الحماية المدنيَّة للأمن السّيبراني
Civil Protection for Cyber Security

بحث مقدَّم من قبل
المدرِّس الدكتور عمَّار ياسر حسون العاندي – جامعة واسط ـ كلية القانون
ay8707651@gmail.com

الخلاصة.
تُعَدُّ الحمايةُ المدنيَّةُ للأمنِ السّيبرانيِّ من أبرزِ مُتطلَّباتِ العصرِ الرَّقميِّ، إذ تستهدفُ حمايةَ الأفرادِ والبنى التحتيَّةِ المدنيَّةِ من التَّهديداتِ الإلكترونيَّةِ المتناميةِ. وفي هذا الإطارِ، سعتْ فرنسا إلى بناءِ منظومةٍ متقدِّمةٍ ترتكزُ على استراتيجيَّاتٍ وطنيَّةٍ وهيئاتٍ متخصِّصةٍ، من أبرزِها الوكالة الوطنيَّة لأمن نظم المعلومات(ANSSI) ، في حين عملت مصرُ على تعزيزِ الإطارِ التشريعيِّ بإصدارِ قوانينَ بارزةٍ، مثل قانون مكافحة الجرائم الإلكترونيَّة المصري لعام 2018 وقانون حماية البيانات المصري لعام 2020، إلى جانبِ تطويرِ مراكزِ استجابةٍ وطنيَّةٍ متخصِّصةٍ.
أمَّا العراق، فقد بدأتْ ملامحُ الحمايةِ المدنيَّةِ فيهِ بالتَّشكُّلِ من خلالِ قانونِ مكافحة الجرائم المعلوماتيَّة العراقي لسنة 2023، وجهودٍ مؤسَّسيَّةٍ تستهدفُ حمايةَ المرافقِ الحيويَّةِ من الهجماتِ الإلكترونيَّةِ، وتكمنُ أهميَّةُ هذه الحمايةِ في تعزيزِ الاستقرارِ الوطنيِّ، وصيانةِ الحقوقِ الرَّقميَّةِ، وضمانِ استمراريَّةِ تقديمِ الخدماتِ العامَّةِ دونَ انقطاعٍ أو تعطيلٍ.

الكلمات المفتاحيَّة: الحماية المدنيَّة، الأمن السيبراني، البيئة الرقميَّة.

Abstract;
Cybersecurity civil protection has become a vital requirement in the digital age, aiming to safeguard individuals and civil infrastructure from cyber threats. France has developed an advanced framework through national strategies and specialized agencies, most notably the National Cybersecurity Agency (ANSSI). In Egypt, the legislative environment has been reinforced by key laws, including the Cybercrime Law of 2018 and the Personal Data Protection Law of 2020, alongside the development of national incident response centers. Iraq has also begun shaping its civil protection landscape with the enactment of the 2023 Cybercrime Law and institutional efforts to secure critical infrastructures.
This protection plays a key role in promoting national stability, ensuring digital rights, and maintaining the continuity of public services.

المُقدِّمة:

في العصرِ الرَّقميِّ الرَّاهنِ، أصبحَ الأمنُ السّيبرانيُّ حَجرَ الزَّاويةِ في حمايةِ المُجتمعاتِ الحديثةِ من التَّهديداتِ الرَّقميَّةِ المُتنامية، ومع تزايدِ الاعتمادِ على التِّكنولوجيا في مؤسَّساتِ الدَّولةِ ومرافقِها الحيويَّة، أضحَت الحاجةُ إلى منظومةٍ فعَّالةٍ للحمايةِ المدنيَّةِ في الفضاءِ السّيبرانيِّ من أبرزِ تحدِّياتِ السِّيادةِ الوطنيَّةِ، وتُشيرُ الحمايةُ المدنيَّةُ للأمنِ السّيبرانيِّ إلى مجموعِ الإجراءاتِ القانونيَّةِ والتنظيميَّةِ والفنيَّةِ التي تتَّخذُها الدَّولةُ لحمايةِ المواطنينَ والمصالحِ المدنيَّةِ من التَّهديداتِ الرَّقميَّة، سواءٌ أكانتْ هجماتٍ خبيثةً، أم اختراقاتٍ، أم تسريباتٍ للبياناتِ، أم تعطيلًا للبنى التحتيَّةِ الحيويَّةِ.وقد أدركتِ الدُّولُ، على اختلافِ أنظمتِها القانونيَّةِ، أهميَّةَ هذه الحمايةِ، فسَعتْ إلى وضعِ أُطرٍ تشريعيَّةٍ واستراتيجيَّةٍ مُتكاملةٍ لضمانِ مرونةِ مؤسَّساتِها واستمراريَّةِ خدماتِها، مع احترامِ حقوقِ الأفرادِ وحُريَّاتِهم الرَّقميَّة. وتمثِّلُ فرنسا نموذجًا رائدًا في هذا المجالِ، من خلالِ بنيةٍ تنظيميَّةٍ مُتقدِّمةٍ تقودُها الوكالةُ الوطنيَّةُ لأمنِ نُظُمِ المعلومات (ANSSI)، واستراتيجيَّةٍ شاملةٍ تُعزِّزُ من صُمودِ القطاعاتِ المدنيَّةِ أمامَ المخاطرِ السّيبرانيَّة، ولا سيَّما في مجالاتِ الطَّاقةِ، والصِّحَّة، والاتِّصالات.أمَّا مصرُ، فقد اتَّخذتْ خلالَ العقدِ الأخيرِ خطواتٍ ملحوظةً لتعزيزِ أمنِها السّيبرانيِّ المدنيِّ، حيثُ أقَرَّتْ قوانينَ مهمَّةً، مثل قانون مكافحة جرائم تقنيَّة المعلوماتِ لسنة 2018 وقانون حمايةِ البياناتِ الشخصيَّةِ لسنة 2020، إلى جانبِ إنشاءِ مراكزَ وطنيَّةٍ للاستجابةِ للطَّوارئ السّيبرانيَّةِ وتطويرِ استراتيجيَّاتٍ للمرونةِ الرَّقميَّةِ في المؤسَّساتِ الحكوميَّةِ والخاصَّة، سعيًا إلى حمايةِ البنيةِ التحتيَّةِ الرَّقميَّة، وضمانِ الحقوقِ الرَّقميَّةِ للمواطنين، والتَّصدِّي لأيِّ تهديداتٍ تمسُّ الأمنَ المدنيَّ.وفي العراق، ورغمَ التحدِّياتِ الأمنيَّةِ والسِّياسيَّة، ظهرتْ جهودٌ تشريعيَّةٌ ومؤسَّسيَّةٌ لتعزيزِ الأمنِ السّيبرانيِّ المدنيِّ، من خلالِ إصدارِ قانون مكافحة الجرائم المعلوماتيَّة لسنة 2023، وتشكيلِ فرقٍ فنيَّةٍ وأمنيَّةٍ مُختصَّةٍ بحمايةِ البنى التحتيَّةِ المدنيَّةِ الحسَّاسة، كما يسعى العراقُ إلى الانخراطِ في الشَّراكاتِ الإقليميَّةِ والدَّوليَّةِ في مجالِ الأمنِ السّيبرانيِّ، وتعزيزِ التَّوعيةِ المجتمعيَّةِ بالأخطارِ الرَّقميَّة، في ظلِّ تصاعُدِ الهجماتِ الإلكترونيَّةِ التي تستهدفُ مؤسَّساتِ الدَّولةِ والمرافقَ الخدميَّة.وعليهِ، تُمثِّلُ دراسةُ الحمايةِ المدنيَّةِ للأمنِ السّيبرانيِّ في هذه الدُّولِ الثَّلاثِ ميدانًا مُهمًّا لفَهمِ كيفيَّةِ تفاعُلِ الأنظمةِ القانونيَّةِ والمؤسَّسيَّةِ مع المخاطرِ الرَّقميَّة، ورَصدِ أوجُهِ التقدُّمِ والقصورِ في بناءِ بيئةٍ إلكترونيَّةٍ آمنةٍ ومستقرَّةٍ تحفظُ مصالحَ الأفرادِ والدَّولةِ على حدٍّ سواء.

أوَّلًا: أهميَّةُ البحث:

تنبعُ أهميَّةُ هذا البحثِ من التَّطوُّرِ المتسارعِ الذي يشهدهُ الفضاءُ الإلكترونيُّ، وتزايدِ التَّهديداتِ التي تستهدفُ الأفرادَ والمؤسَّساتِ عبرَ الوسائلِ الرَّقميَّة، مثلَ الاختراقِ، والتَّشهير، وانتهاكِ الخصوصيَّة، وتعطيلِ الأنظمة، وغيرها من الأفعالِ التي باتتْ تُشكِّلُ مصدرًا فعليًّا للضَّرر. وفي هذا السِّياقِ، يُعَدُّ الأمنُ السّيبرانيُّ جزءًا لا يتجزَّأُ من الأمنِ القوميِّ والعدالةِ الاجتماعيَّة، وتُعَدُّ الحمايةُ المدنيَّةُ أحدَ المُرتكزاتِ الأساسيَّةِ التي يجبُ أن تستجيبَ لهذا التحدِّي.ونظرًا لافتقارِ التَّشريعِ العراقيِّ - حتى الآنَ - إلى قانونٍ خاصٍّ ومُنظَّمٍ يُنظِّمُ الحمايةَ المدنيَّةَ للأمنِ السّيبرانيِّ، فإنَّ هذا الموضوعَ يكتسبُ أهميَّةً مُضاعفةً، من حيثُ الحاجةُ إلى سدِّ الفَراغِ التَّشريعيِّ، وفَهمِ كيفيَّةِ توظيفِ القواعدِ المدنيَّةِ التَّقليديَّةِ في معالجةِ المُستجدَّاتِ الرَّقميَّة، وتقديمِ مقترحاتٍ لتعزيزِ النِّظامِ القانونيِّ العراقيِّ في هذا المجالِ الحسَّاس.

ثانيًا: إشكاليَّةُ البحث:

تنطلقُ إشكاليَّةُ هذا البحثِ من التوتُّرِ القائمِ بين القواعدِ العامَّةِ للمسؤوليَّةِ المدنيَّةِ في العراق، بوصفِها ثمرةً لتطوُّرٍ قانونيٍّ تقليديٍّ يرتبطُ ببيئةٍ ماديَّةٍ واقعيَّة، وبينَ طبيعةِ الفضاءِ السّيبرانيِّ الذي يقومُ على البنى الرَّقميَّةِ غيرِ الماديَّة، ويتَّسمُ بالسُّرعةِ والتَّعقيدِ والعابريَّةِ للحدود. ومن ثمَّ، تُثارُ الإشكاليَّةُ الجوهريَّةُ الآتية:

إلى أيِّ مدى تُشكِّلُ القواعدُ العامَّةُ للمسؤوليَّةِ المدنيَّةِ في القانونِ العراقيِّ إطارًا كافيًا للحمايةِ من الأضرارِ النَّاشئةِ عن الأفعالِ السّيبرانيَّة، وما مدى الحاجةِ إلى تنظيمٍ تشريعيٍّ خاصٍّ يستجيبُ لخصوصيَّةِ هذا الفضاءِ الإلكترونيِّ؟

وتتشعَّبُ عن هذه الإشكاليَّةِ الرَّئيسةِ جملةٌ من الأسئلةِ الفرعيَّة، أبرزُها:

1- ما صورُ الأضرارِ القابلةِ للتَّعويضِ في المجالِ السّيبرانيِّ؟
2- ما التحدِّياتُ القانونيَّةُ والفنيَّةُ التي تُواجهُ المتضرِّرَ في إثباتِ الضَّررِ والمطالبةِ بالتَّعويض؟
3- هل توجَدُ سوابقُ قضائيَّةٌ عراقيَّةٌ تعكسُ توجُّهًا نحوَ الاعترافِ بالضَّررِ السّيبرانيِّ؟
4- ما دورُ التَّشريعاتِ المقارَنةِ في سدِّ النَّقصِ الذي يُعاني منهُ النِّظامُ القانونيُّ العراقيُّ؟

ثالثًا: أهدافُ البحث:

يسعى هذا البحثُ إلى تحقيقِ الأهدافِ الآتية:

1- بيانُ الإطارِ النظريِّ والقانونيِّ للحمايةِ المدنيَّةِ للأمنِ السيبراني، بالاستنادِ إلى القانونِ المدنيِّ العراقيِّ، والمبادئِ العامَّةِ في المسؤوليَّةِ التقصيريَّةِ والعقديَّة.
2- تحليلُ طبيعةِ الضررِ السيبرانيِّ القابلِ للتعويض، وشرحُ صورِ الأضرارِ الماديَّةِ والمعنويَّةِ التي قد تنشأُ عن الأفعالِ الإلكترونيَّة.
3- رصدُ التحدياتِ القانونيَّةِ والإجرائيَّةِ التي تُعيقُ تفعيلَ الحمايةِ المدنيَّةِ في البيئةِ الرقميَّةِ العراقيَّة، ولا سيَّما ما يتعلَّقُ بصعوبةِ الإثباتِ والقصورِ التشريعيِّ.
4- استعراضُ أبرزِ المواقفِ القضائيَّةِ ذاتِ الصِّلةِ لتقييمِ مدى استجابةِ القضاءِ المدنيِّ العراقيِّ للمستجدَّاتِ السيبرانيَّة.

5- تقديمُ توصياتٍ عمليَّةٍ وتشريعيَّةٍ تُسهمُ في بناءِ منظومةٍ قانونيَّةٍ فعَّالةٍ لحمايةِ الحقوقِ الرقميَّةِ في العراق، بما يشملُ الدَّعوةَ إلى سَنِّ قانونٍ خاصٍّ بالأمنِ السيبراني، وقانونٍ لحمايةِ البياناتِ الشخصيَّةِ، وتطويرَ أدواتِ الإثباتِ الرقميِّ.

