المدرسة الوطنية العليا للعلوم السياسية

قسم السياسات العامة والنظم المقارنة

الأمن السيبراني وحماية البيانات الشخصية في القطاع البنكي في الجزائر

دراسة حالة البنك الخارجي الجزائري للفترة الممتدة بين 2020 و 2024.

مذكرة مقدمة استكمالا لمتطلبات نيل شهادة الماستر في العلوم السياسية

تخصص: سياسات عامة وأنظمة مقارنة

إعداد الطالبة:

قسايسية إكرام زينب

إشراف الأستاذ:

عمر بن سليمان

أعضاء لجنة المناقشة:

الرتبة العلمية: اسم ولقب الأستاذ	مؤسسة الانتساب	الصفة
د. فاتح خننو	المدرسة الوطنية العليا للعلوم السياسية	رئيسا
أ. بن سليمان عمر	المدرسة الوطنية العليا للعلوم السياسية	مشرفا
أ.إخلف صارة	المدرسة الوطنية العليا للعلوم السياسية	مناقشا

ذو الحجة 1446 / جوان 2025

بـسم الله الرحمان الرحيم

"ومـا توفيقي إلاّ بالله عليه توكلت وإليه أُنيب "

(سورة هود، الآية: 88)

شكر وتقدير:

أحمد الله عزّ وجلّ الذي وفقني في إتمام هذا البحث العلمي،

والذي ألهمني الصحة والعافية والعزيمة فالحمد لله كثيرا.

أتقدم بجزيل الشكر والتقدير

إلى الأستاذ الفاضل " **عمر بن سليمان** " على تفضله بالإشراف على هذه المذكرة والذي لم يبخل علي بالنصائح والتوجيهات السديدة.

أسأل الله العلي أن يجازيه خير جزاء وأن يكتب خيره في موازين حسناته.

كما أتوجه بالشكر **لأعضاء اللّجنة المناقشة** لتفضلهم بالموافقة على مناقشة هذه المذكرة.

الإهداء:

ما سلكنا البدايات إلا بتيسيره وما بلغنا النهايات غلى بتوفيقه وما حققنا الغايات إلا بفضله فالحمد لله الذي وفقني لتثمين
هذه الخطوة في مساري الدراسي.

اهدي ثمرة نجاحي وتخرجي إلى من وهبني الحياة والأمل والنشأة على شغف الاطلاع والمعرفة ومن علموني أن ارتقي سلم الحياة بحكمة وصبر برا وإحسانا، ووفاء لهما "**والدي العزيز، والدتي العزيزة**" حفظهما الله وأطال عمرهما، لأولئك الذين لديهم ميزة كبيرة في تشجيعي وتحضيري ملاذي الأول والأخير " **أخوتي** "

وأخيرا إلى كل من ساعدني وكان له دور من قريب وبعيد في إتمام هذا العمل.

الملخص

ملخص الدراسة:

يعد الأمن السيبراني عنصرا محوريا في عالم التحول الرقمي نظرا لكونه يعتمد على إجراءات وتقنيات تهدف للحفاظ على سلامة وأمن البيانات الشخصية، لا سيما في القطاعات الحساسة التي تتعامل مع بينات حساسة كالقطاع البنكي.

لذا جاءت هذه الدراسة لتسليط الضوء على الدور المحوري والجوهري للأمن السيبراني في حماية البيانات الشخصية، ساعين في هذه الدراسة إلى توضيح دوره في تأمين البيانات الشخصية والحفاظ على سلامتها ضد التهديدات الماسة بها، من خلال التطرق إلى مختلف التدابير والأليات الفعلية لضمان الحماية على المستوى الوطني، وعلى مستوى البنك الخارجي الجزائري كنموذج تطبيقي.

قد أظهرت النتائج أن الأمن السيبراني يلعب دورا محوريا في حماية البيانات الشخصية من خلال ما يوفره من اليات وتدابير تهدف للوقاية من التهديدات السيبرانية، كما أظهرت الدراسة بأن البنك الخارجي الجزائري يعتمد على اليات وتدابير أمنية تهدف إلى ضمان الحماية الفعلية للبيانات الشخصية، إلى جانب وجود منظومة قانونية ومؤسساتية وتقنية على المستوى الوطني، معنية بحماية المعطيات ذات الطابع الشخصي.

الكلمات المفتاحية: الأمن السيبراني، البيانات الشخصية، البنك الخارجي الجزائري، التهديدات السيبرانية، القطاع البنكي، تدابير أمنية.

Abstract:

In an increasingly digital world, cybersecurity has become a key component of digital transformation. It involves a range of tools and practices aimed at protecting the confidentiality and integrity of personal data particularly in sensitive sectors such as banking, where data security is critical.

This study aims to highlight the crucial role cybersecurity plays in safeguarding personal information. It explores how cybersecurity measures contribute to securing data and preventing breaches, with a focus on both national-level strategies and the specific practices implemented by the Foreign Bank of Algiers (BEA) as a case study.

The findings demonstrate that cybersecurity plays a pivotal role in protecting personal data by offering mechanisms and preventive strategies against cyber threats. The study also reveals that the BEA employs a range of security measures designed to ensure the effective protection of personal information. Additionally, it highlights the presence of a legal, institutional, and technical framework at the national level dedicated to safeguarding personal data.

Keywords: Cyber security, Personal Data, Foreign Bank of Algiers, Cyber Threats, Banking Sector, Security Measures.

مـــقـــدمـــة

أدى التطور في تكنولوجيا المعلومات والاتصالات إلى تغيير جذري في طبيعة الأعمال المصرفية، إذ أصبحت المؤسسات البنكية تعتمد بشكل كبير على الأنظمة الرقمية في إدارة بيانات عملائها ومعاملاتهم المالية، في ظل هذا التحول الرقمي أصبحت البيانات الشخصية للعملاء تمثل أحد أهم الأصول التي يجب حمايتها وتأمينها لاسيما في القطاع البنكي الذي يتعامل يوميا مع كميات ضخمة من المعلومات الخاصة بالعملاء، هذا ما يجعله هدفا مباشر لمختلف الهجمات والتهديدات السيبرانية نظرا لما يمتلكه من بيانات ومعلومات مالية حساسة، إذ يشهد هجمات سيبرانية تفوق القطاعات الأخرى بنسبة 71% و فقا لتقديرات البنك الدولي،

ولمواجهة هذه التهديدات السيبرانية التي تستهدف البيانات الشخصية يستلزم توفير اليات وتدابير تحمي الأنظمة المعلوماتية من جانب، وبيانات وخصوصية العملاء والموظفين من جانب أخر، وهو ما يوفره الأمن السيبراني بوصفه خط الدفاع الأول في مواجهة مختلف التهديدات السيبرانية التي تمس بأمن وسلامة البيانات الشخصية، إذ يعتبر هذا الأخير الضامن لحماية البيانات الشخصية واستقرار المنظومة المالية، بإعتباره أنه يوفر وسائل تقنية وقانونية ومؤسساتية التي تمنع حدوث أي إختراق أو تهديد يمس بأمن البيانات الشخصية.

ومن هذا المنطلق، سعت البنوك الجزائرية بهدف مواكبة التطورات الحاصلة في الفضاء الرقمي إلى تبني اليات وإستراتيجيات متكاملة، تقوم على أبعاد مختلفة تهدف إلى ضمان سرية وسلامة البيانات والتصدي للتهديدات السيبرانية بما يتوافق مع المتطلبات ومعايير أمن المعلومات.

إشكالية الدراسة:

في خضم هذه التطورات الحاصلة في الفضاء الرقمي، وفي ضوء تصاعد التهديدات السيبرانية الماسة بأمن البيانات الشخصية أصبح من الضروري توفير إطار قانوني ومؤسساتي وتقني يوفر الحماية للبيانات باعتبارها تشكل أحد أهم الأصول التي تعتمد علها القطاعات الحيوية لاسيما القطاع البنكي لإدارة معاملاتها، وهوما يوفره الأمن السيبراني بإعتباره وسيلة وقائية تهدف للتصدي ضد التهديدات السيبرانية.
من خلال ما سبق، يمكن أن نطرح الإشكالية على النحو التالي:

ما هو دور الأمن السيبراني في حماية البيانات الشخصية؟

الأسئلة الفرعية:

بقصد الإجابة على الإشكالية الرئيسية، نطرح الأسئلة الفرعية التالية:

1. هل تعد البنية القانونية الوطنية وحدها كافية لضمان حماية البيانات الشخصية؟

2. هل الاستراتيجية الوطنية لحماية البيانات الشخصية القائمة على البعد المؤسساتي وحدها كافية لضمان الحماية الفعلية للبيانات الشخصية والتصدي للمخاطر التي تهددها؟
3. هل يتوفر البنك الخارجي الجزائري على اليات وتدابير أمنية لحماية البيانات الشخصية؟

فرضيات الدراسة

إنطلاقا من الإشكالية المطروحة والأسئلة الفرعية.تم صياغة الفرضيات التالية:

- البنية القانونية الوطنية قد لا تكون كافية للتصدي للتهديدات السيبرانية وضمان حماية فعالة للبيانات الشخصية.
- الإستراتيجية الوطنية لحماية البيانات الشخصية القائمة على البعد المؤسساتي قد لا تكون وحدها كافية لضمان الحماية الفعلية للبيانات الشخصية والتصدي للمخاطر التي تهددها.
- يتوفر البنك الخارجي الجزائري على اليات وتدابير أمنية لحماية البيانات الشخصية.

حدود الدراسة:

أولا: الحدود المكانية: المجال المكاني المخصص لموضوع الدراسة هو البنك الخارجي الجزائري، وتم إختيار هذه المؤسسة باعتباره من بين البنوك العمومية الرائدة في الجزائر، ويعتبر البنك نموذجا فعالا لدراسة السياسة الأمنية المنتهجة على مستوى البنك الخارجي الجزائري من خلال امتلاكه لهيكل داخلي متخصص يتمثل في مديرية أمن أنظمة المعلومات.

ثانيا: الحدود الزمانية: تمت الدراسة خلال الفترة الزمنية ما بين 2020 إلى 2024، وجاء إختيار هذه الفترة بعد صدور المرسوم الرئاسي 20-05 الذي نص على إنشاء مسؤول أمن أنظمة المعلومات.

أهمية الدراسة:

تتجلى أهمية هذا الموضوع في ظل تصاعد التهديدات السيبرانية التي تستهدف البيانات الشخصية خاصة في القطاعات الحساسة كالقطاع البنكي، وهنا تبرز أهمية الموضوع كون الأمن السيبراني هو بمثابة الدرع الوقائي لحماية البيانات الشخصية من التهديدات السيبرانية التي تحصل في الفضاء الرقمي، لذا ارتئيت أن أقوم بدراسة هذا الموضوع وبالخصوص في القطاع البنكي نظرا لحساسيته العالية ومكانته في المنظومة الإقتصادية.

أهداف الدراسة: تسعى الدراسة التي تحقيق مجموعة من الأهداف من بينها:

- التعرف على الإطار العام للأمن السيبراني والبيانات الشخصية.

- التعرف على اليات حماية البيانات الشخصية. في البنك الخارجي الجزائري.
- التعرف على الإستراتجية الوطنية لحماية البيانات الشخصية في الجزائر.

أسباب اختيار الموضوع: تتمثل في أسباب موضوعية وأخرى ذاتية وتتمثل في:

أولا: الأسباب الذاتية: وتتمثل في:

- الرغبة في إثراء المعارف في مجال الأمن السيبراني.
- الرغبة الشخصية في دراسة الموضوع كونه موضوع حديث.

ثانيا: الأسباب الموضوعية: وتتمثل في:

- الاهتمام الكبير الذي أولته الجزائر للأمن السيبراني وحماية البيانات الشخصية.
- في ظل الإستعمال المتزايد لوسائل الإعلام والإتصال وشبكة الأنترنت، أصبح الأمن السيبراني ضرورة حتمية لحماية الأنظمة والبيانات من التهديدات السيبرانية المتزايدة.

مناهج الدراسة: نظرا لطبيعة الموضوع تم إتباع المناهج التالية:

أولا: المنهج الوصفي: تم الإعتماد على هذا المنهج نظرا لملائمته لطبيعة الموضوع حيث تم توظيفه لعرض الإطار المفاهيمي للأمن السيبراني وحماية البيانات الشخصية إلى جانب توظيفه في إستعراض النصوص القانونية والتنظيمية ذات الصلة.

ثانيا: المنهج التحليلي: تم الإعتماد على هذا المنهج في تقييم الإستراتيجية الوطنية لحماية البيانات لشخصية من خلال تحليل مختلف الجوانب القانونية والمؤسساتية والتقنية.

ثالثا: منهج دراسة الحالة: تم إستخدامه في الجانب التطبيقي بغية التعرف على الأليات والتدابير التي يوفرها البنك الخارجي الجزائري في حماية البيانات الشخصية.

الإقترابات المستخدمة في الدراسة: إعتمدت الدراسة على الإقترابات التالية:

أولا: الاقتراب القانوني: تم الاعتماد على هذا الاقتراب من أجل دراسة النصوص القانونية المتعلقة بحماية البيانات الشخصية في الجزائر.

ثانيا: الاقتراب المؤسسي: تم الاعتماد على هذا الاقتراب من خلال دراستنا لمؤسسات التي تعني بحماية البيانات الشخصية، إلى جانب المؤسسات التي تشرف على حماية البيانات في البنوك التجارية.

ثالثا: الإقتراب الأمني: تم الإعتماد على هذا الإقتراب لأنه يمكن من تحليل التهديدات السيبرانية التي تستهدف البيانات الشخصية خاصة في البيئة البنكية.

هيكل الدراسة: من أجل معالجة الإشكالية المطروحة تم تقسيم الدراسة كالتالي:

الفصل الأول: وهو فصل يتناول الإطار المفاهيمي للأمن السيبراني والبيانات الشخصية، وتم تقسيمه إلى 3 مباحث، الأول تم فيه تقديم الإطار المفاهيمي للأمن السيبراني، أما المبحث الثاني فخصص لماهية البيانات الشخصية، أما المبحث الأخير فقد تم التطرق إلى الاليات الإستراتيجية للأمن السيبراني.

الفصل الثاني: سلطنا فيه الضوء على إستراتيجية حماية البيانات الشخصية في الجزائر، حيث تم تقسيمه إلى 3 مباحث، المبحث الأول يتضمن: المنظومة المؤسساتية لحماية البيانات الشخصية في الجزائر، أما المبحث الثاني فقد تناول أهم المؤسسات المشرفة على حماية البيانات الشخصية في الجزائر، ليختم هذا الفصل بمبحث ثالث تطرقت فيه الدراسة إلى الأليات التقنية لحماية البيانات الشخصية.

الفصل الثالث: فهو عبارة عن دراسة ميدانية أين تم التوجه إلى البنك الخارجي الجزائري، حيث تم تقسيم هذا الفصل إلى ثلاث مباحث، المبحث الأول تم فيه تقديم عام للبنك الخارجي الجزائري، أما المبحث الثاني فتم فيه التطرق إلى أليات البنك الخارجي الجزائري لحماية البيانات الشخصية، وختم هذا الفصل بتقديم تقييم عام للإستراتجية الوطنية لحماية البيانات الشخصية في الجزائر.

صعوبات الدراسة: من بين صعوبات الدراسة نجد أهمها:

صعوبة الحصول على المعلومات من مؤسسات الدراسة نظرا لخصوصية واهمية موضوع الدراسة، فكان لزاما على المؤسسة المعنية الأ وهي البنك الخارجي الجزائري التحفظ على المعلومات المتعلقة بها إلا القلة القليلة.

الدراسات السابقة:

الدراسة الأولى لصواق عبد القادر **مساهمة الأمن السيبراني للبيانات في تعزيز ثقة العملاء نحو الخدمات المصرفية الإلكترونية – دراسة ميدانية لدى عينة عملاء بنك التنمية المحلية BDL بولاية غرداية**،، وهي عبارة عن أطروحة دوكتراه في العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، تخصص تسويق الخدمات، (جامعة غرداية، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، قسم العلوم التجارية، 2025/2024)، حيث هدفت هذه الدراسة إلى معرفة أبعاد الأمن السيبراني، وتوضيح مدى مساهمتها في تعزيز ثقة العملاء نحو الخدمات المصرفية الإلكترونية لدى عينة من مستخدمي بطاقات الدفع الإلكتروني ببنك التنمية المحلية بولاية غرداية، وقد خلصت الدراسة أنه يوجد تأثير مباشر لأبعاد الأمن السيبراني في ثقة العملاء، كما توصل الباحث إلى وجود استراتيجية وطنية لحماية البيانات الشخصية، إلا أن الباحث أغفل الجانب المؤسساتي في هذه الإستراتيجية.

الدراسة الثانية لشيماء مرزوق وزين تركية إجلال **إنعاكسات الأمن السيبراني على أمن المعلومات في البنوك**، وهي عبارة عن مذكرة ماستر في العلوم الاقتصادية، تخصص اقتصاد نقدي وبنكي، (جامعة الشهيد الشيخ العربي التبسي، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، قسم العلوم الاقتصادية،2024/2023.)، حيث هدفت هذه الدراسة إلى تبيان تأثير الأمن السيبراني على أمن المعلومات في البنوك، حيث تم إختيار المجتمع المجمع الجهوي لبنك بدر -تبسة، وقد خلصت الدراسة أن الأمن السيبراني يساهم في حماية المعلومات البنكية من الهجمات السيبرانية، كما توصلت الباحثتين في ذات السياق إلى أن الأمن السيبراني يعد ضروري لنجاح النظام المصرفي الإلكتروني، إلا أن الباحثتين أغفلتا الحديث عن تقنيات الأمن السيبراني في تأمين معلومات العملاء المتواجدة على مستوى بنك بدر بتبسة.

الدراسة الثالثة لسمير بارة، " الأمن السيبراني في الجزائر: السياسات والمؤسسات "، وهي مقالة أكاديمية محكمة، تم نشرها في **المجلة الجزائرية للأمن السيبراني**، العدد 04، (جويلية2017)، حيث ركزت هذه الدراسة القوانين والأجهزة العملياتية التي تختص بمكافحة الجرائم المعلوماتية، وتوصلت الدراسة بأن مسألة تحقيق الأمن السيبراني هي مسؤولية وزارة الدفاع الوطني بإعتباره مسؤول أمني داخلي، إلا أن الباحث أهمل جانب التنسيق والتعاون الموجود بين وزارة الدفاع الوطني والمؤسسات الأخرى التي تعنى بالأمن السيبراني في الجزائر.

الدراسة الرابعة لسلمة بورباح، "السياسات العامة الجزائرية في مجال السيبرانية: الواقع والتحديات،" وهي مقالة أكاديمية محكمة، تم نشرها في **مجلة دفاتر السياسة والقانون**، المجلد 15، العدد01، (2023)، هدفت هاته الدراسة إلى بحث سبل بناء سياسات عامة جزائرية متكاملة في الأمن السيبراني، وقد توصلت الدراسة إلى أن بناء سياسات وإستراتيجية وطنية في مجال الأمن السيبراني يتطلب تكثيف التعاون بين القطاعات الحكومية والقطاع الخاص، إلا أن الباحث أغفل الجانب التقني في مسالة بناء الإستراتجية الوطنية لأن الإستراتيجية الوطنية للأمن السيبراني القائمة على البعد القانوني والمؤسساتي تصبح غير فعالة باعتبار الجانب التقني أمر مهم لا يمكن الإستغناء عنه.

من خلال عرض الدراسات السابقة، تتجلى القيمة المضافة لهذه الدراسة من خلال تناولها المتكامل لموضوع حماية البيانات الشخصية في السياق الجزائري وبالضبط في القطاع البنكي، عبر تحليل وتقييم الإستراتيجية الوطنية لحماية البيانات الشخصية، وهو جانب لم تتطرق إليه الدراسات السابقة، التي ركزت في الغالب على الجوانب التقنية والتشريعية بمعزل عن البنية المؤسساتية، كما أبرزت الدراسة بدقة الأدوار المؤسسات المشرفة على حماية البيانات على المستوى الوطني والمؤسسات المشرفة على حماية البيانات الشخصية في البنوك التجارية، وقامت بتحليل العلاقات بينها.

أما على مستوى الحالة التطبيقية، فقد تجاوزت الدراسة التطبيقية الطابع التقني الذي ركزت عليه دراسات سابقة لتتناول السياسة الأمنية المنتهجة على مستوى البنك الخارجي الجزائري في أبعادها المتكاملة: التقنية، التشريعية، المؤسساتية، التنظيمية، هذا ما أتاح تقديم رؤية شاملة لطبيعة الإجراءات المتبعة لحماية البيانات الشخصية داخل مؤسسة مالية عمومية.

الفصل الأول:

إطار مفاهيمي للأمن السيبراني والبيانات الشخصية

تمهيد:

في ضوء التقدم العلمي والتطور التكنولوجي المتسارع في مجال تكنولوجيات الإعلام والاتصال، اتسع مجال استخدام البيانات الشخصية بشكل رقمي، في مختلف المجالات والميادين، هذا ماجعل البيانات الرقمية متداولة، وسهل من عملية الحصول عليها، في ظل تطور وسائل جمعها، وتخزينها، وتحليلها، مما جعلها عرضة للاختراق، والسرقة، واستغلالها لأغراض غير قانونية.

وهنا يأتي الأمن السيبراني بوصفه الضامن لحماية هذه البيانات من مختلف التهديدات التي تمس بأمنها، من خلال وضع آليات وتقنيات تهدف إلى حماية و تامين البيانات، إذ أن حماية البيانات الشخصية لم تعد تقتصر على الجانب التقني فحسب بل أصبحت كذلك قضية قانونية، تستلزم سن قوانين وتشريعات تضمن احترام خصوصية الأفراد وحقوقهم، من خلال هذا الطرح، يسعى هذا الفصل إلى الإحاطة بالمفاهيم المتعلقة بالأمن السيبراني، والبيانات الشخصية، مع تبيان أهمية الأمن السيبراني كأداة لحماية البيانات الشخصية في الفضاء الرقمي، و عليه تم تقسيم هذا الفصل الأول إلى ثلاث مباحث، كما يلي:

المبحث الأول: ماهية الأمن السيبراني.

المبحث الثاني: ماهية البيانات الشخصية.

المبحث الثالث: الآليات الإستراتيجية للأمن السيبراني.

المبحث الأول: ماهية الأمن السيبراني.

في ضل التطورات التي عرفتها العالم في مجال تكنولوجيا المعلومات، أصبح الأمن السيبراني أحد أهم قضايا عصر المعلومات، خاصة مع اعتماد المؤسسات والقطاعات على الأنظمة الرقمية مما زاد من نسبة التهديدات والمخاطر الماسة بالبيانات والمعلومات، مما استلزم ضرورة إحاطة هذا المجال بمفاهيم دقيقة وآليات واضحة لضمان الحماية.

المطلب الأول: مفهوم الأمن السيبراني.

تعتبر مهمة ضبط المفاهيم والمصطلحات تحديا يواجه مختلف الباحثين والدارسين في مختلف التخصصات، نظرا لما تطرحه من إشكاليات لغوية واجرائية تجعل من الصعوبة الاتفاق حول تعريفات واضحة وموحدة، ويعد الأمن السيبراني أحد هذه المصطلحات التي عرفت تعددا في التعاريف المقدمة له، لذا ارتئيت أن أتناول هذا المفهوم على ثلاثة (03) مستويات: المستوى اللغوي، المستوى الاصطلاحي، ثم المستوى الاجرائي.

أولا: مفهوم الأمن السيبراني لغة

الأمن السيبراني مكون من مصطلحين: الأمن، والسيبراني، يشير المعنى اللغوي " للأمن" إلى نقيض الخوف، وهو يشير إلى السلامة والاطمئنان وزوال الخوف، والأمن مصدر الفعل: أَمِنَ، أَمنًا، وأَمَانًا، وأَمَنَةً، أي اطمئنان النفس، وسكون القلب، وزوال الخوف، ويقال: أَمِنَ مِنَ الشَّر أي سَلِمَ مِنهُ، [1]

أما مصطلح السيبراني (cyber)، أصله يوناني وهو مشتق من كلمة (*Kybernetes*)بمعنى الشخص الذي يدير دفة السفينة، حيث تستخدم مجازا للتعبير عن المتحكم (*Govenor*)، ومن مصدر كلمة (*Cybernetics*) التي تعني: النسق، أي الترابط الوثيق الائم على الاعتماد المتبادل، بين علم الاتصالات وأنظمة التحكم الآلي، وفي المفهوم العام تشير إلى ذلك الترابط بين مختلف الآلات أو الأشياء، والكائنات الحية. [2]

---

[1] عبد القادر صواق، بومدين بوداود، عبد اللطيف أولاد حمودة، "أثر جاهزية الامن السيبراني على الخدمات المصرفية الالكترونية من خلال تقليل المخاطر المدركة، دراسة حالة بنك BDLبغرداية"، **مجلة اقتصادية معاصرة**، م 06، ع 01، (2023)، ص. 357.

[2] راشد محمد المري، "الامن السيبراني وحماية الأنظمة الالكترونية"، **مجلة الدراسات القانونية والاقتصادية**، م09، ع01، (مارس 2023)، ص 964.

ثانيا: مفهوم الأمن السيبراني اصطلاحا

هناك العديد من التعاريف التي قدمت لمفهوم الأمن السيبراني وأهمها: إذ عرفه (*Edward AMORSO*) بأنه: "مجموع الوسائل التي تحد من خطر الهجوم على البرمجيات أو الشبكات، بواسطة وسائل وأدوات رقمية لمواجهة القرصنة وكشف الفيروسات الرقمية، ووقفها، وتوفير الاتصالات المستقرة والآمنة."[1]

وقد عرفه كل من (*Lehto Martit*)، و(*Makipekka Neittaan*)،

أن الأمن السيبراني هو: "عبارة عن مجموعة من الإجراءات التي تتخذ في الدفاع ضد هجمات قراصنة الكمبيوتر وعواقبها، ويتضمن تنفيذ التدابير المضادة المطلوبة."[2]

ووفق وزارة الدفاع الأمريكية، فإن الأمن السيبراني هو: "جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية والإلكترونية، من مختلف الجرائم، الهجمات التخريب التجسس والحوادث."[3]

أما وفق الاتحاد الدولي للاتصالات، فإن الأمن السيبراني هو: "مجموعة من المهمات المتمثلة في تجميع الوسائل، والسياسات، والإجراءات الأمنية، والمبادئ التوجيهية، والمقاربات الخاصة بإدارة المخاطر، ومختلف التدريبات والممارسات الفضلى، والتقنيات، الممكن استخدامها لحماية البيئة السيبرانية (الرقمية)، وموجودات المؤسسات والمستخدمين."[4]

بينما قدم المشرع الجزائري تعريفا للأمن السيبراني في القانون 18-04 الصادر سنة 2018، على أنه: "مجموع الأدوات والسياسات، ومفاهيم الأمن والآليات الأمنية، والمبادئ التوجيهية، وطرق تسير المخاطر، والأعمال والتكوين، والممارسات الجيدة والضمانات، والتكنولوجيا التي يمكن استخدامها في حماية الاتصالات الإلكترونية، ضد أي حدث من شأنه المساس بتوفر وسلامة وسرية البيانات المخزنة أو المعالجة أو المرسلة."[5]

---

(1) إدريس عطية، "مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري"، **مجلة مصداقية**، ع 1، ع 1، (ديسمبر 2019)، ص104.

(2) مني عبد الله السمحان، "متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود"، **مجلة كلية التربية**، ع 111، (يوليو 2020)، ص10.

(3) جمال بوزايدة، **محاضرات في الامن السيبراني**، (جامعة الجزائر03: كلية الحقوق والعلومالسياسية،2020 / 2021)، ص. 13.

(4) منى الأشقر جبور، **السيبرانية هاجس العصر**، (بيروت: المركز العربي للبحوث القانونية،2017)، ص. 26.

(5) الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 18-04 المؤرخ في: 24 شعبان 1439، الموافق لـ 10 ماي 2018، المتعلق بالقواعد المتعلقة بالبريد والاتصالات الالكترونية، الجريدة الرسمية، العدد27، الصادرة بتاريخ 13 ماي 2018، المادة: 10.

ثالثا: المفهوم الاجرائي للأمن السيبراني

من خلال ما سبق يمكن القول عن الأمن السيبراني هو: مجموع الإجراءات، والتقنيات، والآليات والتجهيزات المتخصصة، وبرامج الحماية الرقمية، التي تهدف إلى تأمين والإحاطة الأمنية التامة والشاملة بالمعلومات، والبيانات الشخصية، وأنظمة التشغيل، من مختلف الهجمات، أو التهديدات السيبرانية المحتملة.

المطلب الثاني: المفاهيم المرتبطة بالأمن السيبراني.

ما هو ملاحظ أنه كثيرا ما يستخدم في مجال الأمن السيبراني مصطلحات مثل الفضاء السيبراني، أمن المعلومات، التهديدات السيبرانية، الجريمة السيبرانية، مما يؤدي إلى نوع من اللبس أو الخلط بينهما، ومن أجل التمييز بين هذه المصطلحات بهدف تحديد مفهوم الأمن السيبراني بشكل أكثر دقة،ووضوحا وجب تحديد بعض المفاهيم المرتبطة بالأمن السيبراني لكنها لا تحمل نفس معنى لهذا الأخير.

أولا: مفهوم الفضاء السيبراني

الفضاء السيبراني هو مصطلح حديث ظهر في 1982 نتيجة لتطور تكنولوجيات المعلومات، ويشمل جمع الحواسيب والمعلومات التي بداخلها والأنظمة والبرامج والشبكات المفتوحة لاستعمال فئة محددة من المستعملين.[1]إذ عرفته الوكالة الفرنسية لأمن أنظمة الإعلام على أنه: فضاء التواصل المشكل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية.[2]

وعرفه الاتحاد الدولي للاتصالات بأنه: "المجال المادي والغير المادي الذي يتكون من عناصر هي: أجهزة الكمبيوتر الشبكات، البرمجيات حوسبة المعلومات، المحتوى معطيات النقل والتحكم، ومستخدمو كل هذه العناصر."[(3)]

يمكن القول إن الفضاء السيبراني هو عالم افتراضي يتكون من أنظمة الكمبيوتر والشبكات والبرامج والبيانات والمعلومات، إذ يشمل جميع الأنشطة والعمليات التي تتناول العالم الرقمي، بما في ذلك الاتصالات الرقمية عبر الأنترنيت، والتجارة الإلكترونية، وشبكات التواصل الاجتماعي، والخدمات الرقمية،

[(1)]نور الدين حامد إبراهيم،" الفضاء السيبراني: المفاهيم والأبعاد"، **المجلة العلمية للبحوث والدراسات التجارية**، م 38، ع 02، (2024)، ص. 720.

(2)علاء الدين فرحات، "الفضاء السيبراني: تشكيل ساحة المعركة في القرن الحادي والعشرين "، **مجلة العلوم القانونية والسياسية**، م10، ع03، (ديسمبر 2019)، ص90.

[(3)] أميرة عبد العظيم، ومحمد عبد الجواد، "المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام"، **مجلة الشريعة والقانون**، ع 35، (2020)، ص. 397.

والخدمات المصرفية الرقمية عبر الانترنيت، وغيرها. فالأمن السيبراني بمختلف آلياته وإجراءاته هو بمثابة تأمين وحماية لهذا الفضاء الافتراضي من مختلف الهجمات السيبرانية والتهديدات الأمنية الذي يتعرض لها.[1]

ثانيا: مفهوم أمن المعلومات

تعرف لجنة الأمن القومي الأمريكي أمن المعلومات بأنها:" حماية المعلومات وعناصرها الهامة بما في ذلك الأنظمة والأجهزة التي تستخدم وتخزن وترسل هذه المعلومات".[2] كما يمكن تعريفه بأنه: المفاهيم والتقنيات والتدابير التقنية والإدارية المستخدمة لحماية أصول المعلومات من الوصول غير المأذون به عمدا وسهوا أو حيازتها أو الابتزاز بها أو كشفها أو التلاعب بها، أو تعديلها أو فقدها أو إساءة استخدامها.[3]

وعليه أمن المعلومات من زاوية أكاديمية هو العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها، ومن زاوية تقنية هو الوسائل والأدوات الإجراءات اللازم توفيرها لضمان حماية المعلومات من المخاطر الداخلية والخارجية. ومن زاوية قانونية فإن أمن المعلومات هو محل دراسات وتدابير لحماية سرية وسلامة محتوى وتوفر المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة وهو هدف وغرض تشريعات حماية المعلومات من الأنشطة غير المشروعة والغير القانونية التي تستهدف المعلومات ونضمها.[4]

انطلاقا من مفهوم أمن المعلومات يتضح بأن هذا الأخير يهتم بحماية المعلومات شأنه شأن الأمن السيبراني الذي يهدف بدوره كذلك بالإحاطة الأمنية للمعلومات غير أنهما يختلفان من حيث المفهوم أو الوظيفة:

- أمن المعلومات يحافظ على جميع البيانات عند استخدام تطبيق الكتروني معين، أما الأمن السيبراني فإنه يمنع التطبيق نفسه من التجسس عليك أو اختراق قواعد بيانات المستخدم أو الملفات المحفوظة في الجهاز أو الموقع الإلكتروني أو التطبيق.
- يمكن أن يكون نظام أمن المعلومات المستخدم عرضة هو نفسه للاختراق من خلال هجمات سيبرانية عن طريق استخدام أجهزة فك شيفرات أو برمجيات في حين الأمن السيبراني هو مجموعة عمليات

---

[1] محمد دحماني، "الذكاء الاصطناعي كآلية لتعزيز الأمن السيبراني"، **مجلة الفكر القانوني والسياسي**، م 07، ع 02، (2023)، ص. 602.

[2] ذيب بن عايض القحطاني، **أمن المعلومات**، (الرياض: مكتبة الملك فهد الوطنية،2015)، ص58.

[3] المرجع نفسه، ص. 58.

[4] راضية حميدة، "الجريمة الالكترونية عبر مواقع التواصل الاجتماعي: نحو تفعيل دور الأمن السيبراني المعلوماتي "**مجلة الإعلام والمجتمع**، م 05، ع 02، (ديسمبر 2021)، ص. 341.

وإجراءات تستهدف لحماية الجهاز النظام المعلوماتي نفسه من أي فيروسات أو برمجيات ضارة ويتم أخبار المستخدم بذلك لاتخاذ الخطوات المناسبة لحمايته من السرقة.[1]

❖ يمكن لأمن المعلومات إبلاغ المستخدم مالك النظام بمحاولة الاختراق من خلال الإشعارات المتعلقة بالأمان، أما الأمن السيبراني فيمكنه تتبع المتسلل الإلكتروني وتحديد هويته الشخصية والرقمية وجمع المعلومات عنه مما يسهل اتخاذ الإجراءات القضائية المناسبة.

❖ أما من حيث المفهوم فهما متشابهان الى حد كبير لكنهما غير متطابقين، فأمن المعلومات يركز على ثلاثة (03) محاور أساسية: السرية والسلامة وتوفر المعلومات عن طريق تبني المعايير أو المقاييس الأمنية العالمية وأنظمة إدارة أمن ومخاطر المعلومات كما أنه يتضمن جوانب تقنية عديدة مثل التشفير والتخزين والتأمين الفيزيائي.

❖ أما مفهوم الأمن السيبراني فهو اتخاذ كافة التدابير والإجراءات للازمة لتأمين البيانات التي يتم تداولها عبر الشبكات الداخلية والخارجية والتي يتم تخزينها خارج المؤسسة أو داخلها بالإضافة إلى تأمين أنظمة وقنوات الاتصالات والخدمات الإلكترونية من الاختراقات التي تتم من خلال استخدام ثغرات أو ضعف في أنظمة وأدوات تكنولوجيات المعلومات والاتصالات.[2]

ثالثا: مفهوم التهديدات السيبرانية

يقصد التهديدات السيبرانية تلك الهجمات التي تتم باستخدام آليات وشبكات الانترنيت وأجهزة الحاسوب الآلي، وتهدف الى إلحاق الضرر بالأجهزة والشبكات الإلكترونية ذات الاتصال بالأنترنت.[3] كما تعرف التهديدات السيبرانية بأنها: فعل يهدف الى هدم وتجاوز الجدران الرقمية التي تقوم بوظيفة حماية كحواجز أمنية بغرض سرقة المعلومات والبيانات أو الاكتفاء بالاطلاع عليها أو تخريبها أو حتى تغيير مضمونها، وكل ذلك يهدف إلحاق الضرر بالطرف الضحية.[4]

---

[1] أميرة عبد العظيم، محمد عبد الجواد، مرجع سابق، ص. 381.

[2] بن عديد سامية، مداخلة بعنوان مخاطر **الامن السيبراني والمعلوماتي وتطور المعرفة التقنية على برامج الحماية للأنظمة المعلوماتي**، وزارة التعليم العالي والبحث العلمي، جامعة محمد الشريف مساعدية، سوق أهراس، الجزائر، (28 أكتوبر2023)، ص 06.

[3] عبد الغاني شرقي،" التهديدات السيبرانية وإشكالية السيادة: إعادة قراءة للسيادة ومعاهدة واستفاليا"، **مجلة السياسة العالمية**، م 07، ع 02، (2023)، ص. 275.

[4] محمد دحماني، مرجع سابق، ص. 652.

من خلال ما سبق يمكن القول أن التهديدات السيبرانية هي استهداف مواقع الكترونية، أو نظام كمبيوتر أو جهاز كمبيوتر من خلال وسائل الاتصال الالكترونية أخرى، بهدف تدمير أو سرقة هدفا محددا عن طريق اختراق نظام حساس.[1]

رابعا: مفهوم الجريمة السيبرانية

لم يتفق الفقهاء والباحثون على تعريف موحد للجرائم السيبرانية فمنهم:

1. من ينظر إلى الجريمة السيبرانية بالتركيز على موضوعها بحيث يعرف الاتجاه الأول الجريمة السيبرانية على أنها: " كل سلوك أو نشاط غير مشروع يتعلق بنسخ أو تغيير أو حذف البيانات أو المعلومات المخزنة داخل النظام أو الوصول إليها أو تلك التي يتم تحويلها عن طريقه أو هي كل سلوك أو نشاط غير مشروع موجه إلى المعالجة الآلية للبيانات أو نقلها."[2]
2. أما الاتجاه الثاني فينظر إلى الجريمة السيبرانية بالتركيز على وسيلة ارتكاب الجريمة، بحيث عرفها على أنها: " نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود."[3]
3. أما الاتجاه الثالث فحاول الجميع بين الوسيلة التي يتم ارتكاب الجريمة وموضوع هذه الجريمة، بحيث عرفها على أنها: "كل عمل غير قانوني أو كل سلوك غير مشروع يستخدم فيه الحاسب كأداة أو موضوع للجريمة أو هي كل فعل جنائي يكون الحاسب موضوع أو أداة للنشاط الغير المشروع."[4]
4. أما بالنسبة للتعريف القانوني للجريمة السيبرانية في التشريع الجزائري، فنجد أن المشرع الجزائري لم يستقر على استخدام مصطلح للدلالة على هذه " الجرائم" حيث سماها بموجب القانون 04-15 المتضمن قانون العقوبات بجرائم المساس بأنظمة المعالجة الألية للمعطيات، بحيث لم يقدم المشرع الجزائري مفهوما للجرائم السيبرانية في القانون 04- 15 بل اكتفى بالعقاب على بعض الأفعال: تحت عنوان جرائم المساس بنظام المعالجة الألية للمعطيات، ثم بعد صدور القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال مكافحتها، استخدم المشرع مصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال للدلالة على الجرائم السيبرانية[5]، وبحيث أعطى المشرع في القانون 09-04

---

[1] عبد الغاني شرقي، مرجع سابق، ص. 275.

[2] أميرة عبد العظيم محمد عبد الجواد، مرجع سابق، ص. 391.

[3] روان بنت عطية الله الصحفي، "الجرائم السيبرانية"، **المجلة الإلكترونية الشاملة متعددة التخصصات**، ع24، (ماي 2025)، ص 8.

[4] أميرة عبد العظيم محمد عبد الجواد، مرجع سابق،ص. 392.

[5] سميرة معاشي،"الجريمة المعلوماتية دراسة تحليلية لمفهوم الجريمة المعلوماتية "،**مجلة الفكر**، ع 17، (جوان 2018)، ص. 409.

تعريفا للجرائم السيبرانية في المادة 2 من القانون 09-04:" جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية."[1]

بناءا على ما سبق يمكن القول أن الجريمة السيبرانية هي كل فعل مشروع يستهدف تغيير بيانات أو معلومات كيفما كان هذا التغيير سواء كان بواسطة جهاز الحاسوب كما يمكن أن يكون باستخدام جهاز تكنولوجي آخر.

المطلب الثالث: أهداف الأمن السيبراني وخصائصه

أولا: أهداف الأمن السيبراني

1) الحفاظ على دقة وسلامة البيانات والبرامج وعدم فساد حالتها.
2) الحفاظ على البيانات والبرامج للفترة المطلوبة.
3) تعزيز حماية أنظمة التقنيات التشغيلية على كافة الأصعدة ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات وما تحويه من بيانات.
4) التصدي لهجمات وحوادث آمن المعلومات التي تستهدف الأجهزة الحكومية ومؤسسات القطاع العام والخاص.
5) توفير بيئة أمنة موثوقة للتعاملات في مجتمع المعلومات.
6) صمود البنى التحتية الحساسة للهجمات الإلكترونية.
7) توفير المتطلبات اللازمة للحد من المخاطر والجرائم الإلكترونية التي تستهدف المستخدمين.
8) التخلص من نقاط الضعف في أنظمة أمن الحاسب الآلي والأجهزة المحمولة باختلاف أنواعها.
9) سد الثغرات في أنظمة آمن المعلومات.
10) مقاومة البرمجيات الخبيثة.
11) الحد من التجسس والتخريب الإلكتروني على مستوى الحكومة والأفراد.
12) اتخاذ جمع التدابير اللازمة لحماية المواطنين والمستهلكين على حد سواء من المخاطر المحتملة في مجالات استخدام الانترنت المختلفة.

[1] الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 09-04 المؤرخ في: 14 شعبان 1430، الموافق لـ 05أوت2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته، الجريدة الرسمية، العدد47، الصادرة بتاريخ: 05- 08- 2009.المادة: 02.

13) تدريب الأفراد على آليات وإجراءات جديدة لمواجهة التحديات الخاصة باختراق أجهزتهم التقنية بقصد الضرر بمعلوماتهم الشخصية سواء بالإتلاف أو بقصد السرقة.[1]

ثانيا: خصائص الأمن السيبراني

يتميز الأمن السيبراني بعدة سمات ومن أهمها:

1) الأمن السيبراني ليس مسار عمل لمدة واحدة، إنما هو عملية مستمرة ويحتوي على آليات دفاع مبتكرة لكونه يواجه التهديدات التي تقع على الأنظمة والشبكات غيرها.

2) يعمل على خلق نظام بيئي سبراني آمن وإنشاء نظام موثوق به.

3) يقوم بعملية وقائية رقابية مسبقة بهدف البحث عن المخاطر والعمل على حلها وسد الثغرات.

4) يعمل على الدفاع اللاحق والذي يتمثل في قاعدة إرجاع الموضوع إلى ما كان عليه.

5) يوفر خاصية التنبيه الى وجود خطأ أو إساءة استخدام الشبكات التي تعرض من البيانات والمعلومات إلى الخطر داخل المؤسسات، وأيضا تغطية المخاطر الخارجية ومراقبة التهديدات.[2]

المطلب الرابع: أبعاد الأمن السيبراني

أولا: البعد العسكري: وتكمن الميزة النسبية للقوة السيبرانية في قدرتها على ربط الوحدات العسكرية ببعضها البعض عبر الشبكات العسكرية في الفضاء الإلكتروني بما يسمح بسهولة تبادل المعلومات وتدفقها وسرعة اتخاذ القرارات العسكرية، بحيث ان لم يتم استغلال هذه التقنية والتسلح بها، أو تأمينها بشكل جيد عن أي اختراق خارجي سيؤدي بالضرورة إلى شن هجمات الكترونية مضادة على شبكات القوات العسكرية ومن ثم تدمير قواعد البيانات و بالتالي تصبح نقطة ضعف، خاصة إذا لم تكن مؤمنة جيدا من الاختراق، الذي قد يؤدي إلى تدمير قواعد البيانات العسكرية، أو قطع الاتصال بين القيادة والوحدات العسكرية فضلا عن إمكانية التحكم في بعض الأسلحة وخروجها عن السيطرة، طائرات بدون طيار، صواريخ موجهة، أقمار صناعية و غيرها.[3]

---

[1] منى عبد الله السمحان، "متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود"، **مجلة كلية التربية**، ع 11، (جويلية 2020)، ص. 12.

