جامعة محمد خيضر بسكرة

كلية الحقوق والعلوم السياسية

قسم القانون الخاص

مذكرة ماستر

ميدان: الحقوق والعلوم السياسية

فرع الحقوق

تخصص:قانون إداري

قسم قانون عام

رقم:

إعداد الطالبة: عليه زهرة

يوم:

موضوع المذكرة:

تأمين المعاملات الإدارية الإلكترونية

لجنة المناقشة

العضو 1	الرتبة	الجامعة	رئيسا
إلهام خوني	أستاذ محاضر ب	بسكرة	مشرفا
العضو 3	الرتبة	الجامعة	مناقشا

السنة الجامعية:2025-2026


بسم الله الرحمن الرحيم

شكر وتقدير

الحمد لله الذي بنعمته تتمّ الصالحات، وبفضله وتوفيقه، نحمده سبحانه وتعالى على ما أنعم به علينا من توفيق وإعانة لإتمام مذكرة تخرجي، والذي أنار دربي ووفقني لإتمام هذا العمل المتواضع، فله الحمد أولاً وآخراً.

أتقدم بأسمى آيات الشكر والتقدير وأصدق عبارات الامتنان إلى أعز وأغلى الناس على قلبي

إلى أبي الغالي، سندي وقوتي، الذي علّمني الصبر والإصرار، وغرس فيّ حب العمل والاجتهاد، وكان دائمًا الداعم الأول لي في مسيرتي، فجزاه الله عني خير الجزاء.

إلى أمي الحبيبة، نبع الحنان

ومصدر الأمان، التي كانت دعواتها سر نجاحي وتوفيقي، والتي لم تبخل عليّ يومًا بحبها ودعمها ، فكانت لي الأم والمربية والصديقة، والأستاذة حفظها الله وأدامها تاجًا فوق رأسي.

كما لا يفوتني أن أتوجه بجزيل الشكر وعظيم الامتنان إلى أستاذتي المشرفة، التي لم تبخل عليّ بتوجيهاتها القيّمة ونصائحها السديدة، وكانت نعم المرشدة والداعمة طوال فترة إنجاز هذا العمل.

الإهداء

قال تعالى:"وقل اعملوا فيرى الله عملكم ورسوله والمؤمنون"

اهدي هذا العمل إلى **والدي العزيزين** حفظهما الله اللذين كانا سندي و دعائي الدائم، وسببا في كل خطوات نجاحي اهدي ثمرة جهدي المتواضعة عرفانا بفضلهما الكبير.

إلى أختي الكبرى **منال** و إلى أختي و توأم روحي **ذكرى** و إلى الغالية **روميسة** بكل الحب و التقدير.

إلى إخوتي الأعزاء **حسام الدين** و **عادل** و **عبد الرؤف** و **كنان المولود الصغير ابن أخي** الذين كانوا دائما مصدر دعم و سند.

فهرس المحتويات

العنوان	الصفحة
بسملة	ا
الإهداء	ب
الشكر والعرفان	ج
الفهرس	د
مقدمة	01
الفصل الأول : الآليات القانونية لتأمين المعاملات الإدارية الاليكترونية	05
المبحث الأول: تقنيات تامين المعاملات الإدارية الإلكترونية	06
المطلب الأول: التوقيع الالكتروني	06
المطلب الثاني: التصديق الالكتروني	20
المطلب الثالث: التشفير	28
المبحث الثاني: تقنيات و أدوات الأمن السبيراني	34
المطلب الأول: مفهوم الأمن السبيراني	34
المطلب الثاني: أنواع الهجمات السيبرانية	40
الفصل الثاني : الحماية القانونية لتأمين المعاملات الإدارية الاليكترونية	49
المبحث الأول : الحماية الإدارية لتأمين المعاملات الالكترونية:	50
المطلب الأول: مفهوم التوثيق الالكتروني	51
المطلب الثاني: الرقابة الإدارية على المعاملات الإدارية الالكترونية	72
المبحث الثاني الحماية الجزائية لتأمين المعاملات الإدارية الإلكترونية	92
المطلب الأول مفهوم الجريمة الإلكترونية	92
المطلب الثاني:الجريمة المعلوماتية في نطاق القانون الداخلي والعقوبات المقررة لها	103
خاتمة	109
قائمة المصادر والمراجع	111
ملخص	117



مقدمة

مقدمة

لقد عرف العالم في الآونة الأخيرة تطورات كبيرة في جميع المجالات العلمية والتكنولوجية التي أحدثت تغيير للحياة اليومية للإنسان ، وأصبحت من الركائز الجوهرية المعول عليها في تطوير التنمية الاقتصادية والاجتماعية وبذلك تم إدراج البرمجة المعلوماتية داخل عمل الإدارة وساعدها ذلك ظهور شبكة الإنترنت، من أجل تسهيل إجراءات المعاملات الإدارية وكذا التقليل من استخدام الورق، والتخلص من الأساليب التقليدية المعتمدة في تقديم الخدمات وتحسين كفاءة الأداء الإداري، الأمر الذي جعل من المعاملات الإدارية الإلكترونية ضرورة حتمية لمواكبة متطلبات العصر، خاصة في ظل الاعتماد على الأنظمة الرقمية في مختلف مجالات الحياة.

تسعى الحكومات وبعض الدول من بينها الجزائر إلى تحديث الإدارة العمومية من خلال اعتماد تكنولوجيا الإعلام والاتصال بهدف تحسين جودة و فعالية خدمات الإدارة الإلكترونية التي تعتبر من ابرز مظاهر التحول الرقمي الذي يشهده المرفق العام وتهدف إلى الانتقال من الأسلوب البيروقراطي القديم إلى إدارة رقمية مرنة مما يتيح للمواطنين تسهيل مختلف المعاملات الإدارية الإلكترونية، وإنجاز الإجراءات عن بعد بسرعة وشفافية وذلك باستخدام وسائل قانونية وتقنيات متكاملة لضمان سرية وسلامة الوثائق والبيانات التي يتم تبادلها بين الأطراف أثناء إبرام صفقات المعاملات الإلكترونية، غير أن هذا التحول الرقمي رغم ما يحققه من مزايا فإنه يواجه تحديات ومخاطر عديدة لعل أبرزها التهديدات المرتبطة بالأمن السبراني كالاختراقات الإلكترونية والهجمات على الأنظمة الإلكترونية.

أهمية الدراسة

تكمن أهمية الدراسة كونها تعالج موضوعا له أهمية كبيرة في الوقت الحالي نظرا للانتشار الواسع للأعمال الإلكترونية في مختلف الإدارات ،مما يستدعي البحث في طرق تأمين هاته المعاملات الإلكترونية من مخاطر الإختراق ،وحماية سرية البيانات والمحافظة عليها.

أسباب اختيار الموضوع

-الرغبة في التعرف على الوسائل القانونية والتقنية لتأمين المعاملات الإدارية الالكترونية.

- حداثة موضوع تأمين المعاملات الإدارية الإلكترونية في مجال الإدارة وتطبيقاتها مما يستوجب تناوله بالدراسة.

-التعرف على الأمن السبراني وعلاقته بتأمين المعاملات الإدارية الإلكترونية

إشكالية الدراسة

انطلاقا مما سبق ارتأينا طرح الإشكالية التالية :

هل وفق المشرع الجزائري في وضع اليات قانونية لتأمين المعاملات الإدارية الإلكترونية في ظل تزايد الجرائم الإلكترونية التي تمس بسلامة وأمن المعلومات والوثائق الإدارية ؟

ومن الإشكالية نطرح الأسئلة الفرعية التالية:

- ماهي الوسائل القانونية والتقنية لحماية المعلومات والوثائق الإدارية الإلكترونية؟
- ما هو الأمن السبراني ودوره في تأمين المعاملات الإدارية الإلكترونية؟
- ماهي التدابير والإجراءات الجزائية والإدارية للوقاية من الجرائم الإلكترونية؟

وقصد الإجابة على الإشكالية قمنا بصياغة مجموعة الفرضيات:

صعوبات الدراسة

ككل بحث يسعى إلى الوصول حقائق وتماشيا مع المحيط صادفتنا عراقيل، تمكنا من تخطي البعض منها وهناك ما لم نتجاوزها نذكر منها:

قلة الدراسات السابقة للآليات القانونية والتقنية لتأمين المعلومات والوثائق الإدارية.

قلة المراجع في ما يتعلق بموضوع تأمين المعاملات الإدارية الإلكترونية

الدراسات السابقة

- **الدراسة الأولى**

بوعقل مصطفى آلية وقاية المعاملات الإدارية الإلكترونية في ظل حكومة تكنولوجيا المعلومات تهدف هذه الدراسة إلى معالجة أساليب وقاية المعاملات الإدارية الإلكترونية مع الأخذ بعين الاعتبار أساسيات حماية الشبكات المحلية.

❖ **الدراسة الثانية**

عقوني محمد الآليات القانونية والتقنية لحماية التوقيع الالكتروني، تعالج هذه الدراسة مدى نجاعة الآليات القانونية والتقنية التي اقرها المشرع الجزائري في القانون رقم04/15المحدد للقواعد العامة والمتعلقة بالتوقيع والتصديق الالكتروني.

❖ **الدراسة الثالثة**

كبير آمنة التصديق الإلكتروني دراسة مقارنة، تعالج هذه الدراسة البحث عن حلول تقنية قانونية لحماية أمن المعلومات والوثائق عموما.

المنهج المتبع

اعتمدت المنهج الوصفي التحليلي من أجل سرد وتحليل مختلف المفاهيم المتعلقة بالموضوع والكشف عن أهمية الوسائل القانونية في المعاملات الإدارية الالكترونية .

خطة الدراسة

من اجل الإلمام بالموضوع قسمت البحث إلى فصلين وهما:

- **الفصل الأول:** بعنوان الآليات القانونية والتقنية لتأمين المعلومات الإدارية الالكترونية حيث قسمت هذا الفصل إلى مبحثين

- **المبحث الأول** بعنوان الوسائل القانونية والتقنية لتأمين المعاملات الإدارية الإلكترونية
- **المبحث الثاني:** بعنوان تقنيات وأدوات الأمن السبراني

- **الفصل الثاني** بعنوان الحماية الإدارية والجزائية لتأمين المعاملات الإدارية الإلكترونية

- **المبحث الأول:** الحماية الإدارية للمعاملات الإدارية الإلكترونية والجزاءات المترتبة عليها.
- **المبحث الثاني:** الحماية الإدارية والتقنية، مع التركيز على ضمانات أمن المعطيات وآليات الرقابة المفروضة.



الفصل الأول

الآليات القانونية لتأمين المعاملات الإدارية الإلكترونية

تمهيد:

مع التطور السريع للتقنيات الرقمية وازدياد الاعتماد على الأنظمة الإلكترونية في إدارة المعاملات الإدارية، أصبحت الحاجة إلى تأمين هذه المعاملات أمراً حيوياً لضمان سلامة البيانات وصحة الإجراءات القانونية. فالانتقال من المعاملات التقليدية الورقية إلى البيئة الرقمية لم يقتصر على مجرد تغيير الوسيلة، بل فرض تحديات جديدة تتعلق بمصداقية التوقيعات، وسرية المعلومات، وحماية حقوق الأطراف، إضافة إلى الوقاية من المخاطر القانونية المرتبطة بالاحتيال أو التلاعب بالبيانات.

ولهذا، عمد المشرّع والهيئات المختصة إلى وضع منظومة متكاملة تتضمن وسائل قانونية وتقنية لضمان صحة وسلامة المعاملات الإدارية الإلكترونية. وتتمثل هذه الوسائل أساسًا في التوقيع والتصديق الإلكترونيين، الذي يوفر إثبات الإرادة القانونية للأطراف، والتشفير الإلكتروني الذي يضمن حماية البيانات ومنع الوصول غير المصرح به إليها، بالإضافة إلى آليات لحماية الخصوصية ومكافحة الجرائم الإلكترونية التي تستهدف البيئة الرقمية.

المبحث الأول: الوسائل القانونية لتامين المعاملات الإدارية الإلكترونية

يهدف هذا المبحث إلى دراسة الوسائل القانونية المعتمدة لتأمين المعاملات الإدارية الإلكترونية، موضحًا دور كل منها في تعزيز الثقة بالنظام الرقمي وضمان الاعتراف القانوني بالمعاملات المنجزة إلكترونيًا. كما يسعى إلى ربط الجانب القانوني بالجانب التقني، بما يبرز مدى تكامل هذه الوسائل في حماية الحقوق، وتثبيت الحجية القانونية للمعاملات، ورفع مستوى الأمن الرقمي في إدارة الأعمال الإلكترونية.

المطلب الأول: التوقيع الالكتروني:

لقد نشأ التوقيع مع بدايات التعاملات التجارية التي عرفها الإنسان، حيث ارتبط منذ نشأته بفكرة إبرام العقود وتوثيق الالتزامات. وقد اتخذ في مراحله الأولى طابعًا ماديًا، تمثل في استخدام رموز أو علامات أو أشكال توضع على وسائط مختلفة كالفخار أو الجلود أو

المخطوطات، بهدف التعبير عن إرادة الشخص وإثبات ارتباطه القانوني بما يصدر عنه من تصرفات، إلى جانب إضفاء صفة الرسمية على المعاملات المتبادلة بين الأفراد.

ومع التطور المتسارع في وسائل الاتصال وظهور البيئة الرقمية، لم يعد التوقيع التقليدي القائم على الكتابة اليدوية قادرًا على مواكبة طبيعة المعاملات الحديثة التي انتقلت من الشكل المادي إلى الشكل الإلكتروني. وقد فرض هذا التحول ضرورة إيجاد بدائل قانونية وتقنية تتلاءم مع خصوصيات الإدارة الإلكترونية، خاصة في ظل السرعة الكبيرة التي تتم بها المبادلات واتساع نطاقها عبر الحدود دون الحاجة إلى التواجد المادي للأطراف.[1].

في هذا السياق، ظهر التوقيع الإلكتروني ضمن نطاق التعاقد عبر الوسائط الرقمية كآلية تقنية حديثة تهدف إلى توثيق المعاملات والعقود المبرمة إلكترونيًا، حيث أصبح يحل محل التوقيع التقليدي اليدوي، بما يتوافق مع خصوصية هذه المعاملات القائمة على التكنولوجيا. إذ تتم هذه الأخيرة عن بُعد بين أطراف لا يجمعهم مكان واحد، بل يتم تفاعلهم عبر شبكة الإنترنت، الأمر الذي يستلزم إقرار وسائل تضمن سلامة التعبير عن الإرادة، وتؤكد صحة إسناد التصرفات إلى أصحابها داخل البيئة الرقمية[2].

وعلى هذا الأساس، فإن تناول موضوع التوقيع الإلكتروني لابد من التطرق إلى تحديد مفهومه وبيان أهميته ضمن إطار المعاملات الإلكترونية، باعتباره الركيزة الأساسية التي يقوم عليها نظام التصديق الإلكتروني، الذي يشكل بدوره آلية مكملة تسهم في تعزيز الثقة والمصداقية في المعاملات الإدارية والعقود المبرمة في البيئة الرقمية، دون أن يفقد التوقيع وظيفته الجوهرية المتمثلة في التعبير عن الإرادة،.

الفرع الأول: مفهوم التوقيع الالكتروني:

يعتبر التوقيع الإلكتروني بمثابة العنصر الثاني من عناصر الدليل الكتابي المعد أصلا للإثبات، وهو الذي ينسب الورقة إلى من وقعها حتى ولو كانت مكتوبة بخط غيره، وبالرغم من انتشار استخدام تقنيات الاتصال الحديثة في إبرام العقود عن بعد إلا أن التوقيع التقليدي

[1] كرار غانم بستان1، الأستاذة الدكتورة/أودين سلوم1. (2025). الوسائل الالكترونية للتثبت من الأهلية ودورها في حماية المتعاقد الإلكتروني. مجلة العلوم الإنسانية والطبيعية، 6(1) ، 517-534.

[2] أسامة علي إبراهيم الصمادي. (2023). التوقيع الإلكتروني وحجيته في القانون الأردني. مجلة العلوم الإنسانية والطبيعية، 4(3) ، 934-946.

يعتبر من أهم المشكلات التي تقف حجر عثرة أمام مثل هذا النوع من التوقيع، وذلك بهدف حل المشكلات القانونية التي بدأت تفرض نفسها بقوة في مجال إثبات العقود الإلكترونية[1].

وعلى هذا الأساس، سيتم في هذا الفرع تناول مفهوم التوقيع الإلكتروني من منظور فقهي وقانوني، مع إبراز موقف المشرّع الجزائري من تنظيمه.

1. تعريف التوقيع الالكتروني من الناحية الفقيه والقانونية وموقف المشرع الجزائري:

حتى يكتسب المستند قيمته الكاملة في الإثبات، يتعيّن أن يكون مرفقًا بتوقيع صادر عمّن نُسب إليه، بحيث يُعد هذا التوقيع وسيلة مهمة لإسناد مضمون الوثيقة إلى صاحبها. ويُفهم التوقيع، سواء كان تقليديًا أو إلكترونيًا، على أنه تعبير صريح عن إرادة الشخص في الالتزام بتصرف قانوني معيّن، ويمكن أن يتحقق ذلك بوسائل متعددة مثل الإمضاء أو بصمة الإصبع أو الختم.*1*

ونتناول فيما يلي: تعريف التوقيع الالكتروني في الفقه والقانون ثم نتطرق إلى موقف المشرع الجزائري من التوقيع الالكتروني.

ولقد تعددت التعريفات الفقهية والقانونية للتوقيع الالكتروني،وذلك لاختلاف الزاوية التي يُنظر بها كل تعريف فهناك من ركّزت على الوسيلة التي يتم بها التوقيع الالكتروني، وهناك تعريفات أخرى ركزت على الوظيفة التي يقوم بها.

ومن هنا ذهب بعض الفقهاء إلى أن اصطلاح التوقيع له معنيان الأول فعل أو عملية التوقيع ذاتها أي واقعة وضع التوقيع على مستند يحتوي على معلومات معينة تسمح بتمييز شخص الموقع، والمعنى الثاني هو المقصود من التوقيع في نطاق الإثبات الذي يقصد به" علامة خطية خاصة ومميزة يضعها الموقع بأي وسيلة على مستند لإقراره.*3*

و من المنظور القانوني، يُعدّ التوقيع الإلكتروني من المفاهيم المستحدثة التي لم تكن معروفة في البناء التقليدي للنظرية القانونية، الأمر الذي استدعى تدخل التشريعات على المستويين الدولي والوطني لوضع إطار قانوني يضبط أحكامه ويزيل ما يكتنفه من غموض.

[1]الكاتب: سمية عبد العزيز، التوقيع الإلكتروني وسيلة حديثة للإثبات – دراسة مقارنة المجلد 9، العدد 17، الصفحات 160-211، مقال على الانترنت ،2014، الموقع الالكتروني: المعارف.

وقد حظي هذا المفهوم باهتمام واسع من قبل المنظمات الدولية والإقليمية، مما أسهم في بلورة قواعد تنظيمية تبنّتها لاحقًا تشريعات العديد من الدول. وفي هذا السياق، نصت المادة اولى الفقرة الثانية من القانون رقم 02-26المتعلق بخدمات الثقة للمعاملات الإلكترونية وبالتعريف الإلكتروني تنص على ما يلي: "هي بيانات في شكل إلكتروني مرفقة او مرتبطة منطقيا ببيانات اخرى في شكل إلكتروني، يستخدمها الموقع للتوقيع، تستعمل كطريقة للتوثيق. "[3]

كما نصّ المشرّع الجزائري في المادة 02 من القانون رقم 15-04 المؤرخ في 1 فبراير 2015، والمتعلق بتحديد القواعد العامة الخاصة بالتوقيع والتصديق الإلكترونيين، على تنظيم هذا المجال وإرساء أسسه القانونية ومن هنا كانت الخطوة الأولى لميلاد التوقيع الإلكتروني هو صدور القانون النموذجي للتجارة الالكترونية سنة 1996م، والذي أعطى ملامح عامة من التوقيع الالكتروني وهذا بموجب نص المادة 7 منه، حيث قرّر بأنّه:" عندما يشترط القانون وجود توقيع من شخص يستوي ذلك الشرط بالنسبة إلى رسالة البيانات التالية

- استعملت طريقة تقنية تهدف إلى التحقق من هوية ذلك الشخص والتدليل على موافقة ذلك الشخص على المعلومات الواردة في رسالة البيانات.

- يشترط في هذه الطريقة أن تكون موثوقة بالقدر المناسب للغرض الذي أنشئت من اجله رسالة البيانات في ضوء كل الظروف بما في ذلك أي اتفاق متصل بالأمر[1].

وبعد تطرقنا إلى تعريفات الفقهية والقانونية للتوقيع الإلكتروني نرى موقف المشرع الجزائري في النقطة التالية: تنص المادة 327 الفقرة الثانية منن التقنين المدني الوطني

[1]-خديجة عبد اللاوي، أستاذ محاضر قسم "أ"، محاضرات في قانون المعاملات الالكترونية، مطبوعة بيداغوجية موجهة لطالبة السنة أولى ماستر تخصص قانون خاص،2022/2021، ص 98

2-المادة 327 فقرة 2 من الأمر رقم 75-58 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر 1975، المتضمن القانون المدني، المعدل والمتمم.

3اللمادة 01الفقرة 02من القانون رقم 26-02 المؤرخ في 29 شعبان عام 1447 الموافق 17 فبراير سنة 2026، المحدد للقواعد العامة المتعلقة بخدمات الثقة للمعاملات الإلكترونية وبالتعريف الإلكتروني، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 14، الصادرة بتاريخ 18 فبراير 2026. ص 7

المعدل والمتمم على أنه"...يعتد بالتوقيع الالكتروني وفق الشروط وفق الشروط المذكورة في المادة 323 مكرر 1 أعلاه"[2]

2. موقف المشرع الجزائري من التوقيع الإلكتروني:

لم يقدم المشرع الجزائري على وضع تعريف صريح للتوقيع الإلكتروني، وهو توجه يمكن تفسيره برغبته في ترك مهمة ضبط هذا المفهوم للاجتهاد الفقهي، أو باكتفائه بما ورد بشأن تعريف الكتابة الإلكترونية نظرًا للتقارب بينهما. كما قد يكون قد سعى إلى تجنّب التكرار التشريعي الذي وقعت فيه بعض القوانين المقارنة، لاسيما التشريع المصري. غير أنّ هذا النهج لا يخلو من صعوبات عملية، خاصة في ظل تنوّع الوسائل والأنظمة المعلوماتية التي قد يدّعي مستعملوها قيامها بوظيفة التوقيع الإلكتروني. وفي هذا الإطار، شددت التوجيهات الصادرة عن لجنة الأمم المتحدة للقانون التجاري الدولي على ضرورة اعتماد معايير دقيقة يمكن الرجوع إليها لتقييم مدى صلاحية وسيلة معينة لاعتبارها توقيعًا إلكترونيًا، بما يكفل إرساء الثقة القانونية في المعاملات الرقمية.

3. خصائص التوقيع الإلكتروني

يمتاز التوقيع الإلكتروني بخصائص تميزه عن التوقيع التقليدي وهي كالتالي:

- يتكون التوقيع الالكتروني من عناصر منفردة وسمات خاصة بالموقع تتخذ شكل أرقام أو حروف أو إشارات أو رموز أو غيرها.
- أنه يحدد شخصية الموقع ويميزه عن غيره.
- أنه يعبر عن رضاء الموقع بمضمون المحرر.
- التوقيع الالكتروني يتصل برسالة الكترونية وهي عبارة عن معلومات يتم إنشاؤها أو إرسالها أو تسلميها أو تخزينها بوسيلة الكترونية.
- التوقيع الإلكتروني يحقق أغراض ووظائف التوقيع التقليدي متى كان صحيحا وأمكن إثبات نسبته إلى موقعه.
- أنّه يحقق الأمان والخصوصية والسرية في نسبته للموقع بالنسبة للمتعاملين مع أنواعه وخاصة مستخدمي شبكة الانترنت وعقود التجارة الدولية.

4. شروط التوقيع الإلكتروني

أولا: الشروط الشكلية

أ. شهادة التصديق الالكترونية:

تُعتبر شهادة التصديق الإلكتروني وسيلة ضمان للمتعاقدين، إذ تعمل على التحقق من هوية الموقّع بما يمنع انتحال الهوية الشخصية ، كما تكفل سلامة المعاملة الإلكترونية وصحتها وعدم قابليتها للتعديل. وهذا ما يدفع إلى البحث في طبيعتها القانونية وتحديد مركزها.

تعريف شهادة التصديق الالكترونية:

قام المشرّع الجزائري بتعريف شهادة التصديق الإلكتروني في إطار القانون رقم 15-04 المؤرخ في 01 فبراير 2015 المتعلق بالتوقيع والتصديق الإلكترونيين، حيث نصّت المادة 12 فقرة 7 على أن التوقيع الإلكتروني يجب أن يكون مرتبطًا بالبيانات المرتبطة به ارتباطًا يضمن إمكانية الكشف عن أي تعديل قد يطرأ عليها لاحقًا، بما يحقق حماية سلامة الوثيقة الإلكترونية ويعزز مصداقيتها". 1

يُلاحظ من هذا التعريف أن شهادة التصديق الإلكتروني تُعد وثيقة رقمية تهدف إلى التحقق من صحة التوقيع الإلكتروني وضمان حجيته القانونية. كما تسهم هذه الشهادة في إثبات العلاقة بين التوقيع وصاحبه عبر تحديد هويته بدقة، بما يسمح بإسناد التوقيع إلى الشخص المعني دون سواه.

ب. بيانات التحقق من التوقيع الإلكتروني:

نصّت المادة 5 فقرة 2 من نفس القانون على أن بيانات التحقق من التوقيع الإلكتروني هي الرموز أو مفاتيح التشفير العمومية أو أي بيانات أخرى تُستعمل لغرض التحقق من التوقيع الإلكتروني. وتُعد هذه البيانات في شكل رموز وإشارات غير مفهومة، وذلك بهدف حمايتها من اطلاع الغير عليها. كما تتمثل أيضًا في مفتاح تشفير عمومي قد يكون معروفًا لدى أكثر من جهة أو شخص، ويُستخدم في التحقق من التوقيع الإلكتروني وفي معالجة الرسائل المشفّرة. غير أن هذا المفتاح لا يُمكّن من فك شفرة الرسائل التي تم تشفيرها

بالمفتاح الخاص، إذ إن عملية فك التشفير تبقى من صلاحية صاحب المفتاح الخاص وحده.[2]

فالعديد من المستخدمين يستعملون مفاتيح عامة حقيقية لهم، وبإمكانهم نشرها على مواقعهما وأي بيانات أخرى مستعملة من أجل التحقق من التوقيع الالكتروني.

ذلك أن التوقيع الالكتروني لا يعتمد على التشفير فقط، فهناك تقنيات جديدة للتحقق كالتوقيعات البيومترية أو التوقيع بالقلم الإلكتروني، وهي في مجملها صور وأنواع للتوقيع الإلكتروني[1].

نصّ المشرّع في المادة 2 فقرة 2 على أن "الموقّع هو شخص طبيعي يحوز بيانات إنشاء التوقيع الإلكتروني ويتصرف بها لحسابه الخاص أو لحساب الشخص الطبيعي أو المعنوي الذي يمثله"[1] كما عرّفت المادة 3 فقرة 2 من نفس القانون بيانات إنشاء التوقيع الإلكتروني بأنها "بيانات فريدة، مثل الرموز أو مفاتيح التشفير الخاصة، التي يستخدمها الموقّع لإنشاء التوقيع وعليه، فإن منظومة إنشاء بيانات التوقيع الإلكتروني تُعد الأداة أو النظام التقني في إنشاء التوقيع الإلكتروني وتكوينه. [2]"

ثانيا: الشروط الموضوعية للتوقيع الإلكتروني

1. الصفات الواجب توافرها في التوقيع الإلكتروني:

نصّت المادة 7 من القانون رقم 15-04 على مجموعة من شروط التوقيع الإلكتروني، من بينها وجوب إنشائه استنادًا إلى شهادة تصديق إلكتروني موصوفة. ويُفهم من هذا الشرط أن التوقيع الإلكتروني يجب أن يتمتع بحجية قانونية من خلال توثيقه عبر شهادة تصديق صادرة عن هيئة مختصة معتمدة أو مرخص لها، بما يضمن التحقق من

[1] المحامي، الدكتور محمد فواز المطالقة، الوجيز في عقود التجارة الالكترونية، جامعة البلقاء التطبيقية، كليةإربد، ص ص174-178.

[2] ا المادة 5الفقرة 2من قانون 04-15 المتعلق بالتوقيع والتصديق السالف الدكر2015.

1-المادة 2الفقرة 2من القانون رقم 04-15 المؤرخ في 01 فبراير 2015المتعلق التوقيع والتصديق الالكترونيين ، الجريدة الرسمية 06الصادر في 15فبراير 2015.

2 - المادة 03الفقرة 02من القانون 04-15 السالف الذكر.

3 -المادة 07من القانون 04-. 15السالف الذكر .

هوية الموقّع ومنع أي انتحال للشخصية، وذلك وفق إجراءات تصديق معترف بها رسميًا، بما يؤكد نسبة بيانات الرسالة إلى صاحبها وصحة التوقيع

كما يتناول هذا الشرط سالمة التوقيع الإلكتروني وسالمة المعلومات التي وقعها، بحيث أن سلامة المستند الإلكتروني وسالمة التوقيع مرتبطين يبعضهما ارتباطا وثيقا.[3]

2. ارتباط التوقيع الإلكتروني بالموقع دون سواه:

يُفهم من هذا الشرط أن يكون التوقيع المثبّت على المحرر الإلكتروني كاشفًا عن هوية شخص محدد، بحيث يُنسب إليه بصورة واضحة. وحتى يؤدي التوقيع وظيفته الإثباتية، ينبغي أن يميز صاحبه عن غيره من الأشخاص ويحدد شخصيته بدقة، إذ لا يُعتد به قانونًا إذا لم يكن قادرًا على إظهار هوية الموقّع بشكل جلي. ولا يقتصر هذا الشرط على الفقه القانوني فقط، بل تبنّته أيضًا غالبية التشريعات الوطنية والدولية التي أكدت ضرورة توافره لضمان حجية التوقيع الإلكتروني.

3. تحديد هوية الشخص:

يشترط في التوقيع الإلكتروني، حتى يُعتد به كوسيلة للإثبات، أن يكون عنصرًا مُميزًا يحدد هوية الموقّع بدقة ويميزه عن غيره من الأشخاص، وذلك بالنظر إلى اعتماده على معطيات أو رموز سرية خاصة بكل مستخدم. كما ينبغي أن يصدر عن صاحب السند ذاته، حتى وإن تولى شخص آخر إعداد المحرر، على أن تبقى مسؤولية التوقيع منسوبة إلى صاحبه الأصلي.[1]

ولا يُعتد بالتوقيع الإلكتروني إذا صدر عن غير صاحبه، ولو تم ذلك بموجب تفويض، لأنه يُعد تعبيرًا قانونيًا شخصيًا لا يُنسب إلا لمن صدر عنه ويكشف عن هويته. وبناءً على ذلك، فإن التوقيع الذي لا يؤدي وظيفة تحديد هوية صاحبه لا يُعتد به في مجال الإثبات، وهو ما أكدته القاعدة التي تجعل من التوقيع وسيلة لإثبات هوية الموقّع وقبوله بمضمون المحرر الإلكتروني، ".

[1] صبري السعدي، شرح القانون المدني الجزائري – النظرية العامة للالتزامات (مصادر الالتزام: الواقعة القانونية والتصرف القانوني)، دار الهدى للطباعة والنشر والتوزيع، عين مليلة، الجزائر، الطبعة الثانية، 2004، ص 59.

5. أن يكون مصمما بواسطة آلية مؤمنة:

بفضل التطور التقني، أصبح بالإمكان حفظ البيانات الإلكترونية على وسائط رقمية مؤمّنة توفر درجة عالية من الأمان والسرية والثقة بين المتعاقدين، نظرًا لاعتمادها على تقنيات تشفير معقدة تجعل تعديلها أو التلاعب بها أو استرجاعها بصورة غير مشروعة أمرًا بالغ الصعوبة. كما تتولى هيئات التصديق الإلكتروني حفظ وتوثيق التصرفات الإلكترونية الصادرة عن المتعاقدين ضمن أنظمة آمنة تضمن متطلبات الأمن القانوني.