رابعًا: منهجيَّةُ البحثِ:

يعتمدُ هذا البحثُ في دراستِه لموضوعِ الحمايةِ المدنيَّةِ للأمنِ السيبرانيِّ في التشريعِ العراقيِّ على المنهجِ التحليليِّ – الوصفيِّ، بوصفِه المنهجَ الأنسبَ لتحليلِ النصوصِ القانونيَّةِ القائمةِ، واستقراءِ المفاهيمِ المدنيَّةِ ذاتِ الصِّلةِ بالمسؤوليَّةِ الناشئةِ عن الأفعالِ السيبرانيَّةِ، مع رصدِ التحدياتِ العمليَّةِ والتشريعيَّةِ التي تُواجهُ تطبيقَ هذه القواعدِ في الواقعِ الرقميِّ.

خامسًا: خطَّةُ البحثِ:

- **المبحثُ الأوَّلُ: ماهيَّةُ الأمنِ السيبرانيِّ.**
  - المطلبُ الأوَّلُ: مفهومُ الأمنِ السيبرانيِّ.
  - المطلبُ الثاني: عناصرُ الأمنِ السيبرانيِّ.
- **المبحثُ الثاني: حمايةُ الأمنِ السيبرانيِّ والتحدياتُ التي يُواجهُها.**
  - المطلبُ الأوَّلُ: القانونُ المدنيُّ كآليَّةٍ لحمايةِ الأمنِ السيبرانيِّ.
  - المطلبُ الثاني: تحدياتُ الحمايةِ المدنيَّةِ للأمنِ السيبرانيِّ.

المبحث الأوَّل/ ماهيَّةُ الأمنِ السيبرانيِّ

أصبحَ الفضاءُ الرَّقميُّ أحدَ الميادينِ الأساسيَّةِ التي تتحرَّكُ فيها الدُّولُ والأفرادُ على حدٍّ سواءٍ، وتحوَّلَ إلى بيئةٍ حيويَّةٍ تُدارُ من خلالها المعاملاتُ، وتُخزَّنُ فيها المعلوماتُ، وتُمارَسُ فيها الحقوقُ والواجباتُ، غيرَ أنَّ هذا الامتدادَ التكنولوجيَّ صاحَبَهُ نموٌّ مُوازٍ في المخاطرِ والتهديداتِ، تمثَّلَ في أنشطةِ اختراقٍ، وتخريبٍ، وسرقةِ بياناتٍ، وانتحالِ هُويَّةٍ، وجرائمَ إلكترونيَّةٍ تتجاوزُ - في كثيرٍ من الأحيانِ - الحدودَ الجغرافيَّةَ للدُّولِ، ومن هنا برزَ مفهومُ الأمنِ السيبرانيِّ بوصفِه الاستجابةَ القانونيَّةَ والتنظيميَّةَ والتقنيَّةَ لتلكَ التهديداتِ، في سبيلِ حمايةِ النُّظمِ المعلوماتيَّةِ والبنى التحتيَّةِ الرقميَّةِ من المخاطرِ العابرةِ للحدودِ.

ويُعَدُّ الأمنُ السيبرانيُّ - بحسبِ المفهومِ المعاصرِ - مظلَّةً شاملةً تتضمَّنُ الإجراءاتِ والتدابيرَ الراميةَ إلى حفظِ سرِّيَّةِ المعلوماتِ وسلامتِها وتوافُرِها، إلى جانبِ حمايةِ الأفرادِ من الاعتداءاتِ الواقعةِ على خصوصيَّاتِهم الرقميَّةِ أو ممتلكاتِهم المعلوماتيَّةِ، وقد اتَّسعتْ أهمِّيَّةُ هذا المفهومِ تدريجيًّا ليُصبحَ عنصرًا مركزيًّا من عناصرِ الأمنِ القوميِّ للدُّولِ. وعليهِ، فإنَّنا سنبحثُ في مفهومِ الأمنِ السيبرانيِّ من جهةٍ، والعناصرِ التي يقومُ عليها من جهةٍ أخرى، وذلكَ في المطلبَيْنِ الآتيَيْنِ:

المطلب الأوَّل/مفهومُ الأمنِ السيبرانيِّ

جاءَ الأمنُ السيبرانيُّ من كلمتَيْ «Cyber security»، وكلمةُ «سيبر» لاتينيَّةُ الأصلِ، ومعناها «الفضاءُ المعلوماتيُّ»، فيُصبحُ المقصودُ بالأمنِ السيبرانيِّ: «أمنُ الفضاءِ المعلوماتيِّ»، وهو تعبيرٌ أشملُ وأعمُّ من أمنِ المعلوماتِ؛ لذا يُمكنُ القولُ إنَّ الأمنَ السيبرانيَّ هو مجموعةُ الوسائلِ التقنيَّةِ والإداريَّةِ التي تُستخدَمُ لمنعِ الاستخدامِ غيرِ المشروعِ أو سوءِ الاستغلالِ، واستعادةِ المعلوماتِ الإلكترونيَّةِ ونُظُمِ الاتصالاتِ والمعلوماتِ التي تحتويها، بهدفِ ضمانِ توافُرِ واستمراريَّةِ عملِ نُظُمِ المعلوماتِ، وتأمينِ حمايةٍ وسرِّيَّةٍ وخصوصيَّةٍ للبياناتِ الشخصيَّةِ للمواطنينَ[1].ويشملُ الأمنُ السيبرانيُّ أمنَ المعلوماتِ على أجهزةِ وشبكاتِ الحاسبِ الإلكترونيِّ، بما في ذلكَ العمليَّاتُ والآليَّاتُ التي يتمُّ من خلالها حمايةُ مُعدَّاتِ الحاسبِ الإلكترونيِّ والمعلوماتِ والبياناتِ من أيِّ تدخُّلٍ غيرِ مقصودٍ أو غيرِ مسموحٍ به، أو أيِّ تغييرٍ أو إتلافٍ قد يحدثُ، ولقد أصبحَ الأمنُ السيبرانيُّ ركيزةً أساسيَّةً في كلِّ المنظَّماتِ والمؤسَّساتِ، بلْ وفي الدُّولِ، لمواجهةِ الحروبِ الإلكترونيَّةِ المستقبليَّةِ. وتتعدَّدُ مفاهيمُ الأمنِ السيبرانيِّ؛ فهُناكَ مَن يُوسِّعُها لتعبِّرَ عن القدرةِ على حمايةِ بياناتِ الدَّولةِ وشبكاتِها، مثلَ تعريفِ « Lewis J. A.» بأنَّهُ: «حمايةُ شبكاتِ الحاسوبِ والمعلوماتِ التي تحتويها من الاختراقِ أو التدميرِ أو الاضطراباتِ الضارَّةِ»، وهو ما يُعَدُّ من صميمِ مفهومِ الأمنِ السيبرانيِّ[2].

ويتناولُ مفهومُ **الأمنِ السيبرانيِّ** في الفقهِ والتشريعِ الفرنسيِّ مجموعةً من القواعدِ والإجراءاتِ التي تهدفُ إلى حمايةِ الفضاءِ السيبرانيِّ - بما في ذلكَ الأنظمةُ المعلوماتيَّةُ والبنى التحتيَّةُ الرقميَّةُ - من الهجماتِ والتهديداتِ الإلكترونيَّةِ.

والواقعُ أنَّ مصطلحَ «الأمنِ السيبرانيِّ» (la cybersécurité) لم يكنْ رائجًا في الفقهِ القانونيِّ الفرنسيِّ حتَّى العقدَيْنِ الأخيرَيْنِ، غيرَ أنَّ تطوُّرَ التقنيَّةِ الرقميَّةِ، والزيادةَ المتسارعةَ في التهديداتِ الإلكترونيَّةِ، دفعتِ الفقهاءَ الفرنسيِّينَ إلى معالجتِه بجدِّيَّةٍ متزايدةٍ.ويُعرِّفُ الفقهُ الفرنسيُّ الأمنَ السيبرانيَّ بأنَّهُ: «مجموعةٌ من الوسائلِ القانونيَّةِ والتقنيَّةِ والتنظيميَّةِ التي تهدفُ إلى حمايةِ نُظُمِ المعلوماتِ والشبكاتِ الرقميَّةِ من أيِّ اختراقٍ أو تخريبٍ أو تسريبٍ أو استخدامٍ غيرِ مشروعٍ»[3]، ويُعَدُّ الأمنُ السيبرانيُّ - وفقًا للفقهِ الحديثِ - فرعًا من فروعِ الأمنِ القوميِّ، ويشملُ حمايةَ ما يأتي:

- البياناتِ الحسَّاسةِ (Public / Private Data)
- البنى التحتيَّةِ الحيويَّةِ (Infrastructures Critiques)
- العمليَّاتِ الحيويَّةِ في الدَّولةِ (خدماتِ الطَّاقةِ، والصِّحَّةِ، والنَّقلِ، إلخ).

وقد اعتمدَ المُشرِّعُ الفرنسيُّ تعريفًا عمليًّا وواسعًا للأمنِ السيبرانيِّ، ولا سيَّما بعد عامِ 2013م مع صدورِ قوانينَ مهمَّةٍ؛ ومن ذلك **Code de la défense** الذي نصَّ في مادَّتِهِ L.2321-1 على أنَّ الدَّولةَ تتحمَّلُ مسؤوليَّةَ الأمنِ السيبرانيِّ للبنى التحتيَّةِ الحيويَّةِ[4]، وكذلك **Loi de programmation militaire (LPM) 2013-2019** الذي يُعَدُّ نقطةَ تحوُّلٍ؛ إذْ

أقرَّ إلزاميَّةَ اتخاذِ تدابيرَ لحمايةِ نُظُمِ المعلوماتِ الحيويَّةِ[5]، كما أنَّ – **2019 Cybersecurity Act** قد فُعِّلَ في فرنسا بصيغتِه الوطنيَّةِ، ويُعزِّزُ أمنَ المنتجاتِ والخدماتِ الرقميَّةِ[6].

وجديرٌ بالذِّكرِ أنَّ الأمنَ السيبرانيَّ في الفقهِ والتشريعِ الفرنسيَّيْنِ يُشكِّلُ منظومةً متكاملةً تُوازِنُ بين حمايةِ الفضاءِ الرقميِّ من جهةٍ، وضمانِ احترامِ الحقوقِ والحُريَّاتِ من جهةٍ أخرى، وهو يشهدُ تطوُّرًا مستمرًّا في ضوءِ التغيُّراتِ السَّريعةِ في البيئةِ التكنولوجيَّةِ، ويُعدُّ النَّموذجَ الفرنسيَّ من النَّماذجِ المتقدِّمةِ في هذا المجالِ على المستويَيْنِ الأوروبيِّ والدَّوليِّ[7].

ومن جانبٍ آخرَ، يُعَدُّ الأمنُ السيبرانيُّ في العراقِ أحدَ المفاهيمِ الحديثةِ التي برزتْ نتيجةً للتطوُّرِ السَّريعِ في تقنيَّاتِ المعلوماتِ والاتِّصالاتِ، ولا سيَّما مع التزايدِ الكبيرِ في الاعتمادِ على الإنترنتِ والأنظمةِ الرقميَّةِ في مختلفِ مجالاتِ الحياةِ، ويُقصَدُ به - بوجهٍ عامٍّ - حمايةُ الفضاءِ السيبرانيِّ (الرَّقميِّ) من الهجماتِ أو الاختراقاتِ أو أيِّ تهديدٍ يمسُّ سلامةَ المعلوماتِ والأنظمةِ الإلكترونيَّةِ أو خصوصيَّةَ المستخدمينَ.

وجديرٌ بالذِّكرِ - أيضًا - أنَّ مصطلحَ «الأمنِ السيبرانيِّ» لم يكنْ متداولًا في الفقهِ القانونيِّ العراقيِّ قبلَ العقدَيْنِ الأخيرَيْنِ؛ إذْ إنَّ القوانينَ التقليديَّةَ لم تكنْ تتعاملُ مع الفضاءِ الرَّقميِّ بوصفِهِ بيئةً قانونيَّةً مستقلَّةً، ومعَ التَّطوُّرِ التكنولوجيِّ بدأَ الفقهاءُ العراقيُّونَ بتناولِ الأمنِ السيبرانيِّ كفرعٍ حديثٍ من فروعِ القانونِ، يتقاطعُ معَ القانونِ الجنائيِّ، والإداريِّ، والدستوريِّ، وقانونِ المعلوماتيَّةِ. والواقعُ أنَّهُ لا يوجدُ تعريفٌ موحَّدٌ للأمنِ السيبرانيِّ في جميعِ التشريعاتِ، غيرَ أنَّ أغلبَ التَّعاريفِ تدورُ حولَ مضمونٍ مُشتركٍ، ومن أبرزِها: «الإجراءاتُ والتقنيَّاتُ التي تُتَّخذُ لحمايةِ الأنظمةِ، والشبكاتِ، والبرمجيَّاتِ، والمعلوماتِ الرقميَّةِ من الوصولِ غيرِ المُصرَّحِ به، أو التَّخريبِ، أو التَّغييرِ، أو السَّرقةِ، أو الانقطاعِ عنِ الخدمةِ».

