وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جامعة عبد الحميد بن باديس – مستغانم

كلية الحقوق والعلوم السياسية

قسم: القانون الخاص

المرجع:.....

مذكرة نهاية دراسة لنيل شهادة ماستر

حماية و إدارة الخدمات الرقمية في المؤسسات الاقتصادية

ميدان: الحقوق والعلوم السياسية

الشعبة: الحقوق

التخصص: القانون الخاص

من إعداد الطالبة:

– ولد يوسف منال ياسمين

تحت إشراف الأستاذ:

– مشنف محمد

لجنة المناقشة

الأستاذة الدكتورة قايد حفيظ	.....	رئيسا
الأستاذ الدكتور مشنف محمد	.....	مشرفا مقررا
الأستاذ الدكتور زواتين خالد	.....	مناقشا

السنة الجامعية: 2026/2025

نوقشت في:01 جويلية 2026

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي و البحث العلمي
جامعة عبد الحميد بن باديس-مستغانم

UNIVERSITE
Abdelhamid Ibn Badis
MOSTAGANEM

كلية الحقوق و العلوم السياسية

مصلحة التربصات

حررت هذه الوثيقة
من طرف العون
عايد عايدة إيناس

تصريح شرفي خاص بالالتزام بقواعد النزاهة العلمية
في إنجاز البحث

أنا الممضي أدناه , الطالب (ة) :

اللقب : ولد يوسف الإسم : منال ياسمين

الحامل(ة) لبطاقة التعريف الوطنية رقم 1100307890216500 6 والصادرة بتاريخ: 2023.04.25 .

المسجل(ة) بكلية: الحقوق و العلوم السياسية قسم: القانون الخاص

والمكلف(ة) بإنجاز مذكرة ماستر بعنوان:

حماية و إدارة الخدمات الرقمية في المؤسسات الاقتصادية

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

التاريخ: 1 جويلية 2026 .

إمضاء المعني

بلدية مستغانم
نظرا للتصديق المادي لإمضاء
رئيس المجلس الشعبي البلدي
و بالتفويض منه
إمضاء: عزيزة حفيظ عفيف
07 JUIL. 2026

* ملحق القرار الوزاري رقم 933 المؤرخ في 28 جويلية 2016 الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية و مكافحتها.



﴿وَمِنْهُم مَّن يَقُولُ رَبَّنَا آتِنَا فِي الدُّنْيَا حَسَنَةً وَفِي الآخِرَةِ حَسَنَةً وَقِنَا عَذَابَ النَّارِ﴾. الآية 201 من سورة البقرة

إهداء

اهدي ثمرة تعبي

إلى من كانت تحيطني دعواتها و يشجعني حبها، التي من تدير شؤوني بحرص و بدون تعب

" أمي الغالية "

إلى ضلعي الثابت، و فخري الذي أسمو به، و الذي لا يمل من تحقيق متطلباتي

" أبي الغالي "

إلى أخي الأكبر" عبد الله " و أخي الأصغر " أكرم " و إلى أختي الداعمة " شيماء " حفظهم الله و رعاهم من كل سوء

إلى جميع صديقاتي و رفيقات دربي كل باسمها

اهدي هذا الجهد المتواضع إلى كل من يريد أن يستعين أو يبحث للارتقاء بالعلم.

شكر و تقدير

" الحمد لله الذي بفضله و توفيقه تم انجاز هذا العمل، فله الحمد ظاهرا و باطنا."

أتقدم بجزيل الشكر و خالص الامتنان إلى الأستاذ الفضيل : مشنف محمد، على قبوله الإشراف على هذه المذكرة، و تقديم يد العون و الإرشادات بما يفيدني، و على تواضعه و حسن المعاملة، و كان لصبره و سعة صدره الأثر الكبير في إتمام هذا البحث، دمت فخرا لكلية الحقوق و العلوم السياسية.

وأتوجه بجزيل الشكر و الامتنان إلى السادة أعضاء لجنة المناقشة المحترمين، لتكرمهم بمناقشة هذه المذكرة وتطوير هذا العمل وإثرائه، أسأل الله أن يجزيهم خير الجزاء وأن يوفقهم في مسيرتهم العلمية.

مقدمة

شهد العالم في الآونة الأخيرة تطورا متسارعا في مجال التكنولوجيا أدى إلى ظهور ما يدعى بالاقتصاد الرقمي، و قد ساهمت الرقمنة في إحداث تغييرات جوهرية على الخدمات التقليدية التي تقدمها المؤسسات الاقتصادية من خلال تطوير أساليب الإدارة تماشيا مع التحول الذي مس مختلف جوانب الاقتصاد، الأمر الذي أدى إلى بروز مصطلح الخدمات الرقمية.

و هذه الخدمات الحديثة تعد محركا اساسيا لتعزيز الكفاءة التشغيلية و عصرنة تجربة العملاء و تسريع العمليات المالية، بالاعتماد على تقنيات الذكاء الاصطناعي و مختلف التطبيقات و الأنظمة الالكترونية. و في ظل الانتشار الواسع للخدمات الرقمية، ظهرت الحاجة إلى توفير آليات فعالة لحمايتها و إدارتها بما يضمن امن المعلومات و دوام النشاط الاقتصادي.

و تكتسي حماية الخدمات الرقمية أهمية بالغة نسبة للمخاطر التي تصادفها المؤسسات الاقتصادية، كالتهديدات السيبيرانية و اختراق المعلومات المخزنة و غيرها من الجرائم الالكترونية، الأمر الذي ألزم مختلف التشريعات الوطنية منها و العالمية إلى وضع قواعد تنظيمية لتاطير حماية المعاملات الرقمية و تكريس الأمن داخل المؤسسات. فنجاح المؤسسات اليوم لم يعد مرتبطا فقط بالإمكانيات المادية، بل أصبح مرتبطا كذلك بالجوانب التقنية و حدود قدرة المؤسسة على إدماج التحول الرقمي في إدارة خدماتها الالكترونية بكفاءة.

و من خلال ما سبق تبرز أهمية الموضوع في كونه من المواضيع الراهنة التي تجمع بين الجوانب القانونية و التقنية و الإدارية، و لكونه يعالج أهم التحولات المعاصرة و هو التوجه نحو الرقمنة في ظل المنافسة الاقتصادية للمؤسسات.

أسباب اختيار الموضوع

الأسباب التي دفعتني للبحث في الموضوع، منها ذاتية تتعلق برغبتي الخاصة للتعمق في حيثياته كونه يتماشى مع متطلبات العصر، و منها أسباب موضوعية تتمثل في :

- البحث عن مدى فعالية هذه الحماية الرقمية في الوسط الاقتصادي.
- الرغبة في إبراز الإطار القانوني المنظم للخدمات الرقمية.
- يتميز هذا الموضوع بارتباطه مع عدة مجالات كالقانون الرقمي و التجارة الالكترونية، مما يجعله موضوعا حيويا غنيا بالدراسة.
- لاستكمال حلقة البحوث و الدراسات الخاصة بهذا الموضوع .

إشكالية البحث :

و لمعرفة التأطير القانوني للخدمات الرقمية و وسائل حمايتها نطرح الإشكال التالي :

" إلى أي مدى يساهم الإطار القانوني و التنظيمي في حماية و إدارة الخدمات الرقمية داخل المؤسسة الاقتصادية؟.

الصعوبات

هناك صعوبات واجهتنا أثناء تحرير الموضوع و هي كالأتي :

- عدم التفرغ و التأجيل المستمر بسبب الخوف من عدم المثالية.
- ضيق و قلة الوقت.
- صعوبة العثور على كتب كلاسيكية لحداثة الموضوع.

المنهج المتبع

للإجابة عن الإشكالية المطروحة :

اعتمدنا على منهجين اعتمدنا على المنهج الوصفي و المنهج التحليلي، من خلال وصف الظاهرة، حيث حاولنا وصف الأجزاء النظرية المتعلقة بموضوعات إدارة و حماية الخدمات الرقمية ، كما سهل لنا هذا المنهج ضبط مبتغيات الدراسة استعانة بالأدبيات النظرية والدراسات السابقة في الموضوع، و كذا استعمال المنهج التحليلي بالتطرق إلى تحليل النصوص القانوني المتعلقة بالحماية الالكترونية و تقدير فعاليتها على المؤسسات الاقتصادية.

خطة البحث :

حيث قسمنا موضوع بحثنا إلى فصلين، الفصل الأول بعنوان الإطار القانوني لحماية للخدمات الرقمية في المؤسسات الاقتصادية و الذي تطرقنا فيه إلى مفهوم الخدمات الرقمية و دورها في المؤسسات الاقتصادية كمبحث أول أما المبحث الثاني كان بعنوان الأطر القانونية المنظمة لحماية الخدمات الرقمية.

أما الفصل الثاني تطرقنا فيه إلى آليات حماية وإدارة الخدمات الرقمية داخل المؤسسة الاقتصادية، الآليات التقنية والتنظيمية للحماية الرقمية و الذي تناولنا فيه كمبحث أول، و كمبحث ثاني إدارة المخاطر الرقمية و الحوكمة الالكترونية في المؤسسة الاقتصادية .

الفصل الأول :
الإطار القانوني لحماية الخدمات الرقمية في المؤسسات الاقتصادية

الفصل الأول : الإطار القانوني لحماية الخدمات الرقمية في المؤسسات الاقتصادية

تعد الخدمات الرقمية نتيجة من نتائج التحول الرقمي أي إعادة تشكيل وسائل تقديم الخدمات التقليدية و تحويلها إلى خدمات رقمية بالاعتماد على تكنولوجيا الإعلام و الاتصال . و مس هذا التحول مختلف القطاعات خاصة القطاع العام ذلك عبر تقديم أجود الخدمات و تبسيط إجراءاتها. و يقتضي فهم الخدمات الرقمية تناول الإطار ألمفاهيمي لها أولا في المبحث الأول ثم تخصيص المبحث الثاني للإطار القانوني و تنظيمها.

المبحث الأول : مفهوم الخدمات الرقمية و دورها في المؤسسة الاقتصادية

سيتكلف هذا المبحث بعرض مفهوم الخدمة الرقمية بمميزاتها في المؤسسة الاقتصادية ومختلف أنواعها في المطلب الأول، لنعرج بعدها إلى إبراز أهميتها في المطلب الثاني.

المطلب الأول : ماهية الخدمات الرقمية

لإثراء مفهوم الخدمات الرقمية في هذا المطلب، سنتطرق إلى التعريفات المختلفة للخدمة الرقمية و عناوين فرعية أخرى تغطي جوانب المصطلح من خصائصه و أنواعه.

الفرع الأول : تعريف الخدمات الرقمية

مؤخرا استحدثت بعض العمليات الالكترونية في البيئة الاقتصادية كالدفع الالكتروني و الخدمات البنكية عبر التطبيقات و غيرها من العمليات التي كانت في الأصل خدمات عمومية حضورية في المؤسسات الاقتصادية على أساس أنها تعرف بتلك الرابطة التي تجمع بين الإدارة العامة والمواطنين على مستوى تلبية الرغبات، فأصبحت هده الخدمات تقدم عن بعد دون الحاجة إلى الحضور المادي .

التعريف اللغوي

1 الخدمة : مشتقة من الفعل خدم و يقال خدمه خدمة أي قام بحاجته. و في المعاجم العربية، الخدمة هي العمل النافع لفائدة الغير بدون مقابل أو بمقابل، و تعني المساعدة أيضا.[1]

[1] ابن منظور، أبو الفضل جمال الدين محمد بن مكرم، لسان العرب، دار صادر، بيروت، ط3، 1414 هـ، جـ 12، ص 166.

2 الرقمية : نسبة إلى الرقم، و في المعجم الوسيط تدل إلى العلامة الحسابية. لكن في السياق المعلوماتي نقصد بالرقمية تحويل المعلومات إلى لغة الأرقام التي تفهمها أجهزة الحاسوب.[1]

فيمكن تعريف الخدمة الرقمية بأنها كل نشاط يقدم عن بعد يعتمد على معالجة البيانات و تبادلها الكترونيا عبر الشبكات الرقمية لمصلحة المستفيد.

وتشير الخدمة الرقمية بشكل خاص إلى الخدمات التي تستخدم التكنولوجيا الرقمية، وهذا يعني أن المعلومات يتم تخزينها ونقلها ومعالجتها على شكل تسلسل من الأرقام الثنائية ، تستفيد الخدمات الرقمية من الإنترنت والحوسبة السحابية والتقنيات المتقدمة الأخرى لتوفير الخدمات مثل الخدمات المصرفية عبر الإنترنت والتجارة الإلكترونية والبث ووسائل التواصل الاجتماعي.

كما وتشير أيضاً الخدمات الرقمية إلى الخدمات التي تستخدم التكنولوجيا الرقمية على وجه التحديد ، والتي تتضمن تمثيل البيانات ومعالجتها بتنسيق ثنائي (0 و 1)، وغالبًا ما تكون .هذه الخدمات قائمة على الإنترنت أو تعتمد على شبكات الكمبيوتر لتقديمها.

و قد عرفتها منظمة التعاون الاقتصادي و التنمية OECD بشكل غير جامد و في إطار أوسع هو الاقتصاد الرقمي المتضمن للخدمات الرقمية الذي يعتبر جزء منها، بأنه كل نشاط اقتصادي يتعزز باستخدام المدخلات الرقمية في خلق القيمة الاقتصادية.[2]

و بناءا على اتحاد الجامعات الأوروبية EUA، يصاغ التعريف الإجرائي بأنه : التحول الجذري في طريقة تقديم الخدمة العمومية و الوظيفة من الصيغة التقليدية (الورقية او الحضورية) إلى صيغة مستحدثة تعتمد كليا على تكنولوجيا المعلومات، فليست مجرد برنامج بل إعادة تصميم للعملية الإدارية لتصبح خدمة فورية، من خلال واجهة المستخدم التي تعتبر نقطة الالتقاء بين المستخدم و البنية التحتية التقنية للمؤسسة. لكي تسمح في الأخير للبيانات بالانتقال بسلاسة بين الأنظمة المختلفة دون انقطاع.[3]

و رغم تعدد التعريفات المقارنة له، في تشريعات الاتحاد الأوروبي و في الفقه القانوني و في التشريع الجزائري، إضافة إلى منظمة التعاون الاقتصادي و التنمية المذكورة سابقا، إلا انه هناك تقارب في الجوهر بحيث جميعها تتفق على كون الخدمات الرقمية أساسها التكنولوجيا و تقدم عن بعد. غير أن الاختلاف يكون في زاوية المعالجة، إذ يهتم الاتحاد الأوروبي بالإطار التنظيمي و البيئة الرقمية، بينما يهتم الفقه بالطبيعة القانونية و المميزات النظرية لها.[4]

---

[2]OECD.(2019).Digital Economy Outlook. Paris : OECD Publishing.

[3] European University Association (EUA), « Digital Architecture and Digital Services, »

[4] Hand book on measuring digital Platform employementanl Work, 2023 , منظمة التعاون الاقتصادي و التنمية

دوافع التحول إلى الخدمات الرقمية :

–التطور التكنولوجي السريع.

– تزايد عدد لمستخدمين للإنترنت والهواتف الذكية.

– الحاجة إلى السرعة والدقة وتقليل التكاليف.

– تحسين الشفافية ومكافحة البيروقراطية.

– الاستجابة للأزمات مثل جائحة كوفيد-19.

مراحل الانتقال من الخدمة التقليدية إلى الرقمية:

-(01) رقمنة الوثائق : تحويل الملفات الورقية إلى إلكترونية.

-(02) أتمتة الإجراءات: استخدام الأنظمة المعلوماتية لتقليل التدخل البشري.

-(03) الخدمات الإلكترونية: تقديم الخدمة عبر مواقع ومنصات رقمية.

-(04) الخدمات الذكية :دمج الذكاء الاصطناعي وتحليل البيانات تحسين التجربة.

يمثل التحول من الخدمات التقليدية إلى الخدمات الرقمية ضرورة استراتيجية وليس خيارًا، لما له من دور في تحسين الأداء الإداري، تعزيز الثقة بين المواطن والمؤسسة، ودعم التنمية الاقتصادية والاجتماعية. غير أن نجاح هذا التحول يتطلب رؤية شاملة، إطارًا قانونيًا واضحًا، واستثمارًا مستدامًا في الإنسان والتكنولوجيا[1].

[1] البديل، الخدمات من الشكل التقليدي الى الشكل الرقمي، بتاريخ 18يونيو2026، سا 5.51، https:// elbadilabc-ar.dz.

الفرع الثاني : خصائص الخدمات الرقمية في المؤسسات الاقتصادية

إحدى ابرز الخصائص التي تتميز بها الخدمات الحديثة ما يلي :

- الاستغناء الكامل عن الأوراق أو الحد الجزئي منها و بالتالي تتميز بعدم الملموسية و بعدم الاتصال المباشر بين أطراف الخدمة، مما يعزز الشفافية ومكافحة الفساد الإداري في المؤسسات الاقتصادية، و بالتالي يحد من من التلاعب و الاحتيال، عبر استخدام التقنيات الحديثة مثل الذكاء الاصطناعي.

- لا تحدها أي قيود جغرافية، وهذا يؤدي إلى تطوير الشمول المالي، حيث يتيح للأفراد و خاصة في المناطق النائية، التي توفر لهم البنوك الرقمية مثلا حلولا مرنة بواسطة الدفع الالكتروني، فتساعد كلا من الأفراد و المؤسسات على إجراء المعاملات المالية بسرعة و أمان، و عليه دمج المزيد من الأشخاص في الاقتصاد الرقمي و زيادة النمو الاقتصادي.

- الاعتماد على الوسائل التقنية في تقديم الخدمات مثل الذكاء الاصطناعي و غيرها من الخدمات الذكية، مما يحقق كفاءة اكبر في استغلال الموارد، من خلال رقمنة الخدمات، يمكن للشركات و المؤسسات تقليل استهلاك الورق و الطاقة، مما ينعكس إيجابا على البيئة و يساهم في تحقيق الهدف المتعلق بالحفاظ على الموارد الطبيعية.

- جودة الخدمات الالكترونية المقدمة للمستفدين منها .

- تمكين المؤسسات الاقتصادية من تبادل المعلومات فيما بينها لتخفيف الأعباء و كذلك سهولة الاستعمال و الإتاحة للجميع في أي وقت .

- الطابع الديناميكي المرونة، و التكيف مع التطورات و التغيرات الماسة بقطاع الاقتصاد أي تطوير العمليات الاقتصادية عن طريق توفير البيانات و المعلومات و ربطها بمراكز اتخاذ القرار من خلال استخدام تقنية المعلومات.

- السرعة و الفورية في تلبية الحاجيات العامة.

- تقدم الخدمات بشكل آلي دون تدخل بشري مباشر كالردود الآلية و المعالجة التلقائية للطلبات.

- سرية البيانات و سلامتها من خلال اعتمادها نظام الأمن السيبيراني.

- باعتبار المؤسسات الاقتصادية مرافق عامة فمبدأ الاستمرارية يتجلى بشكل كبير من خلال الخدمات الرقمية التي تقدم بشكل مستمر 24 /7 تقريبا بخلاف الخدمات العمومية التقليدية.[1]

- من المعروف ان التطور التكنولوجي سريع و لا نهاية له، حيث انه مستمر، لهذا يجب ان يكون التحول الرقمي للخدمات مستمر أيضا. فيجعل المؤسسات في حالة تأهب دائم لمواكبة التطورات العلمية الحديثة.

- تمتاز الخدمات الرقمية كذلك بعدم السرعة أثناء اختيار الأدوات و البرامج المناسبة لنشاط العمل لان تطبيق التحول الرقمي ياخد وقت أطول. بالإضافة إلى أن التدريب على استخدام هذه الأدوات بفعالية يحتاج وقت كذلك لتدريب الموظفين.

الفرع الثالث : أنواع الخدمات الرقمية

تتعدد أصناف الخدمات الرقمية باختلاف المعيار المعتمد، ليتم تقسيمها على حسب المجال تم على حسب طبيعة الخدمة، و على حسب التكنولوجيا المستخدمة

أنواعها على حسب المجال

أولا : الخدمات الرقمية المالية

تعد من ابرز مظاهر التحول الرقمي في القطاع المالي، و هي مجموعة من الحلول المبتكرة لتمكين المستفيد من إدارة حساباته و إجراء المدفوعات مع الاستفادة من التكنولوجيا المتطورة سواء للتعاملات اليومية أو الاستشارات المالية أو التحويلات الدولية، و على اثر هده الأخيرة بلغت قيمة سوق التكنولوجيا المالية العالمية ما يقارب 340 مليار دولار في عام 2024، من المتوقع أن ترتفع إلى اكتر من 394 مليار دولار عام 2026 قبل أن تقفز إلى حوالي 1.13 تريليون دولار بحلول عام 2032، استنادا إلى تحليلات و تقارير صادرة عن مؤسسات دولية و شركات بحثية موثوقة .[2]

و تتمثل الخدمات المالية الرقمية في إدارة الحسابات المالية ، دلك بعد إنشاء حساب مالي بواسطة الموقع الالكتروني الخاص بالمؤسسة لفائدة المستفيد بعد تقديمه للوثائق المطلوبة، إضافة إلى خدمة فتح الحساب توفر هده الخدمات أيضا ميزة الاستعلام عن الحساب للاطلاع على المعاملات و الرصيد الحالي مع إتاحة استلام تنبيهات بالبريد الالكتروني أو رسائل نصية

[1] عبدلي نزار و آخرون. دور الإدارة الرقمية في تحسين الخدمة العمومية، مؤتمر الإدارة الرقمية،2023 .

[2] https://www.aljazeera.net ,h15.55,le 20avril2026.

2 https://education-financiere.bcm.mr Banque Centrale de Mauritanie,h 17.22 ,le 20 avril 2026.

لمتابعة وضعه المالي، كما تتيح الخدمات المالية الرقمية إدارة الحسابات المالية عن طريق تلقي الشكاوى من الأخطاء التقنية و تسويتها. [1]

أنواعها على حسب طبيعة الخدمة

الخدمات الرقمية المعلوماتية :

تكمن في توفير المعلومات الجاهزة بطرق متقدمة بعد تحليلها وتنظيمها و تخزينها و إدخالها ثم تحويلها إلى صيغ رقمية،فقط دون تنفيذ أنشطة فعلية، كالمواقع الإخبارية والمنصات التعريفية بالخدمات التي بدورها تحتاج إلى التحديث المستمر للبيانات.
فهذا النوع من الخدمات يشكل البنية التحتية التي تسمح بالقيام بالنشاطات التجارية و الحكومية، مثل خدمات مراكز البيانات التي تحيط بالحماية للمعلومات الوطنية و الخاصة. و خدمات الحوسبة السحابية كمنصات الاستضافة الحكومية التي تخزن و تعالج البيانات.[2]

الخدمات الرقمية المعاملاتية :

هي خدمات الكترونية تهدف إلى إتمام معاملة الكترونية، فلا يكتف المستخدم بالحصول على معلومات، بل يقوم بإجراء عمليات كاملة عبر الانترنت كدفع الأموال و إرسال و استقبال البيانات أو استخراج الوثائق اللازمة الإدارية للمؤسسة، و لهذا فهي تحتاج إلى توثيق و امن مرتفع.