[2] خالد ظاهر، عبد الله جابر، السهيل المطيري، "دور التشريعات الجزائية في حماية الأمن السيبراني بدول مجلس التعاون الخليجي"، **مجلة البحوث الفقهية والقانونية**، ع38، (جويلية 2022)، ص. 1006.

[3] لامية طالة، "التهديدات والجرائم السيبرانية وتأثيرها على الأمن القومي للدول واستراتيجيات مكافحتها"، **مجلة معالم للدراسات القانونية والسلبية**، م 04، ع 02، (2020)، ص. 62.

ثانيا: البعد الاقتصادي: أصبح الفضاء السيبراني أساسا للتعاملات الاقتصادية والمالية والتجارية، إذ أصبح يستخدم الكمبيوتر لتنمية الصناعات ودفع الاقتصاد، هذا ما دفع الى ضرورة توفير الأمن السيبراني لحماية هذه المعلومات. [1]

ثالثا: البعد الاجتماعي: يكتسب الأمن السيبراني أهمية كبيرة في المجال الاجتماعي، إذ أصبحت مواقع التواصل الاجتماعي وسيلة اتصال عالمية بين الناس، تزود بالمعلومات والأفكار، ولكن من جهة أخرى تعرض أخلاق المجتمع للخطر لأنها تمس بهوية الأفراد وتهدد الحقوق والحريات والسلم الاجتماعي، وعليه لابد من ترسيخ مفهوم الأمن السيبراني ثم توعية الناس بمخاطر الاختراق. [2]

رابعا: البعد السياسي: تتجلى الأبعاد السياسية للأمن السيبراني في جوهرها في حق الدولة في صون نظامها السياسي ووجودها ومصالحها الاقتصادية، أي حقها وواجبها في العمل لتحقيق رفاهية مواطنيها، وذلك في وقت تؤثر فيها التقنيات على توازن القوى داخل المجتمع، كما أصبح بإمكانه الاطلاع على دوافع القرارات التي تتخذها حكومته، وذلك عبر كم المعلومات الهائل المتاح، أو الذي يتم توزيعه ونشره عبر الانترنت والأجهزة المتصلة ومختلف مواقع التواصل الاجتماعي، إذ يتم استغلال هذه التقنيات بطريقة سلبية من طرف الحركات الإرهابية لتجنيد أفرادها وجمع التمويل لعملياتها هذا ما دفع بالدول للعمل على حماية أمنها من التهديدات والمخاطر التي قد تتعرض لها من خلال شبكة الانترنت.[3]

خامسا: البعد القانوني: يشير البعد القانوني للأمن السيبراني إلى المجموعة الشاملة من القوانين والتشريعات، بحيث يهدف البعد القانوني إلى توفير إطار قانوني يحمي لأفراد والمؤسسات من الاعتداءات السيبرانية ويعاقب المتسببين في الهجمات الإلكترونية فالتطورات التكنولوجية المتسارعة والتحولات أدت إلى تصاعد في أعداد الأعمال الإجرامية والممارسات الغير القانونية في الفضاء السيبراني ما يستدعي وجود ترسانة قانونية تنسجم مع التطورات الحاصلة في الفضاء السيبراني. [4]

---

[1] محمد دحماني، مرجع سابق، ص. 603.

[2] إيمان بوجلة، فطيمة يحياوي، نبيل جحا، **التأمين السيبراني، تجارب دولية**، مذكرة ماستر غير منشورة، (جامعة ابن خلدون: كلية العلوم الاقتصادية والتجارية وعلوم التسيير،2023/2022)، ص. 15.

[3] كاملي محمد، فتيحة زرازقة، **الاستراتيجية الأمنية لتحقيق الامن السيبراني**، مذكرة ماستر غير منشورة، (جامعة عمار ثليجي: كلية الحقوق والعلوم السياسي،2019/2018)، ص. 30.

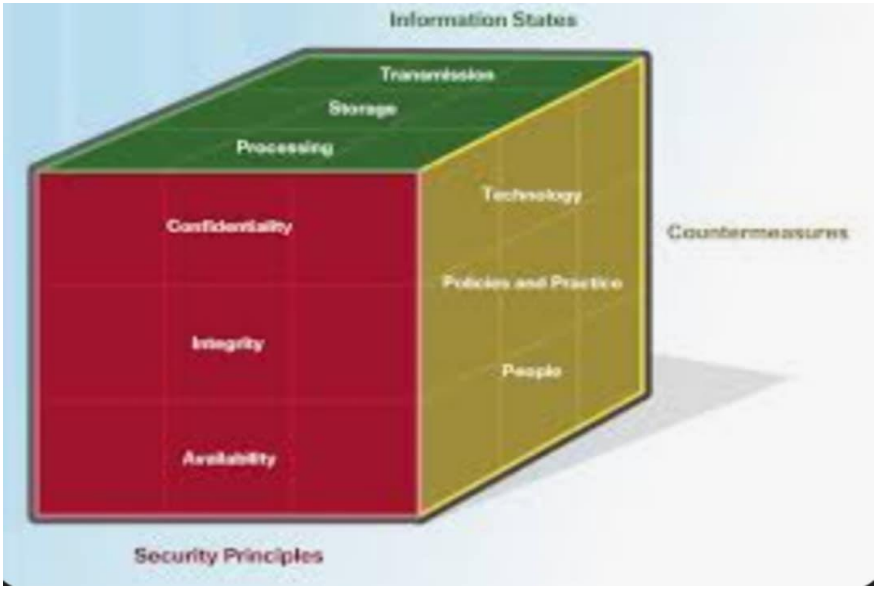
[4] سمير بارة،" الأمن السيبراني في الجزائر: السياسات والمؤسسات"، **المجلة الجزائرية للأمن الإنساني**، م4، (جويلية 2017)، ص. 263.

المطلب الخامس: أبعاد مكعب الأمن السيبراني

أولا: التعريف بمكعب الأمن السيبراني أو مكعب (Mc. Camber)

هو نموذج أو إطار عمل ابتكره جون ما كمبر في 1991 و هو أحد خبراء الأمن السيبراني، للمساعدة في إدارة حماية الشبكات والنطاقات والأنترنيت، إذ يقدم هذا النموذج نهج منظم لتقييم وإدارة المخاطر الأمنية في أنظمة تكنولوجيا المعلومات حيث يهدف إلى تبيان العوامل المتداخلة في تأمين المعلومات وإدارة المخاطر المرتبطة باستخدام، معالجة، تخزين و نقل المعلومات وحمايتها من الضياع أو التعديل، و ضمان توافر المعلومات عند اللزوم فقط للأشخاص المحولين بالوصول لها، بالإضافة لتأمين الأنظمة والأجهزة المستخدمة والإجراءات اللازمة لحمايتها.[1]

الشكل رقم (01): مكعب الأمن السيبراني (مكعب ما كمبر)



المصدر: Cisco Networking Academy,Cyber Security Essentials, vol 1, 1 St Ed, 2008, p 06.

ثانيا: أبعاد مكعب الأمن السيبراني:

يحتوي مكعب الأمن السيبراني على 3 أبعاد تتمثل في:

البعد الأول: مبادئ أمن المعلومات: يحدد البعد الأول لمكعب الأمن السيبراني الأهداف لحماية الفضاء السيبراني والأهداف التي يقدمها البعد الأول، وهي المبادئ الأساسية المتمثلة في السرية *confidentiality* والتماسك *Integrity* والتوافر *Availability* والتي عادة تعرف باسم مثلث «*CIA*»

(1) *SabahAl-fedaghi, Khaled Al-Saqabi,Bernhard Thalheim, **information stream-based model for organizing security**, computer engineering department, University of Kuwait, (April2008), p. 01.*

أو(*CIATriangle*)، إذ تمكن هذه المبادئ خبير الأمن السيبراني من تحديد أولويات والإجراءات عند حماية أي نظام شبكي.[1]

1) السرية (*Confidentiality*): تعني الحفاظ على المعلومات من أي شخص إطلع عليها غير الأشخاص المصرح لهم فقط، بمعنى منع الكشف غير المصرّح به، إذ تضمن السّرية وجود مستوى الحماية المطلوب في كل مكون من المكونات المعالجة للمعلومات، ما يساعد في الحماية من الكشف غير المصرح به عن المعلومة. ويجب أن يكون هذا المستوى من الحماية موجود في جميع مراحل معالجة المعلومة سواء كانت المعلومات مخزنة أو مرسلة أو وصلت إلى وجهتها النهائية.[2]

2) سلامة المعلومات و تكاملها(*DATA Integrity*):وتعني الحفاظ على أمان المعلومة من أي تعديل أو حذف أو إضافة أو إعادة صياغة أو تحويل وهذا أمر بالغ الأهمية لتعزيز الثقة في المعلومة، والتأكد من أنها أصلية دون تغيير، قد تكون المعلومة مشفرة و سريتها محفوظة و لكن يمكن أن تتعرض للتغيير كمعلومة الكترونية، هذا التغيير يجب اكتشافه وهذا ما يوفره هذا العنصر، إذ يهتم هذا العنصر بضمان دقة المعلومة وسلامتها ودقة الأنظمة المعالجة لها وسلامتها من التلاعب والتغير غير المصرح به، بحيث يعني سلامة المعلومات وتكاملها بأنه تم تلقي الرسالة طبقا لما أرسلت به، مما يولد ثقة لدى مستخدمي المعلومة بأنها كاملة في محتواها وصحيحة في مضمونها، وقد تمت معالجتها أثناء انتقالها بالطرق الصحيحة التي لم يطرأ عليها أي تغيير مقصود أو غير مقصود، إضافة إلى اهتمام عنصر سلامة المعلومات وتكاملها بعملية منع التعديل على المعلومة أو تصحيح التعديل، يهتم أيضا بعملية كشف عدم سلامة المعلومة وكشف تعديل على المعلومة.

3) تو افر المعلومة(*Availability*): تشير بتوافر المعلومة إلى سهولة الوصول إليها واستخدامها عند الحاجة من قبل أي فرد أو جهة محددة وفي أي وقت مسموح به، وهي الخدمة التي تحافظ على النظام قيد التشغيل دائما ولهذا تسمى أحيانا (بالاستمرارية) وهي مخصصة لمواجهة أي عطل أو هجوم يمكن أن يتسبب في تعطيل الخدمات مثل هجمات الفيروسات أو هجمات حجب الخدمة والهدف من عنصر توافر المعلومة أن تكون الأجهزة والأنظمة والبرامج والشبكات متاحة في جميع الأوقات التي يحتاج إليها المستخدم، وأن توفر لها الحماية من أي شيء قد يسبب في تعطلها أو عدم توفرها، وفي حال حدوث الأعطال والكوارث يجب أن تكون هناك بدائل جاهزة لتحل محلها تلقائيا و بسرعة.[3]

---

[1] أسامة حسام الدين، **أساسيات الأمن السيبراني**، (المملكة العربية السعودية: أكاديمية سيسكو بجامعة طيبة، 2017)، ص 27.

[2] ذيب بن عايض القحطاني، **أمن المعلومات**، (الرياض: مكتبة الملك فهد الوطنية،2015)، ص. 91.

[3] ذيب بن عايض القحطاني، مرجع سابق، ص. 93-96.

البعد الثاني: حالة البيانات (*STATEOF DATA*): يحتوي الفضاء الإلكتروني على كم هائل من البيانات بالغة الأهمية، ولذلك يجب على خبراء الأمن السيبراني التركيز على حماية البيانات، إذ يركز هذا البعد المتمثل في حالة البيانات (*STATEOF DATA*) على مشاكل حماية البيانات في الفضاء السيبراني في جميع حالتها المحتملة. وتتمثل حالة البيانات هذه في:

1) **البيانات الثابتة أو البيانات المخزنة (*STORAGE DATA*)**: البيانات المخزنة أو الثابتة وتعني بقاء البيانات على حالها في جهاز التخزين حتى مع غياب المستخدم أو البرنامج، يمكن أن يكون جهاز التخزين مرفقا بجهاز الحاسوب أو مركزيا على الشبكة.

2) **البيانات المتنقلة (*DATA IN TRANSIT*)**: وتعني إرسال المعلومات من جهاز إلى جهاز آخر عن طريق الشبكة السلكية أو الشبكية اللاسلكية أو عن طريق أدوات أخرى مثل:*ICLOUD* ، *GOOGL DRIVE*.[1]

3) **البيانات أثناء المعالجة (*DATA IN TRANSIT*)**: وهي عملية تقوم على تحويل البيانات الخام إلى صيغة أسهل للقراء ما يمنحها الشكل والسياق اللازمين لتفسيرها بواسطة أجهزة الكمبيوتر واستخدامها من قبل الموظفين، من قبل المتخصصين في البيانات، تترجم البيانات وتصبح قابلة للقراءة وغالبا ما تكون في شكل رسم بياني، مقاطع، نصوص عادية.[2]

البعد الثالث: طرق وأدوات الحماية (*SABEGUARDS*): البعد الثالث والأخير للنموذج أو مكعب الأمن السيبراني هو طرق وأدوات الحماية (*SABEGUARDS*)، إذ يشير هذا البعد إلى مجموعة التدابير المتخذة لحماية أنظمة الحاسوب والشبكات والبيانات من الوصول غير المصرح به أو السرقة أو التلف، يتضمن هذا البعد على مجموعة من أدوات لتوفير الحماية الشاملة في:

1) **التقنيات المستخدمة في الحماية**: تشمل برمجيات الحماية للبرامج والتطبيقات والخدمات مثل أجهزة الجدران النارية، برامج مكافحة الفيروسات، أنظمة كشف التسلل وما ذلك.

2) **التعلم والتوعية والتدريب**: يتيح التعلم والتوعية والتدريب للأشخاص من التأكد من أن مستخدمي أنظمة المعلومات واعون بأدوارهم ومسؤولياتهم فيما يتعلق بحماية أنظمة المعلومات.

3) **سياسات وإجراءات الأمن السيبراني**: هي مختلف التوجيهات والضوابط الإدارية التي ترسي أسس تطبيق ضمان المعلومات داخل المؤسسة بحيث أن اعتماد تطبيق سياسات من قبل الإدارة العليا أمرا

---

[1] أسامة حسام الدين، مرجع سابق، ص. 38.

[2] *Nikita Duggal*, ***What is Data Processing?, Types x examples Explained***, *in: https://www.sImplilearn.com/What is data process, (03/ 04/ 2025).*

أساسيا لضمان الحد من المخاطر أو القضاء عليها إلى جانب السياسات، يجب توضيح الإجراءات والممارسات المتعلقة بكيفية تطبيق هذه السياسة لضمان سلامة البيانات.[1]

[1] Anthony McCartney, "The McCumber cube model" , **College of Science and technology** (January 2024).

المبحث الثاني: ماهية البيانات الشخصية

تمثل البيانات الشخصية في العصر الحالي عصب المعاملات الإلكترونية في مختلف القطاعات لا سيما في القطاعات الحيوية مثل القطاع البنكي الذي يعتمد بشكل كبير على المعلومات البيانات لإدارة حسابات عملائه وتقديم مختلف الخدمات للزبائن، هذا ما يستلزم سن قوانين وضوابط تكرس حق البنك في استخدام والاطلاع على البيانات بطريقة مشروعة وحق الأفراد في حماية خصوصية بياناتهم.

المطلب الأول: تعريف البيانات الشخصية

قبل أن نتطرق إلى مفهوم البيانات الشخصية من المهم أولا، تحديد مفهوم البيانات.

أولا: تعريف البيانات:

تعرف البيانات بأنها " المادة الخام للمعلومات و التي تتكون من كلمات وأرقام ورموز والتي ليس لها دلالة أو معنى بحد ذاتها، ولا يمكن الاعتماد عليها وحدها لفهم شيء معين "، وتعرف أيضا " كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة تقنية المعلومات كالأرقام والحروف والرموز وما إليها"، كما يمكن تعريفها أنها: "مجموعة من الأرقام والحروف والمطلوب إدخالها إلى الحاسب حتى يقوم بإنتاج المعلومات المطلوبة."[1]

ثانيا: تعريف البيانات الشخصية:

تعرف البيانات الشخصية بأنها: " كل معلومة أو صوت أو صورة متعلقة بشخص ما، معرف وقابل للتعرف عليه سواء بصورة مباشرة أو غير مباشرة ولا سيما من خلال الرجوع الى عناصره المميزة لهويته البدنية أو الفيزيولوجية أو الجينية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية."[2]

تضمنت النسخة الأولى من الإرشادات الصادرة عن منظمة التعاون الاقتصادي والتنمية، سنة 1980 تعريفا للبيانات الشخصية بأنها:" كل معلومة عائدة لشخص طبيعي محدد أو قابل للتحديد."[3]كما أشار نص المادة 02 من اتفاقية مجلس أوروبا لسنة 1981،المتعلقة بحماية الأشخاص فيما يخص التحليل الآلي للبيانات ذات الطابع الشخصي إلى تعريف البيانات الشخصية بأنها:" كل معلومة تخص شخصا

---

[1] جوهر قوادري صامت، "الضوابط القانونية لمعالجة البيانات الشخصية الإلكترونية"، **مجلة الدراسات القانونية المقارنة**،م 06، ع02، (27- 12- 2020)، ص. 469.

[2] منى الأشقر، جبور ومحمد حيدر، **البيانات الشخصية والقوانين العربية :الهم الأمني وحقوق الأفراد**، (بيروت: المركز العربي للبحوث القانونية والقضائية مجلس وزراء العدل العرب، جامعة الدول العربية، ط1، 2018)، ص. 76.

[3] المرجع نفسه، ص. 76.

طبيعيا معروفا أو يمكن التعرف إليه."[1]أما بالنسبة للتعريف القانوني فقد أطلق عليه المشرع الجزائري على مصطلح البيانات الشخصية في العديد من النصوص القانونية، مصطلح المعطيات ذات الطابع الشخصي، من بينها القانون 18-07 فقد عرفها في المادة 03 على أنها: " كل معلومة بغض النظر عن دعامتها متعلقة بشخص معرف أو قابل للتعرف عليه و المشار إليه أدناه الشخص المعني بصفة مباشرة أو غير مباشرة لا سيما بالرجوع إلى رقم التعريف أو عنصر أو عدة عناصر خاصة بهوية البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية".[2]

مما سبق ذكره من تعريفات يمكننا القول بأن البيانات الشخصية هي تلك البينات التي ترتبط بشخص طبيعي محدد أو قابل للتحديد بشكل مباشر أو حتى غير مباشر من خلال الربط بينهما وبين أنماط البيانات الشخصية المحددة سلفا.[3]

المطلب الثاني: أنواع البيانات الشخصية

لم يذكر المشرع الجزائري أنواع البيانات الشخصية أو المعطيات ذات الطابع الشخصي صراحة وإنما أشـــار إلى تعريفها في المادة 03 فقرة 01والفقرة 06 من نفس المادة، حيث ذكر في الفقرة 01 مجموعة من المعطيات الشـخصـــية التي يمكن من خلالها أن يصـــل إلى هوية الشـخص، بينما ذكر في الفقرة 06، مجموعة من المعطيات الشخصية وأطلق عليها "معطيات حساسة" وهذا ما يتضح بما أن المشرع الجزائري صنف البيانات الشخصية إلى صنفين: البيانات الشخصية، والبيانات الحساسة.

أولا: البيانات الشخصية العادية

أشـــار المشـــرع الجزائري من خلال المادة 03 في الفقرة 01 من القانون 18-07المعطيات الغير الحساسة كل المعلومات التي تمكننا من تحديد الشخص والتعرف عليه بالرجوع إلى المظاهر الشخصية والمتعلقة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفســية أو الاقتصــادية أو الثقافية أو الاجتماعية.

---

[1] حليمة علالي، **الحماية الجنائية للمعطيات الشخصية في التشريع الجزائري (قانون18-07)**، مذكرة ماستر غير منشورة، (جامعة قاصدي مرباح، كلية الحقوق والعلوم السياسية،2019/2018)، ص. 10.

[2] الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 18-07 المؤرخ في: 25 رمضان 1439 الموافق لـ 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي، العدد34، الجريدة الرسمية، الصادر بتاريخ 10يونيو 2018، المادة 03.

[3] هبة رمضان رجب،"الحماية القانونية للبيانات الشخصية في عصر التكنولوجيا الرقمية"، **مجلة العلوم القانونية والاقتصادية**، م66، ع 03، (يناير 2024)، ص. 433.

بحيث تشمل البيانات الشخصية العادية على: الاسم واللقب، العنوان، رقم الضمان الاجتماعي، عنوان جهاز الحاسوب (IP)، البصمة، بالإضافة إلى عناصر أخرى تشملها البيانات الشخصية رقم الحساب البنكي، البريد الإلكتروني، رقم الهاتف وتاريخ الميلاد، رقم بطاقة التعريف أو الهوية.[1]

ثانيا: البيانات الشخصية الحساسة

عرفت اللائحة العامة لحماية البيانات الشخصية الحساسةGDPRبأنها: " البيانات التي تكشف عن الأصل العرقي أو الأثيني أو الآراء السياسية أو المعتقدات الدينية أو الفلسفية، أو عضوية النقابات العمالية، أو معالجة البيانات الجينية، والبيانات البيومترية بغرض تحديد هوية الشخص الطبيعي بشكل فريد، أو البيانات المتعلقة بالصحة، أو البيانات المتعلقة بالتوجه الجنسي لشخص طبيعي"، [2]كما قامت اللائحة العامة لحماية البيانات الشخصية بوضع تعريفات للمصطلحات الواردة في التعريف السابق.

فقد عرفت البيانات المتعلقة بالصحة: أنها البيانات الشخصية المتعلقة بالصحة الجسدية أو العقلية للشخص الطبيعي.

كما عرفت البيانات البيومترية: بأنها البيانات الشخصية الناتجة عن معالجة تقنية محددة تتعلق بالخصائص الجسدية أو الفيزيولوجية أو السلوكية لشخص طبيعي، والتي تسمح أو تؤكد التعرف الفريد لذلك الشخص الطبيعي، مثل صور الوجه أو بيانات تنظير الأصابع.[3]

البيانات الجينية: هي البيانات الشخصية المتعلقة بالخصائص الجينية الموروثة أو المكتسبة للشخص الطبيعي والتي تعطي معلومات فريدة عن فيزيولوجيا أو صحة ذلك الشخص الطبيعي والتي تنتج على وجه الخصوص عن تحليل عينة بيولوجية من الشخص المعني، ولذلك يعتبر البعض أن البيانات الجينية ليست بيانات شخصية بل بيانات حساسة.[4]

أما بالنسبة للتعريف القانوني للبيانات الشخصية الحساسة في الجزائر، فقد أعطى المشرع الجزائري تعريفا للبيانات الحساسة في المادة 3 الفقرة 6 من القانون 18-07:" معطيات ذات طابع شخصي تبين الأصل العرقي أو الاثني أو الآراء السياسية أو القناعات الدينية أو الفلسفية أو الانتماء النقابي للشخص المعني أو تكون متعلقة بصحته بما فيها معطياته الجينية."[5]

---

[1] عبد الهادي كحلاوي، مرجع سابق، ص ص. 55،56.

[2] سمير سعد، رشاد سلطان، "تعزيز الحماية القانونية للبيانات الشخصية الحساسة في مجال الاستدلالات، دراسة مقارنة"، **مجلة البحوث القانونية والاقتصادية**، ع 88، (يونيو 2024)، ص 1957.

[3] المرجع نفسه، ص1959.

[4] المرجع نفسه، ص.1059.

[5] الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 18-07، مرجع سابق، المادة 03.

كما حدد المشرع الجزائري في المادة 3 من القانون 18-07 قائمة البيانات الشخصية التي تشمل: البيانات المتعلقة بالعرق والأصل العرقي، البيانات المتعلقة بالآراء السياسية والمعتقدات الدينية أو الفلسفية وعضوية النقابات، البيانات الصحية والبيانات الجينية. ولم يشمل المشرع الجزائري على فئة البيانات البيومترية والبيانات المتعلقة بالحياة الجنسية والتوجه الجنسي للشخص."[1]

ومن خلال ما سبق فيمكن القول أن البيانات الشخصية هي كل البيانات التي تمكننا من الوصول إلى هوية الشخص سواء ما يتعلق بعناصر شخصيته الاجتماعية أو الجينية أو الفيزيولوجية، إلخ.[(2)]

المطلب الثالث: التهديدات السيبرانية التي تمس سلامة البيانات الشخصية.

تنقسم التهديدات السيبرانية التي تمس سلامة وأمن البيانات الشخصية إلى قسمين: مخاطر داخلية، التي تكون نابعة من داخل المنظمة نفسها، مخاطر خارجية، والتي تتمثل في الهجمات الواقعة على أنظمة المعلومات، تتمثل أبرز مظاهر التهديدات السيبرانية بنوعيها فيما يلي:

أولا: التهديدات الداخلية: تشمل التهديدات الداخلية عدة أنواع تتمثل في:

1. **الإهمال وعدم الوعي:** يشكل الموظفون الذين لا يدركون السياسات الأمنية أو لا يتبعونها بشكل صحيح مصدرا كبيرا للمخاطر فمثلا قد يتسبب الإهمال في عدم تحديث البرمجيات بانتظام أو إهمال حماية الأجهزة وتركها بدون قفل أو كلمة مرور أو حتى مشاركة كلمة المرور، في حدوث ثغرات أمنية تسهل الوصول غير المصرح به، إضافة إلى عدم وعي الموظفون بمثل خطورة الرسائل البريد الإلكتروني الاحتيالية أو الروابط الملوثة أو كذلك عدم معرفة الموظفين بالممارسات الأمنية السليمة التي تهدف إلى حماية البيانات الشخصية.
2. **الأعمال الخبيثة المتعمدة:** يشمل هذا النوع من المخاطر التي يقوم بها موظف أو متعاقد أو شخص داخلي بقصد إلحاق الضرر بالمنظمة أو البيانات في المنظمة، بحيث تضمن الأعمال الخبيثة المتعمدة.

أ. تسريب البيانات بشكل عمدي عن طريق نشرها أو إرسالها عبر البريد الإلكتروني إلى أطراف غير مصرح بها.

ب. تخريب الأنظمة عن طريق تحميل برامج ضارة.

ج. جهات خارجية: عن طريق تعاون الموظف مع جهات خارجية لبيع معلومات الشركة للمنافسين.

---

[1] الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 18-07، مرجع سابق، المادة 03.

[(2)] نعيمة بوعقبة،"معالجة البيانات الحساسة بين الحظر وخصوصية المعالجة، قراءة في قانون حماية المعطيات ذات الطابع الشخصي 18-07"، **مجلة سوق القانون**، م 09، ع 01، (2022)، ص 229-230.

3. **سوء الاستخدام المتعمد للموارد:** يحدث هذا النوع من المخاطر في الحالات عندما يستغل الموظفون معلومات الشركة بشكل غير قانوني لتحقيق مصالح شخصية.

4. **الخروقات العارضة: تشمل** أخطاء بشرية غير متعمدة مثل إرسال بيانات حساسة إلى جهة غير صحيحة أو حفظ الملفات في أماكن غير آمنة أو تنزيل برامج ضارة دون قصد تؤدي إلى إصابة النظام ببرامج التجسس أو فيروسات. [1]

ثانيا: التهديدات الخارجية: وتتمثل في:

1. **البرمجيات الخبيثة:** هي برامج تصمم بهدف إلحاق الضرر بالأنظمة والمعلومات دون علم المستخدم أو موافقته، إذ تعمل هذه البرامج على جمع البيانات الحساسة والوصول إلى الأنظمة أو تعطيل خدماتها، ومن أبرز صورها:

أ. **الفيروسات:** الفيروسات الحاسوبية هي برامج قابلة للتنفيذ تصمم بهدف التسبب في أضرار أو تعطيل الأنظمة، تستند آلية عملها إلى برنامج تنفيذي ليتم تشغيلها، وتكون قادرة على استهداف المستخدمين من خلال التكاثر داخل الخلايا الرقمية، عادة تنشر الفيروسات عبر وسائل مختلفة مثل: تحميل الملفات من الأنترنيت أو عبر ملفات مرفقة بالبريد الإلكتروني، كما يمكن أن تتنقل باستخدام وسائل تخزين منتقلة مثال ذاكرات U.S.B وهناك العديد من الأمثلة عن الفيروسات.[2] من الأمثلة الشهيرة لهذا النوع من الفيروسات "فيروس ميليسا" الذي ظهر في عام 1999 وكان في صدارة الفيروسات التي شكلت خطورة كبيرة، بحيث كان يخترق أجهزة الحاسوب إذ يصيب هذا الفيروس مستندات *MicrosoftWord* وينتشر عبر مرفقات البريد الإلكتروني، أدى انتشار فيروس ميليسا إلى تعطيل عمل العديد من الشركات الكبرى مثل *Microsoft Intel* وتسبب هذا الفيروس في خسائر مادية بقيمة 80 مليون دولار وهي تكلفة تعطيل العمل وإزالة الفيروس من الأجهزة المصابة.[3]

ب. **الديدان *Worms*:** تعتبر أيضا من البرمجيات الخبيثة التي تتكاثر بأشكال مستقلة، إذ تقوم الديدان بإبطال عمل الشبكة، بحيث تنتشر وتتكاثر بنفسها وهذا على عكس الفيروسات التي لا تتكاثر وتنتشر بنفسها، عندما تصيب الديدان جهازا معينا تنطلق بداية من هذا الجهاز لتنتشر سرعة كبيرة جدا وتصيب بقية الأجهزة على الشبكة، وتشترك الديدان في الخصائص ولها نفس الهدف، فكل الديدان من نفس النوع

---

[1] نصير بوعكاز، سعيد بوعكاز، **التأمين من المخاطر السيبرانية، تجارب دولية**، مذكرة ماستر غير منشورة، (جامعة ابن خلدون: كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، 2023/2022)، ص. 17.

[2] أسامة حسام الدين، مرجع سابق، ص. 54.

[3] ديتشه فيلله، **تعرف على خمسة من أخطر فيروسات الحاسوب**، في: https://www.aljazeera.net/tech/2016/11/1، بتاريخ:(2025/4/3).

لها نفس الشـــفرة التي تمكنها من اســـتغلال ثغرة معينة ولها نفس طريقة الانتشـــار وتحمل نفس أوامر الهجوم.[1]

هنـاك العـديـد من الأمثلـة على الـديـدان من بينهـا" الـدودة الحمراء (*code Red Worm*)، تم تسميتها بهذا الاسم من قبل شركة أمن الكمبيوتر الأمريكية (eEye Digital Security)، كان أول ظهور لها في: 12. 07. 2001، تعد سريعة في التكاثر لدرجة إنها استطاعت في ظرف أسبوعين إصابة أكثر من 350 ألف خادم حول العالم في أقل من أســـبوعين، إذ تتميز بأنها تتكاثر بدون أي تدخل بشـــري، إذ تعمل هذه الأخيرة من خلال إطلاقها لهجمات من خوادم مصابة بهدف إغراق الوصول إلى مواقع الويب كما استهدفت (*Code Red Worm*) وزارة الدفاع الأمريكية وسيرفر البيت الأبيض.[2]

ت. أحصـــنة طروادة (*Trojan horses*): هو برنامج ضـــار يحمل في طياته أوامر خبيثة داخل عمليات مســـموح بها، مثل اللعب على الأنترنيت، ويشـــتغل هذا النوع من البرمجيات الضـــارة المميزات والصـــلاحيات التي يمتلكها المستخدم الذي قام بتعديل الحصـــان، يختلف حصـــان طروادة من الفيروس، حيث يرفق الحصان نفسه بملف اتغير قابلة للتنفيذ مثل ملفات الصور أو الصوت.[3]

أحد أشهر أحصنة طروادة الذي تستهدف منها الخدمات المصرفية هو (*ZeusTrojan*)أو (*Zbot*) كان أول ظهور لهذا الفيروس في: 2007، اســـتخدم من قبل أحد القراصـــنة الذي ســـرق البيانات المالية للمســـتخدمين من أوروبا الشـــرقية لاستهداف وزارة النقل الأمريكية، يصـيب فيروس (*ZeusTrojan*)نظام مايكروســـوفت ويندوز (*Microsoft Windows*)، إذ يعتمد (*ZeusTrojan*) على أجهزة الكمبيوتر التي تعمل بنظام ويندوز:

الطريقة الأولى: التنزيلات الغير مقصودة من خلال دخول المتسللين إلى مواقع الويب الذي يثق فيها المستخدم ويقومون بإدخال برنامج ضار إلى موقع الويب ومن خلال ذلك يقوم المستخدم بتنزيل الملفات إلى جهاز المستخدم دون علمه وبذلك يكون البرنامج الضار قام بتثبيت نفسه عندما يقوم المستخدم بزيارة موقع الويب.

---

[1] أسامة حسام الدين، مرجع سابق، ص. 54.

[2] *Emmanuel Paquette,**Le ver code red est toujours dans le fruit**,dans:https://www.lesechos.fr/2001/08/le-ver-code-red-est-toujours, (03/4/2025).*

[3] وليم سلامة، وآخرون، **الأمن السيبراني للخدمات المالية والمصرفية**، (برلين: المركزالديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية، ج 01،2022)، ص. 361.

الطريقة الثانية: رسائل التصيد الاحتيالي: يقوم المستخدم بتنزيل برامج ضارة من روابط في رسائل البريد الإلكترونية أو منشور على وسائل التواصل الاجتماعي. اعتمادا على مكتب التحقيقات الفيدرالي الـ(F.B.I) عام 2014، قدر أن البرنامج أصاب ما يقارب مليون جهاز كمبيوتر 25% منها في الولايات المتحدة وقد نتج عن ذلك أضرارا مالية تجاوزت 100 مليون دولار.[1]

ث. **القنابل المنطقية:** هو عبارة عن برنامج خبيث يستعمل محفزا لبدء تشغيل شفرته الخبيثة، هذا المحفز قد يكون إما للوصول لتاريخ معين أو وقت معين أو تشغيل برنامج آخر، أو حذف حساب للمستخدم، وتبقى القنبلة المنطقية كامنة حتى يقع المحفز، وعندما تنشط تباشر فورا بتنفيذ تعليمات برمجية تهدف إلى إلحاق الضرر بأنظمة الحاسوب، يمكن للقنبلة المنطقية أن تدمر قواعد البيانات، تنزل ملفات، تهاجم أو تعرقل عمل نظام التشغيل أو التطبيقات.

ج. **برمجيات الفدية:** تستولي برمجيات الفدية على نظام الكمبيوتر والبيانات بداخله، ولا تعيدها للمستخدم إلا بعد دفع الفدية، التقنية الأكثر شيوعا لهذه البرمجيات هي الوصول إلى بيانات الضحية وتشفيرها بمفتاح غير معروف، بعد ذلك يدفع المستخدم المال مقابل إزالة التشفير واستعادة البيانات، بعض برامج الفدية تستغل الثغرات في الجهاز لإغلاق النظام، تنتشر هذه البرمجيات عن طريق أحصنة طروادة و غالبا ما تحدث نتيجة تنزيل ملف أو استغلال ثغرات في البرامج، يدفع المستخدم الفدية في نظام دفع عبر الأنترنيت وعندما يدفع الضحية يرسل المهاجم برنامج فك التشفير أو رمز القفل.[2]

من بين الأمثلة المعروفة لهذا النوع من برامج الفدية هو الفيروس الذي حمل اسم " أريد البكاء" ظهر لأول مرة في 2017، وهو عبارة عن برنامج ضار يستهدف أجهزة الكمبيوتر التي تعمل بنظام التشغيل(Microsoft Windows)، يقوم فيروس أريد البكاء بتشفير جميع الملفات الموجودة على الحاسب، والطريقة الوحيدة لفك التشفير هو دفع فدية والذي يتم عبر الحاسب باستخدام العملة الرقمية "بت كوينت"، وفي حال تم رفض دفع الفدية يتم حذف البيانات بشكل كامل، استهدف هذا الفيروس مؤسسة الصحة البريطانية، العديد من الدول: روسيا، وألمانيا، والهند، وأوكرانيا، إسبانيا.[3]

ح. **برمجيات الدعاية:** يعمل هذا البرنامج على تفعيل رسائل منبثقة تظهر للمستخدم أثناء استخدامه للحاسوب، تحمل معلومات عن منتج أو خدمة أو سلعة لتحقيق الربح للمهاجم، بحيث تكون برمجيات

---

(1) *Kurt baker, **The Zeus trojan malware-definition and prevention** in:https://www.crowdstrike.com/en-us/cybersecurity-101/malware/zues,(3/4/2025).*

(2) أسامة حسام الدين، مرجع سابق، ص. 55.

(3) *فراس اللو، فيروس "أريد البكاء" ...الفدية في مقابل فك التشفير، في: https://www.aljazeera.net.cdn.a;pproject.org، بتاريخ: (03/2025).*

الدعاية قادرة على تحليل اهتمامات المستخدم ورغباته عن طريق تتبع المواقع التي زارها، بعد ذلك تعرض البرمجية رسائل ذات صلة بما يرغب فيه المستخدم.

خ. **برمجيات الذعر:** هذا النوع من البرامج يقوم بإجبار المستخدم على اتخاذ قرار بناء على تخويفه من شيء أو حدث ما، بحيث أن تخويف الضحية من هذا البرنامج يجعله يقوم بتحميل البرنامج وبالتالي تكون هذه البرامج بهدف التخريب.[1]

2. الهندسة الاجتماعية:

تعرف الهندسة الاجتماعية بأنها محاولة استغلال ثقة الأشخاص من أجل الحصول على المال أو المعلومات السرية مستعملين مواقع التواصل الاجتماعي كالأداة الأبرز من خلال تأثيرها بشكل جماعي على المجتمعات واستعمال أساليب الاحتيال، كما تعرف بأنها نوع من التقنيات المستخدمة من المجرمين الإلكترونيين لاستدراج مستخدمين لإرسال بياناتهم السرية وإصابة أجهزتهم الإلكترونية ببرامج ضارة أو فتح روابط ومواقع مصابة بفيروسات وعلى سبيل المثال: أن يقوم المهاجم بالاتصال بالضحية ويكذب عليه في محاولة لأخذ صلاحيات للوصول للبيانات فيقوم بالتظاهر بأنه يحتاج لمعلومات شخصية أو بيانات لكي يتحقق من هوية المستخدم.[2]

3. **الهجمات:** وتضم نوعين من الهجمات

أ. **هجمات قطع الخدمة:** هو نوع من الهجمات الالكترونية التي تستهدف الشركات بالدرجة الأولى إذ يقوم المهاجمون بتنفيذ هجماتهم على الأنظمة والخوادم والشبكات، وذلك بضخ كميات كبيرة من البيانات والحركة لإرباكها واستنفاذ مواردها. هذا يعيق قدرتها على التعامل مع الطلبات مما يؤدي إلى إيقاف الموقع الإلكتروني وتباطؤه. في هذا النوع من الهجمات، يغرق المهاجم الموقع المستهدف بكمية هائلة من البيانات والطلبات عديمة الفائدة، مما يسبب بطئا شديدا أو تعطل للموقع قد يستمر لأيام، ويحرم المستخدمين من الوصول إلى الخدمة بالإضافة إلى ذلك تتكبد المؤسسات خسائر مالية كبيرة.[3]

ب. **هجمة الرجل الوسط:** هو نوع من الهجمات المشفرة عبر قناة اتصال من قبل طرف ثالث ضار، حيث يستولي على قناة اتصال سرية وشخصية بين نقطتي اتصال او طرفين شرعيين، وفي هذا النوع يمكن

---

[1] أسامة حسام الدين، مرجع سابق، ص.57.

[2] عمر هارون، "الهندسة الاجتماعية الجماعية"، **مجلة الشرطة**، ع 158، (ماي 2024)، ص. 158.

[3] ابراهيم السيد احمد رمضان،" مواجهة الهجمات السيبرانية في ضوء أحكام القانون الدولي"، **مجلة العلوم الاقتصادية والقانونية**، ع 01، (يناير2025)، ص. 1771.

للمهاجم التحكم في حركة الاتصالات بين الضحايا، كما لا يترك المهاجم أدلة او أثار الكترونية لهذه الجريمة، وباختصار يظل المهاجم غير مرئي.[1]

2.هجمات البريد الالكتروني والمتصفح وتشمل على:

أ-البريد المزعج: معروف كذلك بالبريد المهمل (*spam*)، وهو رسائل بريدية تأتي من مصدر غير معروف، في معظم الحالات يكون هذا النوع من هذه الرسائل بغرض الدعاية والإعلان، ومع ذلك يمكن أن يحتوي البريد المزعج على روابط ضارة أو برامج خبيثة أو محتوى مضلل، ويكون الهدف في تلك الحالات هو الحصول على معلومات المستخدم الحساسة مثل كلمات المرور أو أرقام بطاقة الائتمان.[2]

ب-الاصطياد يقوم المهاجم بتظاهر بأنه من جهة معتمدة، ثم يرسل رسائل الكترونية مضللة للضحية. عند فتح الرسالة والنقر على الرابط الخبيث، يتمكن المخترق من الوصول الى المعلومات الحساسة وبيانات الحاسب، بالإضافة الى تثبيت برامج ضارة على الشبكة.[3]

ت-برامج التجسس: برامج يتم تحميلها على أجهزة الكمبيوتر بهدف جمع معلومات حول العميل أثناء تصفحه لشبكة الانترنت. بحيث يتم تثبيت هذه البرامج بموافقة المستخدم أو بدونها أثناء تنزيل إحدى الألعاب أو البرامج كما تسعى برامج التجسس إلى الاطلاع على الملفات الشخصية كلمات المرور، بطاقة الائتمان. [4]

المطلب الرابع: المخاطر المترتبة عن اختراق البيانات الشخصية

يعد اختراق البيانات الشخصية من أخطر التهديدات في الفضاء السيبراني، حيث تؤدي إلى مجموعة من العواقب السلبية على الأفراد والمؤسسات، فبعد حصول المهاجمون على المعلومات الحساسة، مثل أرقام الهوية كلمات المرور وأرقام الحسابات البنكية يتم استخدامها بشكل غير قانوني ما ينعكس بشكل سلبي على الأفراد والمؤسسات، إذ تترتب على اختراق البيانات الشخصية مجموعة واسعة من المخاطر على الأفراد والمؤسسات.

أولا: بالنسبة للمؤسسات: اختراق البيانات يمثل تهديدا كبيرا للمؤسسات، حيث يمكن أن يؤدي إلى عواقب وخيمة تتجاوز مجرد فقدان المعلومات، تتمثل المخاطر في:

---

(1) *Avijit Malik and others, «Man in the middle -attack: Understanding in simple words," **International Journal Of Data Network Science**, 2019, p. 844.*

(2) أسامة حسام الدين، مرجع سابق، ص. 56.

(3) ابراهيم السيد ر مضان، م، رجع سابق، ص. 1773.

(4) أسامة حسام الدين، مرجع سابق، ص. 57.

أ. **الإضرار بالسمعة:** إن الإضرار بالسمعة هي من أبرز التأثيرات السلبية التي تنجم عن اختراق البيانات، عندما تتعرض مؤسسة ما لهجوم سيبراني يتم من خلاله اختراق البيانات الشخصية، فإن ذلك يظهر عجزها عن حماية هذه البيانات مما يؤدي إلى فقدان الأفراد لثقتهم في الجهة التي تجمع وتخزن البيانات هذا التدهور يؤدي إلى فقدان العملاء وبالتالي يضر بسمعة المؤسسة.[1]

ب. **الإضرار بالبنية التحتية أو تعطيل عملها:** اختراق البيانات وتسريبها يمكن أن ينجر عنها أضرار جسيمة على البنية التحتية، خاصة إذا كانت البيانات التي يتم اختراقها تتعلق بأنظمة تشغيلية أو معلومات حساسة مثل كلمات مرور وغيرها التي تخص المؤسسة، إذ يمكن للمتسللين باستخدام تلك البيانات للتحكم أو التلاعب بالأنظمة أو تعطيل أنظمة التحكم في المؤسسة مثل شبكة الاتصالات.[2]

ت. **الخسائر المالية:** يشكل اختراق البيانات الشخصية خطرا ماليا كبيرا على المؤسسات، فبعد وقوع الاختراق تضطر المؤسسات إلى دفع تكاليف الإصلاح بما فيها اصلاح الأنظمة والشبكات والبيانات، كذلك تكاليف لشراء معدات جديدة و حلول للحماية لتحسين أنظمة الأمان الخاصة بها لمنع تكرار حوادث اختراق البيانات وهدا ما يضيف أعباء مالية على المؤسسة ، و من الأمثلة الشهيرة على المؤسسات التي تكبدت خسائر مالية كبيرة جراء تعرضها للاختراق "الشركة الفرنسية للاتصالات (*Orange*) بحيث أسفر الاختراق عن سرقة بيانات أكثر من 1.3 مليون من عملائها وبلغت تكلفة الحوادث أكثر من 24 يورو (29 مليون دولار).

