



جمهورية العراق
وزارة التعليم العالي والبحث العلمي
جامعة القادسية
كلية القانون

المسؤولية المدنية لشركات الأمن السيبراني

(دراسة مقارنة)

رسالة تقدم بها الطالب

أحمد شاكر عبد

إلى مجلس كلية القانون - جامعة القادسية

وهي جزء من متطلبات نيل شهادة الماجستير في القانون الخاص

بإشراف

أ.م.د. صفاء متعب الخزاعي

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

﴿وَأَقُلُّ رَبِّ زِدْنِي عِلْمًا﴾

صدق الله العلي العظيم

سورة طه الآية ﴿114﴾ من

الإهداء

إلى حضرة الرسول المصطفى... سيدنا محمد صلى الله عليه واله
إلى من أحمل اسمة بكل افتخار , وإلى من بقي أثره حاضراً في
مسيرتي رغم غياب حضوره , أسأل الله أن يجعل هذا العمل نوراً في
ذكراه ورفعاً لمقامه ... والذي رحمه الله

إلى من كانت مصدر العقل والحكمة , وإلى من حملت في حضورها
معنى الطيبة والعطاء , وكان لدعائها ووجودها أثرٌ جميل بمسيرتي ...
جدتي العزيزة.

إلى من بها أكبر وعليها أعتد , إلى من وجودها قوة , ومحبتها
عطاء , التي معها عرفت معنى الحياة.....والدتي العزيزة.

إلى من كان سنداً وعوناً , وإلى من كان حضوره محل تقدير و اعتزاز
وكان لدعمه ومساندته أثرٌ طيب في مسيرتي ... عمي العزيز

قبل أن أختتم هذه الصفحة، أتوقف لأسجل عرفاني الخالص لابن خالتي
العزيز، الذي كان له فضل لا يُنسى في إنجاز هذا العمل. فقد كان عوناً
صادقاً حين احتجت، ومحفزاً لي في لحظات التعب، فله مني كل
تقدير ومحبة.

أهدي هذا الجهد المتواضع

شكر وعرّفان

الحمد لله رب العالمين أهل المجد والثناء، والصلاة والسلام على أشرف الأنبياء والمرسلين سيدنا محمد وعلى آله وصحبه.

فإن اللغة بمفرداتها الجمّة تتزاحم في وجدان الباحث لتعبّر عن عظيم الشكر والعرّفان إلى الفقيهة في القانون المتبحرة في مجالاته المتنوّعة الدكتور (أ.م.د. صفاء متعب الخزاعي)، الذي أكرمني برعايته فكان بمنزلة الأخ والسند منذ الوهلة الأولى في كتابة هذه الرسالة، فقدّم العون والنّصح والإرشاد، ولازم هذا العمل خطوة تلو خطوة، حتى صار على الوجه الذي بين أيديكم. فلك من الثناء أجزله ومن الإجلال أخلصه.

وأ تقدّم من الأساتذة أعضاء لجنة المناقشة الأكارم بالشكر الجزيل، لإبداء الموافقة على مناقشة هذه الرسالة، وتقديم ملاحظاتهم التي ستسهم في إثراء محتواها، وتحسين فحواها، وإظهارها بالشكل الحسن.

كما أتقدّم بالشكر والعرّفان إلى كلية القانون في جامعة القادسية وإلى الأساتذة الأفاضل فيها، وأختم بتقديم الامتتان إلى كل من أسدى إليّ نصحا أو يسر لي مصدرا أو مرجعا علميًا ضمن حرم الجامعة أو خارجها.

المستخلص

تنطوي شركات الأمن السيبراني على طبيعة قانونية لا تستقيم مع النماذج التقليدية المعهودة في القانون الخاص؛ فهي وإن اتخذت شكل الكيان التجاري الخاص إلا أن نشاطها يمس وظيفة حماية الأمن الرقمي الوطني التي كانت تحتكرها الدولة تاريخياً، وهو ما يُكسبها طابعاً سيادياً جزئياً ينعكس على طبيعتها التزاماتها ومعياري مسؤوليتها. وقد غدا هذا الإشكال أكثر حدة في ظل التوسع المتسارع في الاعتماد على الأنظمة الرقمية في المعاملات الحكومية والتجارية والمصرفية، إذ باتت هذه الشركات طرفاً محورياً في منظومة الأمن الرقمي لا يمكن إغفال دورها قانونياً، في حين يظل التنظيم المدني الخاص لمسؤوليتها غائباً في معظم الأنظمة المقارنة ولا سيما القانون العراقي الذي لا يزال يُحيل هذا النوع من النزاعات إلى القواعد العامة للمسؤولية المدنية رغم ما تنطوي عليه من قصور في استيعاب خصوصية هذا النشاط.

ويتناول هذا البحث جملةً من المسائل القانونية المتشابكة في هذا الشأن، أولها تكييف هذه الشركات قانونياً وتحديد شروط ثبوت صفتها وخصائصها التي تُميزها عن سائر مقدمي الخدمات التقنية، وثانيها تأصيل الالتزامات الملقاة على عاتقها سواء ما كان منها أساسياً متعلقاً بحماية الأنظمة والبيانات أم ثانوياً متعلقاً بالإفصاح والامتثال التنظيمي، وثالثها الوقوف عند التمييز بين الالتزام ببذل العناية والالتزام بتحقيق النتيجة وما يترتب عليه من أثر مباشر في معيار الخطأ وعبء الإثبات ونطاق التعويض في مواجهة العملاء والغير والجهات الرقابية على حدٍ سواء. ويُفضي البحث في نهاية المطاف إلى تشخيص مواطن الفراغ التشريعي في القانون المدني العراقي وتقديم مقترحات تشريعية تستلهم من التجربة المقارنة وتنسجم مع خصوصية المنظومة القانونية العراقية ومتطلبات الواقع الرقمي المتطور.



فهرست المحتويات





الموضوع	رقم الصفحة
المقدمة	9-1
الفصل الأول : الإطار المفاهيمي لشركات الأمن السيبراني	61-10
المبحث الأول : مفهوم شركات الأمن السيبراني	39-10
المطلب الأول : التعريف بشركات الأمن السيبراني	29-11
الفرع الأول : تعريف شركات الأمن السيبراني	21-11
الفرع الثاني : شروط ثبوت صفة شركة الأمن السيبراني	29-22
المطلب الثاني : خصائص شركات الأمن السيبراني	41-29
الفرع الأول : خصائص داعمة للطابع السيادي للأمن السيبراني	34-30
الفرع الثاني : خصائص مؤكدة للطابع التجاري الخاص	39-34
المبحث الثاني : ذاتية شركات الأمن السيبراني	61-40
المطلب الأول : التكيف القانوني لشركات الأمن السيبراني	49-40
الفرع الأول : مركز الشركة ضمن النظام القانوني	46-41
الفرع الثاني : العلاقة القانونية بين نشاط الشركة والقواعد الخاصة بالأمن السيبراني	49-46
المطلب الثاني : تمييز شركات الأمن السيبراني عما يشته به من الأوضاع	61-49
الفرع الأول : تمييز شركات الأمن السيبراني عن شركات تقنية المعلومات	57-50
الفرع الثاني : تمييز شركات الأمن السيبراني عن مزود الخدمات السحابية	61-58
الفصل الثاني : احكام ممارسة شركات الأمن السيبراني لنشاطها	132-62
المبحث الأول : التزامات شركات الأمن السيبراني تجاه العملاء	86-63
المطلب الأول : الالتزامات الأساسية في حماية الأنظمة والبيانات	76-63
الفرع الأول : حماية الأنظمة الرقمية والبيانات	71-64
الفرع الثاني : منع الاختراقات والحفاظ على استمرارية العمل	76-72
المطلب الثاني : الالتزامات الثانوية في الإفصاح والامتثال	85-76
الفرع الأول : الالتزام بالإفصاح عن المخاطر السيبرانية	81-76
الفرع الثاني : الالتزام بإعداد التقارير والامتثال	85-82
المبحث الثاني : المسؤولية القانونية لشركات الأمن السيبراني	132-86



المحتويات

٠

98-86	المطلب الأول : المسؤولية الناجمة عن الاخلال بالالتزامات الأساسية
92-87	الفرع الأول : الضرر المتعلق بالعملاء
98- 93	الفرع الثاني : الضرر المتعلق بالغير
109-98	المطلب الثاني : المسؤولية الناجمة عن الانتهاك القانوني والتنظيمي
105-99	الفرع الأول : المسؤولية القانونية للشركة ككيان معنوي امام الجهات الرقابية
109-105	الفرع الثاني : المسؤولية الفردية للإدارة والفنيين
132-110	المطالب الثالث : التأمين من مسؤولية شركات الامن السيبراني
123-110	الفرع الأول: مدى قابلية مسؤولية شركات الأمن السيبراني للتأمين
132-123	الفرع الثاني : اثار التأمين من المسؤولية المدنية لشركات الأمن السيبراني
137-133	الخاتمة
150-138	المصادر
A	Abstract



المقدمة

المقدمة

أولاً: بيان جوهر الموضوع

لم تعد المسؤولية المدنية في عصرنا الراهن مجرد أداة لجبر ضرر مادي تقليدي بين طرفين تجمعهما علاقة مباشرة، بل باتت تواجه تحديات جوهرية في مجال يشهد تحولاً متسارعاً هو مجال الأمن السيبراني. ففي بيئة رقمية تتداخل فيها حدود القانون الخاص بوظائف تقليدية كانت حكرّاً على الدولة، نشأت فئة من الكيانات التجارية تتولى حماية الأنظمة والبيانات الرقمية وتقديم خدمات أمنية متخصصة لا يستطيع المستخدم العادي أفراداً كانوا أم مؤسسات الاضطلاع بها بوسائله الذاتية. وهذه الكيانات هي ما بات يُعرف بشركات الأمن السيبراني.

وما يميز هذه الشركات عن سائر مقدمي الخدمات التجارية أنها تعمل في فضاء يجمع بين طابعين متلازمين ومتوترين في آنٍ واحد: فهي من حيث تكوينها كيان خاص يخضع لقواعد السوق والعقد، غير أن نشاطها يمس بصورة مباشرة وظيفة الأمن الرقمي الوطني التي لا تستطيع الدولة اليوم الاضطلاع بها منفردة. هذا التوتر بين الخصوصية التجارية والبُعد السيادي هو الذي يجعل تطبيق قواعد المسؤولية المدنية على نشاطها أمراً لا تكفي له القواعد التقليدية على نحوها المألوف.

والواقع أن القانون المقارن يعكس هذا التوتر بجلاء، فبينما طورت الأنظمة الأمريكية والفرنسية أطراً قانونية متخصصة تعيد رسم حدود المسؤولية في ضوء خصوصية هذا النشاط، يقف النظام القانوني العراقي أمام فراغ تشريعي في هذا الشأن يدفع القاضي والمتعاقد على حدٍ سواء إلى التعامل مع نزاعاتٍ معقدة بأدوات قانونية لم تُصنع أصلاً لمثل هذه الوقائع. ومن هنا تستمد هذه الدراسة مبررها: ليس سداً لفراغ نظري مجرد، بل إسهاماً في مسألة عملية تزداد إلحاحاً كلما توسع الاعتماد على الأنظمة الرقمية في المعاملات الحكومية والمصرفية والتجارية.

ثانياً : إشكالية الدراسة

تنطلق هذه الدراسة من فكرة ان غياب تنظيم مدني خاص لمسؤولية شركات الأمن السيبراني في القانون العراقي، وفي ضوء الطبيعة المزدوجة لهذه الشركات التي تجمع بين الخضوع لقواعد القانون الخاص واتصال نشاطها بالوظائف السيادية للدولة يثير تساؤل هل تكفي قواعد المسؤولية المدنية في صورتها التقليدية لاستيعاب خصوصية هذا النشاط وضمان حقوق المتضررين في التعويض، أم أن هذا الازدواج القانوني يستوجب إعادة النظر في معيار المسؤولية وأساس الإسناد ونطاق التعويض وفق ما يقتضيه الواقع الرقمي المتطور؟

وينفرع عن هذه الإشكالية المحورية تساؤلات فرعية أهمها

أولاً: ما المركز القانوني لشركات الأمن السيبراني في ضوء ازدواجها بين الطابع التجاري الخاص والطابع السيادي الجزئي، وهل يُخرجها هذا الازدواج من دائرة القواعد المدنية العامة أم يُبقيها محكومةً بها مع تشديد معيار المسؤولية؟

ثانياً: ما طبيعة الالتزام القانوني الملقى على عاتق هذه الشركات؟ هل هو التزام ببذل عناية أم التزام بتحقيق نتيجة؟ وكيف يؤثر هذا التمييز على عبء الإثبات في دعاوى المسؤولية؟

ثالثاً: هل يُشدد الطابع السيادي الجزئي من معيار العناية الواجبة، وما أثر ذلك على نطاق مسؤولية هذه الشركات في مواجهة العملاء والأطراف الثالثة؟

رابعاً: ما حدود المسؤولية المدنية لشركات الأمن السيبراني تجاه الغير ممن لا تربطهم بها علاقة تعاقدية مباشرة، وهل تمتد إليهم الحماية القانونية في غياب الرابطة العقدية؟

ثالثاً: فرضية الدراسة

تقوم هذه الدراسة على فرضية مركزية مؤداها أن ما يبدو في ظاهره إشكالية تقنية تتعلق بتكثيف طبيعة التزام شركات الأمن السيبراني ببذل العناية أم بتحقيق النتيجة، وإن كان الأول فهل هي عناية معتادة أم مشددة إنما يكشف في جوهره عن تحول أعمق في بنية القانون المعاصر: وهو تراجع النموذج الهرمي التقليدي القائم على احتكار الدولة لمصادر الإلزام، لصالح نموذج تشاركي يقوم على تعدد الفاعلين وتنوع مصادر المعيارية القانونية.

وتتفرع عن هذه الفرضية المركزية فرضيتان فرعيتان:

الفرضية الأولى: يُجسّد الطابع السيادي الجزئي الذي تكتسبه شركات الأمن السيبراني مظهراً خاصاً لانتقال أشمل: من نموذج الحكومة بوصفها سلطة مركزية تحتكر وظيفة حماية الأمن الوطني، إلى نموذج الحوكمة بوصفها شبكة تشاركية من فاعلين عموميين وخصوصيين تتوزع فيما بينهم عن طريق آليات التفويض والتأهيل والترخيص ممارسة وظيفة كانت حكراً على السيادة. وهذا الانتقال، وإن لم يُخرج الشركة من دائرة القانون الخاص، يُرتّب عليها التزامات موضوعية مشددة تقترب في طبيعتها من التزامات أشخاص القانون العام، مما يسوّغ تشديد معيار مسؤوليتها المدنية.

الفرضية الثانية: يتحول مصدر المعيارية الملزمة لأداء شركات الأمن السيبراني من نموذج التقنين القائم على نص تشريعي أمر صادر عن سلطة تشريعية مركزية سابقة على النزاع إلى نموذج التنظيم القائم على معايير فنية مرنة ومتجددة تصدر عن هيئات تقنية متخصصة كالمعهد الوطني الأمريكي للمعايير والتقنية (NIST) والوكالة الوطنية الفرنسية لأمن نظم المعلومات (ANSSI) وهيئة الإعلام والاتصالات العراقية (CMC)، تستمد قوتها الإلزامية لا من ذاتها نصاً بل من توظيف القضاء المدني لها معياراً موضوعياً في تقدير الخطأ.

وتفترض الدراسة أن هاتين الظاهرتين لا تتحققان بالقدر ذاته في الأنظمة الثلاثة محل المقارنة، بل تتفاوتان تبعاً لنضج البنية المؤسسية والتنظيمية لكل نظام. والفجوة التشريعية في العراق تعكس، على وجه الخصوص، بقاء أقرب إلى منطق الحكومة والتقنين التقليديين في مقابل تقدم النظامين الأمريكي والفرنسي نحو منطق الحوكمة والتنظيم، وهو ما يستوجب تدخلاً تشريعياً وقضائياً لاستكمال هذا الانتقال.

رابعاً: أهمية الدراسة

تستمد هذه الدراسة أهميتها من جانبين، على الجانب النظري، تُعدّ هذه الدراسة من الإسهامات القانونية التي تتناول المسؤولية المدنية لشركات الأمن السيبراني من منظور مدني مقارن، في حين انصرف الفقه القانوني في معظمه حين تناول هذا الموضوع إلى جوانبه الجنائية أو التقنية دون تأصيل مدني رصين لطبيعة المسؤولية وأركانها وأثرها على عبء الإثبات.

أما على الجانب العملي، فثمة حاجة متنامية لا يمكن إغفالها: فالتوسع المتسارع في الاعتماد على الأنظمة الرقمية في المعاملات الحكومية والتجارية والمصرفية العراقية يُفضي حتماً إلى تزايد العلاقات التعاقدية مع شركات الأمن السيبراني، ومعها تزداد النزاعات المحتملة المتعلقة بالإخلال بالالتزامات. والقاضي العراقي اليوم يواجه هذا النوع من الدعاوى دون إطار قانوني خاص يستند إليه. وتسعى هذه الدراسة إلى تزويد المشرع والقضاء والمتعاقد بمادة مقارنة تُعينهم على ملء هذا الفراغ بصورة تنسجم مع خصوصية القانون المدني العراقي ..

خامساً: اهداف الدراسة

تتوخى هذه الدراسة تحقيق جملة من الأهداف العلمية على النحو الآتي:

أولاً: بناء مفهوم قانوني مستقل لشركات الأمن السيبراني مستند إلى مصادر القانون ذاتها تشريعاً وقضاءً وفقهاً بعيداً عن الأوصاف التقنية التي هيمنت على الدراسات السابقة.

ثانياً: تأصيل الطبيعة القانونية للالتزامات الملقاة على عاتق هذه الشركات وتحديد انعكاساتها على معيار الخطأ وعبء الإثبات ونطاق التعويض في مواجهة العملاء والغير والجهات الرقابية.

ثالثاً: توظيف المادة (110/ثانياً) من الدستور العراقي في تأصيل الطابع السيادي الجزئي لنشاط هذه الشركات بوصفه أساساً دستورياً يُسوِّغ تشديد معيار العناية الواجبة ويوسّع نطاق مسؤوليتها المدنية.

رابعاً: تشخيص مواطن الفراغ التشريعي في القانون المدني العراقي تشخيصاً دقيقاً، وتقديم مقترحات تشريعية مدعومة بنصوص مواد مقترحة لتعديل اللائحة التنظيمية رقم 33 لسنة 2025 وإرساء نظام مسؤولية مدنية خاص يضبط هذا النشاط.

سادساً: دراسات سابقة

1- ساجدة نعيم علي الجالودي، "المسؤولية المدنية لمقدمي خدمات الأمن السيبراني وفق أحكام قانون الأمن السيبراني الأردني رقم 16 لسنة 2019 (دراسة تحليلية)"، رسالة ماجستير، كلية الحقوق، جامعة عمان الأهلية، 2024/2023.

تناولت هذه الدراسة المسؤولية المدنية لمقدمي خدمات الأمن السيبراني في ضوء أحكام قانون الأمن السيبراني الأردني رقم 16 لسنة 2019، وانصبَّ اهتمامها على تحديد نطاق هذه المسؤولية وأثر الإخلال بالالتزامات الواقعة على عاتق مقدمي الخدمة سواء داخل حدود صلاحياتهم أم خارجها. وقد خلصت الدراسة إلى أن المشرع الأردني أغفل تحديد نطاق المسؤولية المدنية لمقدمي هذه الخدمات بصورة صريحة، وأوصت بضرورة استحداث نص خاص يُعالج هذا الفراغ التشريعي. وتختلف دراستنا عنها من ثلاثة أوجه جوهرية — أولها أن دراستنا تتناول شركات الأمن السيبراني بوصفها كياناً قانونياً مستقلاً يجمع بين الطابع التجاري الخاص والطابع السيادي الجزئي، بدلاً من الاقتصار على مقدمي الخدمة في ضوء قانون سيبراني بعينه، وثانيها أن دراستنا تُوصِّل طبيعة الالتزام وتُتميز بين الالتزام ببذل العناية والالتزام بتحقيق النتيجة وأثر هذا التمييز على عبء الإثبات، وثالثها أن دراستنا تنتهج المنهج المقارن بين ثلاثة أنظمة تمثل مستويات متفاوتة في النضج التشريعي بدلاً من الاقتصار على نظام قانوني واحد.

2- وليد مرزة حمزة المخزومي ومحمد خزعل عباس، "أمن الفضاء السيبراني، قراءة في المفهوم القانوني"، مجلة العلوم القانونية، كلية القانون، جامعة بغداد، المجلد 37، العدد 2، 2023. تناولت هذه الدراسة المفهوم القانوني للفضاء السيبراني وأمنه، وتمحورت إشكاليته حول تحديد ماهية الأمن السيبراني وبيان ما إذا كان يختلف عن الأمن المادي، وكيفية الانتقال بهذا المفهوم من النطاق التقني الذي نشأ فيه إلى النطاق القانوني. وتختلف دراستنا عنها في أنها تنتقل خطوة أبعد من المفهوم العام للأمن السيبراني إلى تكييف الكيان القانوني الخاص القائم على تقديمه، وتُفرد فصلاً مستقلاً لبحث المسؤولية المدنية الناشئة عن إخلاله بالتزاماته، وهو ما لم تتناوله تلك الدراسة.

3- مصطفى إبراهيم سلمان الشمري، "الأمن السيبراني وأثره في الأمن الوطني العراقي"، مجلة العلوم القانونية والسياسية، جامعة ديالى، المجلد 10، العدد 1، 2021، ص147-190. تناولت هذه الدراسة الأمن السيبراني من زاوية أثره في الأمن الوطني العراقي، نظراً لعلاقته المباشرة بمجالات الحياة العامة كافة من سياسة واقتصاد وأمن وثقافة، وانصرف اهتمامها إلى البعد الأمني والسياسي للظاهرة بما في ذلك علاقتها بالإرهاب والقضاء السيبراني. وتختلف دراستنا عنها في كونها تتناول الموضوع من

زاوية القانون المدني الخاص حصراً، وتبحث في طبيعة الالتزامات التعاقدية لشركات الأمن السيبراني ونطاق مسؤوليتها المدنية، لا في بُعدها الأمني الوطني العام الذي تناولته تلك الدراسة.

4- أحمد هشام فواز العمري، "المسؤولية المدنية لمقدمي خدمات الأمن السيبراني"، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنصورة، المجلد 15، العدد 93، 2025، ص 1-34. هدفت هذه الدراسة إلى بيان المسؤولية المدنية لمقدمي خدمات الأمن السيبراني باستخدام المنهج الوصفي التحليلي والمنهج المقارن بين القوانين ذات الصلة، وتمحورت مشكلتها حول بيان هذه المسؤولية بالرجوع إلى التشريع الأردني تحديداً، وانتهت إلى أن المشرع الأردني لم يعالج في قانون الأمن السيبراني المسائل الفنية للاعتداءات السيبرانية من حيث المضمون والأثر. وتختلف دراستنا عنها في أنها تنحصر في نظام قانوني واحد هو الأردني، في حين تتبنى دراستنا منهجاً مقارناً يشمل ثلاثة أنظمة هي الأمريكي والفرنسي والعراقي، وهي تتناول المسؤولية مباشرة دون تأصيل مسبق لطبيعة الكيان القائم بالنشاط، في حين تُخصّص دراستنا فصلاً كاملاً لتكييف شركة الأمن السيبراني وتمييزها عما يشتهر بها قبل بحث مسؤوليتها.

5- دحموش فايزة وجغام محمد، "شركات الحراسة الخاصة وخدمة الأمن العمومي"، مجلة دراسات وأبحاث، جامعة بسكرة، المجلد 14، العدد 3، يوليو 2022، ص 227. انطلقت هذه الدراسة من واقع التحول الذي شهدته الجزائر، كغيرها من الدول، نحو تقليص تدخل الدولة وتحرير الاقتصاد، مما أدى إلى مشاركة أشخاص القانون الخاص في تأمين مرافق كانت حكرًا على الدولة، حتى المرافق الحساسة كالأمن، من خلال شركات الحراسة الخاصة التي تنقل وسائل الإكراه إلى أطراف غير الدولة. وتمحورت إشكالياتها حول السؤال الآتي: ما حدود المهام المنوطة بشركات الحراسة الخاصة، وما أثر ذلك على جودة خدمة الأمن العمومي؟ وتختلف دراستنا عنها في أن محل بحثها هو تفويض الوظيفة السيادية الأمنية بمعناها التقليدي المادي (حراسة الأشخاص والممتلكات)، في حين ينصرف بحثنا إلى تفويض جزء من الوظيفة السيادية في بُعدها الرقمي عبر شركات الأمن السيبراني. كما أن إشكالياتها تنحصر في حدود المهام وأثرها على جودة الخدمة العمومية، في حين تمتد إشكاليتنا إلى تكييف هذا الكيان قانونياً وتحديد نطاق مسؤوليته المدنية. ومع ذلك فإن هذه الدراسة تمثل سندا مهماً لدراستنا في تأصيل فكرة تفويض الوظائف السيادية للقطاع الخاص، وهي الفكرة التي استثمرناها في تأسيس الطابع السيادي الجزئي لشركات الأمن السيبراني بالاستناد إلى المادة (110/ثانياً) من الدستور العراقي.

سابعاً: منهجية الدراسة ونطاقها

اعتمدت هذه الدراسة المنهج التحليلي المقارن أساساً لها، وقد جاء اختيار هذا المنهج لاعتبارات منهجية موضوعية تفرضها طبيعة الموضوع ذاتها. فالمسؤولية المدنية لشركات الأمن السيبراني موضوع يفتقر في القانون العراقي إلى تنظيم مدني خاص، مما يجعل الاستعانة بالتجربة القانونية المقارنة ضرورة منهجية لا خياراً، إذ لا يمكن تأصيل القواعد الواجبة التطبيق في غياب النص التشريعي الخاص إلا من خلال استقراء ما انتهت إليه الأنظمة القانونية الأكثر تطوراً في هذا الشأن واستخلاص المبادئ القانونية الصالحة للتطبيق في البيئة التشريعية العراقية. كما أن المنهج المقارن يُمكن الباحث من تقييم الحلول القانونية المقترحة بمعيّار موضوعي يتجاوز الاجتهاد الفردي، ويوفر أساساً علمياً رصيناً للمقترحات التشريعية التي تنتهي إليها الدراسة. وقد وقع اختيار الدراسة على ثلاثة أنظمة قانونية مقارنة هي النظام الأمريكي والنظام الفرنسي والنظام العراقي، ولم يكن هذا الاختيار عشوائياً بل قام على اعتبارات موضوعية دقيقة يمكن بيانها على النحو الآتي:

أما اختيار النظام الأمريكي فيعود إلى ريادته في مجال تشريعات الأمن السيبراني وكونه البيئة التي نشأت فيها معظم شركات الأمن السيبراني الكبرى وتطورت فيها أحكام المسؤولية المدنية المتعلقة بها عبر اجتهادات قضائية وتشريعية متراكمة. غير أن النظام القانوني الأمريكي يتسم بتعدد مصادره التشريعية بين المستوى الفيدرالي ومستوى الولايات، وهو تعدد يتعذر معه الإحاطة بجميع قوانين الولايات البالغ عددها خمسين ولاية في إطار دراسة مقارنة منهجية. لذا اقتصرنا هذه الدراسة في تناولها للنظام الأمريكي على القانون الفيدرالي وما يتفرع عنه من تشريعات وتنظيمات وقرارات قضائية صادرة عن المحاكم الفيدرالية، ولا سيما قانون الأمن الداخلي الأمريكي وقانون الإبلاغ عن الحوادث السيبرانية للبنى التحتية الحيوية لعام 2022 والتنظيمات الصادرة عن وكالة الأمن السيبراني وحماية البنية التحتية CISA ومعايير المعهد الوطني للمعايير والتكنولوجيا NIST فضلاً عن القرارات القضائية الفيدرالية ذات الصلة. واستثنى من هذا النطاق قوانين الولايات بوجه عام، مع الإشارة استثنائياً إلى قانون خصوصية المستهلك في كاليفورنيا CCPA بوصفه النموذج الأكثر تطوراً على مستوى الولايات في مجال حماية البيانات الرقمية، ولتأثيره المباشر في توجيه التشريعات الفيدرالية اللاحقة في هذا الشأن.

وأما اختيار النظام الفرنسي فيعود إلى عدة اعتبارات متكاملة، أبرزها أن القانون المدني الفرنسي يُشكّل المرجعية التاريخية والفقهية للقانون المدني العراقي، مما يجعل المقارنة معه مقارنةً في إطار أسرة قانونية واحدة تنتمي إليها الأنظمة اللاتينية، ويُيسّر استيعاب الحلول الفرنسية وتكييفها مع البيئة التشريعية العراقية. يُضاف إلى ذلك أن النظام الفرنسي طوّر إطاراً تنظيمياً متخصصاً للأمن السيبراني تشرف على تطبيقه

الوكالة الوطنية لأمن نظم المعلومات ANSSI ، وهو إطار يجمع بين الضبط التنظيمي الصارم والمرونة التعاقدية بما يجعله نموذجاً قانونياً متقدماً يستحق الدراسة والمقارنة. وقد اقتصرَت الدراسة في تناولها للنظام الفرنسي على القانون المدني الفرنسي والتشريعات والمراسيم التنظيمية الخاصة بالأمن السيبراني والقرارات القضائية الصادرة عن محكمة النقض الفرنسية ومحاكم الاستئناف ذات الصلة.

وأما اختيار النظام العراقي فهو محور الدراسة الأصلي ومنتهاها، إذ تسعى الدراسة إلى تشخيص الفراغ التشريعي في القانون المدني العراقي وتقديم مقترحات تشريعية رصينة تستلهم التجربة المقارنة وتنسجم مع خصوصية المنظومة القانونية العراقية. وقد اعتمدت الدراسة في تناولها للنظام العراقي على القانون المدني العراقي رقم 40 لسنة 1951 واللائحة التنظيمية رقم 33 لسنة 2025 الصادرة عن هيئة الإعلام والاتصالات، باعتبارها الإطار التنظيمي الأحدث الذي يُنظّم نشاط شركات الأمن السيبراني في العراق.

ثامناً : هيكلية الدراسة

اعتمد التقسيم الثنائي أسلوباً لهذه الدراسة، إذ خُصص الفصل الأول للإطار المفاهيمي لشركات الأمن السيبراني وهو مقسم على مبحثين: يتناول المبحث الأول مفهوم شركات الأمن السيبراني من خلال مطلبين، يبحث الأول في تعريف هذه الشركات وشروط ثبوت صفتها القانونية، ويبحث الثاني في خصائصها القانونية. أما المبحث الثاني فيتناول ذاتية شركات الأمن السيبراني من خلال مطلبين، يبحث الأول في التكيف القانوني لهذه الشركات ضمن النظام القانوني، ويبحث الثاني في تمييزها عما يشته به من أوضاع قانونية أخرى.

وخُصص الفصل احكام ممارسة شركات الامن السيبراني لنشاطها وهو مقسم على مبحثين: يتناول المبحث الأول التزامات شركات الأمن السيبراني تجاه عملائها من خلال مطلبين، يبحث الأول في الالتزامات الأساسية في حماية الأنظمة والبيانات، ويبحث الثاني في الالتزامات الثانوية في الإفصاح والامتثال. أما المبحث الثاني فيتناول المسؤولية القانونية الناجمة عن الإخلال بهذه الالتزامات من خلال مطلبين، يبحث الأول في المسؤولية الناجمة عن الإخلال بالالتزامات الأساسية، ويبحث الثاني في المسؤولية الناجمة عن الانتهاك القانوني والتنظيمي.



الفصل الأول

الإطار المفاهيمي لشركات الأمن السيبراني

المبحث الأول : مفهوم شركات الأمن السيبراني

المبحث الثاني : ذاتية شركات الأمن السيبراني

الفصل الأول

الإطار المفاهيمي لشركات الأمن السيبراني

أفرز تطوّر المعاملات الرقمية واقعاً جديداً للعلاقات التعاقدية ولحماية المصالح الخاصة، بحيث لم تعد سلامة المعاملة القانونية متوقعة على صحة الرضا أو مشروعية المحل فحسب، بل غدت مرتبطة أيضاً بأمن النظم المعلوماتية التي تُبرم من خلالها تلك المعاملات وتُنقذ في إطارها. وقد ترتب على ذلك أن أصبح الإخلال بأمن الأنظمة الرقمية سبباً مباشراً لقيام المسؤولية المدنية، سواء على أساس الإخلال بالالتزام التعاقدية أو على أساس الفعل الضار، بما أدخل الأمن السيبراني في صميم البنية الوظيفية للقانون الخاص. وفي هذا السياق برزت شركات الأمن السيبراني بوصفها كيانات قانونية خاصة يُعهد إليها، بموجب عقود، بتحقيق غاية قانونية محددة هي حماية المصالح المعلوماتية للمتعاقدين، وصون سرية البيانات، وضمان استمرارية الأنظمة الرقمية. غير أن اتساع دور هذه الشركات وتزايد اعتماد الأفراد والمؤسسات عليها كشف عن فراغ مفاهيمي في تحديد طبيعتها القانونية، وعن تردد في تكييف مركزها داخل منظومة القانون المدني، وتتمحور الإشكالية القانونية الجوهرية في هذا الصدد حول مدى كفاية القواعد المدنية العامة لاستيعاب هذا النشاط وتحديد مركزه القانوني، إذ يتردد الفقه بين تكييفه في إطار عقود المقاوله والخدمات، وبين الإقرار بخصوصيته المستقلة المستمدة من طبيعة الالتزامات التي يُفرزها واتصاله المباشر بالنظام العام الرقمي وأمن المعاملات، إن هذا الاضطراب لا يمكن تجاوزه بالرجوع إلى توصيفات فنية أو تنظيمية، وإنما يقتضي بناء مفهوم قانوني لشركات الأمن السيبراني يستند إلى مصادر القانون ذاته، أي إلى التشريع، والقضاء، والفقه، لا سيما وأن تكييف الأنشطة الاقتصادية الجديدة لا يستقيم بالرجوع إلى وصفها التقني، بل بتحديد طبيعة الالتزامات التي تُنشئها والمركز الذي يشغله القائم بها داخل منظومة القانون الخاص، إذ إن الالتزام هو العنصر الجوهري الذي تدور حوله المسؤولية المدنية وليس النشاط ذاته.

تأسيساً على ما سبق ارتأينا تقسيم الفصل على بحثين، يُعالج المبحث الأول مفهوم شركات الأمن السيبراني؛ أما المبحث الثاني فيتناول ذاتية شركات الأمن السيبراني.

المبحث الأول

مفهوم شركات الأمن السيبراني

يقتضي البحث في شركات الأمن السيبراني، قبل الخوض في تحديد التزاماتها ونطاق مسؤوليتها، الوقوف على مفهومها القانوني وتحديد هويتها داخل منظومة القانون الخاص. وتكمن الصعوبة في هذا التحديد في أن التشريعات المقارنة، في مختلف الأنظمة، لم تُفرد لهذه الشركات تعريفاً لفظياً مباشراً، بل اكتفت بتنظيم نشاطها وتحديد شروط مزاولته، تاركَةً للفقه والقضاء مهمة استخلاص المفهوم من طبيعة الخدمات والالتزامات. ومن ثَمَّ، فإن الوصول إلى مفهوم قانوني منضبط لهذه الشركات يستلزم تحليل المضمون القانوني لنشاطها عبر مصادر القانون الثلاثة: التشريع، والقضاء، والفقه، ولذلك سنقسم المبحث على مطلبين، الأول لبحث التعريف بشركات الأمن السيبراني، أما الثاني، فيحمل عنوان خصائص شركات الأمن السيبراني.

المطلب الأول

التعريف بشركات الأمن السيبراني

لا يقتصر الأمن السيبراني في حقيقته على كونه نشاطاً تقنياً، وإنما أفرز اتساع نطاقه آثاراً قانونية انعكست على طبيعة بعض العلاقات والالتزامات التي تنشأ في البيئة الرقمية، بحيث أصبحت مقتضيات الحماية الرقمية محلاً للالتزامات القانونية تتعدد مصادرها، ولا تقتصر على مجرد تقديم خدمة تقنية بمقابل. وقد أفضى اتساع الاعتماد على الأنظمة الرقمية إلى ظهور نشاط مهني متخصص اضطلعت به شركات الأمن السيبراني، غير أن تطور هذا النشاط في الممارسة العملية سبق استقرار تصور قانوني جامع لطبيعته ومفهومه في الأنظمة القانونية المقارنة، كما تكاثرت صور التعاقد بشأن خدماته قبل أن يستقر له تعريف تشريعي أو فقهي موحد.

ومن هنا ينبثق السؤال الذي يتصدى له هذا المطلب لا بمجرد حصر التعريفات التي أوردها التشريع والقضاء والفقه، وإنما بتحليل الأسس والعناصر التي يقوم عليها مفهوم قانوني منضبط لشركات الأمن السيبراني يُميّزها عن غيرها من الكيانات التي تزاوّل أنشطة تقنية متقاربة. ذلك أن تحديد نطاق المسؤولية المدنية المترتبة على نشاط هذه الشركات يستلزم، قبل كل شيء، تحديد محلها وأوصافها القانونية والعناصر المميزة لنشاطها إذ لا تنضبط المسؤولية قبل أن ينضبط المفهوم، وعليه نقسم هذا المطلب على فرعين، نخصص الأول لتعريف شركات الأمن السيبراني، والثاني لشروط ثبوت صفتها.



الفرع الأول

تعريف شركات الأمن السيبراني

لا يُراد بالتعريف القانوني لشركات الأمن السيبراني⁽¹⁾ مجرد الإحاطة اللفظية بمفهومها، بل يُراد به تأسيس المعيار الذي يُحدد متى تقوم المسؤولية المدنية لهذه الشركات ومتى تنتفي، فالتعريف الدقيق هو الذي يرسم حدود الالتزام ويُقيّد نطاق التعويض.

⁽¹⁾ يعد مصطلح شركات الأمن السيبراني من المصطلحات المركبة، ولذلك يستلزم فهمه تحليل كل مكون على حدة، بدءاً من الشركة مروراً بالأمن وصولاً إلى السيبرانية، مع استعراض أصل كل مصطلح في اللغة العربية والإنجليزية والفرنسية، فبالنسبة لمصطلح الشركة: الشركة: الاجتماع والاشتراك في الشيء، يقال: شرك القوم في الأمر إذا اجتمعوا فيه، والشركة هي الاشتراك في الشيء، أما في اللغة الإنجليزية فيقال Company مشتقة من اللاتينية companio، بمعنى رفيق أو شريك في المسير، واستخدمت لاحقاً لتدل على الكيان التجاري أو التعاقد بين عدة أفراد لأغراض اقتصادية، أما في الفرنسية فيقال Société وهي مشتقة من اللاتينية societas، وتعني الشراكة أو الجماعة، وهي تُستخدم في القانون الفرنسي للدلالة على الكيان التجاري الذي يجمع أشخاصاً لتحقيق هدف اقتصادي مشترك.