الخدمات الرقمية التفاعلية :

تتيح تفاعل لحظي مباشر بين الأطراف أو شبه مباشر، سواء بين المستخدم و المؤسسة الاقتصادية أو بين المؤسسات الاقتصادية فيما بينها لتعزيز المشاركة الرقمية، كحجز التذاكر و الدفع الالكتروني.

من تطبيقات هذا النوع من الخدمات على ارض الواقع نجد منصات التواصل الاجتماعي التي تساعد على الترويج للمنتجات و بالتالي استقطاب المستثمرين و جلب العملاء، من خلال الحملات الإعلانية و التفاعل مع تعليقات المهتمين بالخدمة.

و من التطبيقات خدمة الزبائن الرقمية من خلال التواصل مع العملاء و الإجابة عن الاستفسارات و تقديم الدعم الفني، مما يساهم في تعزيز رضا الزبون.

---

[2] عمر بن يونس، النظام القانوني للمعلوماتية (دراسة في ضوء التشريع الجزائري)، دار الثقافة للنشر و التوزيع، عمان، 2024، ض 88.

إضافة إلى خدمة الاجتماعات و التواصل المهني عن بعد عبر برامج الاجتماعات الافتراضية عن بعد لتقليل الوقت و التكاليف.

خدمة الأنظمة الرقمية التفاعلية لإدارة بيانات العملاء و تطوير الخطط التسويقية من خلال تحليل سلوكهم عبر أنظمة Salesforce و Hubspot.[1]

المطلب الثاني : أهمية الخدمات الرقمية للاقتصاد و المؤسسة

في عالم يتسارع فيه التحول الرقمي، لم تعد هده الأداءات رفاهية تقنية فحسب، بل أصبحت جزءا أساسيا من تفاصيل الحياة اليومية للإفراد التي تسعى المؤسسات الاقتصادية لتلبيتها. و على اثر هدا المطلب سنوضح دور الرقمنة في تحسين الأداء الاقتصادي، ثم التحول الرقمي و الابتكار التنظيمي و أخيرا نوضح أهميتها من خلال الأثر المترتب على تنافسية المؤسسات.

الفرع الأول : دور الرقمنة في تحسين الأداء الاقتصادي

الرقمنة هي رافعة لتحسين مناخ الأعمال و تعزيز شفافية الاقتصاد و ثقة المتعاملين. و على حسب أقوال الخبراء الاقتصاديين منهم عبد النور قاشي، إن الاقتصاد الرقمي لم يعد خيارا ثانويا بل أصبح ضرورة لبناء واحد حديث قادر على التطور و المنافسة ليجعل المهام أكثر مرونة و فعالية.

كما نلاحظ أن الرقمنة فتحت أفاق جديدة خاصة لدى الشباب الموسوم بالابتكار، مما يدعم نمو الاقتصاد الوطني و يساعده على مواكبة التحولات العالمية. ناهيك عن أهمية التنظيم الذي توفره الرقمنة و بالتالي الحد من الفوضى داخل السوق، فضلا عن توحيد قواعد المعاملات بين مختلف المتعاملين، مما يتيح للسلطات العمومية مراقبة حركة السلع و الخدمات داخل السوق الوطنية و ضبط الممارسات الغير قانونية، الأمر الذي ينعكس إيجابا على النشاطات و يجلب المزيد من المستثمرين.[2]

تخلق التكنولوجيا القيمة الاقتصادية من خلال تقليل التكاليف التشغيلية مثل تكاليف الطباعة، التوزيع، مما يزيد من هامش الأرباح.

[1] الخدمات الرقمية و التحول الالكتروني، مجلة الدراسات القانونية، العدد12، 2020.
[2] سا14.33، ب21 افريل2026،https:\\www.echchaab.com

و تظهر أهميتها في البيانات التي أصبحت موردا استراتيجيا يوازي رأس المال، حيث ترتكز الشركات الكبرى مثل Google على تحليل البيانات الضخمة لفهم سلوك المستهلكين و تطوير خدماتها و هدا ما يسهم في خلق قيمة اقتصادية كبيرة.[1]

أدت أهمية الرقمنة مع نمو البيانات الضخمة في العالم من 33زيتابايت، 33 ألف مليون تريليون بايت عام 2018م إلى 175 " زيتابايت" المتوقعة في عام 2025 . م فمثلاً يمكن للمركبات ذاتية القيادة توليد حوالي " 3 زيتابايت" (3 تريليون بايت) من البيانات كل ساعة، غير بيانات تحديد المواقع. وستستمر زيادة حجم البيانات وسرعتها وتنوعها وضجيجها مع تحديث خوارزميات التعرف على الأنماط وتعلّم الآلة ودمجهما في المركبات ذاتية القيادة والمدن الذكية و"إنترنت الأشياء مصطلح يصف التواصل المباشر بين أشياء ذكية عبر الإنترنت مثل تواصل البشر .

ولتصور هذه الضخامة، فسنحتاج إلى 1,8 بليون سنة لتنزيل 175 " زيتا بايت" من البيانات بمتوسط سرعة 25 ميجابت/ثانية، وحاليا يتعامل أكثر من 5 مليار مستهلك مع البيانات يوميا .وبحلول عام 2025م سيصبحون 6 مليار (80 %من سكان العالم ،) وستنمو البيانات في الوقت الحقيقي إلى 30 %من إجمالي البيانات العالمية، وكل 18 ثانية سيتفاعل كل شخص مع البياناتً عام 2010م إلى 5000 تفاعل يوميا وقد ارتفع معدل التفاعلات لكل شخص من حوالي 300 تفاعل يوميا في الوقت الحاضر.

وتستثمر "الرقمنة" في أتمتة الأعمال لترقى إلى ذكاء الإنسان، وبحلول عام 2030م، ستعتمد 70 % على الأقل من تقنيات الذكاء الاصطناعي، كما سيصل آنذاك مستوى الاستيعاب الكلي لتقنيات الذكاء الاصطناعي في الشركات إلى 50%وسيكون حوالي 35 %من الشركات قد استوعبت الذكاء الاصطناعي بالكامل، مقارنة مع 3 % ، وستكون هذه المعدلات في حينها أسرع من الشركات حاليا من استيعاب التقنيات السابقة، مثل "الويب" والجوال وتخزين السحاب، التي استغرقت من 15 إلى 25 عام.

وبعدما كان متوسط مستوى استيعاب الجيل السابق من التقنيات الرقمية نحو 37 % سنة 2017 توقع أن يصل إلى 70 %بحلول .2035 و بالمقارنة، قد يصل الاستيعاب الكامل للذكاء الاصطناعي إلى مستوى استيعاب التقنيات الرقمية الحالي في غضون ثماني سنوات تقريبا 2027. ويتضح من ذلك تفاوت نسبة استيعاب تقنيات الذكاء اصطناعي في الشركات، وإن كانت هناك تقنيات ذكاء اصطناعي أكثر استيعابا من غيرها مثل أتمتة عمليات الروبوت. وحديثا في ابريل 2019م، أصدرت دار النشر "سبرينجر" أول كتاب دونه الذكاء الاصطناعي من دون تدخل بشري[2].

التحديات التي تواجه تبني المؤسسة للخدمات الإلكترونية

[1] world Bank.(2021).Digital Development Report.Washington,DC :Word Bank

[2] https://qafilah.com/العالم-رقمنة/,) vu le 06/06/2020).

بعد أن أجبرت المؤسسات على تبني هذا النوع من الخدمات، أصبحت تواجه تحديات كبيرة حتى تتمكن من تطبيق هذا النوع من الخدمات على أرض الواقع، ومن أهم هذه التحديات نذكر ما يلي:

بما أن التكنولوجيا تتغير بشكل متواصل نحو الأفضل فإن العملاء بحاجة أيضا لأن يكونوا منفتحين من حيث استعدادهم لقبول الأشكال والأنواع الجديدة من التكنولوجيا، إلا أنه من الخطأ الاعتقاد بأن جميع العملاء سيكونون على نفس الدرجة في قبولهم أو استعدادهم لتبني[1] واحتضان كافة الأشكال المتجددة للتكنولوجيا، فهناك عوامل كثيرة قد تمنع البعض من تحقيق التفاعل المثالي المنشود مع التكنولوجيا بأشكالها المختلفة .وهي عوامل يكون مردها إلى ثلاثة عوامل هي:

- عوامل متعلقة بالعملاء نفسهم.
- عوامل متعلقة بالتكنولوجيا نفسها.
- عوامل متعلقة بمزودي الخدمات وصانعي التكنولوجيا أنفسهم.

متطلبات إرساء الرقمنة

مشروع الرقمنة يتطلب الكثير والكثير بالنظر لحداثته وأهميته البالغة بالنسبة للمؤسسات والدول، حتى تتمكن من مواكبة الركب وفرض نفسها، وإلا فمآلها الفشل والاختفاء، ومن بين أهم المتطلبات التي نرى أنها تكتسي أهمية كبيرة لإرساء مشروع الرقمنة (المتطلبات التقنية والمالية، المتطلبات البشرية)، وسنأتي على تفصيلها تباعا.

- المتطلبات التقنية : توافر الوسائل الالكترونية اللازمة للاستفادة من الخدمات التي تقدمها الرقمنة والتي نستطيع بواسطتها التواصل معها ومنها أجهزة الكمبيوتر الشخصية والمحمولة والهاتف الشبكي وغيرها من الأجهزة التي تمكننا من الاتصال بالشبكة العالمية أو الداخلية في البلد وبأسعار معقولة تتيح لمعظم الناس الحصول عليها[2].

- المتطلبات المالية : يعد مشروع الرقمنة من المشاريع الضخمة التي تحتاج إلى أموال طائلة، لكي نضمن له الاستمرار والنجاح وبلوغ الأهداف المنشودة، من تحسين مستوى البنية التحتية، وتوفير الأجهزة اللازمة والبرامج الالكترونية، وتحديثها من وقت لأخر وتدريب العناصر البشرية باستمرار ، لذلك لابد من توفير التمويل الكافي لهذا المشروع.[3]

[1] محمود عبد الفتاح رضوان, الإدارة الالكترونية و تطبيقاتا الوظيفية ،المجموعة العربية للتدريب و النشر، مصر،2021طبعة1 ،ص13.
فداء محمود حامد، الإدارة الإلكترونية، دار البداية ناشرون وموزعون،ط1 عمان، ،2012 ص88. [2]
محمد الصيرفي، الإدارة الالكترونية، دار الفكر الجامعي، ط1 الاسكندرية، ،2006 ص76.[3]

- المتطلبات البشرية : إن التحول نحو تطبيق الرقمنة لا يعني الاستغناء عن العنصر البشري، ولكن يجب توفير العناصر البشرية التي لديها المهارات والقدرات الإدارية، وتتقبل فكرة الرقمنة وتعي أبعادها و أهدافها لكي تستطيع الوفاء بمتطلبات تطبيق الرقمنة والإلمام بأساليب التعامل مع الوسائل التقنية الحديثة، وذلك عن طريق العناية بعمليات الاختيار للكفاءات والتدريب المكثف على تقنية المعلومات كاستقطاب أفضل الأفراد المؤهلين في مجالات نظم المعلومات والبرمجيات، وتحديد الاحتياجات الحالية والمستقبلية من الأفراد المؤهلين في نظم المعلومات والبرمجيات والعمل على الانترنت، والتمكين الإداري للأفراد من أجل إتاحة الفرصة أمامهم للتعامل السريع مع المتغيرات في البيئة التكنولوجيا. [1]

الفرع الثاني : التحول الرقمي و الابتكار التنظيمي

هناك ترابط بين التحول الرقمي و الابتكار داخل المؤسسات دالك بتأثيره على أداءها، فالتحول الرقمي هو العملية التي تطبقها المؤسسة لدمج التكنولوجيا في جميع مجالات الأعمال، مما يمهد الطريق لتبني التقنيات الجديدة بسرعة اكبر مستقبلا. و هدا ما يساعد المؤسسات على مواكبة توقعات العملاء و منافسة السوق بفعالية. أما الابتكار التنظيمي هو إدخال طرق جديدة في إدارة المؤسسة أو تنظيم النشاط بهدف تحسين الكفاءة.

و هناك فرق بين الرقمنة السابق ذكرها و التحول الرقمي، فالرقمنة هي تحويل الشيء إلى رقمي بينما التحول الرقمي هو تغيير طريقة العمل كليا باستخدام الرقمنة، و على العموم فان كلاهما يدخلان في مجال دراسة أهمية الخدمات الحديثة.

في ظل الخدمات الرقمية، يعتبر التحول الرقمي دافع للابتكار التنظيمي و شرط لنجاحه، لأنه لا يمكن تصور نجاح التحولات المتطورة في بيئة غير تنظيمية و جامدة و ثقافتها لا تقبل التغيير. ويساهم التفاعل بينهما في تحسين الإنتاجية، كما يعتبر التحول دافع حتمي للابتكار و بالتالي إعادة هيكلة التنظيم و تغيير أساليب اتخاذ القرارات داخل المؤسسة، يقوم بتعزيز الابتكار المستمر لان البيانات الدقيقة للمؤسسات تتيح اكتشاف الفرص الجديدة بسرعة، فيعد هدا التحول محفزا رئيسيا لها بدلا من الاكتفاء بمبادرات مؤقتة، يساعد التحول الرقمي على دمج الابتكار في ثقافة المؤسسة الاقتصادية و عليه يجعل الموظفون أكثر تأهبا لتوليد أفكار جديدة باستمرار مما يحافظ على مبدأ استمرارية المرافق.

[1] بشير عباس العلاق، التسويق عبر الانترنت، دار المناهج، الأردن، 2003، ص 217

الحصول على ولاء العملاء بتقديم الدعم الفوري و تخصيص الخدمات وفق احتياجاتهم، إضافة إلى حل المشكلات بسرعة و فعالية الذي بدوره يزيد من فرص النجاح التجاري الموسوم بالسرعة و الائتمان.

من الأمثلة العامة الناجحة للتحول الرقمي المرتبط بالابتكار التنظيمي :

أمازون : استعملت الذكاء الاصطناعي لتقديم تجربة شراء مريحة و استثنائية.
أوبر: حولت صناعة النقل بالكامل من خلال تطبيق بسيط يعتمد على البيانات الابتكار المستمر.
تقليل الأخطاء البشرية من خلال اكتشاف الأخطاء و الأعطال التي تصيب المصانع من خلال وسائل الذكاء الاصطناعي.[1]

الفرع الثالث : اثر الخدمات الرقمية على تنافسية المؤسسات.

تعد مسالة تنافسية المؤسسات من المواضيع المستحدثة في الساحة الرقمية و الاقتصادية، لان الخدمات الحديثة هي المتغير الأكثر تأثيرا و له دلالة إحصائية قوية على تحسين التنافسية. فالمنافسة في الاقتصاد الرقمي تشير إلى التفاعل بين المؤسسات التي تقدم هده الخدمات الذكية، حيث تعتمد على الابتكار المشار إليه سابقا و تحليل البيانات و المنصات الالكترونية، لتزويد المستهلك بمنتجات بكفاءة و فعالية مقارنة بالمنافسين المحليين و الأجانب مما يعني نجاحا مستمرا و رفع عوامل الإنتاج كراس مال المؤسسة.
فالمؤسسات التي لا تعتمد الرقمنة تجد نفسها متأخرة أمام منافسين أكثر تطورا.

وعليه فالنظام التنافسي جاء على أنقاض التخلي عن النظام العام التقليدي واعتماد أساليب جديدة تحقق التوازن بين المصالح العامة والمصالح الخاصة ، إضافة إلى التصدي لمختلف القوى التنافسية التي قد تواجهها المؤسسات داخل سوق الأعمال، خاصة المؤسسات الصغيرة والمتوسطة التي تسعى إلى ضمان حماية مكانتها داخل السوق.

ومن ثم يعرف النظام التنافسي بأنه نظام حديث قائم على المنافسة الحرة بين مختلف الشركات والكيانات في السوق، ويتسم بالحرية الاقتصادية نتيجة لتحول الدولة إلى آلية ضابطة وليست متدخلة كما كان عليه الأمر سابقا ، كما يرتكز لنظام التنافسي بالدرجة الأولى على حرية السوق وضمان المنافسة الحرة في مختلف القطاعات الاقتصادية، بهدف توفري بيئة تنافسية للمتدخلين الاقتصاديين في ظل احترام قواعد اللعبة التنافسية .

---

[1] فريق تحرير راينز، التحول الرقميو الابتكار المؤسسي : دليل شامل لبناء مستقبل رقمي متقدم، مدونة راينز الاستشارية,2 ديسمبر2025، بتاريخ الاطلاع 20 يونيو2026، متاح على الرابط: https:// reinsagcy.com

علاقة التحول الرقمي بالنظام التنافسي

يرتبط النظام التنافسي ارتباطا وثيقا بالتحول الرقمي، حيث أن هذا الأخير يعد عامل أساسيا لتحسين القدرة التنافسية لأي قطاع من حيث نوعية الخدمات المقدمة وجودتها، إذ يمكن للمؤسسات الاستفادة من مختلف الابتكارات ي بيئة الأعمال التنافسية بهدف توسيع نطاقها إلى أسواق محلية وعالمية، وكذا تسهيل عمليات التجارة الالكترونية .

وبالرجوع إلى القطاع الاقتصادي الوطني نجد بان أغلب المؤسسات تسعى جاهدة إلى ضمان استقرارها في السوق وتحسين أدائها، حيث قامت بتبني التحول الرقمي و يظهر دلك في تفعيل مبدأ الشفافية والنزاهة من خلال اعتماد التحول الرقمي في مختلف المعاملات الاقتصادية، وهو ما يقلل من فرص مخالفة قواعد المنافسة الحرة داخل الأسواق و يحد من أي ممارسات تمس بالمنافسة كالممارسات التجارية غري المشروعة والممارسات المقيدة للمنافسة.[1]

أسباب الاهتمام بالتنافسية في ظل الخدمات الذكية :

أهمها العولمة و حركة المتغيرات، التي تعود إلى ضخامة و تعدد الفرص في الأسواق الاقتصادية، التي بات الولوج إليها اخف من الماضي بسبب تقنيات المعلومات و الاتصال التي تعتمد عليها الخدمات، و ثراء المعلومات و سهولة تبادلها في الوسائط الرقمية. بالإضافة إلى المستوى لعالي للجودة و السهولة النسبية في دخول منافسين جدد إلى الأسواق.

و من مظاهر المؤسسات الناجحة و المتفوقة في الأسواق، تلك التي تعتمد على التكنولوجيا الرقمية، فينتج عنها ما يلي :

- تحسين تجربة العميل بطريقة سريعة و سهلة مما يكسب المؤسسات ولاءه و رضاءه، من خلال جمع بياناته و استخدام الاستبيانات ليتم الوصول إلى تفضيلاته لتقديم خدمات مناسبة خاصة بدلا من حلول عامة.

- تحسين الكفاءة التشغيلية و الإنقاص من التكاليف، عن طريق تقليل الاعتماد على العمل اليدوي، و عليه تقليل الأخطاء البشرية و تسريع انجاز العمليات فتولد إنتاجية أعلى بتكلفة اقل.

- الاعتماد على النشاطات المرقمنة يوحد البيانات و يقلل التكرار في العمل، إذا تقليل التعب و كسب سرعة في الأداء، بأقل موارد ممكنة.

- تسويق الخدمات الرقمية الذي يجلب العملاء.

[1]. حداد ياسر، دور التحول الرقمي في حماية النظام التنافسي للمؤسسات ،مجلة البحوث في العقود وقانون الأعمال، المجلد 10 ، العدد02، 2025 .

- تساهم الرقمنة في تطوير الموارد البشرية، بتسهيل التدريب لانتقاء الكفاءات و بالتالي رفع جودة الخدمات، و من ثم زيادة القدرة التنافسية للمؤسسة. [1]

اعتماد العديد من المؤسسات على أنظمة المراقبة الالكترونية للأسواق، بغية تتبع أسعار السلع والخدمات المقدمة للمستهلكين مما يدفع الشركات إلى التنافس فيما بينها من أجل تقدمي أفضل العروض، كما تساعد تلك الأنظمة الرقمية المعتمدة من طرف المؤسسات يف الكشف عن أي ممارسات ماسة بالمنافسة أو الاحتكارية.

تبني المؤسسة لنظام قواعد البيانات الضخمة من أجل تسهيل عملية تحليل البيانات المتعلقة بالمؤسسات المنافسة هلا وكذا الأنشطة الاقتصادية.

فرض المؤسسة لرقابة صارمة بواسطة الأنظمة الرقمية المعتمدة، والتي تمكن من مراقبة السوق بشكل دقيق وفعال، وضبط أي مخالفات قد ترتكب من طرف المنافسين و غيرهم من المتدخلين.

[1] عبد الستار العلي، *التحول الرقمي وإدارة التغيير*، دار المسيرة للنشر والتوزيع، عمان، 2021، ص45.

المبحث الثاني : الأطر القانونية المنظمة لحماية الخدمات الرقمية

تعتمد الدول منظومة قانونية متكاملة لوقاية أو تامين الفضاء الالكتروني، و قد شهدت المنظومة تحديثات أساسية لمواكبة الأعمال الرقمية السريعة، وعليه سيتم التطرق في المطلب الأول إلى الحماية القانونية الوطنية لضمان السيادة الرقمية في البلاد، أما في المطلب الثاني نخصصه للأطر الدولية و المعايير المتعلقة بها.

المطلب الأول : القواعد القانونية الوطنية

لحماية البيئة الرقمية في الجزائر، أفرزت الدولة إستراتيجية في ترقية و تامين الخدمات الالكترونية مع مراعاة توفير الحماية القانونية للخصوصيات الشخصية للأفراد.و نقسم هدا المطلب إلى ثلاث أنواع من القواعد القانونية الوطنية المعتمدة في هدا المجال.

الفرع الأول : قانون التجارة الالكترونية.

يعتبر تنظيم التجارة الالكترونية من أهم المواضيع التي تستلزم إحاطتها بالتشريعات و تاطيرها نظرا لانتشارها الكبير في المجتمعات و تداولها، لهدا اقر المشرع الجزائري بموجب القانون رقم 18-05 المتعلق بالتجارة الالكترونية و شروط ممارستها القانونية وحماية المستهلك، و دلك بالشكل الذي يحقق الأمان للأطراف المتعاقدة عبر الانترنت، خصوصا في ظل التسويق التجاري المصحوب بالنصب و الاحتيال.