وفي هذا السياق، عرفت المادة 11 1" " من القانون 15-04 الآلية المؤمنة بقولها :" الآلية المؤمنة لإنشاء التوقيع الإلكتروني هي آلية إنشاء توقيع إلكتروني ".1

6. سيطرة الموقع على التوقيع:

من بين الشروط الأساسية للتوقيع أن يكون هذا التوقيع تحت سيطرة الموقع كاملة سواء عند إنشائه أو استعماله، بحيث لا يمكن لأحد أن يقل رموزه إلا الموقع ولا يستطيع أحد التوقيع بدلا منه، وبالتالي فإن التوقيع الإلكتروني يجب أن يتم عبر رسائل تخضع بشكل كامل للسيطرة المباشرة لصاحب التوقيع الإلكتروني.

ولكي تتحقق سيطرة الموقع على التوقيع لا بد من إمكانية السيطرة على الوسيط الإلكتروني المتضمن هذا التوقيع، وذلك لضمان أن يكون صاحب التوقيع منفردا به سواء عند التوقيع أو استعماله بأي شكل من الأشكال.2

7. ارتباطه بالبيانات الخاصة به:

رغم إن ارتباط التوقيع الالكتروني بالسند الالكتروني يبدو افتراضيا ،الا انه يحقق الأمان والسرية ،فالبيانات الالكترونية تحفظ على دعامات إلكترونية غير قابلة للتعديل ويكون التوقيع عليها بوسائل مشفرة يصعب إيجادها ،فالتوقيع الالكتروني علم يصعب تزويره لارتكازه على مفتاح التشفير الذي يضمن حمايته.

الفرع الثاني: وظائف التوقيع الإلكتروني:

1. إذا كان التوقيع التقليدي يؤدي دوراً هاماً في تحديد هوية أطراف العقد وتمييز الشخص الذي يصدر عنه التوقيع عن غيره من جهة، ومن جهة أخرى هو تعبير واضح عن انصراف إرادة ذلك الشخص إلى الالتزام بمضمون المحرر وإقراره بصحة ما ورد فيه، فإن ظهور وانتشار التوقيع الإلكتروني أدى إلى بروز وظيفة أخرى تتمثل في التحقق من الحفاظ على سلامة المحرر أثناء التعامل، وتعد هذه الوظيفة بمثابة أساس للثقة في البيئة الإلكترونية في مواجهة المخاطر التي تهدد المحررات الإلكترونية، ولذلك فإنه بواسطة التوقيع الإلكتروني نستطيع تحديد هوية الشخص الذي صدر منه التوقيع ؛ وبواسطة التوقيع الإلكتروني يستطيع صاحبه التعبير عن إرادته ؛ وعن طريق التوقيع الإلكتروني يمكن الحفاظ على سلامة مضمون المحرر الإلكترونيني

2. تحديد هوية الشخص الذي صدر منه التوقيع الالكتروني:

يستوي التوقيع الإلكتروني مع التوقيع التقليدي من حيث مقدرته الدلالية على الشخص الذي قام بالتوقيع، ولا يمكن الاعتداد بالتوقيع الإلكتروني في الإثبات إلا إذا كان يحقق هذه الوظيفة (تحديد هوية الموقع لا سيما وأن الغاية الأساسية من التوقيع هي نسبة ما ورد في المحرّر إلى الشخص الذي قام بتوقيعه)[1].

إن أبرز وظيفة للتوقيع الإلكتروني هي نسبة المحرر لشخص معين، أي تحديد الشخص الذي وقعه بما لا يدع مجالاً للشك في شخصية الموقع أو هويته الإلكترونية، فإذا لم يكن كاشفاً لهوية صاحبه ومحدداً لذاته فلا يجب الأخذ به أو الاعتداد به[2]. وهذه الوظيفة تمنع تزويره أو استخدامه من طرف شخص آخر غير صاحبه، وهذا عن طريق اعتماده على برامج معلومات تقوم بعمليات حسابية جد معقدة ليس من السهل تخمينها عكس التوقيع التقليدي الذي من الممكن تقليده[3] ، مع أن وظيفة التعرف على هوية الموقع تعتبر سهلة في

[1]– فيصل سعيد الغريب، التوقيع الالكتروني وحجيته في الإثبات المنظمة العربية للتنمية الإدارية، بحوث ودراسات،2005، ص 98.

[2] – محمد مأمون أحمد سليمان، التحكيم في منازعات التجارة الالكترونية، رسالة دكتوراه في الحقوق، كلية الحقوق جامعة عين شمس، مصر، 2009، ص 212.

[3]– مدحت محمد محمود عبد العال، المسؤولية المدنية الناشئة عن تقديم خدمة التوقيع الالكتروني، الطبعة الأولى، المركز القومي للإصدارات القانونية، مصر، 2010، ص 17.

التوقيع الإلكتروني عنه في التوقيع التقليدي، لأنه في الأولى تتم بشكل آلي عن طريق استخدام الرقم السري أو المفتاح الخاص .

3. التعبير عن إرادة الموقع

الأصل أن يوجد التوقيع التقليدي على المحرّر الورقي حيث يعد إقراراً من الموقع ورضاء منه بما ورد فيه وقبوله بالالتزامات التي تضمنها، ويسري الحكم ذاته على التوقيع في الشكل الإلكتروني حيث يفترض وجوده على المحرر الإلكتروني قرينة على قبول الموقع بما ورد في المحرر وأنه يرغب في الالتزام بمضمونه، وهو في حقيقة الأمر عملية منطقية فوق كونها مسألة قانونية وذلك أن المفترض عقلاً أن الشخص لا يمكن أن يضع توقيعه على مُحرَّر إلا إذا كان قابلاً بمضمونه[1].وبالرجوع إلى قواعد الإثبات العامة نجد أنه فيما يتعلق بحجية المحرر الورقي العرفي في الإثبات لابد لمن يريد إنكار ما ورد في المحرر أن ينكر صراحة ما نُسب إليه فيه، من خط؛ أو إمضاء؛ أو بصمة؛ أو ختم، وإلا كان حجة عليه بما ورد فيه[2] ، واستناداً لذلك فإن توقيع الشخص على محرر ما يفيد أنه يعلم ويقر بكل ما ورد فيه، وأن إرادته انصرفت إلى قبول الالتزامات الناشئة عنه، ما لم ينكر هذا الشخص ما نسب إليه من توقيع[3].

4. الحفاظ على سلامة مضمون المحرر الإلكتروني:

يسمح التوقيع الرقمي المعتمد على التشفير الامتثال بالتحقق من سلامة مضمون المحرر وذلك بفضل عملية رياضية يطلق عليها دوال أو اقتراحات التمويه، التي يتم من خلالها إنشاء شكل مضغوط من المحرر الإلكتروني يشار إليه بوجه عام بالبصمة الالكترونية للمحرر الإلكتروني، لا يمكن فهمها ولا قراءتها إلا باستخدام مفتاح معين. وبناء على ذلك توفر اقتراحات التمويه ارتباطا استدلالياً قوياً بمضمون المحرر الأصلي وتوفر في الوقت ذاته تأكيداً كافياً على أنه لم يطرأ على المحرر أي تعديل منذ أن وقع رقمياً.

[1]– نور خالد عبد المحسن العبد الرزاق، حجية المحررات والتوقيع الالكتروني في الإثبات عبر شبكة الانترنت، رسالة دكتوراه في الحقوق كلية الحقوق جامعة عين شمس، مصر، 2009، ص 61.

[2]– إيهاب سمير محمد صالح الإثبات بالمحررات الالكترونية دراسة مقارنة رسالة ماجستير في القانون الخاص كلية الحقوق جامعة الأزهر، غزة، فلسطين،2015، ص 42 43.

[3]– أبو عرابي غازي، فياض القضاة، حجية التوقيع الالكتروني، دراسة في التشريع الأردني، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد العشرون، العدد الأول،2004، ص 175.

الفرع الثالث: صور التوقيع الالكتروني:

أدى التقدم التقني في مجال التوقيع الإلكتروني إلى تنوع أشكاله تبعًا لاختلاف الأساليب والتقنيات المستخدمة في إنشائه. فبعض هذه الأشكال يعتمد على رموز أو أرقام تعريفية، بينما يستند بعضها الآخر إلى الخصائص البيومترية للأفراد، في حين تقوم فئة ثالثة على تقنيات التشفير الحديثة.

كما تختلف هذه التوقيعات من حيث درجة التعقيد أو التطور، وكذلك من حيث مستوى الأمان والموثوقية الذي توفره. وتساهم هذه الوسائل في تعزيز حماية المعاملات الإلكترونية وضمان سلامة البيانات المتبادلة عبر شبكات الاتصال، وخاصة شبكة الإنترنت، مع تباينها بين أشكال بسيطة وأخرى متقدمة، حيث تختلف من حيث درجة الأمان والثقة ، كما تساهم في حماية المعاملات الالكترونية وضمان سلامة البيانات المتداولة عبر شبكة الانترنت[1].

أولا: الأشكال البسيطة للتوقيع الالكتروني

إذا كان التوقيع التقليدي، وفق ما استقر عليه أغلب التشريعات المنظمة للإثبات، يقتصر على الإمضاء أو الختم أو بصمة الإصبع، فإن التوقيع الإلكتروني، بحكم حداثته وتطوره، قد اتخذ صورًا متعددة ذات طابع بسيط في بداياته، من بينها التوقيع باستخدام الرمز السري (الكود)، أو عبر القلم الإلكتروني، أو من خلال الماسح الضوئي.

1 – التوقيع الكودي وبالقلم الإلكتروني:

يقصد بالتوقيع الكودي ذلك التوقيع الذي يتم باستخدام البطاقة الممغنطة المقترنة برقم سري، حيث يُنشأ هذا الرقم في شكل مجموعة من الأرقام المركبة التي تُعرف بـ (Cod PIN)، ويُستخدم هذا الرمز السري لإتمام عملية التوقيع الإلكتروني والتحقق من هوية صاحب التوقيع [2] .

[1]–لبيض فايزة ، المرجع السابق ، ص284

[2]–عبد الجبار عبد القادر (سلوى)، أثر استخدام التوقيع الرقمي في العمليات المصرفية، مجلة دراسات محاسبة ومالية، منشور على الموقع الإلكتروني، جامعة بغداد العراق، المجلد الثامن، العدد 22 سنة 2013 ص 323.

2- التوقيع بالقلم الإلكتروني:

يتم هذا النوع من التوقيع بواسطة قلم إلكتروني خاص، يتيح للموقع الكتابة مباشرة على شاشة الحاسب الآلي أو الجهاز اللوحي عبر برنامج مخصص، بما يضمن سلامة التوقيع وعدم إمكانية التلاعب به لاحقًا، والتأكد من إثبات صحته[1].

3 -التوقيع بالماسح الضوئي:

يقوم التوقيع بواسطة الماسح الضوئي على فكرة تحويل التوقيع اليدوي المكتوب إلى صيغة رقمية، ويتم ذلك من خلال مسح التوقيع ورقيًا ضوئيًا ثم إدراجه داخل الملف الإلكتروني المطلوب توقيعه.

ويُستخدم الماسح الضوئي أساسًا لنقل الوثائق والصور الأصلية إلى الشكل الرقمي مع الحفاظ على خصائصها الشكلية، مما يتيح أيضًا رقمنه التوقيع اليدوي وإدراجه في المستندات الإلكترونية. وبذلك ينتقل التوقيع من هيئة ورقية خطية إلى صورة رقمية يمكن حفظها على الحاسوب أو على وسائط تخزين مختلفة، واستعمالها عند الحاجة داخل الوثائق الإلكترونية.

وعند إعادة طباعة الوثيقة، فإن النتيجة تكون غالبًا مطابقة إلى حد كبير للتوقيع الأصلي، خاصة إذا استُخدمت أدوات طباعة وورق ذي جودة عالية[2] .

ثانيا: الأشكال المتقدمة لتوقيع الالكتروني

في ظل التطورات التكنولوجية المتسارعة وتزايد الاعتماد على أسلوب التجارة الإلكترونية، برزت الحاجة الملحّة إلى البحث عن تقنيات فنية متقدمة تتجاوز الصور التقليدية الأولى للتواقيع الإلكترونية، مع الحفاظ في الوقت ذاته على الوظيفة الجوهرية للتوقيع بوصفه وسيلة لإثبات الهوية والتعبير عن الإرادة.

[1] عباس حسوني (فاطمة)، عبد كاظم (حمدية)، التوقيع الإلكتروني وحجيته في الإثبات في ظل قانون التجارة الإلكترونية والمعاملات الإلكتروني، رقم 78 لسنة 2012، مجلة رسالة الحقوق، جامعة كربلاء، كلية القانون، العراق السنة الثامنة، العدد الثاني 2016، ص 393. منشور على الموقع الإلكتروني .asjp.net

[2] -لبيض فايزة ، المرجع السابق ،ص.287

خاصة عند ارتباطها بالكتابة الإلكترونية المتداولة عبر شبكة الإنترنت. ومن بين أهم هذه الصور المستحدثة نجد التوقيع البيومتري والتوقيع الرقمي، لما يوفرانه من ضمانات تقنية وقانونية.

1- التوقيع البيومتري:

يقصد بالتوقيع البيومتري ذلك النوع من التوقيع الذي يقوم على الخصائص الجسدية والسلوكية الفريدة للفرد، والتي يُعتمد عليها في التحقق من هويته وتمييزه عن غيره. ويستند هذا النمط من التوقيع إلى مجموعة من السمات البيولوجية، مثل بصمات الأصابع أو راحة اليد من حيث شكلها،

يتم هذا التوقيع أولا بأخذ صورة إكلينيكية لأجزاء الجسم كالعين أو اليد أو الوجه البشري عن طريق تقنية متخصصة لهذه المهمة، ثم تحفظ وتخزن الصورة بطريقة شفرة من خلال مجموعة أرقام أو خانات رقمية داخل ذاكرة تقنية أو ذاكرة الحاسب الآلي والذي تمت برمجته على أساس ألا يصدر أوامره بفتح القفل المغلق ولا يسمح التعامل به إلا في حالة المطابقة مع البصمة المستخدمة في الذاكرة.

2- التوقيع الرقمي

يقصد بالتوقيع الرقمي مجموعة من البيانات أو المعلومات المرتبطة بنظام بيانات آخر، أو التي تُحوَّل إلى صيغة مشفّرة، بما يتيح التحقق من مصدرها والتأكد من سلامة محتواها وضمان عدم تعرضها لأي تعديل أو تحريف.

ووفقا للمواصفات القياسية العالمية رقم 74982 (ISO) الصادرة عن المنظمة الدولية للمواصفات والمقاييس سنة 1998، عرّف التوقيع الرقمي بأنه: (بيان أو معلومة تتصل بمنظومة بيانات أخرى، والذي يسمح للمرسل إليه إثبات مصدرها والتأكد من سلامة مضمونها وتأمينها ضد أي تحريف أو تعديل).

وتتم عملية إنجاز التوقيع عبر تحويل البيانات الواردة في المحرر، بما في ذلك الكتابة والتوقيع التقليدي، إلى صيغ رقمية مشفّرة تتمثل في أرقام سرية ومعادلات رياضية، لا تكون قابلة للاستخدام أو الفهم إلا من قبل صاحب التوقيع أو من يفوضه قانونًاويعتمد هذا التوقيع

على نظام التشفير الذي عرف بأنه: (مجموعة التقنيات التي تسمح بحماية المعلومات من التعديلات الغير مرغوب فيها أو الحفاظ على خصوصيتها من أي اختراق من خلال رموز سرية أو خاصة)[1].

المطلب الثاني: التصديق الالكتروني

يكتسي التوثيق الإلكتروني أهمية كبيرة في مجال تكنولوجيا الإعلام والإتصال الرقمية، حيث يسهم في توفير بيئة إلكترونية آمنة وموثوقة للتعامل عبر شبكة الإنترنت. وتضطلع جهات التوثيق الإلكتروني بدور الوسيط الموثوق بين أطراف المعاملات الإلكترونية، من خلال التحقق من هوية المتعاملين والتثبت من أهليتهم القانونية لإبرام التصرفات، فضلاً عن ضمان سلامة البيانات المتبادلة وصحة محتواها.

كما تتولى هذه الجهات إصدار شهادات إلكترونية معتمدة تُستخدم في تأمين المعاملات وإضفاء الحجية عليها. ونظرًا لأهمية هذا الدور، فقد حرصت مختلف التشريعات على تنظيم التزامات جهات التوثيق الإلكتروني وتحديد مسؤولياتها القانونية في حال الإخلال بالواجبات الملقاة على عاتقها.

الفرع الأول: تعريف التصديق الإلكتروني :

لقد عرفت المادة الثانية من قانون الأونسترال النموذجي لسنة 2001 التوقيع الإلكتروني بأنه مجموعة من البيانات التي تتخذ شكلاً إلكترونياً، يتم إدراجها ضمن رسالة إلكترونية أو إرفاقها بها أو ربطها بها بشكل منطقي، بما يسمح باستخدامها كوسيلة لتحديد هوية صاحب التوقيع وإظهار موافقته على مضمون الرسالة.

في حين عرف التوجيه الأوروبي التوقيع الإلكتروني بأنه بيان أو معلومة معالجة إلكترونيا، ترتبط منطقيا بمعلومات أو بيانات إلكترونية أخرى كمحرر أو رسالة، والتي تصلح كوسيلة للتمييز *وتحديد* هويته

لم يقم المشرع الجزائري بوضع تعريف صريح للتوقيع الإلكتروني، حيث اكتفى فقط بالاعتراف له بالحجية القانونية في الإثبات في القانون المدني رقم، 10-05 المؤرخ في 20

1.المادة 2 من القانون الأونسترال النموذجي المتعلق بالتوقيعات الإلكترونية سنة 2001

يونيو 2005 من خلال المادة 31 على أنه :" يعتد بالتوقيع الإلكتروني وفق الشروط المذكورة في المادة 323[1] من نفص القانون والتي أقرت الكتابة الإلكترونية بقولها:" يعتبر الإثبات بالكتابة على الورق، بشرط إمكانية التأكد من هوية الشخص الذي أصدرها، وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها". غير أنه تدارك الأمر من خلال القانون رقم 04/15 الخاص بالتوقيع والتصديق الإلكترونيين، وعرف التوقيع الإلكتروني من خلال المادة 2 فقرتها الأولى بأنه:" بيانات في شكل إلكتروني، مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى، تستعمل كوسيلة توثيق"

بالاستناد إلى هذا التعريف، يمكن القول إن التوقيع الإلكتروني يُعد وسيلة من وسائل الإثبات والتوثيق، وقد اتفق جانب من الفقه على ضرورة توافر مجموعة من الخصائص فيه، تتمثل فيما يلي:

يتميز بسمات وخصائص فردية خاصة بالموقع، قد تكون على شكل رموز أو حروف أو إشارات أو حتى أرقام، بحيث تظل مرتبطة به وحده دون غيره.

- يتيح التعرف الدقيق على هوية الشخص الموقع، وذلك من خلال تقنيات وآليات التحقق من الهوية.
- يعكس إرادة ورضا الموقع بالمحتوى الوارد في المحرر أو السند الإلكتروني.
- يُعتبر أداة توثيق مرتبطة بشكل وثيق بالبيانات والمعلومات الإلكترونية بالاستناد إلى هذا التعريف، يمكن القول إن التوقيع الإلكتروني يُعد وسيلة من وسائل الإثبات والتوثيق، وقد اتفق جانب من الفقه على ضرورة توافر مجموعة من الخصائص فيه، تتمثل فيما يلي:
- يتميز بسمات وخصائص فردية خاصة بالموقع، قد تكون على شكل رموز أو حروف أو إشارات أو حتى أرقام، بحيث تظل مرتبطة به وحده دون غيره.[2].

[1]– المادة 323 مكرر 1 من القانون رقم 05/10 المؤرخ في 20 يونيو 2005، المتضمن القانون المدني، جريدة رسمية عدد 11، 2005، جريدة رسمية عدد 04، صادرة بتاريخ 21 يونيو 2005

[2]– عيسى غسان الربضي، القواعد الخاصة لتوقيع الالكتروني ، دار الثقافة للنشر والتوزيع ، الأردن ،2009، ص 48.

أما التصديق الإلكتروني هو أداة تقنية مؤمّنة تُستخدم للتحقق من صحة التوقيع الإلكتروني أو الوثيقة الإلكترونية، بهدف إسنادها بدقة إلى شخص أو جهة معينة، ويصدر عن جهة معتمدة وموثوقة أو عن طرف محايد يتولى هذه المهمة.

كما يُعرَّف التصديق الإلكتروني بأنه مجموعة من الوسائل والعناصر التي تختلف باختلاف الهدف المراد تحقيقه من عملية التوثيق. وفي هذا السياق، يُنظر إليه أيضاً بوصفه عملية تهدف إلى التحقق من هوية المستخدم وضمان موثوقيته، وذلك من خلال الاستعانة بأجهزة وتقنيات أو كيانات مختصة ضمن أنظمة المعلومات والاتصالات، بما يسمح بإثبات شخصية المستخدم والتأكد من صحة البيانات المرتبطة"[1].

يمثل التصديق الإلكتروني إجراءً يهدف إلى ضمان أربعة متطلبات أمنية رئيسية عند تبادل المعلومات عبر الإنترنت، تتمثل في حماية السرية، والتحقق من الهوية، والحفاظ على سلامة البيانات، ومنع إنكار العمليات. وتعمل هذه المتطلبات على تعزيز الثقة في المعاملات الرقمية من خلال الاعتماد على نظام البنية التحتية للمفتاح العام.

الفرع الثاني: جهة التصديق الالكتروني

لضمان المصداقية على المعاملات الإلكترونية، بما فيها عقود التجارة الإلكترونية، تُعد الثقة أساس أي علاقة تجارية، إلا أن تحقيقها يكون أكثر صعوبة في البيئة الرقمية. ومن هنا يظهر دور التصديق الإلكتروني باعتباره آلية تقنية تهدف إلى توفير مجموعة من الضمانات الأمنية عند تبادل المعلومات عبر الإنترنت، تتمثل في سرية البيانات، والتحقق من هوية الأطراف، وسلامة المعلومات، وعدم إمكانية إنكار التصرفات. وتساهم هذه الضمانات في تعزيز الثقة في المعاملات الإلكترونية من خلال الاعتماد على بنية تحتية للمفتاح العام، بما يسمح بإسناد التصرفات إلى أصحابها الفعليين .

فأي شخص يرغب في إتمامها يحتاج إلى التأكد من صحة المعلومات ومصداقيتها، ومن هنا تبرز أهمية تدخل جهة التصديق الإلكتروني، حيث تقوم بدوره الوسيط المؤتمن بين الأطراف المتعاملة لتجنب وقوعهم في شباك الشركات الوهمية وشبكات النصب والاحتيال باستخدامها كل الإمكانيات التقنية والفنية العالية والمتاحة دراسة هذه الجهة يتطلب التطرق

[1]– إلياس ناصيف، العقد الإلكتروني في القانون المقارن، لبنان، منشورات الحلبي الحقوقية، 2009، ص 71.

لمختلف التعريفات التي وضعت بشأنها الفقرة الأولى) وتحديد دورها في مجال إثبات العقد (الفقرة الثانية)[1].

الفقرة الأولى: تعريف جهة التصديق الإلكتروني.

تُثار في الفقه والقانون عدة تسميات لجهة التصديق الإلكتروني، حيث يُطلق عليها أحياناً مقدم خدمات التصديق، بينما يسميها آخرون سلطة المصادقة، في حين يستخدم بعضهم مصطلح جهات التوثيق الإلكتروني. وتجمع هذه التسميات على الإشارة إلى جهة محايدة يقتصر دورها على التحقق من التوقيع الإلكتروني وتقديم الخدمات المرتبطة به. وقد تطورت هذه التسمية في بعض التشريعات إلى مفهوم "مؤدي خدمات الثقة"، نتيجة ظهور خدمات جديدة تهدف إلى تعزيز ثقة المتعاملين عبر شبكة الإنترنت، الأمر الذي أدى إلى تنوع التعاريف الفقهية والقانونية المتعلقة بها والتي ستتطرق إليها فيما يلي:

أولاً: التعاريف الفقهية لجهة التصديق الإلكتروني.

يُعرّف بعض من جانب الفقه جهة التصديق الإلكتروني بأنها هيئة أو جهاز يتولى إصدار شهادات إلكترونية تُثبت صحة البيانات الواردة فيها، وقد تكون هذه الهيئة ذات طابع عام أو خاص. كما يذهب بعض الفقه إلى تعريفها بأنها طرف ثالث محايد وموثوق، يقوم بدور الوسيط بين أطراف المعاملات الإلكترونية، سواء كان هذا الطرف أفراداً أو شركات أو مؤسسات مستقلة، حيث يتولى مهمة توثيق التعاملات الإلكترونية. ويتضح من هذه التعريفات أنها تركز أساساً على الجهة المصدِرة للشهادة من حيث طبيعتها واستقلاليتها، إلى جانب إبراز دورها كوسيط محايد في العملية.

ثانيا: التعاريف القانونية لجهة التصديق الإلكتروني:

وبالنظر إلى قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية، فقد ورد تعريف جهة التصديق الإلكتروني ضمن المادة الثانية في الفقرة (5) تحت تسمية "مقدّم

[1]– لبيض فايزة، المرجع السابق، ص 343.

خدمات التصديق"، حيث اعتبرته شخصًا يقوم بإصدار شهادات إلكترونية، مع إمكانية تقديم خدمات إضافية مرتبطة بالتوقيعات الإلكترونية بصفة عامة.[1]

وقد تبنّت أغلب التشريعات المقارنة هذا المفهوم، إذ نجد التوجيه الأوروبي لسنة 1999 المتعلق بالتوقيعات الإلكترونية، كما تأثر به المرسوم الفرنسي رقم 272-2001، حيث كرّسا نفس الفكرة العامة لدور مزوّد خدمات التصديق.

وفي السياق نفسه، أخذ المشرّع الجزائري بهذا الاتجاه من خلال المادة 2 الفقرة (12) من القانون المتعلق بالتوقيع والتصديق الإلكترونيين، حيث عرّفه بأنه شخص طبيعي أو معنوي يتولى إصدار شهادات التصديق الإلكتروني الموصوفة، مع إمكانية تقديم خدمات أخرى مرتبطة بمجال التصديق الإلكتروني [2]

الفقرة الثانية: دور جهة التصديق الإلكتروني.

تتعدد مهام جهة التصديق الإلكتروني بين التزاماتها تجاه صاحب الشهادة أو الموقع من جهة، وتجاه الغير من جهة أخرى، إضافة إلى المهام المرتبطة بضمان فعالية واستمرارية نظام التصديق الإلكتروني.

في ما يخص علاقتها بصاحب الشهادة والغير، تضطلع جهة التصديق بدور محوري يتمثل في التحقق، وفق آلياتها التقنية الخاصة، من صحة صدور الإرادة التعاقدية الإلكترونية عن الشخص المنسوب إليه التوقيع. ويترتب على اعتماد التوقيع الإلكتروني من طرف جهة محايدة وموثوقة اعتباره دليلاً على نسبته إلى صاحبه، الأمر الذي يستوجب التثبت من هوية الموقع، ومدى تمتعه بالأهلية القانونية، وكذا صلاحياته ووظيفته.

كما تمتد مهام جهة التصديق إلى التحقق من سلامة البيانات المتبادلة ضمن العقد الإلكتروني، والتأكد من جديته وخلوه من مظاهر الغش أو التدليس. وفي هذا الإطار، تعمل هذه الجهات على مراقبة المواقع الإلكترونية ذات الطابع التجاري للتثبت من وجودها الفعلي

[1] المادة 2 الفقرة 5 قانون الأونسيترال النموذجي المتعلق بالتوقيعات الإلكترونية سنة 2001

[2] المادة 2 الفقرة 12 من القانون رقم 04-15المتعلق بالتوقيع والتصديق الالكترونيين السالف الذكر

ومصداقيتها، بما يتيح تزويد المتعاملين، لاسيما المستهلكين، بمعلومات موثوقة حول تلك المواقع، وهو ما يعزز الثقة في المعاملات الإلكترونية ويشجع على الإقدام عليها.

وناهيك على ذلك، تقوم جهة التصديق بتنبيه المتعاملين في حال ثبوت عدم موثوقية بعض المواقع، من خلال إصدار تحذيرات مناسبة، الأمر الذي يدفع الأطراف إلى التحقق المسبق من هوية ومصداقية الطرف المتعاقد، خاصة في المعاملات ذات القيمة المرتفعة.[1]

الفرع الثالث: دور مؤدي خدمات التصديق الإلكتروني.

أولا: مفهوم مقدم خدمات التوثيق الإلكتروني

يستوجب تحديد مفهوم مقدم خدمات التوثيق الإلكتروني والوقوف على طبيعته القانونية، وكذا تمييزه عن غيره من المراكز القانونية المشابهة، البدء بوضع تعريف دقيق له يبرز خصائصه ويحدد نطاق نشاطه.

كما يستلزم الأمر بيان آلية عمله من خلال توضيح مختلف الخدمات التي يقدمها للمتعاملين، إلى جانب إبراز نظام الرقابة المفروض عليه، سواء من حيث تقييم جودة أدائه أو الجهة المختصة بالإشراف عليه في حال تراجع مستوى الخدمات المقدمة.

ويهدف تناول هذه الجوانب مجتمعة إلى تقديم تصور معمق وشامل لمفهوم مقدم خدمات التوثيق الإلكتروني، بعيدًا عن المعالجة السطحية، خاصة بالنظر إلى حداثة هذا المجال وأهميته المتزايدة، فضلاً عن محدودية الإلمام به لدى فئات واسعة من المجتمع، سواء فيما يتعلق بالتوثيق الإلكتروني بصفة عامة أو بمقدمي هذه الخدمات بصفة خاصة[2].

التعريف بمقدم خدمات التوثيق الإلكتروني

تعددت التعاريف الواردة بشأن مقدم خدمات التوثيق الإلكتروني، فمنها ما كرسته التشريعات المنظمة للتوقيع الإلكتروني على المستويين الوطني والدولي، ومنها ما صاغه الفقه القانوني عند تناوله لموضوع التوثيق الإلكتروني. ومن خلال هذه التعاريف يمكن

[1] لبيض فايزة، المرجع السابق، ص 348.

[2] –أكرم تحسين الدخيلي، النظام القانوني للتوثيق الإلكتروني، دراسةمقارنة، ص 67.

استخلاص الشروط الواجب توافرها في مقدم هذه الخدمات، إلى جانب تمييزه عن غيره من الجهات المشابهة، وعلى وجه الخصوص الكاتب العدل الإلكتروني.

شروط مقدم خدمات التوثيق الإلكتروني وتمييزه من الكاتب العدل الإلكتروني

يقصد بمقدم خدمات التوثيق الإلكتروني كيان قانوني يتمتع بالشخصية المعنوية، يتسم بالحياد، ويكون معتمدًا من قبل جهة مختصة في الدولة، يتولى إصدار شهادات التوثيق الإلكتروني وتقديم مختلف الخدمات المرتبطة بالمعاملات والتوقيعات الإلكترونية، وذلك بهدف التحقق من هوية الأطراف وإسناد التصرفات الإلكترونية إلى أصحابها.

وعليه، سيتم تناول هذا الموضوع من خلال تقسيمه إلى فقرتين: تُخصص الأولى لبيان الشروط الواجب توافرها في مقدم خدمات التوثيق الإلكتروني، بينما تُعنى الثانية بتمييزه عن الكاتب العدل الإلكتروني.

وتتمثل أبرز الشروط الواجب توافرها فيما يلي:

أن يكون ذا شخصية معنوية.

أن يكون حاصلًا على ترخيص من الجهة المختصة.

أن يلتزم بالحياد في أداء مهامه.

أن تتوفر لديه الإمكانيات والوسائل التقنية اللازمة لممارسة نشاطه بكفاءة.[1].