أما مصطلح الأمن مأخوذة في اللغة العربية من الجذر "أ م ن"، الذي يدل على الاطمئنان والحماية والاستقرار. وفي اللغة الإنجليزية Security من اللاتينية securitas، وتحمل نفس الدلالة: الحماية، السلامة، الاستقرار، أما في الفرنسية، فهي بلمعنى ذاته يطلق عليها Sécurité securitas مشتقة من اللاتينية.

أما (السيبراني) فلفظ مقترض من الإنجليزية، صيغ على هيئة الاسم المنسوب بإلحاق ياء النسبة به، والنسبة: (إلحاق آخر الاسم ياءً مشددةً مكسوراً ما قبلها، للدلالة على نسبة شيء إلى آخر)؛ فهو صفة تقيّد الموصوف ولا تستقل بمعنى. وأصله السابقة الإنجليزية (cyber) المقطوعة من مصطلح (cybernetics)، الذي صاغه عالم الرياضيات الأمريكي نوربرت وينر سنة 1948 اسماً لعلم التحكم والاتصال، واشتق من الكلمة اليونانية (kybernētēs) بمعنى ربّان السفينة أو قائد دفتها، ومجازاً: المرشد والحاكم ثم استقلت السابقة عن أصلها، وشاع استعمالها بعد أن صاغ الروائي وليم غيبسون مصطلح (cyberspace) سنة 1982، ومع انتشار الإنترنت في مطلع التسعينيات، فصارت تدل على ما يتصل بالحواسيب وشبكات الاتصال الإلكترونية، ولا سيما الإنترنت. وعليه فالسيبراني لغةً: المنسوب إلى الفضاء الذي تنشئه الحواسيب وشبكات الاتصال؛ فلا يدل اللفظ بمفرده على الأمن، وإنما يقيده بمجاله. ومن المصطلحات أعلاه يمكن تعريف شركات الأمن السيبراني لغة بأنها: الكيانات التي تنشأ من اجتماع أفراد أو أطراف متعددة (الشركة) لأداء مهام تتعلق بالحماية والاطمئنان (الأمن) في بيئة رقمية وشبكية محددة (السيبرانية).

لتفاصيل تلك المعاني يراجع: أبو الفضل جمال الدين محمد بن مكرم بن منظور الإفريقي المصري، لسان العرب، ابن منظور، ج2، مادة شرك، دار الحديث، القاهرة، الطبعة المنقحة، 2013، ص33.

المعجم الوسيط، مجمع اللغة العربية بالقاهرة، الطبعة الثانية، القاهرة، مادة أمن، 1972، ص64.

Dan Craigen, Nadia Diakun-Thibault, and Randy Purse, Defining Cybersecurity, Technology Innovation Management Review, 2014, p.14.

مصطفى الغلاييني، جامع الدروس العربية، ج2، ط28، المكتبة العصرية، صيدا - بيروت، 1993، ص71.

وبناءً على ذلك، سيتناول هذا الفرع تعريف شركات الأمن السيبراني من خلال ثلاثة محاور متكاملة وعلى النحو الآتي:

أولاً: تعريف شركات الأمن السيبراني في التشريع

لا يُعرف المشرّع عادةً الشركات الجديدة إلا عبر تنظيم نشاطها وليس عبر تعريف لفظي مباشر. وفي حالة شركات الأمن السيبراني، أظهرت التشريعات في مختلف الأنظمة، أنها تركز على الوظائف والخدمات والإجراءات التي تؤديها هذه الشركات بدل تحديد الكيان ذاته.

1. في التشريع الأمريكي

لم يُعرّف مصطلح شركة الأمن السيبراني صراحة في القانون الفيدرالي الأمريكي⁽¹⁾⁽²⁾، لكن العنوان السادس من قانون الولايات المتحدة للأمن الداخلي⁽³⁾ أشار إلى ما يُعرف بـ (الغرض الأمني السيبراني) وعرفه بأنه: "غرض حماية نظام معلومات أو المعلومات المخزنة فيه أو المعالجة من خلاله أو المارة عبره من التهديدات أو الثغرات السيبرانية"⁽⁴⁾. ويلاحظ أن المشرع الأمريكي اكتفى

(1) ما يجدر الإشارة له، أن قوانين الخصوصية والأمن السيبراني في الولايات المتحدة الأمريكية عدة وتصنف أو ترتبط بحسب القطاع الذي تطرح فيه، فهناك قوانين تحمي البيانات الطبية، والمصرفية/المالية، وبيانات الأطفال. سُنّت قوانين خصوصية خاصة ببيانات صحة المستهلك في بعض الولايات (مثل كاليفورنيا، وكونيكتيكت، ونيفادا، وواشنطن)، وسنستعرض تلك القوانين خلال الدراسة بحسب الحاجة لها.

(2) وتجدر الإشارة إلى وجود بعض المحاولات التشريعية الأمريكية اتجهت إلى وضع تصور لتعريف شركات الأمن السيبراني يُنظر: مشروع قانون مجلس نواب ولاية ميسيسيبي رقم (HB 1541) لسنة 2014، المادة الأولى، الفقرة (2)، المتعلق بمنح ائتمان ضريبي على الدخل لشركات الأمن السيبراني، وقد عرّف شركة الأمن السيبراني بأنها شركة منظمة لتحقيق الربح وتعمل بشكل أساسي في تطوير تكنولوجيا الأمن السيبراني المبتكرة والخاصة.

<https://billstatus.ls.state.ms.us/documents/2014/html/HB/1500-1599/HB1541IN.htm>

تاريخ اخر زيارة في 2026/1/25.

(3) ان العنوان السادس من القانون الأمريكي للولايات المتحدة (U.S.C 6) يمثل التصنيف الرسمي والمعتمد لجميع النصوص القانونية المتعلقة بالأمن الداخلي بعد دمج قانون الامن الداخلي الصادر عام 2002 والتعديلات اللاحقة ضمن القانون الأمريكي الموحد. يشمل هذا العنوان السادس الأحكام القانونية المتعلقة بإنشاء وزارة الأمن الداخلي، تنظيم وظائفها، تحديد سلطاتها، وتنسيق الإجراءات المتعلقة بحماية البنية التحتية الحيوية والأنظمة الداخلية للولايات المتحدة. لذا، يُعتبر الإشارة إليه أكثر دقة من الاكتفاء بذكر القانون الأصلي لعام 2002 (الامن الداخلي الأمريكي) حيث أن العنوان السادس يضم جميع المواد المحدث والمصنفة رسمياً ويتيح الرجوع للنصوص القانونية الكاملة والمعتمدة وهو متاح على الرابط:

<https://www.law.cornell.edu/uscode/text/6/650?u> تاريخ اخر زيارة في 2026/1/25.

(4) نص المادة (6) من قانون الامن الداخلي الأمريكي باللغة الإنجليزية:

بتعريف الغرض الأمني السيبراني لا الشركة ذاتها، وهو نهج يكشف عن توجه وظيفي يُحدد النشاط دون أن يُرسي مفهوماً قانونياً مستقلاً للكيان القائم به، مما يُفضي إلى فراغ مفاهيمي.

و كما عرّف التشريع ذاته (مزود الخدمة) بأنه: " كل كيان يقدم منتجات أو خدمات متعلقة بالحوسبة السحابية وفق المعايير المحددة من المعهد الوطني للمعايير والتكنولوجيا في منشوره رقم 145-800 وأي وثيقة تعديلية أو بديلة"⁽¹⁾، فيلاحظ أن التشريع الأمريكي قد ركّز على الخدمات والإجراءات والتدابير الأمنية⁽²⁾، بدلاً من إيراد تعريف مباشر للكيان أو الشركة التي توفرها.

يتضح مما سبق أن التشريع الأمريكي ركّز على الوظيفة والخدمة، لا على التسمية، بحيث يُستخلص تعريف شركات الأمن السيبراني من طبيعة الخدمات التي تقدمها.

2. في التشريع الفرنسي

لم يضع المشرع الفرنسي تعريفاً مباشراً لشركات الأمن السيبراني، لكنه أنشأ إطاراً وظيفياً وتنظيمياً واضحاً. فقد نصّ مرسوم رقم 350-2015 المؤرخ في 27 آذار/مارس 2015 المتعلق بتأهيل منتجات الأمن وشروط الخدمة على تأهيل مزودي خدمات الأمن السيبراني، وأسند إلى الوكالة

"The term "cybersecurity purpose" means the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability".

⁽¹⁾ نص المادة (3) من قانون الامن الداخلي الأمريكي باللغة الإنجليزية:

"The term "cloud service provider" means an entity offering products or services related to cloud computing, as defined by the National Institute of Standards and Technology in NIST Special Publication 800-145 and any amendatory or superseding document relating thereto."

⁽²⁾ من خلال مراجعة بنود التنفيذ التنظيمي لوكالات مثل وكالة الامن السيبراني وحماية البنية التحتية (CISA) وبعض الأدلة الصادرة عن المعهد الوطني للمعايير والتقنية (NIST)، يتضح أن المفاهيم المستخدمة تشمل "مزود خدمة الأمن السيبراني" أو "بائع الأمن السيبراني" قد استخدمت هذه المصطلحات ضمن أدوات واشتراطات تنظيمية مرتبطة بحماية البنى التحتية الحيوية والمعلوماتية. ومع ذلك، هذه المصطلحات لا ترتقي لتعريف تشريعي موحد، بل تبقى في مستوى التوصيف التنظيمي.

DEPARTMENT OF HOMELAND SECURITY, Cybersecurity and Infrastructure Security Agency, Federal Register/Vol. 89, No. 66/Thursday, April 4, 2024, p. 23644.

الوطنية لأمن نظم المعلومات (ANSSI)⁽¹⁾ مسؤولية اعتماد مزودي الخدمات ومراقبتهم بصفة دورية ضمن نظام مقدمي الخدمات المؤهلين والموثوقين⁽²⁾، الذي يُنظّم عمل الشركات الخاصة في حماية البنية التحتية المعلوماتية والاتصالات⁽³⁾، وقد عرف مرسوم 2015 مقدمي الخدمة والذي اطلق عليهم تسمية مقدمي خدمة الثقة بأنهم: " جميع الأشخاص مقدمي الخدمات الذين يساهمون في أمن أنظمة المعلومات"⁽⁴⁾.

ويلاحظ كذلك أن المرسوم الفرنسي عرّف مقدم الخدمة من خلال وظيفته لا من خلال طبيعته القانونية، إذ ربط الصفة القانونية بالمساهمة في أمن الأنظمة المعلوماتية دون تحديد العناصر الجوهرية المميزة لهذا الكيان عن غيره من مقدمي الخدمات الرقمية.

3. في التشريع العراقي

على مستوى التشريع العراقي، فتضمن تعريفاً صريحاً لشركات الأمن السيبراني عبر تصنيفها، فضلاً على أنّ اللائحة التنظيمية الخاصة بتنظيم عمل الشركات المختصة في خدمات الأمن السيبراني في جمهورية العراق، الصادرة استناداً إلى قرار مجلس المفوضين رقم (33) لسنة 2025، قد وضعت إطاراً تنظيمياً يلامس مضمون هذا المفهوم. فقد نصّت المادة (2) من اللائحة في باب التعاريف على أنّ "المرخص له هو أي جهة مرخصة من قبل الهيئة استناداً لأحكام الأمر 65 النافذ لتقديم خدمات

⁽¹⁾ الوكالة الوطنية لأمن نظم المعلومات (ANSSI) هي الهيئة الفرنسية المختصة بحماية وتأمين البنية التحتية الرقمية الوطنية وأنظمة المعلومات الحيوية، وتشرف على تطوير السياسات والإرشادات والمعايير المتعلقة بالأمن السيبراني، وتقديم الدعم الفني والإشرافي للجهات الحكومية والقطاع الخاص فيما يتعلق بمخاطر التهديدات السيبرانية. تأسست الوكالة بموجب المرسوم الفرنسي رقم 350-2015 الصادر بتاريخ 27 مارس 2015، وتعمل تحت إشراف رئاسة الوزراء الفرنسية.

الاختصار الرسمي بالفرنسية: Agence nationale de la sécurité des systèmes d'information (ANSSI).

⁽²⁾ Prestataires de Services de Confiance Qualifiés ويعرف بنظام PSCO .

⁽³⁾ Décret n° 2015-350 du 27 mars 2015 relatif à la qualification des prestataires de services de confiance pour la sécurité des systèmes d'information, Journal officiel de la République française, 29 mars 2015.

⁽⁴⁾ نص المادة (1) من مرسوم رقم 350-2015 المؤرخ في 27 آذار/مارس 2015 باللغة الفرنسية: " 2° "Prestataire de service de confiance", toute personne fournissant des services qui contribuent à la sécurité des systèmes d'information".



الأمن السيبراني في العراق"، كما عرف شركات الأمن السيبراني عبر تصنيفها تحديداً في المادة (6/ رابعاً-2) والتي نصت على أن: " الفئة الثانية: شركات الأمن السيبراني: حماية الأنظمة والشبكات من الهجمات السيبرانية. تقديم خدمات تحليل التهديدات ومراقبة الأنظمة".

ويستشف من هذا التعريف أن المشرع العراقي ربط الصفة القانونية لشركات الأمن السيبراني بالترخيص لا بالمضمون، مما يعني أن الشركة لا تكتسب هذه الصفة من طبيعة نشاطها الجوهرية، بل من الإذن الممنوح لها بمزاولته، وهو نهج ينطوي على قصور مفاهيمي واضح.

ثانياً: تعريف شركات الأمن السيبراني في القضاء

على المستوى القضائي، لم تشر المحاكم، سواء في الولايات المتحدة أو في فرنسا أو العراق، إلى تعريف مباشر لمصطلح شركات الأمن السيبراني بقدر ما اهتمت بتحديد الصفة العملية لمن يقدمون خدمات الحماية الرقمية وبتحديد مدى مسؤولياتهم المدنية والتعاقدية عند إخلالهم بواجباتهم.

1. على مستوى القضاء الأمريكي

على الرغم من أن القضاء الأمريكي لم يقدم تعريف مباشر لمصطلح شركات الأمن السيبراني، إلا أنه أسهم في تكييف البيئة القانونية التي تعمل ضمنها هذه الشركات، وذلك من خلال اجتهادات راسخة تناولت مفهوم الفضاء السيبراني ذاته. فقد اعتبرت المحكمة العليا الأمريكية في حكمها الصادر في قضية (رينو ضد الاتحاد الأمريكي للحريات المدنية) لعام 1997، أن الفضاء السيبراني "غير مرتبط بأي موقع جغرافي محدد، لكنه متاح لأي شخص، وبأي مكان في العالم مع إمكانيةولوج إلى الإنترنت، مما يسمح بإجراء المعاملات وتبادل الرسائل دون الكشف عن الهوية"، مؤكدة بذلك أن هذا الفضاء يشكل عالم افتراضي متكامل له خصائصه التقنية والاجتماعية الخاصة⁽¹⁾.

وتعدّ هذه الحيثية القضائية نقطة انطلاق لتحديد الإطار الذي تمارس ضمنه شركات الأمن السيبراني أعمالها، إذ تمارس نشاطها في فضاء غير مادي لا يخضع لحدود سيادية تقليدية، ما يجعلها خاضعة لأنماط جديدة من المسؤولية تتصل بواجب الحماية الرقمية وإدارة المخاطر العابرة للحدود. ومن ثم، فإن إقرار القضاء الأمريكي بالطبيعة المستقلة للفضاء السيبراني يُسهم ضمناً في تكييف هذه الشركات ككيانات قانونية ذات نشاط تقني تجاري يمارس ضمن بيئة ذات خصوصية قانونية متميزة

(1) Supreme Court of the United States, Reno v. American Civil Liberties Union, 521 U.S.

وأكد القضاء الأمريكي من خلال قرار محكمة الاستئناف الدائرة الثالثة في قضية لجنة التجارة الفيدرالية الأمريكية ضد وندهام⁽¹⁾ على أن الجهات التي تدير نظم معالجة البيانات وتحميها أو لا تحميها يمكن أن تخضع للرقابة والتطبيقات القانونية للهيئات الرقابية وإن تحرك مسؤوليتها وتُطال بالتعويض⁽²⁾، كما أن قضايا المسؤولية المدنية ضد مزودي الخدمات التقنية ومزودي الخدمة المدارة كثرت في الدعاوى الأخيرة التي رفعتها جهات تضررت من خروقات أمنية، ما يعكس تقبل المحاكم لكون هذه الكيانات طرف قابل للمساءلة المدنية والتعاقدية.

2. على مستوى القضاء الفرنسي

وعلى نحو مشابه، ركزت المحاكم الفرنسية في قضايا متعددة على واجبات مقدّم الخدمة من حيث (الإعلام) و(النصح) و(دقة الأداء الفني) لمستوى الحماية المتفق عليه، فصدرت أحكام استناداً إلى قواعد الالتزام التعاقدي والتقصيري ضدّ مقدّمي خدمات أمنية رقمية عندما ثبت تقصيرهم في أداء التزاماتهم أو في واجبات المعلومات والإرشاد للعميل⁽³⁾، وهو ما يؤكد قبول القضاء الفرنسي بإخضاع هذه الفئة من الكيانات لمسؤولية مدنية واضحة في حال وقوع الخطر أو الضرر الناتج عن فشل أمني.

(1) ويندهام العالمية هي شركة ضيافة تمنح امتيازات وتدير فنادق وتبيع وحدات سكنية مشتركة من خلال ثلاث شركات تابعة. رخصت ويندهام علامتها التجارية لما يقرب من 90 فندقاً مملوكاً بشكل مستقل. يحتوي كل فندق يحمل علامة ويندهام التجارية على نظام إدارة عقارات يعالج معلومات العملاء، بما في ذلك الأسماء، وعناوين المنازل، وعناوين البريد الإلكتروني، وأرقام الهواتف، وأرقام حسابات بطاقات الدفع، وتواريخ انتهاء الصلاحية، ورموز الأمان. تُدير ويندهام هذه الأنظمة وتلزم الفنادق بشرائها وتكوينها وفقاً لمواصفاتها الخاصة. مثلما تُشغل الشركة شبكة حاسوبية في فينيكس، أريزونا، تربط مركز بياناتها بأنظمة إدارة العقارات في كل فندق من فنادق ويندهام، وتزعم لجنة التجارة الفيدرالية (FTC) أن شركة ويندهام، منذ أبريل/نيسان 2008 على الأقل، مارست ممارسات غير عادلة في مجال الأمن السيبراني، "مُجمّعة"، عرضت بيانات المستهلكين الشخصية، بشكل غير معقول وغير ضروري، للوصول غير المصرح به والسرقة".

PRECEDENTIAL , UNITED STATES COURT OF APPEALS , FOR THE THIRD CIRCUIT, No. 14-3514, 2015 < D.C. Civil Action No. 2-13-cv-01887 , p.7-8.

(2) PRECEDENTIAL , UNITED STATES COURT OF APPEALS , FOR THE THIRD CIRCUIT, op.cit , p.12.

(3) في إطار الممارسة القضائية الفرنسية، قضت محكمة الاستئناف في رينس بتاريخ 19 نوفمبر 2024 بأن مزود خدمات أمنية إلكترونية أخفق في الوفاء بالتزاماته القانونية المتعلقة بواجب المعلومات والنصح تجاه العميل الذي تعرّض لهجوم إلكتروني أدى إلى خسارة بيانات حرجية ونسخ احتياطية، ونظراً لاعتقادها بأن هذه الخسائر ناجمة عن إخلال المزود بالعقد، رفعت الشركة العميلة دعوى قضائية ضد المزود لتقصيره في الوفاء بالتزامه بتقديم المعلومات والمشورة



ويلاحظ مما تقدم أن المحاكم الفرنسية ركزت على واجبات مزودي الخدمة من حيث الإعلام، النصح، ودقة الأداء الفني، وأخضعتها للمسؤولية التعاقدية والتقصيرية عند التقصير، مما يعكس الاعتراف القضائي بوجود شركات الأمن السيبراني والتزامها القانوني تجاه العملاء.

3. على مستوى القضاء العراقي

لم نجد في حدود ما اطلعنا عليه ، أي قرار قضائي عراقي يُعرّف صراحةً شركات الأمن السيبراني أو مزودي خدمات الحماية الرقمية. فلم يتم تناولها بعد من منظور قضائي، سواء فيما يتعلق بتحديد نطاق المسؤولية المدنية أو الإلزام التعاقدية لهذه الشركات. ولا يُفهم من غياب السابقة القضائية العراقية أن المشرع العراقي أغفل هذا المجال، بل يعكس حادثة التنظيم القانوني لشركات الأمن السيبراني في العراق، إذ لم تمض على صدور اللائحة رقم 33 لسنة 2025 مدة كافية لتكوّن اجتهاد قضائي راسخ، وأن غياب القضاء هنا دليل على بكاره الميدان لا على إغفاله.

والأداء السليم. في الدرجة الأولى، رفضت المحكمة التجارية في نانت دعاوى الشركة العميلة، معتبرة أنها لم تثبت أي خطأ من جانب المزود. واستأنفت الشركة العميلة هذا القرار، ألغت محكمة استئناف رين، في حكمها الصادر بتاريخ 19 نوفمبر/تشرين الثاني 2024، قرار المحكمة الابتدائية، وأيدت مسؤولية مقدم الخدمة عن عدم الوفاء بالتزاماته بالإبلاغ والنصح والتوجيه والتحذير. ورأت المحكمة أنه كان ينبغي على مقدم الخدمة، بصفته متخصصاً في تكنولوجيا المعلومات، القيام، على وجه الخصوص، بما يلي: "تحليل احتياجات الشركة العميلة لاقتراح بنية آمنة تلبي تلك الاحتياجات؛ تقديم المشورة والتوعية والتحذير للتعامل بشأن عواقب الخيارات التشغيلية المتخذة، وعرض حلول متنوعة مع التكاليف المرتبطة بها. بإخفاقه في الوفاء بهذه الالتزامات، حرم مقدم الخدمة الشركة العميلة من فرصة لتجنب أو تخفيف عواقب الهجوم الإلكتروني"، وبالتالي تم إلزام المزود بتعويض الضرر الناجم عن تقصيره. وقد ركزت المحكمة على طبيعة الخدمات المقدمة والإطار التعاقدية، معتبرة أن المسؤولية المدنية للكيان لا تتعلق بعبارة قانونية أو تشريعية محددة، بل بمستوى الأداء والالتزام الذي يفرضه القانون المدني الفرنسي على مقدمي الخدمات المتخصصة في الأمن السيبراني.

Cour d'appel de Rennes, 3e chambre commerciale, 19 novembre 2024, n° 23/04627, décision disponible sur Avoxa؛ (https://justice.pappers.fr/decision/308f967c2022a1bc6ccc7d1c531902751728a56b?utm_source=chatgpt.com

(. تاريخ اخر زيارة في 2026/6/14)

ثالثاً: تعريف شركات الأمن السيبراني في الفقه المقارن

1. على مستوى الفقه الأمريكي

ذهب جانب من الفقه الأمريكي إلى أن شركات الأمن السيبراني هي: "كيانات خاصة تضطلع بدور شبه حكومي في منظومة الحماية الرقمية، إذ باتت تؤدي وظائف لم تعد الدولة وحدها قادرة على الاضطلاع بها، مما يجعلها أشخاصاً معنوية خاصة تمارس صلاحيات تقترب من الوظائف العامة دون أن تفقد طابعها التجاري"⁽¹⁾. وعلى هذا الأساس، نظر الفقه الأمريكي إلى مزودي خدمات الأمن السيبراني على أنهم كيانات مسؤولة عن حماية الأنظمة والمعلومات الرقمية وفق إطار الالتزامات القانونية المقررة. ويُعدّ واجب الأمن السيبراني التزاماً على الشخص أو الكيان بما يجب عليهم فعله أو كان ينبغي عليهم فعله لتجنب عواقب قانونية غير مرغوب فيها، بما في ذلك الغرامات أو الأوامر القضائية أو التعويضات المدنية. ويشكل هذا الواجب إطاراً للالتزام مدني يمكن تحميل مزودي الخدمة المسؤولية بموجبه عند إخلالهم بالتزاماتهم التعاقدية أو التقصيرية. ويلاحظ أن تحديد هذا الواجب ليس أمر ثابت، بل هو سياقي وديناميكي، يعتمد على طبيعة النشاط والخدمات المقدمة، وعلى مجموعة القوانين واللوائح التنظيمية المطبقة، بما في ذلك المعايير المعترف بها للممارسات الفنية السليمة⁽²⁾. ويكشف هذا المنهج الوظيفي في الفقه الأمريكي عن حقيقة قانونية هي أن شركة الأمن السيبراني لا تكتسب صفتها من اسمها أو تسجيلها، بل من طبيعة الواجب الذي تتحمله تجاه عملائها، وهو واجب يختلف نوعاً لا درجةً عن واجب مزود الخدمة التقنية العادية.

2. على مستوى الفقه الفرنسي

وعلى مستوى الفقه الفرنسي، لم يُفرد الباحثون تعريفاً مستقلاً لشركات الأمن السيبراني، غير أن المقاربة الفقهية الفرنسية قدّمت تعريفاً وظيفياً مقيداً لمزودي هذه الخدمات، إذ ميّز كروكونير بين الكيان الذي يلتزم بتقديم خدمة تقنية عامة وبين الكيان الذي يتحمل التزاماً مستقلاً بحماية الأنظمة المعلوماتية من التهديدات، مؤكداً أن هذا الأخير يخضع لمعايير قانونية أكثر تشدداً تتعلق بطبيعة الالتزام

(1) Kristen E. Eichensehr, "Public-Private Cybersecurity", Texas Law Review, Vol. 95, No. 3, 2017, pp. 467-468,

(2) Charlotte A. Tschider, Locking Down "Reasonable" Cybersecurity Duty, YALE LAW & POLICY REVIEW, 41 : 2 2023, p.86-87-88.

ونطاق المسؤولية⁽¹⁾. وفي هذا الإطار يمكن القول إن شركة الأمن السيبراني في الفقه الفرنسي هي الكيان الذي يتحمل التزاماً وقائياً مستمراً بحماية الأنظمة الرقمية من المخاطر العدائية، وهو التزام يتجاوز مجرد تقديم الخدمة التقنية ليدخل في نطاق الالتزامات ذات الطابع المهني الخاص. وفي الفقه الفرنسي، يُنظر إلى مزودي خدمات الأمن السيبراني على أنهم كيانات تجارية خاصة تقوم بتقديم خدمات حماية وتأمين المعلومات الرقمية والأنظمة والشبكات، بما في ذلك صيانة الأنظمة والتدابير الوقائية والاستجابة للحوادث السيبرانية. ورغم غياب تعريف تشريعي موحد لشركة الأمن السيبراني، فإن هؤلاء المزودين يخضعون لإطار الترخيص والتأهيل التنظيمي، ويقعون تحت طائلة المسؤولية المدنية أو التعاقدية في حال تقصيرهم في أداء التزاماتهم تجاه العملاء أو تجاه الطرف المتضرر⁽²⁾. وبذلك، يبرز الفقه الفرنسي الطبيعة الوظيفية والتنظيمية للتعريف، حيث يُعتمد على أداء الكيان الفعلي والالتزام بمعايير الأمان المعترف بها قانوناً، لا على صياغة تعريف مجرد للمفهوم.

3. على مستوى الفقه العراقي

على مستوى الفقه العراقي، فقد عُرِّفت هذه الشركات بأنها شركات تجارية تقوم بهدف تقديم خدمات أمنية لتوفير الحماية للبيانات والمعلومات في النطاق الإلكتروني⁽³⁾، ويُلاحظ على هذا التعريف أنه وإن تجاوز إشكالية ربط الصفة بوجود نزاع فعلي، إلا أنه يحصر محل النشاط في حماية البيانات والمعلومات دون أن يمتد إلى حماية الأنظمة والشبكات والبنى التحتية الرقمية ذاتها وهو تضيق غير مبرر لمحل الالتزام، إذ إن نشاط شركات الأمن السيبراني في واقعه العملي يتجاوز حماية البيانات ليشمل صون الأنظمة بأسرها والاستجابة للحوادث ومنع الاختراقات، مما يجعل هذا التعريف قاصراً عن استيعاب النطاق الحقيقي لالتزامات هذه الشركات، وعُرِّفت كذلك بأنها "الشركات التجارية

(1) Alexandre Cruquenaire, La cybersécurité dans les contrats informatiques, Larcier, 2022, pp. 313-329.

(2) Cybermalveillance.gouv.fr, Label ExpertCyber et prestataires de cybersécurité، متاح على: <https://www.cybermalveillance.gouv.fr/tous-nos-contenus/label-expertcyber/questions-reponses-faq>. تاريخ اخر زيارة في 2026/6/14

وقد أكدت محكمة النقض الفرنسية التجارية بأن تحديد طبيعة الالتزام سواء كان التزام بذل عناية أم التزام بتحقيق نتيجة يتوقف على صياغة العقد ومضمون الالتزام لا على التسمية، وأن الالتزام الذي يتضمن تحديداً واضحاً للنتيجة المطلوبة يُعدّ التزاماً بتحقيق نتيجة حتى لو كان يتضمن عنصر المهارة والاجتهاد.

Cour de cassation, Chambre commerciale, 1er juin 2022, n° 20-19.476, inédit au bulletin.

(3) علي عبدالامير عبيد، المسؤولية الجنائية الناشئة عن انتهاكات الشركات السيبرانية الخاصة في النزاعات المسلحة، رسالة ماجستير، 2024، ص27.

التي تهدف إلى تقديم خدمات أمنية لتوفير الحماية للبيانات والمعلومات في النطاق الإلكتروني⁽¹⁾، ويلاحظ على التعريف انه يحصر محل النشاط في حماية البيانات والمعلومات دون أن يمتد إلى حماية الأنظمة والبنى التحتية الرقمية ذاتها، وهو تضيق غير مبرر لمحل الالتزام.

تأسيساً على ما سبق، يمكن ان نعرف شركات الامن السيبراني على انها: شخص معنوي ينشأ وفق الأحكام القانونية ويُمنح رخصة لمزاولة نشاط مهني محدد يتمثل في تقديم خدمات حماية وتأمين الأنظمة الرقمية، الشبكات والبيانات. ويخضع هذا الكيان في مزاولة نشاطه لأحكام القوانين ذات الصلة، ويتحمل المسؤولية القانونية الكاملة عن أي إخلال بالتزاماته تجاه العملاء أو الأطراف المتضررة.

وتم اختيار هذا التعريف للأسباب الآتية:

1. يظهر الطابع القانوني تحديداً القانون الخاص بشكل واضح: باستخدام عبارة (شخص معنوي ينشأ وفق الأحكام القانونية)، يلتزم التعريف بالمدخل القانوني للشركة كشخص معنوي مستقل.
2. يبرز الخصوصية بالنشاط محددة: ذكر (تقديم خدمات حماية وتأمين الأنظمة الرقمية، الشبكات والبيانات) يوضح مجال عمل الشركة ويميزها عن أي كيان آخر.
3. يشير إلى الإطار القانوني على نحو شامل: عبارة (يخضع هذا الكيان في مزاولة نشاطه لأحكام القوانين ذات الصلة) تغطي جميع الالتزامات القانونية، سواء مدنية، تجارية أو خاصة.
4. يُوَظَر إلى المسؤولية القانونية: ذكر (يتحمل المسؤولية القانونية الكاملة عن أي إخلال بالتزاماته تجاه العملاء أو الأطراف المتضررة) يربط التعريف مباشرة بالالتزام القانوني الفعلي للشركة، ويجعل التعريف عملياً وقابلاً للتطبيق.

(1) علي عبد الأمير عبيد، المصدر السابق ، ص27. وفي الفقه المصري، عُرِفَتْ بأنها "الشركات التجارية المختصة بتقديم خدمات الأمن السيبراني والتي ترتبط بالنزاعات المتعلقة بأسلحة الفضاء الإلكتروني وشن الهجمات الإلكترونية"، ينظر: مصطفى أحمد أبو الخير، الشركات العسكرية والأمنية الدولية الخاصة، دراسة قانونية سياسية، ط1، اترك للطباعة والنشر والتوزيع، القاهرة، 2008، ص189

الفرع الثاني**شروط ثبوت صفة شركة الأمن السيبراني**

لا يكفي لثبوت صفة شركة الأمن السيبراني بالمعنى القانوني الدقيق أن يدّعي الكيان هذه الصفة أو أن يمارس نشاطاً مجاوراً لها، بل يستلزم الأمر توافر جملة من الشروط التي حددتها التشريعات المقارنة في الأنظمة الثلاثة، وبتخلف أي منها لا يُعدّ الكيان شركة أمن سيبراني بالمعنى القانوني ولا تسري عليه الأحكام المقررة لهذه الشركات⁽¹⁾. وتكتسب هذه الشروط أهميتها العملية من كونها المعيار الحاسم في تحديد نطاق المسؤولية المدنية، إذ إن القاضي أو المحكم حين يواجه نزاعاً يتعلق بإخلال كيان بالتزاماته الأمنية يحتاج أولاً إلى التثبت من أن هذا الكيان هو فعلاً شركة أمن سيبراني حتى يُطبّق عليه الأحكام المناسبة. وتنقسم هذه الشروط إلى قسمين: شروط موضوعية تتعلق بجوهر النشاط ومضمونه، وشروط شكلية تتعلق بالاعتراف القانوني الرسمي والرقابة المؤسسية، ويتعذر الفصل بينهما في التطبيق العملي إذ يكمل كل منهما الآخر.

أولاً: الشروط الموضوعية

تتعلق الشروط الموضوعية بجوهر النشاط الذي يمارسه الكيان ومضمونه الفعلي، وهي شروط لا تثبت بمجرد التصريح أو الادعاء بل تثبت بالواقع الملموس للنشاط المُمارَس.

1- أن يكون النشاط الجوهري للكيان وقائياً أمنياً: يقوم هذا الشرط على أن الكيان لا تثبت له صفة شركة الأمن السيبراني إلا إذا كان نشاطه الجوهري منصباً على الوقاية من التهديدات السيبرانية وإدارة المخاطر الرقمية لا مجرد تشغيل الأنظمة أو صيانتها أو تطويرها. فإذا كان النشاط الجوهري للكيان تقنياً محضاً وكانت الحماية الأمنية فيه مجرد التزام ثانوي أو جانبي، فإن الصفة لا تثبت له وإن استخدم في نشاطه أدوات الأمن السيبراني ذاتها. ففي القانون الأمريكي، يتم تحديد مسؤولية مزودي الخدمات السيبرانية ووظائفهم من خلال المادة السادسة من قانون الأمن الداخلي الأمريكي التي حددت الغرض الأمني السيبراني بأنه غرض حماية نظام معلومات أو المعلومات المخزنة فيه أو المعالجة من خلاله أو المارة عبره من التهديدات أو الثغرات السيبرانية⁽²⁾، وكذلك عرّف ذات التشريع مزود الخدمة

(1) Alexandre Cruquenaire, op.cit, pp. 313-329.

(2) نص المادة (6) من قانون الأمن الداخلي الأمريكي .



بأنه كل كيان يقدم منتجات أو خدمات متعلقة بالحوسبة السحابية وفق المعايير المحددة من المعهد الوطني للمعايير والتكنولوجيا⁽¹⁾. ومن خلال مراجعة بنود التنفيذ التنظيمي لوكالة الأمن السيبراني وحماية البنية التحتية ومعهد المعايير والتكنولوجيا يتضح أن المفاهيم المستخدمة تشمل مزود خدمة الأمن السيبراني أو بائع الأمن السيبراني⁽²⁾، وهي مفاهيم تؤكد أن الغرض الوقائي الأمني هو المعيار الحاسم لا مجرد تقديم الخدمة التقنية.

وفي التشريع الفرنسي، نظم مرسوم 2015-350 المؤرخ في 27 آذار 2015 تأهيل مزودي خدمات الأمن السيبراني وربط صفتهم القانونية بكونهم جميع الأشخاص مقدمي الخدمات الذين يساهمون في أمن أنظمة المعلومات، وهو تعريف وظيفي يجعل طبيعة المساهمة في الأمن لا مجرد تقديم الخدمة التقنية هي الشرط الحاسم لثبوت الصفة. وفي اللائحة العراقية رقم 33 لسنة 2025، جاء تحديد هذا الشرط صريحاً في المادة (6/رابعاً/2) إذ اشترطت لثبوت صفة شركة الأمن السيبراني أن يشمل نشاطها حماية الأنظمة والشبكات من الهجمات السيبرانية وتقديم خدمات تحليل التهديدات ومراقبة الأنظمة.

ويتضح من خلال ما تقدم أن الأنظمة الثلاثة اتفقت على أن الشرط الأول والأساسي لثبوت الصفة هو طبيعة النشاط الوقائي الأمني، غير أنها تباينت في درجة الوضوح، إذ جاء هذا الشرط أكثر تحديداً في التشريع الفرنسي والعراقي اللذين ربطا الصفة القانونية بطبيعة الخدمة ذاتها، في حين بقي القانون الأمريكي وفيهاً لنهاجه الوظيفي الذي يحدد الغرض لا الكيان، وهو قصور مفاهيمي قد يُفضي إلى صعوبات في التطبيق القضائي عند النظر في دعاوى المسؤولية المدنية ضد هذه الشركات.

2- أن يمتلك الكيان القدرة الفنية الفعلية على الحماية: لا يكفي أن يكون النشاط المُعلن وقائياً أمنياً، بل يستلزم ثبوت الصفة أن يمتلك الكيان فعلاً القدرة التقنية على تقديم هذه الحماية بمستوى مقبول. فالكيان الذي يدّعي تقديم خدمات أمن سيبراني من دون أن يمتلك الأدوات والكفاءات الفنية اللازمة لا تثبت له هذه الصفة، لأن الصفة مرتبطة بالقدرة الفعلية لا بمجرد الادعاء. وتنقسم هذه القدرة الفنية إلى محورين متكاملين يقيسان مدى جاهزية الكيان على مستويين زمنيين مختلفين: المحور الأول يتمثل

(1) نص المادة (3) من قانون الأمن الداخلي الأمريكي .

(2) DEPARTMENT OF HOMELAND SECURITY, op.cit, p. 23644.



بالقدرة الوقائية قبل وقوع الحوادث، حيث يُقصد بذلك الالتزام الأساسي لشركة الأمن السيبراني بإنشاء بيئة رقمية مؤمنة قادرة على منع المخاطر قبل وقوعها⁽¹⁾.

وهذه القدرة لا تقتصر على الإجراءات العامة بل تشمل مجموعة من التدابير المتكاملة، في مقدمتها التشفير الذي يحوّل المعلومات إلى رموز غير مفهومة للغير⁽²⁾، بحيث يظل الوصول إليها محصوراً في من يمتلك المفاتيح المناسبة لفكها مما يضمن سرية البيانات أثناء التخزين والنقل⁽³⁾، وكذلك إدارة الهوية وصلاحيات الوصول حيث يتم التحقق من هوية المستخدمين وتحديد مستويات الوصول وفق مبدأ أقل امتياز ومراقبة جميع محاولات الدخول مما يضمن الالتزام بالمستويات المصرح بها

(1) د. عادل موسى عوض جاب الله، وسائل حماية الامن السيبراني (دراسة فقهية تأصيلية مقارنة بالنظم المعاصرة)، بحث منشور في المجلة العلمية في كلية الشريعة والقانون بأسبوط، جامعة الازهر، العدد 34، ج 3، 2022، ص 2243-2244.