مزايا التجارة الالكترونية :

- رؤية مجموعات مختلفة من السلع مرتبة على شاشة الحاسوب، و يمكن اقتناءها عن بعد دون الحاجة إلى التنقل إلى المتاجر و بالتالي تخفيض الوقت و التكاليف.

- تمكن التجارة الالكترونية الزبائن من التمتع بها في أي وقت و زمان، فبالنظر إلى المتاجر العادية تغلق وتفتح في أوقات محددة، بينما المتاجر الرقمية خدماتها متواصلة إلا ما كان منها محددا بميعاد طبيعي.

- بالنسبة للأفراد العاملين في المؤسسات، تتيح لهم التجارة الالكترونية فرصة جمع المعلومات من الأسواق و تمكنهم حتى من التعرف على ما تقدمه المؤسسات المنافسة من بمزايا و مواصفات و أسعار.

- تتجاوز الحدود الجغرافية بإمكانية البيع لزبائن في ولايات بعيدة دون الحاجة لفتح فروع هناك.[1]

[1] رابحي جوهر، ياسع فاطمة، *التجارة الإلكترونية في القانون 18-05*، مذكرة ماستر، جامعة مولود معمري تيزي وزو، الجزائر، 2021، ص.15.

- سهولة الوصول للجمهور المهتم بالمبيعات عبر إعلانات التواصل الاجتماعي.

عيوب التجارة الالكترونية :

- لا يستطيع الزبون من معاينة السلع الالكترونية باللمس أو التحسس قبل طلبها،و هدا ما يولد ضعف الثقة الرقمية لان الزبائن يتخوفون من جودة السلع و التعرض للنصب.

- الاستلام ليس بشكل فوري بل الانتظار لبضعة أيام بعد الحجز و الدفع الالكتروني.

- تقيد في الإجراءات لأنه قد يجد البعض صعوبة للامتثال لكل بنود القانون 18-05، إلا أن المشرع الجزائري قلل من أثار هده العيوب ببعض النصوص كما سنرى لاحقا بالتفصيل.

- المشاكل التي تعترض الخدمات الرقمية للتجارة من قرصنة و تشويش قد يؤثر على نشاط المؤسسات.

- رغم تطور شركات التوصيل، إلا أن الوصول إلى المناطق النائية قد يتأخر أو يشوب عيوب في الطرود أثناء النقل.[1]

- صعوبة حجية إثبات المستندات الالكترونية، لاختلاف طبيعتها على المحررات التقليدية.

- الأمية و حاجز اللغة من أصعب العوائق التي تقف في وجه التجارة الالكترونية و ممارستها الصحيحة، فمن الصعب على الدولة الجزائرية إلي يعاني فيها حوالي 7.5م مليون شخص من أمية الحرف أن تتحول بسهولة إلى الاقتصاد الرقمي و تطبق أسلوب التجارة عبر الانترنت.

شروط ممارسة التجارة الالكترونية :

- الشروط الخاصة بالمورد الالكتروني:

- التسجيل في السجل التجاري أو الحرفي أو الصناعات التقليدية لكل شخص طبيعي او معنوي، و مع تقاعس التجار في القيام بهذا الإجراء، قد أعلمت وزارة التجارة

- نشر نشاط التجارة في موقع الكتروني أو صفحة الكترونية بامتداد com.dz,و التأكد من صحته، حسب ما نصت عليه المادة الثامنة من القانون.

- لا يمكن ممارسة نشاط التجارة الالكترونية إلا بعد إيداع اسم النطاق لدى مصالح المركز

[1] مداني، ليلى، محاضرات في التجارة الالكترونية،كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة أبي بكر بلقايد، تلمسان، الجزائر

الوطني للسجل التجاري، و أي شخص يتعرض لعقوبة التعليق لتسجيله في حالة المخالفة. واسم النطاق عرفه المشرع بموجب المادة 6 من نفس القانون على انه "عبارة عن سلسلة أحرف و/أو أرقام مسجلة لدى السجل الوطني لأسماء النطاق و تسمح التعرف و الولوج إلى الموقع الالكتروني".و الهيئة المختصة بتسجيل اسم النطاق هي مركز أسماء النطاقات.

- تزويد المستهلك بكل المعلومات الكافية حول شخصيه و عنوانه المادي و الالكتروني والخصائص الأساسية للمنتجات و الخدمات و غيرها.

- احترام القوانين التجارية العامة مثل الالتزام بقواعد المنافسة، و حماية المستهلك و عدم ممارسة الغش و التضليل.[1]

- الشروط المتعلقة بالعقد الالكتروني :

- يجب أن تكون كل معاملة تجارية الكترونية مسبوقة بعرض تجاري الكتروني و أن توثق بموجب عقد الكتروني الذي يتم إبرامه عن بعد دون الحضور المادي لأطراف هو يصادق عليه المستهلك.

- توافر الإيجاب و القبول المتطابقين عند التعبير عن الإرادة، فالإيجاب يستلزم أن يكون واضحا بطريقة صريحة أو ضمنية، ولا يمكن أن يكون الإيجاب عن طريق السكوت لأنه لا يحدث أثرا. أما القبول فهي الإرادة الثانية في العقد التي تطابق الإيجاب و التي بدونها لا ينعقد العقد، صادرة عن إرادة واعية و كاملة قادرة على إحداث اثر قانوني سليم، و قد يكون القبول عن طريق البريد الالكتروني أو عن طريق ملء استمارة الكترونية معدة سلفا، و بمجرد الضغط على الزر مرة واحدة ينعقد العقد، على أن يكون قبولا بصورة باتة و واضحة.[2]

- يتضمن العقد الالكتروني على الخصائص التفصيلية للسلع و الخدمات، شروط و كيفيات التسليم، شروط الضمان و خدمات ما بعد البيع، كيفيات معالجة الشكاوى، شروط فسخ العقد الالكتروني، شروط و كيفيات الدفع، الجهة القضائية المختصة في حالة النزاع، مدة العقد حسب الحالة، اللغات المقترحة لإبرام العقد الالكتروني على أساس أنها قد تكون سببا لوقوع المستهلك في عيب من عيوب الرضا بخصوص محل التعاقد بسبب عدم فهمه اللغة المستعملة.

المعاملات المستبعدة من خضوعها للتعامل الالكتروني في ظل التشريع الجزائري بموجب المادة الثالثة من القانون رقم18-05 المتعلق بالتجارة الالكترونية انه

[1] نفس المرجع السابق.

[2] دناي نور الدين، الإيجاب و القبول في العقود الالكترونية، مجلة معالم الدراسات القانونية و السياسية، العدد الثاني،ديسمبر2017،ص 94و95.

" تمارس التجارة الالكترونية في إطار التشريع و التنظيم المعمول به .
غير انه تمنع كل معاملة عن طريق الاتصالات الالكترونية تتعلق بما يأتي :

- لعب القمار و الرهان و اليانصيب،
- المشروبات الكحولية و التبغ،
- المنتجات الصيدلانية،
- المنتجات التي تمس بحقوق الملكية الفكرية أو الصناعية أو التجارية،
- كل سلعة أو خدمة محظورة بموجب التشريع المعمول به،
- كل سلعة أو خدمة تستوجب إعداد عقد رسمي.[1]

- آليات الحماية القانونية للتجارة الالكترونية في التشريع الجزائري :

الشخص عند إبرامه لمختلف العقود الالكترونية، يكتسب صفة المستهلك الالكتروني، هو نفسه المستهلك العادي فقط الاختلاف يكمن في استعماله مختلف الوسائط الرقمية. و نظرا لعدة العقود الالكترونية المبرمة، وضعت عدة آليات و وسائل من اجل تحقيق الحماية الأزمة، لان المستهلك الالكتروني يعتبر الطرف الضعيف في العلاقة التعاقدية، و هي حماية من نوع خاص، و هي مجموعة من القواعد التي تهدف إلى ضمان امن المعلومات. و تتجلى أهمية هده الضمانات في كونها لا تقتصر فقط على مرحلة تنفيذ العقد، بل تبدأ من اللحظات الأولى لتصفح المستهلك في المنصة، ثم تمتد الحماية إلى مرحلة إبرام العقد و تنفيذه تشمل قواعد خاصة تضمن صحة التعاقد و سلامة التنفيذ.

- حماية المستهلك الالكتروني ما قبل إبرام العقد :

اشتراط وضوح الإعلان الالكتروني بان يتضمن هذا الخير معلومات كافية حول السلعة المعروضة، و يعد شرط الوضوح غير متحقق إذا تم وضع البيانات الجوهرية خاصة تلك المتعلقة بالإيجاب في أماكن يصعب الوصول إليها، أو إذا تم عرضها بخط صغير جدا يجعل قراءتها صعبا مما يؤدي بالأضرار بحقه في الاختيار الحر.
و يكمن التضليل في الخدمة الرقمية أيضا، بان يمس منشأ المنتج أو أصله من خلال نسبته إلى منطقة معينة بشكل كاذب، كان يعلن على أن المنتج انه صنع في ألمانيا في حين مصدره دولة أخرى.

اشتراط إعلام المستهلك قبل التعاقد، و هو من واجب المورد الالكتروني المذكور سابقا، ومن الجزاءات المقررة في القانون 18-05 عند الإخلال بالتزام الإعلام، و هو حق المستهلك بإبطال العقد لأنه يعيب إرادته، إذا ثبت أن الإخلال كان سببا في وقوعه في غلط جوهري. و

1 القانون 18-05 المتعلق بالتجارة الالكترونية، السبق دكره.

تترتب المسؤولية المدنية للمورد إذا ما لحق بالمستهلك أي ضرر.[1]

- حماية المستهلك أثناء مرحلة إبرام العقد الالكتروني :

منح المستهلك حق العدول و إرجاع المنتج إذا لم يطابق المواصفات خلال فترة زمنية محددة بعد إبرام العقد من خلال تصريح يعبر فيه عن رغبته في عدم الاستمرار في الالتزام التعاقدي. و قد أشار إليه المشرع في المادة 11 من القانون 18-05 ضمن عبارة :" شروط و أجال العدول عند الاقتضاء"، مما يدل أن تحديد آليات ممارسته ترجع للأطراف المتعاقدة. كما أشار القانون ذاته في المادة 22 [2]منه إلى مدة الحق في العدول إلى 4 أيام، و إلزام المورد الالكتروني بإرجاع المبلغ المدفوع و كافة النفقات الأخرى خلال اجل لا يتعدى 15 يوما من تاريخ استلامه للمنتوج.

و يترتب على استخدام المستهلك لحقه في العدول عن التعاقد زوال العقد واعتباره كان لم يكن، مع التزامه برد السلعة إلى المورد في نفس الحالة التي كان عليها المنتج عند استلامه . أما في حالة انقضاء المهلة المقدرة بأربعة أيام لا يمكن له ممارسة هذا الحق، و يصبح العقد ملزما للجانبين.

- حماية المستهلك عند تنفيذ العقد :

مرحلة تنفيذ العقد مهمة لذلك أولاها المشرع بحماية خاصة لأنها تترجم الالتزامات المتبادلة إلى أفعال ملموسة، و منها الضمانات القانونية العامة من ضمان التعرض ضمان الاستحقاق و ضمان العيوب الخفية.

و يقسم التعرض إلى نوعين : تعرض شخصي صادر عن البائع، و هو عدم الإتيان بأي تصرف مادي أو قانوني من شانه أن يحرم المستهلك من الانتفاع الكلي أو الجزئي بالمنتج ، يمكن للمستهلك أن يلجا إلى القضاء للمطالبة بضمان التعرض ، متى كان قد وقع فعليا أو أدى إلى الانتقاص أو الحرمان من المنتج.

و تعرض صادر عن الغير، يلتزم فيه المورد الالكتروني بدفع التعرض الصادر عن الغير، متى وقع التعرض فعلا و كان متجسدا في ادعاء الغير لملكية المبيع.

أما ضمان الاستحقاق يكون في حالة ما إذا رفع الغير دعوى الاستحقاق ضد المستهلك، وجب على المورد التدخل في الخصومة أو تعويضه عن فقدانه للمبيع.

---

1 الماحي فاطمة الزهرة شريفة، مدى فعالية القانون 18-05 المتعلق بالتجارة الالكترونية في حماية المستهلك الالكتروني من تجاوزات الموردين الالكترونيين ، مجلة الاجتهاد للدراسات القانونية و الاقتصادية، المجلد10، الع3 ،تامنغست، 2021

2 المادة 22، من القانون18-05، نفسه

ضمان العيوب الخفية من جانب البائع الالكتروني، و تعويض الطرف الأخر أو إعادة الثمن إذا ثبت وجود العيب. و حتى يثبت للمستهلك ممارسة هذا الحق، أن يثبت أولا وجود العيب قبيل البيع و ألا يكون على علم بالعيب، أي توافر حسن النية.[1]

الفرع الثاني :قانون حماية المعطيات الشخصية.

- التعريف بقانون حماية المعطيات الشخصية :

في زمن تتسارع فيه تطبيقات الذكاء الاصطناعي بشكل ملحوظ، أصبحت المعطيات الشخصية تمثل ثروة رقمية إستراتيجية، لكنها في المقابل تطرح تحديات قانونية عميقة تمس جوهر الحق في الخصوصية و الحقوق الأساسية للأفراد.

و القانون رقم 25-11 المؤرخ في 24 جويلية 2025، يعدل و يتمم القانون رقم 18-07 المؤرخ في 10 جوان 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، و المعالجة تشمل جمع و تسجيل و حفظ و نشر او تعديل البيانات.

و يمكننا القول أن القواعد القانونية الوقائية لحماية الخصوصية منبعها القانون 18-07، بينما القانون 25-11 يضيف حماية جزئية يغلب عليا الطابع الردعي، دون أن تصل إلى مرتبة الضمانات الوقائية، فتنص على حماية لاحقة بعد وقوع الضرر.

المبادئ الأساسية في معالجة البيانات وفقا للتعديلات هي :

-تحديد الغرض من وراء المعالجة، محدد و لا يتجاوز فيه.

- ضمان تحديث البيانات بشكل دقيق و امن لمنع الاختراق.

- أن تكون المعالجة بطريقة شرعية و عادلة.

فكل عملية متعلقة بمعالجة المعطيات ذات الطابع الشخصي المتعلقة بالصحة التي يكون الغرض منها بحث و دراسة و تقييم البيانات المرتبطة بنشاط الوقاية تخضع لهذا القانون. غير أن المشرع استثنى على سبيل الحصر بعض المعالجات من تطبيق هذا القانون على سبيل الحصر :

- معالجة المعطيات ذات الطابع الشخصي التي يكون الغرض منها المتابعة العلاجية الفردية للمرضى.

1 عقبي يمينة، الضمانات القانونية المقررة لحماية المستهلك الالكتروني أثناء تنفيذ العقد في التشريع الجزائري،مجلة معالم للدراسات القانونية و السياسية، المجلد4، كلية الحقوق و العلوم السياسية،سيدي بلعباس، الجزائر، 2020، ص 305.

- المعالجة التي تسمح بإجراء دراسات انطلاقا من المعطيات التي تم جمعها بخصوص المتابعة العلاجية أو الطبية الفردية كما هو مبين في الفقرة السابقة. و ذلك عندما تتم من القائمين بهذه المتابعة لاستعمالهم الحصري. و حسن فعل المشرع ذلك لان عملية المتابعة العلاجية للمرضى تتم يوميا داخل مؤسسات الصحة من قبل الأطباء المسؤولين عن المعلمة الطبية.

- يستثني كذلك المعطيات لغايات لا تتجاوز ممارسة أنشطة شخصية أو منزلية أو عائلية بصفة حصرية شريطة عدم إحالتها للغير أو نشرها. و يتعلق الأمر كذلك بمعالجة المعطيات ذات الطابع الشخصي المحصل عليها، و المعالجة لمصلحة الدفاع و الأمن الوطنيين.

فيهدف هذا القانون إلى حماية الحياة الشخصية للأفراد، تعزيز الثقة في البيئة الرقمية، و منع الاستغلال الغير قانوني للمعطيات، كما ينظم كيفية جمع و الاستعمال القانوني للبيانات و المعطيات الشخصية، التي تفيد بتحديد هوية كل شخص طبيعي بشكل مباشر او غير مباشر كالاسم و اللقب و البريد الالكتروني و رقم الهوية و غيرها.[1]

- الآليات القانونية الوقائية لحماية المعطيات ذات الطابع الشخصي

خص لقانون 18-07 المعدل ب 25-11 هذه الحماية بمجموعة من الضمانات في مواجهة بعض الاعتداءات، تتمثل في الحقوق المقررة للأشخاص الطبيعيين و في المقابل إلزام المسؤلون ببعض الالتزامات.

فنعبر عن الآليات بالإجراءات الوسائل التي تستخدم لتطبيق الأحكام القانونية في الواقع و هي كالأتي :

- الموافقة الصريحة المسبقة للشخص المعني حسب المادة 4 من القانون 18-07، مع وجود استثناءات تتمثل في إجراء التصريح المسبق و الترخيص.

- تكمن كذلك حقوق المعني بالخصوصية، بداهة الحق في الإعلام بجمع بياناته، الحق في الاطلاع على بياناته لدى الجهات المختصة، الحق في طلب تعديل أو حذف البيانات الغير دقيقة، إضافة إلى الحق في الاعتراض عن المعالجة لأسباب مشروعة.

- أما في ظل القانون 25-11 استحدث آليات جديدة لتشديد الرقابة و ضمان رضا الشخص و سرية بياناته و حقه في الوصول إليها و تصحيحها. فتبنى تعيين مندوب لحماية المعطيات لضمان الامتثال للقوانين داخل المؤسسات، واستحدث سجلات المعالجة التي يمسك بها مسؤوليي المعالجة.

---

1 - مجلة الأستاذ الباحث للدراسات القانونية و السياسية - المجلد04 - العدد02- السنة 2019- ص 1528و1529.

- تبنى التعديل الجديد إنشاء السلطة الوطنية لحماية المعطيات الشخصية (ANPDP)، كهيئة مستقلة تسهر على احترام الضوابط القانونية في هذا المجال، تتمتع بالشخصية المعنوية و الاستقلال المالي و الإداري بعيدا عن أي تأثير خارجي، تتشكل من 16 عضو من بينهم الرئيس يعينون بموجب مرسوم رئاسي لعهدة مدتها خمس سنوات قابلة للتجديد. فهي سلطة ذات طابع ضبطي و رقابي حيث تتولى الإشراف على مدى التزام الفاعلين العموميين و الخواص بالأحكام القانونية ذات الصلة بحماية المعطيات الشخصية، و ذلك وفق رؤية وقائية.

بعض الآليات الجزائية المستحدثة :

استحدث المشرع في الباب الخامس مكرر تحت عنوان "معالجة المعطيات ذات الطابع الشخصي لأغراض الوقاية من الجرائم و الكشف عنها و إجراء التحريات و التحقيقات و المتابعات الجزائية و تنفيذ العقوبات."

فبالنسبة للجهات المخولة لمعالجة هذه المعطيات منها : السلطة القضائية و المديرية العامة للأمن الوطني، الدرك الوطني، مصالح إدارة السجون في حدود سلطتها و اختصاصاته.

و لا يشترط عند اللجوء إلى هذا النوع من المعالجة الموافقة المسبقة للشخص المعني بالمعالجة، كما له الحق بان يعلم مسبقا بهوية المسؤول عن المعالجة و أغراضها و لكن بشكل مقيد، ذلك لتجنب عرقلة التحريات وتدابير الوقاية و حماية الأمن العام و حريات الآخرين.[1]

الفرع الثالث : قانون التوقيع الالكتروني و المعاملات الرقمية.

يمثل هذين القانونين خطوة جديدة نحو تعزيز الأمن الرقمي في الجزائر، عبر تنظيم خدمات التوقيع الالكتروني و تاطيرها، و خدمات الثقة بما يضمن حماية المعاملات الرقمية و تعزيز حجيتها القانونية.

فنعني بالتوقيع الالكتروني المعروف أيضا باسم التصديق الرقمي او الشهادة الالكترونية، هو عملية تهدف إلى ضمان قانونية و سلامة و أمان المعلومات المخزنة الكترونيا. و يستخدم بشكل شائع للتأكد من هوية الأطراف المشاركة في معاملة الكترونية و ضمان عدم تغير في البيانات أثناء النقل.

على المستوى الوطني، ينظم التوقيع الالكتروني بموجب القانون رقم 15-04 المؤرخ في 11 ربيع الثاني 1436 الموافق ل 1 فبراير 2015الذي يحدد القواعد العامة المتعلقة بالتوقيع و التصديق الالكترونيين.

[1] مداخلة بعنوان شرح الأحكام الإجرائية الجديدة للقانون رقم11-25 المعدل و المتمم للقانون07-18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي من إلقاء السيد غليمي رابح.

أما بالنسبة للمعاملات الرقمية فقد اشرنا اليها سابقا، و القانون المؤطر لها يوسع نطاق خدمات الثقة ليشمل :

- التوقيع و الختم الالكترونيين.
- ختم الوقت الالكتروني .
الإرسال الالكتروني المعتمد.
- حفظ و إثبات صحة المعاملات .
- شهادات توثيق آليات الانترنت.

فهو قانون مستحدث يضع الثقة في صميم التحول التكنولوجي، من حماية المعاملات الرقمية إلى الاعتراف القانوني بالوثائق و العقود الرقمية و معادلتها بالوثائق الورقية مع تنظيم حفظها و سلامتها، وصولا إلى التعريف الالكتروني الأمن...

أولا قانون التوقيع الالكتروني
المشرع الجزائري يعرف هذا النوع من التوقيع في المادة 2 الفقرة 1 من القانون 15-04 بأنه "بيانات الكترونية في شكل إلكترونين مرفقة أو مرتبطة منطقيا ببيانات الكترونية أخرى، تستعمل كوسيلة توثيق"، و كما عرفت المادة 7 أيضا التوقيع الالكتروني بأنه :" التوقيع الالكتروني الموصف هو التوقيع الالكتروني الذي تتوفر فيه المتطلبات الآتية :
- أن ينشا على أساس شهادة تصديق الكتروني موصفة.
- أن يرتبط بالموقع دون سواه.
-أن يمكن من تحديد هوية الموقع.
- أن يكون مصمما بواسطة آلية مؤمنة خاصة بإنشاء التوقيع الالكتروني.
- أن يكون منشأ بواسطة وسائل تكون تحت التحكم الحصري للموقع.
- أن يكون مرتبطا بالبيانات الخاصة به، بحيث يمكن الكشف عن التغيرات ألاحقة بهذه البيانات. [1]

و سواء كانت تعريفات تشريعية أخرى أو فقهية، فالغالب ، و يتميز عن غيره من التوقيع التقليدي بما يلي :
- إذا كان التوقيع التقليدي يستند فيه الموقع على قاعدة مادية ورقية في الغالب، فان التوقيع الالكتروني يتم عبر شبكة الانترنت.
- و إذا كانت وظيفة التوقيع التقليدي هو التأكد من صاحب التوقيع، فان مهام التوقيع الالكتروني إضافة إلى التأكد من الهوية، يضمن التوثق من مضمون المحرر الالكتروني و تأمينه من التعديل بواسطة ربط المحرر الالكتروني بالتوقيع.