وتوالتْ فيما بعدُ تعريفاتُ الفقهِ العراقيِّ، حيثُ عرَّفَ الأمنَ السيبرانيَّ بأنَّهُ: «المجموعةُ المتكاملةُ من الإجراءاتِ القانونيَّةِ والتقنيَّةِ والتنظيميَّةِ التي تهدفُ إلى حمايةِ المعلوماتِ والبنى التحتيَّةِ الرقميَّةِ من أيِّ اختراقٍ أو هجومٍ أو استخدامٍ غيرِ مشروعٍ يُهدِّدُ سلامةَ الدَّولةِ أو حقوقَ الأفرادِ في الفضاءِ السيبرانيِّ»[8].وقد أوضحَ بعضُ الفقهِ أنَّ الأمنَ السيبرانيَّ لا يَنحصرُ في حمايةِ المعلوماتِ فحسبُ، بلْ يَتعدَّاهُ إلى حمايةِ السِّيادةِ الوطنيَّةِ في بيئةٍ رقميَّةٍ مفتوحةٍ، وعرَّفوهُ بأنَّهُ: «حمايةُ الدَّولةِ والمجتمعِ من المخاطرِ المرتبطةِ باستخدامِ تكنولوجيا المعلوماتِ، من خلالِ سَنِّ قوانينَ، ووضعِ سياساتٍ، وتطويرِ مهاراتٍ قادرةٍ على منعِ أو التصدِّي للهجماتِ السيبرانيَّةِ بكلِّ صورِها»[9]، كذلكَ عُرِّفَ الأمنُ السيبرانيُّ بأنَّهُ: «مجموعةُ الضوابطِ القانونيَّةِ والإجرائيَّةِ التي تكفلُ سلامةَ استخدامِ شبكاتِ الاتصالاتِ والبياناتِ، بما يضمنُ عدمَ اختراقِها أو إساءةِ استعمالِها أو استغلالِها في ارتكابِ الجرائمِ»[10]. ولم يكُنْ لدى العراقِ في البدايةِ تشريعٌ خاصٌّ ومستقلٌّ بالأمنِ السيبرانيِّ، غيرَ أنَّهُ ومع ازديادِ الحاجةِ إلى تنظيمِ هذا المجالِ، ظهرتْ مسوَّداتُ قوانينَ ومحاولاتٌ تنظيميَّةٌ من خلالِ عدَّةِ نصوصٍ قانونيَّةٍ متفرِّقةٍ، من أبرزِها مشروعُ قانونِ الأمنِ السيبرانيِّ العراقيِّ لعامِ 2022م، وقد تضمَّنَ المشروعُ تعريفًا عامًّا للأمنِ السيبرانيِّ بأنَّهُ: «مجموعةٌ من الوسائلِ التقنيَّةِ والتنظيميَّةِ والإداريَّةِ التي تهدفُ إلى حمايةِ الفضاءِ السيبرانيِّ، ومنعِ استخدامِه في ارتكابِ الجرائمِ الإلكترونيَّةِ، وضمانِ أمنِ المعلوماتِ الرقميَّةِ والأنظمةِ المتَّصلةِ بالشبكاتِ».

وكذلك قانونُ مكافحةِ جرائمِ المعلوماتيَّةِ (قيد التشريعِ أيضًا)، إذ يُكمِّلُ هذا القانونُ الإطارَ القانونيَّ للأمنِ السيبرانيِّ من خلالِ تجريمِ الأفعالِ المرتكَبةِ عبرَ الوسائلِ الرقميَّةِ. وفي السياقِ المقابلِ، يتَّفقُ الفقهُ القانونيُّ المصريُّ على أنَّ الأمنَ السيبرانيَّ هو: «مجموعةُ التدابيرِ والإجراءاتِ الفنيَّةِ والتشريعيَّةِ والتنظيميَّةِ الهادفةِ إلى حمايةِ النُّظمِ المعلوماتيَّةِ، والبنيةِ التحتيَّةِ الرقميَّةِ، والاتصالاتِ من الهجماتِ أو الاستخداماتِ غيرِ المُصرَّحِ بها أو الأفعالِ الإجراميَّةِ في الفضاءِ الإلكترونيِّ». ويُعَدُّ قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 أوَّلَ قانونٍ مصريٍّ مُتخصِّصٍ في مجالِ الأمنِ السيبرانيِّ؛ إذْ تضمَّنَ نصوصًا تُجرِّمُ الدُّخولَ غيرَ المشروعِ على نُظُمِ المعلوماتِ، واعتراضَ البياناتِ، واختراقَ المواقعِ، ونشرَ البرمجيَّاتِ الخبيثةِ، ومن ذلكَ المادَّةُ (1) التي نصَّتْ على أنَّ الهدفَ منهُ هو: «تحقيقُ الأمنِ السيبرانيِّ، والحفاظُ على البياناتِ والمعلوماتِ والأنظمةِ المعلوماتيَّةِ، وضمانُ حقوقِ المستخدمينَ». كما يُعَدُّ قانونُ حمايةِ البياناتِ الشخصيَّةِ رقم 151 لسنة 2020 استكمالًا لمنظومةِ الأمنِ السيبرانيِّ من زاويةِ حمايةِ خصوصيَّةِ البياناتِ؛ إذ يُلزِمُ الجهاتِ بتأمينِ بياناتِ المستخدمينَ، ويُعطي جهازَ حمايةِ البياناتِ الشخصيَّةِ سُلطاتٍ رقابيَّةً وتنظيميَّةً واسعةً، وكذلكَ قانونُ الاتصالاتِ رقم 10 لسنة 2003 الذي نصَّ في بعضِ موادِّه على الالتزامِ بحمايةِ شبكاتِ الاتصالاتِ وسريَّتِها، وهو ما يُعَدُّ جزءًا من منظومةِ الأمنِ السيبرانيِّ.

ويرى الباحثُ أنَّ الأمنَ السيبرانيَّ هو: «منظومةٌ من السياساتِ والإجراءاتِ القانونيَّةِ والتقنيَّةِ والتنظيميَّةِ، تهدفُ إلى حمايةِ الفضاءِ المعلوماتيِّ الرقميِّ للدَّولةِ والأفرادِ من التهديداتِ والهجماتِ الإلكترونيَّةِ، بما يُحقِّقُ سرِّيَّةَ المعلوماتِ وسلامةَ الأنظمةِ الرقميَّةِ وتوافُرَها، ويحفظُ - في الوقتِ ذاتِه - الحقوقَ والحريَّاتِ الأساسيَّةَ داخلَ البيئةِ الإلكترونيَّةِ».

المطلب الثَّاني/ عناصرُ الأمنِ السّيبرانيِّ

في ظلِّ التَّطوُّرِ المُتسارعِ للتِّكنولوجيا الرَّقميَّةِ، أصبحَ الفضاءُ السّيبرانيُّ مُكوِّنًا أساسيًّا من مُكوِّناتِ الحياةِ الحديثةِ، تتداخلُ فيهِ مصالحُ الأفرادِ، وقطاعاتُ الأعمالِ، والحكوماتِ، وقد أدَّى هذا الاعتمادُ المُتزايدُ على البنى التَّحتيَّةِ الرَّقميَّةِ إلى بُروزِ تهديداتٍ غيرِ تقليديَّةٍ تستهدفُ المعلوماتِ والأنظمةَ الإلكترونيَّةَ، ممَّا استوجبَ بناءَ منظومةِ حمايةٍ شاملةٍ تُعرَفُ بـ«الأمنِ السّيبرانيِّ».ومن ثَمَّ، فإنَّ تحقيقَ الأمنِ السّيبرانيِّ لا يقتصرُ على أدواتٍ تقنيَّةٍ أو إجراءاتٍ تنظيميَّةٍ، بل يقومُ على مجموعةٍ من العناصرِ الأساسيَّةِ التي تُشكِّلُ الإطارَ البنيويَّ لأيِّ سياسةٍ أو استراتيجيَّةٍ فعَّالةٍ في هذا المجالِ، وتُعدُّ هذه العناصرُ بمثابةِ الرَّكائزِ التي تهدفُ إلى حفظِ سريَّةِ المعلوماتِ، وضمانِ سلامتِها، وتوفيرِها عندَ الحاجةِ، إلى جانبِ تعزيزِ مصداقيَّةِ النِّظامِ

الرَّقميِّ واستقرارِه في مواجهةِ التَّهديداتِ المستجدَّةِ. وقد تطوَّرت هذه العناصرُ عبرَ تراكمِ الخبراتِ الدوليَّةِ والمعاييرِ التِّقنيَّةِ، وأصبحت تُعرَفُ بثُلاثيَّةِ (السِّريَّةِ، والسَّلامةِ، والتَّوافُرِ)، ومن هنا تكتسبُ دراستُها أهميَّةً خاصَّةً، إذ تُسهمُ في كشفِ مواطنِ الضَّعفِ، ووضعِ الأُطرِ اللازمةِ لبناءِ قدراتٍ دفاعيَّةٍ فعَّالةٍ في مواجهةِ الأخطارِ السّيبرانيَّةِ المُتزايدةِ، وتُشكِّلُ بذلكَ المدخلَ الضَّروريَّ لأيِّ إصلاحٍ تشريعيٍّ أو إداريٍّ في ميدانِ الأمنِ الرَّقميِّ.وتكمنُ العناصرُ الأساسيَّةُ للأمنِ السّيبرانيِّ في الآتي:

أوَّلًا: السِّريَّةُ (Confidentiality) :

تُعدُّ السِّريَّةُ من المبادئِ الجوهريَّةِ التي يقومُ عليها الأمنُ السّيبرانيُّ، وهي تمثِّلُ الضَّمانةَ الأساسيَّةَ لعدمِ إفشاءِ المعلوماتِ لجهاتٍ غيرِ مُخوَّلةٍ بالاطِّلاعِ عليها، فكلُّ نظامٍ معلوماتيٍّ يحتوي على بياناتٍ، بعضُها حسّاسٌ أو سريٌّ، يتطلَّبُ تأمينَه من التَّلاعُبِ أو التَّسرُّبِ أو الكشفِ غيرِ المُصرَّحِ به، سواءٌ من داخلِ المؤسَّسةِ أو خارجِها، ويُقصَدُ بالسِّريَّةِ في هذا السِّياقِ ضمانُ ألَّا يتمَّ الوصولُ إلى المعلوماتِ إلَّا من قِبَلِ الأشخاصِ أو الأنظمةِ المُصرَّحِ لها بذلكَ. ولا يقتصرُ هذا المبدأُ على الجانبِ التِّقنيِّ، بل يشملُ أيضًا البُعدَ القانونيَّ والتَّنظيميَّ، حيثُ تُفرَضُ السِّريَّةُ عبرَ سياساتٍ داخليَّةٍ، ونصوصٍ تشريعيَّةٍ، وآليَّاتٍ رقابيَّةٍ تتكاملُ جميعُها للحفاظِ على خصوصيَّةِ المعلوماتِ، ويتعلَّقُ الأمرُ هنا بجميعِ أنواعِ البياناتِ، بما فيها المعلوماتُ الشَّخصيَّةُ، والملفَّاتُ الطِّبيَّةُ، والمراسلاتُ الحكوميَّةُ، والمعلوماتُ التِّجاريَّةُ الحسّاسةُ، وبياناتُ البنى التَّحتيَّةِ الحيويَّةِ[11].وفي السِّياقِ العالميِّ، تُؤكِّدُ ISO من خلالِ معيارِها الشَّهيرِ ISO/IEC 27001 أنَّ مبدأَ السِّريَّةِ يُعَدُّ من أهمِّ ثلاثِ ركائزَ للأمنِ المعلوماتيِّ إلى جانبِ السَّلامةِ والتَّوافُرِ، وتُحدِّدُ مجموعةً من التَّدابيرِ التِّقنيَّةِ والتَّنظيميَّةِ التي يجبُ اعتمادُها لضمانِ تحقيقِه، مثل أنظمةِ التَّشفيرِ، وإدارةِ كلماتِ المرورِ، وأنظمةِ التَّحكُّمِ في الوصولِ، وسياساتِ تصنيفِ البياناتِ.ومعَ تزايدِ التَّهديداتِ السّيبرانيَّةِ، مثل التَّصيُّدِ الإلكترونيِّ (Phishing) والهجماتِ على قواعدِ البياناتِ، أصبحت حمايةُ السِّريَّةِ أمرًا بالغَ الأهميَّةِ، خاصَّةً مع تزايدِ الاعتمادِ على الحوسبةِ السَّحابيَّةِ، والأجهزةِ المحمولةِ، وتطبيقاتِ الذَّكاءِ الاصطناعيِّ، إذ إنَّ أيَّ تسرُّبٍ للبياناتِ السِّريَّةِ قد يُؤدِّي إلى خسائرَ ماليَّةٍ، وإضرارٍ بالسُّمعةِ، ومسؤوليَّاتٍ قانونيَّةٍ، وتداعياتٍ سياسيَّةٍ[12].

وفي فرنسا، ينصُّ قانونُ الدفاعِ الفرنسي في المادة L. 2321-1 على إلزامِ الدَّولةِ بضمانِ أمنِ نُظُمِ المعلوماتِ الحسَّاسةِ، ويشملُ ذلكَ الحفاظَ على سريَّةِ المعلوماتِ[13]، كما يُلزِمُ قانونُ حمايةِ البياناتِ الشخصيَّةِ الفرنسي (Loi Informatique et Libertés) المُعدَّلِ وفقًا للائحةِ العامَّةِ لحمايةِ البياناتِ – GDPR الهيئاتِ بمعالجةِ البياناتِ بطريقةٍ تكفلُ[14]:

1- السريَّةَ.
2- عدمَ الإفشاءِ غيرِ المشروعِ.
3- الحمايةَ من الوصولِ غيرِ المُصرَّحِ بهِ.

وعمليًّا، تُصنَّفُ بعضُ البياناتِ ضمنَ ما يُعرَفُ بـ Informations classifiées ، وتخضعُ لنظامٍ صارمٍ من حيثُ الوصولِ والتَّخزينِ والتَّبادلِ، كما تُطبِّقُ مؤسَّساتُ الدَّولةِ والشَّركاتُ الخاصَّةُ سياساتِ الوُلوجِ المحدودِ (Accès restreint) والتَّشفيرِ الإجباريِّ في عددٍ من القطاعاتِ الحسَّاسةِ (كقطاعِ الطَّاقةِ، والصِّحَّةِ، والأمنِ)، وتُفرَضُ – في هذا السِّياقِ – من قِبَلِ ANSSI على مشغِّلي البُنى التَّحتيَّةِ الحيويَّةِ معاييرُ صارمةٌ للحفاظِ على السريَّةِ، كما تُجري الهيئةُ عمليَّاتِ تفتيشٍ دوريَّةً[15].

أمَّا في العراق، فإنَّ مبدأَ السريَّةِ يُعاني من فجواتٍ كبيرةٍ سواءٌ على الصَّعيدِ التَّشريعيِّ أو المؤسَّسيِّ؛ إذ لا يوجدُ – حتَّى الآن – قانونٌ وطنيٌّ شاملٌ لحمايةِ البياناتِ الشخصيَّةِ أو السريَّةِ الرَّقميَّةِ، كما أنَّ مشروعَ قانونِ الجرائمِ الإلكترونيَّةِ العراقيِّ المطروحِ منذُ سنواتٍ لا يتضمَّنُ تنظيمًا تفصيليًّا لآليَّاتِ حمايةِ السريَّةِ أو العقوباتِ الدقيقةِ المترتِّبةِ على انتهاكِها[16].