ث. **عقوبات قانونية:** تواجه المؤسسات التي تتعرض لإختراق البيانات وسرقتها مجموعة من المخاطر القانونية، ويتضح ذلك في حال وقوع هجوم سبراني لا يقع اللوم القانوني فقط على المجرمين المتسللين بل تتحمل المؤسسات مسؤولية ذلك في حال تم السماح بالهجوم أو تمكينه جزئيا بسبب إهمال المؤسسة لتحديث البرامج أو تطبيق السياسة أمنية قوية، إضافة إلى ذلك تترتب عن مسؤول الأمن في المؤسسة بعد وقوع الاختراق واكتشافه تحقيقات لتحديد ما إذا كانت المؤسسة قد امتثلت لالتزامات واللوائح المتعلقة بأمن البيانات.[3]

---

(1) *Luke Noonane,* ***5Damaging consequences of Data breach: protect your assests****,* *https://www.metacompliance.com/blog/data-breaches/5-damaging-consquences-of-a-data-breach(2025/04/05).*

(2) أميرة عبد العظيم، محمد عبد الجواد، مرجع سابق، ص. 431.

(3) *Justine Gretten,****cyberattaques quels sont les risques pour votre entreprise ?,*** *dans : Https://www.mailinblack.com/resources/blog/cyberattaques-quels-sont-les-risques-pour-votre-entreprise, (05/04/2025).*

ثانيا: بالنسبة للأفراد: كما سبق الإشارة إلى أن اختراق البيانات له عواقب وخيمة على الأفراد والمؤسسات على حد سواء تتمثل المخاطر التي تترتب على اختراق البيانات للأفراد:

أ. **الابتزاز:** بعد حدوث الاختراق يقوم المهاجمون باستغلال الثغرات أو نقاط الضعف في النظام، إذ يقومون بتشفير البيانات باستخدام مفتاح التشفير والمطالبة بدفع فدية التشفير أو التهديد ببيع أو نشر هذه البيانات إن لم يتم دفعها، [1]مثلما حدث في 2017 برنامج فدية أريدالبكاء بتشفير بيانات العديد من الدول وقام بإرسال رسائل الكترونية لتشفير البيانات وقام بمطالبة بدفع الفدية لتعود الأجهزة إلى عملها الطبيعي.[2]

ب. **تشويه السمعة:** وذلك من خلال استخدام المتسللين لاسم الضحية وتوريطه في نشاط إجرامي، أو نشاط غير قانوني على سبيل المثال، إذا كان المتسللون لديهم معلومات طبية الخاصة بالضحية وقد يستخدموها لتقديم طلب للحصول على خدمات طبية باسمه والحصول على أدوية موصوفة طبيا لأغراض غير قانونية أو كشف عن تفاصيل الحياة الشخصية للضحية لا يريد أن تكون معروفة، هذا ما يؤدي إلى تشويه السمعة.

ج. **الاحتيال المالي:** فبعد اختراق البيانات يقوم المهاجمون باستخدام البيانات المالية المسروقة مثل أرقام أو بطاقة الائتمان، تفاصيل الحسابات البنكية ويتم استخدام تلك البيانات لإجراء عمليات شراء احتيالية عبر الانترنت أو سحب النقود من أجهزة الصراف الآلي.

2- **سرقة الهوية:** تحدث سرقة الهوية عندما يستخدم الفرد المعلومات الشخصية لشخص أخر لارتكاب جرائم الاحتيال أو جرائم أخرى بعد هذا خطرا كبيرا بعد اختراق البيانات لأن المجرمين يمكن استخدام المعلومات المسروقة على قروض أو رهون عقارية وفي نهاية المطاف قد تنتهي بالضحية أن يكون مسؤول عن النفقات المتعلقة بالسرقة بل وربما يتم اتهامهم بارتكاب جرائم ارتكبها الشخص الذي سرق الهوية.[3]

المبحث الثالث: الآليات الإستراتيجية للأمن السيبراني

---

[1] شيماء مرزوق، وزين تركية جلال، **انعكاسات الامن السيبراني على أمن المعلومات في البنوك**، مذكرة ماستر غير منشورة، (جامعة الشهيد الشيخ العربي التبسي: كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، 2024/2023)، ص. 33.

[2] فراس اللو، **فيروس "أريد البكاء" ...الفدية في مقابل فك التشفير**، في: https://www.aljazeera.net.cdn.a;pproject.org،بتاريخ: (03/2025/04).

[3] *Cyber Management school,,**Qu'est-ce que le vol des données ? (Datatheft)**, dans https://www.proofpoint.com/fr/threat-reference/data-theft , (05/04/2025).*

مع تزايد الاعتماد على التكنولوجيا والأنظمة الرقمية في مختلف القطاعات برزت التهديدات السيبرانية كأحد أبرز التحديات التي تواجه المؤسسات والدول حيث تشكل خطرا حقيقيا على سرية البيانات وسلامة الأنظمة خصوصا في المؤسسات الحيوية مثل القطاع البنكي هذا ما يستدعي وضع آليات إستراتيجية للأمن السيبراني تقوم على أسس قانونية وتقنية ومؤسساتية تهدف إلى الوقاية من التهديدات الالكترونية والتصدي لها.

المطلب الأول: الآليات القانونية الدولية لحماية البيانات الشخصية

اهتم التشريع الدولي بموضوع حماية البيانات الشخصية من خلال إقرار جملة من المعاهدات والاتفاقيات الدولية التي تهدف إلى تكريس حماية الخصوصية بصفة عامة والبيانات الشخصية بصفة خاصة.

أولا: الاتفاقيات الدولية والأممية لحماية البيانات الشخصية

من أهم الاتفاقيات والمعاهدات الدولية الرامية إلى حماية البيانات الشخصية للأفراد هي:

1) الاتفاقيات الدولية لحماية حقوق الإنسان:

أولت الاتفاقيات الدولية لحقوق الإنسان أهمية لحماية البيانات الشخصية من خلال إقرارها للحق في الحياة الخاصة، هذا ما تضمن عليه الإعلان العالمي لحقوق الإنسان لسنة 1948 بحيث ورد في المادة 12 من الإعلان العالمي لحقوق الإنسان: "لا يجوز تعرض أحد لتدخل تعسفي في حياته الخاصة أو شؤون أسرته أو مسكنه أو مراسلاته أو لحملاته على شرفه وسمعته ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات"، ويعتبر الحق في حماية البيانات الشخصية مشمولا بهذه المادة لأن الكشف عنها يكشف عن الحياة الخاصة، ويعتبر الإعلان أول إطار قانوني دولي لهذا الحق، [1]وعليه يتبين بأن حماية البيانات الشخصية تستمد أساسها القانوني من مختلف الاتفاقيات الدولية لحقوق الإنسان على اعتبار أن الحق في حماية البيانات الشخصية من حقوق الإنسان عامة وتتدرج ضمن الحياة الخاصة التي تسعى كل القوانين إلى حمايته.[2]

[1] منى الأشقر، جبور و محمد جبور، مرجع سابق، ص. 24.

[2] وريدة جندلي، "حماية المعطيات الشخصية في ضوء التشريع الجزائري والمواثيق الدولية: بين الضمانات والتحديات"، **المجلة الاكاديمية للبحوث القانونية والسياسية**، م 01، ع 01، (2022)، ص. 1421.

2) الاتفاقيات والمعاهدات لحماية المصنفات الأدبية والفنية والرقمية:

تم إبرام العديد من الاتفاقيات والمعاهدات في نطاق حماية البيانات الشخصية المدرجة ضمن المصنفات الأدبية والفنية الرقمية التي يمكن أن تتداول عبر الانترنيت ومن أهم وأبرز المعاهدات هي:

❖ **اتفاقية برن لحماية المصنفات الأدبية والفنية لسنة 1886:** تعد من أقدم المواثيق الدولية التي اهتمت بحماية حقوق المؤلف أبرمت سنة 1886، تضمنت الاتفاقيات جملة من المبادئ الواجب توفرها لحماية مختلف المصنفات الأدبية و الفنية، كما نصت المادة: 02، من اتفاقية برن على تعريف المصنفات بأنها:" كل إنتاج في المجال الأدبي و العلمي و الفني أي كانت طريقة أو تشكل التغيير عنه" بحيث كفلت هذه المعاهدة مجموعة من الحقوق المعنوية على غرار الحق في المطالبة بنسبة المصنف إلى مؤلفه و الحق في الاعتراض على أي تشويه أو تحريض أو تعديل المصنف من شأنه الإضرار بمكانة المؤلف أو بشهرته، ولم تتضمن هذه المعاهدة الإشارة إلى برامج الإعلام الآلي ضمن المصنفات الأدبية و الفنية و لم تعالج هذه الاتفاقية مسألة الوسائل الرقمية و تطبيقات الإعلام الآلي في نقل و تعديل المعطيات ضمن مختلف المؤلفات الرقمية هذا القصور دفع إلى إبرام اتفاقيات أخرى تعني بهذا الجانب منها:

❖ **اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفردية (تريبس):** تم التوقيع على هذه المعاهدة في 1994 وبدأ حيز التطبيق بتاريخ 2000/1/1، احتوت هذه الاتفاقية على العديد من القواعد المكرسة لحماية المصنفات الرقمية وأيضا آليات حماية برامج الحاسوب وقواعد البيانات[1] وهذا ما يؤكد عليه في نص المادة 10 من المعاهدة:" تتمتع برامج الحاسب الآلي (الكمبيوتر) سواء كانت بلغة المصدر أو بلغة الآلة بالحماية باعتبارها أعمالا أدبية بموجب معاهدة برن (1971).[2]

3) اتفاقية بودابست المتعلقة بالجريمة الإلكترونية:

أبرمت الاتفاقية في 2001/11/23 من طرف 26 دولة من أعضاء الاتحاد الأوروبي إضافة إلى كندا، اليابان جنوب إفريقيا والولايات المتحدة الأمريكية ودخلت حيز التنفيذ سنة 2004، إذ تهدف هذه الأخيرة بشكل أساسي إلى إتباع سياسة جنائية مشتركة تهدف إلى حماية المجتمع ضد الجرائم الالكترونية ووضع التشريعات المناسبة وتحفيز التعاون الدولي لمحاولة القضاء على الاعتداءات التي تقع على المعلومات ذات الطابع الشخصي في العالم الرقمي.[3]

---

[1] عبد الهادي كحلاوي مرجع سابق، ص125، 126.

[2] منظمة التجارة العالمية، **الإتفاقية المتعلقة بالجوانب التجارية لحقوق الملكية الفكرية(تريبس)**، 15 أفريل 1994، ص10.

[3] وريدة جندلي، مرجع سابق، ص. 1423.

4) الدليل الإرشادي لمنظمة التعاون الاقتصادي والتنمية

قامت منظمة التعاون الاقتصادي والتنمية 1978 بإعداد القواعد الإرشادية لحماية الخصوصية وضمان نقل البيانات الشخصية عبر الحدود وتم المصادقة على هذه القواعد وتبنيها في 1980 من قبل الدول الكبرى: ألمانيا، بلجيكا، بريطانيا، اليابان، الولايات المتحدة الأمريكية، كندا، والنمسا. بحيث يتضمن هذا الدليل الإرشادي البيانات والمعلومات الشخصية على أنها معطيات تتوفر لها الحماية في كل مرحلة من مراحل الجمع والتخزين والمعالجة.[1]

5) المبادئ التوجيهية للجمعية العامة للأمم المتحدة

تبنت الجمعية العامة للأمم المتحدة مجموعة من المبادئ التوجيهية بموجب القرار رقم 45/95 الصادر في سنة 1990 بحيث أكد هذا القرار على وجوب قيام الدول الأعضاء بفرض رقابة داخلية مع إقرار عقوبات جزائية ضمن القوانين الداخلية للدول المعنية لمخالفين هذه المبادئ التوجيهية، إذ أن تنفيذ هذه الأخيرة واجبة من قبل الدول المعنية بحيث تشمل المبادئ التوجيهية على: مبدأ الأمن، مبدأ صحة البيانات، مبدأ عدم التمييز عند معالجة البيانات الشخصية، مبدأ المشروعية والنزاهة، مبدأ وصول الأشخاص المعنيين بالبيانات لملفاتهم.[2]

ثانيا: الاتفاقيات الإقليمية لحماية البيانات الشخصية

أسفرت الجهود الدولية على إبرام عدة اتفاقيات تعني بحماية البيانات الشخصية.

1) على المستوى الأوروبي: من أهم الاتفاقيات والمعاهدات التي أبرمت على المستوى الأوروبي.

أ. الاتفاقية الأوروبية لحقوق الإنسان لسنة 1950: تم إبرام الاتفاقية في 4 نوفمبر 1950 ودخلت حيز التنفيذ، بتاريخ 3 سبتمبر 1953، نصت الاتفاقية في مادتها الأولى على التزام الدول الأعضاء باحترام حقوق والحريات الخاصة بكل شخص، لاسيما السياسية منها كالحق في حماية الخصوصية اتجاه معالجة البيانات الشخصية. وأكدت المادة 08 من هذه الاتفاقية، على الحق في الخصوصية باعتباره حقا من حقوق الإنسان.[3]

ب. اتفاقية مجلس أوروبا 108: في سنة 1981 أعلنت لجنة وزراء مجلس أوروبا اتفاقية حماية الأفراد في نطاق المعالجة الآلية للبيانات الشخصية في مدينة ستراسبورغ، إذ عملت هذه الاتفاقية على خلق نظام قانوني يضمن حماية للمعطيات الشخصية، كما تتضمن هذه الاتفاقية مجموعة من المبادئ التي

---

[1] كحلاوي عبد الهادي، مرجع سابق، ص. 134 - 136.

[2] كحلاوي عبد الهادي، مرجع سابق، ص. 142.

[3] الاتفاقية الأوروبية لحقوق الإنسان، روما، في:(4 نوفمبر 1950)، مكتبة حقوق الإنسان، جامعة منبوستا.)، المادة 1.

يجب أن يتضمنها تشريع الدولة الموقعة على الاتفاقية، كما نصت هذه الاتفاقية ولخصتها في شروط يجب توافرها في البيانات الشخصية التي تكون باختصار في الفصل الثاني (المادة 05):"بيانات صحيحة، عدم إنشاء البيانات، تحديد المدة الزمنية لحفظ البيانات، حق الشخص المعني في التعرف على البيانات، توفير الحماية الأمنية، تحديد الجهات والأشخاص المرخص لهم، كما نصت الاتفاقية أيضا في مادتها السادسة على أنه يرفض تماما معالجة المعطيات ذات الطابع الشخصي المتعلق بالأصل العرقي والآراء السياسية والمعتقدات الدينية والمتعلقة بالوضع الصحي والحياة الجنسية والأحكام الجنائية.[1]

ج. التوجيه الأوروبي 95-46 المتعلق بحماية المعطيات الشخصية: يمثل التوجيه الأوروبي الأمر التشريعي الخاص بحماية المعطيات ذات الطابع الشخصي صدر عن البرلمان الأوروبي بتاريخ 1995/10/24، تضمن هذا التوجيه مجموعة من المبادئ التي تهدف إلى تامين حماية الحريات والحقوق الأساسية للأشخاص الطبيعيين وعلى وجه الخصوص حياتهم الخاصة حسب ما أكدته المادة الأولى من هذا التوجيه.[2]

د. اللائحة العامة الأوروبية لحماية البيانات (*GDPR*): أعدها البرلمان الأوروبي ومجلس الاتحاد الأوروبي بتاريخ 2016/04/27 ودخلت حيز التنفيذ في 2018/05/25، و تأتي هذه اللائحة الجديدة لتحل محل التوجيه الأوروبي إذ قام هذا النظام بتوسيع من نطاق حماية المعطيات الشخصية بحيث تهدف إلى منح المستخدم التحكم الكامل في بياناته بحيث لا يمكن أن تتم المعالجة إلا بالموافقة المستخدم على ذلك كما يتيح هذا النظام للمستخدم المقيم في بلدان الاتحاد طلب نسخة الكترونية عن بياناته للاطلاع عليها، تتكون اللائحة من مجموعة القوانين تطبق على كل الدول الأعضاء في الاتحاد الأوروبي بهدف خلق إطار تشريعي موحد لكافة دول الاتحاد، إذ تعزز هذه اللائحة حماية لبيانات الأفراد كما تتضمن هذه اللائحة أنواع البيانات المعالجة و تحدد أصحاب البيانات المعنية وكيفية معالجة هذه البيانات في إطار تشريعي منظم.[3]

---

[1] سامية خوانرة، "المبادئ الأساسية لحماية البيانات الشخصية بين الجهود الدولية والتشريع الجزائري"، **مجلة الرسالة للدراسات والبحوث الإنسانية**، م 07، ع 03، (ماي 2022)، ص. 321.

[2] هشام كلو، أحلام شكورة، "الحماية القانونية للمعطيات الشخصية بين الاتفاقيات الدولية والتشريع الجزائري"، **مجلة الحقوق والعلوم السياسية**، م10، ع 02، (2022)، ص. 410.

[3] المرجع نفسه، ص. 411.

ثالثا: اتفاقيات حماية البيانات الشخصية على المستوى الإفريقي

اتفاقية الاتحاد الإفريقي بشأن أمن الفضاء الالكتروني وحماية البيانات الشخصية: تم إبرام الاتفاقية في سنة 2014، إذ تم اعتمادها في الدور 23، في مدينة مالابو المتواجدة في غينيا الاستوائية، تهدف اتفاقية الاتحاد الأوروبي إلى تأسيس نص قانوني يعمل على التصدي للجرائم الإلكترونية على مستوى القارة السمراء، إذ تضمنت الاتفاقية على سبل واليات ومكافحة الجرائم السيبرانية وكذا حماية البيانات الشخصية، وضمان ان يكون تناسق بين التشريعات الوطنية للدول الأعضاء ومضمون الاتفاقية مع احترامها لحقوق الإنسان.[1]

رابعا: اتفاقيات حماية البيانات الشخصية على المستوى العربي

الاتفاقية العربية لمكافحة جرائم تقنية المعلومات: صدرت الاتفاقية بتاريخ 2010/12/21 في القاهرة، حيث تهدف هذه الاتفاقية وفق للمادة الأولى من الفصل الأول للاتفاقية إلى تقرير التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات للحفاظ على أمن الدول العربية ومصالحها وسلامة مجتمعها وأفرادها، وأقرت الاتفاقية إن كل دولة طرف في هذه الاتفاقية ملزمة بتجريم الأفعال الواردة في المواد التي تضمنها الفصل الثاني المعنون ' بالتجريم' وهذه الأفعال تشمل: الاعتداء على سلامة البيانات، جرائم إساءة استخدام وسائل تقنية المعلوماتية، التزوير الاحتيال، الاعتداء على حرمة الحياة الخاصة، الجرائم المتعلقة بالإرهاب بواسطة تقنية المعلومات مثل: نشر أفكار جماعات إرهابية والدعوة إليها، أيضا ما يتعلق بالجريمة المنظمة مثل: غسل الأموال والترويج للمخدرات والاتجار بالبشر والأعضاء البشرية والأسلحة.

إذ انعكست هذه الاتفاقية على الجانب التشريعي العربي فهناك العديد من الدول العربية التي واكبت هذا التطور التقني الحاصل في مجال تكنولوجيا المعلومات وعملت على محاولة التصدي للجرائم بإنشائها لتشريعات خاصة.[2]

---

[1] محمد محمود فياله، "القانون الدولي والتحديات المعاصرة الجريمة السيبرانية نموذجا"، **مجلة الحقوق للبحوث القانونية والاقتصادية**، م 01، ع 01، (يوليو 2024)، ص. 844.

[2] محمد أحمد لبيب أحمد، وآخرون،"دور الاتفاقيات الدولية والإقليمية في مجال الأمن السيبراني وموقف الدولة المصرية منها"، م**جلة الحوكمة والوقاية من الفساد ومكافحته**، ع 01، (سبتمبر 2023)، ص. 153.

المطلب الثاني: الآليات القانونية الوطنية لحماية البيانات الشخصية

كرس المشرع الجزائري جملة من التدابير الوقائية لحماية البيانات الشخصية في عدة نصوص قانونية عامة وخاصة ويتجلى ذلك:

أولا: في الدستور: كفل الدستور 1996 وكذا التعديلات الطارئة عليه سنة 2008، 2016، 2020، حماية للحقوق الأساسية والحريات الفردية، وذلك عن طريق أهم المبادئ الدستورية في عدد من المواد، فقد ورد في المادة 34 من دستور 1996: " تضمن الدولة عدم انتهاك حرمة الإنسان"،[1] كما ورد في المادة 39 من دستور 1996 أنه: "لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه ويحميها القانون، سرية المراسلات والاتصالات الخاصة بكل أشكالها ومضمونة."[2]

من خلال استقراء هذه المادتين التي نص عليها دستور 1996 فإن المشرع حرم انتهاك حرمة حياة المواطن الخاصة، [3] بحيث لم ينص دستور 1996 صراحة على مصطلح "البيانات الشخصية" كما هي معروفة حاليا ولكنه وردت نصوص دستورية تؤسس لحماية الخصوصية لحرمة حياة المواطن الخاص، وفي دستور 2016، كرس المشرع الجزائري حماية دستورية للحق في الحياة الخاصة للأفراد من خلال المادة 40: "تضمن عدم انتهاك حرمة الإنسان". والمادة 46:"لا يجوز انتهاك حرمة حياة المواطن الخاصة، حرمة شرفها ويحميها من القانون. سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة.

لا يجوز بأي شكل المساس بهذه الحقوق دون أمر محلل من السلطة القضائية، ويعاقب القانون على انتهاك هذا الحكم. حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي حق أساسي يضمنه القانون ويعاقب على انتهاكه.[4]

من خلال القراءة المتمعنة للمادتين(40 و46) من دستور 2016، نجد أن المشرع الجزائري نص صراحة لأول مرة على حماية المعطيات ذات الطابع الشخصي، واعتبر حماية المعطيات ذات الطابع الشخصي حقا أساسيا يُعاقب القانون على انتهاكه، وقد أكد على هذا الحق في المادة 47 من دستور2020.

---

[1] العبد شعبان، مسعود مرتقي، **الجرائم السيبرانية في القانون الجزائري**، مذكرة ماستر غير منشورة، (جامعة زيان عاشور: كلية الحقوق والعلوم السياسية، 2022/2021)، ص. 49.

[2] الجمهورية الجزائرية الديمقراطية الشعبية، المرسوم الرئاسي رقم 96-438، المؤرخ في: 26 رجب 1417 الموافق لـ7 ديسمبر 1996، الجريدة الرسمية، العدد 76، الصادر بتاريخ 8 ديسمبر 1996.

[3] منى الأشقر جبور، محمود جبور، مرجع سابق، ص. 27.

[4] الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 16-01، المؤرخ في: 26 جمادى الأولى عام 1437 الموافق لـ06 مارس 2016، الجريدة الرسمية، العدد 14، الصادر بتاريخ: 07 مارس 2016.

ثانيا: قانون العقوبات: كرس المشرع الجزائري حماية للمعطيات الشخصية أثناء معالجتها في القانون 04-15 المتضمن تعديل قانون للعقوبات، حيث خصص المشرع الجزائري في قانون 04-15 القسم السابع بعنوان المساس بأنظمة المعالجة الآلية للمعطيات، إذ تضمن هذا القسم أنواع الجرائم التي ترتكب بنظام المعالجة الآلية للمعطيات والعقوبات التي تسلط على كل من يثبت في حقه اختراق أنظمة معلومات المؤسسات أو الأفراد بطريقة غير شرعية ، كما تختلف هذه العقوبات على حسب جسامة الفعل المنتهك للمعطيات الشخصية،[1] بحيث نصت المواد 394 مكرر إلى 394 مكرر 7 على أنواع الاعتداءات على نظام المعالجة الآلية للمعطيات (الدخول و البقاء الغير المشروع في نظام المعالجة الآلية للمعطيات، الاعتداءات العمدية على نظام المعالجة الآلية للمعطيات، الاعتداءات العمدية على سلامة المعطيات الموجودة داخل النظام) و العقوبات المقررة لها.[2]

ثالثا: قانون العمل: نصت المادة 7 من قانون 11/90 يتعلق بعلاقات العمل: "أن لا يفشوا المعلومات المهنية المتعلقة بالتقنيات والتكنولوجيا وأساليب الصنع و طرق التنظيم وبصفة عامة أن لا يكشفوا مضمون الوثائق الداخلية الخاصة بالهيئة المستخدمة إلا إذ فرضها القانون أو طلبتها سلطتهم السلمية" لا يعد هذا القانون متخصصا في حماية البيانات الشخصية، لكن نص على التزام [3] العمال احترام السر المهني، خاصة بالنسبة للعمال الذين يتعاملون مع معلومات حساسة وبالتالي واجب التزام بالسر المهني يمكن اعتباره شكلا من أشكال حماية البيانات الشخصية .

رابعا: قانون الوظيف العمومي: نصت المادة 48 من الأمر 06-03 الذي يتضمن القانون الأساسي للوظيفة العمومية، " يجب على الموظف التزام بالسر المهني ويمنع عليه أن يكشف محتوى أية وثيقة بحوزته أو أي حدث أو خبر علم به أو اطلع عليه بمناسبة ممارسة مهامه، ما عدا ما تقضيه ضرورة المصلحة، ولا يتحرر الموظف من واجب السر المهني إلا بترخيص مكتوب من السلطة السلمية المؤهلة." [4]إذ أن هذا القانون لا يعالج موضوع حماية البيانات الشخصية بشكل مباشرة لكنه يتضمن نصوص مثل التزام بالسر المهني تكرس حماية للبيانات الشخصية.

---

[1] وريدة جندلي، مرجع سابق، ص. 1418.

[2] الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 04-15، المؤرخ في 27 رمضان 1425 الموافق ل 10 نوفمبر 2004، المعدل والمتمم للأمر رقم 66- 156 المؤرخ في 18 صفر عام 1386 الموافق ل 8يونيو 1966 والمتضمن قانون العقوبات، الجريدة الرسمية، العدد 71، الصادرة بتاريخ:(10/ 11 / 2004)، المادة 394.

[3] الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 90-11، المؤرخ في 26 رمضان 1410 الموافق لـ 21 أفريل 1990، المتعلق بعلاقات العمل، الجريدة الرسمية، العدد 17، الصادر بتاريخ: 25 أفريل 1990، المادة: 07.

[4] الجمهورية الجزائرية الديمقراطية الشعبية، الأمر رقم 06-03، المؤرخ في 19 جمادى الثانية 1427 الموافق لـ 15 يوليو 2006، المتضمن القانون الأساسي العام للوظيفة العمومية، الجريدة الرسمية، العدد 46، الصادرة بتاريخ 21 يوليو 2006، المادة 48.

خامسا: قانون الإجراءات الجزائية: تطرق المشرع الجزائري في هذا القانون إلى الإجراءات التي ينبغي تطبيقها على المستوى الوطني و التي تخدم التحقيقات الجنائية التي ترتكب عبر المنظومة المعلوماتية وجمع الأدلة ذات الطابع الالكتروني على الرغم من وجود صعوبات جملة في مجال مكافحة الإجرام السيبراني على سبيل المثال : تحديد هوية مرتكب الجريمة، ضياع البيانات الالكترونية التي يمكن تعديلها ونقلها أو إزالتها في ثوان معدودة على سبيل المثال : يستطيع الشخص الذي يتحكم في البيانات أن يستغل الثغرات الأمنية في أي منظومة معلوماتية ليقوم بمحو البيانات مهدما بذلك جميع الأدلة التي يقوم عليها التحقيق الجنائي هذا ما يجعل السرية و السرعة من المكونات الأساسية لنجاح التحريات،[1] بالإضافة إلى ذلك تدعمت الإجراءات القانونية بآلية تقنية جديدة تتمثل في : صدور القانون 16-03 المؤرخ في 2016/06/19 يتعلق باستعمال البصمة الوراثية في الإجراءات القضائية و التعرف على هوية الأشخاص كما تم تعزيز الجهات القضائية أربع محاكم مختصة متواجدة في الجزائر، وهران، قسنطينة، ورقلة إضافة إلى ذلك تضمن قانون الإجراءات الجزائرية تمديد [2] لاختصاص المحلى لوكيل الجمهورية في الجرائم الالكترونية في المادة:37 " يجوز تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة الاختصاص محاكم أخرى عن طريق التنظيم، و في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية و الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف." [3]

سادسا: حماية البيانات الشخصية في الأمر 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة: بموجب الأمر 03-05 اعتبر برامج الحاسوب الآلي من المصنفات الأدبية والفنية الواقعة تحت نطاق الحماية وذلك بموجب المادة 4 من الأمر 03-05 "تعتبر على الخصوص مصنفات أدبية أو فنية محمية كما يأتي: "المصنفات الأدبية المكتوبة مثل: المحاولات الأدبية والبحوث العلمية والتقنية الروايات القصص القصائد الشعرية وبرامج الحاسوب والمصنفات الشفوية مثل المحاضرات والخطب المواعظ باقي المصنفات التي تماثلها."[4]

---

[1] عبد القادر صواق، **مساهمة الأمن السيبراني للبيانات في تعزيز الثقة لدى العملاء نحو الخدمات**، أطروحة دكتوراه غير منشورة، (جامعة غرداية: كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، 2025/2024)، ص. 85.

[2] جمال بوازدية، مرجع سابق، ص. 78.

[3] الجمهورية الجزائرية الديمقراطية الشعبية، الأمر رقم 66-155، المؤرخ في 18 صفر 1386 الموافق لـ 8 يونيو 1966. المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، العدد48، الصادرة بتاريخ 8 يونيو 1966.

[4] الجمهورية الجزائرية الديمقراطية الشعبية، الأمر رقم 03-05، المؤرخ في 19 جمادى الأولى 1424 الموافق لـ 19 جويلية 2003، المتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية، العدد 44، الصادر بتاريخ: 23 يوليو 2009، المادة: 04.

تضمن الأمر 03-05 مجموعة من الأفعال الماسة بالمصنفات وبحقوق مؤلفيها وجرمها وجعل مرتكبيها يشكل خرقا لحقوق المؤلف، كما تضمن أيضا في مواده (154،152،151) على أنواع الجرائم المعلوماتية المتعلقة بحقوق المؤلف، وتجريم هذه الأفعال الغير المشروعة الواردة في المواد (156،153،157،158،159).[1]

سابعا: حماية البيانات الشخصية في القانون رقم 09-04 الخاص بقواعد الوقاية من الجرائم المصلة بتكنولوجيات الإعلام والاتصال ومكافحتها: من خلال هذا القانون قام المشرع الجزائري بوضع قواعد إجرائية جديدة يتضمن تحكما جيدا في أساليب مكافحة هذا النوع من الإجرام، كما استحدث القانون 09-04 آليات للتصدي للجرائم المعلوماتية هي: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ومكافحته، إذ تضمن القانون سالف الذكر قواعد إنشائها و اختصاصاتها [2] كما تم توسيع الاختصاص الإقليمي للسلطة القضائية في مجال متابعة الجرائم حيث وردت المادة 15 من القانون 04-09 "زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية تختص المحاكم الجزائية بالنظر في الجرائم المتعلقة بتكنولوجيات الإعلام و الاتصال المرتكبة خارج الإقليم الوطني عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية الاقتصاد الوطني."[3]

ثامنا: حماية البيانات الشخصية في القانون 15-04 المحدد للقواعد العامة للتوقيع والتصديق الالكتروني: في إطار حماية البيانات الشخصية أوجب القانون 15-04 في المادة 42: يجب على مؤدي خدمات التصديق الالكتروني الحفاظ على سرية البيانات والمعلومات المتعلقة بشهادات التصديق الالكتروني المسموحة "[4] للحفاظ على سرية البيانات و المعلومات كما حضر المشرع الجزائري بموجب المادة 4 جمع البيانات للمعني إلا بعد الموافقة الصريحة، كما يجب على مؤدي خدمات التصديق الالكتروني أن يجمع إلا البيانات الشخصية الضرورية لمنح وحفظ شهادة التصديق الالكتروني ولا يمكن استعمال هذه البيانات

---

[1] الجمهورية الجزائرية الديمقراطية الشعبية، الامر 03-05، مرجع سابق، من المادة:(151) إلى المادة: (154)،

[2] سامية ساعد، "حماية البيانات الشخصية المستهلك من مخاطر الدفع الالكتروني"، **مجلة الحقوق والعلوم الإنسانية**، م 15، ع 01، (2022)، ص. 1405.

[3] الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 09-04، المؤرخ في 14 شعبان 1430 الموافق لـ 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادر بتاريخ 16 أوت 2009، المادة 15.

[4] الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 15-04، المؤرخ في 11 ربيع الثاني 1436 الموافق لـ 1 فيفري 2015، المتضمن القواعد العامة المتعلقة بالتوقيع والتصديق الالكتروني، الجريدة الرسمية، العدد 06، الصادر بتاريخ فيفري 2015، المادة: 42.

لأغراض أخرى[1] هذا ما يؤكد أن المشرع الجزائري ألزم على مؤدي خدمات التصديق الالكتروني بألا يتجاوز في جمعه للبيانات و إنما يكتفي بجمع البيانات الضرورية فقط لمنح و حفظ شهادات التصديق الالكتروني و ألا يستغلها لأغراض غير التي جمعت لأجلها .

تاسعا: حماية البيانات الشخصية في القانون 18-05: المتعلق بالتجارة الإلكترونية: حرص المشرع الجزائري على حماية المعلومات والمعطيات ذات الطابع الشخصي في القانون رقم 18-05 بموجب المادة 26:" ينبغي للمورد الالكتروني الذي يقوم بجمع المعطيات ذات الطابع الشخصي ويشكل ملفات الزبائن والزبائن المحتملين، ألا يجمع إلا البيانات الضرورية لإبرام المعاملات التجارية، كما يجب عليه: الحصول على موافقة المستهلكين الإلكترونيين قبل جمع البيانات، ضمان أمن نظم المعلومات وسرية البيانات، الالتزام بالأحكام القانونية والتنظيمية المعمول بها في هذا المجال."[2]

من خلال استقراء المادة 26 يتضح أن المشرع الجزائري بسط حماية البيانات الشخصية من خلال إجبار المورد بجمع البيانات الضرورية فقط للزبائن أو المستهلكين، وأن يلتزم بسرية هذه البيانات الشخصية.

عاشرا: حماية البيانات الشخصية في القانون 18-04 المتعلق بالقواعد العامة للبريد والاتصالات الالكترونية: حدد المشرع الجزائري بموجب القانون 18-04 في المادة 97 مجموعة من الشروط اللازم احترامها بخصوص إنشاء واستغلال شبكات الاتصالات الإلكترونية المفتوحة للجمهور وتقديم خدمات الاتصالات الالكترونية ومن بين هذه الشروط: "شروط خصوصية البيانات والمعلومات التي تم إيصالها بواسطة شبكة الاتصالات الالكترونية، شروط حماية الحياة الخاصة للمشتركين والبيانات ذات الطابع الشخصي."[3]

حادي عشر: حماية البيانات الشخصية في القانون رقم 18-07 الخاص بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي: كرس المشرع الجزائري بموجب القانون رقم 18-07 حماية الحياة الخاصة للأفراد وذلك بنصه المادة (02):"يجب أن تتم معالجة المعطيات ذات الطابع الشخصي، مهما كان مصدرها وشكلها، في إطار احترام الكرامة الإنسانية والحياة الخاصة والحريات العامة

---

[1] الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 15-04، مرجع سابق، المادة: 43.

[2] الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 18-05، المؤرخ في 24 شعبان عام 1439 الموافق لـ 10ماي سنة 2018، المتضمن قانون التجارة الإلكترونية، الجريدة الرسمية، العدد 28، الصادرة في: 16 ماي 2018، المادة: 26.

[3] الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 18-04، المؤرخ في 24 شعبان 1439 الموافق لـ 10 ماي 2018، المتعلق بالقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، الجريدة الرسمية، العدد 27، الصادرة بتاريخ 13 ماي 2018، المادة 97.

وألا تمس بحقوق الأشخاص وشرفهم وسمعتهم."[1] كما حدد القانون سالف الذكر نطاق معالجة البيانات الشخصية في المادة (04)وحدد أيضا المبادئ الأساسية لحماية المعطيات ذات الطابع الشخصي من بينها ضرورة إيداع الموافقة الصريحة للشخص المعني من أجل السماح بمعالجة معطياته الشخصية ، وله الحق في التراجع عن موافقة في أي وقت وذلك في المادة 17،استحدث القانون رقم 18-07 آلية لحماية المعطيات الشخصية للأفراد الطبيعيين في الباب الثالث المتمثلة في السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي حيث حدد القانون تشكيلة السلطة و مهامها في نطاق حماية المعطيات ذات الطابع الشخصي كما منحت المواد: من (32) إلى (37) للشخص المعني حقوق في مجال حماية المعطيات ذات الطابع الشخصي من بينها: الحق في الإعلام، الحق في الولوج ، الحق في الاعتراض، الحق في التصحيح، منع الاستكشاف المباشر[2] في المقابل حدد القانون المتعلق بحماية المعطيات ذات الطابع الشخصي مجموعة من الالتزامات التي يتقيد بها المسؤول من أجل حماية وتأمين المعطيات ذات الطابع الشخصي، من بينها الحفاظ على السر المهني وذلك في المادة (40) و (38) و(39).

المطلب الثالث: الآليات المؤسساتية الدولية والإقليمية لحماية البيانات الشخصية.

كرست معظم الاتفاقيات الدولية العالمية أو الإقليمية جملة من الأجهزة والآليات المؤسسية التي تعني بحماية الخصوصية والبيانات الشخصية، بالإضافة إلى المؤسسات ومختلف الأجهزة التي تعتني بالتنسيق بين الدول في سبيل توقيف المجرمين السيبرانيين الذي يتجاوزون حدود الدول في مجال الجرائم الإلكترونية الماسة بأمن البيانات.

أولا: اللجنة أوروبية لحقوق الإنسان: هي آلية من آليات الأوروبية لحماية الحقوق والحريات أنشئت بموجب المادة 19 من الاتفاقية الأوروبية لحقوق الإنسان: "لضمان احترام الالتزامات التي تعهدت بها الأطراف السامية المتعاقدة في هذه المعاهدة تنشأ لجنة أوروبية لحقوق الإنسان تشار إليها باسم "اللجنة"، [3]إذ تعتبر اللجنة الأوروبية لحقوق الإنسان من بين الأجهزة التي كرستها الاتفاقية الأوروبية لحقوق الإنسان لضمان تنفيذ بنودها في مجال حماية الحقوق والحريات. [4]

---

[1] الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 18-07، المؤرخ في: 25 رمضان 1439 الموافق لـ 10 يونيو 2018، المتعلق بحماية الأشخاص الطبعيين في معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية، العدد 34، الصادر بتاريخ: 10 يونيو 2018، المادة: 02.

[2]الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 18-07، مرجع سابق، من المادة: 32 إلى المادة: 37، ص. 19.

[3]ستراسبورغ، المحكمة الأوروبية لحقوق الانسان، **الاتفاقية الأوروبية لحقوق الانسان**، (04 نوفمبر 1950)، المادة: 19، ص. 10.

[4]كحلاوي عبد الهادي، مرجع سابق، ص. 165.

ثانيا: المحكمة الأوروبية لحقوق الإنسان: أنشئت بموجب الفقرة 2 من المادة 19 من الاتفاقية الأوروبية لحقوق الإنسان" لضمان احترام الالتزامات التي تعهدت بها الأطراف السامية المتعاقدة في هذه المعاهدة تنشأ: محكمة أوروبية لحقوق الإنسان يشار إليها باسم "المحكمة"[1] إذ تعني هذه المؤسسة القضائية بالسهر على تطبيق أحكام الاتفاقية من خلال مراقبة آليات تطبيق الاتفاقية الأوروبية لحماية الحقوق والحريات الأساسية والتي من بينها الحق في حماية الحياة الخاصة.[2]

ثالثا: لجنة الوزراء لمجلس أوروبا :أنشئت بموجب المادة 10 من اتفاقية مجلس أوروبا حيث وردت في الاتفاقية تشكيلة اللجنة، إذ تضم وزراء الخارجية الدول الأعضاء أو من ينول عنه إذا تعذر أحد وزراء خارجية الدول الأعضاء الحضور، وذلك حسب المادة 14 من الميثاق، وهذا ما يجعل اللجنة الوزراء تتمتع بدور مزدوج من حيث إصدار القرارات والتنفيذ، وفي مجال حماية البيانات الشخصية تبنت اتفاقية حماية الأفراد في 1981 [3]وأصبحت ملزمة للدول الأعضاء ابتداء من تاريخ 1985/10/10 هذا ما يؤكد أن الآليات التي أقرتها المنظمات الدولية بسطت جانبا مهما من حماية البيانات الشخصية.[4]

رابعا: المحكمة العربية لحقوق الإنسان: تأست المحكمة العربية لحقوق الإنسان بموجب قرار مجلس جامعة الدول العربية في 2013/03/26 تختص المحكمة حسب المادة 16 من القانون الأساسي للمحكمة العربية لحقوق الإنسان:" بكافة الدعاوي والنزاعات الناشئة عن تفسير الميثاق العربي لحقوق الإنسان أو أي اتفاقية عربية في مجال حقوق الإنسان تكون الدول المتنازعة طرفا فيها، تفصل المحكمة في أي نزاع يثار حول اختصاصها بنظر الدعاوي والطلبات أو الحالات التي تنظرها."[5]

خامسا: اللجنة الإفريقية لحقوق الإنسان والشعوب: هو جهاز انبثق من الميثاق الإفريقي لحقوق الإنسان والشعوب، إذ يعد هذا الجهاز من الآليات الجهوية لتفعيل حقوق، إذ تتمثل مهمتها الأساسية في ضمان تعزيز وحماية الحقوق المبنية في الميثاق الإفريقي لحقوق الإنسان والشعوب، إذ نصت المادة 45 على اختصاصات اللجنة الإفريقية لحقوق الإنسان والشعوب، إذ تختص اللجنة لتلقي الشكاوى من الدول الأعضاء والأفراد بشأن قضايا انتهاك حقوق الإنسان المنصوص عليها في الميثاق.[6]

---

[1] ستراسبورغ، المحكمة الأوروبية لحقوق الانسان، مرجع سابق، المادة 19. ص. 10.

[2] شمس الدين معنصري، **الآليات الأوروبية لحماية حقوق الإنسان والعلوم السياسية**، مذكرة ماجستير غير منشورة، (جامعة محمد خيضر: كلية الحقوق،2011/2010)، ص.117.

[3] شمس الدين معنصري، مرجع سابق، ص. 14.

[4] كحلاوي عبد الهادي، مرجع سابق، ص. 170.

[5] القاهرة، جامعة الدول العربية، **القانون الأساسي للمحكمة العربية لحقوق الإنسان**، (07. 09. 2014)، المادة: 16. ص 22.

[6] علي أبو هاني، الأطرش كريفف،"النظام الإفريقي لحقوق الإنسان ودوره في تعزيز وحماية حقوق الإنسان، وحرياته الأساسية"، **المجلة العربية للأبحاث والدراسات في العلم الانسانية والاجتماعية**، م 13، ع 05، (أكتوبر 2021)، ص. 292.

