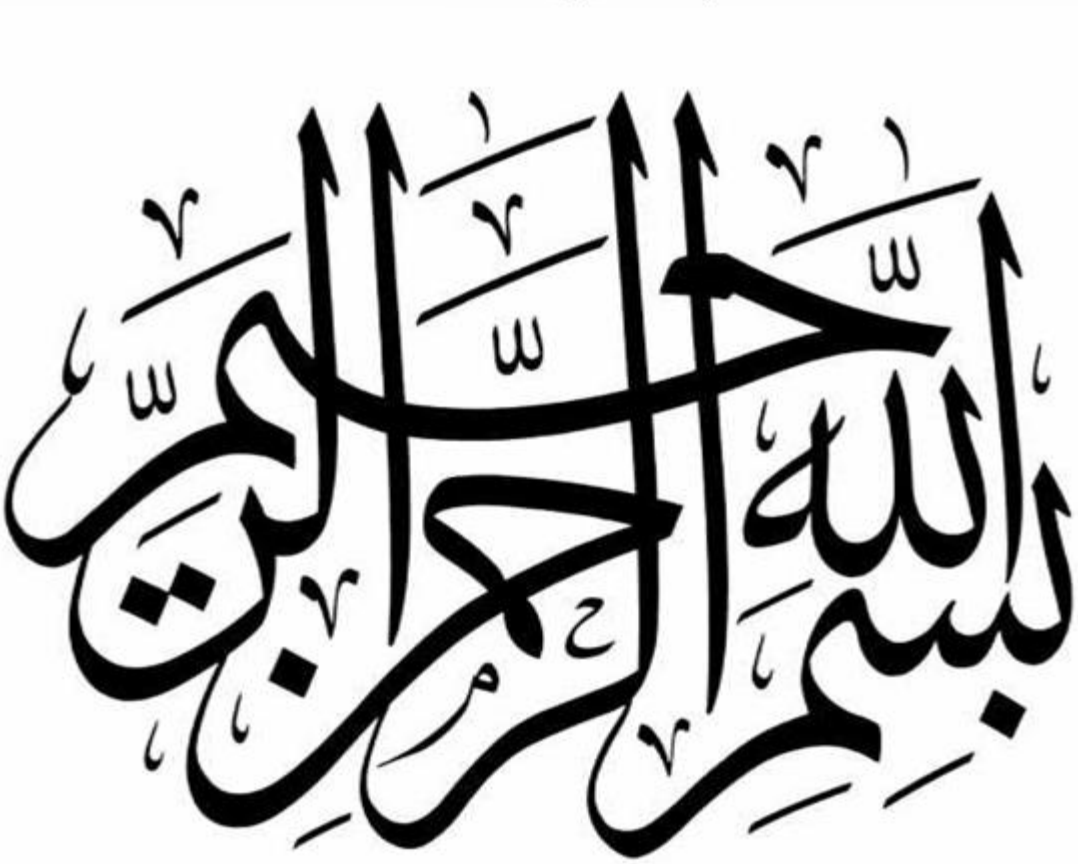
تحت إشراف

د/ عثماني رضوان

لجنة المناقشة

د/حشيقة المجدوب	أستاذ محاضر قسم أ	رئيسا
د/عثماني رضوان	أستاذ محاضر قسم ب	مناقشا ومقررا
د/بن حبيبة إيمان	أستاذ محاضر قسم ب	مناقشا

السنة الجامعية: 2023-2024


بسم الله الرحمن الرحيم

الشكـــر والعـــرفان

في البداية، الشكر والحمد لله، جل جلاله، فإليه ينسب الأمر كله والفضل في إكمال هذه الدراسة.

يسرني أن أتقدم بأصدق عبارات الشكر والتقدير وأسمى آيات الاحترام والثناء أحملها إلى أستاذي الفاضل " عثماني رضوان " الذي منحني ثقته من أجل الإشراف على مذكرة التخرج وعلى حسن تعاونه والتضحية بوقته كي يكتمل هذا العمل، فله أقول جزاك الله خيرا وأدامك الله منارة للعلم.

كما أجزي الشكر وخالص العرفان والتقدير للسادة أعضاء اللجنة الموقرة على تفضلهم وقبولهم المشاركة في مناقشة المذكرة، وتحمل عبء مراجعة هذا العمل، وتصويب أخطائه، فلهم أقول جزاكم الله خيرا.

كما أشكر كل من ساعدني على إنجاز هذه المذكرة من قريب ومن بعيد

الإهـــداء

الحمد لله وكفى والصلاة على الحبيب المصطفى صل الله عليه وسلم أمّا بعد:

الحمد لله الذي وفقنا لتثمين هذه الخطوة في مسيرتنا الدراسية بمذكرتنا هذه ثمرة الجهد والنجاح بفضله تعالى.

أهدي تخرجي الجامعي إلى والدي أطال الله في عمره وإلى نبع الحنان أمّي الحبيبة أطال الله في عمرها.

وإلى جميع أفراد عائلتي.

ولا أنسى أصدقائي الذين شجعوني على المضي قدما في مواصلة وإتمام هذا البحث المتواضع خاصة رفيق الدرب بن خيرة عبد المجيد

بويش عمر

الإهـــداء

الحمد لله الذي بنعمته تتم الصالحات، بعد مسيرة دراسية حملت في طياتها الكثير من الصعوبات والمشقة والتعب، اليوم نقطف ثمرها والحمد لله

إلى من وضع المولى – سبحانه وتعالى – الجنة تحت قدميها، ووقَّرها في كتابه العزيز.....

(أمي الحبيبة)

إلى من كان قوتي عندما تسلل الضعف في لحظات التعب إلى قلبي، الداعم الأول..... أبي الغالي

إلى بسمة الحياة، نبع الأمل الذي يفيض على قلبي بالتفاؤل دوما.

أختي..... الحبيبة

إلى من يسري حبهم في عروقي، من أتشارك معهم الدم والصدق والحنان.....إخوتي الأحباء

إلى صديقاتي ..... إيناس، يسرى، شكرا لكم لأنكم جعلتم رحلة الدراسة ممتعة مليئة بالذكريات، أهدي لكم نجاحي.

إلى جميع هؤلاء أهدي ثمرة جهدي.

فردي سارة

قائمة المختصرات

ق.ج ..... قانون الجزائري

إ.ع.م.ج.ت.م ..... الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

ق.ع ..... قانون العقوبات

ق.إ.ج ..... قانون الإجراءات الجزائية

ص ..... صفحة

ط ..... طبعة

ب.ط ..... بدون طبعة

س.ج..... السنة الجامعية

ج.ر.ج.ج ..... الجريدة الرسمية للجمهورية الجزائرية

ج ..... الجزء

ج.م.ت.إ.إ ..... الجرائم المتصلة بتكنولوجيا الإعلام والإتصال

مقدمة

إن الجريمة هي كل فعل أو سلوك يجرمه القانون ويعاقب عليه بعقوبة جزائية، وهي ظاهرة من الظواهر الاجتماعية القديمة والتي تتطور بتطور الإنسان وباختلاف الزمان والمكان وقد دخل الإنسان مرحلة جديدة من التطور الفكري بظهور ثورة علمية وتكنولوجية خاصة في مجال الاتصالات والمعلومات وظهور شبكة الأنترنت، والتي كانت النواة الأولى لها من خلال المشروع الذي أطلقته وزارة الدفاع الأمريكية في القرن العشرين في سنة 1969 من أجل مساعدة الجيش على الاتصال في حال وجود حرب على أمريكا أو هجوم بالسلاح النووي، أي أنه كانت لها أغراض عسكرية فقط.

بعد ذلك وفي سنة 1972 تحول استخدام شبكة الأنترنت لأغراض سلمية، والتي بدأت في التطور، حيث اتسعت هذه الشبكة في سنة 1986 لتشمل الكثير من الجامعات والمعاهد والمجالات التجارية، وأصبحت تتميز بأنها شبكة حرة ليس لها حدود أو نطاق معين ومستقلة لا تخضع لأي دولة ويمكن استخدامها في أي وقت، وهذا الأمر الذي جعل شبكة الأنترنت متاحة للجميع، ومع تطورها عرفت نهضة في عدة مجالات كالاقتصاد والثقافة والمجال العلمي، وقد اختصرت هذه التقنية المسافات وأزالت الحدود بين الدولة والشعوب، وأصبح العالم عبارة عن قرية صغيرة في هذا الفضاء، واختصرت الجهد على الإنسان، وقد حلت هذه التقنية محل النشاط الذهني للإنسان، وهو ما جعلها تنعكس إيجابا على الحياة المعاصرة للإنسان لتوفيرها له الوقت والتكلفة والجهد وسهلت حياته، الأمر الذي جعل الطلب على هذه التقنية يزداد، وكذا توسع ميادين استعمالها وأصبح من الصعب الاستغناء عنها.

بالرغم من المزايا التي جاءت بها تقنية المعلومات، إلا أن تزايد استخدامها أدى إلى ظهور بعض الجوانب السلبية، وذلك لإساءة استخدامها واستغلالها، مما جعلها تشكل خطرا على أمن واستقرار المجتمع والإضرار بمصلحة الأفراد، وهذا ما أدى إلى ظهور نوع جديد من الجرائم والمعروفة بالجرائم المعلوماتية، والتي تعتبر من الجرائم المنظمة، وهي من أعقد الجرائم وهذا راجع للأساليب الحديثة التي تستخدم في ارتكابها وحداثة أركانها، وأيضا البيئة التي تقع فيها.

ولقد تطورت الجريمة في الآونة الأخيرة تطورا كبيرا، سواء من خلال الأشخاص مرتكبي الجريمة، أو الوسائل والأساليب المستعملة في ارتكابها، حيث أصبحت تمس المعلومات التي تصل بين الحسابات الآلية في جميع أنحاء العالم، والتي تعتبر كمستودع أسرار للأشخاص سواء أسرارهم الخاصة أو أموالهم أو نشاطاتهم.

لارتكاب هذه الجريمة يستخدم المجرم المعلوماتي مجموعة من الأدوات، والتي لا حصر لها حيث توجد أدوات عديدة تمكن المجرم المعلوماتي من ارتكاب جريمته، إذ نجد من بين الأدوات التي يستعملها الحاسوب وملحقاته وبرامجه، والذي يعتبر الأداة الأولى للجرائم الإلكترونية نظرا لانتشاره الواسع بين الناس وسهولة استعماله، وكذلك الاحترافية التي اكتسبها بعض الناس والتي أصبحت تزداد مع مرور الأيام.

كما نجد أيضا البريد الإلكتروني وهو الأداة التي يكون استعمالها شخصيا، والذي من خلاله يتم تبادل الرسائل، والذي استغله المجرم المعلوماتي ليرسل بواسطته فيروسات من أجل نسخ البيانات، أو تدميرها أو لترويج الأكاذيب والشائعات، وأيضا يوجد الهاتف النقال أو المحمول، والذي مع تطوره يمكن من خلاله تصفح شبكة الأنترنت والتصوير وأصبح أداة لارتكاب العديد من الجرائم الإلكترونية كالتشهير باستخدام الصور والفيديوهات.

من بين الأدوات المستعملة أيضا في الجريمة المعلوماتية نجد كذلك الشبكات المحلية والعالمية، ومن أبرزها شبكة الأنترنت، والتي تكون هدفا للجريمة حيث تعتبر مجالا خصبا لارتكاب مختلف أنواع الجرائم المعلوماتية، كالاعتداء على النظام المعلوماتي، والمساس بحرمة الحياة الخاصة.

إن الجريمة المعلوماتية أصبحت من أكثر الجرائم خطورتا وارتكابا نظرا للتطور التكنولوجي الحاصل في العالم، مما تطلب تظافر الجهود التشريعية والأمنية للحيلولة دون تفاقم هذه الظاهرة التي أصبحت تهدد الأفراد والدول.

من أجل ذلك قمنا بطرح الإشكال التالي:

ما أهم السبل التي اتبعها المشرع الوطني والدولي لمواجهة الجريمة المعلوماتية؟

ولدعم الإشكالية الرئيسية أثرنا مجموعة من الأسئلة الفرعية:

- ما لمقصود بالجريمة المعلوماتية وماهي أهم الدوافع التي تؤدي إلى ارتكابها؟

وماهي الخصائص التي تميز الجريمة المعلوماتية وأنواعها؟

- هل استطاع المشرع الجزائري مواكبة تطور مواجهة الجريمة المعلوماتية تشريعيا وقضائيا؟

وهل استطاع المشرع الأممي تبني سياسة وقائية وردعية اتجاه هذه الظاهرة المستحدثة تشريعيا وأمنيا؟

تكمن أهمية دراسة هذا الموضوع في كونه من الجرائم المستحدثة، والأكثر انتشارا وعدم مواكبة جل التشريعات للتطورات من أجل ردع هذه الجرائم بشكل قطعي، والبحث عن الحل الملائم للتعامل مع هذه الجريمة، وتبيان النصوص القانونية التي تجرم هذا الفعل، وتحديد الإجراءات الجديدة لمتابعة هذه الجريمة، وتكمن أهميته أيضا في أنه موضوع واسع يحتاج للتوضيح أكثر، وشرح وتحديد المفاهيم القانونية المرتبطة بهذه الجريمة.

أما بالنسبة للدوافع التي أدت بنا إلى اختيار هذا الموضوع، تتمثل في الرغبة في الإلمام بهذا الموضوع ومعرفة القوانين المنظمة لهذه الجريمة، والأسباب التي تؤدي إلى ارتكابها، وأيضا المؤسسات التي أقرها المشرع الجزائري والتشريع الدولي لمواجهة هذه الجريمة.

بالإضافة إلى الهدف البيداغوجي الخاص بنا كطلبة للحصول على شهادة التخرج أردنا التعرف من خلال هذا الموضوع على أهم الدوافع التي تؤدي بارتكاب هذه الجريمة وتبيان السبل التي اتبعها المشرع لمواجهتها، وكذلك لكونها من الجرائم المستحدثة والأكثر انتشارا في الآونة الأخيرة وكثرة استخدام شبكة الأنترنت وتكنولوجيا الإعلام والاتصال من قبل الأفراد.

من أبرز الصعوبات التي واجهتنا هي تشعب هذا الموضوع وكثرة العناوين، واتساع مجاله، فكلما تناولنا فكرة منه إلا بقي ما يحتاج للتوضيح، بالإضافة إلى تكبد عناء التنقل لاقتناء بعض المراجع لمسافات بعيدة.

وللإحاطة بأهم الجوانب المرتبطة بهذا الموضوع اعتمدنا على المنهج الوصفي، وذلك من خلال تحديد المفاهيم المتعلقة بعناصر البحث، ووصفها بشكل يساعد على توضيح وتبسيط الدراسة، وأيضا الاعتماد على المنهج الإستقرائي التحليلي من خلال تحليل بعض النصوص القانونية.

ومن أجل معالجة الإشكالية المطروحة قمنا بتقسيم هذا العمل إلى فصلين، حيث تطرقنا في **(الفصل الأول)** إلى الإطار المفاهيمي للجريمة المعلوماتية، أما **(الفصل الثاني)** فتطرقنا فيه إلى مكافحتها الوطني والدولي.

نظرا لتفاقم عدد هذه الجرائم واستفحالها والحيز الواسع الذي أصبحت تشغله مما جعلها محط اهتمام الأساتذة والباحثين وقد وجدنا بعض الدراسات السابقة:

- كتاب الجرائم الإلكترونية للأستاذ حسين طاهري والذي بين من خلاله ماهية الجريمة المعلوماتية وخصائصها وسبل مكافحتها على المستوى الوطني والدولي.
- كتاب الآليات القانونية لمكافحة الجريمة الإلكترونية لدكتوراه شنتير خضرة والذي جاء فيه تعريف للجريمة المعلوماتية وأهم خصائصها وبين المؤسسات التي أنشأها المشرع الجزائري والدولي لمواجهة هذه الجريمة.
- أطروحة الدكتوراه تحت عنوان التحقيق الجنائي في الجرائم الإلكترونية للطالب براهيمي جمال، والتي يبين من خلالها الإجراءات المتبعة في التحقيق في الجرائم المعلوماتية وبين الصعوبات التي تعيق المحققين للكشف عنها واقتراح الحلول لتفادي هذه العراقيل.
- رسالة الماجستير تحت عنوان الجريمة المرتكبة عبر الأنترنت للطالب صغير يوسف، حيث بين أنواع هذه الجريمة وسبل مكافحتها، وحدد صعوبات مواجهتها.

الفصل الأول

الإطار المفاهيمي للجريمة المعلوماتية

أدى التطور التكنولوجي وظهور شبكة الأنترنت إلى حدوث نقلة نوعية في حياة الإنسان وجاء بالعديد من المحاسن، والمتمثلة في اختصار المسافات وحسن استغلال الوقت، وتخفيف التكاليف والأعباء وتسهيل نقل المعرفة وسرعة الاتصال مع أي مكان في العالم، مما جعل هذه الشبكة من الأمور الضرورية في حياة الإنسان لكونها تسهل عليه أعماله وتختصر عليه بعد المسافات وعناء التنقل.

بالرغم من الفوائد الكبيرة للأنترنت والمزايا التي جاءت بها، إلا أن هذا لم يمنع من إساءة استخدامها من طرف بعض الأشخاص، والذين استغلوا شبكة الأنترنت والوسائل التكنولوجية الحديثة لارتكاب بعض الجرائم وممارسة بعض الأفعال غير المشروعة من خلال هذه الشبكة والوسائل التكنولوجية، حيث ظهرت ما يعرف بالجريمة المعلوماتية والتي عرفت تطورا كبيرا في مختلف الدول والمجتمعات، إذ تعتبر هذه الجريمة من الجرائم المستحدثة أو ما يعرف بجرائم الجيل الرابع، والتي أصبحت تشكل خطرا على الفرد والمجتمع وأمن الدولة وحتى الأمن والسلم الدوليين، الأمر الذي دفع الفقهاء ومختلف تشريعات الدول والهيئات الدولية إلى دراسة هذا النوع من الجرائم الحديثة، وتحديد تعريف لها، وكذلك تحديد أركانها ومعرفة خصائص هذه الجريمة وأهم أنواعها، وهذا ما سنتناوله في هذا الفصل، حيث قسمنا هذا الفصل إلى مبحثين فخصصنا **(المبحث الأول)** لتحديد ماهية الجريمة المعلوماتية وتبيان أركانها، أما في **(المبحث الثاني)** فخصصناه لتطرق لأهم الخصائص التي تميز الجريمة المعلوماتية والمجرم المعلوماتي وأنواع الجريمة المعلوماتية.

المبحث الأول: ماهية الجريمة المعلوماتية

سعى العديد من الفقهاء والتشريعات الدولية إلى تحديد تعريف للجريمة المعلوماتية وتحديد طبيعتها القانونية، حيث حاول العديد من الفقهاء تقديم تعريف لهذه الجريمة، وكذلك عرفت هذه الجريمة من خلال بعض الاتفاقيات والمعاهدات الدولية، وهذا ما سنتطرق إليه في بحثنا هذا حيث خصصنا **(المطلب الأول)** لتحديد مفهوم الجريمة المعلوماتية فقمنا بتحديد التعريف اللغوي والاصطلاحي، وأيضا التعريف الفقهي وتبيان تعاريف بعض القوانين لها، أما **(المطلب الثاني)** فقمنا بتحديد فيه أهم الدوافع التي تؤدي إلى ارتكاب الجريمة المعلوماتية.

المطلب الأول: مفهوم الجريمة المعلوماتية وأركانها

تعد الجريمة المعلوماتية ظاهرة إجرامية جديدة بحيث يستخدم فيها المجرمون الأذكياء أدوات المعرفة التقنية للقيام بأعمال إجرامية، وتركز هذه الجريمة على المعلومات التي تكون مخزنة ومنقولة عبر الشبكات ونظم المعلوماتية مما يؤثر على الحياة الخاصة للأفراد والأمن الوطني، وأيضا تسبب في تأثير سلبي على التكنولوجيا.

وتمثل نوعا خاصا من الجرائم التي تتطلب فهما عميقا لتقنيات الحوسبة وأنظمة المعلومات ويستلزم المتابعة للأشخاص الذين ارتكبوا تلك الجرائم، كما يمكن وصفها بأنها الجريمة التي يتم ارتكابها إذا قام شخص ما باستخدام معرفته بنظم المعلومات بعمل غير قانوني، وهناك من عرفها بأنها أي عمل غير قانوني يستخدم فيه الحاسب كأداة أو موضوع للجريمة، وترتكب بواسطة الحاسب الألي أو شبكة الأنترنت.[1]

وبالتالي فالجريمة المعلوماتية من الجرائم التي تواجهها مجتمعاتنا اليوم ومن التحديات الأمنية خصوصا باستعمال تقنية المعلومات، والاتصالات وتأثيرها على مؤسسات القطاع العام والخاص، وكذا تأثيرها على الأفراد.

---

[1] محمد سعيد عبد المجيد، المعلوماتية والجريمة تحليل مضمون لبعض الجرائم الإلكترونية، دار مكتبة الإسراء، ط الأولى، مصر، 2006، ص 13.

وعليه فإن المشكلة الأولى والأساسية التي تعترض ظاهرة الجريمة المعلوماتية هي عدم وجود تعريف موحد ومجمع عليه لهذه الجريمة.[1]

عليه سنبين في هذا المطلب في **(فرعه الأول)** مختلف التعريفات اللغوية والاصطلاحية وأيضا التعريفات التي جاء بها الفقهاء لهذه الجريمة، اما **(الفرع الثاني)** فسوف نخصصه لمعرفة أركان الجريمة المعلوماتية.

الفرع الأول: مفهوم الجريمة المعلوماتية

تتميز الجريمة المعلوماتية عن غيرها من الجرائم بطبيعة خاصة، ونظرا لهذه الطبيعة تعددت التعريفات المقدمة لهذه الجريمة، حيث عرفها العديد من الفقهاء كما عرفت أيضا من خلال القوانين التي سنتها الدول بخصوص هذه الجريمة، وأعطت كذلك المنظمات الدولية تعريفات لها، وهذا ما سنخصصه في هذا الفرع حيث سنبين من خلاله التعريف اللغوي والاصطلاحي والقانوني لهذه الجريمة وللمصطلحات المرتبطة بها وأيضا تعريفات الفقهاء لها في (البند الأول)، أما (البند الثاني) فسنتطرق إلى التعريف القانوني وتعريف المنظمات الدولية لها.

البند الأول: التعريف اللغوي والاصطلاحي للجريمة المعلوماتية

قبل تقديم تعريف للجريمة المعلوماتية وجب تعريف المصطلحات المرتبط بها حيث سنعرف كل من الجريمة، ثم نعرف مصطلح المعلوماتية لنتطرق بعدها لتعريف الجريمة المعلوماتية.

أولا: تعريف الجريمة المعلوماتية لغة واصطلاحا

تعددت التعريفات للجريمة المعلوماتية حيث سنتطرق من خلال هذا العنوان إلى تعريفها لغة وإصطلاحا

[1] نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي، ط الأولى، لبنان، 2005، ص27.

1-لغة

هي مجوعة العناصر المتداخلة المؤثرة في طبيعة الأفعال الإجرامية المرتكبة والمرتبطة ارتباطا وثيقا بالحاسب الألي والمعلوماتية، وبالتالي فإنه من الصعب تخيل وجودها دون ارتباطها بالحاسوب.[1]

وكذلك يمكن تعريفها بأنها "تلك الجريمة التي يتم فيها استعمال الآليات والأسلحة الإلكترونية بالهجوم الإلكتروني من أجل تحقيق مكاسب مالية بالأساس".[2]

تعددت المصطلحات اللغوية المرتبطة بالجريمة المعلوماتية مثل الجرائم المعلوماتية les crimes de informatique، وجرائم التقنية العالية les crimes de la haute technologies وجرائم الهاكرز les crimes de hacker السبر كرايمر la cyber criminalité وجرائم الإنترنت les crimes d'internet كل هذه التسميات تدل على الجرائم المعلوماتية المرتكبة إما في بيئة معلوماتية وتكون محددة أو عبر الشبكات المعلوماتية.[3]

2- اصطلاحا

يطلق عليها اصطلاحا "جرائم التكنولوجيا الحديثة" فهي جرائم تكنولوجية باعتبارها مرتبطة ارتباطا بشكل قوي وأساسي بالتكنولوجيا والتي تعتمد أساسا على الحواسيب والتقنيات الحديثة التي قد تظهر في المستقبل، وهي من الجرائم الحديثة نسبيا نظرا لحداثتها حيث ترتبط بالتقنيات الحديثة من الأجهزة والتي تتميز بطاقة تخزينية هائلة وتميزها بالسرعة الفائقة والمرونة في التشغيل.[4]

---

[1] محمد على سكيكر، المرجع السابق، ص 26.

[2] طاهر ياكر، مكافحة الجرائم الإلكترونية بين التشريعات الوطنية والاتفاقيات الدولية، مجلة الصدى للدراسات القانونية، مجلد4، العدد 04، جامعة خميس مليانة، 2022، ص03.

[3] كتاف الرزقي وبونهاك مصطفى، الجريمة الإلكترونية في المدينة الجزائرية، مجلة العلوم الاجتماعية، العدد 01، برلين،2017 ص 333.

[4] نهلة عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة، ط. الثانية، عمان. الأردن، 2008، ص 47.

ويطلق عليها في سياق آخر "كل سلوك أو إجراء ذو طابع غير قانوني الذي يتم من خلاله استخدام الأجهزة الرقمية وتقنياتها والبرامج من أجل كسب فوائد معنوية ومادية لتحقيق أهداف بطريقة غير مشروعة، مثل السرقة والقرصنة واستغلال المعلومات، ويكون له تأثير سلبي.[1]

البند الثاني: تعريفات التشريعات والمنظمات الدولية والفقهاء للجريمة المعلوماتية

لقد عرفت العديد من التشريعات الجريمة المعلوماتية من خلال النصوص القانونية المتعلقة بها كما عرفتها أيضا المنظمات الدولية وهذا ما سنبينه من خلال هذا البند.

أولا: تعريف التشريعات للجريمة المعلوماتية

1-التشريع الجزائري

لقد أطلق المشرع الجزائري تسمية الجرائم المتصلة بتكنولوجيات الإعلام والاتصال على الجريمة المعلوماتية، حيث عرفها في المادة الثانية من القانون رقم 09 – 04 المؤرخ في 05-08-2009 بأنها "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية".[2]

2-**التشريع السعودي**

تم إنشاء نظام مكافحة جرائم المعلومات في المملكة السعودية بموجب المرسوم الملكي رقم م/ 17 الصادر بتاريخ 3/8/ 1428 هـ جاء ذلك بناء على قرار مجلس الوزراء رقم: 79 الصادر بتاريخ 7 / 3 / 1428 هـ، حيث عرف هذا النظام الجرائم المعلوماتية في الفقرة 8 من

[1] ريم علي الرابغي، شهد عبد الرحمان الصبحى، مدى وعي طلبة الدراسات العليا بنظام مكافحة الجرائم المعلوماتية في ظل التحول الرقمي، المجلة العربية للنشر العلمي، العدد 40، 2022، ص 780.

[2] المادة 02 من القانون رقم 09 – 04 مؤرخ في أوت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر.ج.ج، العدد 47.

المادة الأولى بأنها " أي فعل يرتكب متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية، بالمخالفة لأحكام هذا النظام".[1]

3-التشريع القطري

نص المشرع القطري على الجريمة الإلكترونية من خلال القانون رقم 14 لسنة 2014 المتعلق بإصدار قانون مكافحة الجرائم الإلكترونية، حيث قدم في الباب الأول منه تعريف للجريمة المعلوماتية وبعض المصطلحات المرتبطة بها، إذ عرف الجريمة الإلكترونية في المادة الأولى منه على أنها "أي فعل ينطوي على استخدام وسيلة تقنية المعلومات أو نظام معلوماتي أو الشبكة المعلوماتية بطريقة غير مشروعة بما يخالف أحكام القانون"، كما عرف أيضا النظام المعلوماتي على أنه "مجموعة البرامج وأجهزة تستخدم لإنشاء أو استخراج المعلومات أو أرسالها أو استلامها أو عرضها أو معالجتها أو تخزينها"، وعرف كذلك من خلال نفس المادة البرنامج المعلوماتي على أنه "مجموعة البيانات أو الأوامر القابلة للتنفيذ باستخدام وسيلة تقنية المعلومات والمعدة لإنجاز مهمة ما.[2]

4-التشريع السوري

عرف المشرع السوري الجريمة المعلوماتية من خلال المرسوم التشريعي رقم 17 لسنة 2012 المتضمن تطبيق أحكام قانون التواصل على الشبكة ومكافحة الجريمة المعلوماتية "بأنها "هي جريمة ترتكب باستخدام الأجهزة الحاسوبية أو الشبكة أو تقع على المنظومة المعلوماتية أو الشبكة"، كما عرف المشرع السوري من خلال هذا المرسوم التشريعي العديد من المصطلحات المرتبطة بهذه الجريمة، حيث عرف مصطلح المنظومة المعلوماتية على أنها مجموعة متسقة من الأجهزة والبرمجيات الحاسوبية الملحقة بها، كما عرف أيضا التوقيع الإلكتروني على أنه "منظومة معلوماتية لها اسم أو عنوان يعرفها وتتضمن معلومات أو خدمات يمكن الوصول إليها

[1] المادة 08/01، المرسوم الملكي رقم م 17، المتضمن نظام مكافحة الجرائم المعلوماتية، الصادر بتاريخ 08-03-1428 هـ الموافق ل 27-03-2007، بموجب قرار مجلس الوزراء رقم 79 الصادر في 07-03-1428 هـ.

[2] المادة 01، من القانون رقم 14 بإصدار قانون مكافحة الجرائم الإلكترونية، قطر 2014.

عن طريق الشبكة وخاصة الأنترنت، وعرف أيضا مصطلح البرمجيات الخبيثة بأنها برمجيات حاسوبية مصممة لإلحاق الضرر بالأجهزة الحاسوبية أو المنظومات المعلوماتية أو المواقع الإلكترونية أو الشبكة أو تعطيل عملها أو تبطئه أو تخريب مواردها ومحتوياتها أو جمع معلومات عنها وعن بياناتهم دون إذنهم أو إتاحة الدخول إليها أو استخدام مواردها بصورة غير مشروعة.[1]

5-التشريع الكويتي

عرف المشرع الكويتي الجريمة المعلوماتية بموجب القانون رقم 63 لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات، وذلك من خلال نص المادة الأولى منه والتي عرف فيها أيضا العديد من المصطلحات المرتبطة بهذه الجريمة، حيث عرف الجريمة المعلوماتية على أنها "كل فعل يرتكب من خلال استخدام الحاسب الآلي أو الشبكة المعلوماتية أو غير ذلك من وسائل تقنية المعلومات بالمخالفة لأحكام هذا القانون"، كما عرف أيضا الاحتيال الإلكتروني على أنه "التأثير في نظام الكتروني مؤقت أو نظام معلوماتي الكتروني أو شبكة معلوماتية أو مستند أوسجل إلكتروني أو وسيلة تقنية معلوماتية أو نظام أو جهاز حاسب آلي وذلك عن طريق البرمجة أو الحصول أو لإفصاح أو النقل أو النشر لرقم أو كلمة او رمز سري بقصد الحصول على منفعة دون وجه حق أو الإضرار بالغير، كما عرف أيضا البيانات الإلكترونية على أنها "بيانات ذات خصائص إلكترونية في شكل منصوص أو رموز أو أصوات أو رسوم أو صور أوبرامج حاسب آلي وقواعد البيانات.[2]

6-التشريع البحريني

قام المشرع البحريني بتعريفها على أساس عدة أفعال منها "أنها نسخ أو حيازة أو إعادة تكوين أداة إنشاء توقيع إلكتروني لشخص آخر أو الدخول على أداة إنشاء هذا التوقيع دون

[1] المادة 02، من المرسوم التشريعي رقم 17، المتضمن تطبيق أحكام قانون التواصل على الشبكة ومكافحة الجريمة المعلوماتية، المؤرخ في 2012/02/08 سوريا.

[2] المادة 01، من القانون رقم 63 في شأن مكافحة جرائم تقنية المعلومات، الكويت 2015.

تفويض بذلك من هذا الشخص وبسوء نية "كذلك انتحال هوية شخص آخر أو الادعاء زورا بأنه مفوض من قبله في طلب الحصول على شهادة أو قبولها أو طلب تعليق العمل بها أوإلغائها".

إضافة إلى نشر شهادة أو وضعها في متناول أي شخص يحتمل أن يعتمد عليها أوعلى توقيع إلكتروني وارد بها، من خلال البينات المدرجة بهذه الشهادة كالرموز وكلمات السر أومفاتيح التشفير العامة.

وعليه يتمثل مدلول الجريمة المعلوماتية عند المشرع البحريني على أنه يتم فيها استخدام وسائل كهربائية أو مغناطيسية أو كهرومغناطيسية بالاستخدام السلبي أو غير المفوض لتلك الوسائل في سياق غير قانوني.[1]

7-التشريع المصري

لم يقدم المشرع المصري تعريف للجريمة المعلوماتية من خلال القانون رقم 175 لسنة 2018 وإنما تناول بعص صورها وتتمثل الصورة الأولى في الاعتداء على سلامة شبكة وأنظمة وتقنيات المعلومات كجريمة الانتفاع بخدمات الاتصالات والمعلومات دون وجه حق وكذلك جريمة الدخول غير المشروع وجريمة تجاوز حدود الحق وجريمة الاعتراض غير المشروع والاعتداء على البريد الإلكتروني، اما الصورة الثانية فتتمثل في الجرائم المرتكبة بواسطة أنظمة وتقنية المعلومات كجرائم الاحتيال والاعتداء على بطاقات البنوك وأدوات الدفع الإلكتروني، كما تتمثل الصورة الثالثة في الجرائم المتعلقة بالاعتداء على حرمة الحياة الخاصة والمحتوى المعلوماتي غير المشروع.

8-التشريع العراقي

لم يقدم التشريع العراقي من خلال قانون العقوبات رقم 111 لسنة 1969 تعريف جامع للجريمة المعلوماتية وهذا راجع لصدوره قبل بروز هذه الجريمة، بحيث لم تكن هناك جرائم

[1] محمد حماد مرهج الهيتي، الجريمة المعلوماتية دراسة مقارنة، دار الكتب القانونية، مصر- الإمارات، 2014، ص 217.

معلوماتية في تلك السنوات وهذا ما دفع بالسلطة التشريعية في العراق بالمحاولة في سن قانون خاص بهذه الجريمة من أجل مواكبة التطورات في هذا المجال.[1]

9-التشريع التونسي

يعرف التشريع التونسي الجريمة الإلكترونية بناء على المادة الأولى من الفصل الخامس من مرسوم مكافحة الجرائم الإلكترونية رقم 54 لسنة 2022، بأنها "كل فعل مخالف للقانون ويتم باستخدام نظام معلومات أو شبكة اتصال، ويهدف إلى إلحاق الضرر بنظام معلومات أوشبكة اتصال أو بيانات مخزنة أو معالجة فيهما، أو الحصول على هذه البيانات أو إفشائها أوإعاقة عمل نظام معلومات أو شبكة اتصال، أو الإضرار بسمعة شخص أو الاعتداء على حياته الخاصة.[2]

10- التشريع الليبي

حدد التشريع الليبي تعريف الجريمة الإلكترونية من خلال المادة الأولى في الفقرة الأولى منال القانون رقم 5 لسنة 2022 بشأن مكافحة الجرائم الإلكترونية بأنها " كل فعل يرتكب من خلال استخدام أنظمة الحاسب الآلي أو شبكة المعلومات الدولية أو غير ذلك من وسائل تقنية المعلومات بالمخالفة لأحكام هذا القانون".[3]

11- التشريع الأمريكي

عرفها التشريع الأمريكي من خلال القانون رقم 1213 لسنة 1986 لمواجهة الجرائم الإلكترونية، بأنها الاستخدام المصرح به لأنظمة الكمبيوتر المحمية أو ملفات أو بيانات

[1] عماد جاسم محمد حسين الشنكالي، دور الضبط الإداري الإلكتروني في مكافحة الجرائم المعلوماتية، رسالة ماجستير، جامعة تكريت العراق، 2022، ص 14-40.

[2] المادة 01، من مرسوم عدد 54 يتعلق بمكافحة الجرائم المتصلة بأنظمة المعلومات ولاتصال، المؤرخ في 13 سبتمبر 2022، تونس.

[3] المادة 01، من قانون رقم 5 بشأن مكافحة الجرائم الإلكترونية، المؤرخ في 27 سبتمبر 2022، ليبيا.

أو الاستخدام المتعمد الضار لأجهزة الكمبيوتر أو ملفات البيانات، وتتراوح خطورة تلك الجريمة ما بين جنحة من الدرجة الثانية إلى جناية من الدرجة الثالثة[1].

ثانيا: تعريف الجريمة المعلوماتية في إطار المنظمات الدولية

قدمت المنظمات الدولية تعريفا للجريمة المعلوماتية وتتمثل هذه التعريفات فيمايلي:

1-منظمة التعاون الاقتصادي والتنمية

عرفتها منظمة التعاون الاقتصادي والتنمية الجريمة المعلوماتية بأنها " كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها"، وقد تم وضع هذا التعريف من قبل مجموعة الخبراء خلال اجتماع باريس الذي عقد في عام 1983 ضمن حلقة (الإجرام المرتبط بتقنية المعلومات).[2]

2-اتفاقيات الأمم المتحدة

جاء في توصيات مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين الذي عقد في فيينا 2000، تعريف الجريمة الإلكترونية أو جريمة الحواسيب بأنها "أي جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوبي"، وهي تلك الجريمة التي تشمل من الناحية المبدئية على جميع الجرائم التي يمكن ارتكابها في البيئة إلكترونية.[3]

3-اتفاقية مجلس أوربا للجريمة الإلكترونية لعام 2001

تم توقيع اتفاقية مجلس أوربا في 22 نوفمبر 2001 في بودابست ويتكون أعضائها من 45 دولة أوربية و 17 دولة من خارج أوربا حتى تاريخ 2014/10/05 وعرفت الاتفاقية الجريمة المعلوماتية في المواد من 02 إلى 12 بأنها "جرائم الحاسب الآلي في الفصل الثاني فهي جرائم

---

[1] محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، دار النهضة العربية، ط 2009، القاهرة، ص 37.

[2] سمير شعبان، الجريمة الإلكترونية مقارنة تحليلية لتحديد مفهوم الجريمة والمجرم، دراسات وأبحاث، مجلد 2009، العدد 01، الجلفة الجزائر، ص 118.

[3] بوضياف إسمهان، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد 11، سنة 2018 , ص 352.

ضد السرية والنزاهة وتوافر البيانات وأنظمة الحاسب الآلي، والدخول غير المشروع والاعتراض غير القانوني والتدخل في البيانات والتدخل في النظام وإساءة استخدام الأجهزة، وأكد المجلس الأوروبي في تقريره عن الجرائم المتعلقة بالحواسيب أن أي تغيير في بيانات أو المعطيات أو حتى برامج الحاسوب أو محوها أو كتابتها أو أي تدخل أخر في مجال إنجاز البيانات أو معالجتها، وتبعا لذلك تسببت هذه الجرائم في خلق ضرر اقتصادي أو فقدان حيازة ملكية شخص أخر، أو بهدف الحصول على كسب اقتصادي غير مشروع له او لفاعل أخر.[1]

ثالثا: تعريف الجريمة المعلوماتية في الفقه

تعددت تعريفات الجريمة المعلوماتية حيث سعى أغلب الفقهاء إلى تقديم تعريف لها، وهذا ما سنتطرق إليه من خلال هذا العنوان.

عرفها بعض الفقه بأنها "نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة وغير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود".

ولقد عرفها البعض بأنها " الاستخدام غير المصرح به لأنظمة الكومبيوتر المحمية أو ملفات البيانات أو الاستخدام المتعمد الضار لأجهزة الكومبيوتر أو ملفات البيانات".

ويرى البعض أنها" أنماط مستحدثة من السلوك الإجرامي يرتبط بالتقنيات الإلكترونية الحديثة التي صارت محلا لهذه الجريمة أو وسيلة لارتكابها".[2]

كما عرف الفقيه Tiedemann الجريمة الإلكترونية على أنها " تشمل كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب".

---

[1] سعيد بن سالم البادي وزايد بن حمد الجنيبي ويوسف الشيخ يوسف حمزة وأحمد العطاء، مجمع البحوث والدراسات أكاديمية السلطان قابوس، الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، مجلس التعاون لدول الخليج العربية، سلطنة عمان سنة 2010، ص 24.

[2] بهاء المرى، جرائم المحمول والأنترنت، دار الهدى ط أولى، الإسكندرية مصر، 2018، ص 02.

ويرى الفقيهان " Richard totty and Anthony تلك الجرائم التي يكون قد وقع في مراحل ارتكابها بعض العمليات الفعلية داخل نظام الحاسب. [1]

يعرف hestanc وvivant الجريمة المعلوماتية أنها "مجموعة من الأفعال المرتبطة بالمعلوماتية التي يمكن أن تكون جديرة بالعقاب". [2]

ترى الدكتورة "غنية باطلي" أن استعمال مصطلح الجريمة الإلكترونية من شأنه أن يدخل في مفهومها جرائم الحاسوب وغيرها من الجرائم التي يسميها البعض بالجرائم المعلوماتية والغش المعلوماتي أو جرائم الاعتداء على معطيات الحاسب الآلي وجرائم الإنترنت.[3]

يعرفها الفقيه Masse بأنها "الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح" أو هي "كل سلوك غير مشروع يتعلق بالمعلومات المعالجة ونقلها".[4]

ذهب خبراء مختصون من بلجيكا إلى أن جريمة الكومبيوتر هي كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية ويهدف إلى الاعتداء على الأموال المادية أو المعنوية.[5]

عرفها " david tnompasoبأنها أي جريمة تتطلب من فاعلها المعرفة بتقنية الحاسب الآلي".

يرى " Miche Cerdoأنها من أسوء استخدامات الحاسب الآلي وتتمثل في استخدامه كأداة لارتكاب الجريمة، بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسب

---

[1] مريفت محمد حباية، مكافحة الجريمة الإلكترونية دراسة مقارنةفي التشريع الفلسطيني والجزائري، دار البازوزي العلمية، فلسطين، 2022، ص 30-31.

[2] محمود دين، الجريمة الإلكترونية وتحديات الأمن القومي، دار الكتب المصرية ط الثانية، مصر، 2019، ص 26.

[3] رمضاني فاطمة وبدراني علي، القصور التشريعي الجنائي في مجال الجريمة المعلوماتية في التشريعين المغربي والجزائري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 07، العدد 01، 2022، ص 860.

[4] عادل يوسف عبد النبي شكري، الجريمة المعلوماتية وأزمة الشرعية الجزائية، مجلة مركز الدراسات الكوفة، العدد 07، جامعة الكوفة، 2008، ص 133.

[5] محمد كمال محمود الدسوقي، الحماية الجنائية لسرية المعلومات الإلكترونية، دار الفكر والقانون، ط اولى، مصر، 2010، ص 15.

المجني عليه أو بياناته، كما أنه تمتد جريمة الحاسوب لتشمل الاعتداءات المادية، سواء كان هذا الاعتداء على جهاز الحاسوب ذاته أو المعدات المتصلة به، وبذلك الاستخدام غير المشروع لبطاقات الائتمان وانتهاك ماكينات الحاسبات الآلية بما تتضمنه من شبكات تمويل الحاسبات المالية بطريقة إلكترونية وتزييف المكونات المادية والمعنوية للحاسب بل وسرقة جهاز الحاسب في حد ذاته أو مكون من مكوناته.[1]

يعرفها أيضا مهندي حسن طاهر داود بأنها "هي السلوك السيئ المتعمد الذي يستخدم نظم المعلومات لإتلاف المعلومات أو إساءة استخدامها مما يتسبب إما في إلحاق الضرر بالضحية أو حصول الجاني على فوائد لا يستحقها".

وحددها الدكتور هلالي عبد الإله أحمد "كل عمل أو امتناع يأتيه الإنسان إضرارا بمكونات الحاسب وشبكات الاتصال التي يحميها قانون العقوبات ويفرض لها عقابا".[2]

الدكتورة هدى قشقوش التي تناولت الجرائم المعلوماتية بأنها "جرائم الاعتداء على أموال المعلوماتية فهي عبارة عن الأدوات المكونة للحاسب الإلكتروني وبرامجه ومعداته".[3]

كما عرفها كل من الأستاذان روبرت ج. ليند كويست وجاك بولوقنا بأنها "هي الجريمة التي يستعمل فيها الحاسب الآلي كأداة لارتكابها أو يمثل إغراء بذلك أو يكون ضحيتها الكمبيوتر في حد ذاته.[4]

---

[1] محمود دين، المرجع السابق، ص 27.

[2] دريس بالمحجوب، تأثير الجريمة الإلكترونية على الائتمان المالي، سلسلة ندوات محكمة الاستئناف بالرباط، العدد 07، 2016، المغرب، ص 28.

[3] معاشي سميرة، دراسة تحليلية لمفهوم الجريمة المعلوماتية، مجلة المفكر، المجلد 13، العدد 17، جامعة بسكرة، 2008، ص 402.

[4] شنتير خضرة، الآليات القانونية لمكافحة الجريمة الإلكترونية، مؤسسة الكتاب القانوني، ط أولى، الجزائر، 2022، ص 15.