وقد أظهرت تقاريرُ صادرةٌ عن هيئةِ الإعلامِ والاتصالاتِ العراقيَّةِ ووزارةِ التعليمِ العالي والبحثِ العلميِّ العراقيَّةِ وقوعَ حوادثَ متكرِّرةٍ لتسرُّبِ بياناتٍ طلابيَّةٍ ووثائقَ رسميَّةٍ عبرَ الإنترنتِ، دونَ وجودِ جهةٍ مسؤولةٍ تتحمَّلُ المسؤوليَّةَ أو إجراءاتٍ محاسبيةٍ فعّالةٍ، كما أنَّ اعتمادَ بعضِ الدوائرِ الحكوميَّةِ على تطبيقاتٍ غيرِ مُؤمَّنةٍ، أو تخزينَ المعلوماتِ في خوادمَ غيرِ محميَّةٍ، يُضعفُ من قدرةِ الدَّولةِ على فرضِ السريَّةِ الرَّقميَّةِ، ويُعرِّضُ أمنَ المواطنِ والمؤسَّساتِ للخطرِ[17].

وفي ضوءِ ذلكَ، تُصبحُ السريَّةُ عنصرًا لا غِنى عنهُ في بناءِ سيادةٍ رقميَّةٍ حقيقيَّةٍ للعراقِ، فحمايةُ المعلوماتِ ليست مجرَّدَ ترَفٍ قانونيٍّ أو مطلبٍ تقنيٍّ، بل هي ضرورةٌ استراتيجيَّةٌ تمسُّ أمنَ الدَّولةِ، وثقةَ المواطنينِ، ومكانةَ المؤسَّساتِ في النِّظامِ الدوليِّ الرَّقميِّ، ممَّا يستوجبُ إصلاحاتٍ تشريعيَّةً عميقةً، وتطويرَ البُنيةِ التَّحتيَّةِ السّيبرانيَّةِ، وتعزيزَ ثقافةِ الخصوصيَّةِ والامتثالِ لدى الموظَّفينَ والمستخدمينَ.

وفي مصرَ، ينصُّ قانونُ مكافحةِ جرائمِ تقنيةِ المعلوماتِ المصري رقم (175) لسنة 2018 في المادَّة (6) على تجريمِ الدُّخولِ غيرِ المشروعِ إلى موقعٍ أو نظامٍ معلوماتيٍّ بهدفِ الاطِّلاعِ على بياناتٍ سريَّةٍ، كما نصَّ في المادَّة (14) على معاقبةِ الإفشاءِ غيرِ المشروعِ للمعلوماتِ أو البياناتِ التي تمَّ الحصولُ عليها بطريقٍ غيرِ قانونيٍّ، وكذلك نصَّ قانونُ حمايةِ البياناتِ الشخصيَّةِ المصري رقم (151) لسنة 2020 في المادَّة (2) على إلزامِ المُتحكِّمِ والمُعالِجِ في البياناتِ بحفظِ سريَّةِ البياناتِ ومنعِ إفشائِها أو السَّماحِ بالاطِّلاعِ عليها دونَ موافقةٍ، كما نصَّت المادَّةُ (7) على وجوبِ اتِّخاذِ التَّدابيرِ الفنِّيَّةِ والتَّنظيميَّةِ اللازمةِ لحمايةِ سريَّةِ وسلامةِ وتكاملِ البياناتِ. كما نصَّت المادَّةُ (73) من قانونِ الاتصالاتِ المصري رقم (10) لسنة 2003 على تجريمِ إفشاءِ أيَّةِ معلوماتٍ متعلِّقةٍ بمحتوى الاتِّصالاتِ أو بياناتِ المشتركينَ دونَ تصريحٍ. وتأكيدًا لما سبقَ، تُفرَضُ على المؤسَّساتِ التي تتعاملُ مع بياناتِ المواطنينَ – مثل شركاتِ الاتِّصالاتِ، والبنوكِ، والمستشفياتِ – التزاماتٌ

خاصَّةٌ بتأمينِ البياناتِ وضمانِ سريَّتِها، كما ألزمَ قانونُ حمايةِ البياناتِ الشخصيَّةِ الجهاتِ بتعيينِ «مسؤولِ حمايةِ البياناتِ» (DPO) لمراقبةِ مدى التزامِ المؤسَّساتِ بسريَّةِ المعلوماتِ[18].

ثانيًا: سَلامةُ البياناتِ (Integrity):

تُعَدُّ سَلامةُ البياناتِ أحدَ المفاهيمِ الجوهريَّةِ في منظومةِ الأمنِ السّيبرانيِّ، وتُعبِّرُ عن الضَّمانِ القانونيِّ والتِّقنيِّ لعدمِ حدوثِ أيِّ تعديلٍ أو حذفٍ أو إضافةٍ غيرِ مشروعةٍ على البياناتِ، سواءٌ أثناءَ تخزينِها أو نقلِها أو معالجتِها، إذ لا تقتصرُ سَلامةُ البياناتِ على منعِ التَّغييرِ غيرِ المُصرَّحِ بهِ، بل تشملُ – أيضًا – التَّأكُّدَ من أنَّ البياناتِ تعكسُ الحقيقةَ كما أُدخِلَت أوَّلَ مرَّةٍ، وأنَّها ظلَّت في حالتِها الأصليَّةِ دونَ تلاعُبٍ[19]. ومن النَّاحيةِ الفنِّيَّةِ، تتحقَّقُ سَلامةُ البياناتِ عبرَ مجموعةٍ من التِّقنيَّاتِ كالتَّجزئةِ (Hashing)، والتَّوقيعِ الرَّقميِّ، وسجلَّاتِ التَّدقيقِ، التي تعملُ على تتبُّعِ أيِّ تغييراتٍ غيرِ مُصرَّحٍ بها، وتُطلِقُ إنذاراتٍ فوريَّةً عندَ محاولةِ التَّلاعُبِ بالملفَّاتِ. أمَّا على المستوى التَّنظيميِّ، فإنَّ وجودَ سياساتٍ داخليَّةٍ صارمةٍ في المؤسَّساتِ – كإدارةِ النُّسخِ الاحتياطيَّةِ وتحديدِ الصَّلاحيَّاتِ – يُعزِّزُ من قدرةِ النِّظامِ على حمايةِ بياناتِه من التَّغييراتِ العشوائيَّةِ أو المُتعمَّدةِ[20].وفي فرنسا، يُقصَدُ بسَلامةِ البياناتِ في السِّياقِ السّيبرانيِّ: «ضمانُ عدمِ تغييرِ البياناتِ أو التَّلاعُبِ بها أو فقدانِها أثناءَ التَّخزينِ أو النَّقلِ أو المُعالجةِ، سواءٌ عن قصدٍ أو عن طريقِ الخطأِ»[21]. وفي العراقِ، لا يوجدُ نصٌّ صريحٌ ومستقلٌّ يتناولُ مفهومَ سَلامةِ البياناتِ بشكلٍ مباشرٍ، غيرَ أنَّهُ يُمكنُ استنتاجُ حمايتِها من القواعدِ العامَّةِ في القانونِ المدنيِّ العراقيِّ، التي تُجرِّمُ كلَّ فعلٍ يُسبِّبُ ضررًا ماديًّا أو معنويًّا للغيرِ، سواءٌ وقعَ هذا الفعلُ عمدًا أم نتيجةَ إهمالٍ، كما يُنتظرُ أن يتضمَّنَ مشروعُ قانونِ الأمنِ السيبرانيِّ العراقيِّ المرتقبُ أحكامًا تفصيليَّةً بشأنِ حمايةِ سَلامةِ البياناتِ، خاصَّةً في المؤسَّساتِ العامَّةِ والقطاعاتِ الماليَّةِ والطِّبيَّةِ، التي باتت أهدافًا رئيسَةً للهجماتِ الإلكترونيَّةِ[22]. وتُسهمُ سَلامةُ البياناتِ – إلى جانبِ ذلكَ – في دعمِ الحقوقِ الرَّقميَّةِ للأفرادِ، إذ تُشكِّلُ ضمانةً حقيقيَّةً ضدَّ التَّشويهِ أو التَّزويرِ أو المساسِ بمصداقيَّةِ المعاملاتِ الإلكترونيَّةِ، وهو ما يرتبطُ مباشرةً بمبادئِ العدالةِ الرَّقميَّةِ وسيادةِ القانونِ في البيئةِ السّيبرانيَّةِ. وفي هذا السِّياقِ، يُشيرُ الاتحادُ الدوليُّ للاتصالاتِ (ITU)[23] في تقريرِه (ITU Cybersecurity Guide، 2020) إلى أنَّ «أيَّ خللٍ في سَلامةِ البياناتِ يُؤدِّي إلى تقويضِ ثقةِ المستخدمينَ ويُهدِّدُ استقرارَ البنيةِ الرَّقميَّةِ الوطنيَّةِ».

أمَّا سلامةُ البياناتِ في مصر، فتعني: «حمايةَ البياناتِ من التعديلِ أو الحذفِ أو التَّلفِ أو التَّغييرِ غيرِ المشروعِ، بما يَضمنُ بقاءَها على حالتِها الأصليَّةِ أو المصرَّحِ بها فقط»[24].وفي هذا الإطارِ، نصَّتِ المادَّةُ (8) من قانونِ مكافحةِ جرائمِ تقنيةِ المعلوماتِ المصري رقم 175 لسنة 2018 على تجريمِ أيِّ تعديلٍ أو تغييرٍ أو تشويهٍ لمحتوى البياناتِ والمعلوماتِ، كما نصَّتِ المادَّةُ (51) منه على فرضِ عقوباتٍ على مَن يتسبَّبُ عمدًا أو بغيرِ قصدٍ في إفسادِ البياناتِ[25].كذلك نصَّتِ المادَّةُ (2) من قانونِ حمايةِ البياناتِ الشخصيَّةِ المصري رقم 151 لسنة 2020 على التزامِ الجهاتِ المتحكِّمةِ في البياناتِ باتِّخاذِ التدابيرِ التي تَضمنُ «سلامةَ وتكاملَ البياناتِ»، كما نصَّتِ المادَّةُ (7) منه على وجوبِ تنفيذِ ضوابطَ تقنيَّةٍ تَضمنُ ألَّا يتمَّ تعديلُ البياناتِ أو تلفُها دونَ إذنٍ[26].ويُشيرُ قانونُ الاتصالاتِ المصري رقم 10 لسنة 2003 إلى التزامِ شركاتِ الاتصالاتِ بحمايةِ المعلوماتِ المنقولةِ، ومنعِ إفسادِها أو فقدانِها.وعلى صعيدِ التطبيقِ المؤسَّسيِّ، يلتزمُ المجلسُ الأعلى للأمنِ السّيبرانيِ والجهازُ القومي لتنظيمِ الاتصالاتِ بفرضِ سياساتٍ تهدفُ إلى[27]:

1- حمايةِ قواعدِ البياناتِ من التلاعبِ.
2- التحقُّقِ من النَّزاهةِ عبرَ أنظمةِ كشفِ التغييرِ (Intrusion Detection).
3- إجراءِ النَّسخِ الاحتياطيِّ المنتظمِ للبياناتِ.

أمَّا في العراقِ، فلا يوجدُ قانونٌ خاصٌّ بحمايةِ البياناتِ الشخصيَّةِ، وإنَّما يُطبَّقُ القضاءُ القواعدَ العامَّةَ في القانونِ المدنيِّ والجنائيِّ لفضِّ النِّزاعاتِ في حالاتِ الانتهاكِ أو الاختراقِ الإلكترونيِّ.

ثالثًا: التَّوافُرُ (Availability) :

يُعَدُّ مفهومُ التَّوافرِ أحدَ الأركانِ الثلاثةِ الأساسيَّةِ التي يقومُ عليها الأمنُ السّيبرانيُّ، إلى جانبِ السِّرِّيَّةِ وسلامةِ البياناتِ، ويعني في جوهرِه ضمانَ إتاحةِ المعلوماتِ والأنظمةِ والمواردِ التقنيَّةِ للمستخدمينَ المصرَّحِ لهم في الوقتِ المناسبِ، دونَ انقطاعٍ أو تعطيلٍ، بما يُحقِّقُ استمراريَّةَ العملِ وفعاليَّةَ الأداءِ الرَّقميِّ داخلَ المؤسَّساتِ العامَّةِ والخاصَّةِ.ففي عالمٍ يعتمدُ على الأنظمةِ الإلكترونيَّةِ في إدارةِ مختلفِ الخدماتِ الحيويَّةِ - من المصارفِ إلى المستشفياتِ، ومن البنى التحتيَّةِ إلى مؤسَّساتِ الدَّولةِ - يصبحُ الحفاظُ على التَّوافرِ أمرًا لا يُمكنُ التهاونُ فيه؛ إذ إنَّ أيَّ توقُّفٍ غيرِ مُخطَّطٍ لهُ، سواءٌ كانَ ناتجًا عن عطلٍ تقنيٍّ، أو هجومٍ سيبرانيٍّ، أو كارثةٍ طبيعيَّةٍ، قد يؤدِّي إلى خسائرَ كبيرةٍ تتجاوزُ الجانبَ الاقتصاديَّ لتصلَ إلى المساسِ بالأمنِ العامِّ أو حتَّى حياةِ الأفرادِ[28].وفي السِّياقِ السيبرانيِّ، يظهرُ التهديدُ الرَّئيسيُّ للتَّوافرِ في شكلِ هجماتِ «حَجْبِ الخدمةِ» (Denial of Service - DoS) أو هجماتِ «حَجْبِ الخدمةِ الموزَّعةِ» (DDoS)، التي تهدفُ إلى إغراقِ الخوادمِ بطلباتٍ زائفةٍ تُؤدِّي إلى إيقافِها عن العملِ، ممَّا يمنعُ المستخدمينَ الحقيقيِّينَ من الوصولِ إلى الخدماتِ الرَّقميَّةِ، كما أنَّ الفيروساتِ والبرمجيَّاتِ الخبيثةَ التي تُعطِّلُ أنظمةَ التشغيلِ أو تَمحُو البياناتِ تُعَدُّ من أخطرِ التحدياتِ التي تُهدِّدُ عنصرَ التَّوافرِ[29].وتزدادُ أهميَّةُ مفهومِ التوافرِ في البيئاتِ الحكوميَّةِ والخدماتيَّةِ، حيثُ يؤدِّي تعطيلُ الأنظمةِ إلى شللٍ إداريٍّ أو أمنيٍّ شاملٍ، ففي العراقِ على سبيلِ المثالِ، تتعرَّضُ مواقعُ إلكترونيَّةٌ حكوميَّةٌ بين الحينِ والآخرِ إلى أعطالٍ أو اختراقاتٍ تُؤثِّرُ على الوصولِ إلى المعلوماتِ أو تقديمِ المعاملاتِ، ممَّا يعكسُ هشاشةَ التوافرِ الرَّقميِّ، سواءٌ بسببِ ضعفِ البنيةِ التحتيَّةِ، أو نقصِ الكوادرِ التقنيَّةِ المؤهَّلةِ، أو غيابِ خططِ الاستجابةِ للطوارئِ[30].ومن النَّاحيةِ القانونيَّةِ، لم يَرِدْ مفهومُ