3- الخدمات التي يؤديها مقدم خدمات التوثيق الإلكتروني

- الإلكتروني
- يقوم مقدم خدمات التوثيق الإلكتروني بأداء مجموعة من الخدمات المرتبطة بالبيئة الرقمية، تكتسي أهمية بالغة في دعم وتنمية المعاملات الإلكترونية، من خلال تعزيز الثقة والاطمئنان لدى المتعاملين، بما ينعكس إيجابًا على استقرار هذه المعاملات. ويتحقق ذلك عبر إخضاع التصرفات الإلكترونية لإجراءات تقنية

[1] لبيض فايزة، النظام القانوني للتوقيع والتصديق الإلكترونيين، أطروحة دكتوراه، كلية الحقوق، جامعة الجزائر 1، 2016، ص 345–350

وقانونية دقيقة، يشرف عليها كيان محايد ومرخص له من جهة مختصة، تتولى بدورها مراقبة نشاطه لضمان سلامة العمليات وصحة النتائج.

- وتتجلى أهم الخدمات التي يقدمها مقدم خدمات التوثيق الإلكتروني فيما يلي:
- إنشاء التوقيع الإلكتروني وفق آليات تقنية موثوقة.
- إصدار شهادات التوثيق الإلكتروني التي تثبت هوية الأطراف.
- توليد وإصدار المفاتيح الإلكترونية اللازمة لعمليات التشفير.
- حفظ وإدارة المفاتيح الخاصة بالمستخدمين بما يضمن سريتها.
- توفير المعلومات المتعلقة بالمواقع الإلكترونية والتواقيع الإلكترونية للتحقق من مصداقيتها

- **ثانيا: دور مؤدي خدمات التصديق الإلكتروني.**

يقوم دور مؤدي خدمات التصديق الإلكتروني أساساً على تحقيق الأمان القانوني أي التأكيد على شخصية المرسل الذي يستخدم المفتاح العام، وصلاحياته ففي حال غياب مؤدي هذه الخدمات فكيف يمكن لشخصين لم يسبق لهما التعاقد معا التحقق من المفتاح العام المرسل لكل منهما للتحقق من هوية كليهما.

فهذه مشكلة أمان تفتقدها الصفقات المبرمة عن طريق الانترنيت[1]. ولذلك يجب أن توضح الدور أو الوظيفة المنوطة بجهة التصديق بصفة عامة، علما أن المشرع الجزائري قد أوردها بالتفصيل في القانون رقم 15/ 04 ضمن الفرع الثاني تحت عنوان تأدية خدمات التصديق الالكتروني من المادة 41 إلى المادة 50.

الوظيفة الأولى هي منح المفتاح الخاص والعام للشخص الذي يريد التوقيع إلكترونيا، بمعنى أن يتعاقد الموقع مع مؤدي خدمات التصديق الإلكتروني، ليتحصل على مفتاحين أحدهما عام والثاني خاص، فالمفتاح الخاص يستخدمه المُوقع في تشفير الرسالة لإرسالها، والمفتاح العام يستخدمه المرسل إليه لفك شفرة الرسالة، فإذا تم فك التشفير بنجاح يتأكد

1سعيد السيد قنديل التوقيع الإلكتروني، بدون طبعة دار الجامعة الجديدة للنشرة الإسكندرية 73 :2004، ص

المرسل إليه أن الشخص الذي أرسل له المفتاح العام هو الذي قام فعلا بتشفير رسالة المرسل إليه[1].

المطلب الثالث: التشفير

في إطار التعاملات الإلكترونية، وعند دخول المستخدم إلى أحد مواقع التجارة الإلكترونية وقيامه بطلب سلعة أو خدمة، يثور بالنسبة للقائم على الموقع إشكال جوهري يتمثل في ضرورة التحقق من صحة هذا الطلب والتأكد من نسبته إلى صاحبه الحقيقي. ولا يتحقق ذلك بالاعتماد على البيانات الظاهرية فقط كاسم المستخدم أو عنوان البريد الإلكتروني أو غيرها من المعطيات التي توفرها المواقع الإلكترونية، خاصة في ظل تزايد عمليات الاختراق واستعمال هويات الغير في أنشطة غير مشروعة عبر الشبكة، مع بقاء الموقع ملزمًا بتنفيذ التزاماته التعاقدية وعلى رأسها تسليم محل العقد.

ولمواجهة هذه الإشكالات، تم تطوير مجموعة من الوسائل التقنية التي تهدف إلى ضمان تأكيد الاتصال وإثبات صدور البيانات عن النظام المعلوماتي المعني، غير أن هذه الوسائل تبقى محدودة الفعالية نظرًا لما تعانيه من ثغرات أمنية، مما يجعلها غير كافية لتحقيق درجة عالية من الأمان والثقة. وقد أدى ذلك إلى بروز دور طرف ثالث محايد يتمثل في جهات متخصصة في تقديم خدمات التوثيق الإلكتروني، حيث تتولى هذه الجهات إصدار شهادات رقمية تفيد بأن الطلب أو الاستجابة قد صدرت فعلاً عن الجهة المعنية، مع تحديد تاريخ ووقت صدور العملية.

كما تم اعتماد وسائل متعددة للتحقق من هوية المستخدمين، تبدأ بكلمات المرور وقد تمتد إلى وسائل بيو مترية مثل البصمة الصوتية، إلى جانب تقنيات التشفير التي أثارت نقاشًا قانونيًا حول مشروعيتها، بالنظر إلى آثارها المحتملة على حرية تدفق البيانات وانسيابها، وما قد يترتب عنها من مساس بالخصوصية، لاسيما عند تطبيق إجراءات التحقق التي قد تستدعي الاطلاع على بيانات مخزنة خارج نطاق العلاقة التعاقدية محل التنفيذ

2. سامح عبد الواحد التهامي، التعاقد عبر الإنترنت، دار الكتب القانونية، المحلة الكبرى، مصر، 2008، ص 414.

و سنحاول فيما يلي دراسة التشفير وبيان جوانبه القانونية والفنية ليتم توفير الأمن والحماية للتصرفات المبرمة عبر الإنترنت وتطوير التجارة الإلكترونية على النحو التالي:

الفرع الأول: تعريف التشفير

انفرد المشرع التونسي في نصوصه عن باقي التشريعات العربية الخاصة بالتجارة الإلكترونية بتعريف التشفير، كذلك الحال بالنسبة إلى مشروع قانون التجارة الإلكترونية المصري. فعرف المشرع التونسي التشفير بأنه " استعمال رموز وإشارات غير متداولة تصبح بمقتضاها المعلومات المرغوب تحريرها أو إرسالها غير قابلة للفهم من قبل الغير أو استعمال رموز وإشارات لا يمكن وصول المعلومة بدونها[1].

كما عرفه مشروع قانون التجارة الإلكترونية المصري بأنه " تغير في شكل البيانات عن طريق تحويلها إلى رموز أو إشارات لحماية هذه البيانات من اطلاع الغير عليها أو تعديلها أو تغيرها[2]. هذا بالنسبة إلى التشريعات العربية التي تعرضت للتشفير بشكل مباشر، إلا أن بقية التشريعات العربية عالجت التشفير بشكل غير مباشر من خلال قانون التجارة الإلكترونية. وكذلك قانون الأونسيترال النموذجي للتوقيع الإلكتروني، تطرقت إلى عملية التشفير بطريقة غير مباشرة وذلك من خلال التوقيع الإلكتروني الذي يرتكز في الأساس على عملية التشفير. وهذا ما يؤكد أن كافة التشريعات الخاصة بالتجارة الإلكترونية عالجت التشفير سواء أكان بشكل مباشر أو من خلال التوقيع الإلكتروني. ومن هنا يعرّف التشفير الإلكتروني على أنّه:

. يُقصد بالتشفير الإلكتروني أنه آلية تقنية تُستخدم لنقل البيانات وحمايتها من الاطلاع غير المصرح به، إذ يهدف إلى الحفاظ على سرية المعلومات وسلامتها. ويظهر من الناحية الفنية في إعادة صياغة أو ترميز رسالة البيانات قبل إرسالها، باستخدام رموز أو مفاتيح خاصة، بما يضمن عدم إمكانية قراءتها إلا من قبل الجهة المخوّلة بذلك. كما يُعرف بأنه تحويل البيانات إلى صيغة سرية لا يمكن فهمها إلا باستعمال كلمة مرور أو مفتاح سري،

[1] عقوني محمد ، الآليات القانونية والتقنية لحماية التوقيع الالكتروني ، مجلة الفكر ، العدد ،18 ، جامعة محمد خيضر ، بسكرة ، 2019 ، ص303.

[2] عقوني محمد ، الآليات القانونية والتقنية لحماية التوقيع الالكتروني، مرجع سابق ص303

حيث يتم الاعتماد على مفتاح واحد أو مجموعة مفاتيح لإجراء عمليتي التشفير وفك التشفير.

وفي السياق التشريعي، تناول المشرع الجزائري موضوع التشفير ضمن القانون رقم 15-04 المؤرخ في 1 فبراير 2015 المتعلق بالقواعد العامة للتوقيع والتصديق الإلكترونيين، حيث أشار في المادة 2 فقرة 3 إلى البيانات المرتبطة بإنشاء التوقيع الإلكتروني، والمتمثلة في الرموز أو مفاتيح التشفير الخاصة التي يستعملها الموقع لإنتاج توقيعه الإلكتروني

كما نصت الفقرة 5 من المادة نفسها على مفاتيح التشفير العمومية أو غيرها من البيانات المستعملة لأغراض التحقق من صحة التوقيع الإلكتروني. ويُستفاد من ذلك أن المشرع الجزائري لم يقدّم تعريفًا مباشرًا للتشفير، وإنما اعتبره عنصرًا من عناصر إنشاء التوقيع الإلكتروني من جهة، ووسيلة للتحقق منه من جهة أخرى، مميزًا بين نوعين من المفاتيح؛ حيث تُستخدم المفاتيح الخاصة لإنشاء التوقيع الإلكتروني، بينما تُستعمل المفاتيح العمومية للتحقق من صحته.[1]

الفرع الثاني: أنواع التشفير[2]

تتنوع أساليب وأشكال التشفير الإلكتروني، ويمكن بيان أهم هذه الأنواع من الناحية الفنية على النحو الآتي:

التشفير ذو الخصوصية المتميزة (PG)

تُعد هذه الطريقة من أكثر أساليب التشفير كفاءة من حيث حماية البيانات، إذ تتميز بدرجة عالية من الأمان تجعلها قادرة على مواجهة محاولات الاعتداء أو الاختراق للبيانات المشفرة. وتقوم هذه التقنية على استخدام خوارزميات رياضية متقدمة تُدار بواسطة أنظمة تقنية ذات مستوى عالٍ من الخبرة والدقة، وهو ما أكسبها انتشارًا واسعًا في مجال تأمين الرسائل الإلكترونية وحماية البيانات المتبادلة عبر شبكة الإنترنت.

[1] المادة 2 الفقرة 3 والفقرة 5 من القانون رقم 04-15 المتعلق بالوقيع والتصديق الالكترونيين السالف الذكر

[2] -المحامي الدكتور محمد فواز المطالقة ،الوجيز في عقود التجارة الالكترونية ،جامعة البلقاء التطبيقية ،كلية إربد، ص167-169.

ويعتمد هذا النوع على مفتاح تشفير مزدوج الوظيفة، حيث يُستخدم ذات المفتاح في عمليتي التشفير وفك التشفير، وهو ما يُعرف بالمفتاح التقليدي (cryptosystem). ويتميز هذا النظام باستخدام مفاتيح بطول يصل إلى (127) بت، مما يعزز من مستوى الحماية ويقلل من احتمالات الاختراق.

ويهدف هذا الأسلوب إلى تحقيق أمن المعاملات الإلكترونية وسريتها، غير أن فعاليته تقتضي الالتزام بجملة من الشروط، أهمها الحفاظ على سرية المفتاح المستخدم في التشفير وفك التشفير، وضمان عدم تسربه إلى الغير. لذلك يتوجب نقله إلى الطرف الآخر عبر وسائل آمنة وموثوقة، لأن أي إفشاء لهذا المفتاح يؤدي إلى فقدان النظام لفعاليته، ويُتيح للغير الاطلاع على محتوى الرسائل وفك شفراتها، بما يُفقد العلاقة التعاقدية عنصر السرية والحماية.

ولإتمام عملية التشفير من خلال استخدام المفتاح الخاص فلابد من توافر أسلوب يتم من خلاله القيام بتشفير البيانات، فهذه هي الطريقة الأساسية في التشفير حيث يستخدم مفتاح عام للتشفير وهو الذي يستخدمه كافة العملاء الذين يقومون بإرسال البيانات من خلال شبكة الإنترنت عبر رسائل مشفرة بواسطة مفتاح التشفير العام الذي يتم من خلاله التشفير للكافة، إلا أن عملية فك التشفير لا تتم إلا بواسطة المفتاح الخاص المتعارف عليه بين طرفي العلاقة.

وكان الفضل للعالم " فيليب زيميرمان، في اختراع نظام (PGP)لتشفير البيانات ويعتمد في استعماله على مفتاحين للقيام بعملية التشفير المفتاح العام والخاص. فالمفتاح الخاص، يستطيع المستخدم بواسطته تشفير البيانات التي يريد إرسالها إلى الطرف الآخر، كذلك يتمكن بواسطة المفتاح نفسه فك الرموز المشفرة وتحويل النص المشفر إلى نص مقروء. أما المفتاح العام الذي يتم تداوله من قبل الكافة وبحسب اختيارهم فيتم تشفير البيانات بواسطته، إلا أن المفتاح الخاص يمتاز بإمكانية فك شفرة أي رسالة مشفرة بواسطة المفتاح العام المتاح للعامة، فالمفتاح العام يستطيع فقط إرسال رسائل مشفرة، إلا أنه لا يتمكن من فك أي شفرة إطلاقاً، حتى وإن كان كاتب الرسالة نفسه من قام بتشفيرها. بواسطة المفتاح العام – فإنه لا

يستطيع فك شيفرتها، لأنه لا يملك المفتاح الخاص الذي يمكن فك الشفرة من خلاله، لأن المفتاح العام وجد من أجل التشفير فقط وليس من أجل فك الشفرات.

- تشفير القرص الصلب

لم ينحصر نطاق التشفير على حماية البيانات المتبادلة فقط، بل امتد ليشمل تشفير القرص الصلب لأجهزة الحاسوب. وتُعد هذه العملية من الإجراءات التقنية البسيطة في تطبيقها، وفي الوقت ذاته من أكثر الوسائل فعالية من حيث مستوى الحماية الذي توفره مقارنة بغيرها من أساليب التشفير.

إذ يضمن تشفير القرص الصلب تعزيز أمن المعلومات بشكل كبير، من خلال منع أي طرف غير مصرح له من الوصول إلى البيانات المخزنة على الجهاز أو الاطلاع عليها أو التعدي على خصوصيتها، بما يحفظ سرية المعلومات المتبادلة بين أطراف العلاقة ويصون خصوصيتهم في البيئة الرقمية..

الفرع الثالث: طرق التشفير

تعتبر آلية التشفير من أهم الوسائل التقنية المستخدمة في تأمين المعاملات الإلكترونية، إذ يساهم في ضمان سلامة التوقيع الإلكتروني وإسناده إلى صاحبه الحقيقي. فبفضل تقنيات التشفير لا يُنسب التوقيع إلا إلى الموقع الذي صدر عنه فعلاً، كما يتيح كذلك الحفاظ على سرية المعاملات والرسائل المتبادلة عبر الوسائط الإلكترونية. وفي هذا الإطار يمكن الإشارة إلى أهم هذه الأساليب كما يلي:[1]

أولا: تقنية التشفير المتماثل

في هذه التقنية يُستخدم المفتاح أو الرمز السري نفسه في عمليتي تشفير السندات الإلكترونية وفك تشفيرها، أي أن نظام تشفير السندات الإلكترونية يعتمد على مفتاح واحد يُعرف بالمفتاح الخاص، يكون في حيازة كل من مُنشئ السند الإلكتروني ومتلقيه[2].

[1] عباس العبودي تحديات الإثبات بالسندات الالكترونية ومتطلبات النظام القانوني لتجاوزها، ط1، منشورات الحلبي الحقوقية، بيروت، 2010، ص 232. انظر كذلك، محمد فواز المطالقة، المرجع السابق، ص 163.

[2] - عباس العبودي ، المرجع السابق، ص 163.

وتتمثل الجوانب السلبية لألية التشفير في أن المرسل إليه، عند تلقيه سندات إلكترونية من مصادر متعددة، يكون ملزمًا بالاحتفاظ بعدد من المفاتيح الخاصة يتناسب مع عدد هذه المصادر، وهو ما يزيد من صعوبة إدارة المفاتيح. كما أن اشتراك أكثر من طرف في استعمال المفتاح ذاته قد يعرض السندات الإلكترونية لمخاطر أمنية دائمة، تتمثل في احتمال انتقال المفتاح الخاص إلى الغير بصورة مشروعة أو غير مشروعة، الأمر الذي يصعب معه التحقق من هذا الانتقال أو ضبطه، خاصة في الحالات التي يكون فيها كل من مُنشئ السند الإلكتروني ومتلقيه حائزين على المفتاح نفسه[1].

ثانيا: تقنية التشفير غير المتماثل

يطلق على هذه الآلية بالتشفير بالمفتاح العمومي، حيث لا يُستخدم المفتاح نفسه في عمليتي التشفير وفك التشفير كما هو الحال في التشفير المتماثل، وإنما تعتمد على زوج من المفاتيح غير المتماثلة. يتمثل الأول في مفتاح خاص يحتفظ به المستخدم بشكل سري وشخصي، بينما يكون الثاني مفتاحًا عامًا يُتاح للغير ويُوزَّع على المستخدمين الآخرين الراغبين في إرسال سندات إلكترونية مشفرة إليه.

وبناءً على ذلك، يمكن لأي شخص يمتلك المفتاح العام أن يستخدمه لتشفير الرسائل أو السندات الإلكترونية وإرسالها إلى صاحب المفتاح الخاص، في حين لا يستطيع فك هذا التشفير وقراءة محتواها إلا المستخدم الحائز على المفتاح الخاص وحده، مما يضمن سرية المعلومات وتفرد صاحب المفتاح الخاص بالاطلاع عليها.[2].

ثالثا: التشفير عن طريق تأمين تقنيات السندات الإلكترونية

تستعمل هذه التقنية في تأمين وتشفير البيانات المتضمنة في السندات الإلكترونية أثناء نقلها عبر وسائل الاتصال الفوري، بما يضمن قصر الاطلاع على محتواها على كل من المرسل والمرسل إليه فقط. ويُعزز هذا النظام في كثير من التطبيقات بوجود جهة تصديق إلكترونية أو ما يُعرف بالكاتب العدل الإلكتروني، الذي يتولى إصدار شهادات إلكترونية موثقة تُثبت هوية الأطراف وتدعم موثوقية التعاملات الإلكترونية.

[1]– المرجع نفسه ، ص 232.

[2]– المرجع نفسه ، الصفحة نفسها.

وتسهم هذه التقنية في تحقيق التوازن بين سرية المعاملات التجارية وضمان أمنها، حيث تعتمد بعض الأنظمة المعلوماتية على إنشاء بيئة اتصال آمنة عبر خوادم مخصصة، تقوم على معالجة البيانات باستخدام رموز حسابية ومفاتيح تشفير خاصة. كما تقوم آلية الحماية على تزويد المستخدمين بزوج من المفاتيح: مفتاح خاص يحتفظ به المستخدم بسرية، ومفتاح عام يُتاح للغير لاستخدامه في تشفير البيانات الموجهة لها. [1]

المبحث الثاني: تقنيات و أدوات الأمن السيبراني

في ظل التحول الرقمي أصبح الأمن السيبراني ضروريًا لحماية المعلومات من التهديدات المتزايدة، ويعتمد على تقنيات مثل كشف التسلل والتشفير ومكافحة البرمجيات الضارة لضمان أمن البيانات مع أهمية تكامل هذه الأدوات لفعالية أكبر، كما يعد تسيير المخاطر والتعاون بين الجهات المختلفة عنصرين أساسيين لتعزيز الحماية والاستجابة السريعة إضافة إلى دور التكوين المستمر في رفع الوعي **الأمني** وتقوية قدرات العاملين في هذا المجال، لذلك سوف نتطرق في هذا المبحث إلى تقنيات الأمن السيبراني والهجمات السبيرانية الناجمة عنه.

المطلب الأول: مفهوم الأمن السيبراني

يعتبر الأمن السيبراني أحد الركائز الأساسية في المنظومة الأمنية المعاصرة، لما له من دور محوري في حماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصالات والمعلومات. وانطلاقًا من ذلك، فإنه قبل التطرق إلى مختلف تقنيات وأدوات الأمن السيبراني، يستوجب الأمر أولًا تحديد مفهوم هذا الأخير وتعريفه بشكل دقيق، باعتباره الإطار الذي تُبنى عليه آليات الحماية الرقمية.

الفرع الأول: تعريف الأمن السيبراني

تعتبر مهمة ضبط المفاهيم والمصطلحات تحدياً يواجه مختلف الباحثين والدارسين في مختلف التخصصات، وذلك لما يطرحه من إشكاليات تجعل من الصعوبة بمكان الاتفاق على

[1]–عباس العبودي، المرجع السابق، ص 234.

تعريفات واضحة وشاملة وموحدة بين أعضاء المجتمع العلمي، ويعد الأمن السيبراني واحداً من المفاهيم المعقدة التي قدمت لها العديد من التعريف المختلفة .

الأمن هو نقيض الخوف، ويعني السلام والطمأنينة، وهو مصدر الفعل أمن أمناً وأماناً، ويُقصد به اطمئنان النفس وسكون القلب وزوال الخوف، ويقال: أمن من الشر أي سلم منه، وقد عرّفه قاموس بنغوين للعلاقات الدولية بأنه مصطلح يشير إلى غياب ما يهدد القيم النادرة. وعلى الرغم من أن مصطلح الأمن القومي قد شاع بعد الحرب العالمية الثانية، إلا أن جذوره تعود إلى القرن السابع عشر، خاصة بعد معاهدة وستفاليا سنة 1648 التي أسست لنشأة الدولة القومية أو الدولة والأمة، وشكلت حقبة الحرب الباردة الإطار والمناخ الذي تطورت فيه محاولات صياغة مقاربات نظرية وأطر مؤسساتية، وصولًا إلى استخدام تعبير الأمن القومي"، وسادت خلال تلك المرحلة مصطلحات الحرب الباردة مثل الاحتواء والردع والتوازن والتعايش السلمي كعناوين بارزة في هذه المقاربات بهدف تحقيق الأمن والسلم وتجنب الحروب المدمرة التي شهدها النصف الأول من القرن العشرين.

يمكن تعريف الأمن السيبراني أيضًا بأنه أمن الشبكات والأنظمة المعلوماتية والبيانات والمعلومات والأجهزة المتصلة بالإنترنت، وهو المجال المتعلق بالإجراءات والمقاييس والمعايير الواجب اتخاذها أو الالتزام بها لمواجهة التهديدات ومنع التعديات أو الحد من آثارها في أسوأ الأحوال. ويرتبط هذا الأمن ارتباطًا وثيقًا بأمن المعلومات، إذ إن الوصول إلى هذه الأخيرة أو بثها أو الاطلاع عليها أو المتاجرة بها أو تشويهها واستغلالها يعد من أبرز أسباب الاعتداء على الشبكات والإنترنت.

ومن هنا، فإن الأنظمة الإلكترونية تعتمد على المعلومة باعتبارها عنصرًا أساسيًا، بما يفرض تحديد مفهوم الخطر، أي التهديد الذي يتعرض له النظام، إضافة إلى نقاط الضعف أو الثغرات التي قد تعتريه، ثم الإجراءات الواجب اتخاذها لمواجهة هذا الخطر. فالتهديد يتمثل في الأعمال العدائية التي يمكن أن تستهدف النظام، في حين تمثل نقاط الضعف درجة الانكشاف لهذا التهديد في سياق معين، أما الإجراءات الواجب اتخاذها فلا تقتصر على الجانب التقني فقط، بل تشمل أيضًا بناء القدرات والتوعية والتدريب ونقل الخبرات.[1].

[1] فارس محمد العمارات إبراهيم محمد الحمامصه مرجع سابق ص 10

الفرع الثاني: طرق وأدوات الحماية أو الحراسة

أولا : الحماية البرمجية

تتضمن الحماية البرمجية مجموعة البرامج والتطبيقات والخدمات التي تهدف إلى تأمين أنظمة التشغيل وقواعد البيانات وبقية الخدمات العاملة على الحاسوب أو الأجهزة النقالة أو الخوادم. ويقوم مديرو الشبكات بتثبيت برامج الحماية على الأجهزة المضيفة أو الخوادم من أجل توفير طبقات أمان تحمي النظام من التهديدات الإلكترونية. وتوجد العديد من التقنيات البرمجية المستخدمة في تأمين ممتلكات الشركة، منها ما يلي [1]:

الجدار الناري firewall البرمجي : يعتبر الجدار الناري (Firewall) من أهم وسائل الحماية البرمجية في الأنظمة المعلوماتية، نظرًا لما يرافق الاتصال بالإنترنت من مخاطر تتمثل أساسًا في عمليات الاختراق (Intrusion)، الأمر الذي يستوجب اتخاذ تدابير وقائية للحد منها ومنعها. إذ تكون أجهزة الحاسوب المتصلة بالإنترنت أو بالشبكات المختلفة عرضة لهجمات القراصنة والمتطفلين الذين يسعون إلى الوصول غير المشروع إلى البيانات والملفات أو إتلاف البرامج والمعلومات، مما يؤدي إلى خسائر مادية ومعنوية لمستخدمي هذه الأجهزة. ويحدث هذا النوع من الاختراق غالبًا نتيجة غياب وسائل الحماية المناسبة، حيث يتمكن المعتدون من الولوج إلى النظام والتحكم في محتوياته

تُعدّ جدران الحماية النارية (Firewalls) من الوسائل الأساسية للحد من محاولات الاختراق التي يقوم بها قراصنة الحاسوب، حيث تعمل على فحص الاتصالات الواردة إلى جهاز الحاسوب والتحقق منها، ثم السماح فقط بالاتصالات الآمنة والمطابقة لإعدادات الأمان بالدخول.

وتقوم فكرة جدار الحماية على عزل الجهاز أو الشبكة الداخلية عن الشبكات الخارجية، وذلك عبر مراقبة حركة البيانات وتطبيق مجموعة من القواعد الأمنية التي تحدد ما إذا كان يُسمح بالاتصال أو يتم حجبه. وتُحدد هذه القواعد عادة من طرف المستخدم أو من قبل مدير النظام في الشبكات.

[1] خالد وليد محمود، الهجمات عبر الإنترنت ساحة الصراع الإلكتروني الجديدة، المركز العربي الأبحاث ودراسة السياسات، قطر، 2013 صفحة.

كما يُعرف جدار الحماية بأنه برنامج أو جهاز يقوم بتحليل البيانات القادمة من الإنترنت أو من شبكات أخرى، ثم يتخذ قرارًا إما بحظرها أو السماح بمرورها وفقًا لإعدادات الأمان المسبقة. ويساهم أيضًا في منع وصول البرمجيات الخبيثة والمتطفلين إلى الحاسوب عبر الشبكات، إضافة إلى دوره في منع الجهاز من إرسال برمجيات ضارة إلى أجهزة أخرى متصلة. ويوضح الشكل المرفق فيما بعد آلية عمل جدار الحماية الناري[1].

ثانيا: الحماية بالعتاد

يوجد العديد من التقنيات التي تستخدم العتاد الحراسة ممتلكات الشركة :

- أجهزة الجدران النارية توقف المرور الغير مرغوب فيه ويحتوى جهاز الجدار الناري على عدة قواعد تحدد نوعية سيل.
- البيانات المسموح به والغير مسموح به على الشبكة.
- أجهزة كشف الدخلاء Intrusion Détection System IDS انظر الشكل مصممة لاكتشاف بوادر الهجمات أو سيل البيانات الغير عادي على الشبكة وتعطي رسائل تحذيرية.
- أجهزة منع الدخلاء Intrusion Prévention Systems (PS) مصممة لاكتشاف بوادر الهجمات أو الأنشطة الشبكية الغير طبيعية وتقوم بإرسال تحذيرات بالإضافة إلى عمل خطوات تصحيحية.
- خدمات ترشيح المحتوى تقوم بالتحكم في الوصول والتحكم في نقل البيانات الغير لائقة والمحتوى العدواني.

ثالثا. الحماية بالتقنيات السحابية

1. تعريف الأمان السحابي

يُعد أمن المعلومات أحد فروع العلوم التقنية الحديثة، وهو علم يختص بتوفير الحماية اللازمة للمعلومات والبيانات المتداولة عبر شبكة الإنترنت والمخزنة بشكل رقمي، من المخاطر التي قد تهددها، وذلك من خلال اعتماد ممارسات أو استخدام وسائل تحميها من التهديدات

[1] حسن هادي لذيذ، ماجستير حاسبات، مبادئ وأساسيات الحاسب الآلي وتكنولوجيا المعلومات ، العراق. سنه2014،صفحة 69.

الداخلية والخارجية، سواء تعلق الأمر بالوصول غير المصرح به إلى البيانات أو تعديلها أو إساءة استخدامها أو تعطيلها أو تدميرها أو سرقتها[1]

2.الحماية التقنية :

إن تطبيق الحماية القانونية الخاصة بالبيانات الشخصية في بيئة الحوسبة السحابية يواجه مجموعة من الإشكالات التي تحد من فاعليته، ومن أبرزها: صعوبة التعرف على هوية الجاني، وتعذر إثبات الجريمة في ظل الطابع الافتراضي لشبكة الإنترنت، إضافة إلى الإشكالات المرتبطة بتحديد الاختصاص القضائي والقانون الواجب التطبيق على النزاع، فضلاً عن صعوبة تنفيذ العقوبة في حال كان الفاعل مقيماً خارج الدولة، وكذلك التعقيدات المتعلقة بالتعاون القضائي الدولي في هذا المجال. وهو ما فرض ضرورة الاتجاه نحو اعتماد وسائل حماية تتناسب مع الطبيعة التقنية للحوسبة السحابية وشبكة الإنترنت باعتبارهما البيئة التشغيلية لهذه البيانات، وذلك بهدف منع وقوع الاعتداء أو الحد من آثاره على الأقل في حال حدوثه، ومن أهم هذه الوسائل:

التشفير : هو عملية يتم بموجبها تحويل البيانات الشخصية الخاصة بالمستخدم إلى رموز غير مفهومة باستخدام خوارزميات رياضية، بهدف حمايتها من الوصول غير المصرح به وضمان سريتها وسلامتها سواء أثناء التخزين أو النقل، بحيث إذا تمكن المخترق من الوصول إليها فإنه لا يستطيع قراءتها لعدم امتلاكه مفتاح فك التشفير (99)، ويُطبق التشفير في التخزين السحابي على مستويين؛ فقد يقوم المستخدم بتشفير بياناته بنفسه قبل رفعها إلى السحابة من جهازه مستخدماً مفتاحاً خاصاً به وحده، كما يمكن أن يتم التشفير من طرف الخادم، وذلك عبر تشفير البيانات أثناء عملية رفعها إلى السحابة باستخدام مفتاح يديره مزود الخدمة السحابية، وهو ما يعزز حماية هذه البيانات أثناء تخزينها سحابياً.

ومن أحدث خوارزميات التشفير ما يسمى بتشفير العسل، والذي يُستخدم عند التعرض لهجوم القوة الغاشمة ""، وهذا الأخير هو هجوم سيبراني يعتمد على التكرار والتخمين والتجريب المنهجي لجميع الاحتمالات الممكنة بهدف كسر كلمات المرور.

