وزارة التعليم العالي والبحث العلمي

Ministry of High Education and Scientific Research

جامعة محمد البشير الإبراهيمي– برج بوعريريج –

University of Mohamed el Bachir el Ibrahimi-Bba

كلية الحقوق والعلوم السياسية

Faculty of Law and Political Sciences

مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي في الحقوق

تخصص: قانون الإعلام الآلي والأنترنت

الموسومة بـ:

الأمن المعلوماتي في القانون الجزائري

إعداد الطالبتين:

- ريمة بن الشيخ
- منى بن عباس

تحت اشراف الدكتورة:

بلقمري ناهد

لجنة المناقشة:

اسم الأستاذ	الرتبة	الصفة
طاجين نسيمة	أستاذ محاضر قسم ب	رئيسا
بلقمري ناهد	أستاذ محاضر قسم أ	مشرفا ومقررا
صحراوي شهرازاد	أستاذ محاضر قسم ا	ممتحنا

السنة الجامعية: 2025/2024

ملحق بالقرار رقم ....1082.... المؤرخ في ..... 27 ديسمبر 2020

الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي

الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

(الطالب الأول)

أنا الممضي أسفله.

السيد(ة): بن الشيخ ريمة الصفة: طالب، أستاذ، باحث طالبة

الحامل(ة) لبطاقة التعريف الوطنية رقم 117326755 والصادرة بتاريخ 2020/01/29

المسجل(ة) بكلية / معهد الحقوق والعلوم السياسية قسم الحقوق

والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج، مذكرة ماستر، مذكرة ماجستير، أطروحة دكتوراه).

عنوانها: الأمن المعلوماتي في القانون الجزائري

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه.

التاريخ: .....

شوهد لأجل التصديق
السيد: المعنية
بطاقة التعريف الوطنية رقم: .....
مستخرج بتاريخ: .....
العناصر في 29 ماي 2025

توقيع المعني (ة)

ع/ رئيس المجلس الشعبي البلدي وبتفويض منه
ضابط الحالة المدنية
حروز ذهبية

ملحق بالقرار رقم ....1082.... المؤرخ في 27 ديسمبر 2020 .....

الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

موسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي

الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

(الطالب الثاني)

أنا الممضي أسفله،

السيد(ة): بن عباس منى ..... الصفة: طالب، أستاذ، باحث طالبة

الحامل(ة) لبطاقة التعريف الوطنية رقم: 119112159 والصادرة بتاريخ 2024/12/10

المسجل(ة) بكلية / معهد كلية الحقوق والعلوم السياسية قسم الحقوق

والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج، مذكرة ماستر، مذكرة ماجستير، أطروحة دكتوراه).

عنوانها: الأمن المعلوماتي في القانون الدولي.

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه .

التاريخ: .....

توقيع المعني (ة)

Ben Abbes

شوهد قبل التصديق

السيد : المعني

بطاقة التعريف الوطنية رقم :

مستخرج بتاريخ :

العناصر في :

2025 ماي 29

رئيس المجلس الشعبي البلدي و بتفويض منه

ضابط الحالة المدنية

حروز زهير

شكـر وعرفـان

بسم الله الرحمن الرحيم الحمد الله الذي ما نجحنا وما علونا ولا تفوقنا إلا برضاه

الحمد الله الذي ما اجتزنا دربا ولا تخطينا جهدا إلا بفضله وإليه

ينسب الفضل. . .

(وآخر دعواهم أن الحمد لله رب العالمين)

بعد مسيرة دراسية دامت سنوات حملت في طياتها الكثير من الصعوبات والتعب، ها نحن اليوم نقف على تخرجنا نقطف ثمار تعبنا ونرفع قباعتنا

بكل فخر وامتنان. . .

فالحمد الله حبا وشكرا وامتنانا، ما كنا نفعل هذا لولا فضل الله فالحمد الله

على البدء والختام. . .

نهدي هذا النجاح لنا انا وزميلتي أولا، ثم نهدي هذا النجاح إلى والد زميلتي المتوفي ندعو له بالرحمة والمغفرة التي كانت تتمنى أن يكون بجانبها في أكثر يوم فرحها، جبر الله قلبك بلقياه في الجنة رحمه الله وانار قبره.

وإلى الذي زين اسمي بأجمل الألقاب من دعمني بلا حدود وأعطاني بلا مقابل، إلى من غرس في روحي مكارم الاخلاق داعمي الأول في مسيرتي

وسندي إلى فخري واعتزازي أبي.

إهـــــــــداء

إلى من جعل الجنة تحت أقدامها واحتضننا قلبها قبل يدها وسهلت لنا الشدائد بدعائها لنا، القلب الحنون والشمعة التي كانت لنا في الليالي المظلمات سر قوتنا

ونجاحنا ومصباح دربنا الذي وهج حياتنا – والدتنا–

وإلى ضلعنا الثابت وخيرة أيامنا وقرة أعيننا (إخوتنا)

إلى كل عضو في مشوارنا الدراسي وساهم في بلوغنا لهذا الهدف وإلى جميع

الصديقات والزملاء والزميلات ومن كان له بصمة في طريقنا.

إلى من أعظم منا جميعا، إلى الذين ضحوا بحياتهم في سبيل الحرية، إلى من

جعلوا من دمائهم منارة لنا . . . الشهداء.

إلى الذين افنو سنيين حياتهم للحفاظ على كرامتنا، وضحوا بأهلهم وأحبابهم

وذكرياتهم في سبيل عزتنا . . .

ها نحن اليوم أكملنا وأتممنا أول ثمرته بفضله سبحانه وتعالى فالحمد لله على ما وهبنا وأن يجعلنا مباركا وأن يعيننا أينما كنا فمن قال انا لها فنحن لها وإن ابت

رغما عنها فالحمد لله شكرا وامتنانا على البدء والختام

وآخر دعواهم الحمد لله رب العالمين.

2025

قائمة المختصرات:

ق.ع.ج: قانون العقوبات الجزائري.

ج.ر: الجريدة الرسمية

.ج.ج: الجمهورية الجزائرية الديمقراطية الشعبية.

د. ج: دينار جزائري

مقدمة

شهد العالم منذ فجر التاريخ تطورا تدريجيا في أساليب نقل وتبادل المعرفة، إلا أن المعلومات بمفهومها الحديث لم تحتل مكانتها المحورية إلا مع التقدم العلمي والتقني، خاصة في القرن العشرين. فقد أصبح الانسان يعتمد بشكل متزايد على المعلومات لاتخاذ القرارات وفهم الظواهر، وتطوير المجتمعات. ومع ظهور الحواسيب ووسائل الاتصال الحديثة، أحدث العالم الالكتروني موجة من التطورات والتغيرات التي مست مجالات العمل حيث أصبح انتقال المعلومات عبر شبكة الانترنت ميزة تساعد على التقليل تحرص على تلبية الحياة العملية والتقليل من تراكمات الأعمال والسرعة في تبادل المعلومات وانتشار أنظمة المعلومات واعتماد هذه الأخيرة كركيزة رئيسية لسلامة الأعمال، فهي عبارة عن مجموعة من الإجراءات والتدابير الوقائية التي تستخدم لغرض الحماية من الجرائم الالكترونية، ومن مهددات استخدام تقنية المعلومات والتي قد تؤثر سلبا على سرية وسلامة المعلومات وتوفرها في الوقت المناسب. لذا قامت العديد من الدول ببذل الجهود اللازمة سواء كان ذلك على المستوى الوطني أو الدولي بوضع قوانين تحول بادراك هذا الخطر وإعطاء أهمية لنظام أمن المعلومات واعتباره من أهم الأليات التي تتيح للمنظمة تنفيذ أعمالها ونشاطاتها بكفاءة وفعالية دائمة، وذلك بانتهاج السياسة الأمنية التي تحد من انتشار مثل هذه المخاطر كون هذه الأخيرة لا تكتمل إلا إذا تعاون جميع أعضاء المؤسسة بغية تحقيق التطور والاستمرارية. ومع تسارع التطور التكنولوجي وانتشار الانترنت في جميع جوانب الحياة أصبح الأمن المعلوماتي عنصرا أساسيا لضمان حماية البيانات والأنظمة من التهديدات المتزايدة ذلك في إطار دراسة وتقييم امن المعلومات وتأثيره في الحد من المخاطر المحتملة على نظم المعلوماتية.

حيث تعد الجزائر من الدول التي عرفت تقنية المعلوماتية، وبالتالي كان لزاما عليها ايجاد آليات لحماية أمن وسلامة المعلومات من مختلف صور الاعتداء، وهذا ما يدفعنا للسؤال الآتي:

❖ **فيما تتمثل الأليات التي اقرها المشرع الجزائري لحماية قواعد الأمن المعلوماتي؟**

وتندرج تحت هذه الإشكالية الرئيسية، إشكالات تتمثل في الاتي:

- ماهي الجرائم الواقعة على المعلومات؟
- كيف نظم المشرع الجزائري أليات حماية قواعد الأمن المعلوماتي؟
- فيما تتمثل الإجراءات الإجرائية لحماية قواعد الأمن المعلوماتي؟

وتكمن أهمية هذه الدراسة في كونها تتناول موضوعا هاما أصبح محل اهتمام الباحثين في مجال القانون، وهو الأمن المعلوماتي، خاصة في ظل انتشار الجريمة المعلوماتية بشكل لافت، وانعكاساتها على مختلف المجالات مما يتطلب إعطائها أهمية ومحاولة إيجاد آليات لحماية المعلومات والحفاظ على سريتها وسلامتها من السرقة أو التلف أو التعديل وهذا ما يعزز الثقة في استخدام التكنولوجيا ويساهم في الاستقرار الأمني والحفاظ أيضا على الخصوصية من خلال اتخاذ مختلف الإجراءات اللازمة لحماية المعلومات.

وتهدف هذه الدراسة ما يلي:

- التعرف على مفهوم امن المعلومات والمصطلحات المرتبطة به.
- التعرف على مختلف الجرائم الواقعة على المعلومات.
- تسليط الضوء على الأليات والإجراءات اللازمة للحفاظ على امن المعلومات.

وبالنسبة لاختيارنا لهذا الموضوع الأمن المعلوماتي في القانون الجزائري موضوع في غاية الأهمية من خلال تسليط الضوء على تعريف الأمن المعلوماتي والتطرق إلى مختلف الأليات والإجراءات اللازمة لحماية المعلومات والحفاظ على سريتها وسلامتها.

إن اهتمام أي باحث ورغبته في تناول موضوع معين من غيره من المواضيع الأخرى راجع إلى جملة من الاعتبارات المرتبطة بشخصية الباحث واهتماماته، وأخرى موضوعية ترتبط بمواصفات موضوع الدراسة من حيث حداثته وقيمته العلمية ويمكن تلخصيها في:

دوافع ذاتية: تتمثل في اهتمامنا الشخصي بفهم آليات وإجراءات الحماية والمحافظة على أمن وسرية المعلومات في ظل التطورات المتسارعة.

دوافع موضوعية: حيث تتعلق بالقيمة العلمية لموضوع الدراسة، إضافة إلى التحسيس بضرورة تطبيق السياسة الأمنية لمختلف وسائل المعلومات، هذا ما سيفتح المجال حتما أمام الباحثين للاجتهاد أكثر في إثراء هذا الموضوع.

وبالنسبة للدراسات السابقة التي اجريت حول الامن المعلوماتي في القانون الجزائري فهناك مجموعة من الدراسات القليلة وهذا في حدود اطلاعنا، يمكن ذكر منها ما يلي:

1-بورباية صورية، قواعد الأمن المعلوماتي-دراسة مقارنة-، رسالة مقدمة لنيل شهادة الدكتوراه في العلوم، تخصص علوم قانونية، كلية الحقوق والعلوم السياسية، جامعة الجيلالي اليابس سيدي بلعباس، 2015-2016

وتهدف هذه الدراسة الى الكشف عن حداثة استخدام الأدوات التقنية وبرامج الحماية الفنية والقانونية.

وقد طرحت الإشكالية التالية: ماهي الحماية المطلوبة لتحقيق الأمن المعلوماتي؟ وما هو نطاق الجرائم التي تهدد الأمن المعلوماتي؟

تتعرض المؤسسات والشركات والاشخاص والحكومات لخطر سوء استخدام التكنولوجيا الرقمية أو لخطر مرتقب، مما يتطلب حماية فنية تقنية بالدرجة الاولى كإجراء وقائي واتباع خطط واستراتيجيات فنية لدعم الامن المعلوماتي بأهدافه ومبادئه، اضافة الى حماية قانونية تأتي ردعا لتلك السلوكيات المخالفة وحتى لا يتهرب الجاني من العقاب.

2-دراسة عزيزة رابحي، الاسرار المعلوماتية وحمايتها الجزائية، رسالة أطروحة مقدمة لنيل شهادة الدكتوراه تخصص قانون خاص، جامعة أبي بكر بلقايد،2017-2018.

تهدف هذه الدراسة الى الكشف عن الانتهاكات والاختراقات الواقعة على الأنظمة المعلوماتية في ظل التطورات التكنولوجية. والتعرف على السلوكيات المجرمة الماسة بالأسرار المعلوماتية وكيفية إثباتها.

وقد طرحت الإشكالية التالية: كيف سيتم القضاء عليها ومتابعة مرتكبيها في هذه الحالة؟

وتم التوصل الى أن المشرع قد وفق في تسمية الجريمة المعلوماتية بجرائم واقعة على نظام المعالجة الآلية للمعطيات وقد تم التفصيل في كل جريمة على حدى سن عقوبات تتعلق بها ولكن تبقى غير كافية.

وهناك بعض مذكرات الماستر التي تطرقت الى بعض جوانب موضوع الأمن المعلوماتي سواء من جانب دور الامن المعلوماتي في الحد من الجريمة المعلوماتية، وسبل حماية أمن المعلومات في الجزائر، بالإضافة الى التطرق الى أهم المخاطر والتحديات التي تواجه الامن المعلوماتي ومختلف التقنيات لتأمينه.

بالإضافة الى بعض المقالات التي تطرقت الى الموضوع من مختلف جوانبه.

وتتفق دراستنا مع الدراسات السابقة في كونها تطرقت الى موضوع الامن المعلوماتي في القانون الجزائري خاصة من الجانب المفاهيمي، وتختلف عنها في كونها تطرقت إلى الجانب القانوني للأمن المعلوماتي في الجزائر، وذلك بإضافة معلومات جديدة فيما يتعلق مثلا ببعض الاليات المؤسساتية وغيرها والتي صدر بشأنها المرسوم الرئاسي 20-05 ، وللاشارة هنا فإن معظم الدراسات في حدود اطلاعنا على التراث النظري توقفت في 2018 باستثناء بعض المقالات.

وللإلمام بموضوع الدراسة تم اتباع المنهج الوصفي كمنهج أساسي والذي يرتكز على الوصف الدقيق لموضوع الدراسة ويتجلى الاعتماد ذلك من خلال سرد ووصف وتحليل لكل من مفهوم المعلومات وكذلك أمن المعلومات.

وكأي دراسة، فإن عملنا هذا لم يخلو من بعض الصعوبات خاصة من ناحية الحصول على المراجع المتخصصة في الموضوع، بالإضافة الى قلة الدراسات التي تناولت موضوع الأمن المعلوماتي في القانون الجزائري.

وقصد الإلمام بمضامين وحيثيات هذا الموضوع فقد تم تقسيمه الى في فصلين أساسيين، حيث يتمحور الفصل الأول حول الإطار المفاهيمي للأمن المعلوماتي وقد خصص المبحث الأول لعرض ماهية أمن المعلومـــات حيث تطرقنا في مطالبه إلى تعريفها، خصائصها، أبعاد ومخاطر أمن المعلومات واستراتيجيتها، أما المبحث الثاني فتناول الجرائم الواقعة على المعلومات.

أما الفصل الثاني فقد تناول الإطار القانوني للأمن المعلوماتي في الجزائر، حيث تم تقسيمه الى مبحث أول يستعرض الآليات القانونية والمؤسساتية لحماية الجهة جريمة المعلومات من حيث الأليات القانونية والمؤسساتية، أما المبحث الثاني تطرقنا فيه إلى مختلف الإجراءات الجزائية لحماية قواعد الأمن المعلوماتي المتمثلة في الأساليب التالية: أساليب الحماية البرمجية والتقنية، أساليب الحماية التنظيمية والإدارية.

الفصل الأول

الإطار المفاهيمي حول الأمن المعلوماتي

تمهيـــــد:

أصبح الأمن المعلوماتي في العصر الرقمي الحديث جزءا أساسيا من حماية الافراد والمؤسسات والدول ومع التطور التكنولوجي المتسارع، ازدادت أهمية تأمين البيانات الحساسة والشبكات من التهديدات السيبرانية المتزايدة تعقيدا حيث أن تطور الأمن المعلوماتي لم يأت بمحض الصدفة، بل كان استجابة ضرورية للتصدي للهجمات الالكترونية التي تستهدف اختراق الأنظمة وسرقة المعلومات وتعطيل الخدمات.

وفي ظل هذا التطور التكنولوجي والتحول الرقمي في مختلف مجالات الحياة، ظهرت الجرائم المتصلة بالأمن المعلوماتي كأحد أبرز التحديات التي تواجه مختلف الدول. هذه الجرائم تشمل مجموعة واسعة من الأفعال غير القانونية التي ترتكب باستخدام الأنظمة الرقمية. ومن هنا وجب على المؤسسات سواء كانت عامة أو خاصة الاهتمام بمجال الأمن المعلوماتي وضع سياسة لأمن المعلومات وحمايتها من مختلف التهديدات الالكترونية.

ولتوضيح مضامين هذه المفاهيم قمنا بتقسيم هذا الفصل إلى مبحثين كالآتي:

المبحث الأول: مفهوم أمن المعلومات

المبحث الثاني: الجرائم المتعلقة بأمن المعلومات

المبحث الأول: مفهوم أمن المعلومات

يعد أمن المعلومات من بين أهم العناصر الضرورية الواجب توفرها في الإدارات والمؤسسات الحديثة، حيث سنتطرق في هذا المبحث إلى مختلف التعريفات المقدمة لأمن المعلومات، وقسمناه إلى أربع مطالب حيث يتضمن **(المطلب الأول)** تعريف المعلومات وخصائصها، و**(المطلب الثاني)** يتحدث عن تعـــريف أمن المعلومـــات ومكوناته، و**(المطلب الثالث)** تحت عنوان أبعاد ومخاطر أمن المعلومات وأخيرا **(المطلب الرابع)** يتضمن استراتيجية أمن المعلومات.

المطلب الأول: مفهوم المعلومات وخصائصها

تلعب المعلومات دورا فعالا ومهما في الإدارة الحديثة حيث تمثل المادة الأساسية التي يبني عليها القرار، فنجد أن معظم المؤسسات تسعى للحفاظ على هذا المورد وذلك بتوفير الإمكانيات اللازمة لضمان الاستخدام الأمثل لها والوصول إلى أحسن النتائج التي تطمح لها المؤسسة.[1] وقسمنا هذا المطلب إلى فرعين **(الفرع الأول)** يتضمن تعريف المعلومات آليا، أما **(الفرع الثاني)** يضم خصائص المعلومات.

الفرع الأول: تعريف المعلومات

تعرف المعلومات على أنها كل ما يضيف لو عينا أو فهمنا في موضوع ما أو مسألة أو حدث ويمكن إدراكها على أنها حقيقة أو بيانات أو أخبار أو معرفة أو شيء مفهوم.[2]

---

[1] حمودي كاهنة، **نظام أمن المعلومات في الجزائر دراسة حالة بلدية سوق الاثنين ولاية تيزي وزو 2014-2015**، مذكرة مقدمة لنيل شهادة الماستر في العلوم السياسية والعلاقات الدولية، تخصص سياسات عامة وإدارة محلية، كلية الحقوق والعلوم السياسية قسم العلوم السياسية، جامعة مولود العمري_ تيزي وزو 2016، ص 15.

[2] مصباح صالح الفيداعي، **المعلومات والمعلوماتية**، ط1، لجنة التأليف والتعريب والنشر، جامعة الكويت، الكويت، 1999 ص 19.

أما تعريف الدكتور شوقي سالم للمعلومات: فهو ذلك الشيء الذي يغير من الحالة المعرفية للمتلقي (القارئ أو المشاهد أو المستمع، أو أيا كانت الحاسة التي يتم بها التلقي) في موضوع ما.[1]

كما تعرف المعلومات على أنها "بيانات تم تصنيفها بشكل يسمح باستخدامها والاستفادة منها، وبالتالي فالمعلومات لها معنى، وتؤثر في ردود أفعال وسلوك من يستقبلها".

من خلال هذا التعريف يمكننا القول إن المعلومات هي تلك البيانات التي تم إعدادها بعد تحليلها أو تفسيرها أو تجميعها في شكل له معنى، فتصبح لها قيمة ومنفعة، ويمكن تداولها ونشرها في صورة رسمية أو غير رسمية.

بصفة عامة يمكننا القول: إن المعلومات هي كل ما يصل إلى علم الفرد، سواء أكان ذلك بالقراءة أم الاستماع أم المشاهدة، وتتعلق بجوانب وأمور تتصل بحياة الإنسان والأوضاع المحيطة به، والعلاقات التي يقيمها، والظروف التي تلازمه، والإمكانات المتاحة له، والأحداث التي يواجها من وقت لآخر.[2]

الفرع الثاني: خصائص المعلومات

يلتزم نظام المعلومات في أي مؤسسة بشرط تقديم معلومات تساهم في سهولة اتخاذ القرارات وذلك عن طريق استخدام خصائص تحدد ميزة هذا الأخير وقابليته لتلبية متطلبات المؤسسة ومن هنا تستوقفنا خصائص المعلومات التالية:

1-الدقة: وتشمل قابلية المعلومات في تلبية حاجيات المستفيد بصيغة الدقة المتناهية فمعظم الأخطاء الواردة في المعلومات ناتجة عن عدم صحة البيانات التي تم إدخالها والعكس صحيح، كما نجد نوع المعلومة وطبيعة الاستخدام والمستوى الإداري وكذا طبيعة

[1] مصطفى علي اللحام، **المدخل إلى علم المكتبات ومصادر المعلومات**، المنهل، 2016 ص 250.

[2] قدايفة أمينة، **استراتيجية أمن المعلومات**، مجلة أبعاد اقتصادية، العدد 06، جامعة محمد بوقرة – بومرداس، 2016 ص ص 164- 165.

المعايير المستخدمة في القياس وغيرها تساهم في إرجاع صحة البيانات المستخدمة في المعلومة أمر نسبي.

2-التوقيت: إن الوقت المناسب يساعد في إيصال المعلومة للمستفيد وأي تأخير يؤدي إلى إنقاص قيمة المعلومة وعدم استغلالها في الوقت اللازم.

3-الوضوح: لتحقيق الوضوح في المعلومة والاستفادة منها في المجال المطلوب لابد أن تكون بعيدة عن الغموض وسهلة للفهم المباشر.

4-المرونة: وهو تأقلم المعلومة وتعدد أوجه استخدامها لفائدة المستخدمين فكلما كانت المعلومة مستخدمة من طرف تطبيقات متعددة كانت أكثر مرونة والعكس صحيح.

5-الشمول: يجب أن تكون المعلومة أكثر إحاطة بمشكلة البحث وذلك يساعد الإدارة في تسيير مهامها المختلفة عن طريق إيضاح المستفيد لجميع المعطيات اللازمة عن الظاهرة، وبذلك سهولة إيجاد معلومات كافية.