سادسا: المحكمة الإفريقية لحقوق الإنسان والشعوب: جاء في نص البروتوكول المحلق بالميثاق الوطني لحقوق الإنسان والشعوب في مادته الأولى على أنه: تنشأ محكمة افريقية لحقوق الإنسان والشعوب "المحكمة" بحكم اختصاصها ومهمتها هذا البروتوكول، إذ أن المحكمة الإفريقية لحقوق الإنسان لا تشكل بديلا عن اللجنة بل جاءت لتكمل مهام هذه اللجنة في التكفل بقضايا حقوق الإنسان. [1]

إضافة إلى المؤسسات سابقة الذكر والمنبثقة من الاتفاقيات الأولية هناك أجهزة تقوم بالتنسيق مع مختلف الدول وتتولى مهمة ضبط وتوقيف المجرمين السيبرانيين الذين يتواجدون خارج حدود الدول، تتمثل هذه الأجهزة في:

سابعا: المنظمة الدولية للشرطة الجنائية 'الأنتربول: تعد المهمة الأساسية للإنتربول هي مساعدة أجهزة الشرطة في جميع الدول الأعضاء من أجل الوصول الأمن من خلال تبادل البيانات المتعلقة بالجرائم والمجرمين والوصول إليها و تقديم الدعم الفني و الميداني بمختلف أشكاله، إذ حدد القانون الأساسي لمنظمة الأنتربول جملة من الاختصاصات التي تقوم بها الأنتربول: جمع وتبادل المعلومات والبيانات المتعلقة بالجريمة والمجرم، مكافحة جرائم القانون العام: مثل الجريمة السيبرانية، الاتجار بالبشر، الجريمة المنظمة وغيرها، حماية الأمن الدولي: تنسيق الجهود بين الدول الأعضاء خاصة فيما يتعلق بهروب المجرمين. [2]

ثامنا: مركز الشرطة الأوروبية (اليوروبول): أسست في عام 1999 كوكالة تابعة للاتحاد الأوروبي واعتمد مقرها لاهاي يهدف هذا الجهاز إلى مكافحة مجموعة واسعة من الجرائم بما في ذلك الإرهاب، تهريب المخدرات، وكذلك الجرام السيبرانية، كما يقوم اليوروبول بالتنسيق والتعاون بين أجهزة الشرطة في مختلف الدول الأعضاء بالاتحاد الأوروبي للمساهمة في تحقيق الأمن والاستقرار لأوروبا. [3]

تاسعا: منظمة الشرطة الجنائية الإفريقية (الآفريبول):هي هيئة تقنية لدى الاتحاد الإفريقي، مقرها الرئيسي في الجزائر العاصمة، لم يتطرق النظام الأساسي للآفريبول إلى تعريفها واكتفى بتسميتها من خلال المادة الأولى بالنص على أن الآفريبول آلية الاتحاد الإفريقي للتعاون الشرطي، [4] يسعى الآفريبول حسب المادتين (03، 04) من النظام الأساسي لآلية الاتحاد الإفريقي للتعاون الشرطي 'الأفريبول" إلى:

---

[1] علي أبو هاني، الأطرش كريفف، مرجع سابق، ص. 296.

[2] أسامة غربي، "المنظمة الدولية للشرطة الجنائية (الإنتربول) ودورها في مكافحة الجريمة المنظمة"، **المجلة دراسات و أبحاث**، ع 3، (مارس 2011)، ص. 159.

[3] محمد نذير بن عرفه، يوسف حوري، "اليوروبول كآلية لمكافحة الجريمة الالكترونية"، **مجلة الدراسات القانونية والسياسية**، م 11، ع 01،(جانفي 2025)، ص.37.

[4] عبد العزيز لزعر، رشيد زياني، "آليات الاتحاد الإفريقي للتعاون الشرطي (الافريبول) ودورها في مكافحة الجريمة الالكترونية"، **مجلة متون**، م 14، ع 03، (سبتمبر 2021)، ص. 254.

مساعدة مؤسسات الشرطة في الدول الأعضاء على وضع إطار للتعاون بين مؤسسات الشرطة على المستويات الوطنية والإقليمية والقارية والدولية، العمل على تطوير قدرات أجهزة الشرطة في الدول الأعضاء، تشجيع المساعدة الفنية المتبادلة ذات الخبرة العالية والممارسات الجيدة بين مؤسسات الشرطة لتحسين كفاءتها وفاعليتها وتسهيل المساعدة القانونية المتبادلة بالأخص تسليم المجرمين.[1]

المطلب الرابع: المقاييس الدولية للأمن السيبراني (ISO- 2700):

هي سلسلة من المعايير تم نشرها في2009من قبل المنظمة الدولية للمعايير (ISO) واللجنة الكهرو-الكترونية الدولية (*IEC*)،[2]تحدد هذه المعايير الممارسات الجيدة في إدارة امن المعلومات، يغطي جوانب متنوعة مثلا السرية والنزاهة وتوافر المعلومات وذلك لتمكين الشركات من إدارة بياناتها الحساسة بفعالية، إذ ينطبق هذا المعيار على جميع المنظمات، بغض النظر عن الحجم والقطاع، ويوفر نهجا لتحديد المخاطر الأمنية وتقيمها والتخفيف منها.[3]

تتضمن عائلة الـ(ISO-27000) العديد من المعايير التكميلية منها:

- **معيار(ISO-27001):** يعد هذا المعيار الأكثر شهرة في عائلة الـ(ISO-27000)، يحدد هذا المعيار لتنفيذ وإدارة نظام امن المعلومات، يوفر هذا المعيار مجموعة من الإرشادات للشركات من جميع الأحجام وفي جميع القطاعات لإنشاء نظام إدارة امن المعلومات وتنفيذه وصيانته وتحسينه بشكل مستمر، والامتثال لهذا المعيار يعني أن المنظمة او المؤسسة قد نفذت نظام لإدارة المخاطر الأمنية لبياناتها أو البيانات التي تعالجها، وأن هذا النظام يتوافق مع أفضل الممارسات والمبادئ المنصوص عليها في هذا المعيار الدولي.[4]
- **معيار(ISO-27002): هو** معيار دولي يوفر إرشادات للمؤسسات التي تسعى إلى إنشاء وتنفيذ وتحسين نظام إدارة أمن المعلومات الذي يركز على الأمن السيبراني، يحدد هذا المعيار أفضل الممارسات وأهداف التحكم المتعلقة بالجوانب الرئيسية للأمن السيبراني، بما في ذلك التحكم في الوصول، والتشفير، أمن

---

[1] خضرة شنتير، **الآليات القانونية لمكافحة الجريمة الالكترونية، دراسة مقارنة**، أطروحة دكتوراه غير منشورة، (جامعة أحمد دراية، أدرار: كلية الحقوق والعلوم السياسية، 2021/2020)، ص.245.

[2] *Lamia El Fachtali, **Normes ISO 27000**, dans: https://fr.scribd.com/document/30445143/normes-ISO-27000, (7/4/2025).*

[3] *Iso 27000 comprendre et maîtriser les normes pour une sécurité de l'information optimale, dans: Https://www.makeitsafe.fr/Iso,(7/4/2025).*

[4] *Iso/IEC27001 :2022, dans: https//: www.iso.org/fr/standard/27001lifecycle,(7/4/2025)* .

الموارد البشرية والاستجابة للحوادث، توفر هذه المعايير نموذجا مرجعيا عمليا للمؤسسات التي ترغب في حماية بياناتها بشكل فعال ضد التهديدات الالكترونية.[1]

- **المعيار (ISO-27003):** هو معيار يوفر إرشادات لتنفيذ نظام إدارة امن المعلومات، بحيث يركز هذا المعيار على كيفية تنفيذ هذا النظام ويقدم نهج لإنشاء إطار عمل قوي لإدارة امن المعلومات.[2]
- **المعيار (ISO-27004):** يقدم هذا المعيار مساعدة للمؤسسات لقياس فعالية أنظمة إدارة امن المعلومات الخاصة بها وتحسينها بشكل منهجي.
- **المعيار (ISO-27005):** يحدد هذا المعيار كيفية تنفيذ إدارة المخاطر لأنظمة إدارة المعلومات، مع التركيز على كيفية وضع المنهجية التي سيتم استخدامها.
- **المعيار (ISO-27010):** يحدد هذا المعيار كيفية التعامل مع المعلومات عند مشاركتها بين شركات متعددة والمخاطر التي قد تنشا منها.
- **المعيار (ISO-27015):** توفر مبادئ لتطبيق نظام إدارة المعلومات داخل الشركات التي تقدم خدمات مالية مثل: الخدمات المصرفية الإلكترونية.[3]
- **المعيار (ISO-27035):** يغطي هذا المعيار إدارة حوادث امن المعلومات بما في ذلك خطة الاستجابة للحوادث الأمنية الخاصة بالمؤسسة.[4]

---

(1) *ISO/IEC 27002 :2022, dans:https://www.iso.org/fr/standard/75652Html , (07/04/2025).*

(2) *Iso 27003: **guide pratique pour mettre en œuvre un SMSI efficace** dans:https://www.makeitsafe.fr/Iso-27003-guide-pratiques,(7/4/2025).*

(3) *Iso 27000 et l'ensemble de normes de sécurité de l'information, dans:https://www.globalsui.com/fr/iso-27000-et-l-ensemble-de-normes-de-sécurité-de-l'information , (7/4/2025).*

(4) *Série ISO 27000**: Quels sont les standards +leur but**, dans : https://www.iso.org/fr/standard/75652.html , (7/4/2025.*

خلاصة الفصل الأول:

في هذا الفصل تطرقنا إلى الأسس النظرية للأمن السيبراني والبيانات الشخصية، حيث قمنا في المبحث الأول بتحديد مفهوم الأمن السيبراني والمفاهيم المرتبطة به والفصل بينهما، وذكر أهدافه وخصائصه وأبعاده، لننتقل بعدها إلى المبحث الثاني الذي يتمحور حول الإطار المفاهيمي للبيانات الشخصية، حيث قمنا بذكر المفاهيم المتعلقة بالبيانات الشخصية و أنواعها، ثم بعد ذلك تناول مختلف التهديدات السيبرانية التي تمس بأمنها مع ذكر المخاطر التي ترتب عنها، وفي مرحلة لاحقة من الدراسة تناولنا المبحث الثالث المتعلق بالآليات الإستراتيجية للآمن السيبراني إذ تم التركيز في هذا المبحث حول الآليات القانونية الدولية و الوطنية لحماية البيانات الشخصية كما تم تدعيم هذا المبحث باليات مؤسساتية دولية توفر الحماية للبيانات الشخصية، و في النهاية عرضنا المعايير القياسية للأمن السيبراني في سياق حماية البينات الشخصية.

الفصل الثاني:

الإستراتيجية الوطنية لحماية البيانات الشخصية في الجزائر

تمهيد:

أصبحت حماية البيانات الشخصية من بين أولويات الدول في ظل العصر الحالي لما تحمله من أهمية في صون حقوق الأفراد، وفي هذا السياق بادرت الجزائر إلى وضع إستراتيجية وطنية شاملة تركز فيها: على البعد المؤسساتي كوسيلة مهمة لتنفيذ أحكام القوانين والتشريعات، البعد القانوني بوصفه الإطار المنظم والضابط الذي ينظم حماية البيانات الشخصية، البعد التقني الذي يعتبر حجر الأساس في حماية البيانات الشخصية، وقدم تم التركيز في هذا الفصل.

انطلاقا مما سبق نهدف في هذا الفصل إلى التعرف على مرتكزات الإستراتيجية الوطنية لحماية البيانات الشخصية بما فيها البعد التقني والبعد المؤسساتي المتمثل في المؤسسات المشرفة عن حماية البيانات الشخصية، لا سيما تلك التي تنشط على مستوى القطاع البنكي باعتباره من أكثر القطاعات تعرضا للانتهاكات. وعليه تم تقسيم الفصل الثاني إلى ثلاث مباحث وفقا لما يلي:

المبحث الأول: المنظومة المؤسسية لحماية البيانات الشخصية في الجزائر.

المبحث الثاني: المؤسسات المشرفة على حماية البيانات الشخصية في البنوك التجارية.

المبحث الثالث: الآليات التقنية لحماية البيانات الشخصية.

المبحث الأول: المنظومة المؤسسة لحماية البيانات الشخصية في الجزائر

تولي الجزائر أهمية لمسألة حماية البيانات الشخصية ويظهر هذا الاهتمام من خلال إرساء مؤسسات وهيئات وطنية تضطلع من جهة بحماية البيانات الشخصية ومن جهة أخرى بمكافحة كافة أنواع الجرائم المعلوماتية التي تمس بأمن وسلامة البيانات الشخصية.

المطلب الأول: المنظومة المؤسسية الواقعة تحت وصاية رئاسية الجمهورية

تضم المنظومة المؤسسية الواقعة تحت وصاية رئاسة الجمهورية ثلاث مؤسسات تعني بحماية البيانات الشخصية وهي كما يلي:

1- السلطة الوطنية للتصديق الالكتروني:

أنشئت السلطة الوطنية للتصديق الالكتروني بموجب القانون 15-04 المتضمن للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين وهذا في نص المادة 16: " تنشأ لدى الوزير الأول سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي تسمى بالسلطة الوطنية للتصديق الالكتروني تدعى في صلب النص "السلطة" تسجل الاعتمادات المالية اللازمة لسير السلطة ضمن ميزانية الدولة ".[1] كما تضمن أحكام القانون 15-04 المهام التي تقوم بها السلطة الوطنية للتصديق الالكتروني ذلك في نص المادة 30 والتي تتمثل في: ترقية استعمال التوقيع والتصديق الالكترونيين وتطويرهما وضمان موثوقية استعمالهما، إعداد السياسة الوطنية للتصديق الالكتروني والسهر على تطبيقها بعد الحصول على الرأي الايجابي من قبل الهيئة المكلفة بالموافقة، الموافقة على سياسات التصديق الالكتروني الصادرة عن السلطتين الحكومية والاقتصادية للتصديق الالكتروني، إبرام إتفاقيات الاعتراف المتبادل على المستوى الدولي، اقتراح مشاريع تمهيدية لنصوص تشريعية أو تنظيمية تتعلق بالتوقيع الالكتروني أو التصديق الالكتروني على الوزير الأول، القيام بعمليات التدقيق على مستوى السلطتين الحكومية والاقتصادية للتصديق الالكتروني عن طريق الهيئة الحكومية المكلفة بالتدقيق، استشارة السلطة عند إعداد أي مشروع نص تشريعي أو تنظيمي ذي صلة بالتوقيع أو التصديق الالكترونيين.[2]كما تضمنت المادة 19 من القانون 15-04 كذلك تشكيلة السلطة الوطنية للتصديق الالكتروني: " تتشكل السلطة من مجلس و مصالح تقنية: يتشكل مجلس السلطة من خمسة أعضاء من بينهم الرئيس، يعينهم رئيس الجمهورية على

---

[1] الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 15-04، مرجع سابق، المادة 16.

[2] المرجع نفسه، المادة 30.

أساس كفاءتهم، لاسيما في مجال العلوم التقنية المتعلقة بتكنولوجيات الإعلام و الاتصال، و في مجال قانون تكنولوجيات الإعلام و الاتصال، و في اقتصاد تكنولوجيات الإعلام و الاتصال". [1]

2- السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي:

أنشئت السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي بموجب المادة 22 من القانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال حماية المعطيات ذات الطابع الشخصي: " تنشأ لدى رئيس الجمهورية، سلطة إدارية مستقلة لحماية المعطيات ذات الطابع الشخصي، يشار إليه أدناه "السلطة الوطنية" يحدد مقرها بالجزائر العاصمة، تتمتع السلطة الوطنية بالشخصية المعنوية والاستقلال المالي الإداري." [2]تتكون السلطة الوطنية حسب المادة 13 من قانون 18-07 من16 عضوا يتم تعيينهم بناءا على مرسوم رئاسي لعهدة مدتها 5 سنوات قابلة للتجديد منهم: ثلاث شخصيات من بينهم الرئيس، يختارهم رئيس الجمهورية من بين ذوي الاختصاص في مجال عمل السلطة الوطنية، ثلاث قضاة يقترحون من قبل المجلس الأعلى للقضاء من بين قضاة المحكمة العليا مجلس الدولة، عضو من كل غرفة من البرلمان يتم اختياره من قبل رئيس كل غرفة بعد التشاور مع رؤساء المجموعات البرلمانية، ممثل عن المجلس الوطني لحقوق الإنسان، ممثل عن وزير الدفاع الوطني، ممثل عن وزير الشؤون الخارجية، ممثل عن وزير المكلف بالداخلية، ممثل عن وزير العدل حافظ الأختام، ممثل عن الوزير المكلف بالبريد والمواصلات السلكية و اللاسلكية و التكنولوجيات والرقمنة، ممثل عن الوزير المكلف بالصحة، ممثل عن وزير العمل والتشغيل والضمان الاجتماعي، إضافة إلى ذلك يمكن للسلطة الوطنية أن تستعين بأي شخص مؤهل من شأنه مساعدتاه في أشغالها.[3] تضطلع السلطة الوطنية حسب المادة 25 بمجموعة من المهام في مجال حماية المعطيات ذات الطابع الشخصي: إعلام الأشخاص المعنيين والمسؤولين عن المعالجة بحقوقهم وواجباتهم، تقديم الاستشارات للأشخاص والكيانات التي تلجأ لمعالجة المعطيات ذات الطابع الشخصي أو التي تقوم بتجارب أو خبرات من طبيعتها إلى مثل هذه المعالجة،

تلقي الاحتجاجات والطعون والشكاوى بخصوص تنفيذ معالجة المعطيات ذات الطابع الشخصي وإعلام أصحابها بما لها، لترخيص بنقل المعطيات ذات الطابع الشخصي نحو الخارج وفقا للشروط المنصوص عليها في هذا القانون، الأمر بالتعديلات الضرورية لحماية المعطيات ذات الطابع الشخصي محل المعالجة، الأمر بإغلاق المعطيات محل المعالجة، أو سحبها أو إتلافها، نشر التراخيص الممنوعة والآراء

---

[1] الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 15-04، مرجع سابق، المادة 19.

[2] الجمهورية الجزائرية الديمقراطية الشعبية، القانون 18-07، مرجع سابق، المادة 22.

[3] المرجع نفسه، المادة 13.

المدلى بها في السجل الوطني المشار إليها في المادة 28 من هذا القانون، إصدار عقوبات إدارية في حق المسؤول عن المعالجة في حالة خرقه لأحكام هذا القانون، الإجراءات الإدارية الآتية : الإنذار، الأعذار، السحب المؤقت، الغرامة، وضع معايير في مجال المعطيات ذات الطابع الشخصي، وضع قواعد السلوك والأخلاقيات التي تخضع لها معالجة المعطيات ذات الطابع الشخصي، إعداد تقرير سنوي حول نشاطها يرفع إلى رئيس الجمهورية. [1]

1- المحافظة السامية للرقمنة:

هي مؤسسة عمومية ذات طابع خاص أنشئت بموجب المرسوم الرئاسي23-314، تتمتع بالشخصية المعنوية و الاستقلال المالي، توضع تحت وصاية رئاسة الجمهورية، [2] تكلف المحافظة السامية للرقمنة حسب المادة 4 من المرسوم الرئاسي 23-314 بتصميم الإستراتيجية الوطنية للرقمنة بالتشاور مع القطاعات المعنية و المؤسسات والقطاع الاقتصادي والمجتمع المدني، كما تكلف أيضا على توافق مخططات القطاعات المعنية في مجال الرقمنة مع الإستراتيجية الوطنية للرقمنة، لاقتراح كل تدبير من شأنه تعزيز السيادة الرقمية وتطوير المنتوج الوطني، اقتراح انجاز مشاريع بحث في مجال اختصاصها، ضمان توافق الإستراتيجية الوطنية للرقمنة مع متطلبات أمن الأنظمة المعلوماتية، باعتبارها أداة الدولة في هذا المجال، كما تضطلع المحافظة السامية للرقمنة بمهام أخرى من بينها: اقتراح الأدوات القانونية التنظيمية أو أي حل تقني لضمان الفعالية و التحسين المستمر لمحاور التحول الرقمي،[3] وفي سبيل حماية البيانات الشخصية أطلقت المحافظة النسخة الأولى للمرجع الوطني لحكومة البيانات الذي يهدف إلى وضع إطار تنظيمي واضح، يضمن التبادل الآمن والفعال للمعلومات بين القطاعات الوزارية و الهيئات العمومية، كما عملت الإستراتيجية الوطنية للتحول الرقمي على تعزيز الأمن الرقمي، إذ اعتبرت هذا الأخير هو جزء لا يتجزأ لنجاح الإستراتيجية الوطنية للتحول الرقمي التي تشمل حماية البيانات والأنظمة من التهديدات السيبرانية. [4]

يمكن اختصار ما سبق ذكره في الرسم التخطيطي التالي:

---

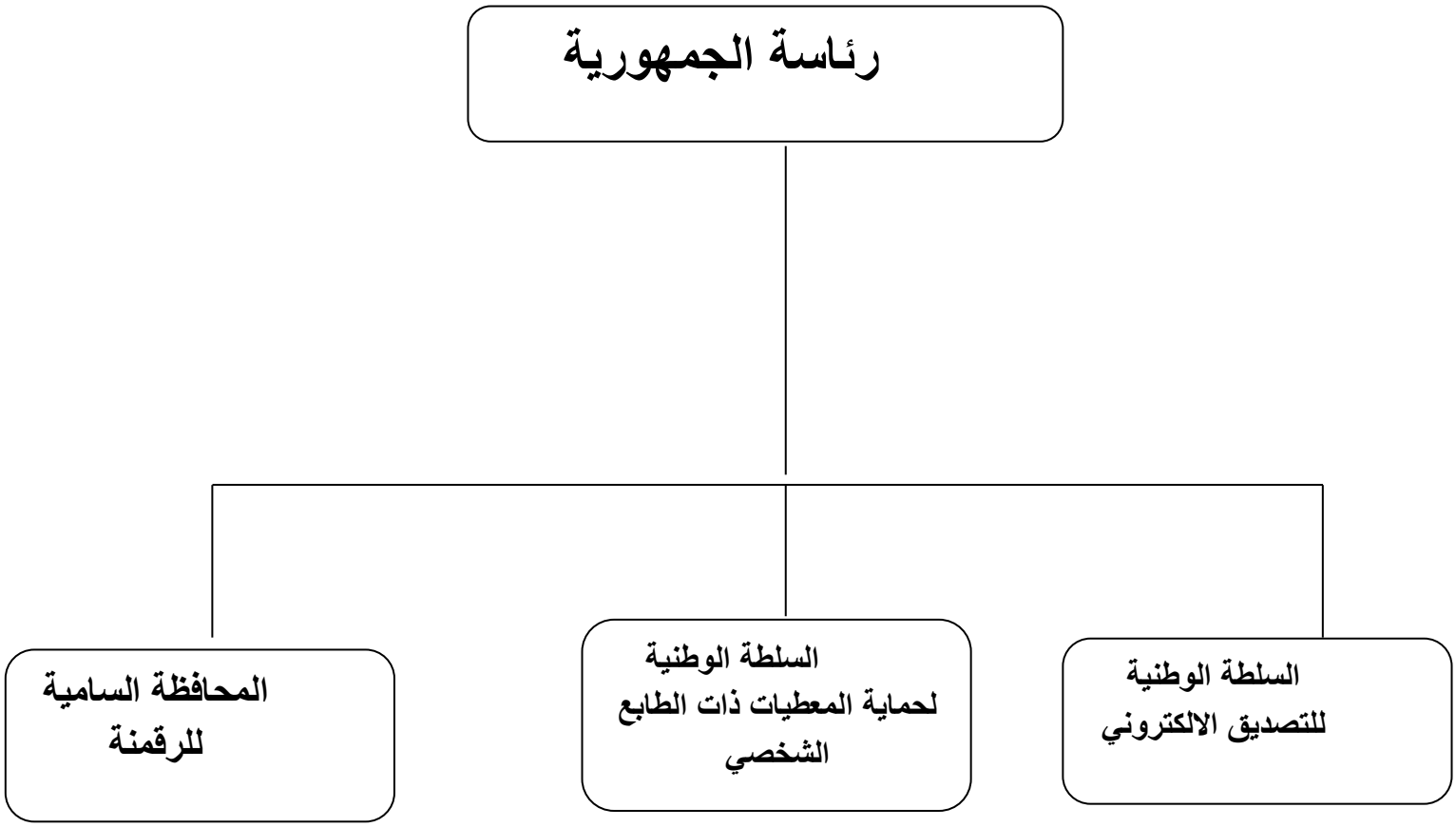
[1] الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 18-07، مرجع سابق، المادة 25.

[2] الجمهورية الجزائرية الديمقراطية الشعبية، المرسوم الرئاسي رقم 23-314، المؤرخ في 20 صفر 1445 الموافق ل 6 سبتمبر 2023، المتضمن إنشاء محافظة سامية للرقمنة وتحديد مهامها وتنظيمها وسيرها، الجريدة الرسمية، العدد 59، الصادر بتاريخ 10 سبتمبر 2023، المادة2.

[3] الجمهورية الجزائرية الديمقراطية الشعبية، المرسوم الرئاسي رقم 23-314، مرجع سابق، المادة 4.

[4] ياقوت زهرة القدس بن عبد الله، لحوكمة البيانات وتعزيز التشغيل البيني في: https://www.elbadilabc-ar.dz/gouveranace- (2025/05/21).

الشكل رقم (02) رسم تخطيطي يوضح المؤسسات الواقعة تحت رئاسة الجمهورية.



المصدر: المخطط من تصور الطالبة بناء على الهياكل المنصوص عليها في النصوص القانونية (القانون 15-04، 18-07، المرسوم الرئاسي23-314).

المطلب الثاني: المنظومة المؤسساتية التابعة لوزارة الدفاع الوطني

هنالك جملة من المؤسسات التابعة لوزارة الدفاع التي تتولى حماية البيانات الشخصية ومكافحة الجريمة المعلوماتية والتي تتمثل في:

1. الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها:

أنشئت الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بموجب المادة 13 من القانون 09-04 مؤرخ في 14 شعبان 1430 الموافق لـ5 أغسطس 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتمثلة بتكنولوجيات الإعلام والاتصال ومكافحتها،[1] تقوم الهيئة

(1) الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 09-04، المؤرخ في 14 شعبان 1430 الموافق لـ4 غشت سنة 2009، والمتضمن القواعد الخاصة للواية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادرة بتاريخ 16 غشت 2009، المادة 13.

الوطنية بمجموعة من المهام حددت في المادة 16: تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك جمع المعلومات وانجاز الخبرات القضائية، وعليه تتدخل الهيئة بطلب من الجهات القضائية المختصة. تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتمثلة بتكنولوجيات الإعلام والاتصال،[1] ولم يحدد القانون 09-04 تشكيلة الهيئة الوطنية بل اكتفى فقط بذكر المهام المنوط بها، حتى بعد صدور المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر 2015 الذي حدد تشكيلة وتنظيم وسير الهيئة الوطنية وذلك في المادة 6 من نفس المرسوم، بحيث تتشكل الهيئة من: لجنة مديرية، مديرية عامة، مديرية للرقابة الوقائية واليقظة الالكترونية، مديرية للتنسيق التقني، مركز العمليات التقنية، ملحقات جهوية، ويرأس اللجنة المديرية الوزير المكلف بالعدل وتتشكل من الأعضاء الآتي ذكرهم: الوزير المكلف بالداخلية، الوزير المكلف بالبريد وتكنولوجيات الإعلام والاتصال، قائد الدرك الوطني، ممثل عن رئاسة الجمهورية ممثل عن وزارة الدفاع الوطني قاضيان من المحكمة العليا يعينهما المجلس الأعلى للقضاء قائد الدرك الوطني، ممثل عن رئاسة الجمهورية ممثل عن وزارة الدفاع الوطني، قاضيان من المحكمة العليا يعينهما المجلس الأعلى للقضاء، [2] إضافة إلى المهام المسندة للهيئة الوطنية في القانون 09-04 أضاف المرسوم الرئاسي رقم 15-261 مهام أخرى تقوم بها الهيئة المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها من بينها: ضمان المراقبة الوقائية للاتصالات الالكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة، تحت سلطة القاضي المختص وباستثناء أي هيئات وطنية أخرى، تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية، السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها، تطوير التعاون مع المؤسسات الهيئات الوطنية المعنية بالجرائم المتمثلة بتكنولوجيات الإعلام والاتصال. المساهمة في تحديث المعايير القانونية في مجال اختصاصها، [3] ثم بعد صدور المرسوم الرئاسي رقم 19-172 الموافق لـ 6 يونيو 2019 الذي يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها

---

[1] الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 09-04، مرجع سابق، المادة 16.

[2] الجمهورية الجزائرية الديمقراطية الشعبية، المرسوم الرئاسي 15-261، المؤرخ في 24 ذي الحجة 1424 الموافق ل8 أكتوبر 2015، المتعلق ب تحديد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، الجريدة الرسمية، العدد 53، الصادر بتاريخ 8أكتوبر 2015، المادة 4.

[3] المرجع نفسه، المادة: 11.

كيفيات سيرها وضعت الهيئة الوطنية تحت سلطة وزير الدفاع بموجب المادة الثانية من المرسوم الرئاسي 19-172،كما أعاد هذا المرسوم تنظيم تشكيلة الهيئة الوطنية بموجب المادة 4 تنظم في: مجلس توجيه ومديرية عام و حيث يرأس مجلس التوجيه وزير الدفاع الوطني أو ممثله تتشكل من الوزارات الآتية : وزارة الدفاع الوطني، الوزارات المكلفة بالداخلية، وزارة العدل، الوزارة المكلفة بالمواصلات السلكية واللاسلكية.[1]

2. مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة:

هي تركيبة ملحقة بدائرة التحضير والاستعمال لأركان الجيش الشعبي والوطني استحدثت في 6 نوفمبر 2015 بقرار من القيادة العليا للجيش الشعبي الوطني على مستوى دائرة الاستعمال والتحضير لأركان الجيش الشعبي الوطني، تتمثل مهام مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة في: حماية وتأمين المنظومات والمنشآت الحيوية لقوات الجيش الشعبي الوطني ضد التهديدات السيبرانية تخطيط وإدراج ومتابعة حالة تقدم نشاطات تجسيد السياسة الشاملة للدفاع السيبراني الرامية لتحقيق بفعالية الحماية ضد التهديدات السيبرانية التي تستهدف أنظمة المعلومات ومنظومات الاتصال وكذا منظومات الأسلحة للجيش الوطني الشعبي، وضع وتطبيق السياسة العامة للدفاع السيبراني في الجيش الشعبي الوطني، تقييم وتعزيز مستوى أمن الأنظمة المستقلة وفي الصعيد العملياتي تتمثل مهام المصلحة في تعزيز قدرة الجيش الوطني الشعبي في مجال الدفاع السيبراني، تساهم هذه المصلحة مع الهيئات الوطنية المعنية في إعداد ووضع السياسة الوطنية المتعلقة بالدفاع السيبراني وضمان التنسيق مع مختلف الهيئات في مجال تأمين المنشآت الرقمية الحساسة. [2]

3. المركز الوطني للإشارة والحروب الإلكترونية:

أنشأت في 2019، هو مؤسسة تابعة لدائرة الإشارة وأنظمة المعلومات والحرب الإلكترونية، يعتبر المركز الوطني للإشارة حسب بيان وزارة الدفاع الوطني هو المكون الأساسي لمنظومة الإشارة للجيش الشعبي الوطني، بحيث يربط من خلال حوامل إشارة مؤمنة على أساس الألياف البصرية جميع مراكز الاتصالات وذلك تجسيدا لإستراتجية اكتساب مقياس التحكم الفعال في التكنولوجيات الحديثة وتوظيفها بإحكام في إضفاء الطابع المهني والمحترف. [3]

---

[1] الجمهورية الجزائرية الديمقراطية الشعبية، المرسوم الرئاسي رقم 19-172، المؤرخ في 3 شوال 1440 الموافق ل 6 يونيو 2019، المتعلق بتحديد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 37، الصادر بتاريخ: 9 يونيو 2019، المادة: 04.

[2] محمد بوكبشة، "الأمن والدفاع السيبراني أولوية قصوى"، **مجلة الجيش**، ع 651، (أكتوبر 2017)، ص35.

[3] قايد صالح الجيش يواصل مساره الوطني النير، في: https://www.elbilad.net/evenemen تاريخ الإطلاع (2025/5/6).

2- المنظومة الوطنية لأمن الأنظمة المعلوماتية:

تعتبر المنظومة الوطنية لأمن الأنظمة المعلوماتية أداة الدولة في مجال أمن الأنظمة المعلوماتية وتشكل الإطار التنظيمي لإعداد الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية وتنسيق تنفيذها، [1] أنشئت بموجب المرسوم الرئاسي 20-05 الصادر في 20 جانفي 2020، تشمل المنظومة الوطنية لأمن الأنظمة المعلوماتية الموضوعة لدى وزارة الدفاع الوطني:

أ- مجلس وطني لأمن الأنظمة المعلومات:

يترأس المجلس الوطني لأمن الأنظمة المعلوماتية وزير الدفاع الوطني أو ممثله و يتكون من: ممثل عن رئاسة الجمهورية، ممثل عن الوزير الأول، الوزير المكلف بالشؤون الخارجية، الوزير المكلف بالداخلية الوزير المكلف بالعدل، الوزير المكلف بالمالية، الوزير المكلف بالطاقة، الوزير المكلف بالاتصالات، الوزير المكلف بالتعليم العالي،[2] يكلف المجلس الوطني لأمن الأنظمة المعلوماتية بإعداد الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية، وفي إطار إعداد الإستراتيجية الوطنية في مجال الأنظمة المعلوماتية يقوم بالمهام التالية: البث في عناصر الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية المقترحة من قبل الوكالة وتحديدها، دراسة مخطط عمل الوكالة وتقرير نشاطها والموافقة عليهما، دراسة التقارير المتعلقة بتنفيذ الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية المقترحة من قبل الوكالة وتحديدها، دراسة مخطط عمل الوكالة و تقرير نشاطها والموافقة عليها، دراسة التقارير المتعلقة بتنفيذ الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية والموافقة عليها، الموافقة على اتفاقيات التعاون والاعتراف المتبادل مع الهيئات الأجنبية في مجال أمن الأنظمة المعلوماتية، الموافقة على سياسة التصديق الالكتروني للسلطة الوطنية للتصديق الالكتروني، الموافقة على تصنيف الأنظمة المعلوماتية، إبداء رأي المجلس بشأن أي مشروع نص تشريعي أو تنظيمي. [3]

ب. وكالة أمن الأنظمة المعلوماتية:

وهي مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية و الاستقلالية المالية، أنشئت بموجب المرسوم الرئاسي 20-05،[4] تتضمن وكالة أمن الأنظمة المعلوماتية لجنة توجيه و تزود بلجنة علمية، و تتكون لجنة التوجيه من ممثلي وزارات :وزارة الدفاع الوطني، الوزارة المكلفة بالشؤون الخارجية،

---

[1] الجمهورية الجزائرية الديمقراطية الشعبية، المرسوم الرئاسي 20-05، المؤرخ في 24 جمادى الأولى 1441 الموافق ل 20 جانفي 2020، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، الجريدة الرسمية، العدد 04، الصادر بتاريخ 26 جانفي2020، المادة 2.

[2] المرجع نفسه، المادة: 02، 03.

[3] المرجع نفسه، المادة: 04.

[4] المرجع نفسه، المادة: 17.

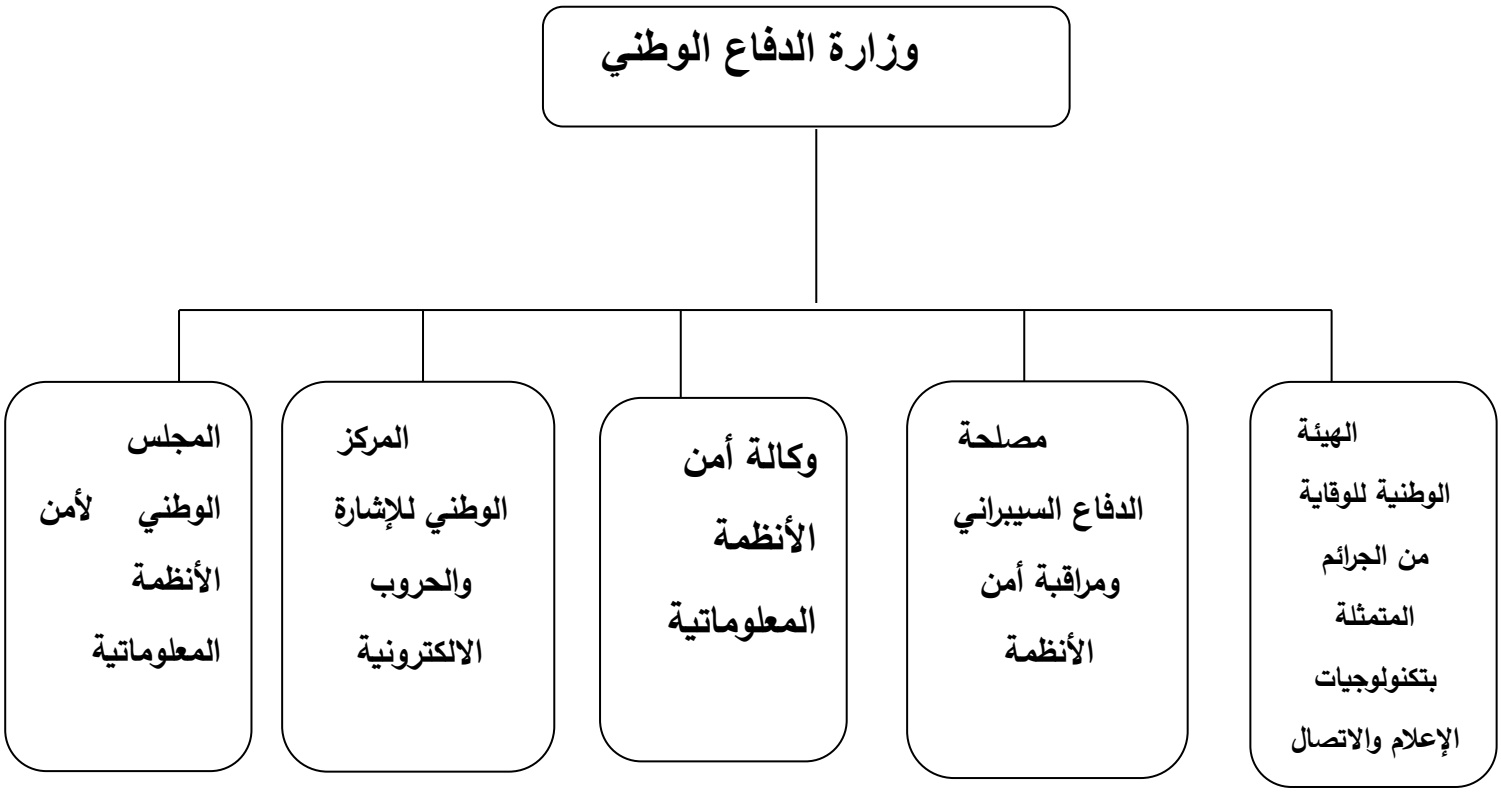
الوزارات المكلفة بالداخلية، الوزارات المكلفة بالعدل، الوزارة المكلفة بالمالية، الوزارة المكلفة بالطاقة، الوزارة المكلفة بالتعلم العالي، الوزارة المكلفة بالصناعة، الوزارة المكلفة بالاتصالات، الوزارة المكلفة بالتجارة، مصالح الأمن، سلطة ضبط البريد و الاتصالات الالكترونية، السلطة الوطنية للتصديق الالكتروني، السلطة الوطنية لحماية البيانات ذات الطابع الشخصي، السلطة الحكومية للتصديق الالكتروني،[1] تكلف وكالة أمن الأنظمة المعلوماتية بالمهام من بينها: تحضير عناصر الإستراتيجية الوطنية في مجال أمن الأنظمة المعلوماتية المحددة من قبل المجلس، تنسيق تنفيذ الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية من قبل المجلس، إجراء تحقيقات رقمية في حالة الهجمات أو الحوادث السيبرانية التي تستهدف المؤسسات الوطنية، المنشورة والمساعدة للإدارات والمؤسسات والهيئات العمومية والخاصة من أجل وضع استراتيجية أمن الأنظمة المعلوماتية، إضافة إلى مهام أخرى تقوم بها وكالة أمن الأنظمة المعلوماتية حددتها المادة 17 من المرسوم الرئاسي 20-05. [2]

ولتلخيص ما سبق ذكره يبين المرسم التخطيطي التالي مختلف المؤسسات التابعة لوزارة الدفاع الوطني.

[1] الجمهورية الجزائرية الديمقراطية الشعبية، المرسوم الرئاسي 20-05، مرجع سابق، المادة 22.

[2] المرجع نفسه، المادة 18.

الشكل رقم (03): رسم تخطيطي يوضح المؤسسات التابعة لوزارة الدفاع الوطني.



المصدر: المخطط من تصور الطالبة بناء على الهياكل المنصوص عليها في النصوص القانونية.(القانون 09-04، المرسوم الرئاسي 20-05.).

2. الوحدات التابعة للدرك الوطني.

في إطار مكافحة الجريمة بكل أنواعها بما فيها الجرائم المعلوماتية التي تمس بأمن وسلامة البيانات، وضعت قيادة الدرك الوطني وحدات متنوعة وعديدة تتوزع على 3 مستويات.

أ. **على المستوى المركزي:** تضم مصالح الدرك الوطني مجموعة من الأجهزة المركزية التي تعمل على مكافحة الجريمة المعلوماتية التالية: [1]

- **المصلحة المركزية للتحريات الجنائية:** أنشأتها القيادة العامة للدرك الوطني في 2008، تقوم المصلحة المركزية للتحريات الجنائية بـ: التنسيق الوطني حول التحقيقات في القضايا الكبرى الخاصة بالجريمة

[1] حسين ربيعي، **اليات البحث والتحري في الجرائم المعلوماتية**، أطروحة دوكتراه غير منشورة، (جامعة باتنة، كلية الحقوق والعلوم السياسية، 2016/2015.) ص183.

المنظمة على غرار تبييض الأموال، التهريب وغيرها كذلك تقوم بالتحري في الجرائم التي لها امتداد عبر التراب الوطني وحتى خارج الجزائر، كما تقوم هذه المصلحة إلى جانب المعهد الوطني للأدلة الجنائية بتنسيق عمل فرق التحري عبر التراب الوطني مع المؤسسات والهيئات التي لها علاقة بقضايا الإجرام الكبيرة.[1]

❖ **المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني:**

أنشئ بموجب المرسوم الرئاسي 04-183 المتعلق بإحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني، وهو حسب المادة من نفس المرسوم، مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلال المالي، يوضع هذا المعهد تحت وصاية وزارة الدفاع الوطني، ويمارس قائد الدرك الوطني سلطات الوصاية بتفويض منه،[2] يقوم المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني حسب المادة 4 من المرسوم الرئاسي رقم 04-183 بمجموعة من المهام: إجراء الخبرات والفحوص العلمية بناء على طلب من القضاة والمحققين والسلطات المؤهلة بغرض إقامة الأدلة التي تسمح بالتعرف على مرتكبي الجناية والجنح، تقديم مساعدة علمية أثناء القيام بالتحريات المعقدة باستخدام مناهج الشرطة العلمية والتقنية، المشاركة في الدراسات و التحاليل المتعلقة بالوقاية والتقليل من كل أشكال الإجرام، تصميم بنوك معطيات وانجازها طبقا للقانون، بما في ذلك تلك الخاصة بالبصمات البينية التي ستكون في تناول المحققين.[3]

❖ **مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها للدرك الوطني:**

هو هيئة تقنية تعمل تحت وصاية مديرية الأمن العمومي والاستعمال لقيادة الدرك الوطني، يقوم مركز الوقاية بمجموعة من المهام، ضمان المراقبة الدائمة والمستمرة على شبكة الانترنيت، القيام بمراقبة الاتصالات الالكترونية بما يسمح به القانون لفائدة وحدات الدرك الوطني والقضائية، مساعدة الوحدات الإقليمية للدرك الوطني في معاينة الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال والبحث عن الأدلة في شبكة الانترنيت، المشاركة في عمليات التحري و التسرب عبر شبكة الانترنيت لفائدة وحدات الدرك الوطني والسلطات القضائية، المشاركة في قمع الجرائم المعلوماتية من خلال التعاون مع مختلف مصالح الأمن والهيئات الوطنية، تنفيذ إجراءات البحث والتحقيق بشأن الجرائم المعلوماتية.