إن أي تعريف للجريمة المعلوماتية يجب أن يراعى فيه عدة نقاط مهمة وهي:

- يجب أن يكون التعريف مفهوما ومقبولا مع فكرة التواصل العالمي للمعلومات والاتصالات مما يجعله موافقا على مستوى العالم ويسهل الجهود الوطنية والدولية لمكافحة الجرائم المعلوماتية والتحقيق الدولي بينهم.
- يجب أن يراعى في هذا التعريف التطور المستمر للتكنولوجيا وملاحظة جميع الأشكال المتغيرة للجرائم المعلوماتية الناتجة عن التقدم والازدهار التكنولوجي.
- أن يشمل جميع الأشكال المختلفة للسلوك الإجرامي ابتداء من القتل إلى الاعتداء على حرمة الحياة الخاصة يتعين توضيح تعريف الجريمة المعلوماتية لبيان الدور الذي يقوم به الحاسب الآلي في ارتكاب الجريمة.[1]

تعتمد تعريفات الجرائم الإلكترونية في الغالب على الهدف من استعمال هذا المصطلح فتشمل الأعمال ضد النزاهة وتوافر بيانات الكمبيوتر أو الأنظمة وتكون أيضا ضد الجريمة السرية، ويقع ضمن المعنى الأوسع لمصطلح الجريمة المعلوماتية فتشمل الأعمال ذات الصلة بالحاسوب لأغراض شخصية أو من أجل تحقيق مكاسب مالية او إضرار يمس بحقوق الأشخاص ومنها الجرائم المتصلة بالهوية والأفعال المتعلقة بمحتويات الكمبيوتر.[2]

الفرع الثاني: أركان الجريمة المعلوماتية

على غرار الجريمة التقليدية تتكون الجريمة المعلوماتية هي الأخرى على مجموعة من الأركان وهي الركن الشرعي والركن المادي والركن المعنوي لكل صورة من صور هذه الجريمة.

[1] نائلة عادل محمد فريد قورة، المرجع السابق، ص 32.

[2] طاهر ياكر، الجرائم الإلكترونية، المرجع السابق، ص 18.

البند الأول: الركن الشرعي

طبقا لمبدأ الشرعية المنصوص عليه في نص المادة الأولى من الأمر 66-156 المعدل والمتمم والمتضمن قانون العقوبات التي تنص على أنه "لا جريمة ولا عقوبة أو تدبير أمن بغير قانون".[1]

كما قد أورد المشرع الجزائري مجموعة من الأفعال التي يشكل ارتكابها جريمة إلكترونية، وذلك من خلال الأمر 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة من خلال المادة 151 و152 منه وبين العقوبات المقررة لها من خلال نص المادة 153 من نفس القانون وكذا المواد من 154 إلى158.[2]

كما نجد أن قانون العقوبات قد تحدث على جرائم المساس بأنظمة المعالجة الآلية للمعطيات من خلال المادة 394 بقولها " ... كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك، "وكذلك في نص المادة 394 مكرر 01 بقولها "... كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريقة الغش المعطيات التي يتضمنها"، كما ذكر الشروع في هذه الجرائم من خلال نص المادة 394 مكرر 07 بقولها "يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها".[3]

كما أورد الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال من خلال القانون رقم 09-04 المؤرخ في 05 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، حيث جاء في نص المادة الثانية منه في الفقرة الأولى الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بقولها "جرائم تكنولوجيا الإعلام والاتصال جرائم المساس

---

[1] المادة 01، من القانون رقم 24-06، مؤرخ في 04/28/ 2024، المعدل والمتمم للأمر 66-155، المؤرخ في 8 يونيو 1966. ج. ر. ج. ج العدد 49.

[2] المادة 151 إلى 153، ق رقم 03-15، المؤرخ في 19 يوليو 2003 المتضمن قانون حقوق المؤلف والحقوق المجاورة، ج.ر. ج. ج، العدد 44.

[3] المادة 394 مكرر إلى 394 مكرر07، من ق. رقم 24-06، المصدر السابق.

بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات أو أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية"، كما نصت المادة 141 على الإساءة إلى رئيس الجمهورية بأي وسيلة إلكترونية وذلك بقولها " ... كل من أساء إلى رئيس الجمهورية بعبارة تتضمن الإهانة أو سبا أو قذفا سواء كان ذلك عن طريق الكتابة أو الرسم أو التصريح أو بأية ألية لبث الصوت أو الصورة أو بأية وسيلة إلكترونية أو معلوماتية أو إعلامية أخرى.[1]

البند الثاني: الركن المادي

يتمثل الركن المادي للجريمة في السلوك الإجرامي أي المظهر الخارجي للفعل والذي يشترطه القانون للعقاب على الجريمة وذلك بشرط تحقيق نتيجة ضارة للسلوك الإجرامي وحتى يكتمل الركن المادي للجريمة لابد من اكتمال عناصره الثلاث والمتمثلة في السلوك المادي والعلاقة السببية والنتيجة الإجرامية. [2]

يتجسد الركن المادي للجريمة المعلوماتية في تخريب المعلومات (المحو –التبديل – الإضافة) والإتلاف العمدي للمنقولات أو السرقة، سواء عن طريق استعمال بطاقات الائتمان أو التزوير أو الجوسسة.[3]

فالركن المادي للجريمة المعلوماتية هو عبارة عن الحركة الاختيارية للجاني، والتي ينتج على القيام بها تغيير في العالم الخارجي ويتخذ السلوك الإجرامي صورتين هما، السلوك الإيجابي وهو الذي يختلف باختلاف نوع الجريمة، حيث يكون في الجرائم البسيطة فعل واحد وعدة أفعال في الجرائم متعددة الأفعال، ويتمثل السلوك الإيجابي في القيام بفعل بكل إدراك وتمييز وحرية الاختيار بارتكاب أفعال يعاقب عليها القانون.

---

[1] المادة 02، من ق 09-04، المصدر السابق.

[2] طاهر ياكر، الجرائم الإلكترونية، المرجع السابق، ص 37.

[3] حسين طاهري، الجرائم الإلكترونية، دار الخلدونية، ط أولى، الجزائر، س 2022، ص 124.

والسلوك السلبي والمتمثل في الامتناع عن القيام بعمل أمر به القانون وبذلك يتخذ موقفا سلبيا لما أمر به القانون، وكان بإمكان الفاعل القيام به ويكون بشكل إرادي كالامتناع عن التبليغ عن الجناة.

بالنسبة للجرائم المعلوماتية يبدأ فيها الركن المادي بضغطة زر على لوحة المفاتيح أو على شاشة الحاسوب أو الهاتف النقال كانتحال شخص شخصية تاجر أو مستثمر والتعرف على أشخاص من خلال المواقع الإلكترونية بهدف الحصول على أموالهم.[1]

كما سبق وذكرنا فإن لكل صورة من صور الجرائم الإلكترونية أركان خاصة بها حيث سنذكر الركن المادي لبعض الصور وهي كالأتي:

اولا: الدخول والبقاء بالغش أو البقاء غير المرخص

يتمثل في الدخول الاحتيالي في نظام محمي أو غير محمي لمن لا حق له في الدخول، أما البقاء يكون أثناء الدخول الشرعي والبقاء أكثر من المدة المحددة بهدف عدم أداء إتاوة، وتعتبر جريمة حتى لو حصل الدخول مباشرة أو عن بعد، وحتى وإن كان الدخول بصفة عرضية يجرم البقاء.

أما المساس بمنظومة المعلومات، طبقا للمادة 394 مكرر 01 من قانون العقوبات التي تنص على أنه " ... كل من أدخل بطريق الغش معطيات في نظام المعالجة الألية أو زوال أو عدل بطريق الغش المعطيات التي يتضمنها"، من خلال نص المادة يتضح لنا أن هذا الفعل المجرم يتخذ صورتين هما:

- إدراج معطيات غريبة عن نظام المعالجة الألية.
- تخريب المعطيات التي يحتوي عليها نظام المعالجة الألية.[2]

[1] يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري، دار الجامعة الجديدة، ط 2019 مصر، ص 131-132.

[2] أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، ج الأول، النشر الجامعي، ط 2022، الجزائر، ص 488.

ثانيا: جريمة تخريب أو تعطيل نظام التشغيل

بالرغم من أن هذه الجريمة ترد لاحقة لجريمة الدخول بالغش إلا أنها مستقلة عنها، والطرق التي تتخذ في تخريب وتعطيل النظام متعددة منها تخريب الجهاز بالفيروس قنبلة منطقة تغيير في الرسم السري وينتج عنه توقف النظام كليا أو جزئيا، كما قد يكون هذا الفعل مستمرا أو دوريا، حيث يكون مستمرا كإتلاف برامج الدخول أو تفعيل عمل فيروس، كما يكون دوريا وذلك بالتشويش على النظام أو قنبلة منطقية تمس النظام في أزمنة محددة.

ثالثا: الركن المادي لجريمة المساس بسلامة المعطيات:

يتمثل الركن المادي لهذه الجريمة في تحقيق إحدى الصور الثلاث لسلوك الإجرامي وهي المحو– التعديل – الإدخال، حيث يكفي تحقق إحدى الصور الثلاث لتحقق الركن المادي للجريمة، ومن أفعال هذه الصور تنطوي على التلاعب بالمعطيات حيث تتبدل فيه الصورة الأصلية بسبب هده الأفعال ومهما كانت النية من القيام بهذه الأفعال حتى وإن كانت بقصد تحسين سرعته ونجاعته.[1]

البند الثالث: الركن المعنوي للجريمة المعلوماتية

يتمثل الركن المعنوي للجريمة المعلوماتية على الإرادة الإجرامية عند الفاعل على غرار الجرائم الأخرى، حيث يتخذ صورة القصد الجنائي أين يتحقق هذا الركن بعلم الجاني بأن الفعل يجرمه القانون وتتجه إرادته إلى ارتكاب هذا الفعل ومن خلال استقراء المواد 394 مكرر و394 مكرر01 و394 مكرر02 و394 مكرر05 من قانون العقوبات يتبين أن الجريمة المعلوماتية جريمة عمدية لا يفترض فيها عنصر الخطأ.[2]

إن الركن المعنوي في مختلف الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات يتخذ صورة القصد الجنائي ونية الغش، إذ تعتبر الجريمة المعلوماتية من الجرائم التقنية العالية

[1] حسين طاهري، المرجع السابق، ص 136–144.

[2] حمزة خضري وعشاش حمزة، خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري، مجلة الدراسات القانونية والسياسية، جامعة الأغواط الجزائر، المجلد السادس، العدد الثاني، جوان 2020، ص 174.

تتطلب من المجرم قدرا من المعرفة والتخصص، حيث لا يمكن تصور وقوعها إلا في صورة العمد لأن الجاني دبرها وخطط لها للحصول على المعلومات أو لاختراق شبكة الحاسوب أوالاعتداء على أنظمة المعالجة الآلية للمعطيات سواء بالإدخال أو المحو أو التعديل.[1]

كما يختلف الركن المعنوي من جريمة إلى أخرى، ففي جريمة الدخول غير المصرح به إلى نظام الحاسب الآلي تستوجب توفر قصدا جنائيا والمتمثل في العلم بأن الدخول إلى النظام بطريقة غير مصرح بها يعتبر جريمة، أما في جريمة الاحتيال الإلكتروني فيشترط فيها توافر القصد الجنائي العام والخاص إذ يكون المجرم يعلم بأن الفعل مجرم قانونا ويقوم بارتكابه مخالفا بذلك القانون واتجاه نيته إلى تحقيق ربح غير مشروع له أو للغير.[2]

أما في جريمة الدخول أو البقاء بالغش فلا يتوفر فيها الركن المعنوي إذا كان مسموح له الدخول في النظام أو البقاء فيه بمعنى أن هذا الفعل مشروع ولا يتوفر الركن المعنوي إذا أخطأ الجاني ودخل وكان يعتقد أنه مسموح له الدخول ويجهل بوجود حظر، أما إذا كان له العلم والإرادة وكان يقصد بارتكاب الجريمة رغبة في تحدي النظام والانتصار عليه والتفوق على وسائل الحماية أو حتى لمجرد الفضول أو التصفح والاطلاع واختراق نظم الحماية والأمن يعتبر قرينة قاطعة على توافر القصد الجنائي لدى الجاني حيث يوجد في هذه الأنظمة معلومات ذات اهمية والدخول إليها يعتبر أمرا خطيرا.

بالنسبة للركن المعنوي في جريمة تخريب أو تعطيل نظام التشغيل يتمثل في اتجاه إرادة الجاني في عرقلة وتعطيل أو فعل الإفساد والعلم أن فعله الإجرامي يؤدي إلى إفساد وتعطيل نظام المعالجة الآلية للمعطيات ويكون ذلك دون رضا صاحب الحق.

بالنسبة لجريمة المساس بسلامة المعطيات يقوم فيها الركن المعنوي على اتجاه إرادة الجاني إلى فعل الإدخال أو المحو أو التعديل، مع علم الجاني بأن فعله ينتج عليه التلاعب

[1] يزيد بوحليط، المرجع السابق، ص 134-135.

[2] حمزة خضري وعشاش حمزة، المرجع السابق، ص 175.

على المعطيات وأن ليس له الحق في القيام بذلك، وأنه يتعدى على صاحب الحق أو دون موافقته.[1]

وعليه تعتبر أغلب الجرائم المعلوماتية من الجرائم العمدية أي أنها ترتكب بشكل قصدي وهذا راجع لطبيعة هذه الجريمة، حيث أنها تتطلب معرفة كافية بالأجهزة الإلكترونية فهي في غالب الأحيان ترتكب من طرف شخص له إلمام بجميع الجوانب الفنية للجريمة، ويقوم بها للوصول لغايته والنتيجة المراد الوصول إليها.[2]

البند الرابع: الشروع في الجريمة المعلوماتية

نص المشرع الجزائري على الشروع من خلال المادة 30 من ق.ع في الفصل الثاني من الباب الأول من الكتاب الثاني وأطلق عليه اسم المحاولة، وعرفها على أنها كل محاولة لارتكاب جناية تكون بالشروع في التنفيذ أو القيام بأعمال تؤدي إلى ارتكاب الجريمة إذا لم يخب أثرها او توقف، أما إذا خاب أثرها نتيجة لظروف خارجة عن إرادة الشخص الذي يرتكبها، كما ورد في نص المادة 31 من نفس القانون على أنه "لا يعاقب على الشروع في مواد الجنح إلا بموجب نص صريح في القانون".[3]

من خلال ما تم ملاحظته في المادة 30 نلاحظ أن الشروع في التشريع الجزائري يقوم على ركنين هما البدء في التنفيذ وانعدام العدول الإرادي.[4]

بالنسبة للشروع في الجريمة المعلوماتية فقد نص المشرع الجزائري من خلال نص المادة 394 مكرر 07 على أنه يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في القسم السابع من نفس القانون بالعقوبات ذاتها المقررة للجنحة، فقد وسع المشرع في نطاق العقوبة في

---

[1] حسين طاهري، المرجع السابق، ص 139-146.

[2] يوسف خليل يوسف العفيفي، الجرائم الإلكترونية في التشريع الفلسطيني، رسالة ماجستير، الجامعة الإسلامية، غزة 2013.

[3] المادة 394 مكرر 07، القانون رقم 24-06، المؤرخ في 28-04-2024، المعدل والمتمم للأمر 66-156، المتضمن قانون العقوبات، ج،ر ج ج العدد 30.

[4] بن عودة صليحة، الشروع في الجرائم المعلوماتية بين الوقوع والردع، مجلة دفاتر الحقوق والعلوم السياسية، المجلد 01، العدد 02، سنة 2021، ص 74.

جرائم المساس بأنظمة المعالجة الألية للمعطيات نظرا لخطورتها فأعطى للشروع في ارتكابها نفس عقوبة الجريمة التامة.[1]

المطلب الثاني: دوافع ارتكاب الجريمة المعلوماتية

تختلف أسباب ارتكاب الجريمة المعلوماتية من شخص لأخر، حيث يرتكبها كل شخص حسب الغاية والهدف المراد الوصول إليه، كما تتكون هذه الجريمة على غرار الجريمة التقليدية من ركن شرعي ومادي ومعنوي، وهذا ما سنتناوله في هذا المطلب، حيث خصصنا **(الفرع الأول)** منه لتبيان بعض الدوافع الذاتية والخارجية التي تؤدي إلى ارتكاب الجريمة المعلوماتية أما **(الفرع الثاني)** فخصصناه للتطرق الأخرى التي تؤدي لارتكاب هذه الجريمة.

الفرع الأول: الدوافع الذاتية والخارجية لارتكاب الجريمة المعلوماتية

تتعدد وتتباين دوافع ارتكاب الجريمة المعلوماتية فمنها ما يعود إلى عوامل شخصية متعلقة بالمجرم (الدوافع الذاتية)، وكذلك منها ما يعود إلى عوامل خارجية وهذا ما سنعالجه من خلال هذا الفرع.

البند الأول: الدوافع الذاتية لارتكاب الجريمة المعلوماتية

تعتبر الدوافع الذاتية لارتكاب الجريمة المعلوماتية تلك الدوافع المرتبطة بشخصية المجرم والتي قد تكون من أجل كسب المال أي دافع مادي، وقد تكون ذات طبيعة ذهنية أو نمطية.

أولا: الدوافع المالية

قد يتجلى ارتكاب الجريمة المعلوماتية من أجل الحصول على ربح مالي وذلك من خلال مساومة البرامج أو المعلومات المتحصل عليها عن طريق الغش، حيث يقوم هؤلاء الأشخاص باستغلال إمكانياتهم ومعرفتهم الفنية في مجال الحواسيب والأنترنت من أجل التلاعب بأنظمة البنوك والسطو عليها وسرقة أموالها وتحويلها.[2]

[1] يزيد بوحليط، المرجع السابق، ص 138-139.

[2] يزيد بوحليط، المرجع نفسه، ص37.

ويعتبر دافع تحقيق الربح المالي من أكثر الأسباب التي تدفع بالمجرم لاقتراف هذا النوع من الجرائم باستعمال تقنية الحاسب الآلي وشبكة الأنترنت، حيث أصبح يحصد مرتكبيها مبالغ مالية ضخمة بانتحالهم شخصية الغير عن طريق وسائل التواصل الاجتماعي والقيام بأعمال غير مشروعة بغرض تحقيق الربح المادي.[1]

ومن أمثلة ذلك ما حدث في فرنسا سنة 1986، حيث كانت المداخيل من جريمة السرقة مع حمل السلاح هو 70000 فرنك فرنسي، أما في جريمة الغش في المجال المعلوماتي حصل منها الجاني على 670.000 فرنك فرنسي، وأشارت الدراسات إلى أنه منذ ظهور هذه الجريمة كان الغرض منها هو تحقيق الكسب المالي، حيث أكد الفقيه parker في دراسة في إحدى المجلات المتخصصة أن جرائم الغش المعلوماتي التي تكون من أجل اختلاس الأموال شكلت نسبة 34٪.[2]

ومن أمثلة الجرائم المعلوماتية التي تهدف إلى تحقيق الربح نجد أيضا ما حدث في الولايات المتحدة الأمريكية أين وقع العديد من المواطنين الأمريكيين ضحية نصب عن طريق الأنترنت، حيث قام مجموعة من الأشخاص بإنشاء مواقع لجمع التبرعات لضحايا أحداث 11 سبتمبر 2001.[3]

كما أعلنت شركة ماستر كارد انترنشونال عن حصول متسللين إلكترونيين على بيانات أكثر من أربعين مليون بطاقة ائتمان لمواطنين أمريكيين وذلك في سنة 2005.

أعلنت أيضا شركة visa usa عن اختراق 22 مليون من بطاقاتها وتسهيل استخدامها في عمليات الاحتيال.

كشفت بعض التقارير أنه قدرت الخسائر المالية على المستوى العالمي بأربع مليارات ومائتي مليون نتيجة لسرقة بيانات بطاقات الائتمان، ووفقا لدليل صادر عن المجلس الوطني

---

[1] شنتير خضرة، المرجع السابق، ص 40.

[2] خالد داودي، المرجع السابق، ص 37-38.

[3] شنتير خضرة، المرجع نفسه، ص 41.

لمكافحة الجرائم بأمريكا في سنة 2004 تم تسجيل حوالي 10 ملايين عملية سرقة البيانات الشخصية بالولايات المتحدة الأمريكية وكلف ذلك خمس بلايين دولار.[1]

ثانيا: الدوافع الذهنية أو النمطية

يسعى مرتكبو الجرائم المعلوماتية إلى تبيان مهاراتهم وتفوقهم وبراعتهم، حيث يسعون دائما إلى تحطيم التقنيات المستحدثة والتفوق عليها وهم لا يقومون بذلك لتوافر النوايا السيئة لديهم بل لتحقيق انتصارات تقنية، وبالتالي فليس لهم خطورة إجرامية كبيرة حيث يتصور في ذهن مرتكبي هذه الجرائم صورة البطل والذكي الذي يستحق الإعجاب وليس مجرم من الواجب محاكمته.[2]

من الملاحظ أن المجرمين الذين يرتكبون الجرائم المعلوماتية بدافع قهر أنظمة الحاسوب أو تجاوز الحماية وتبيان المهارات في هذا المجال يكونون من صغار السن حيث يحاولون من خلالها إثبات تفوقهم العلمي في مجال المعلوماتية وشبكة الأنترنت.[3]

كما قد يكون مرتكبي هذه الجرائم ليست لهم المعرفة الحقيقة لشن الهجمات الإلكترونية إذ أنهم يستعينون بمجموعة من البرامج التي لا تتطلب معرفة كبيرة في استعمالها، حيث يسميهم المختصين في مجال أمن المعلومات أطفال البرامج الجاهزة، حيث أنه لولا هذه البرامج لما تمكنوا من شن هذه الهجمات الإلكترونية وهدفهم من ارتكاب هذه الجرائم هو تحقيق الشهرة والوصول إلى المعلومات والبيانات المحمية والتباهي بها أمام أقرانهم والتظاهر بأنهم قراصنة أنترنت.[4]

---

[1] عبد العزيز بن براهيم بن محمد الشبل، الاعتداءات الإلكترونية، رسالة دكتوراه، جامعة الإمام محمد بن سعود الإسلامية، السعودية، السنة الجامعية 1430-1431 هـ، ص 41-42.

[2] بن مكي نجاة، السياسة الجنائية لمكافحة جرائم المعلوماتية، دار الخلدونية، ط 2017، الجزائر، ص 43.

[3] يزيد بوحليط، المرجع السابق، ص 37-38.

[4] شنتير خضرة، المرجع السابق، ص42.

البند الثاني: الدوافع الخارجية

بالإضافة إلى الدوافع الذاتية نجد أيضا دوافع خارجية تدفع بالمجرم إلى ارتكاب الجريمة المعلوماتية كالرغبة في الانتقام أو تجاوز تعقيدات الوسائل التقنية والرغبة في قهر النظام أو بدافع جنون العظمة.

أولا: الرغبة في الانتقام

قد تدفع الرغبة في الانتقام إلى ارتكاب إحدى الجرائم المعلوماتية كالانتقام من شخص ما أو مؤسسة ما أو الانتقام من رب العمل وحتى الأنظمة السياسية،[1] فقد يفصل عمال إحدى المؤسسات أو الشركات تعسفيا وبغير وجه حق، الأمر الذي يدفع بذلك العامل إلى ارتكاب الجريمة إصرارا منه في الانتقام وجعل المؤسسة أو الشركة تتكبد خسائر كبيرة نتيجة للضرر الذي ألحقه بها وخاصة إذا كانوا يملكون معلومات ومعرفة كافية تخص هذه الجهة.[2]

ومن أمثلة ذلك قيام شاب كان يعمل بإحدى المنشأة وبعد رحيله بأشهر تم تدمير البيانات الخاصة بحسابات وديون المنشأة، كما أنه لوحظ أن الضغوطات النفسية الناجمة عن ضغط العمل الذي يفرضه رب العمل على العمال التقنيين دفعت بعض العاملين لارتكاب جرائم الحاسوب انتقاما من رب العمل كقيامهم بزرع الفيروسات في نظم الكمبيوتر.[3]

ومن بين الأمثلة أيضا عن ارتكاب الجريمة المعلوماتية قيام شاب هندي يبلغ 16 سنة الانتقام من زملائه الذين يسخرون منه، من خلال إنشاء موقع إباحي حيث تضمن الموقع أسماء زملائه وزميلاته ومعلميه ووضع عليها تعليقات لا أخلاقية، وأيضا قيام جهاز المخابرات للكيان الصهيوني باختراق موقع حركة حماس الفلسطينية ونشر صور إباحية عليه، وهذا لغرض تشويه سمعة الحركة.[4]

---

[1] نهلا عبد القادر المومني، المرجع السابق، ص 92.

[2] بن مكي نجاة، المرجع السابق، ص 42.

[3] خالد داودي، الجريمة المعلوماتية، دار الإعصار العلمي، ط أولى، الأردن- عمان، ص 40.

[4] شنتير خضرة، المرجع السابق، ص 43.

ثانيا: الرغبة في قهر النظام والتفوق على تعقيد وسائل التقنية

قد يكون الدافع من وراء ارتكاب الجريمة المعلوماتية أيضا الرغبة في قهر الأنظمة الإلكترونية، حيث يسعى مرتكبي هذه الجرائم إلى إظهار قدراتهم وتفوقهم على الأنظمة الإلكترونية الحديثة وكشف عيوبها،[1] ويتزايد هذا الدافع لدى فئة صغار السن من مرتكبي الجرائم المعلوماتية إذ يقضون أوقاتا طويلة أمام أجهزة الحاسوب رغبة منهم في تبيان تفوقهم على الوسائل التقنية، وذلك من خلال محاولتهم لتجاوز الأمن لهذه الوسائل الأمر الذي جعل المنظمات الإجرامية (مجموعات الجريمة المنظمة) تستدرج هذه الفئة من محترفي الاختراق من أجل المشاركة معهم في جرائمهم من خلال استغلال قدراتهم في الاعتداء على هذه الوسائل، والتي تكون معقدة، وقد يكون حتى باستئجارهم للقيام بهذه الجرائم.[2]

الفرع الثاني: الدوافع الأخرى لارتكاب الجريمة المعلوماتية

بالإضافة إلى الدوافع الذاتية والخارجية التي تدفع بالمجرم لارتكاب الجريمة المعلوماتية نجد أيضا دوافع أخرى لهذه الجريمة والتي سنتطرق إليها كالاتي:

البند الأول: ارتكابها كوسيلة للتسلية والدعابة وجنون العظمة

أولا: ارتكاب الجرائم كوسيلة للتسلية والدعابة

يمكن أن ترتكب هذه الأفعال لغرض المزاح والدعابة، حتى وإن كان لا يقصد من خلالها إحداث ضرر للغير أو نية لارتكاب جريمة، إلا أنه قد ينتج عن مثل هذه الأفعال جرائم كأن يقوم شخص بمسح المعلومات والملفات من جهاز شخص أخر وتكون هذه الملفات تحتوي على معلومات لها أهمية ويحتاجها هذا الشخص، وقد تعرقل عمله في حالة إتلافها حيث يشكل هذا الفعل جريمة إتلاف وتخريب متعمد وهو الفعل الذي يجرمه القانون، ومن غير الممكن اعتبار هذا التصرف مجرد دعابة.[3]

---

[1] شنتير خضرة، المرجع نفسه، ص 43.

[2] خالد داودي، المرجع السابق، ص 41.

[3] بن مكي نجاة، المرجع السابق، ص 43-44.

كما أن العديد من مرتكبي هذه الجرائم يقومون بها لغرض التسلية والمزاح والدخول إلى أنظمة الأخرين إلا أنه يكون دون تأثير يذكر.[1]

ثانيا: دافع جنون العظمة

يقوم بعض المجرمين بارتكاب الجريمة افتخارا بقدراتهم والغرور بها، وذلك بصرف النظر عن الخسائر والأضرار المرتبطة بالجريمة التي يرتكبها، فقد يكون الشخص مغرورا إلا أنه لا يكون على درجة علمية كبيرة، وقد يكون متفوق علميا، ويقوم بهذه الأفعال أمام الغير ليبين إمكانياته وما لديه من معلومات.[2]

البند الثاني: الدوافع السياسية ودافع الإرهاب والتجسس

أولا6: دوافع سياسية

قد ترتكب الجرائم المعلوماتية كذلك لدواعي سياسية، حيث كثيرا ما يتم قرصنة المواقع الحكومية والأجهزة الأمنية، كما قد أصبحت شبكة الأنترنت مجالا يتم من خلاله نشر الأفكار والأخبار التي تتسم بالطابع السياسي أو تمس بأمن الدولة وأنظمة الحكم والإساءة للمسؤولين والشخصيات السياسية بالقذف والتشهير،[3] كما نجد بعض المنظمات تتبنى أراء وأفكار سياسية ولغرض فرض هذه الآراء والدفاع عنها تقوم بأفعال إجرامية ضد معارضيها بالتشهير بهم عن طريق شبكات التواصل الاجتماعي.[4]

---

[1] خالد حسن أحمد لطفي، جرائم الأنترنت بين القرصنة الإلكترونية وجرائم الابتزاز الإلكتروني، دراسة مقارنة، دار الفكر الجامعي، ط أولى، مصر، 2018، ص 74.

[2] غادة نصار الغربي الإرهاب والجريمة الإلكترونية، العربي للنشر والتوزيع، ط الأولى، 2017، القاهرة، ص 55.

[3] ناصر بن محمد البقمي، مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربية، قسم التوزيع والنشر، الإمارات، ص 11.

[4] بن مالك إسمهان، خصائص الجريمة المعلوماتية وأسباب ارتكابها، مجلة البيان للدراسات القانونية، المجلد 04، العدد 01، جامعة برج بوعريريج الجزائر، 2019، ص 118.

ومن أمثلة ذلك التشهير بمسؤولي الدولة عبر مواقع التواصل الاجتماعي ومسؤولي ورؤساء الدول المعادية من خلال ادعاءات كاذبة أو بصور مزيفة لتشويه سمعته أمام المواطنين والدول الأخرى.[1]

ثانيا: دافع الإرهاب والتجسس

ساهم التطور التكنولوجي وظهور الحاسب الآلي وشبكة الأنترنت في انتشار ظاهرة الإرهاب وسهولة التخطيط لها، وارتكابها بسرعة والدعوى إليها والترويج لأفكارها والتحريض على العنف، ومن أمثلة ذلك ما حدث في مصر أين قام أحد الأشخاص بإنشاء شبكة الثورة وهي صفحة على الأنترنت من أجل الترويج لأفكار تلك الجماعة ونشر معلومات وأسماء رجال الشرطة ووضع منشورات ضد أمن الدولة.[2]

أما بالنسبة للتجسس فبعد انتشار الأقمار التجسسية والبث الفضائي، وكذلك مهمات التجسس التي تقوم بها مختلف أجهزة الاستخبارات لبعض الدول للتجسس والحصول على معلومات وأسرار دول أخرى وإفشائها والقيام من خلالها بأعمال تضر بمصلحة تلك الدول، وكذلك نجد التجسس في المجال التجاري كالاستلاء على أسرار العلامات التجارية وبراءات الاختراعات وذلك من اجل المنافسة.[3]

بالإضافة إلى هذه الدوافع التي تؤدي بالأشخاص لارتكاب الجرائم المعلوماتية نجد أيضا بعض الدوافع الأخرى ومن بينها ما يلي:

- التسابق العسكري والفضائي، مثل قيام قراصنة بتوقيع هجمات إلكترونية على وكالة ناسا ومواقع أسلحة تابعة للولايات المتحدة الأمريكية.
- الدعوى للإلحاد حيث ظهرت العديد من المواقع التي تنشر فكرة الإلحاد والمطالبة بإلغاء الدين والدولة وغسيل الأموال، والتي تعتبر من بين أبرز أسباب ارتكاب الجرائم الإلكترونية.[4]

---

[1] ميرفت محمد مبابية، المرجع السابق، ص 85.

[2] ناصر بن محمد القمي المرجع السابق، ص 11.

[3] غادة نصار، المرجع السابق، ص 53.

[4] شنتير خضرة، المرجع السابق، ص 44-45.

- التعاون والتواطؤ على الأضرار حيث يقوم شخص متخصص في هذا المجال بالتعاون مع شخص أخر بتغطية التلاعبات بالأموال داخل المؤسسة.[1]
- حب التعلم والاستطلاع: قد يعتقد بعض مخترقي أجهزة الحاسوب أن المعلومات هي حق للجميع وللجميع الحق في الاستفادة من المعلومات والتعرف عليها وأن لا تبقى حكرا لفئة معينة فقط.[2]

كما أشار مؤلف كتاب قراصنة الانظمة إلى أن أخلاقيات القراصنة تقوم على مبدأين أساسيين هما أنه الدخول إلى الأنظمة يعلمك كيف تسير العالم، وأن عملية جمع المعلومات تكون غير خاضعة للقيود، كما أن غاية هؤلاء القراصنة هو الحصول على المعلومات واكتشاف الأنظمة والعمل مع الجماعة وتعليم بعضهم والبقاء مجهولين حتى يبقون متواجدين أكبر مدة ممكنة داخل النظام.[3]

[1] يزيد بوحليط، المرجع السابق، ص 38.

[2] خالد حسن أحمد لطفي، المرجع السابق، ص 74.

[3] نهلا عبد القادر المومني، المرجع السابق، ص 89-90.

المبحث الثاني: خصائص الجريمة المعلوماتية والمجرم المعلوماتي وأنواعها

تتميز الجريمة المعلوماتية بمجموعة من الخصائص التي تميزها عن بقية الجرائم الأخرى التقليدية، كما يتميز المجرم المعلوماتي بمجموعة من السمات التي تميزه عن غيره من المجرمين العاديين، كما نجد أن الجريمة المعلوماتية تتنوع بحسب طبيعتها والتي قد تكون جرائم ترتكب بواسطة النظام المعلوماتي أو جرائم واقعة على النظام المعلوماتي، وهذا ما سنتطرق إليه في هذا المبحث حيث خصصنا **(المطلب الأول)** لتطرق لأهم الخصائص التي تميز الجريمة المعلوماتية عن الجريمة التقليدية وأهم ما يميز المجرم المعلوماتي عن المجرم التقليدي، أما **(المطلب الثاني)** فخصصناه للتعرف على أنواع الجريمة المعلوماتية.

المطلب الأول: خصائص الجريمة المعلوماتية وسمات المجرم المعلوماتي

تتميز الجريمة المعلوماتية عن غيرها من الجرائم التقليدية بمجموعة من الخصائص التي تتمتع بها دون غيرها باعتبار أنها تنفذ بوسائل غير مادية، فهي لا تقع على أرض الواقع وينتج عنها سفك الدماء ولا كسر الأعضاء، فهي تقع في فضاء افتراضي يضع صعوبات كبيرة من أجل اكتشافها أو ملاحقة مرتكبيها والبحث والتحري عنها مما يؤدي إفلات المجرمين من العقاب، وتنفذ بواسطة الوسائل التكنولوجية الحديثة، كما تتميز بأنها عابرة للحدود تنفذ في بلد وقد تقع النتيجة الإجرامية في دولة أخرى، ومن خلال هذا فإن الجريمة المعلوماتية تتميز بخصائص منفردة لا توجد في الجرائم التقليدية، وهذا ما سنتطرق إليه في **(الفرع الأول)** من هذا المطلب، كما يتميز المجرم المعلوماتي عن بقية المجرمين في كونه له معرفة في مجال الحاسب الآلي، كما تتعد أنماط مرتكبي الجريمة المعلوماتية والتي تختلف حسب الهدف المرجو من الجريمة وهذا ما سنبينه من خلال **(الفرع الثاني)**.

الفرع الأول: خصائص الجريمة المعلوماتية

تتميز الجريمة المعلوماتية عن الجريمة التقليدية بمجموعة من الخصائص وهذا ما سنبينه من خلال هذا الفرع.

البند الأول: خفاء الجريمة المعلوماتية (صعوبة اكتشافها)

ترتكب الجريمة المعلوماتية في الخفاء حيث لا يشعر بها الضحية ويقوم بها الجاني بواسطة جهاز كمبيوتر متصل بشبكة الأنترنت ويكون ذلك عن بعد ويكون فيها الجاني على دراية ومعرفة باستخدام الكمبيوتر للقيام بالجريمة،[1] فالضحية في هذه الجريمة لا يمكنه ملاحظتها رغم أنها قد تقع أثناء تواجده على الشبكة، فالجاني يكون يتمتع بقدرات فنية عالية في أغلب الأحيان تمكنه من تنفيذ الجريمة بدقة ومن أمثلة ذلك ما قام به " **فلاديمير لوفين**" في شهر أوت من سنة 1994 حيث قام باقتحام أنظمة المصرف الامريكي (18) مرة إذ تمكن من فك شفرة حسابات كثيرة من عملاء البنك وقام بالسطو عليها وتحويل هذه المبالغ المالية وذلك من مصرف "**سيتي بنك**".[2]

إن الجرائم المعلوماتية هي من الجرائم التي يصعب اكتشافها وذلك لعدم وجود آثار خارجية لها مثل الجرائم التقليدية، حيث يمكن للمجرم إخفاء أثار الجريمة، وذلك من خلال التلاعب غير المرئي في النبضات أو الذبذبات الإلكترونية وبذلك تمحى أثاره ومنه يصعب ملاحقته وإفلاته من العقاب، ولأن تنفيذها لا يتطلب وجود الفاعل في مكان الجريمة بل يمكن تنفيذ جريمته وهو في مكان بعيد كما توجد عدة أسباب تحول دون اكتشاف الجريمة المعلوماتية منها:

- التكنولوجيا المعقدة وقدرة التخزين الهائلة والسرعة البالغة التي يعمل بها الحاسوب. [3]
- لا تترك بعد ارتكابها أثرا يلمس أو يرى بالعين المجردة وصعوبة الاحتفاظ به إن وجد.

[1] حسين طاهري، المرجع السابق، ص 15.

[2] شنتير خضرة، المرجع السابق، ص 20-21.

[3] يزيد بوحليط، المرجع السابق، ص 82-83.

- ترتكب في الخفاء.
- سهولة محو الدليل والتخلص منه.
- عدم إبلاغ المجني عليه عن هذه الجرائم.[1]
- عدم وجود خطط بديلة عند ضحايا الجرائم المعلوماتية للرد عليها وتفادي أضرارها.[2]

البند الثاني: جريمة ناعمة (أقل عنفا)

إن جرائم الأنترنت لا تتطلب العنف في تنفيذها حيث يتم القيام بها بأقل جهد ممكن على عكس الجرائم التقليدية التي تتميز بالقيام بنوع من الجهد العضلي كممارسة العنف والإيذاء، والأمر الذي يميز الجرائم المعلوماتية أنها جرائم هادئة لا تحتاج إلى العنف وإنما تحتاج إلى القدرة والمعرفة في التعامل مع أجهزة الحاسب الآلي، وكذلك وجود شبكة الأنترنت فيقوم المجرم بتوظيف معرفته في هذا المجال للقيام بالجرائم المختلفة مثل التجسس والاختراق وغيرها فهي من الجرائم النظيفة التي ليس فيها أي أثر للعنف أو الدماء وليس لها أثر خارجي مادي.[3]

إن الجرائم المعلوماتية لا تحتاج في ارتكابها إلى استعمال العنف أو القوة ولا تسفك الدماء أو وقوع جثث فهي تحتاج فقط إلى ضغطة زر على لوحة المفاتيح،[4] فهي تنفذ بأقل جهد وعلى اعتبار أنها تعتمد على الخبرة المعلوماتية لدى مرتكبها.[5]

البند الثالث: جريمة عابرة للحدود

تتميز الجريمة المعلوماتية في أنها جريمة عابرة للحدود وذلك باعتبار أن تقنية المعلومات لها القدرة على اختصار المسافات وجعل العالم قرية صغيرة، حيث تتجاوز هذه الجريمة الحدود

---

[1] بردال سمير، الجريمة المعلوماتية في التشريع الجزائري، مجلة القانون، المركز الجامعي غيليزان، العدد الثاني، جويلية 2010، ص 181.

[2] طاهر ياكر، مكافحة الجرائم الإلكترونية بين التشريعات الوطنية والاتفاقيات الدولية، المرجع السابق، ص 11.

[3] صغير يوسف، الجريمة المرتكبة عبر الأنترنت، رسالة ماجستير، جامعة مولود معمري، تيزي وزو، س.ج 2012-2013 ص 16.

[4] عبد الرحماني أمينة ومرابطين حفيظة، جرائم تكنولوجيا الإعلام والاتصال، رسالة ماجستير، جامعة مولود معمري تيزي وزو، د س، ص 6.

[5] نادرعبد الكريم الغزواني، الحماية الجنائية من جرائم الأنترنت، نور النشر، ط 2017، ص 21.

الجغرافية الأمر الذي يثير تحديات قانونية وحتى سياسية خاصة فيما يتعلق بإجراءات المتابعة الجزائية،[1] كما سهلت هذه الجريمة التواصل بين الأفراد في القارات المختلفة وهذا ما جعلها عابرة للحدود أي أنها تتسم بالطابع الدولي إذ يكون المجرم في دولة والمجني عليه في دولة أخرى، وقد يكون الضرر لحق في دولة ثالثة أو عدة دول وهذا ما جعل الدول في تنازع حول القوانين الواجبة التطبيق واختلاف إجراءات المتابعة من دولة إلى أخرى، مما يتطلب وجود تعاون دولي للقبض على الجناة وتقديمهم للجهات المختصة، كما يحتاج أيضا التحقيق في الجريمة المعلوماتية تفتيش المواقع الإلكترونية أو الأجهزة الإلكترونية تفتيشا ماديا من أجل الحصول على المعلومات أو معاينة مسرح الجريمة الأمر الذي يحتاج إلى تعاون دولي على أرض الواقع.[2]

البند الرابع: امتناع المجني عليهم من التبليغ وصعوبة إثبات الجريمة المعلوماتية

من بين خصائص الجريمة المعلوماتية نجد أيضا امتناع المجني عليهم من التبليغ وكذلك صعوبة إثباتها.

أولا: امتناع المجني عليهم من التبليغ

تتميز الجريمة المعلوماتية بعدم الإبلاغ عنها في غالبية الأحيان، حيث تتسم بتكتم الضحايا وعدم الإعلان عنها، وذلك بسبب خوفهم من الفضيحة خاصة في الجرائم التي تمس خصوصيتهم أو خوفا من رفض الأشخاص من التعامل مع الضحية إذا عرفوا بالهجوم الواقع عليه، مثل حالة المصارف يتجنب الزبائن التعامل معها خوفا على مصالحهم كما أن الشركات التجارية لا تقوم بالتبليغ خوفا من أعمال التحقيق التي تقوم بها الشرطة قد تؤدي إلى احتجاز حواسيبها أو تعطيل شبكاتها لفترة طويلة قد يؤدي في زيادة خسائرها المالية فقد تكون هذه الخسائر أكثر من الخسائر التي تسببت فيها الجريمة أصلا،[3] كما نجد أيضا أنه لم يتم التبليغ

[1] أدهم باسم نمر بغدادي، وسائل البحث والتحري عن الجرائم الإلكترونية، رسالة ماجستير، جامعة النجاح الوطنية فلسطين، 2018، ص 11.

[2] يوسف خليل يوسف العفيفي، المرجع السابق، ص 15-16.

[3] شنتير خضرة، المرجع السابق، ص 23.

عن هذه الجرائم نظرا لعدم اكتشافها من طرف الضحية فمعظم الجرائم اكتشفت بالصدفة وبعد وقت طويل من ارتكابها[1].

ثانيا: صعوبة إثبات الجريمة المعلوماتية

إن الجريمة المعلوماتية من الجرائم التي يصعب الوصول إليها، وذلك لأن المعلومات التي تحملها الأنترنت هي عبارة عن رموز مخزونة في وسائل تخزين مغناطسية ولا يمكن قراءتها إلى عن طريق الحاسوب، الأمر الذي يجعل الدليل يصعب بقائه أو إثباته فالجاني لا يترك ورائه أثر مادي ملموس يمكن فحصه، مما يؤدي إلى صعوبة اكتشاف الجريمة ومعرفة مرتكبها فمن الصعب نسب فعل إجرامي إلى شخص طبيعي، وهو ما جاء في الكثير من القرارات القضائية من أبرزها ما أقرته محكمة الاستئناف لباريس في قرارها الصادر في 27 من أفري 2007 وذلك لكون عنوان برتوكول (IP) لا يدل على ارتكاب الشخص لها و إنما يدل إلا على تسلسل أرقام مرتبطة بالآلة،[2] وبالتالي فإنه حتى وفي حال اكتشاف هذه الجريمة والإبلاغ عنها إلا أن إثباتها يبقى أمرا صعب، حيث تقوم أركانها في بيئة الحاسوب والأنترنت مما يعقد الأمر على سلطات الأمن وجهات التحقيق والملاحقة، إذ تكون البيانات فيها عبارة عن نبضات إلكترونية غير مرئية تنساب عبر النظام المعلوماتي مما يجعل الدليل يمحى ويطمس كليا بكل سهولة من قبل الفاعل، وتختلف وسائل المعاينة لهذه الجريمة عن بقية الجرائم الأخرى التقليدية حيث تخلف هذه الأخيرة أثارا مادية ويتمكن من خلاله سلطات البحث والاستدلال في الكشف عن الجريمة، أما الجريمة المعلوماتية فهي عكس ذلك لا تخلف أثارا مادية والتحقيق فيها يأخذ فترة طويلة الأمر الذي يتيح مجالا للجاني أن يغير أو يعبث ويتلف أثار هذه الجريمة إذا كانت موجودة، الأمر الذي يجعل هذه الأدلة محل شك.

[1] هشام بشير، الآليات الدولية لمكافحة الجريمة الإلكترونية، المركز الدولي للدراسات المستقبلية الاستراتيجية، العدد 90، مصر، 2020، ص 11.

[2] شنتير خضرة، المرجع السابق، ص 24.

وتعود أيضا صعوبة اكتشافها إلى نقص الخبرة الفنية والتقنية لدى الشرطة وجهات الادعاء والقضاء مما يشكل عائقا كبيرا في إثبات الجريمة، حيث تتطلب تأهيل وتدريب هذه الجهات في مجال تقنية المعلومات وكيفية التفتيش والملاحقة في بيئة الحاسوب فنقص الخبرة والتدريب غالبا ما يجعل أجهزة الشرطة تخفق في تقدير أهمية الدليل، فقد يدمر المحقق الدليل بمحوه محتويات أسطوانة صلبة عن طريق الخطأ أو الإهمال[1].