6-القابلية للمقارنة: إن صحة المعلومات تكمن في قابليتها للمقارنة مع باقي المعلومات لمؤسسة ما، وغالبا ما تقارن المعلومات في مجال واحد.

7-الايجاز: يجب على المعلومات أن تكون مختصرة بحيث يتم ذكر المطلوب فقط بمراعاة الحالات الاستثنائية.

8-الموضوعية: وهنا نقصد عدم التحيز، وتعطي المعلومة دون أية رغبة شخصية أو تدخل من طرف معين، أو الانحياز لرؤى معينة، بشكل يتسم بالصدق في المضمون مما يضمن الرجوع إليها عند الحاجة.

9-اقتصادية: تكمن فائدة استخدام المعلومات في قابلية نجاحها وذلك راجع للجانب المالي الذي تتحمله المؤسسة للحصول على المعلومات المرغوبة، فالخاصية الاقتصادية تكمن في إيجاد أكبر قدر ممكن من المعلومات وذلك بأقل التكاليف.

وفي الأخير الملائمة هي النتيجة المرجوة من تطبيق خصائص المعلومات على الظواهر والدراسات.[1]

المطلب الثاني: مفهوم أمن المعلومات ومكوناته

على ضوء التطورات المتسارعة في العالم والتي تؤثر في الإمكانيات والتقنيات المتقدمة المتاحة الرامية إلى حذف منظومات الحواسب بغية السرقة أو تخريب المعلومات أو تدمير الحواسب ومراكزها أدى إلى التفكير الجدي لتحديث الأساليب والإجراءات الدفاعية والوقائية وذلك تبعا للإمكانيات المتوفرة، وهذا ما أدى إلى ظهور مجال أمن المعلومات التي سنتطرق إليه في العناصر التالية:[2]

الفرع الأول: تعريف أمن المعلومات

هناك عدة تعاريف للأمن المعلوماتي نذكرها كالآتي:

- هي المحافظة على اتاحة المعلومات وسلامتها وسريتها وملكيتها والاستفادة منها.
- هي المحافظة على المعلومات من تداخل استخدامها أو تخريبها أو استخدام معلومات مضللة أو تحريفها أو استبدالها أو سوء تفسيرها أو إلغائها أو سوء استخدامها أو الفشل في استخدامها أو الوصول إليها أو إظهارها أو مراقبتها أو نسخها أو سرقتها.[3]
- حيث يتحقق الأمن المعلوماتي بضمان سلامة المعلومات أثناء وجدها في القضاء المعلوماتي وأثناء عمليات النقل والمعالجة والتخزين ضد كل التهديدات التي يمكن أن تمس

[1] حمودي كاهنة، المرجع السابق، ص ص 16- 17.

[2] سليمة سعيدي، بلال حجاز، **نموذج ماكمبر Mc Cumber للأمن المعلوماتي (مدخل وثائقي)** مجلة آفاق لعلم الاجتماع، جامعة قسنطينة 2، الجزائر، العدد 1، جويلية 2020، ص 133.

[3] محمد عبد حسين الطائي، ينال محمود الكيلاني، **إدارة أمن المعلومات**، ط1، عمان، دار الثقافة للنشر والتوزيع، 1436هـ-2015م، ص34.

سلامتها أو تؤدي إلى توظيفها لألحاق أي ضرر مادي أو معنوي سواء بالأشخاص أم المجتمعات أم الهيئات أم الدول.[1]

1-من الناحية القانونية

وبالنسبة للمشرع الجزائري فلم يعرف امن المعلومات كمفهوم وانما وانما نص حديثا على تعريف المعلومات أو بالاصح المعطيات من خلال الامر 06-09 المتعلق بمكافحة التهريب في مادته 02/ط على انها المعلومات: كل المعطيات المعالجة أو غير المعالجة، المحللة أو غير المحللة، وكل وثيقة أو تقرير وكذا الاتصالات الاخرى بمختلف أشكالها بما فيها الالكترونية ونسخها المحقق في صحتها المصادق على مطابقتها[2].

ومن الناحية القانونية فلم يعرفه القانون وانما اشار بعض الباحثين فقط الى انه يعرف: " مجموعة من الإجراءات والقوانين، التي يتم فرضها بهدف تأمين حماية كل المعلومات والوسائط والأجهزة المستخدمة في حفظ ومعالجة وتبادل المعلومات عبر الشبكة". فمن الناحية القانونية نجد الاهتمام بأمن المعلومات من الجانب التشريعي من خلال التركيز على الإجراءات القانونية والعقابية، لتأمين المعلومات من الاختراقات والإضرار بها، إلا أنها أهملت الجانب التقني الذي هو أساس أمن المعلومة وكيفية تهيئته لضمان حمايتها.

2- الناحية التقنية: على أنه الإجراءات والتدابير الوقائية التي تستخدم سواء في المجال الفني أو الوقائي لصيانة المعلومات مثل الأجهزة، والبرمجيات والبيانات المتعلقة بالتطبيقات، وكذلك الافراد العاملين في المجال، ويشير كذلك أمن المعلومات إلى الدخول إلى كل موارد المنشأة من قبل أطراف غير مخولة باستخدام النظام.[3]

---

[1] عبد الوهاب جعيجع، **المعلوماتي وإدارة العلاقات الدولية**، الطبعة 2017م، دار الخلدونية، الجزائر، 2017، ص ص 68- 69.

[2]- الامر رقم 06-09 المؤرخ في 15 يوليو 2006، المتعلق بمكافحة التهريب، ج.ر، ج.ج.د.ش، العدد 47، الصادر بتاريخ 19 يوليو 2006

[3] سوهيلة بضياف، آمنة حمراني، **أمن المعلومات في الجزائر**، الإجراءات والتحديات، المجلة الجزائرية للأمن والتنمية، المجلد 9، العدد 16، جانفي 2020، ص179.

الفرع الثاني: مكونات أمن المعلومات

عند ذكر كلمة أمن المعلومات، وجرائم الحاسوب فإن ما يتبادر إلى الذهن غالبا هو كشف معلومات كان يجب أن تبقى سرا، والحقيقة أن الحفاظ على سرية المعلومات لا يعدو أن يكون جانبا واحدا من جوانب الأمن، أما المتخصصون فيرون لأمن الحاسوب والمعلومات مكونات ثلاثة على درجة واحدة من الأهمية، وهذه المكونات هي:[1]

1-سرية المعلومات (data confidentiality): إن أمن المعلومات يرشدنا إلى اتخاذ مجموعة من التدابير والاحتياطات اللازمة لتفادي الاطلاع على مختلف المعلومات السرية سواء الشخصية منها أو المالية أو المعلومات العسكرية من طرف الأشخاص الغير مصرحين لذلك.

2-سلامة المعلومات (data integrity): في هذا النوع يبرز لنا ضرورة التأكد من محتوى المعلومات وأنها لم تتغير ولم يتم العبث فيها وتدمير أجزاءها، فسلامة وصحة محتوى المعلومات تؤدي بأي مؤسسة إلى اتخاذ قرارات سليمة تضمن الاستمرارية والنجاح لأي عمل مبرمج.

فعلى سبيل المثال نقدم قائمة الأسماء الفائزين في مسابقة التوظيف، حيث يجدر الإشارة إلى ضرورة حماية وأمن هذه القوائم من التغيير المحتمل، فهنالك من يقوم بالعبث بها قصد حذف بعض الأسماء المرشحين ويضع أسماء غيرها مما يسبب ارتباك بين الناس ويحرج الجهة المعنية، وهذا يؤدي إلى تفاقم المشاكل بسبب تخريب المعلومات بأنواعها ومصادرها.

3-ضمان الوصول إلى المعلومات والموارد الحسابية(Availbility): إن سلامة وسرية المعلومات لها دور مهم وفعال، لكن هناك صعوبة في الوصول إليها والاطلاع عليها

[1] خالد بن سليمان الغثبر، مهندس محمد بن عبد الله القحطاني، محمد بن إبراهيم السويل، "**أمن المعلومات بلغة ميسرة**"، الطبعة الأولى، مكتبة الملك فهد الوطنية أثناء النشر، الرياض 1429هـ-2009م، ص 22.

واستخدامها، تصبح بلا منفعة ولا جدوى منها، لأن هذه المعلومات تم استغلالها من طرف مهاجمين بشتى الطرق لحرمان المستفيد من استخدامها، وكذا غرضه هو حذف لتلك المعلومات أو عرقلة استمرار العمل، لذا لا بدا من ضرورة التأكد من أن النظام الخاص بالمعلومات لازال في الخدمة وأنه ذات فائدة ويتميز بالاستمرارية.

حيث تتدرج مكونات أمن المعلومات في إعطاء نظرة مهمة إلى مختلف البرامج والاجهزة التي ينبغي حمايتها والتقنيات اللازمة إتباعها أثناء إجراء تعديل لأي معلومة أو طريقة المعالجة والاسترجاع.[1]

المطلب الثالث: أبعاد ومخاطر أمن المعلومات

يعد أمن المعلومات من القضايا الحيوية في العصر الرقمي، حيث أصبحت البيانات والمعلومات هي العنصر الأساسي في مختلف المجالات، سواء في المؤسسات الحكومية، الشركات الخاصة، أو حتى على المستوى الشخصي. ومع تزايد الاعتماد على التكنولوجيا والاتصال بالأنترنت، برزت العديد من التحديات والمخاطر التي تهدد سرية وسلامة وتوافر المعلومات. حيث قسمنا هذا المطلب إلى فرعين يضم **(الفرع الأول)** أبعاد أمن المعلومات، أما **(الفرع الثاني)** يتضمن مخاطر أمن المعلومات.

الفرع الأول: أبعاد أمن المعلومات

باعتبار توسيع مفهوم الأمن وشموله لقطاعات جديدة، وباعتبار المعلومات تشمل كل النواحي السياسية والعسكرية والاقتصادية والاجتماعية، فإن الأمن المعلوماتي ينسحب على قطاعات مختلفة يمكن إجمالها في الأبعاد التالية:

[1] حمودي كاهنة، المرجع السابق، ص29.

1- البعد السياسي: توسع الخدمات الإدارية عبر فضاء الانترنت، وسعي الدول لإقامة حكومـــات إلكترونية، وضخ بيانات المواطنين بها، وربط مختلف الدوائر الحكومية والخدمية بشبكات المعلوماتية، جعل من خطر الاختراق أو تعرض هذه البيانات للكشف أو الإتلاف أحد أبعاد الأمن القومي، كما أن تمكين المواطنين من الاستفادة من خدمات هذا الفضاء بما يوفره من سرعة أداء الخدمة، واختصار الوقت واقتصاد التنقل جعل العمل على حماية هذه الشبكة وأمنها، وضمان تدفقها واستمرار الخدمة بها مسألة غاية في الأهمية.

2-البعد العسكري: تتعرض الأنظمة العسكرية لهجمات مستمرة في عمليات للتجسس، وتمارس عدة دول هذه العمليات بهدف سرقة تصاميم أنظمة الأسلحة أو الحصول على المعلومات المفيدة بسرقة مخططات المعارك، أو فهم طرق تفكير الأعداء المحتملين، أو الإعداد لتعطيل الشبكات وحرمان الجيوش من استخدامها أثناء الحرب كما يعد أي نظام مرتبط بالإنترنت عرضة للهجوم.

كما تزداد أهمية السيطرة على القضاء الإلكتروني في استعمال التكنولوجيات الحديثة والأسلحة المتقدمة التي يغيب عنها الإنسان لتحل مكانه الآلية والبرمجة، التي منها الطائرات والصواريخ الذكية التي تستقي مساراتها من رصدها للبيئة المحيطة بها

3-البعد الشخصي: إن ما تركنه مواقع التواصل الاجتماعي من معلومات وبيانات يضعها المستخدمون بمحض إرادتهم، وترددها واستعمالها بشكل يومي يجعل عملية غربلتها والتدقيق بها واستخراج الصحيح منها، أمر يسير جدا، مما يجعل إمكانيات استغلال وتوظيف المعلومات الشخصية الهويات في متناول محترفي الإجرام وقد ينطوي على عواقب مدمرة للأشخاص وخصوصياتهم.

كما أن مسارعات الحكومات إلى تبني نظم الحكومات الالكترونية وتدقيق الهويات وحشد كل المعلومات الشخصية والبيولوجية والاجتماعية لكل شخص في ملف خاص به

يجعل اختراق تلك الأنظمة أو تفلت المعلومات منها يلحق أضرار شخصية ومساسا بأمن الأشخاص قد لا يضاهيه خطرا أكبر.

4-البعد الاقتصادي:

تورد شركة سيمنتاك الأمريكية المتخصصة في أمن المعلومات وصاحبة مضاد الفيروسات الشهير نورتون (Norton Antivirus) في تقريرها لسنة 2011 أن تكلفة جرائم المعلومات سنة 2011 عالميا قدرت بنحو 388 مليار دولار أمريكي، وهي أكبر من السوق السوداء لمخدرات الماريخوانا والكوكايين والهيروين مجتمعيـــن التي تقدر بـ288مليار دولار، وهي أعلى من الإنفاق السنوي لمنظمة الأمم المتحدة للأمومة والطفولة " اليونيسيف" بنحو 100ضعف، حيث تصل ميزانيتها إلى 3.65ملايير دولار.

معظم اقتصاديات العالم اليوم محكومة بواسطـــة شبكـــة معلو-اتصالية عبر عالمية، وأي عطب في أي منطقة من العالم سوف يتضرر منه الجميع، وما دامت هذه الشبكة ممتدة عبر العالم فهذا يعني أن هناك أجزاء كبيرة عرضة للهجوم وعدم تمتعها بالحماية الكافية، وأن الهجوم لا يتطلب أدوات كبيرة أو كلفة عالية أو أفراد كثرا، في مقابل ذلك تكون الأضرار عالية وكارثية. لذلك حماية هذه المصالح الاقتصادية الممتدة عبر العالم هي هدف حيوي لكل الأطراف:

الدول والمنظمات الحكومية وغير الحكومية، مما يصعد الحاجة إلى تبني الاستراتيجية العالمية في تثبيت الأمن.

5-البعد الاجتماعي: إن ارتباط أكثر من نصف سكان الأرض بهذه الشبكة المعلوماتية العملاقة وإمكانات التواصل المتاحة بها، في وجود كل الثقافات والإيديولوجيات وكذا وجود عمليات الاستقطاب المذهبية والطائفي – حيث أضحى توظيف الاختلافات المذهبية

والعرقية أحد أسباب الحروب والنزاعات وأحد أهم مهددات الاستقرار السياسي والاجتماعي لدول.[1]

خاصة مع ما شهده فضاء الإنترنت من تطور وقدرة على التفاعل اللحظي عبر شبكات التواصل الاجتماعي، وما لهذه الأخيرة من توظيف في زرع الذهبية والطائفية، والتجنيد لصالح تنظيمات الإرهاب والجريمة المنظمة. كل هذا جعل من حماية المجتمع ومكوناته الاجتماعية الثقافية أحد أبعاد الأمن المعلوماتي، التي كان أحد تجلياتها ما عرف بـ " ثورات الربيع العربي".[2]

الفرع الثاني: مخاطر أمن المعلومات

يتعرض أمن المعلومات إلى عدة مخاطر وتهديدات تؤثر سلبا على مصادر المعلومات، حيث نلاحظ أن تهديدات لا تكون الكترونية فقط بل يمكن أن تكون من طرف أحد أفراد المؤسسة أو بسبب حادث يؤدي إلى ضياع المعلومات، وفي هذا الصدد سنتطرق إلى ذكر عدة أنواع منها:

أولا: خرق الحماية المادية: ويتم هذا الأسلوب عن طريق استخدام أربع تقنيات تساعد على خرق للمعلومات من طرف المهاجم فيتبع الأساليب التالي:

1-التفتيش في مخلفات التقنية(dumps ter diving) : حيث يعتمد المهاجم في هذه التقنية على جميع مخلفات المؤسسة فيسعى جاهدا إلى إيجاد هذه المعلومات على مستوى المواد التي تركتها المؤسسة أو القمامة الخاصة بهم إلى العثور على ما يحتاجه وكذا استخدام مخرجات الكمبيوتر وكذا الأقراص التي تم الاستغناء عنها لتبديلها.

2- الالتقاط السلكي wiretapping : حيث يتم هنا استخدام التواصل السلكي مع الشبكة

[1] عبد الوهاب جعيجع، المرجع السابق ص ص 73-75.

[2] المرجع نفسه ص ص76- 77.

3-استراق الأمواج eavesdropping on èmanations: يتم استخدام لاقطات لتجميع الموجات المنبعثة من النظم باختلاف أنواعها.

4-إلغاء الخدمة: وهنا يقصد به الأضرار والعوائق التي تمنع تقديم الخدمة المطلوبة.

ثانيا: خرق الحماية المتعلقة بالأنظمة داخليا وخارجيا

إذ نجد أن الجهة الداخلية تمثل أكبر مشكل لدى المنظمة، حيث أن اختراق وكذا مختلف الهجمات التي مست المعلومات يكون داخل المنظمة، إذ نجد أن المهاجم ينتمي إلى المنظمة ويعمل في إطارها الداخلي مما يصعب تفادي هذا النوع فهو يمثل الخطر الأكبر لأي مؤسسة كانت، فمعظم تلك الهجمات ناتجة عن عدة أسباب ودوافع أدت بالفرد إلى شن هجوم ضد أنظمة المعلومات للجهة التي يعمل فيها، وتتمثل هذه الأسباب فيما يلي:

-**عدم الرضا:** فهذا السبب يرغم صاحبه باستخدام أساليب تضر المؤسسة التي يعمل فيها، حيث أن انتقامه يكون في تخريب نظم المعلومات لدى هذه الأخيرة مما يعطيه نوع من راحة الذات.

استعراض مواهبهم وقدراتهم على استخدام عدة أساليب وكذا تمكنهم في اختراق الأنظمة والفخر بالمعرفة اليقنة لكن يحدث العكس فهذا الاختراق يؤدي إلى المساس بالنظام وكذا هشاشته.

بغية تحقيق مكاسب مالية ضخمة من وراء الابتزاز بسرقة معلومات سرية وخاصة.

ثالثا: خرق الحماية المتصلة بالاتصالات والمعطيات

1-هجمات المعطيات data attacks: في هذه العملية يتم التطرق إلى ثلاث برامج وهي:

أ-**النسخ غير المصرح به للمعطيات unauthorized copying of data:** وهذه العملية ينتج عنها الدخول غير المصرح به للنظام، وذلك بالاستيلاء على مختلف النسخ المتعلقة بالمعطيات وتتضمن المعلومات والبيانات والبرمجيات.

ب-تحليل الاتصالات traffic anlysis: وفي هذه المرحلة يتم فيها التجسس على مختلف الاتصالات والارتباطات المرتبط بالنظام، لإبراز نقاط الضعف لدى المستخدمين وممارسة مختلف أساليب الرقابة من أجل استخلاص فترة الهجوم المناسبة على حركة النظام.

ج-القوات المخفية covert channrls: حيث يقوم المهاجم هنا بإخفاء مختلف المعطيات والمعلومات التي تم الاستيلاء عليها في موضع معين من النظام، وتعتبر صور من اعتداءات التخزين.

2-هجمات البرمجيات software attacks: في هذا النوع توجد عدة أساليب يتم بواسطتها الدخول إلى النظام ومحاولة تدميره وكذا الاحتيال عليه والعبث بمختلف الوظائف والمعطيات الخاصة به، وهذا الاختراق يؤدي إلى الاستيلاء على معظم البيانات وكذا الوصول بطريقة تقنية ومن بين هذه الأساليب نجد أن الشخص يستخدم طرق تقليدية وبسيطة لتنفيذ احتياله كاستخدامه للبرمجيات الخبيثة والمضرة بالمعطيات، إضافة إلى نقل المعلومات عبر أنفاق النقل...الخ.

رابعا: الهجمات والمخاطر المتصلة بعمليات الحماية:

وهناك تصنيف آخر لمخاطر امن المعلومات وذلك لوجود عدة أنواع من البيانات والتي تحتاج إلى تخزينها وهذه البيانات في حد ذاتها معرضة للتهديدات وفقا لذلك نصنف الأخطار المحتملة التي تتعرض لها نظام المعلومات إلى:[1]

1-المخاطر البشرية: تعد المخاطر التي يتسبب بها الافراد العاملون في النظام من أخطر التهديدات وأكثرها تأثيرا وتشمل الأفعال المقصودة والغير مقصودة من قبل الأشخاص المسموح لهم وغير المسموح لهما باستخدام النظام.

[1] حمودي كاهنة، المرجع السابق، ص ص 31- 33.

2-المخاطر البيئية والطبيعية: هي المخاطر التي يكون مصدرها البيئة أو الطبيعة التي يعمل بها النظام وهي المخاطر التي تقع على مكونات النظام كالأجهزة والبرمجيات والشبكة الحاسوبية. ويشمل الحرائق والكوارث الطبيعية وانقطاع الكهرباء.

3-الخلل في المعدات: يتضمن اعطال أجهزة الحاسوب والطرفيات والتجهيزات الشبكية المرتبطة بالنظام وهذا النوع من الأعطال يتسبب في توقف النظام عن العمل وحجب الخدمة عن المستفيدين.

4-الجرائم المحسوبة: تسبب خسارة كبيرة من خلال الاستخدام والوصول والتعديل لإدارة نظم المعلومات وقد تكون جريمة الحاسوب بريئة نسبيا مثل الاستخدام الغير مفوض للحاسبات أو خطرة كاستخدام الحاسبات لإرسال موجودات المنظمة لحساب منظمات أخرى وهي كالتالي: فيروسات الحاسب، القرصنة جرائم الفضاء الرقمي.

ومن جهة أخرى نجد أن هناك تهديدات أخرى تمس شبكات أمن المعلومات، ويمكن حصرها فيما يلي:

أ-تهديدات غير منظمة: تتشكل من أفراد غير متوقعين الذين يقومون بقرصنة شبكات الانترنت بأدوات كسر كلمات المرور والنصوص المغلقة، إن تشغيل أدوات القرصنة تعد مصدر خطر للشبكة وتزداد بزيادة مهارة هؤلاء الافراد في امتلاكهم أدوات مستخدمة للقرصنة.

ب-تهديدات منظمة: تكون بسبب تنافس تقني من طرف قراصنة يعرفون ثغرات نظم التشغيل بفهم وتطوير واستخدام تقنيات القرصنة المعقدة وذلك باختراق مؤسسات والشركات غير محمية وهذه الجماعات غالبا ما تتعلق بقضايا السرقة والاحتيال.

ج-تهديدات خارجية: تأتي من طرف أفراد خارج المنظمة عن طريق دخولها الشبكات من طرف الانترنت أو خطوط الهاتف.

د-تهديدات داخلية: وهنا بامتلاك الشخص حق الوصول إلى شبكة المنظمة أو بامتلاكه حق الدخول الفيزيائي لاماكن وجود أجهزة ومعدات الشبكة.