(2) عرف القانون الفرنسي التشفير بأنه "كل فعل يؤدي إلى تحويل معلومات أو إشارات غير مقروءة للغير، أو يخرجها بطريقة معكوسة وذلك بالاستعانة بوسائل مادية أو برامج مصممة لذلك". تنظر المادة 17 من قانون رقم 659 / 96 الصادر بتاريخ 26 / 7 / 1996 .

(3) ويبرز التشفير بوظيفته الأمنية في حالتين أساسيتين: أولاً عند تخزين البيانات على الوسائط أو الخوادم، وثانياً أثناء نقلها عبر شبكات غير آمنة مثل شبكة الإنترنت، وفي كلا السياقين، لا يُعد التشفير حاجزاً مادياً أمام الوصول، بل يمثل حاجزاً معرفياً، يحجب المعنى لا المسار، ومن الناحية التقنية، تُحوّل المعلومات أثناء التشفير إلى رموز غير قابلة للفهم إلا باستخدام مفتاح خاص يُعرف بـ "مفتاح التشفير"، وهو ما يسمح فقط للمستقبل المصرح له باستخدام المفتاح المعاكس لإجراء عملية فك التشفير، واسترجاع النص الأصلي المقروء وعلى هذا النحو، يصبح التشفير علماً قائماً بذاته يعنى بتحويل البيانات الواضحة إلى معطيات سرية، ثم إعادة كشفها عند الحاجة من قبل أطراف محددة فقط. لتفاصيل أكثر يراجع: علي محمد دهب، التشفير وامن المعلومات، كلية دراسات الحاسوب والإحصاء - جامعة كردفان، بلا طبعة، بلا سنة نشر، ص 5. كذلك: د. نشوان احمد المجرم، التشفير وامنية المعلومات، ط2، دار الكتب اليمنية للطباعة والنشر والتوزيع، اليمن - صنعاء، 2018، ص 5. كذلك: د. حيدر فالح سليمان، مقدمة في الامن السيبراني، ط1، الذاكرة للنشر والتوزيع، العراق - بغداد، 2024، ص 60.

ويكشف أي نشاط مشبوه⁽¹⁾. وعلى مستوى التشريع الأمريكي يكون كل ذلك وفقاً لإطار العمل الذي يضعه المعهد الوطني الأمريكي للمعايير والتكنولوجيا⁽²⁾.

أما المحور الثاني، فيتمثل بالقدرة على التصدي والاستجابة بعد وقوع الحادث، حيث لا تكتمل صفة شركة الأمن السيبراني بالقدرة الوقائية وحدها، بل تستلزم أيضاً القدرة على التصدي للحادث بعد وقوعها والحد من أثارها. فالكيان الذي يعجز عن الاستجابة الفعالة للحادث السيبرانية لا يستوفي هذا الشرط مهما امتلك من أدوات وقائية. وتشمل هذه القدرة وضع خطط استجابة مسبقة تحدد الأدوار والمسؤوليات والإجراءات الموحدة لتقييم نوع الحادث وخطورته والجهات التي يجب إخطارها، ومن أبرز أدوات هذا المحور أنظمة كشف ومنع التسلل لرصد النشاط غير الطبيعي والاستجابة له، وكذلك الجدران النارية التي تمثل حاجزاً أمنياً بين الإنترنت والشبكات الداخلية وتتحكم في دخول وخروج البيانات وفق سياسات أمان محددة⁽³⁾.

⁽¹⁾ Guillaume Harry , IAM Gestion des identités et des accès: concepts et états de l'art, HAL, Archive Ouverte, 2013, p. 24 et suiv. NIST Special Publication 800-12 Rev. 1, An Introduction to Information Security, U.S. Department of Commerce, National Institute of Standards and Technology (June 2017), p. 62, available at: <https://doi.org/10.6028/NIST.SP.800-12r1>.

⁽²⁾ وفقاً لإطار العمل الذي أقره المعهد الوطني الأمريكي للمعايير والتكنولوجيا، يُعدّ إطار عمل تحسين البنية التحتية الحرجة للأمن السيبراني، الإصدار 1.1 وثيقة رسمية تهدف إلى وضع معايير فنية وقائية تُساعد على التحسين المسبق للأنظمة الرقمية. تشمل هذه المعايير إدارة الهوية والتحكم في الوصول، حماية البيانات والتشفير، استخدام التدابير الوقائية التقنية، والتدريب على الوعي الأمني، بالإضافة إلى سياسات النسخ الاحتياطي والمراقبة الدورية للأنظمة بهدف الحد من المخاطر السيبرانية قبل وقوعها. لتفاصيل أكثر يراجع:

المعهد الوطني الأمريكي للمعايير والتكنولوجيا، إطار عمل تحسين البنية التحتية الحرجة للأمن السيبراني، الإصدار 1.1، 2018، متاح عبر: [https://www.nist.gov/publications/framework-improving-critical-](https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11-arabic-translation)

[infrastructure-cybersecurity-version-11-arabic-translation](https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11-arabic-translation) . تاريخ آخر زيارة في 2026/6/14

⁽³⁾ وليد الزيدي، القرصنة على الانترنت والحاسوب، ط1، دار أسامة للنشر والتوزيع، الأردن - عمان، ص101. د. سعيداني نعيم، الحماية القانونية للحق في الخصوصية المعلوماتية (دراسة مقارنة)، ط1، المؤسسة الحديثة للكتاب، لبنان - بيروت، 2022، ص 440-441.



ومن المحورين اعلاه يتضح أن القدرة الفنية الفعلية شرط موضوعي حقيقي لثبوت الصفة لا مجرد التزام تشغيلي، إذ إن الكيان الذي يفترق إليها يبقى خارج نطاق مفهوم شركة الأمن السيبراني مهما ادّعى هذه الصفة أو حصل على ترخيص بممارستها.

ثانياً: الشروط الشكلية

تتعلق الشروط الشكلية بالاعتراف القانوني الرسمي الذي يمنح الكيان صفة شركة الأمن السيبراني أمام الجهات القانونية والقضائية، وهي شروط تكمل الشروط الموضوعية ولا تغني عنها، بمعنى أن توافر الشروط الموضوعية وحدها لا يكفي لثبوت الصفة ما لم تقترن بالاعتراف الرسمي والرقابة المؤسسية.

1- الترخيص من جهة ذات اختصاص أمني: لا تثبت للكيان صفة شركة الأمن السيبراني إلا بصور ترخيص رسمي من جهة ذات اختصاص أمني لا مجرد جهة تجارية عادية. وما يُميّز هذا الترخيص عن ترخيص أي نشاط تجاري آخر هو ارتباطه بمتطلبات تتصل بالأمن الوطني وحماية البنية التحتية الرقمية، وهو ما يجعله شرطاً موضوعياً في جوهره وإن بدا شكلياً في مظهره. يشمل ذلك التزام الشركة بتقديم المستندات القانونية المطلوبة وتسجيل المعلومات الأساسية واستيفاء شروط الهيئات المنظمة في الدول المقارنة، وهي في القانون الأمريكي المعايير التنظيمية ذات الصلة⁽¹⁾، وفي فرنسا الوكالة الوطنية لأمن نظم المعلومات ANSSI⁽²⁾، وفي العراق هيأت الإعلام والاتصالات⁽³⁾. وقد جاء هذا الترخيص في الأنظمة الثلاثة مقترناً بشروط فنية وأمنية صارمة تتجاوز متطلبات الترخيص

(1) كنا قد بينا أنه لا يوجد قانون موحد ينظم الأمن السيبراني في الولايات المتحدة الأمريكية، وبالتالي تخضع كل رخصة إلى نص القانون الذي ينظمها.

(2) اطلق المشرع الفرنسي على تلك الرخص تسمية الاعتماد، وهي سارية لمدة أقصاها ثلاث سنوات، حيث نصت المادة (14) من مرسوم 2015 على أن: "بناءً على تقرير التقييم، ونتائج التحقيق الإداري مع مقدم الخدمة، عند الاقتضاء، بموجب المادة 1-114 L. من قانون الأمن الداخلي، يُقرر المدير العام للوكالة الوطنية للأمن السيبراني في فرنسا (ANSSI) منح مقدم الخدمة الاعتماد من عدمه. عند منح الاعتماد، يُخطر المدير العام للوكالة مقدم الخدمة بقرار يُثبت امتثاله للقواعد المذكورة في الفقرة الأولى من المادة ١٠، ويُحدد، عند الاقتضاء، مستوى الاعتماد الذي حصل عليه. يُحدد القرار الخدمات المعتمدة، ويتضمن، عند الاقتضاء، الشروط والتحفظات. يُعتبر الاعتماد ساريًا لمدة أقصاها ثلاث سنوات، ويمكن تجديده بنفس الشروط".

(3) نظم المشرع العراقي عبر اللائحة منح التراخيص تحديداً في الفصل الثاني من اللائحة.

التجاري العادي، إذ اشترط المشرع الفرنسي على سبيل المثال اعتماداً سارياً لمدة أقصاها ثلاث سنوات يُجَدّد بنفس الشروط وربطه بنتائج التحقيق الإداري مع مقدم الخدمة.

ويكشف هذا الشرط عن فارق جوهري بين الأنظمة الثلاثة، إذ يتسم النظام الفرنسي بأكبر قدر من التفصيل من خلال نظام التأهيل والاعتماد الذي تشرف عليه ANSSI، في حين تتعدد جهات الترخيص في النظام الأمريكي بتعدد القطاعات مما يُعقّد تطبيق هذا الشرط، أما النظام العراقي فلا يزال في طور بناء منظومته المؤسسية للترخيص مما يعني أن تطبيق هذا الشرط يستند حتى الآن إلى الإطار التنظيمي الذي وضعته اللائحة رقم 33 لسنة 2025 دون أن تتوفر له آليات تطبيق مكتملة.

2- الخضوع للرقابة التنظيمية المستمرة: لا تكتمل صفة شركة الأمن السيبراني بالحصول على الترخيص وحده، بل تستلزم الخضوع لرقابة مؤسسية مستمرة من جهة ذات اختصاص أمني. فالكيان الذي يمارس نشاط الأمن السيبراني بمعزل عن أي رقابة تنظيمية متخصصة لا تثبت له هذه الصفة بصورة مستديمة، لأن الرقابة المستمرة هي الضمان الحقيقي لبقاء الكيان مستوفياً للشروط الموضوعية التي تثبت له الصفة بموجبها. ويتجلى هذا الشرط في التشريعات المقارنة من خلال متطلبات التقارير الدورية والتقييمات الميدانية والاعتماد المستمر كما في المواد 7-10 من مرسوم 350-2015 الفرنسي المتعلق بتأهيل منتجات الأمن وشروط الخدمة، والمواد 5-7 من اللائحة العراقية رقم 33 لعام 2025. وبالعودة إلى اللائحة العامة لحماية البيانات الأوروبية⁽¹⁾ وقوانين مثل قانون خصوصية المستهلك في كاليفورنيا⁽²⁾، تُعدّ البيانات الشخصية من أبرز التزامات شركات الأمن السيبراني في إطار هذه الرقابة، إذ تلتزم الشركات بمبادئ أساسية أبرزها الشفافية والعدالة في استخدام البيانات وتحديد الغرض من

(1) نصت المادة (4) من اللائحة العامة لحماية البيانات الأوروبية (GDPR) على أن البيانات الشخصية هي: "أي معلومات تتعلق بشخص طبيعي محدد أو قابل للتحديد والشخص الطبيعي الذي يمكن تحديده هو الشخص الذي يمكن تحديده بشكل مباشر أو غير مباشر من قبل بعض الأشياء مثل الاسم أو رقم التعريف أو بيانات الموقع أو واحد أو أكثر من العوامل المحددة للفيزيائية الفسيولوجية، الهوية الجينية أو العقلية أو الاقتصادية أو الثقافية أو الاجتماعية لهذا الشخص الطبيعي".

ينظر كذلك: Michel Séjean (dir.), Code de la Cybersécurité Annoté & commenté, 2e éd., Dalloz, Paris, 2024, p. 462.

(2) قانون خصوصية المستهلك في كاليفورنيا يرمز له بـ (CCPA).

California Consumer Privacy Act (CCPA) – Summary and Guidance, Jones Day, 2020, p. 5.

جمعها وتقليل حجمها إلى الحد الضروري ودقتها وتمكين الأفراد من تصحيحها وتحديد فترة التخزين وحذف البيانات بعد انتهائها وضمان السلامة والسرية والإبلاغ عن الحوادث⁽¹⁾.

ولم يعد التعامل مع الحوادث السيبرانية يقتصر على الجوانب الفنية، بل أصبح يُشكّل التزاماً تنظيمياً يقع ضمن نطاق مسؤوليات شركات الأمن السيبراني في إطار الرقابة المستمرة، إذ يقع على عاتق هذه الشركات واجبات تتعلق بالإبلاغ الفوري والدقيق عن الحوادث التي تمس أمن البيانات أو تؤثر في استمرارية الخدمات⁽²⁾. ويُعدّ هذا الشرط من المظاهر الرئيسية لمبدأ الشفافية والمساءلة المؤسسية، ويقوم على تحقيق التوازن بين واجب حماية المعلومات من جهة وحق الجهات المعنية سواء كانت سلطات رقابية أو أطرافاً متضررة في المعرفة والإخطار من جهة أخرى⁽³⁾.

ويُلاحظ أن هذا الشرط هو الأكثر ارتباطاً بطبيعة شركات الأمن السيبراني ذات الطابع الخاص المتصل بالنظام العام الرقمي، وهو ما سيأتي تفصيله في سياق خصائص هذه الشركات. غير أنه يكفي هنا التأكيد على أن الكيان الذي يُخلّ بهذا الشرط ويتهرب من الرقابة التنظيمية المستمرة لا يحتفظ بصفة شركة الأمن السيبراني بصورة مستديمة، وتترتب على ذلك آثار قانونية مباشرة فيما يتعلق بمسؤوليته المدنية⁽⁴⁾.

(1) ينظر في تفاصيل تلك المبادئ كل من: د. محمد احمد سلامة مشعل، الحق في محو البيانات الشخصية (دراسة تحليلية في ضوء لائحة حماية البيانات بالاتحاد الأوروبي GDPR واحكام المحاكم الاوربية)، بلا سنة نشر، ص 37. كذلك: د. امل شافعي و د. ام السعد شافعي، التأسيس للحق في حماية البيانات الشخصية كحق مستقل عن الحق في الخصوصية في تشريع الاتحاد الأوروبي، جامعة الحاج لخزري - باتنة 1، بحث مقدم ال مجلة الباحث القانوني، المجلد 01، العدد 02، 2022، ص 6. كذلك: د. هبة رمضان رجب، الحماية القانونية للبيانات الشخصية في عصر التكنولوجيا الرقمية، بلا عدد، بلا سنة، ص 18. كذلك: سلطان فياض محمد السكر، جريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية في التشريع الأردني، رسالة ماجستير مقدمة لكلية الحقوق - جامعة الشرق الأوسط، 2022، ص 25.

(2) Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive), Article 23.

(3) Directive (UE) 2022/2555, art. 23, in Code de la cybersécurité 2024 annoté et commenté, p. 699

(4) PRECEDENTIAL , UNITED STATES COURT OF APPEALS , FOR THE THIRD CIRCUIT, op.cit ,p.12.



يتضح مما سبق أن ثبوت صفة شركة الأمن السيبراني يقوم على منظومة متكاملة من الشروط الموضوعية والشكلية التي تتكامل فيما بينها ولا يُغني توافر بعضها عن بعضها الآخر. فالشروط الموضوعية تضمن أن يكون النشاط الجوهري للكيان وقائياً أمنياً وأن يمتلك القدرة الفنية الفعلية على الحماية، في حين تضمن الشروط الشكلية الاعتراف القانوني الرسمي بهذه الصفة والرقابة المستمرة للتحقق من استمرار استيفائها. والكيان الذي لا يستوفي هذه الشروط مجتمعة لا تثبت له صفة شركة الأمن السيبراني بالمعنى القانوني، وبالتالي لا تسري عليه الأحكام المقررة لهذه الشركات في مجال المسؤولية المدنية التي ستأتي دراستها تفصيلاً في المطالب اللاحقة.

المطلب الثاني

خصائص شركات الأمن السيبراني

يُعدّ الأمن السيبراني في الأصل نشاطاً ذا طابع سيادي يرتبط مباشرةً بحماية الأمن الوطني والبنى التحتية المعلوماتية للدولة، غير أنّ التطور المتسارع للتقنيات الرقمية، واتساع نطاق المخاطر السيبرانية وتشعبها، أوجد واقع جديد أصبحت معه قدرات الدولة، منفردة، غير كافية لتغطية جميع جوانب الحماية السيبرانية. ومن ثمّ اتجهت التشريعات المقارنة، ومن بينها التشريع العراقي، إلى السماح للقطاع الخاص بممارسة بعض وظائف الحماية الرقمية، وإن تحديد المفهوم القانوني لشركات الأمن السيبراني لا يكتمل بمجرد الوقوف على تعريفها، فإن دراسة خصائصها القانونية تُعدّ أمراً لازماً لفهم طبيعة نشاطها وحدود مسؤوليتها. وتكتسب هذه الدراسة أهميتها من كون هذه الشركات تمارس نشاطاً يتقاطع مع متطلبات الأمن العام، وفي الوقت ذاته تخضع لأحكام القانون الخاص. وانطلاقاً من ذلك سنقسم المطلب على فرعين، الأول نبحث فيه الخصائص الداعمة للطابع السيادي، والثاني الخصائص المؤكدة للطابع التجاري.



الفرع الأول

خصائص داعمة للطابع السيادي للأمن السيبراني

أصبح الأمن السيبراني في العصر المعاصر أحد الأبعاد الأساسية للأمن الوطني لأي دولة، ولا يمكن فصله عن منظومة الأمن الوطني الشاملة. إذ تفرض التطورات الرقمية السريعة والتهديدات السيبرانية المتزايدة أن تبني الدول استراتيجية وطنية للأمن السيبراني تتوازن بين متطلبات حماية الأمن الوطني وضمان حقوق المواطنين في الوصول إلى المعلومات ضمن مجتمع مفتوح. وهذه الاستراتيجية، لضمان فعاليتها، لا يمكن أن تقتصر على الجهات الحكومية فقط، بل يجب أن تشمل جميع أصحاب المصلحة: الأجهزة الأمنية، القضاء، الجهات الحكومية، شركات الأمن السيبراني، المسؤولين عن البنية التحتية الحيوية، والمؤسسات التعليمية، بما يضمن تنسيقاً وتعاوناً فعالاً بين هذه الأطراف⁽¹⁾. وفي هذا الإطار، تصبح شركات الأمن السيبراني أدوات محورية في تنفيذ السياسة السيادية الرقمية للدولة، إذ تمارس نشاطاً يمس المصلحة الوطنية ويحاكي وظائف الدولة في حماية البنى التحتية المعلوماتية الحيوية والبيانات الحساسة. مثلما أن خضوع هذه الشركات لنظم الترخيص والرقابة، وارتباط نشاطها بالمصلحة العامة، يعزز الطابع السيادي لأعمالها، مع الحفاظ على طبيعتها القانونية الخاصة.

وبناءً على ذلك، يمكن تحديد ثلاث خصائص رئيسية لشركات الأمن السيبراني تُبرز هذا الطابع السيادي، يمكن بيانها على النحو الآتي:

أولاً: شركات الأمن السيبراني تمارس نشاط ذات طابع سيادي

تتميز شركات الأمن السيبراني بأن نشاطها لا يقتصر على تقديم خدمات تقنية أو تجارية تقليدية، بل يتضمن مهام محورية تتقاطع مع وظائف الدولة السيادية في حماية الأمن الوطني الرقمي، إذ يشمل نشاط هذه الشركات حماية الأنظمة والشبكات من الهجمات السيبرانية، وتحليل التهديدات، ومراقبة الأنظمة لضمان استقرارها وسلامتها⁽²⁾، فالتبيعة الأساسية لنشاط هذه الشركات يؤكد أن مهامها ليست

(1) مصطفى إبراهيم سلمان الشمري، الأمن السيبراني واثره في الامن الوطني العراقي، مجلة العلوم القانونية والسياسية، كلية القانون والعلوم السياسية، جامعة ديالى، العدد 1، مجلد 10، 2021، ص 162-163.

(2) وقد أقر المشرع العراقي هذا الواقع في اللائحة 33 لسنة 2025، المادة 4/6، الفقرة الثانية من الفقرة الثانية، التي نصّت صراحة على أن شركات الأمن السيبراني تقدم خدمات حماية الأنظمة والشبكات من الهجمات السيبرانية، وتشمل تقديم خدمات تحليل التهديدات ومراقبة الأنظمة.

مجرد خدمات تجارية عادية، بل وظائف ترتبط بحماية مصالح الدولة الوطنية، ويستند هذا الطابع السيادي في جوهره إلى أن الأمن الوطني بموجب المادة (110/ثانياً) من الدستور العراقي اختصاص حصري للسلطة الاتحادية، مما يعني أن أي كيان خاص يمارس نشاطاً في هذا المجال إنما يمارسه بتفويض من الدولة لا بحق أصيل⁽¹⁾. وهذا التفويض هو ما يُضفي على نشاط شركات الأمن السيبراني طابعاً سيادياً جزئياً يُميزه عن سائر الأنشطة التجارية الخاصة، ويُبرر إخضاعه لنظام قانوني خاص يتجاوز قواعد القانون التجاري العادي. ولا يختلف الأمر في النظامين الأمريكي والفرنسي، إذ يقوم كلاهما على مبدأ أن الأمن السيبراني الوطني مسؤولية سيادية تشارك فيها الشركات الخاصة بموجب تفويض تنظيمي لا بصلاحية مستقلة.

إن ما يميز هذا النشاط ويضفي عليه الطابع السيادي هو ارتباطه المباشر بالمصلحة العامة والأمن الوطني. فالبيانات التي تتعامل معها هذه الشركات في الغالب تكون حساسة وتتعلق بالمواطنين والبنى التحتية الحيوية للدولة، غير أن هذا الوصف يطرح تساؤلاً قانونياً جوهرياً مفاده: هل يكفي اتصال النشاط بالأمن الوطني لإضفاء الطابع السيادي على الكيان القائم به؟ والجواب أن السمة التي تُضفي على هذا النشاط الطابع السيادي ليست مجرد ارتباطه بالمصلحة العامة، فكثير من الأنشطة الخاصة ترتبط بالمصلحة العامة دون أن تكتسب طابعاً سيادياً، ما يُميز شركات الأمن السيبراني هو أنها تُمارس صلاحيات تشبه الصلاحيات السيادية في جوهرها كالرقابة على الأنظمة الحيوية وتحليل التهديدات وإدارة الاستجابة للأزمات الرقمية، لكنها تمارسها بتفويض من الدولة لا بحق أصيل، وهذا التفويض هو ما يُبرر خضوعها لنظام ترخيص ورقابة يتجاوز ما هو مقرر للشركات التجارية العادية⁽²⁾.

فضلاً على ذلك، فإن طبيعة المهام التي تقوم بها هذه الشركات تعكس دوراً سيادياً جزئياً، إذ تسهم بشكل مباشر في تنفيذ السياسات الأمنية للدولة على مستوى الوقاية والاستجابة للتهديدات الرقمية.

(1) نصت الفقرة الثانية من المادة (110) من دستور جمهورية العراق لعام 2005 على أن: "وضع سياسة الامن الوطني وتنفيذها، بما في ذلك انشاء قوات مسلحة وادارتها لتأمين حماية وضمان امن حدود العراق، والدفاع عنه".

(2) تعتمد المجتمعات الحديثة بشكل فعال على شبكات الحاسوب التي تسيطر عليها شركات خاصة. في الولايات المتحدة وحدها، تمتلك شركات خاصة ما يقرب من ٨٥٪ من البنية التحتية الرئيسية - أنظمة النقل، وشبكات الاتصالات، والشبكات المالية، وشبكات الكهرباء.

وعلى الرغم من كونها كيانات خاصة، فإن تدخلها في مجال يحمي الأمن الوطني ويعزز استقرار الفضاء السيبراني يجعل نشاطها أقرب إلى وظيفة الدولة من كونه نشاط تجاري محض. ويمكن القول إن هذا الطابع السيادي يتجلى بوضوح في الاعتماد القانوني على اللائحة العراقية، وكذلك في التشريعات المقارنة في فرنسا وأمريكا، حيث تفرض القوانين واللوائح الالتزام بمعايير محددة لضمان أن يكون عمل الشركات متسقاً مع حماية الأمن الوطني والبنى التحتية الحيوية⁽¹⁾.

إن استقرار هذه الطبيعة القانونية والوظيفية للنشاط يجعل من الواضح أن شركات الأمن السيبراني ليست مجرد فاعل اقتصادي يقدم خدمات تقنية، بل هي كيانات تؤدي مهام حيوية تقترب من الوظائف السيادية للدولة، وتحمل مسؤوليات تتجاوز حدود السوق التجاري التقليدي، بما يعزز الطابع السيادي لنشاطها ويثبت موقعها كعنصر محوري ضمن استراتيجية الدولة للأمن السيبراني، فبينما تُقدم الحكومات السلطة التنظيمية، والمعرفة الاستخباراتية، والنفوذ الدبلوماسي، تُؤمّن الشركات الخاصة القدرة التقنية والابتكار وملكية الأصول الرئيسية. ويؤدي هذا التكامل بين دور الدولة والقطاع الخاص إلى تعزيز قدرة النظام القانوني على مواجهة المخاطر السيبرانية بفعالية، فعلى سبيل المثال يُوحّد التعاون الدفاعي السيبراني المشترك للولايات المتحدة (JCDC)، الذي ترأسه وكالة الأمن السيبراني وأمن البنية التحتية (CISA)، الوكالات الفيدرالية وشركات التكنولوجيا الرائدة لمواجهة الهجمات السيبرانية بفعالية⁽²⁾. ويُمثّل هذا دليلاً على طبيعة العمل الذي تمارسه الشركات محل البحث.

وعلى هذا الأساس يتضح أن الطابع السيادي لشركات الأمن السيبراني ليس وصفاً مجازياً بل حقيقة قانونية تترتب عليها آثار جوهرية، أبرزها أن هذه الشركات لا تتمتع بحرية كاملة في ممارسة نشاطها كما هو الحال في الشركات التجارية العادية، بل تخضع لقيود تفرضها طبيعة التفويض السيادي الذي تستمد منه صلاحيتها. بيد أن هذا الطابع السيادي لا يُخرج الشركة من نطاق القانون الخاص كما سيأتي بيانه، بل يُشكّل خصيصة مُقيّدة لحريتها التعاقدية دون أن ينقلها إلى دائرة الأشخاص المعنوية العامة.

⁽¹⁾ في القانون الفرنسي، تُظهر سياسة ANSSI (الوكالة الوطنية لأمن الأنظمة المعلوماتية) أن أمن الفضاء السيبراني يُعالج عبر شراكة فعلية بين الدولة والقطاع الخاص، حيث تعمل ANSSI مع شركات خاصة ضمن شراكة عمومية-خاصة وفقاً للمعايير القانونية المقررة لتعزيز قدرة فرنسا على حماية السيادة الرقمية.

ANSSI, "ANSSI – A driving force of the European Public-Private Partnership on cybersecurity", 03 août 2016, ANSSI Disponible .

⁽²⁾ Mohit Sharma, Sajud E., Naranjan Goklani, Krishna Chaubey, op.cit, p.975.

ثانياً: ازدواجية مصدر الالتزام بين الإرادة التعاقدية والقانون

تتميز شركات الأمن السيبراني عن سائر مقدمي الخدمات الرقمية بأن التزاماتها لا تستمد مصدرها من الإرادة التعاقدية وحدها، بل تتشكل من مصدرين متميزين يعملان في آن واحد، إرادة تعاقدية حرة تُحدد نطاق الخدمة وشروطها بين الشركة وعميلها، والتزامات مفروضة بحكم القانون تتصل بالنظام العام الرقمي وتسري بصرف النظر عما اتفق عليه. وهذه الازدواجية ليست مجرد خصوصية تنظيمية بل هي خاصية جوهرية تنعكس مباشرة على تحديد طبيعة المسؤولية ونطاقها. ويتجلى المصدر القانوني للالتزام بوضوح في إلزام هذه الشركات بتبادل المعلومات والإبلاغ عن الحوادث مع الجهات الحكومية المختصة حتى حين لا يشترط العقد ذلك، وهو ما كرّسه المشرع الأوروبي صراحةً في توجيه NIS2 الصادر عام 2022، الذي أوجب على مزودي خدمات الأمن السيبراني الإبلاغ الفوري عن الحوادث الجسيمة للسلطات الوطنية المختصة⁽¹⁾. وفي الاتجاه ذاته، أكدت محكمة الاستئناف الأمريكية للدائرة الثالثة في قضية وندهام أن الجهات المنوط بها إدارة البيانات وحمايتها تخضع للرقابة التنظيمية للهيئات الحكومية المختصة⁽²⁾، مما يكشف عن انخراط الدولة في تشكيل مضمون الالتزام الخاص بهذه الشركات تجاوزاً لإطار التعاقد.

وبهذا يتحول الالتزام من أداء عقدي يحكمه مبدأ نسبية العقد إلى التزام ذي أبعاد عامة تمس الأمن الوطني الرقمي، فالشركة في مواجهة عميلها ملتزمة بما اتفق عليه، غير أنها في مواجهة المجتمع والدولة تضطلع بوظيفة أوسع يحددها القانون لا الإرادة الفردية. وقد أكد الفقه العراقي أن ارتباط الأمن السيبراني بالأمن الوطني يُفرز التزامات تتجاوز النطاق التعاقدية⁽³⁾، وهو ما أقره المشرع العراقي في اللائحة 33 لسنة 2025 باشتراط التنسيق مع الجهات الرسمية عند التعامل مع البنى التحتية الحيوية وتكمن الأهمية القانونية لهذه الخاصية في أنها تُحدد مصدر الالتزام وطبيعته تحديداً دقيقاً، إذ حين تُخفق الشركة في الإبلاغ أو التنسيق لا يكون الإخلال تعاقدياً فحسب، بل مخالفةً للالتزام نشأ بحكم القانون

(1) Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive), Article 23.

(2) PRECEDENTIAL, UNITED STATES COURT OF APPEALS, FOR THE THIRD CIRCUIT, op.cit, p.12.

(3) مصطفى إبراهيم سلمان الشمري، مصدر سابق، ص162.

مستقلاً عن الإرادة، مما يُرتّب أثراً مباشراً على تكييف المسؤولية المدنية وتحديد نطاقها وهو ما سنتناوله الفصول اللاحقة من هذا البحث.

الفرع الثاني

خصائص مؤكدة للطابع التجاري الخاص

إن فكرة إدماج شركات الأمن السيبراني ضمن شبكة من الفاعلين الذين يجمعون بين بعد أمني من جهة، وتجاري خاص من جهة أخرى، تستلزم إعادة نظر في الطبيعة القانونية لهذه الكيانات. فعلى الرغم من أن هذه الشركات قد تؤدي وظائف تتقاطع مع الأمن العام، فإن طبيعتها عملها وتنظيمها القانوني غالباً ما يضعانها ضمن سوق الخدمات الخاصة أي أنها تخضع لمنطق العرض والطلب، وتتعاقد مع عملائها وفق عقود تجارية-مدنية، وتعمل في إطار تحقيق الربح من خلال ابتكار وتقديم منتجات وخدمات تقنية. وعليه، فإن إبراز الخصائص التي تؤكد الطابع التجاري الخاص لهذه الشركات يسهم في تحليل طبيعتها التزاماتها القانونية، لاسيما فيما يتعلق بمسؤوليتها المدنية عن العقود التي تعقدها مع الافراد او الحكومات على حد سواء، ويمكن بيان تلك الخصائص على النحو التالي:

أولاً: خضوع شركات الأمن السيبراني لآلية السوق وقواعد المنافسة بوصفها

مشروعاً تجارياً

يُعدّ خضوع شركات الأمن السيبراني لآلية السوق وقواعد المنافسة الدليل القانوني الأقوى على أن الطابع السيادي لنشاطها لا يُخرجها من دائرة القانون الخاص، إذ إن الكيان الذي يتنافس في السوق ويسعى للربح ويخضع لقواعد مكافحة الاحتكار لا يمكن وصفه بالشخص المعنوي العام مهما بلغت حساسية نشاطه. وهذا الخضوع للسوق ليس مجرد وصف اقتصادي بل هو معيار قانوني حاسم يُحدد الإطار الذي تعمل فيه الشركة ويرسم حدود مسؤوليتها المدنية تجاه عملائها ومنافسيها والمجتمع، وإن كانت هذه الشركات – على الرغم من ارتباط نشاطها بمصالح عليا تمس الأمن الوطني – تظل في بنيتها القانونية أشخاصاً معنوية خاصة تعمل ضمن الاقتصاد الحر وتسعى لتحقيق الربح من خلال تقديم خدماتها إلى العملاء⁽¹⁾. فالقاعدة في التنظيم القانوني للأنشطة الاقتصادية في التشريعات الحديثة، ومنها

⁽¹⁾ Kristen E. Eichensehr, Public-Private Cybersecurity, Texas Law Review, Vol. 95:467, 2017, p.467.



التشريع العراقي والتشريع الفرنسي والتشريع الأمريكي، أن الشركات الخاصة، مهما بلغت حساسية خدماتها، تخضع لمنطق العرض والطلب وتتنافس في تقديم خدمات ذات قيمة مضافة بهدف كسب العملاء. وهذا الانخراط في البيئة السوقية يجعل نشاطها أقرب ما يكون إلى الأنشطة المهنية التجارية، التي تعتمد على الأداء، الجودة، السمعة، الأسعار، والابتكار التقني كعوامل تنافسية رئيسة، لأنه عندما تنظم الشركات الأمنية السيبرانية وجودها ضمن سوق خاص، فإن دخولها إلى هذا السوق واستمرارها فيه لا يعتمد على تفويض دائم من الدولة بقدر ما يعتمد على مدى قدرتها التنافسية، سواء من جهة الكفاءة التقنية أو القدرة على تقديم خدمة بجودة مناسبة وسعر منافس، حيث يتسم سوق خدمات الأمن السيبراني بخدمات قابلة للتمييز، فتتنافس الشركات على مستوى الجودة، زمن الاستجابة، مستوى الشفافية، وشروط سرية المعلومات، وهذا يكشف عن تناقض ظاهري في طبيعة هذه الشركات يُعدّ في حقيقته توازناً قانونياً دقيقاً: فهي من جهة تستمد صلاحيتها من تفويض سيادي، ومن جهة أخرى تستمر في السوق بقدرتها التنافسية لا بالامتياز الإداري، مما يجعل تقييمها مسألة سوقية تقنية لا مجرد قرار إداري تمنحه الدولة. وهذا التوازن هو ما يجعلها كياناً قانونياً فريداً يحمل بُعداً سيادياً في وظيفته لكنه يظل خاضعاً لمنطق السوق في وجوده واستمراره⁽¹⁾.

وفي النظام الفرنسي، مثلاً، حيث يُرسي المشرع الفرنسي ضمن المرسوم المتعلق بتأهيل منتجات لعام 2015 آلية تأهيل لمزوّد خدمات الثقة ومنتجات الأمن السيبراني، حيث يُطلب من مقدّم الخدمة إثبات مطابقة خدماته أو منتجاته لمعايير أمنية معيّنة قبل حصوله على التأهيل، لكن هذا التأهيل لا يعني تحويل هذه الكيانات إلى هيكل حكومية أو إلى هيئات عامة ذات صفة إدارية خالصة؛ بل تبقى في جوهرها شركات خاصة تخضع بعد حصولها على التأهيل إلى مبدأ حرية المنافسة في سوق الخدمات الأمنية، مع إمكانية دخول شركات جديدة، تقدم عروض مختلفة، التنافس على الجودة أو السعر، وتقديم خدمات متنوعة بحسب الحاجة⁽²⁾.

(1) Kristen E. Eichensehr, op.cit, p.467.

(2) فقد نصّت المادة (2) من المرسوم الفرنسي رقم 384 الصادر سنة 2018 على أن: "يُقدّم طلب تأهيل منتج أمني إلى الوكالة الوطنية للأمن السيبراني في فرنسا (ANSSI). تُتيح الوكالة للجمهور إلكترونياً قائمة الوثائق المطلوب إرفاقها بالطلب، والتي تتضمن وصفاً تفصيلياً للمنتج ووظائفه الأمنية، بالإضافة إلى الأهداف الأمنية التي يسعى إلى تحقيقها.

بمجرد اكتمال الطلب، تتحقق الوكالة، بناءً على الوثائق المُقدّمة، مما يلي:

1. تحديد أهداف أمن المنتج بما يتناسب مع التهديدات التي تُهدّد أمن أنظمة المعلومات؛
2. توافق وظائف أمن المنتج مع الأهداف الأمنية التي يسعى إلى تحقيقها؛
3. توافر الأجهزة والبرامج، وشيفرة المصدر الخاصة بها، والوثائق اللازمة لتقييم وظائف أمن المنتج دون قيود....".

وتأسيساً على ذلك، فإن شركات الأمن السيبراني تخضع ابتداءً لمبدأ حرية ممارسة النشاط التجاري، المنصوص عليه في التشريعات المقارنة، ففي الولايات المتحدة، تعمل شركات الأمن السيبراني ضمن سوق عالي الديناميكية يخضع لقواعد قانون شيرمان Sherman Act⁽¹⁾، وقانون كلايتون Clayton Act⁽²⁾، حيث تخضع صفقات الاندماج والاستحواذ لرقابة دقيقة من قبل هيئة التجارة الاتحادية (FTC) خشية خلق احتكارات رقمية قد تمس شريان الأمن المعلوماتي⁽³⁾.

وفي فرنسا، تُعد الشركات الأمنية الرقمية جزءاً من القطاع التنافسي، وتخضع لمقتضيات قانون التجارة الفرنسي بما فيه من أحكام تتعلق بالمنافسة وتنظيم السوق⁽⁴⁾، إلى جانب خضوعها لرقابة هيئة

(1) وتسمى بقواعد منع الاحتكار وهو حجر الأساس في تنظيم المنافسة في السوق الأمريكي، ويُطبق على جميع المشروعات التجارية بما فيها الشركات العاملة في قطاع الأمن السيبراني، من خلال تجريم الاتفاقات المقيدة للتجارة ومنع إساءة استغلال القوة السوقية، القانون متاح عبر موقع (GPO) U.S. Government Publishing Office على الرابط:

<https://www.govinfo.gov/content/pkg/USCODE-2022-title15/html/USCODE-2022-title15-chap1.htm>. تاريخ اخر زيارة في 2026/6/14

(2) وهو قانون مكمل لقانون شيرمان، ويختص بتنظيم الممارسات التجارية التي قد تؤدي إلى الإضرار بالمنافسة، لا سيما صفقات الاندماج والاستحواذ التي تُجرىها الشركات الكبرى والتي قد تنتج عنها قوة سوقية احتكارية أو تقليل ملحوظ للخيار التنافسي. يمنح القانون سلطات رقابية واضحة لكل من لجنة التجارة الفيدرالية Federal Trade Commission (FTC) ووزارة العدل Department of Justice (DOJ) لمنع أو مراجعة تلك العمليات، القانون منشور عبر موقع (GPO) U.S. Government Publishing Office على الرابط:

<https://www.govinfo.gov/content/pkg/USCODE-2022-title15/html/USCODE-2022-title15-chap1-subchapII.htm>. تاريخ اخر زيارة في 2026/6/14

(3) مراجعة الاندماج (merger review) تشكل جزءاً جوهرياً من نظام مكافحة الاحتكار في الولايات المتحدة، حيث تقوم الهيئات المختصة مثل (FTC) Federal Trade Commission و (DOJ) U.S. Department of Justice بتقييم الصفقات الكبرى للتأكد من عدم تقليص المنافسة أو خلق احتكارات محتملة، لا سيما في الأسواق التقنية والرقمية التي تشمل شركات الأمن السيبراني. كما أن التعديلات الأخيرة على Merger Guidelines منذ 2022 تهدف إلى ضبط الصفقات بما يتوافق مع واقع السوق الحديث وتعزيز المنافسة العادلة. لمزيد من التفاصيل يراجع:

Rachel Brandenburger & Jill Ottenberg, Looking backwards to move forwards: The role of history in current US antitrust enforcement, Journal of Antitrust Enforcement, vol. 11, no. 2 (July 2023), pp. 162–167. DOI: 10.1093/jaenfo/jnad007.