[1]بن لشهب أسماء، حماية البيانات الشخصية للمستخدم في إطار عقود الحوسبة السحابية كلية الحقوق جامعة الإخوة منثوري – قسنطينة –1– المجلد التاسع العدد الأول (2025) مجلة الفكر القانوني والسياسي ص 305

بناء ثقافة الوعي السيبراني:

ينبغي أن يكون فريق العمل في الشركة ملماً بالسياسات الأمنية، كما يتوجب عليه امتلاك المعارف اللازمة لتجنب الهجمات اليومية. ويستند برنامج التوعية الأمنية الفعّال إلى ما يلي :[1]

- بيئة الشركة
- مستوى التهديد

إن تجسيد ثقافة الوعي السيبراني داخل الشركة يُعد جهداً مستمراً تقوده الإدارة العليا، ويستلزم في الوقت نفسه التزام جميع المستخدمين والموظفين. ومن أجل تعزيز هذه الثقافة، ينبغي أن تبدأ الشركة بوضع السياسات والإجراءات الإدارية المناسبة. فعلى سبيل المثال، تخصص العديد من الشركات يوماً سنوياً يُعرف بـ"يوم التوعية الأمنية". كما يمكن تعزيز مستوى الوعي من خلال إعداد الملصقات والنشرات وتوزيعها على أفراد الفريق، إضافة إلى تنظيم ورش عمل وندوات قصيرة، مما يسهم في رفع مستوى الوعي الأمني داخل المؤسسة. 1

المطلب الثاني:أنواع الهجمات السبيرانية

الفرع الأول: مفهوم الهجمات السبيرانية

يتكون مصطلح الهجمات السبيرانيه من كلمتين هما: الهجمات السيبراني، وللوصول إلى تعريف شامل له لا بد من تناول كلٍّ من هذين اللفظين على فرد.

الهجوم :

يُقصد بالهجوم عادةً عملية عسكرية تهدف إلى السيطرة على دولة أو مدينة معينة أو تحقيق هدف محدد. وفي الحقيقة، يُعدّ الهجوم نوعاً من الغزو الذي يُنفَّذ من أجل بلوغ أهداف عسكرية ضمن إطار الاستراتيجيات والعمليات والتكتيكات العسكرية. كما يُعدّ الهجوم من أبرز

[1] أسامة حسام الدين أساسيات الأمن السيبراني أكاديمية سيسكو بجامعة طيبة سبتمبر 2017م ص 43-44

الأساليب التي تعتمد عليها الجيوش لتحقيق الانتصار، إضافة إلى أن نجاح العملية الهجومية يرتبط أيضاً بعنصر الدفاع الذي يُشكّل جانباً أساسياً فيها[1]

السبيراني: هو مصطلح يُطلق على كل ما يرتبط بعالم الفضاء الرقمي أو الإلكتروني، ويشمل شبكات الحاسوب، والإنترنت، وأنظمة المعلومات، والتطبيقات الحديثة. ويُستخدم هذا المفهوم للدلالة على البيئة الافتراضية التي تتم فيها مختلف الأنشطة الرقمية مثل التواصل عبر وسائل التواصل الاجتماعي، وتبادل البيانات، وإجراء المعاملات الإلكترونية كالتسوق وتحويل الأموال.

الهجوم السبيراني:

عرفت بأنها أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الكومبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تعطيليا".

كما عرفها (Michael Schmitt) بأنها تلك الإجراءات التي تتخذها الدولة من أجل الهجوم على نظم المعلومات للعدو يهدف التأثير و الأضرار فيها. والدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة ".

وعرفها عبد القادر محمد فهمي بأنها هجمات تستخدم فيها المنظومة الشبكية والأجهزة الحاسوبية للدولة، أو الفاعلة من غير الدول لتعطيل كفاءة السيطرة والقدرة على التحكم في منظومة أجهزة أو شبكات الحاسوب وما تتضمنه من بيانات ومعلومات للفاعلين الآخرين من الدول وغير الدول، أو تقليلها، أو حتى تدميرها، سواء كان ذلك على مستوى منظومات قوتها العسكرية، وبالشكل الذي يعرض الأمن القومي للدولة إلى تهديد جسيم.

كما تتميز الحرب السبيرانية عن الحزب التقليدية في أن المفهوم التقليدي للحرب ينطوي على استخدام الجيوش النظامية ويسبقها إعلان واضح لحالة الحرب و ميدان قتال محدد، بينما تبدو هجمات الفضاء الالكتروني غير محددة المجال وغامضة الأهداف كونها تتحرك عبر شبكات المعلومات والاتصالات المتعدية للحدود الدولية

[1] الصغير كاوجة الهجمات السبيرانية بين الواقع وسبل المواجهة مجلة الرسالة للدراسات الإسلامية المجلد 06 / العدد 03 / سبتمبر 2022 ص 110

الفرع الثاني: أنواع الهجمات السبيرانية

إن الهجمات السبيرانية تبدأ عندما يتمكن المجرم الإلكتروني من إيقاع ضحيته في المصيدة إقناعه أن المصدر أو الملف المرسل موثوق به، إذ يتم إرسالها على شكل بريد الكتروني أو رسالة نصية. وحينما يتم استقبال المتلقي للرسالة وينقر على الرابط يتم تثبيت برامج ضارة على جهازه أو تجميد النظام كجزء من هجوم برامج الفدية أو اختراق الخصوصية الخاصة به كما تكمن طبيعة الهجمات السبيرانية في مجموعة من العمليات والتي تشمل عمليات التسلل إلى أنظمة الحاسب الآلي، أو تصديرها، أو إتلافها ، أو تغيرها، أو تشفيرها، كما تشمل عمليات زرع برمجيات ضارة للتجسس

ويرى محمد فهمي بأن الهجمات الالكترونية لتشمل أشكال كثيرة، من سرقة المعلومات، والتجسس و نشر معلومات سرية وفضح الأنظمة السياسية لأعراض التحريض ونشر أفكار مضادة و خلق تيارات معارضة، وإثارة احتجاجات.

أولا. البرمجيات الخبيثة :

البرمجيات الخبيثة هي برامج تهدف إلى إلحاق الضرر بالحاسوب أو تعطيله وجمع المعلومات والتجسس وعرقلة العمليات، وتتمكن بطريقة غير شرعية من عدوى نظام الحاسب بدون معرفة أو علم المستخدم من أجل اختراق جهازه والتجسس عليه[1].

1- أنواع البرمجيات الخبيثة

- **ا-الفيروسات**

هي برامج حاسوبية خبيثة مضرة بالحواسيب وتنتقل بين الحواسيب بعدة طرق، وتتكاثر بالاعتماد على ملفات أخرى، وهناك أنواع للفيروسات، منها ما يبدأ عمله بوقت أو حادثة معينة، حتى أصبح هناك تقويم للفيروسات التي ستعمل في يوم ما ، ومنها ما يكون مكوناً من أجزاء متعددة، ومنها ما تتغير صفاته بشكل دوري ومنها ما يكون متخفياً حتى عن برامج مكافح الفيروسات[2].

- **ب ديدان الحاسبة Worms**

[1] جميل حسين طويلة البرمجيات الخبيثة دليل عملي لاستخدام البرمجيات الخبيثة وبرمجيات التجسس وإجراءات الوقاية والحماية منها ص 10

[2] حسن هادي لذيذ، مبادئ وأساسيات الحاسب الآلي وتكنولوجيا المعلومات، العراق، 2014ص 65

هي عبارة عن برامج ضارة تقوم بالتكاثر ذاتياً حيث تقوم باستخدام الشبكة الحاسوبية الإرسال عدة نسخ من نفسها إلى الأجهزة المرتبطة بالشبكة وترسل الدودة نفسها عبر الشبكة دون الحاجة إلى مستخدم لتفعيلها على غرار الفيروس لا تحتاج الدودة إلى أن ترفق نفسها مع برنامج آخر.

- **ج الديدان:**

تلحق ضرر على الشبكة باستهلاك حزمة الشبكة وبالتالي إبطاء الشبكة وجعلها مشلولة بأقل تقدير حيث أن الفيروسات بالأغلب تقوم بتدمير أو تعديل الملفات في الجهاز المستهدف.

- **Trojan Horses أحصنة طروادة**

هو برنامج قائم بذاته أي لا يعتمد في آلية عمله أو انتشاره على برنامج آخر حيث يبدو حصان طروادة للمستخدم على أنه برنامج مفيد ويخدم غاية المستخدم ولكنه يقوم بالعمل في الخفاء محدثاً ثغرات بالنظام تسمح للأشخاص بالدخول أو العمليات غير مصرح بها في النظام بالحدوث.

الفكرة الأساسية من حصان طروادة هو خدع المستخدم على أنه برنامج مفيد بينما هو في الحقيقة يستخدم من قبل المخترقين والمخربين بهدف الوصول للمعلومات المهمة. ومن أنواع أحصنة طروادة:

← الوصول عن بعد Remote Access : هذه البرامج تسمح للمهاجم بأن يتحكم في جهازك عن بعد بشكل مخفي

← مرسل البيانات Data Sender : هذه البرامج ترسل بيانات خاصة بمستخدم النظام دون علمه مثل كلمة المرور المحادثات المخزونة وغيرها من المعلومات الأمنية. ترسل البيانات بواسطة رسالة بريدية أو تزويدها لموقع المهاجم مباشرة.

← معطل خدمات النظام Denial of Service : تعمل هذه البرامج بالتنسيق مع نسخ أخرى مشابهة على أجهزة أخرى مهاجمة على مهاجمة حاسوب معين التوقف عن العمل بشكل كامل أو لجعله بطينا جدا.

← وسيط اتصال Proxy : يتخذ المهاجم وسيطا بينه وبين الضحية الأصلي لكي يصل الى ضحيته بصورة خفية بحيث لو تم اكتشافه فأن أخر نقطة يتم تتبعها هي الحاسبة الوسيطة

← معطل البرامج Blocker : تقوم هذه البرامج بتعطيل بعض البرامج خاصة برامج مكافحة الفيروسات وبرامج جدران الحماية لكي يكون نظامك سهل الاختراق.

2-برامج القنابل المعلوماتية

تُعرف القنبلة المعلوماتية أيضاً باسم "الشفرة الموقوتة"، وهي أحد أنواع البرمجيات الخبيثة صغيرة الحجم التي يتم إدخالها بطرق غير مشروعة وإخفاؤها داخل برامج أخرى. ولا تكون هذه البرمجيات ملفاً متكاملاً في صورتها الظاهرة، بل عبارة عن شيفرة يتم توزيعها على أجزاء متعددة داخل ملفات مختلفة، بحيث يصعب اكتشافها أو تحديدها.

وتعمل هذه الشيفرة على التجمع تلقائياً عند تحقق شرط معين أو في وقت ومكان محددين، أو عند وقوع حدث خاص يتم برمجته مسبقاً، مما يجعل اكتشافها صعباً وقد يستغرق وقتاً طويلاً قد يمتد لأشهر أو سنوات. وتُستخدم هذه البرامج في إتلاف البيانات والمعلومات أو تعديلها أو التأثير على أنظمة التشغيل.

كما قد تُستعمل أحياناً كوسيلة لحماية بعض البرامج ذات الحقوق الفكرية من محاولات الاختراق، وتظهر بشكل خاص في بعض الحملات الترويجية، مثل الأقراص المرفقة بالمجلات التي تحتوي على برامج مجانية. وقد توجد أيضاً في بعض مواقع الإنترنت أو البرامج المؤجرة، حيث يمكن أن تتضمن هذه البرامج شيفرة خفية مرتبطة بشروط العقد، بحيث يتم تفعيلها في حال الإخلال بالاتفاق، كالتوقف عن دفع الرسوم، مما يؤدي إلى تعطيل البرنامج أو إتلافه، دون حاجة إلى تدخل إضافي من مالك البرنامج مباشرة [1].

3-هجوم برامج الفدية:

برامج الفدية هي أحد أنواع البرمجيات الخبيثة التي يستخدمها المجرمون الإلكترونيون، حيث تعمل على منع المستخدم من الوصول إلى نظامه أو تقوم بتشفير بياناته. وبعد ذلك يطلب المهاجمون دفع مبلغ مالي كفدية مقابل إعادة فك التشفير واسترجاع البيانات[2].

[1] نور أمير الموصلي، الهجمات السيبرانية في ضوء القانون الدولي الإنساني بحث مقدم استكمالاً لمتطلبات نيل درجة ماجستير التأهيل والتخصص في القانون الدولي الإنساني الجامعة الافتراضية السورية ماجستير التأهيل والتخصص في القانون الدولي الإنساني ، 2021 ،ص 12.

[2] محمد الصغير كاوجة ، مرجع سابق ،ص 114.

1-برمجيات الفدية:

تُعدّ برامج الفدية: نوعًا من البرمجيات الخبيثة التي تستولي على نظام الحاسوب أو الملفات الموجودة داخله، ثم تمنع المستخدم من الوصول إليها أو استعادتها إلا بعد دفع مبلغ مالي كفدية. وتعتمد هذه البرمجيات غالبًا على تشفير بيانات الضحية باستخدام مفتاح تشفير غير معروف لصاحب الجهاز، مما يجعل الملفات غير قابلة للاستخدام. وبعد ذلك يُطلب من المستخدم دفع الفدية مقابل الحصول على مفتاح فك التشفير واسترجاع بيانته.

ثانيا. برامج التجسس ال Spyware:

فهي البرامج التي تتولى تسجيل حركة مستخدم الانترنت، خدمة الطرف ثالث. وغالبا ما يكون الهدف الكامن وراء ذلك، تجاريا، حيث يعتبر الربح المادي، من أهم الدوافع وراء ممارسة هذه الاعتداءات ، وتعتبر المواقع الإباحية في هذا المجال، مواقعا خطرة، كون ٨٠٪ منها، تحمل برامج تجسس على الأجهزة التي تتصل بها .

1-التصيد :

حملة التصيد الاحتمالي في عندما يتم إرسال رسائل البريد الإلكتروني العشوائية أو غيرها من أشكال الاتصال بشكل جماعي، بهدف خداع المستلمين للقيام بشيء يقوض أمنهم أو أمن المنظمة التي يعملون بها.

قد تحتوي رسائل حملة التصيد الاحتيال على مرفقات مصابة أو روابط المواقع ضارة أو قد يطلبون من المتلقي الرد بمعلومات سرية يعرف نوع آخر من حملات التصيد الاحتمالي باسم التصيد بالرمح، هذه حملات تصيد مستهدفة تحاول خداع أفراد معينين لتعريض أمن المنظمة التي يعملون بها للخطر على عكس حملات التصيد الجماعي، والتي تكون عامة جداً في الأسلوب يتم عادة صياغة رسائل التصيد الاحتيالي بالرمح لتبدو وكأنها رسائل من مصدر موثوق.

2-الانتحال أو الخداع Spoofing :

هو هجوم يتم فيه انتحال شخصية شخص ما أو برنامج ما فمثلا قد يسرق الهكر معلومات بطاقة الائتمان لأحد العملاء ويستخدمها مدعيا انه العميل أو قد يدعى انه الطرف المستقبل فمثلا يريد العميل أن يصل إلى موقع بنك لكن قد يذهب إلى موقع آخر ينتحل موقع البنك دون إدراك منه ويحصل ذلك الموقع من خلال هذه الطريقة على معلومات العميل.

ثالثا. الهندسة الاجتماعية:

هي فن اختراق عقول البشر وخداعهم بهدف الحصول على معلومات أو بيانات أو أموال كانت ستظل خاصة وآمنة ولا يمكن الوصول إليها، كما اعتمدت الهندسة الاجتماعية على التعامل مع الغرائز البشرية التي تعتبر ثغرات موجودة في الطبيعة الإنسانية مثل الخوف والثقة والطمع والفضول والرغبة في المساعدة والانجذاب للأشخاص المشابهين وغيرها من خلال أساليب مختلفة أهمها الإنترنت والرسائل الإلكترونية والمواقع المزيفة والشبكات الاجتماعية.

رابعا: هجمات الحرمان من الخدمة

ومن اسمه، هدفه حرمان المستخدمين من خدمة معينة والتأثير عليها، ويطلق على أخطر أنواعه اسم (DDOS Distributed Denial of service حيث أن المهاجم يستغل في هذا الهجوم مجموعة من أجهزة الكمبيوتر الأشخاص لا يعرفهم ولكنه قام باستغلال ثغرات موجودة في أجهزتهم في أكثر من مكان ويقوم بمهاجمة سيرفر معين أو شبكة باستخدام هذه الأجهزة دون علم أصحابها.

خامسا غربلة الحزم: sniffing

يشبه غربلة الحزم هجوم التصنت على شخص ما، ويحدث عندما يقوم المهاجم بفحص كل المرور الشبكي الذي يمر ببطاقة التوصيل الشبكي (Network Interface Card (NIC والذي يوصل جهاز المهاجم بالشبكة، هذا بغض النظر عن كون المرور موجه له أو لغيره يحقق القراصنة هجوم الغربلة باستخدام تطبيقات برمجية أو جهاز عناد أو كلاهما معا، وكما ترى في الشكل، تتم الغربلة بعرض كل سيل البيانات الشبكي وتستهدف بروتوكول

معين أو خدمة أو حتى نص من مجموعة حروف مثل معلومات الدخول أو كلمة المرور كما يقوم المغربلون بملاحظة سيل البيانات.

سادسا الانتحال

1-هجمة الرجل الوسيط Man-in-the-Middle

يقوم المهاجم يعمل هجمة الرجل الوسيط عن طريق التعرض للاتصال بين الحواسيب بهدف سرقة المعلومات التي تمر عبر الشبكة يمكن للمهاجم أيضا أن يقوم بالتلاعب في الرسائل وتوصيل معلومات غير صحيحة بين الأجهزة، ولأن الأجهزة المضيفة لن تكون على دراية بحدوث تعديل في الرسائل، لذا يقوم المهاجم بالسيطرة على الأجهزة بدون علم المستخدم وخطوات عملي هجمة الرجل الوسيط موجودة في الشكل وهي كالتالي:

- عندما تطلب الضحية فتح صفحة من صفحات الويب، يتم توجيه الطلب نحو جهاز المهاجم.
- يستقبل جهاز المهاجم الطلب ثم يسحب صفحة الويب الحقيقية من الموقع المعتمد.
- يمكن للمهاجم أن يقوم بالتلاعب المصالحة في صفحة الويب بحيث تسمح له بنقل المعلومات من جهاز الضحية.
- يقوم المهاجم بإرسال الصفحة للجهاز الصحية.

2-هجمة ساعة الصفر: Zero Day

وفي بعض الأحيان تسمى تهديد ساعة الصفر أو تهديد اليوم الصفري وهي عبارة عن محاولة استغلال الثغرات الموجودة في البرمجيات والغير معروفة أو لم تفصح عنها الشركة المصنعة. وتشير ساعة الصفر إلى اللحظة التي يتم اكتشاف الهجوم فيها وخلال الوقت التي تستغرقه الشركة المصنعة في تطوير وتوزيع الرفع للثغرات، تكون الشبكة عرضة للهجوم من خلال تلك الثغرات كما نرى في الشكل الدفاع ضد هذه الهجمات ذات الوقع السريع يتطلب من محترفي الأمن السبيراني أن يستخدموا شكلا أكثر تعقيدا للهيكل الشبكي، لذا فلن يمكن وجود نقاط دخول للشبكة بعد ذلك.

الفرع الثالث : إجراءات الوقاية من الهجمات السبيرانية

لكي يتمكن الأشخاص من الوقاية من الهجمات السبيرانية أو كشفها يجب القيام بإعداد عدد من الإجراءات التقنية المتطورة التي تساعد في اكتشاف هذا النوع من الهجمات قبل الإضرار أو الوقوع ضحيتها. ومن تلك الإجراءات ما يلي[1]:

1. تثبيت برامج تقنية تقوم بمكافحة الفيروسات، والبرامج الخبيثة لعدم شرب أي معلومة.
2. وضع التدابير التنظيمية المضادة، والتي تقوم بتوفير التدريب على الأمن السيبراني.
3. نسخ احتياطية للبيانات لتجنب سيناريو فقد أي بيانات عمل مهمة.
4. العمل على تحديث الأنظمة المستخدمة بالكامل لتصحيح ثغرات البرامج وللحماية من تهديدات الأمان الوارد حدوثها.
5. تأمين شبكات الإنترانت اللاسلكية.
6. التأكد من تشغل تشفير الشبكات وتشفير المعلومات عند تخزين أو إرسالها من خلال الإنترنت.

[1] يحيى عبد الناصر العباسي مهندس الشبكات فرع القامشلي كلية الهندسة جامعة قرطبة الخاصة 2022/2023 ص 26

الفصل الثاني

الحماية الإدارية والجزائية للمعاملات الإدارية الالكترونية

تمهيد:

إن تقنية المعلومات الإدارية لها دور كبير في تحسين العمليات والإجراءات داخل المنظومة الحديثة، فهي تساعد على تسهيل وجودة الخدمات المقدمة وذل ك بطريقة إلكترونية سريعة ، والحلول التقنية جاءت كبديل للتقليل من بطء الخدمات التقليدية، وقلة الميزانيات.

وفي ظل انتشار تكنولوجيا المعلومات فتحت بابا كبير لظهور صور من السلوكيات المعادية لسلوكيات المجتمع التي تؤدي إلى انحراف المجتمع والإخلال بالأمن العام للدولة، فهي تمس سرية وسلامة المعلومات والبيانات الشخصية وبالتالي انتهاك حرمة الأشخاص وبذال ك تخرج عن دائرة العقاب والتجريم ، حيث سمحت نظم الكمبيوتر إلى ظهور صورة جديدة من الجرائم كسرقة البيانات والاحتيال الإلكتروني والقرصنة وغيرها من الجرائم.

ولقد سعت بعض الدول إلى مواكبة التحول نحو نظم إدارة الوثائق الإلكترونية، من خلال إصدار النصوص التشريعية اللازمة لذال ك وعلى هذا الأساس حاول المشرع الجزائري توفير الحماية اللازمة لتأمين الوثائق الإلكترونية كما أقر بوضع آليات قانونية إدارية لتأمين المعاملات الإدارية الإلكترونية وكذا العقوبات الجزائية المترتبة على فعل هذه الجرائم للحد من انتشارها والوقاية من مخاطرها . لهذا سو ف نتناول في هذا الفصل الآليات الإدارية لتأمين المعاملات الإدارية الإلكترونية في المبحث الأول وكذا الحماية الجزائية لتأمين المعاملات الإدارية الإلكترونية في المبحث الثاني.

المبحث الأول: الحماية الإدارية لتأمين المعاملات الالكترونية:

تعتبر الحماية الإدارية المعاملات الإدارية الإلكترونية الركيزة الأساسية لخدمة المجتمع فهي مجموعه من الإجراءات القانونية والإدارية لتحسين سير الإدارة وتسهيل عملياتها وضمان حقوق الأفراد والمؤسسات ضد أي اختراق أو تلاعب يمس امن وسرية المعلومات والوثائق الإدارية الإلكترونية ذل ك سنتطرق في هذا المبحث إلى الحماية الإدارية لتأمين المعاملات الإدارية والسلطات الرقابية التي تخضع إليها الإدارة.

المطلب الأول: مفهوم التوثيق الالكتروني

يعتبر التوثيق الالكتروني مجموعة من القواعد المحدد لشروط قبول الشهادات الالكترونية، وتعتبر الكتابة بصفة عامة أهم طرق الثبات وأصلحها فقد كانت الكتابة على

سند مادي وأصبحت حاليا تأخذ شكلا الكترونيا، وصيغت بنفس القيمة القانونية الممنوحة للكتابة التقليدية ولهذا سنعرف التوثيق الالكتروني ثم نعرض شروطه.

الفرع الأول: تعريف التوثيق الالكتروني:

سنتطرق في هذا الفرع إلى تعريف الكتابة الالكترونية ثم نعرف التوثيق الالكتروني

1 الكتابة الالكترونية:

عرّف القانون النموذجي للتجارة الالكترونية بقوله:" أنها تشمل رسالة البيانات وتسهل الاطلاع عليها على نحو يتيح استخدامها عن طريق الرجوع إليها مستقبلا"[1].

ويتجلى أسلوب الكتابة الحديثة على أنها تطوير للكتابة التقليدية لظهور ما يسمى الكمبيوتر وأصبح يمكن التعاقد عن بعد دون حضور مجلس تقاعد واحد في نفس الوقت يتم تبادل الإيجاب والقبول. لذا شرّع المشرع الفرنسي في تعديل القانون المدني سنة2000 ونصّ في المادة 1316 على أن الإثبات الخطي أ الإثبات بالكتابة ينتج عن سلسلة من الخصائص والحروف والأرقام والرموز او إشارات مخصصة تدل على مفهوم واضح مهما كانت دعامة إرسالها[2]، وتقابلها المادة 323 مكرر من الأمر رقم 75–58 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975، المتضمن القانون المدني الجزائري.[3]

وتجدر الملاحظة أن المشرع الجزائري كباقي التشريعات العالمية ساوى بين الكتابة التقليدية والكتابة الالكترونية متى استجمعت هذه الأخيرة شرطان هما:

- الإمكان تحديد هوية الشخص الذي أصدرها.
- وأن يتم حفظها في ظروف تضمن سلامتها.

[1] قارة ملود، التوثيق الإلكتروني، شكله وإجراءاته، كلية الحقوق والعلوم السياسية ، المسيلة ، الجزائر ،2022 ، ص 1545.

[2] المادة 1316 من القانون المدني الفرنسي، المعدل والمتمم، بموجب القانون رقم 2000-230 المؤرخ في 13 مارس 2000 المتعلق بالإثبات الإلكتروني، الجريدة الرسمية للجمهورية، الفرنسية (JORF) العدد62،بتاريخ 14 مارس 2000

[3] المادة 323 مكرر من الأمر رقم 75-58 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975، المتضمن القانون المدني الجزائري، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 78 لسنة 1975، المعدل والمتمم بموجب القانون رقم 05-10 المؤرخ في 20 يونيو 2005، الجريدة الرسمية، العدد 44 لسنة 2005

الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق شريطة استجمعاها للشرطين المذكورين أعلاه، ومتى كان الأمر كذلك التزم القاضي بها على نحو يجسد مبدأ المعادلة الوظيفية بين الكتابتين.

والمشرع اقتدى بالفقه من حيث البحث في شروط الكتابة الالكترونية التي تشترط أولا أن تكون مقروءة بحروف ورموز معروفة في حين أن الشرط الثاني يبقى على الكتابة الالكترونية مستمرة ودائمة سواء كانت على ورق أو على الوسائط الإلكترونية لفقرات معينة من الزمن يمكن طلبها إذا دعت الحاجة لذلك.

أمّا الشرط الثالث فهدف إلى قيد الكتابة على نحو لا تكون قابلة للتعديل فكل تعديل لاحق للبيانات بتم كشفه ببساطة.

ومن بين الوسائط المعدة لحفظ البيانات الالكترونية توجد بطاقة الذاكرة الممغنطة والقرص الصلب وغيرها، فكل ما يشترط فيها أن تكون آمنة وتضمن استمرارية حفظ البيانات.

لكن أهم وسيط الالكترونية هو الطرف الذي أشارت إليه المادة 02 فقرة11 من القانون 04/15 المتضمن القواعد العامة المتعلقة بالتوقيع والتصديق الالكتروني.

2 -تعريف التوثيق الالكتروني

إن وثيقة العمل المصرفي كانت بداية ظهور التوثيق الالكتروني للعمليات المنجزة واختلفت الدول في تقديم تعريف خاص بالتوثيق الإلكتروني فمنهم من وجّه مضمونه إلى إجراءات التوثيق ومنهم من عالج التوثيق من زاوية تحديد الجهات المخوّلة به.

فهذا المشرع الأمريكي الذي أشار إلى أن التوثيق الالكتروني هو:" مصطلح يشير إلى التشفير أو الوسائل الالكترونية الآمنة التي تسمح لمستعمل هذه الوسائل بأن:

- تتأكد من الهوية أو المعلومات المتعلقة بمن تم التعامل معه.
- التأكد من أن الوثائق المثبتة له بين الأطراف المتعاقدة معه لم تعدل ولم تغير الثناء إرسالها.

- التأكد من الوثائق المسلمة أرسلت من قبل الطرف المحدد.

وعرّف مشرع إمارة دبي لسنة 2002 التوثيق الإلكتروني بأنّه:" الإجراءات التي تهدف التحقيق من أن الرسالة الالكترونية قد صدرت من شخص معين والكشف عن أي خطأ أو تعديل من محتويات أو في نقل أو تخزين رسالة إلكترونية. أو السجل الالكتروني خلال فترة زمنية محددة أو تسجيل ذلك أي إجراء يستخدم مناهج حسابية أو رموز أو كلمات أو أرقام تقريبية أو إجراءات للرد أو الإقرار بالاستلام وغيرها من وسائل إجراءات حماية المعلومات" ونقيض هذا نجد أنه لم يعرف التوثيق الالكتروني ولكن عرّف الشخص القائم به.

المشرع الجزائري وقد خالف باقي التشريعات وعرّف التوثيق والتصديق الالكتروني في المادة 02 فقرة11 وعرّف الموثق بأنّه:" شخص طبيعي أو معنوي يقوم بمنح شهادات تصديق الالكتروني موصوفة وقد يقدم خدمات أخرى في مجال التصديق الالكتروني لفائدة المتدخلين في الفرع الحكومي "، وأضافت المادة 12 من نفس القانون إلى تعريف مؤدي خدمات التصديق الإلكتروني بقولها: "كل شخص طبيعي أو معنوي يقوم بمنح شهادات تصديق الكتروني موصوفة وقد يقدم أخرى في مجال التصديق الالكتروني".

و وضحت المادة 02 فقرة12 المقصود بالمتدخلين الحكوميين وهم المؤسسات والإدارات الحكومية والمؤسسات الوطنية المستقلة وكل شخص أو كيان ينتمي الفرع الحكومي بحكم طبيعته أو مهامه.[1]

ثالثا: شروط التوثيق الإلكتروني:

ليكتسب التصرف الالكتروني حجية في الإثبات يعتد بها شأنه شأن التصرف القانوني التقليدي، لابد من توثيقه الكترونيا لدى جهة مرخصة أو معتمدة وهذا التوثيق حتى تكون له قيمة قانونية ويمكن الاحتجاج به أمام أطراف التصرف أو الغير لابد من أن تتوافر شروط عدة وهذه الشروط هي:

1-صدور التوثيق الالكتروني من جهة مرخص لها أو معتمدة:

[1] قارة ملود ، التوثيق الالكتروني ،مرجع سابق ، ص 1546.

يجب أن يصدر التوثيق من جهة مرخص لها أو معتمدة لمزاولة مهنة التوثيق الالكتروني، إذ نص قانون التوقيع الالكتروني والمعاملات الالكترونية العراقي رقم(78) لسنة 2012 في المادة 07 على أنّه:" لا يجوز مزاولة نشاط إصدار شهادات التصديق دون الحصول على ترخيص وفق أحكام هذا القانون".[1]

وذهب المشرع المصري بالاتجاه نفسه في قانون التوقيع الالكتروني المصري رقم(15) لسنة 2004 في المادة 19 إذ لم يجيز مزاولة نشاط تقديم خدمات التوثيق الالكتروني وإصدار الشهادات إلا بعد الحصول على ترخيص مسبق من قبل هيئة تنمية صناعة التكنولوجيا تحدد فيه وظيفة واختصاص مقدم الخدمة وبيان واجباته ومسؤولياته، وكذلك هو الحال بالنسبة للقانون التونسي إذ نص على أنه:" يتعين على كل شخص طبيعي أو معنوي يرغب في العمل في نشاط مزود خدمات التصديق الالكتروني الحصول على ترخيص مسبق من الوكالة الوطنية للمصادقة الالكترونية...".[2]

أما القانون الأردني فقد اشترط بمقدم خدمات التوثيق ان يكون مرخصا له بموجب نظام ترخيص واعتماد جهات التوثيق الالكتروني رقم11 لسنة 2014، وكذلك اعتبر التوقيع الالكتروني موثقا إذا استوفى الشروط التي نص عليها القانون وارتبط بشهادة توثيق الكترونية صادرة عن جهة معتمدة أو مرخص لها أو صادرة من دائرة حكومية أو مؤسسة أو هيئة مفوضة قانونا أو صادرة عن جهة متفق عليها بين أطراف المعاملة. وهذا ما لم يأخذ به قانون آخر.

أمّا التشريعات الدولية فلم ينص القانون النموذجي بشأن التوقيعات الالكترونية الذي وضعته لجنة الأمم المتحدة للقانون التجاري الدولي(الأونسترال) لسنة 2001، على وجوب حصول مقدم خدمات التوثيق على ترخيص لمزاولة المهنة.