---

[1] مصلحة مركزية للتحريات الجنائية لمحاربة الجريمة بالدرك الوطني، في: https://www.echoroukonline.com، تاريخ الإطلاع: (2025/5/6).

[2] الجمهورية الجزائرية الديمقراطية الشعبية، المرسوم الرئاسي 04-183 المؤرخ في 8 جمادى الأولى 1425 الموافق لـ 26 يونيو 2004، المتعلق بإحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، الجريدة الرسمية، العدد 41، الصادر بتاريخ 27 يونيو 2004، المادة 18.

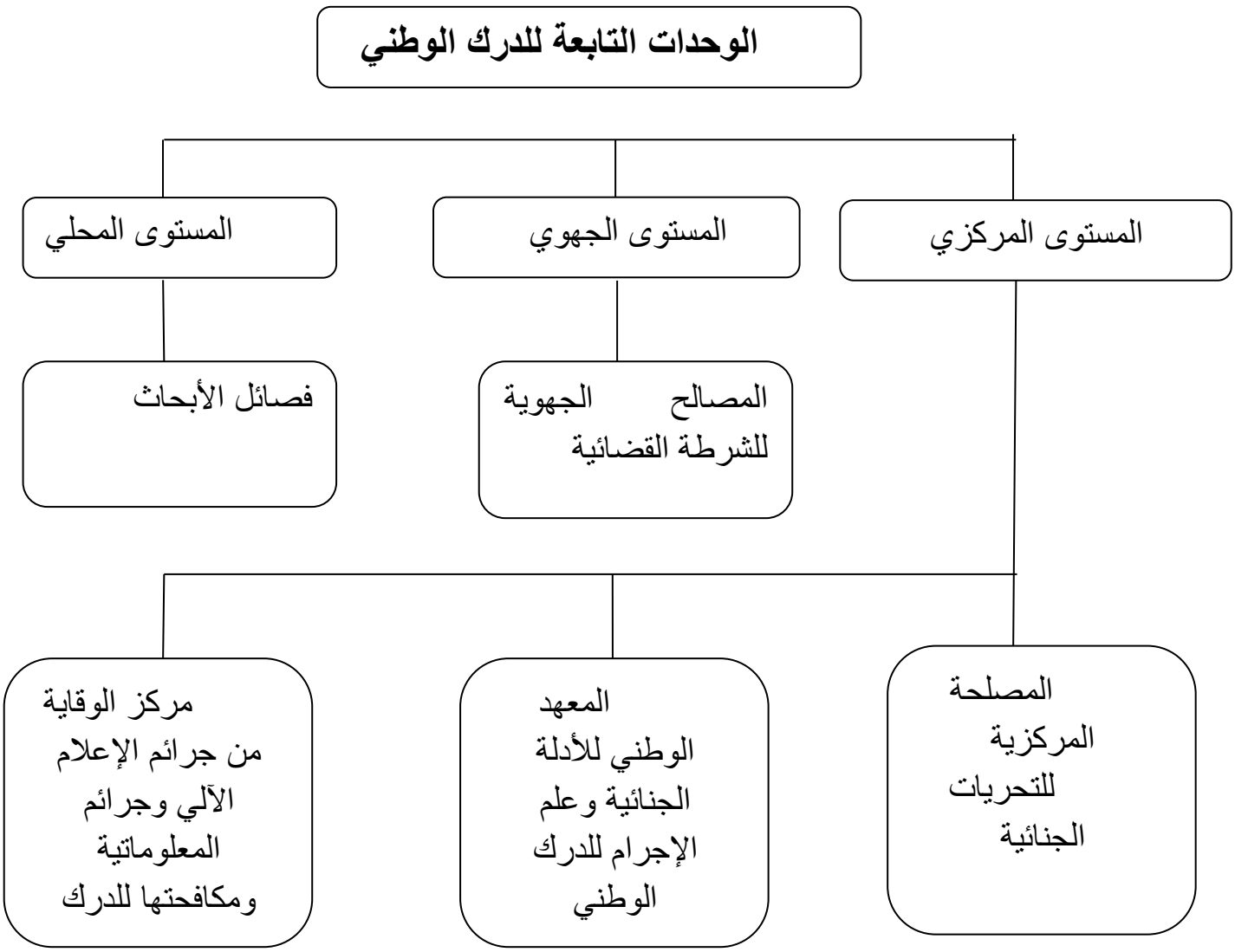
[3] الجمهورية الجزائرية الديمقراطية الشعبية، المرسوم الرئاسي 04-183، مرجع سابق، المادة: 04.

ب. **على المستوى الجهوي:** تتضمن وحدات الدرك الوطني في مجال مكافحة الجريمة المعلوماتية مجموعة من المصالح الجهوية للشرطة القضائية التابعة للدرك الوطني، تختص هذه المصالح بتنسيق النشاطات بين مختلف الوحدات التابعة للشرطة القضائية ودعمها بالوسائل الخاصة للتحريات والأبحاث المعقدة كالجرائم المعلوماتية.

ت. **على المستوى المحلي:** تحتوي وحدات الدرك الوطني على فصائل الأبحاث التي تتضمن بدورها أفراد لهم اختصاص واسع في ميدان الشرطة القضائية، تكلف بمكافحة الأشكال الخطيرة للإجرام المنظم كالجرائم المعلوماتية، القيام بتحقيقات تتطلب تحريات معقدة، كذلك تساهم في تدعيم نشاط الأبحاث والتحريات التي تقوم بها الفرق الإقليمية للدرك الوطني. [1]

[1] حسين ربيعي، **آليات البحث والتحري في الجرائم المعلوماتية**، مرجع سابق، ص 186.

شكل رقم (04): رسم تخطيطي يوضح الوحدات التابعة للدرك الوطني



المصدر: المخطط من تصور الطالبة بناء على الهياكل المنصوص عليها في النصوص القانونية. (المرسوم الرئاسي 04-183)

المطلب الثالث: المنظومة التابعة للأمن الوطني.

وظفت مديرية الأمن الوطني في إطار مكافحة الجريمة بكل أنواعها بما فيها المعلوماتية ووحدات متنوعة، [1] تتوزع على 3 مستويات كما يلي:

أ- المستوى المركزي:

[1] حسين ربيعي، **اليات البحث والتحري في الجرائم المعلوماتية**، مرجع سبق ذكره، ص177.

- **المصلحة المركزية لمكافحة الجرائم السيبرانية:** أنشئت سنة 2015 بمديرية الشرطة القضائية، تقوم المصلحة المركزية بالتنسيق مع مختلف الوحدات في مكافحة الجرائم المعلوماتية بما فيهم فرق مكافحة الجرائم السيبرانية وجهاز العدالة، إذ تباشر مهامها تحت إشراف السلطة القضائية فهي مختصة في تنفيذ تعليمات وإنابات الجهات القضائية على المستوى الوطني، كما تقوم بالتنسيق مع الشرطة الدولية الأنتربول حول تورط أشخاص في قضايا تخص المساس بالقصر باستخدام تكنولوجيا الإعلام والاتصال، حالات سرقة المعلومات الخاصة بالبطاقات البنكية. [1]

- **نيابة مديرية الشرطة العلمية والتقنية التابعة للمديرية العامة للأمن الوطني:**

تتولى نيابة مديرية الشرطة العلمية والتقنية مهمة مكافحة الجرائم المعلوماتية، إذ تضع هذه الأخيرة لتحقيق هذا الهدف وحدات تختص بمكافحة الجرائم المعلوماتية وتتولى أعمال التحري والبحث بشأن الجرائم السيبرانية وهي المخبر المركزي للشرطة العلمية مقره بالجزائر العاصمة الذي يتولى مهام البحث والتحقيق وتحليل الأدلة الجنائية بمختلف أنواعها. [2]

ب. على المستوى الجهوي: تحتوي مديرية الشرطة العلمية والتقنية على مخابر جهوية للشرطة العلمية في كل من ولايتي قسنطينة ووهران، ورقلة، بشار، تمنراست، إذ تكلف هذه المخابر بضمان الدعم التقني لمختلف مصالح الشرطة والأجهزة القضائية في مجال التحريات الإلكترونية، إذ يحتوي كل مخبر جهوي على مصلحة تختص بأعمال البحث والتحقيق القائمة بشأن الجرائم المعلوماتية وتسمى هذه المصلحة بـ"دائرة الأدلة الرقمية والآثار التكنولوجية" وتضم هذه المصلحة بدورها 3 أقسام فرعية:

❖ قسم استغلال الأدلة الرقمية الناتجة عن الحواسيب والشبكات.

- قسم استغلال الأدلة الناتجة عن الهواتف النقالة.
- قسم تحليل الأصوات.

ت. على المستوى المحلي: تتمثل في فرق مكافحة الجرائم المعلوماتية على مستوى مصالحها بأمن الولايات. [3]

---

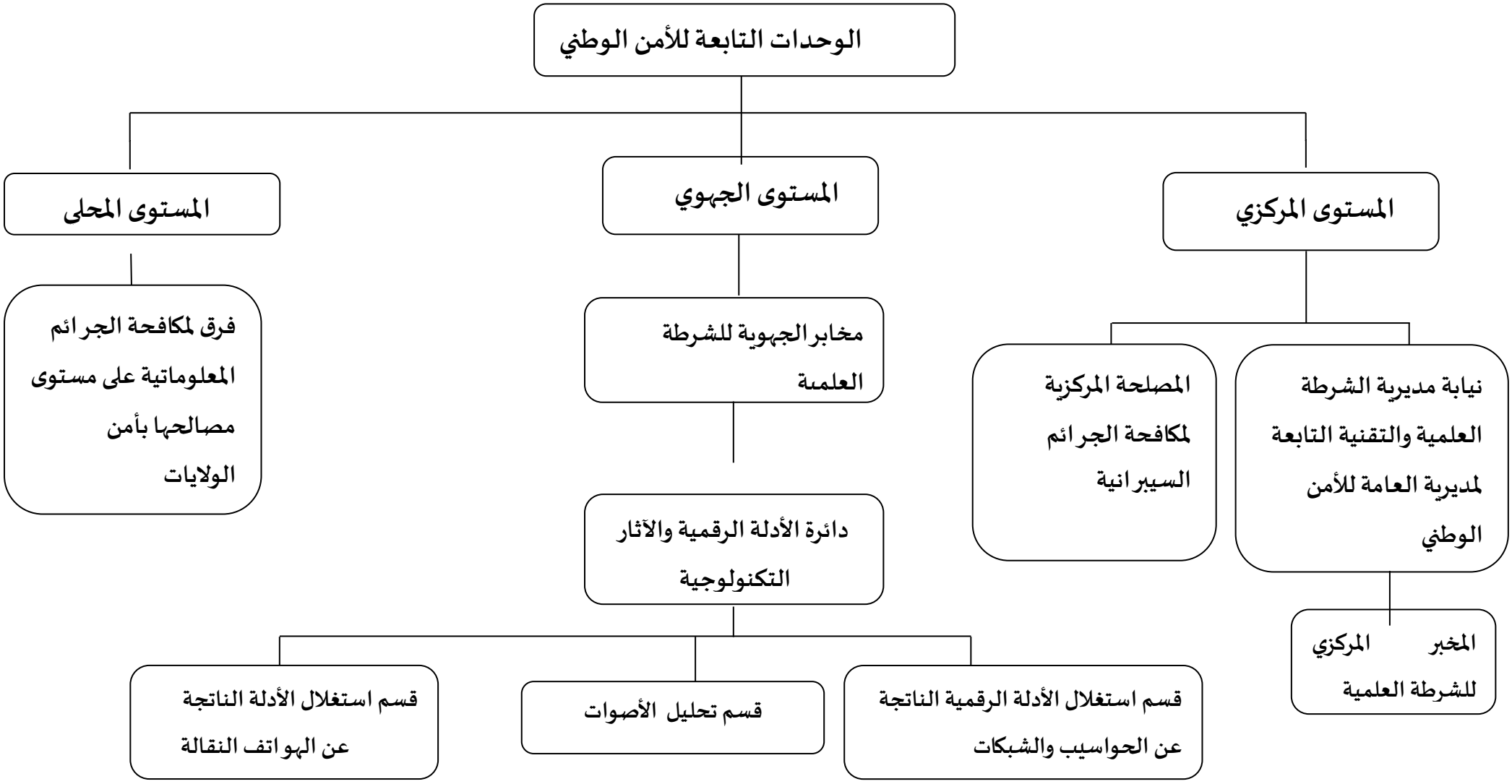
[1] غنية حساني، "العصب الرقمي لرصد الجريمة المعلوماتية"، **مجلة الشرطة**، ع (158)، (2024)، ص 18 وص19.

[2] حسين ربيعي، **اليات البحث والتحري في الجرائم المعلوماتية**، مرجع سبق ذكره، ص177.

[3] عمار حشمان، **الجريمة المعلوماتية في التشريع الجزائري**، مذكرة ماستر غير منشورة (جامعة قاصدي مرباح، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، 2019/2018.) ص39.

وللتوضيح أكثر، يوضح التخطيطي التالي الوحدات التابعة للأمن الوطني.

الشكل رقم (5): رسم تخطيطي يوضح الوحدات التابعة للأمن الوطني



المصدر: المخطط من تصور الطالبة بناء على الهياكل المنصوص عليها في النصوص القانونية.

المطلب الرابع: المنظومة التابعة للسلطة القضائية.

أصدر المشرع الجزائري بغية مواكبة التطورات الحاصلة في الفضاء الرقمي آلية جديدة تختص بمكافحة الجرائم المتعلقة بتكنولوجيا الإعلام و الاتصال المتمثلة في " القطب الجزائي الوطني لمكافحة الجرائم المتعلقة بتكنولوجيا الإعلام و الاتصال "، إذ أنشأ هذا القطب بموجب الأمر رقم 21-11 المتضمن قانون الإجراءات الجزائية في المادة 211 مكرر22 : "ينشأ على مستوى محكمة مقر مجلس قضاء الجزائر، قطب جزئي وطني متخصص في المتابعة والتدقيق في الجرائم المتمثلة بتكنولوجيات الإعلام والاتصال والجرائم المرتبطة بها" تتمثل مهام وكيل الجمهورية لدى الجزائي في مجال مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وقاضي التحقيق ورئيس ذات القطب بالمتابعة والتحقيق والحكم في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وكذا الجرائم المرتبطة بها: الجرائم التي تمس بأمن الدولة أو بالدفاع الوطني، جرائم النشر وترويج أخبار كاذبة بين الجمهور من شأنها المساس بالأمن والسكينة العامة واستقرار المجتمع، جرائم المساس بأنظمة المعالجة الآلية للمعطيات المتعلقة بالإدارات و المؤسسات العمومية. [1]

المطلب الخامس: المنظومة التابعة لوزارة البريد والمواصلات السلكية واللاسلكية.

تضم المنظومة التابعة لوزارة البريد والمواصلات السلكية واللاسلكية أربع مؤسسات تعنى بحماية البيانات الشخصية.

1- سلطة ضبط البريد والاتصالات الإلكترونية:

أنشئت سلطة ضبط البريد والإتصالات الالكترونية بموجب القانون 18-04 المتضمن القواعد العامة المتعلقة بالبريد والإتصالات الالكترونية، وذلك في نص المادة (11): " تنشأ سلطة ضبط مستقلة للبريد والمواصلات الالكترونية، تتمتع بالشخصية المعنوية والاستقلال المالي، وتدعى في صلب النص "سلطة الضبط" يكون مقر سلطة الضبط بمدينة الجزائر." [2] كما تضمن القانون أيضا تشكيلة سلطة ضبط البريد و الاتصالات الالكترونية وذلك في نص المادة 19 و 20 ، إذ تتشكل السلطة من مجلس ومدير عام أما بالنسبة لعضوية مجلس سلطة الضبط فيتكون من 7 أعضاء من بينهم الرئيس يتم تعيينهم من طرف رئيس

[1] الجمهورية الجزائرية الديمقراطية الشعبية، الأمر رقم 21-11، المؤرخ في 16 محرم 1443 الموافق ل 25 غشت 2021، المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، العدد 65، الصادر بتاريخ 26غشت 2021، المادة 12.

[2] الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 18-04، مرجع سابق، المادة 11.

الجمهورية بناءا على اقتراح من الوزير الأول، [1] أما بالنسبة لمهام سلطة ضبط البريد والاتصالات الإلكترونية فقد حددت المادة 13 المهام التي تضطلع بها من بينها: السهر على وجود منافسة فعلية ومشروعة في سوقي البريد والاتصالات الالكترونية باتخاذ كل التدابير الضرورية لترقية واستعادة المنافسة في هاتين السوق، السهر على تجسيد تقاسم منشآت الاتصالات الالكترونية في ظل احترام حق الملكية ،إعداد مخطط وطني للترقيم ودراسة طلبات الأرقام و منحها للمتعاملين ،المصادقة على العروض المرجعية للتوصيل البيني والنفاذ إلى شبكات الاتصال الالكترونية. منح التراخيص العامة لإنشاء أو استغلال شبكات الاتصالات الالكترونية وتوفير خدمات الاتصالات الالكترونية وتراخيص الشبكات الخاصة، وكذا تراخيص تقديم خدمات وأداءات البريد، المصادقة على تجهيزات البريد والاتصالات الالكترونية طبقا للمواصفات والمعايير المحددة عن طريق التنظيم، السهر على احترام متعاملي البريد و الاتصالات الالكترونية للأحكام القانونية و التنظيمية المتعلقة على الخصوص بالبريد والاتصالات الالكترونية والأمن السيبراني، السهر على حماية حقوق المشتركين في خدمات الاتصالات الالكترونية ، وضع إجراء يحدد كيفية معالجة شكاوي المشتركين نشر كل معلومة مفيدة لحماية حقوق المشركين و كذا القيام بحملات تنظيمية تحسيسية وتوعوية. [2]

2- **السلطة الحكومية للتصديق الإلكتروني:** هي سلطة رقابية أنشئت من طرف الوزير المكلف بالبريد وتكنولوجيات الإعلام والاتصال،[3] تتمثل مهام السلطة الحكومية للتصديق الإلكتروني حسب المادة 28 من القانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكتروني في: إعداد سياسة التصديق الالكتروني وعرضها على السلطة الموافقة عليها والسهر على تطبيقها، الموافقة على سياسات التصديق الصادرة على الأطراف التالية الموثوقة والسهر على تطبيقها، نشر شهادة التصديق الإلكتروني، للمفتاح العمومي للسلطة، إرسال كل المعلومات المتعلقة بنشاط التصديق الإلكتروني إلى السلطة دوريا أو بناءا على طلب منها، القيام بعملية التدقيق على مستوى الطرف الثالث الموثوق عن طريق الهيئة الحكومية المكلفة بالتدقيق، طبقا لسياسة التصديق. [4]

3- **السلطة الاقتصادية للتصديق الإلكتروني:** يتم تعيينها من طرف السلطة المكلفة بضبط البريد والمواصلات السلكية واللاسلكية، إذ تكلف هذه السلطة حسب القانون 15-04 في المادة 30 بالمهام الآتية: إعداد السياسة التصديق الإلكتروني وعرضها على السلطة للموافقة عليها والسهر على تطبيقها، منح

---

[1] المرجع نفسه، المادة 19 و20.

[2] الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 18-04، مرجع سابق، المادة 13.

[3] المرجع نفسه، المادة 26.

[4] المرجع نفسه، المادة 28.

التراخيص لمؤيدي خدمات التصديق الالكتروني بعد موافقة السلطة، الموافقة على سياسات التصديق الصادرة عن مؤدي خدمات التصديق الإلكتروني السهر على تطبيقها، الاحتفاظ بشهادات التصديق الإلكتروني المنتهية صلاحيتها والبيانات المرتبطة بمنحها من طرف مؤدي خدمات التصديق الالكتروني بغرض تسليمها إلى السلطات القضائية المختصة عند الاقتضاء، نشر شهادة التصديق الإلكتروني للمفتاح العمومي السلطة، اتخاذ التدابير اللازمة لضمان استمرارية الخدمات التصديق الإلكتروني، إرسال كل المعلومات المتعلقة بنشاط التصديق الإلكتروني إلى السلطة دوريا أو بناء على طلب منها، التحقق من مطابقة طالبي التراخيص مع سياسة التصديق الإلكتروني بنفسها، مطالبة مؤدي خدمات التصديق الإلكتروني وكل شخص معني بأي وثيقة أو معلومة تساعدها في تأدية المهام المخولة لها، إعداد دفتر الشروط الذي يحدد شروط وكيفيات تأدية خدمات التصديق الالكتروني وعرضه. [1]

4- المرجع الوطني لأمن المعلومات:

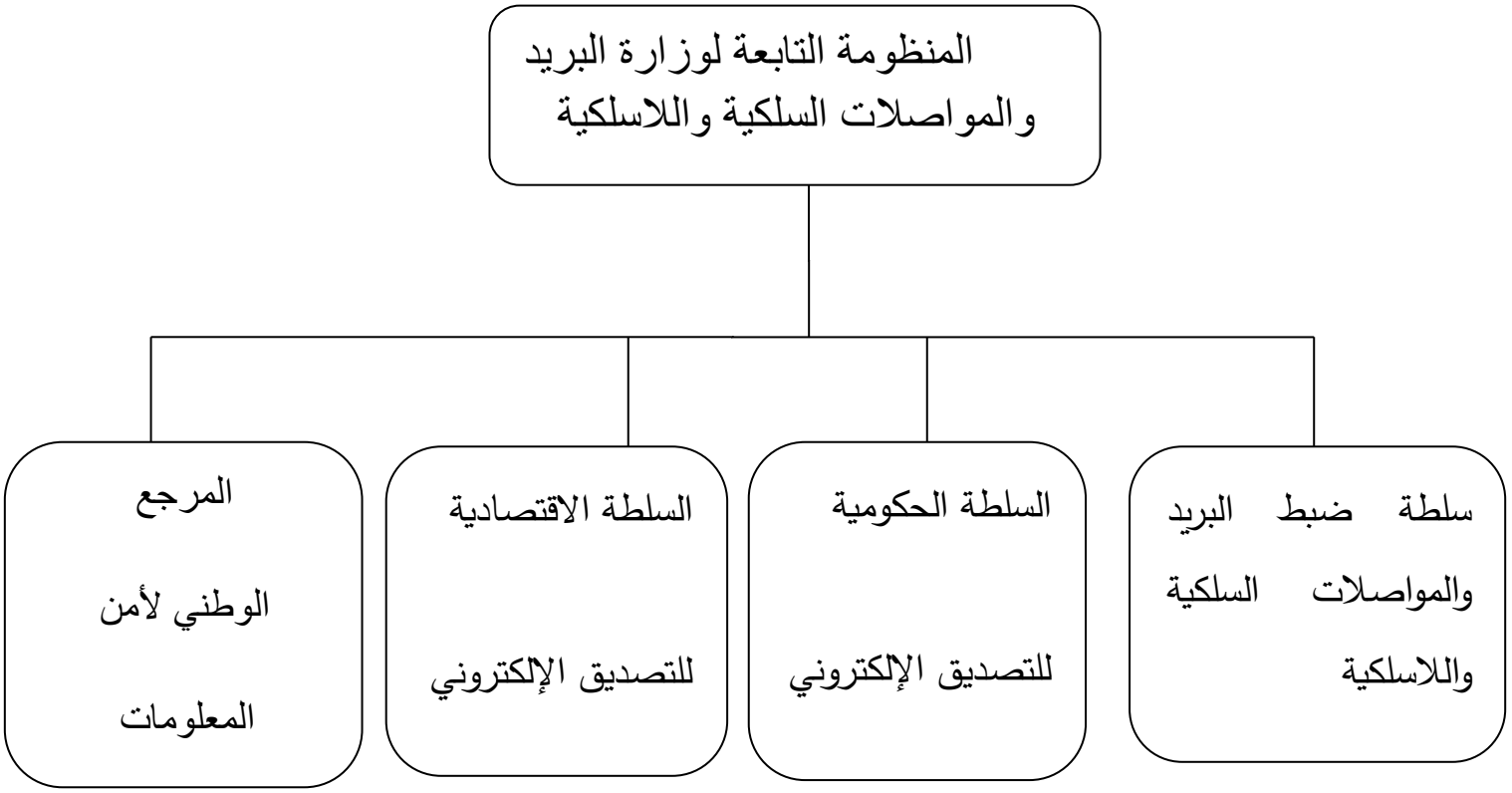
هو دليل أعدته وزارة البريد والمواصلات السلكية واللاسلكية يهدف إلى إقامة حوكمة ونهج موحد لأمن المعلومات داخل الهيئات والمؤسسات هذا المرجع يحدد الحد الأدنى من المتطلبات المتعلقة بالأمن، كما يقدم مرجع الوطني لأمن المعلومات مجموعة من الضوابط الأمنية وأفضل الممارسات الدولية المتمثلة في المعايير الدولية سلسلة ISO27000وRGPD، كما يركز المرجع الوطني لأمن المعلومات على تدريب وتوعية المستخدمين بالمخاطر التي تنطوي عليها، كما يغطي المرجع الوطني لأمن المعلومات 20 مجالا يتمثل في:

- الأمن المادي.
- انترنت الأشياء.
- المراقبة وتسجيل الوقائع..
- إدارة الحوادث الأمنية.
- تسير استمرارية النشاطات.
- الموارد البشرية.
- الأمن المتعلق باستخدام مواقع التواصل الاجتماعي.
- دمج الأمن خلال دورة حياة تطوير البرمجيات.
- متطلبات الأمن المشاريع تكنولوجيا الإعلام والاتصال.
- حماية المعطيات ذات الطابع الشخصي.
- أمن أنظمة المعلومات بالغ الأهمية
- إدارة الموجودات
- إدارة ومراقبة النفاذ.
- أمن أجهزة المحمول.
- أمن الشبكات.
- أمن أنظمة المعلومات.
- الأمن المتعلق بالتشغيل.
- لعلاقة مع الأطراف الثالثة.

[1] الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 15-04، مرجع سابق، المادة 30.

- أمن الحوسبة السحابية.[1]

الشكل رقم (06): رسم تخطيطي يوضح المؤسسات التابعة لوزارة البريد والمواصلات السلكية واللاسلكية.



المصدر: المخطط من تصور الطالبة بناء على الهياكل المنصوص عليها في النصوص القانونية (القانون 18-04، 15-04.).

إنطلاقا من تعدد المؤسسات الفاعلة في مجال حماية البيانات الشخصية وتعدد أداورها المخولة لها بموجب القانون، يظهر أن هذه المؤسسات لا تعمل بمعزل عن الأخرى بل تعمل بالتنسيق فيما بينها لتحقيق الأهداف المرجوة، فعلى سبيل المثال: تتعاون المحافظة السامية للرقمنة مع وكالة أمن الأنظمة المعلوماتية في ضمان توافق الإستراتيجية الوطنية للرقمنة مع متطلبات أمن الأنظمة المعلوماتية، وفي جهة أخرى نجد أن المحافظة السامية للرقمنة تنسق مع كل القطاعات المعنية بالرقمنة من بينها (وزارة البريد والمواصلات السلكية و اللاسلكية) في مجال ضمان توافق الإستراتجية الوطنية للرقمنة مع مخططات القطاعات بما فيها وزارة البريد والمواصلات السلكية و اللاسلكية، كما تنسق أيضا مع السلطة الوطنية لحماية المعطيات

[1] وزارة البريد والمواصلات السلكية واللاسلكية، **مرجع أمن المعلومات**، https: www.mpt.gov.dz تاريخ الإطلاع (2025/05/10).

ذات الطابع الشخصي من خلال ضمان توافق معايير المرجع الوطني لحوكمة البيانات مع القانون المتعلق بحماية المعطيات ذات الطابع الشخصي 18-07، ومن جانب أخر تتعاون السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي مع السلطة القضائية(ضباط و أعوان الشرطة القضائية) في معاينة والبحث عن الجرائم التي نصت عليها أحكام القانون 18-07 إلى جانب تنسيقها مع المرجع الوطني للمعلومات (وزارة البريد والمواصلات السلكية واللاسلكية) في مجال توافق معايير المرجع الوطني لأمن المعلومات مع قوانين المتعلقة بحماية المعطيات ذات الطابع الشخصي المتمثل في القانون 18-07،وفي نفس السياق يسجل تنسيق مستمر بين الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال(وزارة الدفاع الوطني) مع السلطة القضائية في إطار مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، كما تتعاون مع مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها(وحدات الدرك الوطني) في مجال المشاركة في عمليات التحري والتسرب عبر شبكات الانترنت وقمع الجرائم المعلوماتية، وفي ذات السياق تنسق مؤسسات وزارة الدفاع الوطني المتمثلة في مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة والمركز الوطني للإشارة و الحروب الإلكترونية مع بعضها البعض في مجال تأمين الاتصالات العسكرية، إلى جانب تعاون مصلحة الدفاع السيبراني مع وكالة أمن الأنظمة المعلوماتية(وزارة الدفاع)في مجال إعداد الإستراتيجية الوطنية للدفاع السيبراني، كما تتعاون وحدات الدرك الوطني(المعهد الوطني للأدلة الجنائية) مع مصالح الأمن الوطني (المخبر المركزي للشرطة العلمية) في مجال البحث والتحقيق وتحليل الأدلة الجنائية في سبيل قمع الجرائم المعلوماتية، أما بالنسبة للسلطة القضائية (القطب الجزائي) فتتعاون مع الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال (وزارة الدفاع الوطني) و مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها في مجال المتابعة والتحقيق في الجرائم التي تمس بأمن الدولة والدفاع الوطني، هذا التنسيق القائم بين المؤسسات يعبر عن رغبة الدولة في إرساء منظومة وطنية متكاملة لحماية خصوصية المواطنين بما فيهم بياناتهم الشخصية.

المبحث الثاني: المؤسسات المشرفة على حماية البيانات الشخصية في البنوك التجارية

تحظى حماية البيانات الشخصية في البنوك التجارية بأهمية كبيرة نظرا لاعتمادها بشكل كبير على الأنظمة الرقمية في إدارة بيانات عملائها تقدمها للخدمات وفي ظل تزايد حجم المعالجة الالكترونية للبيانات، بررت الحاجة إلى إنشاء مؤسسات تتولى الإشراف على تنظيم الحماية للبيانات الشخصية في البنوك التجارية.

المطلب الأول: دور السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي في حماية البيانات الشخصية.

هي سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلالية المالية و الإدارية يقع مقرها بولاية الجزائر، تتكون من 16 عضوا من بينهم رئيسها، معينون بالمرسوم الرئاسي رقم 22-187،[1] تشرف السلطة الوطنية على ضمان احترام أحكام القانون 18-07 إلى جانب مهام أخرى تكلف بها السلطة الوطنية حددتها المادة 25 من بينها: منح التراخيص وتلقي التصريحات المتعلقة بمعالجة المعطيات ذات الطابع الشخصي، إعلام الأشخاص المعنيين والمسؤولين عن المعالجة بحقوقهم وواجباتهم، الأمر بإغلاق معطيات أو سحبها أو إتلافها، تلقي الاستشارات للأشخاص والكيانات التي تلجأ لمعالجة المعطيات ذات الطابع الشخصي أو التي تقوم بتجارب أو خبرات من طبيعتها أن تؤدي إلى مثل هذه المعالجة، تلقي الاحتجاجات والطعون والشكاوي بخصوص تنفيذ معالجة المعطيات ذات الطابع الشخصي وإعلام أصحابها، وضع معايير في مجال حماية المعطيات ذات الطابع الشخصي، إصدار عقوبات إدارية وفقا لأحكام المادة 46 من هذا القانون في حق المسؤول عن المعالجة في حالة خرقه لأحكام القانون 18-07، إضافة إلى ذلك تتولى السلطة الوطنية مراقبة مدى تقيد المسؤول عن المعالجة بالالتزام بتمكين الشخص المعني بممارسة حقه في الاعتراض على معالجة معطياته ذات الطابع الشخصي لأسباب مشروعة وفقا للمادة 36 من القانون 18-07، كما تشرف السلطة الوطنية على مراقبة مدى التزام مسؤولين المعالجة من خلال اتخاذ جملة التدابير التقنية والتنظيمية الملائمة لحماية سرية وسلامة المعطيات ذات الطابع الشخصي محل المعالجة من الإتلاف العرضي أو الغير مشروع أو الضياع العرضي أو التلف أو النشر أو الولوج غير المرخص[2]، إذ تضمن

(1) الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 18-07، مرجع سابق، المادة 22.

(2) المرجع نفسه، المادة 38.

أحكام هذا القانون مجموعة من الالتزامات يلتزم بها المسؤول عن المعالجة من بينها التزام المسؤول عن المعالجة والأشخاص الذين أطلعوا أثناء ممارسة مهامهم على معطيات ذات الطابع شخصي بالسر المهني حتى بعد انتهاء مهامهم، اختيار المسؤول عن المعالجة معالج من الباطن يقدم الضمانات الكافية المتعلقة بإجراءات السلامة التقنية والتنظيمية للمعالجات الواجب القيام بها و يسهر على احترامها،[1] من خلال ما سبق بين أن السلطة الوطنية تلعب دورا جوهريا في حماية البيانات الشخصية و احترام خصوصية البيانات داخل البنوك التجارية من خلال الصلاحيات و المهام التي خول لها حكام القانون 18-07 في مجال حماية المعطيات ذات الطابع الشخصي.

المطلب الثاني: دوروزارة الدفاع الوطني في حماية البيانات الشخصية.

تلعب مؤسسات وزارة الدفاع الوطني دورا جوهريا في تعزيز أمن البيانات الشخصية داخل البنوك التجارية، ومن بين هذه المؤسسات هي الوكالة الوطنية لأمن الأنظمة المعلوماتية التي أنشئت بموجب المرسوم الرئاسي 20-05 وهي مؤسسة عمومية ذات طابع إداري، تتمتع بالشخصية المعنوية والاستقلالية المالية، [2] إذ تكلف هذه الوكالة بمجموعة من المهام حددتها المادة 18 من المرسوم 20-05 تتمثل في : تحضير عناصر الإستراتيجية الوطنية في مجال امن الأنظمة المعلوماتية المحددة من قبل المجلس، اقتراح كيفيات اعتماد مزودي خدمات التدقيق في مجال أمن الأنظمة المعلوماتية، إجراء تحقيقات رقمية في حالة الهجمات والحوادث السيبرانية التي تستهدف المؤسسات الوطنية، مرافقة الإدارات والمؤسسات والهيئات بالتشاور مع الهياكل المختصة في هذا المجال، معالجة الحوادث المتعلقة بأمن الأنظمة المعلوماتية، ضمان اليقظة الالكترونية في مجال أمن الأنظمة المعلوماتية، السهر على جمع وتحليل وتقييم المعطيات المتصلة بمجال أمن الأنظمة المعلوماتية لاستخلاص المعلومات الملائمة التي تسمح بتأمين منشآت المؤسسات الوطنية،[3] اذن أن الوكالة الوطنية لأمن الأنظمة المعلوماتية لا تتدخل بصفة مباشرة في تنظيم البيانات داخل البنوك أو ممارسة الرقابة على امن البيانات مثلما تفعل السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، بل يظهر دورها في حال حدوث أو وجود تهديدات يمس بسلامة وأمن البيانات وهذا ما نصت عليه أحكام المرسوم الرئاسي 20-05 المادة 18 تقوم الوكالة الوطنية لامن الأنظمة المعلوماتية بفتح تحقيقات في حال حدوث تهديد سيبراني.

---

[1] الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 18-07، مرجع سابق، المادة 38.

[2] الجمهورية الجزائرية الديمقراطية الشعبية، المرسوم الرئاسي 20-05، مرجع سابق، المادة 17.

[3] المرجع نفسه، المادة 18.

المطلب الثالث: دور وزارة البريد والمواصلات السلكية واللاسلكية في حماية البيانات الشخصية.

لعبت وزارة البريد والمواصلات السلكية واللاسلكية دورا محوريا في حماية البيانات الشخصية، وذلك من خلال إنشائها للمرجع الوطني لأمن المعلومات (RNSI)التي تم إطلاقه في عام 2016 يعد هذا المرجع أول دليل يجمع المبادئ التوجيهية وأفضل الممارسات لتأمين المعلومات ويغطي العديد من مجالات الأمن من أجل ضمان الحماية الكافية لأمن الأنظمة المعلومات التابعة للهيئات العامة، اذ تضمنت هذه الوثيقة 07 محاور تمثلت فيما يلي:

- إدارة الموجودات.
- الأمن المادي.
- أمن المستخدم النهائي.
- مراقبة الدورية للأنظمة.
- تأمين الشبكات.
- إدارة مخاطر القدرة على استعادة المعلومات.

ومع تنوع وتطور التهديدات السيبرانية إضافة إلى المتطلبات الجديدة للشريعات واللوائح الجزائرية فيما يتعلق بأمن المعلومات تم تحديث النسخة الأولى للمرجع الوطني لأمن المعلومات 2016، [1] وصدر المرسوم التنفيذي رقم 19-272 الصادر في 7 أكتوبر 2019 المتعلق بالمرجع الوطني لتوافقية أنظمة المعلومات، إذ تضمن هذا المرسوم أهداف هذا المرجع الوطني التي تتمثل في: توحيد صيغ تبادل المعطيات بين هيئتين وبين الإدارة والمواطن قصد تحسين الخدمات الموفرة، ضمان ديمومة أنظمة الإعلام العمومية من خلال استخدام المعايير والمقاييس المعترف بها دوليا كما يهدف أيضا إلى توفير إطار ومجموعة من المتطلبات الأساسية التي من شأنها تمكين تطوير وتنفيذ سياسة أمن أنظمة المعلومات داخل الهيئات العامة والهيئات الفرعية التابعة لها،[2] كما يهدف أيضا إلى زيادة مستوى أمن أنظمة المعلومات وحماية معلومات المنظمات من خلال تنفيذ ضوابط الأمن، وعليه فإن مرجع الوطني لأمن المعلومات يتضمن ضوابط الأمن وأفضل الممارسات الدولية والمعروفة من بينها عائلة ISO/IE27000 التي يجب على الهيئات العامة اعتمادها كما يحدد الحد الأدنى من متطلبات الأمن الكفيلة بضمان حماية الأنظمة المعلوماتية من مختلف التهديدات خاصة بالنسبة للمؤسسات التي تعالج بيانات شخصية أو بيانات حساسة كما هو الحال في البنوك التجارية.

---

[1] وزارة البريد والمواصلات السلكية واللاسلكية، **مرجع أمن المعلومات**، في: www.mpt.gov.dz :https تاريخ الإطلاع (2025/05/10).

[2] الجمهورية الجزائرية الديمقراطية الشعبية، المرسوم التنفيذي رقم 19-271، المؤرخ في 8 صفر 1441 الموافق ل 7أكتوبر 2019، المتعلق بالمرجع الوطني لتوافقية أنظمة الإعلام، الجريدة الرسمية، العدد 63، الصادر في 9 أكتوبر سنة 2019، المادة: 03.

المطلب الرابع: دور بنك الجزائر في حماية البيانات الشخصية.

يعتبر بنك الجزائر بموجب القانون 23-09 المتضمن للقانون النقدي والمصرفي هي مؤسسة وطنية تتمتع بالشخصية المعنوية و الاستقلال المالي،[1] أنشئ بنك الجزائر بموجب القانون 62-144 الذي صوت عليه المجلس التأسيسي إذ يعتبر البنك الجزائري السلطة النقدية التي تخول للمصارف القائمة ممارسة نشاطها المصرفي وفقا للسياسة النقدية المعتمدة، إذ يتولى بنك الجزائر توجيه ورقابة البنوك التجارية لاستقرار نشاطها المصرفي، كما يقوم بنك الجزائر بالحرص على استقرار الأسعار و توفير أفضل الشروط في ميادين النقد و القرض والصرف، كما يكلف أيضا بتنظيم الحركة النقدية ويوجه ويراقب بكل الوسائل الملائمة توزيع القرض وضبط السيولة، كما يسهر أيضا على حسن سير التعهدات المالية اتجاه الخارج وضبط سوق الصرف و لتأكد من سلامة النظام المصرفي وصلابته، يقدم الاستشارة للحكومة في كل تدبير من شأنه أن يحسن ميزان المدفوعات وحركة الأسعار،[2] وبغرض تنظيم النشاط البنكي بين المؤسسات المالية والبنوك بما فيها البنوك التجارية، يقوم البنك الجزائر بإصدار قوانين تنظيمية وتعليمات التي يجب على كل بنك الامتثال لها في جميع الأوقات، وفي إطار حماية البيانات الشخصية وباعتبار بنك الجزائر إحدى المؤسسات المساهمة في تأطير إجراءات الحماية بصفة عامة ومن ضمنها تأطير أنظمة حماية البيانات الشخصية، أصدر بنك الجزائر تعليمة رقم 25-02المتعلقة بالشروط الخاصة للترخيص بتأسيس واعتماد وممارسة نشاط البنك الرقمي، إذ تضمنت هذه التعليمة العناصر الواجب توفرها لتأسيس بنك رقمي ومن بينها عناصر متعلقة بسرية البيانات و خصوصيتها و أنظمة المعلومات الخاصة بتأمين البيانات من بينها: التشفير، جدران الحماية، ورقابة الولوج إلى نظام المعلومات، كما تضمنت التعليمة أيضا مواصفات أجهزة حماية البيانات و حددت في نفس السياق الإطار الخاص التي يستند عليها أمن نظم المعلومات من بينها أنه يقوم على أفضل الممارسات الدولية ومعايير أمن المعلومات المتمثلة في ISO/IEC و GDPR، كما يرتكز أيضا على إطار قانوني وتنظيمي يشمل حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، القواعد المتعلقة بالتوقيع والتصديق الإلكتروني والقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، كما حدد بنك الجزائر في هذه التعليمة أنه يجب أن تتوفر هذه العناصر أيضا على جميع الأجهزة و التدابير المخطط لها في إطار إدارة الحوادث واستمرارية الأنشطة

---

[1] الجمهورية الجزائرية الديمقراطية الشعبية، القانون 23-09، المؤرخ في 3 ذي الحجة 1444 الموافق ل 21 يونيو2023، المتضمن القانون النقدي والمصرفي، الجريدة الرسمية، العدد 43، الصادر في: 27 يونيو 2023، المادة: 09.

[2] تاريخ البنك، في: https://www.bank-of-algeria.dz، تاريخ الاطلاع: (2025/5/6).

للسماح والترخيص بإنشاء بنك رقمي،[1] وفي ذات السياق أصدر بنك الجزائر نظام رقم 25-03 المتعلق بحماية زبائن البنوك والمؤسسات المالية والخاضعين الآخرين، بحيث يتناول هذا النظام القواعد المطبقة في مجال حماية الزبائن وخصص الفصل الرابع للمسؤوليات التي تقع على عاتق الخاضعين اتجاه الزبائن الرامية إلى حماية خصوصية وسرية البيانات، إذ تضمن هذا الفصل واجبات الخاضعين من بينها ضمان حماية المعلومات من خلال وضع تدابير أمنية و آليات حفظ الوثائق المناسبة، كما يجب على الخاضعين إبلاغ زبائنهم واللجنة المصرفية فورا عن كل انتهاك للبيانات من شأنها أن تهدد أمن المعلومات الشخصية، ضمان سرية و سلامة البيانات الشخصية للزبائن، كما يجب على الخاضعين تكييف أنظمتهم الأمنية مع التطورات التكنولوجية وأشكال المخاطر الرقمية الجديدة من جهة أخرى، حدد هذا النظام الالتزامات الزبائن إذ يتعين عليهم حسب النظام تقديم معلومات دقيقة، الإطلاع على الوثائق قبل الاشتراك في أي منتج أو خدمة، إبلاغ البنك أو المؤسسة المالية عن أي معاملة غير عادية أو غير مرخص لها تمس حساباته، حماية سرية معلوماته الشخصية والمالية،[2] وعليه يمكن القول أن بنك الجزائر يضطلع بدور محوري في حماية البيانات الشخصية باعتبار قوانينه وتعليماته الصادرة تمثل الإطار المرجعي لجميع البنوك بما فيها البنوك التجارية.