ومن خلال ما سبق يتبين لنا أنه من أسباب صعوبة إثبات الجريمة المعلوماتية ما يلي:

- لا تترك أثر ارتكابها.
- صعوبة الاحتفاظ الفني بأثرها إن وجدت.
- ضعف الخبرة الفنية لدى المحقق.
- هي جرائم ترتكب في الخفاء.
- سهولة محو الدليل والتخلص منه.
- عدم إبلاغ المجني عليه على هذه الجريمة.
- ترتكب في دولة وتتحقق النتيجة الإجرامية في دولة أخرى.[2]

البند الخامس: سهولة ارتكاب الجريمة المعلوماتية ووقوعها أثناء المعالجة الآلية للمعطيات

تتميز هذه الجريمة بسهولة ارتكابها وأنها تقع أثناء المعالجة الألية للمعطيات

أولا: سهولة ارتكاب الجريمة المعلوماتية

إن ما يميز الجريمة المعلوماتية هو سهولة ارتكابها، وذلك راجع لتمتع الجاني بقدرات فنية تمكنه من ارتكاب جريمته بشكل دقيق، وقد تتم هذه الجريمة في ثواني أو أجزاء من الثانية في بعض الجرائم، حيث أن الكثير من الجرائم لا يتم اكتشافها إلى بعد مرور مدة طويلة مثل جرائم التجسس أو سرقة بيانات خاصة أو سرقة الأموال، والأمر الذي يزيد من سرعة تنفيذ هذه الجريمة هو التقدم التقني الذي ظهرت على ضوئه العديد من البرامج والوسائل التي تساعد

[1] نهلا عبد القادر المومني، المرجع السابق، ص 56-57.

[2] بردال سمير، المرجع السابق، ص 180.

وتساهم في تنفيذ هذه الجريمة بسرعة،[1] فالجريمة المعلوماتية لا تتطلب الإعداد والتحضير قبل ارتكابها ولا تتطلب استخدام معدات وبرامج فيكفي فيها الضغط على لوحة المفاتيح أو ارتكابها بواسطة الهاتف،[2] وما يبين أيضا أن هذه الجريمة سهلة الارتكاب هو أنه أصبح أي رجل عادي يعرف تقنيات بسيطة في استعمال جهاز الحاسوب يمكنه ارتكابها وهذا نتيجة لظهور تطبيقات وبرامج مجانية تسهل ارتكاب الجريمة وسهولة ومرونة التخطيط والتنفيذ وكذلك سهولة تبادل الخبرات والأفكار بين الجناة[3].

ثانيا: وقوعها أثناء المعالجة الألية للمعطيات

تقع الجريمة المعلوماتية أثناء المعالجة الآلية للمعطيات، والمقصود بالمعالجة الألية للمعطيات في الفقه بأنه "كل مركب يتكون من وحدة أو مجموعة وحدات معالجة والتي تتكون كل منها من ذاكرة وبرامج ومعطيات وأجهزة الإدخال والإخراج وأجهزة الربط والتي يربط بينها مجموعة من العلاقات، والتي عن طريقها يتم تحقيق نتيجة معينة وهي معالجة المعطيات على أن يكون هذا المركب خاضعا لنظام الحماية الفنية"، و اشترط المشرع الفرنسي أن يكون لهذه البيانات حماية ووضع الآليات القانونية لحمايتها،[4]

أما المشرع الجزائري لم يعرف أنظمة المعالجة الآلية للمعطيات وإنما اكتفى بذكر العقوبات المقررة للاعتداء عليها في القسم السابع مكرر من الفصل الثاني من الكتاب الثاني من قانون العقوبات في المواد من 394 مكرر إلى غاية 394 مكرر 08، حيث يعاقب كل من دخل عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك أو عن طريق الحذف أو تغيير للمعطيات وتخريب نظام اشتغالها بالحبس من (03) أشهر إلى سنة وبغرامة من 50.000 دج إلى 200.000 دج وتضاعف في حالة حذف أو تغيير

[1] طاهر ياكر، مكافحة الجرائم الإلكترونية بين التشريعات الوطنية والاتفاقيات الدولية، المرجع السابق، ص 10

[2] خالد حسن أحمد لطفي، المرجع السابق، ص 20.

[3] حسين طاهري، المرجع السابق، ص 16-17.

[4] أدهم باسم نمر البغدادي، المرجع السابق، ص 12.

لمعطيات المنظومة،[1] ومن خلال هذا يتبين لنا أن معلومات البيانات المخزنة على الحاسب الآلي هي موضوع الجرائم الإلكترونية وهذه البيانات والمعلومات تعد مكونات معنوية قابلة للنقل والحيازة وبالإمكان سرقتها وإتلافها فمن الضروري أن تكون محلا للحماية من طرف القانون[2].

الفرع الثاني: سمات وشخصية وأنماط المجرم المعلوماتي

يعتبر المجرم المعلوماتي من جماعة الجانب المظلم للحاسوب، حيث يتميز بخبرته ومهاراته في تقنية المعلومات والحاسوب وتساعد قدراته الذهنية والفنية على ارتكاب جرائم إلكترونية بسهولة وبسرعة مقارنة بالجرائم الأخرى، حيث يفتقد بعض المجرمين إلى التخصص والمعرفة في مجال جرائمه.[3]

كذلك المجرمين الإلكترونيين أو ما يسمى القراصنة الإلكترونيين هم أفراد أو مجموعات لا يرتكبون سوى جرائم الحاسوب مما يعني أنهم متخصصون في هذا المجال دون صلة بأي نشاط إجرامي تقليدي أخر، وهذا يظهر أن الشخص الذي يقوم بارتكاب جريمة المعلوماتية عادة ما يكون خبيرا في هذا المجال من الجرائم[4].

يشير بعض الخبراء مثل الأستاذ Parker الذي يعد من أهم الباحثين الذين اهتموا بمجال علم المعلومات بصفة عامة وبالمجرم المعلوماتي بصفة خاصة، إلى أن المجرم الإلكتروني يمثل طائفة خاصة من المجرمين تختلف عن المجرمين التقليديين، وأن هذه الطائفة تشبه في بعض الجوانب جرائم ذو الياقات البيضاء.[5]

---

[1] المواد من 394 مكرر إلى 394مكرر07، ق رقم 24- 06، المصدر السابق.

[2] يوسف خليل يوسف العفيفي، المرجع السابق، ص 15.

[3] لورنس سعيد الحوامدة، الجرائم المعلوماتية أركانها وأليات مكافحتها، مجلة الميزان للدراسات الإسلامية والقانونية، المجلد 4 العدد 01، المملكة العربية السعودية، 2017، ص 13.

[4] غادة نصار، المرجع السابق، ص 43.

[5] بن شهرة شول، السمات الخاصة للجريمة المعلوماتية، مجلة المستقبل للدراسات القانونية، المجلد04، العدد 01، ,جامعة غرداية، 2020، ص 12.

البند الأول: سمات المجرم المعلوماتي

يتميز المجرم المعلوماتي بعدد من السمات والخصائص، ويرمز إليها الأستاذ Parker بكلمة Skram وهي تعني المهارة skills المعرفة knowledge الوسيلة Ressourcesالسلطة AuthoritY وأخيرا الباعثMotives. [1]

أولا: المهارة

يمكن لمجرمي الإنترنت اكتساب الخصائص والمهارات اللازمة لتنفيذ أنشطتهم الإجرامية، وذلك من خلال الدراسة المهنية في مجال تكنولوجيا المعلومات والخبرة المكتسبة في هذا المجال، وحتى التفاعلات الاجتماعية مع الآخرين ومع ذلك يظهر الواقع أن بعض مجرمي الإنترنت الأكثر نجاحًا قد لا يكون لديهم معرفة متقدمة في هذا المجال،[2] كما تعد مهارات الاتصال الحديثة من أهم سمات مجرمي الإنترنت والتي تميزهم عن المجرمين الأخرين حيث تكتسب عن طريق ممارستهم المتكررة للأدوات الإلكترونية وتكتسب غالبا عن طريق التجارب والهوايات مما يتيح لهم ارتكاب جرائمهم بمهارة أفضل[3].

ثانيا: المعرفة

تساعد المعرفة في تقييم إمكانية نجاح الجريمة واحتمالات فشلها، ويستخدم المجرم المعلوماتي المعرفة لبناء تصور كامل للنظام المستهدف، وكذلك يستعمل لاختبار الجريمة على أنظمة مشابهة للأنظمة المستهدفة وذلك قبل ارتكاب الجريمة.[4]

ثالثا: الوسيلة

تشير إلى الوسائل التي يستخدمها الفاعل لإتمام جريمته، ولذلك فإن سهولة التلاعب بأنظمة المحاسبة الآلية تعتبر أحد العوامل الرئيسية التي تساهم في انتشار الجرائم الإلكترونية

---

[1] نائلة عادل محمد فريد قورة، المرجع السابق، ص 57.

[2] بن شهرة شول، المرجع السابق، ص 13.

[3] يونس نفيد، المكافحة التشريعية لبعض الصور الجرائم المعلوماتية وأصناف المجرم المعلوماتي، المجلة العربية للدراسات الأمنية المجلد 38، العدد 02، المملكة العربية السعودية، سنة 2022، ص 139.

[4] بن شهرة شول، المرجع نفسه، ص 13.

وفي معظم الحالات لا يتطلب ذلك مهارة فنية عالية أو تكاليف باهضه، خاصة إذا كان النظام الذي يعمل فيه الكمبيوتر نظام عادي، أما اذا كان نظام غير معروف فإن هذه الطرق ستكون معقدة وصعبة.[1]

رابعا: السلطة

يقصد بالسلطة تلك المزايا والحقوق التي يتمتع بها مجرم الإنترنت والتي تمكنه من ارتكاب الجريمة، حيث يمتلك معظم مجرمي الإنترنت القدرة بشكل مباشر أو غير مباشر على مواجهة المعلومات التي تكون موضوع الجريمة من خلال الحصول على تصاريح غير قانونية مما تسمح لهم بالوصول إلى أنظمة الكمبيوتر، وتتمثل في استخدام الرقم السري الخاص للولوج إلى نظام الكمبيوتر وسرقة البيانات وفتح الملفات وقراءتها وكتابتها وحذف معلومات أو إجراء تغييرات وقد تتضمن هذه التصاريح الحق في استخدام أنظمة الكمبيوتر أو إجراء معاملات معينة أو ببساطة الدخول إلى موقع هذه الأنظمة.[2]

خامسا: الباعث

هو الرغبة في تحقيق مكاسب مالية عبر وسائل غير قانونية ويظل هذا هو السبب الرئيسي لارتكاب الجرائم الإلكترونية، ويعتقد البعض أن الدافع لارتكاب الجرائم الإلكترونية في معظم الحالات ليس لتحقيق مكاسب مالية، وإنما هناك جوانب أخرى مثل الانتقام من صاحب العمل والرغبة في السيطرة على نظام الكمبيوتر واختراق الحاجز الأمني.[3]

---

[1] مزيود سليم، الجرائم المعلوماتية واقعها في الجزائر واليات مكافحتها، المجلة الجزائرية للاقتصاد والمالية، العدد01 ، جامعة المدية، 2014، ص 98.

[2] رضا عسال وعماد عبد الرزاق، الجريمة الإلكترونية والمجرم المعلوماتي، مجلة ببليوفيليا، العدد 05، جامعة العربي تبسة – الجزائر، 2020، ص 155.

[3] سعدات فتوح محمود محمد، خصائص الجرائم المعلوماتية وصفات مرتكبيها في ظل المجتمع المعلوماتية، المؤتمر الدولي الاول لمكافحة الجرائم المعلوماتية، المملكة العربية السعودية، 2015، ص 45.

البند الثاني: شخصية المجرم المعلوماتي

تتميز شخصية المجرم المعلوماتي عن غيره من المجرمين التقليديين، حيث يتميز بمايلي:

أولا: المجرم المعلوماتي الذكي

يتميز دائما بالذكاء المرتفع والكفاءة ولديه قدرة ممتازة على إدارة واختراق أجهزة الكمبيوتر وشبكات المعلومات والوصول إلى البيانات والمعلومات اللازمة وهذا بسبب ذكائهم العالي الذي يفوق المجرم التقليدي، وغالبا ما يكون الشخص الذي يسرق منزلا أو سيارة أقل ذكاء من الشخص الذي يستخدم الكمبيوتر لسرقة مال البنك أو شركة.[1]

يتدخل مجرمو الإنترنت في استخدام البرامج وذلك ببساطة عن طريق حقن الفيروسات أو استخدام القنابل المنطقية أو القنابل الموقوتة أو البرامج الدودية لشل النظام الإلكتروني ومنعه من القيام بوظائفه الطبيعية، وتشكل الجرائم التي يرتكبونها خطرا على المجتمع سواء كأفراد أو مؤسسات أو حتى جماعة منظمة أو غير ذلك[2].

أظهرت دراسة أجريت عام 2009 في المملكة العربية السعودية للباحث عبد الله بن سعود بن محمد السراني على نخبة من الأفراد المتخصصين في مكافحة الجرائم الإلكترونية وخلصت إلى أن 94,2% من العينة درسوا مجرمي المعلومات الذين ارتكبوا جرائم معلوماتية وأكدوا على أن المجرم المعلوماتي يتميز بخصائص محددة بأنه يتمتع بالذكاء العالي والمهارة في استخدام تكنولوجيا الكمبيوتر مثل أنظمة التشغيل والبرمجة والشبكات وقدرته على اختراق الأنظمة والتلاعب بها، كما يخترع أساليبه الخاصة ويمتلك أساليب متقدمة لارتكاب جرائمه وتغطية أثاره، ويمتلك مهارات إلكترونية ممتازة في معالجة النصوص والكلام وإدارة البرامج.[3]

---

[1] محمد سامي السيد أحمد، الدور العملي لوزارة الداخلية في مكافحة الجريمة المعلوماتية، المعهد القومي للملكية الفكرية، العدد الثالث، جامعة حلوان، 2022، ص 158.

[2] محمود دين، المرجع السابق، ص 60-61.

[3] بكوش محمد وهروال نبيلة هبة، خصوصية المجرم الإلكتروني، مجلة البحوث في الحقوق والعلوم السياسية، المجلد07 ، العدد 01 , جامعة تيارت – الجزائر، 2021، ص 78.

ثانيا: اجتماعي

إن اعتبار المجرم المعلوماتي شخصا ذكيا يرجع إلى كونه اجتماعيا، وأنه شخص يمكنه الانسجام مع الأشخاص حوله وتقديم التنازلات وذكائه العالي يسمح له التكيف بسهولة في المجتمع.[1]

هناك أشخاص يرتكبون جرائم حاسوبية ليس بهدف الحصول على الأموال بل لأسباب اجتماعية للمتعة، مثلا أو ببساطة لإثبات تفوقهم على نظام الحاسوب أو البرامج المستخدمة في أمن النظام، والتي لا تهدف إلى الربح من جرائمهم ولكن يكتفون بالتباهي بأنفسهم أو إظهار نقاط الضعف في نظامهم للضحايا وفي أغلب الأحيان يؤدي مثل هذا السلوك إلى أضرار جسيمة بالنظام حتى ولو لم يكشف عن عدائية من جانب المجتمع ويستغل الإمكانيات المتاحة من عملية التصحيح والتعديل والحذف والأرشفة والطباعة وهي بذلك علاقة وثيقة بارتكاب الجريمة.[2]

ثالثا: محترف

يتمتع المجرمون المحترفون بمهارات تقنية عالية وفهم عميق للأنظمة الكمبيوتر والشبكات، ويخططون بدقة لعملياتهم التي ترتكب من قبل أعضائها ولذلك يعد المحترفون من أخطر المجرمين التكنولوجيين، حيث أن هجماتهم موجهة إليهم في المقام الأول لتحقيق مكاسب مالية لأنفسهم أو لجهات تكلفهم وتجبرهم على ارتكاب جرائم حاسوبية، وتهدف بعض هجماتهم إلى تحقيق أهداف سياسية والتعبير عن مواقفهم الفكرية أو النظرية أو الفلسفية، وقد يتخصص بعض المجرمين في نوع معين من جرائم الكمبيوتر مثل التجسس الصناعي أو الاحتيال فالأول يهدف إلى سرقة الأسرار التجارية من الشركات، أما الثاني يسعى من خلاله المجرمون الى الاستيلاء على أموال اخرين ويتميزون بسرقة انشطتهم ولا يتبادلون المعلومات مع الآخرين،[3]

---

[1] رضا عسال وعماد عبد الرزاق، المرجع السابق، ص 155.

[2] عبد الله سيف عبيد سالم أل علي، سمات وأنماط المجرم المعلوماتي في جرائم الاحتيال الإلكتروني، أطروحة دكتوراه، جامعة المنصورة، 2020، ص 20.

[3] سمير شعبان، الجريمة الإلكترونية، المرجع السابق، ص 124.

فمجرمو الإنترنت المحترفون يمثلون فئة من الأفراد الذين تتراوح أعمارهم ما بين 25 إلى 45 عاما، حيث يتمتعون في هذه المرحلة بخبرة تقنية متقدمة وذكاء ومهارات وغالبا ما يتم ارتكاب الجرائم الإلكترونية في هذه المرحلة من قبل هؤلاء الأفراد أثناء العمل في النوادي أو المرافق أو أطر تكنولوجيا المعلومات وهذا يعني أنهم مسؤولون عن أنظمة الكمبيوتر ويعرفون تقنيات التعامل مع أجهزة الكمبيوتر وتنفيذ أنشطتهم بطرق غير قانونية.[1]

رابعا: خوف المجرم المعلوماتي من الكشف عن جريمته

يتميز مرتكبو الجرائم الإلكترونية بالخوف الشديد من الكشف جرائمهم وشؤونهم غالبا ما تؤدي هذه الجريمة إلى صعوبات مالية وفقدان الوظيفة يأتي هذا الخوف أساسا من انتمائه لوسط اجتماعي متميز، مما قد يشكل خوف المجرم من فقدان مكانته الاجتماعية أو المهنية وما يساعد مجرمي الإنترنت في الحفاظ على سرية أنشطتهم هو طبيعة أنظمة الكمبيوتر نفسها، حيث تقوم أجهزة الكمبيوتر بعملها بطريقة ألية وهو ما لا يساعد في الكشف عن الجريمة إن لم تكن كلها والخطوات الواجب تنفيذها معروفة مسبقا، حيث لا توجد فرصة لتدخل عوامل غير متوقعة للكشف عن الجريمة.[2]

خامسا: مجرم عائد إلى الإجرام

يعود العديد من مجرمي الإنترنت لارتكاب جرائم أخرى في مجال الحوسبة رغبة في سد الثغرات التي أدت إلى التعرف عليهم وتقديمهم للمحاكمة في المرة السابقة، وهذا يؤدي إلى العودة إلى الجريمة وقد ينتهي بهم الأمر إلى ذلك في المرة القادمة لتقديمهم للمحاكمة.[3]

---

[1] فيصل كامل نجم الدين، واقع الجريمة الإلكترونية في مواقع التواصل الاجتماعي الحماية النظامية في دول مجلس التعاون الخليجي المجلد 5, العدد 04، جامعة عبد الحميد بن باديس مستغانم – الجزائر،2018، ص 15.

[2] عبد مجلي عبير، الجرائم الإلكترونية، ملتقى إشكالية المصطلح في علوم الإعلام والاتصال في العالم العربي، بيروت 2018، ص5.

[3] محمد سامي السيد أحمد، المرجع السابق، ص 158.

البند الثالث: أنماط مرتكبي الجرائم المعلوماتية

تختلف أنماط مرتكبي الجريمة المعلوماتية حسب طبيعة الجريمة إلى ثلاث أنماط حيث نجد من حيث الهدف وأيضا نجد من حيث مستوى الخبرة، أما النمط الثالث فيتمثل من حيث الأنماط وهذا ما سنبينه من خلال هذا العنوان.

أولا: من حيث الهدف

تختلف أنماط المجرم المعلوماتي من حيث الهدف إلى ذو الياقات البيضاء والرمادية وذو الياقات السوداء.

1-ذوي الياقات البيضاء the white Hat hackers

هم أولئك الذين يتبعوا أوامر السلطات لمهاجمة أجهزة الكمبيوتر وبشكل قانوني ومخطط، وتنظيم الهجمات كما هو مطلوب منهم[1]، بمعنى أن غايتهم تتمثل في كشف الثغرات الأمنية للأنظمة المعلوماتية ومعرفة نقاط ضعفها وتبليغ المسؤولين لتداركها.[2]

2-ذو الياقات الرمادية the Grey Hat hackers

يؤدي قراصنة الياقات الرمادية احيانا مهامهم كقراصنة اشرار وأحيانا لأسباب أخرى، وبعضهم لا يرون أي حرج في هجماتهم كما ينخرطون في مهام القراصنة لأغراض ايجابية مثل اختبار أنظمة الأمن و إيجاد الثغرات فيها،[3] أي أن غايتهم مزدوجة تتمثل أحيانا في الإبلاغ عن الثغرات في الأنظمة المعلوماتية وكشف نقاط ضعفها وأحيانا تكون غايتهم استغلال هذه الثغرات ونقاط الضعف والاستفادة منها.[4]

---

[1] سعدات محمد فتوح، المرجع السابق، ص 43.

[2] ربيعي حسين، المجرم المعلوماتي شخصيته وأصنافه، مجلة العلوم الإنسانية، المجلد 15، العدد 01، جامعة قسنطينة، 2015، ص 296..

[3] سعدات محمد فتوح، المرجع نفسه، ص 43.

[4] ربيعي حسين، المرجع نفسه، ص 296.

3-ذو الياقات السوداء the black Hat hackers

تتمثل غاية هذه الفئة في خرق الأنظمة المعلوماتية بصفة غير مشروعة من أجل الاستفادة منها وتحقيق الربح.[1]

ثانيا: من حيث مستوى الخبرة

تختلف أنماط مرتكبي الجريمة المعلوماتية من حيث مستوى الخبرة هي الأخرى إلى أنواع مختلفة حيث نجد العابثون ونجد أيضا المتلصصون.

1-العابثون Hackers

يشكل القراصنة العابثون فئة فريدة من قراصنة الإنترنت فهم لا يسعون وراء المال أوللانتقام بل يجدون متعة في اختراق أنظمة المعلومات، حيث يعتبرون ذلك تحديا لقدراتهم فمعظمهم ينتمي إلى هواة الحاسوب الذين يملكون شغفا بالتكنولوجيا ورغبة اختبار مهاراتهم في هذا المجال، وتعد دوافع القراصنة العابثين مختلفة عن دوافع قراصنة الإنترنت الاخرين فبينما يركز بعض القراصنة إما على السرقة أو التخريب أما القراصنة العابثون فينجذبون إلى عالم القراصنة بدافع الفضول وحب المعرفة والتعمق في عمل الأنظمة المعلوماتية عادة ما يكون المجرمون من هذا النوع أشخاصا عاديين يشغلون مناصب موثوقة ولديهم معارف ومهارات محددة مطلوبة في مجال الحوسبة والشبكات الإلكترونية.[2]

2-المتلصصون crackers

هم مجموعة من قراصنة الإنترنت ذو مهارات عالية في مجال تكنولوجيا المعلومات يميلون إلى استخدام مهاراتهم لأغراض ضارة ويقومون بكل ما هو سيء وشرير وكل ما يشكل جريمة جنائية من إتلاف وتخريب والإرهاب والابتزاز وكذلك سوء استخدام الأموال عن طريق الاحتيال والسرقة.[3]

---

[1] ربيعي حسين، المرجع السابق، ص 296.

[2] نهلة عبد القادر المومني، المرجع السابق، ص 83.

[3] خليلي سهام، خصوصية المحرم الإلكتروني، مجلة المفكر، العدد 15، جامعة محمد لمين دباغين، سطيف، س 2017 , ص 407.

ثالثا: من حيث الأنماط

تختلف طوائف المجرم المعلوماتي من حيث الأنماط هي الأخرى، حيث نجد الطائفة الأولى تتمثل في الممازحون والطائفة الثانية والمتمثلة في المخترق الخبيث المؤذي وحلال مشاكل الموظفين، أما الطائفة الرابعة هي دعاة التطرف ونجد أيضا طائفة المبرمجين والمهنيين.

1-الطائفة أولى الممازحون Pranksters

هم فئة من قراصنة الإنترنت يهدفون إلى إثارة الفوضى والضحك مع الأخرين دون قصد الإضرار بالضحية ويندرج تحت طائفة الممازحين صغار مجرمي المعلوماتية (الأحداث).[1]

2-المخترق الخبيث المؤذي malicieuse hackers

هم أشخاص ماهرون في استخدام تكنولوجيا اختراق أنظمة الكمبيوتر والشبكات، هدفهم إلحاق الضرر أو تعطيل أو تدمير البيانات ولا يسعون وراء الربح المادي ويندرج تحت هذه الطائفة منشئ فيروسات الكمبيوتر وبرامج التجسس والعديد من موزعيها.[2]

3-الطائفة الثالثة personnel problème solveurs

تعتبر هذه الطائفة من أكثر أنواع مجرمي الإنترنت المعلوماتية انتشارا، ويرتكب هذه الطائفة جرائم إلكترونية تهدف إلى إلحاق الضرر بالضحايا دون إمكانية حلها بالطرق التقليدية بما فيها الجرائم التقليدية.[3]

4-الطائفة الرابعة extrême avocates

هم أفراد من الجماعات الإرهابية الذين يعملون بشكل منظم لاستغلال تقنيات المعلوماتية ولتحقيق أهدافهم الإرهابية، هدفهم نشر الدعاية الإرهابية عبر الإنترنت وتمويل الأنشطة الإرهابية والاعتداء على الأنظمة المعلوماتية للأفراد و الحكومات المعادية بغرض ترهيبهم.[4]

---

[1] نائلة عادل محمد فريد قورة، المرجع السابق، ص 61.

[2] نائلة عادل محمد فريد قورة، المرجع نفسه، ص 62.

[3] بن شهرة شول، المرجع السابق، ص 16.

[4] ربيعي حسين، المرجع السابق، ص 298

5-الطائفة الخامسة المبرمجون les codeurs

هم فئة من المبرمجين ذوي الخبرة في مجال المعلوماتية لا تقل عن خمس سنوات يتمتعون بمهارات برمجية متقدمة في مجال القرصنة المعلوماتية، ويستخدم المبرمجون لغات البرمجة المختلفة لإنشاء وتعديل وتحديث البرامج المعلوماتية، حيث يقومون ببيع هذه المعلومات عبر الإنترنت لصالح مجرمي المعلومات.[1]

6-الطائفة السادسة المهنيون greed motivated

هذا النوع من مجرمي الإنترنت خطير يشكلون خطرا كبيرا على المجتمع عديمي الضمير يسعون فقط وراء الربح، كما يتميزون بالذكاء وأنهم منظمون يمتلكون مهارات عالية ويستخدمونها لتنظيم أنشطتهم، ومن أنشطتهم أنهم ينتجوا المواد الإباحية الإلكترونية تشمل المواد الإباحية القانونية وغير القانونية وغالبا ما تستهدف الأطفال وكذلك القمار الإلكتروني.[2]

المطلب الثاني: أنواع الجرائم المعلوماتية

عرفت الجريمة المعلوماتية اختلافا في تقسيمها حيث قسمها كل اتجاه وفقا لمعيار معين، فهناك من قسمها وفقا للأسلوب المتبع وهناك من قسمها على حسب دوافع ارتكابها وهناك من قسمها على حسب تعدد محل الاعتداء، كما قسمها المشرع الجزائري إلى جرائم واقعة بواسطة النظام المعلوماتي وجرائم واقعة على النظام المعلوماتي، وهو ما سنتطرق إليه في هذا المطلب حيث خصصنا **(الفرع الأول)** لمعرفة الجرائم الواقعة بواسطة النظام المعلوماتي، أما **(الفرع الثاني)** فخصصناه لتبيان الجرائم الواقعة على النظام المعلوماتي.

[1] ربيعي حسين، المرجع السابق، ص 299.

[2] ذياب موسى البدانية، جرائم الإلكترونية المفهوم والأسباب، ملتقى الجرائم المستحدثة في ظل التغيرات والتحولات الإقليمية والدولية عمان، س 2014، ص 21.

الفرع الأول: الجرائم الواقعة بواسطة النظام المعلوماتي

ترتكب هذه الجريمة بواسطة الحاسب الألي حيت يعتبر الوسيلة التي تسهل النتيجة الإجرامية ويزيد من جسامتها ويستخدم فيها النظام المعلوماتي أو برامجه كوسيلة للقيام بالجريمة،[1] وتنقسم الجرائم الواقعة بواسطة النظام المعلوماتي إلى جرائم ضد الأشخاص وجرائم ضد الأموال وضد أمن الدولة.

البند الأول: الجرائم ضد الأشخاص

إن أكثر الجرائم المعلوماتية انتشارا هي الجرائم الواقعة على الأشخاص، حيث أن الأشخاص هم الأكثر تعرضا للانتهاك وهو ما أكدته شركة **جارليك** التي تختص في مجال التأمين الإلكتروني حيث أن أكثر من 60٪ من الجرائم المعلوماتية تستهدف الأفراد ومن بين هذه الجرائم نجد ما يلي:

أولا: التهديد

يهدف الجاني من هذه الجريمة إلى زرع الخوف في المجني عليه والضغط عليه وتخويفه من الأضرار التي قد تلحقه أو تلحق أشخاص لهم صلة به إذا تم القيام بذلك الفعل ومن الضروري أن يكون التهديد بالوعيد بإلحاق الضرر ضد المجني عليه أو ماله أو ضد الغير، ولا يشترط فيه تنفيذ الفعل لأنها تشكل جريمة أخرى، ويكون التهديد إما بالأمر بالقيام بفعل أوالامتناع عنه أو للانتقام وقد أصبحت الأنترنت وجهاز الحاسب الألي من أبرز الوسائل التي يعتمدها الجاني للقيام بجريمته على غرار البريد الإلكتروني أين يقوم الجاني بإرسال رسالة إلى المجني عليه عبر البريد الإلكتروني يهدده فيها بارتكاب جريمة ضد ماله أو نفسه أو بنشر وإسناد له وقائع تمس شرفه ومكانته وإفشاء الأسرار الخاصة به أو عن طريق صفحات الويب،

[1] تميدلي رحيمة، خصوصية الجريمة الإلكترونية في القانون الجزائري، أعمال المؤتمر 14 للجرائم الإلكترونية، طرابلس، سنة 2017، ص 102.

أين يقوم الجاني بإنشاء موقع ويب خاص به ويقوم من خلاله بتهديد شخص أخر ويهدد بإتلاف موقع خاص بشركة ما.[1]

ثانيا: انتحال شخصية والتغرير والاستدراج

سميت هذه الجريمة من قبل بعض المختصين في مجال امن المعلومات بجريمة الألفية الجديدة وهذا نظرا لانتشار ارتكابها بشكل واسع وسرعة كبيرة خاصة في الوسط التجاري، ويقصد بانتحال شخصية قيام الجاني باستعمال شخصية شخص أخر بقصد الاستفادة من سمعته أو ماله أو منصبه، وتتخذ هذه الجريمة عبر شبكة الأنترنت وجهين هما انتحال شخصية الفرد وانتحال شخصية المواقع،[2] كما يمكن أن ترتكب هذه الجريمة لإخفاء هوية شخص مجرم أو تسهيلا لارتكابه جرائم أخرى ونظرا لسهولة ارتكاب هذه الجريمة وجب الاعتماد على وسائل متينة خاصة في مجال المعاملات التجارية عبر شبكة الأنترنت كاستخدام التوقيع الإلكتروني الذي يصعب ارتكاب هذه الجريمة والذي من خلاله يتم توثيق الهوية بشكل أمن.[3]

وبخصوص التغرير والاستدراج يكون ضحاياه في غالب الأحيان صغار السن الذين يستخدمون شبكة الأنترنت إذ يتم إهامهم من طرف المجرمين برغبتهم في تكوين صداقة عبر الأنترنت، والتي بعدها قد تتطور إلى لقاء في الواقع بين الطرفين وقد يكون الضحية في بلد والمجرم في بلد أي تتجاوز الحدود ولا يتم التبليغ في غالب الأحيان عن هذه الحوادث وذلك لعدم إدراك الضحايا بأنه مغرر بهم.[4]

ثالثا: القذف والسب

هي من الجرائم التقليدية لكن مع التطور التكنولوجي وبداية استعمال الأنترنت أصبحت هذه الجريمة ترتكب بأسلوب حديث، وذلك من خلال بث المعلومات والفضائح والصور والرسائل التي تحتقر شخص آخر من أجل المساس بشرف المجني عليه، حيث تعتبر الأنترنت مسرحا

---

[1] خالد حسن أحمد لطفي، المرجع السابق، ص 28-29.

[2] صغير يوسف، المرجع السابق، ص 50-51.

[3] خالد حسن أحمد لطفي، المرجع نفسه، ص 30.

[4] صغير يوسف، المرجع السابق، ص 51.

لارتكاب العديد من الجرائم المتعلقة بالقذف والسب،[1] وتتمثل في نشر إشاعات وأسرار يتم الحصول عليها بطريقة غير مشروعة وأعطى المشرع أهمية بالغة لهذه الجريمة وذلك نظرا لكونها تمس بالحياة الخاصة للأفراد، وقد حظيت الحياة الخاصة للأفراد بحماية قانونية ودستورية في جل تشريعات الدول ومن بينها التشريع الجزائري الذي أعطى أهمية بالغة لها،[2] ويتبين ذلك من خلال نصوص المواد 39 /01 من الدستور التي تنص على أنه" تضمن الدولة عدم انتهاك حرمة الإنسان"، وكذلك المادة 47 من التعديل الدستوري لسنة 2020 التي تنص على أنه "لا يجوز انتهاك حرمة حياة المواطن الخاصة وحرمة شرفه ويحميها القانون وسرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة".[3]

وتتمثل أركان الجريمة في الركن المادي والمعنوي وركن ثالث وهو ركن العلنية، حيث يتكون الركن المادي من عنصرين أساسيين هما فعل الإسناد أي أن يقوم الجاني بنسب واقعة إلى المجني عليه بأي وسيلة من وسائل التعبير، أما العنصر الثاني فهو موضوع الإسناد وذلك أن الواقعة التي يسندها الجاني إلى المجني عليه تمس بشرفه واعتباره ويجب أن تكون هذه الواقعة المسندة إلى المجني عليه قد تتسبب في عقابه أو تشويه سمعته أمام الناس، وبالنسبة للركن المعنوي فيتطلب القصد الجنائي العام والذي يتطلب العلم والإرادة أي علم الجاني بأنه يسند وقائع قد تؤدي إلى عقاب المجني عليه أو احتقاره أمام الناس وتمس بكرامته وشرفه وتتجه إرادته إلى القيام بفعل القذف، أما العلنية فيتمثل في الجهر بالشيء وإظهاره وإعلام الناس به.[4]

أما السب فقد نص عليه المشرع الجزائري من خلال نص المادة 298 مكرر وعلى غرار القذف هو أيضا من الجرائم التقليدية ومع تطور التكنولوجي وظهور الأنترنت تزايدت نسبة هذه الجريمة، ويعرف السب على أنه خدش شرف شخص والمساس باعتباره بدون أن يتضمن ذلك

---

[1] علي صبيح عبد اللامي، المرجع السابق، ص 85.

[2] بن مكي نجاة، المرجع السابق، ص 57.

[3] المادة 39 و47 من المرسوم الرئاسي رقم 20-442 المؤرخ في 30 ديسمبر 2020 المتعلق بإصدار التعديل الدستوري المصادق عليه في إستفتاء أول نوفمبر 2020، ج.ر.ج.،ع 82.

[4] علي صبيح عبد اللامي، المرجع نفسه، ص 89.

إسناد واقعة إليه، ويتمثل الركن المادي لهذه الجريمة في التعبير الذي يكون فيه خدش الشرف واعتبار المجني عليه وذلك بأي وسيلة من وسائل التعبير ومن بينها المواقع الإلكترونية أوالبريد الإلكتروني أو مختلف وسائل التواصل الاجتماعي.

ويقوم هذا الركن على عنصرين هما فعل الإسناد وهو أن يقوم الجاني بإسناد عيب معين يبين فيه كل ما نقص في صفات المجني عليه كوصفه بأوصاف غير لائقة، والعنصر الثاني يتمثل في تعييب المجني عليه وذلك بوصفه بعيب يبين احتقاره دون تحديد واضح لهذا العيب، وقد يكون السب صريحا وضمنيا، أما بالنسبة للركن المعنوي لجريمة السب فيتمثل في القصد الجنائي بعنصريه هما العلم والإرادة أي علم الجاني بمضمون ما قام به وأنه يعتبر سبا وتتجه إرادته إلى القيام بها اتجاه المجني عليه، وبالنسبة لجريمة السب في الشبكة المعلوماتية نجد فيها ركن العلنية وذلك عن طريق قيام الجاني بإسناد عبارات إلى شخص معين ويطلع عليها الجمهور وذلك من خلال غرف الدردشة أو مواقع التواصل الاجتماعي التي يطلع عليها الجمهور وبما أنها متاحة فتتحقق العلنية حتى ولم يشاهدها الأفراد.[1]

رابعا: جريمة الإخلال بالأداب العامة

لقد شجعت الأنترنت على صناعة ونشر المواقع الإباحية ووفرت لها الوسائل وساهمت في عرضها من خلال صور وفيديوهات وحوارات وأصبحت في متناول الجميع،[2] وتدخل ضمن هذه الجرائم جريمة ارتياد المواقع الإباحية والشراء منها والاشتراك فيها وإنشائها وانتشرت المواقع والأفلام الإباحية بشكل كبير والاعتداء على حرمة الأشخاص وأعراضهم وذلك بتركيب صور فاضحة أو الاعتداء على ملكية الشخص في الصورة ووضعها في أوضاع مخلة بالحياء والآداب العامة، ومن أمثلة هذه الجريمة ما قام به مجموعة من الأشخاص بإكراه عدد من الأطفال وإجبارهم على ممارسة الشذوذ الجنسي مع بعضهم ويقومون بتصويرهم وعرض تلك

[1] علي صبيح عبد اللامي، المرجع السابق، ص 90.

[2] خالد حسن أحمد لطفي، المرجع السابق، ص 31.

المقاطع والصور على شبكة الأنترنت ويتم مشاهدتها وتحميلها بمقابل مادي عن طريق الاشتراك.[1]

وكذلك من الجرائم التي تمس بالآداب العامة عبر وسائل التواصل الاجتماعي وشبكة الأنترنت نجد تحريض القاصرين على ممارسة أنشطة جنسية غير مشروعة وإغوائهم بممارستها عبر وسائل الإلكترونية والتحرش الجنسي بالقاصرين عبر الكمبيوتر وتسهيل نشر المواد الفاحشة عبر الأنترنت واستخدام الأنترنت للترويج للدعارة والحصول على صور وهويات بطريقة غير مشروعة لاستغلالها في أنشطة غير مشروعة.[2]

خامسا: الاعتداء على حرمة الحياة الخاصة

لقد أصبحت وسائل التكنولوجية الحديثة تشكل خطرا يهدد الحياة الخاصة للفرد، وأصبح التسلل إلى خصوصيات الأفراد والاعتداء عليها أمرا سهلا، حيث أنه مع التطور التكنولوجي أصبحت الحياة الخاصة تحت التهديد نظرا لامتلاك الغير وسائل التكنولوجية، فأصبحت الحياة الخاصة بيد هؤلاء دون أن يعلم أو يشعر صاحبها بذلك.

واتخذت من هذه التكنولوجيا كوسيلة للدخول في الحياة الخاصة للأفراد وحتى الاعتداء عليها وتحقيق الربح من خلالها، ومع زيادة هذا النوع من الجرائم كان من الضروري على الدول أن تصدر تشريعات وقوانين لوقف هذا النوع من الجرائم،[3] حيث نص المشرع الجزائري من خلال نص المادة 39 من دستور 2020 التي تنص على أنه" تضمن الدولة عدم انتهاك حرمة الإنسان".[4]

وأوردها أيضا في المواد من 303 مكرر إلى 303 مكرر03 من قانون العقوبات، وذلك تماشيا مع الاتفاقية الأوروبية لمكافحة الإجرام المعلوماتي والاتفاقية العربية لمكافحة جرائم تقنية

[1] حسين طاهري، المرجع السابق، ص 22.

[2] يزيد بوحليط، المرجع السابق، ص 65-66.

[3] لينا محمد الأسدي، مدى فعالية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية، دار الحامد، ط أولى، الأردن عمان، 2015، ص 38.

[4] المادة 39 المرسوم الرئاسي، 20-442، المصدر السابق.

المعلومات، ومن الجرائم التي تدخل ضمن صور الاعتداء على حرمة الحياة الخاصة نجد جريمة التقاط الأحاديث والصور دون رخصة المنصوص عليها في المادة 303 مكرر، ونلاحظ من خلال ما جاء في نص المادة أن المشرع الجزائري أورد عبارة بأي تقنية كانت وذلك لغرض مواكبة التطورات التكنولوجية والتقنية نظرا لكثرة ارتكاب هذه الجريمة عن طريق هذه الوسائل، كما نجد صورة أخرى للاعتداء على حرمة الحياة الخاصة والمتمثلة في جريمة إعلان التسجيل أو الصور أو الوثائق المنصوص عليها في المادة 303 مكرر.[1]

البند الثاني: الجرائم الواقعة على الأموال

ساهم ظهور شبكة الأنترنت في التطور في مختلف المجالات خاصة في مجال المعاملات التجارية، حيث أصبحت معظم المعاملات تتم عبر شبكة الأنترنت على غرار البيع والشراء وتطورت من خلاله وسائل الدفع، وفي ظل هذا التطور المالي عبر شبكة الأنترنت انتهز المجرمين الفرصة من أجل السطو عليها، وظهرت عدة جرائم ضد الأموال عبر شبكة الأنترنت مثل السطو والسرقة والتحويل الإلكتروني غير المشروع للأموال وقرصنة أرقام البطاقات مغنطيسية،[2] والعديد من الجرائم والتي سنذكر منها ما يلي:

أولا: انتهاك حقوق الملكية الفكرية

أصبح النظام المعلوماتي يعتبر أداة للاعتداء على حقوق الملكية الفكرية، ويتجلى ذلك من خلال السطو على المعلومات التي يتضمنها نظام معلوماتي أخر وتخزين واستخدام المعلومات دون علم صاحبها أو أخذ إذن منه إذ يعتبر اعتداء على الحقوق المعنوية وعلى قيمتها المادية،[3] إذ تعتبر الملكية مال قائم بذاته والذي يتكون من برامج الحاسوب ومحركات البحث وغيرها، وقد نص عليها المشرع الجزائري من خلال الأمر 03-05 المتضمن حقوق المؤلف والحقوق المجاورة، ووفر الحماية لأي مصنف وأسلوب تعبيره ودرجة جدارته ووجهته

[1] يزيد بوحليط، المرجع السابق، ص 221 إلى 225.

[2] صغير يوسف، المرجع السابق، ص 44.

[3] خالد حسن أحمد لطفي، المرجع السابق، ص 37.

بمجرد إيداعه سواء كان المصنف مسجلا أو في أمانة دعامة تسمح بإحالة المصنف إلى الجمهور وإبلاغه، وقد نصت المادة 12 من الأمر 03-05 بأن المؤلف يتمتع بحقوق مادية ومعنوية على المصنف الذي أبدعه.[1]

مع ظهور تكنولوجيا المعلومات ظهرت معها ما يسمى بالمصنفات الرقمية وهي لا تختلف عن التقليدية إلا في كونها تكون إلكترونية على عكس التقليدية التي تكون في شكل ورقي، وقد حظيت الملكية الفكرية بأهمية كبيرة على المستوى الدولي والوطني خاصة مع ظهور شبكة الأنترنت، حيث أدرك المشرعين خطورة الجريمة المعلوماتية على الملكية الفكرية إذ قاموا بتوقيع مجموعة من الاتفاقيات وتشريع القوانين للحد من الاعتداء على الملكية الفكرية بوسائل تكنولوجيا المعلومات والاتصال، ومن بين القوانين والاتفاقيات نجد اتفاقية بارن كأول اتفاقية في مجال تأصيل الملكية الفكرية، وكذلك اتفاقية بودابست المتعلقة بالجرائم المعلوماتية والتي من خلالها تم منع الاعتداء على الملكية الفكرية، أما على المستوى الوطني فعمل المشرع الجزائري في قواعد الملكية الفكرية وذلك لمواكبة التطور التكنولوجي وحماية الملكية الفكرية في المجال المعلوماتي.[2]

ثانيا: التزوير المعلوماتي

يعرف التزوير على أنه هو تغيير الحقيقة في محرر بالطرق التي حددها القانون، وأن يكون التغيير من شأنه أن يلحق ضررا بالغير،[3] ومع التطور التكنولوجي وظهور الحاسب الألي أصبح التزوير يتم أيضا عن طريق تقنية المعلومات وظهر ما يسمى بالتزوير المعلوماتي، وهو الذي يتم على محررات الحاسب الألي سواء كانت محررات ورقية مثل التي يتم طباعتها عن طريق ألة الطباعة أو كانت مرسومة عن طريق الراسم وتقع الجريمة عند قيام الموظف بتغيير الحقيقة مثل موظف البنك الذي يغير الحقيقة في البيان البنكي أين يقوم بإثبات سداد جزء من

[1] حسين طاهري، المرجع السابق ص 54.

[2] رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة دكتوراه، جامعة تلمسان، س.ج 2017-2018 ص 228-229.

[3] حسين طاهري، المرجع نفسه، ص 92-93.