(4) نصت المادة 2-420 من قانون التجارة الفرنسي الصادر 2001 على أنه و" بموجب الشروط المنصوص عليها في المادة 1-420 L، يُحظر استغلال أي شركة أو مجموعة شركات لوضع مهيمن في السوق الداخلية أو جزء كبير منه. وقد يشمل هذا الاستغلال، على وجه الخصوص، رفض البيع، أو البيع المشروط، أو شروط البيع التمييزية، بالإضافة إلى إنهاء علاقات العمل القائمة لمجرد رفض الشريك الخضوع لشروط تجارية غير مبررة. علاوة على ذلك، يُحظر

المنافسة الفرنسية، لا سيما عندما يتعلق الأمر بمنع الاتفاقات المقيّدة للمنافسة أو إساءة استغلال الوضع المهيمن في أي قطاع بما في ذلك قطاع الأمن الرقمي⁽¹⁾، وهو قطاع يشهد توسع واضح وتفاوت كبير في قدرات الشركات.

أما في العراق، فبالرغم من ندرة التنظيمات الخاصة بالمنافسة الرقمية، فإن شركات الأمن السيبراني بصفتها شركات خاصة تخضع في المبدأ لأحكام قانون الشركات رقم 21 لسنة 1997 المعدل، ولأحكام قانون التجارة فيما يتعلق بوجوب التسجيل، ومسك الدفاتر التجارية، وضوابط المنافسة العامة⁽²⁾، فضلاً عن خضوعها – شأنها شأن بقية المشاريع التجارية – لأحكام قانون حماية المستهلك رقم 1 لسنة 2010 حين يتعلق الأمر بالشفافية في تقديم الخدمات وما يرتبط به من إعلانات وممارسات تجارية⁽³⁾.

وعلى هذا الأساس، تندرج شركات الأمن السيبراني ضمن نموذج الشركات الخاصة التي تقدم خدمات رقمية، وتتنافس في السوق وفق معايير متعددة تتعلق بجودة الخدمات، الكفاءة التقنية، مستوى الحماية، زمن الاستجابة، وامثالها للمعايير القانونية والفنية. وعلى الرغم من حساسية طبيعة نشاطها وارتباطه بمصالح الأمن الوطني، فإن هذه الشركات تخضع لمبادئ المنافسة وقواعد السوق نفسها التي تُنظّم عمل أي نشاط تجاري، بما يضمن حماية المستهلك، تعزيز الابتكار، والحفاظ على ديناميكية السوق. فالتنافسية في هذا القطاع لا تعتمد على الأسعار وحدها، بل تشمل التميّز الفني والخدمات المصممة وفق احتياجات العملاء، وتعدد نماذج التعاقد وتقديم حلول متكاملة لاستجابة الحوادث وحماية البيانات، بما يتيح للشركات الفرصة للبقاء ضمن السوق مع الالتزام بالقواعد القانونية ومنع الممارسات الاحتكارية. ومن ثم، يصبح خضوع شركات الأمن السيبراني لقواعد المنافسة أمراً جوهرياً لضمان نزاهة السوق، وتأكيد أن النشاط التجاري لهذه الشركات يتم وفق إطار قانوني متوازن يجمع بين حماية

استغلال أي شركة أو مجموعة شركات لحالة التبعية الاقتصادية التي يجد العميل أو المورد نفسه فيها تجاهها بقدر ما قد يؤثر ذلك على سير المنافسة أو هيكلها. وقد يشمل هذا الاستغلال، على وجه الخصوص، رفض البيع، أو البيع المشروط، أو شروط البيع التمييزية، بالإضافة إلى إنهاء علاقات العمل القائمة لمجرد رفض الشريك الخضوع لشروط تجارية غير مبررة...".

القانون متاح على الرابط: <https://www.wipo.int/wipolex/en/legislation/details/23228> . تاريخ اخر زيارة في 2026/6/14

(1) Autorité de la concurrence – "Enforcing competition rules: combating cartels and abuses of dominant position", site officiel, consulté le.

(2) تنظر مواد الفصل الثالث من قانون التجارة العراقي النافذ (واجبات التاجر).

(3) تنظر مواد الفصل الرابع من قانون حماية المستهلك العراقي النافذ (واجبات المجهز والمعلن).



المصلحة العامة وتحقيق الربح المشروع، دون أن يمنحها أي امتياز رسمي أو احتكار مفترض في مواجهة العملاء والمستهلكين⁽¹⁾.

ثانياً: استقلال شركات الأمن السيبراني كشخص معنوي خاص عن الدولة

يُشكّل الاستقلال القانوني لشركات الأمن السيبراني كشخص معنوي خاص الخاصية الحاسمة التي تُرجّح الطابع المدني على الطابع السيادي في تكييف هذه الشركات. فالشخص المعنوي الخاص الذي يتمتع بذمة مالية مستقلة وأهلية قانونية كاملة ويتحمل مسؤوليته المدنية باسمه الخاص لا يمكن إدراجه ضمن منظومة الأشخاص المعنوية العامة مهما اتصل نشاطه بالوظائف السيادية للدولة، وهو ما يميزها عن الجهات ذات الطابع السيادي ويجعل نشاطها خاضعاً للقوانين العامة للشركات والتجارة. وهذا الاستقلال هو الركيزة التي يقوم عليها نظام المسؤولية المدنية لهذه الشركات، مع حرية كاملة في تحديد سياسات عملها وعقودها التجارية. ويعكس هذا الاستقلال قدرة الشركة على ممارسة النشاط التجاري بحرية، سواء في تقديم خدماتها للقطاع الخاص أو العام، مع الحفاظ على حقها في التعاقد المباشر مع العملاء وتحديد الشروط والأسعار ونطاق الخدمات. وتعتبر هذه الخصيصة جوهرية في إبراز الطابع الخاص لشركة الأمن السيبراني، إذ تؤكد أنها ليست ذراعاً للدولة، بل كيان مستقل يتحمل مسؤولياته القانونية والتعاقدية، وإن كان يعمل على ممارسة نشاط ذو طابع سيادي يفرض عليه بعض الالتزامات كما مر بنا. في الولايات المتحدة الأمريكية، تُعامل شركات الأمن السيبراني كشخصيات معنوية قانونية مستقلة، مما يمنحها الحق في ممارسة الأعمال التجارية بحرية ضمن الإطار القانوني العام. وتخضع هذه الشركات لأحكام القانون فيما يتعلق بالعقود التجارية، وتلتزم بالقوانين الفيدرالية ذات الصلة عند التعامل مع البيانات الحساسة أو القطاع الحكومي، ويتيح هذا الاستقلال للشركة توقيع

(1) وبالعودة إلى الفقه المهتم بهذا الشأن وجدنا أنه يشير إلى وجود تحديات كبيرة عند إخضاع الشركات الرقمية عموماً (بما فيها شركات الأمن السيبراني) لقواعد المنافسة التقليدية، وذلك لأسباب عدة أهمها: أولاً، طبيعة الخدمات الرقمية التي قد تُقدّم مجاناً أو تعتمد على بيانات المستخدمين، ما يجعل تقييم قوة السوق بالمعايير التقليدية مثل السعر والحصة السوقية غير كافٍ؛ ثانياً، التحديات المتعلقة بالخصوصية، محدودية خيارات المستهلك، وإمكانية التلاعب بالخوارزميات؛ ثالثاً، صعوبة قياس الابتكار وقيمة الخدمات التقنية المتقدمة ضمن إطار المنافسة التقليدي. ومن ثم، يؤكد الباحثون على ضرورة تطوير القانون لضمان نزاهة المنافسة، وحماية المستهلك، وتشجيع الابتكار، مع الأخذ بعين الاعتبار خصوصية الأسواق الرقمية وخصائصها الفريدة. لتفاصيل أكثر عن تلك التحديات يراجع:

عقود مباشرة مع العملاء، تحديد مستوى الخدمات، الشروط المالية، والمسؤوليات القانونية، بما في ذلك الالتزام بعقود مستوى الخدمة وضمان تعويضات مناسبة في حال إخلال أي طرف بالتزاماته⁽¹⁾.

أما في فرنسا، فإن الشركات بصفتها شركات تتمتع بشخصية مستقلة تتمتع بحرية التعاقد وفق القانون المدني الفرنسي والقانون التجاري الفرنسي، وتتمكن من تقديم خدمات الأمن السيبراني لكل من القطاعين العام والخاص ضمن إطار عقود تجارية مستقلة من حيث التكوين. وتحدد هذه العقود الالتزامات القانونية والفنية للشركة تجاه العملاء، بما يشمل حماية البيانات، مستوى الخدمة، السرية، وخطط الاستجابة للطوارئ. ويؤكد هذا الاستقلال القانوني على الطابع الخاص للشركة، رغم إمكانية تعاملها مع الدولة أو القطاع العام بموجب عقود محددة، دون أن تصبح جزءاً من الإدارة السيادية المباشرة.

و في العراق، وبرغم غياب تنظيمات متخصصة للأمن السيبراني، فإن شركات هذا القطاع، باعتبارها شركات خاصة مسجلة وفق قانون الشركات رقم 21 لسنة 1997 وملتزمة بأحكام قانون التجارة رقم 30 لسنة 1984، تمتلك استقلالية كشخص معنوي خاص، مما يمكنها من توقيع عقود مباشرة مع العملاء وتحديد نطاق خدماتها وأسعار تلك الخدمات والتزاماتها. ويظل التسجيل القانوني للشركة، مسك الدفاتر، والتقيّد بقوانين حماية المستهلك رقم 1 لسنة 2010 من المتطلبات الأساسية التي تعزز شرعيتها القانونية، بينما يظل الحرية التجارية والتعاقدية من أبرز مظاهر الطابع الخاص للشركة، ما يجعلها مسؤولة قانونياً عن أي إخلال بالتزاماتها تجاه العملاء.

وتأسيساً على ما تقدم في هذا المطلب، يتضح أن شركات الأمن السيبراني تجمع بين طابعين لا يتعارضان بل يتكاملان: طابع سيادي جزئي تستمدّه من التفويض الذي تمنحه إياه الدولة، وطابع تجاري خاص تستمدّه من استقلالها القانوني وخضوعها لمنطق السوق والعقد. والراجح في ضوء طبيعة هذه الرسالة التي تنهض على أحكام القانون المدني أن الطابع التجاري الخاص هو الغالب والأصيل، لأن الشركة مهما اتصل نشاطها بالمصلحة العامة تبقى في نهاية المطاف شخصاً معنوياً خاصاً تحكمه قواعد القانون الخاص وتقوم مسؤوليته المدنية على أحكام العقد والمسؤولية التقصيرية.

(1) Daniel Chibuiké Okoro, An Evaluation of Cybersecurity Frameworks and Privacy Regulations for Companies in the Digital Age: A Legal Approach, aUniversity of Uyo, Nigeria, Volume 25, Issue 4, Page 431-440, 2025; Article no.AJEBA.133682 ISSN: 2456-639X , p.437.



المبحث الثاني

ذاتية شركات الأمن السيبراني

يقتضي البحث في شركات الأمن السيبراني، بعد تحديد إطارها المفاهيمي وخصائصها العامة، الانتقال إلى بيان ذاتيتها القانونية داخل النظام القانوني، وذلك من خلال تحديد مركزها القانوني وطبيعة نشاطها، وبيان موقعها من القواعد العامة والخاصة التي تحكم هذا النشاط. وتبرز أهمية هذا التحديد بالنظر إلى خصوصية الدور الذي تؤديه شركات الأمن السيبراني، إذ تمارس نشاطاً يرتبط بحماية المصالح الرقمية للأفراد والمؤسسات، وما يترتب على ذلك من آثار قانونية تتعلق بطبيعة الالتزامات الملقة على عاتقها وحدود مسؤوليتها. وهو ما يفرض ضرورة الوقوف على التكييف القانوني الصحيح لهذه الشركات، بعيداً عن الخلط بينها وبين غيرها من الكيانات التي تمارس أنشطة قريبة في ظاهرها. وعليه، قُسم هذا المبحث إلى مطلبين؛ خُصص الأول للتكييف القانوني لشركات الأمن السيبراني، بينما خُصص الثاني لتمييزها عما يشته به من الأوضاع القانونية الأخرى.

المطلب الأول

التكييف القانوني لشركات الأمن السيبراني

يقتضي تحديد الوضع القانوني لشركات الأمن السيبراني الوقوف على طبيعة المركز الذي تشغله هذه الشركات داخل النظام القانوني، ولا سيما في ظل خصوصية النشاط الذي تمارسه والآثار التي يترتبها على المصالح الرقمية للأفراد والمؤسسات. فمجرد وصف هذا النشاط أو بيان طابعه التقني لا يكفي لإدراك الإطار القانوني الذي يحكمه، ما لم يُستكمل ذلك بتكييف قانوني يحدّد القواعد الواجبة التطبيق. ويؤثر هذا التكييف جملة من المسائل المرتبطة بمدى خضوع شركات الأمن السيبراني لقواعد القانون الخاص، وحدود تأثير نشاطها بالقواعد الخاصة بالأمن السيبراني، وما يترتب على ذلك من انعكاسات على طبيعة التزاماتها القانونية. ويُعدّ الوقوف على هذه المسائل مدخل ضروري لفهم الأساس القانوني للمسؤولية التي قد تنشأ عن ممارسة هذا النشاط.

وعلى هذا الأساس، يُعالج هذا المطلب، في فرعين، مركز شركات الأمن السيبراني ضمن النظام القانوني، ثم العلاقة القانونية بين نشاطها والقواعد الخاصة بالأمن السيبراني.

الفرع الأول

مركز الشركة ضمن النظام القانوني

يُعد تحديد مركز شركة الأمن السيبراني ضمن النظام القانوني من المسائل الجوهرية التي يتوقف عليها فهم طبيعة التزاماتها، وحدود مسؤوليتها، ونطاق خضوعها لقواعد القانون الخاص أو العام. ولا يمكن مقارنة هذا المركز مقارنة سليمة إلا بالعودة إلى القواعد العامة التي تحكم نظرية الشخص المعنوي في القانون المدني، وما استقر عليه الفقه والقضاء من معايير تميّز بين الأشخاص المعنوية الخاصة والأشخاص المعنوية العامة⁽¹⁾.

تنشأ شركات الأمن السيبراني، من حيث الأصل، وفق القواعد العامة لتأسيس الأشخاص المعنوية الخاصة، وبإرادة مؤسسيها، وتهدف إلى ممارسة نشاط اقتصادي منظم يتمثل في تقديم خدمات حماية وتأمين الأنظمة الرقمية والمعلوماتية. وطبقاً للمبادئ المستقرة في القانون المدني، فإن الشخصية المعنوية تُمنح للكيان الذي يعترف له القانون بوجود مستقل عن الأشخاص المكوّنين له، ويخوّله أهلية اكتساب الحقوق وتحمل الالتزامات باسمه الخاص⁽²⁾.

إن العبرة في تحديد الطبيعة القانونية للشخص المعنوي لا تقوم على طبيعة النشاط الذي يباشره، وإنما على الأساس القانوني الذي يستمد منه وجوده، وطريقة إنشائه لتحقيق الهدف الذي نشأ من أجله⁽³⁾.

(1) الشخصية الاعتبارية هي ذلك الشخص الخاضع للقانون المدني الذي يتكون من مجموعة من الأشخاص (أو الشخص الطبيعي) الذين يستوفون الشروط التي وضعها القانون لاكتساب هذه الصفة، واستقر الفقه والقضاء على أن التمييز بين الأشخاص المعنوية العامة والأشخاص المعنوية الخاصة لا يقوم على طبيعة النشاط في حد ذاته، وإنما يستند إلى مجموعة من المعايير المتكاملة، في مقدمتها طريقة إنشاء الكيان، والغاية التي يهدف إليها، ومدى خضوعه لقواعد القانون العام، وتمتعه بامتيازات السلطة العامة، وهو ما أكدّه الفقه الإداري التقليدي والحديث على السواء.

Cristian MACSIM, Legal Person Subject to Civil Law, Volume 9, Issue 1, 2021, p.14.

(2) د. محمد مصطفى زرباني، الشركات التجارية، دراسة في النشأة التعاقدية والنظام القانوني، المطبعة العالمية، 2020، ص73.

(3) نصّت المادة (47) من القانون المدني العراقي على ان: "الأشخاص المعنوية هي: أ-الدولة. ب-الادارات والمنشآت العامة التي يمنحها القانون شخصية معنوية مستقلة عن شخصية الدولة بالشروط التي يحددها. ج- الالوية والبلديات والقرى التي يمنحها القانون شخصية معنوية بالشروط التي يحددها. د- الطوائف الدينية التي يمنحها القانون شخصية معنوية بالشروط التي يحددها. هـ- الأوقاف. و- الشركات التجارية والمدنية الا ما استثنى منها بنص في القانون. ز- الجمعيات المؤسسة وفقاً للأحكام المقررة في القانون. ح- كل مجموعة من الاشخاص او الاموال يمنحها القانون شخصية معنوية".

ومدى ارتباط ذلك بالإدارة العامة⁽¹⁾. فمتى نشأ الكيان بإرادة خاصة، ولم يكن مرفق عام، ولم يُنشأ بنص تشريعي خاص يمنحه صفة الشخص العام، فإنه يظل خاضع – من حيث الأصل – لنظام الأشخاص المعنوية الخاصة، ولو كان نشاطه وثيق الصلة بمصالح عامة أو وظائف ذات حساسية خاصة.

ومن هذا المنطلق، فإن مجرد اضطلاع شركة الأمن السيبراني بنشاط يرتبط بحماية البيانات، أو تأمين البنى التحتية الرقمية، أو المساهمة في الحد من المخاطر التي تهدد الأمن السيبراني الوطني، ومهما كانت طبيعة النشاط حساسة فهذا لا يكفي بذاته لنقلها من نطاق القانون الخاص إلى دائرة الأشخاص المعنوية العامة، ما لم يتدخل المشرع بنص صريح يُغيّر من طبيعتها القانونية ويخضعها لنظام قانوني مغاير⁽²⁾. ويُعدّ هذا المبدأ، أي حياد طبيعة النشاط في تحديد الطبيعة القانونية للكيان، ركيزة جوهريّة في الفكر القانوني المدني المقارن، لأنه يقطع الطريق أمام كل محاولة لتوسيع نطاق القانون العام على حساب القانون الخاص بذريعة حساسية النشاط أو ارتباطه بالمصلحة العامة. فلو قُبل العكس لأدى ذلك إلى إخضاع كل شركة تمس خدماتها مصلحة عامة لنظام الأشخاص المعنوية العامة، وهو ما يُفضي إلى اضطراب جسيم في منظومة القانون الخاص وتآكل تدريجي في مبدأ الاستقلال القانوني للشركات.

ويُستخلص من ذلك أن مركز شركة الأمن السيبراني داخل النظام القانوني لا يُحدّد بالنظر إلى طبيعة الوظائف التي تؤديها أو حساسية المصالح التي تسهم في حمايتها، وإنما يُحدّد ابتداءً بالرجوع إلى الإطار القانوني الذي نشأت في ظله، والأساس النظامي الذي تستمد منه شخصيتها القانونية. فهي، من حيث التأسيس والتنظيم، تُنشأ وفق القواعد العامة التي تحكم الشركات التجارية، وبإرادة خاصة، وتُسجّل في السجلات المختصة، وتتمتع بذمة مالية مستقلة، وبأهلية قانونية كاملة تخولّها مباشرة النشاط

(1) وتبعا لتصنيف المعهد الوطني للإحصاء الفرنسي الشخصية المعنوية باعتبارها مجموعة تتمتع بالشخصية القانونية، إلى شخصيات معنوية من الحق العام وشخصيات معنوية من الحق الخاص، ولكل فئة نظامها القانوني الخاص بها، ففي القانون الفرنسي، الذي يُعد مرجعاً في المقاربات المدنية المقارنة، يُنظر إلى الشخصيات المعنوية العامة على أنها خاضعة للقانون العام (مثل الدولة والهيئات العامة) في حين تخضع الشخصيات المعنوية الخاصة للقانون الخاص (مثل الشركات والجمعيات)، وهو معيار معتمد في الفقه القانوني.

الموقع الرسمي للمعهد الوطني للإحصاء والدراسات الاقتصادية الفرنسي متاح على الرابط:

تاريخ اخر زيارة في 2026/6/14. <https://www.insee.fr/fr/metadonnees/definition/c1251>.

(2) Randy E. Barnett, Four Senses of the Public Law–Private Law Distinction Four Senses of the Public Law–Private Law Distinction , Harvard Journal of Law & Public Policy, Vol. 9, 1986 . p.271.

الاقتصادي، وإبرام العقود، وتحمل الالتزامات الناشئة عنها⁽¹⁾. ولا تتمتع هذه الشركات، بحكم نشأتها، بأي من خصائص الأشخاص المعنوية العامة، فلا تمارس سلطة عامة، ولا تتمتع بامتيازات السلطة العامة، ولا تُعد جزءاً من التنظيم الإداري للدولة، ولا تخضع في علاقاتها التعاقدية لقواعد القانون العام، بل تظل خاضعة – من حيث الأصل – لأحكام القانون الخاص⁽²⁾. ويترتب على هذا التكييف أن ارتباط نشاط الشركة بحماية المصالح الرقمية أو الإسهام في تأمين البنى التحتية المعلوماتية للدولة لا يُنشئ بذاته مركز قانوني عام، ولا يُغيّر من طبيعتها كشخص معنوي خاص، ما دام هذا الارتباط لم يُترجم بتدخل تشريعي صريح يُخضعها لنظام قانوني استثنائي أو يمنحها صفة الشخص العام.

وعلى هذا الأساس، يغدو التمييز بين التنظيم القانوني للنشاط والتكييف القانوني للكيان القائم به مسألةً جوهرية لا يجوز إغفالها. فإخضاع شركات الأمن السيبراني لنظم ترخيص أو رقابة خاصة أو إلزامها بمعايير أمنية صارمة هو في حقيقته تنظيم للنشاط لا تغيير في طبيعة الكيان، تماماً كما أن خضوع شركات الأدوية لرقابة صحية مشددة لا يُخرجها من دائرة القانون الخاص، وكما أن خضوع البنوك لرقابة مصرفية صارمة لا يجعلها أشخاصاً معنوية عامة. والمعيار الحاسم في كل هذه الحالات واحد: ما هو الأساس القانوني الذي نشأ عليه الكيان؟ لا ما هو النشاط الذي يمارسه.

وعلى مستوى القوانين المقارنة وتحديداً في النظام القانوني الأمريكي، تُعد شركات الأمن السيبراني شركات خاصة تتمتع بالشخصية المعنوية الكاملة، وتخضع من حيث الأصل لقواعد القانون التجاري والمدني، بما في ذلك قواعد المنافسة ومنع الاحتكار. ويُستدل على طبيعتها كشركات خاصة من خضوعها – شأنها شأن سائر المشاريع التجارية – لقوانين مكافحة الاحتكار، وعلى رأسها قانون شيرمان وقانون كلايتون، التي تهدف إلى منع الاتفاقات المقيدة للتجارة وإساءة استغلال الوضع المهيمن في السوق⁽³⁾. وفي الوقت ذاته، تخضع هذه الشركات لرقابة تنظيمية مشددة من قبل الهيئات المختصة،

(1) د. حسين الماحي، الشركات التجارية، دار النهضة العربية، القاهرة، 2010، ص16.

(2) Yasmine Budustour & Leen Budustour, The Doctrine of Separate Legal Personality and Its Significance in International Business, SSRN Electronic Journal, 2023, p.4.

(3) نصت المادة 2، القسم 15 من قانون شيرمان الصادر في العام 1890 والمعدل مؤخراً في 2004 على أن: " يُعتبر كل شخص يحتكر، أو يحاول احتكار، أو يتآمر أو يتحد مع أي شخص آخر، أو أشخاص آخرين، لاحتكار أي جزء من التجارة بين الولايات المختلفة، أو مع الدول الأجنبية، مُذنّباً بارتكاب جناية، ويُعاقب عند إدانته بغرامة لا تتجاوز 100,000,000 دولار أمريكي إذا كان شركة، أو 1,000,000 دولار أمريكي إذا كان أي شخص آخر، أو بالسجن لمدة لا تتجاوز 10 سنوات، أو بكلا العقوبتين، وذلك حسب تقدير المحكمة".

أما قانون كلايتون لعام 1914 المعدل وهو قانون مكمل لقانون شيرمان يركز بشكل خاص على منع عمليات الاندماج أو الاستحواذ التي قد تُقلّل المنافسة بشكل كبير، ومنع التسعير التمييزي وغيره من الممارسات المضرة بالمنافسة، فقد

ولا سيما لجنة التجارة الفيدرالية ووزارة العدل الأمريكية، سواء في ما يتعلق بحماية البيانات، أو أمن الأنظمة، أو عمليات الاندماج والاستحواذ⁽¹⁾. دون أن يُفهم من ذلك انتقالها إلى فئة الأشخاص المعنوية العامة، إذ تظل الرقابة هنا ذات طابع تنظيمي لا مؤسسي، ولا تُمس الأساس القانوني لنشأة الشركة أو طبيعتها الخاصة.

ويكشف النظام الأمريكي بجلاء أن التوتر الظاهر بين متطلبات الأمن القومي وحرية النشاط الاقتصادي ليس تناقضاً جوهرياً بل توتر يُحسم عبر آلية التنظيم لا عبر إعادة تكييف الكيان. فالدولة تحمي أمنها القومي من خلال تنظيم النشاط ورقابته، لا من خلال تأميم الكيانات القائمة به أو إدماجها في جهازها الإداري، وهذا هو المنهج الذي يضمن استمرار حوافز الابتكار في القطاع الخاص مع صون المصلحة العامة.

لا يختلف الوضع في فرنسا من حيث المبدأ، إذ تُعتبر شركات الأمن السيبراني أشخاص معنوية خاصة تخضع للقانون المدني والتجاري، وتتمتع بالاستقلال القانوني في ممارسة نشاطها. غير أن

نصت المادة (2) منه على أن: "يُحظر على أي شخص يمارس التجارة، سواء بشكل مباشر أو غير مباشر، التمييز في الأسعار بين مشتري سلع من نفس النوع والجودة، أثناء ممارسته لهذه التجارة، سواء بشكل مباشر أو غير مباشر، حيث تكون أي من عمليات الشراء المتضمنة في هذا التمييز تجارية، وحيث تُباع هذه السلع للاستخدام أو الاستهلاك أو إعادة البيع داخل الولايات المتحدة أو أي إقليم تابع لها أو مقاطعة كولومبيا أو أي منطقة تابعة لها أو أي مكان آخر يخضع لولاية الولايات المتحدة، وحيث قد يكون أثر هذا التمييز هو تقليل المنافسة بشكل كبير أو خلق احتكار في أي مجال من مجالات التجارة، أو الإضرار بالمنافسة أو تدميرها أو منعها مع أي شخص يمنح أو يتلقى عن علم فوائد هذا التمييز، أو مع عملاء أي منهما: شريطة ألا يمنع أي شيء وارد هنا الفروقات التي تراعي فقط الاختلافات في تكلفة التصنيع أو البيع أو التسليم الناتج عن اختلاف الطرق أو الكميات التي تُباع أو تُسلم بها هذه السلع إلى هؤلاء المشتريين: شريطة، مع ذلك، أن يجوز للجنة التجارة الفيدرالية، بعد إجراء التحقيق اللازم وعقد جلسة استماع لجميع الأطراف المعنية، تحديد ووضع حدود للكميات، ومراجعتها حسبما تراه ضرورياً، فيما يتعلق بسلع معينة أو فئات معينة من السلع، حيث تجد أن المشتريين المتاحين بكميات أكبر قليلون جداً لدرجة تجعل الفروقات الناجمة عن ذلك تمييزية بشكل غير عادل أو تشجع على الاحتكار في أي مجال من مجالات التجارة...".

⁽¹⁾ يحظر قانون لجنة التجارة الفيدرالية "أساليب المنافسة غير العادلة" و"الأفعال أو الممارسات غير العادلة أو الخادعة". وقد قضت المحكمة العليا بأن جميع انتهاكات قانون شيرمان تُعد انتهاكاً لقانون لجنة التجارة الفيدرالية. وبالتالي، فبالرغم من أن لجنة التجارة الفيدرالية لا تُنفذ قانون شيرمان رسمياً، فأنها تستطيع رفع دعاوى بموجب قانون لجنة التجارة الفيدرالية ضد نفس أنواع الأنشطة التي تُخالف قانون شيرمان. كما يشمل قانون لجنة التجارة الفيدرالية ممارسات أخرى تضر بالمنافسة، ولكنها قد لا تندرج ضمن فئات السلوك المحظورة رسمياً بموجب قانون شيرمان. تختص لجنة التجارة الفيدرالية وحدها برفع الدعاوى بموجب قانونها. لتفاصيل أكثر ينظر: قوانين مكافحة الاحتكار الأمريكية، الموقع الرسمي للجنة التجارة الفيدرالية الأمريكية، متاح على: <https://www.ftc.gov/advice-guidance/competition-guidance/guide-antitrust-laws/antitrust-laws>

تاريخ اخر زيارة في 2026 / 1/24

خصوصية النشاط دفعت المشرع الفرنسي إلى إخضاع هذه الشركات لنظام رقابي وفني صارم، تشرف عليه الوكالة الوطنية لأمن نظم المعلومات (ANSSI)⁽¹⁾. ويُعد المرسوم رقم 350-2015 المتعلق بتأهيل المنتجات والخدمات الأمنية مثال واضح على هذا الاتجاه، إذ يقتصر أثره على تنظيم شروط التأهيل الفني للمنتجات والخدمات⁽²⁾، من دون أن ينشئ صفة عامة للشركات المؤهلة أو يدمجها في التنظيم الإداري للدولة.

ويُظهر هذا الإطار أن القانون الفرنسي يميّز بوضوح بين الرقابة السيادية على النشاط والطبيعة القانونية الخاصة للكيان، ويؤكد أن إخضاع الشركة لقواعد تنظيمية مشددة لا يعني فقدانها لصفة الشخص المعنوي الخاص.

كرّس المشرع العراقي هذا التوجه من خلال لائحة تنظيم شركات الأمن السيبراني رقم 33 لسنة 2025، التي وضعت إطار قانوني خاص ينظم نشاط هذه الشركات، ويحدد التزاماتها تجاه حماية الأنظمة والبنى التحتية الرقمية، والتنسيق مع الجهات المختصة. ومع ذلك، لم تخرج اللائحة عن القواعد العامة للقانون الخاص، إذ أبقت على استقلال الشركة كشخص معنوي خاص، مخوّلة بالتعاقد مباشرة مع العملاء، وتحديد نطاق خدماته وأسعاره، وتحمل المسؤولية المدنية عن أي إخلال بالتزاماته. ويعكس هذا الإطار توجهاً تشريعياً يسعى إلى الجمع بين متطلبات حماية الأمن الوطني والحفاظ على الطابع التجاري الخاص للنشاط.

وخلاصة ما تقدم أن مركز شركة الأمن السيبراني ضمن النظام القانوني لا يقبل التردد بين القانون العام والقانون الخاص، بل هو مركز محسوم لصالح القانون الخاص بحكم الأساس القانوني الذي نشأت عليه هذه الشركات، غير أنه مركز مُقَيّد بالتزامات تنظيمية ذات طابع أمر تفرضها حساسية النشاط واتصاله بالمصلحة العامة. وهو ما له أثر قانوني مباشر، إذ يعني أن المسؤولية المدنية لهذه الشركات تخضع للقواعد العامة في القانون الخاص من عقد ومسؤولية تقصيرية، مع مراعاة ما تفرضه

(1) Adejoke T. Odebade¹, Elhadj Benkhelifa, A Comparative Study of National Cyber Security Strategies of ten nations, , p.2.

(2) أشارت المادة (2) من المرسوم الفرنسي المتعلق بتأهيل المنتجات والخدمات الأمنية على أن: "يتم إرسال طلب التأهيل لمنتج أمني إلى الوكالة الوطنية لأمن أنظمة المعلومات. قم بالتخزين مع التصرف العام من خلال الاطلاع إلكترونياً على قائمة القطع المجمعة حسب الطلب، والتي تحتوي على وصف تفصيلي للمنتج ووظائف الأمان الخاصة به بالإضافة إلى أهداف الأمان...".



الالتزامات التنظيمية من تشديد في معايير العناية الواجبة. وهذا ما سيأتي تفصيله في الفرع الثاني من هذا المطلب.

الفرع الثاني

العلاقة القانونية بين نشاط الشركة والقواعد الخاصة بالأمن السيبراني

يكتسب نشاط شركات الأمن السيبراني أهمية خاصة في إطار التكييف القانوني، ليس فقط بالنظر إلى طبيعته التقنية، وإنما لما يثيره من إشكاليات قانونية ناجمة عن امتداده إلى مجالات تمس بصورة مباشرة الأمن الوطني والمصلحة العامة مما يستدعي قواعد خاصة لضمان هذه المصالح، وهو ما يطرح تساؤل حول كيفية تفاعل هذه الشركة مع القواعد الخاصة بالأمن السيبراني وهل تمارس نشاطها في إطار القانون الخاص؟ وأن الإجابة على هذا التساؤل تُحدد الأساس الذي تقوم عليه مسؤولية هذه الشركات المدنية، إذ إن طبيعة الالتزام القانوني تتوقف على طبيعة القواعد التي تحكمه. وتكمن الإشكالية في أن نشاط هذه الشركات لا يقتصر على توفير حلول تقنية أو إدارية لحماية الأنظمة الرقمية⁽¹⁾، بل يمتد ليشمل حماية البنى التحتية الحيوية وتأمين البيانات ذات الطابع الاستراتيجي والمساهمة في رصد التهديدات السيبرانية، مما يجعله خاضعاً لإطار قانوني مزدوج يجمع بين الالتزامات التعاقدية الخاصة والالتزامات التنظيمية العامة، دون أن يُفضي هذا الازدواج إلى المساس باستقلالية الشركة كشخص معنوي خاص⁽²⁾.

ويُلاحظ في هذا السياق أن اعتماد الدول المتزايد على شركات الأمن السيبراني في تأمين بنيتها الرقمية، سواء من حيث الأجهزة والبرمجيات أو بروتوكولات الحماية وخدمات الأمن، قد أفضى إلى نشوء علاقة تشابك واضحة بين القطاعين العام والخاص في إدارة البنى التحتية والبيانات والخدمات ذات الحساسية العالية⁽³⁾. ويتعزز هذا التشابك من خلال اضطلاع هذه الشركات، في العديد من الحالات،

(1) Devika Sharma. Sandeep Reddy. Hamza Shahid, Cybersecurity Obligations for Critical Infrastructure: Emerging Legal Norms, Enforcement Gaps, and Governance Challenges, Legal Studies in Digital Age, Vol. 2, No. 3, 2023, p.49.

(2) ibd.

(3) Louise Marie Hurel , Private Authority and the Political Economy of Private Companies in Cybersecurity Crises and Conflicts ,p. 5

بتقديم الدعم الفني والتقني والتدريب في إطار برامج بناء القدرات الوطنية أو الاستجابة للأزمات السيبرانية، مع إشراف السلطات العامة، مما يكرّس استمرارية التعاون المؤسسي بين الدولة والفاعل الخاص في مجال يُعدّ من صميم الأمن الوطني المعاصر.

والأثر القانوني لهذا الانخراط المتقدم في مجالات ذات بعد سيادي لا يتجلى في إدماج الشركة في التنظيم الإداري للدولة أو نزع صفتها الخاصة، بل يتجلى في شيء أكثر دقة وأعمق أثراً وهو تشديد معيار العناية الواجبة المفروض على الشركة في علاقاتها التعاقدية. فالشركة التي تخضع لالتزامات تنظيمية أمرّة تتعلق بالسرية والجاهزية والتعاون مع الجهات المختصة لا يُقاس إخلالها بمعيار الشخص المعقول العادي في القانون الخاص⁽¹⁾، بل يُقاس بمعيار أشد يستوجب استيفاء تلك الالتزامات التنظيمية. ومن هنا تظهر القيمة القانونية الحقيقية للإطار التنظيمي المزدوج: إنه لا يُغيّر طبيعة الكيان لكنه يُشدّد معيار مسؤوليته المدنية⁽²⁾.

وفي هذا السياق، يتعين على الشركات الالتزام بمجموعة من المعايير التقنية والتنظيمية، مثل تطبيق البروتوكولات الدولية للسلامة الرقمية، إدارة مخاطر اختراق البيانات، وضمان استمرارية الخدمة في الحالات الطارئة⁽³⁾. مثلما يشمل الالتزام دمج معايير الأمان ضمن العقود مع العملاء، بما في ذلك عقود مستوى الخدمة (SLA)، التي تحدد واجبات الشركة ومسؤوليتها في حال إخلالها بالتزاماتها التقنية أو التعاقدية. يبرز هذا التوازن بين الاستقلال القانوني والالتزام التنظيمي طبيعة النشاط المزدوج للشركة، الذي يجمع بين الوظائف التجارية والمهام ذات الطابع السيادي الجزئي.

وفي الولايات المتحدة، تُعد شركات الأمن السيبراني كيانات قانونية مستقلة، تمتلك أهلية كاملة لممارسة النشاط التجاري وتحديد نطاق الخدمات والأسعار، مع مسؤولية مباشرة تجاه العملاء وفق قواعد القانون المدني والتجاري الأمريكي. إلا أن هذا الاستقلال القانوني لا يعفي الشركة من الالتزام بمجموعة متكاملة من المعايير التنظيمية والتقنية، وتظهر هذه الآليات بوضوح من خلال تفاعل الشركة

(1) د. أنور سلطان، مصادر الالتزام في القانون المدني، ط10، دار الثقافة للنشر والتوزيع، عمان، 2018، ص234.

(2) Devika Sharma. Sandeep Reddy. Hamza Shahid, op.cit, p.50.