يمكن القول ان المخاطر التي تتعرض لها المعلومات متعددة لتعدد المعلومات، وتزايد نسبة الاختراق بزيادة أهمية المعلومة وكلما كانت المعلومة ذات أهمية كان الاختراق أكثر توسعا في النظام.[1]

المطلب الرابع: استراتيجية أمن المعلومات

إن استراتيجية أمن المعلومات هي مجموعة القواعد التي يطبقها الأشخاص لدى التعامل مع التقنية ومع المعلومات داخل المنظمة وتتصل بشؤون الدخول إلى المعلومات والعمل على نظمها وإدارتها، حيث قسمنا هذا المطلب إلى ثلاث فروع حيث يتضمن **(الفرع الأول)** مفهوم استراتيجية أمن المعلومات، أما **(الفرع الثاني)** يضم خصائص استراتيجية أمن المعلومات، وأخيرا **(الفرع الثالث)** تحت عنوان أهداف استراتيجية أمن المعلومات.

الفرع الأول: مفهوم استراتيجية أمن المعلومات

تعرف بأنها " مجموعة القواعد التي تتعلق بالوصول إلى المعلومات والتصرف فيها، ونقلها داخل هيكل يعتمد على المعلومة عنصرا أساسيا في تحسين أدائه، وبلوغ أهدافه".

كما تعرف أيضا على أنها " مجموعة القواعد التي يطبقها الأشخاص لدى التعامل مع التقنية ومع المعلومات داخل المنشأة، وتتصل بشؤون الدخول الى المعلومات والعمل على نظمها وإدارتها ".

وتعرف على أنها" الخطة التي تعرف الاستعمال المقبول لجميع الوسائط الالكترونية في شركة أو منظمة."

[1] المرجع نفسه، ص ص 33- 34.

الفرع الثاني: خصائص استراتيجية أمن المعلومات

من بين أهم مميزات وخصائص استراتيجية أمن المعلومات ما يلي:

- يجب أن تكون مناسبة اقتصاديا (ذات جدوى اقتصادية)
- يجب أن تكون مفهومة للمستخدمين.
- يجب أن تكون واقعية تتناسب مع واقع المنظمة.
- يجب أن تكون متناغمة مع أهداف المنظمة.
- يجب أن تكون مرنة وقابلة للمعالجة.
- يجب أن توفر حماية معقولة لأهداف الإدارة المعلنة.
- يجب أن تكون مستقلة.

الفرع الثالث: أهداف استراتيجية أمن المعلومات

تتمثل أهداف الاستراتيجية الأمنية في:

- ترجمة وتوضيح الأمن كما تم تعريفه في القواعد والمبادئ والأهداف العليا للمنظمة.
- تعريف المستخدمين بمسؤولياتهم وواجباتهم تجاه أمن نظم المعلومات، والذي يتضمن الأفراد، الأجهزة، البرامج، المعلومات...الخ.

-بيان الإجراءات التي يجب اتباعها لتفادي المخاطر والمهددات، والتعامل معها إذا ما وقعت.

- تحديد الآليات التي يتم من خلالها تنفيذ وتحقيق المسؤوليات والواجبات لكل مستخدم.[1]

المبحث الثاني: الجرائم الواقعة على المعلومات

[1] قدايفة أمينة، المرجع السابق، ص ص 170- 171.

تعد الجرائم الواقعة على المعلومات من الجرائم الحديثة التي نشأت نتيجة التقدم التكنولوجي وانتشار استخدام الحاسوب وشبكة الإنترنت في مختلف مجالات الحياة. هذه الجرائم تستهدف المعلومات الإلكترونية، سواء كانت مخزنة أو متداولة عبر الشبكات، وتتم غالبا باستخدام وسائل إلكترونية متطورة يصعب تتبعها أو التحقق من هوية مرتكبيها بسهولة.

وعليه سنقسم هذا المبحث إلى خمس مطالب، **(المطلب الأول)** سيضم جريمة الاتلاف وجريمة الدخول أو البقاء غير المصرح بهما، و**(المطلب الثاني)** سيضم جريمة الاعتراض المعلوماتي وجريمة التعامل في المعلومات غير مشروعة، أما **(المطلب الثالث)** جريمة التزوير والغش المعلوماتي، و**(المطلب الرابع)** المصنفات المحمية بموجب حقوق الملكية الفكرية في البيئة الرقمية، وأخيرا **(المطلب الخامس)** صور الاعتداء على المصنفات المعلوماتية – الرقمية.

المطلب الأول: جريمة الإتلاف

سنتطرق في هذا المطلب إلى فرعين: **(الفرع الأول)** نتناول فيه جريمة الاتلاف، أما **(الفرع الثاني)** جريمة الدخول أو البقاء غير المصرح بهما.

الفرع الأول: جريمة الاتلاف

إن حماية شبكة المعلومات يستلزم التدخل لتجريم الأفعال التي تهدف إلى التخريب أو التعطيل أو اتلاف الأجهزة المادية المتمثلة في الحاسوب، أو البيانات أو المعلومات الموجودة بداخله[1].

فالاعتداءات المعلوماتية التي تقع على المكونات المادية المتصلة بالحاسب وملحقاته كالشاشة والمعدات والشبكات، فلا توجد أي صعوبة في تجريمها وتطبيق النصوص التقليدية الجزائية، فهي جرائم سهلة التجريم والعقاب والقبض على الفاعلين.

[1] كوثر مازوني، "**الجريمة المعلوماتية "–أعمال ندوة وطنية**، ط1، دار الخلدونية، القبة القديمة، الجزائر، 2022، ص 353.

أما الاتلاف المعلوماتي هو ما يقصده الاعتداء الإلكتروني الموجهة للمعلوماتية، مما تحتويه من بيانات أو البرامج تستخدم فيه الأنترنت كوسيلة لتنفيذه، وهذا الاعتداء يهدف المكونات غير المادية للكمبيوتر سواء البيانات أو البرامج دون المكونات المادية المتصلة بالحاسب الآلي، كالشاشات والأشرطة والكابلات والأقراص الممغنطة وغيرها مما يعتبر من الأجهزة المادية للحاسب الآلي.

الاتلاف هو تخريب الشيء محل الجريمة بإفساده أو تعطيله أو وقف نشاطه وقيمته أو تدميره أو جعله غير صالح للاستعمال كليًا أو جزئيًا، كما أنه كل ما يقلل من قيمته الاقتصادية أو ينقص من كفاءته للاستعمال أو الغاية المعدة لها وللاعتداءات ثلاث أهداف تتمثل فيما يلي:

1-البرامج: وهي الأوامر المترتبة في شق معين لإنجاز الأعمال، وهي إما مستقلة عن النظام أو مخزنة فيه.

2-المعطيات: وهي الدم الحي للأنظمة، وما يكون محل لجرائم الحاسب وتشمل كافة البيانات المدخلة والمعلومات المستخرجة عقب معالجتها، وتمتد بمعناها الواسع للبرمجيات المخزنة داخل النظام، وقد تكون المعطيات في صور لإدخال أو الإخراج أو التخزين أو التبادل بين النظم عبر الشبكات، وقد تخزن داخل النظم على وسائط التخزين وخارجه.

3-الاتصالات: وتشمل شبكة الاتصال التي تربط أجهزة التقنية مع بعض محليًا ونطاقيًا ودوليًا وتنتج فرصة اختراق النظم عبرها، كما أنها بذاتها محل اعتداء وموطن من مواطن الخطر الحقيقي.

مثال: في قضية مصر قصت محكمة النقض المصرية في أحد أحكامها في قضية سرقة الكهرباء على غرار ما ذهب إليه في سرقة خط تلفوني، حيث قام أحد الأشخاص بتحويل مسار خط تلفون خاص بأحد الأشخاص إلى منزله واستعماله طيلة مدة تعطيله، وعللت حكمها بقولها أن الجاني قد استولى على الطاقة الكهربائية المغناطيسية

التي تعمل على نقل الصوت عبر الأسلاك، ولذلك يكون قد سيطر عليها واستغلها دون أن يكون قد سيطر عليها واستعملها دون أن يكون مرخصًا له ودون مقابل لذلك[1].

هذا مما أدى إلى الاستنتاج من بعض الفقهاء بحقيقة الاتلاف من الممكن أن يقع على الأموال ذات طبيعة غير مادية، كما هو الأمر بالنسبة لجريمة السرقة، وكما اعترفت بذلك التشريعات وأن الاتلاف من الممكن أن يقع على تلك الأموال ولكن بما يلائم طبيعتها.[2]

– ينصب الاتلاف على المعطيات المخزنة في نظم المعالجة الآلية للمعطيات والبرامج والمعطيات المتبادلة من الشيكات المغلقة أو المفتوحة وينتج عن هذه الأساليب، إما محو كلي للمعطيات أو تشويه من أجل اتلاف أجزاء منها، وتتخذ أساليب اتلاف المعطيات عمومًا صور يندرج في نطاقها العديد من الوسائل التقنية أولها الدخول غير المرخص به، النظام وإدخال معطيات من خلال الاتصال عبر نقاط الارتباط السلكي والموجات الموجودة عبر الشبكة الأنترنت للدخول إلى نظام الكمبيوتر بغرض الاتصال مع المعطيات أو البرامج المخزنة في النظام، ويتطلب هذا النشاط غالبًا تجاوز أو اختراق إجراءات الحماية التقنية للنظام، كتجاوز كلمة السرد password وإجراءات التعريف بالمستخدم أو التوصل لنقطة ضعف في نظام حماية البرامج والنفاذ منها.

–توجد وسيلة أخرى وهي نشر الفيروسات التي هي عبارة عن برامج مضرة بالمعطيات، وهي أكثر رواجًا وشيوعًا وأكثر الظواهر معالجة على مستوى الدراسات التقنية القانونية.[3]

الفرع الثاني: جريمة الدخول أو البقاء غير مصرح بهما

[1] المرجع نفسه، ص 354.

[2] حسن طاهري، "**الجرائم الإلكترونية**"، الطبعة 1، دار الخلدونية، القبة القديمة، الجزائر، 2022، ص ص 64- 65.

[3] كوثر مازوني، المرجع السابق، ص 141.

لقد تم تصنيف هذه الجريمة تحت باب الجرائم المعلوماتية المرتكبة بواسطة النظام المعلوماتي، وتعتبر أهم الجرائم أو بالأحرى يعد الدخول أو البقاء غير المصرح بهما إلى النظام المعلوماتي.

نصت على هذه الجريمة المادة 394 مكرر من ق. ع تبدأ هذه الجريمة منذ اللحظة التي يبدأ فيها الجاني التجول داخل النظام أو يستمر في التجول بداخله بعد انتهاء الوقت المحدد، لأنه الغرض يتعلق بدخول غير مشروع أي مع علم الجاني أنه ليس له حق الدخول للعلم بتحقق البقاء المعاقب عليه داخل النظام المعلوماتي مستقلاً عن الدخول لنظام، أو قد يجتمعا ويكون البقاء معاقب عليه استقلالاً عندما يكون الدخول إلى النظام مصرح به، والمثال على ذلك الدخول إلى النظام عن طريق الخطأ أو الصدفة.

حيث يتوجب في هذه الحالة على المتدخل قطع الاتصال والانسحاب فورًا من داخل النظام، ولكن إذا بقي رغم ذلك فإنه يعاقب على جريمة البقاء داخل النظام بعد المدة المحددة له للبقاء داخله.

أولا: تجريم الدخول والبقاء على الصعيد الدولي والداخلي

نصت إتفاقية بوداست: على جريمة الدخول أو البقاء في المادة الثانية تحت عنوان "الدخول غير قانوني" والتي تشير إلى أنه يجب على كل طرف يتبنى الإجراءات التشريعية أو أي إجراءات يرى أنها ضرورية من أجل اعتبارها جريمة جنائية وفقا للقانون الداخلي الولوج العمدي لكل أو لجزء من جهاز الحاسب الآلي بدون حق، كما يمكن له أن يشترط أن ترتكب الجريمة من خلال انتهاء إجراءات الأمن بغية الحصول على بيانات الحاسب أو أي نية إجرامية أو ترتكب الجريمة في الحاسب الآلي يكون متصلا عن بعد بحاسب آلي آخر.

وأشارت المذكرة التفسيرية لاتفاقية بوداست بأن الدخول غير مصرح به يعد الجريمة الرئيسية التي تنطوي على التهديد أو التعدي على الأمن المعلوماتي، بمعنى السرية والسلامة

وإتاحة النظم والبيانات المعلوماتية، إذ أن هذا الدخول يمكن أن يترتب عليه الوصول إلى بيانات سرية مثل كلمة المرور.

فقد تعرضت الكثير من أنظمة الحسابات الآلية، وبصفة خاصة تلك التي تعمل من خلال شبكة المعلومات إلى اختراق بواسطة أشخاص غير مصرح لهم بالدخول إليها، وفي و. م. أ حيث كان الظهور الأول لهذه الظاهرة، حيث أطلق آنذاك على هؤلاء الذين يدخلون إلى أنظمة الحسابات الآلية بدون تصريح "القراصنة" قياسًا على الأشخاص الذين كانوا يقومون في الماضي باعتراض البرامج الإذاعية.

وجرم السلوك أيضًا القانون العربي النموذجي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها عام 2004 في المادة الثالثة، كل من دخل عمدًا وبغير وجه حق موقعًا نظامًا معلوماتيًا يعاقب بالحبس والغرامة.

فالولوج أو الدخول إلى النظام المعلوماتي يكفي معرفة الطريقة الواجب اتباعها، مما يفسح المجال للمتدخل الحصول على كل ما يريد من المعلومات المخزنة في هذا النظام.

وأكثر من ذلك فإن عملية الدخول تسمح له بالدخول إلى شبكات المؤسسات والإدارة الحائزة لهذا النظام، كما تسمح له بالوصول إلى شبكات أخرى تكون مرتبطة به، ويضم الولوج غير المصرح به للاختراق الذي يحدث لنظام بأكمله أو جزء منه.

-فإذا دخل شخص ما للنظام فيكون بمقدوره معرفة كل المعلومات التي يريد الحصول عليها مثل: البيانات والسجلات الخاصة بالعملاء في البنوك والبيانات الشخصية للمواطنين في السجلات المدنية والأسرار العسكرية للدولة وبرامج الكمبيوتر بصفة عامة.[1]

وقد يتعرض النظام المعلوماتي إلى الاختراق من قبل أفراد غير مصرح لهم بالدخول إليه أو بقاء فيه، وقد ساهم في انتشار هذه الظاهرة تطور الاتصالات وتنمية الشبكة المعلوماتية.

[1] المرجع نفسه، ص ص 146- 147.

فبعد ظهور الأنترنت ازدادت عملية التدخل خطورة، وأهم الجناة يدخلون في الشبكات المرتبطة بالأنترنت فيتوصلون إلى المعلومات ولو كانت محمية، مما قاد إلى زيادة درجة حمايتها، وإزاء هذه المخاطر نادت الدول لعقد المؤتمرات بهدف وضع الاتفاقيات الدولية للحد من مخاطر استعمال هذه التقنيات.

ويتحقق الدخول غير مشروع، متى كان ذلك الدخول مخالفًا لإرادة صاحب النظام أو مما له الحق السيطرة عليه، ويتحقق الاختراق أو الدخول غير مصرح به حين يضع مالك النظام قيودًا على الدخول إلى ذلك النظام، ولا يحترم الجاني هذه القيود أو كان هذا الأمر يتطلب سداد مبالغ من النقود لم يسددها الجاني الذي قام بالدخول غير مشروع إلى النظام.

ويمكن القول بصفة عامة أن الدخول غير مصرح به إلى النظام المعلوماتي يتحقق بالوصول إلى المعلومات والبيانات المخزنـة داخلـه دون إرضاء المسـؤول عن هذا النظام، أو المعلومات التي يحتوي عليها أو هو بقول آخر إساءة استخدام الحاسب الآلي ونظامه عن طريق الشخص غير مرخص له باستخدامه والدخول إليه للوصول إلى المعلومات والبيانـات المخزنة

بداخله لاستخدامها لغرض ما، والشعور بالنجاح في اختراق الحاسب الآلي.

ويترتب في الكثير من الحالات الدخول غير المصرح به خسائر مادية كبيرة، بل تترتب على هذه الخسائر وقف هذا الدخول، ولو لم يترتب عليه أضرار فعلية تلحق بالنظام وبالمعلومات التي يحتوي عليها[1].

مثال: حالة التي يمكن فيها أحد الأشخاص الدخول إلى النظام الحاسب الآلي بأحد المعامل الخاصة بتصنيع وتجربة الأسلحة النووية بكاليفورنيا، و.م.أ، وقد تحمل المعمل خسائر مادية قدرت بمائة ألف دولار أمريكي، وهي تكلفة الأبحاث التي أجريت لمحاولة وقف هذا الدخول غير المسموح به.

[1] المرجع نفسه، ص 148.

وقد تم تجريم فعل الدخول والبقاء غير مصرح به إلى نظام المعلوماتي، كما أنه ينبغي تحديد المحل الذي ينصب عليه فعل الدخول، والذي قد يكون معلومة أو نظم للحاسب الآلي أو شبكة معلومات، ومن ناحية أخرى فإن تحديد الهدف الذي يعاقب عملية الدخول قد أثار خلافا أظهرته النصوص القانونية المختلفة التي تناولت جريمة الدخول وبقاء غير مصرح بهما.

فالدخول غير مصرح به إلى النظام المعلوماتي سيمتد عدم مشروعيته من كونه غير مصرح به أو كونه مخالفا لأحكام القانون، إلا أن هذا الدخول قد يكون مقصودا في ذاته، كما قد يكون مقصودا باعتباره وسيلة لتحقيق غاية أخرى، وسواء تمثلت هذه الغاية إلى الحصول على المعلومات لتحقيق غرض ما، أو كان الدخول في النظام ممر يتم من خلال الدخول من نظام آخر من الصعب على الفاعل الدخول إليه[1].

ثانيا: أركان جريمة الدخول أو البقاء غير المصرح بهما

1-الركن المادي:

انطلاقًا من نص المادة 394 مكرر من ق. ع. ج والنصوص القانونية السابقة فإن تحقيق الركن المادي لجريمة الدخول أو البقاء غير المصرح بهما، ويتسم بسلوك إجرامي يرتكبه الجاني قد يتخذه صورة الدخول المنطقي، وذلك لفتح الباب يؤدي إلى نظام المعالجة الآلية بمكوناته وأحيانًا يتخذ صورة البقاء، وينصب هذا السلوك على محل معين هو المعلومات ونظم معالجتها، والركن المادي هو عبارة عن نشاط إيجابي من جانب الجاني ويكون الاتصال بطريق الغش ويتحقق الركن المادي بإحدى الصور التالية.

أ-اختراق الأجهزة الرئيسية: بطريقة الغش إلى نظام المعالجة الآلية للمعطيات.

[1] المادة 394-الجرائم المتعلقة بالمعلومات-المتضمن قانون العقوبات، ج, ر, ج, ج, د, ش، العدد 30، 30أبريل 2024.

ب-البقاء أو المكوث: بطريقة الغش في نظام المعالجة الآلية وأجزاء منه، ومن خلال نص المادة 394 مكرر أنه هناك صورة بسيطة لدخول إلى النظام أو البقاء فيه، وأخرى شدد فيها المشرع العقوبة، إذ نصت المادة 394 من ق. ع. ج أنه تضاعف العقوبة، إذ ترتب على ذلك حذف أو تغيير لمعطيات المنظومة تكون العقوبة بالحبس من ستة شهر إلى سنتين والغرامة من 50.000دج إلى 150.000دج.

إذن السلوك في جريمة الدخول أو الولوج إلى نظام أو البقاء فيه غير المصرح بهما يتحقق بفعل الدخول أو البقاء.

ج-فعل الدخول غير المصرح به: فعل الدخول يشكل الركن المادي في هذه الجريمة لا يقصد به الدخول المادي إلى المكان الذي يتواجد به الحاسوب ونظامه، بل يقصد به الدخول باستخدام الوسائل الفنية والتقنية إلى النظام المعلومات، أي الدخول المعنوي أو الإلكتروني.

والاتصال بالحاسب الآلي خاص بشخص الغير بدون موافقته ويتخذ الدخول صورًا مختلفة فمنها أن يقوم الفاعل بتشغيل الجهاز المتعلق، وبالتالي الاطلاع على ما به من بيانات ومنها ما يقوم به الفاعل من استخدام برامج الدخول في النظام بدون إذن صاحبه فيطلع على ما يقوم به صاحب الجهاز، أو ينتقل بين أجزاء الجهاز ليطلع على ما يحتويه أقسام هذا الجهاز من معلومات.

د-البقاء غير مصرح به: يقصد بفعل البقاء التواجد داخل نظام المعالجة الألية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام[1].

2-الركن المعنوي: (القصد الجنائي)

[1] عزيزة رابحي، **الأسرار المعلوماتية وحمايتها الجزائية**، رسالة أطروحة لنيل شهادة دكتوراه، تخصص قانون خاص، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، الجزائر، 2018/2017، ص ص 168- 173.

هو عبارة عن قصد جنائي بعنصرين العلم والإرادة فيتحقق علم الجاني بأنه يدخل بصورة غير مشروعة إلى نظام المعالجة الألية، حيث أن صورة الركن المعنوي تتمثل بالقصد الجنائي فإن هذه الجريمة لا تتحقق بالخطأ، وأن نتيجة إرادته إلى ارتكاب هذه الجريمة، أي أن اكتمال هذه الجريمة يستدعي توفر الركن المعنوي ويتوافر سوء نية الجاني.[1]

المطلب الثاني: جريمة الاعتراض المعلوماتي

في ظل التطورات المتسارعة في مجال تقنية المعلومات والاتصالات، برزت أنماط جديدة من الجرائم التي تستهدف البيانات والمعلومات المخزنة أو المتبادلة عبر الوسائط القمية، ومن بين هذه الجرائم الحديثة "جريمة الاعتراض المعلوماتي"، نظرا لما تشكله من انتهاك لخصوصية الأفراد وتهديد لأمن المعلومات.

يقصد بجريمة الاعتراض المعلوماتي قيام شخص باعتراض أو التقاط بيانات تنقل عبر شبكة معلوماتية دون إذن أو وجه حق.

لذا سنتطــرق في هذا المطلب إلى **(الفرع الأول)** جريمة لاعتراض المعلومــاتي و**(الفرع الثاني)** جريمة التعامل في المعلومات غير مشروعة.

الفرع الأول: جريمة الاعتراض المعلوماتي

هو التنصت ونقل البيانات التي تتم داخل جهاز الحاسب، أو التي تتم عبر جهازين عن بعد عبر الشبكة المعلوماتية.

هو إلتقاط أو تنصت أو تسجيل أو مراقبة الاتصالات والمراسلات التي تتم بوسـائل إلكترونية، وبالتالي أي اعتراض لأي بيانات كانت مرسلة أو متداولة إلكترونيا ودون وجه حق يشكل جريمة تستحق العقاب.

أولا: أركان جريمة الاعتراض المعلوماتي (غير المشروع)

1-الركن المادي:

[1] المرجع نفسه، ص ص 177- 179.

يتمثل الركن المادي في جريمة الاعتراض غير القانوني للبيانات في فعل الاعتراض الذي يشمل أفعال التنصت أو الالتقاط أو مراقبة الاتصالات أو إعاقة سير البيانات، أو المعلومات الإلكترونية المرسلة عبر الشبكة المعلوماتية أو عبر وسائل تقنية.

أ-استعمال وسائل فنية غير علنية لفعل الاعتراض:

يشترط لقيام هذه الجريمة أن يتم اعتراض البيانات والمعلومات باستخدام وسائل فنية معنية غير علنية تتعلق بالتنصت أو التحكم أو مراقبة محتوى الاتصالات[1].