الفاتورة من صاحب الشأن إلا أنه في الحقيقة قام بسدادها كلها، وكذلك من صور تزوير المعلومات إساءة استخدام الصورة حيث يقوم بتغيير الصورة في الوثيقة المطبوعة ويتم عرضها على شاشة الحاسب الألي.[1]

ثالثا: القرصنة الإلكترونية

هي عملية تتم عن طريق شبكة الأنترنت وتتمثل في اختراق الحاسوب أو المواقع والتي تكون غالبا متصلة بشبكة الأنترنت، حيث يقوم بهذه الجريمة شخص أو عدة أشخاص لهم دراية ومعرفة باختراق برامج الحاسوب وكيفيات وطرق إدارتها أي أن لهم مستوى عالي في مجال البرمجة ويستعطون بواسطة برامج مساعدة من اختراق الحاسوب والاطلاع على معلوماته.[2]

تشير القرصنة الإلكترونية إلى استعمال وسائل الاتصال وتكنولوجيا المعلومات الحديثة في أعمال غير مشروعة لغرض التحايل على أنظمة المعالجة الألية للبيانات، وبالتالي فهي دخول غير مصرح به إلى أجهزة الغير وشبكاتهم الإلكترونية بهدف المساس بسلامة المحتوى أو تعطيل إمكانيات أنظمة الكمبيوتر أو المساس بالسرية.[3]

تتنوع القرصنة الإلكترونية وذلك تبعا للدافع والغاية المراد تحقيقها، حيث نجد القرصنة الانتقامية وذلك رغبتا في الانتقام ورد الهجمات مثل الهجمات الإلكترونية التي شنها الإيرانيون ضد صحف ومواقع إلكترونية للكيان الصهيوني، ونجد أيضا القرصنة السياسية وهي أكثر الجرائم انتشارا حيث أن 58% من عمليات القرصنة التي وقعت قام بها قراصنة ينشطون في المجال السياسي، كما نجد أيضا القرصنة الذاتية وقرصنة الهواة حيث تتمثل الأولى في قرصنة بعض الدول لنفسها لاتهام دول أخرى بهذه القرصنة مثل إتهام الولايات المتحدة الأمريكية والدول الغربية لروسيا أما الثانية فتتمثل في قيام بعض القراصنة باختراق المواقع الشخصيات

[1] لينا محمد الاسدي، المرجع السابق، ص 52-53.

[2] مريم بالطه وأسيا برغيت، الأمن المعلوماتي في مواجهة القرصنة الإلكترونية، دراسات في حقوق الإنسان، المجلد 06 ، العدد 01، جامعة الجزائر، 2022.

[3] بن شريف أحلام وبوغرارة الصالح، القرصنة الإلكترونية أنواعها أشكالها وطرق التصدي لها، المجلة الجزائرية للعلوم السياسية والعلاقات الدولية، المجلد 05، العدد01، جامعة الجزائر، 2012.

العامة بغية جمع المعلومات أو المحادثات أو الصور الخاصة بالشخصية ويتم نشرها إلى العلن أو ابتزازهم من أجل الحصول على المال.[1]

رابعا: التحويل الإلكتروني غير المشروع للأموال

مع بداية استخدام البطاقات الائتمانية عبر شبكة الأنترنت ظهر الكثير من المجرمين الذين يتسللون للسطو عليها لكونها نقود إلكترونية، وهذا الأمر ليس بالصعب فلصوص بطاقات الائتمان بإمكانهم سرقة الألاف من أرقام البطاقات في يوم واحد وذلك عبر شبكة الأنترنت ويقوم ببيع المعلومات لأشخاص أخرين وتكون العملية من خلال الحصول على كلمة السر الخاصة بملفات أنظمة الكمبيوتر الخاص بالمجني عليه فيقوم الجاني بالدخول إلى النظام المعلوماتي وتكون غالبا من طرف العاملين الذين يقومون بإدخال البيانات في ذاكرة الجهاز، أومن قبل المتواجدين على الشبكة خلال وقت عمليات تبادل البيانات،[2] وتتم عملية التحويل ببعض الطرق مثل الاحتيال والنصب وذلك بإيهام المجني عليه بوجود مشروع من أجل أن يمنحهم المال أو باستخدام بطاقات الدفع الإلكترونية عبر الأنترنت وذلك بالتحويل الإلكتروني من حساب بطاقة العميل إلى الدائن عن طريق التسوية الإلكترونية للهيئات الدولية.[3]

خامسا: سرقة المال المعلوماتي

تتمثل جريمة سرقة المال المعلوماتي في أخذ المعلومات واستخدامها عبر شبكة الأنترنت وتخريب النسخة الأصلية وحرمان صاحبها منها فالجاني يستولي على المعلومات المخزنة في الجهاز وإتلافها يؤدي إلى تحقق فعل الاختلاس، وتعتبر المعلومات مال مملوك للغير وبذلك تتحقق عليها جريمة السرقة كما تتحقق هذه الجريمة من خلال أسلوبين الأول يتمثل في الالتقاط غير المشروع للبيانات وذلك باستخدام الطرق التالية الخداع والتجسس المعلوماتي وتقنية تفجير الموقع المستهدف، أما الأسلوب الثاني فيتمثل في سرقة منفعة

[1] بن شريف أحلام وبوغرارة الصالح، المرجع السابق.

[2] صغير يوسف، المرجع السابق، ص 44-45.

[3] خالد حسن أحمد لطفي، المرجع السابق، ص 34.

الحاسب الألي ويقصد به استخدام الحاسب الألي للغير دون علم مالكه للانتفاع به وتحقيق أغراض شخصية أو تجارية، فهي لا تهدف إلى غرض إجرامي وإنما تهدف إلى تحقيق منافع مالية إذ يقوم الجاني باستخدام الحاسب الألي من أجل الدخول إلى شبكة الأنترنت والوصول إلى البنوك والمصارف وتحويل الأموال إلى حسابات أخرى.[1]

سادسا: تجارة المخدرات

كان في القديم الأولياء يحذرون أولادهم من رفقاء السوء وذلك خوفا من أن يؤثروا عليهم سلبا في تصرفاتهم وأفعالهم خاصة في جرهم وتعريفهم بأفة المخدرات التي أصبحت تتفشى في جميع مجتمعات العالم، إلا أنه وبعد ظهور شبكة الأنترنت زادت مخاوف الأولياء على أبنائهم إذ مع ظهورها ظهرت بعض المواقع ما يعرف بمواقع السوء ومن بينها مواقع تروج لتجارة المخدرات، بل ذهب إلى أبعد من ذلك أين أصبحت تعلم وتنشر كيفية صناعتها وزراعتها بمختلف أنواعها وأصنافها، حيث يدخل المراهق إلى مثل هذه المواقع ويسعى إلى تطبيق ما جاء فيها.

بالرغم من خطورة هذه المواقع ومدى تأثيرها على الأطفال والمراهقين وحتى الشباب إلا أنه لم تدق ناقوس الخطر بعد ولم يزد الاهتمام بأثارها السلبية مثل الاهتمام الذي لقيته مواجهة إنشاء المواقع الإباحية، إلا أنه قامت بعض الدول بعقد مؤتمرات واتفاقيات الدولية على غرار اتفاقية مكافحة المخدرات لسنة 1961 واتفاقية المؤثرات العقلية لسنة 1971 واتفاقية الأمم المتحدة لمكافحة الإتجار غير مشروع للمخدرات والمؤثرات العقلية لسنة 1988، أما على المستوى العربي نجد الاتفاقية العربية لمكافحة الإتجار غير المشروع للمخدرات والمؤثرات العقلية لسنة 1986 والقانون النموذجي الموحد للمخدرات.[2]

[1] خالد حسن أحمد لطفي، المرجع السابق، ص 32.

[2] عبد الصبور عبد القوي على حصري، المحكمة الرقمية والجريمة المعلوماتية، مكتبة القانون والاقتصاد، ط أولى، السعودية 2012، ص 148-149.

سابعا: الاحتيال المعلوماتي

مع ظهور الثورة التكنولوجية وما تبعها من ظهور البنوك الإلكترونية وتحويل الأموال إلكترونيا زاد من ارتكاب الجريمة المعلوماتية خاصة جريمة الاحتيال المعلوماتي، حيث ركزت المؤسسات المالية مثل البنوك والمصارف عملها بشكل واسع باستخدام الأنظمة المعلوماتية لإجراء المعاملات والتحويلات المالية، وذلك للقيام بهذه المعاملات في أي مكان في العالم دون الحاجة إلى التنقل المباشر للمصرف وازداد ارتكاب جرائم الاحتيال المعلوماتي في نطاق واسع وتسبب في تكبد خسائر فادحة الأمر الذي يجعل الأفراد يفقدون الثقة في الوسائل التقنية الحديثة من أجل نقل أموالهم، ويعرف الاحتيال المعلوماتي على أنه "سلوك احتيالي يتعلق بعملية التحسيب الإلكتروني من أجل كسب فائدة ومصلحة مالية"، وعرفته هيئة الأمم المتحدة بأنه" إدخال البيانات أو محوها أو تعديلها أو كبتها أو برامج الحاسوب أو التدخل المؤثر في معالجة البيانات التي تسبب خسارة اقتصادية أو فقد حيازة ملكية شخص أخر بقصد الحصول على كسب اقتصادي غير مشروع له أو لشخص أخر.

إن الاحتيال المعلوماتي مثله مثل الجرائم المعلوماتية بوجه عام يمكن أن يكون مرتكبه من الأشخاص المسموح لهم الدخول إلى نظام الحاسب الآلي، وقد يكون غير مسموح لهم بالدخول.[1]

ترتكب جريمة الاحتيال الإلكتروني من خلال مجموعة الوسائل ونذكر منها التلاعب في مرحلتي إدخال وإخراج البيانات والتلاعب في البرامج والتلاعب في البيانات التي يتم تحويلها عن بعد، وأيضا استعمال شيفرة غير صحيحة للدخول إلى نظام مدفوع الأجر.[2]

البند الثالث: الجرائم الواقعة على أمن الدولة

أصبحت النظم المعلوماتية تستخدم في ارتكاب بعض الجرائم تمس أمن الدول ومصالحها، حيث يؤدي هذا النوع من الجرائم إلى الفتك بالمجتمعات والدول، ومن بين الجرائم

[1] نهلاعبد القادر مومني، المرجع السابق، ص 186-188-189.

[2] نهلا عبد القادر المومني، المرجع نفسه، ص 190-193-194-195.

التي تقع على أمن الدولة نجد جريمة الإرهاب، حيث أصبحت الجماعات الإرهابية تستخدم الأنترنت ووسائل التواصل الاجتماعي في الترويج للأفكار والتجنيد وغيرها، وكذلك نجد جريمة التجسس والتي أصبحت بعض الدول تستخدم الأنترنت للتجسس على الدول الأخرى والاطلاع على أسرارها وقواتها العسكرية والاقتصادية.

أولا: جريمة الإرهاب

لقد أدت التطورات التي عرفها العصر الحديث بروز ظاهرة عالمية وهي ظاهرة الارهاب وذلك نتيجة العوامل الاجتماعية والثقافية والسياسية التي اقرتها التطورات والسرعة المتلاحقة، حيث برزت العديد من الجماعات المسلحة والقيام بالعمليات الارهابية بمختلف انحاء العالم، واصبحت هذه الجماعات تقوم ببث ونشر ثقافة الارهاب عبر شبكة الانترنت من خلال مواقع تمثل المنظمات الارهابية والتي اصبحت تزداد مع تزايد هذه المنظمات.[1]

يعرف الارهاب الالكتروني على أنه هو العدوان او التخويف او التهديد المادي اوالمعنوي الذي يصدر من الدولة او الجماعات او الافراد على دينه او نفسه او عرض او عقله او ماله بدون وجه حق، وذلك عن طريق استعمال الوسائل الالكترونية، حيث تستغل المجموعات الارهابية وسائل الاتصال وشبكة الانترنت لغرض تخويف وترويع الاخرين وتهديدهم،[2] كما يعرف ايضا على أنه التوظيف السلبي لشبكة الانترنت بإثارة الفزع والتخويف والتهديد والعدوان بهدف تحقيق اهداف معينة.[3]

تستخدم الجماعات الارهابية الشبكة المعلوماتية للقيام بعملياتها الإرهابية، وذلك من خلال البريد الالكتروني وإنشاء مواقع على الانترنت واختراق المواقع ومع تزايد هذا النوع من الجريمة والتي تمس بأمن الدولة، مما دفع بعض الدول الى إنشاء آليات لمواجهة هذه الظاهرة ومن بين هذه الدول نجد الولايات المتحدة الأمريكية، حيث أنشأ الرئيس الأمريكي بيل كلنتون لجنة

[1] صغير يوسف، المرجع السابق، ص 55.

[2] رفدة عيادة الهاشمي، الإرهاب الإلكتروني دار أمجد للنشر والتوزيع الطبعة الأولى سنة 2019، ص 20-21.

[3] علي صبيح عبد اللامي، المرجع السابق، ص 153.

خاصة تعمل على حماية الأماكن الحساسة في أمريكا أين قامت هذه اللجنة بتحديد الأماكن التي من المحتمل أن تكون مستهدفة مثل مصادر الطاقة والاتصالات، وأيضا تم إنشاء مركز الحروب المعلوماتية من قبل وكالة الاستخبارات المركزية وتم توظيف الالاف من خبراء أمن المعلومات.[1]

ثانيا: جريمة التجسس الالكتروني

يعتبر التجسس من الجرائم القديمة، حيث كان يتخذ أشكالا مختلفة وأساليب عديدة من أجل تحقيق غايات متباينة، قد تتعلق بالأمور العسكرية أو السياسية وحتى الاقتصادية والصناعية إذ أصبحت تشكل خطرا على أمن الدولة ومصالحها، ومع ظهور الرسائل التقنية أضحت ترتكب هذه الجريمة من خلال هذه الرسائل ومنه ظهرت ما تعرف بالجريمة التجسس الإلكتروني فأصبح الأفراد وحتى الدول يرتكبون هذه الجريمة لتحقيق غرض معين.[2]

تعددت التعريفات لجريمة التجسس المعلوماتي حيث عرفت في قانون الجرائم المعلوماتية على أنها دخول الجاني إلى الشبكة المعلوماتية أو نظام المعلومات للحصول على محتوى إلكتروني ليس متاح للجمهور ويمس بالأمن الوطني والعلاقات الخارجية للدول أو السلامة العامة والاقتصاد الوطني.[3]

ويعرف أيضا بأنه استعمال وسائل تقنية المعلومات من أجل الدخول بشكل غير قانوني في أنظمة المعلومات الإلكترونية للدول والحكومات والتنصت عليها لغرض الحصول على المعلومات المهمة التي تتعلق بنظامها وأسرارها المتعلقة بالجانب العسكري والأمني والسياسي والاقتصادي.[4]

---

[1] عبد الصبور عبد القوي على مصري، المرجع السابق، ص 161.

[2] ضرغام جابر عطوش أل مواش، جريمة التجسس المعلوماتي، المركز العربي، ط أولى، مصر، 2017، ص 11.

[3] علي صبيح عبد اللامي، المرجع السابق، ص 156.

[4] علي عبود جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، منشورات زين الحقوقية، ط أولى، بيروت، س 2013، ص 569.

ويتمثل الركن المادي لجريمة التجسس في فعل الدخول وبشكل غير قانوني وغير مشروع في نظام المعلومات الإلكتروني لدولة ما باستخدام تقنية المعلومات الحديثة وتتمثل صورة الدخول في جريمة التجسس المعلوماتي في عدة صور أهمها قيام الفاعل بتشغيل أجهزة نظام معلوماتي مغلق والاطلاع على البيانات الموجودة فيه، أو الدخول في نظام معلومات إلكتروني للحكومات والدول باستخدام برامج للدخول فيها وهذا للاطلاع على المعلومات الموجودة فيها دون إذنها ولا يشترط الاطلاع على الملفات والمعلومات الموجودة في النظام لتقع جريمة التجسس بل يكفي أن يدخل الجاني للنظام حتى وإن لم يتمكن من الاطلاع وفتح الملفات والمعلومات.

أما الركن المعنوي لهذه الجريمة يستلزم توافر القصد الجنائي لكونها من الجرائم العمدية ويتمثل في نية الحصول على معلومات تمس أمن الدولة داخليا أو خارجيا أما إذا وقع الدخول في النظام عن طريق الخطأ لا تقوم الجريمة.[1]

الفرع الثاني: الجرائم الواقعة على النظام المعلوماتي

يسمى النظام المعلوماتي بأنه كل مجموعة تتكون من وحدة أو كل وحدة تعالج المعلومات بطريقة محددة والتي تحتوي على الذاكرة والبرامج والبيانات وأجهزة الإدخال والإخراج وأجهزة الربط ومجموعة العلاقات التي تربط بينها وينتج نتيجة محددة وهي معالجة البيانات، وبالتالي يكون هذا المركب محصن لنظام الحماية الفنية،[2] وعليه تنقسم الجرائم الواقعة على النظام المعلوماتي إلى ثلاث جرائم، وهي جرائم ضد المكونات المادية والجرائم الواقعة على برامج النظام المعلوماتي والجرائم المعلوماتية الواقعة على المعلومات المدرجة بالنظام المعلوماتي.

البند الأول: الجرائم الواقعة على المكونات المادية للنظام المعلوماتي

يراد بالمكونات المادية للنظام المعلوماتي أنها هي الأجهزة والمعدات المتصلة بالنظام والمستخدمة في تشغيله مثل الأقراص المدمجة الأسطوانات والأشرطة والكابلات ونظرا للطبيعة

[1] علي عبود جعفر، المرجع السابق، ص 580 إلى 582.

[2] علي صبيح عبد اللامي، المرجع السابق، ص 165.

المادية لهذه الأجهزة فإن الجرائم المرتكبة ضدها تعتبر تقليدية مثل السرقة وخيانة الأمانة والإتلاف العمدي والإحراق والعبث بمفاتيح التشغيل مما تسبب في خسائر فادحة، وقد حدثت مثل هذه الجرائم في فرنسا وأسفرت على سقوط معدات المؤسسات الكبيرة والمتخصصة في بيع الأنظمة وتوثيق المعلومات الحسابية وقدرت الأضرار بنحو 5 ملايين فرنك فرنسي.[1]

وفي السياق نفسه يتكون الحاسوب من جزئين رئيسيين هما المكونات المادية (المكونات الصلبة) والمكونات غير الصلبة (البرامج أو المعطيات)، وتصنف جرائم الاعتداء على كيانات الحاسوب المادية من بين الجرائم التقليدية، حيث تتعلق بالاعتداء على مال منقول علاوة على ذلك تخضع جرائم الاعتداء على كيانات الحاسوب المادية لقواعد ومبادئ ونصوص القانون الجنائي، وترتكب هذه الجرائم تعبيرا عن موقف سياسي من التقنية وقد تستهدف هذه الجرائم أمن أو أنظمة الدولة، وكذلك قد تستخدم التقنية كأداة لرفض قوة الدولة وفعالية نظامها.[2]

البند الثاني: الجرائم الواقعة على البرامج المعلوماتية

هي مجموعة من الجرائم التي تتضمن تقديماً أو إنتاجاً أو توزيعاً أو حوز جهاز أو برنامجا معلوماتيا أو بيانات معدة أو كلمات سر أو رموز دخول بغرض ارتكاب أي من جرائم تقنية المعلومات.[3]

يقدم البرنامج المعلوماتي على مجموعة من التعليمات والأوامر التي يمكن للحاسوب تنفيذها وتكون جاهزة لأداء مهمة ما، أما البرامج المعلوماتية فهي عبارة عن مجموعة من البرامج والبيانات التي يمكن أن تؤدي وظائف معينة، وبالتالي فإن البرامج المعلوماتية ليست مادية.[4]

---

[1] بوضياف أسمهان، المرجع السابق، ص 359.

[2] علي صبيح عبد اللامي، المرجع السابق، ص 170.

[3] عماد مفلح الحسبان وعزالدين أحمد النعيمي وعدنان محمد الضمور وياسر طالب الخزاعلة، الجرائم المستحدثة (المعلوماتية، الإلكترونية، السيبرانية)، دار الخليج للنشر والتوزيع، 2023 الأردن، ص 140.

[4] فارس محمد العمارات، جرائم العصر من الرقمية إلى السيبرانية، دار الخليج للنشر والتوزيع، ط الأولى، الأردن 2023، ص 46.

أولا: البرامج التطبيقية

هي جميع البرامج التي كتبها المبرمجون في مختلف المؤسسات للاستفادة من إمكانيات الحاسوب في إنجاز الأعمال بكفاءة وفعالية،[1] وكذلك هي برامج مصممة لأداء مهام محددة تلبي احتياجات المستخدمين في مختلف المجالات ويمكن استخدامها من قبل جميع العملاء سواء كانوا شركات أو أشخاصا طبعيين بغض النظر عن مستوى خبرتهم، تعمل أيضا على جميع أنواع الحواسيب سواء كانت أجهزة كمبيوتر مكتبي أو أجهزة حاسوب محمولة أو هواتف ذكية أو أجهزة لوحية ضف إلى ذلك تكتب البرامج التطبيقية بلغات برمجة عالية المستوى.[2]

يقوم الجاني بتحديد البرنامج والتلاعب به لتحقيق مكاسب مالية من خلال تعديله أوتغييره لغرض الاستفادة منه بطريقة غير مشروعة، حيث يتم اختلاس النقود حتى ولو كان مبلغا صغيرا عن طريق اقتطاعه بمرور الوقت لتحقيق فائدة دون إثارة الشبهات أما التلاعب فيأخذ عدة طرق فقد يتم عن طريق إخفاء البرنامج الفرعي داخل البرنامج الأصلي، كذلك يسمح له بالدخول غير المصرح به إلى النظام المعلوماتي كما يمتاز هذا البرنامج بالصعوبة لدقته وصغر حجمه.[3]

ثانيا: برامج التشغيل

هو البرنامج المسؤول عن تشغيل الحاسوب وأي برنامج حاسوبي آخر لا ينفصل عن نظام التشغيل، كما يعتبر نظام التشغيل بمثابة حلقة الوصل بين المستخدم والكمبيوتر فهو يتيح للمستخدم تفاعلاً مع الجهاز من خلال واجهة سهلة الاستخدام، بالإضافة إلى ذلك يقدم نظام التشغيل مجموعة واسعة من الأوامر التي تمكن المستخدم من إدارة الملفات وتصميم البرامج وفتحها وحفظها،[4] ومن الجرائم التي تقع عليها المصيدة التي تزرع عيوب والثغرات في البرنامج

---

[1] محمد هاشم ماقورا، الحماية الجنائية لبرامج لحاسب الآلي، مجلة دراسات وأبحاث، العدد 01 جامعة الجلفة، س 2009 ص 154.

[2] محمد حماد مرهج الهيتي، المرجع السابق، ص462.

[3] خالد حسن أحمد، المرجع السابق، ص39-40.

[4] عبد الفاتح عارف التميمي، مهارات الكمبيوتر، اليازوري للنشر والتوزيع، عمان، أردن , 2012 , ص 35.

من قبل المبرمجين، حيث تشكل هذه العيوب والأخطاء ممرات وفواصل مما يسمح بإجراء التعديلات واختراقات للوصول إلى ذلك البرنامج، أيضا يمكن للمبرمجين التحكم في النظام من خلال البرنامج الوهمي وأيضا من برنامج تشغيل النظام المعلوماتي.[1]

البند الثالث: الجرائم المعلوماتية الواقعة على المعلومات المدرجة بالنظام المعلوماتي

يميز العديد من الباحثين بين المعلومات والبيانات "المعطيات" فالبيانات جزء أساسي لمعالجة أجهزة الكمبيوتر والتي تُعَدّ برنامج لها من أجل الوصول إلى المعلومات باستخدام الكمبيوتر، يتم أولا استرجاع البيانات بحيث يمكن تخزينها في الحاسب الآلي ومعالجتها لتحويليها إلى معلومات.[2]

تتكون البيانات من العديد من المفاهيم التي يمكن تلخيصها في كلمات أو أرقام أو رموز أوحقائق أو إحصائيات أساسية لا علاقة لها ببعضها، يمكن استخدامها في تكوين الفكر والمعرفة الإنسانية أو الأدوات والمعدات المستخدمة لهذا الغرض وهي ما تسمى بعملية المعالجة الألية، وعليه فإن معلومات المعالجة الآلية تهدف إلى جعل رسالة محددة من شخص معين قابلة للتوصيل إلى شخص آخر عن طريق إشارة أو اتصال مما تمكنها من الوصول إلى الغير وبذلك يساهم في معالجة المعلومة من خلال نقل المعلومات أو التواصل الفعال.[3]

وتتعدد الجرائم الواقعة على المعلومات المدرجة بالنظام المعلوماتي كالتلاعب أو الإتلاف.

أولا: التلاعب

يمكن أن يتم التلاعب في المعلومات في النظام المعلوماتي بطرق مباشرة أو غير مباشرة وهذا ما سنبينه من خلال هذا العنوان.

1-الطرق المباشرة

---

[1] خلدون عيشة، الطبيعة الخاصة للجريمة الإلكترونية وصورها، مجلة دراسات وأبحاث، العدد 09، جامعة جلفة، الجزائر، 2012، ص 124.

[2] علي صبيح اللامي، المرجع السابق، ص 181- 182.

[3] دردار نادية، جريمة التلاعب في نظام المعالجة الالية للمعطيات في قانون العقوبات، المجلد 17، العدد 01، جامعة سوق اهراس، 2023، ص 825.

يتم التلاعب المباشر من خلال إدخال المعلومات من قبل مسؤولي إدارة المعلومات على سبيل المثال إضافة مستخدمين غير موجودين في الحقيقة للحصول على رواتب غير مستحقة وتحويل مبالغ وهمية لموظفي البنوك باستخدام نظام البنك المعلوماتي يتم تسجيلها وإعادة نقلها وتحويلها إلى حساب آخر في بنك آخر بغرض اختلاس الأموال.

2-الطرق غير مباشرة

يمكن للمتسللين اختراق النظام والتلاعب بالمعلومات عن طريق الوصول غير المصرح به إلى قواعد البيانات أو استخدام المعلومات المسروقة، مثل استخدام كلمة المرور أو مفتاح الشفرة للوصول إلى البيانات واستخدامها للحصول على منافع اقتصادية أو احتيالية أو سرقة الأموال.[1]

ثانيا: الإتلاف

يعرف البعض الإتلاف بأنه جعل الشيء غير صالح الاستخدام أو جعله عديم الفائدة أو تعطيله بشكل كلي أو جزئي ما يؤدي إلى توقفه على أداء وظيفته المقررة بالكامل سواء كان ذلك نتيجة لإفناء مادته أو هلاكه بالكامل، زيادة على ذلك فإن إتلاف برنامج حاسوب ومعلومات تشير أيضا إلى تدمير وحذف تعليمات البرنامج والبيانات وهو ما يسمى تدمير نظام المعلومات، وفي كثير من الأحيان لا يسعى مرتكبو مثل هذه الهجمات إلى تحقيق مكاسب مالية لأنفسهم بل ببساطة إلى عرقلة نظام المعلومات.[2]

وفي ذات السياق فإن جريمة الإتلاف في مجال المعلوماتية تشمل الاعتداء على سلامة الأنظمة والبيانات الحاسوبية، حيث يتم تعطيل أو تدمير البرامج أو البيانات عمدا عن طريق الإزالة أو التشويه أو التدخل في الأداء الطبيعي للحاسوب، وتهدد هذه الجريمة الأمن السبيراني

[1] سورية دبيش، أنواع الجرائم الإلكترونية وإجراءات مكافحتها، مجلة العلوم السياسية والقانون، المركز الديموقراطي العربي العدد الأول، برلين ألمانيا، سنة 2017، ص 276.

[2] احمد بن مسعود، جرائم المساس بأنظمة المعالجة الألية للمعطيات في التشريع الجزائري، مجلة الحقوق والعلوم الإنسانية، المجلد 10 العدد 01، جامعة جلفة، 2017، ص 486.

وخصوصية المعلومات، وقد تنجم عن الوصول غير المصرح به أو البقاء غير المصرح به داخل نظام حاسوبي.[1]

كما ترتكب جرائم إتلاف المعلومات بوسائل عديدة لعل أهمها الفيروسات، وهو عبارة عن مجموعة من التعليمات المشفرة التي تلحق نفسها تلقائيا ببرنامج تطبيقي أو مكون من مكونات النظام وتنتج نسخا متطابقة تتحكم في أداء النظام الذي أصابته وتختلف هذه الفيروسات باختلاف المهمة التي صنعت من اجلها، كما أن القنبلة المعلوماتية هي عبارة عن برنامج ينشأ من قبل مصمم النظام المعلوماتي يتم تمريره داخل النظام المعلوماتي بغرض تدميره، وبهدف جعله يعمل بعد فترة زمنية معينة عندما يكون النظام المعلوماتي الرقمي قيد الاستعمال.[2]

كما قد عالج المشرع الجزائري هذا النوع من الجرائم طبقا لنص 394 مكرر 1 على معاقبة أي شخص يقوم بإدخال المعطيات بطريقة غير مشروعة في نظام المعالجة الآلية، وذلك بغرض الغش أو يقوم بإزالة أو تعديل أو تغيير المعطيات الموجودة في هذا النظام كما تنص على فرض عقوبة الحبس لمدة تتراوح بين 6 اشهر إلى 3 سنوات وبغرامة من 500,000 دج إلى 2,000,000 دج.[3]

[1] وقاص ناصر، الطبيعة القانونية لجرائم المستحدثة ووسائل ارتكابها جريمة الإنترنت، مجلة البحوث القانونية والسياسية، مجلد 3 , العدد 16 ,سعيدة –الجزائر، س 2021، ص 130.

[2] إبراهيم محمد ين محمود الزنداني، الجرائم الإلكترونية من منظور الشريعة الإسلامية واحكامها في القانون القطري والقانون اليمني رسالة ماجستير، جامعة فطاني، 2018، ص 67.

[3] المادة 394 مكرر 01 من القانون رقم 24–06 المصدر السابق.

الفصل الثاني

مكافحة الجريمة المعلوماتية على المستوى الوطني والدولي

بعد التطرق إلى ماهية الجريمة المعلوماتية من خلال تقديم تعريف لها، وتحديد أسباب ارتكابها وتبيان أنواعها والأركان المكونة لها، سوف نتطرق في هذا الفصل إلى سبل مواجهتها على المستوى الوطني والدولي، حيث اهتمت التشريعات الوطنية والدولية بمواجهة هذه الظاهرة نظرا لسرعة تفشي هذه الجريمة، وأصبحت تشكل خطرا على المجتمع والأفراد مما دفع بمعظم تشريعات الدول إلى رفع التحدي لمواجهتها ومجابهة الصعوبات التي عرفتها الدول، خاصة فيما يتعلق بالتقصي والتحقيق فيها، وأيضا صعوبة إثباتها وتحديد الجاني، وأيضا صعوبة تحديد مكان ارتكاب الجريمة، حيث عملت الدول على تعزيز ترسانتها القانونية للحد من هذه الجريمة وتجلى ذلك في إنشاء آليات قانونية بسن قواعد قانونية في هذا المجال، وكذلك النص على مجموعة من الإجراءات المستحدثة في مثل هذه الجرائم، بالإضافة إلى إنشاء آليات قضائية تختص بمتابعة الجرائم المعلوماتية وهذا ما اتخذه المشرع الجزائري.

وبالرغم من سعي جل التشريعات للحد من هذه الجريمة بما فيها المشرع الجزائري، إلا أن ذلك لم يكن كافيا وهذا راجع لكونها تتميز بأنها ذات طابع دولي وعابرة للحدود الوطنية، فقد ترتكب الجريمة في دولة وتحقق النتيجة الإجرامية في دولة أخرى، مما دفع الدول إلى عقد اتفاقيات تعاون بينها وكذا الاتفاقيات القضائية في مجال استلام وتسليم المجرمين وتبادل الخبرات بين الدول، وبالإضافة إلى هذه الاتفاقيات قامت هيئة الأمم المتحدة بتشكيل آليات واتفاقيات وإصدار القرارات بخصوص الجريمة المعلوماتية لمواجهتها على المستوى الدولي، من خلال إنشاء مؤسسات على غرار آلية الشرطة الجنائية الدولية (الإنتربول)، وتم أيضا إنشاء بعض الآليات لمواجهة الجريمة المعلوماتية على المستوى الإقليمي من خلال الاتحاد الأوروبي والاتحاد الإفريقي، وكذلك الجامعة العربية، وهذا ما سنتطرق إليه في فصلنا هذا الذي قسمناه إلى مبحثين حيث خصصنا **(المبحث الأول)** لتطرق إلى المواجهة على المستوى الوطني، أما **(المبحث الثاني)** فقمنا بتخصصيه لمعرفة مواجهة الجريمة المعلوماتية على المستوى الدولي.

المبحث الأول: مكافحة الجريمة المعلوماتية على المستوى الوطني

مع تزايد ظاهرة الإجرام المعلوماتي عبر تقنيات وتكنولوجيا الاتصال، سعى المشرع الجزائري إلى الحد من هذه الظاهرة نظرا لخطورتها، فالثروة الاقتصادية الكبيرة التي تتمتع بها المعلومة وكذا القيمة التي أولاها المشرع لحماية الحياة الخاصة للأفراد من خلال الدستور ومختلف القوانين جعلته يبحث عن الأليات والسبل الفعالة لمواجهة هذه الجريمة، وذلك بإنشاء مجموعة من المؤسسات التي تعمل على الوقاية من هذه الجرائم، وكذلك من خلال إصدار قوانين تعاقب عليها، وللتعرف على هذه الأليات والإجراءات التي قسمنا مبحثنا هذا إلى مطلبين، حيث سنتطرق في **(المطلب الأول)** إلى الأليات المؤسساتية التي أنشأت لمواجهة الجريمة المعلوماتية، أما **(المطلب الثاني)** فسنبين فيه الأليات القانونية والإجرائية والقضائية التي أقرها المشرع للحد من هذه الظاهرة.

المطلب الأول: الأليات المؤسساتية لمواجهة الجريمة المعلوماتية

سخر المشرع الجزائري مجموعة من المؤسسات والهيئات المستقلة ذات الطابع الإداري لمجابهة الإجرام الإلكتروني، وإصدار مجموعة من المراسيم الرئاسية والتنظيمية التي أنشأ من خلالها هذه المؤسسات على غرار الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال والسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي **(الفرع الأول)**، وكذلك المنظومة الوطنية لأمن الأنظمة المعلوماتية بالإضافة إلى مصالح الشرطة والدرك المختصة في الجرائم المعلوماتية **(الفرع الثاني)**.

الفرع الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال والسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي

أنشأ المشرع الجزائري مجموعة من المؤسسات على غرار كل من الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال التي أنشأها بموجب المرسوم الرئاسي 15-256، الذي عدل تشكيلة ومهام الهيئة، كما قام أيضا بإنشاء السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي بموجب القانون 18-07، وهذا ما سنتطرق إليه من خلال هذا الفرع حيث خصصنا البند الأول، للتطرق إلى تشكيلة ومهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، أما البند الثاني فسنتطرق فيه إلى مهام وتشكيل السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي.

البند الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

انتهجت الجزائر مؤخرا إصلاحا في المجال القانوني والأمني والسياسي وإصلاح العدالة وهذا لمواجهة الجريمة المعلوماتية، وفي هذا السياق تم إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، والذي عرف عدة تعديلات آخرها المرسوم الرئاسي 21-349.[1]

تعد الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال سلطة إدارية مستقلة تتمتع بالشخصية الاعتبارية والاستقلال المالي، توضع تحت سلطة رئيس الجمهورية، ويقع مقرها بالجزائر العاصمة ويمكن نقله لمكان أخر من الإقليم الوطني بموجب مرسوم رئاسي وهذا ما جاء من خلال نص المادة 02 و03 من المرسوم الرئاسي 21-349.[2]

[1] شنتير خضرة، المرجع السابق، ص 168-169.

[2] المادة 02 و03، من المرسوم الرئاسي 21-349 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، المؤرخ في 2021/11/01، ج.ر.ج.ج، العدد 86.

أولا: تنظيم وتشكيل الهيئة

تتكون الهيئة من مجلس توجيه ومديرية عامة، وهم تحت سلطة رئيس الجمهورية ويقدمان له عرضا عن نشاطاتهما.[1]

1-مجلس التوجيه

طبقا لما ورد في نص المادة 06 من المرسوم السالف الذكر، فإن الأمين العام لرئاسة الجمهورية هو من يتولى رئاسة مجلس التوجيه، ويتكون من الأعضاء الآتي ذكرهم: الأمين العام لوزارة الشؤون الخارجية والجالية الوطنية بالخارج، والأمين العام لوزارة الداخلية والجماعات المحلية والتهيئة العمرانية والأمين العام لوزارة العدل والأمين العام لوزارة البريد والمواصلات السلكية واللاسلكية وقائد الدرك الوطني والمدير العام للأمن الداخلي، وكذلك المدير المركزي لأمن الجيش لأركان الجيش الوطني الشعبي والمدير العام للأمن الوطني ورئيس مصلحة الدفاع السبيراني ومراقبة أمن الأنظمة لأركان الجيش الوطني الشعبي، وممثل عن رئاسة الجمهورية يعينه رئيس الجمهورية كما يتولى الأمانة المدير العام للهيئة.

2-المديرية العامة

على عكس مجلس التوجيه يترأس المديرية العامة مدير، يتم تعيينه بموجب مرسوم رئاسي وتنتهي مهامه بنفس الشكل طبقا لقاعدة توازي الأشكال، وتعتبر وظيفته من الوظائف السامية في الدولة، وتضم هذه المديرية مديريتين ومصلحتين وهم مديرية وهم مديرية المراقبة الوقائية واليقظة الإلكترونية ومديرية الإدارة والوسائل، أما المصلحتين فتتمثل في مصلحة الدراسات والتلخيص ومصلحة للتعاون واليقظة التكنولوجية، كما تضم أيضا ملحقة جهوية وهذا ما ورد خلال نص المادة 11 من المرسوم الرئاسي 21-349 والمادة 09 من نفس المرسوم بالنسبة لطريقة التعيين.[2]

[1] المادة 05، من المرسوم الرئاسي 21-439، المصدر السابق.

[2] المادة 06-09-11، من المرسوم الرئاسي 21-349، المصدر نفسه.

ثانيا: مهام الهيئة

نص القانون 09-04 المتضمن قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها من خلال المادة 14 منه على المهام المنوطة بالهيئة، والمتمثلة في تفعيل وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته ومساعدة السلطات القضائية ومصالح الضبطية القضائية في التحريات التي تقوم بها بخصوص الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بما في ذلك تجميع المعلومات، وإنجاز الخبرات القضائية وتبادل المعلومات مع نظيراتها في الخارج.[1]

بالإضافة إلى المهام المنوطة إلى الهيئة في القانون 09-04 حددت المادة 04 من المرسوم الرئاسي 21-349 بعض المهام الأخرى التي تكلف بها الهيئة على وجه الخصوص، والمتمثلة في تحديد المخطط الوطني للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومواجهتها- تفعيل وتنظيم عمليات الوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال ومواجهتها- التكفل بالمراقبة الوقائية للاتصالات الإلكترونية تحت صلاحية قاضي مختص- ضمان المراقبة الإلكترونية في الأمور التي تتعلق بأمن الجيش وذلك بالتشارك مع المصالح المختصة لوزارة الدفاع، كما تقوم الهيئة أيضا بتجميع وتسجيل وحفظ المعطيات الرقمية للأنظمة المعلوماتية وتقييد مصادرها من أجل استخدامها في الإجراءات القضائية – المساهمة في تكوين اختصاصيين من المحققين في ميدان التحريات التقنية المتصلة بتكنولوجيا الإعلام والاتصال- مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة جرائم تكنولوجيا الإعلام والاتصال، وأخيرا العمل على إنجاز المساعدة الصادرة من البلدان الأجنبية وتحسين تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها.[2]

[1] المادة 14، من القانون رقم 09-04، المصدر السابق.

[2] المادة 04، من المرسوم الرئاسي 21-439، المصدر السابق.

يتضح من خلال هذه المواد وكذا المادة 07 التي حددت المهام المسندة إلى مجلس التوجيه، أن الهيئة سالفة الذكر تختص في مراقبة الاتصالات كإجراء وقائي من الجرائم التي تأخذ وصف أنها أعمال إرهابية والاعتداء على أمن الدولة، فالهيئة تقوم بالتحري في الجرائم التي تمس أمن الدولة، مثل جرائم الإرهاب والخيانة العظمى التي تستعمل فيها الوسائل الإلكترونية، ومنحها المشرع الحق في استعمال أساليب تحري خاصة، وذلك راجع لخطورة هذه الجرائم على أمن الدولة،[1] وتقسم مهام الهيئة إلى دور وقائي للوقاية من الجرائم الإرهابية أوالمساس بأمن الدولة ودور المكافحة لمختلف الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال، ومساعدة الهيئات القضائية بعد حدوث الجريمة.[2]

البند الثاني: السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي

تعتبر المعطيات الشخصية بيانات ذات أهمية كبيرة، وذلك راجع لتطور الأنترنت فبعد التعرف على اسم الشخص وعنوانه الإلكتروني، أصبح يتعرف عليه بصورته وصوته وبياناته المالية والبيومترية والاجتماعية، إذ تعتبر هذه البيانات والمعطيات مرتبطة بالحياة الخاصة للأفراد، وأصبحت هذه المعطيات والبيانات تتداول بشكل واسع، مما جعل الدول تضع تشريعات لحمايتها ومن بينهم المشرع الجزائري الذي تتجلى مساعيه في حماية الحق في الخصوصية للأفراد من خلال التعديل الدستوري لسنة 2020 وقبلها التعديل الدستوري لسنة 2016[3]، حيث جاء في المادة 47 منه على أنه "لكل شخص الحق في حماية حياته الخاصة وشرفه ولكل شخص الحق في سرية مراسلاته واتصالاته الخاصة في أي شكل كانت...حماية الأشخاص

[1] سهيلة بوزيرة، الهيئة الوطنية للوقاية من ج. م.ت.إ.إ وسرية المعطيات الشخصية الإلكترونية ومكافحة ج إلكترونية، المجلة النقدية للقانون والعلوم السياسية، المجلد 17، ع 02 جامعة تيزي وزو، 2022، ص 563.

[2] حابت أمال، دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها في مواجهة ج.م.ت.إ.إ، المجلة الدولية للبحوث القانونية والسياسية، المجلد 05، العدد 03، جامعة واد سوف، 2021، ص 467.

[3] خالدي فتيحة، السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي كألية لحماية الحق في الخصوصية، مجلة الحقوق والعلوم السياسية، المجلد 13، العدد 04، جامعة البويرة، 2020، ص 47.

عند معالجة المعطيات ذات الطابع الشخصي حق أساسي"،[1] ثم تم بعدها إصدار القانون رقم 18-07 الصادر في 10-06-2018 المتضمن حماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي، والذي نص في بابه الثالث على السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، حيث تتضمن مواده إنشاء وتشكيل السلطة وتحديد المهام المسندة لها.

أولا: نشأة وتشكيل الهيئة

تم إنشاء لدى رئيس الجمهورية سلطة وطنية لحماية المعطيات ذات الطابع الشخصي وهي سلطة إدارية تتمتع بالشخصية الاعتبارية لها ذمة مالية ومستقلة إداريا، ويكون مقرها بالجزائر العاصمة وهو ما ورد في نص المادة 22 من القانون 18-07.

تتشكل السلطة من 16 عضو يتم اختيار من بينهم الرئيس وشخصيتين يختارهم رئيس الجمهورية من أصحاب الاختصاص في مجال السلطة الوطنية، و(03) قضاة يختارهم المجلس الأعلى للقضاء من قضاة المحكمة العليا ومجلس الدولة، وعضو من كل غرفة من البرلمان يختار بعد التشاور مع رؤساء المجموعات البرلمانية فيه، بالإضافة إلى ممثل عن المجلس الوطني لحقوق الإنسان وممثل عن كل وزارة من الوزارات وهي ممثل عن وزارة الدفاع الوطني ممثل عن وزير الشؤون الخارجية_ ممثل عن وزير الداخلية _ ممثل عن وزير العدل حافظ الأختام _ ممثل عن وزير الصحة – ممثل عن وزير العمل والتشغيل والضمان الاجتماعي.

يكون اختيار أعضائها وفقا لاختصاصهم القانوني أو التقني في ميدان معالجة المعطيات ذات الطابع الشخصي، ويتم تعيينهم بموجب مرسوم رئاسي لمدة (05) سنوات قابلة للتجديد، ويؤدون وذلك قبل تنصيبهم في وظائفهم اليمين أمام مجلس قضاء العاصمة.[2]

[1] المادة 47، من المرسوم رئاسي رقم 20-442، المصدر السابق.

[2] المادة 22 إلى 24، من القانون رقم 18-07 المؤرخ في 10 يوليو 2018 المتضمن حماية الأشخاص الطبعيين في مجال المعطيات ذات الطابع الشخصي ج.ر.ج.ج العدد 34.