[1] قانون رقم 15-04 مؤرخ في 01 فبراير 2015، يحدد القواعد العامة المتعلقة بالتوقيع و التصديق الالكترونيين، ج رج ج. عدد 6، صادر ف 10-02-2015 .

- و الميزة الأخرى المعترف بها للتوقيع الالكتروني هو انه يسمح بالتعاقد عن بعد، و يمنح المستند صفة المحرر الأصلي و بالتالي معدا كوسيلة إثبات.

تطبيقات التوقيع الالكتروني:

لهذا النوع من التوقيع مجالات التي يستخدم فيها على المعاملات القانونية بين الأفراد و المؤسسات ، و هي على النحو التالي :

1 البطاقات الممغنطة وسيلة للدفع تحل محل النقود، باستخدام الرقم السري، و هي أنواع منها :

- البطاقة الائتمانية هي بطاقة مستطيلة من البلاستيك، تحمل اسم البنك المصدر لها وشعارها و توقيع حاملها و رقم و اسم هذا الأخير، و بمقتضى هذه البطاقة يستطيع حاملها أن يسحب المبلغ المالي من أجهزة الصراف الآلي، أو وسيلة للوفاء.
- بطاقة الحساب.
- بطاقة الوفاء تعرف ببطاقة الدفع، تخول لحاملها دفع ثمن الخدمات التي يحصل عليها من بعض المحلات التجارية التي تقبل الدفع الكترونيا، ي يكون ذلك بتحويل الثمن من رصيد العميل إلى رصيد البائع.
- بطاقة الصراف الآلي، فالتحويل من حساب إلى حساب يكون أليا عبر جهاز الصرف و دون التوقيع الورقي الصادر نتيجة السحب.
- البطاقة الذكية و تمتاز بحماية كبيرة ضد التزوير، و تعمل عن طريق التعرف على السمات الشخصية للفرد مثل مسح قرنية العين.[1]

2 الشيكات الالكترونية هي تطور لفكرة الشيك التقليدي، فينشا الساحب الشيك عبر المنصة المخصصة لذلك و يقوم بتوقيعها الكترونيا ثم يرسلها إلى المستفيد، فيقوم هذا الأخير بإيداعه عن بعد في البنك لتتم عملية التحقق و الصرف.

3 النقود الالكترونية و يستعمل هذا المصطلح للإشارة إلى الأنظمة الحديثة لتبادل المعلومات و تحويل الوحدات النقدية الالكترونية عبر الانترنت، مثل شركة ديجي كاش التي تصدر نقودا الكترونية لحاملها، فمن يحوزها يمتلك قيمتها المالية دون معرفة شخصية حامل النقود.[2]

---

1 علاء محمد عيد النصيرات، حجية التوقيع الالكتروني في الإثبات، دراسة مقارنة، ط1، دار الثقافة للنشر و التوزيع، الأردن،2005، ص 41 و 42 و 43.

2 شريف محمد غنام، محفظة النقود الالكترونية، د ط، دار النهضة العربية، القاهرة، 2003، ص 7.

4 التوقيع الالكتروني عبر البريد الالكتروني، يسمح هذا النظام بتبادل المراسلات أيا كان حجمها و يعتبر بذلك وسيلة للتعاقد من خلال إرسال و استقبال المراسلات الالكترونية موقعة بالطريقة المناسبة بين المتعاقدين، باستعمال التوقيع الرقمي أو التوقيع البيومتري أو التوقيع بالقلم الالكتروني أو غيره.

ثانيا : قانون المعاملات الرقمية

يأتي هذا القانون رقم 26-02 المؤرخ في 29 شعبان 1447 ه الموافق ل 17 فبراير 2026، بالتحديد لتنظيم الإطار القانوني للهوية الرقمية و خدمات التصديق الالكتروني، بما يواكب التحول الرقمي و تعزيز الأمان في المعاملات الالكترونية.

له طابع إصلاحي لان الفكرة الجوهرية فيه ليست إضافة تعريفات بل إعادة ترتيب البنية القانونية لمعاملات الالكترونية في الجزائر و خصوصا التي كانت محل غموض أو تشتت سابقا، كما أن الأشغال البرلمانية الرسمية اوظحت أن النص يهدف إلى تجاوز نقائص قانون 15-04، ليبني الترابط بين المفهوم و الإجراء و الأثر القانوني، و إزالة القيود التي أعاقت تنفيذ هذا القانون.

نلخص العوائق و الملاحظات أساسا في :
- صعوبات في ترشيد الموارد، لتعدد السلطات و إلحاقهم بمؤسسات مختلفة.
- صعوبات تطبيق التوقيع الالكتروني في مؤسسات الدولة بسبب ثقل الإجراءات و الرسوم المطبقة.

و كان من الضروري استبدال مخطط التصديق السابق بايطار تنظيمي جديد للتقليل من الأعباء المالية بالاعتماد على العناصر المشكلة على النحو التالي :
- مؤدي خدمات التصديق الالكتروني للفرع الحكومي.
- الطرف الثالث الموثوق بالنسبة للفرع الحكومي.

تجدر الإشارة إن قانون 15-04 لا ينص على مهام الطرف الثالث الموثوق، لكن المشروع الجديد أخد بتأطيرهم. نضيف أن المهام الموكلة إلى مقدم خدمات التصديق الالكتروني هي ذاتها المحدد في القانون 15-04.

مثال عن المفاهيم الجديدة التي استحدثها، فقد عرفت المادة 2 التعريف الالكتروني ولكن لم يربطه المشرع بمجرد بطاقة أو أداة تقني، بل بناه على مفاهيم متدرجة و هي خاصية، و هوية، ووسيلة تعريف، و منظومة تعريف، و عملية موثقة. و هذه المصطلحات تنقل النقاش من ماهية الهوية الرقمية إلى كيفية إثبات هذه الهوية و بأي مستوى من الضمان.

و في سياق أخر، خصص القانون 26-02 بابا للمراقبة و العقوبات :
- لكيفيات إجراء المراقبة على الأطراف الثلاثة الموثوقة و مؤيدي خدمات الثقة،
- لكيفيات اعتماد مؤيدي خدمة التدقيق المؤهلين لذالك بصفة دورية،
- لمراجعة العقوبات المالية و الإدارية المطبقة عليهم في حالة الإخلال بالشروط المفروضة عليهم.[1]

إن مشروع هذا القانون يلغي أحكام قانون 15-04 ، غير انه تبقى نصوصه التطبيقية سارية المفعول إلى غاية نشر النصوص التطبيقية لمشروع هذا القانون.

المطلب الثاني : القواعد الدولية و المعايير التقنية المتعلقة بالحماية

تشمل هذه المنظومة ابرز القواعد المتعلقة بالحماية المعلوماتية، المتكونة من الاتفاقيات والمعايير و التشريعات التي تامن البيئة الرقمية، و عليه نقسم هذا المطلب على فروع بالنحو التالي .

الفرع الأول : المعايير الدولية للأمن السيبيراني

الفضاء السيبيراني رغم أهميته في البيئة الرقمية وتأثيرها على الحياة السياسية و الاقتصادية، إلا أن المنظومة القانونية الدولية تعاني من فراغ تنظيمي و قانوني واضح، مما أتاح لبعض القوى الكبرى من إنشاء العمليات الدائرة تحت مظلة الأمم المتحدة مثل مجموعة الخبراء الحكوميين ووضع معايير طوعي لتنظيم الأمن السيبيراني.

يعرف المعهد الوطني للمعايير و التكنولوجيا الأمن السيبيراني بأنه"القدرة على الحماية أو الدفاع عن استخدام الفضاء السيبيراني من الهجمات الالكترونية". فيقوم بحماية المؤسسة في أصول معلوماتها من التدمير، لان أجهزة الكمبيوتر و البيانات و البرامج من المكونات الأساسية في كل مؤسسة في العالم. ونذكر بعضها على النحو التالي :

1 المنظمة الدولية للتوحيد القياسي ايزو الذي أنشئ في عام 1947، هو هيئة غير حكومية تتعاون مع اللجنة الدولية الكهروتقنية. و أشهر المعايير التابعة له هو 27002 ايزو، و هذا المعيار يتضمن التوجيهات منها [2]:

السياسة الأمنية Policy Security
إدارة الأصول management Asset
الأمن البيئي و المادي Security environnemental and physical

[1] القانون رقم 26-02 المؤرخ في 17 فبراير 2026، يحدد القواعد العامة المتعلقة بخدمات الثقة للمعاملات الإلكترونية وبالتعريف الإلكتروني، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 14.

[2] https://www.iso27002security.com/index.html، vu le 18.23 , 22mai2026.

إدارة الحوادث الأمنية للمعلومات management incident Security information
إدارة استمرارية الأعمال management continuity business

2 قانون FISMAوهو اختصار لAct management Security information federal
و معناه قانون إدارة امن المعلومات الفيدرالي هو قانون أمريكي، و ينفذ البرنامج عن طريق
التدريب على الوعي القومي.
التخطيط لتوفير الحماية الكافية لنظم المعلومات.
الاختبار الدوري لفعالية السياسة المنتهجة.[1]

4 قانون HIPPA، Health Insurance Portability and Accountability Act قانون أمريكي يهدف إلى حماية المعلومات و البيانات الطبية للأفراد و ضمان سريتها، من خلال حماية خصوصية المرضى و تقليل الاحتيال داخل قطاع الصحة.[2]

من أهم القواعد التي جاء بها هي: قاعدة الخصوصية لتي تتيح للمريض حق الاطلاع على ملفه الطبي و تحمي معلوماته الصحية الشخصية.
قاعدة إخطار الأفراد عند حدوث أي تسريب لبياناتهم.
قاعدة الأمن التي تفرض إجراءات التشفير و كلمات المرور و غيرها من الإجراءات التقنية.[3]

ولإشارة فان المعايير السابقة الذكر ليست الوحيدة المعتمدة، و إنما أكثرها شهرة و تطبيقا على المستوى العالمي، إضافة إلى انه لا يستفاد من هذه المعايير إلا إذا تم تنفيذها بالشكل الصحيح. و ينبغي كذلك وجود تعاون كامل لأفراد المنظومة كل حسب دوره لتحقيق النتيجة المرجوة.

الاعتبارات الأخلاقية و القانونية :

هناك مجموعة من الأخلاقيات المعتمدة عند إجراء اختبارات الأمن السيبيراني، لضمان مشروعية العملية و تحترم حقوق الأطراف و هي :
- الحصول على إذن خطي و صريح و ذلك من قبل مالكي البيانات قبل الشروع في أي عملية امن سيبيراني، و أخذ موافقتهم بعقد أو اتفاقية رسمية.
- الامتثال للقوانين و التنظيمات فمثلا القرصنة الأخلاقية المرخص بها تختلف عن القرصنة الغير مشروعة في وجود الإذن. فيجب التأكد من أن جميع خطوات الاختبار تقع ضمن إطار القانون.
- السلوك الأخلاقي و المهني فالهدف من عمليات الأمن السيبيراني و اختبارات الاختراق

1 https://csrc.nist.gov/groups/SMA/fisma/overview.html ,view 19.53, 25 may2026.

2 U.S.Congress, Health Insurance Portability and Accountability Act of 1996, Public Law 104- 191 . .

تكون مشروعة و الهدف منها تعزيز امن المؤسسات، و تجنب أي تعارض للمصالح و عدم الانحراف عن الأهداف الأصلية.

الحفاظ على السرية وخصوصية البيانات لوجود معلومات حساسة كالبيانات المالية و الأسرار التجارية . فبعد الانتهاء من الاختبار وجب إتلاف أي بيانات سرية تم حصدها وفقا لشروط الاتفاق مع الجهة المالكة.[1]

الفرع الثاني :التوجيهات الدولية حول حماية المعلومات و الخدمات الرقمية.

لا يمكن للفرد أن يستفيد من الخدمات الرقمية إلا بعد إدراجه لبياناته الشخصية على منصات افتراضية، و لتعزيز المرونة السيبيرانية و توفير الحماية، تعتمد التوجيهات الدولية على معايير تضمن سرية و سلامة البيانات، و تتركز هذه السياسة الأمنية من معايير أساسية من بينها

1 "سياسة امن المعلومات" و يكفل توجيه إدارة المؤسسات للتوافق مع القوانين و اللوائح ذات الصلة، و يشتمل على معيارين فرعيين هما :
الوثيقة العامة لسياسة امن المعلومات.
المراجعة لسياسة امن المعلومات.

وكلاهما ينفذان بعد تطبيق التوجيهات التالية :
- ضرورة إرفاق وثيقة سياسة امن المعلومات بموافقة الإدارة العليا للمؤسسة .
- بعد إجازة الوثيقة و اخذ الموافقة من الإدارة العليا، يلزم تعميمها على كل المنسوبين و الجهات الخارجية ذات العلاقة.
- ضرورة الانتباه إلى عدم احتواء الوثيقة على معلومات حساسة عن المنظمة عند توزيعها.

فبعد موافقة الإدارة العليا على وثيقة امن المعلومات، يتم تنظيم هذه السياسة داخليا و خارجيا.

و تعرض التوجيهات كيفية التنظيم الخارجي و ذلك بتوفير الموارد المادية و البشرية، و تحديد مهام كل فاعل في المنظمة، زيادة إلى وضع تعريف خاص للمعلومات الواجب حمايتها، إضافة إلى توثيق أي عملية أمنية أو عملية تعيين الجهة المسؤولية عن أي أصل موجود.

تحدد التوجيهات كذلك الأطراف الخارجية التي تدير معالجة المعلومات و السيطرة على دخول هذه الأطراف، كما تأخذ الاحتياطات الأمنية اللازمة لإتاحة المعلومات و مرافقها الأطراف الخارجية و ذلك بحصر هذه الفئة في أطراف مقدمي خدمات الانترنت و مزودي الشبكات و المستشارون و الموردين و الموظفين المؤقتين و غيرهم...
تكمن هذه التوجيهات أيضا في نوع الوصول المتاحة للأطراف الخارجية و تحديد المرافق

كتاب الأمن السيبيراني تعلم الأمن السيبيراني من الصفر حتى الاحتراف ص 269 و270.

التي تستخدمها عند تخزين و معالجة المعلومات. كما توجه السياسة إلى وضع قيود على نسخ المعلومات أو الكشف عنها عن طريق الأطراف الخارجية.

2 توجيهات خاصة بالتحكم في الوصول إلى المعلومات من قبل الأفراد المصرح لهم فقط، ذلك بإنشاء قواعد للدخول مبنية على مبدأ كل شيء ممنوع ما لم يسمح به صراحة، و توجيهات متعلقة بإدارة دخول المستخدم من تسجيله إلى إدارة كلمة المرور وصولا إلى مراجعة وصول المستخدم للنظام.[1]

كما تضيف توجيهات هذا المعيار طريقة التحكم في الوصول لنظم التشغيل للمستخدمين المصرح لهم فقط و توثيق المحاولات الناجحة و الفاشلة لهم، فلا تظهر أي معرفات عن النظام إلا بعد الدخول الناجح و لا أية رسائل مساعدة أثناء العملية، و تشير التوجيهات إلى فرض وضع كلمات مرور قوية مع إمكانية تغييرها.

3 توجيهات متعلقة بمعيار تطوير و صيانة أنظمة المعلومات، للحفاظ على استمرارية الأمان و تجنب الخسائر و إساءة استخدام المعلومات، و يدخل في ضمنها معايير فرعية :
- الشروط الأمنية لنظم المعلومات المتمثلة في إلزامية تلاءم المتطلبات الأمنية مع قيمة و حساسية المعلومات الموجودة بالنظام و الأضرار المحتملة من الاختراق الأمني، و شرط تحديد هذه المتطلبات في عقود الجهات التي تنفذها.
- المعالجة في التطبيقات التي تفيد صحة البيانات المدخلة ووضع رقابة على عمليات المراجعة و التحقق من صحة رسائل النظام، بوضع إجراءات لمنع تشغيل برامج بطريق الخطأ، و تحديد مسؤوليات جميع الموظفين المساهمين في إدخال البيانات.

- إدارة الثغرات التقنية للحد من استغلال نقاط الضعف التقنية، عبر الجرد الكامل لأصول البرامج و التطبيقات، و تمحيص المخاطر المرتبطة بالثغرات التقنية.[2]

الفرع الثالث : دور الهيئات الدولية في تنظيم الأمن الرقمي

الأمن الرقمي في الدول هو محور كل سياسة أمنية، و لان التهديدات الرقمية لا تعترف بالحدود الجغرافية، اضطرت الدول من خلال هيئات تعمل عل بناء امن جماعي رقمي الى إنشاء معايير و اتفاقيات تكافح الجرائم الالكترونية العابرة للحدود.

فيكمن التعاون الدولي من خلال الاستراتيجيات الإقليمية و الدولية التالية :

[1] المجلة الدولية لعلوم المكتبات و المعلومات، مج 2 ، ع 2(ابريل- يونيو 2015).

[2] نفس المرجع السابق.

1 الإستراتيجية الإقليمية على المستوى العربي نجد الاتفاقية التي تبنتها جامعة الدول العربية، هدفها التعاون العربي لمكافحة جرائم تقنية المعلومات و الحفاظ على الثروات المالية و المعلوماتية للمؤسسات الحكومية و الاقتصادية و الخاصة من القرصنة الالكترونية.

و تنص المادة 14 من هذه الاتفاقية على ضرورة التعاون على تبادل المعلومات الخاصة بالجرائم المتعلقة بالهجمات الإلكترونية و البنى التحتية للاتصالات و المواقع و المعلومات، إضافة إلى التحريات في سبيل المساعدة للقبض على المجرمين أو المحكوم عليهم بجرائم سيبرانية وفقا للنظام القانوني لكل دولة ، و نصت المادة أيضا على تبادل الخبرات و المشاريع التدريبية و التقنية بين الدول لرفع مستوى الأداء .

2 الإستراتيجية الدولية نجد العديد من الجهود و التنسيق المشترك لتحقيق الأمن الرقمي الدولي، من بينها اتفاقية بودابست لمكافحة الجريمة المعلوماتية التي ترمي إلى موائمة عناصر القانون الجنائي المحلي و الأحكام المتصلة بالجرائم في مجال الجريمة الالكترونية، و تضمنت هذه الاتفاقية مجموعة من المعايير و المبادئ العامة المتعلقة بالتعاون الدولي في مجال الشؤون الجنائية و حددت الإجراءات المتعلقة بطلبات المساعدة المتبادلة بين الدول في غياب الاتفاقية الدولية، و التي تهدف إلى النقاط التالية :

- توحيد عناصر القانون الجزائي المحلي و الأحكام المتعلقة بالجرائم الالكترونية.
- توفير الإجراءات القانونية الخاصة بالتحري.
- جمع معلومات عن حركة البيانات و عن إمكان التدخل في محتواها.
- تدريب الموظفين المكلفين بتنفيذ القوانين، و إلحاقهم بالمعدات اللازمة للتعامل مع الجرائم ذات التقنية العالية .

و مازالت الأعمال متواصلة لإيجاد حلول دولية ناجعة لمحاربة النشاطات الارهابية الرقمية، و للإشارة أن مثل هذه الهيئات الدولية تفرض على الجميع الامتثال التنظيمي و القانوني عبر التوجيهات و المعايير الصارمة لحماية البيانات، و أي تقاعس أو عدم الامتثال لها يعرض المؤسسات لغرامات مالية ضخمة و إجراءات قانونية ردعية.[1]

1 مجلة المعرفة العدد الحادي عشر- دجنبر 2023 الأمن السيبيراني و رهانات التحول الرقمي في المغرب سعيد اوغان جامعة محمد الخامس الرباط المغرب.

الفصل الثاني :
آليات حماية و إدارة الخدمات الرقمية داخل المؤسسة الاقتصادية

الفصل الثاني : آليات حماية و إدارة الخدمات الرقمية داخل المؤسسة الاقتصادية

تعتبر الرقابة الرقمية في المؤسسات ضرورة حتمية، من خلال العمليات المنتظمة للتأكد من مدى تنفيذ الخطط و إدارة الخدمات و محاولة اكتشاف الانحرافات عن الأهداف الموضوعية و حمايتها، و هده الآليات المستخدمة تكون وفق برامج حاسوبية للوصول إلى النتائج المطلوبة بدقة اكبر. ومن هذا المنطلق سنتطرق في هذا الفصل إلى مختلف الآليات المعتمدة في المبحث الأول ثم نتطرق إلى كيفية إدارة هذه الخدمات نحو السياق الصحيح.

المبحث الأول : الآليات التقنية و التنظيمية للحماية الرقمية

عندما نتحدث عن الآليات التقنية للحماية نقصد منها تلك الأدوات و البرمجيات المستخدمة خصيصا لحماية البنية المعلوماتية و تركز على العنصر البشري و الإجراءات، أما بالنسبة للآليات التنظيمية تتمثل أساسا في الأطر الإدارية و القانونية و الهيكلية المحددة لكيفية إدارة الأمن، و سيتناول كل منها على حدة في مطلبين اثنين.

المطلب الأول : آليات الحماية التقنية

الفرع الأول : التشفير و أنظمة الجدار الناري

يعتبران من ركائز منظومة الحماية التقنية الرقمية

1 التشفير

تعتبر البيانات محلا للقرصنة كممارسة سلبية للثورة التكنولوجية عن طريق استغلالها بدون مقابل أو ترخيص، و آن التشفير يضمن الحماية الفعالة لها من خلال إتاحة المعلومات للمستخدمين المصرح لهم فقط.

فنقصد بمصطلح التشفير بخوارزمية تحول النص العادي الرقمي إلى معلومات مشفرة باستخدام الرياضيات المتطورة، و لا يمكن فك التشفير إلا بأكواد و مفاتيح خاصة، من خلالها يصبح معناها غير مفهوم بالنسبة إلى أي شخص غير مصرح له بالاطلاع عليها. و كل شخص يعترض رسالة خلال انتقالها يطلق عليه اسم معترض أو متنصت أو غريم. و بطبيعة الحال لا يمكن لهذا المعترض فك خوارزمية التشفير إلا ادا توافرت المجموعة اللازمة من المعلومات لتمكينه من معرفة المفتاح الصحيح لتفكيك الشيفرة. [1]

[1] بيير، البرشت.(2018). علم التشفير(ترجمة مؤسسة هنداوي). مؤسسة هنداوي للتعليم الثقافة.