[1] المادة 07 من قانون التوقيع الإلكتروني والمعاملات الإلكترونية رقم (78) لسنة 2012، الصادر عن مجلس النواب العراقي، المنشور في الجريدة الرسمية "الوقائع العراقية"، العدد (4256)، بتاريخ 5 نوفمبر 2012، النافذ ابتداءً من سنة 2012

[2] المادة 19 من قانون التوقيع الالكتروني المصري رقم 15 لسنة 2001 الصادر بتاريخ 22أفريل، 2004 الجريدة الرسمية لجمهورية مصر العربية، العدد17

مما سبق نجد أن الأفضل وللزيادة في الأمان والثقة واستقرار المعاملات أن يحصل مقدم خدمة التوثيق الالكتروني على ترخيص من الجهة المختصة في الدولة.[1]

2-صدور شهادة التوثيق الإلكتروني من مقدم خدمات التوثيق الإلكتروني:

أن يُصدر مقدم الخدمات التوثيق شهادة إلكترونية وظيفتها نسبة التصرف الإلكتروني إلى صاحبه بصورة مؤكدة أي تنسب التوقيع إلى من صدر عنه بصورة لا تقبل الشك، والتي من شأنها(الشهادة) أن تكشف أي تعديل أو تغيير يجري على السند أو المحرر الالكتروني من صاحب العلاقة أو الغير وهذه الشهادة تسمى شهادة التوثيق الإلكتروني.

3- مراعاة الإجراءات القانونية:

أن يصدر التوثيق الالكتروني وفقا للإجراءات المنصوص عليها وفق أحكام القانون، إذ تتشدد بعض القوانين كقانون التوقيع الالكتروني والمعاملات الالكترونية العراقي وقانون التوقيع الالكتروني المصري في إجراءات التوثيق الالكتروني وتنص عليها وتخضعها لرقابة الجهات المختصة في الدولة ولا تفضل تركها لإرادة الأطراف لما في ذلك من خطورة تعرضها للتعديل والتغيير ومن ثم فقدان الثقة والأمان بالتعاملات الإلكترونية وعلى عكس ذلك فقد أعطى المشرع الأردني المؤقت أطراف المعاملة مساحة أوسع في حرية الاختيار بين الإجراءات المعتمدة والإجراءات المقبولة تجاريا والإجراءات المتفق عليها بين أطراف المعاملة الالكترونية.

4-تعلق التوثيق الالكتروني على تصرف قابل للتوثيق:

أن ينصب التوثيق على تصرف الكتروني قابل للتوثيق الالكتروني وإلا كان التوثيق من غير قيمة قانونية إذ هنالك تصرفات لا يمكن إجراءها بطريقة الكترونية ومن ثم يستحيل توثيقها الكترونيا كالتصرفات التي اشترط فيها القانون شكلية معينة كالزواج إذ نص قانون

[1] أكرم تحسين الدخيلي، النظام القانوني للتوثيق الإلكتروني، الطبعة الأولى، مكتبة زين الحقوقية والأدبية، 2018 ،ص 25.

التوقيع الكرتوني والمعاملات الالكترونية العراقي فقي المادة 3 على أن: "ثانيا: لا تسري أحكام هذا القانون على ما يلي:[1]

أ-المعاملات المتعلقة بمسائل الأحوال الشخصية والمواد الشخصية.

ب-إنشاء الوصية والوقوف وتعديل أحكامها.

ج-المعاملات المتعلقة بالتصرف بالأموال غير المنقولة بما في ذلك الوكالات المتعلقة بها وسندات ملكيتها وإنشاء الحقوق العينية عليها باستثناء عقود الإيجار الخاصة بهذه الأموال.

د- المعاملات التي رسم لها القانون شكلية معينة.

هـ - إجراءات المحاكم والإعلانات القضائية والإعلانات بالحضور وأوامر التفتيش وأوامر القبض والأحكام القضائية.

الفرع الثاني: إجراءات التوثيق الالكتروني:

لقد اتفقت التشريعات على إجراءات الكترونية تقع على عاتق التوثيق ومباشرتها من أجل حماية صاحب الشهادة الالكترونية وأطراف العقد لذا سنستدرج في الفرع الأول: إجراء التحقق من صحة البيانات ثم إجراء التعليق العام بشهادة الكترونية أو إلغائها في الحالات التي تستوجب ذلك.

أولا_ إجراءات التوثيق الالكتروني بالتحقق من صحة البيانات المقدمة أو صحة الشهادات الالكترونية الصادرة من الجزائر أو خارجها:

وتلتزم هنا جهات التوثيق باتخاذ الإجراءات الممكنة التي تسمح من تثبيت صحة البيانات الشخصية المتعلقة بالمتعاملين وصفاتهم المميزة التي سيتم المصادقة عليها وتضمنها في الشهادة وهذا الإجراء جوهري من خلال اتصال مباشر بتقديم الأوراق الثبوتية، وعملا بالتوجيه الأوروبي93/1999 الذي ألزم جهات التوثيق بالسعي قبل إصدار الشهادة إلى اتخاذ إجراءات كافية لجمع المعلومات المتعلقة بطالب الشهادة الإلكترونية وأجاز له الحصول عليها من الغير بناء على موافقة مكتوبة وأنه ألزمها بعدم استعمال المعلومات

[1] أكرم تحسين الدخيلي، النظام القانوني للتوثيق الإلكتروني، ص 26-28.

خارج نطاق التوثيق ويلتزم بالبيانات المقدمة له فلا يجوز اتخاذ أي إجراء أو عمل يهدف إلى تعديل مضمونها أو ما يصطلح عليها حظر معالجة البيانات الالكترونية.

فضلا عن ذلك تتخذ جهات التصديق الكرتوني عملية تحديث المعلومات المصادق عليها كما نضع بنك معلومات يتضمن شهادات المصادقة الصدارة عنه وتعمل على الخصوص بنشر تاريخ إصدارها وتاريخ انتهاء مدة صلاحيتها أو توقيف مفعولها أو إلغائها.

أما بيانات التحقق في صحته فهي البيانات المستخدمة للتحقق من مصداقية التوثيق وصحته كالترميز والتشفير وتختص جهات التوثيق بتمكين الغير بالوسائل التي تحدد هوية الشخص المذكور في الشهادة الالكترونية والشخص الذي يحوز أداة التوقيع.

أما بخصوص الشخص المعنوي فقد ألزم المشرع الجزائري في المادة 44 فقرة 02 من القانون 04/15 جهة التصديق بقيد سجل يدوم فيه هوية وصفة الممثل القانوني للأشخاص الاعتبارية أين يمكن تحديد هوية الشخص الطبيعي عند كل استعمال.[1]

ثانيا: إصدار الشهادة الالكترونية:

تعتبر الشهادة الالكترونية جوهر عمل جهات التصديق الالكتروني لكونها تعطي الثقة والأمان لاستكمال المعاملة الالكترونية،وبهذا المعنى فهي سند أمان صادر عن جهة مختصة يفيد قيد تسجيل المعاملة وهذه الشهادة هي رسالة الكترونية تسلم من شخص ثالث موثوق فيه تكون لها وظيفة ربط التويع بصاحبه وتحتوي على المعلومات الكاملة عن المتعامل من هوية وعنوان وأهلية وصفة وطبيعة الشخص القانونية واسم الشهادة والمفتاح العمومي والرقم التسلسلي وتاريخ صلاحية الشهادة وتاريخ انقضائها وحتى تاريخ تسليمها للمعني وهذا الإجراء في حال اكتماله تتجلى نتيجته في صدور شهادة توثيقية مستوفية لكامل شروط استخراجها.[2]

وتوسّع المشرع الجزائري في وصف الشهادة الالكترونية وقام بتقسيمها إلى نوعين مقارنة ببعض القوانين المقارنة فموجب المادة 03 من المرسوم التنفيذي 07/162 عرف

[1] المادة 44الفقره 02من قانون 04-15السالف الذكر

[2] قارة ملود ، توثيق الالكتروني ، مرجع سابق ، ص1553 .

نوعين من الشهادات:[1] شهادة عادية وشهادة موصوفة الأولى تعتبر وثيقة في شكل الكتروني تثبت الصلة بين معطيات فحص التوقيع الالكتروني والموقع أما الشهادة الثانية أي الموصوفة فهي الشهادة الموصوفة للتوقيع الالكتروني المنصوص عليها في المادة 03 فقرة 09 بأنّها شهادة تستجيب للشروط المحددة ولم ينص عليها المشرع الجزائري.[2]

كما تعرّف أيضا بأنّها" نتائج عمليات النماذج، التكوين، التنظيم، أو تحويل البيانات بطريقة تؤدي إلى زيادة مستوى المعرفة للمستقبل".[3]

من خلال هذا التعريف يمكننا القول إنّ 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: إنّ المعلومات هي كل ما يصل إلى علم الفرد، سواء أكان ذلك بالقراءة أم بالاستماع أم المشاهدة وتتعلق بجوانب وأمور تتصل بحياة الإنسان والأوضاع المحيطة به، والعلاقات التي يقيمها والظروف التي تلازمه والإمكانيات المتاحة له والأحداث التي يواجهها من وقت لآخر.

الفرع ثالث: ضوابط عملية معالجة المعطيات ذات الطابع الشخصي

اتجه الفقه الفرنسي في تعريفهم للحق في الحياة الخاصة إلى وضع قائمة للقيم التي تعطيها فكرة الخصوصية فحاولوا وضع قائمة بالحالات والأمور التي تدخل في إطار الحياة الخاصة فذكروا الحياة العائلية والحياة المهنية والحق في الصورة وكشف الضرائب وكشف الراتب والمرض ومكان قضاء أوقات الفراغ والموارد المالية.

وقد أضاف البعض الآخر الحق في الاسم والحق في الشرف والاعتبار والحق في النسيان وماضي الشخص وأضاف البعض الأخر الحياة الروحية الداخلية التي يمارسها الإنسان خلف بابه المغلق.

[1] المادة 03من المرسوم التنفيذي رقم 07-162 السابق الذكر

[2] قارة ملود ، توثيق الالكتروني ، مرجع سابق ، ص1554.

[3] قدايفية أمينة، استراتيجية أمن المعلومات، جامعه أمحمد بوقره ، بومرداس، ص 164.

أما بالنسبة للمشرع الجزائري فقد عرّف لنا المعطيات ذات الطابع الشخصي من خلال المادة 03 من القانون 18-07 بأنها: "كل معلومة بغض النظر عن دعامتها متعلقة بشخص معرف أو قابل للتعرف عليه والمشار إليه أدناه (الشخص المعني) بصفة مباشرة أو غير مباشرة لاسيما بالرجوع إلى رقم التعريف أو عنصر أو عدة عناصر خاصة بهويته البدينة أو الفيزيولوجية الجينية أو البيومترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية.[1]

وتتم المعالجة من خلال ضوابط تحدد حقوق الشخص المعني بعملية المعالجة والالتزامات الملقاة على عاتق المسئول عن عملية المعالجة ومنه قسم هذا الجانب الأول لحقوق المعني بعملية المعالجة والثاني نتناول فيه إلتزامات المسؤول عن المعالجة.

أولا: حقوق الشخص المعنى بعملية المعالجة:

ضبط المشرع الجزائري عملية معالجة المعطيات ذات الطابع الشخصي من خلال إعطاء الشخص المعني بعملية المعالجة مجموعة من الحقوق تحفظ له خصوصية وسرية معطياته والمتمثلة في:

-الحق في الإعلام:

تنص المادة 32 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، على وجوب الإعلام المسبق للشخص المعني بعملية معالجة بياناته الشخصية، وذلك من خلال تزويده بجملة من المعلومات الأساسية التي تضمن الشفافية وحماية رضاه الحر[22]

ويشمل هذا الإعلام وجوب تحديد هوية المسؤول عن المعالجة وصفته القانونية ووسائل الاتصال به، إضافة إلى الغرض أو الأغراض المحددة من معالجة المعطيات، بما يتيح

[1] خلوف حسام، باطلي غنية، الآليات القانونية لحماية المعطيات ذات الطابع الشخصي، مجلة الدراسات القانونية والاقتصادية، المجلد 05،العدد01، جامعه سطيف، 2022 ،ص1633.

[2] المادة 32 ، من القانون 18/07 ، المؤرخ في 25 رمضان عام 1439هـ الموافق 10 يونيو 2018،المعدل والمتمم بالقانون رقم 25-11 المؤرخ في 24 يوليو 2025 ، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

للمعني فهم الأساس الذي تتم عليه هذه المعالجة ومدى مشروعيتها. كما يتعين إعلامه، عند الاقتضاء، بالمعلومات الإضافية التي قد تكون ضرورية لضمان وضوح العملية، لاسيما هوية المرسل إليه أو فئات المرسلين إليهم الذين قد تُحوَّل إليهم البيانات. ،.[1]

_الحق في الولوج:

تنص المادة 34 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي على تكريس حق الشخص المعني في الولوج إلى بياناته الشخصية ومعرفة كيفية معالجتها، وذلك من خلال تمكينه من طلب الاستفسار والتأكد من معالجة معطياته من طرف المسؤول عن المعالجة، مع بيان الأغراض التي تتم من أجلها هذه المعالجة، وكذا فئات المعطيات محل المعالجة، إضافة إلى الجهات أو الفئات التي تم أو يمكن أن تُرسل إليها هذه البيانات.1

_ الحق في التصحيح

تنص المادة 35 من القانون 07-18 المتعلق بحماية الاشخاص الطبعيين ذات الطابع الشخصي أن حقّ الشخص في طلب تصحيح أو تحيين أو مسح أو غلق معطياته الشخصية متى تبيّن أنها غير مكتملة أو غير صحيحة أو أن معالجتها تتم بصفة غير قانونية. ويُقدَّم طلب التصحيح إلى المسؤول عن المعالجة، الذي يلتزم بالاستجابة له وإجراء التصحيحات اللازمة مجانًا لفائدة المعني، وذلك في أجل أقصاه عشرة (10) أيام.[2]

وفي حال رفض الطلب أو عدم الرد عليه خلال الأجل القانوني المحدد، يمكن لصاحب الشأن اللجوء إلى السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، التي تتولى بدورها فتح تحقيقات قانونية واتخاذ الإجراءات المناسبة للتصحيح، مع إعلام المعني بمآل طلبه ونتائج المعالجة.

1 المادة 34من القانون 07-18 المتعلق بحماية الاشخاص الطبيعيين ذات الطابع الشخصي، المؤرخ في 25رمضان 1439، الموافق ل 10يونيو 2018،الجريدة الرسمية العدد34من القانون 18-07السالف الذكر

[2] المادة 35ن القانون رقم 07-18 المعدل والمتمم بالقانون رقم 11-25 السالف الذكر

_الحق في الاعتراض:

تنص المادة 36 من القانون 07-18 على أنه يحقّ للشخص المعني أن يعترض، لأسباب مشروعة، على معالجة معطياته ذات الطابع الشخصي. كما يجوز له رفض استخدام هذه المعطيات لأغراض دعائية، ولا سيما التجارية منها، دون أن يكون ملزماً بتقديم أي تبرير أو سبب لاعتراضه.[1]

منع الاستكشاف المباشر

يمنع بموجب القانون 18/07 القيام بأي عملية استكشاف مباشر باستخدام أي وسيلة تكنولوجية تعتمد على بيانات شخص طبيعي، وبأي صيغة كانت، ما لم يتم الحصول على موافقة صريحة من صاحب البيانات.

ومع ذلك، يُسمح بالاستكشاف المباشر عبر البريد الإلكتروني في حالات محددة، خاصة عندما تكون بيانات الاتصال قد تم الحصول عليها من المرسل إليه بغرض بيع منتج أو تقديم خدمة، أو عندما يتعلق الأمر بالترويج لمنتجات أو خدمات مماثلة لتلك التي سبق أن قدمها نفس الشخص الطبيعي أو الاعتباري، بشرط أن يتم ذلك بشكل واضح وصريح ودون أي غموض.

ثانيا: إلتزامات الشخص المعني بالمعالجة:

نص عليها المشرع بعنوان إلتزامات الشخص المعني بالمعالجة في القانون 07-18 المعدل والمتتم بالقانون 11-25 المتعلق بحماية الاشخاص الطبيعين في مجال معالجة المعطيات ذات الطابع الشخصي

[1] المادة 36من القانون رقم 07-18 المعدل والمتمم بالقانون رقم 11-25

1-سلامة المعالجة:

نص المادة 38 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي (المعدل والمتمم بالقانون 25-11) هو:يتعين على المسؤول عن المعالجة أن يتخذ التدابير التقنية والتنظيمية المناسبة لحماية المعطيات ذات الطابع الشخصي من التلف العرضي أو غير المشروع، أو الفقدان العرضي، أو التغيير، أو الإفشاء أو الوصول غير المصرح به، خاصة عندما تتضمن المعالجة نقل المعطيات عبر شبكة، وكذلك من أي شكل آخر من أشكال المعالجة غير المشروعة.[1]

2-سرية المعالجة: إن مبدأ سرية المعالجة التزام المسؤول عن المعالجة، وكل من يتدخل في عمليات معالجة المعطيات ذات الطابع الشخصي، بضمان عدم إفشاء هذه المعطيات أو إتاحتها للغير غير المخوّل لهم قانونًا، مع الحرص على الاطلاع عليها يكون فقط من الأشخاص المرخّص لهم حصراً، وذلك تحت طائلة الالتزام الصارم بالسر المهني في جميع مراحل المعالجة. ويهدف هذا المبدأ إلى حماية الحياة الخاصة للأفراد وضمان عدم المساس بخصوصية البيانات الشخصية أو استخدامها خارج الأغراض التي جُمعت من أجلها.[2]

الفرع الرابع: سرية الوثائق الإدارية

1 _تعريف الوثائق وأنواعها

يُعدّ مفهوم الوثيقة من المفاهيم التي يصعب ضبطها بشكل دقيق، وذلك نتيجة تباين المقاربات التشريعية وتعدد الاستخدامات في المجالات العلمية والأكاديمية والإدارية، حيث يستعمل مصطلح الوثائق إلى جانب مصطلحات أخرى مترادفة أو قريبة المعنى مثل المحررات والسندات والأرشيف والمحفوظات، وهو ما أدى إلى اختلاف الفقهاء والباحثين في تحديد مدلوله.

[1] المادة 38 من القانون رقم 07-18 المعدل والمتمم بالقانون رقم 11- 25 السالف الذكر

[2] حمليل نوارة، "حماية المعطيات الشخصية في مواجهة الإدارة الإلكترونية "، المجلة النقدية للقانون والعلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة مولود معمري – تيزي وزو، الجزائر، المجلد 15، العدد 02، سنة 2020، ص 47

وعلى مستوى التشريع الجزائري، لم يرد تعريف محدد ودقيق لمصطلح الوثيقة الإدارية، رغم استعماله في العديد من النصوص القانونية والتنظيمية، حيث يتضح من خلال هذه النصوص أن المشرع استعمله للدلالة على كل وثيقة ذات طابع عمومي يتم تداولها داخل الإدارة الجزائرية وتتضمن معلومات يتم الحصول عليها بشكل مباشر أو غير مباشر، مثل الرسائل والخرائط والصور والأشرطة المغناطيسية والأفلام والأقراص الضوئية وغيرها من الوسائط.1[1]

وقد جاء القانون رقم 21/09 المتعلق بحماية المعلومات والوثائق الإدارية ليقرّ مفهوم الوثيقة في مادته الثالثة (البند 02)، حيث عُرفت بأنها: "المراسلات والمحررات والمستندات التي أنشأتها أو حصلت عليها أي من السلطات المعنية أثناء ممارسة نشاطها".[2]

3 أنواع الوثائق الإدارية ::

حسب نوعية العمل:

تمثل طبيعة العمل الإداري في أن جزءاً منه يتكرر بشكل واسع داخل مختلف الإدارات، مما يجعله عملاً ذا طابع عام ومشترك بين أغلب المصالح. في حين توجد أعمال أخرى تتميز بالخصوصية، إذ تنفرد بها كل إدارة بحسب مهامها واختصاصاتها الفنية، وهو ما ينعكس على طبيعة الوثائق الناتجة عنها من حيث التصنيف والتداول داخل المؤسسة. وبناءً على ذلك، تُصنف الوثائق الإدارية باعتبارها ناتجة عن النشاط الإداري إلى نوعين رئيسيين: وثائق مشتركة تستعملها مختلف الإدارات التي تتشابه في وظائفها، مثل تسيير الموارد البشرية والمالية ومكاتب الاستقبال والتعامل مع المواطنين ومصالح الضبط، ووثائق خاصة ترتبط بهياكل أو مصالح معينة وفق تنظيمها وأهدافها.

كما يعتمد قانون الأرشيف الصادر في أوت 1988 على معيار دورة حياة الوثيقة وقيمتها الإدارية لتصنيفها، حيث يميز بين الوثائق النشطة التي تكون ذات قيمة إدارية

[1] اسماعيل علي محمود، مرجع سابق ص، 110

[2] المادة 03البند 02 من الأمر رقم 21–19 المتعلق بحماية المعلومات والوثائق الإدارية، المؤرخ في 27شوال عام 1442الموافق ل 08يونيو، 2021 الجريدة الرسمية العدد 45.الصادرفي 09يونيو 2021.

مرتفعة منذ لحظة إنشائها، باعتبارها وثائق قيد الاستعمال وتدخل في إطار المعالجة والمتابعة الإدارية.

عنصر الثبات: تُعدّ الوثائق التي يمكن نقلها أو تداولها من مصلحة إدارية إلى أخرى، أو من إدارة إلى مستفيد من خدمة تابعة لإدارة أخرى، مثل وسائل الاتصال، وثائق قابلة للحركة زمانًا ومكانًا. ومن بين هذه الوثائق تلك الأكثر تداولًا والتي تساهم في ربط العلاقات بين الإدارة ومختلف الهياكل الإدارية، سواء داخل المؤسسة أو خارجها. في المقابل، توجد وثائق لا يمكن نقلها إلا في حالات استثنائية، مثل السجلات و الدفاتر.[1]

الفرع الخامس: الأرشيف

باشرت الجزائر منذ السنوات الأولى للاستقلال عملية تقنين مجال الأرشيف، من خلال توفير إطار قانوني يضمن التسيير الفعّال لهذا القطاع الحيوي. وتبرز أهمية التشريعات في هذا المجال في كونها أداة أساسية لتنظيم أساليب التسيير وتحديد العلاقات بين منتجي الأرشيف ومسيريه والمستفيدين منه.

و ستتناول هذه الدراسة مظاهر الحماية القانونية التي أقرّها المشرّع الجزائري للأرشيف، وما يعكسه ذلك من اهتمام تشريعي صارم يهدف إلى معالجة مختلف الإشكالات التي قد يتعرض لها هذا القطاع.

أولا: المركز القانوني للأرشيف:

قبل التطرق إلى الحماية القانونية للأرشيف، من الضروري تحديد مركزه القانوني. فتصنيف الأرشيف من حيث طبيعته القانونية يرتبط بالجهة التي قامت بإنتاجه، أي مصدره، مما يؤدي إلى تقسيمه إلى أرشيف عمومي (Publique) وأرشيف خاص (Privé).

وقد اعتمدت معظم النصوص القانونية المنظمة لمجال الأرشيف هذا التمييز الثنائي. فالأرشيف العمومي يخضع لقواعد القانون العام، ويتميز بعدم قابليته للتملك أو التصرف فيه بالبيع أو الشراء أو الهبة، كما لا يجوز الحجز عليه أو اكتسابه بالتقادم، باعتباره جزءًا من

[1] إسماعيل علي محمود مرجع سابق 111.

الملكية العمومية. في المقابل، يخرج الأرشيف الخاص عن نطاق المؤسسات العمومية، إذ تنتجه هيئات أو مؤسسات غير تابعة للقطاع العام، وتبقى ملكيته خاضعة للجهة التي أنشأته.

وفي الجزائر، يُعد القانون 88-09 الصادر بتاريخ 26 جانفي 1988 النص المرجعي الذي تناول تعريف الأرشيف، حيث عرّفته المادة الثانية بأنه مجموعة من الوثائق التي تتضمن معلومات مهما كان تاريخها أو شكلها أو وسيلة حفظها، والتي تنتج أو تستقبل من طرف شخص طبيعي أو معنوي، أو مصلحة أو هيئة عمومية كانت أو خاصة، أثناء ممارسة نشاطها.[1]

كما تنص المادة 03 على أن الأرشيف يتكوّن من مجموع الوثائق الناتجة أو المستلمة من الدولة أو الحزب أو الجماعات المحلية أو الأشخاص الطبيعيين أو المعنويين، سواء في القطاع العام أو الخاص، أثناء ممارسة نشاطهم، وذلك بالنظر إلى قيمتها أو فائدتها، سواء احتُفظ بها لدى مالكها أو حائزها أو نُقلت إلى مؤسسة الأرشيف المختصة..[2]

ثانيا: الحماية القانونية للأرشيف:

1-الحماية الجزائية:

يتبين من خلال التطور التاريخي لمفهوم الأرشيف أن هذا النوع من الحماية لم يكن موضع اهتمام خلال عصور التاريخ السابقة ولم يحظ باهتمام إلا مؤخرا في دول أوروبا وأمريكا وحديثا جدا في الدول العربية حيث لم تخلو أغلب التشريعات المعاصرة الخاصة بالأرشيف من نصوص تجرم بعض صور الاعتداء الخطيرة على الأرشيف لذلك كان لابد من اللجوء إلى العقوبات الجنائية لما تشمل عليه من قوة ردع زاجرة تكفل حماية أكثر فعالية للأرشيف وظهر.

[1] ختير فوزية فاطمة، الأرشيف ومهنة الأرشيفي في الجزائل،دراسة ميدانية بالغرب الجزائري، رسالة دكتورا في العلوم علم المكتبات والعلوم الوثائقية، كلية العلوم الإنسانية والعلوم الإسلامية، سنة2014/2015،ص 45

[2] كمال درواز، الحماية القانونية للأرشيف في التشريع الجزائري، مجلة المكتبات والمعلومات ، 2003 ،ص 116.

هذا الأخير في الجزائر سنة 1988 وتحديدا في القانون 09/88 المؤرخ في 26 يناير 1988 فجمع في مواده بين أحكام القانون العام 'الجنائي' وأحكام القانون الخاص "المدني".

2- الحماية المدنية للأرشيف:

تقوم المسؤولية المدنية في الأصل على جبر الضرر الناتج عن الاعتداءات التي تمس المصنفات الأدبية والفنية والعلمية، وذلك متى توفرت أركانها الثلاثة المتمثلة في الخطأ والضرر وعلاقة السببية، سواء تعلقت هذه المسؤولية بالمجال العقدي أو التقصيري. غير أن نطاق هذه القواعد يرتبط أساسًا بحماية حقوق المؤلف والحقوق المجاورة، وهو ما يجعل تطبيقها على الأرشيف محل إشكال قانوني.[1]

فالوثيقة الأرشيفية لا تندرج ضمن المصنفات الفكرية ذات الطابع الأدبي أو الفني أو العلمي، بل تتميز بطبيعة إدارية ووظيفية خاصة، الأمر الذي يخرجها من مجال الحماية المقررة لحقوق المؤلف. ورغم أن المشرع الجزائري قد أقر حماية قانونية لحق المؤلف في حالات الغش والاعتداء والاحتيال، إلا أن الأرشيف لا يخضع لنفس النظام القانوني بشكل مباشر، ولا تخضع حمايته لنظام المسؤولية العقدية أو التقصيرية التقليدية بصورتها المباشرة فإذا رجعنا لأحكام القانون المدني لا نجد أي نص يتطرق بصراحة لحماية الأرشيف ولا يمكن أن نطبق عليه القواعد العامة في مجال المسؤولية العقدية لأنها تنشا بتوافر شروط معينة كأن يكون هناك عقد تام وصحيح بين المسئول والمتضرر كذلك الشأن في المسؤولية التقصيرية التي لا يشترط فيها القيام بعقد صحيح لان الاعتداء يقع من شخص لا تربطه علاقة تعاقدية مع صاحب المصنف محل الاعتداء.

3-الحماية الدولية للأرشيف:

بفعل التطور المتسارع للتكنولوجيا الحديثة ووسائل الاتصال، وتزايد حجم العلاقات والمبادلات الدولية في مختلف المجالات، برزت الحاجة إلى إبرام اتفاقيات دولية تُعنى بتنظيم حماية الأرشيف وصونه من مختلف صور الاعتداء أو الضياع. وقد تجسدت هذه الحماية في إطار اتفاقيات دولية متعددة الأشكال، يمكن تصنيفها إلى نوعين رئيسيين:[2]

[1] الحمايه المدنية كمال درواز الحمايةالقانونيةلأرشيف في الجزائر مرجع سابق ص 122
[2] الحماية دوليه كمال درواز الحماية القانونية لأرشيف في الجزائر مرجع سابق ص126

-الاتفاقيات الثنائية:

و هي اتفاقيات تُبرم بين دولتين فقط، بهدف تبادل الالتزام بحماية الأرشيف الخاص بكل دولة داخل إقليم الدولة الأخرى، بما يضمن توفير مستوى من الحماية المتبادلة للوثائق الأرشيفية بين الطرفين.

-الاتفاقيات الإقليمية أو الدولية:

وهي اتفاقيات تُعقد بين مجموعة من الدول، سواء كانت دولًا تنتمي إلى إقليم جغرافي واحد (اتفاقيات إقليمية)، أو دولًا من أقاليم مختلفة (اتفاقيات دولية). وتتميز هذه الاتفاقيات باتساع نطاقها، مما يتيح للدولة الواحدة ضمان حماية أرشيفها في عدد أكبر من الدول الموقعة، وبالتالي تعزيز فعالية الحماية القانونية الدولية للأرشيف

المطلب الثاني: الرقابة الإدارية على المعاملات الإدارية الالكترونية

الفرع الأول: الرقابة الداخلية وبيئة النظم الالكترونية:

شهد مفهوم الرقابة الداخلية تطورًا تدريجيًا مهمًا تماشيًا مع التحولات الاقتصادية السريعة. فلم تعد تقتصر على حماية النقدية فقط، بل أصبحت نظامًا متكاملًا من السياسات والإجراءات التي تضعها الإدارة العليا لضمان تحقيق أهداف المؤسسة بكفاءة وفعالية.

و يرجع هذا التطور إلى توسع حجم الوحدات الاقتصادية وتعقد نشاطها وتعدد أهدافها، مما جعل من الصعب الاعتماد على المراجعة التفصيلية لكل العمليات. لذلك أصبحت الرقابة الداخلية أداة أساسية يعتمد عليها مراقبو الحسابات لتقييم النظام المالي والإداري للوحدة الاقتصادية .

أولا: أدوات الرقابة الداخلية:

يتطلب أي نظام رقابي فعال توفر وسائل وأدوات تمكّنه من تقييم مدى فاعلية الأنشطة ودرجة توافقها مع الخطط الموضوعة وتحقيق الأهداف. وتتنوع هذه الوسائل بين بسيطة ومعقدة، كما تختلف من حيث نطاق استخدامها، إذ قد تُستخدم لتقييم الأداء الكلي للمؤسسة، لكنها في مجملها تهدف إلى تحقيق نفس الغاية الرقابية.

ويرى الشريف أن دور الإدارة يتمثل في اختيار الأداة الرقابية المناسبة التي تسهّل عملية الرقابة من جهة، وتُعد وسيلة فعالة للاتصال داخل المؤسسة وخارجها من جهة أخرى. كما أن أدوات الرقابة تتيح تزويد الإدارة بمؤشرات موضوعية حول اتجاهات الأداء، مثل الموازنات التخطيطية والنسب المالية التي تعكس الوضع المالي بشكل واضح وملموس.