المطلب الخامس: مديرية أمن أنظمة المعلومات التابعة للبنوك التجارية

بعد صدور المرسوم الرئاسي 20-05 المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية والذي نص على التزام المؤسسات والإدارات والهيئات العمومية والمتعاملون الخواص بتعيين مسؤولهم المكلف بأمن الأنظمة المعلوماتية في أجل أقصاه سنة،[3] قامت البنوك التجارية في الجزائر بتطبيق ما جاء به أحكام المرسوم 20-05 إذ تم تعيين على مستوى كل بنك مسؤول عن أمن أنظمة المعلومات (RSSI)يكلف بمجموعة من المهام وردت في المرجع الوطني لأمن المعلومات، إذ يقوم المسؤول بالمهام التالية:

1) تطوير والمشاركة في صياغة وتحديث مختلف وثائق الأمن (السياسات والإجراءات وما إلى ذلك) بشكل منتظم.
2) تقديم المشورة للإدارة بشأن الخيارات الفنية والتنظيمية لضمان أمن أنظمة المعلومات.
3) إعداد خريطة المخاطر المرتبطة بأمن نظام المعلومات، وضمان تنفيذ خطط المعالجة المختلفة.

---

[1] الجمهورية الجزائرية الديمقراطية الشعبية، بنك الجزائر، التعليمة رقم 25-02، المؤرخة في 2 مارس 2025، المتعلقة بالشروط الخاصة للترخيص بتأسيس واعتماد وممارسة نشاط البنك الرقمي، في: https://www.bank-of-algeria.dz، بتاريخ (2025/5/6).

[2] الجمهورية الجزائرية الديمقراطية الشعبية، بنك الجزائر، نظام رقم 25-03، لمؤرخ في 15 شوال 1446 الموافق ل 14 أفريل 2025، المتعلق بحماية زبائن البنوك، والمؤسسات المالية، والخاضعين الأخرين، في: https://www.bank-of-algeria.dz، بتاريخ (2025/5/6).

[3] الجمهورية الجزائرية الديمقراطية الشعبية، المرسوم الرئاسي 20-05، مرجع سابق، المادة 41.

4) تقييم ومراقبة مستوى أمان أنظمة المعلومات الخاصة بالمنظمة.

5) المشاركة في تنفيذ خطة استمرارية الأعمال وفعالية خطة التعافي من الكوارث في مجال تكنولوجيا المعلومات.

6) إعداد برنامج توعوي وتدريبي حول موضوع أمن المعلومات للموظفين المتعاملين مع نظام المعلومات.

7) توفير الدعم للهياكل المختلفة لضمان تكامل واستيعاب عنصر الأمن في مختلف مراحل المشروع، وبعد دخول أنظمة المعلومات إلى الإنتاج.

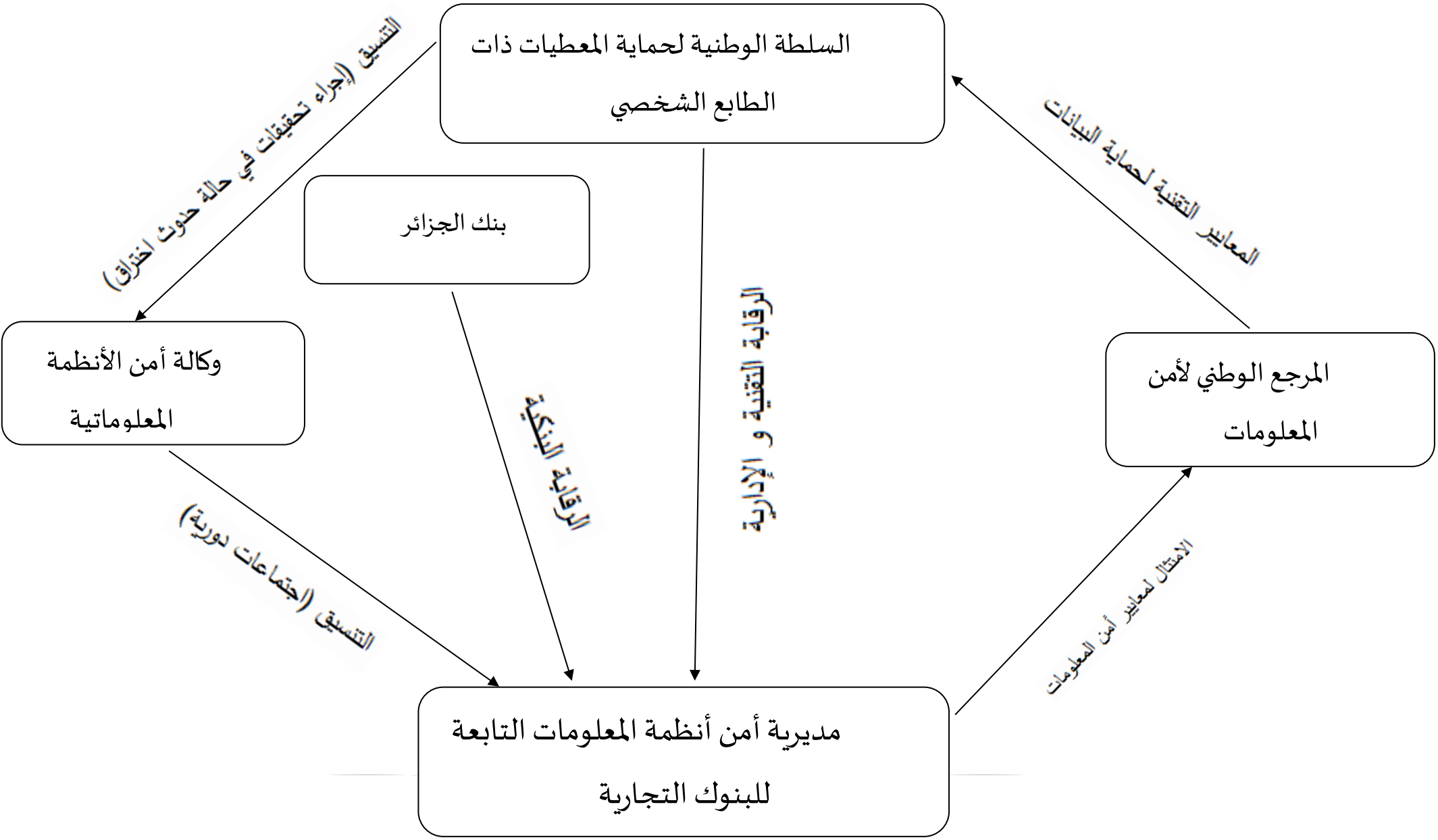
8) تنفيذ مهام التدقيق والتحقيق على فترات زمنية منتظمة أو بعد وقوع الحادث.

9) تولي دور مسؤول حوكمة أمن المعلومات إذا لزم الأمر. [1]

من خلال ما سبق، يمكن القول بأن هناك تداخل وظيفي وتنسيق بين مختلف المؤسسات التي تشرف على حماية البيانات الشخصية في البنوك التجارية، وهذا ما يوضحه الرسم التخطيطي، فعلى سبيل المثال تقوم السلطة الوطنية لحماية المعطيات ذات الطابع الشخصية بموجب الصلاحيات المخولة له في القانون 18-07 بالتنسيق مع وكالة امن الأنظمة ال في إجراء تحقيق في حالة حدوث إختراق البيانات، كما تقوم السلطة الوطنية بالرقابة على مديرية أمن أنظمة المعلومات في مدى إلتزامها بإتخاذ التدابير بشأن حماية البيانات، وفي جهة أخرى يقوم بنك الجزائر بالرقابة على مديرية أمن أنظمة المعلومات في مدى إلتزامهم بالتعليمات و الأنظمة التي تعزز حماية للبيانات الشخصية للزبائن.

(1) République algérienne démocratique et populaire, ministère des postes et des télécommunications, **guide nationale référentiel de la sécurité de l'information** (2024) p202.

الشكل رقم (07): رسم تخطيطي يوضح المؤسسات المشرفة على حماية البيانات الشخصية في البنوك التجارية



المصدر: المخطط من تصور الطالبة بناء على الهياكل المنصوص عليها في النصوص القانونية (18-07، المرسوم الرئاسي 20-05، القانون 23-09.).

المبحث الثالث: الأليات التقنية لحماية البيانات الشخصية.

بهدف حماية وتأمين أنظمة المعلومات من مختلف التهديدات التي تمس بأمنها أصبحت الوسائل التقنية ضرورية لحماية نظم المعلومات والبيانات الشخصية، إذ هناك العديد من الوسائل التي تهدف على الحفاظ على أمن البيانات الشخصية والتي سيتم تناولها في هذا المبحث.

المطلب الأول: آلية التشفير و أنواعه.

1. **مفهوم التشفير:** التشفير أو كما يسمى بالتعمية، عرفه الدكتور محمد السويل بأنه " تحويل نص واضح أو مقروء إلى نص غير واضح أو نص معمى بطريقة تستطيع بواسطتها الأطراف المتعارف عليها فقط أن تحل التعمية وتحول النص الغير واضح أو المعمى إلى نص مقروء."[1] كما يعرف أيضا بأنها: "إخفاء المعلومات السرية بطريقة يصبح من خلالها معناها غير مفهوم بالنسبة إلى أي شخص غير مصرح له بالاطلاع عليها." [2] إذ يمر التشفير بمرحلتين أساسيتين هما الاولى تشفير النص الصريح وتحويله إلى رموز غير مفهومة أو مقروءة بلغة مفهومة وذلك باستخدام خوارزمية وعمليات رياضية والمرحلة الثانية: فك التشفير وهي إعادة النص المشفر إلى وضعه السابق كنص مفهوم ومقروء باستخدام خوارزمية فك التشفير والمفتاح السري الذي تكون مشركا بين المستقبل والمرسل. [3]

2. **أنواع التشفير:**

ينقسم التشفير إلى نوعين هما.

أ- التشفير المتماثل (SYMMETRIC ENCRYPTION):

يتم في هذا النوع من نظام التشفير باستخدام مفتاحا متناظرا يكون مشتركا بين المرسل والمستقبل، ويتم استخدام هذا المفتاح في عملية التشفير أي عند تحويل النص الصريح إلى رموز ويستعمل أيضا عند فك التشفير أي عند تحويل النص المشفر وإعادته إلى ما كان عليه سابقا باستخدام خوارزمية فك التشفير والمفتاح السري المشترك.

---

[1] ذيب بن عايض القحطاني، مرجع سابق، ص 108.

[2] فريد يابيروشون ميرفي، **علم التشفير مقدمة قصيرة جدا**، ترجمة: محمد سعد طنطاوي (جمهورية مصر العربية، مؤسسة هنداوي للتعليم والثقافة، ط1، 2012) ص 15.

[3] جمال بوزادية، مرجع سابق، ص75.

❖ النص الصريح: هو النص الأصلي الذي يتم إدخاله إلى خوارزمية التشفير.

❖ خوارزمية التشفير: تشمل خوارزمية التشفير مجموعة الخطوات التي يتم تطبيقها على النص الصريح لتحويله إلى صيغة مشفرة باستخدام المفتاح السري.

❖ المفتاح السري: وهو المفتاح الذي يكون مشتركا بين المستقبل والمرسل ويتم استخدامه لإنتاج النص المشفر وفك التشفير.

❖ النص المشفر: وهي الرسالة التي تنتجها خوارزمية التشفير في كل من النص الصريح والمفتاح السري.

❖ خوارزمية فك التشفير: مجموعة القواعد المستخدمة في فك النص المشفر وتحويله إلى نص مقروء وبصيغة مفهومة.

ولنجاح نظام التشفير المتناظر بمعنى الحصول على نظام تشفير آمن يجب أن يتوفر شرطين أساسيين وهما:

- استخدام خوارزمية تشفير قوية.
- توزيع المفتاح على المرسل والمستقبل بطريقته آمنة وسرية.

إذ تكمن قوة نظام التشفير بنوعيه في سرية المفتاح السري وقوته بحيث يجب أن يكون المفتاح مشركا فقط بين المستقبل والمرسل ولا يتم مشاركته خارج إطار هذين الشخصين. [1]

ب- التشفير الغير متماثل Asymmetric Encryption

يطلق عليه أيضا اسم التشفير بالمفتاح العام، يختلف هذا النوع من التشفير عن نظام التشفير المتماثل، كون التشفير الغير متماثل يتم استخدام مفتحان منفصلان لكل من المستقبل والمرسل أحدهما عام يستخدم للتشفير ويمكن الإطلاع عليه من قبل المستخدمين جميعا، والأخر خاص لفك التشفير لا يعلم به سوى المستقبل فقط. [2]

يتكون التشفير الغير متماثل من 6 مكونات رئيسية:

1) النص الصريح: النص الأصلي المراد تشفيره.
2) خوارزمية التشفير: مجموعة المطبقة على النص الصريح لتحويله إلى نص مشفر.
3) المفتاح عام: يمتلكه المستقبل والمرسل يستخدم التشفير، ويمكن لأي شخص الإطلاع عليه.

[1] ذيب بن عاض القحطاني، مرجع سابق، ص112 وص 113.

[2] عبد القادر صواق، مرجع سابق، ص .76

4) المفتاح الخاص: مفتاح خاص سري، يكون لكل طرف مفتاح خاص به، يستخدمه لفك التشفير الرسائل الواردة إليه.

5) النص المشفر: والرسالة التي تنتجها خوارزمية التشفير في كل من النص الصريح والمفتاح العام المرسل إليه.

6) خوارزمية فك التشفير: هي خطوات يتم تطبيقها لتحويل النص المشفر وإعادته إلى النص الأصلي.

المطلب الثاني: آليات تأمين الوصول إلى البيانات.

تتضمن آليات تأمين الوصول إلى البيانات مختلف الوسائل التي بموجبها بتم التأكيد من عدم تعرض البيانات للأخطار التي تتمثل في إمكانية الكشف عنها والإطلاع عليها من قبل أشخاص غير مخولين بذلك، [1] إذ تتألف آليات تأمين الوصول إلى البيانات من شقين:

1- الوسائل الأمنية للتعرف والتحقق من شخصية المستخدم:

هي الوسائل الهادفة إلى ضمان استخدام النظام أو الأشخاص من قبل الأشخاص المصرح لهم بذلك وتضم هذه الرسائل ما يلي:

- **كلمة المرور:** عبارة عن سلسلة من الأحرف تستخدم بهدف إثبات والتحقق من هوية المستخدم، [2] ويستحسن أن نستخدم كلمات المرور بطول 8 أحرف على الأقل، بمعنى ألا ترتبط بمعلومات شخصية للمستخدم مثل اسمه أو تاريخ ميلاده حتى لا تكون قابلة للاختراق وألا تكون طويلة لدرجة أنهم لا يستطيعون حفظها. [3]

- **بصمة الوجه:** هو عبارة عن برنامج إلكتروني يتم استخدامه في عملية التحقق من هوية المستخدمين عن طريق الوجه، إذ يقوم البرنامج بالتقاط صورة مباشرة لوجه المستخدم وتحليل معالم الوجه، ومقارنتها بالصورة المحفوظة سلفا، وإذا كان هناك تطابقا بالمقارنة مع الصورة الموجودة في قاعدة البيانات يرخص للمستخدم بالوصول. [4]

---

[1] فتيحة حزام، "حماية الأنظمة الرقمية بين الآليات التقنية وأجهزة الحماية قراءة في أحكام المرسوم الرئاسي 20-05"، **مجلة الحقوق والعلوم السياسية**، ع 3، (أكتوبر 2020)، ص. 174.

[2] جمال بوازيدية، مرجع سابق، ص. 74.

[3] أسامة حسام الدين، مرجع سابق، ص. 91.

[4] هيام إسماعيل، عبد الفتاح السحماوي، "بصمة الوجه الإلكتروني وحجيتها في الإثبات المدني دراسة مقارنة"، **مجلة البحوث القانونية والاقتصادية**، م2، ع 2، (يوليو 2023)، ص. 24.

- **بصمة الأصابع:** بصمة الأصبع هي بصمة فريدة لكل فرد، تعمل هذه التقنية من خلال التقاط صورة لبصمة الأصبع من خلال أجهزة تسمى بمستشعرات بصمات الأصابع، بحيث يقوم المستخدم بوضع إصبعه على جهاز الإستشعار، ثوم يقوم هذا الأخير بالتقاط صورة لإصبع المستخدم ويقوم بمقارنتها بالصورة المخزنة في قاعدة البيانات إذا كان هناك تطابق مع الصورة الملتقطة سابقا، يرخص للمستخدم بالدخول. (1)

- **الأقفال الإلكترونية:** توفر هذه التقنية مستوى من الحماية للبيانات الشخصية، إذ تستخدم الأقفال الإلكترونية تقنيات مثل أدوات التعرف البيولوجي كالبصمة، التعرف على إصبعه الأصابع، وإدخال رموز السرية او كود عبر لوحة مفاتيح مثبتة على الأبواب ما يسهل على المستخدم إذا كان مصرحا له بالدخول بكل سهولة. (2)

2- وسائل التحكم في الوصول إلى البيانات:

بعد التأكد من شخصية المستخدم يأتي بعدها الشق الثاني المتمثل في وسائل التحكم في الوصول إلى البيانات إذ يركز هذا الجانب على القدرة على حماية هذه البيانات من خلال التأكد من كل طلب للدخول إلى البيانات إذا كان مسموحا به لهذا المستخدم أم لا، تتمثل وسائل التحكم بالوصول إلى البيانات في مجموعة من التقنيات من بينها:

- **مصفوفة الدخول (Access Matrix):** وهي من الوسائل المشهورة للتحكم في الدخول إلى البيانات، بحيث يتم في هذه المصفوفة تنظيم العلاقات بين أجزاء النظام على هيئة مصفوفة ثلاثية(S,O,A) حيث تمثل:

S : تمثل الكيانات الفعالة (**ACTIVE INTITIES**) للنظام وهي اختصار (**subjects**)وبمعنى آخر تمثل مستخدمي النظام (**users**).

O: اختصارا (**Objects**) وهي تشمل على الأشياء المطلوب حمايتها مثل الملفات والبرامج ووسائط التخزين ...الخ.

(1) *La République Française, Club de la Sécurité des systèmes D'information Française,* ***Technique contrôle d'accès par biomiterie2003,*** *p9.*

(2) *ALLAL Mohammed Racim et Bouayad DEBBAGH,* ***Etude et réalisation d'une serrure Electronique****, mémoire de master (université Aboubakar, Belkaid-Telmcen, Faculté de technologie,2022/2023.) p 8,9.*

A: تمثل وحدات المصفوفة حيث أن الوحدة تعطي حق أو امتياز تنفيذ عملية معينة مثل الكتابة أو القراءة من الكيان**(s) إلى الكيان(O)**.[1]

- **تسجيل الدخول الواحد (single sign-on)** اختصرت تقنية تسجيل الدخول الواحد الكثير من الوقت على مديري الشبكات الأنظمة، فبدلا من أن يقوم المستخدم بحفظ عدد كبير من كلمات المرور عند رغبته في الدخول إلى أي من تلك الأنظمة أو الشبكات فمثلا قد ينسى المستخدم كلمة المرور الخاصة به أو يخلط فيما بينها، هذا ما يدفع إلى إلغاء جميع كلمات المرور الخاصة بذلك المستخدم، ومن هنا ظهرت فكرة استخدام هذه التقنية حيث يدخل المستخدم مرة واحدة من خلال نظام مخصص لهذا الغرض وبعدها يمنح الترخيص للموظف الوصول إلى المباني والأنظمة والتطبيقات المعنية وفقا للصلاحيات المخولة له. [2]

المطلب الثالث: الحماية من البرمجيات الخبيثة.

تتضمن الحماية من البرمجيات الخبيثة مختلف التقنيات التي تهدف إلى حماية البيانات الشخصية من مختلف التهديدات بما فيها البرمجيات الخبيثة وتتمثل هذه الوسائل في:

❖ **برامج مكافحة الفيروسات**: هو برنامج يقوم باكتشاف الفيروسات الموجودة على جهاز الكمبيوتر والقضاء عليها ويتخذ الخطوات اللازمة لمنعها من التسبب في الضرر[3] كما يعرف أيضا بأنه برنامج أمان مصمم لمنع الفيروسات وأنواع أخرى من البرامج الضارة واكتشافها وفحصها وإزالتها من أجهزة الكمبيوتر والشبكات والأجهزة، التهديدات السيبرانية بما في ذلك أحصنة طروادة، الديدان وغيرها، [4] إذ يتم تثبيت برنامج مكافحة الفيروسات على الكمبيوتر مثل أي برنامج كلاسيكي آخر، وعند تثبيته يتم تشغيله ويقوم بفحص أجهزة الكمبيوتر للكشف عن البرامج الضارة للحد من انتشارها و تتضمن العديد من برامج مكافحة الفيروسات اكتشاف التهديدات والحماية في الوقت الفعلي من الثغرات الأمنية المحتملة واجراء عملية فحص للنظام لمراقبة الجهاز، وعند فحص برنامج مكافحة الفيروسات لأجهزة الحاسوب ويكتشف

---

[1] محمد فهمي طلبة، **فيروسات الحاسوب وأمن البيانات**، (جمهورية مصر العربية، مطابع المكتب المصري الحديث، 1997)، ص. 235.

[2] ذيب بن عائض القحطاني، مرجع سابق، ص. 170.

[3] *Salma Bahaza et tidjani Mammeri, **Déploiement d'une solution Antivirus sein du réseau de campus universitaire Ouargla**, mémoire de master, non publier, (université Kasdi Merbah Ouargla, faculté des nouvelles technologies de l'information de la communication, 2024/2015) p 12.*

[4] *Nesrine Adad, **La mise au point d'un antivirus**, Mémoire de Master, non publier, (université Abou Baker Belkaid-Telmcen, Faculté des sciences Département D'informatique,2015/2016) p23*

بأن هناك برنامج ضار يقوم إما بإزالته تلقائيا أو إخبار المستخدمين بالعدوى وحثهم على تنظيف الملفات. (1)

❖ **الجدران النارية:**

هي مجموعة من المكونات المختلفة للأجهزة (المادية) والبرامج التي تتحكم في حركة المرور الداخلية والخارجية للبيانات وفقا لسياسة الأمن،[2] كما يعرف أيضا بأنه برنامج أو جهاز يقوم بفحص المعلومات القادمة من الانترنت أو الشبكة ثم يمنعها من الوصول إلى الكمبيوتر أو يسمح لها بذلك اعتماد على إعدادات جدار الحماية للمستخدم، [3] إذ تهدف هذه الجدران النارية أولا إلى تصفية كل حركة مرور متبادلة مع الشبكة الخارجية والسماح فقط لحركة المرور المصرح بها المرور، إذ يتم استخدام جدار الحماية في كثير من الأحيان لمنع تسرب المعلومات وبالتالي فهو يمثل سيطرة حقيقية على حركة المرور لشبكة المنشآت والمؤسسات لأنه يوفر القدرة على التحكم في الوصول إلى أنظمة الموقع المحمي. [4]

- **نظام كشف التسلل (*intrusion detection system*) :**

يقصد بنظام كشف التسلل مجموعة من مكونات البرامج أو الأجهزة التي تمثل وظيفتها الرئيسية في اكتشاف وتحليل الأنشطة الغير الطبيعية أو المشبوهة التي تحدث في الشبكة وبالتالي فإنه يوفر المعرفة بمحاولات الاختراق الناجحة والفاشلة، [5] كما يعرف أيضا بأنه برنامج أو جهاز يعمل على أنظمة المراقبة واكتشاف علامات التطفل ثم وضعها بحكمة على الشبكة أو النظام لأنظمة المراقبة و تحديد الأنشطة المشبوهة أو غير الطبيعية على هذا الهدف وتنبيه مديري الأمن وبهذه الطريقة يمكن الحصول على معلومات حول المحاولات الناجحة أو غير الناجحة لمهاجمة النظام و التطفل عليه، [6] هناك نوعان رئيسان من أنظمة كشف التسلل وهما:

أ- **نظام كشف التسلل القائم على الشبكة(*Network IDS*) :**

---

(1) *LINDA Rosencrance and kinza Yaser, antivirus (anti-malware) dans: https://www.Lemagit.fr/definition/antivirus-anti-malawer , (15/05/2025).*

(2) *Nessrine Hadad, op.cit, p. 19.*

(3) *Selma Bahaza et Tidjani Mammeri, op.cit, p19*

(4) *Nessrine Hadad, op.cit, p19.*

(5) *Embarka ben Brahim et selyana Amiche, **mise place d'une solution de détection d'intrusion**, mémoire de master (faculté de génie Electrique et informatique, université Mouloud Mammeri de Tizi-Ouzou, 2017) , p51.*

(6) *El Gharbi Selmani, **mise en place d'un IDS pour sécuriser un réseau en utilisant snort**, mémoire de master (faculté de génie électrique et d'informatique, université Moloud mammeri Tizi-ouzou, 2019/2020) p32.*

هي أنظمة كشف التسلل مخصصة للشبكة، وهي تمثل عادة جهاز يستمع إلى جزء الشبكة المراد مراقبتها وجهاز استشعار ومحركا يقوم بتحليل حركة نقل البيانات للكشف عن الافتراضات في الوقت الفعلي، وبالتالي يتابع نظام (NIDS) جميع البيانات المارة في الوسط الناقل ثم يقوم بتحليلها وإنشاء تنبيهات إذا ظهرت أي حزم خطيرة. [1]

ب-نظام كشف التسلل القائم على المضيف *(HOST BASED IDS (HIDS)*

يراقب نظام كشف التسلل القائم على المضيف تشغيل أو حالة الجهاز الذي تم تثبيته عليه، من اجل اكتشاف الهجمات، إذ يقوم بتحليل المعلومات المتعلقة بهذا المضيف حصريا مع التحقق من سجلات النظام ويدرس سلامة أنظمة الملفات إذ يركز هذا النوع على أنشطة المضيف وليس على حركة مرور الشركة. [2]

- **نظام منع التسلل *(les systèmes de prévention d'intrusion)***

هو مكون برمجي ومادي وظيفته الأساسية هي منع أي نشاط مشبوه يتم اكتشافه داخل النظام، فهو في عمله بشبه كثيرا نظام كشف التسلل إذ يقوم بالتقاط حركة المرور على الشبكة ثم يقوم بتحليلها، ولكن بدلا من تنبيه المستخدم إلى وجود تسلل أو هجوم، يتفاعل نظام اكتشاف التسلل تلقائيا دون تدخل المستخدم ويمنع التسللات بشكل مباشر عن طريق إسقاط الحزم الغير المشروعة لإعلام المستخدم. [3]

المطلب الرابع: آليات ضمان سلامة البيانات.

تتضمن اليات سلامة البيانات مختلف الوسائل التي تهدف إلى حماية البيانات الشخصية من التلاعب أو التغيير الغير المصرح به والتي تتمثل في:

أ- التصديق (التوقيع الرقمي):

يستخدم التوقيع الرقمي للتحقق من هوية أصل البيانات والمعلومات، كذلك يستخدم لإثبات المعلومات، تعمل تقنية التصديق الرقمي من خلال توقيع المرسل على رسالة باستخدام مفتاح سري، ثم بعدها يقوم بإرسالها وبعدها يقوم المستقبل بتلقي الرسالة ويقوم المستقبل بالتحقق من صحة التوقيع باستخدام المفتاح العام للموقع وهذا بهدف التحقق من صحة التوقيع، إذ يتكون التصديق الرقمي من عمليتين أساستين:

- **التوقيع:** وهو عملية إنتاج التصديق الرقمي، ومدخلاتها هي الرسالة: الرسالة والمفتاح السري للموقع.

(1) *Embarka ben Brahim et selyana amiche, Op; cit, p. 42.*

(2) *Elgharbi selmani, op.it, p19.*

(3) *Elgharbi selmani, op.it,p39 et 40.*

- **التحقق من صحة التوقيع: هي** عملية التحقق من أن التوقيع تم من الشخص المعني على الرسالة المعنية، ومدخلاتها هي: الرسالة والمفتاح العام للموقع، ونتيجتها إحدى حالتين: إما مطابق، أو غير مطابق.[1]

ب-البصمة الرقمية:

تعرف البصمة الرقمية أيضا باسم التشفير باتجاه واحد تقوم هذه التقنية على تشفير رسالة بإستخدام مفتاح الشفرة بحيث يتميز هذا المفتاح بأنه لا توجد طريقة فيه لفك التشفير والحصول على الرسالة الأصلية منه، البصمة الرقمية او التشفير باتجاه واحد تستخدم في أغلب الأحيان في التوقيع(التصديق) الرقمي للتأكد من صحة البيانات المنقولة، كما تستخدم البصمة الرقمية للتحقق من عدم تلاعب بالبيانات أو ملفات معينة، فمثلا إذا تلقى المستقبل رسالة فهناك إحمال أن يكون قد تم التلاعب بها عمدا، فهذا يستلزم ان يتم التأكيد من تطابق نسخة الرسالة التي وصلت مع الرسالة الأصلية. (2)

[1] عبد القادر صواق، مرجع سابق، ص ص. 76 - 78.

(2) فتيحة حزام، مرجع سابق، ص. 180.

خلاصة الفصل الثاني:

تناول هذا الفصل الإطار العام لحماية البيانات الشخصية في الجزائر، حيث تم التركيز في المبحث الأول على الجانب المؤسساتي من خلال عرض الهيئات الوطنية المشرفة على حماية البيانات الشخصية في الجزائر في مقدمتها المنظومة الواقعة تحت رئاسة الجمهورية، المنظومة التابعة لوزارة الدفاع الوطني، منظومة الأمن الوطني ووزارة البريد والمواصلات السلكية واللاسلكية، ثم لننتقل بعدها إلى المبحث الثاني الذي يستعرض المؤسسات المشرفة على حماية البيانات الشخصية في البنوك التجارية في مقدمتها السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، وكالة أمن الأنظمة المعلوماتية، وزارة البريد والمواصلات السلكية واللاسلكية، بنك الجزائر وفي الأخير مديرية أمن أنظمة المعلومات، وأخيرا تم عرض الفصل الثالث الذي يسلط الضوء على أهم الآليات التقنية لحماية البيانات الشخصية المتمثلة في آلية التشفير، آليات تأمين الوصول إلى البيانات، الحماية من البرمجيات الخبيثة، آليات ضمان سلامة البيانات.

الفصل الثالث:

دراسة حالة البنك الخارجي الجزائري

تمهيد:

بعد ما تم التعرض إلى الإطار المفاهيمي للأمن السيبراني والبيانات الشخصية، والتعرف على إستراتيجية حماية البيانات الشخصية في الجزائر، سيتم في هذا الفصل الاطلاع على آليات حماية البيانات الشخصية في البنك الخارجي الجزائري بتبني أسلوب دارسة الحالة كأحد الأساليب الهامة التي يستخدمها المنهج الوصفي والتحليلي الذي تم اعتماده في هذه الدراسة.

لذا قسم الفصل الثالث إلى ثلاث مباحث هي:

المبحث الأول: تقديم عن البنك الخارجي الجزائري.

المبحث الثاني: اليات البنك الخارجي الجزائري في حماية البيانات الشخصية.

لمبحث الثلث: تقييم إستراتيجية حماية البيانات الشخصية في الجزائر.

المبحث الأول: تقديم عن البنك الخارجي الجزائري

يقدم هذا المبحث نظرة شاملة حول البنك الخارجي الجزائري، حيث يتضمن نشأة البنك ووظائفه وهيكله التنظيمي إضافة إلى الخدمات المصرفية التي يقدمها لعملائه.

المطلب الأول: تعريف بالبنك الخارجي الجزائري.

تأسس البنك الخارجي الجزائري بموجب الأمر رقم 64-204 المؤرخ في جمادى الثانية 1387 الموافق لـ 1 أكتوبر 1967، وهذا هو ثالث وآخر بنك يتم تأسيسه تبعا لقرارات تأميم القطاع البنكي.[1]

بلغ رأس ماله حسب الأمر رقم 67-204 20 مليون دينار جزائري ليرتفع إلى 150 مليار دينار جزائري وفي 2019 بلغ رأس مال البنك الخارجي الجزائر إلى 230 مليار دينار جزائري بعد ترخيص من مجلس النقد والقرض[2]مقره الاجتماعي بشارع 17 العقيد عميروش بالجزائر العاصمة.

يملك البنك الخارجي الجزائري شبكة لـ 110 وكالة منتشرة في التجمعات الحضارية الكبرى ومناطق الصناعة.[3]

المطلب الثاني: وظائف البنك الخارجي الجزائري.

- وضع وكلات وفروع في الخارج بهدف تطوير توسع التجارة الجزائرية.
- يمكنها تنفيذ كل العمليات المصرفية الداخلية والخارجية التي تتلائم مع هدفه.
- يقدم الخدمات المطلوبة من طرف الزبائن.
- يقوم البنك الخارجي الجزائري بدور الوسيط في تنفيذ العمليات التجارية مع الدول الأجنبية.
- تسهيل وتطوير العلاقات الاقتصادية بين الجزائر والدول الأخرى.
- بالإضافة إلى تمويلاتها الخاصة فإنها تتدخل بالاحتياطي وضمان الوفاء أو حتى باتفاقات القرض مع مراسلين أجانب لترقية الصفقات التجارية مع دول أخرى.

[1] الجمهورية الجزائرية الديمقراطية الشعبية، البنك الخارجي الجزائري، في: https://www.bea.dz/article، بتاريخ (20225/5/17).

[2] بنك الخارجي لجزائري يرفع رأسماله إلى 230 مليار دينار جزائري، في: https://www.aps.dz/ar/economie، تاريخ الإطلاع (2025/5/17).

[3] الجمهورية الجزائرية الديمقراطية الشعبية، البنك الخارجي الجزائري، مرجع سابق.

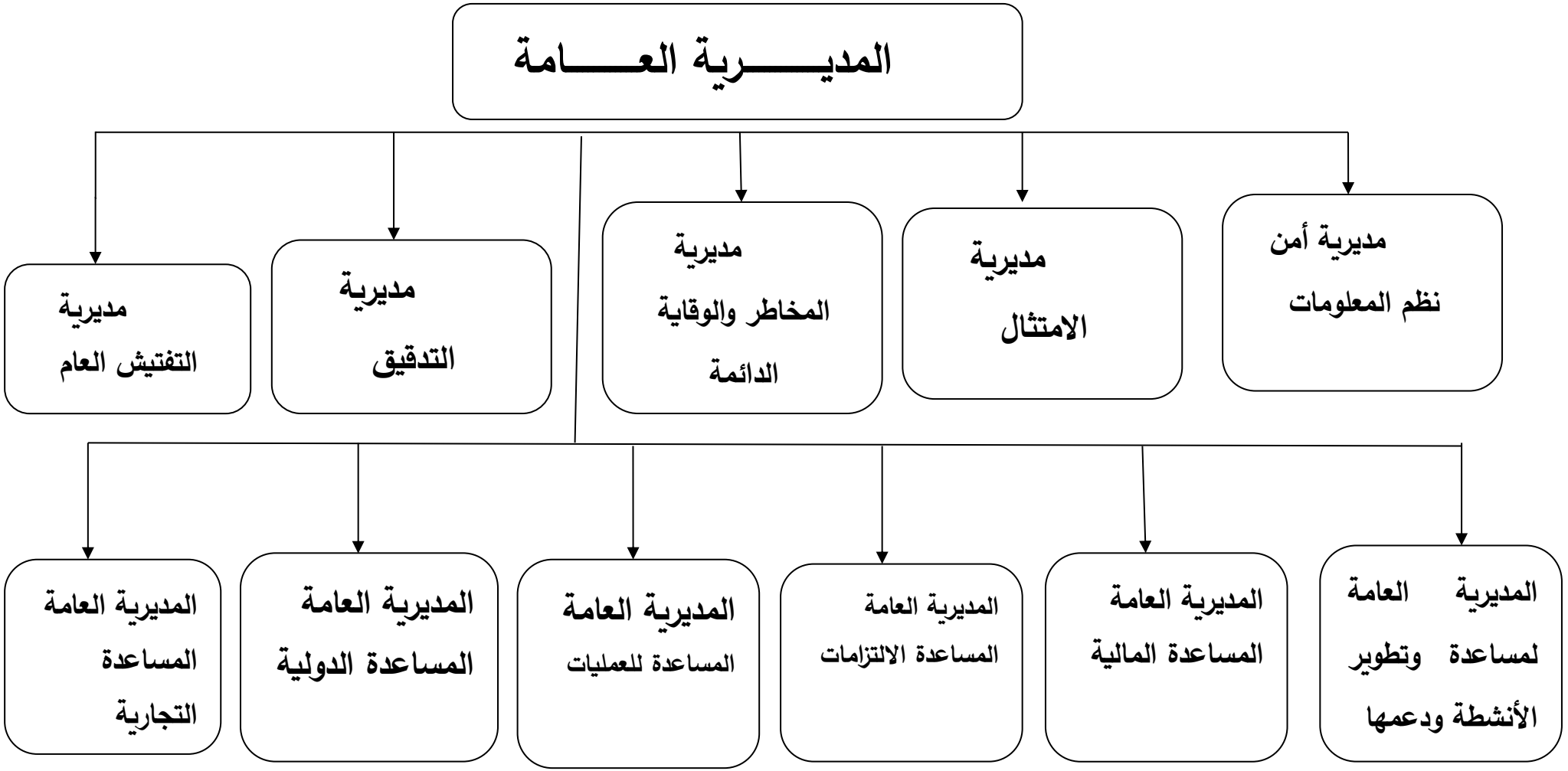
- تشارك في كل نظام مؤسسة تأمين للتعامل الخارجي ويمكن لها أن تكلف بالتسيير والمراقبة مع الخارج.[1]

المطلب الثالث: الهيكل التنظيمي للبنك الخارجي الجزائري.

نظرا للتحفظ التي أبدته السلطة العليا ازاء تقديم معلومات تفصيلية حول التنظيمي الهيكلي والفعلي لمديرية الأمن المعلوماتي تم الاكتفاء بالتنظيم الهيكلي العام للبنك الخارجي الجزائري لسنة 2023، إذ لم تكن المديرية أمن نظم المعلومات ضمن الهيكل التنظيمي آنذاك وتم استحداثها لاحقا في سنة 2024 تماشيا مع التطورات والمتطلبات الجديدة في مجال حماية الأنظمة والمعلومات.

[1] الجمهورية الجزائرية الديمقراطية الشعبية، الأمر رقم 67 – 204، المؤرخ في 26 جمادى الثانية 1387 الموافق ل 1 أكتوبر 1967، المتضمن إحداث بنك الجزائر الخارجي، الجريدة الرسمية، العدد86، الصادر في 2 رجب 1387، المادة 1.

شكل رقم (08): الهيكل التنظيمي للبنك الخارجي الجزائري.



المصدر: موقع البنك الخارجي الجزائر، في: https://www.bea.dz/article، تاريخ الاطلاع: (20225/5/17).

المطلب الرابع: الخدمات المصرفية الإلكترونية التي يقدمها البنك الخارجي الجزائري.

تعد الخدمات المصرفية أحد الركائز المهمة لدى القطاع البنكي، إذ تعد أحد العوامل الرئيسية لاستقراره واكتسابه سمعة ومصداقية وذلك ناتج عن جودة الخدمات التي يقدمها فبفضل هاته الخدمات يمكن فهم آليات سير البنوك ومساهمتها في دعم النشاط الاقتصادي وعلى هذا السياق سنتمكن من تلخيص بعض الخدمات المصرفية التي يقدمها البنك الخارجي الجزائري والمتمثلة في:

- **التحويلات المالية:**

تتيح هذه الخدمات للعملاء إرسال واستقبال الأموال عبر الحدود بسرعة وبأمان باستخدام نظام SWIFT، الذي يضمن تحويل الأموال من البنوك في مختلف الدول، إذ تمكن الشركات من دفع الفواتير واستلام المدفوعات من شركاؤها التجاريين.[1]

- **الدفع الإلكتروني:**

يوفر البنك الخارجي الجزائري مجموعة متنوعة من البطاقات الدولية والمحلية لتلبية احتياجات عملاءه، من بين هذه البطاقات نجد:

أ- البطاقات المحلية وتتضمن:

- البطاقة الكلاسيكية *CARTE CIB CLASSIQUE*
- البطاقة الذهبية *CARTE CIB GOLD*

ب- البطاقات الدولية وتتضمن:

- البطاقة الكلاسيكية *CARTES CLQSSIQUE*
- بطاقات الدفع المسبق *CARTES PREPAYEE*
- البطاقة البلاتينية *CARTES PLATINUM*
- بطاقات العملCARTES BUSINESS
- بطاقات الأعمال العالمية *CARTES WORLD BUSINESS*

ت- البطاقات الأمريكية وتتضمن:

- البطاقات البلاتينية *CARTES PLATINUM*

[1] فاتح مرزوق وياسين عطا الله، "الخدمات المصرفية ودروها في تسهيل التجارة الخارجية دراسة حالة بنك الخارجي الجزائري BEA"، **مجلة الجغرافيا الاقتصادية**، م (02)، ع (01)، (2025) 46.

- البطاقات الذهبية *CARTES GOLD*
- البطاقات الخضراء *CARTES GREEN*

أ- تطبيق MA BANQUE MOBILE لإدارة حسابات العملاء.

هو تطبيق يوفره البنك الخارجي الجزائري لزبائنه لتمكنهم من إدارة حساباتهم والإطلاع عليها، يوفر هذا التطبيق العديد من المزايا من بينها:

- إدارة البطاقة المصرفية للعملاء وإمكانية طلب بطاقة بنكية في دقائق معدودة.
- الوصول إلى رقم التعريف المصرفي RIB بسهولة أكبر.
- إتباع سعر الصرف باستخدام محمول العملات الخاص بالزبون.
- إجراء التحويلات عبر الانترنت.
- الاتصال بفروع الوكالات التابعة للبنك الخارجي الجزائري.
- عرض أرصدة الحسابات والمعاملات الأخيرة للزبون.[1]

ب- التمويل الإلكتروني:

يقدم البنك الخارجي الجزائري للعملاء قروض وتسهيلات ائتمانية عبر الأنترنت، تمكن للشركات من بطلب للحصول على تمويل لمشاريعها التجارية أو لتمويل عملياتها اليومية دون الحاجة إلى زيارة الفروع البنكية، مما يوفر الوقت ويسرع عملية الحصول على التمويل.[2]

[1] الجمهورية الجزائرية الديمقراطية الشعبية، البنك الخارجي الجزائري، مرجع سابق.

[2] فاتح مرزوق وياسين عطا الله، مرجع سابق، ص67.

المبحث الثاني: آليات البنك الخارجي الجزائري في حماية البيانات الشخصية.

يعتمد البنك الخارجي الجزائري على مجموعة من الآليات المؤسساتية، القانونية، والتقنية والتنظيمية التي تهدف إلى حماية البيانات الشخصية من أي تهديد وخطر يمس بأمنها وسلامتها.

المطلب الأول: الآليات القانونية للبنك الخارجي الجزائري في حماية البيانات الشخصي.

من خلال المقابلة التي أجريت مع مدير أمن أنظمة المعلومات بتاريخ 2025/2/10 على الساعة: 9:30 توصلت النتائج إلى أن البنك الخارجي الجزائري يعتمد على مجموعة من القوانين لضمان حماية البيانات الشخصية والحفاظ على سيرتها، ومن بين القوانين التي يلتزم بها البنك في مجال حماية المعطيات ذات الطابع الشخصي:

نجد القانون 18-07 الصادر في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي ويتجلى مظاهر الالتزام البنك بأحكام القانون 18-07 من خلال احترام مسؤول المعالجة للحقوق التي يتمتع بها الشخص المعني والتي من بينها: الحق في الإعلام، الحق في الولوج، الحق في التصحيح، الحق في الاعتراض ومنع الاستكشاف المباشر،[1] كما لا يقوم بأي معالجة للبيانات دون الحصول على تصريح أو ترخيص مسبق تسمح له بذلك[2]، علاوة على ذلك يضع البنك الخارجي الجزائري لتطبيق ما جاءت المادة 38 من نفس القانون مختلف التدابير التقنية و التنظيمية الملائمة لحماية المعطيات ذات الطابع الشخصي من الإتلاف العرضي أو الغير المشروع،[3] كما يلتزم البنك أيضا باختيار معالج من الباطن يقدم الضمانات الكافية المتعلقة بإجراءات السلامة التقنية والتنظيمية للمعالجات الواجب القيام بها ويسهر على احترامها،[4] كذلك التزامه بالسر المهني بمناسبة إطلاعه على معطيات ذات طابع شخصي[5] وإضافة إلى هذا الإطار القانوني، فقد وضع البنك نظام داخلي وهو وثيقة يضعها تحدد

[1] الجمهورية الجزائرية الديمقراطية الشعبية، القانون 18-07، مرجع سابق، المادة 36،35،34،32 و37.

[2] المرجع نفسه، المادة15.