إن ما يميز هذه السلطة أنها مستقلة في عملها وعدم خضوع أعضائها إلى السلطة الهرمية ولا يتلقون أوامر من أي وزارة، ولا يمكنهم أن يكونوا موظفين أولهم مصلحة في مؤسسة أو شركة تعمل في مجال الاتصالات ومعالجة المعطيات.[1]

ثانيا: مهام السلطة

تعمل السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي على مدى مناسبة معالجة المعطيات ذات الطابع الشخصي لأحكام القانون رقم 18-07 المؤرخ في يوليو 2018، وضمان عدم استعمال تكنولوجيا الإعلام والاتصال في أي أخطار ضد حقوق الأشخاص وحرياتهم.[2]

ولتحقيق هذا الغرض نصت المادة 25 من القانون 18-07 على مهام السلطة، والمتمثلة في منح الإذن واستلام التصريحات المتعلقة بمعالجة المعطيات ذات الطابع الشخصي وإبلاغ الأشخاص المعنيين والمسؤولين عن المعالجة بحقوقهم وواجباتهم، وكذلك تتلقى الاحتجاجات والطعون والشكاوى المتعلقة بتنفيذ معالجة المعطيات ذات الطابع الشخصي، وأيضا منح الرخص بنقل المعطيات ذات الطابع الشخصي إلى الخارج، كما تأمر السلطة بالقيام بالتغيرات اللازمة لحماية المعطيات ذات الطابع الشخصي لمعالجة وإغلاق المعطيات أو سحبها أوإتلافها، وترفع الهيئة اقتراحاتها التي قد تحسن وتسهل الإطار التشريعي والتنظيمي لمعالجة المعطيات ذات الطابع الشخصي وتنشر الرخص الممنوحة والآراء التي أدلت بها في السجل الوطني وتطوير علاقات التعاون مع السلطات الأجنبية التي في نفس مجالها، بالإضافة إلى هذه المهام تصدر السلطة أيضا عقوبات إدارية وتضع معايير في ميدان حماية المعطيات ذات الطابع الشخصي وتحدد قواعد السلوك والأخلاقيات التي تخضع لها معالجة المعطيات ذات الطابع الشخصي.

---

[1] خالدي فتيحة، المرجع السابق، ص 49.

[2] قرانة عادل وبوحديد فارس، مهام السلطة الوطنية لحماية المعطيات الشخصية في التشريع الجزائري، مجلة العلوم القانونية والإدارية المجلد السادس، العدد الثاني، جامعة الجلفة، س 2021، ص 1062.

في حالة إن عاينت السلطة لوقائع تشكل وصف جزائي والتي تدخل ضمن مهامها، تخطر النائب العام، كما تعد السلطة تقريرا سنويا حول نشاطاتها لرئيس الجمهورية.[1]

تعتمد السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي مجموعة من الإجراءات الإدارية في حالة وجود تجاوزات والمتمثلة في الإنذار والإعذار والغرامة، بالإضافة إلى السحب النهائي أو المؤقت لمدة تتجاوز سنة لوصل التصريح أو الترخيص وتكون قراراتها قابلة للطعن أمام مجلس الدولة، كما تناط بالسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي مجموعة من القواعد الإجرائية والمتمثلة في إجراء التحريات المطلوبة ومعاينة المحلات والأماكن التي تتم فيها المعالجة باستثناء السكن، كما مكنها المشرع من الدخول إلى المعطيات وجميع المعلومات والوثائق.[2]

تم إنشاء لدى السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي لجنة الخدمات الاجتماعية بموجب القرار المؤرخ في جانفي 2024 وذلك تبعا لأحكام المرسوم 32-303 المتعلق بتسيير الخدمات الاجتماعية في المادة 21 منه.[3]

الفرع الثاني: المنظومة الوطنية لأمن الأنظمة المعلوماتية ومصالح الأمن المختصة في مواجهة الجريمة المعلوماتية

بالإضافة إلى المؤسسات التي ذكرناها في الفرع السابق، قام المشرع أيضا بإنشاء المنظومة الوطنية لأمن الأنظمة المعلوماتية من خلال المرسوم 20-05، بالإضافة إلى ذلك تم إنشاء بعض الفرق المتخصصة في مواجهة الجريمة المعلوماتية على مستوى المصالح الأمنية والمتمثلة في مصالح الأمن الوطني والدرك الوطني.

---

[1] المادة 25، من القانون رقم 18-07، المصدر السابق.

[2] قرانة عادل وبوحديد فارس، المرجع السابق، ص 1068-1069,

[3] القرار المؤرخ في 10 جانفي 2024 المتعلق بإنشاء لجنة الخدمات الإجتماعية للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، ج.ر.ح.ج العدد 29.

البند الأول: المنظومة الوطنية للأمن الأنظمة المعلوماتية

تشكل المعلومات ثروة حقيقية وطائلة، وهذا ما دفع بجميع الأطراف من دول ومؤسسات وشركات إلى السعي لحمايتها من مختلف المخاطر، خاصة الهجمات الإلكترونية، حيث أصبح حمايتها ضرورة ملحة وذلك استجابة لمتطلبات العصر، وتعتبر الجزائر من بين الدول التي سعت إلى حماية المعلومات، ويتجلى ذلك من خلال إصدار المرسوم 20-05 المؤرخ في 20 يناير 2020 المتضمن وضع منظومة وطنية لأمن الأنظمة المعلوماتية،[1] والذي يعتبر كوسيلة للدولة في ميدان أمن الأنظمة المعلوماتية والإطار التنظيمي للتحضير لاستراتيجيتها وهو ما جاء في المادة 02 من المرسوم الرئاسي 20-05، وأكدت المادة 03 على أنه توضع الهيئة لدى وزارة الدفاع الوطني، وتتشكل من مجلس وطني لأمن الأنظمة المعلوماتية يسند إليه وضع الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية والموافقة عليها، ووكالة لأمن الأنظمة المعلوماتية تقوم بتنسيق تطبيق الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية.

أولا: المجلس الوطني لأمن الأنظمة المعلوماتية

يتشكل المجلس من مجموعة من الأعضاء، وأسندت له مجموعة من المهام التي تدخل في إطار الاستراتيجية الوطنية في مجال أمن الأنظمة المعلوماتية.

1-تشكيل المجلس

طبقا لأحكام المادة 05 من المرسوم الرئاسي 20-05 يرأس المجلس الوطني وزير الدفاع أو ممثله، ويتكون من ممثل عن رئاسة الجمهورية وممثل عن الوزير الأول وممثل عن الوزير المكلف بالشؤون الخارجية وممثلين عن الوزراء المكلفين بكل من الداخلية والعدل والمالية بالإضافة إلى ممثل عن الوزير المكلف بالطاقة والوزير المكلف بالاتصالات ووزير التعليم العالي.

[1] شنتير خضرة، المرجع السابق، ص 192-193.

وليؤدي المجلس مهامه فيتوفر على أمانة تقنية توضع تحت سلطة رئيس المجلس، ويسيرها أمين عام يتم تعيينه طبقا لتنظيم المعمول به بوزارة الدفاع، كما استحدث المشرع بموجب القانون رقم 15-04 المجلس الوطني لأمن الأنظمة المعلوماتية، ومنح له مجموعة من الصلاحيات، كما تتبع طرقا لتسييرها وتتشكل من مجموعة من الأعضاء.[1]

2-مهام المجلس

طبقا لما ورد في نص المادة 04 من المرسوم الرئاسي 20-05 فإنه يناط بالمجلس بعض المهام والتي تدخل في إطار إعداد الاستراتيجية الوطنية في مجال أمن الأنظمة المعلوماتية، ومن المهام التي يتولاها نجد البث في عناصر الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية التي تقترحها الوكالة وتحديدها- دراسة مخطط عمل الوكالة وتحديد نشاطاتها -دراسة التقارير التي تتعلق بتطبيق استراتيجيتها الوطنية والموافقة عليها، كما تقوم أيضا بالموافقة على سياسة التصديق الإلكتروني للسلطة الوطنية للتصديق الإلكتروني والموافقة على تصنيف الأنظمة المعلوماتية، وأيضا اقتراح ملائمة الإطار الهيكلي أو التنظيمي الخاص بأمن الأنظمة المعلوماتية عند الحاجة وإعطاء رأيها في مشاريع القوانين المتعلقة بأمن الأنظمة المعلوماتية.[2]

3- سير المجلس

يتم سير المجلس وفقا لما ورد في نصوص المواد من 11 إلى 16 من نفس المرسوم، حيث يقوم المجلس بالمصادقة على نظامه الداخلي، ويجتمع كلما دعت الضرورة إلى ذلك، ويكون باستدعاء من رئيسه ويتولى الرئيس إعداد جدول أعمال اجتماعات المجلس ويحدد تاريخها ويرسل الاستدعاء إلى الأعضاء مرفوق بجدول الأعمال وذلك قبل (05) أيام على الأقل من تاريخ الاجتماع، ويمكن تبليغ جدول الأعمال خلال انعقاد الجلسة في حالة

[1] حزام فتيحة، الحماية المؤسساتية للأنظمة الرقمية في الفترة التشريعية من 2009-2020، الأكاديمية للدراسات الاجتماعية والإنسانية المجلد 13، ع 01 جامعة بومرداس، 2021، ص 280.

[2] المادة من 02 إلى06، من المرسوم الرئاسي رقم 20-05 المؤرخ في 20جانفي 2020 المتعلق بوضع منظومة وطنية لأمن الانظمة المعلوماتية، ج.ر.ج.ج العدد 04.

الاستعجال وتتخذ قرارات المجلس بالأغلبية، أما في حالة التساوي يرجح صوت الرئيس، ويتم تدوين نتائج أشغال الاجتماعات في محضر، وتكون نتائج أعمال المجلس تبعا للحالة بقرارات وتوصيات وأراء وتقارير.[1]

ثانيا: وكالة أمن الأنظمة المعلوماتية

استحدثت مختلف الدول وكالة وطنية للأمن المعلومات، على غرار المشرع التونسي الذي استحدثها بموجب القانون المتعلق بالسلامة المعلوماتية سنة 2014، أما المشرع الجزائري فكان متأخرا في تبنيه لها مقارنة بنظيره التونسي، حيث استحدثها حتى سنة 2020، وتعتبر الوكالة الوطنية لأمن الأنظمة المعلوماتية مؤسسة عمومية ذات طابع إداري، تتمتع بالشخصية الاعتبارية والاستقلالية المالية، ويقع مقرها في مدينة الجزائر العاصمة، وهو ما ورد في نص المادة 17 من المرسوم الرئاسي 20-05.[2]

1-مهام الوكالة

منح المرسوم الرئاسي 20-05 في المادة 18 منه صلاحيات عديدة للوكالة الوطنية لأمن الأنظمة المعلوماتية، حيث تتولى الإعداد لعناصر الاستراتيجية الوطنية في مجال أمن الأنظمة المعلوماتية وعرضها على المجلس – تنسيق تطبيق الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية المحددة من قبل المجلس – إجراء تحقيقات رقمية في حالة الهجمات أو الحوادث السيبيرانية التي تستهدف المؤسسات الوطنية- السهر على جمع وتحليل وتقييم المعطيات المتصلة بمجال أمن الأنظمة المعلوماتية – متابعة عمليات التدقيق لأمن الأنظمة المعلوماتية – ضمان اليقظة التكنولوجيا في مجال أمن الأنظمة المعلوماتية – جرد الأنظمة المعلوماتية وعرضها على المجلس للموافقة على تصنيفها – إعداد وتحيين خارطة للأنظمة المعلوماتية

[1] المادة من 11 إلى 16، من المرسوم الرئاسي 20-05، المصدر السابق.

[2] حزام فتيحة، المرجع السابق، ص 182-183.

المصنفة – اعتماد منظومات إنشاء وفحص الإمضاء الإلكتروني– تعزيز ثقافة تأمين الأنظمة المعلوماتية – إعداد تقارير دورية وحصيلة سنوية عن نشاطها.

2-التنظيم والتسيير

تتولى لجنة التوجيه إدارة الوكالة وتزود بلجنة علمية يسيرها مدير عام، كما تتوفر على مركز وطني عملياتي لأمن الأنظمة المعلوماتية ومديريات ومصالح تقنية وإدارية توضع تحت سلطة المدير، والذي يتم تعيينه تبعا للتنظيم المعمول به في وزارة الدفاع، وتتشكل لجنة التوجيه من عدة أعضاء وهم ممثل عن وزارة الدفاع الوطني– الوزارة المكلفة بالشؤون الخارجية– الوزارة المكلفة بالداخلية – الوزارة المكلفة بالعدل – الوزارة المكلفة بالمالية – الوزارة المكلفة بالطاقة – الوزارة المكلفة بالتعليم العالي– الوزارة المكلفة بالصناعة – الوزارة المكلفة بالاتصالات – الوزارة المكلفة بالتجارة – مصالح الأمن سلطة ضبط البريد والاتصالات الإلكترونية – السلطة الوطنية للتصديق الإلكتروني– السلطة الوطنية لحماية البيانات ذات الطابع الشخصي – السلطة الحكومية للتصديق الإلكتروني وهذا ما جاء في نصوص المواد 21 و22 من المرسوم الرئاسي 20-05.[1]

تكلف اللجنة خصيصا ببعض المهام المنصوص عليها في المادة 24 من المرسوم الرئاسي سالف الذكر وهي: دراسة البرامج السنوية والمتعددة السنوات لتنفيذ الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية والمصادقة عليها– تقييم نتائج مجموعة الأعمال التي قامت بها الوكالة – تحديد الطرق والوسائل اللازمة للاستجابة للحاجات الوطنية في مجال أمن الأنظمة المعلوماتية – ضبط الطرق والوسائل اللازمة لترقية البحث والتطوير في مجال أمن الأنظمة المعلوماتية والتطبيقات ذات الصلة بالاحتياجات الوطنية – التداول في المسائل التي تتعلق بتنظيم وسير الوكالة –الموافقة على النظام الداخلي للوكالة.[2]

[1] حزام فتيحة، المرجع السابق، ص 281.

[2] المادة 24، المرسوم الرئاسي 20-05، المصدر السابق.

البند الثاني: مصالح الأمن المختصة في مكافحة الجريمة المعلوماتية

وضعت الدولة الجزائرية مكافحة الجريمة المعلوماتية من أولوياتها وهذا للتحديات الأمنية المتزايدة ولتوفير الأمن العمومي في الفضاء الإلكتروني، ولهذا الغرض قامت مصالح الأمن بإنشاء فرق متخصصة لمكافحة هذه الجريمة على مستوى كل من المديرية العامة للأمن الوطني وقيادة الدرك الوطني.

أولا: دور الشرطة الجزائرية في مواجهة الجريمة الإلكترونية

لقد كان للمتغيرات المترتبة عن استخدام التكنولوجيا الحديثة وشبكة الأنترنت تأثيرا على الأوضاع الأمنية، الأمر الذي جعل الأجهزة الأمنية ومن بينها مصالح الشرطة أمام تحديات كبيرة لحماية المجتمع من مساوئ استخدام شبكة الأنترنت، مما دفعها إلى إتباع أساليب التقدم التكنولوجي، وذلك بالاعتماد على التقنيات الحديثة لمواجهة هذه الجريمة.[1]

وفي هذا السياق أصدر المدير العام للأمن الوطني قرار بإنشاء المصلحة المركزية لمكافحة الجريمة السبيرانية في سنة 2011، والتي كانت عبارة عن خلية تابعة لنيابة مديرية القضايا الاقتصادية والمالية بمديرية الشرطة القضائية، وفي سنة 2015 تم وضعها كمصلحة مركزية لمكافحة الجريمة المعلوماتية، والتي أوكلت لها مهام مساعدة مصالح الشرطة القضائية في مجال التحريات التقنية، والمشاركة في حماية الأنظمة المعلوماتية والفضاء السبيراني الوطني والتعاون والمشاركة في التحقيقات والتحريات ذات البعد الوطني والدولي في مجال مكافحة الجرائم المتصلة بتكنلوجيا الإعلام والاتصال، بالإضافة إلى اليقظة المعلوماتية والبحث عن الشبكات المتنوعة عن كل محتوى غير شرعي يشكل في حد ذاته جريمة في قانون العقوبات او مخالف للنظام العام، والمساهمة أيضا في التكوين التخصصي لعناصر الشرطة على مستوى أمن الولايات والعاملين بفرق مكافحة الجريمة المعلوماتية.

[1] طاهر ياكر، الجرائم الإلكترونية، المرجع السابق، ص 172.

كما قامت المديرية العامة بإنشاء فرقة متخصصة على مستوى أمن الولايات تختص بمكافحة الجرائم المعلوماتية تابعة للمصلحة الولائية للشرطة القضائية، تتولى مهمة استقبال الشكاوى في مجال الجرائم المعلوماتية والبحث والتحري في الجرائم المعلوماتية تحت إشراف الجهات القضائية وتوعية وتحسيس المواطنين بمخاطر الانترنت.[1]

سجلت المديرية العامة للأمن الوطني في إطار مواجهة هذه الجريمة خلال الفترة الممتدة من 01 جانفي إلى غاية 31 أكتوبر من سنة 2023 حوالي 3325 قضية.[2]

كما قامت أيضا المدرية العامة للأمن الوطني بعقد اتفاقية توأمة مع الاتحاد الأوروبي في 11جوان 2019 تحت عنوان الخبرة العلمية والتقنية، مما يرفع من خبرة الشرطة العلمية والتقنية الجزائرية ومواكبة المعايير الأوروبية الحسنة.[3]

ثانيا: دور الدرك الوطني في مكافحة الجريمة الإلكترونية

إن لجهاز الدرك الوطني دور فعال في مكافحة الجريمة المعلوماتية، من خلال توفيره للإمكانيات البشرية والمادية مخصصة لهذا الغرض، وكانت البداية الفعلية لمواجهة هذه الجريمة سنة 2004، ثم بعد ذلك تم إنشاء مركز الوقاية من جرائم الإعلام الألي والجرائم المعلوماتية في سنة 2008 لغرض تأمين منظومة المعلومات لخدمة الأمن العمومي ومساعدة باقي الأجهزة الأمنية الأخرى لتأدية مهامها.[4]

سعيا من جهاز الدرك الوطني لتقديم خدمات أمنية ترتقي إلى مستوى تطلعات المواطن وفي ظل التطور التكنولوجي الحاصل تم تكوين إطارات وأعوان الدرك الوطني بشكل متواصل

---

[1] سميحة بلقاسم وحميد بوشوشة، الجريم الإلكترونية بعد جديد للإجرام في الجزائر، مجلة العلوم الإنسانية، المجلد 10، ع 01، جامعة ام البواقي، جوان 2023، ص 548.

[2] ح غنية، الجريمة السبيرانية تهديد حقيقي في عصر التكنولوجيا، مجلة الشرطة، ع 157، 2024، ص 09.

[3] شنتير خضرة، المرجع السابق، ص 208.

[4] شنتير خضرة، المرجع نفسه، ص 213-214.

في هذا المجال، وتم إنشاء مجموعة من الهياكل على غرار المعهد الوطني للأدلة الجنائية وعلم الإجرام ومركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية.

1- المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني

تم بموجب المرسوم الرئاسي 04-183 في يونيو 2004 إنشاء المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني، وهو عبارة عن مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلال المالي، ويوضع هذا المعهد تحت وصاية وزارة الدفاع الوطني ويمارس قائد الدرك الوطني سلطات الوصاية بتفويض منه، يقع مقرها بالجزائر العاصمة ويمكن نقله لمكان أخر داخل الوطن بقرار من وزير الدفاع الوطني.

وقد أوكلت لهذا المعهد عدة مهام من خلال نص المادة 04 من هذا المرسوم كإجراء الخبرات والفحوصات العلمية لغرض إقامة الأدلة التي تمكن من التعرف على مرتكبي الجنايات والجنح وذلك استنادا على طلب من القضاة أو المحققين أو السلطات المؤهلة بالوقاية والتقليل من كل أشكال الإجرام – تصميم بتوك معطيات وإنجازها طبقا للقانون – المشاركة في تحديد السياسة الجنائية المثلى لمكافحة الإجرام – المبادرة بالبحوث المتعلقة بالإجرام وإجرائها باللجوء إلى تكنولوجيا الدقيقة.

يتولى إدارة المعهد مدير عام، ويسيره مجلس توجيه ويزود بمجلس علمي وهذا ما ورد في نص المادة 05، كما يتكون المجلس وفقا للمادة 06 من مجموعة من الهياكل والمتمثلة في مديرية الأدلة الجنائية ومديرية الدراسات والبحوث الإجرامية، بالإضافة إلى مصلحة للتنظيم والمناهج ومصلحة للإدارة والوسائل.[1]

طبقا للمادة 08 من نفس المرسوم السالف الذكر، يتولى مهام المدير العام للمعهد ضابط سامي من الدرك الوطني، يتم تعيينه بموجب مرسوم رئاسي بناء على اقتراح من وزير الدفاع

[1] المادة من 02 إلى 06، من المرسوم الرئاسي 04-183 المؤرخ في 26 يونيو 2004 المتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني، ج.ر.ج.ج، العدد 41.

وتنتهي مهامه بنفس الشكل، ويكون المدير العام للمعهد المسؤول عن السير العام للمعهد وتسييره وله السلطة السلمية والتأديبية على جميع المستخدمين.

كما يتكون المعهد من مجلس توجيه الذي يحدد برامج عمل المعهد ويقر شروط سيره العام ويقيم النتائج الرئيسية، ويتكون مجلس التوجيه من الرئيس وممثل وزير الدفاع ويضم الأعضاء التاليين: ممثل وزير الداخلية – ممثل وزير العدل – ممثل وزير المالية – ممثل وزير الطاقة والمناجم – ممثل وزير التجارة – ممثل وزير التهيئة العمرانية والبيئة – ممثل وزير الصحة والسكان – ممثل وزير الفلاحة – ممثل وزير البريد وتكنولوجيا الإعلام والإتصال – ممثل وزير الصناعة – ممثل وزير النقل وهذا ماجاء في كل من المادة 10و11 من المرسوم الرئاسي 04-183.

بالإضافة إلى مجلس التوجيه يتكون المعهد أيضا من اللجنة العلمية والذي تتمثل أبرز مهمة له طبقا للمادة 17 من نفس المرسوم في مساعدة المدير العام للمعهد في تحديد النشطات العلمية والتقنية وأعمال التكوين وضبط مناهج جديدة في مجال التحريات.[1]

2- مركز الوقاية من جرائم تكنولوجيا الإعلام الآلي والجرائم المعلوماتية ومكافحتها للدرك الوطني

تم إنشاء هذا المركز كخدمة للأمن العمومي في سنة 2008، وهو بمثابة مركز توثيق يقع مقره ببئر مراد رايس، يتولى هذا المركز تحليل معطيات وبيانات الجرائم المعلوماتية وتحديد هوية مرتكبها وهذا لغرض تأمين الأنظمة المعلوماتية خاصة المتعلقة بالمؤسسات الرسمية والبنوك والأفراد.

كما يقوم هذا المركز أيضا ببعض المهام والمتمثلة على غرار توفير المساعدة التقنية للمحققين وحفظ الأدلة واستخدام التكنولوجيا الرقمية لتوجيه التحقيقات ومساعدة الأجهزة الأمنية الأخرى لتأدية مهامها وضمان المراقبة الدائمة والمستمرة على شبكة الأنترنت، ويقوم أيضا

[1] المادة 08 إلى11 و17، المرسوم الرئاسي 04-183، المصدر السابق.

بمراقبة الاتصالات الإلكترونية والمشاركة في التحري والتسرب عبر شبكة الأنترنت من خلال التعاون مع مختلف مصالح الأمن والهيئات الوطنية ويساعد وحدات الدرك من أجل معاينة الجرائم المرتبطة بتكنولوجيا الإعلام والإتصال والبحث عن الأدلة.[1]

في إطار مواجهة مصالح الدرك الوطني للجريمة المعلوماتية تم تسجيل 2838 جريمة في سنة 2021 أما في سنة 2022 عرفت ارتفاعا بتسجيل 4600 قضية، وأن 65٪ إلى 75٪ من هذه الجرائم تمس بالحياة الخاصة للأفراد.[2]

المطلب الثاني: الآليات القانونية والإجرائية والقضائية لمواجهة الجريمة المعلوماتية

مع التطور التكنولوجي الحاصل وتزايد ظاهرة الإجرام المعلوماتي، سعت الدول إلى مواكبة هذه الظاهرة والتكيف معها للحد منها ومن بينها الجزائر التي وضعت مجموعة من الأليات القانونية والقضائية تتماشى معها، ويتجلى ذلك في سن قوانين موضوعية جديدة وإجراء تعديلات عليها، على غرار قانون العقوبات وقانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وكذلك وضع قواعد شكلية يبين من خلالها الإجراءات الواجبة الإتباع في البحث والتحري والمحاكمة في هذه الجريمة، كما تم أيضا إنشاء بعض الآليات القضائية وتكوين القضاة في هذا المجال وهذا ما سنتطرق إليه في مطلبنا هذا حيث خصصنا **(الفرع الأول)** لمعرفة القوانين التي جاء بها المشرع الجزائري لمواجهة الجريمة المعلوماتية، أما **(الفرع الثاني)** سنبين من خلاله الإجراءات التي أقرها المشرع في مجال البحث والتحري عن هذه الجريمة، كما خصصنا **(الفرع الثالث)** لتحديد الأليات القضائية التي أضافها المشرع لمواجهة هذه الجريمة وتحديد الاستراتيجية التي اتبعتها وزارة العدل في هذا المجال.

[1] سميحة بلقاسم وحميد بوشوشة، المرجع السابق، ص 551-552.

[2] موقع الشروق /https://www.echoroukonline.com، تاريخ الاطلاع 2024/06/06 على الساعة 16.15

الفرع الأول: الآليات القانونية لمواجهة الجريمة المعلوماتية

وضع المشرع الجزائري آليات تشريعية من أجل مواجهة الجريمة المعلوماتية على غرار قانون العقوبات الذي لم يكن كافي، مما دفع به إلى وضع ترسانة من القوانين الخاصة للحد منها، مثل قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، والقانون المتعلق بالتصديق الإلكتروني وقانون متعلق بالقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية.

البند الاول: قانون العقوبات

نص المشرع الجزائري على الجريمة المعلوماتية من خلال الفصل الثالث في القسم السابع مكرر من القانون رقم 04-05 المؤرخ في 10 نوفمبر 2004 تحت عنوان المساس بأنظمة المعالجة الألية للمعطيات من خلال المواد 394 مكرر إلى 394 مكرر 07، حيث يعاقب على هذه الجريمة بالحبس من (03) أشهر إلى سنة وبغرامة من 50.000 إلى 100.000 دج لكل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الألية للمعطيات أو يحاول ذلك وقد تضاعف العقوبة لتصبح الحبس من (06) أشهر إلى سنتين وغرامة من 50.000 إلى 150.000 دج في حالة ما إذا ترتب عن هذا الفعل حذف أوتغيير لمعطيات أو تخريب نظام أشغال المنظومة، أما في حالة قيام الجاني عن طريق الغش إما بتصميم أو بحث أو تجمع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أومرسلة عن طريق منظومة معلوماتية وحالة قيامه بحيازة أو إنشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها فهنا يعاقب بالحبس من شهرين إلى ثلاث سنوات وبغرامة من 1000.000 إلى 5000.000 دج.[1]

كما نصت المادة 394 مكرر 03 على أنه تضاعف العقوبات في حالة استهدافها للدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، أما الشخص المعنوي طبقا للمادة 394 مكرر 04 في حالة ارتكابه لهذه الجريمة، يعاقب بغرامة تعادل خمس مرات الحد الأقصى

[1] المواد من 394 مكرر إلى 394 مكرر 02، من القانون 24-06، المصدر السابق.

للغرامة المقررة للشخص الطبيعي، كما يعاقب الشريك وفقا للمادة 394 مكرر 05 بالعقوبة ذاتها للجريمة، أما بالنسبة للشروع فيعاقب أيضا بالعقوبة المقررة للجريمة طبقا للمادة 394مكرر 07.[1]

قام المشرع أيضا من خلال تعديل سنة 2016، بإضافة نص جديد المتمثل في المادة 87 مكرر12 والتي نصت على جناية تجنيد الأشخاص لصالح إرهابي أو منظومة إرهابية باستخدام وسائل تكنولوجيا الإعلام والاتصال.[2]

أضاف المشرع الجزائري تعديلا أخرا للأمر 66-156 وذلك بموجب القانون 24-06 المؤرخ في 28 أبريل 2024 المتضمن قانون العقوبات، حيث تم من خلال هذا القانون إضافة المادة 63 مكرر، التي تعتبر كل جزائري مرتكبا لجريمة الخيانة ويتم معاقبته بالسجن المؤبد في حالة تسريبه لمعلومات أو وثائق سرية تتعلق بالأمن الوطني أو الدفاع الوطني أو الاقتصاد الوطني عبر وسائل التواصل الاجتماعي لفائدة دولة أجنبية أو أحد عملائها، وأيضا جاء بالمادة 63 مكرر01، والتي تعاقب بالسجن من (20) سنة إلى (30) سنة كل من يقوم بقصد إضرار بمصالح الدولة الجزائرية واستقرار مؤسستها بتسريب معلومات أو وثائق سرية تتعلق بالأمن الوطني أو الدفاع الوطني أو الاقتصاد الوطني عبر وسائل التواصل الاجتماعي، كما عدلت أيضا بموجب هذا القانون المادة 96 حيث أصبح يعاقب كل من يوزع أو يقوم بوضع منشورات أو نشرات أو أوراق أو فيديوهات أو تسجيلات صوتية للبيع أو يعرضها لأنظار الجمهور أويحوز بقصد التوزيع أو عرضها بغرض الدعاية بالحبس من سنة (01) إلى خمس (05) سنوات وبغرامة من 100.000 دج إلى 500.000 دج وتضاعف العقوبة إذا كان مصدرها أجنبي، كما يجوز للجهات القضائية أن تحكم بالحرمان من حق أو أكثر من الحقوق الوطنية كما جاء في نص المادة 100 من نفس القانون والتي أضافت التحريض المباشر على تجمهر

[1] المادة من 394مكرر03 إلى 394مكرر 07، من القانون رقم 24-06، المصدر السابق.

[2] راضية عمور، الجريمة الإلكترونية وأليات مكافحتها في التشريع الجزائري، المجلة الأكاديمية للبحث القانونية والسياسية، المجلد السادس، العدد الأول، جامعة الأغواط، 2022، ص 96-97.

غير مسلح باستخدام تكنولوجيا الإعلام والاتصال وأبقت على نفس العقوبة والمقدرة بالحبس من شهر إلى ستة أشهر وغرامة من 20.000 دج إلى 100.000 دج أو بإحداهما.[1]

البند الثاني: مواجهة الجريمة المعلوماتية بموجب قوانين خاصة

بالإضافة إلى قانون العقوبات، أقر المشرع الجزائري مجموعة من القوانين الخاصة والمتمثلة في كل من قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وكذا القانون المتعلق بالبريد والاتصالات الإلكترونية والقانون المتعلق بحقوق المؤلف والحقوق المجاورة والقانون المتعلق بالتصديق الإلكتروني، وهذا ما سنبينه من خلال هذا البند.

أولا: القانون رقم 09-04

أدى تزايد الاعتداءات على معطيات الحاسوب وضعف الحماية والنصوص القانونية التي تحمي هذه المعطيات إلى ضرورة تدخل المشرع لسن قواعد قانونية جديدة تمكنه من مواجهة هذه الاعتداءات وردعها، ويتجلى ذلك من صدور القانون 09-04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، حدد من خلاله المشرع مفهوم المصطلحات التقنية، وأكد أيضا على المحافظة على سرية الاتصالات ومراقبة الاتصالات الإلكترونية وتسجيل مضمونها والقيام بإجراءات التفتيش والحجز داخل المنظومة المعلوماتية، وتكون المراقبة بإذن مسبق من الجهات القضائية، كما يبين أيضا الالتزامات التي تقع على عاتق المتعاملين في مجال الاتصالات الإلكترونية، بالإضافة إلى نصه على إنشاء هيئة وطنية للوقاية من الإجرام المتصل بتكنولوجيا الإعلام والاتصال ومكافحته.[2]

لقد استحدث هذا القانون تدابير جديدة للتصدي للجريمة المعلوماتية، وتتمثل في تدابير وقائية تساعد في الكشف على الاعتداءات المحتملة والتدخل السريع لصدها والمنصوص عليها

[1] المادة 06-08، من القانون رقم 24-06، المصدر السابق.

[2] شنتير خضرة، المرجع السابق، ص 228-229.

في نص المادة 04 من القانون 09-04، ونص أيضا على تدابير أخرى إجرائية تكمل الإجراءات المنصوص عليها في قانون الإجراءات الجزائية.[1]

كما نصت المادة 13 من نفس القانون على إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، أما التدابير الإجرائية فتمثلت في تفتيش المنظومات المعلوماتية وهو ما بينته المادة 05 من هذا القانون.[2]

ثانيا: مواجهة الجريمة المعلوماتية في ظل قانون البريد والاتصالات الإلكترونية (18-04)

جاء القانون 18-04 المتعلق بالبريد والاتصالات الإلكترونية بمجموعة من القواعد والضوابط لمواجهة الجرائم المتصلة بتكنولوجيا المعلومات، حيث أقر هذا القانون إنشاء سلطة ضبط للبريد والاتصالات الإلكترونية تتمتع بالاستقلالية،[3] وتم إنشاء بموجب هذا القانون سلطة ضبط مستقلة للبريد والاتصالات الإلكترونية لها الشخصية الاعتبارية والاستقلال المالي يقع مقرها بالجزائر العاصمة، وتتولى هذه السلطة مهمة ضمان ضبط أسواق البريد والاتصالات لحساب الدولة إضافة إلى بعض المهام التي تدخل في هذا الإطار والمنصوص عليها في نص المادة 13، أما بالنسبة لتشكيلتها فقد نصت عليها المادة 20 والتي تتكون من 07 أعضاء يعينهم رئيس الجمهورية باقتراح من الوزير الأول من بينهم الرئيس وذلك لمدة (03) سنوات قابلة لتجديد مرة واحدة يكون تعيينهم وفقا لكفاءتهم في المجال التقني والقانوني والاقتصادي.

نص هذا القانون على الجرائم المتعلقة بالبريد والاتصالات الإلكترونية والعقوبات المقررة لها من خلال نصوص المواد من 164 إلى 188 منه، ومن بين الأفعال المجرمة نجد انتهاك سرية المراسلات المرسلة عن طريق البريد أو الاتصالات الإلكترونية أو نشرها أو استعمالها دون ترخيص من المرسل أو المرسل إليه، وهذا ما نصت عليه المادة 164 ومن الأفعال المجرمة أيضا نجد فتح أو تحويل أو تخريب للبريد أو المساعدة في ارتكاب هذه الأفعال والتي

---

[1] راضية عمور، المرجع السابق، ص 104.

[2] المادة 04-05 -13، من القانون رقم 09-04، المصدر السابق.

[3] سميحة بلقاسم وحميد بوشوشة، المرجع السابق، ص 545.

نصت عليها المادة 165، بالإضافة إلى هذه الأفعال جرم هذا القانون بعض الأفعال الأخرى مثل تقديم خدمات البريد بدون ترخيص المنصوص عليها في نص المادة 34 من هذا القانون والجريمة المنصوص عليها في نص المادة 175 والمتمثلة في تحويل خطوط الاتصالات الإلكترونية واستغلال خطوط الاتصالات الإلكترونية المحولة. [1]

ثالثا: مواجهة الجريمة المعلوماتية في ظل حقوق المؤلف والحقوق المجاورة (03-05)

اعتبر القانون 03-05 أن المصنف الفكري من معطيات الحاسب الألي التي وجب حمايتها وفرض عقوبات على الاعتداء عليها، حيث تعد من الحقوق المالية والأدبية التي يتمتع بها مؤلف البرامج والبيانات،[2] حيث نصت المادة 04 في الفقرة (أ) على أن برامج الحاسب الآلي تعتبر من المصنفات الأدبية، وكذلك المادة 05 في فقرتها الأولى التي اعتبرت قواعد البيانات أيضا مصنفا محميا، فقد منح المشرع من خلال هذا القانون حماية جزائية لهذه البرامج وقواعد البيانات من جرائم التقليد المنصوص عليها في نص المادة 151 منه،[3] وتبين الأفعال التي تشكل جريمة تقليد والتي تشمل كل اعتداء على حق من حقوق المؤلف من بينها حقوق مؤلفي البرامج.[4]

كما نصت المادة 153 على العقوبات المقررة على الشخص الذي يرتكب جنحة التقليد، حيث يعاقب بالحبس من (06) أشهر إلى ثلاث سنوات وبغرامة من 500.000 إلى 1.000.000 دج، كما يعاقب أيضا طبقا للمادة 154 كل من يشارك بعمله أو من خلال الوسائل التي يحوزها في هذه الجريمة ويعاقب بنفس العقوبة المقررة للفاعل الأصلي، وأيضا

---

[1] المادة. من 11-12-13 و، م. من 164 إلى 188، من القانون رقم 18-04 المؤرخ في 10 مايو 2018 الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، ج.ر.ج.ج، ع 27.

[2] بدر الدين خلاف، التنظيم القانوني للجريمة المعلوماتية في الجزائر، مجلة العلوم القانونية والاجتماعية، المجلد السادس، العدد الثاني، جامعة الجلفة، جوان 2021، ص 343.

[3] المادة 04-05، من القانون رقم 03-05 المؤرخ في19 يوليو 2003 المتعلق بحماية حقوق المؤلف والحقوق المجاورة، ج.ر ج. ج، العدد 44.

[4] شنتير خضرة، المرجع السابق، ص 166.

يعتبر مرتكبا لهذه الجريمة ويعاقب على نفس العقوبة المقررة لها كل من رفض دفع المكافئات المستحقة للمؤلف أو لأي مالك للحقوق المجاورة، وفي حالة العود تضاعف العقوبة طبقا للمادة 156 ويمكن الغلق المؤقت للمؤسسة التي يستعملها المقلد أو شريكه، أو يمكن أن تقرر الغلق النهائي.[1]

رابعا: مواجهة الجريمة المعلوماتية في ظل القانون المتعلق بالتوقيع والتصديق الإلكتروني (15-04)

قد أقر المشرع الجزائري القانون 15-04 لغرض تحديد القواعد العامة التي تتعلق بالتوقيع والتصديق الإلكترونيين، حيث نص هذا القانون على أنه يتم استعمال التوقيع الإلكتروني من أجل توثيق هوية الموقع وإثبات قبوله مضمون الكتابة في الشكل الإلكتروني، وهو ما نصت عليه المادة 06 من هذا القانون، كما نصت المادة 08 من نفس القانون على أنه يعتبر التوقيع الإلكتروني الموصوف بمثابة توقيع مكتوب سواء كان هذا التوقيع لشخص طبيعي أو معنوي ولا يمكن طبقا للمادة 09 من تجريد التوقيع الإلكتروني من فعاليته أو رفضه كدليل أمام القضاء بسبب شكله الإلكتروني أو اعتباره أنه لا يعتمد على شهادة تصديق إلكتروني موصوفة أو لعدم إنشائه عن طريق ألية مؤمنة لإنشاء التوقيع الإلكتروني.

نص المشرع الجزائري من خلال الفصل الثاني من الباب الثاني على آليات إنشاء التوقيع الإلكتروني الموصوف والتحقق منه، حيث أكد على أنه يجب أن تكون هذه الأليات مؤمنة طبقا للمادة 10 ونص من خلال المادة 11 من نفس القانون على المتطلبات الواجب توافرها، حيث يجب أن تضمن عن طريق الوسائل التقنية والإجراءات المناسبة مايلي: أن لا تكون البيانات مصادفة المستخدمة لإنشاء التوقيع الإلكتروني مرة واحدة فقط، وأن لا يكون إيجاد البيانات المستعملة عن طريق الاستنتاج، وأن يكون محمي من أي تزوير وأن تكون محمية بشكل

[1] المادة 151 إلى 156، من الأمر رقم 03-05، المصدر السابق.

موثوق من قبل الموقع الشرعي من أي استخدام من طرف الآخرين، وأن لا تعدل هذه البيانات ويمكن أن تمنع من عرضها على الموقع قبل عملية التوقيع.[1]

جاء المشرع الجزائري في الفصل الثاني من الباب الثالث بسلطات التصديق الإلكتروني والمتمثلة في السلطة الوطنية للتصديق الإلكتروني، وهي سلطة إدارية مستقلة تنشأ لدى الوزير الأول لها الشخصية الاعتبارية والاستقلال المالي، تتولى تسجيل الاعتمادات المالية لسير السلطة وتكلف بترقية استخدام التوقيع والتصديق الإلكترونيين وضمان توثيق استعمالهما وتتشكل الهيئة طبقا للمادة 19 من مجلس ومصالح إدارية وتقنية ومن 05 أعضاء يعينهم رئيس الجمهورية بناءا على كفاءتهم في عدة مجالات منها الإعلام والاتصال والجانب القانوني والاقتصادي المتعلق بتكنولوجيا الإعلام والاتصال.[2]

بالإضافة إلى هذه السلطة أنشأ هذا القانون كل من السلطة الحكومية للتصديق الإلكتروني والسلطة الاقتصادية، حيث تعتبر الأولى سلطة تتمتع بالشخصية الاعتبارية والاستقلال المالي تنشأ لدى الوزير المكلف بالبريد والتكنولوجيات الإعلام والاتصال، حيث تتولى هذه السلطة مراقبة نشاط التصديق الإلكتروني وتوفير خدمات التصديق الإلكتروني، أما السلطة الاقتصادية فيتم تعيينها من قبل السلطة المكلفة بضبط البريد والمواصلات السلكية واللاسلكية وتناط بها عدة مهام تدخل في إطار متابعة ومراقبة مؤدي خدمات التصديق الإلكتروني، والذين يقدمون خدمة التوقيع والتصديق الإلكترونيين لصالح الجمهور.[3]

[1] المادة 06 إلى 10، من القانون رقم 15-04 المؤرخ في 01 فبراير 2015 الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكتروني، ج، ر.ج.ج العدد 06.

[2] المادة 16 إلى 20، من القانون رقم 15-04، المصدر نفسه.

[3] المادة 26 إلى 30، القانون رقم 15-04، المصدر نفسه.

الفرع الثاني: الآليات الإجرائية لمواجهة الجريمة المعلوماتية

نص المشرع الجزائري على الإجراءات الواجبة إتباعها لتحقيق في الجريمة المعلوماتية على غرار الجرائم الأخرى، والمتمثلة في الإجراءات العامة كالمعاينة والتفتيش والضبط والخبرة، كما نص أيضا على مجموعة من الأساليب الخاصة للتحقيق في الجريمة مثل اعتراض المرسالات وتسجيل الأصوات والتقاط الصور وكذلك التسرب.

البند الأول: الإجراءات العامة للتحقيق في الجريمة المعلوماتية

يعتبر التحقيق الابتدائي من أهم مراحل سير الدعوى العمومية، ويتمثل في الإجراءات التي تقوم بها المصالح المختصة في التحقيق وهذا من أجل إثبات الجريمة وكشف فاعلها ونسبها إليه، بحيث وضع المشرع تعديلات من أجل مواجهة الجريمة المعلوماتية خاصة من خلال جرائم التي تمس بأنظمة المعالجة الألية للمعطيات من خلال نصه على التفتيش والمعاينة والضبط وإجراء الخبرة.[1]

أولا: التفتيش الإلكتروني

إن التفتيش هو إجراء من إجراءات التحقيق تختص به سلطات التحقيق على غرار قاضي التحقيق والنيابة العامة، وقد يخول استثناءا إلى ضباط الشرطة القضائية ويهدف للبحث عن الأدلة للجريمة وإثبات وقوعها ونسبها لمرتكبها، وبالتالي فهو وسيلة للإثبات المادي يهدف إلى ضبط الأدلة المادية المتعلقة بالجريمة، وهذا ما يتنافى مع برامج وبيانات الحاسب الآلي ومعطيات شبكات الأنترنت التي تعتبر ذات طبيعة غير مادية أي ليس له مظهر مادي ملموس وهذا ما يثير تساؤل حول إمكانية تفتيش هذه المكونات غير المادية للحاسب الآلي.

كما يتكون أيضا الحاسب الآلي من مكونات مادية كوحدات المعالجة المركزية ووحدات التخزين ووحدات الإدخال، فالمكونات المادية تخضع لتفتيش بالنظر لطبيعة المكان إن كان

[1] بن مكي نجاة، المرجع السابق، ص 217.

عام أو خاص فتطبق عليها نفس الإجراءات المعمول بها في قانون الإجراءات الجزائية في الجرائم التقليدية.[1]

أما بالنسبة لتفتيش المكونات غير المادية للحاسب الآلي فقد أثار جدلا فقهيا حول مدى إمكانية أن تكون محلا للتفتيش أم لا، حيث ذهب البعض إلى القول إن المكونات غير المادية للحاسب الآلي ليس لها مظهر مادي ملموس في المحيط الخارجي، وذلك يتنافى مع الغرض من التفتيش والمتمثل في الوصول إلى الأدلة المادية المترتبة عن الجريمة.

كما رأى البعض بإمكانية تفتيشها من خلال تسجيل وتخزين وتحميل الذبذبات والموجات والنبضات الإلكترونية في دعائم مادية مما يمكن من إخضاعها للتفتيش، وقد عملت جل التشريعات على وضع قوانين خاصة تمكن من تفتيش المكونات غير مادية، وهو ما سع إليه أيضا المشرع الجزائري الذي قام باستحداث قواعد قانونية جديد تسمح بتفتيش المكونات غير المادية للحاسب الألي،[2] وذلك من خلال القانون رقم 09-04 في نص المادة 05 منه السماح لضباط الشرطة القضائية والجهات القضائية المختصة بإجراء التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها أو إلى منظومة تخزين معلومات.[3]

ثانيا: الضبط

يعرف الضبط في الجريمة المعلوماتية، بأنه استعمال البرامج لغرض الدخول إلى البيانات المراد ضبطها، بالإضافة إلى وضع اليد على تلك الدلائل المادية، وقد نظم المشرع الجزائري ضبط الأدلة الإلكترونية من خلال العديد من القوانين منها القانون 09-04 في نص المادة 6 منه، والتي مكنت الجهات التي تقوم بالتفتيش في منظومة معلوماتية من ضبط أو حجز بيانات ومعطيات تساعد في الكشف عن الجريمة، كما جاءت المادة 27 من المرسوم الرئاسي المتعلق

[1] براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة لنيل شهادة دكتوراه، جامعة تيزي وزو، 2018، ص 13إلى 15.