التوافر صراحةً في التشريعاتِ العراقيَّة، غيرَ أنَّهُ يدخلُ ضمنيًّا في التزاماتِ الجهاتِ الحكوميَّةِ والخاصَّةِ التي تُقدِّمُ خدماتٍ إلكترونيَّةً، ويُعَدُّ الإخلالُ به نوعًا من التَّقصيرِ الذي قد يُرتِّبُ مسؤوليَّةً قانونيَّةً، خاصَّةً إذا كانَ ناتجًا عن إهمالٍ في حمايةِ الأنظمةِ أو فشلٍ في اتِّخاذِ التدابيرِ الوقائيَّةِ المناسبةِ، ويُتوقَّعُ أن يتضمَّنَ مشروعُ قانونِ الأمنِ السّيبراني العراقي – في حالِ إقرارِهِ – موادَّ واضحةً تُنظِّمُ التزاماتِ المؤسَّساتِ بضمانِ استمراريَّةِ الخدمةِ الرَّقميَّةِ وحمايتِها من الانقطاعِ[31].ويَستلزمُ تحقيقُ التوافرِ اتِّخاذَ إجراءاتٍ متعدِّدةٍ، تبدأُ من تصميمِ الأنظمةِ بطريقةٍ تَضمنُ المرونةَ وتَتحمَّلُ الأعطالَ الجزئيَّةَ، إلى وضعِ خططِ النَّسخِ الاحتياطيِّ واستردادِ البياناتِ، وتأمينِ مصادرِ الطَّاقةِ البديلةِ، وتدريبِ فِرَقٍ تقنيَّةٍ للتعاملِ مع الطوارئِ، كما يُعَدُّ الوعيُ المؤسَّسيُّ عنصرًا حاسمًا، إذ لا يُمكنُ فصلُ الجانبِ الفنِّيِّ عن الجانبِ التَّنظيميِّ في بناءِ منظومةِ توافرٍ رقميٍّ فعَّالةٍ.وعلى الصعيدِ الدَّوليِّ، توصي معاييرُ مثل ISO/IEC 27001 و NIST Cybersecurity Framework بضرورةِ إدماجِ التوافرِ كجزءٍ أساسيٍّ من سياساتِ الأمنِ السيبراني، مؤكِّدةً أنَّ فقدانَ التوافرِ، حتَّى وإن لم يَصحبْه اختراقٌ للبياناتِ، يُعَدُّ تهديدًا أمنيًّا لا يقلُّ خطورةً عن التَّسريبِ أو التزويرِ[32]، ويُعرَّفُ هذا المفهومُ بأنَّه: «ضمانُ إمكانيَّةِ الوصولِ إلى البياناتِ والأنظمةِ والخدماتِ المعلوماتيَّةِ في الوقتِ المناسبِ ودونَ انقطاعٍ للأشخاصِ المصرَّحِ لهم، سواءٌ كانوا أفرادًا أو مؤسَّساتٍ، مع استمرارِ عملِ البنيةِ التحتيَّةِ الرَّقميَّةِ بكفاءةٍ عاليةٍ رغمَ التهديداتِ أو الأعطالِ أو الهجماتِ».وقد أكَّدَ قانونُ الدفاعِ الفرنسي في **المادة1-L.2321** ، على حمايةِ البنى التحتيَّةِ الحيويَّةِ بما يشملُ ضمانَ «استمراريَّةِ عملِ نظمِ المعلوماتِ»، وهو لُبُّ مبدأِ التوافرِ[33].وفي مصرَ، نصَّ قانونُ مكافحةِ جرائمِ تقنيةِ المعلوماتِ المصري رقم 175 لسنةِ 2018 في المادَّةِ (18) على معاقبةِ مَن يتسبَّبُ عمدًا في «إعاقةٍ أو تعطيلِ الوصولِ إلى موقعٍ أو نظامٍ معلوماتيٍّ»، كما نصَّ في المادَّةِ (20) على تجريمِ الاعتداءِ على المواقعِ أو الأنظمةِ الحكوميَّةِ بقصدِ تعطيلِ الخدمةِ. وعليهِ، فإنَّ تحقيقَ التوافرِ لا يُعَدُّ مجرَّدَ مسألةٍ تقنيَّةٍ، بل هو أداةٌ جوهريَّةٌ لحمايةِ الحقوقِ والحُرِّيَّاتِ في العصرِ الرَّقميِّ، ويُفترضُ أن يتعاملَ معهُ المشرِّعُ والمؤسَّساتُ والبنى التحتيَّةُ بقدْرٍ عالٍ من الجِدِّيَّةِ والاحترافيَّةِ.

رابعًا: المرونة السّيبرانيَّة (Cyber Resilience):

إنَّ هذا المفهومَ يتجاوزُ الأبعادَ التقنيَّةَ الضيِّقةَ ليرتبطَ بالحوكمةِ، وإدارةِ المخاطرِ، والقدرةِ التشغيليَّةِ، والتخطيطِ الاستراتيجيِّ. فالمرونةُ السيبرانيَّةُ لا تنفي أهميَّةَ الوقايةِ، ولكنَّها تنظرُ إلى الهجماتِ باعتبارِها أمرًا محتملًا دائمًا، ومن ثمَّ يتحوَّلُ التَّركيزُ نحو بناءِ نُظُمٍ قادرةٍ على امتصاصِ الصَّدمةِ، ثمَّ التَّعافي السَّريعِ، والتكيُّفِ مع التهديداتِ الجديدةِ، وهذا الطابعُ التكيُّفيُّ هو ما يُضفي على المرونةِ السيبرانيَّةِ أهميَّتَها في السِّياقاتِ المعقَّدةِ وغيرِ المتوقَّعةِ[34].وقد عرَّفتها وثائقُ المعهدِ القومي الأمريكي للمعاييرِ والتقنيةِ (NIST) بأنَّها «القدرةُ على الاستعدادِ والتصدِّي والتعافي من الحوادثِ السيبرانيَّةِ مع الحفاظِ على استمراريَّةِ تقديمِ الخدماتِ الأساسيَّةِ»، وهو تعريفٌ يُبرزُ البُعدَ العمليَّ والتشغيليَّ لهذا المفهومِ، كما أنَّ الاتحادَ الدوليَّ للاتصالاتِ (ITU) أدرجَها ضمنَ الرَّكائزِ الكُبرى لاستراتيجيَّاتِ الأمنِ السّيبراني الوطنيِّ، مُشيرًا إلى أنَّ المرونةَ لا تقتصرُ على التِّكنولوجيا، بل تشملُ أيضًا الثَّقافةَ المؤسَّسيَّةَ، والقيادةَ، والتدريبَ، والوعيَ[35].

المبحث الثاني/حمايةُ الأمنِ السّيبراني والتحدياتُ التي يُواجهُها

مع تَنامي استخدامِ التِّكنولوجيا في مؤسَّساتِ الدَّولةِ والقطاعِ الخاصِّ، تصاعدت صُوَرُ الهجماتِ السيبرانيَّةِ، سواءٌ من خلالِ اختراقِ المواقعِ الحكوميَّةِ، أو تسريبِ بياناتِ المواطنينَ، أو انتهاكِ الخصوصيَّةِ عبرَ المنصَّاتِ الرَّقميَّةِ. وعلى الرَّغمِ من ذلك، لا يزالُ الإطارُ القانونيُّ لحمايةِ الأمنِ السيبرانيِّ في العراقِ يُعاني من التشتُّتِ، والفَراغِ التشريعيِّ، وضعفِ التَّنفيذِ؛ إذ لم يصدرْ حتَّى الآنَ قانونٌ خاصٌّ يُنظِّمُ تنظيمًا شاملًا الأمنَ السيبرانيَّ بمستوياتِهِ المختلفةِ (الجنائيَّةِ، والمدنيَّةِ، والتنظيميَّةِ).

وتزدادُ التحدِّياتُ تعقيدًا أمامَ الحمايةِ القانونيَّةِ للأمنِ السيبرانيِّ بسببِ عدَّةِ عواملَ، أبرزُها: ضعفُ البنيةِ التحتيَّةِ الرَّقميَّةِ في مؤسَّساتِ الدَّولةِ، وغيابُ جهةٍ تنظيميَّةٍ مستقلَّةٍ للأمنِ السيبرانيِّ، وضعفُ التنسيقِ بينَ السُّلطاتِ القضائيَّةِ والتقنيَّةِ، وقلَّةُ الكفاءاتِ المتخصِّصةِ في الأدلَّةِ الرَّقميَّةِ، إلى جانبِ الغموضِ الذي يكتنفُ بعضَ المفاهيمِ القانونيَّةِ عندَ تطبيقِها في البيئةِ الرَّقميَّةِ. ويُشكِّلُ هذا الواقعُ دافعًا قويًّا لدراسةِ الإطارِ القانونيِّ لحمايةِ الأمنِ السيبرانيِّ في العراقِ، وتحليلِ مدى استجابتِه للتحدِّياتِ المعاصرةِ، مع التَّركيزِ على الجوانبِ المدنيَّةِ التي تمثِّلُ الحمايةَ غيرَ الزجريَّةِ، والتي تهدفُ إلى إنصافِ المتضرِّرينَ من الاعتداءاتِ السيبرانيَّةِ، وضمانِ جبرِ الأضرارِ التي تمسُّ حقوقَ الأفرادِ وحُرِّيَّاتِهم الرَّقميَّةِ.وفي إطارِ هذا المبحثِ، سنبحثُ في بيانِ الحمايةِ المدنيَّةِ للأمنِ السيبرانيِّ من جهةٍ، والتحدِّياتِ التي تُواجهُها تلك الحمايةُ من جهةٍ أخرى، وذلك في المطلبينِ الآتيينِ:

المطلب الأوَّل/ القانون المدني كآليَّةٍ لحماية الأمن السيبراني

يُشكِّلُ الأمنُ السيبرانيُّ جزءًا أساسيًّا من الأمنِ القومي للدُّولِ في العصرِ الرَّقميِّ، إذ لم تَعُدِ التَّهديداتُ مقتصرةً على الأشكالِ التَّقليديَّةِ، بل امتدَّت إلى المجالِ الرَّقميِّ، ممَّا استدعى تطويرَ منظومةٍ قانونيَّةٍ مُتكاملةٍ لحمايةِ الفضاءِ السيبرانيِّ.

وفي العراقِ، بدأت ملامحُ الاهتمامِ بالأمنِ السيبرانيِّ تتبلورُ من خلالِ محاولاتٍ تشريعيَّةٍ متفرِّقةٍ، رغمَ غيابِ قانونٍ موحَّدٍ ومُخصَّصٍ يُنظِّمُ هذا المجالَ حتَّى الآنَ.وتُعَدُّ الحمايةُ المدنيَّةُ إحدى الآليَّاتِ القانونيَّةِ الأساسيَّةِ في هذا الإطارِ، إذ تهدفُ إلى حمايةِ الحقوقِ المدنيَّةِ للأفرادِ والمؤسَّساتِ من الاعتداءاتِ السيبرانيَّةِ، وتكفلُ التَّعويضَ عن الأضرارِ، وترسِّخُ مبدأَ المسؤوليَّةِ المدنيَّةِ عن الأفعالِ الضَّارَّةِ عبرَ الإنترنت، ويُفيدُ الإطارُ القانونيُّ العامُّ للحمايةِ المدنيَّةِ للأمنِ السيبرانيِّ أنَّ العراقَ لم يُصدِرْ – حتَّى تاريخِ كتابةِ هذه الورقةِ – قانونًا خاصًّا للأمنِ السيبرانيِّ، غيرَ أنَّ العديدَ من القوانينِ العامَّةِ تُستخدَمُ لتغطيةِ الجوانبِ المدنيَّةِ المتعلِّقةِ بالجرائمِ السيبرانيَّةِ.وفي ظلِّ التَّحوُّلِ المتسارعِ نحوَ الرَّقمنةِ، أصبحت الحمايةُ المدنيَّةُ للأمنِ