ب-أن يكون الاعتراض غير مشروع:

كما يشرط في هذا السلوك أن يكون بدون حق أو بصفة غير مشروعة، فهذه الجريمة قد تقع من أي شخص كانت صفته سواء كان يعمل في مجال الأنظمة المعلوماتية، أم لا علاقة له بذلك، غير أنه يجب أن لا يكون الجاني من هؤلاء المصرح لهم بالحصول على تلك المعلومات، فإذا كان المتهم بالقيم بالتنصت على المحادثات أو التقاط البيانات أو المعلومات المرسلة أو تسجيلها ممن لهم الحق أو المصرح لهم مسبقًا.

2-الركن المعنوي:

بالتوافر القصد الجنائي العام بعنصريه العلم والإرادة، أما القصد الخاص يستخلص من تلك النصوص، حيث جاء في المادة الثالثة من اتفاقية بودابست أن يكون الاعتراض عمدًا وبدون حق، وعليه يجب أن يعلم الجاني بأن حصوله على تلك المعلومات، أو البيانات وأن التنصت على المحادثات وتسجيل والتقاط البيانات المعلوماتية تم بوجه غير مشروع وضد إرادة صاحب الاتصال أو ضد رغبة صاحب السيطرة.

1-الأغراض غير القانوني في التشريع الجزائري:

[1] محمد خليفة، "**خصوصية الجريمة الالكترونية وجهود المشرع الجزائري في مواجهتها**"، مجلة دراسات وأبحاث، المجلد1، العدد1، جامعة الجلفة، 2009 ، ص386.

يعتبر التنصت على الاتصالات أو على ما هو مرسل عن طريق الشبكة المعلوماتية، أو أي نظام معلوماتي ونص في قانون العقوبات المعدل والمتمم 06-23 على مادة جديدة تشمل الاعتداء على حرمة الحياة الخاصة، جاء فيها أنه يعاقب...كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص.

- التقاط أو تسجيل أو نقل مكالمات خاصة أو سرية بغير إذن صاحبها أو رضاه.
- بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص، بغير إذن صاحبها أو رضاه[1].

والأساس في جريمة الاعتراض المعلوماتي غير المشروع هو حماية حرية الاتصالات وعدم إعاقة سيرها، أو اعتراضها حتى ولم تكن المعلومات سرية ولكن أطراف الاتصال أرادو أن تكون بوسيلة سرية أو غير علنية.

الفرع الثاني: جريمة التعامل في المعلومات غير مشروعة

تعتبر من أهم الجرائم ضد المعلومات وأخطرها فقد عرض المشرع الجزائري من جانبه على التحقيق من أثار الاعتداءات على المعلومات، فيما إذا تم الحصول عليها بطرق غير مشروعة من خلال تجريم التعامل في هذه المعلومات غير مشروعة، هذا وقد جرم كل الأفعال التي بواسطتها يتم الحصول على هذه الأخيرة من خلال نصوص المواد 394 مكرر، ومن أجل وقاية أكثر من هذه المخاطر فإنه يجب على قانون العقوبات أن يحظر الأفعال راجحة الخطورة من المبدع قبل ارتكاب الجرائم.

فالغاية من تجريم مثل الأفعال هي وقائية، لأن هذه الجرائم يهدف المشرع من خلال تجريمها إلى منع وقوع الضرر.[2]

وجريمة التعامل في المعلومات الغير مشروعة مثل كل جريمة تتكون من ركنين:

[1] المرجع نفسه، ص 384.

[2] عزيزة رابحة، المرجع السابق ص ص 168- 173.

أولا: الركن المادي

يتكون الركن من مجرد السلوك الإجرامي دون النتيجة الإجرامية.

1-السلوك الإجرامي:

يقوم الركن المادي لجريمة التعامل في المعلومات غير مشروعة على مجرد توافر السلوك الإجرامي الذي يتخذ صورتين:

أ-التعامل في معطيات صالحة لارتكاب الجريمة:

تجرم المادة 394 مكرر 02 من مجموعة من الأفعال الخطرة التي لو تركت بدون تجريم لأدت إلى حدوث جرائم أخرى، هذه الأفعال تشمل كافة أشكال

التعامل الواقعة على المعطيات لا سيما المتعلقة بالقطاع البنوك، والتي تسبق عملية استعمال هذه المعطيات في ارتكاب الجريمة، فالمعطيات قبل هذه المرحلة الأخيرة تمر بالعديد من المراحل حتى تصل إلى يد الجاني، فيرتكب بها جريمته وهذه المراحل تبدأ من تصميم هذه المعطيات والبحث فيها وتجميعها وصولاً إلى جعلها في متناول الغير وتحت تصرفه ذلك بتوفيرها أو نشرها أو الاتجار فيها، ولا يشترط أن تقع هذه الأفعال مجتمعة لتقوم الجريمة، بل يكفي أن تقع إحداهما فقط، وهذه الأفعال هي التصميم والبحث والتجميع والتوفير (الوضع تحت تصرف أو العرض) والنشر والإيجار.

ب-التعامل في معطيات متحصلة من جريمة:

هي صورة الثانية من جريمة التعامل في المعلومات غير مشروعة، وتتحقق بواحد من أربعة أفعال هي حيازة المعطيات متحصلة من جريمة الدخول أو بقاء غير مصرح بهما، أو تلاعب بالمعلومات أو إفشاء هذه المعلومات أو نشرها أو استعمالها، أي أنه يكفي تحقيق واحد من هذه الأفعال حتى تقوم الجريمة[1].

ج-النتيجة الإجرامية:

[1] المرجع نفسه، ص 170.

جريمة التعامل في المعلومات غير مشروعة، هي من جرائم الخطر لا يتطلب لقيامها حدوث نتيجة معينة، فالمشرع جرم تلك الأفعال يمكن أن تؤدي إلى ضرر فعلى.[1]

ثانيا: الركن المعنوي

جريمة التعامل في المعلومات غير مشروعة جريمة عمدية، ويستفاد ذلك من عبارة المادة 394 مكرر 02، عمدًا وعن طريق الغش.

1-القصد الجنائي العام:

يتوفر القصد العام بالعنصرين هما:

أ-العلم: لابد أن يحيط الجاني العام علمًا كافيًا بكافة العناصر الداخلية في تشكيل الجريمة ومن قبيل ذلك ضرورة علم المتعامل أنه يقوم بالتعامل في المعلومات غير مشروعة.

ب-الإرادة: لا يكفي أن يكون المتعامل عالمًا بما يفعل لقيام جريمة المتعامل بمعلومات غير مشروعة، بل يجب أن تكون إرادته متجهة إلى تحقيق واتيان أحد المظاهر السلوكية التي نص عليها المشرع، ومن قبل ذلك نشر واتجار وحيازة المعلومات وذلك رغم علمه بصفتها الغير مشروعة.

2-القصد الجنائي الخاص: يتخذ القصد الجنائي الخاص صورتين:

أ-القصد الخاص في جريمة التعامل في معلومات صالحة لارتكاب الجريمة: اشترطت اتفاقية بودابست في المادة 06 أنه لا يعاقب على التعامل في الوسائل الصالحة لارتكاب جريمة، إلا إذا كان الغرض هو التعامل بنية ارتكاب الجريمة، والمقصود بذلك اتجاه القصد في التعامل بهذه المعلومات، إلا إذا كان قصده سيء يتمثل في إعدادها ولاستعمالها في جريمة ما.

ب-القصد الجنائي الخاص بجريمة التعامل في معلومات متحصلة من الجريمة: يجب توافر القصد الجنائي العام ذلك لأن المعلومات المتحصل عليها من جريمة وطبيعتها الثابتة،

[1] محمد خلفة، المرجع السابق، ص ص 384-386.

وما تجدر الإشارة عليه أن المشرع الجزائري من خلال نص المادة 394 مكرر 02، تم تجريم التعامل في معلومات غير مشروعة.

وأخيرا نخلص إلى أن جريمة التعامل في معلومات متحصلة من الجريمة، وتقوم على القصد الجنائي العام وحده ولا تتطلب قصد خاص.[1]

المطلب الثالث: جريمة التزوير

تُعد جريمة التزوير من الجرائم الخطيرة التي تهدد الثقة العامة، وتؤثر سلبا على استقرار المعاملات القانونية والإدارية والمالية، وهي من الجرائم التي تمس صدق الوثائق والمحررات، سواء كانت رسمية أو عرفية، إذ تقوم على تغيير الحقيقة في محرر بقصد استعماله على نحو يُلحق ضررًا بالغير أو يحقق مصلحة غير مشروعة للجاني أو لغيره.

وقد عرفت القوانين والتشريعات التزوير باعتباره فعلا إجراميا يرتكب من خلال إحداث تغيير متعمد في بيانات محرر موجود أو إنشاء محرر مزور من الأســـاس، بما يُظهره وكأنه حقيقـــي وصـادر. وسنتنـــاول في هذا المطلب ما يلي: **(الفرع الأول)** جريمـة التـــزوير، أما **(الفرع الثاني)** جريمة الغش.

الفرع الأول: جريمة التزوير

تعتبر جريمة التزوير صعبة التعريف فهناك من الفقهاء العرب من عرفها بأنها: "تغيير الحقيقة في محرر بإحدى الطرق التي نص عليها القانون من شأنه إحداث ضرر مقترن بنية استعمال المحرر المزور فيما أحده له.

أولا: تعريف المشرع الجزائري

[1] رابحة عزيزة، المرجع السابق، ص ص 170-171.

1-لغة: وهو من الزور: الميل والكذب: فالتزوير يكون في القول والفعل والكذب يكون في العقول.

فالتزوير هو محاولة تزيين الكذب وطمس الحقيقة وإلباس الباطل ثوب الحق.

2-اصطلاحا: عرفه جارو (Gareu) التزوير يتكون من تغيير الحقيقة بقصد الغش تغييرا من شأنه أن يسبب ضررًا.

وعرفه قوان (Guan) التزوير بصفته جريمة هو تزييف في الحقيقة من شأنه الإضرار ويقع في المحرر بإحدى الوسائل المبنية في القانون.

3-فقها: بأنه تغيير الحقيقة في المستندات المعالجة آليا والمستندات المعلوماتية، وذلك بنية استعمالها[1].

ثانيا: وسيلة التزوير المعلوماتي:

التزوير المعلوماتي يقع في محرر مكتوب بلغة معينة أو بطريقة الصورة، كما مر بنا وقد يقع في أي مخرجات الحاسب الآلي، ولو كان مطبوعًا على دعامة أو وسيلة غير عادية، ومن ضمنها الشرائط الممغنطة والمسجلة حتى تضمنت صورة وكانت صورة ذات أثر في المستند المعلوماتي الذي يترتب حقا أو أثر قانونيا معينا، ويتحقق التزوير عن طريق إساءة استعمال الصور، سواء كانت للإنسان أو جماد أو حيوان متى تم تغيير الصورة في الوثيقة المطبوعة على شريط أو مسجل وجرى عرضها على الحاسب الآلي.

ونصت المادة 1/144 القانون الفرنسي أن التزوير هو كل تغيير تدليس للحقيقة سواء كان في المحررات العرفية أو الرسمية.

ثالثا: تطبيقات صور التزوير عن طريق الحاسب الآلي

[1] أمال شيخي، **جريمة التزوير في التشريع الجزائري**، مذكرة تخرج لنيل شهادة الماستر، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة مولاي طاهر، سعيدة، الجزائر، 2019/2018، ص ص 16-18.

في إحدى القضايا الذي طرحت على محاكم أبو ظبي ودول الإمارات العربية، قام أحد المشتركين بشبكة الأنترنت بإدارة أبو ظبي عن طريق استخدام الماسح الضوئي لامرأة وارسالها إلى المشتركين الآخرين الذين تبدأ أسماءهم بحرف ×× من خلال البريد الإلكتروني الخاص به، وقد جرت محاكمته طبقا لمواد 2/46 و198-261-362 من ق. ع. ج، في دولة الإمارات.

فإن وقوع التزوير المعلوماتي لصورة عن طريق جهاز الحاسب الآلي ضوئيا ونقلها إلى جهاز الحاسب الآلي وإدخالها إلى البيانات المخزنة في الذاكرة، وعرضها على الشاشة دون طباعة ورقية سيما أن التزوير المعلومـــاتي لا يتطلب مستند ورقي المكتـوب أو المطبوع، ذلك أن المخرجات الحاسب الآلي والتي يظهر فيها التزوير المعلوماتي قد يكون لا ورقية.[1]

رابعا: أنواع التزوير المعلوماتي

لقد نص المشرع الجزائري على التزوير في المحررات الرسمية في المواد 214-215 و216 من ق. ع، ج، وقسمه إلى قسمين:

- نصت عليه المادتين 214-215 من ق. ع. ج، وهو التزوير من جهة المحرر أي جهة التي أصدرت الوثائق.
- نصت عليه المادة 216 من ق. ع. ج، وهو التزوير الذي يمكن أن يقع من طرف أي شخص من غير الأشخاص المذكورين في المادتين السابقين.

1-التزوير المادي: وهو الأسلوب الذي يترك أثرا ماديًا على العبث في المحرر، وقد تبين هذا الأثر بالحواس المجردة، وقد تبين بالاستعانة بالخبرة الفنية من فحص المحرر، وما يحمله من مظاهر علامات مادية، وهذه المظاهر هي من قبيل المحو الطمس، تقليد الخط الغير وبنسبة كتابة أو إمضاء إلى غير صاحبها أو اصطناع المحرر بأكمله، ويدخل هذا

[1] طاهري حسين، المرجع السابق، ص ص 92- 93.

تحت إطار إضافة شروط وإدخالها في صلب المحرر بعد انشاءه، وكذا محرر مزور بأكمله من قبل المزور، فهنا يعاقب على التزوير حتى ولو كان محتوى المحرر صحيحًا دون أن تكون هناك حاجة لإثبات تزوير الوقائع والأحكام.[1]

وتقوم جريمة التزوير بالتقليد بالمحررات العرفية والدفاتر التجارية، والأوراق الخاصة التي تطلع كمبدأ ثبوت بالكتابة أو في المحررات الرسمية كتذاكر السكك الحديدية.

2-انتحال شخصية الغير: يلحق بهذه المرتبة لتزوير المعنوي انتحال شخصية الغير سواء كان هذا الغير موجودا بالفعل أو شخصية خيالية.

مثال: أداء شخص بشهادته في جلسة بالاسم منتحل أو حضور شخص باسم آخر محكوم عليه، ليحل محله في الشغل مقابل الغرامة المحكوم بها بإثبات هذا الحضور في الأوراق الرسمية المعدة لذلك، أو انتحال شخصية الغير أمام الطب الشرعي أو في محظر تحقيق جنائي.

وانتحال شخصية الغير بالطريق المعلوماتي أمر وارد ضد التحقيق الجنائي، وذلك لأنه في التحقيق الجنائي توجد وسائل عديدة لثبت في شخصية المتهم، فهناك بصمات العادية لأصابع اليد وهناك البصمة الصوتية، وهناك الصورة الشخصية وفصيلة الدم والخلايا التي يمكن عن طريق فحصها التثبت من شخصية الإنسان، ثم هناك كذلك ما يسمى بالحامض المنوي وهو نوع من الدليل يمكن عن طريقه أن يثبت على وجه اليقين شخصية الإنسان.

خامسا: تغيير المحررات أو الأختام أو الإمضاءات أو زيادة كلمات

يقصد بهذه الطريقة كل ما يمكنه إدخاله من تغيير لطلب المحرر أو الإمضاء أو الختم الموضوع عليه، وذلك لإحداث تعديل في معناه، ويدخل ضمن هذه الطريقة زيادة كلمات على المحرر.

[1] المرجع نفسه، ص 98.

ويشترط أن يقع التغيير بالحذف أو بالإضافة أو بالتعديل بعد إتمام المحرر، وأما التغيير الحاصل أثناء التحرير فهو تزوير معنوي لامادي، ويشترط كذلك أن يقع التغيير بغير علم ذوي الشأن ولا موافقتهم إلا فإن تزوير كاتفاق المتعاقدين على زيادة عبارات في عقد عرفي أو على حذف شيء منها، ولو بعد تحريره والتوقيع عليه منهما، وتحدث الإضافة بزيادة كلمة أو اسم ورد في المحرر أو الإمضاء، أو الزيادة رقم المبلغ الموجود أو المكتوب في المحرر ويهدف الإرادة إلى تزوير ذلك المحرر واستخدامه وتغيير المعاقب عليه هو التغيير الذي تم على غير إرادة من حرر المستند أو المحرر، فلو تم بناء على اتفاق بين الموقعين دون المساس بحق الغير، حصول الاتلاف في مضمون المحرر نفسه إلا إذا تضمن ذلك مخالفة قواعد المعينة نص عليها للقيام بتحرير المستند أو ما به من بيانات على نحو يخالف الحقيقة.[1]

سادسا: الفرق بين جريمة التزوير والمفاهيم المشابهة له

1-جريمة التزوير وجريمة النصب: من وسائل النصب التي نص عليها القانون في المادة 372 ق. ع. ج[2] استعمال الطرق الاحتيالية وهي بطبيعتها تحتوي على أكاذيب أي تغيير للحقيقة، كما أن من وسائله اتخاذ اسم كاذب أو صفة غير صحيحة، ولما كان جوهر التزوير تغيير الحقيقة فكثيرا ما يختلط النصب بالتزوير، أي ما يعد تزويرا من الوقائع المعروضة على المحكمة وليس في الأمر صعوبة، إذا كانت هذه الأكاذيب واردة في المحررات فإنها قد تكون كافية لاعتبار الفعل نصبًا، لعدم توفير أركان التزوير.

2-أركان جريمة النصب: وقوع فعل مادي وهو الاحتيال بالطرق التي حددتها المادة 372 ق. ع. ج.

[1] المرجع نفسه، ص ص 95- 96.

[2]- المادة 372 من قانون 24-06 المصدر السابق.

- استلام الأموال أو المنقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو إبراء من التزامات.
- قيام رابطة شفافية بين الفعل المادي واستلام الأموال والمنقولات.
- توفر القصد الجنائي باعتبار أن الجريمة النصب جريمة عصبية.

3-جريمة التزوير وخيانة الأمانة: التزوير في المحرر هو تغيير الحقيقة بقصد الغش، وقد يحدث تغيير في المحرر بممضاة أو مختومة على بياض فملأ الفراغ فوق الإمضاء أو الختم أو التوقيع بكتابة تختلف مما حصل لاتفاق عليه من أصحاب الشأن، أو على خلاف ما قصده صاحب الإمضاء يعتبر تزويرا ماديا بطريق الاصطناع السند أو المحرر.

ولتفرقة بين ما يعد تزويرا وما يعد خيانة أمانة في ورقة ممضاة على بياض، مما يدخل في المادة 381 ق. ع. ج[1] بتعيين تحديد نطاق وفق شروط:

- وجود ورقة موقعة على بياض وسلمت للجاني على سبيل الأمان.
- فعل الخيانة وهو القيام المودع لديه الورقة بتحريره عليها، كما نصت المادة زورا التزاما أو ابداء منه أو أي تصرف آخر يمكن أن يعرض الشخص الموقع عليه أو ذمة المالية للضرر.
- وجود القصد الجنائي فجريمة خيانة الأمانة في الورقة الموقعة على بياض جريمة عمدية تتطلب أن يعلم الجاني بكافة مقوماتها المادية من جهة، وأن تتجه إرادته إلى تحقيق النتيجة.

[1]- المادة 381 من القانون 24-06 المصدر نفسه.

4-جريمة التزوير وشهادة الزور: شهادة الزور هي تعمد اليمين أو تزوير كتأكيد لقول الحقيقة، وسواء كانت مكتوبة أو منطوقة بشأن مسألة أساسية لإجراء قضائي أساسها الكذب والباطل، إلا أن شهادة الزور يتعلق بالأقوال أو التزوير يتعدى ذلك إلى الأفعال.[1]

5-الضرر: هو العنصر الجوهري في الركن المادي لجريمة التزوير هو ذلك الضرر الفعلي المباشر المنتمي إلى العالم الخارجي، وإلى نية الجاني والذي يتمثل في إهدار حق ومصلحة يحميها القانون.

أ-أنواع الضرر: يتنوع الضرر المتطلب لقيام جريمة التزوير إلى ضرر مادي، معنوي، حال، محتمل، فردي، اجتماعي.

- **الضرر المادي:** هو الذي يصيب المجني عليه في ذمته المالية إذ أن كل ما يمس عناصر الذمة المالية يؤدي إلى الإنقاص من عناصرها الإيجابية أو الزيادة في عناصرها السلبية أو المديونية، وهذا النوع يضر كثير للوقوع في الحياة العملية لأن المزور يستهدف في أغلب الأحيان سلب وثروة الغير، وعلى سبيل المثال: عقد بيع أو إيجار أو اصطناع سند دين.

- **الضرر المعنوي:** هو ما يصيب الشخص في سمعته أو اعتباره ومكانته الاجتماعية مثال: أن يضع شخص محررا ينسبه إلى شخص ويضمن اعترافا بارتكاب الجريمة، أي أن يقوم شخص بتزوير عقد الزواج عرفي، والممرضة التي تسجل طفلاً تحت اســم غير والديه، وتسمى باسم الغير في تحقيق الجنائي.

- **الضرر الحال:** هو الذي يحقق فعلا، ويتم ذلك باستعمال المحرر المزور فيها زور من أجله.

- **الضرر المحتمل:** هو الذي لم يقع بعد ولكن يحتمل وقوعه، ولا يشترط لقيام جريمة التزوير أن يكون الضرر قد وقع فعلاً بل يكفي أن يكون محتمل وقوعه.

[1] أمال شيحي، المرجع السابق، ص ص 23- 28.

- **الضرر الفردي:** هو الضرر الذي يلحق بالفرد أو هيئة خاصة سواء كان ماديا أو معنويا حالا أو محتملا.

- **الضرر الاجتماعي:** هو ما يصيب الصالح العام في مجموعة دون أن يصيب فردا بذاته أو هيئة خاصة والضرر الاجتماعي الناتج عن التزوير المحـررات قد يكـون ماديا أو معنويا، مثال: تزوير سداد الرسوم أو الضرائب أو الغرامة، دخول شخص الامتحان باسم شخص آخر أو من ينتحل شخصيته المحكوم عليه بعقوبة لينفذها بدلا عنه[1].

ب-التزوير بطريقة الاصطناع: التزوير بهذه الطريقة أمر وارد إذ يمكن للجاني أن يدخل ما يريد من المعلومات أو البيانات إلى جهاز الحاسب الآلي، وينسب صورها على شخص ما أو جهة ما ثم يقوم باستخراجها من جهاز الحـــاسب الآلي بوصفهـــا منسوبة إلى ذلك الشخـــص أو تلك الجهة، وكذلك تزوير النقود الورقية بطريقة الحاسب الآلي تعد من طرق الاصطناع كما هي من التقليد، وذلك لأن الاصطناع على خلق المحرر بأكمله وتشبيه إلى غيره وليس هناك صعوبة في عملية إدخال عناصر المحرر المراد تزويره إلى جهاز الحاسب الآلي سواء عن طريق الماسح الضوئي أو عن طريق لوحة المفاتيح، بل عن طريق استدعاء المعلوماتي في شبكة المعلومات الدولية تم صياغتها في هيئة المحرر المزور الذي يطبعه الجاني، ويعد ذلك خارج الجهاز واستعماله إن رغب في ذلك بوقوع التزوير المعلوماتي بهذه الطريقة هو أمر ممكن في ظل التقديم العلمي لجهاز الحاسب الآلي وملحقاته.