كما ينقسم نظام الرقابة الداخلية إلى ثلاثة أنظمة فرعية تُعد أدواته الأساسية، وهي: نظام الرقابة الإدارية، ونظام الرقابة المحاسبية، ونظام الوسيتم التطرق إلى هذه النظم بشيء من التفصيل:[1]

1-النظام المتكامل للرقابة الداخلية في ظل التشغيل الإلكتروني للبيانات:

يمكن وضع إطار لنظام متكامل للرقابة الداخلية يقوم على المفهوم الواسع للرقابة الداخلية، حيث يُقسَّم إلى ثلاثة أنظمة فرعية تتمثل في: الرقابة الإدارية، والرقابة المحاسبية، والرقابة التشغيلية. ويهدف كل نظام فرعي إلى تحقيق مجموعة من الأهداف من خلال إجراءات رقابية مناسبة، بحيث تتكامل هذه الأنظمة لتحقيق الهدف العام للرقابة الداخلية، والمتمثل في منع الأخطاء والمخالفات أو اكتشافها أو تصحيحها، وتقليل آثار الخسائر الناتجة عنها.[2]

وعليه سنقوم بالتركيز في هذا المطلب على العناصر الآتية:

_ الرقابة الإدارية.

_ الرقابة التشغيلية.

_ الرقابة المحاسبية.

[1] علي أبو الفتح أحمد شتا، تطوير ادوات الرقابه الداخلية لهدف حماية البيانات المعدة إلكترونيا، دراسة مقارنة، جامعة القاهرة،سنة 2011، ص42

[2] د. بو سبعين تسعديت، محاضرات في نظام الرقابة الداخلية، مطبوعة موجهة لطلبة السنة الثالثة في العلوم المالية والمحاسبة، 2019_2020، ص 37.

أ_ الرقابة الإدارية

لتحقق الرقابة الإدارية أهدافها في ظل التشغيل الالكتروني للبيانات لا بد لها من:[1]

_الرقابة التنظيمية:

وتقوم الرقابة الإدارية على وجود خطة تنظيمية سليمة تحدد مختلف الإدارات والأقسام داخل المنشأة، مع بيان اختصاصات وواجبات ومسؤوليات كل إدارة أو قسم، إضافة إلى تحديد نطاق التفويض المناسب للسلطات الوظيفية. وفي هذا الإطار، تشمل الإجراءات التالية:[2]

-فصل قسم التشغيل الالكتروني للبيانات عن الأقسام المستفيدة من خدمات الحاسوب الآلي، حيث تكون هذه الأخيرة مسئولة عن ما يحدث من أخطاء أو مخالفات خارج قسم التشغيل مثل نسيان بيانات عملية ما.

-فصل المهام بين العاملين في قسم التشغيل الالكتروني للبيانات مثل النظم ومعدي البرامج، رقابة وصيانة نظام التشغيل، وإدخال البيانات وتشغيل الحاسوب الآلي.

-فصل المهام داخل الأقسام المستفيدة حيث يؤدي ذلك إلى تدنية احتمال وجود أخطاء أو مخالفات.

_الرقابة على إعداد وتوثيق النظام:

يسهم الإعداد الجيد والتوثيق الدقيق لنظام التشغيل الإلكتروني للبيانات في تسهيل عملية مراجعته، من خلال توفير مستندات داعمة تمثل أدلة كافية لأغراض التدقيق والرقابة. وتركز الرقابة على إعداد النظام على تصميم نظام رقابي فعال يضمن التحكم في تطبيقات الحاسوب الإلكتروني، بينما تهدف الرقابة على توثيق النظام إلى حفظ وتوثيق مختلف السجلات والتقارير وأوراق العمل، إضافة إلى وصف النظام وبرامجه وتعليمات تشغيله، بما يوضح آليات العمل ويساعد على أداء مهام معالجة البيانات بكفاءة.

[1] بوطروة فضيلة، دراسة وتقييم فعالية نظام الرقابة الداخلية في البنوك، دراسة حالة ، الصندوق الوطني للتعاون الفلاحي، مرجع سابق ص38.39.40

[2] بوطروة فضيلة، دراسة وتقييم فعالية نظام الرقابة الداخلية في البنوك، دراسة حالة ، الصندوق الوطني للتعاون الفلاحي، مرجع سابق ص38.39.40

_ الرقابة على أمن النظم:

يمكن الحد أو التخلص من أغلب المخالفات المرتبطة بأنظمة الحاسوب من خلال التخطيط الإداري السليم لأمن النظم، إلى جانب توفير الحماية اللازمة للتجهيزات والبرامج. ويهدف ذلك إلى ضمان حسن استغلال النظام وتحقيق أقصى استفادة ممكنة من إمكانياته.[1]

ب _ الرقابة التشغيلية:

تحقق الرقابة التشغيلية أهدافها في ظل بيئة نظام ألية و يجب أن تتضمن التدابير او الإجراءات الآتية:[2]

*** الرقابة من خلال الوحدات الآلية والبرامج:**

تتمثل الرقابة الألية من خلال الوحدات الآلية في مجموعة من الإجراءات التي يضعها مصممو أنظمة الحاسوب بهدف ضمان دقة تشغيلها وسلامة عملها. ومن بين هذه الإجراءات فحص الحرف الزائد، تتمثل الرقابة من خلال الوحدات الآلية في مجموعة من الإجراءات التي يضعها مصممو أنظمة الحاسوب بهدف ضمان دقة تشغيلها وسلامة عملها. ومن بين هذه الإجراءات فحص الحرف الزائد، وهو عبارة عن وحدة تخزين إضافية تُلحق بحرف أو كلمة أو مجموعة من البيانات، بهدف الكشف عن الأخطاء الإلكترونية والأخطاء التي قد تحدث أثناء عمليات تحويل البيانات.

أما الرقابة من خلال البرامج، فتعني اعتماد مجموعة من البرمجيات التي تقوم بتنفيذ وظائف رقابية مهمة على مستوى النظام ككل، بما يساهم في تحسين دقة المعالجة وضمان سلامة العمليات داخل النظام المعلوماتي عبارة عن وحدة تخزين إضافية تُلحق بحرف أو كلمة أو مجموعة من البيانات، بهدف الكشف عن الأخطاء الإلكترونية والأخطاء التي قد تحدث أثناء عمليات تحويل البيانات.

[1] بو سبعين تسعديت، المرجع السابق، ص 38

[2] بوطروة فضيلة، دراسة وتقييم فعالية نظام الرقابة الداخلية في البنوك، دراسة حالة ، الصندوق الوطني للتعاون الفلاحي، مرجع سابق ص38.39.40

أما الرقابة من خلال البرامج، فتعني اعتماد مجموعة من البرمجيات التي تقوم بتنفيذ وظائف رقابية مهمة على مستوى النظام ككل، بما يساهم في تحسين دقة المعالجة وضمان سلامة العمليات داخل النظام المعلوماتي.

*** الرقابة على أمن النظام:**

إن ضعف الرقابة على أمن النظام قد يؤدي إلى تنفيذ عمليات غير مصرح بها، وعدم دقة التقارير وسجلات البيانات، إضافة إلى فقدان الأصول والبيانات المهمة، وانتهاك سرية المعلومات. ويُقصد بأمن النظام حماية مكونات الحاسوب الإلكتروني، بما في ذلك التجهيزات وملفات البيانات والبرامج، من مختلف المخاطر البيئية والمخالفات المتعلقة باستخدام الحاسوب.

وانطلاقًا من هذا التعريف، يتضمن أمن النظام مجموعة من الإجراءات الأساسية، أهمها:

-الرقابة على أمن التجهيزات.

-الرقابة على أمن البرامج والبيانات.

ت_ الرقابة المحاسبية:

لضمان الرقابة المحاسبية أهدافها في ظل نظم التشغيل الالكتروني للبيانات ينبغي أن تتضمن الإجراءات التالية:

***إجراءات الرقابة على إعداد البيانات:**

تقوم الرقابة المحاسبية على إعداد البيانات حيث تهدف إلى ضمان دقة المعلومات قبل إدخالها إلى نظام الحاسوب الإلكتروني، وذلك من خلال الوقاية من الأخطاء والمخالفات أو اكتشافها والعمل على تصحيحها والحد من آثارها. وفي هذا الإطار، تتضمن هذه الرقابة مجموعة من الإجراءات ، من بينها نذكر ما يلي:

-إجراء الفحص اليدوي للبيانات وذلك قبل تحويلها لقسم التشغيل الإلكتروني.

-تصميم سند جيد للمراجعة يمكن من تتبع الأخطاء والمخالفات في المستندات الأصلية وتصحيحها ويتكون سند المراجعة من نسخة يدوية.

***إجراءات اختبار الرقابة على المدخلات:**

توجد طريقتان لإدخال البيانات هما طريقة الإدخال الجماعي وطريقة الإدخال الفوري للبيانات، فالطريقة الأولى يتم جمع البيانات من المستندات الأصلية وتصحيحها، ثم يتم إدخالها للحاسوب الإلكتروني في مجموعات، أما في ظل طريقة الإدخال الفوري فيتم إدخال البيانات بمجرد الانتهاء منها.[1]

وعموما تلعب إجراءات الرقابة على إعداد البيانات دورا هاما في منع أخطاء ومخالفات الحاسبات، أو اكتشافها أو الرقابة على تصحيحها وتدنية خسائرها ومن أهم هذه الإجراءات:

-فحص بيانات المدخلات وذلك قبل إدخالها للحاسوب الالكتروني للتحقق من دقتها وعدم تحريفها.

-لتحقق من صيانة المستندات الأصلية في صورة يمكن للحاسوب الالكتروني قراءتها وذلك على أسطوانات وأشرطة ممغنطة وغيرها من وسائط التخزين.

2-مكونات نظام الرقابة الداخلية:

توجد طريقتان لإدخال البيانات، هما: الإدخال الجماعي والإدخال الفوري. ففي الطريقة الأولى يتم جمع البيانات من المستندات الأصلية، التحقق من صحتها وتصحيحها، ثم إدخالها إلى الحاسوب الإلكتروني على شكل دفعات أو مجموعات. أما في طريقة الإدخال الفوري، فتُدخل البيانات مباشرة بمجرد إعدادها أو توفرها من اهم هذه الإجراءات:

_إدراك الطالب لمختلف مكونات نظام الرقابة الداخلية.

_ تمكن الطالب من تحليل مختلف العلاقات التي تربط بين مكونات نظام الرقابة الداخلية.

[1] بو سبعين تسعديت، مرجع سابق، ص 39.

ثانيا: مكونات نظام الرقابة الداخلية وفقا _COSOوهي كالآتي:

_بيئة الرقابة:

تُعدّ بيئة الرقابة أحد المؤشرات الأساسية على فاعلية نظام الرقابة الداخلية داخل المؤسسة، إذ إن وجود أقسام للتدقيق الداخلي، إلى جانب أنظمة حاسوبية متطورة، يعكس مستوى جيدًا من الرقابة. كما يزداد هذا الفاعل عندما تُولي الإدارة اهتمامًا كافيًا بتقارير هذه الأقسام المتعلقة بالتجاوزات أو حالات الاختلاس، وتعمل على اتخاذ الإجراءات التصحيحية المناسبة لمعالجة أوجه القصور ولقد اعطت لجنة cosoاهمية بالغه لبيئة نظم الرقابة الداخلية والتي تشمل على عناصر أساسية كالأتي:

_النزاهة والقيم الأخلاقية واتجاهات الإدارة:

وتعتبر هذه العناصر من المكونات الأساسية لبيئة الرقابة الداخلية، حيث تؤثر بشكل مباشر في سلوك العاملين داخل المؤسسة. إذ إن تعزيز قيم النزاهة والالتزام الأخلاقي يسهم في الحد من المخالفات والملاحظات داخل بيئة العمل. ومن هذا المنطلق، تقع على عاتق الإدارة مسؤولية ترسيخ منظومة من القيم الأخلاقية التي تحفّز العاملين على الالتزام بسياساتها، وتمنع السلوكيات غير القانونية أو غير الأخلاقية التي قد تؤثر سلبًا على معاملات المؤسسة. كما تعمل هذه القيم على ترسيخ ممارسات عمل منظمة ونمطية تتسم بالقبول والالتزام المهني.[1]

_الالتزام بالكفاءة:

يتحقق ذلك من خلال وجود مستويات للأداء داخل المؤسسة مع ضمان الالتزام بها، وهذا يتطلب رسم سياسات واستراتيجيات، وعقد دورات تدريبية لتهيئة موارد بشرية ذات كفاءة عالية، وتزويدها بالمهارات والمعرفة اللازمة لإنجاز الأعمال التي تحددها مهمات الوظيفة.

أ_دور ومشاركة مجلس الإدارة أو لجنة المراجعة:

[1] بو سعيدي تسعديت، مرجع سابق، ص 32.

وهذه اللجنة تتكون من المديرين أو أعضاء مجلس الإدارة غير التنفيذيين ومن مهام هذه اللجنة:

_ متابعة أنشطة الإدارة وفحصها.

_ تفويض الإدارة بمسؤولية الرقابة الداخلية.

_ تقليل احتمال أن تقوم الإدارة بتجاهل الضوابط الموجودة.

ب_فلسفة الإدارة ونمط التشغيل:

إذ أن فلسفة الإدارة ونمطها التشغيلي تمثل مؤشرا على مدى الاهتمام بإيجاد بيئة رقابية فعالة، ويمكن ملاحظة ذلك من خلال نظرتها إلى ضرورة الدقة والعدالة في القوائم المالية، وكذلك اعتمادها على تطبيق الإجراءات والتعليمات الصادرة من الجهات الرقابية.

ت_الهيكل التنظيمي:

إن الهيكل التنظيمي يوفر للجهة الرقابية الإطار الذي يتم من خلاله تخطيط وتنفيذ ومراقبة ومراجعة أنشطتها لتحقيق الأهداف المرجوة، ولتحقيق هذه الأهداف يجب اعتماد هيكل تنظيمي واضح ومفهوم ومرن وشامل، بشكل يغطي كافة احتياجات المنظمة وقادر على مواكبة التطورات المستقبلية، ويتضمن الخطوط الرئيسية للصلاحيات والمسؤوليات والواجبات.

ث_تحديد وتوزيع الصلاحيات والمسؤوليات:

وذلك بتحديد الصلاحيات والمسؤوليات للأنشطة، والكيفية التي يتم بموجبها لجميع البيانات المناسبة لكل مستوى من أجل إعداد التقارير الدقيقة والواضحة.

ج_سياسات الموارد البشرية وممارستها:

وهذه السياسات والممارسات تتعلق بالأفراد الذين يشكلون أهم نواحي الرقابة الداخلية، ومن أمثلتها: التعيين والتوجيه وتقديم المشورة والترقية والتعويض والإجراءات التصحيحية.[1]

[1] دكتورة بوسبعين تسعديت، محاضرات في نظام الرقابة الداخلية مرجع سابق ص33

ح_ تقييم المخاطر:

وهي عملية يتم بموجبها تحديد مخاطر العمل وكيفية استجابة الإدارة لهذه المخاطر، وخاصة ما يتعلق منها بإعداد القوائم المالية والأحداث والظروف الخارجية والداخلية، والتي قد تؤثر بشكل سلبي في قدرة المؤسسة على إعداد التقارير حول المعلومات المالية، وبما يتوافق مع إقرارات الإدارة في البيانات المالية إذ يجب على إدارة الجهة الخاضعة للرقابة.

الفرع الثالث: الهيئات الرقابية والتنضيمية: سنتناول في هذا الفرع دور السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي وكذ ا الهيئة الوطنية للوقاية من الفساد ثم نتطرق إلى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال[1]. كالتالي:

أولا: السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي:

نصت المادة 22 من القانون 07-18المتعلق بحماية الأشخاص ذات الطابع الشخصي تلى ما يلي[2]:

تنشأ لدى رئيس الجمهورية سلطة إدارية مستقلة لحماية المعطيات ذات الطابع الشخصي، يشار إليها أدناه" السلطة الوطنية" يحدد مقرها بالجزائر العاصمة.

تتمتع السلطة الوطنية بالشخصية المعنوية والاستقلال المالي والإداري تقييد ميزانية السلطة الوطنية في ميزانية الدولة وتخضع للمراقبة المالية طبقا للتشريع المعمول به.

- تعد السلطة الوطنية نظامها الداخلي الذي يحدد لاسيما كيفيات تنظيمها وسيرها، ونصادق عليه.
- المادة 23: من القانون السالف الذكر 07-18 المتعلق بحماية الاشخاص الطبيعيين ذات الطابع الشخصي[3]:

تتشكل السلطة الوطنية من :

[1] رضوان علي، رزق الله العربي،بن مهيدي، المكافحة المؤسساتية للجريمة الإلكترونية في التشريع الجزائري، المجلة الأكاديمية للبحوث القانونيه والسياسية، المجلد09،العدد02 سنه 2025 ص1388

[2] مادة 22من القانون18-07 المتعلق بحماية الاشخاص الطبيعين ذات الطابع الشخصي مرجع سابق.

[3] المادة 23من القانون 07-18 المتعلق بحماية الاشخاص الطبيعين ذات الطابع الشخصي مرجع سالف الذكر.

- ثلاث (03) شخصيات: من بينهم الرئيس يختاره رئيس الجمهورية من بين ذوي الاختصاص في مجال عمل السلطة الوطنية.
- ثلاثة (03) قضاة: يقترحهم المجلس الأعلى للقضاة من بين قضاة المحكمة العليا ومجلس الدولة.
- عضو عن كل غرفة من البرلمان: يتم اختياره من قبل رئيس كل غرفة، بعد التشاور مع رؤساء المجموعات البرلمانية.
- ممثل(01) عن المجلس الوطني لحقوق الإنسان.
- ممثل(01)عن وزير الدفاع الوطني.
- ممثل(01)عن وزير الشؤون الخارجية.
- ممثل(01)عن الوزير المكلف بالداخلية.
- ممثل(01)عن وزير العدل، حافظ الأختام.
- ممثل(01)عن الوزير المكلف بالبريد والمواصلات السلكية واللاسلكية والتكنولوجيات الرقمية.
- ممثل(01)عن الوزير المكلف بالصحة.2
- ممثل(01)عن وزير العمل والتشغيل والضمان الاجتماعي.

- يتم اختيار السلطة الوطنية حسب اختصاصهم القانوني أو التقني في مجال معالجة المعطيات ذات الطابع الشخصي.
- يمكن السلطة الوطنية أن تستعين بأي شخص مؤهل من شأنه مساعدتها في أشغالها.
- يعين رئيس وأعضاء السلطة الوطنية بموجب مرسوم رئاسي لعهدة مدتها خمس سنوات قابلة للتجديد.[1]

نصت المادة24 من القانون-18 07: يؤدي أعضاء السلطة الوطنية قبل التنصيب في وظائفهم اليمين أمام مجلس قضاء الجزائر، في الصيغة الآتية:

"أقسم بالله العظيم أن أؤدي مهمتي كعضو في السلطة لحماية المعطيات ذات الطابع الشخصي بكل استقلالية وحياد وشرف ونزاهة، وأن أحافظ على سرية المداولات".[1]

[1] المادة 24، من القانون 18/07 ، السالف الذكر.

كما تناولت المادة26 من القانون 07- 18المتعلق بحماية الاشخاص الطبيعيين ذات الطابع الشخصي:

يجب على رئيس وأعضاء السلطة الوطنية المحافظة على الطابع السري للمعطيات ذات الطابع الشخصي والمعلومات التي اطلعوا عليها بهذه الصفة ولو بعد انتهاء مهامهم، ما لم يوجد نص قانوني يقضي بخلاف ذلك.

- لا يجوز لرئيس السلطة الوطنية وأعضائها أن يمتلكوا بصفة مباشرة أو غير مباشرة مصالح في أي مؤسسة تمارس نشاطاتها في مجال معالجة المعطيات ذات الطابع الشخصي.
- يستفيد رئيس وأعضاء السلطة الوطنية من حماية الدولة ضد التهديدات أو الإهانات أو الاعتداءات من أي طبيعة كانت التي قد يتعرضون لها بسبب أو خلال تأديتهم مهامهم أو بمناسبتها.
- يحدد النظام التعويضي لأعضاء السلطة الوطنية وشروط وكيفيات منحه عن طريق التنظيم.[2]

و يرى الباحث من خلال دراسات أن هناك سلطات إدارية تقوم بممارسة الرقابة الإدارية لممارسة المعطيات ذات الطابع الشخص و أهمها :

ثانيا : الهيئة الوطنية للوقاية من الفساد ومكافحته[3]

في إطار تعزيز الجهود الوطنية للوقاية من الفساد ومكافحته، أنشأ المشرّع الجزائري هيئة متخصصة ذات أهمية بالغة، تتمثل في الهيئة الوطنية للوقاية من الفساد ومكافحته، وذلك بموجب القانون رقم 06-01 المتعلق بالوقاية من الفساد ومكافحته المعدّل والمتمم. وقد أسندت لهذه الهيئة مهمة محورية تتمثل في التصدي لظاهرة الفساد بمختلف أشكاله، ولا

[2] المادة 26، من القانون 18/07 ، السالف الذكر.

[3] حاجة عبد العالي، الآليات القانونية لمكافحة الفساد في الجزائر ، أطروحة لنيل شهادة الدكتوراه علوم في الحقوق تخصص قانون عام، سنة 2013/2012، ص 484-485.

سيما الفساد الإداري، حيث نصّت المادة 17 من هذا القانون على إنشاء هيئة وطنية تُكلّف بالوقاية من الفساد ومكافحته، بهدف تنفيذ الاستراتيجية الوطنية في مجال مكافحة الفساد.[1]

1-النظام القانوني للهيئة الوطنية للوقاية من الفساد ومكافحته

تشير بداية إلى أن المشرّع الجزائري خصّص الباب الثالث من القانون رقم 06-01 المعدّل والمتمم للهيئة الوطنية للوقاية من الفساد ومكافحته، كما عزّز ذلك بالمرسوم الرئاسي رقم 06-413 المعدّل والمتمم الذي يحدّد تشكيلة هذه الهيئة وتنظيمها.

ويستوجب دراسة النظام القانوني لهذه الهيئة التطرّق إلى طبيعتها القانونية من جهة، وتحديد تشكيلتها وكيفية تنظيمها من جهة أخرى، باعتبارها جهازًا محوريًا في منظومة الوقاية من الفساد ومكافحته

أ_ تحديد طبيعة الهيئة الوطنية للوقاية من الفساد ومكافحته:

على غرار التشريعات المقارنة، أنشأ المشرّع الجزائري هيئة متخصصة في مكافحة الفساد تتمثل في الهيئة الوطنية للوقاية من الفساد ومكافحته، وذلك بموجب القانون رقم 06-01 المعدّل والمتمم. وقد نصّت الفقرة الأولى من المادة 18 من هذا القانون على الطبيعة القانونية للهيئة، حيث اعتبرتها:

سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي، وتوضع لدى رئيس الجمهورية.[2]

ويُستفاد من هذا النص أن الهيئة الوطنية للوقاية من الفساد ومكافحته تتمتع بجملة من الخصائص التي تُجسّد طبيعتها القانونية المتميزة، ويمكن إبراز هذه الخصائص فيما يليكم يلي:

_الهيئة سلطة إدارية مستقلة

يُستفاد من المادة 18 الفقرة الأولى من القانون رقم 06-01 المتعلق بالوقاية من الفساد ومكافحته، وكذا المادة 02 من المرسوم الرئاسي رقم 06-413 المعدل والمتمم، أن الهيئة الوطنية للوقاية من الفساد ومكافحته تُعد سلطة إدارية مستقلة. وتجدر الإشارة إلى أن

[1] تهميش 1 المادة 17 من القانون رقم 01-06. المتعلق بالوقاية من الفساد ومكافحته، الجريدة الرسمية العدد 18 الصادر بتاريخ 08مارس 2006.

[2] المادة 18 الفقرة الأولى من القانون 01-06 التعلق بالوقاية من الفساد ومكافحته المؤرخ 20فبراير 2006 الجريدة الرسمية العدد 14 الصادر بتاريخ 08مارس 2006المعدل والمتمم..

السلطات الإدارية المستقلة تُعتبر من الأساليب الحديثة لممارسة السلطة العامة، إذ تتمتع بقدر من الاستقلالية في اتخاذ القرار وبسلطات فعلية، وقد أنشئت أساساً لضبط النشاط الاقتصادي والمالي بما يحقق التوازن وحسن سير المرافق، حيث تجمع بين وظيفتي التسيير والرقابة. [1]

إن تكييف المشرع للهيئة بأنها سلطة إدارية مستقلة يعني أنها تتميز بالطابع الإداري والسلطوي وهي تنظيم جديد وغير مصنف ضمن الهرم الإداري التقليدي والذي يقوم على تقسيم الإدارة العامة إلى إدارة مركزية وأخرى لا مركزية، كما أنها ليست بمؤسسة عمومية أو هيئة قضائية، فهي هيئة إدارية خاصة مستقلة عن الحكومة ولا تخضع لرقابتها كما أنها تتمتع بسلطة تمكنها من ممارسة امتيازات السلطة العامة هذا من ناحية ومن ناحية أخرى فإنها هيئة مستقلة وهي بالتالي لا تخضع لأي رقابة رئاسية أو وصائية من طرق السلطة التنفيذية ولكن لا يعنى هذا عدم وجود أية علاقة أو تأثير لهذه الأخيرة على عمل ومهام الهيئة وخاصة الرقابية منها.

_تمتع الهيئة بالشخصية المعنوية والاستقلال المالي

أعطى المشرع الجزائري للهيئة الوطنية للوقاية من الفساد ومكافحته، بموجب المادة 18 الفقرة الأولى من القانون رقم 06-01، الشخصية المعنوية قصد تمكينها من أداء مهامها على أكمل وجه. ويُلاحظ في هذا السياق أنه، ورغم أن الاستقلال المالي يُعد من الآثار القانونية المترتبة عن تمتع الشخص المعنوي بالشخصية القانونية، إلى جانب أهلية التقاضي وبقية الحقوق والالتزامات، فإن المشرع قد نص صراحة على الاستقلال المالي إلى جانب تقرير الشخصية المعنوية.

_تبعية الهيئة الرئيس الجمهورية

تُعتبر هذه الخاصية ثالث سمة مميزة للهيئة، والتي يمكن استخلاصها أيضاً من المادة 18 الفقرة الأولى من القانون رقم 06-01 المتعلق بالوقاية من الفساد ومكافحته. غير أنه يلاحظ أن موقع الهيئة لدى رئيس الجمهورية يثير إشكالاً على مستوى التكييف القانوني المتعلق باستقلاليتها، ذلك أن إلحاقها برئاسة الجمهورية قد يُفهم منه أنها لا تتمتع بالاستقلالية الكاملة، باعتبارها ترتبط عضوياً بالسلطة التنفيذية

[1] تهميش المادة 18الفقرة 01من القانون 01-06المتعلق بالوقاية من الفساد ومكافحته السالف الذكر.

ثالثا: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال [1]

تناول القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، في فصله الخامس، على إنشاء هيئة وطنية مكلفة بالوقاية من الجرائم المعلوماتية أو ما يُعرف بالجرائم الإلكترونية. غير أن هذا القانون لم يتضمن أحكاماً تفصيلية تتعلق بتشكيلة هذه الهيئة أو تنظيمها أو آليات سيرها ونطاق عملها، حيث أحال في المادة 13 منه إلى التنظيم، بنصها على أنه: «تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها... وتحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم».2

وفي هذا الإطار، تم وضع الهيئة تحت سلطة وزارة الدفاع الوطني، حيث اتخذ مقرها بالجزائر العاصمة مع إمكانية نقله إلى أي مكان آخر بموجب قرار صادر عن السلطة المختصة. كما تم تكييفها بوصفها سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي.

وقد جاء المرسوم الرئاسي رقم 19-172 ليعدل ويكمل هيكلها التنظيمي، حيث أصبحت تضم مجلس توجيه يُعنى بتحديد التوجهات العامة، ومديرية عامة تتولى التسيير التنفيذي، وهو ما يعكس تطوراً في بنيتها الإدارية وتدعيم آليات عملها بما ينسجم مع طبيعة المهام المسندة إليها في مجال الوقاية من الجرائم المعلوماتية ومكافحتها.[2]

1-مجلس التوجيه:

بعد أن تم وضع الهيئة تحت وصاية وزارة الدفاع الوطني بدلًا من إشراف وزارة العدل وفقًا للمرسوم الرئاسي 15-261 الملغى، أصبحت تُدار من خلال مجلس التوجيه الذي عوّض اللجنة المديرية السابقة.

[1] د مجذوب نوال، د طالب محمد كريم، الجريمة المعلوماتية و أثرها على التنمية الاقتصادية، الطبعة 01، ص 2020.

2 المادة 13من القانون رقم -04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا اعلام واتصال ، المؤرخ في 05اوت 2009،الجريدة الرسمية العدد 47الصادر بتاريخ 16أوت 2009.

[2] المادة 09 من المرسوم الرئاسي 19-172 السالف الذكر

ويرأس هذا المجلس وزير الدفاع الوطني القائد الأعلى للقوات المسلحة (رئيس الجمهورية من الناحية الدستورية)، بينما يتولى عمليًا نائب وزير الدفاع رئاسة أشغاله، وذلك وفقًا لما نصّت عليه المادة 5 من المرسوم الرئاسي 19-172.

ويتشكل المجلس كذلك من ممثلين عن وزارات الدفاع الوطني والداخلية والعدل والمواصلات السلكية واللاسلكية، في حين أُنيطت مهمة الأمانة العامة للمجلس بالمديرية العامة المختصة. ،[1]

2-المديرية العامة

بموجب المادة 9 من المرسوم الرئاسي 19_172 السالف الذكر فإنه تنشأ مديرية عامة يترأسها مدير عام يعين طبقا للتنظيم المعمول به في وزارة الدفاع الوطني وهو ما نصت عليه، المادة 19 من ذات المرسوم ويتضح لنا الطابع الأمني للهيئة من خلال التشكيلة التي يغلب عليها عامل الانتساب للمؤسسة العسكرية [2]

كما أن المديرية من الناحية التنظيمية تضم بموجب المادة 10 من ذات المرسوم مديريتان هما المديرية التقنية ومديرية للإدارة والوسائل.[3]

3-كيفيات سير الهيئة ومهامها:

لقد طال مهام الهيئة بعض التغيرات وذلك على مستوى مجلس التوجيه أو المديرية العامة وعليه نورد مهام الهيئة فيما يلي:

رغم أن القانون المتضمن القواعد الخاصة المتصلة بجرائم الإعلام ومكافحتها قد نص في المادة 14 منه على مهام الهيئة بصفة واضحة، إلا أنه في المرسوم الرئاسي السالف الذكر فصل في هذه المهام ووزعها على مجلس التوجيه والمديرية العامة:

4_مهام مجلس التوجيه:

[1] المادة 5 من المرسوم الرئاسي رقم 19-172 المؤرخ في 11 يونيو 2019، المتعلق بتحديد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 38، الصادر بتاريخ 12 يونيو، 2019

[2] ا لمادة 19من المرسوم الرئاسي 19-172 السالف الذكر

[3] المادة 10من المرسوم الرئاسي 172-19 السالف الذكر

يتولى مجلس التوجيه أساسًا دراسة الاستراتيجية الوطنية للوقاية من الجرائم المعلوماتية وتكنولوجيات الإعلام والاتصال ومكافحتها، كما يناقش سبل تعزيز التعاون بين مختلف المؤسسات والهيئات الوطنية المعنية بهذا المجال. ويقوم كذلك بتقييم دوري لمستوى التهديدات المرتبطة بالجرائم الإلكترونية والأهداف المسطرة لمواجهتها، مع اقتراح كل الإجراءات والأنشطة المتعلقة بالبحث والتطوير وتقييم التدابير العملية لمكافحة هذه الجرائم. إضافة إلى ذلك، يقدم المجلس اقتراحات تدخل ضمن مجال اختصاص الهيئة، ويساهم في ضبط الإطار والمعايير القانونية ذات الصلة، كما يدرس ميزانية الهيئة ويصادق عليها.

ومن حيث التنظيم والتسيير، يعقد المجلس اجتماعاته في دورتين عاديتين بناءً على استدعاء من رئيسه، ويمكن أن يجتمع في دورات غير عادية عند الاقتضاء، إما بدعوة من الرئيس أو بطلب من أحد أعضائه أو من المدير العام للهيئة كلما دعت الحاجة العملية لذلك، وذلك وفق ما نصت عليه المادة 6 من المرسوم المذكور. كما حددت المادة 8 قواعد وكيفيات سير مجلس التوجيه بموجب قرار صادر عن وزير الدفاع الوطني.