السيبرانيِّ من الضَّرورات الأساسيَّةِ التي تستهدفُ الحفاظَ على استقرارِ المجتمعاتِ الحديثةِ، وحمايةَ الأفرادِ والمرافقِ المدنيَّةِ من التَّهديداتِ الرَّقميَّةِ المتزايدةِ، ولا تقتصرُ هذه الحمايةُ على الجانبِ الأمنيِّ فحسب، بل تشملُ أيضًا ضمانَ استمراريَّةِ الخدماتِ العامَّةِ، وسلامةَ البياناتِ، وصيانةَ الحقوقِ الرَّقميَّةِ للمواطنينَ، في ظلِّ تصاعدِ وتيرةِ الهجماتِ الإلكترونيَّةِ التي لم تَعُدْ تُفرِّقُ بينَ المرافقِ العسكريَّةِ والكياناتِ المدنيَّةِ. وقد أولَتْ فرنسا اهتمامًا مبكِّرًا بهذا الجانبِ، باعتبارِها من الدُّولِ الرَّائدةِ في بناءِ بنيةٍ سيبرانيَّةٍ مدنيَّةٍ متقدِّمةٍ؛ حيثُ اعتمدت منذ عام 2013 قانون البرمجة العسكريَّة (Loi de programmation militaire)[36]، الذي ألزَمَ الشركاتِ والمؤسَّساتِ المشغِّلةَ للبنى التحتيَّةِ الحيويَّةِ - كقطاعاتِ الطَّاقةِ، والصِّحَّةِ، والاتِّصالاتِ - بوضعِ تدابيرِ حمايةٍ رقميَّةٍ صارمةٍ، والإبلاغِ الإجباريِّ عن أيِّ خروقاتٍ إلى الوكالةِ الوطنيَّةِ لأمن نظم المعلومات (ANSSI)، وهي الهيئةُ التي تُمثِّلُ الذِّراعَ الفنِّيَّ الرَّئيسيَّ في تنسيقِ وتنفيذِ سياسةِ الدَّولةِ في مجالِ الحمايةِ السيبرانيَّةِ[37]. كما أسهمَ قانونُ الجمهوريَّةِ الرقميَّةِ لعام 2016 في تعزيزِ هذا التوجُّهِ، من خلالِ إرساءِ حقوقٍ رقميَّةٍ واضحةٍ للمواطنينَ، وفرضِ التزاماتٍ على الهيئاتِ العامَّةِ والخاصَّةِ فيما يتعلَّقُ بحمايةِ البياناتِ وتوفيرِ الشفافيَّةِ في معالجتِها، وتتمثَّلُ الحمايةُ المدنيَّةُ في فرنسا أيضًا في تعزيزِ مفهومِ «المرونة الرقميَّة»، حيثُ تعملُ المؤسَّساتُ على تطويرِ خططٍ لاستمراريَّةِ الخدمةِ حتَّى في حالةِ التعرُّضِ لهجومٍ سيبرانيٍّ، بما يَضمنُ عدمَ تعطُّلِ المرافقِ العامَّةِ الحيويَّةِ.

أمَّا في مصر، فقد شهدت السنواتُ الأخيرةُ تطوُّرًا لافتًا في البنيةِ التشريعيَّةِ والتنظيميَّةِ المعنيَّةِ بالحمايةِ السيبرانيَّةِ، خاصَّةً بعد صدورِ قانون مكافحةِ جرائمِ تقنية المعلومات رقم 175 لسنة 2018[38]، والذي يُعَدُّ أوَّلَ تشريعٍ مصريٍّ مُتكاملٍ يُنظِّمُ الأمنَ السيبرانيَّ بشكلٍ مباشرٍ، ولم يقتصرْ هذا القانونُ على تجريمِ الأفعالِ الإلكترونيَّةِ، بل تضمَّنَ في موادِّه التزامَ الجهاتِ مُقدِّمةِ الخدمةِ باتِّخاذِ وسائلِ الحمايةِ الفنِّيَّةِ، وفرضَ رقابةٍ على حركةِ البياناتِ، وإنشاءَ سجلاتٍ إلكترونيَّةٍ تُسهِّلُ تتبُّعَ أيِّ خرقٍ أمنيٍّ، كما عزَّزَ قانونُ حماية البيانات الشخصيَّة المصري رقم 151 لسنة 2020 من الحمايةِ المدنيَّةِ للمواطنِ، من خلالِ فرضِ التزاماتٍ قانونيَّةٍ على المُتحكِّمينَ في البياناتِ بخصوصِ الحفاظِ على سريَّتِها وسلامتِها وتوافُرِها[39].وقد أنشأتِ الدولةُ مراكزَ فنِّيَّةً متخصِّصةً مثل المركز المصريِّ للاستجابةِ لطوارئ الحاسبات(EG-CERT) ، إضافةً إلى المجلس الأعلى للأمن السيبراني الذي يُنسِّقُ بين الوزاراتِ والهيئاتِ لضمانِ التكامُلِ في إدارةِ التهديداتِ، وتُستخدَمُ آليَّاتٌ تقنيَّةٌ متقدِّمةٌ مثل التوقيعِ الإلكترونيِّ، والمصادقةِ الثنائيَّةِ، وتشفيرِ البياناتِ، لحمايةِ التعاملاتِ الحكوميَّةِ والمدنيَّةِ، لا سيَّما عبرَ بوابةِ مصر الرقميَّة.وفي العراق، تُعَدُّ الحمايةُ المدنيَّةُ للأمنِ السيبرانيِّ حديثةَ النشأةِ نسبيًّا، إذ جاء قانون مكافحة الجرائم المعلوماتية رقم 31 لسنة 2023[40] ليُؤسِّسَ - للمرَّةِ الأولى - منظومةً قانونيَّةً تُنظِّمُ حمايةَ الفضاءِ المدنيِّ من التهديداتِ السيبرانيَّةِ، ورغمَ أنَّ هذا القانونَ لا يرقى بعدُ إلى مستوى تشريعاتِ بعضِ الدُّولِ المتقدِّمةِ، فإنَّهُ يُمثِّلُ خطوةً أولى في بناءِ بيئةٍ سيبرانيَّةٍ أكثرَ أمنًا، خصوصًا مع ما يشهدهُ العراقُ من استهدافٍ متكرِّرٍ للبنى التحتيَّةِ، لا سيَّما في قطاعَي الاتِّصالاتِ والطاقةِ، وتضطلعُ وزارةُ الداخليَّةِ العراقيَّةِ، من خلالِ مديريَّةِ حمايةِ البنى التحتيَّةِ الحَرِجَةِ، بدورٍ محوريٍّ في هذا الجانبِ، كما يسعى الجهازُ المركزيُّ لتكنولوجيا المعلومات التابعُ للأمانة العامَّة لمجلس الوزراء العراقي إلى وضعِ سياساتٍ لحمايةِ النُّظُمِ الحكوميَّةِ، وتعتمدُ الدولةُ - في الوقتِ الراهنِ- على جهودٍ مؤسسيَّةٍ ومبادراتٍ تدريبيَّةٍ لتأهيلِ الكوادرِ وتطويرِ نُظُمِ الاستجابةِ للحوادثِ، في انتظارِ اكتمالِ البنيةِ التشريعيَّةِ والتقنيَّةِ اللازمةِ لتأمينِ القطاعِ المدنيِّ[41].وعندَ المقارنةِ، نرى أنَّ الوضعَ في الدولِ الثلاثِ يُبرزُ تبايُنًا واضحًا في مستوى النُّضجِ السيبرانيِّ المدنيِّ؛ فبينما تُمثِّلُ فرنسا نموذجًا مؤسسيًّا وتشريعيًّا ناضجًا، تسعى مصرُ إلى تعزيزِ منظومتِها عبرَ تطويرِ التشريعاتِ وتفعيلِ الأُطرِ المؤسَّسيَّةِ، في حين لا يزالُ العراقُ في طورِ التأسيسِ، ويواجهُ تحدِّياتٍ تتعلَّقُ بالقدراتِ الفنِّيَّةِ والمواردِ البشريَّةِ. ومعَ ذلكَ، فإنَّ التوجُّهَ المشتركَ بين هذه الدولِ نحوَ ترسيخِ الحمايةِ المدنيَّةِ الرقميَّةِ يُجسِّدُ وعيًا متزايدًا بأهمِّيَّةِ الأمنِ السيبرانيِّ كعنصرٍ أساسيٍّ في حفظِ السِّلمِ المجتمعيِّ وتعزيزِ الاستقرارِ المؤسسيِّ في البيئةِ الرقميَّةِ. ويُلاحَظُ أنَّهُ يتمُّ الاعتمادُ - حاليًّا - على القواعدِ العامَّةِ في المسؤوليَّةِ التقصيريَّةِ والعقديَّةِ المنصوصِ عليها في القانون المدني المصري لتأسيسِ الحمايةِ المدنيَّةِ في مجالِ الأمنِ السيبرانيِّ.

المطلب الثاني/تحدِّياتُ الحمايةِ المدنيَّةِ للأمنِ السيبرانيِّ

مع تصاعُدِ الاعتمادِ على التكنولوجيا والاتِّصالاتِ الرقميَّةِ، أصبحَ الأمنُ السيبرانيُّ أحدَ أبرزِ التحدِّياتِ القانونيَّةِ المعاصرةِ، خصوصًا في الدولِ النامية مثل العراق، حيثُ تتسارعُ وتيرةُ الجرائمِ الإلكترونيَّةِ في ظلِّ تطوُّرِ وسائلِ الاختراقِ والقرصنةِ الرقميَّةِ، ورغمَ وجودِ إطارٍ عامٍّ للمسؤوليَّةِ المدنيَّةِ في القانون المدني العراقي رقم 40 لسنة 1951[42]، فإنَّ الحمايةَ المدنيَّةَ للأمنِ السيبرانيِّ ما زالتْ تواجهُ عدَّةَ تحدِّياتٍ بنيويَّةٍ وتشريعيَّةٍ وفنِّيَّةٍ تُعيقُ فعاليَّةَ التعويضِ وإنصافَ المتضرِّرينَ.

أوَّلًا: غيابُ قانونٍ خاصٍّ يُنظِّمُ الحمايةَ المدنيَّةَ السيبرانيَّةَ:

رغمَ الجهودِ التشريعيَّةِ المبذولةِ، لم يُصوَّتْ حتَّى الآنَ على قانون مكافحة الجرائم الإلكترونيَّة العراقي، ممَّا يعني أنَّ المتضرِّرينَ من الأفعالِ السيبرانيَّةِ لا يجدونَ سوى القواعدِ العامَّةِ للمسؤوليَّةِ المدنيَّةِ الواردةِ في القانونِ المدنيِّ، وهي قواعدُ لا تتلاءمُ في كثيرٍ من تفاصيلِها مع طبيعةِ الفضاءِ السيبرانيِّ، إذ وُضِعتْ في سياقٍ تقليديٍّ لم يكنْ يتصوَّرُ وجودَ ضررٍ ناتجٍ عن اختراقٍ إلكترونيٍّ أو تسريبِ بياناتٍ أو هجومٍ معلوماتيٍّ[43].

ثانيًا: صعوبةُ إثباتِ الضررِ السيبرانيِّ أمامَ القضاءِ المدنيِّ:

من أبرزِ التحدِّياتِ في مجالِ الحمايةِ المدنيَّةِ الإلكترونيَّةِ صعوبةُ إثباتِ الضررِ والرابطةِ السببيَّةِ، ويعودُ ذلكَ إلى عدَّةِ أسبابٍ، من أهمِّها:

1- طبيعةُ الأضرارِ الإلكترونيَّةِ غيرِ الملموسةِ، مثل التشهيرِ أو فقدانِ البياناتِ.
2- صعوبةُ تحديدِ هُويَّةِ الجاني.
3- ضعفُ أدواتِ التحليلِ الرقميِّ القضائيِّ في العراقِ.
فعلى سبيلِ المثالِ، يتطلَّبُ إثباتُ أنَّ ضررًا ناتجًا عن اختراقٍ قد أدَّى إلى خسائرَ تجاريَّةٍ وجودَ أدلَّةٍ رقميَّةٍ موثوقةٍ مثل سجلاتِ الخادمِ (Logs)، وهذا يستلزمُ خبرةً فنِّيَّةً عاليةً وتنسيقًا مع جهاتٍ تقنيَّةٍ مثل وزارة الداخليَّة العراقيَّة أو شركاتِ الإنترنتِ[44].

ثالثًا: غيابُ قانونٍ لحمايةِ البياناتِ الشخصيَّةِ:
يُعَدُّ الفراغُ التشريعيُّ في موضوعِ حمايةِ البياناتِ الشخصيَّةِ من أكبرِ معوِّقاتِ الحمايةِ المدنيَّةِ السيبرانيَّةِ؛ فحتَّى الآنَ، لا يوجدُ في العراقِ قانونٌ يُنظِّمُ كيفيَّةَ جمعِ ومعالجةِ وتخزينِ واستخدامِ البياناتِ الشخصيَّةِ للمواطنينَ، على غرارِ التشريعاتِ الأوروبيَّةِ مثل اللائحةِ العامَّةِ لحمايةِ البيانات (GDPR)[45] ، ونتيجةً لذلكَ، فإنَّ أيَّ انتهاكٍ لخصوصيَّةِ البياناتِ - كحالاتِ تسريبِ معلوماتِ المواطنينَ من قواعدِ بياناتٍ رسميَّةٍ أو مصرفيَّةٍ - لا يُقابَلُ بنصٍّ قانونيٍّ مباشرٍ، بل يُحالُ إلى القواعدِ العامَّةِ في المسؤوليَّةِ التقصيريَّةِ، وهو ما يُضعِفُ فاعليَّةَ الحمايةِ القانونيَّةِ في هذا المجالِ[46].

رابعًا: ضعفُ الوعيِ القانونيِّ والرَّقميِّ لدى المتقاضينَ:
يُعاني عددٌ كبيرٌ من المواطنينَ، بل وحتَّى بعضُ المحامينَ، من ضعفٍ في الفهمِ القانونيِّ للتقنياتِ الرقميَّةِ، وهو ما يحدُّ من اللجوءِ إلى القضاءِ المدنيِّ في حالاتِ الضَّررِ السيبرانيِّ. وغالبًا ما يُنظَرُ إلى الجرائمِ السيبرانيَّةِ على أنَّها ذاتُ طابعٍ جنائيٍّ فقط، بينما يُهمَلُ جانبُ التعويضِ المدنيِّ، رغمَ أهميَّتِه في جبرِ الضَّررِ وردِّ الاعتبارِ للمتضرِّرِ[47].