- **الركن المعنوي:** يقع التزوير المعنوي بإحدى الطرفين:

1-تغيير إقرار أولى الشأن.

2-جعل واقعة مزورة في صورة واقعة صحيحة، أو واقعة غير معرفة بها في صورة واقعة معرف بها[2].

---

[1] محمد الشريف بولعراس، **جريمة التزوير المعلوماتي**، مذكرة لنيل شهادة الماستر، تخصص قانون، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعريريج، الجزائر، 2022/2021، ص ص 53- 54.

[2] المرجع نفسه، ص 46.

- **تغيير إقرار أولي الشأن:** تتحقق هذه الطريقة حين يقوم كاتب المحـــرر بتغير البيانـــات التي تطلب منه كتابتها، وكذلك عند تدوينها والجاني لا ينسب كل بيانات المحرر المزور لنفسه، بل ينسب بعضها للغير ثم أنه يخالف ما أملاه عليه الغير وبدون بيانات مخالفة أو مشوقة فيغير مضمونة المحرر، ولذلك فهذه الطريقة لا تتيسر إلا عند انشاء المحرر فضلا عن صعوبتها في الاثبات، إذ لا يتيسر ذلك سوى بمقارنة ما كتبه الجاني مع من كان يجب عليه أن يكتبه أو إثبات ما كان يجب عليه أن يكتبه أمر صعب.

وقد يتصور قيام الموظف العام بتغيير الحقيقة في البيان البنكي الذي يحصل على بياناته من ذوي الشأن أو فاتورة تلفون، فثبت سداد جزء منها على حين أن صاحب الشأن سددها كاملة إذ ثبت سددها كاملة، إذ أثبتت التسوية المالية لمعاملات أحد العملاء في البنك من البنوك بالمخالصة الحقيقية وكل ذلك يتم عند انشاء المستندات المثبتة للمعاملات أو التي تبرئ ذمة ذوي الشأن، وذلك عن طريق الحاسب الآلي الذي تداخل في حياتنا على نحو مستحيل الخلاص منه.

والحاصل مما سبق أن تغيير اقرارات ذوي الشأن كطريقة التزوير المعنوي ليس هناك صعوبة في وقوع التزوير المعلوماتي بها سواء كان ذلك في محرر الرسمي حرره موظف عام في محرر عرفي لعلاقات الأفراد فيما بينهم والأمر متوقف على انتشار مظاهر المعلوماتية في حياتنا اليومية[1].

- **جعل الواقعة مزورة في صورة واقعة صحيحة:** ومن تطبيقات محكمة النقض في شأن تزوير المحررات الرسمية بهذه الطريقة ما نصت بتوافر عندما يثبت المحقق في المحضر التحقيق أنه لم يعثر في مسكن المتهم على أشياء تفيد في اثبات الجريمة، في حين أنه عثر على هذه الأشياء بالفعل أو أن يثبت المؤدون خلو الزوجية من الموانع الشرعية، في حين أن هذه الموانع متوفرة ومن مقصود أن يقدم الموظف–الميكروفيلم والمطلوب منه تدوين

[1] المرجع نفسه، ص 49.

الحكم وتوثيقها في نظـــام الحفظ المعروف، بالميكروفيلم بالتلاعب في مضمون الحكم على غير الحقيقة وتعد النسخة المحفوظة غير مطابقة للحكم الصادر، وأن يقوم الموظف المختص بتقرير الرسوم في الدعاوي المدنية بالقضاء العادي أو الإداري لمجلس الدولة بالتلاعب في مقدار الرسم المطلوب دفعة توصلا لتخفيف أو تشديد الرسم قبل المدعي المدني، وذلك بمقتضى قسيمة التي يستخرجها من الحاسب الآلي الذي يدون عليه هذه البيانات، وهناك أخطاء قد تحدث في التحقيق الجنائي العادي تعد تزوير كإثبات واقعة معينة أو خطأ عن عمد في تدوين اسم المتهم أو مكان حصول الواقعة أو زمانها، أو وقت تنفيذ الإجراء الجاني على نحو يفيد المتهم أو يضره، وكل هذه الوقائع كما يحدث التـلاعب فيها في التحقيـق الجنائي الورقـــي، أي المكتوب، فمن الوارد وقوعها في التحقيق المعلوماتي أو التحقيق الجنائي على بعد، ويعد نموذجا مثاليا لجعل واقعة مزورة في صورة واقعية صحيحة بالطريق المعلوماتي:

ج-التزوير المحررات العرفية: يقوم التزوير في المحررات العرفية متى أثبت محصل في شركة تجارية المبالغ التي حصلها عن عمالة في دفتر القسائم بأقل من المبالغ التي قبضها المتهم، وتقع بطريقة الحاسب الآلي[1].

سابعا: أركان جريمة التزوير المعلوماتي

1-الركن المادي: هو الوقوع في نشاط إجرامي من شأنه تغيير الحقيقة في محرر بطريقة ما، ونص عليه القانون وأن يكون من شأن هذا التغيير إلحاق الضرر بالغير، أو احتمال حدوثه وفق شروط هي:

أ-تغيير الحقيقة: هو الأساس الذي يقوم عليه جريمة التزوير كأن يقوم أحدهم بإثبات بيانات مطابقة للحقيقة، فلا تقوم جريمة التزوير حتى ولو كان ذلك الشخص يعتقد بعدم صحة هذه البيانات وحتى ولو ترتب عليه فعله ضرر في حق الغير، فتغيير الحقيقة يجد

[1] المرجع نفسه، ص 50.

نطاقه في استبدال للحقيقة بما يخالفها، بمعنى إدخال تغيير على المحرر المراد تزويره على نحو يغير مضمونه أو شكله[1].

ومما تجدر الإشارة إليه أن التزوير المعلوماتي لا يتم من قبل مشغل الحاسب الآلي فحسب، وإنما أن يقع من شخص عادي ليس له أي دراية بتشغيل الكمبيوتر ولا يتمتع بأي قدر من الكفاءات والمهارات الفنية والعلمية لتشغيل هذا الجهاز الإلكتروني، ومع ذلك فإنه يرتكب التزوير المعلوماتي، كما هو الحال بالنسبة لشخص الذي يعتمد على فتح حساب جاري فيقوم باستعمال اسم شخص آخر أو الانصاف بصفة ليست له، أو بتقرير وقائع كاذبة أو أي أمر من شأن المستند المبرمج إثباته.

ب-وجود محرر إلكتروني: أن يتخذ المحرر شكلا كتابيا، لما هو محرر فيجب أن يكون مكتوبا وبأي لغة فقد تكون لغة محلية أو أجنبية.

ج-أنواع الكتابة:

- الكتابة المستبنية المرسومة وهي ظاهرة معنوية التي يكون لها بقاء بعد الفراغ منها ويمكن قراءتها وفهم معناها، مثل: أن يكتب في أعلى الورقـــة من فلان إلى فلان، وهذا النوع أعلى درجات الكتابة وهو مقبول لدى جميع المذاهب ويصح به التصرف كالبيع والإجار والزواج والطلاق...إلخ.

- الكتابة المستبنية غير المنسية وهي ظاهرة غير معنوية، أي هي المكتوبة على شيء فتظهر وتثبت عليه كالكتابة على الورق أو على اللوح، ولكن غير معنية بالاسم المرسل والمرسل إليه.

2-أن يحدث المحرر أثر قانونيا:

[1] المرجع نفسه، ص 32.

أ-مدى انطباق معنى المحرر على المحرر الإلكتروني: ذكر المقنن 323 مكرر من قانون الجزائري يعرف فيها لإثبات بالكتابة على أنها إنتاج لإثبات بالكتابة من تسلسل الحروف × وأوصاف وأرقام، وأي علامات أو رموز ذات معنى مفهوم.

وبصدور القانون 05-10 المعدل والمتمم للقانون المدني الجزائري انتقل المشرع من النظام الورقي إلى النظام الإلكتروني قيمة الوثيقة المعلوماتية في الإثبات. [1]

ب-الركن المعنوي لجريمة التزوير المعلوماتي: تعد الجرائم في المحررات من الجرائم العمدية، ولذلك يتخذ ركنها المعنوي صورة القصد الجنائي.

-**القصد الجنائي العام:** يقوم القصد العام على العلم والإرادة، فهو يتطلب علم جنائي بتوافر جميع أركان التزوير، وإرادته لتحقيق النشاط الإجرامي والنتيجة المترتبة عليه، ويعني ذلك ضرورة انصراف علم الجنائي إلى أنه يغير الحقيقة بطريقة من الطرق التي حـــددها القانون، كما يجب أن يتصرف أثر هذا التغيير هو أحدث الضرر للغير أو احتمال حدوثه.

- **القصد الجنائي الخاص:** يلزم توافره في التزوير المادي أو المعنوي، فالقصد لا يغير تبعا لطريقة ارتكاب التزوير، واستعمال المحرر المزور فيما غيرت الحقيقة من أجله ولا يشترط توافر هذا القصد أن يستعمل هذا المحرر المزور فعلا، فيكفي أن يكون هذا الاستعمال هو غاية الجاني وقت تغيير الحقيقة[2].

الفرع الثاني: جريمة الغش المعلوماتي:

إن دراسة جريمة الغش المعلوماتي تعد من الموضوعات البالغة التعقيد، وذلك لارتباطها بالحاسب الآلي واستخدامه إلى جانب تعدد صور هذه الجريمة.

أولا: أركان جريمة الغش المعلوماتي

[1] المرجع نفسه، ص ص 35- 37.

[2] أمال شيخي، المرجع السابق، ص ص 45- 47.

1-الركن المادي: يتجسد الركن المادي في جريمة الغش المعلوماتي من خلال نص المادة 394 مكرر 01 من القانون رقم 04-15 في عملية إدخال، وبطريقة الغش معطيات في نظام المعالجة الآلية أو إزالة أو تعديل بطريقة الغش المعطيات التي يتضمنها، والمساس بالمنظومة المعلوماتية، ومن خلال دراسة الركن المادي للغش المعلوماتي لابد من توضيح مسألة إن كانت هذه الجريمة وقتية مستمرة[1].

2-الركن المعنوي:

أ-القصد الجنائي العام في جريمة الغش المعلوماتي: من خلال نص المادة 394 فإن الغش المعلوماتي لا يتحقق بالخطأ، كما لو توصل أحدهم مصادقة أو عن طريق الخطأ مع النظام واستمرار البقاء داخله مع علمه واتجاه إرادته، ويتطلب الغش المعلوماتي في صورة التلاعب بالمعلومات نظام معالجة قصد جنائيا عاما وذلك بحسب ما ورد في المادة 394.

ب-القصد الجنائي الخاص في جريمة الغش المعلوماتي: إن جريمة الغش المعلوماتي، لا تتطلب قصدًا جنائيًا خاص مثل قصد الإضرار أو نية الاضرار بالغير، فهذا الجانب يعتبرها من جرائم الخطر وليست من جرائم الضرر.

إلا أن الغش يكون عند معرفة الشخص بغياب حق الدخول أو البقاء في نظام المعالجة الآلية، ونستنتج أن جريمة الغش المعلوماتي تتطلب القصد الجنائي العام بجانب القصد الجنائي الخاص، كل أشكال الاعتداء على وظيفة الحاسب الآلي بنية الغش، أو أي نية إجرامية مشابهة للغش[2].

ثانيا: خصائص جريمة الغش المعلوماتي

[1] فادية عليوان، **جريمة الغش المعلوماتي في التشريع الجزائري**، مذكرة لنيل شهادة الماستر، قانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة مولاي الطاهر، سعيدة، الجزائر، 2015/2014، ص 13.

[2] المرجع نفسه، ص ص 28-29.

- الخسائر المادية الناجمة عنها كبيرة جدا قياسا بالجرائم التقليدية خاصة جرائم الأموال، وترتكب من فئات متعددة تجعل من التنبؤ فيه أمر صعب تنطوي على سلوكات غير مألوفة.

1-جريمة الغش المعلوماتي ذات طابع عالمي: ترتكب في إطار مجتمع معلوماتي لا يعترف بالحدود الجغرافية، فعالمية الشبكات التي من بينها شبكة الأنترنت التي تغير أساس المجتمع المعلوماتي، التي تسهل ارتكاب جريمة الغش المعلوماتي من دولة إلى أخرى، فهي تغيير شكل جديد من الأشكال العابرة للحدود.

2-صعوبة اثبات جريمة الغش المعلوماتي: إن إثبات جريمة الغش المعلوماتي أمر صعب جدا لأنها لا تترك أثر يصعب فنيا الاحتفاظ بآثارها أن تركت أثر، كذلك يصعب في هذا النوع من الجرائم على المحقق التقليدي أن يفهم حدودها الإجرامية وما تخلفه من أثار غير مرئية، وذلك لاعتمادها على الذكاء ومن جهة الخداع والتظليل في التعرف على مرتكبها من جهة أخرى[1].

المطلب الرابع: صور الاعتداء على المصنفات المعلوماتية-الرقمية-

في عصر الثورة الرقمية والانفجار المعلوماتي، أصبحت المصنفات المعلوماتية-مثل البرمجيات، قواعد البيانات، المواقع الالكترونية، الكتب الرقمية، والتطبيقات، من أهم الموارد التي يعتمد عليها الأفراد والمؤسسات على حد سواء، ومع تنامي هذه الأهمية، تزايدت صور الاعتداء على هذه المصنفات، مما يشكل انتهاكا صارخا للحقوق الفكرية والقانونية لأصحابها.

تتنوع صور الاعتداء على المصنفات المعلوماتية فقد تشمل نسح المحت. في هذا المطلب تطرقنا إلى **(الفرع الأول)** الاعتداء على المصنفات المعلوماتية، أما **(الفرع الثاني)** صور وأشكال الاعتداء غير مباشر على المصنف.

الفرع الأول: الاعتداءات على المصنفات المعلوماتية

[1] المرجع نفسه، ص ص 31- 32.

إن مبدأ العام لحماية حقوق الملكية الفكرية سواء أدبية أو فنية أو حقوق الملكية الصناعية هو حماية الحقوق المترتبة لأصحابهـــا على مصنفـــات أو ابتكارات مهما كانت، ومتى تميزت بالأصالة بالنسبة لحقوق التأليف ومتى تميزت بطابع الابتكار وقابليتها لتطبيق الصناعي واستفاء الشروط الشكلية بالنسبة للبراءة والرسوم والنماذج، أما بالنسبة للعلامات فمتى توفرت فيها الشروط الموضوعية والشروط الشكلية.

ولا شك أن هذا المبدأ يمتد حتى فيما يخص استغلال هذه الابتكارات، والمصنفات عبر الأنظمة المعلوماتية المختلفة أو ثبتها إلكترونيا.

وبالتالي يقتصر التجريم على انتهاكات حقوق المؤلف والحقوق المجاورة، وإذا ما تم ارتكابها عن طريق نظام معلوماتي وعلى نطاق تجاري.

كما أن اتفاقية العربية لمكافحة لجرائم تقنية المعلومات المحررة بالقاهرة 2010 نصت على تجريم الانتهاكات المتعلقة بحقوق المؤلف والحقوق المجاورة في المادة 07.

وأما المشرع الجزائري فلقد تعرض بصفة عامة للجرائم الواقعة على حقوق المؤلف المتمثلة في جريمة التقيد في الأمر 03-05 تحت عنوان أحكام جزائية.

أولا: الاعتداء على الحق الأدبي لمؤلف المصنف:

لم ينص المشرع الجزائري على جميع الاعتـداءات الواقعـــة على كـــل حقوق المؤلف، وإنما جرم البعض منها ضمن أحكام المادة 151 من قانون المؤلف حقوق المجاورة[1].

1-الكشف غير المشروع للمصنف: للمؤلف المصنف الحق وحده في الكشف عن مصنفه باسمه الخاص أو باســم مستعار، كما يمكن له تحويله للغير ويعود هذا الحق إلى ورثته بعد وفاته المادة 22 من الأمر 03-05.

[1] صورية بوربابة، **قواعد الأمن المعلوماتي**، أطروحة دكتوراه في العلوم، تخصص قانون خاص، كلية الحقوق والعلوم السياسية، جامعة سيدي بلعباس-الجزائر-، 2015-2016 ص ص 167- 166

2-المساس بسلامة المصنف: حق تعديل أو تغيير أو حذف أو إضافـة في مصنف ما يمكن كذلك للمؤلف وحده، ولا يمكن للغير الاعتراض على ذلك ما لم يكن فيه إخلال أو مساس بمصالحهم، فمن يرتكب أحد الأفعال السابقة يتوافر بحقه النشاط الإجرامي لجريمة التقليد.

3 -الاعتداء على الحقوق المالية لمؤلف المصنف: تقع أفعال الاعتداء على الحق المالي لمؤلف المصنف باستغلاله أيا كانت صورة هذا الاستغلال سواء بالنسخ أو الاستعمال أو الترجمة سواء وقع النسخ كليا أو جزئيا، ويقع جرم النسخ أيضا سواء تم النسخ المصنف باسم مؤلفه الحقيقي أو باسم شخص آخر، أو باسم الجاني نفسه أو باسم خيالي، ويدخل في حكم الاستنساخ تثبيت برمجية في جهاز آخر غير مرخص به لتثبيت في الاستنساخ غير المشروع، ومن ذلك ما قضت به المحكمة الإصلاحية.

فإذا كان من حق المؤلف أو من له الحق المالي على المصنف هو وحده المخول بإجراء النسخ وبأي شكل أو وسيلة كانت، إلا أن المشرع الجزائري لم يعطه هذا الحق على إطلاقه، ويظهر ذلك من خلال الاستثناءات الواردة في الأمر 03-05 فيما يخص المواد 41-51، وكذا فيما يخص استنساخ برامج الحاسب الآلي دون إذن من مؤلفها بموجب المادتين 52-53 من الأمر 03-05.[1]

4-قيام الفعل دون موافقة صاحب المصنف: لا يكفي توافر النشاط أو السلوك الإجرامي لأفعال التقليد، بل يشترط إلى ذلك عدم موافقة صاحب المصنف على تلك الأفعال.

ولقد اشترط المشرع الجزائري ضرورة الإذن الكتابي من المؤلف يتنازل به عن حقوقه المادية وذلك طبقا للمادة 62 من الأمر 03-05، إذ تعتبر كتابة الإذن شرط وجود لقيام التصرف ولا شرط إثبات، كما أن الإذن اللاحق على عملية الاستنساخ أو التقليد لا يمكن أن يأخذ

[1] المرجع نفسه، ص 169.

حكم الإذن السابق، وبالتالي موافقة صاحب المصنف بعد تمام الجريمة لا تحول دون متابعته.

5-وقوع الاعتداء بواسطة نظام معلوماتي: لاعتبار الاعتداءات الواقعة على حقوق الملكية الفكرية والحقوق المجاورة كشكل من أشكال الإجرام المعلوماتي ويشترط أن تتم بواسطة نظام معلوماتي، وهذا الشرط مفترض حتى وإن لم يتم النص عليه صراحة ذلك أن النظام المعلوماتي أو الشبكة المعلوماتية جزء من الجريمة المعلوماتية، وبالرجوع إلى التشريع الجزائري نجد أن المشرع وسع من دائرة التجريم لصورة جنحة التقليد كل من ينتهك الحقوق المحمية بموجب الأمر، فيبلغ المصنف أو الأداء عن طريق أو بأي وسيلة نقل أخرى للإشارات تحمل صوتا أو صورا أو أصواتا بأي منظومة معالجة آلية.

وأخيرا تبليغ المصنف بدون إذن صاحبه أو من له حق علية بأي وسيلة بما فيها منظومة المعالجة الآلية بشكل جريمة تقليد وتخضع لجزاء جرائم الملكية الفكرية[1].

الفرع الثاني: صور وأشكال الاعتداء غير المباشر على المصنف

حدد المشرع الجزائري الجرائم الملحقة بجريمة التقليد في المادة 151* الفقرة 3-4-5 من الأمر 03-05.

أولا: استيراد وتصدير مصنفات مقلدة

جرم المشرع الجزائري في الفقرة 3 المادة 151 أفعال التصدير والاستيراد المصنفات أو أداة مقلدة من وإلى الجزائر، وبالتالي التوسيع من صور جريمة التقليد.

---

[1] المرجع نفسه، ص 70.

* تنص المادة 151 من الأمر 03-05 :" يعد مرتكبا لجنحة التقليد كل من يقوم بالأعمال الآتية: -الكشف غير المشروع للمصنف أو المساس بسلامة مصنف أو أداء لفنان مؤد او عازف.

- استنساخ مصنف أو أداء بأي اسلوب من الأساليب في شكل نسخ مقلدة.
- بيع نسخ مقلدة لمصنف أو أداء
- تأجير أو وضع رهن التداول لنسخ مقلدة لمصنف أو أداء.

كما يعتبر التقليد مجرد عرض المصنفات المقلدة المستوردة، أو إعدادها بغرض تصديرها سواء تعلق الأمر بمصنفات وطنية أو أجنبية.

ثانيا: تتبع أو تأخير أو وضع رهن التداول المصنفات مقلدة

البيع بموجب التشريع وهو الذي يتم بمقتضاه نقل حق استغلال مصنف مقلد إلى المشتري مقابل ثمن، أما التأجير فهو وضع المصنف المقلد أو نسخ منه لدى الغير القصد تمكينه من استعمالها والانتفاع منها لمدة معينة مقابل دفع أجر مالي.

وتقوم جريمة التقليد حتى يتداول المصنف المقلد، بإعطائه لشخص ما لمشاهدته حتى ولو لم يكن ذلك بثمن.

ثالثا: رفض إعطاء مكافآت المستحقة للمؤلف أو لصاحب الحق

انفرد المشرع الجزائري بهذه الصورة من جرائم التقليد عن باقي التشريعات وأخضعها لنفس عقوبة التقليد المباشرة، والأصل في استغلال المصنف أن يكون بمقابل مادي أو بما يسمى بالمكافآت المستحقة لصاحب المصنف عن حق من حقوقه المادية سواء كليا، أو بصفة مؤقتة وفي حالة امتناع الشخص المكلف بدفع المكافأة المستحقة.

وما يمكن ملاحظته كذلك على تفرد المشرع الجزائري بهذه الصورة أنه لم يولي اهتماما لصور أخرى قد شكل اعتداءات أو انتهاك لحق المؤلف في ظل الثورة التكنولوجية، من بينها القيام بفك أو تعطيل أو إزالة عن قصد أو بسوء نية لأي حماية يستحقها صاحب المصنف أو الأداء لتشفير مصنفه الموجود على شبكة الأنترنت، أو أي نظام معلوماتي آخر.[1]

خلاصة الفصل:

نستنتج في الأخير أن نظام الأمن المعلوماتي من أهم التقنيات الحديثة التي يجب على كل مؤسسة تبنيها والسير في نمطها، فهذا الأخير يقوم بتقييم مدى كفاءة وفعالية

[1] صورية بورباية، المرجع السابق، ص ص170-172.