(3) مع ذلك، تشير الإدارة السيبرانية الأمريكية الى ان: " للشركات الخاصة الحق في إطلاق بعض خدمات الأمن السيبراني - التدابير الدفاعية مثل التحديثات، وتطبيق برامج مكافحة الفيروسات، والضوابط الإدارية - ولكن لا يُسمح لها بتنفيذ تدابير أخرى - التدابير الهجومية مثل الرد بالهجوم، ودعم الدفاع السيبراني النشط.

Booz Allen Hamilton, Booz Allen to help US Cyber Command boost cybersecurity. 13 July 2016. <https://www.boozallen.com/e/media/press-release/booz-allen-to-help-us-cyber-command-boost-cyber-security.html>.. تاريخ اخر زيارة في 2026/6/14



مع العقود، حيث يجب أن تتضمن الاتفاقيات التعاقدية أحكاماً تقنية واضحة لضمان الامتثال، مما يحفظ توازن بين استقلال الشركة القانوني وبين مسؤولياتها تجاه حماية العملاء والمصلحة العامة⁽¹⁾.

في النظام الفرنسي، يخضع تنظيم الأمن السيبراني لإطار قانوني مؤسس يُركّز بشكل واضح على حماية الفضاء الرقمي والمصلحة الوطنية، وتُناط الجهة الوطنية المعنية بأمن النظم المعلوماتية بمهمة وضع المعايير ومتابعة تنفيذ الالتزامات التنظيمية ذات الصلة وهي الوكالة الوطنية لأمن نظم المعلومات⁽²⁾. وتنطوي هذه القواعد على متطلبات تتعلق بتأهيل المنتجات والحلول الأمنية قبل طرحها في السوق، بما في ذلك تقديم المستندات والمعلومات التي تبيّن الوظائف المقصودة منها ومدى توافقها مع المقاصد الوطنية لحماية الأمن الرقمي. ويُمكن التمييز بين طبيعة هذه الإجراءات من جهة، وبين الوضع القانوني للشركة من جهة أخرى؛ إذ تظل الشركة، من حيث الأصل، شخصاً معنوياً خاصاً مستقلاً قادراً على إبرام العقود وتنظيم علاقاتها التعاقدية مع الزبائن من القطاعين العام والخاص، وتحديد شروط الخدمة والمقابل المالي وفق أحكام القانون المدني والتجاري الفرنسية. وفي الوقت نفسه، تمثل الالتزامات التنظيمية المفروضة عليها أداة ضبط قانوني لنشاطها في المجال الذي يمسّ الأمن الوطني والمصلحة العامة، إذ تفرض عليها الامتثال لمعايير محددة، وتخضع في ذلك لمتابعة الجهة المنظمة، بما يحقق التكامل بين أهمية الدور الذي تؤديه في حماية الفضاء الرقمي وبين احترام قواعد النظام القانوني الفرنسي في هذا المجال⁽³⁾.

(1) تظهر التجربة الأمريكية وجود حوكمة مشتركة للأمن السيبراني بين القطاعين العام والخاص. وتُسلط هذه الحوكمة الضوء على أربعة مجالات نجحت فيها في سياق التصدي للتهديدات السيبرانية الدولية: (1) تعطيل شبكات أجهزة الكمبيوتر المصابة التي تستخدمها الجماعات الإجرامية العابرة للحدود؛ (2) معالجة ثغرات البرامج؛ (3) إسناد الاختراقات السيبرانية إلى جهات فاعلة مرتبطة بالدولة أو مدعومة منها؛ (4) حماية الأنظمة المملوكة للقطاع الخاص من الجهات الفاعلة المتطورة.

Louise Marie Hurel, op.cit, p10.

(2) Philippe VITEL and Henrik BLIDDAL , FRENCH CYBER SECURITY AND DEFENCE: AN OVERVIEW, Vitel & Bliddal, vol.32, 2015 ,p.3.

(3) يمكن للوكالة الوطنية لأمن نظم المعلومات (ANSSI) وضع قواعد أمنية إلزامية للأنظمة الحيوية للمشغلين ذات الأهمية الحيوية؛ ويجب إخطارها بالحوادث التي تقع على الأنظمة الحيوية للمشغلين (شركات الأمن السيبراني) ذات الأهمية الحيوية؛ ويمكنها فرض عمليات تفتيش أمنية؛ ويمكنها فرض تدابير محددة في حالة الأزمات الكبرى. وقد تم إنجاز هذه المهام بثلاثة مراسيم صادرة عن الوكالة الوطنية لأمن نظم المعلومات.

Philippe VITEL and Henrik BLIDDAL, opcit, p.7.



تبنى العراق نموذج متوازن في اللائحة 33 لسنة 2025، حيث تحدد التزامات شركات الأمن السيبراني تجاه حماية الأنظمة والشبكات الحيوية، وضمان الامتثال للمعايير الفنية والتنظيمية، والتنسيق مع الجهات الرسمية عند مواجهة التهديدات السيبرانية. في الوقت نفسه، تمنح اللائحة الشركات استقلالية كشخص معنوي خاص، بما يتيح لها ممارسة النشاط التجاري بحرية، تحديد نطاق الخدمات والأسعار، وصياغة العقود مع العملاء، مع تحمل المسؤولية المدنية عن أي إخلال بالتزاماتها. هذا التوازن بين الالتزام التنظيمي والاستقلالية القانونية يجعل الشركات قادرة على تحقيق حماية البنية التحتية الوطنية، مع الحفاظ على مرونة السوق والقدرة على الابتكار.

وعليه أن القواعد الخاصة بالأمن السيبراني لا تُنشئ لشركات الأمن السيبراني مركزاً قانونياً جديداً خارج القانون الخاص، بل تُحدد المضمون الموضوعي للالتزامات التي تتحملها داخل هذا القانون. وهذا التمييز الدقيق بين المركز القانوني من جهة ومضمون الالتزام من جهة أخرى هو مفتاح فهم المسؤولية المدنية لهذه الشركات، إذ تخضع هذه المسؤولية للقواعد العامة في القانون الخاص شكلاً وإجراءً، لكنها تتميز في مضمونها بتشديد معيار العناية الواجبة وتوسيع نطاق الالتزامات المفروضة على الشركة بحكم طبيعة نشاطها الاستثنائية. وهذا ما يستدعي تناول تمييز هذه الشركات عما يشتهى بها من أوضاع قانونية أخرى في المطلب التالي.

المطلب الثاني

تمييز شركات الأمن السيبراني عما يشتهى بها من الأوضاع

لا يكفي لتحديد المركز القانوني لشركات الأمن السيبراني الوقوف عند تعريفها أو تكييف طبيعة نشاطها، لأن ذلك قد يظل قاصراً ما لم يُستكمل بتمييزها عما يقاربها من أوضاع قانونية أخرى قد تتشابه معها في المظهر أو في بعض أدوات العمل، مع اختلافها عنها في الحقيقة من حيث طبيعة الالتزام ومحله وآثاره. ذلك أن هذه الشركات تختلط في التطبيق العملي إما بشركات تقنية المعلومات التي تقدم خدمات رقمية عامة، أو بمزود خدمات الحوسبة السحابية الذين يوفرون البيئة التقنية التي تجري فيها العمليات الرقمية، وهو خلط يفضي إلى اضطراب في تحديد القواعد الواجبة التطبيق وفي ضبط نطاق المسؤولية المدنية. والحال أن النشاط الذي تمارسه شركات الأمن السيبراني يقوم على تقديم خدمات موجهة خصيصاً إلى حماية النظم والبيانات الرقمية من المخاطر والاعتداءات، في إطار قانوني يخضع لترخيص خاص، ويلقي على عاتق الشركة التزامات تتجاوز مجرد تقديم خدمة تقنية أو توفير مواد حوسبية. ومن ثم، فإن تمييز هذه الشركات يعد ضرورة لضبط مركزها في النظام القانوني

وتحديد القواعد الواجبة التطبيق على نشاطها ومسؤوليتها. وعلى هذا الأساس نقسم المطلب على فرعين، يُخصص الفرع الأول لتمييزها عن شركات تقنية المعلومات، ويُخصص الفرع الثاني لتمييزها عن مزودي خدمات الحوسبة السحابية.

الفرع الأول

تمييز شركات الأمن السيبراني عن شركات تقنية المعلومات

يمثل الخلط بين شركات الأمن السيبراني وشركات تقنية المعلومات أحد أبرز التحديات في التطبيق القانوني العملي. فكلتا الفئتين تعمل ضمن الفضاء الرقمي وقد تستخدمان وسائط تقنية مشابهة⁽¹⁾، غير أن هذا التشابه يقتصر على الوسائل ولا يمتد إلى طبيعة النشاط، المركز القانوني، أو نطاق الالتزامات المترتبة على كل منهما. يقتضي الفصل بين هذه الفئتين فهم طبيعة كل نشاط وتحديد نطاق المسؤولية المدنية المرتبطة به. وشركات تقنية المعلومات هي، في جوهرها، شركات تجارية خاصة يكون محل نشاطها هو تقديم خدمات رقمية تتعلق بإنشاء أو تطوير أو تشغيل أو صيانة نظم المعلومات والبرمجيات والشبكات وقواعد البيانات لصالح الغير⁽²⁾، وذلك مقابل أجر. ويقوم نشاطها القانوني على فكرة الخدمة التقنية التي تهدف إلى تمكين الزبون من استعمال نظام معلوماتي أو بنية رقمية صالحة للعمل⁽³⁾، دون أن تمتد لى ضمان أمن هذا النظام في مواجهة المخاطر العدائية أو الهجمات الخارجية.

يندرج نشاط شركات تقنية المعلومات ضمن عقود المقايضة أو عقود تقديم الخدمات، بحسب ما إذا كان محل التزامها هو إنشاء النظام أو تشغيله أو صيانته، فالشركة التي تطور برنامج لإدارة البيانات،

(1) Arina Alexei. Anatolie Alexei, THE DIFFERENCE BETWEEN CYBER SECURITY VS INFORMATION SECURITY, Journal of Engineering Science , Vol. XXIX, no. 4 (2022), pp. 72 – 83 ,p.73-74.

(2) د. عبد الفتاح محمود كيلاني، مدى المسؤولية القانونية لمقدمي خدمات الانترنت، دار الجامعة الجديدة، الإسكندرية، 2011، ص487.

(3) DataGuard. "What is the Difference Between IT and Cyber Security? DataGuard , 2023General online article. Stocks on: <https://www.dataguard.com/blog/what-is-the-difference-between-it-and-cyber-security>. (2026/6/14 تاريخ اخر زيارة في

أو تشغل خادم لاستضافة مواقع الزبائن، أو تدير شبكة داخل مؤسسة، ومن ثمّ تلتزم بتقديم وظيفة تقنية تتمثل في جعل النظام صالح للاستعمال، وليس بجعله آمن في مواجهة الاعتداءات الرقمية، وإن وجود متطلبات امان او حماية للبيانات في عقود تقنية المعلومات لا يعني ان نشاط الشركة هو أمن سيبراني بالمعنى القانوني بل التزام جانبي⁽¹⁾.

ويظهر هذا المعنى بوضوح في القوانين المقارنة. ففي النظام الأمريكي، يُنظر إلى مزودي خدمات تقنية المعلومات باعتبارهم أطراف متعاقدة على تقديم خدمة رقمية، ويُقاس إخلالهم بواجباتهم وفق معيار الأداء المهني والعناية الفنية، لا وفق معيار الحماية من الهجمات السيبرانية. فمسؤوليتهم تقوم متى ما ثبت أنهم أخفقوا في تشغيل النظام أو صيانتته أو تطويره وفق الأصول الفنية المتعارف عليها، لا لمجرد تعرض النظام لاختراق صادر من طرف ثالث⁽²⁾.

(1) فعلى مستوى الولايات المتحدة الامريكية يتم تنظيم التعاقد الحكومي الأمريكي مع مزودي الخدمات التقنية وقد يشترط عناصر حماية ضمن العقد وذلك التزاماً بقواعد اللائحة الفيدرالية للمشتريات او تنظيم المشتريات الاتحادي (FRA) الذي يحدد كيف تشتري الحكومة الامريكية السلع والخدمات من المتعاقدين معها، حيث نصت المادة (2-ج) من الجزء (39-101) على ان: " عند اقتناء تكنولوجيا المعلومات، يجب على الوكالات تضمين سياسات ومتطلبات أمن تكنولوجيا المعلومات المناسبة، بما في ذلك استخدام إعدادات الأمان الشائعة المتاحة على موقع المعهد الوطني للمعايير والتكنولوجيا على الرابط <http://checklists.nist.gov>. وينبغي على مسؤولي التعاقد في الوكالات التشاور مع المسؤول المختص لضمان دمج المعايير المناسبة".

النص باللغة الإنجليزية:

"In acquiring information technology, agencies shall include the appropriate information technology security policies and requirements, including use of common security configurations available from the National Institute of Standards and Technology's website at <http://checklists.nist.gov>. Agency contracting officers should consult with the requiring official to ensure the appropriate standards are incorporated."

اللائحة متاحة على الرابط: <https://www.acquisition.gov> . تاريخ اخر زيارة في 2026/6/14

(2) ففي النظام الأمريكي، يُنظر إلى مزودي خدمات تقنية المعلومات باعتبارهم أطرافاً متعاقدة على تقديم خدمة رقمية، ويُقاس إخلالهم بواجباتهم وفق معيار الأداء المهني والمعايير التعاقدية، لا وفق معيار الحماية من الهجمات السيبرانية. ففي سياق القواعد القضائية والتنظيمية الأمريكية، مسؤولية مزودي الخدمات التقنية تنشأ أساساً عن إخلالهم بالالتزامات التعاقدية أو الإخلال بالمعايير المهنية المتفق عليها، وليس تلقائياً بسبب تعرض النظام لاختراق صادر من طرف ثالث. Reasonable' Cybersecurity Duty", Yale Law & Policy Review (2023).

تاريخ اخر زيارة في 2026/6/14 . <https://www.nortonrosefulbright.com/>.

وفي القانون الفرنسي، يسير الاتجاه ذاته، بحيث يميز بين مقدم الخدمة الرقمية الذي يلتزم بتمكين الزبون من الانتفاع بنظام معلوماتي، وبين الفاعل في مجال أمن الأنظمة المعلوماتية الذي يتحمل التزاماً مستقلاً بحماية ذلك النظام من المخاطر. فشرركات البرمجيات، وشرركات الاستضافة، وشرركات إدارة النظم، تُعد في الأصل شرركات تقنية معلومات، وتخضع لقواعد المسؤولية العقدية العادية عن إخلالها بواجب التنفيذ أو الصيانة، دون أن تفترض مسؤوليتها تلقائياً عن أي اعتداء معلوماتي خارجي، ويؤسس قانون الثقة في الاقتصاد الرقمي لعام 2004 المعدل على أن مزودي الخدمات التقنية (مثل مزودي الاستضافة والبرمجيات) لا يتحملون مسؤولية حماية سيبرانية مستقلة تلقائياً، بل تُقاس مسؤوليتهم ضمن الإطار التعاقدية العام وإخلالهم بالتزامات التنفيذ أو الصيانة، ما لم يثبت علمهم بالمحتوى غير المشروع أو نص آخر يفرض عليه ذلك⁽¹⁾.

أما في العراق، فإن شرركات تقنية المعلومات تعمل في إطار قانون الشرركات وقانون التجارة، وتبرم عقود مقولة أو خدمات مع الزبائن لتطوير الأنظمة أو تشغيلها أو إدارتها. ولم يكن، قبل ظهور تنظيم خاص للأمن السيبراني، ثمة نظام قانوني يفرض عليها التزامات تتعلق بحماية الأمن الرقمي أو إدارة المخاطر السيبرانية، وإنما كانت مسؤوليتها تنحصر في حدود الالتزام التعاقدية الفني الذي قبلته الشركة بموجب العقد المبرم مع الزبون دون أن تمتد إلى أي بعد أمني وقائي.

إن الالتباس بين شرركات تقنية المعلومات وشرركات الأمن السيبراني ينبع في المقام الأول من اشتراك كليتهما في الفضاء الرقمي واستخدام أدوات تقنية متقاربة. فكل من الفئتين قد تتعامل مع الخوادم، والشبكات، ونظم التشغيل، وقواعد البيانات، والبرمجيات، وقد تدخل إلى البنية الرقمية للزبون لإجراء عمليات فنية متعلقة بالنظام. ومن هنا، قد يظن الملاحظ أن الشركة المكلفة بتطوير النظام وتشغيله هي ذاتها الشركة المكلفة بحمايته، غير أن هذا التقاطع يظل محصوراً في مستوى الوسائل،

(1) نصت الفقرة (6) من المادة (6) من قانون الثقة في الاقتصاد الرقمي الفرنسي رقم 575 لعام 2004 المعدل على أن: " لا يخضع الأشخاص المشار إليهم في الفقرتين 1 و 2 لالتزام عام بمراقبة المعلومات التي ينقلونها أو يخزنونها، ولا لالتزام عام بالبحث عن الحقائق أو الظروف التي تكشف عن أنشطة غير قانونية. ولا يخل ما سبق بأي نشاط مراقبة محدد ومؤقت تطلبه السلطة القضائية. "

النص باللغة الفرنسية:

" Les personnes mentionnées aux 1 et 2 ne sont pas soumises à une obligation générale de surveiller les informations qu'elles transmettent ou stockent, ni à une obligation générale de rechercher des faits ou des circonstances révélant des activités illicites. Le précédent alinéa est sans préjudice de toute activité de surveillance ciblée et temporaire demandée par l'autorité judiciaire. "

دون أن يمتد إلى طبيعة الالتزام القانوني أو نطاق المسؤولية لكل فئة. وهذا التقاطع في الأداة دون الالتزام هو مصدر الخلط القانوني الأخطر في هذا المجال، إذ يدفع بعض المتعاقدين إلى افتراض أن الشركة التي طوّرت النظام هي ذاتها المسؤولة عن حمايته، وهو افتراض يفتقر إلى سند قانوني سليم. فشركة تقنية المعلومات تدخل إلى النظام لتُنشئه أو تُشغله أو تُصلحه، وهي بذلك دائن بخدمة تقنية محددة. أما شركة الأمن السيبراني فتدخل إليه لتُحصّنه وتراقبه وتمنع الاعتداء عليه، وهي بذلك ضامن لسلامة النظام في مواجهة التهديدات الخارجية. والفارق بين الدائن بخدمة والضامن للسلامة فارق جوهري في القانون المدني ينعكس مباشرة على طبيعة الالتزام وعبء الإثبات ونطاق التعويض⁽¹⁾.

1. من حيث طبيعة النشاط

تمارس شركات تقنية المعلومات نشاط خدمي وتقني يقتصر في جوهره على تمكين الزبون من استعمال النظام الرقمي أو البنية التحتية الرقمية كما صُممت للعمل. ويشمل ذلك تطوير النظام، تشغيله، صيانتته، وإدارة البرمجيات والشبكات وفق ما تم الاتفاق عليه في العقد⁽²⁾، من دون أن يمتد نشاطها إلى مجال حماية النظام من الهجمات الرقمية أو الوقاية من المخاطر السيبرانية⁽³⁾. فعلى الرغم من أن بعض شركات تقنية المعلومات قد تتخذ إجراءات تقنية للحفاظ على سرية البيانات أو سلامة النظام أثناء التشغيل، فإن هذا النشاط يقتصر على وظيفة تقنية داخلية مماثلة لأمن المعلومات، الذي يركز على سرية وسلامة وتوافر البيانات⁽⁴⁾، من دون أن يشمل حماية البنية الرقمية من الاعتداءات أو المخاطر العدائية.

(1) حازم الشمري، توظيف القوة السيبرانية في استراتيجيات الدول الكبرى، دار انكي للنشر والتوزيع، بغداد، 2022، ص40.

(2) محمد عبد الظاهر حسين، المسؤولية القانونية في مجال شبكات الانترنت، دار النهضة العربية، القاهرة، 2002، ص28.

(3) Paweł Zajac, The Liability of Entities Providing Services by Electronic Means for Digital Content, 2021, P.389.390

(4) يعرف امن المعلومات بأنه: " الحفاظ على سرية المعلومات وسلامتها وتوافرها". ويشير أمن المعلومات، وفقاً لمعهد إسكال للتقنيات المتقدمة (SANS)، المتخصص في تدريب أمن المعلومات والأمن السيبراني، إلى "العمليات والمنهجيات المصممة والمطبقة لحماية المعلومات أو البيانات السرية والخاصة والحساسة، سواء كانت مطبوعة أو إلكترونية أو أي شكل آخر، من الوصول غير المصرح به أو الاستخدام أو سوء الاستخدام أو الإفصاح أو التدمير أو التعديل أو التعطيل". Arina Alexei. Anatolie Alexei, op.cit,p.75-76.

SANS Institute. Information Security Resources. Available online: <https://www.sans.org/information-security> .

في المقابل، تمارس شركات الأمن السيبراني نشاط وقائي وحماي مخصص لتأمين الأنظمة الرقمية والشبكات والبيانات ضد الاعتداءات الرقمية، الاختراقات، والتهديدات السيبرانية، مع رصد مستمر للمخاطر والاستجابة للحوادث الرقمية. وتختلف بذلك عن شركات تقنية المعلومات في وظيفتها الجوهرية؛ فشركة الأمن السيبراني لا تُنشئ النظام بل تحميه، وتعمل في مجال الوقاية الأمنية وإدارة المخاطر. وبذلك يكتسب نشاطها طابع استثنائي وحساس، خصوصاً عند ارتباطه بالبنية التحتية الرقمية الحيوية أو الحساسة، وهو ما ينعكس مباشرة على طبيعة الالتزامات القانوني⁽¹⁾.

2. من حيث طبيعة الالتزام

يقتصر التزام شركة تقنية المعلومات في الأصل على أداء خدمة تقنية وفق الأصول المهنية، مثل تشغيل الأنظمة الرقمية، صيانتها، وتطويرها؛ وذلك باستخدام الوسائل والخبرات الفنية المتاحة⁽²⁾، دون أن تضمن تحقيق نتيجة محددة كالحماية من الهجمات الرقمية أو المخاطر السيبرانية. وبذلك يندرج التزام هذه الشركات ضمن التزام بذل العناية، والذي يقتضي بذل الجهد واجتهاد محترف، بشرط احترام معايير المهنة وعدم الإهمال، دون ضمان تحقيق هدف محدد. في هذا النوع من الالتزامات، لا تكون المسؤولية المدنية للمدين قائمة بمجرد عدم تحقيق الناتج، بل تثار فقط عند ثبوت التقصير في بذل العناية والجهد المهني المطلوب.

ويترتب على هذا التكييف أثر إجرائي بالغ الأهمية، فالمتضرر الذي يرفع دعوى ضد شركة تقنية معلومات بسبب اختراق لحق بنظامه يحمل عبء إثبات أن الشركة قصرت في بذل العناية المهنية المطلوبة، لا أن الاختراق وقع فحسب. وهذا يعني أن وقوع الاختراق ذاته لا يُنشئ قرينة على الإخلال في مواجهة شركة تقنية المعلومات، إذ قد تنتفي مسؤوليتها بإثبات أنها بذلت العناية المهنية الكاملة وأن الاختراق جاء من سبب خارجي لا صلة له بالتزامها التعاقد⁽³⁾.

على النقيض من التزام شركات تقنية المعلومات، يُلزم مزود خدمة الأمن السيبراني بتحقيق مستوى معيّن من الحماية الأمنية على نحو مستمر، يشمل منع الاعتداءات الرقمية، رصد المخاطر،

(1) Devika Sharma. Sandeep Reddy. Hamza Shahid, op.cit, p.49.

(2) Paweł Zajac , op.cit, P.392

(3) C. Warren Axelrod, Using Contracts to Reduce Cybersecurity Risks, CrossTalk July/August 2017,p.28.

الاستجابة للحوادث، والتخفيف من آثارها⁽¹⁾. وهذا الالتزام يقرب طبيعة مسؤوليته من التزام بتحقيق نتيجة، أو على الأقل يكون هجين بين التزام العناية وتحقيق النتيجة باعتبار أن الهدف النهائي (مستوى الأمان المتفق عليه) محدداً في عقد الخدمة والترخيص الذي يخضع له.

فيلاحظ في الالتزام بتحقيق نتيجة، يكون محل الالتزام هو النتيجة المتفق عليها نفسها، بحيث يكفي لقيام المسؤولية المدنية أن لا تتحقق النتيجة المتفق عليها، ما لم يثبت للمدين أن هناك سبباً خارجياً قاهراً حال دون تحقيقها⁽²⁾. وهذا يختلف عن التزام بذل العناية الذي لا يقوم إلزام المسؤول إلا عند الغلط أو التقصير في الجهد المهني. وعلى هذا الأساس، فإن إخلال شركة الأمن السيبراني بعدم تحقيق الحماية المتفق عليها أو التقصير في الاستجابة للمخاطر يمكن أن يؤسس مباشرة للمسؤولية المدنية، لأن الالتزام يتجه نحو تحقيق نتيجة أمنية محددة، وليست مجرد بذل جهود تقنية⁽³⁾.

وتكشف العقود الأمنية المتقدمة عن هذه الحقيقة القانونية بصورة جلية، إذ تتضمن في الغالب بنوداً تحدد مستويات الأداء الأمني المطلوب كمستويات كشف التهديد وزمن الاستجابة ومستوى الوقاية. وهذه البنود لا تُنشئ مجرد التزامات تعاقدية عادية، بل تُحوّل الالتزام من بذل عناية إلى تحقيق نتيجة، بحيث يكفي لقيام المسؤولية المدنية التحقق من أن مستوى الأداء المتفق عليه لم يتحقق دون حاجة إلى إثبات تقصير الشركة. وهذا هو الفارق الإجرائي الحاسم بين الفئتين في دعاوى المسؤولية المدنية: أمام شركة تقنية المعلومات يثبت المدعي التقصير، وأمام شركة الأمن السيبراني يثبت عدم تحقق النتيجة⁽⁴⁾.

أما أثر ذلك على المسؤولية المدنية، فيلاحظ أنّ التمييز بين التزام بذل العناية والتزام تحقيق نتيجة له أثر مباشر على عبء الإثبات ونشوء المسؤولية المدنية، في حالة التزام بذل العناية (كما في شركات تقنية المعلومات)، يجب على المدعي إثبات أن الشركة لم تبذل المستوى المقبول من الجهد المهني، وإلا فلا تقوم مسؤولية مدنية لمجرد عدم تحقق نتيجة معينة. أما في حالة التزام بتحقيق نتيجة (أو التزام يقترب منه)، فيكفي لقيام المسؤولية المدنية أن لا تتحقق النتيجة المتفق عليها، ما لم يثبت

(1) Md Nazrul Islam Khan. Md Soyeb Rabbi, CYBERCRIME, LEGAL ACCOUNTABILITY, AND CONTRACTUAL RISK: A SYSTEMATIC REVIEW OF JURISPRUDENCE AND PROTECTIVE FRAMEWORKS , American Journal of Advanced Technology and Engineering Solutions, Volume 04 Issue 01 (2024),p.73.

(2) د. محمد حسين منصور، المسؤولية الالكترونية، دار الجامعة الجديدة، مصر، 2007، ص71.

(3) احمد هشام فواز العمري، المسؤولية المدنية لمقدمي خدمات الامن السيبراني، أبحاث الدراسات العليا، كلية الحقوق، جامعة المنصورة، مجلد15، عدد35، 2025، ص17.

(4) Md Nazrul Islam Khan. Op.cit, p.73.

المدين وجود سبب قاهر حال بينه وبين تحقيقها، وهو ما يجعل المسؤولية أوسع وأشدّ بالنسبة لشركات الأمن السيبراني مقارنة بشركات تقنية المعلومات.

3. من حيث المركز القانوني

لا يختلف المركز القانوني لشركات الأمن السيبراني، من حيث الأصل، عن المركز القانوني لشركات تقنية المعلومات، فكلاهما أشخاص معنوية خاصة تمارس نشاطها في إطار تعاقدية، وتخضع لقواعد القانون الخاص وقانون الشركات. غير أن هذا التماثل في الإطار الشكلي لا ينفى وجود اختلاف جوهري في الوصف الوظيفي للمركز القانوني داخل العقد. فشركة تقنية المعلومات تشغل مركز مقدّم خدمة تقنية، ينحصر دورها في تنفيذ أعمال فنية متفق عليها⁽¹⁾، ويظل محل التزامها محصور في أداء تقني يمكن تقييمه بمعايير الكفاءة المهنية.

أما شركة الأمن السيبراني، فبرغم احتفاظها بالمركز التعاقدية ذاته من حيث الشكل، فإنها تشغل مركزاً وظيفياً مغايراً، يتمثل في مقدّم خدمة وقائية حمانية، يضع النظام الرقمي محل العقد تحت عهده الأمنية، ويُنَاط به واجب حماية هذا النظام من المخاطر العدائية⁽²⁾. وهذا الاختلاف لا يغيّر من طبيعتها كشركة خاصة، لكنه يُعيد توصيف مركزها القانوني داخل العلاقة التعاقدية بوصفه مركز مشدد للالتزامات.

ويترتب على ذلك أن اختلاف المركز القانوني هنا ليس اختلاف في الطبيعة القانونية، بل في مدى المسؤولية المترتبة على هذا المركز، بحيث تُقاس مسؤولية شركة الأمن السيبراني بمعيار أشدّ يرتبط بحساسية النشاط وطبيعته الوقائية، دون أن يؤدي ذلك إلى إخراجها من دائرة القانون الخاص.

4. من حيث الارتباط بالأمن والنظام العام الرقمي

يمثل اتصال النشاط بالنظام العام أحد أهم المعايير الفاصلة بين شركات تقنية المعلومات وشركات الأمن السيبراني. فنشاط شركات تقنية المعلومات، مهما بلغت أهميته الاقتصادية، يظل موجّهاً إلى تمكين الزبون من تشغيل نظامه أو إدارته، دون أن يترتب عليه، في ذاته، مساس مباشر بالمصالح الجوهرية للمجتمع أو استقرار الفضاء الرقمي، ومن ثم لا يُعد نشاط متصل بالنظام العام، بل يظل محكوم بمنطق التعاقد الخاص وقواعد المسؤولية المدنية التقليدية.

(1) Paweł Zajac , op.cit, P.392

(2) Md Nazrul Islam Khan. Md Soyeb Rabbi, op.cit,p.73.

أما نشاط شركات الأمن السيبراني، فإنه يتجاوز الإطار التعاقدي الفردي ليتصل اتصال مباشر بالنظام العام والمصالح الأساسية المرتبطة بحماية الفضاء السيبراني، واستقرار البنى التحتية الرقمية، وصيانة الثقة في المعاملات الإلكترونية والاقتصاد الرقمي المتداخل مع العناصر المادية والاقتصادية والاجتماعية والسياسية لأي مجتمع⁽¹⁾، فالمساس بهذه المصالح لا يقتصر أثره على طرفي العقد، بل يمتد إلى المجتمع ككل، لما قد يترتب عليه من تعطيل مرافق حيوية، أو تهديد أمن البيانات العامة والخاصة، أو الإخلال باستقرار المعاملات⁽²⁾.

ويترتب على هذا الاتصال أن نشاط شركات الأمن السيبراني، وإن أنجز من خلال أشخاص معنوية خاصة، يُعد من حيث الغاية والوظيفة نشاطاً ذا بعد وقائي ذي طابع سيادي، يبرر إخضاعه لنظام قانوني خاص، ويُفسر تشدد المشرع في تنظيمه والرقابة عليه، قياساً بشركات تقنية المعلومات التي تبقى أنشطتها محصورة في دائرة المصالح الخاصة باختلاف صورها⁽³⁾. وعلى هذا الأساس، فإن اختلاف درجة اتصال النشاط بالنظام العام الرقمي يؤدي إلى اختلاف جوهري في نطاق المسؤولية المدنية، بحيث تُقاس مسؤولية شركات الأمن السيبراني بمعيار أشدّ يرتبط بوظيفتها الوقائية وحماية مصلحة عامة، لا بمجرد إخلال تعاقدية فردي.

وخلاصة ما تقدم أن التمييز بين شركات الأمن السيبراني وشركات تقنية المعلومات ليس مجرد تصنيف أكاديمي بل له أثر قانوني مباشر على ثلاثة مستويات: أولها طبيعة الالتزام ، إذ يختلف بين بذل عناية وتحقيق نتيجة، وثانيها عبء الإثبات ، إذ يختلف بين إثبات التقصير وإثبات عدم تحقق النتيجة، وثالثها نطاق التعويض ، إذ يمتد في شركات الأمن السيبراني ليشمل الأضرار الناجمة عن الاختراق ذاته لا مجرد التقصير في الأداء. وهذه الفوارق الثلاثة هي التي تجعل الخلط بين الفئتين خطأ قانونياً ذا عواقب على مستوى المسؤولية المدنية، لا مجرد تسمية غير دقيقة.

(1) Mariarosaria Taddeo, Is Cybersecurity a Public Good?, Editorial ,Volume 29, pages 349–354, (2019) ,p.350.

(2) ibd.

(3) Kinza yasar, Definition, information technology (IT), 2024, <https://www.techtarget.com/>.

الفرع الثاني

تميز شركات الأمن السيبراني عن مزودي خدمات الحوسبة السحابية

يُعدّ التمييز بين شركات الأمن السيبراني ومزودي خدمات الحوسبة السحابية من أدق الإشكاليات في إطار التكييف القانوني لهذه الكيانات، لا سيما أن العلاقة بينهما ليست علاقة تنافس أو تشابه وظيفي بسيط، بل هي في أحيان كثيرة علاقة تعاون وتكامل تقني، مما يجعل الخلط بينهما أمراً وارداً على صعيد الممارسة القانونية والتعاقدية. فكلهما يعمل في الفضاء الرقمي، وكلهما قد يتعامل مع البيانات والشبكات، وكثيراً ما يُبرم بين الطرفين عقود مشتركة تجمعهما مع الجهة المستفيدة ذاتها. ومع ذلك، فإن الاشتراك في البيئة التقنية لا يعني الاشتراك في الطبيعة القانونية أو في درجة الالتزام أو في نطاق المسؤولية. ولفهم هذا التمييز على النحو الصحيح، يتعين تناوله من خلال أربعة محاور متكاملة: طبيعة النشاط، ثم طبيعة الالتزام وأثره على المسؤولية المدنية، ثم المركز القانوني والرقابي، وأخيراً الموقف من الأمن والنظام العام الرقمي.

أولاً: من حيث طبيعة النشاط

يتمحور نشاط مزود خدمات الحوسبة السحابية حول توفير موارد حوسبية عبر الشبكة، تشمل القدرة التخزينية، والطاقة المعالجة، وخدمات الاتصال والبنية التحتية، وذلك وفق نماذج تقديم متعددة تتراوح بين البنية التحتية والبرمجيات، وقد عرّف المعهد الوطني للمعايير والتقنية الأمريكي (NIST) الحوسبة السحابية بأنها "نموذج لتمكين الوصول الشبكي الملائم وعند الطلب إلى مجموعة مشتركة من موارد الحوسبة القابلة للتكوين والتي يمكن توفيرها وإصدارها بسرعة بأدنى قدر من الإدارة أو تفاعل مزود الخدمة"⁽¹⁾. ويلاحظ بهذا المعنى إن مزود الحوسبة السحابية يقدم أساساً الوعاء التقني الذي تجري فيه العمليات الرقمية، دون أن يكون الأمان بالضرورة محل التزامه الجوهري.

في المقابل، لا يُمثّل نشاط شركة الأمن السيبراني توفيراً للموارد أو البنى التحتية، بل يتمحور حول الحماية والوقاية والاستجابة. فهي تُعنى بمراقبة التهديدات السيبرانية ورصدها، وكشف الاختراقات، وتحليل الثغرات، وإدارة الهوية والوصول، وتأمين قنوات الاتصال⁽²⁾، والفارق الجوهري أن شركة

(1) NIST SP 800-145: Peter Mell & Timothy Grance, "The NIST Definition of Cloud Computing", National Institute of Standards and Technology, Special Publication 800-145, U.S. Department of Commerce, September 2011, p.2.

(2) Guillaume Harry, IAM - Gestion des identités et des accès: Protégez vos systèmes d'information, ENI Editions, 2021, pp. 45-49.



الأمن السيبراني تعمل على حماية ما يجري داخل البيئة التقنية، بينما يعمل مزود الحوسبة السحابية على توفير البيئة التقنية ذاتها. ولهذا التمييز أثر حاسم في تحديد نطاق الالتزام ومن يتحمل تبعة الإخلال به.

وعلى الصعيد العملي، قد يجمع مزود الحوسبة السحابية بعض خدمات الأمن الأساسية ضمن حزمة خدماته، كجدران الحماية وبروتوكولات التشفير وأنظمة منع التطفل، غير أن هذه العناصر تُعدّ استثنائية وإضافية في طبيعتها، وتتنبثق من حاجة تقنية لا من تكليف قانوني مخصص بالحماية الأمنية⁽¹⁾.

ثانياً: من حيث طبيعة الالتزام وأثره على المسؤولية

تتمحور الإشكالية القانونية الكبرى في هذا التمييز حول سؤال محوري: هل يلتزم مزود خدمات الحوسبة السحابية ببذل العناية أم بتحقيق النتيجة؟ والإجابة على هذا السؤال ليست جامدة، إذ تتوقف على مضمون العقد المبرم وطبيعة الخدمة المتفق عليها، فمزود الحوسبة السحابية يلتزم في جوهره بضمان الوصول إلى الموارد الحوسبية وتشغيلها، وهو ما يعبر عنه في عقود الخدمة باتفاقيات مستوى الخدمة (SLA)، التي تُحدد معدلات التوفر والكفاءة التشغيلية المطلوبة. غير أن هذه العقود، في غالبيتها، تُفرّق بوضوح بين مسؤولية المزود عن البنية التحتية التقنية ومسؤولية المستخدم عن أمان بياناته. وقد أرسى اللائحة العامة لحماية البيانات (GDPR) هذا التمييز بصورة صريحة، إذ يُصنّف مزود الخدمة السحابية بحسب الأحوال باعتباره "معالج بيانات" (data processor) "يُلزم باتباع تعليمات المسؤول عن البيانات، لا بضمان الأمن من تلقاء نفسه"⁽²⁾. أما شركة الأمن السيبراني، فهي في موضع مستقل تماماً، إذ تُلزم بتحقيق مستوى معين من الحماية بصرف النظر عن تعليمات المستخدم أو إهماله، وهو ما يُرسّخه نموذج المسؤولية المشتركة السائد في عقود الحوسبة السحابية ذاتها.

وهذا النموذج يكشف بحد ذاته عن جوهر التمييز: في عقود الحوسبة السحابية، تقوم المسؤولية الأمنية على توزيع واضح للمهام، حيث يتولى المزود تأمين البنية التحتية، ويتحمل الزبون مسؤولية تأمين بياناته وتطبيقاته، في حين في عقود الأمن السيبراني، تتمركز المسؤولية في شركة الأمن بوصفها الطرف الاحترافي المكلف حصرياً بالحماية. ولهذا الفارق انعكاس مباشر على عبء الإثبات؛

⁽¹⁾ NIST Cybersecurity Framework v1.1: Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology, Version 1.1, April 16, 2018, pp. 6-8.

⁽²⁾ Regulation (EU) 2016/679 (GDPR), Article 4(8): Definition of "processor"; Article 28: Obligations of processors.