5-مهام المديرية العامة:

تتولى المديرية العامة للهيئة الإشراف على السير الحسن لمختلف أنشطتها، من خلال تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، إضافة إلى تبادل المعلومات مع الهيئات الأجنبية النظيرة في إطار التعاون الأمني، بما يسمح بتجميع المعطيات المتعلقة بمرتكبي هذه الجرائم والتعرف عليهم وتحديد أماكن تواجدهم.

كما تضطلع المديرية بمهام إدارية وتنظيمية تتمثل في إعداد مشروع ميزانية الهيئة، ووضع وتنفيذ برامج عملها، إلى جانب التنسيق والمتابعة والرقابة على نشاط هياكلها الداخلية. وتتكفل كذلك بالتحضير لاجتماعات مجلس التوجيه، باعتبارها تمارس مهام الأمانة العامة له وفق ما نصت عليه المادة 5 الفقرة الأخيرة من المرسوم المذكور.[1]

[1] المادة، 05الفقرك الأخيرة من المرسوم الرئاسي 19-172 السالف الذكر

وتتولى أيضاً إعداد التقرير السنوي لنشاطات الهيئة، بالإضافة إلى مسك محاسبتها وفق قواعد المحاسبة العمومية، وهو ما أكدته المادة 17 من المرسوم ذاته. [1]

المبحث الثاني : الحماية الجزائية لتأمين المعاملات الإدارية الإلكترونية

إن التطور الإلكتروني التقني لأساليب ارتكاب الجرائم الإلكترونية وخصوصا عبر الإنترنت أو أجهزة الحاسوب ووسائل التواصل الاجتماعي مما أدى إلى العديد من المخاطر سواء على مستوى النظام الإلكتروني أو نظم الشبكات مما يتطلب على المشرع إصدار قوانين وإجراءات جزائية لردع مختلف أنواع الجرائم الإلكترونية وكذا معاقبه الأشخاص الذين يسيئون استعمال تكنولوجيا المعلومات لأغراض إجرامية، وسنتناول في هذا المبحث مفهوم الجريمة الإلكترونية وأنواعها والعقوبات المقررة لها.

المطلب الأول: مفهوم الجريمة الإلكترونية

اختلف الفقه لي وضع تعريف مانع جامع للجريمة الإلكترونية فأحيانا يكون الحاسوب وسيلة لارتكابها بواسطة الانترنت وأحيانا يكون هدف لها، لذالك سنتناول في هذا المطلب تعريف الجرائم الإلكترونية وكذا خصائصها ثم نتطرق إلى أنواعها.

الفرع الأول تعريف الجريمة الإلكترونية

تُعد الجرائم الإلكترونية من الظواهر الحديثة المرتبطة بتطور تكنولوجيا المعلومات والاتصال، الأمر الذي جعل من الصعب وضع تعريف جامع ودقيق لها. وقد دفع هذا التداخل الفقهي والتقني العديد من الباحثين إلى محاولة ضبط مفهومها، حيث برز في هذا الإطار اتجاهان رئيسيان: اتجاه ضيق يقتصر في تعريفه على الأفعال غير المشروعة التي تستهدف النظم المعلوماتية بشكل مباشر، واتجاه موسّع يشمل كل السلوكيات الإجرامية التي تُرتكب باستخدام أو عبر وسائل تكنولوجيا المعلومات والاتصال، لنخلص في الأخير إلى بيان موقف المشرع الجزائري من هذه الإشكالية.

وفي هذا السياق، يُلاحظ عدم وجود اتفاق سواء على المستوى الفقهي أو التشريعي حول مصطلح موحد للدلالة على هذه الظاهرة الإجرامية الناشئة في بيئة الحاسوب والإنترنت. وقد رافق هذا التعدد في التسميات مسار نشأة وتطور الإجرام المرتبط بالتكنولوجيا، حيث

[1] 2 المادة 17من المرسوم الرئاسي 172–19 المرجع نفسه

استُخدمت عدة مصطلحات مثل: جرائم الغش المعلوماتي، الجرائم المعلوماتية، الجرائم الإلكترونية، جرائم الحاسب الآلي، جرائم تقنية المعلومات، الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، جرائم التكنولوجيا الحديثة، وجرائم الحاسوب والإنترنت. ويعود هذا التباين إلى عدة عوامل، أهمها التطور السريع والمتواصل لتكنولوجيا المعلومات والاتصالات واتساع مجالات استخدامها وتعدد صورها[1]

أولا الاتجاه الضيق لمفهوم الجرائم الإلكترونية:

يقوم الاتجاه الضيق على حصر الجريمة الإلكترونية في الأفعال غير المشروعة المرتبطة مباشرة بالحاسوب، سواء باعتباره أداة لارتكاب الجريمة أو هدفًا لها. وقد عرّفها بعض الفقه على أنها الجرائم التي تتم بواسطة الحاسوب أو تقع عليه أو داخل أنظمته، أو تلك التي تمس بالمعطيات والبرامج المعلوماتية.

ويربط أنصار هذا الاتجاه مفهوم الجريمة الإلكترونية بضرورة توفر معرفة تقنية لدى الجاني، مع التركيز على الجرائم التي تستهدف النظم المعلوماتية بصفة مباشرة.

غير أن هذا الاتجاه يُنتقد لكونه يضيّق من نطاق الجرائم الإلكترونية، إذ يستبعد العديد من الأفعال التي تُرتكب باستخدام وسائل تكنولوجيا المعلومات دون الحاجة إلى خبرة تقنية عالية، مثل الاحتيال عبر الإنترنت، مما يجعله تعريفًا غير شامل.

ثانيا الاتجاه الموسع لمفهوم الجرائم الإلكترونية:

اتجاه الموسع لمفهوم الجرائم الإلكترونية على عكس الاتجاه السابق، يذهب فريق من الفقهاء إلى التوسع في مفهوم الجرائم الإلكترونية أو المعلوماتية وعدم حصرها في الحاسوب وحده أو في موضوع الجريمة أو في شخص مستخدمه، وإنما بالتقنية ذاتها المستخدمة في كافة الأجهزة المعلوماتية أو الإلكترونية، فيعرفونها على أنها " كل فعل إجرامي أو متعمد أيا كانت صلته بالمعلوماتية، ينشأ عنه خسارة بالمجني عليه، أو كسبا يحققه الفاعل. كما عرفتها منظمة التعاون الاقتصادي والتنمية(OCDE)بأنها كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية والمعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل

[1] يزيد بوحليط مرجع سابق ص32

التقنية المعلوماتية، كما تعرف أيضا على أنها تلك الجرائم المرتكبة ضد الأملاك باستعمال التقنية المعلوماتية.[1]

إن هذه التعريفات واسعة تتيح الإحاطة الشاملة قدر الإمكان بظاهرة جرائم التقنية، كما أنها تعبر عن الطابع التقني أو المميز الذي تنطوي تحته أبرز صورها، كما أنه يتيح إمكانية التعامل مع التطورات التقنية المستقبلية، ويعرفها آخرون على أنها كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها ، إذ يعتمد هذا التعريف على معيارين : أولهما وصف السلوك، وثانيهما اتصال السلوك بالمعالجة الآلية للبيانات أو نقلها، كما يجمع الفقه الفرنسي بصفة عامة على القول بأن فكرة الغش المعلوماتي **(Fraude Informatique)**التي تعادل جرائم الحاسب الآلي تشمل العديد من الأفعال المتنوعة، حيث عرف كل من الفقيه مشال**(Michel)**والفقيه ريدو **(Redo)**الجريمة المعلوماتية بأنها سوء استخدام الحاسب ويشمل الحالات المتعلقة بالولوج غير المصرح به لحاسب المجني عليه أو بياناته، وكذا الاستخدام غير المشروع البطاقات الائتمان وانتهاك ماكينات الحاسب الآلية بما تتضمنه من شبكات تحويل الحسابات المالية بطرق إلكترونية وتزييف المكونات المادية والمعنوية للحاسب وسرقة الحاسب الآلي في حد ذاته أو أي مكون من مكوناته ، كما عرفت المادة من القانون العربي النموذجي الموحد بشأن مكافحة سوء استخدام تكنولوجيا المعلومات والاتصال لسنة 2003 الجرائم الإلكترونية على أنها " كل فعل مؤثم يتم ارتكابه عبر أي وسيط إلكتروني، وعرفت المادة نفسها الوسيط الإلكتروني على أنه:" شبكة الحاسب الآلي أو الانترنيت أو أي شبكة إلكترونية أخرى ، أو هي مجموعة المخالفات التي تقع على شبكات الاتصال عموما وعلى شبكة الإنترنت خصوصا.[2]

وبذلك تمثل هذه التعاريف المفهوم الموسع للجرائم الإلكترونية، والتي تتم بالحاسوب سواء كان هدفا لها أو وسيلة لارتكابها، أو عن طريق شبكة الإنترنت أو بأي وسيلة إلكترونية أخرى تظهر مستقبلا كوسائل الاتصال الحديثة مثل الهاتف النقال وجهاز الفاكس وغيرها[3].

[1] يزيد بوحليط مرجع سابق، ص33.

[2] المرجع نفسه، ص34.

[3] المرجع نفسه ، ص35.

مما لا شك فيه أن هذا الاتجاه ينطوي على توسع كبير لمفهوم الجرائم الالكترونية، فهي كل جريمة تتم بمساعدة الحاسوب أو في محيطه، أو عن طريق شبكة الإنترنت أو أجهزة الاتصال الحديثة. وبناء على التعريفات السابقة تتخذ الجريمة الإلكترونية صور عديدة، تتمثل في استخدام الحاسوب كوسيلة لارتكاب الجرائم أو الاعتداء على الحاسوب نفسه ونظامه أو استخدام أي وسيلة إلكترونية أخرى توفرها التقنيات الحديثة، بمعنى آخر فإن الجرائم الإلكترونية تزاوج بين تقنية الحوسبة وتقنية الاتصالات الحديثة، فإذا عدنا للحقيقة الأولى المتصلة بولادة وتطور تقنية المعلومات نجد أن تقنية المعلومات تشمل فرعين جرى بحكم التطور تقاربهما واندماجهما، فرع الحوسبة وفرع الاتصال أما الحوسبة فتقوم على استخدام وسائل التقنية لإدارة وتنظيم ومعالجة البيانات في إطار تنفيذ مهام محددة تتصل بعلمي الحساب والمنطق، أما الاتصال فهو قائم على وسائل تقنية لنقل المعلومات بجميع دلالاتها، هذه الدلالات يحددها الأستاذ زياينغ إكزيوو **(Zhange Yuexiao)** بالرسائل.

يُستخلص من اختلاف الفقه حول تعريف الجريمة الإلكترونية أن مردّه يعود إلى تباين المعايير المعتمدة وزاوية النظر إلى هذه الظاهرة المستحدثة. وبناءً على ذلك، يمكن تقديم تعريف جامع لها بأنها: سلوك غير مشروع ومعاقب عليه قانونًا، يصدر عن إرادة جرمية، ويكون محله معطيات الحاسوب بمفهومها الواسع، سواء تعلق الأمر بالبيانات المدخلة أو المعالجة أو المخزنة أو المتبادلة، أو بالبرامج والمعلومات المستخرجة.

ويشمل هذا السلوك الفعل الإيجابي والامتناع، ولا تكتسب الصفة الإجرامية إلا بنص قانوني صريح، باعتبار أن التجريم من اختصاص المشرّع. كما يُقصد بالحاسوب في هذا الإطار النظام التقني الشامل الذي يجمع بين تقنيات الحوسبة والاتصال، بما في ذلك الشبكات.

وعليه، فإن أي تعريف دقيق للجريمة الإلكترونية يجب أن يراعي طابعها العالمي، وأن يكون مرنًا يستوعب التطور التكنولوجي المستمر، مع إبراز خصوصيتها من حيث تنوع صور السلوك الإجرامي والدور المحوري للحاسوب فيما يلي: 1

-يجب أن يتلاءم هذا التعريف مع فكرة عالمية المعلومات والاتصالات وأن يكون واضحا عالميا.

-يجب مراعاة التطورات المتلاحقة في عالم الحوسبة والاتصال ويسمح باستيعاب كل ما

يستجد من صور للجرائم الإلكترونية.

-يجب توضيح خصوصية الجرائم الإلكترونية لما تحتويه على أشكال مختلفة للسلوك الإجرامي بحيث يظهرا جليا دور الحاسوب في ارتكاب هذه الجرائم.

ثانيا موقف المشرع الجزائري : [1]

نتيجة للتطور التكنولوجي وما أفرزته الثورة المعلوماتية من أنماط إجرامية مستحدثة، سارع المشرّع الجزائري، على غرار باقي التشريعات المقارنة، إلى تعديل قانون العقوبات بموجب القانون رقم 15-04 المؤرخ في 10 نوفمبر 2004، حيث أدرج قسمًا سابعًا مكررًا بعنوان جرائم المساس بأنظمة المعالجة الآلية للمعطيات، وذلك بهدف توفير حماية جزائية للأنظمة المعلوماتية وسدّ الفراغ التشريعي في هذا المجال

قام المشرع الجزائري بتعديل قانون العقوبات بموجب القانون رقم : 04 15 المؤرخ في 10 نوفمبر 2004، بإضافة قسم سابع مكرر تحت عنوان جرائم المساس بأنظمة المعالجة الآلية للمعطيات من المادة (394) مكرر ، حيث جاء في أسباب هذا التعديل : إن التقدم التكنولوجي وانتشار وسائل الاتصال الحديثة أدى الى بروز أشكال جديدة للإجرام مما دفع بالكثير من الدول إلى النص على معاقبتها، وأن الجزائر على غرار هذه الدول تسعى من خلال هذا المشروع إلى توفير حماية جزائية للأنظمة المعلوماتية وأساليب المعالجة الآلية للمعطيات وأن هذه التعديلات من شأنها سد الفراغ القانوني في بعض المجالات، وسوف يمكن لا محالة من مواجهة بعض أشكال الإجرام الجديد. من جانب آخر أقر المشرع الجزائري بمسؤولية الشخص المعنوي وعاقب على الشروع والاتفاق الجنائي، وشدّد من العقوبات في بعض هذه الجرائم ، يذكر أننا سنتطرق في بحثنا هذا إلى جملة القوانين التي أقرها المشرع الجزائري بخصوص مكافحة الجرائم الإلكترونية سواء بموجب القانون العام أو بموجب القانون الخاص[2].

اعتمد المشرع الجزائري مصطلح الجرائم المتصلة بتكنولوجيات الإعلام والاتصال للإشارة إلى ما يُعرف بالجرائم الإلكترونية أو المعلوماتية، حيث قام بتحديد مفهومها بموجب أحكام المادة 02الفقرة1 القانون رقم 09-04 المؤرخ في 5 غشت 2009، المتضمن القواعد

[1] يزيد بوحليط مرجع سابق، ص36.

[2] المادتين 394مكررتعديل قانون العقوبات الجزائري بموجب القانون رقم 15-04 المؤرخ في 10نوفمبر 2004.

الخاصة للوقاية من هذه الجرائم ومكافحتها. ووفقًا لهذا النص، تُعرّف هذه الجرائم بأنها تلك التي تمس بأنظمة المعالجة الآلية للمعطيات كما هو منصوص عليه في قانون العقوبات، إضافة إلى كل جريمة تُرتكب أو يُسهّل ارتكابها باستخدام منظومة معلوماتية للاتصالات أ و أنها : " جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية ...".[1]

الفرع الثاني خصائص الجرائم الالكترونية

تتميز جرائم الإنترنت بعدة خصائص و مميزات تختلف عن باقي الجرائم التقليدية ومن أهمها ما يلي:

أولا : الحاسب الآلي (أداة ارتكاب الجريمة)

جريمة الإنترنت لا بد وأن ترتكب عن طريق الحاسب الآلي، و هو أول أمر يميزها عن الجريمة التقليدية إضافة إلى أن مرتكبها هو شخص يتمتع بخبرة فائقة في مجال الحاسب الآلي و المعلوماتية.

ثانياً: جريمة دائمة التطور

برغم من حداثة جرائم الإنترنت، إلا إنها ويعكس باقي الجرائم الأخرى في تطور مستمر ذلك أن أساليب ارتكاب هذه الجرائم من السهولة بحيث تنتقل من مكان لآخر في ذلك الوقت، فالمجرم الإلكتروني يستطيع التعرف على أجدى الطرقة لارتكاب الجريمة عن طريق الاتصال بأقرانه من مختلف دول العالم، حيث أن جرائم الإنترنت تتميز بإمكانية تكوين تشكيلات إجرامية تضم العديد من الأفراد على مستوى الدولي، و يكون الربط بينهم عن طريق شبكة الإنترنت.

ثالثا: جريمة عابرة للحدود

[1] المادة 2الفقرة 1 من القانون 04-09 المؤرخ في 5غشت 2009المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال الجريدة الرسمية العدد 47 الصادر بتاريخ 16غشت 2009.

فارتكاب الجريمة قد يتم بالدخول إلى نظام حاسوب في دولة عن طريق شخص يعيش في دولة أخرى، الأمر الذي يثير تساؤلات عدة حول وقت ارتكاب الجريمة نظراً لاختلاف المواقيت الدولية عن بعضها البعض، و كذلك عن القانون واجب التطبيق على هذه الجريمة، هل هو قانون دولة ارتكاب الفعل الضار أم الدولة الحادث فيها العثور.

رابعاً: عدم الإبلاغ عنها

لا يتم – في الغالب الأعم – الإبلاغ عن جرائم الإنترنت إما لعدم اكتشاف الضحية لها وإما خشيته من التشهير، لذا نجد أن معظم الإنترنت تم اكتشافها بالمصادفة، بل و بعد وقت طويل من ارتكابها، زد على ذلك أن الجرائم لم تكتشف هي أكثر بكثير من ذلك التي كشف الستار عنها . فالرقم المظلم بين حقيقة عند هذه الجرائم المرتكبة، و العدد الذي تم اكتشافها، هو رقم خطير.

خامساً: سهولة إخفاء معالمها

من السهل معالم جريمة الإنترنت و صعوبة تتبع مرتكبيها، لذا فهذه الجرائم لا تترك أي أثرها بعد ارتكابها، علاوة على صعوبة الاحتفاظ الفئى بآثارها إن وجدت، فهذه الجرائم لا تترك أثرا، فليست هناك أموال أو مجوهرات مفقودة، وإنما هي أرقام تتغير في السجلات، ولذا فإن معظم جرائم الإنترنت تم اكتشافها بالمصادفة وبعد وقت طويل من ارتكابها .

سادسا: صعوبة كشف وملاحقة مرتكبها

سبب ذلك أن الجاني غالبا ما يتلف أي أثر من الممكن ان يخلفه وراءه، أضف لذلك أن ارتكاب الجريمة من خارج حدود الدولة و بوسائل تقنية متطورة قد يضيع الفرصة في اكتشاف مرتكبها .

سابعا : جريمة صعبة الإثبات

تتميز هذه الجريمة بصعوبة إثباتها، ومرجع ذلك هو قلة عدد المختصين في تعقب مثل هذا النوع من الجرائم حيث تنعدم الآثار التقليدية للجرائم كالبصمات مثلا، إضافة لسهولة محو و تدمير الدليل المادي في زمن قصير جداً.

ثامناً: جريمة هادئة لا عنف فيها

لا تحتاج جرائم الإنترنت إلى عنف أو مجهود كبير كما هو الحال في الجرائم الاعتيادية التقليدية، و إنما تنفذ دون جهد بذكر ذلك أنها تعتمد على الخبرة المعلوماتية لدى مرتكبها.

تاسعا: نقص الخبرة الفنية لدى الجهات المختصة بالتحقيق

اكتشاف جرائم الإنترنت يتطلب إلهاما بالأمور الفنية و التقنية لدى أجهزة الشرطة و النيابة العامة و القضاء، وذلك للتوصل إلى مرتكبي مثل هذا النوع من الجرائم ذات التقنية المتطورة و الأساليب المعقدة، الأمر الذي وجدت معه هذه الجهات نفسها أنها غير قادرة على التعامل مع هذا النوع من الجرائم[1]

الفرع الثالث: أنواع الجرائم الالكترونية

تتعدد الجرائم الإلكترونية بتعدد الوسائل والغايات التي ترتكب من أجلها، ويمكن تصنيفها إلى الأنواع التالية:

أولا: جرائم الاختراق والتجسس

نتيجة للتطور التقني والثورة الالكترونية التي ألقت بظلالها على مناحي الحياة كافة أصبحت شبكة الإنترنت ميداناً الصراعات من نوع جديد حملت كل أدوات التدمير الإلكتروني كالتجسس والاختراق وتدمير المواقع الإلكترونية الحكومية وغير الحكومية، والتحكم في تغيير قواعد بيانات قد تصل في خطورتها إلى تهديد الأمن القومي لبعض الدول، مما دفع بعض خبراء الإنترنت. وعادة ما يعرف الهكر بأنه شخص غامض. يخترق كيف ما يشاء والناس تخاف منه . ويعتبر شخصية كبيرة ويكون له أعوان يلحقون خلف شهرته وقد يتلبسون بها في عصرنا الحالي انقلبت الموازين ، أصبح الصغار كبارا بعقولهم في عالمهم أعمارهم تتراوح ما بين 16 سنة و20 سنة.. في هذا السن تجد كثيرين محترفين في عالم الهكر، منهم الطيب ومنهم الخبيث المخترقون أجناس... وقد تجد فيهم من يساعد الناس في استرجاع بياناتهم وبريدهم الالكتروني، ومنهم من يقوم بسرقة الناس مدعيا انه

[1] محمد عبيد الكعبي، مرجع سابق ،ص39

شخص طيب وهو في الأصل متلصص يريد أن يخترق عبثا.[1]تشمل التسلل إلى الأنظمة الإلكترونية والمواقع بقصد الاطلاع على بيانات سرية أو التلاعب بها.مثلاختراق البريد الإلكتروني، أو التجسس على حسابات الأفراد، أو سرقة بيانات الشركات.[2]

ثانيا: جرائم سرقة الهوية والاحتيال الإلكتروني

تحدث سرقة الهوية عندما يسرق شخص ما هويتك و يتظاهر بأنه أنت.

تتضمن الاستيلاء على المعلومات الشخصية لشخص ما واستخدامها دون إذنه لتحقيق مكاسب غير مشروع.مثل سرقة بيانات البطاقات البنكية واستخدامها للشراء، أو إنشاء حسابات وهمية باسم الضحية[3].

ثالثا: جرائم الابتزاز الإلكتروني

تُعد جريمة الابتزاز الإلكتروني من أخطر الجرائم المعلوماتية، حيث يقوم الجاني بتهديد الضحية بنشر معلومات أو صور خاصة، قد تكون صحيحة أو مفبركة، بهدف إجباره على دفع مبالغ مالية أو تنفيذ مطالب معينة. وتتم هذه الجريمة غالبًا عبر وسائل التواصل الاجتماعي أو البريد الإلكتروني، من خلال استغلال البيانات الشخصية أو اختراق الحسابات. كما تشمل نشر الشائعات وتشويه السمعة للنيل من الأفراد أو المؤسسات، بقصد الضغط عليهم وتحقيق مكاسب غير مشروعة[4].: حيث تهدف إلى تهديد الضحايا بنشر معلومات حساسة أو صور خاصة مقابل دفع مبالغ مالية أو تنفيذ طلبات معينة.تنتشر هذه الجريمة خاصة عبر وسائل التواصل الاجتماعي.[5]

رابعا: جرائم التشهير والقذف الإلكتروني

وهي الجرائم التي ترتكب ضد الأفراد باستعمال النظام الإلكتروني عن طريق الشبكة العنكبوتية المادة 297 من القانون العقوبات الجزائري السب ب" يعتبر السب كل كلام سيء أو مصطلح يحتوي على تحقير أو قدحا لا يرتكز على إسناد ظاهرة."يمكن أن نعرف القذف

[1] الدكتورة بشرى حسين الحمداني، القرصنة الالكترونية، أسلحة الحرب الحديثة، الطبعة الأولى دار أسامة للنشر التوزيع، 2014، ص 13.

[2]فضيلة الشيخ حذيفة بن حسين القحطاني مسؤول إفتاء محافظة صلاح الدين، الجرائم الالكترونية، الأحكام و الضوابط، العراق، ص 18.

[3] مرجع سابق، ينظر الصفحة نفسها.

[4] الدكتورة بشرى حسين الحمداني، القرصنة الالكترونية، أسلحة الحرب الحديثة، الطبعة الأولى دار أسامة للنشر التوزيع، 2014، ص 12.

[5] فضيلة الشيخ حذيفه بن حسان القحطاني مرجع سابق ص 19

بأنه هو إسناد وصمة محددة تتطلب عقاب من تنسب إليه أو التنمر إسنادا عموديا يفيد نسبة الأمر إلى الفرد على أن يحتوي ذلك إسناد ظاهرة معنية إلية"فالفرق بين السب والقذف يتعلق إستاد وصمة محددة إلى شخص في حين أن السب لا يتعلق بذلك.إن جريمتي السب والقذف عن طريق الوسائط الافتراضية ضد الأشخاص من بين الجرائم التي انتشرت بكثرة مؤخرا نظرا للاستغلال السيئ للوسائل التكنولوجية الحديثة.[1]

تتعلق باستخدام الإنترنت لتشويه سمعة الآخرين أو نشر معلومات كاذبة عنهم.نشر أخبار غير صحيحة أو صور مفبركة للإساءة إلى سمعة شخص أو جهة معينة[2].

خامسا جرائم القرصنة وسرقة الملكية الفكرية:تواجه شبكة الإنترنت ما يسمى بالقرصنة من قبل بعض الجماعات التي تؤمن بالحرية المطلقة في الرأي والتعبير والاستخدام أيضا، وهي جماعات تستطيع أن تدخل عبر طرق خاصة تخترق أجهزة الحاسوب الأرقام السرية للأشخاص وإلى بريدهم الإلكتروني ما يؤدي إلى معرفة أسرار الناس وخصوصيات أعمارهم وحياتهم الشخصية، وهذه أيضا مسألة هامة أثارت أخلاقيات الالتزام في استخدام الإنترنت[3].تشمل نسخ أو توزيع البرامج، أو الأفلام، أو الكتب، أو الموسيقى بدون إذن صاحب الحق. تعد هذه الجريمة انتهاكاً لحقوق المؤلفين والشركات.[4]

سادسا جرائم غسيل الأموال الإلكترونية:استخدام التقنيات الحديثة لتحويل الأموال المكتسبة بطرق غير شرعية وجعلها تبدو كأنها شرعية.تستخدم فيها العملات الرقمية كوسيلة لإخفاء مسار الأموال[5].

سابعا جرائم الإرهاب الإلكتروني:في ظل غياب تعريف موحد للإرهاب العادي. تعددت أيضا تعريفات الإرهاب الإلكتروني، فقد عرفه قاموس "لاروس "Larousse" "بأنه "مجموعة من

[1]عبد الكريم زنتوت، الجريمة الإلكترونية وسبل مواجهتها في الجزائر ، المجلد 13،العدد 1، سنة2025،صفحه،323

[2]ففضيلة الشيخ حذيفة بن حسين القحطاني مسؤول إفتاء محافظة صلاح الدين، الجرائم الالكترونية، الأحكام و الضوابط، العراق، ص 18.

[3] الدكتورة بشرى حسين الحمداني، القرصنة الالكترونية، أسلحة الحرب الحديثة، الطبعة الأولى دار أسامة للنشر التوزيع، 2014، ص 12.

[4] فضيلة الشيخ حذيفة بن حسين القحطاني مرجع سابق ص 19.

[5] فضيلة الشيخ حذيفة بن حسين القحطاني مرجع سابق نفس الصفحة.

الهجمات الخطيرة (فيروسات قرصنة ... الخ) على حواسيب شبكات وأنظمة الإعلام الآلي المؤسسة أو هيئة ترتكب الخلق فوضى عامة يهدف بث الرعب.[1]

المطلب الثاني : الجريمة المعلوماتية في نطاق القانون الداخلي و العقوبات المقررة لها

سنتطرق في هذا المحور إلى الجريمة المعلوماتية في القانون الجزائري و خارج قانون العقوبات

الفرع الأول : الجريمة المعلوماتية في مجال قانون العقوبات

تعتبر الجريمة المعلوماتية من أبرز التحديات التي أفرزها التطور التكنولوجي، حيث تدخل المشرّع الجزائري لتنظيمها من خلال تعديل قانون العقوبات، بإدراج نصوص خاصة تجرّم الأفعال المرتكبة عبر أنظمة المعالجة الآلية للمعطيات. ويمكن تقسيم هذه الجرائم إلى ثلاث فئات رئيسية

أولا :الجرائم المعلوماتية الماسة بأنظمة المعالجة الآلية للمعطيات

تناول المشرّع الجزائري تكريس الحماية الجزائية للأنظمة المعلوماتية من خلال إدراج أحكام خاصة ضمن القسم السابع مكرر من قانون العقوبات، وذلك بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، حيث نصّت المواد من 394 مكرر إلى 394 مكرر 7 على تجريم مجموعة من الأفعال، تتمثل أساسًا في إطار أحكام التعديل الذي شمل قانون العقوبات لسنة 2004، بموجب القانون رقم 04-15 المؤرخ في 10/11/2004 ، في إطار أحكام القسم السابع مكرر المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات، هذه المواد هي من 394 مكرر إلى 394 مكرر 7 ، والمتمثلة في الجرائم التالية[2]:

1 **جريمة الدخول في كل أو جزء من منظومة للمعالجة الآلية لمعطيات (م 394 مكرر /1) أو محاولة ذلك**

[1] الدكتور طاهر عباسة، جريمة الإرهاب الالكتروني في ضوء أحكام الاتفاقية العربية لمكافحة تقنية الجرائم، مجلة العلوم القانونية و السياسية، المجلد 09، العدد 03، 2018، ص 81..

[2] بن دراح علي إبراهيم، محاضرات في الجرائم المعلوماتية، تخصص القانون الدولي الجنائي، قسم الحقوق و العلوم السياسية، الاغواط، 2021/2019، ص 45-47 .

تنص المادة 394 مكرر على أنه يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك. " لقد جرم المشرع فعل الدخول بطريق غير شرعية إلى أي منظومة معلوماتية دخولا غير شرعي، وذلك حين عبر عنه بطريق الغش، كما أن المشرع لم يفرق بين الدخول إلى جزء من المنظومة أوكلها.

وهنا سيتخلص من نص المادة ما يلي:

-التسليم بتوفير القصد الجنائي بمجرد الدخول إلى نظام معلوماتي عن طريق الغش.

-عدم الاعتداد بنتائج هذا الدخول حتى ولو يسبب أي تخريب أو إضرار بالبيانات لكون اعتبارها جريمة وقتية.

-مجرد المحاولة يعتبر في حد ذاته جريمة حتى وان لم يتحقق فعلا[1].

بالرجوع إلى نفس المادة السابقة وفي نفس الفقرة 1 فان المشرع قد فرق بين فعل الدخول غير الشرعي والبقاء فيه ، وذلك باعتبار كل فعل يعتبر مجرما، فالبقاء قرينة على توفر القصد الجنائي، كما تعتبر جريمة مستمرة ، على عكس الجريمة الأولى، غير أن المشرع لم يفرق بين البقاء غير الشرعي أو مجرد المحاولة على غرار الجريمة الأولى.2

2 جريمة حذف أو تغيير في معطيات المنظومة (م394 مكرر /2) كنتيجة للدخول غير الشرعي أو البقاء واعتبارهما كجريمتين مضاعفتين

تنص المادة 394 مكرر في فقرتها الثانية على أنه " تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير المعطيات المنظومة وعليه فإن المشرع الجزائري فرق بين عملية حذف البيانات وعملية تغييرها، اللذين يعتبرهما كنتيجة لفعل الدخول غير الشرعي أو البقاء كما اعتبرهما جريمة مضاعفتين وذلك نتيجة لخطورة النتائج المترتبة عنهما.

3 جريمة تخريب نظام الاشتغال كنتيجة للدخول غير الشرعي أو البقاء (م 394 مكرر/3)

نصت المادة 394 مكرر 3 على أنه " وإذا ترتب على الأفعال المذكورة أعلاه تخريب اشتغال المنظومة تكون العقوبة الحبس من 6 أشهر إلى سنتين والغرامة من 50.000 دج إلى 150.000 دج" وعلى أساس ذلك لم يعتبر المشرع الجزائري جريمة تخريب نظام

[1] المادة 394مكرر من قانون العقوبات الجزائر ي السالف الذكر .