المؤسسة داخليا، إضافة إلى الأساليب والخطوات اللازمة اعتمادها لضمان حماية كافية لمختلف البيانات والمعلومات من الجريمة المعلوماتيـــة وخطورتها على الأمـــن المعلوماتي، فالجريمة المعلوماتية لها آثار سلبية وهي عابرة للحدود، وتعرف بالجرائم المرتبطة بتكنولوجيات الإعلام والاتصال لكونها سهلة الارتكاب نتيجة للاستخدام السلبي لتقنية المعلومات، بما توفره من تسهيلات ومرتكبو هذه الجرائم يتسمون بالذكاء والدراية في التعامل والمهارات في المعالجة الآلية للمعطيات

المعلوماتية الرقمية، ويلجئون إلى مختلف الأساليب للوصول إلى المعلومات المخزنة في ذاكرة المعلومات، كجريمة الدخول وبقاء غير مصرح بهما وتعامل غير مشروع والغش والاعتراض وتزوير وغيرها من جرائم، وهذه الجرائم قد تكون منقولات معنوية بما فيها المعلومات والبيانات وحق الملكية.

ومن مخاطرها انتهاك خصوصية الأشخاص، والتعدي على أسرارهم نتيجة الاعتماد الكبير للأفراد على الوسائل التكنولوجية لحفظ بيانـــاتهم ومعلومـــاتهم الشخصية والماليـــة، التعدي على قيم الأخلاقية والتحريض على الدعارة، وذلك نتيجة تيسير نقل الصور، تهديد البيئة الاقتصادية لدول وذلك بتسهيلها عملية السطور الإلكتروني على الودائع والأموال الخاصة بالمؤسسات المالية والحكومية والاقتصادية، كجرائم النصب والاحتيال الإلكتروني، واختراق الأنظمة الإلكترونية لدول بغرض اتلاف وتعطيل وإيقاف تلك الأنظمة على العمل.

الفصل الثاني

الإطار القانوني للأمن المعلوماتي في الجزائر

تمهيد:

شهد العالم تطورا كبيرا في مجال تكنولوجيا المعلومات والاتصالات، ما أدى إلى ظهور نوع جديد من الجرائم يعرف ب " الجريمة المعلوماتية " أو الجريمة الإلكترونية" والتي ترتكب باستخدام الوسائل الإلكترونية أو تستهدف بها نظم المعلومات. وقد أصبحت هذه الجرائم تشكل تحديا حقيقيا للأمن القانوني والاجتماعي والاقتصادي، لما لها من طابع عابر للحدود، وصعوبة في إثباتها وكشف مرتكبيها. وفي الجزائر أدرك المشرع خطورة هذا النوع من الجرائم فسعى إلى وضع إطار قانوني لمواجهتها من خلال سن نصوص قانونية خاصة وتنظيمية تهدف إلى مكافحة هذا النوع من الجرائم من أبرزها القانون رقم 18-04 [1] المتعلق بحماية نظم المعلومات.

ويهدف هذا البحث إلى تسليط الضوء على الآليات والأساليب التي تبناها المشرع لمواجهة جرائم المعلومات، ذلك من خلال تقسيمنا لهذا الفصل إلى مبحثين كالآتي:

المبحث الأول: أليات تحقيق أمن المعلومات في الجزائر

المبحث الثاني: الأساليب الإجرائية لحماية قواعد الأمن المعلوماتي

[1]- القانون 18-04، المؤرخ

المبحث الأول: آليات تحقيق أمن المعلومات في الجزائر

الجزائر ليست بمنأى عن الثورة التي أحدثتها المعلوماتية لهذا كان لزاما على المشرع الجزائري أن يسايرها بإحداث تعديل في قانون العقوبات ومن أسباب هذا التعديل أن التقدم التكنولوجي وانتشار وسائل الاتصال الحديثة أدى إلى إبراز أشكال جديدة من الإجرام مما دفع بالكثير من الدول إلى بذل جهود لتوفير الحماية الجزائية للأنظمة المعلوماتية.

وإن الجزائر على غرار هذه الدول تسعى من خلال هذا المشروع إلى النص على معاقبتها وتوفير حماية جزائية للأنظمة المعلوماتية وأساليب المعالجة الآلية للمعطيات وأن هذه التعديلات من شأنها سد الفراغ القانوني في بعض المجالات وسوف يمكن لامحالة من مواجهة بعض أشكال الإجرام الجديد فكانت المحاولات من الحد من هذه الظاهرة المستحدثة بتأمين المعلومات المتداولة عبر شبكة الأنترنت من المخاطر التي تهددها.[1]

وسنتطرق من خلال هذا المبحث إلى الأليات القانونية والمؤسساتية من خلال تقسيمنا هذا المبحث إلى مطلبين حيث يضم **(المطلب الأول)** الآليات القانونية (التشريعية)، أما **(المطلب الثاني)** يتضمن الآليات المؤسساتية.

المطلب الأول: الأليات القانونية (التشريعية)

لعل من أهم الأساليب القانونية والتقنية وحتى الفنية التي استحدثتها الدول والمجتمع الدولي، لمحاولة تفادي الوقوع في هذا النوع من الجرائم، تتمثل في القوانين التي استحدثتها هذه الدول، تماشيا مع التطور التكنولوجي والمعلوماتي وتغلغله في جميع ميادين الحياة

[1] فشار عطا الله، **مواجهة الجريمة المعلوماتية في التشريع الجزائري**، الملتقى المغربي حول القانون والمعلوماتية، اكاديمية الدراسات العليا، ليبيا، أكتوبر، 2009، ص 35.

والتي أصبحت تشكل خطر على هذه المجتمعات، مادامت تهدد خصوصيات وأمن المعلوماتي لدول وأفراد على حد سواء.[1]

هذا ما سيتم بيانه في هذا المبحث من خلال بيان الأساليب الإجرائية التي استحدثها المشرع الجزائري في هذا المجال، حيث قسمنا هذا المطلب إلى ثلاث فروع حيث يضم **(الفرع الأول)** الأمن المعلوماتي في قانون العقوبات، أما **(الفرع الثاني)** يتضمن القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها و**(الفرع الثالث)** يضم القانون 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة.

الفرع الأول: الأمن المعلوماتي في قانون العقوبات

المعدل بموجب القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004 المتعلقة بالمساس بالشبكة المعلوماتية والذي تضم ثلاثة أصناف هيا:

-الجرائم المتعلقة بالمساس بالسرية ووحدة وأمن المعطيات في نظام ما.

-التزوير المعلوماتي والمساس بالمعطيات.

-الجرائم المتعلقة بالبحث والجمع والحيازة أو بث أو التجارة بالمعطيات.

حيث يعتبر قانون العقوبات وسيلة ردعية للكف عن ارتكاب الجرائم بصفة عامة، وبما أن الجرائم المعلوماتية تلحق أضرار بالغير فقد أقر المشرع عقوبات ردعية لتلك الجرائم.

وقد استحدث المشرع الجزائري مجموعة من العقوبات لمرتكبي الجرائم الالكترونية من خلال مجموعة من المواد القانونية. فقد تضمن المادة 394 مكرر مجموعة من العقوبات التي تتراوح بين الحبس من ستة (6) أشهر إلى سنتين (2) وبغرامة من 60.000دج إلى 200.000دج، كل من للمعالجة الآلية للمعطيات أو يحاول ذلك.

[1] حوالف عبد الصمد، "**الأليات القانونية لتلافي الجريمة المعلوماتية والحد من انتشارها وفقا للتشريع الجزائري**"، مجلة الفكر القانوني والسياسي، كلية الحقوق والعلوم السياسية جامعة تلمسان، العدد 4، 2018، ص91.

حيث تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المعلومة. إذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة، تكون العقوبة الحبس من سنة (1) إلى ثلاث (3) سنوات والغرامة من 100.000دج إلى 300.00دج. كما نصت المادة 394مكرر1 على أن يعاقب بالحبس من سنة (1) إلى ثلاث (3) سنوات وبغرامة من 500.000دج إلى 2.000.000دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الالية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها. أما المادة 394 مكرر2 تنص على أن يعاقب بالحبس من سنة(1) إلى (5) سنوات وبغرامة 1.000.000دج إلى 5.000.000دج، كل من يقوم عمدا وعن طريق الغش ونصت لمادة 394 مكرر3 على " يعاقب بالحبس من سنتين (2) على عشر (10) سنوات وبغرامة من 700.000دج إلى 2.000.000دج، إذا استهدفت الجرائم المنصوص عليها في هذا القسم الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الاخلال بتطبيق العقوبات الأشد".[1]

أما فيما يتعلق بأنشطة الإنترنت المجسدة لجرائم المحتوى الضار والتصريف القانوني:

نصت مواد القسم السابع مكرر من ق ع خاصة المادة 394 مكرر2/2 على تجريم أفعال الحيازة، الإفشاء والنشر التي تطرأ على المعطيات الآلية بهدف المنافسة غير المشروعة، وذلك بعقوبتي الحبس والغرامة إضافة إلى ما نصت عليه المادة 394 مكرر 6 بتوقيع عقوبة تكميلية في غلق المواقع التي تكون محلا لجريمة من الجرائم المنصوص عليها في القسم الرابع مكرر من قانون العقوبات الجزائري. [2]

[1] المواد من 394 إلى 394مكرر3 من القانون رقم 24-06 مؤرخ في 28 أبريل 2024، المتضمن قانون العقوبات، ج. ر، ج. ج. د ش، العدد 30، 28 أبريل 2024.

[2] المواد 394مكرر 2و394مكرر 6 من قانون 04-15 المؤرخ في 28 أبريل 2024، المتضمن قانون العقوبات، المصدر نفسه

تمثل الجزاءات المقررة بموجب الفصل السابع مكرر في العقوبات الأصلية وهي: عقوبة الحبس والغرامة، وعقوبات تكميلية بموجب نص ا المادة 394 مكرر6 والمتمثلة في: إغلاق المواقع والمحل وأماكن الاستغلال ومصادرة الأجهزة والبرامج والوسائل المستخدمة سواء إن كانت الجريمة قد ارتكبت بعلم مالكها، ومثال ذلك إغلاق مقهى الانترنت الذي ترتكب فيه الجرائم بشرط علم مالكها وقد أورد المشرع ظروفا نشدد بها العقوبة للجريمة وهي:

– حالة الدخول والبقاء غير المشروع إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة أو تخريب للنظام

– إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام المواد:

394،152/ مكرر، و394 مكرر 2 من قانون 15–04 المؤرخ في 2004/11/10 أكد المشرع الجزائري أيضا بموجب المادة 394 مكرر5 على تجريم الاشتراك (سواء شخص طبيعي أو معنوي) في مجموعة اتفاق بغرض الاعداد لجريمة من جرائم الماسة بالأنظمة المعلوماتية –بعقوبة الجريمة –بفعل أو بعدة أفعال مادية وكان التحضير مجسد، أي بمعنى آخر فإن المشرع استثنى العقاب على الاعمال التحضيرية للجرائم المعلوماتية المرتكبة من طرف شخص منفرد.[1]

كما تنص المادة 394 مكرر4 من ق ع على الجرائم المعلوماتية للشخص المعنوي حيث أقر المشرع الجزائري المسؤولية الجزائرية للأشخاص المعنوية، وشدد عقوبة الغرامة في جرائم الاعتداء على نظم المعالجة الآلية، حيث أن الغرامة المطبقة على الشخص المعنوي تتراوح بين واحد إلى خمس أضعاف الغرامة المقررة على الشخص الطبيعي.

[1] علاوي محمد، المرجع السابق، ص64.

والعقاب على الشروع في الجريمة المعلوماتية طبقا لنص المادة 394 مكرر 7 من قانون العقوبات: أن فعل الشروع او البدء في ارتكاب الجريمة يعاقب عليه بنفس العقوبة المقررة للجنحة ذاتها، ونظرا لكون جرائم الاعتداء على نظام المعالجة الآلية ذات وصف جنحي أقر المشرع العقاب لها بمثل الجريمة نفسها.[1]

الفرع الثاني: القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها

يحتوي القانون 09-04 على 19 مادة موزعة على ستة فصول ومستمدا بنوده من الاتفاقيات الدولية خاصة منها بوداباست حول الجرائم المعلوماتية 2001. بالإضافة إلى ذلك وضع قواعد خاصة تجيز مراقبة الاتصالات الالكترونية في المادة(4) في الحالات التالية:

الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب وجرائم أمن الدولة. معلومات حول اعتداء على منظومة معلوماتية تهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني لمقتضيات التحريات والتحقيقات القضائية في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة ولا يجوز القيام بعمليات المراقبة في كل الحالات إلا بإذن مكتوب من السلطة القضائية المختصة. كما تناول القانون في الفصل الثالث القواعد الإجرائية لتفتيش المنظومات المعلوماتية، وفي الفصل الرابع التزامات مقدمي الخدمات. وفي الفصل الخامس أدرج إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحته وتضمن الفصل السادس التعاون والمساعدات القضائية الدولية.[2]

الفرع الثالث: الأمن المعلوماتي في قانون الإجراءات الجزائية

[1] فاروق خلف، المرجع السابق، ص ص 16-17.

[2] القانون 09-04 المؤرخ في 2009/08/05، المتضمن الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج. ر. ج. ج، د. ش، العدد 47، 5 أوت 2009.

قام المشرع الجزائري بتمديد الاختصاص المحلي لوكيل الجمهورية في مجال الجرائم الالكترونية طبقا للمادة 37فقرة02 من قانون الإجراءات الجزائية (الأمر 66-155) المتضمن قانون الإجراءات الجزائية المعدل والمتمم).[1]

حيث يمتد الاختصاص المحلي إذا تعلق الأمر بجرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبيض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وجرائم الفساد والتهريب.

كما تعد هذه الجرائم أيضا من الجرائم الموصوفة طبقا للتشريع الجنائي الجزائري.

كما نص على التفتيش في المادة 45 فقرة7 من نفس القانون المعدل، حيث اعتبر أن التفتيش المنصب على المنظومة المعلوماتية يختلف من التفتيش المتعرف عليه من حيث القواعد الإجرائية العامة والشروط الشكلية والموضوعية، وبالتالي لا تطبق عليه المادة 44 من قانون الإجراءات الجزائية إذا تعلق الأمر بالجرائم الالكترونية ونص على توقيف النظر في جريمة المساس بأنظمة المعالجة الآلية للمعطيات طبقا للمادة 51 فقرة06 من القانون (قانون الإجراءات الجزائية). (الأمر 66-155 المتضمن قانون الإجراءات الجزائية الجزائري المعدل والمتمم).

كما نص أيضا قانون الإجراءات الجزائية بموجب المادة 65 مكرر3 فقرة 5 أنه في حالة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات فإن وكيل الجمهورية المختص يقوم بوضع الترتيبات التقنية دون موافقة المعني، من أجل التقاط وتثبت وبث وتسجيل الكلام المتفوه بصفة خاصة أو سرية في أماكن خاصة أو عامة.

وفي عام 2006، أدخل المشرع تعديل آخر على قانون العقوبات بموجب القانون رقم06-24 المؤرخ في 20 ديسمبر 2006، من هذا التعديل القسم السابع مكرر والخاص

[1] الأمر 66-155 المؤرخ في 06/08/ 1966 المتضمن قانون الإجراءات الجزائية، المعدل والمتمم، ج، ر. ج. ج. د. ش، العدد 30، الصادر في 8 أوت 1966.

بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وقد تم تشديد العقوبة المقررة لهذه الأفعال. [1]

وبعد تعديل قانون العقوبات الجزائري بموجب القانون رقم16-03 المؤرخ في 19 يونيو 2016 ضمن القسم السابع مكرر من قانون العقوبات بموجب المواد من 394 مكرر إلى المادة 394 مكرر8. وضمن نطاق الفصل الثالث الخاص بالجنايات والجنح ضد الأموال.[2]

من بين هذه الجرائم: الغش أو الشروع في كل جزء من المنظومة للمعالجة الآلية للمعطيات، حذف أو تغير لمعطيات المنظمة، إدخال أو تعديل في نظام المعطيات، تصميم أو بحث او تجميع أو توفير أو نشر أو حيازة أو إفشاء أو استعمال المعطيات، تكوين جمعية الأشرار.[3]

الفرع الثالث: القانون 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة

صدر في 19 يوليو 2003 نص على تجريم انتهاك حقوق المؤلف والحقوق المجاورة عن طريق التقليد بأي وسيلة كانت، بما فيها منظومة المعـــالجة المعلوماتيـــة (المادة 152)، وتعتبر حقوق المؤلف محمية في ضوء الدستور الجزائري فقد نص في المادة 54 منه على الحماية القانونية للحريات والملكيات، حيث جاء فيها أن حرية الابداع الفكري والفني والعلمي للمواطن مضمونة في إطار القانون وحقوق التأليف محمية قانونيا، وقد سمح

[1] قانون رقم 24-06 المؤرخ في 28 أبريل سنة2024، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 8 يونيو سنة 1966 والمتضمن قانون العقوبات، ج. ر، ج. ج. د. ش، العدد 30، الصادر بتاريخ 30 أبريل سنة 2024.

[2] المواد 394إلى المواد 394 مكرر 8 ومن القانون رقم 16-03 المؤرخ في 19 يونيو 2016 من قانون العقوبات، ج. ر، ج. ج. د. ش، العدد 30، 2016 معدل ومتمم

[3] عائشة عبد الحميد، "**الجرائم المعلوماتية وكيفية مكافحتها**"، مجلة الاناسة وعلوم المجتمع، العدد 07، جامعة المسيلة الجزائر، 2020، ص ص132- 133.

قانون 03-05 في المادة (3) منه بإدخال برامج الحاسب الآلي في إطار المصنفات المحمية بموجب حق المؤلف، ونصت المادة (41) منه على عدم الاستنساخ الخطي لأي مصنف سواء كان كتاب كامل أو موسيقى أو قاعدة بيانات رقمية وعدم استنساخ برامج الحاسب إلا في الحالات المنصوص عليها في المادة 52 من هذا الأمر.[1]

المطلب الثاني: الأليات المؤسساتية

لمواجهة هذا النوع المستحدث والمعقد من الجرائم، برزت الحاجة إلى تطوير آليات مؤسساتية فعالة تعمل على التصدي لها، سواء من خلال التشريع أو الوقاية أو التحقيق أو المتابعة القضائية. وتشمل هذه الآليات الهيئة الوطنية للوقاية من جرائم المتصلة بتكنولوجيا الإعلام والاتصال كهيئة وطنية مستحدثة، الهيئات القضائية الجزائية المختصة، المعهد الوطني للأدلة والمديرية العامة للأمن المعلوماتي.

الفرع الأول: الهيئة الوطنية للوقاية من جرائم المتصلة بتكنولوجيا الإعلام والاتصال

نص المشرع في المادة 13 من القانون 09-04 على ضرورة إنشاء هيئة ذات وظيفة تنسيقية تعمل على اتخاذ الإجراءات اللازمة للوقاية من هذه الجرائم، وتتولى تنشيط وتنسيق عملية الوقاية من الجرائم الإلكترونية، وكذلك مصاحبة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن هذه الجرائم.

أولا: التعريف بالهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

[1] سوهيلة بضياف، آمنة حمراني، المرجع السابق، ص 184.

تعرف حسب أحكام المواد من 01 إلى 04 من القانون 09-04 بأنها سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي وتوضع لدى الوزير المكلف بالعدل، ويقع مقرها بالجزائر العاصمة.

ثانيا: مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

تنص المادة 14 من نفس القانون على أنه" تتولى الهيئة المذكورة في المادة 13 خصوصا المهام التالية:

– تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، وكذلك مساعدة السلطة القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، بما في ذلك تجميع المعلومات وتبدلها مع نظيرتها في الخارج قصد جمع المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وتحديد تواجدهم.

ثالثا: تشكيل الهيئة

تطبيقا للمادة 13 من القانون رقم 09-04 المؤرخ في 14 شعبان 1430 الموافق 5 غشت سنة 2009 والمذكور أعلاه، يهدف هذا المرسوم إلى تحديد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها التي تدعى في صلب النص " الهيئة "، حيث يحدد مقر الهيئة بمدينة الجزائر ويمكن نقله إلى أي مكان آخر من التراب الوطني بموجب قرار من وزير الدفاع الوطني وهذا ما نصت عليه المادة 3 من المرسوم19-172 ونصت المادة 4 من نفس المرسوم على أن تنظم الهيئة في مجلس توجيه ومديرية عامة.[1]

[1] مرسوم رئاسي رقم 19-172 مؤرخ في 6 يونيو سنة 2019 يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها، ج. ر. ج. د. ش، العدد 37، الصادر بتاريخ6 يونيو 2019.

أ-**مجلس توجيه:** حسب ما نصت عليه المادة 5 من نفس المرسوم يرأس مجلس التوجيه وزير الدفاع الوطني أو ممثله ويتشكل من ممثلي الوزارات الآتية:

- وزارة الدفاع الوطني.
- الوزارة المكلفة بالداخلية.
- وزارة العدل.
- الوزارة المكلفة بالمواصلات السلكية واللاسلكية تتولى المديرية العامة أمانة المجلس.

يكلف مجلس التوجيه هذا ما نصت عليه المادة 6 على الخصوص بما يأتي:

- التداول حول الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.
- التداول حول مسائل التطوير والتعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال.
- القيام بتقييم حالة التهديد في مجال الجرائم المتصلة بتكنولوجيا الإعلام والاتصال للتمكن من تحديد مضامين عمليات المراقبة الواجب القيام بها والاهداف المنشودة بدقة.
- اقتراح كل نشاط يتصل بالبحث وتقييم الأعمال المباشرة في مجال الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.
- الموافقة على برنامج عمل الهيئة.
- إعداد نظامه الداخلي والمصادقة عليه أثناء أول اجتماع له.
- دراسة التقرير السنوي لنشاطات الهيئة والمصادقة عليه.
- إبداء رأيه في كل مسألة تتصل بمهام الهيئة.
- تقديم كل اقتراح يتصل بمجال اختصاص الهيئة.

- المساهمة في ضبط المعايير القانونية في مجال اختصاصه.[1]
- دراسة مشروع ميزانية الهيئة والموافقة عليه.

حيث تنص المادة 7و8 من ذات المرسوم " يجتمع مجلس التوجيه في دورة عادية مرتين(2) في السنة، بناء على استدعاء من رئيسه". ويمكن أن يجتمع في دورة غير عادية كلما كان ذلك ضروريا، بناء على استدعاء من رئيسه أو بطلب من أحد أعضائه أو من المدير العام للهيئة.

المادة 8 تنص على" تحدد قواعد وكيفيات سير مجلس التوجيه بموجب قرار من وزير الدفاع الوطني".

ب-المديرية العامة: يدير المديرية العامة مدير عام، وتتولى على الخصوص الصلاحيات الآتية:

- السهر على حسن سير المهنة.
- إعداد مشروع ميزانية الهيئة.
- إعداد وتنفيذ برنامج عمل الهيئة.
- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.
- تبادل المعلومات مع مثيلاتها الأجنبية بغرض تجميع كل المعطيات المتعلقة بتحديد مكان مرتكبي الجرائم المتصلة بتكنولوجيا الإعلام والاتصال والتعرف عليهم.
- تحضير اجتماعات مجلس التوجيه.
- إعداد التقرير السنوي لنشاطات الهيئة.

حيث أن المدير العام هو الآمر بصرف ميزانية الهيئة، وتضم المديرية العامة حسب المادة 10 من نفس المرسوم ما يلي:

[1] المادة 6 من المرسوم الرئاسي 19-172، المصدر نفسه.

- مديرية تقنية.
- مديرية للإدارة والوسائل.
- مصالح.