فالمتضرر من إخلال مزود الحوسبة السحابية مُلزم بإثبات الخطأ في أداء الخدمة التقنية المتفق عليها، بينما يكفي المتضرر من إخلال شركة الأمن السيبراني بإثبات تحقق الضرر وعدم تحقق النتيجة الأمنية الموعودة، ليتحول عبء الإثبات نحو الشركة لدرء المسؤولية عبر إثبات السبب الأجنبي، قد أرسّت التشريعات الحديثة هذا الفارق بصورة متزايدة، إذ تفرض التوجيهات الأوروبية، ولا سيما التوجيه NIS2، التزامات محددة على مزودي الخدمات السحابية بوصفهم كياناً رقمياً أساسياً، دون أن تسوّي بينهم وبين شركات الأمن السيبراني التي تخضع لنظام ترخيص وإشراف أكثر تشدداً. كما تُلزم المادة الثالثة والعشرون من ذات التوجيه مزودي الخدمات الرقمية الجوهرية بالإفصاح عن الحوادث الأمنية⁽¹⁾، وهو التزام يُظهر أن هؤلاء المزودين يُحكمون بواجب التبليغ لا بالالتزام ضمان الأمن الشامل.

ثالثاً: من حيث المركز القانوني

في المقابل، تشغل شركة الأمن السيبراني مركزاً قانونياً يمكن توصيفه بأنه "حارس رقمي"، يتولى بموجب عقد أو بموجب القانون مباشرةً حماية الفضاء الرقمي للجهة المستفيدة. وهذا المركز يستوجب بالضرورة رقابة أكثر تشدداً، تشمل شرط الترخيص المسبق، والامتثال للمعايير الأمنية الوطنية والدولية كمعايير NIST ومتطلبات التصديق والاعتماد الصادرة عن جهات كوكالة الوطنية الفرنسية لأمن نظم المعلومات (ANSSI) وأنظمة التحقق من الكفاءة المهنية.⁽²⁾

وعلى الصعيد العراقي، وإن لم يتناول التشريع تاريخياً هذا التمييز بصورة مباشرة، فإن اللائحة رقم 33 لسنة 2025 جاءت لتضع أطراً تنظيمية تستهدف بصفة أساسية الجهات الممارسة لنشاط الأمن السيبراني، في حين يخضع مزودو خدمات الحوسبة السحابية لمنظومة تنظيمية مغايرة تركز على قانون الاتصالات والشركات. وهذا التفريق التشريعي في الرقابة ليس تقنياً بامتياز، بل له مبرراته القانونية العميقة التي تعكس اختلاف درجة الخطر القانوني المصاحب لكل نشاط.

رابعاً: من حيث الموقف من الأمن والنظام العام الرقمي

يتصل نشاط مزود خدمات الحوسبة السحابية بالنظام العام الرقمي بصفة غير مباشرة، من حيث أن انقطاع الخدمة أو تسريب البيانات قد يلحق ضرراً اجتماعياً واقتصادياً واسعاً. غير أن هذا الاتصال يبقى في مستوى الأثر والتداعيات لا على مستوى الوظيفة الأصلية. وقد عكس القانون الكاليفورني

⁽¹⁾ Directive (EU) 2022/2555 (NIS2 Directive), Article 23: Reporting obligations.

⁽²⁾ ANSSI, Référentiel d'exigences applicables aux prestataires de service de confiance qualifiés, v2.0, 2015, Article 14; Décret n° 2015-350 du 27 mars 2015.

لخصوصية المستهلك (CCPA) هذا التصور بتحميل المستخدمين قدراً من المسؤولية عن حماية بياناتهم في البيانات السحابية⁽¹⁾، وهو ما يؤكد أن المزود ليس الضامن الوحيد للأمن.

أما شركة الأمن السيبراني، فتُمثّل في ذاتها خط الدفاع الأول والأساسي عن الأمن الرقمي بوصفه قيمة تعلو على الطرفين المتعاقدين. وقد جرى الفقه القانوني الحديث على توصيف نشاطها بأنه ينطوي على بُعد سيادي وظيفي، إذ أن تأمين الفضاء الرقمي والبنى التحتية الحيوية لا يُفضي إلى مصالح خاصة فحسب، بل يتصل بمنظومة الثقة الرقمية التي يقوم عليها الاقتصاد الحديث والنظام الأمني الوطني. ويُفضي هذا الاتصال إلى نتيجة قانونية بالغة الأهمية، أن خطأ شركة الأمن السيبراني الذي يُفضي إلى حادثة سيبرانية تطلّ بنى تحتية حيوية لا يُقاس وفق معايير الإخلال التعاقدية العادي فحسب، بل قد يرتقي إلى مستوى الخطأ الجسيم ذي الأثر الجمعي.

يتضح مما سبق أن شركة الأمن السيبراني ومزود خدمات الحوسبة السحابية، وإن اشتركا في العمل داخل البيئة الرقمية، يتباينان في كل ما له أثر قانوني: في طبيعة النشاط الذي يمارسه كل منهما، وفي مصدر التزامه ودرجة تشدده، وفي نمط الرقابة التي يخضع لها، وفي صلته بالنظام العام الرقمي. وهذا التمييز ليس ترفاً أكاديمياً، بل هو شرط ضروري لتحديد من يتحمل المسؤولية القانونية عند وقوع الحادثة السيبرانية، وما هو معيار هذه المسؤولية وكيفية إثباتها. ولعل الفقه القانوني المقارن والتشريعات الحديثة يسيران في اتجاه واحد يُرسّخ هذا التمييز ويُضفي عليه طابعاً تنظيمياً متزايد الأهمية.

⁽¹⁾ California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.100 et seq. (2018).



الفصل الثاني

أحكام ممارسة شركات الأمن السيبراني لنشاطها

المبحث الأول : التزامات شركات الأمن السيبراني تجاه العملاء

المبحث الثاني : المسؤولية القانونية لشركات الأمن السيبراني

الفصل الثاني

أحكام ممارسة شركات الأمن السيبراني لنشاطها

مع التوسع المتسارع للأنظمة الرقمية واعتماد المؤسسات والأفراد على الشبكات والبيانات الإلكترونية، برزت شركات الأمن السيبراني كعنصر أساسي لضمان حماية المعلومات وتأمين استمرارية العمل. إلا أن هذه الأهمية العملية لا يقابلها إطار مدني خاص ينظم هذا النشاط، مما يستدعي الاستعانة بالمبادئ العامة للقانون المدني في تحديد الالتزامات القانونية للشركات ومسؤوليتها أمام العملاء والجهات الأخرى.

وتكتسب دراسة هذه الالتزامات ومسؤوليتها أهمية مضاعفة حين ندرك أن الأنظمة القانونية الثلاثة المقارنة تتباين تبايناً جوهرياً في درجة تطورها التشريعي في هذا الشأن، وهو تباين لا يقتصر على الصياغة التشريعية بل يمتد إلى الفلسفة القانونية الكامنة وراء تنظيم هذا النشاط. فالنظام الفرنسي طور إطاراً تنظيمياً متخصصاً تشرف على تطبيقه الوكالة الوطنية لأمن نظم المعلومات، يقوم على معايير تأهيل صارمة ورقابة مستمرة تُشدّد معيار العناية الواجبة في مواجهة مزودي الخدمات الأمنية وترفعه إلى مستوى يقترب من الالتزام بتحقيق نتيجة. في حين يعتمد النظام الأمريكي على تعدد الأطر التنظيمية بحسب القطاعات دون أن يُرسي نظاماً موحداً للمسؤولية المدنية، مما يُفضي إلى تفاوت في معيار المسؤولية بحسب طبيعة القطاع الذي تعمل فيه الشركة. أما النظام العراقي فلا يزال في طور بناء منظومته التشريعية المتخصصة، إذ لم تتجاوز اللائحة التنظيمية رقم 33 لسنة 2025 حدود التنظيم الإداري للنشاط دون أن تُؤسس لنظام مسؤولية مدنية خاص، مما يُلقي على عاتق القواعد العامة للقانون المدني مهمة سد هذا الفراغ بما تحمله من تحديات تتعلق بتحديد طبيعة الالتزام ومعيار الخطأ ونطاق التعويض. وهذا التباين بين الأنظمة الثلاثة هو ما يجعل المنهج المقارن أداة منهجية لا غنى عنها لاستجلاء القواعد الواجبة التطبيق على التزامات شركات الأمن السيبراني ومسؤوليتها المدنية، والوقوف على أوجه القصور التشريعي في النظام العراقي بما يُمكن من تقديم مقترحات تشريعية رصينة تنسجم مع خصوصية القانون المدني العراقي ومتطلبات الواقع الرقمي المتطور.

ولأجل ما تقدم ينقسم هذا الفصل إلى مبحثين، المبحث الأول بعنوان التزامات شركات الأمن السيبراني تجاه العملاء، والمبحث الثاني بعنوان المسؤولية القانونية لشركات الأمن السيبراني.

المبحث الأول

التزامات شركات الأمن السيبراني تجاه العملاء

تكتسب الالتزامات الملقاة على عاتق شركات الأمن السيبراني تجاه عملائها أهمية خاصة، نظراً لطبيعة النشاط الذي ينصب على حماية الأنظمة الرقمية والبيانات، وما يرتبط به من مخاطر جسيمة في حال الإخلال بمستوى الأمان المطلوب. وفي ظل غياب تنظيم مدني خاص، يشكل القانون المدني المرجعية الأساسية لتحديد نطاق هذه الالتزامات، من خلال تطبيق قواعد حسن النية، وحماية المصالح المشروعة، والمسؤولية عن الضرر الناشئ عن الإخلال. وتتحدد هذه الالتزامات في إطار العلاقة التعاقدية التي تربط الشركة بالعميل، بما يفرض تمييزاً بين التزامات جوهرية تمس محل العقد مباشرة، وأخرى مكملّة تهدف إلى تعزيز فعالية الحماية وتحقيق الشفافية في تنفيذ الالتزام. فأما الالتزامات الأساسية، فتتمثل في حماية الأنظمة الرقمية، وضمان سرية البيانات، وتأمين استمرارية العمل، وهي التزامات ترتبط مباشرة بالغرض من التعاقد. وأما الالتزامات الثانوية، فتتعلق بإدارة المخاطر، والكشف عن التهديدات، والإعلام الدوري، وإعداد التقارير الفنية، بما يعكس امتداد الالتزام إلى ما يقتضيه التنفيذ حسن النية.

وعليه، ينقسم هذا المبحث إلى مطلبين: يتناول الأول الالتزامات الأساسية في حماية الأنظمة والبيانات، في حين يخصص الثاني لمبحث الالتزامات الثانوية المرتبطة بإدارة المخاطر والإعلام.

المطلب الأول

الالتزامات الأساسية في حماية الأنظمة والبيانات

تتسم الالتزامات الأساسية لشركات الأمن السيبراني بالحساسية الشديدة، لكونها تمس مباشرة حماية البيانات والأنظمة الرقمية للعميل، وهو ما يترتب عليه أثر مباشر على استمرارية الأعمال وحفظ الحقوق الأساسية للطرف المتعاقد. هذه الالتزامات ليست مجرد واجبات شكلية، بل تمثل جوهر العلاقة التعاقدية بين الشركة والعميل، حيث يكتسب الوفاء بها طابعاً جوهرياً لضمان الثقة والفاعلية في تقديم الخدمات السيبرانية. وتشمل هذه الالتزامات مستويات متعددة من التدابير الوقائية والإجرائية، بحيث يُنظر إلى كل مستوى باعتباره ركناً لا غنى عنه في الحفاظ على الأمن الرقمي، إذ يُشكّل الامتثال لمعايير حماية



الأنظمة الرقمية واستمرارية العمل اللبنة الأولى في بناء منظومة الحماية التعاقدية المنشودة. ولأجل ذلك قُسم هذا المطلب على فرعين: الأول لبحث حماية الأنظمة الرقمية والبيانات، والثاني لمعالجة منع الاختراقات والحفاظ على استمرارية العمل.

الفرع الأول

حماية الأنظمة الرقمية والبيانات

لا يمكن مقارنة التزامات شركات الأمن السيبراني تجاه العملاء دون الوقوف عند الالتزام الذي يشكّل جوهر نشاط هذه الشركات ومبرر وجودها القانوني. هذا الالتزام، المتمثل في حماية الأنظمة الرقمية والبيانات، لا يندرج ضمن الالتزامات التبعية أو الثانوية التي قد تفرضها طبيعة بعض العقود التقنية، بل يتخذ موقع الالتزام الأصلي الذي يقوم عليه البناء العقدي برمته، بحيث يغدو محل العقد ذاته وليس مجرد أثر من آثاره. ومن ثم، فإن تحديد طبيعته القانونية يُعد مسألة محورية، لما يترتب عليه من آثار مباشرة في تكييف العلاقة التعاقدية وتحديد نطاق المسؤولية المدنية الناشئة عن الإخلال به، سواء تعلق الأمر بالضرر الواقع على العملاء مباشرة أو بما قد يلحق بالغير نتيجة الإهمال أو التقصير في الوفاء بهذا الالتزام⁽¹⁾.

يختلف الالتزام بحماية الأنظمة الرقمية والبيانات في عقود الأمن السيبراني عن الالتزامات المتعارف عليها في عقود تقنية المعلومات التقليدية من حيث المضمون والوظيفة. ففي عقود تقنية المعلومات، ينصرف التزام المتعهد إلى إنشاء النظام، تشغيله أو صيانته، بحيث تُعد الحماية مجرد عنصر مكمل يهدف إلى ضمان حسن أداء الخدمة التقنية، دون أن تشكل الغاية الأساسية للعقد⁽²⁾. أما في عقود الأمن السيبراني، فإن الحماية تمثل الغاية الجوهرية التي يستند إليها العقد، فهي الالتزام الأساسي الذي لا يقوم العقد بدونه، ويشمل مراقبة الأنظمة، منع الاختراقات، التخفيف من المخاطر الرقمية، وضمان سلامة البيانات واستمرارية العمل. لهذا، فإن طبيعة هذا الالتزام تجعل إخلال شركة الأمن السيبراني به يؤدي

(1) احمد هشام فواز العمري، المسؤولية المدنية لمقدمي خدمات الامن السيبراني، كلية الحقوق، جامعة المنصورة، 2023-

2024، ص16.

(2) C. Warren Axelrod, op.cit ,p.28.

مباشرة إلى نشوء المسؤولية المدنية، إذ يُقارب الالتزام تحقيق نتيجة محددة، خلافاً لما هو معمول به في عقود التقنية التقليدية حيث يكون الالتزام التعاقدي محصوراً في بذل العناية المهنية⁽¹⁾.

وعليه أن إخلال شركة الأمن السيبراني بواجب حماية الأنظمة والبيانات لا يُعدّ إخلالاً عرضياً أو ثانوياً، وإنما يُمثّل إخلالاً بمحل الالتزام ذاته، بما يؤدي إلى التأثير على التوازن العقدي. وهذا ما يبرر إخضاع هذا الالتزام لمعيار قانوني أكثر تشدداً في تقدير التنفيذ والإخلال، مقارنة بالالتزامات التقنية التقليدية التي تُقاس في الغالب بمعيار العناية المهنية⁽²⁾، وإذا كان هذا الالتزام يجد أساسه الأول في الإرادة العقدية للأطراف، فإن مضمونه لا يُترك لهذه الإرادة على إطلاقها، بل يتحدد في ضوء القواعد العامة التي تحكم تنفيذ الالتزامات، ولا سيما مبدأ حسن النية، الذي يفرض على المدين تنفيذ التزامه بطريقة تحقق الغاية المقصودة من العقد⁽³⁾. وفي هذا السياق، فإن التزام شركة الأمن السيبراني لا يقتصر على اتخاذ تدابير شكلية للحماية، وإنما يمتد إلى تحقيق مستوى فعلي من الأمان يتناسب مع طبيعة النظام محل الحماية، وحجم المخاطر التي تحيط به.

ولفهم كيفية تجسيد هذا الالتزام عملياً، يمكن النظر في النظم القانونية المقارنة، فعلى مستوى القانون الأمريكي، يُستمد الالتزام الأساسي لشركة الأمن السيبراني بحماية الأنظمة الرقمية والبيانات من مجموعة المصادر القانونية والتقنية المترابطة، إذ لا يوجد نص تشريعي صريح يفرض هذا الالتزام بالمفهوم المدني التقليدي، لكن تعريف (الغرض من الأمن السيبراني) ضمن قانون الأمن الداخلي الأمريكي يوضح أن الغاية الأساسية هي حماية نظام المعلومات أو المعلومات المخزنة عليه أو المعالجة بواسطته أو المتداولة فيه من أي تهديد سيبراني أو ثغرة أمنية⁽⁴⁾، هذا التعريف يعكس أن الالتزام بحماية الأنظمة والبيانات يشكّل الالتزام الجوهرية الأساسي لشركة الأمن السيبراني، لا مجرد التزام تابع أو ثانوي، وأن العقد يعكس ان الحماية تمثل الغاية الجوهرية، ويتحدد مضمون هذا الالتزام في القانون الأمريكي من

(1) Alexandre Cruquenaire, "La cybersécurité dans les contrats informatiques: une application fertile de la notion d'obligation essentielle", in *Penser, écrire et interpréter le droit: liber amicorum Xavier Thunis*, Larcier, Bruxelles, 2022, pp. 313-329.

(2) Paweł Zajac , op.cit, P.392

(3) منذر الفضل، الوسيط في شرح القانون المدني، دار ثاراس، أبريل، 2006، ص215. حسام الدين كامل الاهواني، مصادر الالتزام، دار النهضة العربية، مصر، 1991-1992، ص210. محمد دغمان، الزامية العقد، ط2، مجلد1، منشورات زين الحقوقية، 2018، ص80.

(4) تنص المادة (6/650) من قانون الامن الداخلي الأمريكي على ان: " الغرض من الأمن السيبراني، يعني مصطلح "الغرض من الأمن السيبراني" الغرض من حماية نظام المعلومات أو المعلومات المخزنة على نظام المعلومات أو التي تتم معالجتها أو التي تمر عبر نظام المعلومات من تهديدات الأمن السيبراني أو الثغرات الأمنية".

خلال ثلاثة عناصر متكاملة، أولها صون سرية البيانات من أي وصول غير مصرح به، وثانيها ضمان سلامة المعلومات بمعنى منع تعديلها أو تدميرها، وثالثها ضمان توافر النظام واستمرار عمله في مواجهة التهديدات السيبرانية. وتُعرف هذه العناصر الثلاثة في الأدبيات القانونية الأمريكية بمثلث الأمن السيبراني المتمثل في السرية والسلامة والتوافر، وهو المعيار الذي تعتمد المحاكم الأمريكية في تقدير مدى وفاء شركة الأمن السيبراني بالتزامها.

وتتمثل طبيعة هذا الالتزام في واجب الوقاية والتدابير العملية، كما يظهر في تعريف التدابير الدفاعية التي تشمل أي إجراء أو تقنية تطبق للكشف عن تهديد أو ثغرة أمنية، أو منعها، أو التخفيف من آثارها⁽¹⁾، مما يبرز أن الالتزام يمتد إلى تحقيق مستوى محدد وفعلي من الأمان للنظام الرقمي، وليس مجرد بذل عناية شكلية. كما يوضح تعريف مخاطر الأمن السيبراني⁽²⁾، وتهديد الأمن السيبراني⁽³⁾ نطاق المخاطر التي يجب على الشركة مواجهتها، بما في ذلك الوصول غير المصرح به، والتعديل، والتدمير، أو أي فعل عدائي آخر على النظام، مع استثناء الأفعال البسيطة مثل انتهاك شروط خدمة المستهلك. وتتجسد عناصر هذا المثلث الثلاثة عملياً في الالتزامات التعاقدية الملموسة التي يفرضها بند التأمين

(1) تنص المادة (9/650) من قانون الأمن الداخلي الأمريكي على أن: "التدابير الدفاعية (أ) بشكل عام باستثناء ما هو منصوص عليه في الفقرة الفرعية (ب)، يُقصد بمصطلح "التدابير الدفاعية" أي إجراء أو جهاز أو عملية أو توقيع أو تقنية أو أي تدبير آخر يُطبق على نظام معلومات أو معلومات مخزنة عليه أو مُعالجة بواسطته أو عابرة له، وذلك للكشف عن تهديد معروف أو مشتبه به للأمن السيبراني أو ثغرة أمنية، أو منعه أو التخفيف من آثاره. (ب) الاستثناءات لا تشمل مصطلح "التدابير الدفاعية" أي تدبير يُدمر أو يُعطّل أو يُتيح الوصول غير المصرح به إلى نظام معلومات أو معلومات مخزنة عليه أو مُعالجة بواسطته أو عابرة له، أو يلحق بها ضرراً جسيماً، ما لم يكن مملوكاً لـ: (1) الكيان الخاص، كما هو مُعرّف في المادة 1501 من هذا القانون، الذي يُشغل التدبير؛ أو (2) أي كيان آخر أو كيان اتحادي مُخوّل بتقديم الموافقة، وقد قدم موافقته لذلك الكيان الخاص لتشغيل هذا التدبير".

(2) تنص المادة (7/650) من قانون الأمن الداخلي الأمريكي على أن: "مخاطر الأمن السيبراني، يشير مصطلح "مخاطر الأمن السيبراني" إلى: (أ) التهديدات ونقاط الضعف التي تواجه المعلومات أو أنظمة المعلومات، وأي عواقب ناجمة عن الوصول غير المصرح به، أو الاستخدام، أو الإفصاح، أو التدهور، أو التعطيل، أو التعديل، أو التدمير لهذه المعلومات أو أنظمة المعلومات، بما في ذلك العواقب الناجمة عن عمل إرهابي؛ و (ب) لا يشمل أي إجراء ينطوي فقط على انتهاك شروط خدمة المستهلك أو اتفاقية ترخيص المستهلك".

(3) تنص المادة (8/650) من قانون الأمن الداخلي الأمريكي على أن: "تهديدات الأمن السيبراني: (أ) بشكل عام باستثناء ما هو منصوص عليه في الفقرة الفرعية (ب)، يُقصد بمصطلح "تهديدات الأمن السيبراني" أي فعل، غير محمي بموجب التعديل الأول لدستور الولايات المتحدة، على نظام معلومات أو من خلاله، قد يؤدي إلى محاولة غير مصرح بها للتأثير سلباً على أمن نظام المعلومات أو توافره أو سرّيته أو سلامته، أو على المعلومات المخزنة فيه أو التي تتم معالجتها أو التي تمر عبره. (ب) الاستثناءات: لا يشمل مصطلح "تهديدات الأمن السيبراني" أي فعل ينطوي فقط على انتهاك شروط خدمة المستهلك أو اتفاقية ترخيص المستهلك".

الأساسي لأنظمة المعلومات الخاضعة للمتعاقدين على كل متعاقد فيدرالي يتعامل مع أنظمة معلوماتية حكومية، إذ يُحقق عنصر السرية من خلال إلزام المتعاقد بتقييد الوصول إلى نظام المعلومات على المستخدمين المصرّح لهم والتحقق من هويتهم كشرط مسبق للوصول، ويُحقق عنصر السلامة من خلال إلزامه بتعقيم أو إتلاف وسائط المعلومات قبل التخلص منها، وتوفير الحماية من الأكواد الخبيثة وتحديث آلياتها باستمرار⁽¹⁾.

ويُلاحظ أنّ هذا الالتزام هجين بين التزام بذل العناية، والالتزام بتحقيق نتيجة، إذ يُتوقع من شركة الأمن السيبراني أن تتخذ جميع التدابير الفنية المتعارف عليها لضمان حماية النظام، ويُقاس إخلالها بمستوى الأداء المهني المعتمد في القطاع، الذي غالباً ما يُدمج ضمن شروط العقد. ولا يعني وصف هذا الالتزام بالطبيعة المختلطة ترك تكيفه من دون ضابط، بل يقتضي الأمر التمييز بين مرحلتين: مرحلة تنفيذ التدابير الفنية، حيث يظل الالتزام أقرب إلى التزام ببذل عناية مهنية مشددة، ومرحلة تحقق الحماية الفعلية، حيث يقترب من الالتزام بتحقيق نتيجة، متى كان مستوى الأمان قابلاً للتحديد تعاقدياً أو وفقاً للمعايير المهنية المستقرة. ومؤدى ذلك أن القاضي لا يكفي بالتحقق من مباشرة الوسائل، بل يمتد رقابته إلى تقييم مدى كفايتها في تحقيق الغاية الأمنية محل التعاقد.

ويتيح هذا التقييم للقاضي تحديد ما إذا كانت الشركة قد أوفت بالتزاماتها، مع الإقرار بأن إخلال الشركة بعدم تحقيق مستوى الأمان المتفق عليه يمكن أن يُؤسس مباشرة للمسؤولية المدنية، ما لم يكن هناك سبب قاهر خارج عن إرادتها. ومن ثمّ، يصبح الالتزام بحماية الأنظمة الرقمية والبيانات الالتزام الأساسي الذي يقوم عليه عقد خدمات الأمن السيبراني، ويُشكل الإطار الذي تُقاس من خلاله العلاقة التعاقدية ونطاق المسؤولية المدنية، بما يضمن أن الهدف من العقد لا يقتصر على تقديم خدمة تقنية فحسب، بل على تحقيق حالة فعلية ومستمرة من الأمان الرقمي، مما يعكس الطبيعة الجوهرية والحساسة لهذا الالتزام في العقود الأمريكية الخاصة بالأمن السيبراني.

أما في القانون الفرنسي، فإن التزام شركة الأمن السيبراني بحماية الأنظمة الرقمية والبيانات لا يقوم على نص مدني خاص يُفرد له تنظيماً مباشراً، وإنما يتشكل في إطار تفاعل دقيق بين القواعد العامة التي تحكم تنفيذ الالتزامات وبين التنظيمات الخاصة التي تعكس الطبيعة التقنية والحساسة لهذا النشاط.

(1) ينظر البند 52.204-21 الموسوم بـ (التأمين الأساسي لأنظمة المعلومات الخاضعة للمتعاقدين)، الصادر ضمن اللائحة التنظيمية الفيدرالية الأمريكية للمشتريات (FAR)، بصيغته المعدلة في نوفمبر 2021، الفقرة (ب)(1)، البنود المتعلقة بتقييد الوصول والتحقق من الهوية تحقيقاً لعنصر السرية، والبنود المتعلقة بإتلاف وسائط المعلومات والحماية من الأكواد الخبيثة تحقيقاً لعنصر السلامة.

فالقانون المدني الفرنسي الصادر بموجب الأمر رقم 131-2016 المؤرخ في 10 فبراير 2016 المعدّل لقانون العقود والنظام العام للالتزامات والإثبات، وبموجب نص المادة 1104 منه، لا يكفي بإقرار مبدأ حسن النية بوصفه التزاماً سلوكياً مجرداً، بل يمنحه وظيفة إنشائية تحدد مضمون الالتزام ذاته، إذ يفرض على المدين تنفيذ التزامه على نحو يحقق الغاية التي من أجلها أبرم العقد⁽¹⁾. وفي هذا الإطار، لا يُتصور أن يقتصر دور شركة الأمن السيبراني على اتخاذ تدابير شكلية أو جزئية للحماية، ما دام محل التعاقد ينصرف، في جوهره، إلى تأمين النظام المعلوماتي وصون البيانات المرتبطة به من المخاطر التي تهدده.

ويتعرّز هذا المعنى عند النظر إلى التنظيمات الخاصة في مجال أمن نظم المعلومات، حيث يكشف المرسوم المتعلق بتأهيل منتجات وخدمات الأمن السيبراني عن تصور تشريعي واضح لمضمون الحماية المطلوبة، إذ يُعرّف منتج الأمن بأنه كل وسيلة أو برنامج يؤدي وظيفة تسهم في أمن نظم المعلومات، كما يُقر بأن مقدم الخدمة هو من يتولى تقديم خدمات تُسهم في تحقيق هذا الأمن. ولا يقف التنظيم عند حدود التعريف، بل يمتد ليلزم بتحديد أهداف أمنية تتناسب مع طبيعة التهديدات، والتحقق من توافق الوظائف الأمنية مع هذه الأهداف، بما يضمن فعالية الحماية لا مجرد وجودها الشكلي⁽²⁾. وتتجسد هذه المتطلبات الفنية عملياً في الشروط التعاقدية المعتمدة في الصفقات العامة الفرنسية، التي تُلزم مقدّم الخدمة باحترام

(1) نصت المادة (1104) من القانون المدني الفرنسي الصادر بموجب الأمر رقم 131-2016 المؤرخ في 10 فبراير 2016 المعدّل لقانون العقود والنظام العام للالتزامات والإثبات على ما يأتي: "يجب أن يتم بحسن نية كل من التفاوض على العقود إبرامها وتنفيذها".

كذلك ينظر: أيمن إبراهيم العشماوي، مفهوم العقد وتطوره، دراسة مقارنة، دار النهضة العربية، القاهرة، 2002، ص 17. (2) تنص المادة (2) مرسوم رقم 350-2015 المؤرخ في 27 آذار/مارس 2015 المتعلق بتأهيل منتجات الأمن وشروط الخدمة الفرنسي على أن: "يُقَدّم طلب تأهيل منتج أمني إلى الوكالة الوطنية الفرنسية للأمن السيبراني (ANSSI). وتُتيح الوكالة للجمهور إلكترونياً قائمة المستندات المطلوبة مع الطلب، والتي تتضمن وصفاً تفصيلياً للمنتج ووظائفه الأمنية، فضلاً عن الأهداف الأمنية التي يسعى إلى تحقيقها. بعد اكتمال الطلب، تتحقق الوكالة، استناداً إلى المستندات المقدّمة، مما يلي:

1. تحديد الأهداف الأمنية للمنتج بما يتناسب مع التهديدات التي تواجه أمن نظم المعلومات؛
 2. توافق الوظائف الأمنية للمنتج مع الأهداف الأمنية التي يسعى إلى تحقيقها؛
 3. توفر الأجهزة والبرامج وشفراتها المصدرية والوثائق اللازمة لتقييم الوظائف الأمنية للمنتج دون أي قيود.
- عندما ترى الوكالة الوطنية الفرنسية للأمن السيبراني (ANSSI) استيفاء الشروط المذكورة في البنود من 1 إلى 3، تدعو مُقدّم الطلب إلى تقييم الوظائف الأمنية للمنتج للحصول على التأهيل. وإلا، فإنه يُبلغ مقدّم الطلب بالأسباب التي تجعل المنتج غير مؤهل".

سياسات أمن النظم المعلوماتية الخاصة بالمستفيد والخضوع لرقابة وتدقيق أمني مستمر على الوسائل المستخدمة⁽¹⁾.

ومؤدى ذلك أن المشرّع، وإن لم يصغ التزام الحماية في قالب مدني صريح، إلا أنه حدّد مضمونه من خلال ربطه بنتيجة موضوعية تتمثل في تحقيق مستوى من الأمان قابل للتقييم في ضوء طبيعة المخاطر، ويتشكل مضمون هذا الالتزام في القانون الفرنسي من خلال ما تُقرره مرجعيات الوكالة الوطنية لأمن نظم المعلومات من معايير فنية ملزمة تُحدد ما يجب أن تشملته الحماية، إذ تمتد لتشمل تحديد الأهداف الأمنية للنظام محل الحماية، والتحقق من توافق الوظائف الأمنية مع هذه الأهداف، ومراقبة مستوى الحماية بصورة مستمرة. ومؤدى ذلك أنّ مضمون الالتزام لا يتحدد بمجرد الاتفاق العقدي، بل يمتد ليشمل ما تفرضه هذه المرجعيات التقنية من متطلبات موضوعية.

في ضوء ذلك، يتحدد التزام شركة الأمن السيبراني في القانون الفرنسي، بوصفه التزاماً يتجاوز الإطار التقليدي للالتزام ببذل العناية، ذلك أن معيار تنفيذه لا يُقاس بمجرد اتخاذ الوسائل، بل بمدى كفايتها وفعاليتها في تحقيق الغاية الأمنية التي قام عليها العقد. وهو ما يؤدي إلى إخضاع هذا الالتزام لمعيار مشدد، يقترب في مضمونه من الالتزام بتحقيق نتيجة، أو على الأقل من التزام مهني مُعزّز، تتسع فيه دائرة المسؤولية المدنية كلما تعلّق الأمر بمخاطر جسيمة تمس سلامة الأنظمة والبيانات، وبما يعكس الطبيعة الخاصة للنشاط الذي تمارسه شركات الأمن السيبراني⁽²⁾.

أما في القانون العراقي، فإن غياب تنظيم مدني خاص يُفرد التزام الحماية في مجال الأمن السيبراني لا يعني غياب الأساس القانوني له، بل يقتضي استخلاصه في إطار القواعد العامة التي تحكم تنفيذ الالتزامات، والتي تفرض على المدين تنفيذ التزامه بما يتفق مع طبيعته وبحسن نية، على نحو يحقق

⁽¹⁾ تنظر المادة (2) من كراس الشروط والأحكام المبسطة للأمن السيبراني الفرنسي، الجريدة الرسمية رقم 0223 بتاريخ 27 سبتمبر 2018، حيث نصت المادة (2) (سياسات الامن) على ان: "1- يلتزم المرشّحون والمتعاقدون باحترام مقتضيات سياسات أمن النظم المعلوماتية الخاصة بالجهات المستفيدة، متى كانت هذه السياسات قد نُشرت قبل التعاقد. 2- يسري الحكم ذاته على الملاحق التقنية لهذه السياسات متى كانت متاحة بناءً على طلب مُسبّب. 3- يسري المرجع العام للأمن وسياسة أمن نظم المعلومات الخاصة بالدولة على عقود الجهات الخاضعة لهذين النصين، دون حاجة إلى إشارة صريحة لذلك في كراس الشروط".

⁽²⁾ Olivier Iteanu, "Cybersécurité: une obligation de résultat?", disponible sur: <https://www.iteanu.law/en/cybersecurite-une-obligation-de-resultat/>. تاريخ اخر زيارة في

الغاية التي اتجه إليها التعاقد⁽¹⁾. وفي هذا السياق، لا يُفهم الالتزام الواقع على عاتق شركة الأمن السيبراني بوصفه التزاماً فنياً مجرداً، بل باعتباره التزاماً وظيفياً يتحدد مضمونه في ضوء الغاية الجوهرية للعقد، والمتمثلة في تأمين النظام المعلوماتي وحماية البيانات المرتبطة به من المخاطر التي تهدده. ويتعزز هذا الاستخلاص عند النظر إلى التنظيم الخاص الذي استحدثه قرار مجلس المفوضين رقم (33) لسنة 2025، والذي، وإن جاء في إطار تنظيمي، إلا أنه يكشف عن تصور تشريعي واضح لطبيعة النشاط ومضمونه. فقد نصت المادة (2) منه على تعريف "المرخص له" بأنه الجهة المخولة بتقديم خدمات الأمن السيبراني، في حين جاءت المادة (6/رابعاً-2) لتحديد شركات الأمن السيبراني بوصفها تلك التي تتولى حماية الأنظمة والشبكات من الهجمات السيبرانية، وتقديم خدمات تحليل التهديدات ومراقبة الأنظمة. ولا تقف دلالة هذه النصوص عند حد التعريف أو التصنيف، بل تمتد لتحديد جوهر الالتزام الذي ينهض به هذا النوع من الشركات، إذ تُسند إليها صراحة وظيفة الحماية بوصفها الغاية الأساسية لنشاطها، ويتحدد مضمون هذا الالتزام في القانون العراقي من خلال ما أورده المادة (6/رابعاً-2) من قرار مجلس المفوضين رقم (33) لسنة 2025 من وظائف محددة تضطلع بها شركات الأمن السيبراني، تشمل حماية الأنظمة والشبكات من الهجمات السيبرانية، وتقديم خدمات تحليل التهديدات، ومراقبة الأنظمة بصورة مستمرة. وهذه الوظائف الثلاث تُشكّل في مجموعها المضمون الوظيفي للالتزام التعاقدي، بحيث لا يُعدّ الإخلال بأي منها إخلالاً جزئياً، بل إخلالاً بمحل الالتزام ذاته.

ومن ثم، فإن هذا التنظيم، رغم طابعه غير المدني، يُسهم في تحديد مضمون الالتزام التعاقدي، ويؤكد أن الحماية ليست مجرد عنصر ثانوي أو التزام تابع، بل تمثل محل الالتزام ذاته، الأمر الذي يترتب عليه تكييف إخلال الشركة به بوصفه إخلالاً بالالتزام أصلي. وهو ما يفتح المجال لإخضاعه لأحكام المسؤولية العقدية وفق القواعد العامة، لا سيما في ضوء ما يفرضه مبدأ حسن النية من التزام على المدين بأن يحقق من خلال تنفيذه النتيجة التي قصدها المتعاقدان، لا أن يكتفي باتخاذ تدابير شكلية أو غير كافية.

وعلى هذا الأساس، فإن التنظيم الخاص المتمثل باللائحة لا يُنشئ الالتزام من فراغ، بل يكشف عن مضمونه ويوجهه، في حين تتولى القواعد العامة إضفاء الأثر القانوني عليه، لا سيما في مجال المسؤولية العقدية، حيث يُعدّ الإخلال بالحماية المقررة إخلالاً بالالتزام أصلي يُقاس في ضوء الغاية التي حددها كل من العقد والتنظيم معاً.

(1) السيد بدوي، نحو نظرية عامة لمبدأ حسن النية في المعاملات المدنية، أطروحة دكتوراة، كلية الحقوق، جامعة القاهرة، 1989، ص73.

وفي ضوء ذلك، يتحدد التزام شركة الأمن السيبراني في القانون العراقي ، بوصفه التزاماً يتجاوز الإطار التقليدي للالتزام ببذل العناية، ذلك أن معيار تنفيذه لا يُقاس بمجرد مباشرة الوسائل، بل بمدى كفايتها في تحقيق الحماية الفعلية التي يقوم عليها العقد. وهو ما يبرر إخضاع هذا الالتزام لمعيار مشدد في تقدير التنفيذ والإخلال، ويقربه – بحسب ظروف كل حالة – من نموذج الالتزام بتحقيق نتيجة، أو على الأقل من التزام مهني معزز، تتسع فيه دائرة المسؤولية المدنية كلما ثبت عدم تحقق مستوى الأمان الذي يُفترض أن توفره شركة متخصصة في هذا المجال

ولا يقف نطاق هذا الالتزام عند حد توفير وسائل تقنية للحماية، بل يمتد ليشمل مجموعة متكاملة من الوظائف التي تهدف إلى تحقيق حالة مستمرة من الأمان، بما في ذلك تأمين الأنظمة ضد الاختراق، حماية البيانات من الوصول غير المشروع، مراقبة الأنشطة غير الطبيعية، وضمان استمرارية عمل النظام في مواجهة المخاطر المحتملة⁽¹⁾. ومن ثم، فإن محل الالتزام لا يتمثل في عمل محدد أو إجراء منفرد، بل في حالة قانونية مستمرة تُقاس بمدى تحقق مستوى ملائم من الأمان للنظام.