[2] براهيمي جمال، المرجع نفسه، ص 17 إلى 19.

[3] المادة 05، من القانون رقم 09-04، المصدر السابق.

بالتصديق على الاتفاقية العربية لمكافحة الجرائم المعلوماتية التي عقدت في القاهرة خلال سنة 2010، والتي تستوجب تبني الإجراءات اللازمة قصد التمكين من ضبط وتأمين المعلومات المتعلقة بتقنية المعلومات التي يتم التوصل إليها بعد القيام بالتفتيش.

وينصب الضبط على الأشياء المادية وغير المادية، كما يمكن أن يكون محلا للضبط أيضا العقار مثل أن تترك الجريمة المعلوماتية أثارا بمكان ما فقد يشمل عقار بالتخصيص مثل الحاسب الآلي الذي يوجد بمقهى الأنترنت وآلات التصوير والطابعة، وتكون كذلك محلا للتفتيش الأوراق التنظيمية وبطاقة الذاكرة والأسطوانات المدمجة والماسح الضوئي ووحدة المعالجة المركزية.[1]

ثالثا: المعاينة

تعرف المعاينة أنها إجراء يتم بمقتضاه انتقال المحقق أو القاضي لمكان الجريمة ليشاهد ويجمع الأثار الموجودة فيه، أما بالنسبة إلى مسرح الجريمة المعلوماتية فتتم المعاينة فيه في داخل الحاسوب والبيانات الرقمية وفي ذاكرته وفي الأقراص الصلبة، وتكون المعاينة بمعاينة الأثار والبصمات الإلكترونية التي يتركها مستخدم الشبكة المعلوماتية والأنترنت، حيث تتمثل في الرسائل المرسلة والواردة وكل الاتصالات الإلكترونية، فهي تتم داخل الأجهزة وشبكة الأنترنت ومن خلال هذه المعاينة يتم التعرف على المواقع الإلكترونية التي زارها المتهم والملفات التي حملها والحسابات التي اخترقها، فالمعاينة تكون في العالم الافتراضي أيضا وليس في العالم المادي فقط، ويتطلب لإجراء المعاينة مجموعة من الضوابط حتى تتم بشكل صحيح وتتمثل هذه الضوابط في الإعداد الجيد قبل المعاينة وذلك بإخطار المختصين الذين يتولون المعاينة حتى يتسنى له إعداد خطة وتحضير الإمكانيات اللازمة لضبط الأدلة الإلكترونية والملاحظة الجيدة للطريقة التي تم من خلالها إعداد النظام والأثار الإلكترونية، وكذلك التحفظ على المعلومات الموجودة بالقرب من الأجهزة وفي سلة المهملات وعدم نقل أي مادة معلوماتية

[1] شنتير خضرة، المرجع السابق، ص 110 إلى117.

من مسرح الجريمة قبل إجراء الاختبارات، وأيضا الحرص على عدم إتلاف أي بيانات يتم استخراجها من الجهاز.[1]

رابعا: الخبرة

تعتبر الخبرة الفنية من إجراءات التحقيق ومن خلالها يتم الاستعانة بشخص له قدرات ومؤهلات فنية وعلمية لا يكتسبها المحققين والقضاة بهدف الكشف عن دليل يكشف حقيقة وقوع الجريمة، ولها أهمية كبيرة في مساعدة السلطات المختصة في الكشف عن الجريمة، حيث يستعينون بأصحاب الخبرة والذين لهم كفاءة وخبرة كبيرة في تقنية المعلومات، ونظرا للتحولات التكنولوجية الحديثة والتطور التكنولوجي الهائل في مجال الإعلام والاتصال زادت الحاجة إلى الخبرة الفنية للتحقيق في الجريمة المعلوماتية، حيث أصبحت الجهات القضائية في حاجة ماسة إلى خبراء في مجال تقنية المعلومات، إذ أصبحت هذه السلطات تعجز عن الكشف عن الجريمة في حال غياب الخبير الفني ونقس الكفاءة اللازمة لها لمواجهة تقنية المعلومات مما يؤدي إلى فقد الدليل ومحو أثاره، مما دفع المشرع الجزائري من إلى وضع القانون 09-04 والسماح من خلاله للجهات المكلفة بالتحقيق وتفتيش المنظومة المعلوماتية الاستعانة بأي شخص له دراية وعلم بعمل المنظومة المعلوماتية أو بالتدابير المتخذة لحماية معطيات المعلومات التي تتضمنها من تقديم لها المساعدة ومنحها المعلومات اللازمة للقيام بمهمتها، كما تخضع الخبرة الفنية إلى ضوابط قانونية وفنية فبالنسبة للضوابط الفنية تتمثل في نفس الضوابط المنصوص عليها في الجريمة التقليدية، أما بالنسبة للضوابط الفنية فهي تخضع لتقنيات منها ما قبل التشغيل والفحص وتقنيات التشغيل والفحص ولها وسائل علمية لإنجاز الخبرة الإلكترونية، وتتمثل في برتوكول الأنترنت IP ونظام البروكسي وبرنامج TRACE ROUTE وأنظمة كشف

[1] شنتير خضرة، المرجع السابق، ص 73 إلى77.

الاختراق IDS، وكذلك برامج مراجعة العمليات الحاسوبية واسترجاعها وبرنامج الدمج وفك الدمج.[1]

البند الثاني: الإجراءات الخاصة بالتحقيق في الجريمة المعلوماتية

أصبح مرتكبي الجرائم المعلوماتية يستعلمون التقنيات الحديثة في مختلف الجرائم، حيث سهلت هذه الأخيرة تنقلاتهم وساهمة في امتداد الجرائم إلى خارج الحدود الوطنية، فأصبح من الصعب تتبع نشاطاتهم وتحركاتهم، الأمر الذي دفع بمختلف التشريعات بوضع أساليب لمواجهة هذه الجريمة ومن بينهم المشرع الجزائري الذي قام بتعديل قانون الإجراءات الجزائية بموجب القانون رقم 06-22 والذي استحدث من خلاله مجموعة من الإجراءات الخاصة لمواجهة الجريمة المعلوماتية، والمتمثلة في التسرب والتقاط الصور واعتراض المراسلات وتسجيل الأصوات والمراقبة الإلكترونية وحفظ المعطيات، بالإضافة إلى هذه الأساليب وسع أيضا المشرع الجزائري من الاختصاص الإقليمي لضباط الشرطة القضائية وكل من وكلاء الجمهورية وقضاة التحقيق.

أولا: التسرب.

التسرب هو توغل واختراق ضابط أو عون شرطة قضائية لجماعة إجرامية وكسب ثقتهم،[2] وقد نصت المادة 65 مكرر12 على هذا الإجراء بقولها "يقصد بالتسرب قيام ضابط أوعون شرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أوخاف..."، وللقيام بهذه العملية يسمح لضابط أو عون شرطة القضائية الذي يقوم بهذه العملية

[1] براهيمي جمال، المرجع السابق، ص من 73إلى 80.

[2] شيح نجية، إجراء التسرب في القانون الجزائري وسيلة لمكافحة الجرائم المستحدثة، معارف، العدد 25 جامعة البويرة، س 2018، ص 03.

باستخدام هوية مستعارة، ويسمح لهم أيضا القيام بعمليات أو حيازة أو نقل أو تسليم مواد أوأموال أو وثائق دون أن يكون مسؤولا جزائيا.[1]

تتم عملية التسرب في الجرائم المعلوماتية في دخول ضابط أو عون شرطة القضائية إلى شبكة الأنترنت والمشاركة في ملفات مباشرة التي تبين تقنيات الاختراق، ونشر الفيروسات وانخراطه في مجموعات الدردشة ونوادي الهاكر، ويستخدم اسما مستعارا ويظهر لهم بشكل طبيعي كأنه مثلهم، وهذا للكشف هويتهم وعن أعمالهم الإجرامية.[2]

ثانيا: اعتراض المراسلات والتقاط الصور وتسجيل الأصوات

إن اعتراض المراسلات من إجراءات التحري الخاصة التي تكون من خلال الاتصالات السلكية واللاسلكية، حيث يعرف بأنه الاستماع خلسة إلى الحديث الخاص عبر الهاتف الثابت أو النقال بمراقبة المشتبه فيهم من خلال استراق السمع للمحادثات التي تتم عبر شبكات الهواتف، وهي من أهم الوسائل التي تستعمل للحصول على الدليل وتقديمه في ملف الإجراءات، وتتم هذه العملية من خلال استعمال وسائل التكنولوجية والتقنية المتطورة دون علم الأشخاص، وقد أعطى المشرع لهذه الخصوصية حماية في مختلف القوانين خاصة في الدستور إلا أنه في بعض الأحيان توجب ضرورة التحقيق والتحري اعتراض المراسلات خاصة فيما يتعلق بجريمة المساس بأنظمة المعالجة الألية للمعطيات من أجل كشف سرها والوصول إلى الدليل وهذا ما يبيح الفعل، ففي الأصل أن هذا الفعل يعتبر انتهاك لحرمة الحياة الخاصة وأجاز المشرع استثناءا انتهاك هذا الحق في مسائل ضيقة بهدف إظهار الحقيقة والكشف عن الجريمة.[3]

أما بالنسبة لتسجيل الأصوات نص عليه من خلال المادة 65 مكرر05 في فقرتها الثالثة ويقصد به تسجيل النقل الآلي للأمواج الصوتية من مصادرها على دعامة مغناطسية والتي

[1] محمد حزيط، أصول الإجراءات الجزائية في ق.ج، دار بلقيس، ط ثالثة، الجزائر، س 2022، ص 179 إلى181.

[2] براهيمي جمال، المرجع السابق، ص 85.

[3] طاهر ياكر، الجرائم الإلكترونية، المرجع السابق، ص 106-107.

تكون في شكل قرص مضغوط أو دعامة USB أو بطاقة ذاكرة وتكون في شكل ملف صوتي من أجل العودة للاستماع إليها ومعرفة مضمونها.

أما التقاط الصور فهو أسلوب يستخدم في البحث والتحري نص عليه في المادة 65 مكرر05، وهو المراقبة التي تكون بواسطة كاميرات وأجهزة تلتقط صور وصوت لوضعيات الأشخاص في مكان معين، وهي أيضا عبارة عن معاينة للأشخاص تستعمل فيها الأجهزة الفتوغرافية من قبل ضابط الشرطة القضائية من أجل ضبط المشتبه فيهم عند ارتكابهم للجريمة وتحديد زمان ومكان التقاط الصور بهدف استخدامها كدليل لإثبات الجريمة أمام المحاكم الجزائية.[1]

ثالثا: المراقبة الإلكترونية

إن المراقبة الإلكترونية هي من الإجراءات التي جاء بها القانون 09-04 في نص المادة الثالثة منه، حيث أجازت وضع الترتيبات التقنية لمراقبة الاتصالات وتجميع وتسجيل محتواها وذلك إذا دعت مقتضيات التحقيق القيام بذلك، ويقصد بالمراقبة الإلكترونية أنه عمل يقوم به المراقب باستعمال تقنيات الإلكترونية بهدف جمع المعلومات عن المشتبه فيه، ويقصد باستخدام التقنية الإلكترونية في المراقبة الإلكترونية في مراقبة الأجهزة التي يهدف من خلالها تشغيل البيانات وفقا لبرنامج موضوع مسبقا للحصول على النتائج المطلوبة تبرر هذا الإجراء كوسيلة فقط، فهو أيضا من التدابير الوقائية للوقاية من الجرائم المعلوماتية، وهو ما جاء في نص المادة 04 من القانون 09-04 التي أكدت على أنه تتم عملية المراقبة للوقاية من بعض الجرائم على غرار جرائم الإرهاب والتخريب والجرائم الماسة بأمن الدولة.[2]

[1] طاهر ياكر، الجرائم الإلكترونية، المرجع السابق، ص 108.

[2] طاهر ياكر، الجرائم الإلكترونية، المرجع نفسه، ص 113.

رابعا: امتداد الاختصاص المحلي لضباط الشرطة القضائية

يتحدد الاختصاص الإقليمي لضباط الشرطة القضائية طبقا للمادة 16 في الحدود التي يباشرون فيها وظائفهم، إلا أنه استثناءا سمح المشرع بامتداد الاختصاص المحلي لضباط الشرطة القضائية إذا تعلق الأمر بمجموعة من الجرائم المذكورة على سبيل الحصر، ومن بينها جريمة المساس بأنظمة المعالجة الألية للمعطيات والتي تدخل ضمن الجريمة المعلوماتية، حيث يمتد اختصاص ضباط الشرطة القضائية ليشمل كافة التراب الوطني، ويعملون تحت إشراف النائب العام للمجلس القضائي المختص إقليميا ويتم إعلام وكيل الجمهورية المختص إقليميا،[1] كما يمكن لضباط وأعوان الشرطة القضائية تمديد عمليات المراقبة وذلك في حالة عدم اعتراض وكيل الجمهورية ويكون ذلك في حالة وجود ضدهم مبرر يشتبه فيهم ارتكابهم لمجموعة من الجرائم ومن بينها جريمة المساس بأنظمة المعالجة الألية للمعطيات، ومن خلال هذا الإجراء يتم ملاحقة مرتكب الجريمة المعلوماتية عبر كافة التراب الوطني وبالخصوص في حالة وجود جمعية أشرار.[2]

خامسا: توسيع اختصاص الجهات القضائية

لقد وسع المشرع الجزائري من اختصاص الجهات القضائية في الجرائم المعلوماتية، وذلك بتوسيع اختصاص كل من وكيل الجمهورية وقاضي التحقيق، فطبقا للمادة 37 من قانون الإجراءات الجزائية يتحدد الاختصاص المحلي لوكيل الجمهورية بمكان وقوع الجريمة ومحل إقامة أحد الأشخاص المشتبه فيهم، أوفي مكان القبض على أحد المشتبه فيهم حتى ولو حدث القبض لسبب أخر.[3]

---

[1] المادة 16، من القانون 21 -11، المؤرخ في 25 غشت 2021، المعدل والمتمم للامر 66-155، المتضمن قانون الإجراءات الجزائية، ج.ر.ج.ج، العدد 65.

[2] يزيد بوحليط، المرجع السابق، ص 395.

[3] المادة 37، من ق 21-11، المصدر السابق.

إلا أنه استثناءا يجوز تمديد الاختصاص في جرائم معينة مثل الجريمة المنظمة والجريمة العابرة للحدود الوطنية وجريمة الإرهاب وجريمة الإرهاب والجريمة الماسة بأنظمة المعالجة الألية للمعطيات، أما بالنسبة لقاضي التحقيق فيتحدد اختصاصه المحلي طبقا للمادة 40 من قانون الإجراءات الجزائية والذي يتحدد بمكان وقوع الجريمة أو محل إقامة الأشخاص المشتبه فيهم أو محل القبض على هؤلاء الأشخاص، وقد وسع المشرع من الاختصاص المحلي لقاضي التحقيق طبقا للفقرة الثانية من نفس المادة وذلك في جرائم محددة من بينها جرائم المساس بأنظمة المعالجة الألية للمعطيات، وبالتالي يصبح لقاضي التحقيق اختصاص إقليمي يتجاوز اختصاصه، ويمكنه التنقل للقيام بمهام التحقيق أو ندب ضابط شرطة قضائية.[1]

الفرع الثالث: الآليات القضائية لمواجهة الجريمة المعلوماتية

بالإضافة إلى الآليات المؤسساتية والقواعد القانونية التي وضعها المشرع لمواجهة الجريمة المعلوماتية، تم إنشاء آليات قضائية لمواجهة هذه الجريمة، حيث أقر المشرع الجزائري إنشاء أقطاب جزائية متخصصة لمواجهة الجرائم المعلوماتية من خلال الأمر 20-04 الذي تم من خلاله إنشاء القطب الجزائي الاقتصادي والمالي، وكذلك القانون رقم 21-11 المتعلق بإنشاء قطب جزائي متخصص في جرائم تكنولوجيا الإعلام والاتصال، واللذان يكتسيان طبيعة قضائية على عكس الهيئات الأخرى التي أنشأتها والتي تعتبر سلطات إدارية مستقلة، وبناء على هذا يعتبر القطب الجزائي المتخصص كوسيلة لتأكيد فعالية الأجهزة القضائية لمواجهة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.[2]

كما اهتم أيضا بالقيام بتكوين المورد البشري من خلال تكوين قضاة متخصصين في مثل هذه الجرائم من خلال توقيع اتفاقيات الشراكة مع بعض المؤسسات الأجنبية وتبادل الخبرات معها وإكساب القضاة الخبرة والكفاءة من أجل معالجة هذه الجرائم.

---

[1] شنتير خضرة، المرجع السابق، ص 214-215.

[2] بن عمير أمينة وبوحلايس إلهام، القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، مجلة البحوث في العقود وقانون الأعمال، المجلد 07، العدد 01، جامعة قسنطينة، 2022 ص 72.

البند الأول: القطب الجزائي الاقتصادي والمالي

القطب الاقتصادي والمالي هو جهاز قضائي متخصص بالنظر في نوع معين من الجرائم، وهي الجرائم الاقتصادية والمالية، ولقد أدت مجموعة من العوامل والأسباب بالمشرع الجزائري بالبحث عن آليات جديدة للتصدي لمواجهة الجريمة الاقتصادية والمالية المعقدة نظرا للأضرار التي تسببها للاقتصاد الوطني، ومن بين الآليات التي وجدها المشرع لمواجهة هذه الجريمة نجد القطب الجزائي الاقتصادي والمالي ومن الاسباب الدافعة لإنشائه نجد:

– قلت خبرة القضاة في مجال الجريمة المنظمة والمستحدثة وعدم وجود أساليب حديثة وفعالة لمواجهة هذه الجريمة.

- مسايرة مصالح البحث والتحري.
- الارتقاء بجهاز القضاء من خلال تكييف العدالة مع التطورات داخل الوطن وعلى المستوى الدولي وعصرنة قطاع العدالة.
- فتح أكبر ملفات الفساد المالي والاقتصادي أواخر سنة 2019 والتي كانت عبءً على المحاكم العادية وذلك لتعقيداتها وخصوصياتها.[1]

أنشأ المشرع الجزائري القطب الجزائري القطب الاقتصادي والمالي بموجب الأمر 20–04 المعدل والمتمم للأمر 66–155 المتضمن قانون الإجراءات الجزائية، إذ أحدثه من خلال هذا الأمر في الباب الرابع تحت عنوان القطب الجزائي الاقتصادي والمالي، حيث جاء في نص المادة 211 مكرر على أنه ينشأ قطب وطني متخصص لمكافحة الجريمة الاقتصادية والمالية وذلك على مستوى محكمة مقر مجلس قضاء الجزائر.[2]

[1] شهرزاد دراجي، القطب الجزائي الإقتصادي والمالي المستحدث، مجلة الدراسات القانونية والإقتصادية، المجلد 05، العدد 02، المركز الجامعي بريكة، 2022، ص 818–819.

[2] المادة 211 مكرر، من الأمر رقم 20–04، المؤرخ في 30–08–2020 المعدل والمتمم للأمر 66–155 المتضمن قانون الإجراءات الجزائية، ج.ر.ج.ج، العدد 51.

أولا: الاختصاص المحلي للقطب الاقتصادي والمالي

جاء في نص المادة 211 مكرر01 على انه يمارس كل من وكيل الجمهورية وقاضي التحقيق وكذلك رئيس القطب صلاحياتهم عبر كامل التراب الوطني، كما أنهم يمارسون أيضا اختصاصا مشتركا مع الاختصاص الوارد عن تطبيق المواد 37 و40 و329 من قانون الإجراءات الجزائية والتي تنص على تمديد الاختصاص الإقليمي لكل من وكيل الجمهورية وقاضي التحقيق ومحكمة الجنح في حالة الجرائم المذكورة على سبيل الحصر، وهي جرائم المخدرات والجريمة المنظمة العابرة للحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف.[1]

أقر المشرع الجزائري هذه المعايير حرصا منه على فعالية وسرعة معالجة الجرائم المالية المعقدة والمستحدثة.[2]

ثانيا: الاختصاص النوعي للقطب الجزائي الاقتصادي والمالي

حدد المشرع الجزائري الاختصاص النوعي من خلال المادة 211 مكرر02 و211 مكرر03 وهي جرائم ذات طابع اقتصادي ومالي والتي ذكرها على سبيل الحصر والمتمثلة في

1- الجرائم المنصوص عليها في المادة 119 مكرر من قانون العقوبات التي تنص على إهمال الموظف المؤدي إلى غلى سرقة أو إتلاف او اختلاس أو ضياع أموال عمومية أوخاصة أو وثائق ومستندات، وكذلك الجرائم المنصوص عليها في نصوص المواد 389 مكرر و389 مكرر01 و389 مكرر02 و389 مكرر03 من نفس القانون والتي تنص على تبييض الأموال.

2- الجرائم المنصوص عليها في الامر 96-22 المتعلق بقمع مخالفة التشريع والتنظيم الخاصين بالصرف وحركة رؤوس الأموال.

---

[1] المادة 211 مكرر01 – 211 مكرر 02، الامر 20-04، المصدر السابق.

[2] شهرزاد دراجي، المرجع السابق، ص 818-819.

3- الجرائم المنصوص عليها في القانون 06-01 المتعلق بالوقاية من الفساد ومكافحته

4- الجرائم المنصوص عليها في المواد من 11 إلى 15 من الأمر رقم 05-06 المتعلق بمكافحة التهريب والتي تنص على حيازة مخزن معد للتهريب أو وسيلة نقل تستخدم في ذلك، وكذلك استعمال وسيلة نقل في التهريب واستعمال سلاح ناري في التهريب وتهريب الأسلحة، وأفعال التهريب التي تهدد الأمن الوطني والصحة العمومية والاقتصاد الوطني.

كما جاء في نص المادة 211 مكرر03 أنه يتولى القطب البحث والتحري والمتابعة والتحقيق والحكم في الجرائم الاقتصادية والمالية الأكثر تعقيدا، ويقصد بها الجرائم التي ترتكب بتعدد الفاعليين والشركاء أو المتضررين أو لاتساع مجالها الجغرافي أو لجسامة أضرارها أو لكونها تكون في إطار منظم وعابرة للحدود الوطنية أو لاستعمال تكنولوجيا الإعلام والاتصال في ارتكابها وتتطلب اللجوء إلى وسائل خاصة وتحتاج لخبرة فنية.[1]

يختص القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بالجرائم التي ترتكب بواسطة المنظومة المعلوماتية، إلا أنه طبقا للمادة 211 مكرر28 من الأمر 21-11 إذا كانت هذه الجرائم ذات طابع اقتصادي ومالي يؤول الاختصاص للقطب الاقتصادي والمالي.[2]

البند الثاني: القطب الجزائي الوطني المتخصص في مكافحة جرائم تكنولوجيا الإعلام والاتصال

عدل المشرع الجزائري بموجب القانون 21-11 الأمر 66-155 المتضمن قانون الإجراءات الجزائية، حيث جاء هذا القانون ليتمم الكتاب الأول منه، وذلك بإضافة باب سادس تحت عنوان القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.[3]

---

[1] المادة 211 مكرر02 -211 مكرر03، من الأمر 20-04، المصدر السابق،

[2] شهرزاد دراجي، المرجع السابق، ص 821.

[3] المادة 01-02، الأمر 21-11 المؤرخ في 25 غشت 2021 المتمم للأمر 66-155 المتضمن قانون الإجراءات الجزائية، ج.ر.ج.ج، العدد 65.

نصت المادة 211 مكرر22 على أنه يتم إنشاء قطب جزائي على مستوى مجلس قضاء الجزائر يختص في التحقيق ومتابعة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال والجرائم التي ترتبط بها.[1]

حدد المشرع الجزائري من خلال هذا الأمر اختصاصات القطب الجزائي، حيث يتمتع باختصاص نوعي واختصاص إقليمي موسع، ويتجلى ذلك من خلال نص المادة 211 مكرر23 و211 مكرر24 وكذلك المادة 211 مكرر25.

أولا: الاختصاص النوعي

منح المشرع الجزائري الاختصاص للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنلوجيا الإعلام والاتصال، في متابعة نوع واحد من الجرائم وهي الجرائم المتصلة بتكنولوجيا الإعلام والاتصال والجرائم المتصلة بها، وهو ما ورد من خلال نص المادة 211 مكرر24 حيث أكدت المادة على أنه يختص وكيل الجمهورية وقاضي التحقيق ورئيس القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بالتحقيق والمتابعة والحكم في هذه الجرائم، وتتمثل في الجرائم ضد أمن الدولة أو الدفاع الوطني ونشر وترويج أخبار كاذبة والتي من شأنها المساس بالسكينة العامة واستقرار المجتمع، ونشر وترويج أخبار مغرضة من شأنها المساس بالنظام العام والأمن العام في طابع منظم وعابر للحدود، وجرائم المساس بأنظمة المعالجة الآلية للمعطيات المتعلقة بالمؤسسات العمومية، وكذلك جرائم التمييز وخطاب الكراهية والإتجار بالبشر والأعضاء البشرية.

ويختص أيضا وكيل الجمهورية وقاضي التحقيق وقاضي الحكم لدى القطب الجزائي المتخصص طبقا للمادة 211 مكرر25 بالتحقيق والمتابعة والحكم في الجرائم المعقدة في مجال تكنولوجيا الإعلام والاتصال، ويقصد بها الجرائم التي يكون تعدد الفاعلين أو الشركاء أوالمتضررين وكذلك لاتساع الرقعة الجغرافية أو الأضرار الجسيمة التي تترتب عليها أو لكونها

[1] المادة 211 مكرر22، من الأمر 21-11 المصدر السابق.

تكون في إطار منظم وعابرة للحدود الوطنية، أو لكونها تمس بالنظام العام والأمن العام وتتطلب استعمال وسائل خاصة للتحري وخبرة فنية والتعاون القضائي الدولي.

وطبقا لأحكام المادة 211 مكرر26 تطبق الإجراءات التي يعمل بها وكيل الجمهورية وقاضي التحقيق لدى القطب الجزائي نفس الإجراءات المنصوص عليها في نص المادة 211 مكرر 19 والمادة 211 مكرر 21، وبالعودة إلى هاتين المادتين فإن التقارير الإخبارية والتحقيقات في هذه الجرائم ترسل من قبل مصالح الضبطية القضائية إلى وكيل الجمهورية بمحكمة مقر مجلس قضاء الجزائر ويتلقى ضباط الشرطة القضائية التعليمات منه مباشرة، وفي حال فتح تحقيق قضائي يتلقون الإنابات القضائية من قاضي التحقيق المخطر بالملف، وإن تبين لقاضي التحقيق أن الوقائع المخطر بها لا تدخل ضمن اختصاصاته يصدر أمر بعدم الاختصاص، ويكون إما تلقائيا وبعد أخذ رأي وكيل الجمهورية، أو بناء على التماسات وكيل الجمهورية، ويتم تحويل الملف إلى النيابة العامة المختصة إقليميا عندما يصبح أمر قاضي التحقيق نهائيا وذلك بسعي وكيل الجمهورية.[1]

ثانيا: الاختصاص المحلي

وسع المشرع الجزائري من دائرة الاختصاص المحلي للقطب الجزائي الوطني لمكافحة جرائم تكنولوجيا الإعلام والاتصال، وهذا ما نصت عليه المادة 211 مكرر23، والتي نصت على أنه يمارس كل من وكيل الجمهورية وقاضي التحقيق ورئيس القطب صلاحياتهم عبر كامل التراب الوطني، وقد تطرق إليه المشرع الجزائري بنوع من الدقة في اختصاص هذا القطب، حيث منح له اختصاص حصري واختصاص مشترك، ويتمثل الاختصاص الحصري فما خوله المشرع للقطب بموجب نص المادة 211 مكرر 26 بمنحها اختصاصا حصريا في الجرائم المنصوص عليها في المادة 211 مكرر 24 والمادة 211 مكرر 25 وذلك عبر كامل التراب الوطني وهذا

[1] المادة 211 مكرر24 –211 مكرر25، من الأمر 21–11 المتمم للأمر، المصدر السابق.

راجع إلى خصوصية هذه الجرائم، وتكون بتشكيلة متخصصة في مثل هذه الجرائم التي تتسم بالتعقيد والخطورة وتمدد حتى خارج التراب الوطني.

أما بالنسبة للاختصاص المشترك يقوم فيه اختصاص القطب طبقا للمادة 211 مكرر27 وذلك بمناسبة وجود جريمة ماسة بأنظمة المعالجة، والذي يمتد فيه أيضا الاختصاص المحلي لوكيل الجمهورية لمحاكم أخرى طبقا لنص المادة 37، وكذلك امتداد الاختصاص الإقليمي لقاضي التحقيق المنصوص عليها في المادة 40 من قانون الإجراءات الجزائية وامتداد الاختصاص الإقليمي للمحاكم المنصوص عليها في المادة 329 لمحاكم أخرى باعتباره قطبا جزائيا.[1]

قد يتزامن اختصاص القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال مع اختصاص محكمة مقر مجلس قضاء الجزائر طبقا لما ورد في المواد من 211 مكرر16 إلى 211 مكرر21، والتي حددت الاختصاص المحلي لمحكمة مقر مجلس قضاء الجزائر في مجال جرائم الإرهاب والجريمة العابرة للحدود الوطنية، وهذا راجع لخطورة أثارها والأبعاد التي تأخذها الجريمة، وفي تزامن الاختصاص بين المحكمة والقطب يؤول الاختصاص طبقا للمادة 211 مكرر29 إلى محكمة مقر المجلس.

كما قد يتزامن الاختصاص أيضا مع القطب الاقتصادي والمالي، حيث تم إنشاء هذا الأخير بموجب الأمر 20-04 وذلك على مستوى محكمة مقر مجلس قضاء الجزائر، ويمتد اختصاصه أيضا عبر كامل التراب الوطني ويختص في الجرائم المنصوص عليها في قانون العقوبات مثل جريمة الاختلاس والغدر المنصوص عليها في المادة 119 مكرر وجريمة تبييض الأموال المنصوص عليها في المواد 389 مكرر و389 مكرر01 و389 مكرر02 بالإضافة إلى الجرائم المنصوص عليها في الأمر 96-22 المتعلق بقمع مخالفة التشريع الخاص بالصرف وحركة رؤوس الأموال من وإلى الخارج، والجرائم المنصوص عليها في الأمر

[1] بن عيمور أمينة وبوحلايس إلهام، المرجع السابق، ص 75.

05-06 المتعلق بمكافحة التهريب، وعليه فإذا كانت الجريمة من اختصاص القطبين وفي حالة وجود تنازع إيجابي بينهم يؤول الاختصاص وجوبا إلى القطب الاقتصادي والمالي وهذا ما نصت عليه المادة 211 مكرر28 من قانون الإجراءات الجزائية.[1]

البند الثالث: تكوين القضاة في مجال الجريمة المعلوماتية

بالإضافة إلى الآليات القضائية التي تم إنشائها عملت الجزائر أيضا على تكوين القضاة في مجال الجريمة السبيرانية، حيث تم تكوين القضاة في إطار الاتفاقيات الدولية، ومن بين هذه الاتفاقيات نجد التكوينات التي تلقاها القضاة في إطار البرنامج الأوروبي لمكافحة الجريمة السبيرانية من سنة 2015 إلى غاية 2019 والتي سنبينها في الجدول الآتي:

تكوين القضاة في إطار البرنامج الأوروبي لمكافحة الجريمة السبيرانية من 2015 إلى 2022

السنوات	2015	2016	2017	2018	2019	2020	2021	2022	المجموعة
عدد التكوينات	01	01	-	02	05	08	23	16	56
القضاة	02	-	-	23	11	46	88	140	310
الإطارات	-	02	-	-	-	-	16	09	27

كما تم أيضا في إطار هذا البرنامج تكوين 25 قاضيا في إطار الجريمة المعلوماتية والأدلة الإلكترونية من 29 جانفي إلى 02 فيفري 2023 في المدرسة العليا للقضاء، أين تم من خلالها معرفة المفاهيم المتعلقة بتكنولوجيا الإعلام والاتصال والإطار القانوني الوطني

[1] بن يونس فريدة، استحداث قطب جزائي وطني لمكافحة الجرائم السبيرانية ومتابعتها، مجلة الدراسة القانونية والاقتصادية، المجلد 05 العدد 01 جامعة مسيلة، س 2022 ص 1723-1724.

والدولي المتعلق بالجريمة السبيرانية، والتعاون القضائي في هذا المجال وكذلك في الأدلة الإلكترونية[1].

كما أكد وكيل الجمهورية الرئيسي لدى القطب الجزائي الاقتصادي والمالي خلال مداخلة له في اليوم الدراسي الذي تم تنظيمه بمقر مجلس قضاء الجزائر في شهر مارس من هذه السنة والذي كان تحت عنوان الإطار المفاهيمي للجريمة المعلوماتية على ضرورة إلمام القضاة بتقنيات والمخططات التي يقوم بها المجرم المعلوماتي، حيث يشكل الضرر المادي المترتب عن الجريمة الإلكترونية الخطر الأكبر لذا وجب زيادة حماية بيانات الأشخاص والشركات.[2]

[1] موقع وزارة العدل، https://www.mjustice.dz/، تاريخ الاطلاع 29-05-2024، على الساعة 20.15.

[2] موقع الشروق أونلاين، https://www.echoroukonline.com/، تاريخ الاطلاع 2024/06/01 على الساعة 10.30.

المبحث الثاني: مكافحة الجريمة المعلوماتية على المستوى الدولي والإقليمي

تشكل الجرائم المعلوماتية تهديدا خطيرا وأصبحت مكافحتها أكثر أهمية في ظل تزايد التكنولوجيا واستخدام الانترنت في حياة الفرد والشركات والحكومات، فمن الضروري التعاون الدولي لمكافحة هذه الجرائم لتعزيز الأمن الرقمي العالمي وحماية المجتمعات من التهديدات السيبرانية، فالتعاون الدولي في هذا المجال ليس ضروريا فقط لمكافحة الجرائم المعلوماتية، بل أيضا لمواجهة التحديات المستقبلية التي قد تظهر مع تطور التكنولوجيا، وهذا الامر لا يمكن لأي دولة أن تحققه بمفردها، لابد من أن يكون هذا التعاون بالجهود المشتركة من قبل الدول المختلفة، وعلى ذلك سوف نتناول في **(المطلب الأول)** إلى الجهود الدولية لمكافحة الجريمة المعلوماتية، أما **(المطلب الثاني)** فخصصناه الجهود الإقليمية لمكافحة الجريمة المعلوماتية.

المطلب الأول: مكافحة الجريمة المعلوماتية على المستوى الدولي

من المستحيل مكافحة الجرائم المعلوماتية الا اذا كان هناك تعاون دولي على المستويين القانوني والجنائي، وكذلك في إطار الجهد الدولي المبذول على مستوى نظام العدالة الجنائية، حيث هناك العديد من الهيئات والمنظمات الدولية التي تلعب دورا هاما في إطار إبرام الاتفاقيات من أجل إثبات ضرورة التعاون الدولي لمكافحة جرائم المعلوماتية،[1] وتجسدت مساعي هذه المنظمات الدولية ومنظمة الأمم المتحدة من خلال عقد اتفاقيات ومعاهدات وإصدار قرارات لوضع أليات للحد من هذه الجريمة، كما نجد أيضا الدور الفعال والتعاون بين الأجهزة الأمنية المختلفة في إطار التعاون الشرطي الدولي، والذي تجسد في جهود المنظمة الدولية للشرطة الجنائية (الإنتربول)، وفي هذا الإطار سنبين من خلال مطلبنا هذا دور كل

[1] فاروق خلف، الآليات القانونية لمكافحة الجريمة المعلوماتية، مجلة الحقوق والحريات، المجلد 3، العدد 2، جامعة محمد خيضر بسكرة، سنة 2015، ص 11.

من المنظمات الدولية ومنظمة الأمم في مواجهة الجريمة المعلوماتية (الفرع الأول)، أما (الفرع الثاني) سنبين من خلاله التعاون الدولي في المجال الشرطي.

الفرع الأول: دور هيئة الأمم المتحدة والمنظمات الدولية الأخرى في مكافحة الجريمة المعلوماتية

قامت الأمم المتحدة بجهود كبيرة في محاربة جرائم الإنترنت، بهدف تقليل الأضرار الجسيمة التي تلحق بالبشرية بشكل عام حيث تعتقد الأمم المتحدة أن منع هذه الجريمة ومكافحتها يتطلب تعاون دولي نظرا للطبيعة العابرة للحدود، والأبعاد الدولية لسوء استخدام الكمبيوتر والجرائم المتعلقة به، وعليه تهدف هذه الجهود إلى الحفاظ على السلام والأمن الدوليين وتعزيز العلاقات الودية بما في ذلك الجرائم الإلكترونية والمصادقة على العديد من الاتفاقيات الدولية ذات صلة بهذا الموضوع.[1]

البند الأول: دور الأمم المتحدة في مواجهة الجريمة المعلوماتية

عملت هيئة الأمم المتحدة على مواجهة الجريمة المعلوماتية من خلال إصدار مجموعة من القرارات وكذلك الاتفاقيات والمعاهدات، وأيضا عقد العديد من المؤتمرات وهذا ما سنبينه من خلال هذا البند.

أولا: قرارات الجمعية العامة للأمم المتحدة

ومن أبرز قرارات الجمعية العامة للأمم المتحدة مايلي:

1-القرار 45 /121 لسنة 1990 دليل منع الجرائم المتصلة بأجهزة الكمبيوتر ومكافحتها في عام 1994.

2-قرار رقم 55 /63 المؤرخ في 2002/12/4 والقرار رقم 121/56 المؤرخ في 2001/12/19 بشأن مكافحة استعمال التكنولوجيا الإدارية و الجنائية لتقنية المعلومات،

[1] محمود محمد صفاء الدين علي شرشر، الجهود الدولية ولتشريعية لمكافحة جرائم الإنترنت، المجلد 54، العدد 03، جامعة المنوفية مصر، 2021، ص 528.

ويطلب هذا القرار من الدول الأعضاء وضع تشريعات وطنية لمكافحة سوء استخدام تكنولوجيا المعلومات ومع مراعاة عمل لجنة منع الجريمة للعدالة الجنائية.[1]

3-القرار رقم 57 /239المؤرخ في 31 /2003/01 والقرار 199/58 الصادر في 2004/01/30 تأسست ثقافة عالمية للأمن المعلوماتي وتمت دعوة الدول الأعضاء للتعاون من أجل تعزيز هذه الثقافة.

4-إضافة إلى قرار لجنة مكافحة المخدرات رقم 48 /5 بشأن تعزيز الدولي لمنع ارتكاب الجرائم المتعلقة بالمخدرات عبر استخدام الإنترنت.[2]

5-قرار 230/65 قررت الجمعية العامة طلبا إلى لجنة منع الجريمة العدالة الجنائية إنشاء فريق خبراء حكومي دولي مفتوح العضوية لإجراء دراسة شاملة حول مشكلة الجريمة السيبرانية والتدابير التي تتخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص لمواجهتها بما في ذلك تبادل المعلومات حول التشريعات الوطنية والمساعدة التقنية والتعاون الدولي.[3]

6- قرار 282/75 بتاريخ 26 ماي 2021، لمحاربة استخدام تكنولوجيا المعلومات والاتصالات للأغراض إجرامية.[4]

7-قرار 78 /213 تعزيز حقوق الإنسان وحمايتها في ظل التكنولوجيا الرقمية.

8-قرار 237/78 التطورات في مجال تكنولوجيا المعلومات والاتصالات سواء السلكية أواللاسلكية في إطار الأمن المعلوماتي.

9-قرار78 /243 تنفيذ استراتيجية تكنولوجيا المعلومات والاتصالات.[1]

---

[1] فاروق خلف، المرجع السابق، ص11.

[2] سهيلة هادي، آليات تعزيز حق الإنسان في الأمن المعلوماتي، مجلة للعلوم القانونية الإقتصادية والسياسية، المجلد 54، العدد *05، كلية الحقوق، جامعة خيضر بسكرة، س 2017، ص 235.

[3] دراسة شاملة عن الجريمة السيبرانية، مسودة صادرة عن مكتب الأمم المتحدة المعني بالمخدرات والجريمة.

[4] https://www.un.org/ar/ga/75 بتاريخ 2024/04/20 على الساعة 23.00 ليلا.

ثانيا: اتفاقيات الأمم المتحدة في مجال مكافحة الجريمة المعلوماتية

عقدت هيئة الأمم المتحدة العديد من الاتفاقيات وسنذكر من خلال هذا البند أبرزها وهي:

1- اتفاقية برن الدولية لحماية المصنفات الأدبية والفنية

تم توقيع عليها في عام 1971 في سويسرا من قبل 120 دولة، و بموجب اتفاقية برن الدولية تُعتبر برامج الكمبيوتر بالغة المصدر أو الآلة، أعمالًا أدبية محمية بموجب الاتفاقية كما تمنح المادة 09 من الاتفاقية لأصحاب حقوق المؤلف الحق الحصري في السماح بإنشاء نسخ من هذه المصنفات بأي شكل من الأشكال، ومن عيوب هذه الاتفاقية أنها لم تحدد قائمة محددة بالمصنفات المحمية بل تركت ذلك للتشريعات الوطنية لكل دولة، وقد أدى ذلك إلى غموض وعدم اتساق في نطاق الحماية بين الدول المختلفة، أيضا اعتبرت الاتفاقية برامج الكمبيوتر من بين المصنفات المحمية، لكنها لم تمنحها حماية خاصة، وبالتالي يمكن القول أن حماية البرامج المعلوماتية لم تكن موضوعًا مباشرًا لهذه الاتفاقية وربما يعود السبب في ذلك إلى أن حجم القرصنة في ذلك الوقت لم يكن كبيرًا كما هو الحال اليوم.[2]

وتستند هذه الاتفاقية إلى ثلاث مبادئ أساسية:

- **مبدأ المعاملة الوطنية**

تتمتع المصنفات التي يبدعها المؤلفون في دولة متعاقدة بنفس الحماية التي تتمتع بها المصنفات التي يبدعها المؤلفون داخل أراضي أي دولة متعاقدة أخرى. وبعبارة أخرى، لا يجوز تمييز الأعمال الأجنبية ضد الأعمال المحلية.

- **مبدأ الحماية التلقائية**

لا يتطلب حماية حقوق المؤلف بموجب اتفاقية برن أي إجراءات رسمية من قبل المؤلف مثل التسجيل أو الترخيص فور إنشاء العمل، يتمتع بحماية تلقائية بموجب الاتفاقية

[1] موقع هيئة الأمم المتحدة، https://www.un.org/ar/ga/78/، بتاريخ 20/04/ 2024، على الساعة 00.41.

[2] محمود صفاء الدين علي شرشر، المرجع السابق، ص 539.

- **مبدأ استقلال الحماية**

اتفاقية برن لحماية حقوق المؤلف لا تعتمد على مستوى الحماية في بلد المنشأ للعمل. حتى إذا كانت الحماية ضعيفة في بلد المنشأ، فإن العمل سيظل محميًا وفقًا للحد الأدنى من معايير الحماية في الدول الأخرى المتعاقدة[1]

2-اتفاقية تريبس

وتعد اتفاقية تريبس من المعاهدات الأخرى المنجزة في مجال حماية الملكية الفكرية، خاصة في ظل انتشار السرقة الإلكترونية للأعمال الفنية دون احترام لحقوق المالكين المادية والمعنوية، وتم التوقيع على اتفاقية تريبس من قبل الدول الأعضاء في **منظمة التجارة العالمية (WTO)** وتهدف إلى معالجة الاختلافات بين المعايير الدولية والمحلية في حقوق الملكية الفكرية، وتتضمن الاتفاقية العديد من الإجراءات الهامة والفعالة لمنع الاعتداءات على حقوق الملكية الفكرية، كما تقدم حماية دولية جنائية ومدنية وإدارية لبرامج الحاسوب والمكتبات الفكرية بشكل عام،[2] كما اكدت المادة 41 من الاتفاقية على ضرورة دعم وحماية حقوق الملكية الفكرية الرقمية و على أهمية توازن هذه الحماية مع عدم إعاقة التجارة الدولية، وتم اعتماد هذه الاتفاقية في المادة 61 كوسيلة لمكافحة انتهاك حقوق الملكية الفكرية من خلال التعاون الدولي مثل تبادل المعلومات الإدارية حول السلع والمواد التي تشكل انتهاكًا لحقوق الملكية الفكرية مثل التقليد.[3]

3-اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للوطنية UNTOC لعام 2000

تم اعتماد اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للوطنية في عام 2000 في باليرمو بإيطاليا، وقد أظهرت هذه الاتفاقية إرادة المجتمع الدولي السياسية لمواجهة التحدي العالمي من خلال استجابة عالمية فالجريمة لا تعترف بالحدود الوطنية، وبتالي يجب أن

---

[1] https://www.wipo.int/treaties/ar/، بتاريخ 2024/5/31، على الساعة 10:30 صباحا.

[2] محمود مدين، المرجع السابق، ص 164.

[3] خالد حسن أحمد لطفي، المرجع السابق، ص95 و96.

يتجاوز تنفيد القانون هذه الحدود أيضا، وتحدد اتفاقية الأمم المتحدة المجالات التي تكافح فيها الأطراف الجريمة المنظمة العابرة للوطنية بما في ذلك الجرائم الإلكترونية والجرائم المتعلقة بالهوية والمواد الضارة بالبيئة والقرصنة وتجارة الأعضاء والأدوية المزيفة، ويتطلب ظهور هذه الجرائم الجديدة إلى الحاجة إلى استجابات فعالة من أجهزة إنفاذ القانون لتكييف جهودها وقدراتها مع هذه التحديات الجديدة،[1] حيث تعمل الأمم المتحدة على صياغة معاهدة دولية لمكافحة الجرائم السيبرانية منذ خمس سنوات، إذ جرت أخر جولة من المفاوضات في فبراير 2024 ومن المتوقع أن يتم إصدار النصوص النهائية للمعاهدة في أواخر مايو أو يونيو لعام 2024، هذا يعني أن الدول الأعضاء قد تتلقى النص النهائي للمعاهدة قريبا لتقييمه والتوقيع عليه.