و قد يحاول المعترضين فك الشفرة عن طريق التشفير بكل مفتاح فك تشفير ممكن الى حين تحديد المفتاح الصحيح.

و على ضوء ذلك نذكر بان للتشفير نوعين من الأنظمة نظام التشفير المتناظر و الغير متناظر، فالتشفير المتناظر يعمل بمفتاح واحد و هنا يكمن الخطر لان إذا عرف المعترض ذلك المفتاح تصبح البيانات معرضة للخرق بسهولة عبر نفس المفتاح، أما في التشفير الغير متناظر يوجد مفتاحان واحد عام يقوم بالتشفير و أخر خاص يعمل على فكه، لذلك معرفة المفتاح العام تكون دون جدوى للطرف المعترض.

فيكون التشفير هدفه الرئيسي هو عصمة البيانات و سلامتها وليس فقط إخفاء المعلومات، كما يعتبر وسيلة إثبات الهوية الرقمية عبر شهادات مشفرة تصدرها سلطات تصديق معتمدة.

إذا و تكمن علاقته بالمؤسسات الاقتصادية في حماية خدماتها الرقمية عبر ضمان سرية الاتصالات بين الموظفين و حتى العملاء بتحويل البيانات على اشكال غير مفهومة للغير الذي لا يحوز على مفتاح فك التشفير، و نرى ذلك كثيرا في خدمات الدفع الالكتروني و التحويل المالي.

2 أنظمة الجدار الناري

يعرف بالجيل الجديد من جدار الحماية و هو نظام ضد التهديدات السيبيرانية و في نفس الوقت يسمح للاتصالات الرقمية أن تنقل بحرية، و يعمل هذا النظام عبر ترشيح البيانات المرسلة و المستقبلة عبر الشبكة بناءا على قواعد حددها المستخدم. إلا أن هذا النظام محدود الحماية لأنه لا يحمي الهجمات الخارجية أو المحمولة عبر وسائط خارجية ك USB .

و تكمن أهميته في استباق اكتشاف المخاطر التي تصيب البيانات المخزنة عند استعمال اي نوع من الشبكات بتصفية حركة المرور الداخلة للشبكة أو الخارجة منها.

و يعمل على مراقبة حركة البيانات، و تطبيق القواعد و السياسات الأمنية ،و تحليل الحزم، اكتشاف الأنشطة غير الطبيعية، و كذا إنشاء حاجز بين الشبكة الداخلية و الخارجية.[1]

أنواعه :

- جدار الحماية القائم على تصفية الحزم (packet-filtering firewall)
يقارن كل حزمة بيانات بقواعد معينة كحظر بعض الإجراءات و البروتوكولات بدون فحص الحزم.
-جدار الحماية ذي الحالة (stateful inspectation firewall)
يقوم بفحص الحزم بإنشاء جدول يحتفظ بالاتصالات المسموحة بها فيه.

[1] الحشاني، خالد. امن الشبكات و الجدران النارية. دار الكتب العلمية، 2018.

- جدار الحماية المبني على الوكيل (proxy firewall)
يحمي البيانات بطريقة غير مباشرة من خلال مرور الطلبات عبر خادم الوكيل أولا الذي يقرر بسماح المرور أو منعه. و هو أكثر انتشارا في المؤسسات التي بحاجة عالية من الرقابة.
- جدار الحماية السحابي (Cloud firewall)
خاص بالتطبيقات و الخوادم السحابية الحديثة يراقبها ثم يطبق قواعد و سياسات الأمن.
- جدار الحماية على مستوى التطبيقات web application firewall)
مهمته الأساسية المراقبة و التحليل فيما يتعلق بالبيانات المتبادلة بين المستخدم و التطبيق، و يمنعه قبل الوصول إليه. [1]

تكمن علاقة أنظمة الجدار الناري و المؤسسات الاقتصادية في توفير الحماية اللازمة للبيانات المخزنة من اجل تقديم الخدمات الرقمية في بيئة سليمة لا تعود على المستخدم بضرر. و كل ذلك من خلال منع الوصول الغير شرعي إلى المعلومات الحساسة، تنظيم حركة المرور الشبكي المشار إليه أعلاه داخل المؤسسات، يقلل تأثير هذه الهجمات و الخسائر المالية نتيجة تسرب المعلومات.

أما بالنسبة للعملاء فهو يعزز الثقة من خلال حماية معلوماتهم الخاصة، و بالتالي سمعة المؤسسة و إنتاجيتها في السوق الرقمي.

و لا ننسى أن كلا من نظام التشفير و الجدار الناري يكملان بعضهما و هنا يكمن مبدآ امن المعلومات، فحتى و إن تم فك التشفير مازال هناك خط دفاعي ثاني لا يسمح بقراءة البيانات.

الفرع الثاني نظم الكشف و الاستجابة للتهديدات

يرمز إليه ب TDR يعني الأدوات التي تستعملها المؤسسات في الكشف عن الثغرة الأمنية الرقمية و المصممة للتحقيق فيها و الحد منها، لذا فان الدمج الفعال للتقنيات و قدرتها على تحليل كميات هائلة من الهجمات في وقت قصير يمكن المؤسسات من التعرف على الأنماط الغير العادية و التنبؤ بالتهديدات المحتملة بشكل أفضل. و إن الاستجابة المبكرة للكشف يمنع وقوع حوادث أمنية كبرى ربما ليس بوسع المؤسسات تحملها، فبدلا من توظيف حارس امن ليراقب شاشات الحاسوب الخاصة بالشركة تقوم النظم الرقمية بهذه المهام أسرع من البشر بحيث تحقق استمرارية الخدمة.

و من الأعمال الرئيسية التي تقوم بها هذه النظم القيام بالاتي:
- المراقبة المستمرة من خلال البحث عن النشاطات المشبوهة
- كشف حركة المرور الغير عادية على الشبكة
- تحليل التهديد و طبيعة الهجوم لتقوم بتحديد الاستجابة المناسبة

[1] الحارثي، محمد بن علي. امن الشبكات و الحماية من الاختراقات. الرياض، دار المؤيد للنشر و التوزيع،2018.

- الرد الآلي و التلقائي لعزل الأنظمة المخترقة
- الإصلاح و التعافي بمجرد تحسين دفاعات الأمن لتفادي حدوثها مستقبلا
-التطوير الدائم و ذلك بترقية خوارزميات الكشف من نسخة قديمة إلى واحدة جديدة احدث و أفضل.

تتمثل أشكال التهديدات التي تواجهها الأنظمة في المؤسسات على النحو التالي :

انتهاكات البيانات كبيانات المستثمرين و الأسرار التجارية.
- فيروسات الفدية و البرامج برنامج ضار و برامج التجسس فلا يكتفون بغلق البيانات بل يقومون بتهديد الضحية بنشرها على الانترنت.
- الاختطاف الرقمي كسرقة الرموز الأمنية للمدراء الماليين او تقمص شخصية رئيس مجلس الإدارة عبر استنساخ الأصوات المفبركة بالذكاء الاصطناعي.
- هجمات شبكة الروبوتات.
- تهديدات الهوية و سرقتها و انتحالها لتجاوز خطوط الدفاع التقليدية دون نشوب أي إنذار.
كما يمكن أن تستهدف السرقة الهويات الرقمية الخاصة بالبرمجيات التي عادة ما لا يولى إليها أهمية بالغة مقارنة بهوية الموظفين أو العملاء.
- حملات التصيد الاحتيالي عبارة عن حملات توهم الأفراد بصحة معلومات ما مصاغة بتقنيات الذكاء الاصطناعي و لكن في الأساس هي غير صحيحة ليكشف العملاء عن بياناتهم الخاصة.
- التهديدات الداخلية من الموظفين الحاليين و السابقين، يكون ذلك عند الانحراف على قاعدة تخصيص الأهداف كون الموظفين لديه ميزة التفاعل مع البنية التحتية و البيانات للمؤسسة فينحرف عن الغرض الذي عين من اجله و هي حماية و إدارة الخدمات الرقمية، سواء كانت نيته الكسب المالي السريع او يكون موظفا مهملا أو يكون متطفلا. [1]

آلية عمل أنظمة الكشف و الاستجابة للتهديدات:
أنظمة الكشف تحمي الخدمات الرقمية من خلال مجموعة من الآليات المتطورة التي تهدف إلى التعرف على العمليات الضارة و منع حدوثها مسبقا، بدءا من التحليل القائم على القواعد و انتهاء بالتكيف مع التهديدات و الاستجابة ضدها، و تمر الأنظمة بمرحلتين أساسيتين :

المرحلة الأولى : تركز على تحليل السلوكات بتقييم الأنماط المعتادة للاستخدام في الشبكة و تقارنها مع الأنماط الحديثة لرصد أي انحرافات محتملة. إذ يتميز النظام بالتعلم الآلي و عليه يستطيع أن يتعلم من البيانات السابقة و يحسن قدرته على تحديد التهديدات الجديدة، و يتم التعرف عليها كذلك بناءا على توقيعات معروفة أو ما يدعى بتكنولوجيا التوقيع.

[1] خالد مصطفى قنديل، جرائم تقنية المعلومات و الامن السيبيراني، دار الجامعة الجديدة، مصر،2022.

المرحلة الثانية: الاستجابة و معناها تنفيذ أنظمة الكشف للبروتوكولات و الإجراءات الفورية تعكس سرعتها في التصدي للتهديدات كعزل الجهاز المصاب.
علاوة على ذلك تعزز بعض الأنظمة خاصية التكيف التلقائي، بحيث يمكنها تعديل بنيتها على طبيعة التهديدات الجديدة التي تم كشفها. بهذه الطريقة تضمن فعالية الحماية و تسهيل حالة الاستجابة ضد الهجمات المتطورة التي تواجهها المؤسسات اليوم.[1]

الفرع الثالث :حماية قواعد البيانات و البنى التحتية الرقمية

يمكن أن يكون مخزون المؤسسة من البيانات منجم ذهب، عند استخدامها بالشكل الصحيح، فيمكنها أن تعزز التحليلات التي تساعد المؤسسة على العمل بكفاءة اكبر و تجنب الأخطاء، و من واجبها وضع الاستراتيجيات الصحيحة في مكانها و تحسين البنية التحتية للبيانات.

المقصود بالبنية الأساسية للبيانات :
هي النظام البيئي للتكنولوجيا و العمليات و الأشخاص المسئولين عن بيانات المؤسسة و الذي يتضمن المكونات التقنية كالخوادم و الشبكات و البرامج بما فيها من أنظمة التشغيل و الخدمات السحابة المختلفة.
عندما تتمكن المؤسسة من تحليل بياناتها التشغيلية بسهولة تفرز بين ما هو ناجح و ما هو غير ذلك.

تحسين البنية التحتية للبيانات :
لتجنب العيوب الشائعة على قاعدة البيانات و و لكي تبقى متأقلمة مع التحول الرقمي نشير إلى أهم المزايا التي يجب مراعاتها عند تحسين البنية و المساعدة على تغطية جميع القواعد :

- إدارة البيانات و تنفيذ خطتها التي تتضمن ادوار و مسؤوليات الأفراد القائمين على إدارتها و تعيين مالكيها، أيضا قواعد و إرشادات لفرق تكنولوجيا المعلومات التي يمكنها الوصول إليها.

- استخدام تقنيات الأتمتة التي تساعد على تنفيذ العمليات بشكل تلقائي دون تدخل البشري ، إضافة إلى تقنيات الحوسبة السحابية التي تخزن البيانات و تشغل البرامج دون الحاجة إلى بنية تحتية مكلفة.

- تنظيم البيانات في مجموعات منطقية من خلال تصنيفها و تجميع البيانات المتشابهة أو المرتبطة في فئات محددة تسهل استخدامها بكفاءة.

[1] محمد الهادي، امن المعلومات و الشبكات، الدار الجامعية، القاهرة ،2019.

- تخزين بيانات التعريف لتتبع أصل البيانات و هذا يساعد على التأكد من موثوقيتها، و دعم عمليات البحث و الوصول السريع للبيانات . [1]

- استخدام بروتوكولات الأمان لحماية البنية الأساسية التي تهدف الى تامين تبادل البيانات و ضمان سريتها أثناء الاتصال عبر الشبكات.

- مراقبة أداء النظام بانتظام لضمان كفاءة الأنظمة المعلوماتية و بالتالي استمرارية الخدمات الرقمية و تقليل التكاليف الناجمة عن الأعطال المفاجئة.

- التخطيط لسيناريوهات النمو المستقبلية كون المؤسسة تقوم بإنشاء كميات كبيرة من المعلومات.

- التركيز على قابلية التوسع و المرونة لان حوسبة المؤسسات تحتاج الى التغيير على مدار اليوم او حتى بالشهر و السنة، فمثلا يحتاج تجار التجزئة عبر الانترنت الى التخطيط للاستخدام الكثيف خلال العطلات.

- إعطاء الأولوية للسرعة و سعة التخزين.

- الاستثمار في تدريب الموظفين على التكنولوجيا الحديثة لتقليل الأخطاء التقنية الناتجة عن سوء الاستخدام و عبر التعامل السليم مع البيانات الحساسة و احترام سياسات الأمن الرقمي داخل المؤسسة.

و على كل حال يجب مراجعة البنية الأساسية للبيانات عند الاعتماد على تقنية جديدة، مثل التعلم الآلي و الذكاء الاصطناعي أو إجراءات أمنية جديدة. [2]

البنية التحتية الرقمية:

تعتبر البنية التحتية التكنولوجية ضرورة لتحقيق التنمية المستدامة و التحول الرقمي الشامل، فهي مجموعة من الأجهزة و الشبكات و المرافق التي تدعم عمليات تكنولوجيا المعلومات كمنصات الخدمات الرقمية و أنظمة الأمن السيبيراني و شبكات الألياف البصرية

وزارات المالية يجب أن تفكر في البنية التحتية العامة الرقمية كما تفكر في الطرق وشبكات الكهرباء:

لن تبني أي حكومة عشرات الطرق التي تربط نفس المكانين. إلا أن هذا يحدث في كثير من الأحيان مع الخدمات الرقمية. فالبلدان تخصص مليارات من أموالها للإنفاق على تكنولوجيا المعلومات دون أن تدرك الحاجة إلى التعامل مع هذه الأنظمة باعتبارها بنية تحتية

ريتشارد هيكس، وساتياروبا شيخار، "التحويل الرقمي، التنمية، والمجتمعات الحضرية المهمشة: إطار تطبيقي لعدالة البيانات"، مجلة *المعلومات والاتصالات والمجتمع*، مجلد 22، عدد 14، 2019، ص. 2092-2111 .

[2] نفس المرجع السابق

مشتركة. ويؤدي هذا المنهج المنفصل عن الواقع إلى تشتت الأنظمة، مما يزيد من صعوبة تشارك البيانات بين الهيئات العامة ومع القطاع الخاص، أو الاستفادة منها.

فماذا لو تعاملنا مع مجموعة من الأنظمة الرقمية الرئيسية - مثل الهويات الرقمية، ومنصات تبادل البيانات، وبيانات الاعتماد، والخدمات المشتركة الأخرى التي تدفع الوظائف الأساسية على مستوى الحكومة والاقتصاد - بالطريقة نفسها التي نتعامل بها مع الطرق أو شبكات الكهرباء؟ أي باعتبارها أنظمة ضرورية للاستخدام المتكرر.

ولا ينشأ أكبر تأثير اقتصادي للبنية التحتية العامة الرقمية، على غرار تأثير أنواع البنية التحتية الأخرى، من التأثيرات المباشرة بل من الأنشطة الاقتصادية واسعة النطاق التي تتيحها، مثل خط سكك حديدية جديد يحفز النمو على طول مساره. فعلى سبيل المثال، أدخلت مالاوي تحسينات كبيرة على أسواق الائتمان عن طريق تمكين المقرضين من التحقق من هويات المقترضين بمزيد من الدقة حينما استحدثت نظام تحديد الهوية البيومترية. وأطلق هذا الأمر العنان لفرص اقتصادية جديدة عن طريق تقليل مخاطر التعثر في السداد وزيادة إمكانية الحصول على الائتمان، ولا سيما للفئات المهمشة.

وعلى الرغم من هذا، فإن هذه النتائج الإيجابية ليست مضمونة. فكثير من البلدان استثمر في البنية التحتية العامة الرقمية، ولكنها لا تنظمها ولا تمولها باعتبارها بنية تحتية. وتحدد مبادرة وضع خريطة عالمية للبنية التحتية العامة الرقمية العالمية، بقيادة كلية لندن الجامعية، ما يربو على 64 برنامجا للهوية الرقمية الوطنية، و97 نظاما للمدفوعات الرقمية، و103 منصات لتبادل البيانات ذات إمكانات شبيهة بالبنية التحتية. إلا أن القليل منها فقط قيد الاستخدام على نطاق واسع. ويستخدم أكثر من خدمتين عامتين ما لا يزيد على نصف أنظمة الهوية الوطنية تقريبا. ولدى جنوب إفريقيا ثماني منصات وطنية لتبادل البيانات تعمل كل منها بمعزل عن الأخرى.[1]

المطلب الثاني آليات الحماية التنظيمية و الإدارية

نقصد باليات الحماية التنظيمية و الإدارية، مجموعة التدابير الاستباقية و العلاجية التي تعتمدها المؤسسات. فالجانب التنظيمي نقصد به الصلاحيات و تصنيف الوثائق، أما الجانب الإداري يكمن في الرقابة على أنظمة الأمن.

الفرع الأول سياسات الأمن المعلوماتي داخل المؤسسة

المؤسسات الاقتصادية تعتمد على مجموعة من الأساليب للحماية المادية و البرمجية و أساليب للحماية التنظيمية و الإدارية كما تضع سياسة أمنية خاصة بها. و مايهمنا السياسة على ضوء الحماية التنظيمية و الإدارية المكلفة بها دائرة الإحصاء و الإعلام الالي يشرف عليها مهندس إحصاء، و مهندس إعلام التي مهمته المحافظة على الأمن المعلوماتي للمؤسسة، الا ان درجة

[1] https://www.imf.org، البنية التحتية الرقمية، صندوق النقد الدولي،2026 مارس، 21.00.

الحماية تختلف من مؤسسة الى اخرى لان كل منها لها بيانات خاصة وحتى الموظفين لكل مؤسسة لهم درجة وعي مختلفة باهمية الأمن.

يوفر نظام امن المعلومات الحماية المطلوبة للمعلومات المالية و الشخصية و المعلومات السرية المخزنة في من الأشكال الرقمية. و ذلك عبر تنفيذ برامج المنظمة الأمني و توضح كيف تحمي الموارد و الأصول التقنية كما تسهل الاستجابة السريعة لطلبات المعلومات من العملاء و الشركاء و المدققين.و كل هذا بمثابة الامتثال للمتطلبات التنظيمية لان السياسة الأمنية تساعد على تحديد الثغرات الأمنية المتعلقة بالمتطلبات التنظيمية و معالجتها.

عناصر امن المعلومات :

يجب ان تحتوي سياسة امن المعلومات التي تضعها المنظمة على العناصر التالية :

1 السرية يعني إتاحتها فقط لمن لديه إمكانية الوصول المأذون بها ذلك عبر تنفيذ تقنية تشفير البيانات، و في المؤسسات الاقتصادية تظهر السرية في امن المعلومات في الموظفين الذين يحتاجون لاستخدام البيانات من اجل أداء أعمالهم هم المسموح لهم بالوصول إليها.

2 النزاهة في تعبئة البيانات بشكل كامل دون نقصان أو تقصير، لتعزيز مصداقية المؤسسة و للاعتماد عليها أثناء اتخاذ الخطط المستقبلية.
التوافر أي إمكانية إتاحة الأنظمة و الخدمات للمستخدمين في الوقت المناسب أو اي وقت دون انقطاع.

3 تحديد الغرض أو الهدف المترتب عن النهج الذي تتبعه سياسة امن المعلومات خاصة منها المعايير و المتطلبات المعتمدة من قبل المؤسسة.
تحديد غرض احترام حقوق الموظفين و العملاء كالخدمات المتعلقة بالرد على الشكاوى . أن تكون السياسة غرضها الحفاظ على سمعة المنظمة المنشاة لها.

4 الجمهور الذي تخصه السياسة بالحماية من غيره .

5 نشر الوعي و السلوك الأمني داخل موظفي المنظمة بإلحاقهم بدورات تدريبية.

استراتيجيات امن المعلومات
من ابرز أساليب حماية المعلومات الممكن للمؤسسات اعتمادها كالأتي :

- تشفير البيانات و كل المعلومات الحساسة التي تنقل بكميات هائلة عبر الانترنت .
- النسخ الاحتياطية من البيانات و لتوفير مصدر احترازي منها في حال تعرضها للانتهاك، فيمكن استعادتها كما هي دون نقصان . [1]

[1] أمينة قدايفة، *استراتيجية أمن المعلومات*، جامعة أمحمد بوقرة، بومرداس، الجزائر، 2016، ص15 .

– تصحيح البرمجيات يعني تحديث تطبيقات البرامج لمعالجة نقاط الضعف أو إضافة ميزات جديدة لاستمرار توافقها مع مختلف الأدوات الحديثة.

– التوثيق متعدد العوامل أي تقديم للمستخدم أشكال مختلفة من تحديد الهوية قبل الوصول إلى أي حساب، و على المؤسسات تبني هذه التقنية نظرا لدورها في الحد من المخاطر الالكترونية مثل برنامج تكسير كلمات المرور المتطور.

- تخطيط الاستجابة للحوادث عبر اكتشاف الهجمات و احتوائها و التعافي منها، و عليه يعقد اجتماع رسمي لتقييم أداء الفريق و سير العمليات.
- امن الشبكة كتوفير أنظمة كشف و منع التسلل و أنظمة التحكم في الوصول إلى الشبكة.

وظائف امن المعلومات:

-مهندس امن المعلومات هو الذي يصمم ي يدمج النظم المستخدمة في الأجهزة الالكترونية، ففي المؤسسات الاقتصادية يكون هو المسئول على توفير الخبرة التقنية لدعم عمليات استعراض البائعين و المشاريع.
- أخصائي دعم تكنولوجيا المعلومات هو الذي يكتشف و يحلل المشكلات الرقمية و يوضح للعملاء كيفية استخدام البرامج الخاصة بالأعمال.
- محلل مخاطر امن المعلومات بدراسة التهديدات المحتملة إلى جانب مراقبة نشاط الشبكة و إبداء رأيه في تنفيذ بروتوكولات السلامة. و يكون عمله إما مع موظفي الحماية في نفس الشركة أو مع الخبراء أو المتطوعين الخارجيين.
- مقيم امن المعلومات مهمته تقييم الضوابط الأمنية داخل أنظمة الشبكة للتوصل الى نقاط الضعف عن طريق تحرير تقرير عن ذلك .