خامسًا: عدمُ وجودِ قضاءٍ متخصِّصٍ في الجرائمِ الإلكترونيَّةِ المدنيَّةِ:
لا توجدُ - حتَّى الآنَ - محاكمُ متخصِّصةٌ في القضايا السيبرانيَّةِ، سواءٌ المدنيَّةِ أو الجنائيَّةِ، ممَّا يعني أنَّ هذه القضايا تُعرَضُ على محاكمِ البداءةِ العراقيَّةِ وفقَ الإجراءاتِ العامَّةِ، التي قد لا تمتلكُ الكفاءةَ الفنيَّةَ الكافيةَ للتعاملِ مع النِّزاعاتِ الرقميَّةِ المعقَّدةِ، خاصَّةً تلكَ المتعلِّقةَ بالمسؤوليَّةِ المدنيَّةِ، وحسابِ التعويضِ، والتحقيقِ الفنِّيِّ في الضررِ[48].

سادسًا: نقصُ الهيئاتِ الرَّقابيَّةِ السيبرانيَّةِ المدنيَّةِ:
تعتمدُ مؤسَّساتُ الدولةِ في الوقتِ الحاليِّ على مديريَّةِ الجرائمِ المعلوماتيَّةِ في وزارةِ الداخليَّةِ العراقيَّةِ، وهي جهةٌ ذاتُ طابعٍ أمنيٍّ وجنائيٍّ بحتٍ، أمَّا في الجانبِ المدنيِّ، فلا توجدُ هيئةٌ مستقلَّةٌ مختصَّةٌ بحمايةِ الخصوصيَّةِ أو بمتابعةِ الأضرارِ السيبرانيَّةِ المدنيَّةِ[49]، وهو ما يتعارضُ مع التوجُّهاتِ الحديثةِ التي تتبنَّاها دولٌ كثيرةٌ أنشأتْ هيئاتٍ مدنيَّةً متخصِّصةً، مثل:
1- هيئاتِ حمايةِ البياناتِ (Data Protection Authorities) .
2- هيئاتِ الحوكمةِ الرقميَّةِ.

سابعًا: تداخُلُ الاختصاصِ القضائيِّ والإقليميِّ:
بسببِ الطبيعةِ العابرةِ للحدودِ في الجرائمِ السيبرانيَّةِ، يُثارُ دائمًا سؤالُ الولايةِ القضائيَّةِ: مَن المسؤولُ عندَ حدوثِ ضررٍ سبَّبَهُ موقعٌ إلكترونيٌّ خارجَ العراقِ؟ أو شركةُ تخزينِ بياناتٍ مقرُّها في الخارجِ؟ والواقعُ أنَّ القواعدَ التقليديَّةَ للاختصاصِ المحلِّيِّ لا تكفي لضبطِ هذه الحالاتِ، ممَّا يُضعِفُ إمكانيَّةَ المطالبةِ بالتعويضِ من أطرافٍ أجنبيَّةٍ[50].

ويَرى الباحثُ أنَّ التحدِّياتِ البنيويَّةَ والتشريعيَّةَ والفنِّيَّةَ التي تُواجهُ الحمايةَ المدنيَّةَ للأمنِ السيبرانيِّ في العراقِ تُشكِّلُ عائقًا جوهريًّا أمامَ تحقيقِ حمايةٍ قانونيَّةٍ فعّالةٍ لحقوقِ الأفرادِ المتضرِّرينَ من الأفعالِ السيبرانيَّةِ؛ إذ يؤدّي غيابُ التشريعاتِ المتخصِّصةِ، وصعوبةُ الإثباتِ الرقميِّ أمامَ القضاءِ المدنيِّ، وافتقارُ المنظومةِ القضائيَّةِ إلى الكفاءاتِ والهيئاتِ المتخصِّصةِ، إلى تعطيلِ سُبلِ التعويضِ وجبرِ الضَّررِ، ويُضعفُ ثقةَ المتقاضينَ في جدوى حمايةِ القانونِ المدنيِّ من مخاطرِ الفضاءِ الإلكترونيِّ، رغمَ تفاقمِ هذهِ المخاطرِ واتِّساعِ نطاقِها. وانطلاقًا من ذلك، **يُوصي الباحثُ** بضرورةِ الإسراعِ في تبنّي تشريعٍ وطنيٍّ متكاملٍ يُنظِّمُ الحمايةَ المدنيَّةَ للأمنِ السيبرانيِّ، يتضمَّنُ أحكامًا خاصَّةً بالمسؤوليَّةِ المدنيَّةِ عن الأضرارِ الرقميَّةِ، وآليَّاتٍ واضحةً لإثباتِها، وإنشاءَ محاكمَ أو دوائرَ متخصِّصةٍ في القضايا السيبرانيَّةِ، فضلًا عن استحداثِ هيئةٍ وطنيَّةٍ مستقلَّةٍ لحمايةِ البياناتِ والخصوصيَّةِ الرقميَّةِ، وذلكَ بما يُعزِّزُ من فاعليَّةِ النظامِ القانونيِّ في مواكبةِ التحوُّلاتِ الرقميَّةِ المتسارعةِ وضمانِ إنصافِ المتضرِّرينَ.

الخاتمةُ
لقد أصبحتْ قضايا الأمنِ السيبرانيِّ اليومَ من أبرزِ التحدِّياتِ القانونيَّةِ التي تُواجهُ الدُّولَ والمجتمعاتِ في ظلِّ الثورةِ الرقميَّةِ التي تشهدُها البشريَّةُ، حيثُ أفرزتِ البيئةُ الإلكترونيَّةُ أنماطًا جديدةً من الأضرارِ التي تطالُ الأفرادَ والمؤسَّساتِ، وتتطلَّبُ أدواتٍ قانونيَّةً فعّالةً لحمايتِها وضمانِ جبرِها، وقد سعى هذا البحثُ إلى تسليطِ الضَّوءِ على أحدِ الأبعادِ الحيويَّةِ لهذه الحمايةِ، وهو البُعدُ **المدنيُّ غيرُ العقابيِّ**، من خلالِ دراسةِ مدى فاعليَّةِ القواعدِ القانونيَّةِ العراقيَّةِ في توفيرِ الحمايةِ المدنيَّةِ للأمنِ السيبرانيِّ، وتحليلِ أوجهِ القصورِ والتحدِّياتِ والاحتياجاتِ التشريعيَّةِ المُلحَّةِ. وتوصَّلَ البحثُ إلى أنَّ العراقَ لا يزالُ يفتقرُ إلى إطارٍ قانونيٍّ خاصٍّ ومنظَّمٍ يُنظِّمُ الحمايةَ المدنيَّةَ من الأضرارِ النَّاجمةِ عن الاعتداءاتِ السيبرانيَّةِ، وأنَّ الاعتمادَ على قواعدِ المسؤوليَّةِ التقليديَّةِ في القانونِ المدنيِّ العراقيِّ رقم 40 لسنة 1951 لا يُلبّي متطلَّباتِ الواقعِ الرقميِّ، وذلك بسببِ تعقيدِ طبيعةِ الضَّررِ السيبرانيِّ، وصعوبةِ إثباتِه، وغيابِ التخصُّصِ القضائيِّ، وانعدامِ قانونٍ لحمايةِ البياناتِ الشخصيَّةِ.

كما تبيَّنَ أنَّ تحقيقَ الحمايةِ المدنيَّةِ الكاملةِ للأمنِ السيبرانيِّ في العراق لا يُمكِنُ أن يتحقَّقَ إلَّا من خلالِ **منظومةٍ تشريعيَّةٍ متكاملةٍ**، تشملُ قانونًا خاصًّا بالأمنِ السيبرانيِّ، وآخرَ لحمايةِ البياناتِ، إلى جانبِ تهيئةٍ بيئةٍ قضائيَّةٍ وفنِّيَّةٍ تستوعبُ الخصوصيَّاتِ الرقميَّةَ.وفي ضوءِ النتائجِ المتوصَّلِ إليها، فإنَّ الحاجةَ باتتْ مُلحَّةً لوضعِ حلولٍ تشريعيَّةٍ ومؤسَّسيَّةٍ جذريَّةٍ تُواكِبُ التحدِّياتِ الرقميَّةَ، وتُعزِّزُ من الثقةِ العامَّةِ في الفضاءِ الإلكترونيِّ، وتُمكِّنُ الأفرادَ من الدِّفاعِ عن حقوقِهم المدنيَّةِ إذا ما اعتُدِيَ عليهم رقميًّا، بما ينسجمُ مع المعاييرِ الدوليَّةِ وحقوقِ الإنسانِ في البيئةِ السيبرانيَّةِ.

وعليهِ، فإنَّ الحمايةَ المدنيَّةَ للأمنِ السيبرانيِّ لَم تَعُدْ خيارًا قانونيًّا ثانويًّا، بل أصبحتْ **ضرورةً قانونيَّةً وأمنيَّةً واجتماعيَّةً**، لا يُمكِنُ للنِّظامِ القانونيِّ العراقيِّ أن يُواكِبَ تطوُّراتِ العصرِ دونَ أن يجعلَها أولويَّةً تشريعيَّةً وقضائيَّةً.

أوَّلًا: النَّتائجُ:

أسفرَت الدراسةُ عن جملةٍ من النَّتائجِ التي تُبيِّنُ مواطنَ القصورِ التشريعيِّ والعمليِّ في منظومةِ الحمايةِ المدنيَّةِ للأمنِ السيبرانيِّ في العراق، وذلكَ على النحوِ الآتي:

1- إنَّ غيابَ قانونٍ خاصٍّ يُنظِّمُ الحمايةَ المدنيَّةَ للأمنِ السيبرانيِّ في العراقِ بشكلٍ شاملٍ يُعَدُّ من أبرزِ مواطنِ القصورِ التشريعيِّ، وهو ما يفتحُ المجالَ أمامَ اجتهاداتٍ متباينةٍ في تفسيرِ القواعدِ العامَّةِ.

2- تعتمدُ الحمايةُ المدنيَّةُ في الوقتِ الراهنِ على القانونِ المدنيِّ العراقيِّ رقم 40 لسنة 1951، وتحديدًا قواعدِ المسؤوليَّةِ التقصيريَّةِ والعقديَّةِ، غيرَ أنَّ هذه القواعدَ لم تُصمَّمْ للتعاملِ مع طبيعةِ الأضرارِ الرقميَّةِ المعقَّدةِ.

3- الضررُ السيبرانيُّ - سواءٌ أكانَ ماديًّا أم معنويًّا - قابلٌ للتعويضِ من الناحيةِ النظريَّةِ بموجبِ النصوصِ المدنيَّةِ، لكنَّ إثباتَه أمامَ القضاءِ يُواجِهُ صعوباتٍ فنِّيَّةً كبيرةً في ظلِّ ضعفِ البنيةِ التحتيَّةِ الرقميَّةِ للمؤسَّساتِ القضائيَّةِ.

4- لا توجدُ محاكمُ أو دوائرُ مدنيَّةٌ متخصِّصةٌ في نظرِ المنازعاتِ ذاتِ الطابعِ السيبرانيِّ، ممَّا يؤدِّي إلى بُطءِ الإجراءاتِ وضعفِ الكفاءةِ في تقديرِ الأدلَّةِ الرقميَّةِ والضَّررِ غيرِ الملموسِ.

5- لا يزالُ الوعيُ القانونيُّ لدى الأفرادِ والمحامينَ والقضاةِ بمسألةِ الأمنِ السيبرانيِّ والمسؤوليَّةِ المدنيَّةِ عنهُ محدودًا، وهو ما يُضعِفُ من فرصِ إقامةِ الدَّعاوى المدنيَّةِ النَّاجحةِ في هذا السِّياقِ.

6- تضمُّ مسودةُ قانونِ مكافحةِ الجرائمِ الإلكترونيَّةِ العراقي إشاراتٍ إيجابيَّةً إلى الحقِّ بالتعويضِ المدنيِّ، لكنَّها لم تُقرَّ حتَّى الآنَ، ممَّا يجعلُها غيرَ مُلزمةٍ وغيرَ مُفعَّلةٍ.

7- إنَّ انعدامَ قانونٍ خاصٍّ بحمايةِ البياناتِ الشخصيَّةِ في العراقِ يُضعِفُ من ضماناتِ الأفرادِ عندَ انتهاكِ خصوصيَّاتِهم الرَّقميَّةِ، ويُعقِّدُ من سُبُلِ التعويضِ المدنيِّ.

ثانيًا: التَّوصياتُ:

استنادًا إلى ما تقدَّمَ من نتائجَ، يُوصي الباحثُ باتِّخاذِ الإجراءاتِ التشريعيَّةِ والمؤسَّسيَّةِ الآتيةِ:

1- **الإسراعُ في تشريعِ قانونٍ خاصٍّ بالأمنِ السيبرانيِّ في العراق**، يتضمَّنُ تنظيمًا دقيقًا للمسؤوليَّةِ المدنيَّةِ النَّاشئةِ عن الأفعالِ الرقميَّةِ، ويُحدِّدُ صورَ الضررِ القابلِ للتعويضِ وآليَّاتِ الإثباتِ.

2- **إصدارُ قانونٍ لحمايةِ البياناتِ الشخصيَّةِ**، يتضمَّنُ مبادئَ واضحةً حولَ كيفيَّةِ جمعِ البياناتِ وتخزينِها واستخدامِها، ويكفلُ للأفرادِ حقَّ المطالبةِ بالتعويضِ عندَ وقوعِ أيِّ انتهاكٍ.

3- **إنشاءُ محاكمَ أو هيئاتٍ مدنيَّةٍ رقميَّةٍ متخصِّصةٍ في نظرِ المنازعاتِ السيبرانيَّةِ**، تتولَّى الفصلَ في الدعاوى المتعلِّقةِ بالتعويضِ عن الأضرارِ الإلكترونيَّةِ بكفاءةٍ وسرعةٍ.

4- **تدريبُ القضاةِ والمحامينَ والموظَّفينَ القانونيِّينَ على قضايا الأمنِ السيبرانيِّ** والأدلَّةِ الرقميَّةِ، وتطويرُ برامجَ دراسيَّةٍ وتدريبيَّةٍ متخصِّصةٍ في هذا المجالِ.