4-المعاهدة العالمية للجرائم الإلكترونية

تم عقد لقاء في مارس 2022، للجنة الأممية المخصصة لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيا المعلومات والاتصالات لأهداف إجرامية، والتي ترأست الجزائر دورتها الأولى حيث من خلالها عرض مشروع المعاهدة خلال الدورة 78 للجمعية العامة للأمم المتحدة المزمع عقدها خلال هذه السنة (2024).[2]

وفي هذا السياق تعمل الأمم المتحدة على صياغة معاهدة دولية لمكافحة الجرائم السيبرانية منذ خمس سنوات، اختتمت الجولة الأخيرة من المفاوضات في فبراير 2024، تاركةً وراءها نصًا قيد التطوير، ومن المقرر إصدار النسخة النهائية للمعاهدة خلال عام2024، ستُتيح هذه المعاهدة للدول الأعضاء تقييمها والتصويت على تبنيها، مما يعني أنه من المرجح أن تتسلمه الدول الأعضاء وتقوم بتقييمه قريبًا.[3]

---

[1] هه لاله محمد تقي محمد أمين، التعاون الدولي في مواجهة الجرائم المستحدثة، أطروحة نيل شهادة الدكتوراه، فلسفة في القانون العام جامعة السليمانية العراق، ص 24.

[2] موقع وكالة الأنباء الجزائرية، https://www.aps.dz/ar/، تاريخ الاطلاع 2024/05/31، على الساعة 18.30.

[3] موقع أخبار الأمم المتحدة، https://news.un.org/ar/ بتاريخ 2024/05/30، على الساعة 11.00 صباحا.

وبخصوص التطورات الحاصلة لهذه الاتفاقية أكد "**جيت سينغ شيما**" أن الأعمال لن تكتمل عند نهاية هذه الدورة حيث تم تعليق العملية من قبل مكتب الأمم المتحدة المعني بالمخدرات والجريمة على أن تتواصل المفاوضات في وقت لاحق، وأكد أن غالبية الدول تريد رؤية نتيجة لهذه المعاهدة أو حتى لا ينظر إليها أنها تعيق وتعرقل العملية والإضرار بها وأنه تم إصدار بيان مشترك من قبل المجتمع المدني والخبراء والفنيين على أنه على الدول عدم المصادقة على هذه الاتفاقية وذلك لأنها لا تفي بالغرض.[1]

كما أعلنت هيومن رايت ووتش، وهي منظمة غير حكومية للدفاع عن حقوق الإنسان أن المعاهدة العالمية المتعلقة بالجرائم الإلكترونية المحتمل المصادقة عليها أنه يمكن استخدامها كذريعة لإسكات منتقدي الحكومات، وأنه بدلا من توقيع المعاهدة ولابد من إصلاح القوانين التي تتعارض مع حقوق الإنسان، واستشارة منظمة حقوق الإنسان في كل خطوة.[2]

ثالثا: المؤتمرات التي عقدتها الأمم المتحدة لمكافحة الجريمة المعلوماتية

سعيا من هيئة الأمم المتحدة لمواجهة الجريمة المعلوماتية عقدت العديد من المؤتمرات لدراسة أسباب هذه الجريمة وتقديم الحلول للحد منها ومواجهتها وتتمثل فيمايلي:

1-المؤتمر السابع لمنع الجريمة ومعاملة المجرمين

عقد المؤتمر السابع في الفترة من 26 أوت إلى 06 سبتمبر 1985 تم تكليف لجنة خبراء حماية نظم المعلومات بدراسة موضوع حماية نظم المعالجة الآلية والهجمات الحاسوبية وإعداد تقرير للمؤتمر والغرض من ذلك تقديمه إلى المؤتمر الثامن.[3]

---

[1] موقع أخبار هيئة الأمم المتحدة، https://news.un.org/ar/story بتاريخ 2024/05/30، على الساعة 11:30.

[2] موقع هيومن وايتس ووتش، https://www.hrw.org/ar ، تاريخ الاطلاع 2024/05/30، على الساعة 12:10.

[3] بيدي أمال، جهود الأمم المتحدة في مكافحة السيبرانية، مجلة الحقوق والعلوم الإنسانية، المجلد 08، العدد 01، جامعة الجلفة الجزائر، 2022، ص 306.

2-المؤتمر الثامن لمنع الجريمة ومعاملة المجرمين هافانا كوبا 1990

شارك في المؤتمر 127 حكومة و46 منظمة غير حكومية، حيث أوصى المؤتمر الثامن باتخاذ بتدابير لمكافحة الجريمة المنظمة والإرهاب في إطار موضوع منع الجريمة والعدالة الجنائية على المستوى الدولي في القرن الحادي والعشرين، حث المؤتمر بإجراء بحث حول بنية الجريمة المنظمة وتقييم التدابير المضافة للقائمة وتعزيز التعاون الدولي في مكافحة الإرهاب وإنشاء لجنة حكومية دولية للحد من الجريمة وتعزيز العدالة الجنائية.[1]

3- **المؤتمر التاسع للأمم المتحدة حول منع الجريمة معاملة المجرمين**

أقيم المؤتمر التاسع للأمم المتحدة حول منع الجريمة ومعاملة المجرمين في القاهرة بمصر بين 28 أفريل و5 ماي، وقد عالج هذا المؤتمر العديد من القضايا المهمة المتعلقة بالجريمة والعدالة الجنائية بما في ذلك حماية حقوق الإنسان في حياته ومليكته الفكرية من مخاطر التكنولوجيا المتزايدة، كما شدد المؤتمر على أهمية تنسيق والتعاون بين الدول الأعضاء لا تخاد بعض الإجراءات اللازمة لمكافحة الجريمة ومنعها.[2]

4- **المؤتمر الحادي العشر**

عقد ببانكوك بتايلند في 2005 تناول هذا المؤتمر العديد من المواضيع حول تدعيم التعاون الدولي في مجال إنفاذ القانون بما في ذلك إجراءات تسليم المجرمين وتعزيز إصلاح العدالة الجنائية، وكذلك تم مناقشة استراتيجيات منع الجريمة وإجراءات منع الإرهاب والتصدي للجريمة الاقتصادية مثل: جرائم غسل الأموال، و طرق وقاية من الجرائم الحاسوبية.[3]

5- المؤتمر الثاني عشر

عقد في سلفادور بالبرازيل عام 2010 وناقش هذا المؤتمر على دور العدالة في التنمية وتم التأكيد على ضرورة إتباع نهج شامل لإصلاح أنظمة العدالة الجنائية لتعزيز قدراتها كما تم

---

[1] https://unis.unvienna.org/pdf بتاريخ2024/05/01 ، على الساعة ،15:09 مساءا.

[2] أمال بيدي، المرجع السابق، ص 308.

[3] https://unis.unvienna.org/pdf بتاريخ 01/05/ 2024 على الساعة 22:00.

أيضا الإقرار على ضرورة البحث عن سبل لمنع ومكافحة الأشكال الجديدة للجريمة على الصعيد العالمي وتأكيد على ضرورة تعزيز التعاون الدولي والإقليمي من أجل منع الجريمة وملاحقة المجرمين قضائيا ومعاقبتهم، وأيضا البحث الشامل عن الجريمة السيبرانية وطرق مكافحتها من قبل الدول الأعضاء والمجتمع الدولي والقطاع الخاص ومن بين التدابير والوسائل للتصدي لهذه الجريمة نجد تبادل المعلومات والتشريعات الوطنية والمساعدة التقنية، كما تم اقتراح إجراءات جديدة لمكافحة هذه الجريمة.[1]

6-المؤتمر الثالث عشر

عقد المؤتمر الثالث عشر في الدوحة بقطر من فترة 12 إلى 19 أفريل 2015، وتم تأكيد في هذا المؤتمر على مكافحة الإجرام بشتى أنواعه وأشكاله على الصعيدين المحلي والدولي وشدد عدة متحدثون في المؤتمر على أهمية التوعية العامة بمخاطر الجريمة السيبرانية وطرق مكافحتها، كالاحتيال الاقتصادي وتهديد الخصوصية والتزوير والجرائم المتصلة بالهوية واستغلال الأطفال جنسيا من خلال الإنترنت، وأيضا الثغرات في أنظمة الأمن لتسمح باختراق البيانات وسرقتها ووجهت الدعوى إلى تعزيز التعاون الدولي وتبادل الممارسات الجيدة في هذا المجال، ودعا البعض إلى وضع إطار قانوني دولي جديد للتصدي للجريمة السيبرانية وتعزيز الأمن السيبراني، مما يؤدي إلى تحقيق التوازن بين إنفاذ القانون وحقوق الإنسان واحترام الخصوصية، وأكد اخرون على ضرورة تطبيق القوانين والمواثيق الدولية الموجودة لمكافحة الجريمة الإلكترونية.[2]

[1] موقع الجزيرة نت،https://www.aljazeera.net/news بتاريخ 2024/05/01 على الساعة 21.40.

[2] https://www.unodc.org بتاريخ 2024/05/01 على الساعة 22.00 مساءا.

البند الثاني: دور المنظمات الدولية الأخرى في مجال مكافحة الإجرام السيبراني

اتخذت عدة منظمات دولية مبادرات كمنظمة التعاون الاقتصادي والتنمية Ocde والاتحاد الدولي للاتصالات ومنظمة الدول الامريكية OAS المنتدى العالمي WFF والمنظمة العالمية للملكية الفكرية WIPO الدول G8.

أولا: الاتحاد الدولي للاتصالات(itu)

شهد قانون الاتصالات تطورات عديدة على مر الزمن والذي بدأ بحماية الكابلات البحرية واصبح الأن قانون الاتصالات حديث تحت قيادة الاتحاد الدولي للاتصالات، حيث تحول الاتحاد الدولي للاتصالات إلى منظمة رائدة في مجال تكنولوجيا الاتصالات، وتنص المادة 35 من ميثاق الاتحاد الدولي للاتصالات على عملية التدخل في أنشطة الاتصالات، كما ظهر الإعلان الخاص بالقمة العالمية لمجتمع المعلومات على بناء الثقة والأمن في استخدام تكنولوجيا الاتصالات، يقوم الاتحاد الدولي للاتصالات بدعم التعاون بين الشركات الخاصة والوكالات الحكومية لإنشاء شبكة تكنولوجيا الإنترنت، وكذلك تنسيقا للجهود ووضع استراتيجيات لأمن المعلومات العالمي.[1]

قاد الاتحاد الدولي للاتصالات ملتقى دولي رئيسي لهذه الأنشطة، ويعمل مع مجلس أوربا في إنجاز الاتفاقية الأوربية بشأن الجرائم السيبرانية وإنشاء إطار قانوني دولي لمواجهتها، وقد عمل التحالف الدولي مع الإنتربول الدولي واليوروبول الخاص بالاتحاد الدولي بالإضافة إلى منظمة الأمن، ومكتب الأمم المتحدة لمكافحة الجريمة والمخدرات، حيث تهدف هذه الجهود إلى تعزيز الأمن السيبراني.[2]

تمت الموافقة على القرار رقم 45 لعام 2006 من قبل الاتحاد الدولي لاتصالات، والذي تم إصداره خلال المؤتمر العالمي لتنمية الاتصالات، ودعى القرار إلى إنشاء مؤتمر يتناول أمن

[1] عادل عبد الصادق، الإرهاب الإلكتروني القوة في العلاقات الدولية نمط جديد وتحديات مختلفة، مركز الأهرام للدراسات السياسية والاستراتيجية، ط اولى، القاهرة، ص 323.

[2] عادل عبد الصادق، المرجع نفسه، صفحة 323.

المعلومات ومكافحة الرسائل الاقتحامين والهجمات السيبرانية بالإضافة إلى إطلاق جدول أعمال معالجة التحديات المتزايدة في أمن الإنترنت، وتقديم حلول لتحسين أمن الإنترنت، وقد نشرت في عام 2008 استراتيجية تشمل التدابير القانونية والتقنية والتشغيلية لبناء القدرات.[1]

ثانيا: المنظمة العالمية للملكية الفكرية " الويبو"

هي اتفاقية حق المؤلف التي اعتمدتها المنظمة العالمية للملكية الفكرية عام 1996 والتي توفر حماية إضافية لحقوق التأليف والنشر، مع مراعاة التطورات في تكنولوجيا المعلومات، كما تشمل الحماية بموجب هذه الاتفاقية برامج الحاسوب، وذلك من خلال اعتمادها لنصوص قانونية طبقا للمادة 4 و5 من اتفاقية تريبس.[2]

ثالثا: المنتدى الاقتصادي العالمي (WFF)

في عام 2018 أصدر المنتدى الاقتصادي العالمي WFF دليلا يعرف باسم دليل المرونة السيبرانية للتعاون بين القطاعين الحكومي والخاص، يهدف هذا الدليل إلى تزويد الحكومات والشركات الخاصة بإرشادات حول كيفية التعاون لتطوير سياسات فعالة لأمن الإنترنت، ويقدم الدليل إطارا عمليا يتكون من ثلاث طبقات للتعاون بين القطاعين الحكومي والخاص وتحديد الأدوار والمسؤوليات وتقسيم القدرات ووضع خطط لتحسين القدرات، كما يركز الدليل على ثلاث قدرات رئيسية وهي المتانة والمرونة والدفاع، حيث كل واحدة منها تقوي قدرات الأخرى وتعرف "المتانة بأنها القدرة على منع وصد واحتواء التهديدات السيبرانية"، أما المرونة فتعني "القدرة على الإدارة والتعامل مع الخروقات الإلكترونية التي قد تحدث"، أما الدفاع فهو "القدرة على استباق الهجمات الإلكترونية وتعطيلها والاستجابة لها".

وعليه فإن هذا الإطار يعتمد على العمل على المبادرات السابقة من المنتدى الاقتصادي العالمي، بما في ذلك مجلس أجندة المخاطر والمرونة الوطنية لعام 2014، والورقة البيضاء

[1] فرح يحي وعاترة، التهديدات السيبرانية على الأمن القومي، العربي للنشر والتوزيع، ط 2023، القاهرة، ص 72.

[2] طاهر الياكر، الجرائم الإلكترونية، المرجع السابق، ص 160.

فهم الخطر السيبراني النظامي لعام 2016، كما ناقش المنتدى الاقتصادي العالمي أيضا المخاطر السيبرانية وربطها بالتأثيرات الاقتصادية والتبعات التجارية لنقص الأمن السيبراني.[1]

رابعا: منظمة التعاون الاقتصادي والتنمية OCED

تهدف هذه المنظمة إلى تحقيق أعلى مستوى من النمو الاقتصادي وتنسيق التنمية الاقتصادية مع التنمية الاجتماعية، وبدأت المنظمة بالتركيز على الجرائم الإلكترونية عام 1978، عندما قامت بوضع مجموعة من الإرشادات والقواعد المتعلقة بتكنولوجيا المعلومات ودليل لحماية الخصوصية وكانت قواعد نقل البيانات من المبادئ التوجيهية الأولى، التي تم اعتمادها من قبل مجلس المنظمة في عام 1980 ويوصى الأعضاء بالالتزام بها.[2]

وتقوم المنظمة التي تضم 34 دولة بوضع توصيات إرشادية بشأن أمن نظم المعلومات، ومن بين أعمال منظمة التعاون الاقتصادي والتنمية في مجال مكافحة الجرائم الإلكترونية، وتم التوصل إلى اتفاق بأن يتضمن قانون العقوبات في كل دولة مجموعة من الأفعال كالتلاعب في البيانات المعالجة آليا بما في ذلك حذفها والتجسس المعلوماتي وتدمير المعلومات و قرصنة البرمجيات، وكذلك الوصول إلى البيانات أو نقلها بشكل غير قانوني وكذلك اعتراض استخدام المعطيات أو نقلها.[3]

---

[1] موقع potomac institute for policy studies ، https://potomacinstitute.org بتاريخ 2024/04/24 على الساعة 6.42 صباحا.

[2] مراد مشوش، الجهود الدولية لمكافحة الإجرام السيبراني، المجلد 12، العدد 02، جامعة غرادية، س 2019، ص 709

[3] فاروق خلف، المرجع السابق، ص 12.

الفرع الثاني: التعاون الدولي في المجال الشرطي لمكافحة الجريمة المعلوماتية

تعد الأجهزة الشرطية من أبرز أجهزة العدالة الجنائية في مجال مكافحة الجريمة حيث تقوم بدور هام في التحقيق في الجرائم وجمع الأدلة.[1]

البند الأول: المنظمة الدولية للشرطة الجنائية (الإنتربول)

المنظمة الدولية للشرطة الجنائية (الإنتربول) المعروفة أيضا باسم اللجنة الدولية للشرطة الجنائية Icpo ومقرها بباريس بفرنسا، وقد أعيد تسميتها بالمنظمة الدولية للشرطة الجنائية وتضم أكثر من 182 دولة عضوا وهي مسؤولة عن تعاون أجهزة الشرطة في الدول الأطراف في القبض على المجرمين، كما تهدف المنظمة إلى تحديد وتشجيع التعاون بين أجهزة الشرطة في الدول الأطراف من جمع البيانات والمعلومات المتعلقة بالجريمة والجرائم وذلك من خلال أمانة مركزية مشتركة بين الدول الأعضاء لمكافحة الجريمة بفعالية، وقد أنشأت المنظمة عدة مراكز اتصالات إقليمية، حيث نجد في طوكيو ونيوزيلندا ونيروبي وأذربيجان وبونيس يرس لجعل عملية نقل الرسائل سهلة، بالإضافة إلى مكتب إقليمي فرعي في بانكوك، وقد يتم وضع نموذجين أحدهما مخصص للدول المركزية التي تتواصل مع أجهزة الشرطة في جميع أنحاء العالم والآخر للدول اللامركزية، حيث تتواصل أجهزة الشرطة الوطنية مع بعضها البعض مباشرة.[2]

أولا: مبادئ المنظمة الدولية للشرطة الجنائية (الإنتربول).

تتمثل المبادئ الأساسية لمنظمة الإنتربول في النقاط التالية:

- احترام السيادة الوطنية للدول الأعضاء في المنظمة، أي تقوم العلاقات بين سلطات الشرطة الوطنية على احترام السيادة الوطنية واحترام القوانين والأنظمة الوطنية للدول الأعضاء على

---

[1] عائشة عبد الحميد، النظام القانوني للمنظمة الدولية للشرطة الجنائية (الإنتربول) ودورها في المجال التعاون القضائي الشرطي المجلة الأكاديمية للأبحاث والنشر العلمي، المجلد 11، جامعة الطارف، الجزائر، 2020، ص 6.

[2] غانم مرضي الشمري، الجرائم المعلوماتية ماهيتها وخصائصها وكيفية التصدي لها قانونيا، دار الثقافة، ط أولى، عمان، ص 96-97.

النحو المنصوص عليه في المادة 02 من النظام الأساسي للإنتربول وتنسيق أنشطتها لتحقيق أهداف الإنتربول.

- تنفيذ قرارات الجمعية العامة للإنتربول طبقا للمادة 09 من ميثاق المنظمة على أن جميع الدول الأعضاء ملزمة لتنفيذ أي قرارات تتخذها الجمعية العامة، وتقع ضمن اختصاصها.[1]
- المساهمة في تمويل المنظمة وفقا للمادة 38من القانون الأساسي للمنظمة تتألف مواردها من اشتراكات مالية من الأعضاء والهبات والوصايا والتبرعات وأية موارد أخرى بشرط موافقتها عليها بمعرفة اللجنة التنفيذية وفقا للمادة 52 من القانون الأساسي للمنظمة، كما تفرض اللجنة التنفيذية للمنظمة الدولية للشرطة الجنائية عقوبات على الدول الأعضاء المتأخرة في سداد مساهمتها، بالإضافة إلى ذلك تتلقى المنظمة الدولية للشرطة الجنائية بعض الموارد كالمطبوعات الصادرة عن المنظمة، أما بالنسبة للموارد المالية الخاصة بها فإنها تشكل 05 بالمئة من إجمالي موارد المنظمة.[2]

ثانيا: أجهزة المنظمة الدولية للشرطة الجنائية (الإنتربول)

لضمان حسن سير هذه الهيئة تتشكل هذه المنظمة من مجموع من الأجهزة وهي كالأتي:

1- الجمعية العامة

هي الهيئة العليا للمنظمة وتتألف من ممثلي الدول الأعضاء وتعقد اجتماعا استثنائيا مرة واحدة في السنة، وتختص الجمعية العامة بتقرير السياسة العامة للمنظمة وإصدار القرارات بشأن المسائل التي لها سلطة التعامل معها.[3]

---

[1] بلعبور محمد نذير، دور المنظمة الدولية للشرطة الجنائية في مكافحة الجريمة المنظمة، مجلة البحوث القانونية والاقتصادية، المجلد 02، العدد 02، جامعة عمار ثليجي لأغواط الجزائر، ص 33.

[2] بوعبسة محمد، المنظمة الدولية للشرطة الجنائية ودورها في مكافحة الجرائم، مجلة القانون، العدد 09 جامعة مستغانم الجزائر، س 2018، ص 256.

[3] بوعبسة محمد، المرجع نفسه، ص 34.

2-اللجنة التنفيذية

تتألف اللجنة التنفيذية للإنتربول من رئيس وثلاث نواب وتسعة أعضاء تنتخبهم الجمعية العامة من بين ممثلي الدول الأعضاء، وينتخب الرئيس لمدة أربع سنوات ويتطلب انتخابه أغلبيته ثلثي الأصوات، بينما ينتخب الأعضاء الآخرون لمدة ثلاث سنوات وعند انتخاب أعضاء اللجنة التنفيذية يجب على الجمعية العامة أن تراعي مبدأ التمثيل الجغرافي الملائم وأن تنظر في انتخاب أعضاء من مختلف البلدان.[1]

3-الأمانة العامة

تقوم الأمانة العامة للإنتربول بتنسيق الأنشطة اليومية لمكافحة مختلف أنواع الجرائم ويتولى إدارتها الأمين العام تتألف، الأمانة العامة من ضباط الشرطة المدنيين، ويقع مقرها الرئيسي في ليون، بينما تمتلك مجمعا عالميا للابتكار في سنغافورة والعديد من المكاتب الفرعية في أنحاء مختلفة من العالم.[2]

4-المكاتب المركزية الوطنية

تنشأ المكاتب المركزية الوطنية في الدول الأعضاء وتعمل كحلقة وصل بين أجهزة الشرطة الوطنية وأمانة الانتربول.[3]

5-المستشارون

يقدم المستشارون التقارير والدراسات العلمية إلى اللجنة التنفيذية أو إلى الأمين العام بناء على دعوة من الجمعية العامة وفقا للمادة 47 من القواعد العامة لمنظمة الشرطة الجنائية.[4]

---

[1] مجاهدي خديجة، استراتيجية المنظمة الدولية للشرطة الجنائية في مكافحة الجريمة المنظمة، مجلة الدراسات القانونية، المجلد 2 العدد 2، جامعة مولود معمري، تيزي وزو، الجزائر ،2016، ص 4.

[2] موقع الإنتربول، https://www.interpol.int/ar/3/3 بتاريخ 2024/05/02 على الساعة 15.00 مساءا.

[3] بالعبور محمد نذير، المرجع السابق، ص 35.

[4] بو عبسة محمد، المرجع السابق، ص 257.

ثالثا: أهداف المنظمة الدولية للشرطة الجنائية (الإنتربول)

تهدف آلية الأفريبول من خلال مواجهتها للجريمة المعلوماتية إلى تحقيق مجموعة من الأهداف وهي:

- الحد من الضرر والأثر العالمي للجريمة السيبرانية.[1]
- تنص المادة 2 من النظام الأساسي للمنظمة على أن تعمل المنظمة على ضمان وتطوير أوسع وضرورة تعزيز التعاون بين جميع سلطات الشرطة الجنائية في إطار النظم القائمة في كل بلد والتزامها بالبيان العالمي للحقوق الإنسان وأن المنظمة تهدف إلى إنشاء وتطوير جميع المؤسسات التي يمكن أن تسهم بفعالية في منع جرائم القانون العام ، بينما تنص المادة 3 من النظام الأساسي أن المنظمة تحظر أي أنشطة تتعلق بالقضايا ذات الطابع السياسي أو الديني أو العنصري.[2]

البند الثاني: شرطة الويب الدولية

تأسست هذه المنظمة الأمنية في الولايات المتحدة عام 1986، حيث تعمل على استقبال الشكاوي من مستخدمي الشبكة وتعقب المجرمين والهاكرز وجمع الأدلة ضدهم وتقديمهم إلى العدالة.[3]

حيث تهدف الشرطة الويب الدولية لحماية تكنولوجيا المعلومات والفضاء الإلكتروني من كافة أشكال التهديدات والمخاطر والجرائم الإلكترونية وحماية مستخدمي الأنترنت سواء كانوا

[1] موقع الإنتربول، https://www.interpol.int/ar/3/3 بتاريخ 2024/05/02 على الساعة 16.09.

[2] أسامة غريبي، المنظمة الدولية للشرطة الجنائية الإنتربول ودورها في مكافحة الجريمة المنظمة، مجلة دولية علمية محكمة، المجلد 3 العدد 3، جامعة يحي فارس، المدية، الجزائر، 2011، ص 161.

[3] فريد ناشف، آليات التعاون الدولي في مكافحة الجرائم الإلكترونية، مجلة البحوث في الحقوق والعلوم السياسية، المجلد 8، العدد 1 جامعة البليدة، الجزائر،2022، ص 439.

أفرادا أو منظمات مجتمعية مختلفة مع الحفاظ على حقوقهم ودون المساس بحرياتهم الشخصية وحقوقهم الدستورية.[1]

كما تهدف الهيئة لضبط ومكافحة الجريمة المعلوماتية بجميع أشكالها وأنواعها والقبض على مرتكبيها وتستقبل جميع البلاغات المتعلقة بالجرائم المعلوماتية، أيضا تقديم الدعم الفني والأدلة المادية لبعض أجهزة الشرطة لضبط جرائم الأنترنت كذلك تقوم بتزويد الجهات المختصة بوزارة الداخلية الأجهزة المعينة وإعداد التحقيقات الفنية والقانونية.[2]

ويضم فريق العمل بهذه المنظمة خبراء من أجهزة إنفاذ القانون والوكالات الحكومية وضباط الشرطة والمتطوعين الفنيين من 61 دولة ويسهل اتساع نطاق أنشطة المنظمة وأعمالها بالتعاون مع وكالات إنفاذ القانون في الدول الأعضاء، فإن ذلك يسهل الأمر لفريق العمل بتعقب الأعمال الإجرامية المرتكبة عبر الإنترنت في جميع أنحاء العالم في إطار المسائل القانونية والتنظيمية التي تحكم تداول المعلومات عبر الإنترنت، فهناك من يرى أنه من الضروري وضع ضوابط وقواعد لا تؤدي إلى المساس بالحريات العامة في تبادل المعلومات وحقوق الإنسان وأنه ينبغي عدم استخدام الأنترنت لأغراض إجرامية أو لنشر المواد الإباحية الضارة بالمجتمع.[3]

تشير التقديرات شركة Statista إلى أن التكلفة العالمية للجرائم السيبرانية سترتفع بشكل هائل من 8.44 تريليون دولار في عام 2022 إلى 23,82 دولار بحلول عام 2027، كما سنلاحظ من خلال الجدول الآتي تنبؤات حول ازدياد جرائم السيبرانية وذلك من عام 2025 إلى عام 2027.

---

[1] طاهر ياكر، الجرائم الإلكترونية، المرجع السابق، ص 169.

[2] طاهر ياكر، الجرائم الإلكترونية، المرجع نفسه، ص 170.

[3] فريد ناشف، المرجع السابق، ص 439.

جدول (1) ازدياد وتنبؤات معدلات الجرائم السيبرانية في العالم

السنة	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027
عدد الجرائم السيبرانية (تريليون دولار)	0.86	1.16	2.95	5.99	8.44	11.50	14.57	17.65	20.74	23.82

أشارت شركة Statista أن في عام 2023 كان حافلا بالجرائم السيبرانية، حيث وقع فيها حوادث أمن رقمي من شركات عالمية معروفة، وبعض مؤسسات رسمية دولية، ومن بين الأمثلة التي وقعت في عام 2023 وهي:

- سجلات الأطفال Kid Security :تطبيق يسمح للآباء بمراقبة أطفالهم عبر الإنترنت، حيث تم الكشف عن اختراق أكثر من 300 مليون سجل البيانات، بما في ذلك21000 رقم هاتف و31000 عنوان بريد إلكتروني، وتم الكشف أيضا عن بعض البيانات بطاقة الدفع.
- شركة طيران أوروبا: في أكتوبر 2023، طلبت شركة الطيران Air Europe من عملائها إلغاء جميع بطاقات الائتمان بعد وصول المتسللين إلى المعلومات أثناء اختراق.
- مايكروسوفتت: في يونيو 2023، أعلنت شركة مايكروسوفت الاختراق هائل، حيث تمكنت مجموعة من قراصنة مدعومة من الصين سرقة مفتاح تشفير بالغ الحساسية، وذلك سمح للمهاجمين بالوصول إلى أنظمة البريد الإلكتروني المستندة إلى السحابة Outlook ل 25 مؤسسة، بما في ذلك العديد من الوكالات الحكومية الأمريكية.
- مديرية الهجرة الإندونيسية: تم تسريب جوازات السفر لأكثر من 34 مليون إندونيسي بعد دخول المتسللين بشكل غير قانوني إلى مديرية الهجرة التابعة لوزارة القانون وحقوق الإنسان ونسب الهجوم إلى ناشط قرصنة يعرف باسم بيوركا، الذي سرق كميات هائلة من البيانات الشخصية

وأدرجها على الويب المظلم مقابل 10000 دولار، كما تضمنت البيانات الاسم الكامل والجنس ورقم جواز وتاريخ ميلاد للمقيمين الإندونيسيين.[1]

المطلب الثاني: الجهود الإقليمية لمواجهة الجريمة المعلوماتية

تلعب الجهود الإقليمية دورا هاما في تعزيز التعاون الدولي لمكافحة الجريمة الإلكترونية، وذلك من خلال الاتفاقيات والمعاهدات الإقليمية، وعليه سنحاول التطرق في (الفرع الأول) إلى المجهودات المبذولة على الصعيد الأوربي، أما (الفرع الثاني) على الصعيد العربي، أما (الفرع الثالث) فخصصناه على المستوى الإفريقي.

الفرع الأول: على المستوى الأوربي

مع تزايد التحديات التي تواجه الأمن السيبراني في أوربا أصبح التعاون الدولي أمرا ضروريا لمكافحة الجريمة السيبرانية بشكل بفعال، لتأتي اتفاقية بودابست التي وقعتها الدول الأعضاء في مجلس أوربا كخطوة هامة في هذا السياق، حيث تهدف هذه الاتفاقية إلى توحيد التشريعات وتحسين التعاون بين الدول الأعضاء في مجال مكافحة الجريمة المعلوماتية، بالإضافة إلى ذلك تم تطوير برتوكولات لاحقة تعزز اتفاقية توسيع نطاق التعاون الدولي مما يعزز الجهود المشتركة لتحسين الأمن السيبراني وحماية البيانات في أوربا.

البند الأول: وحدة التعاون القضائي الأوربية (أور جيست) Euro just

هي منظمة اتحادية أنشئت بقرار من مجلس الاتحاد الأوربي في عام 2002، الهدف منها هو تعزيز مكافحة جميع أشكال الجرائم الخطيرة، وتشجيع التعاون القضائي في مجال مكافحة الجريمة وتيسير تنسيق التحقيقات والملاحقات القضائية في الدول الأعضاء ولاسيما في الجرائم الخطيرة، وقد أنشأت فكرة إنشاء وحدة التعاون القضائي لأول مرة في قمة مجلس أوربا في تامبيري بفنلندا في عام 1999، وذلك لخلق بيئة من الحرية والأمن والعدالة في الاتحاد

[1] satatista technology market outlook national cyber security organizations FBI.IMf

الأوربي ولتعزيز مكافحة الجريمة العابرة للحدود من خلال التشجيع على التعاون بين السلطات على أساس التضامن، وقد ساهمت الهجمات الإرهابية التي وقعت في الولايات المتحدة الأمريكية في 11 سبتمبر 2001 في تسريع إنشاء يورو جست كوحدة للتنسيق القضائي، مع تركيز على مكافحة الإرهاب.[1]

كما تساهم أيضا المنظمة في التحقيق في قضايا الجريمة المعلوماتية، حيث أنها تستند إلى التحليل الذي أجرته يوروبول، تتألف هذه الهيئة من مدعين عامين وقضاة وضباط شرطة من الدول الأعضاء في الاتحاد الأوربي، حيث يتم تعيينهم وفقا لنظامهم القانوني الوطني ويتمتعون بصلاحيات متكافئة وتتعلق أنشطة يورو جست، وبتبادل البيانات وتخزينها.[2]

البند الثاني: اتفاقية بودابست لمكافحة الجرائم المعلوماتية لسنة 2001 وبرتوكولاتها

تم توقيع على اتفاقية مجلس أوربا بشأن الجرائم الإلكترونية، والمعروفة أيضا باسم اتفاقية بودابست في عام 2001 وهي أول اتفاقية دولية توحد القوانين الوطنية المتعلقة بالسلوك الإجرامي في الفضاء الإلكتروني، وتلزم الدول الموقعة عليها باعتماد قوانين جنائية لأنواع معينة من الجرائم المعلوماتية، وقد تجاوزت حدودها الإقليمية لتتيح لدول غير الأوربية للانضمام إليها مثل الولايات المتحدة الأمريكية، وبفضل دورها المحوري في تعزيز الأمن السيبراني تعد اتفاقية بودابست من أهم الاتفاقيات الدولية فيهذا المجال،[3] وقد تم توقيع عليها من قبل 30 دولة بتاريخ 23 نوفمبر 2001 في العاصمة المجرية بودابست، كذلك وقعت على هذه الاتفاقية العديد من الدول غير الأعضاء في مجلس أوربا بما في ذلك كندا واليابان وجنوب إفريقيا وصادقت عليها الولايات المتحدة الأمريكية، وعلى الرغم من أنها نشأت أصلا في أوربا إلا أنها تتسم بطابع

[1] محمد كمال محمود الدسوقي، المرجع السابق، ص 138.

[2] مناصرة يوسف، المرجع السابق، 282.

[3] سهيلة هادي، المرجع السابق، ص 237.

دولي، حيث يمكن للبلدان خارج المجموعة الأوربية أن تصبح أعضاء فيها أيضا، وفقا للمادة 28 من المعاهدة.[1]

تعتبر المعاهدة الوحيدة المتعددة الأطراف المتعلقة بمكافحة الجرائم الحاسوبية والجرائم المرتكبة على الإنترنت والجرائم المرتكبة ضد الأشخاص، وقد أصبحت دعامة أساسية منذ دخولها حيز النفاذ في 1 جويلية 2004.[2]

تنقسم الاتفاقية إلى ثلاث أقسام يتناول القسم الأول مجموعة الجرائم التي يمكن أن تتعرض لها الإنترنت والحواسيب، أما القسم الثاني مجموعة من الإجراءات الجنائية التي يمكن توحيدها في مواجهة هذه الجرائم، بينما القسم الثالث يتضمن التعاون الدولي بين الدول الأعضاء الموقعة على الاتفاقية،[3] ومن بين أهدافها نجد:

- تنسيق عناصر القانون الجنائي الوطني مع الأحكام المتعلقة بالجريمة السيبرانية.
- توفير الإجراءات القانونية اللازمة للتحقيق والملاحقة القضائية للجرائم المرتكبة عبر الإنترنت.
- حماية البيانات المخزنة على أجهزة الكمبيوتر.[4]
- تعيين نظام سريع وفعال للتعاون الدولي.

[1] فريد ناشف، المرجع السابق، ص 433.

[2] قطاف سليمان وبوقرين عبد الحليم، مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية، مجلة البحوث الثانوية والاقتصادية، المجلد05 ، العدد02، جامعة عمار ثليجي، الأغواط، الجزائر، 2022، ص 79.

[3] خليل يوسف جندي، المواجهة التشريعية للجريمة المعلوماتية على المستويين الدولي والوطني، دراسة مقارنة، مجلة كلية القانون للعلوم القانونية والسياسية، المجلد 07، العدد 26، جامعة دهوك، 2018، العراق، ص 100.

[4] شويرب جيلالي ومراد فايزة، الأليات الدولية القانونية والوطنية لمكافحة الجريمة السيبرانية، مجلة الدراسات القانونية والسياسية، المجلد 08، العدد 02، جامعة عمار ثليجي، الأغواط، الجزائر 2023، ص 157.

أولا: بروتوكول الإضافي المتعلق بكراهية الأجانب والعنصرية عن طريق نظم الكمبيوتر عام 2003

وضحت المادة 03 من هذا برتوكول نشر المواد المتصلة بالعنصرية وكراهية الأجانب عبر أنظمة الكمبيوتر.

وتعرف المادة02 من البرتوكول الإضافي المواد العنصرية والمعادية للأجانب "بأنها أي مادة تهدف إلى الترويج للكراهية والعنف ضد الأفراد أو الجماعات على أساس العرق أو الدين أو الجنسية"، وتتمثل هذه المواد في الخطاب العنصري والتهديدات بالعنف والتمييز والتحريض على الكراهية ونشر معلومات مضللة أو كاذبة بهدف إثارة الكراهية أو التمييز.

كما تلزم المادة03 من البرتوكول الإضافي لاتفاقية بودابست بتجريم أي سلوك يتضمن توزيع أو إتاحة مواد عنصرية ومعادية للأجانب عبر أنظمة الكمبيوتر، ويقصد بالتوزيع أي تحميل المواد على الإنترنت وإرسالها عبر البريد الإلكتروني ونشرها على مواقع التواصل الاجتماعي أو مشاركتها عبر أي وسيلة أخرى عن طريق الإنترنت.

ويقصد بإتاحة إلى وضع المواد العنصرية والمعادية للأجانب في متناول الأخرين لاستخدامها ومن بين الاستثناءات المادة 03 أنها لا تجرم الاتصالات الخاصة أو التعبيرات التي يتم تبادلها عبر أنظمة الكمبيوتر ذلك لأن هذه الاتصالات محمية بموجب المادة 08 من الاتفاقية الأوربية لحقوق الإنسان التي تضمن الحق في حرية التعبير.[1]

ثانيا: البرتوكول الإضافي الثاني للاتفاقية المتعلقة بالجريمة الإلكترونية بشأن تعزيز التعاون والكشف عن الأدلة الإلكترونية عام 2012

تهدف المادة 06 من البرتوكول الإضافي الثاني لاتفاقية بودابست إلى تسهيل تبادل المعلومات بين الدول الأطراف حول تسجيل أسماء النطاقات في سياق التحقيقات أو الإجراءات

[1] -https://rm.coe.int/explanatory-report-additional-protocol بتاريخ 2024/05/03 على الساعة 18.40 مساءا.

الجنائية، أما المادة 08 تهدف إلى تسهيل إنفاذ أوامر الكشف عن المعلومات المشتركين وبيانات حركة الاتصالات الصادرة عن دولة طرف أخرى في سياق التحقيقات والإجراءات الجنائية، حيث تلزم كل دولة طرف باتخاذ التدابير اللازمة لتمكين سلطاتها المختصة من إصدار أمر يتم تقديمه كجزء من طلب موجه إلى دول طرف اخرى يهدف هذا الأمر إلى إجبار مقدمي خدمات الإنترنت الموجودين في أراضي الدولة المتلقية على تقديم مايلي:

- معلومات المشتركين.
- بيانات حركة الاتصالات المحددة والمخزنة والموجودة في حيازة مقدم الخدمة أو تحت حكمه.

تهدف المادة 09 إلى تسهيل تبادل بيانات الكمبيوتر المخزنة بسرعة في حالات الطوارئ مثل وقوع الهجمات السيبرانية، كما تختص المادة 14 من قواعد حماية البيانات الشخصية للمعلومات. [1]

البند الثالث: الاتحاد الأوربي

في 7 يناير 2006 ناقش الاتحاد الأوربي مسألة الجريمة السيبرانية في بيان المفوضية الأوربية (الهيئة التشريعية للاتحاد الأوربي) الموجه إلى المجلس والبرلمان الأوربي ولجنة الشؤون الاقتصادية، بعنوان إنشاء مجتمع معلوماتي أمن من خلال تعزيز البنية التحتية للمعلومات ومكافحة الجرائم المتصلة بالحاسوب، كما تناولت التهديدات السيبرانية والجوانب الإجرائية مثل اعتراض الاتصالات والاحتفاظ ببيانات حركة المرور والوصول إلى المعلومات واستخدامها خلسة، والتعاون العملي على المستوى الدولي، وكذلك المسائل المتعلقة بالاختصاص القضائي، كما قدمت مقترحات بشأن التدابير القانونية في هذا الصدد ومن أبرز

[1] https://rm.coe.int/ara بتاريخ 2024/05/03 على الساعة 19.50 مساءا.

إنجازات الاتحاد الأوربي في مجال السيبرانية إنشاء وكالة الشرطة الأوربية (يوروبول) وخدمة التعاون القضائي (يورجيست).[1]

البند الرابع: المنظمة الأوربية للشرطة الجنائية (يوروبول)

المنظمة الأوربية للشرطة الجنائية (يوروبول) هي وكالة التعاون الشرطي المسؤولة عن التعامل مع المعلومات المتعلقة بالنشاط الإجرامي في أوربا، وهدفها هو تحسين كفاءة السلطات المختصة في الدول الأعضاء وتعزيز التعاون في مجال منع ومكافحة الأشكال الخطيرة للجريمة المنظمة عبر الحدود الوطنية، ومن اختصاصات اليوروبول مكافحة مختلف أشكال الجريمة الحاسوبية التي تسيرها الإنترنت، وفي عام 2013 أنشأت المنظمة الأوربية للشرطة الجنائية (يوروبول) المركز الأوربي لمكافحة الجريمة السيبرانية (EC3)، بهدف تعزيز استجابة أجهزة إنفاذ القانون للجريمة الإلكترونية في الاتحاد الأوربي وحماية المواطنين الأوروبيين والشركات والحكومات الأوربية من الجرائم الإلكترونية، ومنذ إنشائه ساهم المركز الأوربي للجريمة السيبرانية (EC3) في مكافحة الجريمة المعلوماتية وشارك في عشرات العمليات البارزة ومئات عمليات الدعم الميداني التي أسفرت على مئات الاعتقالات وتحليل مئات الآلاف من الملفات وينشر المركز الأوربي (EC3) تقييما سنويا للتهديدات الجريمة المنظمة على الإنترنت وتقارير استراتيجية رئيسية عن النتائج والتهديدات الناشئة في مجال جرائم الإنترنت.[2]

الفرع الثاني: على المستوى العربي

شاركت الهيئات العربية مثل جامعة الدول العربية في جهود مكافحة الجرية المعلوماتية بالإضافة إلى الجهود التي بذلتها الدول العربية من خلال إصدار قوانين وتشريعات تهدف إلى تحديد الأنشطة الغير قانونية على الإنترنت وتحديد العقوبات المناسبة، وتأتي مبادرة القانون

[1] خالد حازم إبراهيم، دور الأجهزة الأمنية في الإثبات الجنائي في الجرائم المتعلقة بشبكة المعلومات الدولية الإنترنت، دراسة مقارنة دار النهضة العربية، للنشر والتوزيع، ط1، مصر ،2000 ص 374 375.

[2] مناصرة يوسف، جرائم المساس بأنظمة المعالجة الآلية المعطيات، دراسة مقارنة، دار الخلدونية، ط 2018، الجزائر، ص 280.

النموذجي الاسترشادي كأداة دولية توفر إطارا موحدا، ويسعى مجلس وزراء العرب للاتصالات وتكنولوجيا المعلومات إلى تنسيق الجهود مكافحة الجريمة المعلوماتية في العالم العربي وتطوير السياسات والاستراتيجيات العربية الموحدة في هذا المجال بهدف تعزيز التعاون والتنسيق بين الدول العربية وتحسين القدرات الوطنية والإقليمية للتصدي لهذا التحدي المتزايد.

البند الأول: اتفاقية الجامعة العربية لمكافحة الجريمة المعلوماتية

تأسست جامعة الدول العربية في عام 1944 أي قبل إنشاء الأمم المتحدة بثمانية أشهر، حيث تعتبر جامعة الدول العربية أول منظمة دولية إفريقية أسيوية في العالم ومنذ 22 مارس 1945 انضمت العديد من الدول الإفريقية والآسيوية إلى جامعة الدول العربية.[1]

كما تصدر جامعة الدول العربية توجيهات بشأن مكافحة الجريمة السيبرانية، حيث وقعت الدول العربية على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في عام 21 ديسمبر 2010 لتقنين وتجريم الاستخدام غير المشروع للفضاء الإلكتروني، وكذلك لتعزيز التعاون بين الدول العربية لمكافحة الجرائم الإلكترونية وحماية امنها وسلامتها الاجتماعية.[2]

أولا: مجلس وزراء العدل العرب

بناء على قرار رقم (299) لسنة 1996 وبدراسة الفصل التاسع الخاص بانتهاكات الحقوق الشخصية ضد الأفراد، نجد أن القانون قد خصص فصلا لانتهاكات الحقوق الفردية، وذلك في المواد من 461 إلى 464 حيث تناولت المواد من 461 إلى 463 ضرورة حماية الحياة الخاصة والأسرار الشخصية من مخاطر المعالجة الآلية وكيفية جمع المعلومات الاسمية وكيف يمكن الاطلاع على هذه المعلومات، وتنص المادة 464 على فرض عقوبات على الأشخاص الذين يقومون عن طريق الاحتيال بالوصول إلى كل أو جزء من نظام معالجة المعلومات الآلي

[1] محمود محمد صفاء الدين علي شرشر، المرجع السابق، ص 551.