الفرع الثاني : إدارة الهوية الرقمية و الصلاحيات

ادارة الهويات و الصلاحيات هو اطار للعمليات الاقتصادية التي تسهل من ادارة الهويات الالكترونية، فالاطار يتضمن سياسات المنظمة و مجموعة التقنيات لادارة الهويات. و لفهم اوظح حول إدارة الهويات الرقمية و الصلاحيات، من المهم ان نفهم ان الهوية و الصلاحية هما شيئان مختلفان نسبيا و منفصلان.

تعد الهوية الرقمية كحجر زاوية لا غنى عنه لأي جهة أو شركة تطمح للريادة، و للتحقق من الشخصية ليس بالبطاقات البلاستيكية و التواقيع الورقية بل أصبح منظومة ذكية اعم و اكبر تشمل حتى البيانات البيومترية و التوثيق متعدد العوامل.[1]

[1] إبراهيم عطية محمود المهدي، الحق في الهوية الرقمية في ضوء حماية البيانات الشخصية والخصوصية المعلوماتية، دراسة وصفية تحليلية مقارنة *مجلة البحوث القانونية والاقتصادية*، جامعة المنصورة،2023،ص500.

فنعرف الهوية الرقمية بأنها مجموعة السمات التي تتميز بها مؤسسة ما، تشمل تاريخ التصفح و البيانات البيومترية من بصمة الوجه و الإصبع ، التوقيع الرقمي و السجلات الحكومية الموحدة. لان في غياب الحضور الجسدي يتطلب تقنيات متطورة لضمان أن الشخص لدى النظام هو فعلا من يدعيه، و هنا تكمن قوة حلول إدارة الهوية، التي تهيئ الأمان العالي و تجربة المستخدم السلسة.

أما مصطلح الصلاحية نقصد به القدرة على السيطرة على نظام يستخدم مجموعة من أوراق الاعتماد التي يمتلكها المستخدم، و يقدمها بناءا على متطلبات النظام و وجوب إلغاءها عندما لا تكون مطلوبة.

أهمية إدارة الهوية الرقمية و الصلاحيات في المؤسسات الاقتصادية و تعزيز خدماتها تكمن في أنها بمثابة المحرك الأساسي للثقة في الخدمات الرقمية لعدة أسباب، كونها تعزز الأمن السيبيراني من خلال تقنيات التحقق القوية، و ترفع الكفاءة التشغيلية ناهيك عن تقليل الوقت المستهلك، و بالطبع تحسين تجربة العميل لأنه لن يكون ملزما على تكرار إدخال البيانات. كما تتيح الهوية الرقمية للمؤسسات القدرة على التعامل مع الأزمات بسرعة و كفاءة من خلال الرسائل الموجهة و المباشرة، و بهذه الطريقة تبني تفاعل مستمر مع جمهورها و الحضور الرقمي في أذهان العملاء و المستثمرين من خلال الردود السريعة و التحديثات المستمرة و بالتالي تمكين الجمهور من رؤية المؤسسة ككيان ديناميكي و متاح دائما للتفاعل.

مكونات نظام الهوية الرقمية:

من اجل نظام حماية قوي، يجب أن تتوافر عناصر تقنية و إدارية و تكاملها يحقق نجاح الهوية الرقمية :

1 السمات التعريفية و هي تلك المعلومات الأساسية كالاسم و رقم الهوية الوطنية و العنوان الوظيفي و البريد الالكتروني. فهذه البيانات بمثابة البطاقة التعريفية للمستخدم.

2 وسائل التوثيق التي تقسم إلى ثلاث مجموعات،المجموعة الأولى التي تحتوي على كلمات المرور و رقم التعريف الشخصي ، ثم الأسئلة الأمنية التي تطرح عادة أثناء إنشاء المستخدم لحسابه والإجابة عنها .
المجموعة الثانية هي كل ما يحوزه المستخدم من أداة أو جهاز فيزيائي أو رقمي خاص به كالرسائل النصية المؤقتة و مفاتيح الصغيرة التي توصل بالكمبيوتر لتأكيد الهوية. أما المجموعة الثالثة التي تعد من أهم الوسائل لأنها عبارة عن خصائص بيولوجية و جسدية مرتبطة بالمستخدم كبصمة الأصبع أو العين أو الصوت.[1]

3 إدارة الصلاحيات و يأتي بعد التحقق من الهوية و هنا يكمن دور الإدارة إما بالسماح

[1] مفيدة طاير مقومات و تحديات تشكيل الهوية الرقمية للمؤسسة في العصر الرقمي، المجلة العلمية للتكنولوجيا و علوم الاعاقة، المجلد2، العدد4،2020، ص220.

للمستخدم بالولوج للبيانات ام فقط يكتفي بالقراءة، أي حصر الوصول إليها أو حتى تقليل الصلاحيات للمستخدم بالحد الأدنى لأداء وظيفته فقط.

المصادقة من صحة هويات المستخدمين أو الأجهزة باستخدام كلمات المرور او الرموز المميزة الأمنية . ثم تقوم المصادقة التكيفية بتعديل المتطلبات بناءا على السياق مثل المطالبة بتحقق إضافي إذا قام المستخدم بالتسجيل من موقع غير معتاد.

5 التفويض للمستخدمين من عدمه فيما يخص ما يمكنهم فعله ضمن البيئة الرقمية.

كيفية ممارسة إدارة الهوية بفعالية

لتفعيل التحقق من الهوية الرقمية يتبع الإطار الرباعي الأتي :

التحقق من صحة المستندات و اتساق البيانات للحد من الاحتيال .
- تأكيد تفاصيل هوية المستخدم بمصادر بيانات مستقلة كوكالات الائتمان.
- دفع المخاطر باستخدام الإشارات بعد تحليل السلوكيات المشبوه فيها و الهويات الاصطناعية.
- تقرير القبول أو الرفض من خلال قواعد قابلة للتفسير و تفعيل المصادقة .

كيفية تقوية إدارة الهوية و الصلاحيات :

بمان إدارة الهويات و الصلاحيات هي الحلقة الأضعف في أي مؤسسة لأنه يمكن اختراقها بسهولة، لذلك وجب تقوية هذا النظام بتحديد إدارتها بشكل منفصل و جعلها تتماشى مع أهداف المنظمة، و الحفاظ على دور حياة المستخدم و مراجعتها بشكل دوري.

تحتوي دورة حياة المستخدم داخل المؤسسة على عمليات الانضمام و التحويلات و الاستقالة، فعندما ينضم شخص إلى المؤسسة يتم تزويده بهوية خاصة تدعى بمعرف الموظف. و يتم تزويده ببعض المعلومات الأساسية مثل بيانات البريد الالكتروني و الواتساب و غيرها. و استنادا على دور المستخدم، يتم تزويد ملف التعريف الخاص به بوصول إلى التطبيق أو البنية التحتية بناءا على الحاجة إلى معرفة الأساس الذي يسمى بالدور- التحكم في الوصول المعتمد(R B A C) .

ثم أثناء التحكم في الوصول المعتمد يجب تبني أسلوب الوصول الأقل امتيازا. عندما يزيد أو تنقص المسؤوليات في ملفه الشخصي لابد من توفير الوصول أو إلغاء توفيره. و هذا الأسلوب يحتوي على عملية الموافقة المحددة .

و عندما ينتقل المستخدم بين ملفات تعريف مختلفة يطلق عليه اسم المحرك. و الحركة تكون إما أفقية أو راسية و في كل الأحوال يجب مراجعة الوصول و إدارته.[1]

[1] المرجع نفسه

عندما يستقيل المستخدم يلغى وصوله إلى المعلومات المميزة بالسرية، و يسمى حينها بالمستقيل و العملية تدعى بالمستقيلين.

الفرع الثالث : إجراءات التدقيق و المراقبة الدورية

التدقيق بشكل عام و المدقق بصفة خاصة هو فحص أنظمة الرقابة الداخلية و البيانات و الحسابات و الدفاتر الخاصة بالمشروع قيد التدقيق و إبداء الرأي على مدى موثوقية البيانات الرقمية، اما المراقبة فهي نشاط لا يختلف من حيث المبدا عن التدقيق لان هدفها الاول التاكد من صحة المعلومات فهي تمثل نظام يحتوي على خطة و اجراءات تنظيمية تطبق لضمان التسيير المنظم لمجمل الانشطة و كذا اكتشاف الغش و الاخطاء ة تجنبها مستقبلا .

فالتدقيق و المراقبة و ان كانا مصطلحان متشابهان الا انهما مختلفان في الجوهر، فالمراقبة تكون انية و بشكل دوري مستمر لكن التدقيق يتم بشكل دوري متباعد. نضيف ان المراقبة يقوم بها فريق تكنولوجيا المعلومات او ادارة الامان الداخلي بينما التدقيق من اختصاص شخص محدد بمثابة مفتش يدعى بالمدقق الداخلي الرقمي او محافظ الحسابات.

و ان ابرز اهداف التدقيق هو التاكد من ان موارد تكنولوجيا المعلومات تؤدي الى تحقيق الاهداف التنظيمية بفعالية و نلخص بقية الاهداف في :

-مراجعة ضوابط نظم تكنولوجيا امعلومات للتاكيد على دقتها و فعاليتها .
- تقييم العمليات المرتبطة بعمليات مجال معين مثل نظام اروتب او نظام المحاسبة المالية.
- تققيم اداء النظام و امنه، على سبيا المثال نظام الحجز في السكك الحديدية.
- فحص عملية تطوير النظام و الاجراءات.
- فيحين هدف المراقبة الدورية الحفاظ على تشغيل النظام و حمايته الان.

و منه نجمل مكونات التدقيق في التقييم المبدئي للوضع الحالي للانظمة ثم استخدام ادوات تقنية لجمع البيانات و عليه تحليل العمليات و مقارنتها بالمعايير العالمية و اخيرا اعداد تقارير تقدم فيها التوصيات لتحسين الاداء القمي و تقليل المخاطر.[1]

و بالرغم من الفروقات بين الوظيفتين الا انه يوجد علاقة تكاملية بينهما لانه لا يمكن ان ينجح التدقيق الرقمي دون مخرجات انظمة المراقبة، كما يمكن للتدقيق ان ينبه المراقبة حول الثغرات الامنية التي ربما تفشل في رصدها عن طريق التوصيات التي تشملها تقارير التدقيق.

المشرع الجائري قد حرص على الزامية توظيف كلاهما في المؤسسات، فمثلا فرض وضع اليات المراقبة المستمرة و تعيين مسؤول داخلي لامن المعلومات لتطبيق الامتثال لقرارات

---

[1] تومي، ميلود، وعلون، محمد الأمين، "التدقيق الداخلي كآلية للحد من الفساد الإداري والمالي في المؤسسة الاقتصادية"، جامعة الوادي، 2016، ص. 12

السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي.
و حتى انه رتب مسؤوليات على مسيري المؤسسات و ملاحقتهم بتهمة اساءة الاستغلال الوظيفة او اهمال التدابير الرقابية المفروضة في ظل قانون الوقاية من الفساد و مكافحته 06-01، ذلك في حالة غياب انظمة المراقبة الدوية او اهمال تقارير التدقيق الرقمي.

و هذا من خلال :

-تقييم البنية التحتية الرقمية
- التدقيق في صلاحيات المستخدمين
- فحص أنظمة الحماية
- مراجعة سياسات الأمن ألمعلوماتي
- اختبار الثغرات الأمنية
- تدقيق السجلات الالكترونية
- التأكد من الامتثال القانوني و التنظيمي فالمشرع الجزائري كرس الحماية الرقمية و الامتثال لها عن طريق ارساء منظومة قانونية تجمع بين التدقيق و المراقبة الدورية و تحقيق الامن السيبيراني و حماية المعطيات و الزامية التصريح بالحوادث الرقمية و الاحتفاظ بالسجلات.

و ان استخدام التدقيق الالكتروني يحسن من جودة الخدمة الرقمية و يغير من اجراءات المتبعة من طرف المدقق و يرفع من كفاءاته لتصبح اكثر سهولة.

اجراءات المراقبة الدورية:

-المراقية المستمرة للشبكات.
- تحديث الانظمة و البرمجيات.
- متابعة سجلات الاحداث .
- فحص اداء الانظمة.
- مراقبة انظمة الحماية.
– اجراء تقييمات دورية للمخاطر.
- تدريب المستخدميين و الموظفبن و تحسين مهاراتهم من خلال تحديد نقاط الضعف و القوة بالتالي تقدير جهودهم و تحفيزهم على اداء خدمة رقمية افضل. [1]

[1] المرجع نفسه.

المبحث الثاني : ادارة المخاطر الرقمية و الحوكمة الالكترونية في المؤسسة الاقتصادية

اثر التحديات التي افرزتها المنظومة الاقتصادية و هي المخاطر المترتبة عن الاستعمال المكثف لتكنولوجيا المعلومات و الشبكات، برزت الحاجة الملحة إلى إدارة المخاطر من اجل الحوكمة الرقمية بابتكار حلول عصرية من اجل استمرار المؤسسات و نجاحها ،و سيتم تفصيل آلياتهما و أهميتهما في المطلين الآتيين.

المطلب الأول : إدارة المخاطر الرقمية

تحديد المخاطر المحتملة يحمي المؤسسة من خرق بياناتها و يقيها من تكبد الخسائر المالية او الأضرار بسمعتها، و في ظل العواقب الوخيمة التي تتعرض لها نتيجة هذه المخاطر وجب وضع الاستراتيجيات القوية التي تساعد على إدارتها و منع حدوثها او التقليل من نتائجها السلبية.

الفرع الأول : تحليل و تقييم المخاطر التقنية

الهدف من هذه الخطوة هو تحديد أولويات المخاطر الرقمية و التي تتطلب اكبر قدر من الاهتمام، ووفقا للعملية يتم تصنيفها بناءا على النتائج إلى مستويات مرتفعة و متوسطة و منخفضة. فمن الأجدر معرفة ماهية المخاطر الموجودة و تحليلها حسب مدى خطورتها ثم اتخاذ قرار بشان أي المخاطر يحتاج ميزانية و علاجا أولا .

فالخطر هو الحادث الامني و نعني به اي شيء يلحق الضرر بالموظفين او الاشخاص المرتبطين بهم، او يسبب فقدانا او تلفا للاصول.

أنواع المخاطر التقنية:
تتعدد المخاطر السيبيرانية التي تعترض المؤسسات و من أشهرها :
- التنصت و يعني اختراق حركة المرور من اجل سرقة المعلومات الهامة و ذلك من خلال
- الوصول إلى المعلومات المرسلة و المتبادلة بين المواقع المضيفة و المستخدم.
- سرقة كلمة المرور التي كلما كانت سهلة كلما تم اختراقها أسهل و هذا عبر التنصت أو التخمين.
- البرامج الضارة و الغير مألوفة التي تلحق الضرر بالأجهزة لان المجرمون يستهدفون البيانات المصرفية و الشخصية للمستخدمين بغرض سرقتها. [1]
- عمليات الاحتيال بالوسائل المتنوعة الأخرى لسرقة البيانات من خلال رسالة عبر البريد الالكتروني تتطلب من المستخدم تعبئة بياناته و لسوء الحظ كثير من المستخدمين يقعون في

[1] بلعويجي، هدى، *إدارة المخاطر في المؤسسة الاقتصادية الجزائرية*، مذكرة ماستر، جامعة المسيلة، الجزائر، 2021، ص28 .

هذا الفخ مما يجعل هذه الوسيلة من أشهر المخاطر التقنية. الهجوم على المواقع الغير مشفرة عبر اكواد محددة تعطل الموقع و يرسلون هذه الاكواد إلى الموقع بمجرد الوصول إليه من اجل التعطيل أو سرقة المعلومات المطلوبة.

-الهندسة الاجتماعية باستخدام مواقع التواصل الاجتماعي و امتلاك مهارات الإقناع للتمكن من الوصول إلى المعلومات و عادة ما يلجا المجرم إلى حيلة التنكر في هوية شخص أخر كمسئول من جهة البنك و غيرها من الجهات الرسمية .

استراتيجيات التحليل و التقييم

1 لابد من تحديد أصول المؤسسة قبل تحليلها و تقييمها ثم تحديد قدر امتثالها لسياسات امن المعلومات، وعليه يتم تقييم المخاطر مبدئيا لاستعراض الخيارات المتاحة من اجل التخفيف من حدة المخاطر. و يركز في الأخير على المخاطر التي لها تأثير اقتصادي سلبي على المؤسسة و التي تسبب الخسائر التالية :

-خسائر تشغيلية ناتجة عن تأثر مستوى التشغيل لمنظومة العمل و استمرارية تقديم الخدمات الرقمية بسبب أعمال التخريب و إصابة نظم المعلومات بفيروسات الكمبيوتر أو توقف الخدمة المقدمة للعملاء .

- خسائر قانونية نتيجة العقوبات المالية المنصوص عليها في العقود القانونية نتيجة إفشاء المعلومات لأفراد أو جهات غير مصرح لهم بمعرفتها.

- خسائر مالية بسبب الإخلال بالاتفاقيات و فقدان السرية.

- خسائر إستراتيجية بسبب تأثر الإيرادات المستقبلية و فقدان العملاء و تأثر سمعة المؤسسة.

إستراتيجية إدارة المخاطر :

بمجرد تحديد المخاطر و منهجية حمايتها يبدأ الاختيار بين احد الأساليب الموالية :

-تجنب التهديدات لان المعدات التقنية لا ترقى للحماية.

- تقليل المخاطر عبر تنفيذ ضوابط التخفيف من المخاطر.

- قبول المخاطر لفترة من الزمن إذا كانت التكلفة تزيد عن العائد المتوقع.

- التامين على التكنولوجيا المستخدمة لدى طرف أخر كشركة التامين.

مرحلة التحليل :

توفر هذه العملية المعلومات التي تستند إليها المؤسسة في إعطاء الأولوية للمخاطر بناءا على احتمالية وقوعها و من ثم التدابير ألازمة لإدارة تلك المخاطر. و من الطرق المعتمدة

- تحليل ربطة العنق التي هي عبارة عن أداة بصرية تستعملها المؤسسات لاكتشاف مسببات المخاطر.[1]

[1] المرجع نفسه.

- مصفوفة تحليل المخاطر أداة بصرية تصنف المخاطر في محورين يتضمن الأول احتمالية حدوث الخطر بينما يتضمن الثاني شدة تأثير الخطر في حال وقوعه، و في كل خلية نجد

سيناريو مخاطر محدد و يتم تحديد مستوى مخاطر مناظر بناءا على تقاطع الاحتمال و الشدة.

-تحليلSWIFT و معنى هذه كلمة التقنية التي تعتمد على طرح سؤال ماذا لو what if technique ، و هي عملية تعتمد على تحليل المخاطر باستخدام جلسات العصف الذهني المبرمجة للتنبؤ بالأحداث التي ممكن أن تقع في سيناريوهات معينة.

- تحليلDELPHI و هي إستراتيجية تعتمد على إنشاء فريق من المحللين و الاخصائين في إدارة المخاطر و الحصول على أرائهم.

- تحليل شجرة القرار التي تعد تمثيل بياني يحتوي على القرارات و عواقبها المحتملة و من خلالها تحدد المؤسسة مختلف الخيارات المتاحة بطريقة منهجية و تتعرف على نتائج كل خيار، و تستفيد منها عندما تحتاج إلى اتخاذ قرارا معقدا في ظل تعدد الخيارات و بدائلها و في النهاية يتم تحليل و اختيار المسار الأفضل.

- مصفوفة الاحتمالات و النتائج و بهذه الطريقة يتم حساب التأثير المحتمل للمخاطر و تنفذ في المراحل الأولى من المشاريع أو في حال نقص في البيانات الكمية ، و على إثرها تصنف التهديدات إلى مستويات عالية أو متوسطة أو منخفضة حتى تحدد المؤسسة المخاطر التي تتطلب اهتماما فورا و من ثم تبدأ في تخصيص الموارد لها.

الفوائد الرئيسية لتحليل المخاطر :

-تقليل حالة عدم اليقين من خلال تحديد الاختراقات المحتملة في وقت مبكر،مما يؤدي الى ثقة اكبر في عملية اتخاذ القرار.
- تحسين التخطيط و تخصيص الموارد بشكل أفضل و تقدير الجدول الزمني و التخطيط للطوارئ، و بالتاي حماية تلك الموارد. تعزيز نتائج مشاريع الخاصة بالمؤسسة عبر تقليل الاضطرابات و ضمان التسليم في الوقت المناسب و الحفاظ على معايير الجودة.

مرحلة رصد و تقييم :

تحديد قيمة المعلومات فلا يمكن حماية شيء مجهول، و معظم المؤسسات لا تملك ميزانية ضخمة لإدارة المخاطر مما يستلزم تحديد نطاق الأصول الأكثر أهمية للأعمال. و عليه تقوم ادارة استمرارية الاعمال بتنفيد هده المرحلة على تقييم و تصنيف الخطر بناءا على مصفوفتي تقييم اثر الانقطاع و تقييم احتمالية التهديد.[1]
يتم احتساب درجة المخاطر الكامنة عبر المعادلة التالية :

[1] المرجع نفسه.

درجة المخاطر الكامنة = الاثر* الاحتمالية.
و حسب الخريطة الحرارية للمخاطر يتم تصنيف المخاطر بناءا على مستوى قبول الخطر لدى المؤسسة ، حيث يتم قبول او ادارة مخاطر التعطل المنخفضة و المتوسطة و لكن لا يمكن قبول مخاطلر التعطل العالية.

الفرع الثاني : خطط استمرارية الأعمال في حال الهجمات و الأعطال

استمرارية الأعمال هي قدرة المؤسسة على الحفاظ على وظائف الأعمال الحيوية و تقليل فترة التعطل في حالة حدوث أزمة كالهجمات الالكترونية و انقطاع الكهرباء غير المتوقع يجعل من الصعب أو حتى من المستحيل على المؤسسة مواصلة العمل كالمعتاد، فيمكن أن تؤدي الحوادث الطبيعية إلى فقدان الطاقة الكهربائية المستخدمة لتشغيل المرافق أو خدمات تكنولوجيا المعلومات الهامة و بالتالي يمكن للكيانات الإجرامية أو الدول القومية مقاطعة العمليات أو الاحتفاظ بالبيانات للحصول على فدية .

و على سبيل المثال، عندما تكون هناك شركة تمويل متمركزة في احد المدن الكبرى، يمكن أن تشمل خطة استمرارية العمل لديها نسخ المعلومات و البيانات الخاصة بعملائها على خوادم خارجية خارج موقع الشركة، و بالتاي في حال وقوع أي عطل في موقع الشركة، لا يوجد قلق بشان فقدان تلك البيانات، حيث يمكن الوصول إليها من أي فرع تابع للشركة. و مع ذلك هناك نقطة مهمة و هي أن خطة استمرارية العمل قد لا تكون فعال عندما تؤثر الكارثة على عدد كبير من الأشخاص ، مثل انتشار الأوبئة. ومع ذل فإنها قادرة على تحسين إدارة المخاطر و الحد من انتشار أثارها بشكل أوسع، ما يرتب توفير التكاليف، فالإستراتيجية تحدد الحلول الواجب تطبيقها لاستعادة أعمالها وفق الأوقات المستهدفة.