1-المديرية التقنية: حسب المادة 11 تكلف المديرية التقنية بمهمة المراقبة الوقائية للاتصالات الإلكترونية في إطار الوقاية من الجرائم الموصوفة بالأفعال الإرهابية والتخريبية والاعتداء على أمن الدولة.

تتولى المديرية التقنية، على الخصوص ما يأتي:

- مساعدة السلطات القضائية ومصالح الشرطة القضائية بناء على طلبها بما في ذلك في مجال الخبرات القضائية في إطار مكافحة الجريمة المتصلة بتكنولوجيا الإعلام والاتصال والجرائم التي تتطلب اللجوء إلى أساليب التحري الخاصة للهيئة.
- جمع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها وتتبعها بغرض استعمالها في الإجراءات القضائية.

كما جاء كذلك في نص المادتين 13 و14 حيث تمارس المديرية التقنية مهامها المرتبطة بالشرطة القضائية وفقا لأحكام التشريع المعمول به، لاسيما الأمر رقم 66-155 المؤرخ في 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية.[1]

- تضع المديرية التقنية التجهيزات والوسائل والأجهزة التقنية الضرورية لتنفيذ مهامها على مستوى المنشآت القاعدية للمتعاملين ومقدمي الخدمات في مفهوم التشريع المعمول به. يلزم المتعاملون ومقدمو الخدمات بتقديم المساعدة الضرورية للمديرية التقنية من أجل تنفيذ مهامها.

[1] المواد من 10 إلى14 من المرسوم الرئاسي19 -172، المصدر نفسه

2-مديرية الإدارة والوسائل: تكلف مديرية الإدارة والوسائل، حسب نص المادة 15 من نفس المرسوم على الخصوص بما يأتي:

- الإسناد التمويني والإسناد التقني للهيئة.
- صيانة العتاد والوسائل والمنشآت القاعدية.
- إعداد احتياجات الهيئة في إطار تحضير تقديرات الميزانية.

3-أحكام مالية: تشتمل ميزانية الهيئة على باب للإيرادات وباب النفقات المادة 16.

أ-في باب الإيرادات:

- الإعانات التي تمنحها الدولة.
- عائدات كل النشاطات المرتبطة بموضوعها.

ب-في باب النفقات:

- نفقات التسيير.
- نفقات التجهيز.

نصت المادة 17 على أن تمسك محاسبة الهيئة حسب قواعد المحاسبة العمومية.[1]

رابعا: اختصاصاتها

بينت الفقرة المادة 04 من المرسوم الرئاسي 19-172المهام الأساسية التي تكلف بها هذه الهيئة وهي على سبيل الحصر، الهدف منها هو الوقاية من الجرائم الإلكترونية ومكافحة هذه الأخيرة من خلال الإسهام في أعمال البحث والتحقيق ومد يد العون لمصالح الشرطة القضائية، وأبرز مهام هذه الهيئة هي:

- اقتراح عناصر الاستراتيجية الوطنية للوقاية عن الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

[1] المواد 15إلى17من المرسوم الرئاسي 19-172، المصدر نفسه.

– تنشيط وتنسيق عمليات الوقاية عن الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

– مساعدة السلطة القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المعلوماتية من خلال مدها بالمعلومات والخيرات القضائية.

– ضمان المراقبة للاتصالات الإلكترونية قد اكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والماسة بأمن الدولة وذلك تحت سلطة القاضي المختص وباستثناء أي هيئات وطنية أخرى.

– تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية.

– السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها.

– المساهمة في تكوين المحققين المتخصصين في مجال التقنية المتصلة بتكنولوجيا الإعلام والاتصال.

– المساهمة في تحديث المعايير القانونية في مجال اختصاصها.[1]

الفرع الثاني: الهيئات الجزائية المختصة

والمتمثلة في الأقطاب القضائية الجزائية المتخصصة والتي تم إنشاؤها بموجب القانون 04-14[2] تختص بالنظر في القضايا المتعلقة بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات طبقا للمواد 37-40-329 من قانون الإجراءات الجزائية الجزائري، هذه من

[1] عبد العزيز أحمد، **خصوصية التحقيق في الجريمة المعلوماتية**، مذكرة مقدمة لنيل شهادة الماستر في الحقوق تخصص القانون الجنائي وعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة الدكتور الطاهر مولاي سعيدة، 2021-2022، ص ص57، 58.

[2]– القانون 04-14، المؤرخ في 10 نوفمبر 2004، المعدل والمتمم للأمر رقم 66-155، المؤرخ في 08 يونيو 1966 والمتضمن قانون الاجراءات الجزائية، ج.ر، ج.ج.د.ش العدد 71، الصادر بتاريخ في 10 نوفمبر 2004.

جهة أما فيما يتعلق بالاختصاص الإقليمي للأقطاب المتخصصة، فإنه يمكن النظر في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، ومرتكبة خارج الوطن وحتى ولو كان مرتكبها أجنبيا، لكن في حالة ما إذا كانت تستهدف مؤسسات الدولة أو مؤسسات الدفاع الوطني.[1]

الفرع الثالث: المعهد الوطني للأدلة والمديرية العامة للأمن المعلوماتي

أولا: المعهد الوطني للأدلة الجنائية وعلم الجرائم

أنشأ بموجب المرسوم الرئاسي رقم 04-432 المؤرخ في 2004/12/20 وتم تنظيم المصالح والأقسام والمخابر فيه بموجب قرار وزاري مشترك مؤرخ في 2007/04/14 والذي تضمن مصلحة الخبرات الخاصة بالدلائل التكنولوجية، يتكون المعهد الوطني للأدلة الجنائية وعلم الإجرام من احدى عشرة دائرة متخصصة في مجالات مختلفة، جميعها تضمن إنجازه الخبرة، التكوين والتعليم تقديم المساعدات التقنية، البحوث، الدراسات والتحاليل في علم الجريمة.

دائرة الإعلام الآلي والالكتروني مكلفة بمعالجة وتحليل وتقديم كل دليل رقمي وتماثلي للعدالة كما تقدم مساعدة تقنية للمحققين في التحقيقات المعقدة. أفراد الدائرة يسهرون على تأمين اليقظة التكنولوجية من أجل تحسين المعارف، التقنيات والطرق المستعملة في مختلف الخبرات العلمية لإنجاز المهام المنوطة بها، تنسم الدائرة إلى ثلاث مخابر وذلك حسب نوع المعلومات سمعية، بصرية، والإعلام الآلي.

كل مخبر مزود بقضية مهمتها إنشاء المعطيات من حوامل المعلومات وضمان نزاهة وشرعية الدليل وهذه المخابر هي:

1- مخبر الإعلام الآلي.

2- مخبر الفيديو.

[1] عائشة عبد الحميد، المرجع السابق، ص 136.

3- مخبر الصوت.

أ-مخبر الإعلام الآلي: من مهامـــه:

- تحليل ومعالجـــة حوامـــل المعطيـات الرقمية الهاتف، الشريحة، القـرص الصلب، ذاكرة الفلاش.
- تحديد التزوير الرقمي للبطاقات البنكية.

ب-مخبر الفيديو: يختص مخبر الفيديو بمقارنة الأوجه وشرعية الصورة والفيديو وإعادة بناء مسرح الجريمة بالتشكيل ثلاثي الأبعاد وتحسين نوعية الصورة (فيديو-صورة) بمختلف التقنيات.

ج-مخبر الصوت: ومن المهام التي يؤديها: تحسين نوعية إشارة الصوت بنزع التشويش وتعديل السرعة ومعرفة وتحديد المتكلم وتحديد شرعية التسجيلات الصوتية.

ثانيا: المديرية العامة للأمن الوطني:

1- الجانب القانوني: والمتمثل في النصوص القانونية الأتية:

- القانون 22-06 المؤرخ في 2006/12/10 والقانون 05-03 من القانون المدني.
- القانون 04-09 المؤرخ في 2009/08/05 وقانون العقوبات المواد من 394 مكرر إلى 394 مكرر 7.

أ-الجانب التنظيمي: ويتمثل في التكوين المتواصل والتخصيص والتكوين الأولى وتدعيم مخابر الشرطة العلمية تدعيم المصالح الولائية للشرطة القضائية وتدعيم وهيكلة مصالح الشرطة القضائية للتصدي للجريمة.

ب-الجانب التوعوي: لم تغفل المديرية العامة للأمن الوطني عن الجانب الوقائي التوعوي يظهر ذلك من خلال برمجتها المديرية العامة لخطوات استباقية للتصدي للجريمة الكترونية عن طريق تنظيم دروس توعوية في مختلف الأطوار الدراسية وكذا المشاركة في الملتقيات

والندوات الوطنية وجميع التظاهرات التي من شأنها توعية المواطن حول خطورة الجرائم الالكترونية.

ج-الجانب الدولي: في إطار مكافحة الجريمة الالكترونية ونظرا للبعد الدولي الذي عادة ما يتخذه هذا النوع من الجرائم، لم تغفل المديرية العامة للأمن الوطني استغلال عضويتها الفعالة في هاته الأخيرة تتيح مجالات للتبادل INTRPOL المنظمة الدولية للشرطة الجنائية المعلوماتي الدولي وتسهل الإجراءات القضائية المتعلقة بتسليم المجرمين، وكذا مباشرة الانابات القضائية الدولية ونشر أوامر القبض للمبحوث عنهم دوليا.[1]

وللاشارة فقد استحدث المشرع الجزائري لحماية الأنظمة الرقمية هيئة مؤسساتية جديدة وذلك بموجب المرسوم الرئاسي 20-05 [2]وهي:

- **المجلس الوطني لأمن الأنظمة المعلوماتية:**

ويكلف بإعداد الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية، والموافقة عليها وتوجيهها.

وتضم تشكيلة هذا المجلس رئيسا يتمثل في وزير الدفاع الوطني أو ممثله، ويتكون من ممثل عن رئاسة الجمهورية، وممثل عن الوزير الأول، الوزير المكلف بالشؤون الخارجية ، الوزير المكلف بالداخلية، الوزير المكلف بالعدل، الوزير المكلف بالمالية، الوزير المكلف بالطاقة، الوزير المكلف بالاتصالات، الوزير المكلف بالتعليم العالي، كما يمكن أن يستعين المجلس باي شخص أو مؤسسة من شأنه تنويره في أعماله

وتتمثل مهامه في ما يلي:

---

[1] بن نعوم خالد أمين، "**إجراءات التحقيق في الجريمة المعلوماتية في التشريع الجزائري**"، مذكرة لنيل شهادة الماستر، تخصص قانون قضائي، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس مستغانم، 2019/2018 ص ص 44، 45.

[2] المرسوم الرئاسي رقم 20-05 المؤرخ في 20 جانفي 2020، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، ج.ر، ج.ج.د.ش، العدد 04، الصادر بتاريخ 26 جانفي 2020.

- البت في عناصر الاستراتيجية الوطنية لامن الأنظمة المعلوماتية المقترحة من قبل الوكالة وتحديدها
- دراسة مخطط عمل الوكالة وتقرير نشاطاتها والموافقة عليهما.
- دراسة التقارير المتعلقة بتنفيذ الاستراتيجية الوطنية لأمن الانظمة المعلوماتية، والموافقة عليها.
- الموافقة على اتفاقات التعاون والاعتراف المتبادل مع الهيئات الاجنبية في مجال امن الانظمة المعلوماتية.
- الموافقة على سياسة التصديق الالكتروني للسلطة الوطنية للتصديق الالكتروني
- الموافقة على تصنيف الانظمة المعلوماتية.
- اقتراح ملاءمة الاطار الهيكلي أو التنظيمي الخاص بأمن الانظمة المعلوماتية، عند الحاجة.
- ويبدي المجلس رأيا مطابقا في أي مشروع نص تشريعي أو تنظيمي ذي صلة بأمن الانظمة المعلوماتية.

وكالة أمن الأنظمة المعلوماتية:

حسب المادة 17 [1]من المرسوم هي عبارة عن مؤسسة عمومية ذات طابع اداري تتمتع بالشخصية المعنوية والاستقلالية المالية.

ويحدد مقر الوكالة في مدينة الجزائر.

وتكلف الوكالة بالمهام التالية:

- تحضير عناصر الاستراتيجية الوطنية في مجال أمن الانظمة المعلوماتية وعرضها على المجلس

[1] المادة 17 من المرسوم الرئاسي 20-05 ، المصدر نفسه.

- تنسيق تنفيذ الاستراتيجية الوطنية لأمن المعلوماتية المحددة من قبل المجلس.
- اقتراح كيفيات اعتماد مزودي خدمات التدقيق في مجال أمن الانظمة المعلوماتية.
- اجراء تحقيقات رقمية في حالة الهجمات أو الحوادث السبيرانية التي تستهدف المؤسسات الوطنية
- السهر على جمع وتحليل وتقييم المعطيات المتصلة بمجال أمن الانظمة المعلوماتية لاستخلاص المعلومات الملائمة التي تسمح بتامين منشآت المؤسسات الوطنية.
- متابعة عمليات التدقيق لأمن الانظمة المعلوماتية.
- تقديم المشورة والمساعدة للادارات والمؤسسات والهيئات العمومية والخاصة من أجل وضع استراتيجية أمن الانظمة المعلوماتية.
- ضمان اليقظة التكنولوجية في مجال أمن الانظمة المعلوماتية
- مرافقة الادارات والمؤسسات والهيئات، بالتشاور مع الهياكل المختصة في هذا المجال، في معالجة الحوادث المتصلة بأمن الانظمة المعلوماتية.
- جرد الانظمة المعلوماتية وعرضها على المجلس للموافقة على تصنيفها.
- اعداد وتحيين خارطة للانظمة المعلوماتية المصنفة.
- اقتراح مشاريع نصوص تشريعية أو تنظيمية في مجال أمن الانظمة المعلوماتية، بعد الرأي المطابق للمجلس.
- اعداد وتحديث المرجعيات والاجراءات والادلة العملية وتقديم توصيات في ميدان أمن الانظمة المعلوماتية.
- اعتماد متنجات أمن الانظمة المعلوماتية والتصديق عليها.
- اعتماد منظومات انشاء وفحص الامضاء الالكتروني.

- تحديد معايير واجراءات منح علامة الجودة و/ أو التصديق و/أو اعتماد المنتجات ومقدمي الخدمات في مجال امن الانظمة المعلوماتية طبقا للتشريع والتنظيم المعمول بهما.
- القيام بنشاطات التكوين والتوعية ذات الصلة بامن الانظمة المعلوماتية.
- تقديم توجيهات تتعلق بتكوين أعوان المؤسسات العمومية، في مجال أمن الانظمة المعلوماتية.
- اقتراح تدابير الترقية والبحث والتطوير للحلول الوطنية في مجال أمن الانظمة المعلوماتية.
- تنشيط وتوجيه انشطة البحث والتطوير في مجال أمن الانظمة المعلوماتية.
- اقتراح مشاريع اتفاقات التعاون والاعتراف المتبادل مع الهيئات الدولية في مجال اختصاصها.
- ابرام مشاريع شراكة في مجال أمن الانظمة المعلوماتية بعد موافقة المجلس.
- تعزيز ثقافة تامين الانظمة المعلوماتية.
- اعداد تقارير دورية وحصيلة سنوية عن نشاطها.
- اعداد وتحيين خارطة حالات هشاشة الانظمة المعلوماتية على المستوى الوطني.
- ضمان تبادل المعلومات مع الامانة التقنية للجنة الوطنية لتصنيف النقط الحساسة.
- التنظيم والمشاركة في الاحداث والتظاهرات العلمية والتقنية المتعلقة بأمن الانظمة المعلوماتية[1].

وتنص المادة 20: تدير الوكالة لجنة توجيه وزود بلجنة علمية.

يسير الوكالة مدير عام وتتوفر على مركز وطني عملياتي لأمن الانظمة المعلوماتية مديريات ومصالح تقنية وادارية موضوعة تحت سلطته.

وتشير المادة 21: يعين رئيس لجنة التوجيه طبقا للتنظيم المعمول به في وزارة الدفاع الوطني.

المادة22: تتكون لجنة التوجيه من ممثلي:

- 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 الالكترونية.
- السلطة الوطنية للتصديق الالكتروني
- الهيئة الوطنية لحماية البيانات ذات الطابع الشخصي.
- السلطة الحكومية للتصديق الالكتروني.
- وعلى سبيل الاستشارة، المدير العام للوكالة

تتولى مصالح الوكالة أمانة لجنة التوجيه.

يمكن ان تستعين لجنة التوجيه بأي شخص أو مؤسسة من شأنها تنويرها في أعمالها[1].

بالإضافة الى السلطة الوطنية للتصديق الالكتروني

أولا: تعريفها

تنشأ لدى الوزير الأول سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي، تسمى السلطة الوطنية للتصديق الالكتروني وتدعى في صلب النص" السلطة ".

ثانيا: مهامها

نصت عليها المادة 18 من القانون 15-04 مهامها وهوما كالآتي:

1-إعداد سياستها للتصديق الالكتروني والسهر على تطبيقها بعد الحصول على الرأي الإيجابي من قبل الهيئة المكلفة بالموافقة.

2-الموافقة على سياسات التصديق الالكتروني الصادرة على السلطتين الحكومية والاقتصادية للتصديق الالكتروني.

3-إبرام اتفاقيات الاعتراف المتبادل على المستوى الدولي.

4-اقتراح مشاريع تمهيدية لنصوص تشريعية أو تنظيمية تتعلق بالتوقيع الالكتروني أو التصديق الالكتروني على الوزير الأول.

5-القيام بعمليات التدقيق على مستوى السلطتين الحكومية المكلفة بالتدقيق.[2]

[1] المواد من 20 الى 22 من المرسوم الرئاسي رقم 20-05 المصدر نفسه.

[2]قانون رقم 15-04 مؤرخ في 11 ربيع الثاني عام 1436 الموافق أول فبراير سنة 2005، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، ج، ر, ج، ج، د، ش, العدد06، فبراير 2015.

ثالثا: تشكيلتها

نصت المادة 19 من القانون 15-04 على تشكيلة السلطة ذلك أنها تتشكل من مجلس ومصالح تقنية وإدارية.

-يتشكل مجلس السلطة من خمسة(5) أعضاء من بيتهم رئيس، يعينهم رئيس الجمهورية على أساس كفاءاتهم، لاسيما في مجال العلوم التقنية المتعلقة بتكنولوجيا الاعلام والاتصال.

- يسير المصالح التقنية والإدارية للسلطة مدير عام يعينه رئيس الجمهورية، بناء على اقتراح من الوزير الأول. حيث يحدد تنظيم هذه المصالح وسيرها ومهامها عن طريق التنظيم.[1]

المبحث الثاني: الأساليب الإجرائية لحماية قواعد الأمن المعلوماتي

تعد قواعد الأمن المعلوماتي من الركائز الأساسية لحماية البيانات والأنظمة في العصر الرقمي الحديث. ومع ازدياد التهديدات السيبرانية وتطورها المستمر، بات من الضروري اتباع أساليب إجرائية فعالة لضمان الحفاظ على سرية المعلومات وسلامتها وتوفرها. تهدف هذه الأساليب إلى وضع إطار منظم للوقاية من الاختراقات، ورصد التهديدات، والاستجابة للحوادث بطريقة مدروسة. حيث سنتطرق في هذا المبحث إلى ثلاث مطالب: **(المطلب الأول)** أساليب الحماية المادية، أما **(المطلب الثاني)** أساليب الحماية البرمجية والتقنية، **(المطلب الثالث)** أساليب الحماية التنظيمية والإدارية.

المطلب الأول: أساليب الحماية المادية

[1] المواد 18-19 من القانون رقم 15-04 المصدر نفسه.

الأمن المادي أو الأمن الفيزيائي يشمل أمن المباني وأجهزة الحاسوب، والمعدات الأخرى وأجهزة الاتصال والتكييف والطاقة، ويتحقق هذا الأخير من خلال:

الفرع الأول: السيطرة على المداخيل

يجب العناية بالحماية المادية والمراكز المعلوماتية من خلال أحكام السيطرة والرقابة على مداخيلها للوصول إلى القدر المطلوب من أمن المعلومات، حيث تصمم إجراءات الأمن المادية لمواجهة الأخطار الناتجة عن الأشخاص ذوي النوايا السيئة أو الذين لديهم تصاريح الدخول للمنشأة وبالإضافة للمتسللين من خارج المنشأ، لذا يجب اتخاذ إجراءات شاملة ضد الأخطاء من خلال تحديد حركة الدخول والخروج ليلا ونهارا.[1]

ولتأمين الأجهزة والبنية التحتية المادية يجب توفير الإجراءات اللازمة:

- كاميرات المراقبة.
- إقفال الأمان.
- التحكم في الوصول الفيزيائي (بطاقات الهوية).[2]

الفرع الثاني: نظام الدائرة التلفزيونية الغلقة (GCTV)

وهي مجموعة من الكاميرات التصوير التليفزيونية التي يمكن التحكم فيها، وتراقب هذه الكاميرات مداخل المنظمة ومداخل غرف النظام، وهي متصلة بأجهزة إنذار وعند حدوث أي خطر تتم عملية التنبيه.[3]

المطلب الثاني: أساليب الحماية البرمجية والتقنية

[1] محمد بغداد، **الأمن المعلوماتي وسبل حماية في الجزائر**، مذكرة لنيل شهادة ماستر، تخصص تسيير وإدارة – الجماعات المحلية، كلية الحقوق والعلوم السياسية، جامعة مولاي طاهر، سعيدة، 2017-2018، ص 57.

[2] https://books.gool.dz_(25/04/2025) 12.00 h.

[3] محمد بغداد، المرجع السابق، ص 57.

نحن في عصر تتسارع فيه التطورات التقنية بشكل غريب ولذا أصبحت حماية المعلومات والأنظمة ضرورة حتمية لضمان استمرارية الأعمال وحماية البيانات من المخاطر، لذا تتعدد أساليب الحماية البرمجية والتقنية.

الفرع الأول: التشفير (cryptoptography)

التشفير هو "علم الكتابة السرية" استخدمه المصريون القدماء، ويعرف كذلك بأنه العلم الذي يحول المعلومة الواضحة إلى معلومة سرية غير قابلة للفهم، و"نذكر هنا ضرورة التشفير حال الاتصال عبر وسائط غير موثوقة، وخاصة حالة التراسل من خـــلال الأنترنت، وتتم عملية التشفير بنقل المعلومة من طرف الآخر عبر وسيط.

وبالنسبة للمشرع الجزائري فلم يعرف تقنية التشفير لكنه تطرق من خلال نص المادة الثانية الفقرتين الثامنة والتاسعة من القانون 15-04 المتعلق بالتوقيع والمصادقة الالكترونيين، حيث اشارة في الفقرة الثامنة الى اعتماد التشفير على المفتاح الخاص ويقصد به عبارة عن سلسلة من الاعداد يحوزها حصريا الموقع فقط، وتستخدم لإنشاء التوقيع الالكتروني، ويرتبط هذا المفتاح بمفتاح تشفير عمومي[1]، وهو بذلك تحت السيطرة والسلطة المطلقة لصاحب التوقيع الإلكتروني الذي يتعين عليه توفير شروط السلامة لحماية المفتاح من مخاطر استعماله من طرف الغير خاصة بعدم الكشف عنه لاي شخص آخر وهذا المفتاح يستعمل لتشفير الوثائق وامضائها[2].

[1] الفقرة الثامنة من المادة الثانية، القانون 15-04، المؤرخ في 1 فبراير 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، ج.ر، ج.ج.د.ش، العدد 06، الصادر بتاريخ 10 فبراير 2015.