[3] المرجع نفسه، المادة 38

[4] المرجع نفسه، المادة 39.

[5] المرجع نفسه، المادة 40.

القواعد المتعلقة بالسلامة داخل البنك وتحدد العقوبات المفروضة في حال عدم الامتثال لهذه الوثيقة، يتضمن النظام الداخلي بصفة عامة القواعد الواجب احترامها في مجال حماية المعطيات ذات الطابع الشخصي من بينها التحكم في الوصول إلى الأنظمة و منع أي شكل من الوصول غير المصرح به من طرف الموظفين، و في حال حدوث انتهاك لمقتضيات القانون الداخلي يعاقب الموظف بموجب هذا القانون،[1] لكن للاطلاع على تفاصيل محتويات الوثيقة لم يكن متاح بحكم أن هذه الوثيقة هي سرية ولا يمكن مشاركتها خارج إطار الموظفين لذلك تم الاكتفاء فقط بشرح عام لمقتضيات النظام الداخلي للبنك بصفة عامة.

المطلب الثاني: الآليات المؤسساتية للبنك الخارجي الجزائري في حماية البيانات الشخصية.

من خلال المقابلة التي أجريت مع السيدة أيت زيان مريم، مهندسة في أمن أنظمة المعلومات بالبنك الخارجي الجزائري بتاريخ 17 فيفري 2025، توصلت النتائج إلى أن البنك الخارجي الجزائري يمتلك هياكل مؤسساتية لضمان حماية البيانات الشخصية والتي تضم.

- **مسؤول أمن نظم المعلومات (RSSI):**

تنفيذا لمقتضيات المرسوم الرئاسي 20-05 المتعلق بوضع منظومة وطنية الأنظمة المعلوماتية التي نصت على التزام كل المؤسسات والإدارات والهيئات العمومية والمتعاملون الخواص بتعيين مسؤولهم المكلف بأمن الأنظمة المعلوماتية في أجل أقصاه سنة، تم تعيين مسؤول عن أمن الأنظمة المعلوماتية على مستوى بنك الخارجي الجزائري يكلف بمجموعة من المهام من بينها ضمان حماية البيانات الشخصية وفقا لما تقضيه أحكام القانون 18-07 من خلال احترام حقوق المعني أثناء المعالجة وتنفيذ الالتزامات بوصفه مسؤول عن المعالجة.

- **مديرية أمن الأنظمة المعلومات (DSSI):**

تتواجد على مستوى بنك الخارجي الجزائري مديرية تعنى بمسألة أمن المعلومات ويترأس هذه المديرية مسؤول مكلف بأمن نظم المعلومات يسمى "مدير أمن الأنظمة المعلومات "ويقوم في هذا السياق بمجموعة من المهام من بينها وضع التدابير الأمنية والتقنية لحماية البيانات الشخصية،[2] إضافة إلى مهام أخرى تضمنها المرجع الوطني لأمن المعلومات.[3]

- **السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي (ANPDP):**

[1] معلومات مقدمة من طرف السيدة أيت زيان مريم، مهندسة في أمن أنظمة المعلومات، البنك الخارجي الجزائري.

[2] مقابلة مع السيدة أيت زيان مريم، مهندسة في أمن أنظمة المعلومات بالبنك الخارجي الجزائري، بتاريخ 17 فيفري 2025، على الساعة 9:30.

[3] *République algérienne démocratique et populaire, ministère des postes et des télécommunications, **guide nationale référentiel de la sécurité de l'information**, op,cit, p18.*

لا تعتبر السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي من بين الهياكل المؤسسية للبنك الخارجي الجزائري بل هي سلطة وطنية مستقلة أنشئت بموجب القانون 18-07 تتولى مهام الإشراف والسهر على تطبيق أحكام القانون 18-07، إلى جانب مهام أخرى تضطلع بها منها المراقبة والتدقيق، كما تعتبر جهة رقابية تراقب مدى التزام المسؤولين عن المعالجة بوضع التدابير التقنية والأمنية لحماية البيانات الشخصية من مختلف المخاطر التي تمس سلامتها[1] فمن خلال الصلاحيات المخولة لها والممنوحة لها في نفس القانون تقوم بممارسة الرقابة على البنوك بما فيها البنك الخارجي الجزائري في مدى التزامه وامتثاله مع متطلبات القانون 18-07 بما فيها احترام المسؤول المعالجة لحقوق المعني للمعالجة ومعالجة البيانات بترخيص من السلطة،[2] كما تقوم بالتدقيق والتحقيق في حالة حدوث اختراق وتسرب للبيانات وبالتالي السلطة الوطنية ليست ضمن الآليات المؤسساتية للبنك الخارجي الجزائري بل تقوم بالتنسيق مع البنك الخارجي الجزائري في مجال حماية المعطيات ذات الطابع الشخصي.[3]

- **وكالة أمن الأنظمة المعلوماتية:**

هي مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلال المالي تضطلع وكالة أمن الأنظمة المعلوماتية بمجموعة من المهام من بينها تنسيق تنفيذ الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية المحددة من قبل المجلس، تحضير عناصر الإستراتيجية الوطنية في مجال أمن الأنظمة المعلوماتية وعرضها على المجلس[4] كما تقوم وكالة أمن الأنظمة المعلوماتية بحكم أنها مؤسسة عمومية بالتنسيق مع البنك الخارجي الجزائري من خلال إجراء تحقيقات رقمية في حال حدوث اختراق أو حوادث سيبرانية تمس بأمن البيانات.[5]

المطلب الثالث: الآليات التقنية للبنك الخارجي الجزائري في حماية البيانات الشخصية.

من خلال المقابلة التي أجريت مع السيدة ايت زيان مريم بتاريخ 5 مارس 2024 توصلت النتائج التالية: إستنادا على أحكام المادة 38 من القانون 18-07، التي تلزم مسؤولين المعالجة بوضع تدابير

[1] الجمهورية الجزائرية الديمقراطية الشعبية، السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، النظام الداخلي للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي (جويلية 2023)، ص15.

[2] االجمهورية الجزائرية الديمقراطية الشعبية، النظام الداخلي للسلطة الوطنية لحميات المعطيات ذات الطابع الشخصي، مرجع سابق، المواد53،51،48،46.

[3] مقابلة مع السيدة أيت زيان مريم، مهندسة في أمن أنظمة المعلومات بالبنك الخارجي الجزائري، بتاريخ 17 فيفري 2025، على الساعة 9:30.

[4] الجمهورية الجزائرية الديمقراطية الشعبية، المرسوم الرئاسي 20-05 مرجع سابق، المادة 17و 18.

[5] مقابلة مع مدير أمن أنظمة المعلومات بالبنك الخارجي الجزائري، بتاريخ المعلومات التي أجريت بتاريخ 2025/2/10 على الساعة 9:30.

أمنية وتقنية لتأمين البيانات الشخصية، بادر البنك الخارجي الجزائري إلى اعتماد جملة من الآليات والتقنيات التي تهدف إلى تأمين وحماية البيانات الشخصية، إذ تنقسم هذه الآليات إلى قسمين:

القسم الأول: يتمثل في الأمن المادي *la sécurité matérielle*:

هو مجموعة الإجراءات الأمنية التي تهدف لضمان عدم الوصول غير المصرح لهم إلى المعدات الخاصة والمواد بمراكز البيانات،[1] تتألف إجراءات الأمن المادي من:

1- **تأمين مراكز البيانات (*sécurisation des centres de donnée*)** تتواجد مراكز البيانات في مواقع إستراتيجية بعيدا عن المدن الكبرى، وهذا جزء من الأمن المادي لأن تواجده في موقع بعيد يزيل العديد من التهديدات المادية، لكن هذا البعد يعد غير كافيا لحماية مراكز البيانات،[2] ضوابط تتمثل في:

❖ **الوصول المقيد (*Accès restent*):**

ويعني أنه يسمح فقط للأشخاص المصرح لهم بالوصول إلى مناطق أو معلومات معنية، فهو اجراء أمني يستخدم لمنع الوصول غير المصرح به وحماية الأصول القيمة.[3]

❖ **المراقبة بالفيديو (*surveillance vidéo*)**

تتكون المراقبة بالفيديو من نظام من الكاميرات والشاشات وأجهزة التسجيل والتي يمكنها التقاط الصور ومقاطع الفيديو لحماية مراكز البيانات، بحيث يعمل نظام المراقبة بالفيديو على تأمين وحماية مراكز البيانات من خلال منع فقدان البيانات والخروقات فبمساعدة المراقبة بالفيديو من الممكن بسهولة مراقبة من يدخل إلى أي منطقة وماهي أنشطة التي يقوم بها بمجرد دخوله.[4]

❖ **التحكم البيومتري (*contrôle biométrique*):**

هو استخدام خصائص بيولوجية فريدة مثل التعريف بالمستخدم والسماح له بالوصول المصرح به إلى الأنظمة أو المرافق أو الأجهزة من بين هذه الخصائص البيولوجية.

أ- **بصمة الوجه:**

---

[1] الهيئة الوطنية لامن وسلامة المعلومات، سياسة الأمان المادي، فـي: https://nissa.gov.ly/main-services/pysical بتاريخ (2025/05/17).

[2] *Tout Savoir Sur La Sécurité des datacenters (centre de donnés) https://www.proofpoint.com/fr/threat-reference/data-center-securite, (17/05/2025).*

[3] *john sileo, garantir la protection des information sensibles, dans :https://www.oodrive.com/fr/guide/diffusion-restreinte, (17/05/2025).*

[4] *Guide Complet du contrôle d'accès biométrique, dans https://sirixmonitoring.com/fr/blog/guide-du-controle-dacces-biometrique, (17/05/2025).*

تستخدم في نظام التحكم البيومتري من خلال التعرف على الوجه بشكل متكرر لتحديد هوية المستخدمين، يقوم هذا النظام بالتقاط شكل وجه الشخص واستخراج خصائص معينة اعتمادا على النظام المستخدم، بحيث يسمح هذا النظام بتحديد هوية المستخدم باستخدام كاميرا مراقبة فيديو تكون موضوعة عند مدخل مركز البيانات أو منطقة آمنة يقوم هذا النظام من خلال الصورة الملتقطة، بتحديد ما إذا كان الموظف مخولا بالوصول إلى هذا المكان بناءا على الصلاحيات المخولة له.[1]

ب- بصمة الأصابع:

تقنية تساعد في تأمين مراكز البيانات من خلال تقييد الوصول إلى المناطق الحساسة، تعمل هذه التقنية من خلال استخدام ماسح بصمات الأصابع لإنشاء قالب لكل موظف لتسجيله في النظام وبعد ذلك عندما يقوم الموظف بوضع إصبعه أمام قارئ بصمات الأصابع لفتح باب على سبيل المثال يتم مقارنة بصمات أصابعه بالنموذج المخزن في قاعدة البيانات، إذا تطابقت البيانات مع بصمات أصابع الموظف يتم الترخيص له بالوصول.[2]

ت- بصمة الصوت:

يستخدم نظام التحكم في الوصول من خلال التعرف على الصوت أنماط الصوت من اجل منح أو رفض الوصول إلى منطقة أو نظام أو خدمة آمنة، يقوم مطابقة صوت المستخدم مع بصمات الصوت المسجلة مسبقا والمخزنة في قاعدة البيانات.[3]

2- تأمين الأماكن الحساسة (*sécurisation des locaux sensibles*):

يتم حماية وتأمين الأماكن الحساسة فيها عن طريق:

❖ **التحكم في الوصول المادي (*contrôle d'accès physique*):**

وهو مجموعة من الآليات التي تضمن أمن المباني والمستخدمين من خلال تقييد الوصول للأشخاص المصرح لهم فقط كما يسمح أيضا بالتحكم في دخول أو خروج الموظفين ومن آليات التحكم في الوصول المادي هي:

أ- لوحات المفاتيح الرمزية (les claviers à code):

---

1. La république Française, Club de la sécurité des systèmes d'information français, *op.cit, p13*
2. *Mise en place d'un système de contrôle d'accès par empreintes digitales et prespectives d'évolution, dans: https://riflbiometrics.com/mise-en-place-dun-systeme-de-controle-dacces-par-empreintes,(17/05/2025).*
3. Kahina oukil et Zerbout, op.cit, p13.

تكون لوحات المفاتيح الرقمية مثبتة على الأبواب إذ تمكن هذه التقنية للمستخدمين بإدخال رمز وصول شخصي لفتح المدخل.[1]

ب- جهاز الاتصال الداخلي الصوتي (inter phone):

يشكل جهاز الاتصال الداخلي الصوتي إمكانية التعرف الأولي على المستخدمين وحتى غير الموظفين باستخدام صوتهم، قبل فتح الباب الأمامي لهم عن بعد، وبعد اجتياز هذا الفحص الأولي يسمح لهم بالوصول.[2]

ت- التحكم البيومتري (contrôle biométrique)

لقد سبق الإشارة إلى تقنيات التحكم البيومتري المتمثلة في بصمة الوجه، الأصابع، الصوت، كآلية لضمان حماية البنوك والتحكم في وصول الأشخاص المصرح لهم فقط.

❖ **كاميرات المراقبة (caméras de surveillance)**

تعد كاميرات المراقبة إجراء وقائي يمنع أي محاولة اقتحام أو سرقة للبيانات، وبالتالي فهي وسيلة لضمان حماية الموظفين ومن جهة أخرى للبيانات.

3- **الجدران النارية (pare-feu):**

هو برنامج أو جهاز يقوم بفحص المعلومات القادمة من الأنترنت أو الشبكة ثم يمنعها من الوصول إلى الكمبيوتر أو يسمح لها بذلك، إعتمادا على جدار الحماية الخاص بالمؤسسة، يساعد جدار الحماية على منع المستخدمين او البرامج الضارة من الوصول إلى جهاز الكمبيوتر الخاص بالمستخدم عبر الشبكة أو الأنترنت، يمكن لجدار الحماية أيضا منع جهاز الكمبيوتر الخاص بالمستخدم من إرسال البرامج الضارة إلى أجهزة كمبيوتر أخرى.[3]

4- **أنظمة النسخ الاحتياطية (système de sauvegarde redondants):**

---

[1] *Les contrôles d'accès physiques pour la gestion des accès et la sécurité de vos locaux, https://heimdoor.com/actualites/controle-acces-physiques, (17/05/2025).*

[2] *interphone connecté comment la domatique révolutionne l'expérience de sécurité, dans : https://www.access-protection.fr/actualites/interphone-connecte-comment-la-domotique-revolutionne-lexperience-de-securite/, (17/05/2025).*

[3] *Salma Bahaza et tidjani Mammeri, op.cit, p11.*

النسخ الاحتياطي للبيانات هو عملية تكرار البيانات من موقعها الأساسي إلى وجهة ثانوية لحمايتها من الضياع بسبب الكوارث أو الحوادث أو الأعطال، هناك عدة طرق لعمل نسخ احتياطية لبيانات من بينها: [1]

أ- الوسائط:

الأقراص المضغوطة وأقراص DVD ومحركات أقراص USB وما إلى ذلك، بمعنى جهاز تخزين صغير ومتصل وسهل الإزالة مناسب للنسخ الاحتياطي.

ب- نسخة احتياطية:

لتنظيم النسخ الاحتياطي للبيانات لاستعادة البيانات بعد وقوع الحادث مثلا فقدان القرص الصلب، فمن المستحسن اختيار نسخة احتياطية يدوية واحدة على الأقل لنسخ البيانات الهامة إلى جهاز كمبيوتر شخصي.[2]

ت- التخزين خارج الموقع (Stockage hors site)

يشير النسخ الاحتياطي خارج الموقع إلى تخزين نسخ من البيانات في مكان يكون بعيد ومنفصل عن نظام التخزين الأساسي هذا ما يضمن في حالة فشل وحدة التخزين الأساسية أو تعرضها للاختراق، تظل البيانات آمنة ويمكن الوصول إليها.

القسم الثاني: يتمثل في أمن البرمجيات (sécurité logicielle)

هي مجموعة من الممارسات والتدابير والتقنيات التي تهدف إلى تأمين البرامج ضد التهديدات والثغرات الأمنية التي قد تعرض سلامة البيانات وسريتها ووظائفها للحظر وهو مهم لحماية برامج الكمبيوتر وأنظمتها من الوصول غير المصرح به أو التعديل أو الكشف أو التلف،[3] تتمثل التدابير التقنية لأمن البرمجيات في:

1- **حلول الحماية (*antivirus*):**

تتمثل في برامج مكافحة الفيروسات بهدف حماية مناصب العمل والبيانات من البرامج الضارة.

2- **جدارحماية تطبيقات الويب (*web application firewall*):**

---

[1] Sauvegarde des données, *Définition, types et solutions f*

[2] *Fonctionnement d'un système de sauvegarde redondant, dans* https://www.oodrive.com/fr/blog/sauvegarde/sauvegarde-donnees (18/05/2025).

[3] *Guide complet, : Sécurité logicielle dans*https://www.vpnunlimited.com/fr/help/cybersecurity/software-security, *(18/05/2025).*

تعمل جدران حماية تطبيقات الويب على حماية مواقع الويب وتطبيقات الهاتف المحمول من مختلف الهجمات، إذ تقوم جدران حماية التطبيقات على الويب بمراقبة وتصفية وحظر حزم البيانات المرسلة والمستقبلة إلى تطبيقات الويب، مما يحميها من التهديدات، تعمل جدران حماية تطبيقات الويب (waf) من خلال وضعه بين المستخدم وخادم الويب، ويقوم تصفية حركة المرور وتحليل جميع الطلبات من حركة المرور على الأنترنيت والسماح للطلبات المشروعة بالمرور واعتراض الطلبات الضارة.[1]

3- **إدارة الوصول المتميز *(priviliged Access management):***

إدارة الوصول المتميز عبارة عن حل تلقائي لإدارة كلمات المرور يوفر التحكم الأمن في الوصول والتدقيق والتنبيه والتسجيل لجميع الحسابات المتميزة.[2]

1- **تشفير البيانات أثناء النقل وفي حالة السكون (*chiffrent des donnés en transit et en repos):***

يشير تشفير البيانات أثناء النقل إلى تأمين البيانات أثناء انتقالها من مكان إلى آخر مثل بين المستخدم والخادم، أو بين نظامين، وبذلك يعد تشفير البيانات أثناء النقل ضروريا لضمان عدم إمكانية اعتراض البيانات أو تغييرها من قبل أطراف غير مصرح لهم أثناء عملية النقل، ولتشفير البيانات أثناء النقل يتم استخدام برتوكولات تشفير مصممة لتوفير اتصالات أمنة عبر شبكة الكمبيوتر من بينها:

- ***SSL (Secure socket layer):***

طبقة المقاييس الآمنة يستخدم هذا البرتوكول لإنشاء اتصالات آمنة عبر الانترنيت بما في ذلك تشفير البيانات بين العميل والخادم.

- ***TLS (Transport layer Security):***

تعني بأمان طبقة النقل ويستخدم لتأمين الاتصالات عبر شبكة الكمبيوتر من خلال ضمان سلامة وسرية ومصداقية البيانات المتبادلة، إضافة إلى ذلك كذلك يتم بنفس المنطق تشفير البيانات المخزنة سواءا على محركات الأقراص الصلبة أو على قواعد البيانات أو أنظمة تخزين الشبكة أو النسخ الاحتياطية بهدف التأكد من عدم تمكن الأشخاص الغير مصرح لهم من قراءة البيانات حتى لو تمكنوا من الوصول إلى وسائط التخزين.[3]

---

[1] *Qu'est-ce qu'un pare-feu d'application web (waf), dans : https://www.f5.com/fr_fr/glossary/web-application-firewall-waf, (18/05/2025).*

[2] *Yacine Hadj Sadok et Abderrahmane, **Etude et mise en place d'un PAM**, Mémoire de MASTER, (Faculté des sciences, université Saad Dahlab, Blida, 2022/2023) p11.*

[3] *Centre D'expertise En Sécurité De L'information, **Chiffrement des données en transit et au repos** (université Du Québec, Juillet 2024.) p6.*

المطلب الرابع: الآليات التنظيمية والإجراءات الإدارية للبنك الخارجي الجزائري في حماية البيانات الشخصية.

تجسيدا لما جاء به القانون 18-07 بشأن إلتزام المسؤول باتخاذ التدابير التنظيمية والتقنية الملائمة لحماية المعطيات محل المعالجة، وضع البنك الخارجي الجزائر مجموعة من الآليات التنظيمية والإجراءات الإدارية لتأمين البيانات الشخصية وحمايتها وتتمثل هذه الآليات في:

1- بالنسبة للآليات التنظيمية:

وهي تشمل الآليات الموضوعة من طرف البنك الخارجي الجزائري التي تنظم سياسة حماية البيانات الشخصية والتي تتمثل في:

أ- سياسة أمن انظمة المعلومات (*politique de sécurité des système d'information*):

وثيقة تحدد القواعد التي يجب على أولئك الذين لديهم إمكانية الوصول إلى موارد الشبكة وبيناتها إتباعها من أجل حماية البيانات ضد الهجمات والتهديدات،[1] إضافة إلى ذلك يجب على مسؤول أمن نظم بالمعلومات عند إعداده لسياسة امن نظم المعلومات أن تتوافق مع الضوابط الواردة في المرجع الوطني لأمن المعلومات من بين هذه الضوابط:

- ❖ يجب أن نتوافق سياسة أمن نظم المعلومات مع متطلبات إستراتيجية المؤسسة.
- ❖ يجب على قسم الأمن السيبراني التأكد من تنفيذ الضوابط والمتطلبات المدرجة في سياسات الأمن.
- ❖ يجب أن تتم الموافقة على سياسة أمن المعلومات من قبل المدير الأعلى للمؤسسة بعد التحقق من صحتها من قبل لجنة من المعلومات إذا كانت موجودة.
- ❖ تتأكد الإدارة من نشر سياسات الأمن للأطراف المعنية (موظفي المنظمة وجهات الخارجية).
- ❖ ينبغي مراجعة سياسات الأمن وتحديثها على فترات منظمة أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية والمعيارية ذات الصلة، يجب أن يتم اعتماده من قبل الإدارة.[2]

---

[1] *Nouara Messahel et Khadra Saadi, **installation et configuration d'un firewall logiciel** mémoire de master, (univeristé Mouloud Mammeri de Tizi Ouzou, faculté de Génie électrique et d'informatique, 2016/2017) p23.*

[2] *République algérienne démocratique et populaire, ministère des postes et des télécommunications, **guide nationale référentiel de la sécurité de l'information**, op,cit,, p 17.*

❖ يجب أن تستمد سياسة أمن لنظم المعلومات من هذا الإطار ويمكن دعمها بالمعايير والقواعد والممارسات الجيدة في مجال أمن المعلومات، أما بالنسبة لما نظمته الوثيقة من قواعد ومحتويات فلم يتم الاطلاع على محتوى الوثيقة نظرا للطابع الحساس والسري لهذه الوثيقة.

ب- ميثاق الأمن *charte de sécurité*:

مجموعة القواعد التي تهدف إلى رفع مستوى وعي الموظفين بالمخاطر التي يواجهها أثناء عملهم كما تحدد القواعد الواجب احترامها من قبل الموظفين أثناء عملهم،[1] وفي هذا السياق قدم الدليل الوطني لأمن المعلومات نموذج لميثاق الأمن وهو بمثابة دليل إرشادي لتوجيه المؤسسات الجزائرية بهدف تطويرها سياستها الأمنية بما تتماشى مع طبيعة نشاط بما يعنى أن النموذج المقدم من طرف المرجع الوطني لا يعد ملزما أن يتم اعتماده كما هو وإنما يتم صياغته على حسب نشاط المؤسسة لأنه ميثاق لأمن ليس خاص فقط بالبنوك و إنما بكل المؤسسات، حيث تضمن النموذج الذي جاء به الدليل الوطني لأمن المعلومات مجموعة من المواد التي تتوفر في ميثاق الأمن وهي كالتالي:

- **المادة1: الغرض**

وهي تتمثل في أهداف الميثاق الذي يسعى إلى تحقيقه من بينه تحديد شروط وأحكام استخدام موارد تكنولوجيا المعلومات الخاصة بالمنطقة، ويحدد أيضا قواعد الأمان التي يجب على المستخدمين إتباعها.

- **المادة2: نطاق التطبيق**

حددت هذه المادة الأشخاص الذي ينطبق عليهم الميثاق وهم الأشخاص الذي لديهم إمكانية الوصول، بشكل دائم أو مؤقت إلى موارد تكنولوجيا المعلومات الخاصة بالمنظمة.

- **المادة3: ملكية موارد تكنولوجيا المعلومات.**

حددت هذه المادة ملكية موارد تكنولوجيا المعلومات المتمثلة في الملكية الحصرية للمنظمة والمتمثلة في جميع موارد تكنولوجيا المعلومات المتاحة للمستخدمين وجميع البيانات المضافة على أجهزة المنظمة والمنقولة عبر شبكاتها هي ملكية حصرية للمنظمة.

- **المادة 4: شروط الوصول إلى الموارد وشبكة الحاسوب.**

بحيث تضمنت هذه المادة توفر شرط المصادقة المسبقة للوصول إلى الموارد وشبكة الحاسوب.

[1] معلومات مقدمة من طرف السيدة أيت زيان مريم، مهندسة في أمن أنظمة المعلومات في البنك الخارجي الجزائري.

- **المادة 5: مسؤولية المستخدم.**

حددت بأن المسؤول الوحيد عن استخدام وسائل المصادقة هو المستخدم.

- **المادة6: حماية وسائل المصادقة.**

من أجل الحفاظ على وسائل المصادقة المتاحة للمستخدم يجب عليه حماية وحفظ معلوماته وتغييرها بشكل دوري، كما يمنع مشاركتها مع الغير.

- **المادة7: استخدام موارد تكنولوجيا المعلومات.**

حددت المادة 7 من النموذج قواعد استخدام موارد تكنولوجيا المعلومات.

- **المادة 8: التزامات المنظمة تجاه المستخدمين.**

حددت هذه المادة واجبات المنظمة اتجاه المستخدمين من بينها تزويد المنظمة للمستخدم بالموارد التكنولوجية اللازمة لأداء المهام الموكلة إليه.[1]

- **المادة9: التزامات المستخدم.**

ورد في هذه المادة واجبات المستخدم من بينها: الالتزام بالقوانين واللوائح المعمول بها، احترام هذا الميثاق وكذلك الإجراءات والسياسات المختلفة للمنظمة.

- **المادة10: السلامة والحماية في مكان العمل.**

وضحت هذه المادة التزام المستخدم بتعليمات السلامة.

- **المادة11: استخدام الرسائل الإلكترونية المهنية.**

توفر المنظمة للمستخدمين حسابات مراسلة الكترونية تسمح لهم بإرسال واستقبال الرسائل الإلكترونية والمهنية ويمنع استخدام الرسائل المهنية لأغراض غير مهنية.

- **المادة 12: استخدام الأنترنت.**

[1] *République algérienne démocratique et populaire, ministère des postes et des télécommunications, **guide nationale référentiel de la sécurité de l'information**, op.cit, p 78et 79.*

تحدد هذه المادة بشروط المستخدمون الذين لديهم إمكانية الوصول إلى الأنترنت من بينها لا ألا يستخدم هذه الخدمة لأي أغرا خبيثة أو فاحشة أو احتيالية أو كراهية أو تشهيرية وألا يتم تقديم معلومات تتعلق بوظيفتهم أو رتبتهم أو مسؤوليتهم على شبكات التواصل الاجتماعي.

- **المادة 13: الأجهزة المحمولة ووسائط التخزين.**

نصت هذه المادة على واجبات المستخدم من بينها إبلاغ الإدارة عن أي فقدان أو سرقة لجهاز محمول ووسيلة تخزين احترافية، منع نقل المستندات عن طريق الرسائل القابلة للإزالة من أشخاص خارج المؤسسة.

- **المادة14: التدابير الأمنية الواجب تطبيقها عند السفر إلى الخارج.**

وتضمنت مجموعة من الالتزامات الواجبة على المستخدم أثناء السفر إلى الخارج.

- **المادة 15: إنهاء العلاقة بين المستخدم والمؤسسة.**

نصت على ما يجب أن يقوم به المستخدم عند إنهاء علاقته مع المؤسسة.[1]

- **المادة16: إدارة الحوادث.**

نصت على ما يجب أن تقوم به المؤسسة أثناء وقوع الحادث.

- **المادة 17: عدم الالتزام بالميثاق.**

نصت على معاقبة المستخدم في حالة انتهاكه لما جاء به ميثاق الأمن.

- **المادة 18: دخول الاتفاقية حيز التنفيذ.**

بحيث حددت أن ميثاق يدخل حيز التنفيذ عند التوقيع عليه من المستخدم وفي حالة رفضه للتوقيع يمنع من الوصول إلى موارد تكنولوجيا المعلومات.[2]

أما بالنسبة ميثاق الأمن الخاص للبنك الخارجي الجزائر فلم يكن متاح بحكم أن ميثاق الأمن هو وثيقة داخلية لا يمكن مشاركتها خارج إطار الموظفين، لذلك تم الاكتفاء بعرض نموذج الذي قدمته المرجع

[1] *République algérienne démocratique et populaire, ministère des postes et des télécommunications, **guide nationale référentiel de la sécurité de l'information**, op.cit, p 80,81,82.*

[2] *République algérienne démocratique et populaire, ministère des postes et des télécommunications, **guide nationale référentiel de la sécurité de l'information**, op.cit, p 82.*

الوطني لأمن المعلومات لأنه يمثل وثيقة مرجعية للهيئات والمؤسسات لضمان الامتثال لمتطلبات حماية المعطيات ذات الطابع الشخصي.

2- **الإجراءات الإدارية**: تشمل الإجراءات الإدارية الموضوعة من طرف البنك الخارجي الجزائري التي تؤمن الحماية للبيانات الشخصية.

- **توعية الموظفين (*SENSIBILISATION DES Employés*):**

إن وعي الموظفين بأمن البيانات الشخصية أمر بالغ الأهمية في حماية البيانات الشخصية من التهديدات الأمنية، حيث أن تحقيق الأمن لا يظهر فقط على وجود بنية تقنية لحماية البيانات بل يتطلب الأمر وعي الموظفين بما يحدث في الفضاء السيبراني، من خلال دورات تكوينية ينظمها البنك من أجل تدريبهم كيفية تجنب المخاطر الأمنية وكيف حماية أنفسهم.[1]

- **اختبار الثغرات الأمنية (*test de vulnérabilité*):**

هو عملية تحليل وتحديد وتقييم نقاط الضعف الأمنية المحتملة في البنية التحتية لتكنولوجيا المعلومات الخاصة بالمؤسسة بشكل منهجي بحيث يساعد اختبار الثغرات الأمنية في اكتشاف نقاط الضعف المحتملة في البنية التحتية الخاصة بالبنك، تقييم التأثير والمخاطر المرتبطة لكل ثغرة، تطوير استراتيجيات لمعالجة نقاط الضعف المحتملة في البنية التحتية الخاصة بالبنك، تقييم التأثير والمخاطر المرتبطة بكل ثغرة، تطوير استراتيجيات لمعالجة نقاط الضعف المحددة وإعطائها الأولوية.[2]

- **عملية التدقيق المنتظمة (*des audits réguliers*):**

تعتبر عمليات التدقيق أمر بالغ الأهمية لأنها تساعد البنوك على تحديد نقاط الضعف المحتملة في البنية التحتية لتكنولوجيا المعلومات الخاصة بها، إذ يتم إجراء التدقيق من خلال قياس مدى إمتثال البنك لمجموعة من المعايير المحددة، يتيح هذا الإجراء التحقق من اليات الحماية الموجودة والتأكد من أنها تعمل بشكل صحيح لحماية البيانات الحساسة ضد أي تهديد.[3]

المبحث الثالث: تقييم إستراتيجية حماية البيانات الشخصية في الجزائر.

[1] *معلومات مقدمة من طرف السيدة أيت زيان مريم، مهندسة في أمن أنظمة المعلومات في البنك الخارجي الجزائري.*

[2] *Qu'est-ce qu'un test de vulnérabilité ? https://www.vumetric.com/fr/blogue/quest-ce-que-le-test-de-vulnerabilite- (18/05/2025.).*

[3] *L'importance des audits de sécurité réguliers pour maintenir la protection des données, https://bienvenum.org/limportance-des-audits-de-securite-reguliers-pour-maintenir-la-protection-des-donnees, (19/05/2025).*

يهدف هذا المبحث إلى تقديم نظرة تقييمية لإستراتيجية حماية البيانات الشخصية من خلال التركيز على 4 ابعاد: القانونية، المؤسساتية، التقنية، التنظيمية.

المطلب الأول: تقييم البنية القانونية لحماية البيانات الشخصية في الجزائر.

أولت الجزائر أهمية كبيرة لمسألة حماية البيانات الشخصية ويظهر هذا الاهتمام جليا من خلال تكريسها لترسانة قانونية متكاملة تؤطر حماية للبيانات الشخصية، بدءا من دستور 1996 وصولا إلى دستور 2016 الذي كرس في المادة 46 الحق في حماية الحياة الخاصة للمواطن وسرية المراسلات والاتصالات الخاصة بكل أشكالها، كما تم في هذا السياق تعزيز البنية القانونية بقوانين خاصة لم تنص بصراحة على حماية المعطيات ذات الطابع الشخصي إلا أنه يمكن القول أنه كانت هناك بعض المحاولات لإرساء حماية للبيانات الشخصية، من بينها الأمر 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة الذي تضمن إشارة غير مباشرة إلى حماية البيانات من خلال اعتباره بأن برامج الحاسوب الآلي تدخل ضمن المصنفات الرقمية الواقعة تحت نطاق الحماية، القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها، الذي عزز أساليب مكافحة الجرائم المعلوماتية والتصدي لها، القانون 15-04 المتعلق بالتوقيع والتصديق الإلكتروني الذي أشار إلى أن على مؤدي خدمات التصديق الإلكتروني الحفاظ على سرية البيانات والمعلومات المتعلقة بشهادات التصديق الإلكتروني المسموحة، القانون 18-05 المتعلق بالتجارة الإلكترونية الذي ألزم على المتعاملين بجمع البيانات الضرورية فقط، ثم بعد ذلك صدر القانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال المعطيات ذات الطابع الشخصي الذي يعتبر الإطار القانوني الأساسي الذي يؤطر وينظم مسألة حماية البيانات الشخصية في الجزائر. لما جاء من مبادئ والتزامات وأحكام تتراوح مابين الجزائية والإدارية، كما جاء القانون بآلية تكرس تطبيق القانون 18-07 وتسهر على حسن التزامه في كل الهيئات والمؤسسات التي تحوز على بيانات الشخصية.

بناءا على ما سبق، يمكن تقييم البنية القانونية بالتركيز على 3 معايير من حيث قوة المنظومة القانونية، تماسك المنظومة القانونية ضد الثغرات الأمنية، وصرامتها من حيث الردع.

أولا معيار القوة: و تعني مدة قدرة القانون على إرساء حماية فعلية للبيانات الشخصية أي قدرته على فرض الالتزام بأحكام القانون، تجسد قوة البنية القانونية في تكامل النصوص وفعاليتها، حيث تستمد هذه القوة من الدستور الجزائري بوصفه القانون الاسمي للدولة كما كرس دستور 2016 حماية الحق في الحياة الخاصة وهو ما أكد عليه دستور 2020 في الفقرة الثالثة من المادة 47 حماية الأشخاص عند

معالجة المعطيات ذات الطابع الشخصي، إلى جانب نصوص تنظيمية أخرى مثل القانون 15-04 الذي يلزم مؤدي خدمات التصديق الإلكتروني للحفاظ على سرية البيانات والمعلومات المتعلقة بشهادات التصديق الالكتروني المسموحة، قانون التجارة الإلكترونية 18-05 الذي يلزم المتعاملين بضمان سرية البيانات وحمايتها فضلا عن القانون 18-07 الذي يعتبر بحر الأساس في المنظومة القانونية في الجزائر لأنه جاء بالكثير في مجال حماية المعطيات ذات الطابع الشخصي، إذ يقر هذا القانون التزامات على مسؤولي المعالجة من بينها اتخاذ تدابير تقنية لحماية البيانات الشخصية والتزام بالسر المهني، وعليه يمكن القول أنه يوجد تكامل بين النصوص القانونية هذا ما يعزز قوة المنظومة القانونية في الجزائر.

ثانيا: معيار تماسك المنظومة القانونية ضد الثغرات الأمنية.

لقد سبق الإشارة إلا أن المنظومة القانونية في الجزائر تستمد قوتها من خلال تعدد القوانين والتشريعات وتكاملها فهي مكملة لبعضها البعض، هذا التكامل والانسجام الموجود بين القوانين يجعلها متماسكة وصامدة ضد الثغرات الأمنية، إذ يمكن القول إن أغلب النصوص القانونية تتضمن الإشارة إلى الجانب التقني في حماية البيانات الشخصية، والدليل على ذلك القانون 15-04 المتعلق القواعد العامة للتصديق والتوقيع الالكترونيين الذي نص على توفير الوسائل التقنية لحماية البيانات المستخدمة لإنشاء التوقيع الإلكتروني إلى جانب ذلك القانون 18-07 الذي يفرض على المسؤولين عن المعالجة اتخاذ تدابير أمنية و تقنية مثل التحكم بالوصول، التشفير برمجيات الحماية ضد البرامج الخبيثة لأن توفير الحماية التقنية للبيانات بشكل جدار دفاعيا لحماية البيانات من أي اختراق أو تسرب للبيانات، من خلال هذا الطرح يمكن القول بأن المنظومة القانونية في الجزائر تظهر تماسك بفضل تعدد النصوص القانونية التي تقر بضرورة اتخاذ تدابير تقنية لحماية البيانات الشخصية وهو بذلك تأمين مختلف الثغرات الأمنية.

المعيار الثالث: الصرامة في الردع.

توفر النصوص القانونية لحماية البيانات الشخصية آليات ردعية فعالة ضد منتهكي أحكام هذه القوانين وتتجسد هذه الآليات الردعية في القانون 18-07 الذي نص على إجراءات إدارية تتخذهم السلطة الوطنية في حق المؤول عن المعالجة في حالة خرقه لأحكام هذا القانون والتي تتمثل في: الانذار، الاعذار، السحب المؤقت، إضافة إلى أحكام جزائية تتمثل في السجن وغرامات مالية.

في حال معالجة البيانات دون إحترام الكرامة الإنسانية أو الحياة الخاصة أو الحرية العامة للشخص المعني، أو في حال معالجة البيانات دون موافقة الشخص المعني، أو في حال جمع معطيات ذات طابع شخصي بطريقة غير نزيهة أو غير مشروعة، كما يضاف إلى ذلك قانون 15-04 الذي يعزز هذا الطابع

الردعي خاصة في المادة 70و71 التي تنص على فرض عقوبات تتراوح بين الحبس وفرض غرامات مالية في حالة عدم التزام مؤدي خدمات التصديق الالكتروني بالحفاظ على سرية البيانات والمعلومات أو في حالة جمع البيانات الشخصية للمعني دون موافقته إلى جانب ذلك، قانون العقوبات الذي يتضمن آليات ردعية في المادة 394 مكرر، بحيث يفرض قانون العقوبات جزاءات تتمثل في الحبس وفرض غرامات في حال الدخول أو البقاء عن طريق الغش في كل جزء من منظومة المعالجة الآلية للمعطيات أو في حالة إدخال بطريقة الغش المعطيات، من خلال ما سبق يمكن القول أن البنية القانونية للجزائر تظهر صرامة واضحة في الجانب الردعي من خلال غرامات و الجن تبعا لخطورة الفعل المرتكب.

المطلب الثاني: تقييم البنية المؤسساتية لحماية البيانات الشخصية في الجزائر.

إن إرساء مؤسسات وهياكل وطنية تعنى بمسألة حماية البيانات الشخصية تعكس اهتمام واضحا من طرف الدولة الجزائرية بشأن مسألة البيانات الشخصية وتأمينها، إذ يتجسد ويبرز بوضوح هذا الاهتمام من خلال تعدد الهياكل المختصة من جهة بحماية البيانات وضمان سريتها ومن جهة أخرى لمكافحة أشكال التهديدات والجرائم المعلوماتية الماسة بأمنها، ويبرز في هذا السياق عدة مؤسسات وطنية تضطلع بأدوار محورية في حماية المعطيات ذات الطابع الشخصي وعلى رأس هذه المنظومة نجد السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي التي تعتبر الهيئة الرقابية والمكلفة بتطبيق أحكام القانون 18-07 التي من بينها إصدار التراخيص ومنحها علاوة على ذلك تضطلع السلطة بأدوار محورية في حماية حقوق المعني و ضمانها إضافة إلى إصدار أحكام تتراوح مابين الجزائية والإدارية لتجريم الأفعال المنتهكة بالقانون 18-07 إضافة إلى المحافظة السامية للرقمنة بما تتوافق من متطلبات أمن الأنظمة المعلوماتية، إلى جانب المؤسسات التابعة لوزارة الدفاع الوطني التي تلعب دورا حاسما في تأمين المنشآت الرقمية ومن أبرز هذه المؤسسات الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال مصلحة الدفاع السيبراني ومراقبة امن الأنظمة المركز الوطني للإشارة والحروب الإلكترونية، وكالة أمن الأنظمة المعلوماتية، المجلس الوطني لامن الأنظمة المعلوماتية، فضلا عن الوحدات التابعة للدرك الوطني والفرق التقنية للامن الوطني التي تساهم في محاربة كافة انواع الجرائم المعلوماتية في إطار التنسيق المؤسسي إلى جانب السلطة القضائية المتمثلة في القطب الجزائي المتخصص في محاربة الجرائم المعلوماتية، كما تشمل هذه المنظومة أيضا سلطة ضبط البريد والاتصالات الإلكترونية يتبين من خلال هذا العرض أنه يوجد تكامل و تنوع بين المؤسسات التي تعني بأمن البيانات، إذ يتجسد هذا التكامل من خلال توزيع المهام التعاون بين مختلف الهياكل في رصد التهديدات السيبرانية على سبيل المثال التعاون الوثيق الموجود بين القطاعات الوزارية

المتمثلة في وزارة البريد والاتصالات الإلكترونية وزارة الدفاع الوطني في مجال تأمين آمن الشبكات كذلك التكامل الموجود بين المجلس الوطني لأمن أنظمة المعلوماتية والسلطة الوطنية للتصديق الالكتروني، هذا التنسيق المؤسساتي الموجود يعبر عن توحيد الجهود لتحقيق أهداف حماية البيانات الشخصية بشكل أكثر فعالية.

من خلال هذا الطرح، يمكن تقييم البنية المؤسساتية بالتركيز على معيار الكفاءة بكل فعالية وفي هذا الإطار تتميز البنية المؤسساتية في الجزائر بالتنوع نتيجة تعدد الهيئات و الهياكل التي تعني بحماية البيانات الشخصية ويشمل هذا التنوع في المؤسسات الواقعة الرئاسة الجمهورية المتمثلة في السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، والمحافظة السامية للرقمنة، وكالة أمن الأنظمة المعلوماتية، المؤسسات التابعة لوزارة الدفاع المتمثلة في الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة إلى جانب وزارة البريد والمواصلات السلكية واللاسلكية والسلطة القضائية، إذ تعمل المؤسسات بالتنسيق مع البعض بهدف تحقيق أهدافها بفعالية على سبيل المثال : تتعاون المحافظة السامية للرقمنة مع وكالة امن الأنظمة المعلوماتية بهدف ضمان أن الإستراتيجية الوطنية للرقمنة تتوافق مع متطلبات أمن الأنظمة بينما تتنسق السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي مع السلطة القضائية (ضباط والشرطة القضائية) في مجال معاينة والبحث عن الجرائم المنصوص عنها في أحكام القانون 18-07 كما تتعاون الهيئة الوطنية للوقاية من جرائم الإعلام والاتصال مع السلطة القضائية في مجال مكافحة الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال إلى جانب تعاون وحدات الدرك الوطني (مركز الوقاية من جرائم الإعلام والجرائم المعلوماتية) مع السلطة القضائية في مجال المشاركة في عمليات التحري والتسرب عبر شبكات الانترنت هذا التقاسم الواضح في المهام والتنسيق الموجود يوضع تعاون البنية المؤسساتية فهي ليست مجرد مؤسسات تعمل بمعزل عن الأخرى بل تتكامل وتتقاسم الجهود لتحقيق الهدف المسطر وهو حماية البيانات الشخصية.