ويترتب على هذا التكييف أثر مباشر في مجال المسؤولية المدنية، إذ لا يُشترط لقيام مسؤولية شركة الأمن السيبراني إثبات خطأ تقني محدد بقدر ما يكفي إثبات عدم تحقق مستوى الحماية المتفق عليه أو المفترض مهنيًا، ما لم تثبت الشركة وجود سبب أجنبي لا يد لها فيه. ومؤدى ذلك انتقال عبء الإثبات عملياً إلى عاتق الشركة، التي تلتزم بإثبات أنها اتخذت من التدابير ما يكفي لتحقيق الغاية الأمنية، وهو ما يعكس تشديداً واضحاً في نطاق مسؤوليتها مقارنة بالالتزامات التقنية التقليدية.

⁽¹⁾Devika Sharma, Sandeep Reddy, Hamza Shahid, "Cybersecurity Obligations for Critical Infrastructure: Emerging Legal Norms, Enforcement Gaps, and Governance Challenges", Legal Studies in Digital Age, Vol. 2, No. 3, 2023, pp. 49–63.

الفرع الثاني

منع الاختراقات والحفاظ على استمرارية العمل

ينطلق الالتزام بمنع الاختراقات والحفاظ على استمرارية العمل في عقود الأمن السيبراني من حقيقة أن الهدف من هذه العقود لا يقتصر على اتخاذ التدابير الوقائية تجاه المخاطر السيبرانية، بل يمتد إلى ضمان قدرة النظام الرقمي على الاستمرار في أداء وظائفه الأساسية في مواجهة التهديدات التي تستهدف توافره، وهو عنصر جوهري في مفهوم الأمن السيبراني ذاته، ويتميز هذا الالتزام عن الالتزام السابق في الفرع الأول تمايزاً جوهرياً؛ إذ لا يقتصر على اتخاذ التدابير الوقائية قبل وقوع الاختراق، بل يمتد ليشمل ثلاثة عناصر متكاملة، أولها الاستجابة الفورية للحوادث السيبرانية، وثانيها احتواء أثر الاختراق ومنع انتشاره، وثالثها ضمان التعافي واستعادة النظام إلى حالة التشغيل الطبيعية في مدة معقولة. وهذه العناصر الثلاثة مجتمعة هي التي تُشكّل مضمون الالتزام باستمرارية العمل بالمفهوم القانوني الدقيق.

إن النصوص القانونية في النظام الأمريكي، بخاصة ما ورد في تعريف تهديدات الأمن السيبراني في النظام الأمريكي الذي يشمل الأفعال التي قد تؤثر سلباً ليس فقط على سرية وسلامة المعلومات، وإنما أيضاً على توافر النظام، تؤكد أن الإضرار بقدرة النظام على الاستمرار في العمل يشكل جزءاً من المخاطر التي تستدعي تدخل شركة الأمن السيبراني⁽¹⁾، ومن ثم يمكن استنباط أن التزام الاستمرارية ينبع من وظيفة الحماية نفسها، إذ لا معنى للحماية المتوخاة إذا لم يمتد أثرها إلى ضمان استمرارية الأداء في مواجهة المخاطر المحققة أو المحتملة. ويتعين أن لا يُفهم هذا الالتزام باعتباره مجرد التزام تقني، بل باعتباره التزاماً مدنياً يرتبط ارتباطاً وثيقاً بمحل العقد وغاية المتعاقدين⁽²⁾، بحيث لا يقتصر التزام الشركة على منع وقوع الخطر، وإنما يمتد إلى ضمان أن يظل النظام قابلاً للاستعمال والتشغيل رغم تقلبات الخطر السيبراني.

وفي هذا السياق، يظهر الالتزام الأمريكي في ضوء ما تتبناه المعايير المهنية والتوجيهات التنظيمية القائمة، إذ أن غياب نص تشريعي اتحادي صريح لا يحول دون استخلاص هذا الالتزام ضمن نطاق الالتزام المدني، خاصة عندما يُنظر إلى المعايير المقبولة في هذا المجال⁽³⁾، مثل المعايير المتضمنة في إطار عمل الأمن السيبراني الصادر عن المعهد الوطني للمعايير والتقنية (NIST)، الذي يتضمن ضمن

(1) المادة (8) من قانون الامن الداخلي الأمريكي.

(2) علي مُحَيِّي الدين القرّة داغي، مبدا الرضا في العقود، ج1، ط3، دار البشائر، 2008، ص91.

(3) Jeff Kosseff, Defining Cybersecurity Law, Vol. 103:985 , 2018 , p.988.

وظائفه الأساسية مرحلة الاستجابة ومرحلة التعافي⁽¹⁾. تعمل هذه المراحل على وضع دلالة مهنية واضحة لمدى وجوب ضمان استمرار الأداء التشغيلي عقب وقوع حوادث سيبرانية، ولا يمكن اعتبارها مجرد توصيات فنية ضمنية فقط، بل تمثل معياراً فعلياً يمكن للقاضي أن يستقي منه معياراً لتقييم ما إذا كانت شركة الأمن السيبراني قد أوفت بالتزاماتها التعاقدية فيما يتعلق بضمان استمرارية العمل، وتكتسب مرحلتا الاستجابة والتعافي في إطار عمل المعهد الوطني أهمية قانونية بالغة، إذ تُحدد معياراً موضوعياً لما يجب أن تُنجزه الشركة بعد وقوع الحادثة لا قبلها، وهو ما يُميز الالتزام باستمرارية العمل عن مجرد الالتزام بالوقاية، ويرتب في حال الإخلال به مسؤولية مستقلة لا تندرج تحت مسؤولية الإخلال بالتدابير الوقائية، بالنظر إلى أن التأثير على التوافر يعتبر من المخاطر الواقعة في صلب مفهوم الأمن السيبراني الأمريكي، وهو توجه جديد نحو توسيع نطاق ما يعد (أداء معقول) في تنفيذ الالتزامات⁽²⁾. ويترجم هذا الإطار المهني نفسه إلى التزامات تعاقدية إلزامية يفرضها بند التأمين الأساسي لأنظمة المعلومات الخاضعة للمتعاقد، الذي يُلزم المتعاقد بمراقبة الاتصالات التنظيمية وحمايتها عند الحدود الخارجية والداخلية لنظام المعلومات، وتحديد ثغرات النظام والإبلاغ عنها وتصحيحها في الوقت المناسب، وبإجراء فحوصات دورية للنظام وفحوصات فورية للملفات الواردة من مصادر خارجية، بما يضمن استمرارية الأداء التشغيلي عقب وقوع الحادثة السيبرانية⁽³⁾، ومن ثم، فإن إخلال الشركة بعجزها عن استعادة النظام أو الحفاظ على وظائفه الحيوية بعد وقوع الخطر، يمكن أن يؤسس لإخلال بالتزامه الأساسي المتصل بتوافر واستمرارية النظام، ما لم تثبت الأسباب الخارجية عن إرادتها.

(1) The NIST Cybersecurity Framework (CSF) 2.0, NIST CSWP 29 , 2024 ,p.5.

(2) Md Nazrul Islam Khan¹;Debashish Goswami, CYBERCRIME AND CONTRACTUAL LIABILITY: A SYSTEMATIC REVIEW OF LEGAL PRECEDENTS AND RISK MITIGATION FRAMEWORKS, Journal of Sustainable Development and Policy, Volume 01, Issue 01(2025) ,p.5.

كذلك يُنظر في الالتزامات القانونية لشركات الأمن السيبراني وما يترتب على الإخلال بها من مسؤولية مدنية وتنظيمية مستقلة:

Isaac Ijuo, Chizoba Okonkwo, Chinenye Umekwe, Ajibola Yusuff, Julius Samson, Cybersecurity Law: Individual Rights, Corporate Liability, Compliance, and Operational Resilience, ResearchGate, 2025, pp. 1–17, available at: <https://www.researchgate.net>. تاريخ آخر زيارة في 2026/6/14

(3) ينظر البند 204.52–21 الموسوم بـ (التأمين الأساسي لأنظمة المعلومات الخاضعة للمتعاقد)، الفقرة (ب)(1)، البنود المتعلقة بمراقبة الاتصالات وتصحيح الثغرات والفحص الدوري تحقيقاً لعنصر التوافر واستمرارية الأداء.

أما في السياق القانوني الفرنسي، فإن الالتزام بمنع الاختراقات والحفاظ على استمرارية العمل يتفاعل مع المبادئ العامة للقانون المدني، ولاسيما الالتزام بحسن النية في تنفيذ العقود كما نصت عليه المادة 1104 من القانون المدني الفرنسي. يتطلب حسن النية تنفيذ الالتزام بطريقة تحقق الغاية المقصودة من التعاقد، ولا يقتصر ذلك على القيام بإجراءات شكلية، بل يشمل ضمان فعالية الأداء والتشغيل المتواصل للنظام المعلوماتي. تتعزز هذه القاعدة العامة من خلال التنظيمات الخاصة بالأمن السيبراني، سواء على المستوى الوطني أو في سياق تطبيق توجيهات الاتحاد الأوروبي مثل توجيه NIS2⁽¹⁾، الذي يضع على عاتق مزودي الخدمات الرقمية التزامات ملموسة تتعلق بكيفية إدارة المخاطر، والكشف عن التهديدات، ومتابعة الحوادث، وإعادة النظام إلى حالة التشغيل بعد وقوع الخطر⁽²⁾. ويترجم هذا التوجيه التنظيمي عملياً إلى شروط تعاقدية محددة تلزم مزود الخدمة بالحفاظ على الحالة الأمنية للأنظمة وتحديثها بصفة دائمة، وبالإبلاغ الفوري عن أي ثغرة أمنية تُكتشف خلال تنفيذ العقد⁽³⁾.

تكشف هذه التوجيهات، التي تُفهم كمصدر تنظيمي مؤثر في النظام القانوني الفرنسي، عن تصور يشترط ليس فقط اتخاذ التدابير المادية لمواجهة الاختراقات، بل تحقيق مستوى من الاستمرارية يضمن أن يظل النظام في حالة تشغيلية، بعيداً عن التعطل أو الانقطاع. وعلى هذا الأساس، يمكن للقاضي الفرنسي أن يقيّم إخلال شركة الأمن السيبراني وفق معيار يتجاوز مجرد بذل العناية المهنية التقليدية، ليمتد إلى

(1) صدر توجيه يُعرف باسم NIS2 في الاتحاد الأوروبي أواخر عام 2022. ويتناول هذا التوجيه بشكل خاص البنى التحتية الحيوية الأوروبية، موسعاً نطاقها بشكل كبير مقارنةً بتوجيه سابق كان يقتصر على اعتبار قطاعي الطاقة والنقل قطاعات حيوية. ويركز التوجيه على الأمن السيبراني للبنى التحتية الحيوية.

Jukka Ruohonenra, A Systematic Literature Review on the NIS2 Directive, a University of Southern Denmark, Sønderborg, Denmark, arXiv:2412.08084v1 [cs.CR] 11 Dec 2024, p.1.

كذلك يُنظر في توجيه الأمن السيبراني الأوروبي الثاني الذي يلزم مزودي الخدمات الرقمية باتخاذ تدابير متكاملة لإدارة المخاطر تشمل منع الحوادث والاستجابة لها وضمان استمرارية الخدمات وإعادة تشغيل الأنظمة عقب وقوع الحوادث:

Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (directive SRI 2), JOUE, L333, 27 décembre 2022, considérant (1) et article 21, disponible sur: <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32022L2555>. تاريخ اخر زيارة في 2026/6/14.

(2) Jukka Ruohonenra, A Systematic Literature Review on the NIS2 Directive, op.cit. p.9

(3) تنظر المواد (5) و (6) من كراس الشروط والأحكام المبسطة للأمن السيبراني الفرنسي.

تقييم ما إذا كانت الإجراءات المتخذة قد أفضت فعلاً إلى تحقيق مستوى من الاستمرارية يتناسب وطبيعة المخاطر المستهدفة والغايات العقدية المتوخاة.

في النظام العراقي، وعلى الرغم من غياب نص مدني صريح يعالج التزامات منع الاختراقات واستمرارية العمل بشكل مفصل، فإن الإطار التنظيمي الخاص بشركات الأمن السيبراني، كما يتجلى في قرار مجلس المفوضين رقم (33) لسنة 2025، يقدم أساساً عملياً لتحديد مضمون هذا الالتزام في سياق القواعد العامة للعقد المدني. فالتعريفات الواردة في هذا القرار لشركات الأمن السيبراني بوصفها الجهات المخولة بحماية الأنظمة والشبكات وتحليل التهديدات ومراقبة الأنظمة، لا تكتفي بالإشارة إلى وظيفة الوقاية فحسب، بل تلمّح إلى نشاط مستمر يتطلب متابعة نفسية للأداء ومنع حالات الانقطاع والتعطيل، وهو الأمر الذي يرتبط بمدى قدرة النظام على الاستمرار في العمل.

وتفرض قواعد تنفيذ الالتزامات بمقتضى القانون المدني العراقي، وخاصة مبدأ حسن النية، على الشركة ألا تكتفي باتخاذ تدابير شكلية أو ناقصة، بل أن تعمل على تحقيق الغاية الأساسية للعقد، والتي لا يمكن تصورها بدون عنصر من الاستمرارية في الأداء الوظيفي للنظام. وفي حال فشل النظام في الاستجابة للتهديدات أو توقفه عن أداء وظائفه الأساسية نتيجة إخفاق التدابير المتخذة، يمكن اعتبار ذلك إخلالاً بالالتزام أصيل يستوجب المسؤولية المدنية، نظراً لارتباطه الوثيق بالغاية العقدية الأساسية وتحقيق الانتفاع المتفق عليه.

ويلاحظ أن الالتزام بمنع الاختراقات والحفاظ على استمرارية العمل، وإن اختلفت صياغاته التشريعية والتنظيمية، يتحدد في جوهره باعتباره امتداداً جوهرياً للالتزام بالحماية، يرتبط بوجود حالة تشغيلية مستمرة للنظام المعلوماتي. ففي الولايات المتحدة، يتعين على شركة الأمن السيبراني أن تستند إلى ما هو معترف به من معايير مهنية وتقنية لتضمن استمرارية التوفر، وفي فرنسا يمتد التزام حسن النية في التنفيذ ليشمل ضمان فعالية الأداء التشغيلي، مدعوماً بتنظيمات تؤكد على وجوب تحقيق مستوى من استمرارية الخدمات، ويلاحظ أن الإطار العراقي يفقر إلى نص صريح يُحدد المدة الزمنية الواجبة للاستجابة وإعادة تشغيل النظام، مما يترك للقاضي المدني سلطة تقديرية واسعة في تحديد معيار المعقولية وفق ظروف كل حالة⁽¹⁾. وهذا الفراغ التشريعي يُعدّ من أبرز القصور في المنظومة التنظيمية العراقية

(1) ينصرف مفهوم المعقولية الى توصيف الأفعال ومدى انسجامها مع التصرف الحكيم وملائمته وفقاً للظروف الزمانية والمكانية، فهو الميزان المتكفل بتوجيه التصرفات. لتفاصيل أكثر عن المعقولية يراجع: فارس حامد عبد الكريم، المعيار القانوني، ط1، بلا دار ومكان نشر، 2009، ص99. كذلك ينظر: هديل خضير كاظم البديري، المعقولية في الالتزام العقدي، دراسة مقارنة، رسالة ماجستير، كلية القانون، جامعة كربلاء، 2018، ص18.

المتعلقة بالأمن السيبراني، ويستدعي تدخلاً تشريعياً صريحاً لتحديد معايير موضوعية للاستجابة والتعافي على غرار ما أرسته المعايير الأمريكية وما كرّسه توجيه NIS2 الأوروبي.

المطلب الثاني

الالتزامات الثانوية في الإفصاح والامتثال

تشير الالتزامات المتعلقة بالإفصاح والامتثال في عقود الأمن السيبراني مسألة تحديد موقعها ضمن البناء العقدي، لتمييزها عن الالتزامات التي تنصب مباشرة على تحقيق الحماية التقنية. فهي لا تتجه إلى إنشاء الحماية بذاتها، وإنما تتصل بتنظيم تنفيذها وتمكين العميل من الإحاطة بالمخاطر المرتبطة بها. ولا يُقصد بوصف هذه الالتزامات بالثانوية التقليل من شأنها، وإنما الإشارة إلى أنها لا تنصب على محل الأداء الأصلي، بل تُعد من الالتزامات المرافقة لتنفيذ العقد، والتي تفرضها طبيعته ومقتضياته. وتبرز أهميتها في كونها تلازم تنفيذ الالتزام الأصلي، إذ يمتد دور شركة الأمن السيبراني إلى إعلام العميل بالمخاطر ومتابعة مستوى الأداء الأمني، فضلاً عما تفرضه متطلبات الامتثال من التزامات بالإفصاح والمتابعة. وعلى هذا الأساس، يُقسّم هذا المطلب إلى فرعين: يتناول الأول الالتزام بالإفصاح عن المخاطر السيبرانية، ويُخصّص الثاني لبيان الالتزام بإعداد التقارير الدورية وما يرتبط به من متطلبات الامتثال.

الفرع الأول

الالتزام بالإفصاح عن المخاطر السيبرانية

يشكل الالتزام بالإفصاح عن المخاطر السيبرانية في عقود شركات الأمن السيبراني أداة أساسية لضمان تنفيذ الالتزام الرئيس المتمثل في حماية الأنظمة والبيانات. فالالتزام هنا ثانوي من حيث طبيعة النشاط، بمعنى أنه لا يخلق حماية مباشرة، ولكنه يُعد شرط ضروري لضمان أن التدابير الوقائية المتخذة تحقق الغاية العقدية المنشودة⁽¹⁾. ومن هذا المنطلق، يصبح الإفصاح وسيلة تمكّن الطرف المتعاقد من الإحاطة بالمخاطر، وتقييمها، والتصرف بطريقة تقلل من احتمالات وقوع الضرر، سواء على بياناته أو

(1) خالد جمال احمد حسن، الالتزام بالإعلام قبل التعاقد، دراسة مقارنة، دار النهضة العربية، القاهرة، 1996، ص259.

على مصالح الغير المرتبطة بالنظام، ما يرسخ مبدأ حسن النية في تنفيذ الالتزامات ويعكس روح التوازن التعاقدية⁽¹⁾.

في الولايات المتحدة، ينشأ الالتزام بالإفصاح في عقود شركات الأمن السيبراني عن تلاقي مبادئ القانون العام للعقود مع التزامات خاصة منصوص عليها في التشريعات المتعلقة بالأمن القومي والبنية التحتية الحيوية. ويجد هذا الالتزام أساسه القانوني في نظرية التفاوت المعلوماتي، إذ تمتلك شركة الأمن السيبراني معرفة فنية متخصصة لا يستطيع العميل الوصول إليها أو تقييمها بوسائله العادية، مما يُنشئ في جانبها التزاماً بالإفصاح عن كل ما من شأنه التأثير على قراره في إدارة المخاطر المرتبطة بأنظمتها. ومن حيث المبادئ العامة، يُستند هذا الالتزام على مبدأ حسن النية الذي يُلزم كل طرف بتنفيذ التزاماته العقدية بما يحقق الغاية الأساسية للعقد ويضمن حماية مصالح الطرف الآخر، حيث نصت المادة (205) على أن: "يفرض كل عقد على كل طرف واجب حسن النية والتعامل العادل في تنفيذه وإنفاذه"⁽²⁾، وهو ما يمكن اعتباره قاعدة عامة تحكم العلاقة بين مزود الخدمة وعميله. وبموجب هذا الإطار العام، يصبح من مسؤولية شركة الأمن السيبراني الإفصاح عن المخاطر الجوهرية المرتبطة بأنظمتها، بما يتيح للطرف المتعاقد اتخاذ التدابير الوقائية الملائمة لتقليل احتمال وقوع أضرار مادية أو معنوية.

على صعيد القوانين الخاصة، تنص المادة 13 من قانون الأمن الداخلي على إنشاء ما يُعرف بـ "منظمة تبادل وتحليل المعلومات" التي تهدف إلى جمع وتحليل معلومات البنية التحتية الحيوية، بما في ذلك مخاطر وحوادث الأمن السيبراني، والتواصل أو الإفصاح عنها للجهات المعنية، سواء لأغراض الوقاية أو اكتشاف المخاطر أو التخفيف من أثارها، أو حتى النشر الطوعي للأعضاء والحكومات المعنية⁽³⁾. ويكشف هذا الموقف عن طبيعة الالتزام بالإفصاح في سياق الأمن السيبراني، التي تتجاوز

(1) عبد القادر الاقصاوي، الالتزام بضمان السلامة في العقود، ط1، دار الفكر العربي، مصر، 2010، ص185. زاهية حورية سي يوسف، المسؤولية المدنية للمنتج، دار هومه للطباعة والنشر، الجزائر، 2009، ص137.

(2) النص باللغة الإنجليزية:

Every contract imposes upon each party a duty of good faith and fair dealing in its performance and its enforcement.

(3) نصت المادة (13) من قانون الامن الداخلي الأمريكي على ان: " منظمة تبادل وتحليل المعلومات: يُقصد بمصطلح "منظمة تبادل وتحليل المعلومات" أي كيان أو جهة تعاون رسمية أو غير رسمية تُنشئها أو تستخدمها مؤسسات القطاعين العام والخاص، لأغراض الآتية:

(أ) جمع وتحليل معلومات البنية التحتية الحيوية، بما في ذلك المعلومات المتعلقة بمخاطر وحوادث الأمن السيبراني، بهدف فهم أفضل لمشاكل الأمن والترابطات المتعلقة بالبنية التحتية الحيوية، بما في ذلك مخاطر وحوادث الأمن السيبراني، والأنظمة المحمية، وذلك لضمان توافرها وسلامتها وموثوقيتها؛

مجرد إعلام العميل، لتشمل الإبلاغ للجهات الرسمية والرقابية بما يحقق توازنًا بين حماية الأنظمة، الالتزام القانوني تجاه الدولة، وحقوق الأطراف المتعاقدة.

ويلاحظ أن الالتزام بالإفصاح له أهمية خاصة عند دمجها مع المبادئ العامة للعقد، إذ يُظهر أن الإفصاح ليس مجرد واجب شكلي، بل آلية لضمان فعالية الالتزام الأساسي بحماية الأنظمة والبيانات. فالالتزام العام يفرض على الشركات تقديم المعلومات الجوهرية للطرف المتعاقد، بما يعكس حسن النية ويحقق التوازن بين الحقوق والالتزامات⁽¹⁾، بينما تضع القوانين الخاصة حدودًا دقيقة لطبيعة الإفصاح ومجاله، خصوصًا عند التعامل مع معلومات حساسة تتعلق بالبنية التحتية الحيوية والأمن القومي. وهكذا، فإن أي إخلال بالإفصاح، سواء تجاه العميل أو تجاه الجهات الرسمية، قد يُعد إخلالًا جزئيًا أو كليًا بالالتزام الأساسي للشركة، ويؤدي إلى تحميلها المسؤولية التعاقدية أو التقصيرية.

ويترتب على هذا النهج أثر ملموس على تحديد نطاق المسؤولية، حيث يُقاس الأداء ليس على أساس الإجراءات الشكلية فحسب، بل على مدى فعالية المعلومات المقدمة ومدى قدرتها على تمكين العميل من حماية مصالحه. وهذا يعكس فهمًا متقدمًا للالتزام بالإفصاح باعتباره عنصرًا أساسيًا لتحقيق الغاية العقدية، ويبرز التفاعل بين الالتزام العام بالقانون المدني والالتزامات الخاصة المنصوص عليها في التشريعات الأمريكية للأمن السيبراني، بما يشكل معيارًا متينًا لتقييم الالتزام ومسؤولية الشركة في حال الإخلال.

وفي القانون الفرنسي، يُستند الالتزام بالإفصاح في عقود شركات الأمن السيبراني إلى مبدأ حسن النية في تنفيذ العقد المنصوص عليه في المادة 1104 من القانون المدني، والذي يلزم الأطراف بتنفيذ التزاماتهم بما يتوافق مع الغرض الأساسي للعقد ويحقق التوازن بين حقوقهم وواجباتهم. ويمثل هذا المبدأ الإطار العام الذي يحدد مسؤولية مزود الخدمة في تقديم المعلومات الجوهرية للطرف المتعاقد حول المخاطر المرتبطة بالأنظمة الرقمية، بما يمكنه من اتخاذ التدابير الوقائية اللازمة، وضمان فعالية التدابير

(ب) التواصل أو الإفصاح عن معلومات البنية التحتية الحيوية، بما في ذلك مخاطر وحوادث الأمن السيبراني، للمساعدة في منع أو اكتشاف أو تخفيف أو التعافي من آثار أي تدخل أو اختراق أو خلل يتعلق بالبنية التحتية الحيوية، بما في ذلك مخاطر وحوادث الأمن السيبراني، أو الأنظمة المحمية. و

(ج) نشر معلومات البنية التحتية الحيوية طواعية، بما في ذلك مخاطر وحوادث الأمن السيبراني، لأعضائها، وحكومات الولايات والحكومات المحلية والفيدرالية، أو أي كيانات أخرى قد تساعد في تنفيذ الأغراض المحددة في الفقرتين الفرعيتين (أ) و(ب)."

(1) د. عبد المنعم فرج صدة، أحكام الالتزام، شركة مكتبة و مطبعة مصطفى البابي الحلبي و أولاده، دون مكان نشر، 1965، ص4 وما بعدها.

الأمنية التي تمثل الالتزام الأساسي للشركة، ويجد هذا الالتزام تعزيزاً إضافياً في نظرية الالتزام بالإعلام التي استقر عليها الفقه الفرنسي، والتي تُقرر أن كل طرف يمتلك معلومات جوهرية يجهلها الطرف الآخر ملزم بالإفصاح عنها متى كانت ذات أثر حاسم في قرار التعاقد أو في تنفيذه.

وعلى صعيد الالتزامات الخاصة، نصت المادة 15 من المرسوم المتعلق بتأهيل منتجات الأمن وشروط الخدمة والمعدلة بموجب المرسوم رقم 1139-2019 على وجوب إفصاح مزود الخدمة للوكالة الوطنية الفرنسية لأمن المعلومات فوراً عن أي تغيير في ظروف التأهيل، وبين المرسوم أنه في حال مخالفة الشروط أو التحفظات أو تغيير الظروف القانونية أو الواقعية، يحق للوكالة تعليق التأهيل أو إلغاؤه بعد إتاحة الفرصة لمزود الخدمة لعرض ملاحظاته⁽¹⁾. ويشير النص إلى ازدواجية وظيفة الإفصاح، فهو يضمن شفافية مزود الخدمة تجاه الجهات الرسمية ويتيح الرقابة على مدى امتثالها، وفي الوقت نفسه يعكس أهمية الالتزام تجاه العملاء، حيث أن أي قصور في الإفصاح قد يؤدي إلى إخلال فعلي بحماية بياناتهم أو بمصالحهم، ما يجعل الإفصاح جزءاً من تنفيذ الالتزام الأساسي. ويتكامل هذا الالتزام التنظيمي مع ما تفرضه الشروط التعاقدية النموذجية في الصفقات العامة الفرنسية من واجب إبلاغ فوري عن أي ثغرة أو خرق أمني، عبر قنوات إعلام مخصصة لا تُمزج بالتدفقات التجارية، وتسجيل هذه الثغرات لدى السلطات المختصة وفق آجال محددة⁽²⁾.

وينبغي ملاحظة أن الالتزام بالإفصاح في فرنسا يتوزع على مستويات متكاملة، الإفصاح للعميل حول المخاطر المحتملة على أنظمتها، وهو ما يعزز قدرة العميل على اتخاذ التدابير الوقائية، والإفصاح للجهات الرقابية مثل ANSSI لضمان الامتثال للقواعد الخاصة، بالإضافة إلى الإفصاح الداخلي ضمن الشركة لتنسيق الإجراءات الأمنية ومراجعة الخطط المتخذة. ويؤكد هذا التوزيع أن الإفصاح لا يمثل مجرد واجب شكلي، بل أداة جوهرية لضمان حسن تنفيذ الالتزام الأساس، ومقياساً لتقييم مسؤولية مزود الخدمة في حال حدوث إخلال.

(1) نصت المادة (15) من المرسوم الفرنسي على أنه: "يجوز للوكالة الوطنية الفرنسية لأمن المعلومات (ANSSI) التحقق في أي وقت من امتثال مزود الخدمة للقواعد التي تم بموجبها تأهيله. ويتعين على مزود الخدمة إبلاغ الوكالة الوطنية الفرنسية لأمن المعلومات (ANSSI) فوراً بأي تغيير يطرأ على الظروف التي تم بموجبها تأهيله.

في حال مخالفة الشروط والتحفظات المنصوص عليها في قرار التأهيل، أو في حال حدوث تغيير في الظروف القانونية أو الواقعية التي تم بموجبها تأهيل مزود الخدمة، يجوز للمدير العام للوكالة الوطنية الفرنسية لأمن المعلومات (ANSSI)، بعد إتاحة الفرصة لمزود الخدمة لعرض ملاحظاته، تعليق التأهيل أو إلغاؤه".

(2) ينظر المادة (6) من كراس الشروط والأحكام المبسطة للأمن السيبراني الفرنسي.



علاوة على ذلك، يلاحظ أن هناك تفاعل بين الالتزامات العامة والخاصة، فبينما يفرض القانون المدني الالتزام العام بتقديم المعلومات الجوهرية للطرف المتعاقد، تحدد القواعد الخاصة، مثل مرسوم ANSSI، نطاق الإفصاح وطرقه، مع مراعاة طبيعة النشاط وحساسية المعلومات. وهذا التفاعل يعكس ضرورة الموازنة بين حقوق العميل، الامتثال التنظيمي، وحماية الأسرار التقنية، بحيث يُعتبر أي إخلال بالإفصاح – سواء تجاه العميل أو الجهات الرسمية – سبباً لتحميل مزود الخدمة المسؤولية التعاقدية، ويعكس تأثيره المحتمل على فعالية الالتزام الأساسي بحماية الأنظمة.

وعليه، يتضح أن الالتزام بالإفصاح لدى شركات الأمن السيبراني في فرنسا يتجاوز مجرد التزام معلوماتي، ليصبح عنصراً تكميلياً حاسماً لضمان تنفيذ الالتزام الأساسي بشكل فعال، ومقياساً لمدى التزام الشركة بالقواعد العامة والخاصة في مجال الأمن الرقمي، ويضع الأساس لمقارنة دقيقة مع الإطار الأمريكي والعراقي لتحديد نطاق الالتزام وحدوده العملية.

أما في العراق، فينشأ الالتزام بالإفصاح في عقود شركات الأمن السيبراني على أساس القواعد العامة في القانون المدني، ولا سيما مبدأ حسن النية في تنفيذ العقد، الذي يفرض على الأطراف الالتزام بسلوك إيجابي يقتضي تمكين الطرف الآخر من المعلومات الجوهرية المرتبطة بتنفيذ الالتزام⁽¹⁾، بما يحقق الغاية التعاقدية ويضمن التوازن بين الحقوق والالتزامات. وفي ضوء الطبيعة الفنية لعقود الأمن السيبراني، يتخذ هذا الالتزام بعداً خاصاً، إذ يكون مزود الخدمة في مركز فني متفوق، الأمر الذي يفرض عليه عدم كتمان المخاطر التي لا يستطيع العميل إدراكها بوسائله العادية، وتمكينه من اتخاذ التدابير الوقائية اللازمة. وعلى هذا الأساس، يغدو الإفصاح التزاماً وظيفياً ملازماً لتنفيذ الالتزام الرئيس بحماية الأنظمة والبيانات، بحيث إن أي نقص في المعلومات المقدمة من شأنه أن يقيّد قدرة العميل على حماية مصالحه، وقد يفضي إلى إخلال فعلي بمقتضيات الحماية المتفق عليها.

وعلى صعيد الالتزامات الخاصة، نظم قرار مجلس المفوضين رقم (33) لسنة 2025 نشاط شركات الأمن السيبراني وحدد الإطار العام لواجباتها في حماية الأنظمة والشبكات وتحليل التهديدات، كما تضمن تطبيقاً محدداً للالتزام بالإفصاح في مجال الإبلاغ عن الحوادث، إذ نصت الفقرة (17) من البند (ثانياً) من المادة (12) على التزام هذه الشركات بـ "إعلام الجهات المختصة في حال حدوث أي مشكلة فنية أو خرق أمني في أي من النشاطات التي تقدمها". فيلاحظ من النص إقرار المشرع بصورة خاصة من صور الإفصاح التنظيمي، يتمثل في الإبلاغ عن المخاطر والحوادث السيبرانية، بما يحقق تمكين

(1) نصّت الفقرة الأولى من المادة (150) من القانون المدني العراقي على: "يجب تنفيذ العقد طبقاً لما اشتمل عليه وبطريقة تتفق مع ما يوجبه حسن النية".



الجهات المختصة من متابعة الأوضاع الفنية واتخاذ ما يلزم من تدابير، ويحد من تفاقم الأضرار المحتملة. ومع ذلك، فإن هذا التنظيم يظل جزئياً، إذ لم يرد في القرار نص عام يقرر التزاماً شاملاً بالإفصاح تجاه العملاء، الأمر الذي يُبقي هذا الجانب خاضعاً في أساسه للقواعد العامة في القانون المدني.

ويكتسب الالتزام بالإفصاح في هذا الإطار أبعاداً متعددة، تتوزع بين الإفصاح للعميل بوصفه وسيلة لتمكينه من تقييم المخاطر واتخاذ التدابير الوقائية المناسبة، والإفصاح للجهات المختصة في الحدود التي رسمها القرار التنظيمي، فضلاً عن الإفصاح الداخلي داخل الشركة بما يضمن تنسيق التدابير الأمنية ومراجعة خطط إدارة المخاطر. ويؤكد هذا التعدد أن الإفصاح لا يقتصر على كونه التزاماً شكلياً، بل يمثل أداة أساسية لضمان حسن تنفيذ الالتزام الرئيسي⁽¹⁾، وعنصرًا لازماً لتحقيق فعالية الحماية في مواجهة التهديدات السيبرانية.

وعند الربط بين القواعد العامة والتنظيم الخاص، يتضح أن الالتزام بالإفصاح في العراق يقوم على تداخل وظيفي بين مصدرين: أولهما القواعد العامة التي تفرض، في إطار حسن النية، تقديم المعلومات الجوهرية للطرف المتعاقد، وثانيهما التنظيم الخاص الذي أقر التزاماً محدداً بالإفصاح في مجال الإبلاغ عن الحوادث الأمنية. ويترتب على هذا التداخل أن أي إخلال بالإفصاح، سواء تعلق بالمعلومات الجوهرية التي يجب تقديمها للعميل، أم بالإبلاغ عن الحوادث في مواجهة الجهات المختصة، يمكن أن يشكل إخلالاً بالتزامات مزود الخدمة، ويؤدي إلى قيام مسؤوليته التعاقدية أو التقصيرية بحسب الأحوال، لاسيما إذا ترتب على هذا الإخلال تفاقم الضرر أو تعذر تداركه في الوقت المناسب.

بناءً على ما تقدم، يتحدد الإخلال بالالتزام بالإفصاح بمعيار موضوعي يقوم على النتيجة لا على الشكل، فمتى أدى القصور في المعلومات المقدمة إلى حرمان العميل من القدرة على إدارة المخاطر التي تهدد أنظمتها، أو أعاق رقابة الجهات المختصة، تحققت المسؤولية بصرف النظر عن درجة التفصيل الشكلي في التقارير المقدمة.

(1) د. حسن علي الذنون، شرح القانون المدني، أصول الالتزام، مطبعة المعارف، بغداد، 1970، ص140.

الفرع الثاني

الالتزام بإعداد التقارير والامتثال

يتميز الالتزام بإعداد التقارير والامتثال عن الالتزام بالإفصاح المبكّر في الفرع السابق تمايزاً جوهرياً؛ فبينما ينصبّ الإفصاح على تمكين العميل من الإحاطة بالمخاطر القائمة في لحظة بعينها، يمتد الالتزام بإعداد التقارير والامتثال ليشمل رصد مستوى الحماية على امتداد مدة العقد كله، وقياسه بمعايير موضوعية قابلة للتحقق. ومن هنا تبرز الوظيفة القانونية المزدوجة لهذا الالتزام؛ إذ يُشكّل من جهة أداة لإثبات الوفاء بالالتزام الأصلي أو نفيه⁽¹⁾، ويمثّل من جهة أخرى معياراً مرجعياً يستند إليه القاضي المدني في تقدير مدى كفاية الأداء الأمني وتحديد نطاق المسؤولية. ولا يُقصد بالتقارير في هذا السياق مجرد وثائق إدارية شكلية، بل يُراد بها منظومة متكاملة من البيانات الموضوعية التي تعكس الحالة الأمنية الفعلية للنظام في فترات زمنية محددة، وتُمكن العميل والجهات الرقابية على حدٍّ سواء من التحقق المستمر من مستوى الحماية المقدمة. أما الامتثال فيُراد به التزام الشركة بالمعايير الفنية والتنظيمية المعتمدة في القطاع، باعتبارها المقياس الموضوعي الذي تُقاس به فعالية الأداء الأمني لا مجرد حسن النية في التنفيذ⁽²⁾.

على صعيد القانون الأمريكي، يُستمد الالتزام بإعداد التقارير والامتثال من منظومة قانونية متكاملة تجمع بين القواعد العامة للعقود والتشريعات الخاصة بالأمن السيبراني. فعلى مستوى القواعد العامة، يفرض مبدأ العناية الواجبة على شركة الأمن السيبراني توثيق أدائها الأمني بصورة منتظمة، بما يُمكن العميل من التحقق المستمر من مستوى الحماية المقدمة، ويُتيح للقضاء تقدير مدى الوفاء بالالتزام التعاقدية وفق معيار موضوعي لا تقديري. وعلى مستوى التشريعات الخاصة، تُنشئ المادة (13/650) من قانون الأمن الداخلي الأمريكي منظومة تبادل وتحليل المعلومات التي تُلزم شركات الأمن السيبراني بجمع المعلومات المتعلقة بالمخاطر وحوادث الأمن السيبراني وتحليلها والإفصاح عنها للجهات المعنية⁽³⁾.

(1) د. عبد الحي حجازي، النظرية العامة للالتزام، ج3، أحكام الالتزام، مطبعة نهضة مصر، 1953، ص8 وما بعدها.
(2) Adebola Folorunso, Ifeoluwa Wada, Bunmi Samuel and Viqaruddin Mohammed, Security compliance and its implication for cybersecurity, World Journal of Advanced Research and Reviews, 2024, 24(01), 2105–2121, p.2106.

(3) نصّت الفقرة (13) من قانون الأمن الداخلي الأمريكي: "منظمة تبادل وتحليل المعلومات: يُقصد بمصطلح "منظمة تبادل وتحليل المعلومات" أي كيان أو جهة تعاون رسمية أو غير رسمية تُنشئها أو تستخدمها مؤسسات القطاعين العام والخاص، للأغراض التالية: (أ) جمع وتحليل معلومات البنية التحتية الحيوية، بما في ذلك المعلومات المتعلقة بمخاطر وحوادث الأمن السيبراني، بهدف فهم أفضل لمشاكل الأمن والترابطات المتعلقة بالبنية التحتية الحيوية، بما في ذلك مخاطر وحوادث الأمن



فيما توسّع المادة (26/650) نطاق هذا الالتزام ليشمل توفير المعلومات واستلامها ونشرها بكافة صيغها⁽¹⁾. ويُضاف إلى ذلك أن إطار عمل المعهد الوطني للمعايير والتقنية يُرسي منظومة متكاملة من متطلبات التوثيق والتقييم الدوري التي باتت تُوظف قضائياً معياراً موضوعياً للحكم على مستوى الامتثال الأمني⁽²⁾، بما يعني أن إخلال الشركة بالتزامها بإعداد التقارير لا يُشكّل قصوراً إدارياً فحسب، بل يُرتّب مسؤولية مدنية مستقلة متى ثبت أن هذا الإخلال أعاق قدرة العميل على إدارة المخاطر التي تهدد أنظمتها.