و تتضمن الإستراتيجية على تفاصيل الموارد اللازمة لتطبيق هذه الحلول و لا تنحصر الموارد على الجانب المالي بل يمتد إلى الكادر البشري و المعدات و الأنظمة و غيرها من الموارد.

و تتنوع احتياجات المؤسسة عند تشكيل إستراتيجية ناجحة لاستمرارية الأعمال و تختلف الخطط تبعا لحجم المؤسسة و الصناعة و احتياجات الأعمال و المخاطر المحتملة التي قد تواجهها، و هذا هو السبب في أن جميع المنظمات بحاجة إلى خطة المسماة ب (BCP) .

و إن استمرارية الأعمال ليست عرضا دائما، يجب ممارسة الخطة و اختبارها بانتظام حتى يكون الأشخاص على دراية بمسؤولياتهم و يمكن تحديد الثغرات في الخطة وإغلاقها. [1]

و التي تحتوي على ثلاث مراحل ونذكرها على النحو التالي :
1 الاستجابة الأولية بتحديد شدة الضرر بعد اكتشاف الاضطراب، و سيقوم بسرد الإجراءات التي يجب اتخاذها، لذلك يتطلب الأمر فقط مواكبة الضرر مع تدابير الاستجابة المناسبة.

[1]. أحمد محمد علي، *إدارة المخاطر واستمرارية الأعمال في المؤسسات المعاصرة*، دار الجامعة الجديدة، القاهرة، 2021، ص. 45

2 نقل المناطق المتضررة من العمل بعيدا عن الأذى، كحالة تلف البنية التحتية نحتاج إلى نقل المعدات إلى جزء أخر من المكتب.
3 التعافي و إصلاح المشكلة بعد عزل المنطقة المتضررة باسترجاع الأنظمة و الخدمات خلال وقت قياسي بعد أي حادث.

المكونات الرئيسية لتخطيط استمرارية العمل:

يهدف التخطيط القوي أيضا إلى تجنب استياء العملاء و تقليل الجداول الزمنية للتعافي و العودة إلى النشاط بسرعة. و لتحقيق زيادة الثقة في فريق العمل، و منه نذكر فرق الاستجابة للحوادث المتكونة من فرق إدارة الأزمات و فرق التعافي من المخاطر على النحو التالي:

فريق الاستجابة للحوادث:
يعمل بشكل فوري في حال وقوع الخطر للتأكد من سلامة الموظفين و أصول المؤسسة، و يتكون من إدارة الأمن و السلامة و إدارة المباني.

فريق إدارة الأزمات :
تركز خطة إدارة الأزمات على المشاكل التي تواجهها المؤسسة و آلية التعامل معها، فتحتوي الخطة على مهام أعضاء فريق إدارة الأزمات و مسؤولياتهم و مؤشرات تفعيل خطط التعافي و فرق الاستجابة، كما تشير الخطة إلى أصحاب المصلحة و الجهات الخارجية اللازم إبلاغها عند وقوع الأزمات.

و بالنسبة إلى فريق إدارة الأزمات يبدأ عمله عند إصدار توجيه من القائد أو المؤول أو من ينوب عنه على تقييم النتائج المحتملة المتعلقة بالعمليات الحرجة، و من ثم يتم اخذ قرار تفعيل خطة استمرارية الأعمال و تحديد الوقت المتوقع لاستئناف الأعمال.
كما لفرق الأزمات مهمة أخرى و هي توجيه الفرق الأخرى بالمهام اللازمة.

فريق تعافي الأعمال:

خطط تعافي الأعمال خاصة باستعادة أعمال الإدارات التي تمتلك إجراءات حرجة قد يؤثر انقطاعها على المؤسسة، و تقدم نسخة منها لدى جميع فرق التعافي في الدارة. و تشمل الخطة على جميع الإجراءات الحرجة و أوقات استعادتها و منظومة التواصل الداخلي و جميع الموارد البشرية و التقنية و المعدات اللازم توافرها لاسترجاع الخدمات.

و يعمل فريق تعافي الأعمال على إعادة الخدمات المنقطعة خلال مدة محددة لا تتجاوز الفترة الزمنية القصوى المسموح بها للانقطاع، بالإضافة إلى رفع التقارير إلى إدارة الأزمات.[1]

[1] المرجع نفسه.

عوامل نجاح استمرارية الأعمال
ليتم تعزيز دور خطط استمرارية الأعمال و ضمان تحقيقه للأهداف المرجوة منه، نحصر أهم العوامل الممكنة لذلك :

- وجود دعم من مسئولي المؤسسات لتنفيذ إستراتيجية استمرار الأعمال.

- إنشاء لجنة رسمية خاصة مكونة من فريق قيادي لإدارة الخطط تسهم في إبراز النهج الرسمي و التنسيق فيما بين إدارات المؤسسة.

- مواءمة إستراتيجية الأعمال مع نهج إدارة المخاطر و ضمان التكامل فيما بينهما.

- اتاحة الموارد المالية و البشرية الكافية لاستحداث وظائف ادارة استمرارية الاعمال و الحفاظ على استمرار عملية تنفيذها.

- رفع الوعي حول اهمية هذه الخطط عبر ورش العمل و التمارين و الاختبارات و الحملات التوعوية الداخلية.

الفرع الثالث : ادارة الازمات الالكترونية و الاستجابة للحوادث

ادارة الازمات يركزعلى الجوانب التقنية لإدارة الحدث الأمني، فإن إدارة الأزمات تأخذ منظورا أوسع. يتضمن التنسيق العام لاستجابة المنظمة للأزمة بطريقة تعالج التحديات التشغيلية والتواصلية معا. تهدف إدارة الأزمات إلى الحفاظ على الثقة بين أصحاب المصلحة أو استعادتها، والتخفيف من أي آثار سلبية، وضمان قدرة المنظمة على العودة إلى العمل كالمعتاد بأسرع وقت ممكن.[1]

بينما الاستجابة للحوادث هو النهج المنظم لمعالجة وإدارة تبعات الخرق الأمني أو الهجوم السيبراني. الهدف الأساسي من الاستجابة للحوادث هو السيطرة على الوضع، والحد من الأضرار المحتملة، وتقليل المخاطر المرتبطة بالحادث. تشمل خطة مفصلة تحدد استراتيجية الشركة للتعامل مع التهديدات المحتملة، لضمان أن يكون الاستجابة سريعة وفعالة وأقل قدر من الاضطراب في العمليات عند وقوع حادث

و ينبغي ان تضع المؤسسات اجراءات للابلاغ عن بيانات الحوادث وتحليلها و مشاركتها و استخدامها داخليا. و تقاطع هذه التخصصات هو حيث يكمن الفن الحقيقي لتجاوز العاصفة الرقمية. في هذا المفترق يتقاطع التقنية مع التكتيك، حيث يتقاطع التخطيط الاستراتيجي مع التواصل الفعال، وحيث يتم اختبار وتشكيل مرونة المنظمة.

[1]. أمينة غربي وآخرون، *دور تكنولوجيا المعلومات والاتصال في إدارة الأزمات في المؤسسة*، جامعة الوادي، 2023 .

الاستجابة للحوادث خطوة بخطوة:

عند اكتشاف أن بيانات المؤسسة الحساسة قد تعرضت للاختراق، وأن ثقة العملاء قد تضررت، وأن العمليات توقفت تمامًا. يمكن أن تكون عواقب الهجوم السيبراني ساحقة، لكن الاستجابة الفعالة يمكن أن تصنع الفارق بين كارثة واستعادة ناجحة عبر الخطوات الاساسية .التي يجب اتباعها:

الكشف و التعرف: التعرف على حدوث الهجوم السيبراني من خلال أدوات المراقبة والكشف في النظام

- الاحتواء : عزل الأنظمة المتأثرة لتجنب المزيد من الأضرار وإيقاف انتشار الهجوم.

الوضع المتدهور : إعادة تشغيل الخدمات الحيوية في وضع متدهور إذا كان الحادث قد أوقف خدمات هامة.

- الازالة : القضاء على البرمجيات الخبيثة وتصحيح الثغرات لإزالة التهديد.

- الاسترداد : استعادة الأنظمة والبيانات إلى حالتها السابقة للهجوم مع ضمان أمانها ووظيفتها.

- التواصل : إبلاغ الأطراف المعنية، إشعار المعنيين، والتنسيق مع السلطات القانونية.

- التوثيق و التحليل : تسجيل الحادث وجهود الاستجابة لأغراض المرجعية المستقبلية والتعلم.

- مراجعة ما بعد الحادث : فحص الحادث، تحديث سياسات الأمان، وتدريب الموظفين لتحسين الاستجابات المستقبلية.[1]

المطلب الثاني : الحوكمة الرقمية و دورها في حماية الخدمات

الحوكمة الرقمية هي الإطار التنظيمي و التشريعي الذي يدير استخدام التكنولوجيا، و أسفرت النتائج عن التحول نجو النظم الرقمية ليس مجرد خيار تقني، بل توجه استراتيجي يهدف إلى رفع كفاءة المؤسسات الاقتصادية للاستجابة لاحتياجات المجتمع من خلال وضع سياسات صارمة لأمن المعلومات

الفرع الأول : مفهوم الحوكمة الرقمية في المؤسسات

الحوكمة الالكترونية هي إحدى طرق استخدام التكنولوجيا الحديثة لتحسين عمليات الحكم و الإدارة في المؤسسات لتكريس تسهيل الإجراءات الإدارية و زيادة الشفافية و المشاركة المجتمعية. و يقتضي الاعتماد على أسلوب الحوكمة الالتزام بمجموعة من المبادئ و القوانين التي من شانها إنجاح العملية الحيوية، و التجارب قد أثبتت أن التخلي عن هذا النمط

[1] Grispos, G. et al., *Security Incident Response Criteria*, 2015.

من الإدارة يعني بالضرورة فشل المشاريع المبرمجة أو عدم تحقيق الأهداف بالصورة المرضية على اقل تقدير.

و تعرفها منظمة التعاون الاقتصادي و التنمية بأنها مجموعة من العلاقات بين إدارة الشركة و مجلس إدارتها و مساهميها و ذوي المصلحة الآخرين، و تقدم حوكمة الشركات الهيكل الذي من خلاله توضح أهداف الشركة و تعين وسائل انجاز تلك الأهداف و الرقابة على الأداء.

و علافها البنك الدولي بأنها الحكم الراشد المرادف للتسيير الأمثل الذي يسعى للإجابة على مختلف الانتقادات الموجهة للشركات التي تشكك في الإصلاحات الهيكلية المسيرة بطريقة علوية أي من الأعلى إلى الأسفل.

و بالتالي يمكن القول بان الحوكمة هي تلك النظام الذي يتم عبره إدارة و توجيه و تنظيم المؤسسات، لتحقق رسالتها و الأهداف المرسومة لها، و عليه ضمان مصالح جميع الأطراف من مدراء و مستخدمين أو زبائن، شركاء أو مساهمين و غيرهم. و بشكل خاص الحوكمة الرقمية هي استخدام التكنولوجيا في إدارة و تسيير المؤسسات وفق معايير الحوكمة، و عصرنة أداء الخدمات الرقمية.[1]

مبادئ الحوكمة :
تتمثل في ستة مبادئ اساسية :

-الشفافية : حرية تدفق المعلومات الى المعنيين دون شرط، فاحتكار وصول المعلومات الى اخرين غير المعنيين يؤثر على العلاقات بين هؤلاء و ادارة المؤسسة سلبا.

- المشاركة : فالسياسة المؤسساتية تقتضي مشاركة الافراد المنتمين للمؤسسة في ادارة المؤسسة و خصوصا اثناء اتخاذ اقرارات، مما ينمي انتماءهم للمؤسسة و من ثم ولاءهم و زيادة الاداء.

- المساءلة : و هي مساءلة كل مسؤول عن اداءه في المؤسسة، و تحفيزه عند الاخلاص .

- المسؤولية : معناها وجوب القيام بالمهام الملقاة على عاتق كل فرد في مجلس إدارة المؤسسة فضلا عن التقصير و الإهمال، مما يولد الرقابة و اليقظة على العمليات.

- العدالة و المساواة : إتاحة الفرص دون استثناء مهما كانت الأسباب و لكن تكون المفاضلة بين الجميع على أساس الكفاءة و الانجاز.

الاستقلالية : حرية العمل في حدود قانونية دون الضغوطات الخارجية كتقديم المصلحة الشخصية عن مصلحة المؤسسة او ما يعرف بتعارض المصالح.

[1] لعيداني نعيمة، كشرود بشير، *تطبيق نظام الحوكمة بالمؤسسات الإعلامية*، جامعة الوادي، 2022.

مبادئ الحوكمة الالكترونية
نجمعها في النقاط التالية

-القيمة المضافة عند تحقيق جودة الخدمات و الميزة التنافسية مما يحقق قيمة أكثر لتلبية احتياجات المستخدمين.

- الانسجام الاستراتيجي تناسق بين أهداف المؤسسة و التكنولوجيا من حيث الفعالية.

- إدارة الموارد كل من الموارد البشرة و التقنية وجب حسن إدارتها، إلزامية تكوين الموظفين و تحصيل الموارد التكنولوجية و التأكد من تحقيقها لأهداف المؤسسة.

- قياس أداء العاملين و جودة الخدمات وفعالية الوسائل التكنولوجية باستخدام مجموعة من المؤشرات التي تقوم بالتحليل و الإحصاء الكمي للمعطيات.

- إدارة المخاطر و الإلمام بها باستخدام امن المعلومات و الحفظ الرقمي.

العلاقة بين الحوكمة الرقمية و التحول الرقمي تتبلور في كون التحول الرقمي هو الوسيلة الأساسية لتحقيق الحوكمة من خلال تطوير البنية التحتية التكنولوجية، و مثال على الانسجام بينهما هو حينما يتطلب تقديم الخدمات الالكترونية وجود قوانين تنظم المعاملات و التوقيع الرقمي و حجية الأدلة الالكترونية.

و حين تطبيق و استخدام الذكاء الاصطناعي في اتخاذ القرارات الإدارية يتطلب وضع معايير أخلاقية و قانونية تضمن عدم وجود تحيزات في هذه القرارات و تحدد المسؤولية في حالة وجود أخطاء. تساهم الحوكمة الرقمية في ضمان استخدام الذكاء الاصطناعي بشكل مسؤول اعبر وضع مبادئ توجيهية لاستخدامه و تحديد آليات للرقابة.

هناك ايضا انظمة يمكن للمؤسسات الاعتماد عليها لتعزيز حوكمتها مثل

نظام دوك سويت و هو نظام متكامل لادارة الوثائق و الاتصالات الإدارية حيث يسهم في أتمتة عمليات الحوكمة و الامتثال التنظيمي.

نظام خدماتي، الذي يتيح متابعة أداء المؤسسات و تقييم الامتثال للسياسات الداخلية و الخارجية.[1]

الفرع الثاني: دور مجلس الإدارة في الأمن السيبيراني

تواجه مؤسسات اليوم مطالب متزايدة لتبني التقنيات الجديدة من اجل الحفاظ على قدرتها التنافسية في السوق و عليه سنتعرض إلى مهمة و ادوار التي يلعبها أعضاء مجلس الإدارة في قيادة مؤسساتهم فيما يتعلق بهذا الشأن. و من ثم يتم تعيين خبراء التكنولوجيا و إنشاء لجان

[1] صالح أحمد مفتاح، *الحوكمة الرقمية ودورها في رفع جودة الخدمات وتحسين الأداء المؤسسي*، المجلة الشاملة للدراسات الإنسانية والتربوية، 2025

التكنولوجيا على مستوى مجلس الادارة و تفويض المسؤوليات إلى لجنة التدقيق كوسيلة لإدارة المخاطر و فهم الدور الحالي و المستقبلي لآليات الحوكمة .

الهيكل التنظيمي لمجلس الإدارة

مجلس الإدارة أو ما يدعى بفريق الأمن السيبيراني يمثل الهيئة التي تحكم المؤسسة يتم اختياره من مجموعات مختلفة من المساهمين و هو مسؤول عن مراقبة تنفيذ أهداف المؤسسة كما حددتها الجمعية العامة. بالنسبة للأفراد المكونين له يتم انتخابهم و يعملون وفق مصالح المالكين، و عليه فمجلس الإدارة هو عبارة عن مجموعة من الأعضاء يفوضهم المساهمون عن طريق الجمعية العمومية للمستثمرين من اجل إدارة المؤسسة و هم يدينون بإخلاصهم للمؤسسة و يخضعون للمساءلة من طرف المساهمين.

و يتمثل دور مجلس الادارة في الامن:
دور مجلس الادارة يتمثل في الرقابة الفعالة و القيادة الاستراتيجية فهو من يوجه المؤسسة لبناية درع حماية قوي، و توزيع المسؤوليات لفرق الادارة النفيدية من اجل حماية الاصول من التهديدات و ضمان استمرارية الاعمال.

و نلخص الجهود التطبيقية في حوكمة الامن السيبيراني بالبنوك العمومية الجزائرية كتطبيق عملي على دور جهاز الحماية في المؤسسات :

-استحداث لجنة الاستقرار المالي المكلفة بالرقابة الاحترازية الكلية و الادارة الفعالة للازمات.
اللجنة الوطنية للدفع المكلفة بتطوير وسائل الدفع الالكترونية.
- الدينار الرقمي الجزائري توسيع وسائل الدفع لتشمل الشكل الالكتروني.
- النظام 24_04 المؤرخ في 13 اكتوبر 2024 المتعلق بالشروط الخاصة للترخييص بتاسيس واعتماد ممارسة نشاط البنك الرقمي و المادة 6 منه تنص على يجب ان يؤسس البنك مقرا اجتماعيا لتلقي الشكاوى و من اجل الإغراض الإدارية.
- ضمان سلامة التقارير المحاسبية و المالية للشركة بتعيين مدقق مستقل.
- الإشراف على عمليات الإفصاح و الاتصالات.

التعيينات في مجلس الإدارة

-تكون التعيينات وفق إجراءات رسمية و شفافة لترشيح مدراء أكفاء و جدد في الإدارة.
- إلزامية تكوين الاعضاء مرة واحدة كل عام على الأقل لضمان حسن الأداء و تحقيق العضوية المتوافقة مع احتياجات المجلس.
- يجب على جميع المديرين أن يقدم لإعادة انتخابه على فترات منتظمة و مرة على الأقل كل ثلاث سنوات.

- عقود خدمة المديرين التنفيذيين لا تزيد على ثلاث سنوات قابلة للتجديد و لكن بعد موافقة المساهمين بناءا على توصية المجلس.[1]

الفرع الثالث : الامتثال للمعايير القانونية و الرقمية

في عالم مليء بالتحديات الرقمية و تزايد حجم و نوع البيانات و الخدمات الرقمية، اصبح الامتثال لقوانين حماية البيانات أمرا حيويا لضمان امن المعلومات.

نقصد بالامتثال الالتزام بالقوانين و السياسات التي تنظم عمل المؤسسات، سواء خارجية أو داخلية، يعني أن المؤسسة تعمل وفقا للمعايير المحلية و الدولية، و هو ليس مجرد التزام قانوني لتجنب المخالفات بل يعد عاملا أساسيا في بناء سمعة المؤسسة و ثقة الأطراف ذات الصلة بها و لقدرتها على النمو و التوسع.

و أن ابرز الفوائد المباشرة للامتثال القانوني انه يحد من تعرض المؤسسة للعقوبات المالية و الإدارية، و في عالم الأعمال الحديث لم تعد الجهات المختصة بالرقابة تتساهل مع المخالفات، خاصة في القضايا المتعلقة بالبيانات و الخصوصية و مكافحة الفساد و حماية المستهلك.

و عليه وجود نظام فعال لا ينظر إليه انه إهدار للموارد المادية أو تكلفة إضافية، بل استثمارا وقائيا يحمي المؤسسة من خسائر اكبر قد تنتج من عدم الالتزام و لن تعاني من الغرامات فقط بل تمتد إلى تعطل العمليات و استنزاف الإدارة في المتابعة القانونية و تراجع ثقة الغير. [2] كيفية تطبيق إدارة التزامات

حماية البيانات و الخصوصية .
- التحكم في الوصول و الصلاحيات من خلال تحديد مستويات مختلفة من الوصول للمستخدمين، بناءا على دورهم و صلاحياتهم و هدا يمنع الوصول الغير مصرح به إلى المعلومات الحساسة.
- توثيق السياسات و الإجراءات التقارير و المتابعة و تكون تقارير دورية حول حالة التزامات الامتثال من قبل المشرفين و اتخاذ القرارات اللازمة للتحسين و تقديم التقارير للجهات المختصة.

كيفية إنشاء خطة امتثال عالمية

بعد التعرف على اللوائح و المعايير التي يجب الالتزام بها، يحين وقت بدء العمل على خطة الامتثال.

---

[1] .غلاب فاتح، *دور مجلس الإدارة في مراقبة تطبيق حوكمة الشركات في المؤسسة الجزائرية للأقمشة الصناعية والتقنية*، جامعة المسيلة/الوادي، 2019

[2] الامتثال في الشركات، مدونة ملتزم، تاريخ الاطلاع : 6 جوان 2026، Moltazim.com .

الخطوة الأولى، تشكيل فريق الامتثال فلتشكيل الفريق أو قيادته في كلتا الحالتين توزع الأدوار و المسؤوليات على النحو التالي:

مدير الامتثال يضع الاستراتيجيات العامة للإدارة و يشرف على تنفيذها.

- رئيس قسم مكافحة غسل الأموال الذي ينسق السياسات المعنية بمكافحة غسل الأموال.
- محلل يدير عمليات التحقق من هوية العملاء و يتولى المهام اليدوية الضرورية.
- التعاون الشامل تشير تجارب بعض الخبراء إلى أن نجاح قسم الامتثال يعتمد بشدة على مدى
- تواصله مع بقية الإدارات، بما يضمن تحقيق أهداف المؤسسة و التقيد بالأنظمة.
- التدريب المستمر فنظرا للتحديثات التي تطرأ على اللوائح فان التدريب المستمر يعد أهم الأنشطة لكافة الفريق.

الخطوة الثانية، تقييم المخاطر و تحديد النطاق

التقييم لان فهم طبيعة المخاطر كما شرحنا سابق يعد عنصرا أساسيا، خصوصا عند التعامل مع عدد كبير من المستخدمين لأنه يساعد على حصر ابرز النقاط المحتملة التي تقود الى تعريض المؤسسة لمشاكل رقابية.

تحديد النطاق الجغرافي قد تتداخل بعض التشريعات الخاصة بكل بلد او تتعارض لذا يجب توفر تصور واضح بكل القوانين المطبقة.