المطلب الثالث: تقييم المنظومة التقنية لحماية البيانات الشخصية في الجزائر.

تتمثل المنظومة التقنية خط الدفاع الأول في حماية البيانات الشخصية وهو ما نصت عليه التشريعات والقوانين في الجزائر من خلال فرض على مسؤولي المعالجة وضع تدابير تقنية لحماية البيانات الشخصية تتمثل في أنظمة التشفير، جدران الحماية، برامج مكافحة الفيروسات، أنظمة كشف و منع التسلل، أنظمة التحكم في الوصول هذا ما يبرز الدور المحوري للمنظومة التقنية في تأمين الحماية للبيانات

الشخصية ضد التهديدات التي تمس بأمنها و سلامتها إذ أن وجود نصوص قانونية وتشريعات تجرم منتهكي البيانات غير كافية وحدها لتوفير الحماية بل تتطلب وجود آليات تقنية فعالة تحمي البيانات من الوصول الغير مصرح به أو التعديل أو الإتلاف.

من خلال ما سبق فيمكن تقييم البنية التقنية في الجزائر بناء على معيار الفاعلية والتي تعني قدرة الوسائل التقنية على تحقيق أهدافها بفعالية والتي تتضمن حماية البيانات وسريتها ضد التهديدات والمخاطر السيبرانية انطلاقا من المادة 38 من القانون 18-07 والتي تنص على ضرورة اتخاذ المسؤولين في المؤسسات والهيئات تدابير تقنية، باشرت كل المؤسسات التي تحوز على البيانات التي تبني تدابير تقنية من بينها البنك الخارجي الجزائري بوصفه مؤسسة مالية من بينها: آليات التشفير، بروتوكولات الحماية أثناء نقل البيانات، أنظمة التحكم في الوصول المادي، المراقبة بالفيديو، تأمين مراكز البيانات وغيرها من الآليات التي تحد من الوصول الغير المصرح به إلى البيانات، إن فعالية هذه الأنظمة لا تقاس بتعددها أي بوجود العديد من الوسائل التقنية وإنما تقاس بمدى بقدرتها على التصدي ضد التهديدات والاختراقات وقدرتها على بسط الحماية للبيانات الشخصية.

المطلب الرابع: تقييم الآليات التنظيمية لحماية البيانات الشخصية في الجزائر.

تعتبر الآليات التنظيمية من الركائز الأساسية لضمان تطبيق السياسات والإجراءات اللازمة لحماية البيانات الشخصية، فهي تحدد المسؤوليات والقواعد والإجراءات لضمان مستويات الأمن في المؤسسات، وتندرج ضمن هذه الآليات التنظيمية وثيقتين هما: ميثاق أمن المعلومات، سياسة أمن أنظمة المعلومات، وفي هذا السياق قدم المرجع الوطني لأمن المعلومات نموذجا موحدا لميثاق أمن المعلومات، كما قدم مجموعة من الضوابط الواجب توفرها في سياسة أمن أنظمة المعلومات، إذ تعتبر هذين للوثيقتين الأخيريتين بمثابة وثيقة مرجعية تلزم كل المؤسسات بالامتثال لمعايير نظم المعلومات واحترامها.

انطلاقا مما سبق ذكره يمكن تقييم الآليات التقنية المطبقة على مستوى الهيئات والمؤسسات بصفة عامة لأن ميثاق الأمن وسياسة أمن أنظمة المعلومات تختلف و تتفاوت من مؤسسة إلى أخرى على حسب نشاطها فمثلا بالنسبة للقطاعات الحساسة التي تتعامل مع بيانات حساسة مثل البنوك تحتاج إلى سياسات صارمة مقارنة بمؤسسات أخرى بسيطة لا تحتاج إلى وثيقة صارمة تحدد سلوكيات الأفراد فيها، بحكم أن قوة الميثاق أمن المعلومات تظهر في كونه صارم أي يحتوي على عقوبات أو غرامات في بعض الأحيان، يمكن القول أن الدليل الإرشادي المقدم من طرف وزارة البريد والمواصلات السلكية يحمل طابعا ردعيا المتمثل في (المادة 17 : تنص على معاقبة المستخدم في حالة انتهاكه لما جاء به الميثاق) لكن لم تحدد

هذه المادة نوع العقوبة التي تتخذ للمستخدم في حال انتهاكه لأحكام الميثاق، بل ترك هذا الأمر للمؤسسة أو الهيئة، وعليه يمكن القول أن ميثاق الأمن و سياسة أمن أنظمة المعلومات هما وثيقتين أساسيتين في المؤسسات والقطاعات خاصة القطاعات الحساسة مثل البنوك لأنهما يتضمنان قواعد تهدف إلى ضمان مستوى الأمن.

خلاصة الفصل الثالث:

تضمن هذا الفصل الدراسة الميدانية والتي شملت البنك الخارجي الجزائري وذلك من أجل معرفة الوسائل والآليات التي يستخدمها البنك الخارجي الجزائري في حماية البيانات الشخصية، حيث تم تعرف على مختلف الآليات المؤسساتية القانونية، التقنية، التنظيمية المستخدمة لحماية البيانات الشخصية على مستوى البنك الخارجي الجزائري، كما تناول هذا الفصل إجراء تقييم للبنية المؤسساتية والقانونية والتقنية والتنظيمية بناءا على معيار الكفاءة والفاعلية والصرامة في الردع والقوة، إذ أظهر التقييم أن الجزائر تمتلك منظومة متكاملة، تقوم على وجود إطار قانوني واضح وهيئات متخصصة تتكامل أدوارها في ما بينها لتحقيق الحماية للبيانات الشخصية إلى جانب وجود بنية تقنية تساهم في تعزيز مستوى الحماية.

الخـــاتمة

خاتمة

من خلال هذه الدراسة تم تسليط الضوء على دور الأمن السيبراني في حماية البيانات الشخصية على مستوى القطاع البنكي، حيث تم تناول الإستراتيجية الوطنية لحماية البيانات الشخصية التي بدورها تركز على أبعاد مؤسساتية وقانونية وتقنية، تعزز وتضمن الحماية الفعلية للمعطيات ذات الطابع الشخصي، أما في الجانب التطبيقي فقد تم تناول اليات التي يوفرها البنك الخارجي الجزائري في حمايته لبينات عملائه وموظفينه، ثم في الأخير تم تقييم الإستراتيجية الوطنية لحماية البيانات الشخصية بأبعادها المختلفة.

وفي هذا الإطار تم إختبار فرضيات الدراسة، وتوصلنا إلى:

- **الفرضية الأولى:** البنية القانونية الوطنية قد لا تكون كافية للتصدي للتهديدات السيبرانية وضمان حماية فعالة للبيانات الشخصية.، لم يتم إثبات هذه الفرضية، لأن المنظومة القانونية التي تؤطر مسألة حماية البيانات الشخصية في الجزائر لا تضمن وحدها الحماية الفعلية للبيانات الشخصية، بل يستلزم الأمر وجود اليات تقنية تقوم على التشفير والتحكم في الوصول المادي وأنظمة الحماية من البرمجيات الخبيثة إلى جانب اليات مؤسساتية تسهر على تطبيق أحكام القوانين.
- **الفرضية الثانية:** الإستراتيجية الوطنية لحماية البيانات الشخصية القائمة على البعد المؤسساتي قد لا تكون وحدها كافية لضمان الحماية الفعلية للبيانات الشخصية والتصدي للمخاطر التي تهددها. يتم إثبات هذه الفرضية، لأن الإستراتيجية الوطنية لحماية البيانات الشخصية لا تقوم فقط على البعد المؤسساتي لضمان الحماية الفعلية للبيانات الشخصية، وإنما تكون مدعومة أيضا بإطار قانوني لتنظيم مسألة حماية البيانات الشخصية من الإنتهاك أو الإستعمال الغير مشروع وتجريم الأفعال الغير المشروعة التي تمس بأمن المعطيات ذات الطابع الشخصي، إلى جانب اليأت تقنية، هذا ما يوضح أن الإستراتيجية الوطنية لحماية البيانات الشخصية تقوم على اليات متكاملة لتحقيق الأهداف المرجوة في مجال حماية المعطيات ذات الطابع الشخصي.
- **الفرضية الثالثة:** يتوفر البنك الخارجي الجزائري على آليات وتدابير أمنية لحماية البيانات الشخصية، تم إثبات هذه الفرضية، فمن خلال المقابلة التي أجريت مع مدير أمن أنظمة المعلومات ومهندسة أمن أنظمة المعلومات، تبين أن البنك الخارجي الجزائري يتوفر على اليات وتدابير أمنية تحمي بها بيانات عملائها وموظفيها.

من خلال ما سبق، خلصت الدراسة إلى جملة من النتائج من بينها:

- أن الأمن السيبراني في الجزائر يركز على بعدين أساسين: وهو البعد الوقائي يتمثل في مؤسسات تضطلع بمهام حماية البيانات الشخصية وضمان سريتها إلى جانب اليات قانونية توفر الحماية للشخص المعني بمعالجة بياناته، وبعد ردعي يتمثل في وجود مؤسسات تعنى بتجريم الأفعال المنتهكة في حق البيانات الشخصية، إلى جانب اليات قانونية تعاقب الأفعال الغير المشروعة التي تمس بسلامة البيانات الشخصية.
- إن حماية البيانات الشخصية لا تركز فقط على البعد القانوني لضمان الحماية الفعلية للبيانات الشخصية، وإنما أيضا تركز على البعد المؤسساتي والبعد التقني، وبذلك تصبح منظومة متكاملة وقادرة على التصدي للهجمات السيبرانية وتحقيق الأهداف المرجوة.
- تمتلك الجزائر اليات مؤسساتية لا تعمل بمعزل عن الأخرى، بل يتم التعاون والتنسيق فيما بينهم بما يضمن تبادل الخبرات وتنسيق الجهود في سبيل تأمين الحماية الفعلية للبيانات الشخصية.
- إلى جانب إمتلاك الجزائر منظومة مؤسساتية على المستوى الوطني تضطلع بمهام إستراتيجية في مجال حماية المعطيات ذات الطابع الشخصي، تمتلك منظومة مؤسساتية تقوم بالإشراف مباشرة على حماية البيانات الشخصية في البنوك التجارية من خلال الرقابة على هذه الأخيرة في مدى إلتزامها وامتثالها لأحكام القوانين المتعلقة بحماية المعطيات ذات الطابع الشخصي.
- تعتبر السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي هي المسؤولة الوحيدة على المستوى الوطني في مسالة ضمان الحماية للشخص المعني بالمعالجة بما فيها صون حقوقه.
- يعتبر القانون 18-07 هو القانون الوحيد الذي ينص بصراحة على حماية البيانات الشخصية، ويكرس الحقوق لتي يتمتع بها الشخص المعني أثناء المعالجة.، باعتبار أنه أول قانون مخصص ومفصل لحماية المعطيات ذات الطابع الشخصي.
- يلعب الامن السيبراني دورا جوهريا في حماية البيانات الشخصية، بوصفه وسيلة دفاعية، إذ يقوم من جهة بتوفير بيئة أمنة من خلال أدوات وإجراءات تقنية تتمثل في التشفير وجدران الحماية وغيرها من الوسائل التقنية للتصدي للمخاطر والتهديدات الماسة بأمنها، من جهة أخرى يقوم بتوفير إطار قانوني يضمن حماية البيانات الشخصية بما فيها حقوق الأشخاص المعني بالمعالجة، على جانب توفير إطار مؤسساتي يقوم السهر على تطبيق أحكام القانون، ويقوم في ذات السياق

بالتعاون في التنسيق في مجال حماية المعطيات بما فيها و محاربة كل أنواع الجرائم الماسة بالمعالجة الألية للمعطيات.

- يتوفر البنك الخارجي الجزائري لضمان حماية فعلية لبيانات عملائه وموظفينه على اليات تقنية واليات تنظيمية وإجراءات إدارية ما يبين بأنه ملتزم تماما ومتوافق مع أحكام القانون 18-07.
- تعد السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي هي السلطة الوحيدة التي تقوم بممارسة الرقابة على مسؤول المعالجة بخصوص توفير اليات حماية البيانات الشخصية. وتنفيذه للالتزامات المنصوص عليها في القانون 18-07.
- أظهر تقييم الإستراتيجية الوطنية لحماية البيانات الشخصية وجود بنية مؤسساتية قائمة تنسق وتتعاون مع بعضها البعض في مجال حماية المعطيات ذات الطابع الشخصي وبنية قانونية متكاملة تقوم على جانب ردعي لتجريم منتهكي البيانات الشخصية وبنية تقنية تتضمن اليات تقنية لتوفير بيئة سليمة للبيانات الشخصية، إلى جانب اليات تنظيمية صارمة داخل المؤسسات والهيئات تتضمن هي الأخرى جوانب ردعي لمنع الوصول الغير المصرح به إلى البيانات.

ومن بين التوصيات التي يمكن تقديمها:

- تعميم القيام بحملات تحسيسية وتوعوية وطنية موجهة للمواطنين للتوعية بأهمية البيانات الشخصية، والخاطر المترتبة في حال مشاركة البيانات عبر الوسائط الرقمية.

- ضرورة إرساء سلطة مستقلة تتقاسم المهام مع السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، بإعتبار أن هذه الأخيرة تتكلف بمهام إستراتيجية ومركزية ووتحمل كافة أعباء حماية البيانات الشخصية، ما يجعلها من الصعب أن تقوم بكل هاته المهام بمفردها.

- تنظيم دورات تكوينية وتدريبية على المستوى الوطني لموظفي المؤسسات العمومية والقطاعات الحساسات بما فيها القطاع البنكي، على كيفية التعامل مع الحوادث السيبرانية.

قائمة الملاحق

دليل المقابلة

الطالبة: قسايسية إكرام زينب.

أتقدم إلى سيادتكم المحترمة، لإجراء مقابلة في إطار علمي لإستكمال إعداد مذكرة تخرج لنيل شهادة الماستر في العلوم السياسية، بهدف جمع المعطيات والبيانات حول موضوع: أهمية الأمن السيبراني في حماية البيانات الشخصية في القطاع البنكي في الجزائر دراسة حالة البنك الخارجي الجزائري من الفترة الممتدة 2020 إلى 2024.

- مقابلة مع السيدة أيت زيان مريم، مهندسة في أمن أنظمة المعلومات بالبنك الخارجي الجزائري، بتاريخ 17 فيفري 2025، على الساعة 9:30.

1. **ماهي الأليات التي يلتزم بها البنك الخارجي الجزائري لحماية البيانات الشخصية على المستوى القانوني؟**
2. **فيما تتمثل اليات التقنية للبنك الخارجي الجزائري في حماية البيانات الشخصية؟**
3. **كيف يتم تطبيق القانون 18-07 داخل البنك؟**
4. **هل هناك سلطة رقابية تقوم بممارسة الرقابة على البنك الخارجي الجزائري في مسألة حماية البيانات الشخصية؟**

- مقابلة مع مدير أمن أنظمة المعلومات بالبنك الخارجي الجزائري، بتاريخ المعلومات التي أجريت بتاريخ 2025/2/10 على الساعة 9:30.

1. **هل تقوم السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي بدورات تدقيق منتظمة؟**
2. **بناءا على أي مرسوم تم تعيين مسؤول أمن نظم المعلومات؟**
3. **ماهي المهام التي يقوم بها مسؤول أمن نظم المعلومات؟**
4. **هل يوجد على مستوى كل بنك مديرية أووحدة مختصة بأمن نظم المعلومات؟**

قائمة المراجع

أولا: المصادر باللغة العربية

أولا: الاتفاقيات الدولية:

1. منظمة التجارة العالمية. الإتفاقية المتعلقة بالجوانب التجارية لحقوق الملكية الفكرية(تريبس). (15أفريل 1944).

2. الاتفاقية الأوروبية لحقوق الإنسان،.روما. في:(4 نوفمبر 1950). مكتبة حقوق الإنسان. جامعة منبوستا.).

3. القاهرة. جامعة الدول العربية. القانون الأساسي للمحكمة العربية لحقوق الإنسان. (07سبتمبر. 2014).

4. ستراسبورغ. المحكمة الأوروبية لحقوق الانسان. الاتفاقية الأوروبية لحقوق الانسان. (04 نوفمبر 1950).

ثانيا: القوانين والمصادر الرسمية.

أ- القوانين:

1. الجمهورية الجزائرية الديمقراطية الشعبية. القانون رقم 18-04 المؤرخ في: 24 شعبان 1439. الموافق لـ 10 ماي 2018.المتعلق بالقواعد المتعلقة بالبريد والاتصالات الالكترونية. الجريدة الرسمية. العدد 27. الصادرة بتاريخ 13 ماي 2018.

2. الجمهورية الجزائرية الديمقراطية الشعبية. القانون رقم 09-04 المؤرخ في: 14 شعبان 1430. الموافق لـ 05 أوت 2009.المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته الجريدة الرسمية. العدد 47. الصادرة بتاريخ: 05- 08- 2009.

3. الجمهورية الجزائرية الديمقراطية الشعبية. القانون رقم 18-07 المؤرخ في: 25 رمضان 1439 الموافق لـ 10 يونيو 2018. المتعلق بحماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي. الجريدة الرسمية. العدد 34. الصادرة بتاريخ 10يونيو2018.

4. الجمهورية الجزائرية الديمقراطية الشعبية. القانون رقم 16-01. المؤرخ في: 26 جمادى الأولى عام 1437 الموافق لـ06 مارس 2016. الجريدة الرسمية. العدد 14. الصادر بتاريخ: 07 مارس 2016.

5. الجمهورية الجزائرية الديمقراطية الشعبية. القانون رقم 04-15. المؤرخ في 27 رمضان 1425 الموافق ل 10 نوفمبر 2004. المعدل والمتمم للأمر رقم 66- 156 المؤرخ في 18 صفر عام 1386 الموافق ل 8يونيو 1966 والمتضمن قانون العقوبات. الجريدة الرسمية. العدد 71. الصادرة بتاريخ: 10 نوفمبر 2011.
6. الجمهورية الجزائرية الديمقراطية الشعبية. القانون رقم 90-11. المؤرخ في 26 رمضان 1410 الموافق لـ 21 أفريل 1990. المتعلق بعلاقات العمل، الجريدة الرسمية. العدد 17. الصادر بتاريخ: 25 أفريل 1990.
7. الجمهورية الجزائرية الديمقراطية الشعبية. القانون رقم 15-04. المؤرخ في 11 ربيع الثاني 1436 الموافق لـ 1 فيفري 2015. المتضمن القواعد العامة المتعلقة بالتوقيع والتصديق الالكتروني. الجريدة الرسمية. العدد 06. الصادر بتاريخ فيفري 2015.
8. الجمهورية الجزائرية الديمقراطية الشعبية. القانون رقم 18-05. المؤرخ في 24 شعبان عام 1439 الموافق لـ 10ماي سنة 2018. المتضمن قانون التجارة الإلكترونية. الجريدة الرسمية. العدد 28. الصادر بتاريخ 16 ماي2018.
9. الجمهورية الجزائرية الديمقراطية الشعبية. القانون 23-09. المؤرخ في 3 ذي الحجة 1444 الموافق ل 21 يونيو2023. المتضمن القانون النقدي والمصرفي. الجريدة الرسمية. العدد 43. الصادر في 27 يونيو 2023.
10. الجمهورية الجزائرية الديمقراطية الشعبية، بنك الجزائر، نظام رقم 25-03المؤرخ في 15 شوال 1446 الموافق ل 14 أفريل 2025. المتعلق بحماية زبائن البنوك. والمؤسسات المالية. والخاضعين الأخرين. في: https://www.bank-of-algeria.dz.
11. الجمهورية الجزائرية الديمقراطية الشعبية. بنك الجزائر. التعليمة رقم 25-02. المؤرخة في 2 مارس 2025.المتعلقة بالشروط الخاصة للترخيص بتأسيس واعتماد وممارسة نشاط البنك الرقمي، في: https://www.bank-of-algeria.dz.

ب- المراسيم:

1. الجمهورية الجزائرية الديمقراطية الشعبية. المرسوم الرئاسي رقم 96-438. المؤرخ في: 26 رجب 1417 الموافق لـ 7 ديسمبر 1996. الجريدة الرسمية. العدد 76. الصادر بتاريخ 8 ديسمبر 1996.
2. الجمهورية الجزائرية الديمقراطية الشعبية. المرسوم الرئاسي رقم 23- 314. المؤرخ في 20 صفر 1445 الموافق ل 6 سبتمبر 2023. المتضمن إنشاء محافظة سامية للرقمنة وتحديد مهامها وتنظيمها وسيرها. الجريدة الرسمية. العدد 59. الصادر بتاريخ 10 سبتمبر 2023.

3. الجمهورية الجزائرية الديمقراطية الشعبية. المرسوم الرئاسي 15-261. المؤرخ في 24 ذي الحجة 1424 الموافق ل8 أكتوبر 2015. المتعلق ب تحديد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها. الجريدة الرسمية. العدد 53، الصادر بتاريخ 8أكتوبر 2015.

4. الجمهورية الجزائرية الديمقراطية الشعبية. المرسوم الرئاسي رقم 19-172. المؤرخ في 3 شوال 1440 الموافق ل 6 يونيو 2019. المتعلق بتحديد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها. الجريدة الرسمية. العدد 37. الصادر بتاريخ 9 يونيو 2019.

5. الجمهورية الجزائرية الديمقراطية الشعبية. المرسوم الرئاسي 20-05. المؤرخ في 24 جمادى الأولى 1441 الموافق ل 20 جانفي 2020. المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية. الجريدة الرسمية. العدد 04. الصادر بتاريخ 26 جانفي2020.

6. الجمهورية الجزائرية الديمقراطية الشعبية. المرسوم الرئاسي 04-183 المؤرخ في 8 جمادى الأولى 1425 الموافق ل 26 يونيو 2004. المتعلق بإحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي. الجريدة الرسمية. العدد 41. الصادر بتاريخ 27 يونيو 2004،

7. الجمهورية الجزائرية الديمقراطية الشعبية. المرسوم التنفيذي رقم 19-271. المؤرخ في 8 صفر 1441 الموافق ل 7أكتوبر 2019.المتعلق بالمرجع الوطني لتوافقية أنظمة الإعلام. الجريدة الرسمية. العدد63. الصادر في 9 أكتوبر سنة 2019.

ت- الأوامر:

1. الجمهورية الجزائرية الديمقراطية الشعبية، الأمر رقم 06-03، المؤرخ في 19 جمادى الثانية 1427 الموافق لـ 15 يوليو 2006. المتضمن القانون الأساسي العام للوظيفة العمومية. الجريدة الرسمية. العدد 46. الصادرة بتاريخ 21 يوليو 2006.

2. الجمهورية الجزائرية الديمقراطية الشعبية. الأمر رقم 66-155. المؤرخ في 18 صفر 1386الموافق لـ 8 يونيو 1966. المتضمن قانون الإجراءات الجزائية. الجريدة الرسمية. العدد48. الصادرة بتاريخ 8 يونيو 1966.

3. الجمهورية الجزائرية الديمقراطية الشعبية. الأمر رقم 03-05. المؤرخ في 19 جمادى الأولى 1424 الموافق لـ 19 جويلية 2003. المتعلق بحقوق المؤلف والحقوق المجاورة. الجريدة الرسمية. العدد 44. الصادر بتاريخ: 23 يوليو 2009.
4. الجمهورية الجزائرية الديمقراطية الشعبية. الأمر رقم 21- 11. المؤرخ في 16 محرم 1443 الموافق ل 25 غشت 2021. المتضمن قانون الإجراءات الجزائية. الجريدة الرسمية. العدد 65. الصادر بتاريخ 26غشت 2021.
5. الجمهورية الجزائرية الديمقراطية الشعبية. الأمر رقم 67 – 204. المؤرخ في 26 جمادى الثانية 1387 الموافق ل 1 أكتوبر 1967.المتضمن إحداث بنك الجزائر الخارجي. الجريدة الرسمية. العدد86. الصادر في 2 رجب 1387.

ثالثا: الكتب والمؤلفات العامة

1. منى الأشقر جبور. **السيبرانية هاجس العصر**. (بيروت. المركز العربي للبحوث القانونية.2017).
2. أسامة حسام الدين. **أساسيات الأمن السيبراني**. (المملكة العربية السعودية. أكاديمية سيسكو بجامعة طيبة. 2017).
3. ذيب بن عايض القحطاني. **أمن المعلومات**. (الرياض. مكتبة الملك فهد الوطنية. (2015).
4. منى الأشقر. جبور ومحمد حيدر. **البيانات الشخصية والقوانين العربية :الهم الأمني وحقوق الأفراد**. (بيروت. المركز العربي للبحوث القانونية والقضائية. مجلس وزراء العدل العرب. جامعة الدول العربية. ط1. 2018).
5. وليم سلامة وآخرون، **الأمن السيبراني للخدمات المالية والمصرفية**. (برلين: المركزالديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية. ج1. 2022)،
6. فريد يابيروشون ميرفي. **علم التشفير مقدمة قصيرة جدا ترجمة: محمد سعد طنطاوي** (جمهورية مصر العربية. مؤسسة هنداوي للتعليم والثقافة. ط1. 2012).
7. محمد فهمي طلبة، **فيروسات الحاسوب وأمن البيانات** (جمهورية مصر العربية. مطابع المكتب المصري الحديث. موسوعة داتا كمبيوتر. 1997).

رابعا : المقالات العلمية

1. عبد القادر صواق، بومدين بوداود. عبد اللطيف أولاد حمودة. "أثر جاهزية الامن السيبراني على الخدمات المصرفية الالكترونية من خلال تقليل المخاطر المدركة. دراسة حالة بنك BDLبغرداية". **مجلة اقتصادية معاصرة**. م 06.ع 01. (2023)،

2. راشد محمد المري. "الامن السيبراني وحماية الأنظمة الالكترونية". **مجلة الدراسات القانونية والاقتصادية**. م09. ع01. (مارس 2023)،
3. إدريس عطية. "مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري". **مجلة مصداقية**. م1.ع 1. (ديسمبر 2019).
4. مني عبد الله السمحان. "متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود". **مجلة كلية التربية**. ع 111. (يوليو 2020).
5. نور الدين حامد إبراهيم." الفضاء السيبراني: المفاهيم والأبعاد". **المجلة العلمية للبحوث والدراسات التجارية**. م 38.ع 02. (2024).
6. علاء الدين فرحات. "الفضاء السيبراني: تشكيل ساحة المعركة في القرن الحادي والعشرين ". **مجلة العلوم القانونية والسياسية**. م10. ع03. (ديسمبر 2019).
7. أميرة عبد العظيم. ومحمد عبد الجواد. "المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام". **مجلة الشريعة والقانون**. ع 35. (2020).
8. محمد دحماني. "الذكاء الاصطناعي كألية لتعزيز الأمن السيبراني". **مجلة الفكر القانوني والسياسي**. م 07. ع 02. (2023).
9. راضية حميدة. "الجريمة الالكترونية عبر مواقع التواصل الاجتماعي: نحو تفعيل دور الأمن السيبراني المعلوماتي "**مجلة الإعلام والمجتمع**. م 05. ع 02. (ديسمبر 2021).
10. عبد الغاني شرقي." التهديدات السيبرانية وإشكالية السيادة: إعادة قراءة للسيادة ومعاهدة واستفاليا". **مجلة السياسة العالمية**. م 07. ع 02. (2023).
11. روان بنت عطية الله الصحفي. "الجرائم السيبرانية". **المجلة الإلكترونية الشاملة متعددة التخصصات**. ع24. (ماي 2025).
12. سميرة معاشي."الجريمة المعلوماتية دراسة تحليلية لمفهوم الجريمة المعلوماتية". **مجلة الفكر**. ع 17. (جوان 2018).
13. منى عبد الله السمحان. "متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود"، **مجلة كلية التربية**. ع 11. (جويلية 2020).
14. خالد ظاهر. عبد الله جابر. السهيل المطيري. "دور التشريعات الجزائية في حماية الأمن السيبراني بدول مجلس التعاون الخليجي". **مجلة البحوث الفقهية والقانونية**. ع38. (جويلية 2022).

15. لامية طالة. "التهديدات والجرائم السيبرانية وتأثيرها على الأمن القومي للدول واستراتيجيات مكافحتها". **مجلة معالم للدراسات القانونية والسلبية.** م 04.ع 02. (2020).
16. سمير بارة." الأمن السيبراني في الجزائر: السياسات والمؤسسات". **المجلة الجزائرية للأمن الإنساني**. م4. (جويلية 2017).
17. جوهر قوادري صامت. "الضوابط القانونية لمعالجة البيانات الشخصية الإلكترونية". **مجلة الدراسات القانونية المقارنة**. م 06.ع02. (27- 12- 2020).
18. هبة رمضان رجب. "الحماية القانونية للبيانات الشخصية في عصر التكنولوجيا الرقمية"، **مجلة العلوم القانونية والاقتصادية**. م66. ع 03. (يناير 2024).
19. سمير سعد ورشاد سلطان. تعزيز الحماية القانونية للبيانات الشخصية الحساسة في مجال الاستدلالات. دراسة مقارنة". **مجلة البحوث القانونية والاقتصادية**. ع 88. (يونيو 2024).
20. نعيمة بوعقبة."معالجة البيانات الحساسة بين الحظر وخصوصية المعالجة. قراءة في قانون حماية المعطيات ذات الطابع الشخصي 18-07". **مجلة سوق القانون**. م 09. ع 01. (2022)،
21. عمر هارون."الهندسةالاجتماعية الجماعية". **مجلة الشرطة**. ع 158. (ماي 2024). ص. 158.
22. ابراهيم السيد احمد رمضان." مواجهة الهجمات السيبرانية في ضوء أحكام القانون الدولي". **مجلة العلوم الاقتصادية والقانونية**. ع 01. (يناير2025).
23. وريدة جندلي. "حماية المعطيات الشخصية في ضوء التشريع الجزائري والمواثيق الدولية: بين الضمانات والتحديات". **المجلة الاكاديمية للبحوث القانونية والسياسية**. م 01. ع 01. (2022).
24. سامية خوانرة. "المبادئ الأساسية لحماية البيانات الشخصية بين الجهود الدولية والتشريع الجزائري". **مجلة الرسالة للدراسات والبحوث الإنسانية**. م 07. ع 03. (ماي 2022).
25. هشام كلو. أحلام شكورة. "الحماية القانونية للمعطيات الشخصية بين الاتفاقيات الدولية والتشريع الجزائري". **مجلة الحقوق والعلوم السياسية**. م10.ع 02. (2022).
26. محمد محمود فياله. "القانون الدولي والتحديات المعاصرة الجريمة السيبرانية نموذجا"، **مجلة الحقوق للبحوث القانونية والاقتصادية**، م 01، ع 01، (يوليو 2024)،
27. محمد أحمد لبيب أحمد. وآخرون."دور الاتفاقيات الدولية والإقليمية في مجال الأمن السيبراني وموقف الدولة المصرية منها". م**جلة الحوكمة والوقاية من الفساد ومكافحته**. ع 01. (سبتمبر 2023)،

28. سامية ساعد."حماية البيانات الشخصية المستهلك من مخاطر الدفع الالكتروني". **مجلة الحقوق والعلوم الإنسانية**. م 15. ع 01. (2022).

29. علي أبو هاني، الأطرش كريفف."النظام الإفريقي لحقوق الإنسان ودوره في تعزيز وحماية حقوق الإنسان، وحرياته الأساسية". **المجلة العربية للأبحاث والدراسات في العلم الانسانية والاجتماعية**. م 13.ع 05. (أكتوبر 2021).

30. أسامة غربي."المنظمة الدولية للشرطة الجنائية (الإنتربول) ودورها في مكافحة الجريمة المنظمة". **المجلة دراسات و أبحاث**. ع 3. (مارس 2011).

31. محمد نذير بن عرفه. يوسف حوري. "اليوروبول كآلية لمكافحة الجريمة الالكترونية". **مجلة الدراسات القانونية والسياسية**. م 11.ع 01. (جانفي 2025).

32. عبد العزيز لزعر. رشيد زياني. "آليات الاتحاد الإفريقي للتعاون الشرطي (الافريبول) ودورها في مكافحة الجريمة الالكترونية" .**مجلة متون**. م 14. ع 03. (سبتمبر 2021).

33. محمد بوكبشة. "الأمن والدفاع السيبراني أولوية قصوى". **مجلة الجيش**. ع 651. (أكتوبر 2017).

34. غنية حساني. "العصب الرقمي لرصد الجريمة المعلوماتية". **مجلة الشرطة**. ع (158). (2024).

35. فتيحة حزام. "حماية الأنظمة الرقمية بين الآليات التقنية وأجهزة الحماية قراءة في أحكام المرسوم الرئاسي 20-05". **مجلة الحقوق والعلوم السياسية.** ع 3. (أكتوبر 2020).

36. هيام اسماعيل عبد الفتاح السحماوي."بصمة الوجه الإلكتروني وحجيتها في الإثبات المدني دراسة مقارنة". **مجلة البحوث القانونية والاقتصادية.** م2.ع2.(يوليو 2023).

37. فاتح مرزوق وياسين عطا الله."الخدمات المصرفية ودروها في تسهيل التجارة الخارجية دراسة حالة بنك الخارجي الجزائري BEA". **مجلة الجغر افيا الاقتصادية**. م 2.ع1.(2025).

خامسا: المداخلات في الملتقيات والندوات الأكاديمية

1. بن عديد سامية، مداخلة بعنوان مخاطر **الامن السيبر اني والمعلوماتي وتطور المعرفة التقنية على برامج الحماية للأنظمة المعلوماتي**. وزارة التعليم العالي والبحث العلمي. جامعة محمد الشريف مساعدية. سوق أهراس. الجزائر. (28 أكتوبر2023).

سادسا: المذكرات والرسائل الجامعية:

أ- أطروحات الدكتوراه

1. عبد الهادي كحلاوي .الحماية **القانونية للبيانات الشخصية**. أطروحة دوكتراه غير منشورة. (جامعة أحمد دراية بأدرار. قسم العلوم الحقوق والعلوم السياسية. 2022/2021.).
2. خضرة شنتير. **الآليات القانونية لمكافحة الجريمة الالكترونية دراسة مقارنة.** أطروحة دكتوراه غير منشورة. (جامعة أحمد دراية. أدرار: كلية الحقوق والعلوم السياسية. 2021/2020).
3. حسين ربيعي. **اليات البحث والتحري في الجرائم المعلوماتية.** أطروحة دوكتراه غير منشورة. (جامعة باتنة. كلية الحقوق والعلوم السياسية. 2016/2015.).
4. عبد القادر صواق. **مساهمة الأمن السيبراني للبيانات في تعزيز الثقة لدى العملاء نحو الخدمات.** أطروحة دكتوراه غير منشورة. (جامعة غرداية: كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير. 2025/2024).

ب- مذكرات الماستر:

1. إيمان بوجلة. فطيمة يحياوي. نبيل جحا. **التأمين السيبراني. تجارب دولية**. مذكرة ماستر غير منشورة. (جامعة ابن خلدون: كلية العلوم الاقتصادية والتجارية وعلوم التسيير.2023/2022).
2. كاملي محمد، فتيحة زرازقة. **الاستراتيجية الأمنية لتحقيق الامن السيبراني**. مذكرة ماستر غير منشورة. (جامعة عمار ثليجي: كلية الحقوق والعلوم السياسية.2019/2018).
3. حليمة علالي، **الحماية الجنائية للمعطيات الشخصية في التشريع الجزائري (قانون18-07)**. مذكرة ماستر غير منشورة. (جامعة قاصدي مرباح. كلية الحقوق والعلوم السياسية.2019/2018).
4. نصير بوعكاز. سعيد بوعكاز. **التأمين من المخاطر السيبرانية تجارب دولية**. مذكرة ماستر غير منشورة. (جامعة ابن خلدون: كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير. 2023/2022).
5. شيماء مرزوق. وزين تركية جلال. **انعكاسات الامن السيبراني على أمن المعلومات في البنوك**. مذكرة ماستر غير منشورة. (جامعة الشهيد الشيخ العربي التبسي: كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير. 2024/2023).
6. العبد شعبان. مسعود مرتقي. **الجرائم السيبرانية في القانون الجزائري**، مذكرة ماستر غير منشورة. (جامعة زيان عاشور: كلية الحقوق والعلوم السياسية. 2022/2021).

7. عمار حشمان. **الجريمة المعلوماتية في التشريع الجزائري**. مذكرة ماستر غير منشورة (جامعة قاصدي مرباح. كلية العلوم الاقتصادية والتجارية وعلوم التسيير. 2019/2018.).

سابعا: المحاضرات:

1. جمال بوزايدة. **محاضرات في الامن السيبراني**. (جامعة الجزائر03: كلية الحقوق والعلوم السياسية.2020 / 2021).

تاسعا: المقابلات:

1. مقابلة مع السيدة أيت زيان مريم، مهندسة في أمن أنظمة المعلومات بالبنك الخارجي الجزائري، بتاريخ 17 فيفري 2025، على الساعة 9:30.
2. مقابلة مع مدير أمن أنظمة المعلومات بالبنك الخارجي الجزائري، بتاريخ المعلومات التي أجريت بتاريخ 2025/2/10 على الساعة 9:30.

عاشرا: المواقع الإلكترونية:

أ- المواقع الرسمية:

1. وزارة البريد والمواصلات السلكية واللاسلكية. **مرجع أمن المعلومات**. https: www.mpt.gov.dz
2. الجمهورية الجزائرية الديمقراطية الشعبية، **البنك الخارجي الجزائري**، في :*https://www.bea.dz/article*.
3. تاريخ البنك، https://www.bank-of-algeria.dz.
4. بنك الخارجي لجزائري يرفع رأسماله إلى 230 مليار دينار جزائري، في:*https://www.aps.dz/ar/economie*،

ب- المواقع الغير الرسمية:

1. دويتشه فيلله. **تعرف على خمسة من أخطر فيروسات الحاسوب في:** https://www.aljazeera.net/tech/2016/11/1:.
2. *فراس اللو. فيروس "أريد البكاء" ...الفدية في مقابل فك التشفير. في: https://www.aljazeera.net.cdn.a;pproject.org*،).
3. ياقوت زهرة القدس بن عبد الله. **لحوكمة البيانات وتعزيز التشغيل البيني** في: https://www.elbadilabc-ar.dz/gouveranace-/
4. قايد صالح الجيش يواصل مساره الوطني النير. في: https://www.elbilad.net/evenemen

I. المصادر باللغة الأجنبية:

1. Anthony McCartney. "The McCumber cube model". **College of Science and technology** (January 2024).
2. *Avijit Malik and others. «Man in the middle -attack: Understanding in simple words." **International Journal Of Data Network Science**. (2019).*
3. *Cyber Management school. **Qu'est-ce que le vol des données ? (Datatheft) . Dans :** https://www.proofpoint.com/fr/threat-reference/data-theft.*
4. *Centre D'expertise En Sécurité De L'information, **Chiffrement des données en transit et au repos** (université Du Québec, Juillet 2024.)*
5. *Diffusion restreinte: garantir la protection la protection des information sensibles, dans :https://www.oodrive.com/fr/guide/diffusion-restreinte.*
6. *Embarka ben Brahim et selyana Amiche, **mise place d'une solution de détection d'intrusion**. Mémoire de master (faculté de génie Electrique et informatique. Université Mouloud Mammeri de tizi-ouzou.2017.).*
7. *El Gharbi Selmani. **Mise en place d'un IDS pour sécuriser un réseau en utilisant snort.** mémoire de master (faculté de génie électrique et d'informatique. université Moloud mammeri Tizi-ouzou. 2019/2020).*
8. *Fonctionnement d'un système de sauvegarde redondant, dans :https://www.oodrive.com/fr/blog/sauvegarde/sauvegarde-donnees.*
9. *Justine Gretten. **Cyberattaques quels sont les risques pour votreentreprise.Dans :** Https://www.mailinblack.com/resources/blog/cyberattaues.*
10. *Iso 27000 comprendre et maîtriser les normes pour une sécurité de l'information optimale. Dans : Https://www.makeitsafe.fr/Iso.*

11. *Iso/IEC27001 :2022, dans : https// : www.iso.org/fr/standard/27001lifecycle.*
12. *Iso 27003 : **guide pratique pour mettre en œuvre un SMSI efficace** dans :https://www.makeitsafe.fr/Iso-27003-guide-pratiques.*
13. *Interphone connecte : comment la domatique révolutionne l'expérience de sécurité, dans :https://www.access-protection.fr/actualites/interphone-connecte-comment-la-domotique-revolutionne-lexperience-de-securite/.*
14. *Guide Complet du contrôle d'accès biométrique. dans :https://sirixmonitoring.com/fr/blog/guide-du-controle-dacces-biometrique*
15. *Kurt baker. **The Zeus trojan malware-definition and prevention** in:https://www.crowdstrike.com/en-us/cybersecurity-101/malware/zues.*
16. *Luke Noonane. **5Damaging consequences of Data breach: protect your assests**.in; https://www.metacompliance.com/blog/data-breaches/5-damaging-consquences-of-a-data-breach.*
17. *Lamia El Fachtali. **Normes ISO 27000**. Dans : https://fr.scribd.com/document/30445143/normes-ISO-27000.*
18. *L'importance des audits de sécurité réguliers pour maintenir la protection des données. dans :https://bienvenum.org/limportance-des-audits-de-securite-reguliers-pour-maintenir-la-protection-des-donnees*
19. *Qu'est-ce qu'un pare-feu d'application web (waf). dans : https://www.f5.com/fr_fr/glossary/web-application-firewall-waf*
20. *Qu'est-ce qu'un test de vulnérabilité ?dans ; https://www.vumetric.com/fr/blogue/quest-ce-que-le-test-de-vulnerabilite-*

21. *La République algérienne démocratique et populaire. ministère des postes et des télécommunications.* ***guide nationale référentiel de la sécurité de l'information****.(2020).*
22. *La République Française. Club de la Sécurité des systèmes D'information Française.* ***Technique de contrôle d'accès par biométrie. (2003).***
23. *Les contrôles d'accès physiques pour la gestion des accès et la sécurité de vos locaux, dans . :* *https://heimdoor.com/actualites/controle-acces-physiques.*
24. *Nouara Messahel et Khadra Saadi.* ***Installation et configuration d'un firewall logiciel****. mémoire de master. (univeristé Mouloud Mammeri de Tizi Ouzou. Faculté de Génie électrique et d'informatique. 2016/2017).*

25. *Nikita Dugga.* ***what is Data Processing? Types x examples Explained****. in: https://www.sImplilearn.com/What is data process.*
26. *Nesrine Adad****, La mise au point d'un antivirus****, Mémoire de Master (université Abou Baker Belkaid-Telmcen. Faculté des sciences Département D'informatique.2015/2016).*
27. *SabahAl-fedaghi. Khaled Al-Saqab. Bernhard Thalheim.* ***information stream-based model for organizing security.*** *computer engineering department. University of Kuwait. (April2008).*
28. *Salma Bahaza et tidjani Mammeri.* ***Déploiement d'une solution Antivirus sein du réseau de campus universitaire Ouargla****. Mémoire de master (université kasdi Merbah Ouargla. Faculté des nouvelles technologies de l'information de la communication. 2024/2015).*
29. *Sauvegarde des donnéés : Définition. types et solutions. dans ;https://objectfirst.com/fr/guides/data-backup/data-backup-definition-options-types-and-solutions/.*

30. *Tout Savoir Sur La Sécurité des datacenters (centre de données). dans :https://www.proofpoint.com/fr/threat-reference/data-center-securite.*

31. *Yacine Hadj Sadok et Abderrahmane. **Etude et mise en place d'un PAM**. Mémoire de MASTER. (Faculté des sciences. Université Saad Dahlab. Blida. 2022/2023).*

فهـــرس الأشكال

فهرس الأشكال

قائمة المختصرات

الرمز	مدلوله
Iso	***المنظمة الدولية للتوحيد القياسي***
IDS	***نظام كشف التسلل***
NIDS	***نظام كشف التسلل القائم على المضيف***
HIDS	***نظام كشف التسلل القائم على الشبكة***
GDPR	***اللائحة الأوروبية العامة لحماية البيانات***
RSSI	***مسؤول أمن نظم المعلومات***
DSSI	***مديرية أمن نظم المعلومات***
ANPDP	***السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي***
SSL	***طبقة المقابس الأمنة***
TLS	***أمان طبقة النقل***

فهرس المواضيع