الاشتغال جريمة مستقلة بذاتها على غرار الدخول غير الشرعي أو البقاء ، بل باعتبارها نتيجة للجرائم السابقة، وذلك يرجع إلى أنه من الممكن حدوث تخريب لهذا النظام ابتداء دون توفر القصد الجنائي إلا عندما يكون كنتيجة لجريمة سابقة[1].

4 جريمة إدخال معطيات في نظام المعالجة الآلية أو إزالتها أو تعديلها عن طريق الغش (م 394 مكرر /1)

نصت المادة 394 مكرر 1 على أنه "يعاقب بالحبس من 6 أشهر إلى 3 سنوات وبغرامة من 500.000 إلى 2.000.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل" ومنه فان المشرع قد اعتبر أن إدخال معطيات مغشوشة في نظام المعالجة الآلية جريمة معلوماتية تستوجب عقوبة ، والتي ضاعفها إذا ما قورنت بالعقوبات السابقة، و إذا كان قد ربط فعل الحذف بالنتيجة المترتبة عن الدخول غير الشرعي أو البقاء، فقد اعتبر جريمة الإزالة جريمة مستقلة في حد ذاتها تستوجب نفس العقوبة السابقة بالرغم من اتفاقية بودابست وكذا المشرع الفرنسي استعمل مصطلح الحذف لاستخدامه ضمن نفس المعنى.

5 جريمة تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في المعطيات عمدا وعن طريق الغش (م 394 مكرر2/1)

نصت المادة 394 مكرر 2 في فقرتها الأولى على انه "يعاقب بالحبس من شهرين إلى 3 سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج كل من يقوم عمدا، وعن طريق الغش تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.،[2]

6 جريمة حيازة أو إفشاء أو نشر أو استعمال معطيات المتحصل عليها من الجرائم المذكورة سابقا عمدا وعن طريق الغش (م 394 مكرر 2/2)

[1] المادة 349مكرر والمادة 394مكرر 1 العقوبات الجزائري، أمر رقم 66-156 المؤرخ في 8 يونيو 1966، المعدل والمتمم بالقانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، الجريدة الرسمية، العدد 71، 2004،

1 [2] المادة 394مكرر 2الفقرة 1من قانون العقوبات الجزائري 156–66 السالف الذكر.

فكما أقر المشرع جرمية الانفعال المذكورة سابقا ، فان حيازة معطيات أو إفشائها أو نشرها أو استعمالها يعتبر جريمة يعاقب عليها القانون.[1]

ثانيا الجرائم المعلومات الواقعة على الأشخاص و الأموال

1 - الجرائم المعلومات الواقعة على الأشخاص

أ -القذف والسب و الاهانة على حرمة الأشخاص

تناول المشرّع الجزائري في المواد 296 و297 و298 من قانون العقوبات على تجريم الأفعال الماسّة بشرف واعتبار الأشخاص، من خلال صور القذف والسبّ والإهانة، غير أنّ هذه النصوص جاءت خالية من الإشارة الصريحة إلى ارتكاب هذه الجرائم عبر الوسائط المعلوماتية الحديثة. ومع التطور المتسارع لوسائل الاتصال وتكنولوجيات الإعلام، تدخّل المشرّع لسد هذا الفراغ القانوني، حيث تمّ تجريم هذه الأفعال في إطارها الإلكتروني بموجب القانون رقم 01-09 المؤرخ في 26 جوان 2001، الذي أضاف المادة 144 مكرر إلى قانون العقوبات. وقد نصّت هذه المادة على معاقبة كل من يرتكب هذه الجرائم باستعمال الوسائل الإلكترونية أو المعلوماتية، بعقوبة الحبس من ثلاثة (3) أشهر إلى اثني عشر (12) شهراً، وبغرامة مالية تتراوح بين 50.000 دج و250.000 . كل شخص قام بالسب أو القذف سواء كان ذلك عن طريق الكتابة أو الرسم أو التصريح أو بأية آلية لبث الصوت أو الصورة أو بأية وسيلة إلكترونية أو معلوماتية أو إعلامية أخرى تباشر النيابة العامة إجراءات المتابعة الجزائية تلقائيا . في حالة العود تضاعف عقوبات الحبس والغرامة المنصوص.[2]

تنص المادة 302 من قانون العقوبات المصري على أن يعد قاذفا كل من أساء لغيره بواسطة إحدى الطرق السيئة بالمادة 171 من هذا القانون أموراً لو كانت صادقة لأوجبت عقاب من أسندت إليه بالعقوبات المقررة لذلك قانوناً أو أوجبت احتقاره عند أهل وطنه، الخ[3].

---

[1] المادة 394مكرر 2الفقرة 2من قانون العقوبات الجزائر ي

[2] بن دراح علي إبراهيم، محاضرات في الجرائم المعلوماتية، تخصص القانون الدولي الجنائي، قسم الحقوق و العلوم السياسية، الاغواط، 2021/2019، ص 51.

[3] نجاد البرعي، محامي بالنقض، جرائم الصحافة و النشر، القاهرة، مصر، ص 28.

ب – جريمة الاستغلال الجنسي للأطفال عبر شبكة الانترنت

في ضل قانون العقوبات الجزائري نصت المادة 333 فقرة 1 من قانون العقوبات الجزائري على أن يعاقب بالحبس من خمس (5) سنوات إلى عشر (10) سنوات وبغرامة من 500.000 دج إلى 1.000.000 دج كل من صور قاصرا لم يكمل 18 سنة بأي وسيلة كانت وهو يمارس أنشطة جنسية بصفة مبينة. حقيقية أو غير حقيقية، أو صور الأعضاء الجنسية للقاصر لأغراض جنسية.[1]

2 – جرائم المعلومات الواقعة على الأموال

تتنوع الجرائم المعلوماتية الماسة بالأموال، وعلى رأسها النصب الإلكتروني، من أكثر صور الجريمة شيوعًا وخطورة في العصر الرقمي، وذلك بفعل الانتشار الواسع لاستخدام شبكة الإنترنت وتطور تقنيات الحواسيب والاتصال. وقد أفرز هذا التطور أنماطًا جديدة من السلوك الإجرامي الذي يعتمد على الوسائط الإلكترونية كأداة للاحتيال والاستيلاء غير المشروع على أموال الغير.[2]

3 – العقوبات المقررة لجرائم النصب و الاحتيال الالكتروني

أ – العقوبات المقررة للشخص الطبيعي

تفرض غرامة مالية على مرتكب جريمة النصب والاحتيال تتراوح بين 100،000دج و 500،000 دج، حسب جسامة الفعل وضرره حيث يأخذ القاضي بعين الاعتبار المبلغ الذي تم الحصول عليه بشكل غير قانوني، وكذلك نوع الضحية وطبيعة التحايل. على سبيل المثال، في الحالات التي يتسبب فيها الجاني في خسائر مالية جسيمة للضحية أو مجموعة من الضحايا، قد تزداد قيمة الغرامة المفروضة لتصل إلى غاية 1.000.000 دج خاصة إذا ما وقعت الجنحة على مجموعة تزيد عن ثلاثة أشخاص[3].

[1] شاكر سليمان، الآليات القانونية لحماية الطفل من جرائم الاستغلال الجنسي عبر شبكة الانترنت (دراسة مقارنة)، مجلة حقوق الانسان و الحريات العامة، المجلد08، العدد01، ص 106.

[2] بن دراح علي إبراهيم، محاضرات في الجرائم المعلوماتية، تخصص القانون الدولي الجنائي، قسم الحقوق و العلوم السياسية، الاغواط، 2021/2019، ص 54.

[3] الأمر رقم 66–156 المؤرخ في 18 صفر عام 1386 الموافق ل 08 جويلية سنة 1966، يتضمن قانون العقوبات(الجريدة الرسمية عدد 49 سنة 1966) المعدل بالقانون رقم 24–06 المؤرخ في 28 أفريل سنة 2024، (الجريدة الرسمية عدد 30 لسنة 2024).

ب – العقوبات المقررة لشخص المعنوي:

تنص المادة 372من قانون العقوبات الجزائر على مايلي:

تفرض غرامه مالية في حال ثبوت مسؤولية الشخص المعنوي في جريمة النصب أو الاحتيال، تفرض عليه غرامة تعادل خمسة أضعاف الحد الأقصى للغرامة المقررة للشخص الطبيعي، مما يعني أنه يمكن أن يصل مبلغ الغرامة 2.500.000 دج. هذا النص يهدف إلى تحميل المؤسسات مسؤولية فعلية عن سلوكيات موظفيها، ويُعتبر بمثابة أداة للحد من السلوكيات غير القانونية التي قد تضر بالاقتصاد الوطني[1].

كما نصت المادة 108 من قانون 02-26 المتعلق بخدمات الثقة للمعاملات الإلكترونية والتوقيع الإلكتروني "يعد الشخص المعنوي مسؤولا جزائيا على الجرائم المنصوص عليها في هذا القانون حسب القواعد المنصوص عليها في قانون العقوبات"[2]

[1] المادة 372من الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 08 جوان سنة 1966، المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، العدد 49، لسنة 1966، المعدل والمتمم،

2-اللمادة 108من القانون رقم 02-26المتعلق بخدمات الثقة للمعاملات الإلكترونية والتوقيع الإلكتروني ، السالف الذكر ص18



خاتمة



خاتمة

تعتبر عملية تأمين المعاملات الإدارية الإلكترونية ركيزة أساسية في الجزائر لتجسيد فكرة أو مشروع "الجزائر الإلكترونية "وضمان استمرارية الخدمات الرقمية وحمايتها من التهديدات السبيرانية ومختلف الجرائم الإلكترونية، لذلك قمت من خلال هذا البحث على تسليط الضوء على الوسائل القانونية والتقنية لتأمين المعلومات والوثائق الإدارية التي أقرها المشرع الجزائري في القانون 15/04 المدعمة لحماية التوقيع والتصديق الالكترونيين من القرصنة والاختراقات الإلكترونية، ويستعمل التوقيع الالكتروني لتوثيق هوية الموقع وإثبات قبوله مضمون الكتابة في الشكل الإلكتروني كما يعتبر التشفير الإلكتروني أهم طريقة لتأمين المعاملات الإدارية الإلكترونية فهو عبارة عن عمليات رياضية يتم بها تحويل النص المراد.

إرساله إلى رموز لا يتاح فهمها إلا من خلال فك الشفر وتحويل هذه الرموز والإشارات إلى نصوص مفهومة ومقروءة، ونلاحظ أيضا أن الأمن السبراني يلعب دورا هاما في مواجهة الهجمات السبيرانية التي قد تستهدف الأنظمة الإدارية من بينها الجرائم الإلكترونية كالاحتيال وسرقه البيانات وغيرها وفي هذا السياق تطرقنا إلى الإجراءات الجزائية المعاملات الإدارية الإلكترونية والحماية الإدارية والتقنية لضمان امن المعلومات والجزائيات القانونية المترتبة على الجرائم الإلكترونية.

وفي ختام بحثي هذا في ختام هذا البحث حول الوثائق لتأمين المعاملات الإدارية الإلكترونية وما يرتبط بها من وسائل قانونية أو إدارية يتّضح أن التحول الرقمي للإدارة العمومية يمثل خطوة استراتيجية لتعزيز فعالية المرفق العام وتحقيق الشفافية وسرعة الأداء، غير أنّه في المقابل يفتح المجال أمام أنماط جديدة من الجرائم، خاصة تلك المتعلقة بالغش، تزوير الوثائق الإلكترونية، الاختراقات المعلوماتية، والاعتداء على الأنظمة والبيانات. لذالك يستوجب اجراءات وقائية تتمثل في الحماية الإدارية والعقوبات الجزائية التي تترتب على المخالفات والجرائم التي تمس أمن المعلومات والوثائق الإدارية ونستنتج مما سبق النتائج التالية:

_تزايد أهمية الوثيقة الإلكترونية: أصبحت الوثائق الإلكترونية والتوقيع الإلكتروني وسائل قانونية أساسية في المعاملات الإدارية، تتمتع بحجية قانونية متى استوفت الشروط التقنية والقانونية.

_تطور الإطار القانوني لقانون المعاملات الإدارية الإلكترونية ، حيث سعى المشرع الجزائري إلى مواكبة التطور التكنولوجي والرقمنة من خلال سن قوانين خاصة بخدمات الثقة بين المتعاملين و التوقيع الالكتروني .

_ تبين أن الجرائم المرتبطة بتكنولوجيا الإعلام والإتصال وخصوصا المرتبطة بالإدارة كالتزوير الإلكتروني و انتحال الهوية ، اصبحت اكثر تعقيدا وخطورة مقارنة بالأساليب التقليدية.

_نقص الوعي الأمني بين الموظفين يزيد من خطورة ارتكاب الجرائم الإلكترونية على مستوى الادارة.

_اهمية التكامل بين الأليات القانونية والإدارية وكذا الحماية الإدارية والعقوبات الجزائية الصارمة للحد من انتشار الجرائم الإلكترونية التي تمس أمن الإدارة.

واستنادا على ما سبق يمكن اقتراح مجموعة من التوصيات العملية:

_ضرورة تجديد او تحيين للقوانين المتعلقة بالمعاملات الإلكترونية بشكل كل مستمر لمواكبة التطور التكنولوجي والتحول الرقمي السريع.

_تعزيز انظمة الأمن المعلوماتي داخل القطاع الإداري من خلال إعتماد ألية التشفير ونظام كشف التسلل، والجدران النارية.

_فرض قوانين صارمة على الأنظمة المعلوماتية و إنشاء وحدات إدارية لمتابعة أمن المعلومات

_ تنظم دورات تدريبية وتكوينية للموظفين وذلك لزيادة ثقافة الوعي والأمن السبيراني.

_نشر الثقافة الإلكترونية القانونية بين الموظفين وتوعيتهم بمخاطر الجرائم المعلوماتية التي تمس أمن المعلومات والوثائق الإدارية.

_ تعزيز التعاون بين الهيئات القانونية و التقنية والقضائية وتكافل الجهود الدولية لمكافحة الجرائم الإلكترونية داخل او خارج الوطن.



قائمة المراجع و المصادر



أولا :القوانين

1. القانون رقم 09_88 المتعلق بالأرشيف، المؤرخ في 26جانفي 1988، الجريدة الرسمية العدد 04 الصادر بتاريخ 27جانفي1988.
2. قانون التوقيع الالكتروني المصري رقم 15 لسنة 2001 الصادر بتاريخ 22أفريل، 2004 الجريدة الرسمية لجمهورية مصر العربية، العدد117
3. القانون رقم15-04المؤرخ في 01 فبراير 201 المتعلق التوقيع والتصديق الالكترونيين ، الجريدة الرسمية 06 الصادر في 15فبراير 2015.

4. القانون رقم 26-02 المؤرخ في 29 شعبان عام 1447 الموافق 17 فبراير سنة 2026، المحدد للقواعد العامة المتعلقة بخدمات الثقة للمعاملات الإلكترونية وبالتعريف الإلكتروني، الجريدة الرسمية ، العدد 14، الصادرة بتاريخ 18 فبراير 2026.
5. القانون 06-01المتعلق بالوقاية من الفساد ومكافحته المؤرخ 20فبراير 2006 الجريدة الرسمية العدد 14 الصادر بتاريخ 08مارس 2006المعدل والمتمم..
6. القانون رقم 18-07المتعلق بحماية الاشخاص الطبيعيين ذات الطابع الشخصي، المعدل والمتمم بالقانون رقم 25-11المؤرخ في 24 يونيو 2025 المتعلق بحمايةالاشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع شخصي، الجريدة الرسمية العدد48، الصادر بتاريخ 24جويلية 2025.

ثانيا: الأوامر

_ الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 08 جوان سنة 1966، المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، العدد 49، لسنة 1966، المعدل والمتمم،

ـ الأمر رقم 75-58 المؤرخ في 26 سبتمبر 1975، المتضمن القانون المدني، المعدل والمتمم بالقانون رقم 05-10 المؤرخ في 20 يونيو 2005، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 44 لسنة 2005.

ـالأمر رقم 21-19 المتعلق بحماية المعلومات والوثائق الإدارية، المؤرخ في 27شوال عام 1442الموافق ل 08يونيو، 2021 الجريدة الرسمية العدد 45.الصادرفي09 يونيو2021.

ثالثا.: المراسيم

ـالمرسوم الرئاسي رقم 172-19،المؤرخ في 11يونيو 2019، المتعلق بتحديد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها وتنضيمها وكيفية سيرها، الجريدة الرسمية الجمهورية الجزائرية الشعبية، العدد، 38 الصادر بتاريخ 12يونيو2019.

-رابعا :الكتب

- أكرم تحسين الدخيلي، النظام القانوني للتوثيق الإلكتروني، دراسة مقارنة, دار الثقافة للنشر والتوزيع، عمّان، الأردن، الطبعة الأولى، 2012

- المحامي الدكتور محمد فواز المطالقة ،الوجيز في عقود التجارة الالكترونية، دار الثقافة للنشر والتوزيع، عمّان، الأردن، الطبعة الأولى، 2010.

- إلياس ناصيف، العقد الإلكتروني في القانون المقارن، لبنان، منشورات الحلبي الحقوقية، 2009.

- خالد وليد محمود، الهجمات عبر الإنترنت ساحة الصراع الإلكتروني الجديدة، المركز العربي الأبحاث ودراسة السياسات، قطر، 2013.

- سامح عبد الواحد التهامي التعاقد عبر الانترنت دار الكتب القانونية، المجلة الكبرى، مصر2008.

- سعيد السيد قنديل التوقيع الإلكتروني، بدون طبعة دار الجامعة الجديدة للنشر الإسكندرية 2004.

- عباس العبودي تحديات الإثبات بالسندات الالكترونية ومتطلبات النظام القانوني لتجاوزها، ط1، منشورات الحلبي الحقوقية، بيروت، 2010.
- عيسى غسان الربضي، القواعد الخاصة لتوقيع الالكتروني ، دار الثقافة للنشر والتوزيع ، الأردن ،2009.
- فارس محمد العمارات إبراهيم محمد الحمامصه الأمن السبيراني المفهوم وتحديات العصر ط1 ،2022.
-حسام الدين، أسامة، أساسيات الأمن السيبراني (Cybersecurity Essentials)، مادة تدريبية ضمن أكاديمية سيسكو، جامعة طيبة، المملكة العربية السعودية، سبتمبر 2017.
-إسماعيل علي محمود، المراسلات الإدارية، الطبعة الأولى، مؤسسة طيبه للنشر و التوزيع، 2018.
-أكرم تحسين الدخيلي، النظام القانوني للتوثيق الإلكتروني، الطبعة الأولى، مكتبة زين الحقوقية والأدبية، 2018.
-بن دراح علي إبراهيم، محاضرات في الجرائم المعلوماتية، تخصص القانون الدولي الجنائي، قسم الحقوق و العلوم السياسية، الاغواط، 2021/2019.
-جميل حسين طويلة، البرمجيات الخبيثة: دليل عملي لاستخدام البرمجيات الخبيثة وبرمجيات التجسس وطرق الوقاية والحماية منها، كتاب إلكتروني، الأمن السيبراني، مصر، 2015.
-صبري السعدي، شرح القانون المدني الجزائري – النظرية العامة للالتزامات (مصادر الالتزام: الواقعة القانونية والتصرف القانوني)، دار الهدى للطباعة والنشر والتوزيع، عين مليلة، الجزائر، الطبعة الثانية،
-د. مجدوب نوال ود. طالب محمد كريم، الطبعة الأولى، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، برلين – ألمانيا، دون سنة النشر.
-الدكتورة بشرى حسين الحمداني، القرصنة الالكترونية، أسلحة الحرب الحديثة، الطبعة الأولى دار أسامة للنشر و التوزيع، 2014.
-الدكتورة بشرى حسين الحمداني، القرصنة الالكترونية، أسلحة الحرب الحديثة، الطبعة الأولى دار أسامة للنشر و التوزيع، 2014.

-علي أبو الفتح أحمد شتا، تطوير أدوات الرقابة الداخلية لهدف حماية البيانات المعدة إلكترونيا، دراسة مقارنة، جامعة القاهرة.

- فرحاوي عبد العزيز، المسؤولية الجزائية للشخص المعنوي في التشريع الجزائري، مجلة الأدب و العلوم الاجتماعية، جامعة سطيف2، المجلد 16.، العدد2،سنة 2019

_ حذيفة بن حسين القحطاني مسؤول إفتاء محافظة صلاح الدين، الجرائم الالكترونية، الأحكام و الضوابط، العراق، 2025.

-فيصل سعيد الغريب، التوقيع الالكتروني وحجيته في الإثبات المنظمة العربية للتنمية الإدارية، بحوث ودراسات،2005.

-محمد عبد لله القحطاني، خالد سليمان عبد الله ، أمن المعلومات بلغة ميسرة، الطبعة، الأولى، الرياض، 2009.

-محمد مرياتي، أمن تقنية المعلومات: نصائح من الخبراء، مدينة الملك عبد العزيز للعلوم والتقنية، الرياض، دون تاريخ نشر.

-مدحت محمد محمود عبد العال، المسؤولية المدنية الناشئة عن تقديم خدمة التوقيع الالكتروني، الطبعة الأولى، المركز القومي للإصدارات القانونية، مصر، 2010.

- نجاد البرعي، محامي بالنقض، جرائم الصحافة و النشر، القاهرة، مصر، سنة .2004

-محمد فواز المطالقة، الوجيز في العقود والتجارة الإلكترونية، دار الثقافة للنشر والتوزيع، عمّان، الأردن، الطبعه الأولى، 2010.

مقالات

_ أبو عرابي غازي، فياض القضاة، حجية التوقيع الالكتروني، دراسة في التشريع الأردني، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد العشرون، العدد الأول،2004.

1. أسامة علي إبراهيم الصمادي، التوقيع الإلكتروني وحجيته في القانون الأردني، مجلة العلوم الإنسانية والطبيعية، 2023.
2. بن لشهب أسماء، حماية البيانات الشخصية للمستخدم في إطار عقود الحوسبة السحابية كلية الحقوق جامعة الإخوة متنوري – قسنطينة –1–، المجلد التاسع،العدد الأول مجلة الفكر القانوني والسياس،2025.
3. خلوف حسام، باطلي غنية، الآليات القانونية لحماية المعطيات ذات الطابع الشخصي، مجلة الدراسات القانونية والاقتصادية، المجلد 05،العدد01، جامعه سطيف، 2022.
4. الدكتور طاهر عباسة، جريمة الإرهاب الالكتروني في ضوء أحكام الاتفاقية العربية لمكافحة تقنية الجرائم، مجلة العلوم القانونية و السياسية، المجلد 09، العدد 03، 2018.
5. عبد العزيز، سمية، «التوقيع الإلكتروني وسيلة حديثة للإثبات – دراسة مقارنة»، مجلة معارف، المجلد 9، العدد 17، ديسمبر 2014،
6. شاكر سليمان، الآليات القانونية لحماية الطفل من جرائم الاستغلال الجنسي عبر شبكة الانترنت (دراسة مقارنة)، مجلة حقوق الانسان و الحريات العامة، المجلد08، العدد01، الجزائر 2023.
7. الصغير كاوجة الهجمات السبيرانية بين الواقع وسبل المواجهة مجلة الرسالة للدراسات الإسلامية المجلد 06 / العدد 03 / سبتمبر 2022.
8. عباس حسوني (فاطمة)، عبد كاظم (حمدية)، التوقيع الإلكتروني وحجيته في الإثبات في ظل قانون التجارة الإلكترونية والمعاملات الإلكتروني، رقم 78 لسنة 2012، مجلة رسالة الحقوق، جامعة كربلاء، كلية القانون، العراق السنة الثامنة، العدد الثاني 2016.
9. سلوى عبد الجبار عبد القادر، أثر استخدام التوقيع الرقمي في العمليات المصرفية الإلكترونية، مجلة دراسات محاسبية ومالية، المجلد 8، العدد 22، معهد الدراسات المحاسبية والمالية، جامعة بغداد، العراق، 31 مارس 2013،

10. عبد الكريم زنتوت، الجريمة الإلكترونية وسبل مواجهتها في الجزائر ، المجلد 13،العدد 1، سنة2025.
11. عقوني محمد ، الآليات القانونية والتقنية لحماية التوقيع الالكتروني ، مجلة الفكر ، العدد ،18 ، جامعة محمد خيضر ، بسكرة ، 2019.
12. قارة مولود، التوثيق الإلكتروني: شكله وإجراءاته، مجلة الأستاذ الباحث للدراسات القانونية و السياسية، المجلد 6، العدد 3، جامعة ابن خلدون, تيارت، الجزائر، 25 جانفي2022
13. قدايفة أمينة، استراتيجية أمن المعلومات، مجلة أبعاد اقتصادية، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة أمحمد بوقرة بومرداس، الجزائر، المجلد6, العدد 1، **2016**.
14. كرار غانم بستان1، الأستاذة الدكتورة/أودين سلوم1، الوسائل الالكترونية للتثبت من الأهلية ودورها في حماية المتعاقد الإلكتروني، مجلة العلوم الإنسانية والطبيعية، 2025.
15. كمال درواز، الحماية القانونية للأرشيف في التشريع الجزائري، مجلة المكتبات والمعلومات، جامعة منتوري قسنطينة 2، معهد علم المكتبات والتوثيق، المجلد 2، العدد 1، ديسمبر
16. محمد فواز المطالقة، الوجيز في العقود والتجارة الإلكترونية، دار الثقافة للنشر و التوزيع، عمّان، الأردن، الطبعه الأولى، 2010
17. يحيى عبد الناصر العباسي، مشروع تخرج في هندسة الشبكات، كلية الهندسة، جامعة قرطبة الخاصة، فرع القامشلي، 2023.
18. رضوان علي، رزق الله العربي، بن مهيدي، المكافحة المؤسساتية للجريمة الإلكترونية في التشريع الجزائري، المجلة الأكاديمية للبحوث القانونيه والسياسي المجلد09، العدد02 سنه 2025.

الرسائل:

1. حاجة عبد العالي، الآليات القانونية لمكافحة الفساد في الجزائر، أطروحة لنيل شهادة الدكتوراه علوم في الحقوق تخصص قانون عام، سنة 2013/2012.

2. لبيض فايزة، عقد التجارة الالكترونية من حيث الإبرام والإثبات، جامعة قسنطينة، الإخوة منتوري، كلية الحقوق قسم القانون الخاص، أطروحة لنيل شهادة دكتوراه علوم في القانون تخصص قانون الأعمال،2024/2023،
3. محمد مأمون أحمد سليمان، التحكيم في منازعات التجارة الالكترونية، رسالة دكتوراه في الحقوق، كلية الحقوق جامعة عين شمس، مصر، 2009.
4. نور خالد عبد المحسن العبد الرزاق، حجية المحررات والتوقيع الالكتروني في الإثبات عبر شبكة الانترنت، رسالة دكتوراه في الحقوق كلية الحقوق جامعة عين شمس، مصر، 2009.
5. حسن هادي لذيذ، ماجستير حاسبات، مبادئ وأساسيات الحاسب الآلي وتكنولوجيا المعلومات، العراق. سنه2014.
6. إيهاب سمير محمد صالح الإثبات بالمحررات الالكترونية دراسة مقارنة رسالة ماجستير في القانون الخاص كلية الحقوق جامعة الأزهر، غزة، فلسطين،2015.
7. نور أمير الموصلي، الهجمات السبيرانية في ضوء القانون الدولي الإنساني بحث مقدم استكمالاً لمتطلبات نيل درجة ماجستير التأهيل والتخصص في القانون الدولي الإنساني الجامعة الافتراضية السورية ماجستير التأهيل والتخصص في القانون الدولي الإنساني ، 2021.

المطبوعات

-خديجة عبد اللاوي، أستاذ محاضر قسم "أ"، محاضرات في قانون المعاملات الالكترونية، مطبوعة بيداغوجية موجهة لطالبة السنة أولى ماستر تخصص قانون خاص،2022/2021،

-د. بو سبعين تسعديت، محاضرات في نظام الرقابة الداخلية، مطبوعة موجهة لطلبة السنة الثالثة في العلوم المالية والمحاسبة، 2019_2020.



ملخص البحث

الملخص

لقد شهد العالم تحوّلًا متسارعًا نحو الرقمنة، حيث أصبحت الإدارة الإلكترونية أحد الركائز الأساسية لتحديث المرافق العامة وتحسين جودة الخدمات المقدّمة للمواطنين. وفي هذا السياق، برزت المعاملات الإدارية الإلكترونية كآلية فعّالة لتبسيط الإجراءات وتحقيق الشفافية والسرعة في الأداء الإداري. غير أنّ هذا التحوّل الرقمي، رغم ما يتيحه من مزايا، يطرح تحديات قانونية متزايدة، خاصة في ما يتعلق بحماية البيانات وضمان سلامة المعاملات من مختلف المخاطر الإلكترونية.

وعليه، يكتسي موضوع تأمين المعاملات الإدارية الإلكترونية أهمية بالغة، باعتباره يشكّل حجر الزاوية في بناء الثقة في البيئة الرقمية. إذ يتطلب هذا التأمين تبنّي منظومة متكاملة تجمع بين الحماية الإدارية من خلال وضع سياسات تنظيمية فعّالة، والحماية الجزائية عبر تجريم الأفعال الماسة بأمن الأنظمة المعلوماتية، إضافة إلى توفير إطار قانوني يضفي الشرعية والحجية على المعاملات الإلكترونية، خاصة من خلال تنظيم التوقيع والتصديق الإلكترونيين. كما لا يمكن إغفال الدور المحوري للأمن السبيراني باعتباره الجانب التقني الذي يهدف إلى حماية البنى التحتية الرقمية من الاختراقات والهجمات المختلفة.

وفي ظل تزايد الجرائم الإلكترونية وتنوع أشكالها، من اختراق الأنظمة إلى الاحتيال وسرقة الهوية الرقمية، أصبح من الضروري اعتماد استراتيجيات متعددة الأبعاد لمكافحتها، ترتكز على تضافر الجهود القانونية والتقنية والإدارية، إلى جانب تعزيز الوعي الرقمي لدى المستخدمين. و من هذا المنطلق، يسعى هذا الموضوع إلى إبراز مختلف الآليات والوسائل اللازمة لتأمين المعاملات الإدارية الإلكترونية، وتحليل أبعادها القانونية والتقنية، بما يساهم في تحقيق إدارة إلكترونية آمنة وفعّالة.

الكلمات المفتاحيَّة

تامين المعاملات الإدارية – الأمن الالكتروني – الإدارة الالكترونية

ABSTRACT

The world has witnessed an accelerated transformation towards digitalization، where electronic administration has become one of the fundamental pillars for modernizing public facilities and improving the quality of services provided to citizens. In this context، electronic administrative transactions have emerged as an effective mechanism for simplifying procedures and achieving transparency and speed in administrative performance. However، this digital transformation، despite the advantages it offers، raises increasing legal challenges، especially with regard to data protection and ensuring the safety of transactions from various electronic risks.

Accordingly، the subject of securing electronic administrative transactions acquires great importance، as it constitutes the cornerstone in building trust in the digital environment. This security requires the adoption of an integrated system that combines administrative protection through the establishment of effective regulatory policies، and penal protection through the criminalization of acts affecting the security of information systems، in addition to providing a legal framework that grants legitimacy and evidentiary value to electronic transactions، especially through the regulation of electronic signature and electronic certification. The pivotal role of cyber security also cannot be overlooked، as it represents the technical aspect aimed at protecting digital infrastructures from breaches and various attacks.

In light of the increasing cybercrimes and the diversity of their forms، from system breaches to fraud and digital identity theft، it has become necessary to adopt multidimensional strategies to combat them، based on the combined efforts of legal، technical، and administrative measures، alongside enhancing digital awareness among users. From this standpoint، this topic seeks to highlight the various mechanisms and means necessary for securing electronic administrative transactions، and to analyze their legal and technical dimensions، in a way that contributes to achieving a secure and effective electronic administration.

Keywords
Administrative Transaction Security – Cyber security –Electronic Administratio