[2] قطفان سليمان، بوقرين عبد الحليم، المرجع السابق، ص 81.

أو منع أو تعطيل نظام التشغيل من أداء وظائفه العادية أو تغيير المعلومات داخل النظام، كذلك تزوير المستندات المعالجة الالية وسرقة المعلومات.[1]

ثانيا: القانون الإمارات العربي الإسترشادي لمواجهة الجرائم تقنية المعلومات

يعد القانون الإمارات العربي الاسترشادي لمكافحة الجرائم تقنية المعلومات الذي تم اعتماده كذلك من قبل مجلس الوزراء العدل العرب في دورته 19 بالقرار رقم 495 / 19 بتاريخ 08 / 10 / 2003، واعتمده مجلس وزراء الداخلية العرب في دورته 21 بالقرار رقم 417 /21 في عام 2004، والذي يشمل 27 مادة تختص في العقوبات للجرائم الإنترنت.[2]

ثالثا: القانون العربي الإسترشادي بشأن حماية حقوق الملكية الفكرية

يعد قرار مجلس وزراء العدل العرب رقم 635 الصادر في نوفمبر 2006 خطوة هامة نحو تعزيز حماية الملكية الفكرية في الوطن العربي ، فقد نص القرار على إنشاء لجنة مهمتها وضع مبادئ توجيهية للقانون العربي للملكية الفكرية، حيث قامت إدارة الملكية الفكرية والتنافسية برئاسة هذه اللجنة، والتي ضمت خبراء من مختلف الدول العربية وعقدت اللجنة عشر اجتماعات خلال الفترة من عام 2007 إلى 2016، حيث ناقشت مختلف القضايا المتعلقة بحقوق الملكية الفكرية.[3]

رابعا: اتفاقية العربية لمكافحة جرائم تقنية المعلومات

تم توقيع عليها في القاهرة في 21 ديسمبر 2010 كما وافقت عليها مصر للانضمام إلى الاتفاقية بموجب قرار رئيس الجمهورية رقم 276 وتم إصداره في 19 أوت 2014 كما تم نشر الاتفاقية في الجريدة الرسمية رقم 46 بتاريخ 13 نوفمبر 2014، حيث تهدف هذه الاتفاقية إلى تعزيز التعاون بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، وعليه فإن الاتفاقية

[1] فاروق خلف، المرجع السابق، ص 15،

[2] فاروق خلف، المرجع نفسه، ص 15.

[3] https://www.unescwa.org بتاريخ 2024/05/04 على الساعة 00.00 مساءا.

تغطي نطاقا واسعا من جرائم التقنية بما في ذلك الاعتداء على سلامة البيانات وجرائم إساءة استخدام وسائل تقنية المعلومات والتزوير والاحتيال والجرائم المتعلقة بالإرهاب.[1]

خامسا: القانون العربي الإسترشادي للإثبات بالتقنيات الحديثة

وقد اعتمد بموجب القرار رقم 771 / 24 الصادر عن مجلس وزراء العدل العرب (27 / 11 / 2008) ويتألف من سبعة فصول و24 مادة، ويتضمن الفصل الخامس والمواد من23 إلى 32 وما يليها يعالج الجرائم والعقوبات الخاصة بالجرائم الإلكترونية.[2]

البند الثاني: المكتب العربي للشرطة الجنائية

في عام 1960 أنشأ مجلس وزراء الداخلية العرب مركز الشرطة العربية بموجب اتفاقية إنشاء الجمعية العربية لحماية الرعاية الجنائية، ويعتبر مركز الشرطة الجنائية بدمشق مكتباً متخصصاً للجمعية وينظم أعمالها والأنشطة على مستوى الوزارات الثلاث (وزارة الداخلية وزارة العدل والشؤون الاجتماعية) في الدول العربية، وهذا المكتب مسؤول بشكل خاص عن الحفاظ ودعم التعاون بين قوات الشرطة في الدول الأعضاء لمكافحة الجريمة ومحاكمة المجرمين داخل أراضيها وإنفاذ القوانين واللوائح الحالية لكل دولة وتقديم المساعدة التي تطلبها كل دولة ضمن نطاقها تمويل وتحسين خدمات الشرطة.[3]

الفرع الثالث: على المستوى الإفريقي

هذا الفرع يتضمن أهم جهود الاتحاد الإفريقي مع استبيان أجهزة الشرطة أفريبول ومهامها

البند الأول: الاتحاد الإفريقي

في القمة الثالثة والعشرين لاتحاد الإفريقي صادق رؤساء الدول والحكومات الإفريقية على اتفاقية الاتحاد الإفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية، ووفقا لديباجة

[1] حاتم أحمد محمد بطيخ، تطور السياسة التشريعية في مجال مكافحة جرائم التقنية المعلومات، مجلة الدراسات القانونية والاقتصادية المجلد 07، العدد 02، القاهرة 2021، ص 26.

[2] خلف فاروق، المرجع السابق، ص 15.

[3] محمد كمال محمود الدسوقي، المرجع السابق، ص 140،

الاتفاقية التي توضح خلفية إنشائها فإن السبب الرئيس لوجودها هو الوفاء بالالتزامات التي قطعتها للدول الأعضاء في الاتحاد الإفريقي حاليا على المستوى الأقاليم الفرعية ولبناء مجتمع المعلومات وذلك أساسا من خلال تعزيز التشريعات القائمة بشأن تكنولوجيا المعلومات والاتصالات في الدول الأعضاء والجماعات الاقتصادية الإقليمية وتنظيم قطاع تكنولوجي مزدهر، وتحديد القواعد الأمنية اللازمة لإنشاء فضاء رقمي موثوق به للمعاملات الإلكترونية وحماية البيانات الشخصية ومكافحة الجرائم الإلكترونية.[1]

البند الثاني: الشرطة الجنائية الإفريقية (الأفريبول)

تعرف الأفريبول بأنها هيئة فنية تابعة للاتحاد الإفريقي تهدف إلى تعزيز التعاون الشرطي بين الدول الإفريقية، وتمثل مهمتها في تبادل المعلومات والخبرات وتشجيع على التعاون بين أجهزة الشركة الإفريقية ولم يحدد النظام الأساسي للأفريبول تعريفا لهذه الآلية ويشير فقط إلى المادة الاولى على أن أفريبول هي "آلية الاتحاد الإفريقي للتعاون الشرطي كما يحدد الجزائر العاصمة كمقر لآلية أفريبول، ويسمح بعقد اجتماعات أفريبول في دول أخرى بناء على طلب من تلك الدول.[2]

أولا: أجهزة آلية الاتحاد الإفريقي للتعاون الشرطي

1- الجمعية العامة:

هي الهيئة العليا لأفريبول وهي مسؤولة عن تقديم التوجيه بشأن التعاون الشرطي في إفريقيا وتتألف الجمعية العامة من رؤساء الشرطة، وتعتبر الجمعية العامة هي الهيئة العليا لأفريبول، وهي المسؤولة عن تقديم التوجيه بشأن التعاون الشرطي في إفريقيا، وتتألف الجمعية العامة من رؤساء الشرطة، كما يتشكل مكتب الجمعية العامة من 05 أعضاء رئيس و03 نواب ومقرر ويتم انتخاب أعضاء المكتب بالتناوب لولاية مدتها سنتين غير

[1] مناصرة يوسف، المرجع السابق، ص 276.

[2] عبد العزيز لزعر، آلية الاتحاد الإفريقي للتعاون الشرطي الأفريبول ودورها في مكافحة الجريمة الإلكترونية، مجلة متون، المجلد 13 العدد 03، جامعة مولاي الطاهر، سعيدة الجزائر ،2021، ص 254.

قابلة للتجديد ويمثلون الأقاليم الخمسة للاتحاد الإفريقي طبقا للمادة 08 فقرة 03 من النظام الأساسي لآلية الاتحاد الإفريقي للتعاون الشرطي الأفريبول.[1]

2-لجنة التوجيه

تتألف لجنة التوجيه من 5 أعضاء من مكتب الجمعية العامة ومفوض الاتحاد الإفريقي للسلم والأمن ورؤساء وكالات التعاون الشرطي الإقليمية والأمين العام لأفريبول ويرأس اللجنة التوجيهية رئيس الجمعية العامة.

3- الأمانة

يتم تحديد تشكيل أمانة أفريبول وفقا للقواعد والإجراءات المعمول بها في الاتحاد الإفريقي وتتألف أمانة الأفريبول من الرئيس التنفيذي والأمين العام وعدد كاف من الموظفين المؤهلين وذوي الخبرة، ويتم تعيين مدير الأمانة بواسطة جمعية العامة للأفريبول بناء على توصية لجنة التوجيه التابعة لها، أما باقي أعضاء يتم تعينهم وفقا لقواعد موظفي الاتحاد الإفريقي.[2]

4-مكاتب الاتصال الوطنية في أفريبول

يتعين على كل دولة عضو في الية أفريبول، أن تنشئ مكتب اتصال وطني وفقا لتشريعاتها الوطنية من أجل تسيير أنشطة هذه الآلية، كما تم إنشاء أكثر من 30 مكتب اتصال وطني وتشير المادة 06 من النظام الأساسي للأفريبول إلى أنه تكلف اللجنة الفنية المتخصصة للدفاع والسلامة والأمن بمسؤولية التوجيه والتوجيه السياسي بشأن مسائل الشرطة في إفريقيا، بالإضافة إلى ذلك تم تكليف هذه اللجنة بعدد من صلاحيات، بما في ذلك التوسط بين الجمعية العامة

[1] أحلام بو كربوعة، آلية الاتحاد الإفريقي للتعاون الشرطي أفريبول، ودورها في مكافحة ظاهرة الإرهاب، المجلد 34، العدد 4 حوليات جامعة العربي بن المهيدي أم البواقي، الجزائر، 2022، ص 609.

[2] عبد العزيز لزعر، المرجع السابق، ص 256.

وهيئة صنع السياسة التابعة للاتحاد الإفريقي على النحو المطلوب في النظام الأساسي لأفريبول والمساعدة في اعتماد البرنامج السنوي للاتحاد الإفريقي.[1]

ثانيا: مهام الشرطة الجنائية الإفريقية الأفريبول

نصت المادة 03 و04 من النظام الأساسي لآلية الاتحاد الإفريقي أفريبول على عدة مهام وهي:

- مساعدة مؤسسات الشرطة في الدول الأعضاء على وضع إطار للتعاون على المستويات الإقليمية والوطنية والقارية والدولية.
- العمل على تطوير قدرات أجهزة الشرطية في الدول الأعضاء وذلك من خلال برامج تدريبية متقدمة للشرطة وإنشاء مراكز امتياز إفريقية.
- تعزيز التنسيق مع هيئات مماثلة في منع ومكافحة الجريمة.
- تشجيع المساعدة التقنية المتبادلة بين المنظمات الشرطية ذات الخبرة والممارسات الجيدة لتحسين كفاءتها وفعاليتها.
- تسهيل تبادل المعلومات والاستخبارات وتقاسمها لمنع الجريمة وكشفها وتسهيل التحقيق فيها.
- تطوير الأدوات القارية لمنع الجريمة.

تحضير استراتيجية إفريقية منسقة ،لمكافحة مختلف أنواع الجرائم الخطيرة بما في ذلك الجرائم السيبرانية.[2]

[1] خديجة خالدي، آلية الاتحاد الإفريقي للتعاون الشرطي أفريبول، مجلة العلوم الاجتماعية والإنسانية، المجل د11، العدد 15، جامعة العربي تبسي تبسة، س 2018، ص 76.

[2] شنتير خضرة، المرجع السابق، ص 20.

الخاتمة

نستخلص من خلال ما سبق دراسته أن الموضوع الجريمة المعلوماتية يعد من أهم المواضيع الحيوية في عصرنا الحالي نظرا لخطورتها وتأثيراتها السلبية على المجتمع، ولذلك تتطلب هذه الظاهرة دراسة مستفيضة و معمقة من قبل جميع الجهات المعنية من باحثين وحكومات وشركات ومؤسسات دولية، وذلك بفهم ماهيتها وخصائصها و تطوراتها لوضع خطط فعالة لمكافحتها، كما رأينا كيف استجابت العديد من الدول لهذا الخطر التقني وحرصت على تطوير أنظمتها التشريعية باستحداث أدوات تشريعية تستجيب لظاهرة الجرائم التكنولوجية الحديثة، وتشمل الجهود المبذولة لمكافحة الجريمة السيبرانية إصدار قوانين وطنية خاصة أما على الصعيد الدولي تعمل الدول مع المنظمات الدولية مثل الإنتربول وتلتزم الدول بالاتفاقيات الدولية على سبيل مثال اتفاقية بودابست، وعلى المستوى الإقليمي يتم من خلال مبادرات المنظمات مثل الاتحاد الإفريقي وجامعة الدول العربية مما يسهم في تنسيق الجهود الرامية إلى مكافحة هذه الجريمة وتعزيز الاستجابات العالمية.

من خلال هذا البحث توصلنا إلى جملة من النتائج من أبرزها مايلي:

- عدم وجود تعريف موحد للجريمة المعلوماتية.
- تنوع أشكال الجريمة المعلوماتية وخطورتها.
- جرائم الإنترنت ذات بعد دولي ولا تحدها حدود وطنية أو قومية مما يتطلب تعاونا دوليا للحد منها.
- لا تترك الجريمة المعلوماتية اثارا مادية على عكس الجريمة التقليدية التي تترك اثارا مادية في مسرح الجريمة.
- تشكل الجرائم المعلوماتية تهديدا خطيرا على الاستقرار الدولي.
- المجرم المعلوماتي هو رجل يتميز بتفوقه على المجرم التقليدي حيث يمتلك معرفة وكفاءة عالية ويتميز بذكائه وقدرته على الهروب من العقاب.
- لا يمكن لأي دولة بمفردها أن تكافح الجرائم الإلكترونية لابد من الدخول في اتفاقيات الدولية الخاصة بمكافحة الجرائم المعلوماتية.

- يعد التعاون الأمني الدولي بين أجهزة الشرطة الجنائية المتخصصة في مكافحة الجرائم المعلوماتية في الدول أحد أهم الوسائل لمنع الجرائم المعلوماتية.
- تطور تقنيات الجرائم الإلكترونية باستمرار.

إن تحديد الطبيعة القانونية للمعلومات موضوع معقد يثير نقاشا بين القانونين والخبراء حيث كان الاتجاه السائد ينفي عن المعلومات كونها من القيم المالية، ويرى لها طبيعة من نوع خاص فالمعلومات كانت تعتبر غير مادية ولا يمكن تملكها بنفس الطريقة التي يمكن بها تملك الأشياء المادية ومع التطور الهائل لتكنولوجيا المعلومات والاتصالات ظهر اتجاه أكثر حداثة يرى أن للمعلومات قيمة مالية يمكن الاعتداء عليها شأنها في ذلك شأن القيم بشكل عام، كما لها قيمة اقتصادية كبيرة.

- تم إنشاء قطب جزائي خاص بالجريمة المعلوماتية بموجب الأمر رقم 21- 11 المؤرخ في 26 اغسطس 2021 المتمم لقانون الإجراءات الجزائية.
- سن مجموعة من قواعد قانونية مثل قانون 09-04يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- وضع المشرع تعديل لقانون العقوبات بموجب القانون 24-06 والذي عدل من عقوبات بعض الجرائم التي ترتكب بواسطة مواقع التواصل الاجتماعي.

بعد عرضنا لأهم النتائج المتوصل إليها نختم بحثنا بمجموعة من الاقتراحات والتي من شأنها أن تساهم في مواجهة الجريمة المعلوماتية ولعل من أبرزها مايلي:

- نشر ثقافة الأمن المعلوماتي بين الأفراد والمؤسسات.
- استخدام برامج مكافحة الفيروسات وبرامج الحماية الأخرى.
- حماية البيانات الشخصية من خلال استخدام تقنيات التشفير والتحكم في الوصول.
- سن تشريعات دولية موحدة لمكافحة الجريمة المعلوماتية.
- المشرع الجزائري لم يخصص قانون خاص للجريمة المعلوماتية.
- تطوير القوانين والتشريعات لمكافحة الجرائم الإلكترونية.

- دعم الدول النامية في مجال مكافحة الجرائم الإلكترونية من خلال تقديم المساعدة التقنية والمالية.
- يمكن استخدام الذكاء الاصطناعي لتحديد التهديدات الإلكترونية بشكل فعال وأكثر دقة.
- ضرورة التبليغ الفوري عن حوادث الجرائم الإلكترونية من أجل التحفظ على الأدلة المتحصل عليها والتي تتسم بسرعة الزوال.
- إنشاء محاكم متخصصة بالجرائم الإلكترونية أو على الأقل غرف متخصصة في كل المجالس القضائية.
- الحذر من رسائل البريد الإلكتروني المشبوهة.
- إلقاء محاضرات توعية حول مخاطر الجرائم الإلكترونية وكيفية حماية الأشخاص منها في مختلف أمكان التواصل مثل المدارس والجامعات والمراكز الثقافية.
- إنشاء برامج تعليمية إلكترونية حول الأنظمة المعلوماتية والجرائم الإلكترونية لتسهيل الوصول إليها من قبل الجميع.

القيام بحملات توعوية وطنية تنظمها السلطات والمجتمع المدني.

قائمة المصادروالمراجع

أولا: المصادر.

1) **التعديل الدستوري لسنة 2020: المرسوم رئاسي رقم 20-442 مؤرخ في 30ديسمبر 2020 يتعلق بإصدار التعديل الدستوري المصادق عليه في استفتاء أول نوفمبر سنة 2020 الجريدة الرسمية العدد 82.**
2) **القانون رقم 04-15 المؤرخ 10 نوفمبر 2004 المعدل والمتمم للأمر 66-155 المتضمن قانون العقوبات الجريدة الرسمية العدد 71.**
3) **القانون رقم 09 – 04 مؤرخ في أوت سنة 2009 , يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، رقم 47 المؤرخة في 14/ 08 / 2009.**
4) **المرسوم التشريعي رقم 17، المتضمن تطبيق أحكام قانون التواصل على الشبكة ومكافحة الجريمة المعلوماتية، المؤرخ في 2012/02/08 سوريا.**
5) **من القانون رقم 14 بإصدار قانون مكافحة الجرائم الإلكترونية، قطر 2014.**
6) **القانون رقم 63 في شأن مكافحة جرائم تقنية المعلومات، الكويت 2015.**
7) **القانون رقم 15-04 المؤرخ في 01 فبراير 2015 الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكتروني الجريدة الرسمية، العدد 06.**
8) **القانون رقم 18-04 المؤرخ في 10 مايو 2018 الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية الجريدة الرسمية العدد 27.**
9) **القانون رقم 18-07 المؤرخ في 10 يوليو 2018 المتضمن حماية الأشخاص الطبعيين في مجال المعطيات ذات الطابع الشخصي الجريدة الرسمية العدد 34.**
10) **القانون رقم 24-06 المؤرخ في 28-04-2024 المعدل والمتمم للأمر 66-156 المتضمن قانون العقوبات الجريدة الرسمية العدد 30.**
11) **من قانون رقم 5 بشأن مكافحة الجرائم الإلكترونية، المؤرخ في 27 سبتمبر 2022، ليبيا.**

12) المرسوم 54 يتعلق بمكافحة الجرائم المتصلة بأنظمة المعلومات ولاتصال، المؤرخ في 13 سبتمبر 2022، تونس.
13) الأمر رقم 03-15 المؤرخ في 19 يوليو 2003 المتضمن قانون حقوق المؤلف والحقوق المجاورة، الجريدة الرسمية، العدد 44.
14) الأمر 20-04 المؤرخ في 30-08-2020 المعدل والمتمم للأمر 66-155 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، العدد 51.
15) الأمر 21-11 المؤرخ في 25 غشت 2021 المتمم للأمر 66-155 المتضمن قانون الإجراءات الجزائية الجريدة الرسمية العدد 65.
16) المرسوم الرئاسي 04-183 المؤرخ في 26 يونيو 2004 المتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني الجريدة الرسمية العدد 41.
17) المرسوم الرئاسي رقم 20-05 المؤرخ في 20جانفي 2020 المتعلق بوضع منظومة وطنية لأمن الانظمة المعلوماتية الجريدة الرسمية العدد 04.
18) المرسوم الرئاسي 21-349 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، المؤرخ في 2021/11/01، الجريدة الرسمية، العدد 86.
19) القرار المؤرخ في 10 جانفي 2024 المتعلق بإنشاء لجنة الخدمات الاجتماعية للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي الجريدة الرسمية، العدد 29.

ثانيا: المراجع

1- الكتب العامة:

1) أحسن بوسقيعة الوجيز في القانون الجزائي الخاص ج الأول النشر الجامعي ط 2022 الجديد الجزائر، 2022.
2) بهاء المرى، جرائم المحمول والإنترنت، دار الهدي، الطبعة الأولى، الإسكندرية مصر، سنة 2018.
3) بن مكي نجاة، السياسة الجنائية لمكافحة جرائم المعلوماتية، دار الخلدونية، الطبعة 2017 الجزائر.
4) حزيط محمد، أصول الإجراءات الجزائية في القانون الجزائري، دار بلقيس، الطبعة الثالثة، الجزائر سنة 2022
5) خالد داودي، الجريمة المعلوماتية، دار الإعصار الطبعة الأولى الجزائر، 2018.
6) خالد حسن أحمد لطفي، جرائم الأنترنت بين القرصنة الإلكترونية وجرائم الابتزاز الإلكتروني دراسة مقارنة، دار الفكر الجامعي، الطبعة الأولى، مصر 2018.
7) سليم بن ساعد البادي وزايد بن حمد الجنيبي ويوسف الشيخ يوسف حمزة وأحمد العطاء، مجمع البحوث والدراسات أكاديمية السلطان قابوس الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها مجلس التعاون لدول الخليج العربية، سلطنة عمان سنة 2010.
8) شنتير خضرة الأليات القانونية لمكافحة الجريمة الإلكترونية دراسة مقارنة، مؤسسة الكتاب القانوني، الطبعة الأولى الجزائر، سنة 2022.
9) طاهر ياكر الجرائم الإلكترونية دار بلقيس الطبعة 2024 الجزائر سنة 2024.

10) عبد الصبور عبد القوي على حصري، المحكمة الرقمية والجريمة المعلوماتية، مكتبة القانون والاقتصاد، الطبعة الأولى، سنة 2012.

11) عبد الفاتح عارف التميمي، مهارات الكمبيوتر، اليازوري للنشر والتوزيع، عمان، أردن، سنة 2012.

12) عماد مفلح الحسبان وأخرون، الجرائم المستحدثة (المعلوماتية، الإلكترونية، السيبرانية)، ,دار الخليج للنشر والتوزيع، الأردن، سنة 2023.

13) غانم مرضي الشمري، الجرائم المعلوماتية ماهيتها وخصائصها وكيفية التصدي لها قانونيا دار الثقافة، الطبعة الأولى، عمان 2016.

14) فارس محمد العمارات، جرائم العصر من الرقمية إلى السيبرانية، دار الخليج للنشر والتوزيع، الطبعة الأولى، الأردن، سنة 2023.

15) محمد سعيد عبد المجيد، المعلوماتية والجريمة تحليل مضمون لبعض الجرائم الإلكترونية دار مكتبة الإسراء، الطبعة الأولى مصر سنة 2006.

16) محمد علي سكيكر، الجريمة المعلوماتية وكيفية التصدي لها، دار الجمهورية وصحافة دون طبعة، الإسكندرية 2010.

17) محمد حماد مرهج الهيتي، الجريمة المعلوماتية دراسة مقارنة، دار الكتب القانونية، مصر، الإمارات، سنة 2014.

18) محمود دين، الجريمة الإلكترونية وتحديات الأمن القومي، دار الكتب المصرية الطبعة الثانية، مصر، 2019.

19) ميرفت محمد حبابية، مكافحة جريمة الإلكترونية دراسة مقارنة في التشريع الفلسطيني والجزائري دار البازوزي العلمية، طبعة 2022، سنة 2022.

20) نائلة عادل محمد فريد قورة, جرائم الحاسب الألي الاقتصادية، الطبعة الأولى، لبنان سنة 2005.
21) نهلة عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة، الطبعة الأولى 2008 الطبعة الثانية عمان أردن.
22) نادر عبد الكريم الغزواني، الحماية الجنائية من جرائم الأنترنت، نور النشر، طبعة 2016، دون بلد، سنة 2016.
23) يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري، دار الجامعة الجديدة، قالمة الجزائر، سنة 2019

2- الكتب الخاصة:

1) حدة بوخلفة، المسؤولية الجنائية لمقدمي خدمات الأنترنت، دار هومه، دون طبعة الجزائر سنة 2019.
2) خالد حازم إبراهيم دور الأجهزة الأمنية في الإثبات الجنائي في الجرائم المتعلقة بشبكة المعلومات الدولية الإنترنت، دراسة مقارنة دار النهضة العربية، للنشر والتوزيع، الطبعة الأولى، مصر، سنة 2000.
3) رفد عيادة الهاشمي، الإرهاب الإلكتروني دار أمجد للنشر والتوزيع الطبعة الأولى سنة 2019.
4) ضرغام جابر عطوش أل مواش، جريمة التجسس المعلوماتي، المركز العربي، الطبعة الأولى، مصر، سنة 2017.
5) عادل عبد الصادق، الإرهاب الإلكتروني، القوة في العلاقات الدولية نمط جديد وتحديات مختلفة، مركز الأهرام للدراسات السياسية والاستراتيجية، الطبعة الأولى، القاهرة، 2009.
6) علي عبود جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة منشورات زين الحقوقية، الطبعة الأولى، بيروت، سنة 2013.

7) علي صبيح عبد اللامي، دور السياسة الوقائية في الحد من الجرائم المعلوماتية، دار دروب المعرفة، دون طبعة مصر، سنة 2023.
8) غانم مرضي الشمري، الجرائم المعلوماتية ماهيتها وخصائصها و كيفية التصدي لها قانونيا ،دار الثقافة الطبعة الأولى عمان سنة 2016 .
9) غادة نصار الغربي، الإرهاب والجريمة الإلكترونية، العربي للنشر والتوزيع الطبعة الأولى، القاهرة، سنة 2017.
10) فرح يحي وعاترة، التهديدات السيبرانية على الأمن القومي، العربي للنشر والتوزيع طبعة 2023 القاهرة، سنة 2023.
11) لينا محمد الأسدي، مدى فاعلية أحكام القانون الجنائي في مكافحة الحريمة المعلوماتية، دار الحامد، الطبيعة الأولى، الأردن، سنة 2014.
12) مناصرة يوسف، جرائم المساس بأنظمة المعالجة الآلية المعطيات، دراسة مقارنة، دار الخلدونية دون طبعة الجزائر، سنة 2018.

ثالثا: المقالات

1) أسامة غريبي، المنظمة الدولية للشرطة الجنائية الإنتربول ودورها في مكافحة الجريمة المنظمة، مجلة دولية علمية محكمة، المجلد 03، العدد 03، جامعة يحي فارس، المدية الجزائر، سنة 2011.
https://www.asjp.cerist.dz/en/article/4235
2) أحمد بن مسعود، جرائم المساس بأنظمة المعالجة الألية للمعطيات في التشريع الجزائري، مجلة الحقوق والعلوم الإنسانية، المجلد 10, العدد 01 ,جامعة جلفة، سنة 2017
https://www.asjp.cerist.dz/en/article/18306

3) أحلام بوكربوعة، آلية الاتحاد الإفريقي للتعاون الشرطي أفريبول، ودورها في مكافحة ظاهرة الإرهاب، المجلد 34، العدد 4، حوليات جامعة العربي بن المهيدي أم البواقي، الجزائر، سنة 2020. https://www.asjp.cerist.dz/en/article/142267
4) بوضياف أسمهان، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد 11، سنة 2018. https://www.asjp.cerist.dz/en/article/81720
5) بن مالك إسمهان، خصائص الجريمة المعلوماتية وأسباب ارتكابها، مجلة البيان للدراسات القانونية، المجلد04، العدد01، جامعة برج بوعريريج الجزائر، سنة 2019. https://www.asjp.cerist.dz/en/article/181041
6) بالعبور محمد نذير وبوغوفالة بوعيشة، دور المنظمة الدولية للشرطة الجنائية في مكافحة الجريمة المنظمة، مجلة البحوث القانونية والاقتصادية، المجلد 02، العدد 02، جامعة عمار ثليجي لأغواط، الجزائر، سنة 2020.
https://www.asjp.cerist.dz/en/article/114314
7) بن شهرة شول، السمات الخاصة للجريمة المعلوماتية، مجلة المستقبل للدراسات القانونية، المجلد04، العدد01 ،,جامعة غرادية، سنة 2020. https://www.asjp.cerist.dz/en/article/129107
8) بدر الدين خلاف، التنظيم القانوني للجريمة المعلوماتية في الجزائر، مجلة العلوم القانونية والإجتماعية، المجلد السادس، العدد الثاني، جامعة الجلفة، جوان 2021. https://www.asjp.cerist.dz/en/article/152224
9) بن يونس فريدة، استحداث قطب جزائي وطني لمكافحة الجرائم السبيرانية ومتابعتها، مجلة الدراسة القانونية والاقتصادية، المجلد05، العدد01، جامعة مسيلة، سنة 2022. https://www.asjp.cerist.dz/en/article/191646

10) بن عمیور أمینة وبوحلایس إلهام، القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، مجلة البحوث في العقود وقانون الأعمال، المجلد 07، العدد01، جامعة قسنطينة، سنة 2022 .
https://www.asjp.cerist.dz/en/article/178907
11) بيدي أمال، جهود الأمم المتحدة في مكافحة السيبرانية، مجلة الحقوق والعلوم الإنسانية، المجلد08 ، العدد01، جامعة الجلفة، الجزائر 2022.
https://www.asjp.cerist.dz/en/article/190487
12) حمزة خضري وعشاش حمزة، خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري، مجلة الدراسات القانونية والسياسية، جامعة الأغواط الجزائر، المجلد السادس، العدد الثاني، جوان 2020.
https://www.asjp.cerist.dz/en/article/116332
13) حابت أمال، دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها في مواجهة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، المجلة الدولية للبحوث القانونية والسياسية المجلد05، العدد 03 جامعة الوادي سنة 2021.
https://www.asjp.cerist.dz/en/article/174814
14) حاتم أحمد محمد بطيخ، تطور السياسة التشريعية في مجال مكافحة جرائم التقنية المعلومات، مجلة الدراسات القانونية والاقتصادية، المجلد 07، العدد 02، القاهرة 2021. https://jdl.journals.ekb.eg/article_191190.html
15) خالدي فتيحة، السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي كألية لحماية الحق في الخصوصية مجلة الحقوق والعلوم السياسية المجلد13، العدد 04، جامعة البويرة، سنة 2020.
https://www.asjp.cerist.dz/en/article/138811

16) خلدون عيشة، الطبيعة الخاصة للجريمة الإلكترونية وصورها، مجلة دراسات وأبحاث، العدد 09 ,جامعة جلفة، الجزائر، سنة 2012.
https://www.asjp.cerist.dz/en/article/3841
17) خديجة خالدي، آلية الاتحاد الإفريقي للتعاون الشرطي أفريبول، مجلة العلوم الاجتماعية والإنسانية، المجلد 11 العدد 15 جامعة العربي تبسي تبسة، سنة 2018
https://www.asjp.cerist.dz/en/article/59399
18) خلدون عيشة، الجريمة المعلوماتية في القانون الدولي والجزائري، مجلة (18 .القانون والعلوم السياسية، المجلد09، العدد 01 2023
https://www.asjp.cerist.dz/en/article/219864
19) دردار نادية، جريمة التلاعب في في نظام المعالجة الالية للمعطيات في قانون العقوبات، المجلد 17، العدد 01، جامعة سوق هراس، سنة 2023.
https://www.asjp.cerist.dz/en/article/218775
20) ربيعي حسين، المجرم المعلوماتي شخصيته وأصنافه، مجلة العلوم الإنسانية، المجلد 15، العدد 01، جامعة قسنطينة، سنة 2015.
https://www.asjp.cerist.dz/en/article/88190
21) رضا عسال وعماد عبد الرزاق، الجريمة الإلكترونية والمجرم المعلوماتي، مجلة ببليوفيليا ,العدد05، جامعة العربي تبسة –الجزائر، سنة 2020.
https://www.asjp.cerist.dz/en/article/123844
22) رمضاني فاطمة بدراني علي، القصور التشريعي الجنائي في مجال الجريمة المعلوماتية في التشريعين المغربي والجزائري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد07 العدد01، سنة 2022.
https://www.asjp.cerist.dz/en/article/192879

23) سمير شعبان، مقارنة تحليلة لتحديد مفهوم الجريمة والمجرم، دراسات وأبحاث مجلد 2009، العدد01، جامعة الجلفة الجزائر 2009. https://www.asjp.cerist.dz/en/article/4421

24) سورية دبيش، أنواع الجرائم الإلكترونية وإجراءات مكافحتها، مجلة العلوم السياسية والقانون، المركز الديموقراطي العربي، العدد الأول، برلين ألمانيا، سنة 2017. https://archive.org/details/20200618_20200618_1227

25) سهيلة هادي، أليات تعزيز حق الإنسان في الأمن المعلوماتي، مجلة للعلوم القانونية الاقتصادية والسياسية، المجلد 54، العدد05 ، كلية الحقوق، جامعة خيضر بسكرة، سنة 2017. https://www.asjp.cerist.dz/en/article/83207

26) سهيلة بوزيرة، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وسرية المعطيات الشخصية الإلكترونية ومكافحة الجريمة الإلكترونية، المجلة النقدية للقانون والعلوم السياسية، المجلد 17 العدد 02 جامعة تيزي وزو، سنة 2022. https://www.asjp.cerist.dz/en/article/209229

27) سميحة بلقاسم وحميد بوشوشة، الجريم الإلكترونية بعد جديد للإجرام في الجزائر مجلة العلوم الإنسانية المجلد 10، العدد01، جامعة ام البواقي، جوان 2023. https://www.asjp.cerist.dz/en/article/226117

28) شيح نجية وعبد الكريم فايزي، إجراء التسرب في القانون الجزائري، وسيلة لمكافحة الجرائم المستحدثة، معارف العدد 25، جامعة البويرة، سنة 2018. https://www.asjp.cerist.dz/en/article/99210

29) شهرزاد دراجي وبن شيخ نور الدين، القطب الجزائي الاقتصادي والمالي المستحدث، مجلة الدراسات القانونية والاقتصادية، المجلد 05، العدد 02، المركز الجامعي بريكة، سنة 2022، https://www.asjp.cerist.dz/en/article/211233

30) طاهر ياكر، مكافحة الجرائم الإلكترونية بين التشريعات الوطنية والإتفاقيات الدولية مجلة الصدى للدراسات القانونية، المجلد 04، العدد 04، جامعة خميس مليانة سنة 2022. https://www.asjp.cerist.dz/en/article/209810

31) عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية وأزمة الشرعية الجزائية، مجلة مركز الدراسات الكوفة، العدد السابع، جامعة الكوفة، سنة 2008.

32) عبد العزيز لزعر، ألية الإتحاد الإفريقي للتعاون الشرطي الأفريبول ودورها في مكافحة الجريمة الإلكترونية، مجلة متون، المجلد 13 العدد 03، جامعة مولاي الطاهر سعيدة، الجزائر سنة 2021. https://www.asjp.cerist.dz/en/article/163571

33) عائشة عبد الحميد، النظام القانوني للمنظمة الدولية للشرطة الجنائية (الإنتربول) ودورها في المجال التعاون القضائي الشرطي، المجلة الأكاديمية للأبحاث والنشر العلمي، المجلد 11، جامعة الطارف، الجزائر، سنة 2020.

34) فاروق خلف، الأليات القانونية لمكافحة الجريمة المعلوماتية، مجلة الحقوق والحريات، المجلد 03، العدد 02، جامعة محمد خيضر بسكرة، سنة 2015. https://www.asjp.cerist.dz/en/article/139256

35) فيصل كامل نجم الدين، واقع الجريمة الإلكترونية في مواقع التواصل الإجتماعي الحماية النظامية في دول مجلس التعاون الخليجي، المجلد 05، العدد 02، جامعة عبد الحميد بن باديس مستغانم – الجزائر، سنة 2018. https://www.asjp.cerist.dz/en/article/99089

36) فريد ناشف، أليات التعاون الدولي في مكافحة الجرائم الإلكترونية، مجلة البحوث في الحقوق والعلوم السياسية، المجلد 08، العدد 01، جامعة البليدة الجزائر، سنة 2022. http://dspace.univ-tiaret.dz/handle

37) قرانة عادل وبوحديد فارس، مهام السلطة الوطنية لحماية المعطيات الشخصية في التشريع الجزائري، مجلة العلوم القانونية والإدارية، المجلد 06، العدد 02، جامعة الجلفة، سنة 2021. https://www.asjp.cerist.dz/en/article/152268

38) قطاف سليمان، بوقرين عبد الحليم، مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية مجلة البحوث الثانوية والاقتصادية، المجلد 05، العدد 02، جامعة عمار ثليجي الأغواط، الجزائر، سنة 2022. https://theses-algerie.com/1629109523280971

39)كتاف الرزقي وبونهاك مصطفى، مجلة العلوم الاجتماعية، العدد 01، برلين سنة 2017. https://democraticac.de/?p=50220

40) لورنس سعيد الحوامدة الجرائم المعلوماتية أركانها وأليات مكافحتها، مجلة الميزان للدراسات الإسلامية والقانونية المجلد 04، العدد 01، المملكة العربية السعودية 2017. https://portal.arid.my/20039/Publications/Details/2090

41) محمد هاشم ماقورا، الحماية الجنائية لبرامج لحاسب الالي، مجلة دراسات وأبحاث، العدد 01 جامعة الجلفة، سنة 2009. https://www.asjp.cerist.dz/en/article/4423

42) مزيود سليم، الجرائم المعلوماتية واقعها في الجزائر واليات مكافحتها، المجلة الجزائرية للاقتصاد والمالية، العدد01 ، جامعة المدية، سنة 2014. https://www.asjp.cerist.dz/en/article/187298

43) مجاهدي خديجة، استراتيجية المنظمة الدولية للشرطة الجنائية في مكافحة الجريمة المنظمة، مجلة الدراسات القانونية، المجلد 02، العدد 02، جامعة مولود معمري، تيزي وزو، الجزائر 2016. https://www.asjp.cerist.dz/en/article/21221

44) محمد السعيد الزناتي، الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية مجلة إليزا للبحوث والدراسات، العدد الثاني جامعة إيليزي الجزائر، سنة 2017. https://www.asjp.cerist.dz/en/article/67442

45) معاشي سميرة، دراسة تحليلية للمفهوم الجريمة المعلوماتية، مجلة المفكر، العدد 17، المجلد 13، بسكرة الجزائر سنة 2018. https://www.asjp.cerist.dz/en/article/53584

46) مراد مشوش، الجهود الدولية لمكافحة الإجرام السيبراني، المجلد 12، العدد 02، جامعة غرادية سنة 2019. https://www.asjp.cerist.dz/en/article/108893

47) محمود محمد صفاء الدين علي شرشر، الجهود الدولية والتشريعية لمكافحة جرائم الإنترنت، المجلد 54، العدد 03، جامعة المنوفية مصر، سنة 2021. https://jslem.journals.ekb.eg/article_202042_31732.html

48) محمد سامي السيد أحمد، الدور العملي لوزارة الداخلية في مكافحة الجريمة المعلوماتية، المعهد القومي للملكية الفكرية، العدد الثالث، جامعة حلوان، سنة 2022.

49) هشام بشير، الأليات الدولية لمكافحة الجريمة الإلكترونية، المركز الدولي للدراسات المستقبلية الاستراتيجية، العدد 90، مصر، سنة 2012.

50) وقاص ناصر، الطبيعة القانونية لجرائم المستحدثة ووسائل إرتكابها جريمة الإنترنت، مجلة البحوث القانونية والسياسية، مجلد03، العدد 16 ,سعيدة –الجزائر، 2021.

51) يونس نفيذ, المكافحة التشريعية لبعض الصور الجرائم المعلوماتية وأصناف المجرم المعلوماتي، المجلة العربية للدراسات الأمنية، المجلد 38، العدد 02 ،المملكة العربية السعودية، سنة 2022.

رابعا: الملتقيات والمؤتمرات

1) ذياب موسى البدانية، جرائم الإلكترونية المفهوم والأسباب، ملتقى الجرائم المستحدثة في ظل التغيرات والتحولات الإقليمية والدولية، عمان، سنة 2014 .

2) سعدات فتوح محمود محمد، خصائص الجرائم المعلوماتية وصفات مرتكبيها في ظل المجتمع المعلوماتية، المؤتمر الدولي الاول لمكافحة الجرائم المعلوماتية، المملكة العربية السعودية، سنة 2015.

3) تميدلي رحيمة، خصوصية الجريمة الإلكترونية في القانون الجزائري، أعمال المؤتمر 14 للجرائم الإلكترونية، طرابلس، سنة 2017.

4) عبد مجلي عبير، الجرائم الإلكترونية، ملتقى إشكالية المصطلح في علوم الإعلام والاتصال في العالم العربي، بيروت، سنة 2018.

خامسا: الرسائل والأطروحات

أ) أطروحات الدكتوراه

1) عبد العزيز بن براهيم بن محمد الشبل، الاعتداءات الإلكترونية، رسالة دكتوراه، جامعة الإمام محمد بن سعود الإسلامية، السعودية، السنة الجامعية 1430-1431 هـ.

2) براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة لنيل شهادة دكتوراه، جامعة تيزي وزو، سنة 2018.

3) رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة دكتوراه جامعة تلمسان، السنة الجامعية 2017-2018.

4) هه لاله محمد تقي محمد أمين، التعاون الدولي في مواجهة الجرائم المستحدثة، أطروحة نيل شهادة الدكتوراه فلسفة في القانون العام، جامعة السليمانية، العراق 2019.

ب) رسائل الماجستير

1) **صغير يوسف، الجريمة المرتكبة عبر الأنترنت رسالة ماجستير، جامعة مولود معمري تيزي وزو السنة الجامعية 2012-2013.**
2) **أدهم باسم نمر بغدادي، وسائل البحث والتحري عن الجرائم الإلكترونية، رسالة ماجستير، جامعة النجاح الوطنية فلسطين، سنة 2018.**
3) **إبراهيم محمد بن محمود الزنداني، الجرائم الإلكترونية من منظور الشريعة الإسلامية وأحكامها في القانون القطري القانون اليمني، رسالة ماجستير، جامعة فطاني، سنة 2018.**
4) **عبد الله سيف عبيد سالم أل علي، سمات وأنماط المجرم المعلوماتي في جرائم الاحتيال الإلكتروني، أطروحة دكتوراه، جامعة المنصورة، سنة 2020.**
5) **عبد الرحماني أمينة ومرابطين حفيظة، جرائم تكنولوجيا الإعلام والاتصال، رسالة ماجيستر جامعة مولود معمري تيزي وزو دون سنة 2021، الجزائر.**
6) **عماد جاسم محمد حسين الشنكالي، دور الضبط الغداري الإلكتروني في مكافحة الجرائم المعلوماتية، رسالة ماجستير، جامعة تكريت العراق، 2022،**

خامسا: المواقع الإلكترونية:

1) **موقع وزارة الاتصالات والتقانة السورية moct.gov.sy**
2) **موقع منا رايت، Menaright.org / sites**
3) **https://www.unescwa.org ، موقع لجنة الأمم المتحدة الاقتصادية والاجتماعية لغربي أسيا.**
4) **موقع مجلس أوروبا، https://rm.coe.int/ara**
5) **موقع الإنتربول، https://www.interpol.int/ar/3/3**

6) موقع الجزيرة نت، https://www.aljazeera.net/new
7) موقع وزارة العدل، https://www.mjustice.dz/
8) موقع جريدة الجزائر الجديدة، www.eldjazaireldjadida.dz
9) موقع منظمة الويبو، https://www.wipo.int/treaties/ar
10) موقع الشروق أونلاين، https://www.echoroukonline.com/

الفهـــرس

الفهرس

ملخص الدراسة

الملخص:

تطورت تكنولوجيا الإعلام والاتصال لتصبح وسيلة لارتكاب الجرائم الإلكترونية، ولمواجهة هذه الجرائم اتخذ المشرع الجزائري عدة قوانين، بما في ذلك قانون العقوبات وقانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وأضاف المشرع أجهزة ومؤسسات إدارية متخصصة لمتابعة هذه الجرائم، وأخرى مؤسسات قضائية مثل القطب الجزائي الوطني، علاوة على ذلك تبذل جهود دولية لمكافحة الجرائم الإلكترونية من خلال التعاون في إطار المنظمات الدولية مثل الأمم المتحدة والاتفاقيات الدولية، بما في ذلك الاتحاد الأوروبي والاتحاد الإفريقي والجامعة العربية، والتعاون الشرطي بين الدول لتبادل المعلومات وتنسيق الجهود في مواجهة هذه الجرائم الإلكترونية على المستويين الدولي والإقليمي.

الكلمات مفتاحية:

قانون العقوبات/ قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال/ الجهود الدولية والإقليمية لمكافحة الجريمة المعلوماتية.

Abstract:

Information and communication technology has evolved into a means of committing cybercrime. In order to deal with such crimes, the Algerian legislature has adopted several laws, including the Penal Code and the Law on the Prevention of Crimes related to Information and Communication Technology. The legislature has added specialized administrative agencies and institutions to follow up on such crimes and other judicial institutions, such as the National Penal Pole. In addition, international efforts are being made to combat cybercrime through cooperation within international organizations such as the United Nations and international conventions, including the European Union, the African Union and the League of Arab States, and police cooperation among States to exchange information and coordinate efforts to counter such cybercrime at the international and regional level