5- **تعزيزُ أدواتِ الإثباتِ الرقميِّ أمامَ القضاءِ المدنيِّ**، من خلالِ التعاونِ بين السُّلطةِ القضائيَّةِ والجهاتِ الأمنيَّةِ والتقنيَّةِ المختصَّةِ، لضمانِ عدالةِ المحاكمةِ وكفاءةِ الإثباتِ.

6- **تبنِّي مبدأِ "التعويضِ الوقائيِّ"** في الحالاتِ التي يصعُبُ فيها تقديرُ الضَّررِ بدقَّةٍ، لضمانِ الحدِّ الأدنى من الإنصافِ للمتضرِّرينَ من الاعتداءاتِ السيبرانيَّةِ.

7- **الاستفادةُ من التَّجاربِ المقارنةِ**، ولا سيَّما التشريعاتِ الأوروبيَّةِ مثلِ اللائحةِ العامَّةِ لحمايةِ البياناتِ (GDPR)، وتجربتَي الإماراتِ العربيَّةِ المتَّحدةِ ومصر، في تطويرِ منظومةِ الحمايةِ المدنيَّةِ الرقميَّةِ في العراق.

الهوامش

(1) منى عبد الله السمحان، مُتطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإداريَّة، بحث منشور في مجلة كلية التربية-جامعة المنصورة، عدد 111 لسنة 2020، ص9.

(2) إيهاب خليفة، الأمن السيبراني، الماهيَّة والإشكاليَّات، أوراق مصريَّة، القاهرة، 2019، ص 5.

(3)**Thierry Berthier**, *Cybersécurité et cyberdéfense : enjeux et perspectives*, Presses Universitaires de France, 2019, P.83.

(4)Code de la défense – Article L2321-1

ينص على اختصاص الدولة في حماية نظم المعلومات والبنى التحتيَّة الحيويَّة.

https://www.legifrance.gouv.fr

(5) **Loi de programmation militaire (LPM) 2013-2019** – Loi n° 2013-1168 du 18 décembre 2013 – تُعنى بحماية نظم المعلومات الحيويَّة وتمنح صلاحيات أوسع، مرجع أساسي للتشريع السيبراني في فرنسا.

(6) Règlement (UE) 2019/881 – Cybersecurity Act قانون أوروبي ينسجم مع التوجهات الفرنسيَّة ويعزز الأمن السيبراني على مستوى المنتجات والخدمات الرقميَّة.

(7) **Vincent Gautrais**, *La gouvernance de la cybersécurité*, Revue Lamy Droit de l'immatériel, 2022, P. 117.

(8) محمد كاظم حسن، "الأمن السيبراني في العراق بين الحاجة التشريعيَّة والتحديات الواقعيَّة"، *مجلة القانون والاقتصاد*، العدد 54، 2021، ص 107.

(9) أمل فاضل الساعدي، *القانون الجنائي والأمن السيبراني: دراسة مقارنة*، دار صفاء للنشر، عمان، 2022، ص 51.

(10) علي كريم الحيدري، "الحماية الجنائيَّة للأمن السيبراني: دراسة تحليليَّة"، رسالة ماجستير غير منشورة، كلية القانون – جامعة الكوفة، 2020، ص23.

(11) NIST SP 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, 2020.

(12) د. زينب عبد الستار، "حماية البيانات الشخصيَّة في البيئة الرقميَّة: دراسة مقارنة"، مجلة القانون والسياسة، جامعة كركوك، 2022، ص 18.

(13) **Berthier, Thierry.** *Cybersécurité et cyberdéfense : Enjeux et pratiques*, PUF, 2019, p. 67.

(14) **Arpagian, Nicolas.** *La cybersécurité*, Que sais-je?, Presses Universitaires de France, 2021, p. 54.

(15) **Gautrais, Vincent.** *Le droit à la confidentialité dans l'environnement numérique*, Revue Lex Electronica, 2020, p. 93.

(16) وزارة الاتصالات العراقيَّة، رؤية العراق للتحوُّل الرقمي، 2023.

(17) مركز الإعلام الرقمي العراقيDMC ، "تحليل الخروقات الأمنيَّة للبيانات الحكوميَّة"، 2022.

(18) **د. سامي قرقورة**، *حماية البيانات الشخصيَّة بين القانون المصري والاتفاقيَّات الدوليَّة*، المجلة المصريَّة للقانون والتقنية، عدد خاص 2022، ص 13.

(19) ISO/IEC 27001, *Information Security Management Systems*, 2013.

(20) NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, 2018.

(21) Arpagian, Nicolas. *La cybersécurité*, PUF, 2021.

(22) حسن علي عبد الكريم، "الحماية القانونيَّة لسلامة البيانات في القانون العراقي"، مجلة الدراسات القانونيَّة، جامعة بغداد، العدد 4، 2022، ص 12.

(23) ITU, *Cybersecurity Guide for Developing Countries*, Geneva, 2020.

(24) د. شريف كامل، *الأمن السيبراني في القانون المصري*، دار النهضة العربيَّة، 2020، ص 32.

(25) قانون 175 لسنة 2018، المواد 8 و15.

(26) قانون 151 لسنة 2020، المواد 2 و7.

(27) د. محمد بلال، *جرائم تقنية المعلومات في القانون المصري والمقارن*، 2021، ص 49.

(28) د. زينب عبد الستار، "حماية البيانات الشخصيَّة في البيئة الرقميَّة، مرجع سابق، ص 19.

(29) ISO/IEC 27001, *Information Security Management Systems*, 2013.

(30) ITU, *Cybersecurity Guide for Developing Countries*, Geneva, 2020.

(31) محمد عبد الكريم العاني، "إشكاليَّة استمراريَّة الخدمة الإلكترونيَّة في القانون العراقي"، مجلة البحوث القانونيَّة والسياسيَّة، جامعة الموصل، العدد 2، 2022، ص 23.

(32) NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, 2018.

(33) **Règlement (UE) 2016/679 (GDPR),** Article 32

(34) محمد جبار الكعبي، "الاستراتيجيَّة الوطنيَّة للأمن السيبراني في العراق: الفراغ التشريعي والتحديات الأمنيَّة"، مجلة دراسات أمنيَّة، جامعة النهرين، العدد 6، 2023، ص 17.

(35) NIST SP 800-160 Vol. 2, Developing Cyber Resilient Systems, 2021.ITU, National Cybersecurity Strategy Guide, Geneva, 2021.

(36) *Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019, modifiée par Loi n° 2019-1474 du 28 décembre 2019.*

(37) Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.

(38) قانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات، *الجريدة الرسميَّة المصريَّة*، العدد 33 مكرر (أ)، 14 أغسطس 2018.

(39) قانون رقم 151 لسنة 2020 بشأن حماية البيانات الشخصيَّة، *الجريدة الرسميَّة المصريَّة*، العدد 32 مكرر (ج)، 5 نوفمبر 2020.

(40) قانون مكافحة الجرائم المعلوماتيَّة رقم 31 لسنة 2023، *الوقائع العراقيَّة*، العدد 4720، 13 مارس 2023.

(41) وزارة الداخليَّة العراقيَّة – مديريَّة حماية البنى التحتيَّة https://moi.gov.iq . (2024).

الجهاز المركزي لتكنولوجيا المعلومات – الأمانة العامَّة لمجلس الوزراء العراقيhttps://it.gov.iq . (2024).

(42) القانون المدني العراقي، المادة 204 – 206.

(43) عبد الله الزيدي، الجرائم الإلكترونيَّة في القانون العراقي والمقارن، دار الثقافة، عمَّان، 2020، ص 110.

(44) ياسين عبد الجبار، المسؤوليَّة المدنيَّة في البيئة الرقميَّة، مجلة القانون المقارن، العدد 9، 2021، ص 42.

(45) مسودة قانون حماية البيانات الشخصيَّة، مجلس النواب العراقي، لجنة الأمن والدفاع، 2022 (غير مُقرّة).

(46) محمد العزاوي، الخصوصيَّة الرقميَّة في العراق: الحاجة لقانون حماية البيانات،مجلة المستقبل الرقمي، العدد 3،2023، ص19-3.

(47) أحمد الجنابي، الثغرات القانونيَّة في جرائم الإنترنت في العراق، المركز العراقي للسياسات الرقميَّة، 2021، ص 23.

(48) مجلس القضاء الأعلى – تقرير لجنة تطوير الأداء القضائي، 2022، الفقرة 17.

(49) تقرير البنك الدولي، تعزيز الأمن السيبراني في الشرق الأوسط، 2021، ص 28.

(50) طارق الكبيسي، الاختصاص القضائي في الجرائم المعلوماتيَّة عبر الحدود، مجلة القانون الدولي، العدد 12، 2022، ص54.

قائمة المراجع

أولًا: الكتب العامَّة:

1. أحمد الجنابي، الثغرات القانونيَّة في جرائم الإنترنت في العراق، المركز العراقي للسياسات الرقميَّة، 2021.
2. أمل فاضل الساعدي، *القانون الجنائي والأمن السيبراني: دراسة مقارنة*، دار صفاء للنشر، عمَّان، 2022.
3. إيهاب خليفة، الأمن السيبراني، الماهيَّة والإشكاليَّات، أوراق مصريَّة، القاهرة، 2019.
4. عبد الله الزيدي، الجرائم الإلكترونيَّة في القانون العراقي والمقارن، دار الثقافة، عمان، 2020.
5. منى جبور الأشقر، السيبرانيَّة هاجس العصر، جامعة الدول العربيَّة، القاهرة، المركز العربي للبحوث القانونيَّة والقضائيَّة، القاهرة، 2017.

ثانيًا: الرسائل العلميَّة:

1. علي كريم الحيدري، "الحماية الجنائيَّة للأمن السيبراني: دراسة تحليليَّة"، رسالة ماجستير غير منشورة، كلية القانون – جامعة الكوفة، 2020.

ثالثًا: الأبحاث العلميَّة:

1. حسن علي عبد الكريم"الحماية القانونيَّة لسلامة البيانات في القانون العراقي"،مجلة الدراسات القانونيَّة،جامعة بغداد،العدد2022،4.
2. زينب عبد الستار، "حماية البيانات الشخصيَّة في البيئة الرقميَّة: دراسة مقارنة"، مجلة القانون والسياسة، جامعة كركوك، 2022.
3. طارق الكبيسي، الاختصاص القضائي في الجرائم المعلوماتيَّة عبر الحدود، مجلة القانون الدولي، العدد 12، 2022.
4. محمد العزاوي، الخصوصيَّة الرقميَّة في العراق: الحاجة لقانون حماية البيانات، مجلة المستقبل الرقمي، العدد 3، 2023.
5. محمد جبار الكعبي، "الاستراتيجيَّة الوطنيَّة للأمن السيبراني في العراق: الفراغ التشريعي والتحديات الأمنيَّة"، مجلة دراسات أمنيَّة، جامعة النهرين، العدد 6، 2023.
6. محمد عبد الكريم العاني، "إشكاليَّة استمراريَّة الخدمة الإلكترونيَّة في القانون العراقي"، مجلة البحوث القانونيَّة والسياسيَّة، جامعة الموصل، العدد 2، 2022.
7. محمدكاظم حسن،"الأمن السيبراني في العراق بين الحاجة التشريعيَّة والتحديات الواقعيَّة"*مجلة القانون والاقتصاد*،العدد2021،54.
8. منى عبد الله السمحان، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإداريَّة، مجلة كلية التربية-جامعة المنصورة، عدد 111 لسنة 2020.
9. ياسين عبد الجبار، المسؤوليَّة المدنيَّة في البيئة الرقميَّة، مجلة القانون المقارن، العدد 9، 2021.

رابعًا: المراجع الرسميَّة:

(1): القوانين والتشريعات:

1- القانون المدني العراقي، مطبعة الحكومة، بغداد، 1951.
2- قانون الاتصالات رقم 10 لسنة 2003.
3- قانون الدفاع العسكري الفرنسي 2013.
4- قانون الأمن السيبراني الفرنسي 2019.
5- قانون حماية البيانات الشخصيَّة رقم 151 لسنة 2020.
6- مشروع قانون مكافحة الجرائم الإلكترونيَّة، مجلس النواب العراقي، 2021.
7- مسودة قانون حماية البيانات الشخصيَّة، مجلس النواب العراقي، لجنة الأمن والدفاع، 2022 (غير مُقرَّة).

(2): التقارير والدوريَّات والوثائق المؤسَّسيَّة:

1- الجريدة الرسميَّة العراقيَّة، الوقائع العراقيَّة، العدد 4672، 2022.
2- البنك الدولي، تقرير «تعزيز الأمن السيبراني في الشرق الأوسط»، 2021، ص 28.
3- مجلس القضاء الأعلى – تقرير لجنة تطوير الأداء القضائي، 2022، الفقرة 17.
4- مركز الإعلام الرقمي العراقي (DMC)، «تحليل الخروقات الأمنيَّة للبيانات الحكوميَّة»، 2022.
5- وزارة الاتصالات العراقيَّة، تقرير «واقع الخدمات الرقميَّة والبنية التحتيَّة في العراق»، 2022.
6- وزارة الاتصالات العراقيَّة، «رؤية العراق للتحوُّل الرقمي»، 2023.

خامسًا: المراجع الأجنبيَّة:

1. **Thierry Berthier**, *Cybersécurité et cyberdéfense : enjeux et perspectives*, Presses Universitaires de France, 2019.
2. **Vincent Gautrais**, *La gouvernance de la cybersécurité*, Revue Lamy Droit de l'immatériel, 2022.
3. **Berthier, Thierry.** *Cybersécurité et cyberdéfense : Enjeux et pratiques*, PUF, 2019.
4. **Arpagian, Nicolas.** *La cybersécurité*, Que sais-je?, Presses Universitaires de France, 2021.
5. G**autrais, Vincent.** *Le droit à la confidentialité dans l'environnement numérique*, Revue Lex Electronica, 2020.
6. ITU, *Cybersecurity Guide for Developing Countries*, Geneva, 2020.
7. NIST SP 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, 2020.
8. NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, 2018.
9. World Economic Forum, Cyber Resilience Playbook for Public-Private Collaboration, 2022.