[2]- حزام فتيحة، "**حماية الانظمة الرقمية بين الآليات التقنية وأجهزة الحماية قراءة في أحكام المرسوم الرئاسي 20-05**"، مجلة الحقوق والعلوم الانسانية، جامعة الجلفة، المجلد 13، العدد 03، أكتوبر 2020ص 177

وتشير الفقرة التاسعة ومن نفس المادة الى المفتاح العمومي ايضا وهو عبارة عن سلسلة من الاعداد تكون موضوعة في متناول الجمهور بهدف تمكينهم من التحقق من الامضاء الالكتروني ، وتدرج في شهادة التصديق الالكتروني.[1]

وهناك ثلاث أجزاء هامة لفهم عملية التشفير: تشفير البيانات وفك تشفير البيانات.

أولا: برامج مكافحة الفيروسات

هي البرامج المضادة لفيروسات تستخدم لمنع واكتشاف فيروسات الحاسوب، وبرامج التجسس وغيرها من أشكال البرمجيات الخبيثة، ولكن مهما كانت برامج مكافحة الفيروسات مفيدة فإنه في بعض الأحيان يمكن أن تكون لها عيوب، فهي تقلل أداء الحاسوب إذ لم تكن مصممة بكفاءة.

ثانيا: طرق التشفير

هناك منظومتين للتشفير:

1-منظومة التشفير المتناسق أو التماثلي: وتسمى بالتشفير السيميتريSymétrique وهذه الطريقة تعتمد على مفتاح سري واحد متبادل ويعني ذلك أن مرسل الرسالة الالكترونية ومستقبلها يستخدمان نفس المفتاح للتشفير ولفك رموز الرسالة، ولكن نظرا لضرورة إطلاع الطرف المتعاقد مع صاحب التوقيع على الرقم السري وإلى كل من يتعاقد معه، وما قد يؤدي غليه من فقد الأمن والسرية مما أدى إلى ظهور منظومة أدق وأوثق.

2-منظومة التشفير اللامتناسق أو اللاتماثلي(Asymétrique)هذا النوع من التشفير أم اكتشافه في الولايات الأمريكية المتحدة عام 1978 من طرق ثلاث علماء رياضيات، ولقد جاء هذا النظام حلا لمشكلة التوزيـــع غير الأمـــن للمفاتيـح في مجـال التشفيـر المتناظر، خصوصا عدد استخدام مفتاح واحد.

[1] الفقرة التاسعة من المادة الثانية من القانون 15-04، المصدر السابق.

يستخدم التشفير اللامتناظر مفتاحيـــن مرتبطين بعـــلاقة ريـــاضية معقدة عند بنائهما، ويدعي هذين المفتاحين بالمفتاح العام (Public Key) والمفتاح الخاص (Private Key).

فالمفتاح الخاص يكون معروفا لدى شخص واحد أو جهة واحدة فقط، وتحت السيطرة والسلطة المطلقة لصاحب التوقيع وهو المرسل، الذي يتعين عليه توفر شروط السلامة لحماية مفتاحه الخاص من مخاطر استعماله من طرف الغير، وهذا المفتاح يستعمل لتشفير المحررات وتوقيعها. في حين المفتاح العمومي كما يدل عليه اسمه، هو مفتاح معروف عادة على نطاق واسع، ويستخدم من قبل شخص موثوق به للتثبت من صحة التوقيع الالكتروني، ويمكن معرفته لأكثر من خلال معرفة المفتاح العام.[1]

ثالثا: جدران الحماية (Firewall)

جدران الحماية هو أداة أو نظام أمني يستخدم لحماية الشبكات وأجهزة الكمبيوتر من الوصول غير مصرح به أو هجمات إلكترونية، وتتمثل أهميته في:

- الحماية من الاختراقات والهجمات.
- تعزيز خصوصية البيانات.
- تقليل المخاطر الأمنية.
- تحسين إدارة الشبكة.

رابعا: أنواع جدران الحماية

1-جدران الحماية المستند من الأجهزة: جهاز فعلي يوفر حماية للشبكة بالكامل.

2-جدران الحماية البرمجية: برنامج يتم تثبيته على جهاز الكمبيوتر أو الخادم، يحمي الأجهزة الفردية وأنظمة التشغيل.

[1] بوربابة صورية، المرجع السابق، ص 52.

3-جدران الحماية السحابية: خدمة تقدم عبر السحابة لحماية التطبيقات والبيانات.[1]

خامسا: أدوات منع وكشف الاختراق

تضاف أدوات صد أو منع الاختراقات إلى مستويات الحماية التي يجب توفيرهـا للنظام، وتعتبر هذه الإضافات بمثابة حماية مبكرة للنظام، ويجب استخدام أدوات الكشف من الاختراقات، ويجب كذلك فحص هذه الوسائل من فترة لفترة حتى يتمكن النظام من العمل بفعالية.[2]

الفرع الثاني: التقنيات المتقدمة لحماية من المعلومات

1- الذكاء الاصطناعي والتعلم الآلي:

- كشف التحليل وتهديدات بشكل تلقائي باستخدام الذكاء الاصطناعي.

الأدوات: -Darktroce- Bmwatson for cyber security.

2-الحوسبة السحابية الأمنةcecureloud conputiry :

- تأمين الخدمات السحابية باستخدام التشفير والتحكم في الوصول وإدارة الهوية.

الأدوات: Awssecurity Hub

-Microsoft Azure Securty lerter.[3]

المطلب الثالث: أساليب الحماية التنظيمية والإدارية

مع التقدم التكنولوجي المتسارع والاعتماد المتزايد على الأنظمة الرقمية، أصبحت حماية المعلومات أمر ضروري لضمان وديمومة الأعمال والحفاظ على الخصوصية.

وفي هذا السياق ستناول أبرز أساليب الحماية التنظيمية والإدارية، وأهميتها في بناء مؤسسات قادرة على الاستدامة والتطور.

[1] المرجع نفسه، ص 74.

[2] محمد بغداد، المرجع السابق، ص ص 58-60.

[3] https://books.gool.dz _(25/04/2025) 12.00 h.، المرجع السابق

الفرع الأول: تصنيف المعلومات

تصنف المعلومات حسب أهميتها بغرض حماية ومعرفة التي تتطلبها، فمن المعلومات ما لا يحتاج إلى حماية بالمطلق ويتحصل عليها من يريد ومتى يشاء، وهناك معلومة تتطلب السرية وضمان عدم الإفشاء.

أولا: الحماية عن طريق القوانين والتشريعات والاتفاقيات الدولية

تتمثل هذه الوسائل أساسا في ضرورة تطوير اتفاقيات دولية في مجال الأمن المعلوماتي تماشيا مع التطورات والتغيرات الحاصلة في المجال الرقمي، وفي المقابل يجب على الحكومات سن قوانين والعقوبات الرادعة لمرتكبي الجرائم المعلوماتية.

ثانيا: التوعية داخل المؤسسة وخارجها

لا يمكن تحقيق الأمن المعلوماتي من دون وعي شامل وكامل، إذ أن من الضروري على المؤسسة مباشرة جملة من الحملات التوعوية لموظفيها وكذلك للمتعاملين معها، تشرح لهم المخاطر المحتملة وكيفية تفاديها، وتستند التوعية الفعالة على المدى الطويل والمتوسط لتشجيع التغيير في السلوكيات العادات والمعتقدات.[1]

الفرع الثاني: وضع سياسة للأمن المعلوماتي

هي مجموعة من القواعد والقوانين والممارسات التي تضبط عمل المؤسسة وتحمي مصادرها لتحقيق غايات أمنية ولتكن جدية وممكنة، يجب أن تمنح هناك القوانين للأفراد القدرة على تحديد الأفعال الحسنة والأفعال التي تتنافى مع هذه السياسات.

1-متطلبات سياسة أمن المعلومات:

- أن تكون تكلفتها معقولة ومناسبة.
- أن تتوافق مع أسلوب أداء الموظفين لأعمالهم وتعاملهم مع العالم الخارجي.
- أن تلبي المتطلبات القانونية في بيئة المؤسسة.

[1] محمد بغداد، المرجع السابق، ص 65.

- أن تراعي العوامل الإجرائية.[1]

[1] المرجع نفسه، ص 66.

خلاصة:

في ظل التحول الرقمي المتسارع أصبحت حماية الأمن المعلوماتي من الأوليات الاستراتيجية للدول، ومن بينها الجزائر وتبنت هذه الأخيرة مجموعة من الأليات القانونية لمواجهة التهديدات السيبرانية، من خلال إصدار قوانين متخصصة مثل قانون الوقاية من الجرائم المعلوماتية ومكافحتها، وإضافة إلى إدراج أحكام جزائية في قانون العقوبات بالاعتداء على نظم المعلومات والمعطيات الرقمية، كما أن تعزيز التعاون الدولي والانخراط في الاتفاقيات الإقليمية والدولية يمثل دعامة أساسية في هذا المجال، مما يستدعي مواصلة تطوير الإطار القانوني وتحديث الوسائل التقنية إلى جانب تعزيز التوعية، وبناء قدرات الكوادر المتخصصة لضمان أمن المعلومات وحماية السيادة الرقمية للبلاد وضرورة مواكبة التطورات التكنولوجية السريعة والتحديات الأمنية المتغيرة وتشجيع على الابتكار للاستقرار الرقمي وضمان استمرارية الخدمات الرقمية لتكون الثقة بين المستخدمين والمؤسسات.

الذي يحرره رئيس تشكيلة الحكم ويأمر بغلق الملف وبأمر غير قابل للطعن، وفقا لنص المادة 973 من قانون الإجراءات المدنية والإدارية.

خاتمة

نستنتج من خلال دراستنا لموضوع الأمن المعلوماتي في القانون الجزائري، أن العديد من المخاطر والمعوقات التي تعيق استمرارية النظام وحداثته، إذ أقر المشرع الجزائري عدة آليات لحماية قواعد الأمن المعلوماتي، نظرا لأهمية البيانات والمعلومات في العصر الرقمي من بينها التشريعات والقوانين الخاصة بأمن المعلومات كقانون مكافحة الجرائم المعلوماتية، وحماية البيانات الشخصية، والأساليب الإدارية والتنظيمية كذلك إصدار المعايير والسياسات الأمنية ملزمة لتعاون الدولي والتوعية والتدريب لتنظيم حملات توعية للمجتمع لتعزيز الثقافة المعلوماتية والأمنية.

حيث يعد نظام أمن المعلومات من أكثر الأساليب انتشارا في زمن العولمة حيث أن المنظمات أصبحت تعتمد في سياستها وبرامجها على الأجهزة الالكترونية مما يستدعي تبني استراتيجية محكمة التي تقوم على حماية جميع موارد المنظمة سواء داخليا أو خارجيا، وهذا ما يساهم في ضمان استمرارية وفعالية نظام المعلوماتي وتحقيق السرية التامة للمعلومات. وهذا ما أدى بالكثير من الباحثين في المجال القانوني للعزوف عن الحديث في هذا المجـــال، وعلى كل فإنه يمكن الوقوف على النتائج والاقتراحات التالية:

- **النتائج:**

تتمثل أهم النتائج التي توصلنا اليها من خلال دراستنا لهذا الموضوع في مجموعة من الاثار القانونية والتنظيمية التي تهدف الى حماية المعلومات من خلال ما يلي:

- ان المشرع الجزائري لم يعطى تعريفا واضحا ودقيقا لمفهوم الأمن المعلوماتي.
- يعد نظام الأمن المعلوماتي من أهم التقنيات الحديثة ويجب على كل مؤسسة تبنيها وسير في نمطها
- تظهر خطورة الجرائم المعلوماتية في كونها عابرة للحدود ولها أثار سلبية على مرتكبيها، بالاضافة الى صعوبة اثباتها

- تطور الجرائم الواقعة على المعلومات بتطور تكنولوجيا الاعلام والاتصال وهو ما يفرض على المشرع العمل على مواكبة هذه التطورات ومحاولة السيطرة على مثل هذه الجرائم.
- باعتبار ان الامن المعلوماتي من المواضيع الهامة فقد عملت الدولة على توفير مختلف الأساليب والاليات اللازمة لضمان الحماية الكافية للبيانات والمعلومات سواء من جانب سن القوانين، او انشاء مؤسسات ولكن تبقى غير كافية نظر لما يشهده العالم من تطورات في التكنولوجيا وكل ما يتعلق بالمعلومات من أنظمة وأيضا تطور الجريمة وانتشارها.
- من الناحية التقنية من المستحيل الوصول الى نظام آمن وسري لأي قاعدة معلوماتية بشكل كامل.
- **الاقتراحات**

- ضرورة سن قوانين قائمة بذاتها تعمل على حماية الانظمة المعلوماتية ووضع العقوبات والإجراءات لحماية هذه المعلومات والحفاظ على سلامتها وسريتها.
- العمل على الاستفادة من خبرات وتجارب الدول الرائدة في مجال مكافحة الجريمة، وتطوير حماية أنظمة المعلوماتية.
- ضرورة تعزيز التعاون الدولي لمكافحة الجرائم المتصلة بأمن المعلومات، باعتبار ان الجرائم الواقعة على المعلومات قد تكون عابرة للحدود.
- إلزامية الاستمرار لمواكبة التطورات التقنية وضع انظمة حماية عالية، وتوعية المستخدمين، وبناء كوادر وقدرات مختصة لضمان أمن المعلومات.
- تشجيع المؤسسات على تأمين أنظمتها المعلوماتية.
- توفير مختلف الأساليب والإجراءات اللازمة لضمان حماية كافية للبيانات والمعلومات.

قائمة المصادر والمراجع

قائمة المصادر والمراجع:

أولا: قائمة المصادر

أ-القوانين:

1.القانون 04-14، المؤرخ في 10 نوفمبر 2004، المعدل والمتمم للأمر رقم 66-155، المؤرخ في 08 يونيو 1966 والمتضمن قانون الاجراءات الجزائية، ج.ر، ج.ج.د.ش العدد 71، الصادر بتاريخ في 10 نوفمبر 2004.

2.القانون 09-04 المؤرخ في 2009/08/05، المتضمن الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج.ر.ج.ج، د، ش، العدد 47، 5 أوت 2009.

3. 15-04، المؤرخ في 1 فبراير 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، ج.ر، ج.ج.د.ش، العدد 06، الصادر بتاريخ 10 فبراير 2015.

4.القانون رقم 24-06 المؤرخ في 28 أبريل سنة2024، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 8 يونيو سنة 1966 والمتضمن قانون العقوبات، ج. ر، ج. ج.د. ش العدد 30، الصادر بتاريخ 30 أبريل سنة 2024.

ب-الأوامر

1.الأمر 66-155 المؤرخ في 06/08/ 1966 المتضمن قانون الإجراءات الجزائية، ج، ر. ج، ج، د، ش، المعدل والمتمم، العدد 30، الصادر في8أوت 1966.

2. الامر رقم 06-09 المؤرخ في 15 يوليو 2006، المتعلق بمكافحة التهريب، ج.ر، ج.ج.د.ش، العدد 47، الصادر بتاريخ 19 يوليو 2006

ج-المراسيم:

1.مرسوم الرئاسي 19-172مؤرخ في 6 يونيو 2019 يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها. المتضمن قانون العقوبات، ج، ر، ج، ج، د. ش، العدد 37، 6 يونيو 2019.

2. المرسوم الرئاسي رقم 20-05 المؤرخ في 20 جانفي 2020، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، ج.ر، ج.ج.د.ش، العدد 04، الصادر بتاريخ 26 جانفي 2020.

ثانيا: قائمة المراجع

1-الكتب:

1. حسن طاهري، الجرائم الإلكترونية، ط1، دار الخلدونية، القبة القديمة، الجزائر، 2022.

2. خالد بن سليمان الغثبر، مهندس محمد بن عبد الله القحطاني، محمد بن إبراهيم السويل، **أمن المعلومات بلغة ميسرة**، ط1، مكتبة الملك فهد الوطنية أثناء النشر، الرياض 1429هـ-2009م.

3. عبد الوهاب جعيجع، **المعلوماتي وإدارة العلاقات الدولية**، الطبعة 1439هـ-2017م، دار الخلدونية، الجزائر، 2017.

4. كوثر مازوني، **الجريمة المعلوماتية**-أعمال ندوة وطنية، ط1، دار الخلدونية، القبة القديمة، الجزائر، 2022.

5. محمد عبد حسين الطائي، ينال محمود الكيلاني، **إدارة أمن المعلومات**، ط1، عمان، دار الثقافة للنشر والتوزيع، 1436-2015م.

6. مصباح صالح الفيداعي، **المعلومات والمعلوماتية**، ط1، الكويت: جامعة الكويت، لجنة التأليف والتعريب والنشر، 1999.

7. مصطفى علي اللحام، **المدخل إلى علم المكتبات ومصادر المعلومات**، المنهل، 2016.

2- المقالات:

1. حوالف عبد الصمد، "**الأليات القانونية لتلافي الجريمة المعلوماتية والحد من انتشارها وفقا للتشريع الجزائري**"، مجلة الفكر القانوني والسياسي، كلية الحقوق والعلوم السياسية جامعة تلمسان، العدد الرابع، 2018.

2. سليمة سعيدي، بلال حجاز، **نموذج ماكمبر Mc Cumber للأمن المعلوماتي (مدخل وثائقي)** مجلة آفاق لعلم الاجتماع، جامعة قسنطينة 2، الجزائر، العدد 1، جويلية 2020.

3. سوهيلة بضياف، آمنة حمراني، "**أمن المعلومات في الجزائر، الإجراءات والتحديات**"، المجلة الجزائرية للأمن والتنمية، المجلد 9، العدد 16، جانفي 2020.

4. عائشة عبد الحميد، "**الجرائم المعلوماتية وكيفية مكافحتها**"، مجلة الاناسة وعلوم المجتمع، العدد 07، جامعة المسيلة، الجزائر، 2020.

5. قدايفة أمينة، "**استراتيجية أمن المعلومات**"، مجلة أبعاد اقتصادية، جامعة محمد بوقرة – بومرداس، العدد 06، 2016.

6. محمد خليفة، "**خصوصية الجريمة الالكترونية وجهود المشرع الجزائري في مواجهتها**"، مجلة دراسات وأبحاث، جامعة الجلفة، المجلد1، العدد1، 2009.

7. حزام فتيحة، "**حماية الانظمة الرقمية بين الآليات التقنية وأجهزة الحماية قراءة في أحكام المرسوم الرئاسي 20-05**"، مجلة الحقوق والعلوم الانسانية، جامعة الجلفة، المجلد 13، العدد 03، أكتوبر 2020.

3- الأطروحات والرسائل الجامعية:

أ-أطروحات الدكتوراه:

1. بورابة صورية، **قواعد الأمن المعلوماتي-دراسة مقارنة-**، رسالة مقدمة لنيل شهادة الدكتوراه في العلوم، كلية الحقوق والعلوم السياسية، جامعة الجيلالي الياس. سيدي بلعباس، تخصص علوم قانونية، فرع قانون خاص، 2015-2016.

2. عزيزة رابحة، **الأسرار المعلوماتية وحمايتها الجزائية**، أطروحة لنيل شهادة الدكتوراه، علوم في القانون الخاص، جامعة أبو بكر بلقايد، تلمسان، الجزائر، 2017، 2018.

ب-مذكرات الماستر:

1. أمال شيخي، **جريمة التزوير في التشريع الجزائري**، مذكرة تخرج لنيل شهادة الماستر، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقــوق والعلوم السياسية، جامعة مولاي طاهر، سعيدة، الجزائر، 2019/2018.

2. بن نعوم خالد أمين، **إجراءات التحقيق في الجريمة المعلوماتية في التشريع الجزائري**، مذكرة لنيل شهادة الماستر، تخصص قانون قضائي، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس مستغانم، 2019/2018.

3. حمودي كاهنة، **نظام أمن المعلومات في الجزائر دراسة حالة بلدية سوق الإثنين ولاية تيزي وزو 2014_2017**، مذكرة مقدمة لنيل شهادة الماستر في العلوم السياسية والعلاقات الدولية، تخصص سياسات عامة وإدارة محلية، كلية الحقوق والعلوم السياسية قسم العلوم السياسية، جامعة مولود العمري_ تيزي وزو 2016.

4. عبد العزيز أحمد، **خصوصية التحقيق في الجريمة المعلوماتية**، مذكرة مقدمة لنيل شهادة الماستر في الحقوق تخصص القانون الجنائي وعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة الدكتور الطاهر مولاي سعيدة، 2021-2022.

5. فادية عليوان، **جريمة الغش المعلوماتي في التشريع الجزائري**، مذكرة لنيل شهادة الماستر، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة مولاي الطاهر، سعيدة، الجزائر، 2015/2014.

6. محمد الشريف بولعراس، **جريمة التزوير المعلوماتي**، مذكـرة لنيل شهـادة الماستر، تخصص قانون، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعريريج، الجزائر، 2022/2021.

7. محمد بغداد، **الأمن المعلوماتي وسبل حماية في الجزائر**، مذكرة لنيل شهادة ماستر، تخصص تسيير وإدارة – الجماعات المحلية، كلية الحقوق والعلوم السياسية، جامعة مولاي طاهر، سعيدة، 2017-2018.

4-مداخلات:

1. فشار عطا الله، **مواجهة الجريمة المعلوماتية في التشريع الجزائري**، الملتقى المغربي حول القانون والمعلوماتية، اكاديمية الدراسات العليا، ليبيا، أكتوبر، 2009.

5-المواقع الإلكترونية:

1. https://books.gool.dz.

فهـرس المحتويـات

فهـــرس المحتويـــات

الملخص:

يشهد العالم تطورا متسارعا في التكنولوجيا الحديثة، وتعتمد المؤسسات والهيئات الحكومية بشكل متزايد عليها. وقد أدى هذا الاعتماد الكبير إلى جعل قضية أمن المعلومات ذات أهمية قصوى لضمان فعالية إدارة المعلومات وحمايتها من مختلف الجرائم الواقعة على المعلومات التي انتشرت بانتشار استخدام الحاسوب وشبكة الانترنت في مختلف مجالات الحياة.

حيث تسعى هذه الدراسة إلى استكشاف المفاهيم المتعلقة بأمن المعلومات وتسليط الضوء على الإجراءات والأساليب المتنوعة المتبعة في هذا المجال. إضافة إلى أن الأمن المعلوماتي في القانون الجزائري يهدف إلى حماية الأنظمة المعلوماتية والشبكات الالكترونية من الهجمات والتسلل وضمان سرية البيانات الشخصية وتوفير بنية آمنة لتعامل مع المعلومات وحمايتها من المخاطر.

الكلمات مفتاحية: الأمن المعلوماتي، القانون الجزائري، الجرائم المعلوماتية، حماية المعلومات، أنظمة المعلومات.

Abstract:

The world is witnessing rapid development in modern technology, and institutions and institutions and government agencies increasingly rely on it. This heavy reliance has made the issue of information security of utmost importance to ensure the effectiveness of information management and its protection from various information crimes that have spread use of computers and the internet in various areas of life.

This study seeks to explore the concepts related to information secutity and shed light on the various procedures and methods used in this field. In addition, information security in Algerian law aims to protect information systems and electronic networks from attacks and intrusion, ensure the confidentiality of personal date, and provide a secure structure for handing information and protecting from risks.

Keywords Information security, Algerian law, information crimes, information protection, information systems,.