الخطوة الثالثة ، مراجعة القوانين المحلية و الدولية

فمن الضروري الإلمام بقوانين الأسواق الرئيسية كمعايير الأمان مثلISO 27001.
السياسات الداخلية التي تأتي بعد حصر المتطلبات الخارجية و تطبق على كافة أقسام المنظمة بروتوكولات العناية الواجبة .
أدلة التعامل مع التنبيهات المحتملة أثناء عمليات الفحص.
تضمين إجراءات حماية البيانات.

الخطوة الرابعة، اعتماد الحلول التكنولوجية

هنا يأتي دور الحلول التقنية التي تتيح أتمتة المهام و توسيع نطاق عمليات الامتثال عبر الذكاء الاصطناعي خاصة إذا كانت قاعدة المستخدمين ضخمة.

الخطوة الخامسة،المراقبة و التدقيق المستمر

من مراقبة المستخدمين بصفة دائمة، فضلا عن تتبع العمليات المالية و اجرتء تدقيقات منتظمة.

المراقبة المستمرة ما يقارب 80% من عمليات الاحتيال تظهر بعد مرحلة تسجيل العميل.
لذلك، توصي الهيئات العالمية مثل GAFI بالمراجعة الدورية لمراقبة أي إشارات تحذيرية محتملة قد تظهر بمرور الوقت[1].

مراقبة المعاملات إذا ظهرت معاملة تنافي تاريخ المستخدم المتوقع، ينبغي التحرّك وإجراء التحقيق اللازم

التدقيقات سواء كانت داخلية للتأكد من سلامة العمليات أو خارجية للحصول على شهادات تُعزز المصداقية أمام المستثمرين والجهات التنظيمية.
تحديد مؤشرات الأداء الأساسية يشمل ذلك معدل الإيجابيات الكاذبة والسلبية، ومتوسط زمن

التحقق، وتكلفة التحقق الواحدة، ومستوى رضا المستخدم.

الخطوة السادسة، إمكانية التوسع و التكيف مع التغيير

تُعدّ المرونة في التوسّع أمرًا حاسمًا في بيئة تنظيمية دائمة التبدّل. كما ذكرنا في البداية، يجب أن يكون برنامج الامتثال قادرا على النمو مع المؤسسة والتأقلم مع القوانين الجديدة دون تعقيد سير العمل، و دلك من خلال التأهب المسبق للتغيرات كن على إطلاع دائم بآخر تحديثات وغيرها من الجهات الرقابية الدولية. لذا يُستحسن ابتكار آليات مرنة تتيح تكييف الإجراءات سريعًا عند ظهور توجيهات جديدة.

معرفة الأسواق الحديثة فالحلول الرقمية المعتمدة تدعم التحقق من وثائق معظم بلدان العالم و هدا يساعد في التوسع الجغرافي
التحسين المستمر :اجمع ملاحظات الموظفين والعملاء باستمرار لتطوير العمليات وجعلها أكثر سلاسة وفعالية[2].

[1] التوقيعات الرقمية و اعرف عميلك : ثنائي الامان و الامتثال، ديديت، ، تاريخ الاطلاع : 6 جوان 2026 https//:didit.me .
[2] المرجع نفسه.

خاتمة

تطرقنا في دراستنا هده إلى موضوع إدارة و حماية الخدمات الرقمية في المؤسسة الاقتصادية، و دلك لكون انه موضوع دو أهمية كبيرة خاصة في الآونة الأخيرة، و كذلك كون أن العديد من الأشخاص لا يزال يجهلون كيفية إدارة و حماية الخدمات الرقمية، و يوجد العديد من يمارس هده النشاطات بدون الالتزام بالشروط المنصوص عليها، و هدا يعود لعدم دراية البعض منهم و تهاون البعض الأخر على الالتزام، رغم أن عدم الالتزام بهده الضوابط و الشروط القانونية يؤدي إلى التعرض إلى المساءلات و لعقوبات و إلى الخسائر المادية.

و على الرغم من المميزات التي تميز الخدمات الرقمية و محاولة التشريعات و التنظيمات وضع نظام قانوني لها إلا أنها لا تزال تواجه العديد من المشاكل تعيق تقدم أنشطتها و دلك راجع لعدم كفاية التقنيات الفنية و التنظيم التشريعي الكامل المحلي و الدولي.

و في نهاية هده الدراسة التي حاولنا الإلمام بكل جوانبها، نخلص إلى عدة نتائج و اقتراحات

النتائج :

- إدارة الخدمات الرقمية نشاط عابر للحدود تتم بواسطة تبادل البيانات عن طريق الوسائل الالكترونية الحديثة.

- الإدارة الفعالة للخدمات الرقمية تساهم في ضمان استمرارية النشاط الاقتصادي و تعزيز كفاءتها التشغيلية.

- رغم المزايا الكثيرة التي تتميز بها الخدمات إلا أنها محاطة بالعديد من المخاطر القانونية و الجرائم المعلوماتية.

ترتبط فعالية حماية الخدمات الرقمية بوجود إستراتيجية شاملة تجمع بين الجوانب التقنية والتنظيمية و البشرية.

-يعتبر تطبيق سياسات امن المعلومات احد اهم الوسائل لحماية الأصول الرقمية و الحد من المخاطر الالكترونية.

و على ضوء ما سبق ولمواجهة التحديات التي تواجه الخدمات الرقمية و حمايتها و إدارتها نقترح التوصيات التالية :

- محاولة نشر الوعي المعرفي و التعريف بهده الخدمات و الوسائل الخاصة بحمايتها و إدارتها لتجنب الوقوع في المخاطر و معرفة طرق التصرف حتى لا يبقى العميل الطرف الأضعف.

- تطوير وتعزيز البنية التحتية من حيث جودة شبكات الاتصال وتحسينها بشكل يسهل التعامل

- مراقبة الأشخاص الغير متقيدين بالشروط المنصوص عليها بشكل اكبر و تسليط العقوبات اللازمة عليهم.

- دعم كل النشاطات التي من شانها تطوير هذا النوع من الخدمات و الحفاظ على اداءها و التي لا تخالف ما نص عليه القانون.

وفي الختام، فإن نجاح المؤسسات الاقتصادية في تحقيق التحول الرقمي لا يعتمد فقط على امتلاك التكنولوجيا، بل يرتكز أيضًا على حسن إدارتها وحمايتها من المخاطر المحتملة، من خلال تطبيق السياسات الأمنية، وتدريب الموارد البشرية، والالتزام بالمعايير الدولية في إدارة الخدمات الرقمية. ويسهم ذلك في تعزيز ثقة العملاء والشركاء، وتحقيق ميزة تنافسية، ودعم النمو والاستدامة في بيئة اقتصادية تتسم بالتطور الرقمي المتسارع.

قائمة المصادر و المراجع

اولا : المصادر

النصوص القانونية

القوانين الوطنية

النصوص التشريعية

قانون رقم 15-04 مؤرخ في 01 فبراير 2015، يحدد القواعد العامة المتعلقة بالتوقيع و التصديق الالكترونيين، ج رج ج. عدد 6، صادر ف 10-02-2015.

القانون رقم 18-05 مؤرخ في 24 شعبان عام 1439 الموافق 10 مايو 2018، المتعلق بالتجارة الإلكترونية، نُشر في الجريدة الرسمية رقم 28 بتاريخ 16 ماي 2018.

القانون رقم 26-02 المؤرخ في 17 فبراير 2026، يحدد القواعد العامة المتعلقة بخدمات الثقة للمعاملات الإلكترونية وبالتعريف الإلكتروني، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد14.

ثانيا: المراجع

الكتب

كتب عامة

1 ابن منظور، أبو الفضل جمال الدين محمد بن مكرم، لسان العرب، دار صادر، بيروت، ط3، 1414 هـ، جـ 12، ص166 .

كتب خاصة

1 أحمد محمد علي، *إدارة المخاطر واستمرارية الأعمال في المؤسسات المعاصرة*، دار الجامعة الجديدة، القاهرة، 2021، ص45.

2 أمينة غربي وآخرون، *دور تكنولوجيا المعلومات والاتصال في إدارة الأزمات في المؤسسة*، جامعة الوادي، 2023.

3 أمينة قدايفة، *استراتيجية أمن المعلومات*، جامعة أمحمد بوقرة، بومرداس، الجزائر، 2016، ص15.

4 الحارثي، محمد بن علي. امن الشبكات و الحماية من الاختراقات. الرياض، دار المؤيد للنشر و التوزيع،2018.

5 الحشاني، خالد. امن الشبكات و الجدران النارية. دار الكتب العلمية،2018.

6 الماحي فاطمة الزهرة شريفة، مدى فعالية القانون 18-05 المتعلق بالتجارة الالكترونية في حماية المستهلك الالكتروني من تجاوزات الموردين الالكترونيين ، مجلة الاجتهاد للدراسات القانونية و الاقتصادية، المجلد10، الع3 ،تامنغست،2021.

7 بيبر، البرشت.(2018). علم التشفير(ترجمة مؤسسة هنداوي). مؤسسة هنداوي للتعليم الثقافة.

8 تومي، ميلود، وعلون، محمد الأمين، "التدقيق الداخلي كآلية للحد من الفساد الإداري والمالي في المؤسسة الاقتصادية"، جامعة الوادي، 2016، ص12.

9 خالد مصطفى قنديل، جرائم تقنية المعلومات و الامن السيبيراني، دار الجامعة الجديدة، مصر،2022.

10 دناي نور الدين، الإيجاب و القبول في العقود الالكترونية، مجلة معالم الدراسات القانونية و السياسية، العدد الثاني،ديسمبر2017،ص 94و95.

11 شريف محمد غنام، محفظة النقود الالكترونية، د ط، دار النهضة العربية، القاهرة، 2003، ص 7.

12 عبد الستار العلي، *التحول الرقمي وإدارة التغيير*، دار المسيرة للنشر والتوزيع، عمان، 2021، ص45.

13 عقبي يمينة، الضمانات القانونية المقررة لحماية المستهلك الالكتروني أثناء تنفيذ العقد في التشريع الجزائري،مجلة معالم للدراسات القانونية و السياسية، المجلد4، كلية الحقوق و العلوم السياسية،سيدي بلعباس، الجزائر، 2020، ص 305.

14 علاء محمد عيد النصيرات، حجية التوقيع الالكتروني في الإثبات، دراسة مقارنة، ط1، دار الثقافة للنشر و التوزيع، الأردن،2005، ص 41 و 42 و 43.

15 عمر بن يونس، النظام القانوني للمعلوماتية (دراسة في ضوء التشريع الجزائري)، دار الثقافة للنشر و التوزيع، عمان، 2024، ض 88.

16غلاب فاتح، *دور مجلس الإدارة في مراقبة تطبيق حوكمة الشركات في المؤسسة الجزائرية للأقمشة الصناعية والتقنية*، جامعة المسيلة/الوادي،2019.

17 لعيداني نعيمة، كشرود بشير، *تطبيق نظام الحوكمة بالمؤسسات الإعلامية*، جامعة الوادي، 2022.

18 محمد الهادي، امن المعلومات و الشبكات، الدار الجامعية، القاهرة ،2019.

فداء محمود حامد، الإدارة الإلكترونية، دار البداية ناشرون وموزعون،ط1، عمان، ،2012 ص88.

19 محمد الصيرفي، الإدارة الالكترونية، دار الفكر الجامعي، ط1، الاسكندرية، ،2006 ص76.

20 محمود عبد الفتاح رضوان، الإدارة الالكترونية و تطبيقاتها الوظيفية،المجموعة العربية للتدريب و النشر، مصر، طبعة1، ص13.

21 بشير عباس العلاق، التسويق عبر الانترنت، دار المناهج، الأردن، ،2003 ص217.

الرسائل و المذكرات

1 عبد الرحمان بن عنتر، "نحو تحسين الإنتاجية و تدعيم القدرة التنافسية للمنتجات الصناعية"، أطروحة مقدمة لنيل شهادة الماجستير في العلوم الاقتصادية، جامعة الجزائر، 2004، ص 158و 152.

2 بلعويجي، هدى، *إدارة المخاطر في المؤسسة الاقتصادية الجزائرية*، مذكرة ماستر، جامعة المسيلة، الجزائر، 2021، ص28.

3 رابحي جوهر، ياسع فاطمة، *التجارة الإلكترونية في القانون 18-05*، مذكرة ماستر، جامعة مولود معمري تيزي وزو، الجزائر، 2021، ص.15.

المجلات

1 إبراهيم عطية محمود المهدي، الحق في الهوية الرقمية في ضوء حماية البيانات الشخصية

والخصوصية المعلوماتية، دراسة وصفية تحليلية مقارنة *مجلة البحوث القانونية والاقتصادية*، جامعة المنصورة،2023،ص500.

2 أستاذ الباحث للدراسات القانونية و السياسية - المجلد04 - العدد02- السنة 2019- ص 1528و1529.

3 ريتشارد هيكس، وساتياروبا شيخار، "التحويل الرقمي، التنمية، والمجتمعات الحضرية المهمشة: إطار تطبيقي لعدالة البيانات"، مجلة *المعلومات والاتصالات والمجتمع*، مجلد 22، عدد 14، 2019، ص. 2092-2111.

4 سعيد اوغان مجلة المعرفة العدد الحادي عشر- دجنبر 2023 الأمن السيبيراني و رهانات التحول الرقمي في المغرب جامعة محمد الخامس الرباط المغرب.

5 صالح أحمد مفتاح، *الحوكمة الرقمية ودورها في رفع جودة الخدمات وتحسين الأداء المؤسسي*، المجلة الشاملة للدراسات الإنسانية والتربوية، 2025.

6 عقبي يمينة، الضمانات القانونية المقررة لحماية المستهلك الالكتروني أثناء تنفيذ العقد في التشريع الجزائري،مجلة معالم للدراسات القانونية و السياسية، المجلد4، كلية الحقوق و العلوم السياسية،سيدي بلعباس، الجزائر، 2020، ص 305.

7 مفيدة طاير مقومات و تحديات تشكيل الهوية الرقمية للمؤسسة في العصر الرقمي، المجلة العلمية للتكنولوجيا و علوم الاعاقة، المجلد2، العدد2020،4، ص220.

8 الخدمات الرقمية و التحول الالكتروني، مجلة الدراسات القانونية، العدد12، 2020.

9 المجلة الدولية لعلوم المكتبات و المعلومات، مج 2 ، ع 2(ابريل- يونيو 2015).

10 حداد ياسر، دور التحول الرقمي في حماية النظام التنافسي للمؤسسات ،مجلة البحوث في العقود وقانون الأعمال، المجلد 10 ، العدد02، 2025 .

المقالات

1عبدلي نزار و آخرون. دور الإدارة الرقمية في تحسين الخدمة العمومية، مؤتمر الإدارة الرقمية،2023.

2 الوزارة الأولى، بيان اجتماع الحكومة المؤرخ في 1 ديسمبر 2025 المتعلق بالبوابة الوطنية للخدمات الرقمية، متاح على الموقع الرسمي،

10 ماي premier-ministre.gov.dz
2026،

المداخلات

1 غليمي رابح، مداخلة بعنوان شرح الأحكام الإجرائية الجديدة للقانون رقم11-25 المعدل و المتمم للقانون07-18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

تجمع النقد الآلي، التقرير السنوي لنشاط الدفع الالكتروني في الجزائر لعام 2025، ص 12.

مواقع الانترنت

1 البنية التحتية الرقمية، صندوق النقد الدولي،2026 مارس، 21.00.
https://www.imf.org.

2 الامتثال في الشركات، مدونة ملتزم، تاريخ الاطلاع : 6 جوان2026،

Moltazim.com.

3 التوقيعات الرقمية و اعرف عميلك : ثنائي الامان الامتثال، ديديت، ، تاريخ الاطلاع : 6 جوان. didit.me//:https

4 elbadilabc-ar.dz://https البديل، الخدمات من الشكل التقليدي الى الشكل الرقمي، بتاريخ 18يونيو2026، سا 5.51،

https:\\www.echchaab.com ، سا14.33، ب21 افريل2026.

https://qafilah.com ، العالم-رقمنة vu le 06/06/2020

7 فريق تحرير راينز، التحول الرقميو الابتكار المؤسسي : دليل شامل لبناء مستقبل رقمي متقدم، مدونة راينز الاستشارية,2 ديسمبر2025، بتاريخ الاطلاع 20 يونيو2026، متاح على الرابط:
https//: reinsagcy.com

المراجع باللغة الاجنبية

النصوص التشريعية

1 U.S.Congress, Health Insurance Portability and Accountability Act of 1996, Public Law 104- 191

المقالات و المداخلات

1 OECD.(2019).Digital Economy Outlook. Paris : OECD Publishing.

2 Hand book on measuring digital Platform employementanl Work, 2023, منظمة التعاون الاقتصادي و التنمية

المواقع الالكترونية

1 https://education-financiere.bcm.mr Banque Centrale de Mauritanie,h 17.22 ,le 20 avril 2026.

2 https://csrc.nist.gov/groups/SMA/fisma/overview.html

3 European University Association (EUA), « Digital Architecture and Digital Services, »

4 https://education-financiere.bcm.mr Banque Centrale de Mauritanie
world Bank.(2021).Digital Development Report.Washington,DC :Word Bank

5 https://www.iso27002security.com/index.html

https://csrc.nist.gov/groups/SMA/fisma/overview.html ,view 19.53, 25 may2026

الفهرس

الفهرس

اهداء

شكر

مقدمة 1

الفصل الأول : الإطار القانوني لحماية الخدمات الرقمية في المؤسسات الاقتصادية.....4

المبحث الأول: مفهوم الخدمات الرقمية و دورها في المؤسسة الاقتصادية.....5

المطلب الأول : ماهية الخدمات الرقمية.....5

الفرع الأول : تعريف الخدمات الرقمية.....5

الفرع الثاني : خصائص الخدمات الرقمية في المؤسسات الاقتصادية .....

الفرع الثالث : أنواع الخدمات الرقمية.....9

المطلب الثاني : أهمية الخدمات الرقمية للاقتصاد و المؤسسة.....12

الفرع الأول : دور الرقمنة في تحسين الأداء الاقتصادي.....12

الفرع الثاني : التحول الرقمي و الابتكار التنظيمي 15

الفرع الثالث : اثر الخدمات الرقمية على تنافسية المؤسسات.....16

المبحث الثاني : الأطر القانونية المنظمة لحماية الخدمات الرقمية.....18

المطلب الأول : القواعد القانونية الوطنية.....18

الفرع الأول : قانون التجارة الالكترونية.....18
الفرع الثاني : قانون حماية المعطيات الشخصية.....23
الفرع الثالث : قانون التوقيع الالكتروني و المعاملات الرقمية.....25
المطلب الثاني : القواعد الدولية و المعايير التقنية المتعلقة بالحماية.....29
الفرع الأول : المعايير الدولية للأمن السيبيراني.....29
الفرع الثاني : التوجيهات الدولية حول حماية المعلومات و الخدمات الرقمية.....31
الفرع الثالث: دور الهيئات الدولية في تنظيم الأمن الرقمي.....32
الفصل الثاني : آليات حماية و إدارة الخدمات الرقمية داخل المؤسسة الاقتصادية
المبحث الأول : الآليات التقنية و التنظيمية للحماية الرقمية.....35
المطلب الأول : آليات الحماية التقنية.....34
الفرع الأول : التشفير و أنظمة الجدار الناري.....34
الفرع الثاني : نظم الكشف و الاستجابة للتهديدات.....37
الفرع الثالث : حماية قواعد البيانات و البنى التحتية الرقمية.....39
المطلب الثاني : آليات الحماية التنظيمية و الإدارية.....41
الفرع الأول : سياسات الأمن المعلوماتي داخل المؤسسة.....41
الفرع الثاني : إدارة الهوية الرقمية و الصلاحيات.....43
الفرع الثالث : إجراءات التدقيق و المراقبة الدورية.....46
المبحث الثاني : ادارة المخاطر الرقمية و الحوكمة الالكترونية في المؤسسة الاقتصادية 48
المطلب الاول : إدارة المخاطر الرقمية..... 48
الفرع الأول : تحليل و تقييم المخاطر التقنية 48

الفرع الثاني : خطط استمرارية الاعمال في حال الهجمات و الاعطال.....51
الفرع الثالث : ادارة الازمات الالكترونية و الاستجابة للحوادث 53
المطلب الثاني : الحوكمة الرقمية و دورها في حماية الخدمات 54
الفرع الأول : مفهوم الحوكمة الرقمية في المؤسسات 54
الفرع الثاني دور مجلس الادارة في الامن السيبيراني.....56
الفرع الثالث : الامتثال للمعايير القانونية و الرقمية.....58
خاتمة.....64
قائمة المراجع.....69

ملخص مذكرة الماستر

تمثل حماية وإدارة الخدمات الرقمية عنصرًا أساسيًا في نجاح المؤسسات الاقتصادية الحديثة. فمن خلال تطبيق سياسات أمنية فعالة، وإدارة تقنية احترافية، تستطيع المؤسسات حماية أصولها الرقمية، وضمان استمرارية أعمالها، وتقديم خدمات آمنة و موثوقة، مما يعزز قدرتها على المنافسة والنمو في بيئة الأعمال الرقمية . تشمل حماية الخدمات الرقمية مجموعة من الإجراءات والتقنيات التي تهدف إلى حماية الأنظمة والبيانات من التهديدات الإلكترونية، مثل الاختراقات . تعني إدارة الخدمات الرقمية تخطيط وتشغيل وصيانة وتحسين الخدمات التقنية بما يضمن تحقيق أهداف المؤسسة وتلبية احتياجات العملاء . و عليها وجب تطوير بنيتها التكنولوجية، وتبني أفضل الممارسات في إدارة الخدمات، تكون أكثر قدرة على مواجهة التهديدات، وضمان استمرارية أعمالها، وتحقيق النمو والتميز في بيئة اقتصادية تعتمد بشكل متزايد على الحلول الرقمية.

الكلمات المفتاحية:

1/ إدارة الخدمات الرقمية 2/ الأمن السيبيراني 3/ امن المعلومات
4/ استمرارية الأعمال 5 / المؤسسات الاقتصادية 6/التحول الرقمي

Abstract of Master's Thesis

The protection and management of digital services are essential for modern economic institutions. Effective security measures protect digital assets, ensure business continuity, and provide reliable services. Digital service protection includes technologies and practices that secure systems and data from cyber threats. Digital service management focuses on planning, operating, and improving digital services to achieve organizational goals and meet customer needs. By adopting best practices and strengthening their technological infrastructure, institutions can enhance efficiency, reduce risks, and support sustainable growth in the digital economy.

Keywords:

1/digital service management **2/** Cybersecurity**3/**information security
4/Business Continuity **5/**Economic Institutions **6/**Digital Transformation