أما في القانون الفرنسي، فيركز الالتزام بإعداد التقارير والامتثال على ركيزتين متكاملتين. الركيزة الأولى هي مبدأ حسن النية المنصوص عليه في المادة (1104) من القانون المدني الفرنسي، الذي يفرض على الشركة تنفيذ التزاماتها بطريقة تُمكن العميل من الرقابة المستمرة على مستوى الأداء الأمني، لا أن تكتفي بتقديم تقارير شكلية لا تعكس الواقع الفعلي للحالة الأمنية. والركيزة الثانية هي التنظيم الخاص الصادر عن الوكالة الوطنية لأمن نظم المعلومات، إذ تُحدد المادة (10) من مرسوم تأهيل منتجات الأمن آلية تقييم الخدمات المقدمة وفق المعايير الفنية المعتمدة، بما يشمل مراجعة الوثائق والفحص الميداني وتقييم الكوادر البشرية والتقنية⁽³⁾، فيما تُلزم المادة (15) من المرسوم ذاته مزود الخدمة بالإفصاح الفوري

السيبراني، والأنظمة المحمية، وذلك لضمان توافرها وسلامتها وموثوقيتها؛ (ب) التواصل أو الإفصاح عن معلومات البنية التحتية الحيوية، بما في ذلك مخاطر وحوادث الأمن السيبراني، للمساعدة في منع أو كشف أو تخفيف أو التعافي من آثار أي تدخل أو اختراق أو خلل يتعلق بالبنية التحتية الحيوية، بما في ذلك مخاطر وحوادث الأمن السيبراني، أو الأنظمة المحمية. و (ج) نشر معلومات البنية التحتية الحيوية طواعية، بما في ذلك مخاطر وحوادث الأمن السيبراني، لأعضائها، وحكومات الولايات والحكومات المحلية والفيدرالية، أو أي كيانات أخرى قد تساعد في تنفيذ الأغراض المحددة في الفقرتين الفرعيتين (أ) و(ب)".

(1) نصّت الفقرة (26) من قانون الامن الداخلي الأمريكي: "يشير مصطلح "المشاركة" (بما في ذلك جميع تصريفاته) إلى توفير واستلام ونشر (بما في ذلك جميع تصريفات كل مصطلح من هذه المصطلحات)".

(2) يُنظر في توظيف إطار عمل المعهد الوطني للمعايير والتقنية معياراً قضائياً لتقييم الامتثال الأمني:

Charlotte A. Tschider, "Locking Down 'Reasonable' Cybersecurity Duty", Yale Law & Policy Review, Vol. 41, p. 75, 2022 .

(3) نصّت المادة (10) من المرسوم الفرنسي على أن: "تُقيم الخدمات التي يقدمها مقدم الخدمة وفقاً للقواعد المنصوص عليها في المعايير الخاصة بكل نوع من أنواع الخدمات. تُطوّر هذه المعايير من قبل الوكالة الوطنية الفرنسية لأمن المعلومات (ANSSI) ويُقرّها رئيس الوزراء. ولأغراض الأمن القومي، قد تتطلب المعايير من مقدم الخدمة الامتثال لأحكام المواد R. 1-2311 وما يليها من قانون الدفاع الفرنسي. يُجرى التقييم ميدانياً وعن طريق مراجعة الوثائق من قبل مركز تقييم معتمد، وفقاً للشروط المنصوص عليها في القسم 2 من هذا الفصل. ويهدف التقييم إلى ضمان امتثال مقدم الخدمة للمعايير المذكورة في الفقرة الأولى، ولا سيما امتلاكه كوادر مؤهلة، بالإضافة إلى الموارد التقنية والمباني اللازمة لتقديم خدماته. يُجرى التقييم



عن أي تغيير في ظروف التأهيل⁽¹⁾. وتُعزّز منظومة التقارير والامتثال هذه بما تفرضه الشروط التعاقدية المبسّطة للأمن السيبراني من توثيق شامل للتدفقات وأجهزة التحكم، وتقديم شهادات وتصنيفات أمنية معترف بها كدليل اقتصادي على جدية الالتزام، فضلاً عن وجوب مسايرة أحدث المعايير التقنية المعتمدة في القطاع⁽²⁾، ويترتب على هذا التنظيم أن الامتثال لمعايير الوكالة الوطنية لا يُعدّ مجرد التزام تنظيمي، بل يُشكّل معياراً قانونياً يستند إليه القاضي الفرنسي في تقدير مدى وفاء الشركة بالتزاماتها التعاقدية، بما يعني أن القصور في التقارير أو في الامتثال للمعايير المعتمدة يُؤسس مباشرةً للمسؤولية العقدية دون حاجة إلى إثبات خطأ تقني محدد.

وفي القانون العراقي، يستند الالتزام بإعداد التقارير والامتثال إلى مصدرين متكاملين. أولهما القواعد العامة في القانون المدني، ولا سيما مبدأ حسن النية المُقرر في المادة (150) منه، الذي يفرض على الشركة أن يكون تنفيذها موجهاً فعلاً نحو تحقيق الغاية الأمنية التي قصدها المتعاقدان، لا أن تكتفي باتخاذ إجراءات شكلية. وثانيهما التنظيم الخاص المستحدث بموجب قرار مجلس المفوضين رقم (33) لسنة 2025، الذي أرسى منظومة من الالتزامات التقريرية تشمل إصدار أدوات التقييم وقياس الالتزام دورياً، وإلزام المرخص له بمراجعة سياسات الأمان السيبراني بصورة منتظمة وتقديم تقارير فصلية عن أنشطته⁽³⁾.

ميدانياً وعن طريق مراجعة الوثائق من قبل مركز تقييم معتمد، وفقاً للشروط المنصوص عليها في القسم 2 من هذا الفصل. عندما يتطلب التقييم خبرة فنية متخصصة لا تتوفر لدى مراكز التقييم، تقدم الوكالة الوطنية الفرنسية لأمن المعلومات (ANSSI) المساعدة لهذه المراكز. وفي حال عدم وجود مركز تقييم معتمد، يجوز للوكالة الوطنية الفرنسية لأمن المعلومات (ANSSI) تقييم خدمات مزود الخدمة".

⁽¹⁾ نصّت المادة (15) من المرسوم الفرنسي على أن: "يجوز للوكالة الوطنية الفرنسية لأمن المعلومات (ANSSI) التحقق في أي وقت من امتثال مزود الخدمة للقواعد التي تم بموجبها تأهيله. ويتعين على مزود الخدمة إبلاغ الوكالة الوطنية الفرنسية لأمن المعلومات (ANSSI) فوراً بأي تغيير يطرأ على الظروف التي تم بموجبها تأهيله. في حال مخالفة الشروط والتحفّظات المنصوص عليها في قرار التأهيل، أو في حال حدوث تغيير في الظروف القانونية أو الواقعية التي تم بموجبها تأهيل مزود الخدمة، يجوز للمدير العام للوكالة الوطنية الفرنسية لأمن المعلومات (ANSSI)، بعد إتاحة الفرصة لمزود الخدمة لعرض ملاحظاته".

⁽²⁾ تنظر المواد (4) و (9) و (11) من كراس الشروط والأحكام المبسّطة للأمن السيبراني الفرنسي.

⁽³⁾ المادة (12/ثانياً/6) والمادة (12/ثانياً/12) من قرار مجلس المفوضين رقم (33) لسنة 2025.



غير أن هذا التنظيم يظل قاصراً من وجهين، أولهما أنه لم يُحدد معايير موضوعية واضحة لمضمون هذه التقارير ومستوى تفصيلها، وثانيهما أنه لم يُرتَّب صراحةً المسؤولية المدنية على الإخلال بهذه الالتزامات، مما يُبقي هذا الجانب خاضعاً للقواعد العامة وما تتيحه من هامش تقديري واسع للقاضي المدني، وهو ما يُعدّ من أبرز مواطن القصور في المنظومة التنظيمية العراقية الراهنة ويستدعي تدخلاً تشريعياً صريحاً لمعالجته.

ويتجلى من استعراض المواقف القانونية المقارنة أن ثمة قاسماً مشتركاً يجمعها، يتمثل في الاعتراف بأن التقارير والامتنال ليسا التزامين شكليين، بل أداتان قانونيتان لإثبات الوفاء أو نفيه في عقود الأمن السيبراني. غير أن الأنظمة تتباين في مستوى تطور هذه الأداة؛ فالقانون الأمريكي يوظف المعايير المهنية معياراً قضائياً موضوعياً، والقانون الفرنسي يُرسي نظام تقييم مستقل تتولاه الوكالة الوطنية، في حين يظل القانون العراقي رهيناً بالقواعد العامة في غياب معايير موضوعية محددة تضبط مستوى الأداء التقريبي المطلوب.

ويترتب على الإخلال بهذا الالتزام في النظم الثلاثة مسؤولية مدنية مستقلة متى ثبت أن القصور في التقارير أو في الامتنال للمعايير المعتمدة قد أعاق قدرة العميل على إدارة المخاطر أو أفضى إلى تفاقم الضرر، لا سيما في الحالات التي يُثبت فيها أن الاطلاع المبكر على المعلومات كان كفيلاً بتجنب الضرر أو تقليل أثره.

المبحث الثاني

المسؤولية القانونية لشركات الأمن السيبراني

لا تنفصل المسؤولية القانونية لشركات الأمن السيبراني عن الطبيعة الخاصة للالتزامات التي تقع على عاتقها، إذ إن الإخلال بهذه الالتزامات لا يُفضي دائماً إلى مسؤولية ذات طابع واحد أو ذات مصدر موحد. فشركة الأمن السيبراني، بحكم موقعها في العلاقة التعاقدية وبحكم طبيعة نشاطها الذي يمس أنظمة الغير وبياناتهم، قد تجد نفسها في مواجهة مسؤولية مدنية تجاه عميلها المباشر حين تُخل بالالتزاماتها الجوهرية، وفي مواجهة مسؤولية موسّعة تمتد إلى الغير الذي لم يكن طرفاً في العقد غير أنه تضرر من الإخفاق الأمني. يُضاف إلى ذلك بُعد آخر لا يقل أهمية، يتصل بالمسؤولية الناجمة عن الانتهاك القانوني والتنظيمي، سواء في مواجهة الجهات الرقابية المختصة، أم على مستوى الأشخاص الطبيعيين المكلفين بالإدارة والتنفيذ الفني داخل الشركة. وتكتسب هذه المسؤولية خصوصية بالغة تميّزها عن المسؤولية المدنية في عقود الخدمات التقليدية؛ فهي من جهة تنهض في ظل علاقة تعاقدية تقوم على التخصص الفني وتفاوت المعلومات بين الشركة وعميلها، ومن جهة أخرى تنتشعب آثارها لتطال أطرافاً لم تكن في الأصل جزءاً من العلاقة العقدية. ومن هنا تبرز الحاجة إلى تحليل هذه المسؤولية في شقيها الرئيسيين، المسؤولية الناجمة عن الإخلال بالالتزامات الأساسية، والمسؤولية الناجمة عن الانتهاك القانوني والتنظيمي، وذلك من خلال استحضار ما تقدمه النظم القانونية المقارنة في الولايات المتحدة وفرنسا والعراق من حلول ومعالجات. وعليه يقسم هذا المبحث إلى مطلبين، الأول يُعنى الأول بالمسؤولية الناجمة عن الإخلال بالالتزامات الأساسية، ويتناول الثاني المسؤولية الناجمة عن الانتهاك القانوني والتنظيمي.

المطلب الأول

المسؤولية الناجمة عن الإخلال بالالتزامات الأساسية

لا يكفي في تحديد نطاق المسؤولية المدنية لشركات الأمن السيبراني الوقوف عند مجرد ثبوت الإخلال بالالتزام، بل يقتضي الأمر تحديد الجهة المتضررة وطبيعة العلاقة التي تربطها بالشركة، إذ إن هذا التحديد هو الذي يرسم حدود المسؤولية ويُعيّن أساسها القانوني. فحين يتعلق الضرر بالعمل المتعاقد مباشرة، تنهض المسؤولية في إطارها العقدي، قائمة على الإخلال بالتزام أصيل يُشكّل محل العقد ذاته. أما حين يمتد الضرر ليطال الغير الذي لا تربطه بالشركة رابطة تعاقدية، فإن المسؤولية تنتقل إلى أساس مغاير يجد سنده في القواعد العامة للمسؤولية التقصيرية. وهذا التمييز ليس ترفاً نظرياً، بل هو ذو أثر

عملي مباشر في تحديد شروط قيام المسؤولية وطريقة الإثبات ونطاق التعويض. وعليه يتفرع هذا المطلب إلى فرعين، يتناول الأول المسؤولية عن الضرر المتعلق بالعملاء، ويُخصص الثاني للمسؤولية عن الضرر المتعلق بالغير.

الفرع الأول

الضرر المتعلق بالعملاء

يقع الضرر المتعلق بالعميل في عقود الأمن السيبراني في قلب المسؤولية العقدية، إذ تربط الشركة بعميلها رابطة تعاقدية مباشرة تُلقِي على الأولى التزامات جوهرية تنصبّ على محل العقد ذاته. وما يُميز هذه المسؤولية العقدية عن غيرها من المسؤوليات في العقود الخدمية التقليدية، هو أن الإخلال لا يتعلق بالتزام هامشي يمكن تصحيحه أو تداركه، بل يمس الغاية الجوهرية التي من أجلها أبرم العقد أصلاً، وهي تحقيق حالة مستمرة من الأمان للنظام المعلوماتي للعميل وصون بياناته من المخاطر التي تتهددها. ومن هنا تنشأ إشكالية قانونية محورية تتصل بتحديد طبيعة الالتزام الذي أخلّت به الشركة، أهو التزام ببذل عناية أم التزام بتحقيق نتيجة؟ وذلك لما يترتب على هذا التحديد من أثر مباشر في تحديد معيار الإخلال وكيفية الإثبات ونطاق التعويض⁽¹⁾.

لا يقوم النظام الأمريكي على نص تقني موحّد يُنظّم المسؤولية العقدية لشركات الأمن السيبراني تجاه عملائها، وإنما تتشكل هذه المسؤولية من خلال تفاعل مبادئ القانون العام للعقود مع ما تفرضه طبيعة النشاط من التزامات خاصة. ويُشكّل مبدأ حسن النية والتعامل العادل في تنفيذ الالتزامات، المُقرر في المادة (205) من إعادة بيان قانون العقود الثاني، الركيزة العامة التي تحكم العلاقة بين الشركة وعميلها، إذ يفرض على كل طرف تنفيذ التزاماته على نحو يحقق الغاية التي اتجهت إليها إرادة المتعاقدين⁽²⁾.

(1) د. مصطفى الخطيب، الموجز في النظرية العامة للالتزامات، مطبعة قرطبة، دون مكان نشر، 2019، ص16.

(2) Restatement (Second) of Contracts, American Law Institute, § 205, 1981, which provides: "Every contract imposes upon each party a duty of good faith and fair dealing in its performance and enforcement"، إعادة بيان قانون العقود الأمريكي الثاني، معهد القانون الأمريكي، المادة (205)، 1981،

متاح على الموقع الرسمي لمعهد القانون الأمريكي <https://www.ali.org> : تاريخ اخر زيارة في 2026/6/14

وتُحدد المسؤولية العقدية في القانون الأمريكي وفق نظرية الإخلال بالعقد، التي تستلزم إثبات أربعة عناصر متلازمة، وجود عقد صحيح النشأة، وإخلال الشركة بالتزام ثابت بموجبه، وتحقيق ضرر فعلي للعميل، وقيام رابطة السببية بين الإخلال والضرر⁽¹⁾. غير أن تطبيق هذه العناصر على عقود الأمن السيبراني يكتسب خصوصية بالغة، تتمثل أساساً في مسألة تحديد معيار الإخلال. فالقضاء الأمريكي لم يستقر على معيار موحد في هذا الشأن، وإنما تباينت المحاكم في تكييف طبيعة الالتزام تبعاً لمضمون العقد المبرم بين الطرفين وطبيعة الخدمة المقدمة.

وفي هذا السياق، ميّزت المحاكم الأمريكية بين صورتين، الأولى حين يلتزم العقد بتحقيق مستوى محدد وقابل للقياس من الحماية، كضمان عدم اختراق النظام أو ضمان سرية بيانات بعينها، ففي هذه الحالة يقترب الالتزام من الالتزام بتحقيق نتيجة، ويكفي العميل إثبات أن النتيجة المتفق عليها لم تتحقق لتقوم مسؤولية الشركة. والثانية حين ينصبّ العقد على بذل جهد مهني في مواجهة تهديدات متجددة غير محددة سلفاً، فيغدو الالتزام أقرب إلى الالتزام ببذل عناية مهنية مشددة، ويلتزم العميل بإثبات أن الشركة قصّرت عن مستوى الأداء المهني المعتمد في القطاع⁽²⁾.

وقد وظّف القضاء الأمريكي معايير المعهد الوطني للمعايير والتقنية بوصفها مرجعاً موضوعياً لتقدير مستوى الأداء المهني المطلوب⁽³⁾، فأصبحت هذه المعايير أداة قضائية لقياس الإخلال لا مجرد

(1) Cornell Law School, Legal Information Institute, "Breach of Contract", last reviewed June 2022, available at: https://www.law.cornell.edu/wex/breach_of_contract . تاريخ اخر زيارة في 2026/6/14

(2) يُنظر في معيار الإخلال بالالتزام في القانون الأمريكي وعناصر الإهمال المهني: Cornell Law School, Legal Information Institute, "Negligence", last reviewed July 2023, available at: <https://www.law.cornell.edu/wex/negligence> ؛ وكذلك Cornell Law School, Legal Information Institute, "Breach of Contract", last reviewed June 2022, available at: https://www.law.cornell.edu/wex/breach_of_contract . تاريخ اخر زيارة في 2026/6/14

(3) أن توظيف معايير المعهد الوطني للمعايير والتقنية في تحديد الواجب المعقول لشركات الأمن السيبراني يُشكّل اتجاهاً قضائياً متنامياً يُقيس الإخلال بمدى توافق الأداء الفعلي مع المعايير المهنية المستقرة لا بالنية أو القصد. يُنظر في معيار الأداء المهني المعتمد في القانون الأمريكي وتوظيف المحاكم لمعايير المعهد الوطني للمعايير والتقنية أداة قضائية:

Charlotte A. Tschider, "Locking Down 'Reasonable' Cybersecurity Duty", Yale Law & Policy Review, Vol. 41, p. 75, 2022 .

توصيات فنية⁽¹⁾. ومؤدى ذلك أن إخلال الشركة لا يُقاس بالنية أو القصد، وإنما بمدى توافق أدائها الفعلي مع ما يقتضيه المستوى المهني المعتمد في مواجهة التهديدات التي تعرض لها نظام العميل.

وفيما يخص نطاق التعويض المستحق للعميل، يتقيد القضاء الأمريكي بمبدأ التوقع المعقول للضرر وقت إبرام العقد، فلا يُعوّض عن الأضرار التي كانت خارج نطاق ما يمكن توقعه عند التعاقد⁽²⁾. غير أن محاكم عديدة وسّعت نطاق الأضرار القابلة للتعويض في عقود الأمن السيبراني لتشمل ما يترتب على انكشاف البيانات من تكاليف الإخطار القانوني، وأتعاب إجراءات التقاضي، والأضرار السمعية القابلة للتقييم المالي الموضوعي، فضلاً عن الخسارة التجارية المباشرة الناجمة عن توقف النظام أو تعطله⁽³⁾.

أما بالنسبة للقانون الفرنسي، فيُتيح القانون المدني الفرنسي إطاراً تحليلياً أكثر دقة وتماسكاً في معالجة مسؤولية شركات الأمن السيبراني تجاه عملائها، وذلك بفضل التمييز الراسخ في الفقه والقضاء الفرنسيين بين الالتزام بتحقيق نتيجة والالتزام ببذل عناية، وما يترتب على هذا التمييز من أثر حاسم في توزيع عبء الإثبات وتحديد نطاق المسؤولية.

وتُشكّل المادة (1-1231) من القانون المدني الفرنسي الأساس التشريعي للمسؤولية العقدية، إذ تُقرر مسؤولية المدين عن الأضرار الناجمة عن عدم تنفيذ التزامه أو التأخر فيه، ما لم يُثبت أن عدم التنفيذ يعود لقوة قاهرة لا يمكن نسبته إليه⁽⁴⁾. وتتحدد الإشكالية الجوهرية في تكييف طبيعة الالتزام الذي تخلّ به شركة الأمن السيبراني، لما لهذا التكييف من أثر مباشر في تحديد من يتحمل عبء الإثبات.

(1) National Institute of Standards and Technology, The NIST Cybersecurity Framework (CSF) 2.0, NIST CSWP 29, February 26, 2024.

(2) تنص المادة (351) من إعادة بيان قانون العقود الأمريكي الثاني على أن: "لا يُعوّض عن الخسارة التي لم يكن للطرف المخل بالعقد سبب للتوقع بأنها نتيجة محتملة للإخلال وقت إبرام العقد".

(3) في قضية ريمياس ضد مجموعة نيومان ماركوس، تعرضت شركة نيومان ماركوس عام 2013 لاختراق سيبراني أسفر عن سرقة بيانات بطاقات ائتمان نحو 350,000 عميل، فأقام هؤلاء دعوى جماعية يطالبون فيها بالتعويض. وقد رأت محكمة الاستئناف الأمريكية للدائرة السابعة أن الأضرار القابلة للتعويض في مثل هذه القضايا لا تقتصر على الخسارة المالية المباشرة، بل تمتد لتشمل تكاليف معالجة الرسوم الاحتياطية، وتكاليف مراقبة الائتمان وحماية الهوية، والأضرار المستقبلية المحتملة الناجمة عن سرقة البيانات، وهو ما يعكس توجه القضاء الأمريكي نحو توسيع نطاق الأضرار القابلة للتعويض في قضايا انكشاف البيانات لتتجاوز الإطار التقليدي المقيد بالضرر المتوقع وقت إبرام العقد:

Remijas v. Neiman Marcus Group, LLC, No. 14-3122, United States Court of Appeals for the Seventh Circuit, decided July 20, 2015.

(4) نصت المادة (1-1231) من القانون المدني الفرنسي على أن: "يُحكم على المدين، عند الاقتضاء، بدفع تعويضات عن الأضرار سواء بسبب عدم تنفيذ الالتزام أو بسبب التأخر في تنفيذه، ما لم يُثبت أن التنفيذ قد حال دونه القوة القاهرة".

فإن كَيْفَ الالتزام بوصفه التزاماً بتحقيق نتيجة، كفى العمل إثبات عدم تحقق النتيجة الموعودة دون حاجة إلى إثبات خطأ محدد، وانتقل عبء الإثبات إلى الشركة لثبوت هي السبب الأجنبي. أما إن كُيفَ بوصفه التزاماً ببذل عناية، وجب على العمل عند ذلك إثبات أن الشركة قصّرت عن مستوى العناية المهنية المطلوب⁽¹⁾.

والراجح في الفقه الفرنسي أن الالتزام في عقود الأمن السيبراني ذو طبيعة مختلطة؛ فهو يقترب من الالتزام بتحقيق نتيجة حين يتعلق بضمان سرية بيانات بعينها أو بمستوى أمان محدد تعاقدياً، ويتراجع نحو الالتزام ببذل عناية مشددة حين يتصل بمواجهة تهديدات متطورة وغير متوقعة⁽²⁾.

ويستقر الفقه الفرنسي على أن مزود الخدمة التقنية الذي يضطلع بمهمة مستمرة في حماية الأنظمة لا يمكنه الاكتفاء بإثبات أنه اتخذ تدابير شكلية للحماية في لحظة بعينها، بل عليه إثبات أنه حافظ على مستوى الأداء المطلوب طوال مدة تنفيذ العقد⁽³⁾، وهو ما يتوافق مع طبيعة عقود الأمن السيبراني التي تفرض التزاماً مستمراً لا ينتهي بإعداد النظام.

وفيما يتعلق بنطاق التعويض، تُطبق المادة (4-1231) من القانون المدني الفرنسي قاعدة قصر التعويض في المسؤولية العقدية على الأضرار المتوقعة وقت إبرام العقد، وحتى في حالة ثبوت الخطأ

(1) يُعدّ التمييز بين الالتزام بتحقيق نتيجة والالتزام ببذل عناية من أرسخ المبادئ في القانون المدني الفرنسي، وقد أرساه الفقيه رونييه ديموج في مطلع القرن العشرين واستقر عليه القضاء الفرنسي. ومن أبرز تطبيقاته حكم محكمة النقض الفرنسية الشهير المعروف بحكم ميرسييه، الصادر عن الدائرة المدنية في 20 مايو 1936، الذي ميّز لأول مرة بين نوعي الالتزام في عقد الطبيب مع مريضه، وأثر تأثيراً بالغاً في تطور نظرية الالتزام في القانون الفرنسي:

Cour de cassation, Chambre civile, 20 mai 1936, arrêt Mercier, Gazette du Palais 1936, 2, p. 41; Recueil Dalloz 1936, p. 88.

يُنظر أيضاً في شرح هذا التمييز وأثره في توزيع عبء الإثبات:

Philippe Malaurie, Laurent Aynès et Philippe Stoffel-Munck, Droit des obligations, LGDJ, Paris, 2020.

(2) يُنظر في الطبيعة المختلطة للالتزام في عقود الخدمات التقنية والتمييز بين الالتزام بتحقيق نتيجة والالتزام ببذل عناية وأثره في توزيع عبء الإثبات:

Hervé Jacquemin, "Contrats informatiques", Revue du Droit des Technologies de l'information, n° 35, 2009, pp. 29-41.

(3) يُنظر في مبدأ استمرارية الالتزام طوال مدة تنفيذ العقد في عقود الخدمات التقنية:

Hervé Jacquemin, "Contrats informatiques", Revue du Droit des Technologies de l'information, n° 35, 2009, pp. 35-38.

الجسيم أو الغش من جانب شركة الأمن السيبراني، يظل التعويض وفق صريح المادة (4-1231) من القانون المدني الفرنسي مقصوراً على ما يُعدّ نتيجة مباشرة وفورية لعدم التنفيذ⁽¹⁾، وهو ما يعكس حرص المشرع الفرنسي على ضبط نطاق التعويض العقدي حتى في أشد حالات الإخلال خطورة.

أما فيما يتعلق بالقانون العراقي، فيستند القانون المدني العراقي النافذ في تنظيم المسؤولية العقدية إلى منظومة من الأحكام العامة التي تنطبق على سائر العقود بما فيها عقود الأمن السيبراني في غياب نص خاص. تُشكّل المادة (169) منه الركيزة الأساسية في تحديد نطاق التعويض، إذ تقضي في فقرتها الثانية بأن يشمل التعويض ما لحق الدائن من خسارة وما فاتته من كسب بشرط أن يكون ذلك نتيجة طبيعية لعدم وفاء المدين بالتزامه⁽²⁾. وتُكمل الفقرة الثالثة من المادة ذاتها هذه القاعدة بتحديد معيار التوقع، إذ تقصر التعويض على ما يكون متوقعاً عادةً وقت التعاقد ما لم يثبت الغش أو الخطأ الجسيم⁽³⁾. أما المادة (168) فنُقرر مسؤولية المدين عند استحالة التنفيذ ما لم يُثبت السبب الأجنبي⁽⁴⁾.

وبتطبيق هذه القواعد على عقود الأمن السيبراني، يتضح أن إثبات مسؤولية الشركة أمام القضاء العراقي يستلزم توافر ثلاثة عناصر متلازمة، ثبوت الإخلال بالالتزام التعاقدية المتمثل في عدم تحقيق مستوى الحماية المتفق عليه أو المفترض مهنيّاً، وتحقيق الضرر الفعلي للعميل سواء أكان مادياً كتلف البيانات أو توقف النظام، أم معنوياً كالإضرار بسمعة المؤسسة وثقة عملائها، وقيام رابطة السببية بين الإخلال والضرر بمعنى أن يكون الضرر نتيجة طبيعية ومباشرة للتقصير الثابت في جانب الشركة.

(1) نصّت المادة (4-1231) من القانون المدني الفرنسي على أن: "حتى في الحالة التي يكون فيها عدم تنفيذ العقد ناجماً عن خطأ جسيم أو غش، لا يشمل التعويض إلا ما يُعدّ نتيجة مباشرة وفورية لعدم التنفيذ".

(2) نصّت الفقرة الثانية من المادة (169) من القانون المدني العراقي على أن: "ويكون التعويض عن كل التزام ينشأ عن العقد سواء كان التزاماً بنقل ملكية أو منفعة أو أي حق عيني آخر أو التزاماً بعمل أو بامتناع عن عمل ويشمل ما لحق الدائن من خسارة وما فاتته من كسب بسبب ضياع الحق عليه أو بسبب التأخر في استيفائه بشرط أن يكون هذا نتيجة طبيعية لعدم وفاء المدين بالالتزام أو لتأخره عن الوفاء به".

(3) نصّت الفقرة الثالثة من المادة (169) من القانون المدني العراقي على أن: "إذا كان المدين لم يرتكب غشاً أو خطأ جسيماً فلا يجاوز في التعويض ما يكون متوقعاً عادةً وقت التعاقد من خسارة تحل أو كسب يفوت".

(4) نصّت المادة (168) من القانون المدني العراقي على أن: "إذا استحال على الملتزم بالعقد أن ينفذ الالتزام عيناً حكم عليه بالتعويض لعدم الوفاء بالتزامه ما لم يثبت استحالة التنفيذ قد نشأت عن سبب اجنبي لا يد له فيه، وكذلك يكون الحكم إذا تأخر الملتزم في تنفيذ التزامه".

كذلك ينظر: علي علي سليمان، النظرية العامة للالتزام، مصادر الالتزام في القانون المدني الجزائري، ط5، ديوان المطبوعات الجامعية، 2003، ص102.



ويُلاحظ في هذا الإطار أن المادة (150) من القانون المدني العراقي، التي تُقرر مبدأ حسن النية في تنفيذ العقود، تؤدي وظيفة تفسيرية بالغة الأهمية في تحديد مضمون الالتزام ومعياري تنفيذه؛ إذ لا يكفي أن تُثبت الشركة أنها اتخذت تدابير شكلية للحماية، بل يجب أن يكون تنفيذها قد اتجه فعلاً نحو تحقيق الغاية الأمنية التي قصدها المتعاقدان⁽¹⁾. وهو ما يُقرّب المعيار المعتمد في القانون العراقي من المعيار الموضوعي القائم على الغاية لا على الوسيلة.

وعلى الرغم من خلو التنظيم المدني العراقي من نص يُميز صراحةً بين الالتزام بتحقيق نتيجة والالتزام ببذل عناية، إلا أن المبادئ العامة تسمح باستخلاص هذا التمييز من خلال الغاية التعاقدية وطبيعة النشاط. وقد أضاف قرار مجلس المفوضين رقم (33) لسنة 2025 أداةً موضوعية في يد القاضي المدني، إذ يُحدد الإطار التنظيمي مستوى الأداء المطلوب من شركات الأمن السيبراني، ويمكن توظيفه معياراً مرجعياً لتقدير مدى وفاء الشركة بالتزاماتها التعاقدية في مواجهة العميل⁽²⁾.

يتجلى من استعراض المواقف القانونية المقارنة، أن ثمة قاسماً مشتركاً يجمعها، يتمثل في الاعتراف بأن مسؤولية شركة الأمن السيبراني تجاه عميلها لا تُقاس بمعيار النية أو القصد، وإنما بمعيار موضوعي يرتبط بتحقيق الغاية الأمنية التي قام عليها العقد. غير أن هذه الأنظمة تتباين في الأداة القانونية التي توصل إلى هذه النتيجة؛ فالقانون الفرنسي يصل إليها عن طريق التمييز الدقيق بين نوعي الالتزام وما يترتب على ذلك من توزيع لعبء الإثبات، في حين يصل القانون الأمريكي إليها عبر توظيف المعايير المهنية المعتمدة أداةً قضائية لقياس الإخلال، أما القانون العراقي فيستند إلى مبدأ حسن النية وتحقيق الغاية التعاقدية بوصفهما المحور الذي تدور حوله المسؤولية. والمحصلة العملية واحدة في النظم الثلاثة: لا تستطيع شركة الأمن السيبراني دفع المسؤولية بمجرد إثبات أنها بذلت جهداً، ما لم تُثبت أن هذا الجهد كان كافياً لتحقيق الغاية الأمنية المنشودة أو أن تخلف هذه الغاية يعود إلى سبب أجنبي خارج عن إرادتها.

(1) د. حسن علي الذنون، مصدر سابق، ص 140.

(2) المادة (6/رابعاً-2) من قرار مجلس المفوضين.

الفرع الثاني

الضرر المتعلق بالغير

لا تقف آثار الإخلال بالتزامات الأمن السيبراني عند حدود العلاقة التعاقدية التي تربط الشركة بعميلها المباشر، بل كثيراً ما تمتد لتطال أطرافاً ثالثة لم تكن طرفاً في العقد وفقاً لشروط معينة⁽¹⁾، غير أنها تضررت من الإخفاق الأمني تضرراً مباشراً أو غير مباشر. وتتعدد فئات هؤلاء الأطراف وتتباين طبيعة أضرارهم؛ فمنهم عملاء الشركة المتعاقدة الذين تحتفظ الشركة ببياناتهم الشخصية والمالية، ومنهم الشركاء التجاريون المرتبطون بنفس المنظومة الرقمية، ومنهم من يقع عليهم الضرر بصورة غير مباشرة جراء انتشار آثار الاختراق خارج نطاق النظام الأصلي. وتُشكل مسؤولية شركة الأمن السيبراني تجاه هؤلاء إشكالية قانونية بالغة الدقة، إذ لا يمكن تأسيسها على الرابطة العقدية المنعدمة بينهم وبين الشركة، وإنما تجد سندها في قواعد المسؤولية التقصيرية القائمة على الخطأ والضرر وعلاقة السببية. وما يُضفي على هذه المسؤولية خصوصية إضافية هو أن الضرر الواقع على الغير في سياق الأمن السيبراني كثيراً ما يكون ضرراً مركباً يجمع بين الأبعاد المالية والمعنوية والمستقبلية، مما يستدعي تحليلاً دقيقاً لمدى استيعاب كل نظام قانوني لهذه الأبعاد في إطار قواعد المسؤولية التقصيرية.

يُعالج القانون الأمريكي مسؤولية شركة الأمن السيبراني تجاه الغير في إطار قواعد المسؤولية التقصيرية المستمدة من القانون العام، والتي تقوم على إثبات خمسة عناصر متلازمة، وجود واجب قانوني يلزم الشركة بعدم الإضرار بالغير، وإخلال الشركة بهذا الواجب، وتحقيق الضرر للغير، وقيام رابطة سببية مباشرة بين الإخلال والضرر، وقيام رابطة السببية الفعلية. غير أن الإشكالية الجوهرية في هذا السياق تتمحور حول مدى امتداد واجب العناية الذي تلتزم به شركة الأمن السيبراني تجاه العميل ليشمل الغير الذي لا تربطه بالشركة أي رابطة تعاقدية مباشرة⁽²⁾.

(1) زوليخة حيمر، مسؤولية المدين العقدي عن فعل الغير، دراسة تحليلية، حوليات جامعة قلمة للعلوم الاجتماعية والإنسانية، قلمة، عدد 1، 2024، ص 221. محفوظ لشعب، المبادئ العامة للقانون الجزائري، ط5، ديوان المطبوعات الجامعية، الجزائر، 2011، ص 214.

(2) أن واجب العناية يمتد ليشمل الغير متى كان سلوك المدعى عليه يُنشئ خطر الضرر عليهم، وأن المحاكم تعترف باستثناءات تفرض واجباً إيجابياً تجاه الغير في الحالات التي تنشأ فيها علاقة خاصة بين الأطراف تنطوي على قدر من الاعتماد والسيطرة، وهو ما ينطبق تماماً على علاقة شركة الأمن السيبراني بأصحاب البيانات المحفوظة في أنظمة عميلها. يُنظر في عناصر المسؤولية التقصيرية في القانون الأمريكي ومدى امتداد واجب العناية ليشمل الغير:

وفي هذا الصدد، ميّز القضاء الأمريكي بين ثلاث فئات من الغير المتضررين. أما الفئة الأولى فهي عملاء الشركة المتعاقدة الذين تحتفظ هذه الأخيرة ببياناتهم الشخصية والمالية، وقد استقر القضاء الأمريكي على أن شركة الأمن السيبراني تدين لهؤلاء بواجب عناية مستقل عن العلاقة التعاقدية، متى كان في مقدورها توقع أن إخفاقها الأمني سيؤدي إلى الإضرار بهم. وقد كرّست قضية ريمياس ضد مجموعة نيومان ماركوس هذا التوجه حين اعترفت المحكمة بأن أصحاب البيانات المسربة يملكون حق المطالبة بالتعويض عن أضرار انكشاف بياناتهم، بما فيها تكاليف الحماية المستقبلية وأضرار سرقة الهوية المحتملة⁽¹⁾. وأما الفئة الثانية فهي الشركاء التجاريون المرتبطون بالمنظومة الرقمية ذاتها، حيث يتوسع نطاق المسؤولية ليشمل كل من كان في وضع يجعل الضرر الواقع عليه متوقعاً بصورة معقولة، وذلك استناداً إلى مبدأ التوقع المعقول للضرر الذي يحكم تحديد نطاق واجب العناية في القانون الأمريكي⁽²⁾. وأما الفئة الثالثة، فهم الأشخاص المتضررون بصورة غير مباشرة، فإن القضاء الأمريكي يتحفظ في

Cornell Law School, Legal Information Institute, "Negligence", last reviewed July 2023, available at: <https://www.law.cornell.edu/wex/negligence> ; تاريخ اخر زيارة في 2026/6/14

Cornell Law School, Legal Information Institute, "Duty of Care", last reviewed March 2026, available at: https://www.law.cornell.edu/wex/duty_of_care. تاريخ اخر زيارة في 2026/6/14

(1) في قضية ريمياس ضد مجموعة نيومان ماركوس تعرضت شركة نيومان ماركوس عام 2013 لاختراق سيبراني أسفر عن سرقة بيانات بطاقات ائتمان نحو 350,000 عميل. وقد اعترفت محكمة الاستئناف الأمريكية للدائرة السابعة بأن أصحاب البيانات المسربة يملكون حق المطالبة بالتعويض عن أضرار انكشاف بياناتهم بما فيها تكاليف الحماية المستقبلية وأضرار سرقة الهوية المحتملة، مكرّسةً بذلك واجب العناية المستقل الذي تدين به الشركة لعملاء الطرف المتعاقد:

Remijas v. Neiman Marcus Group, LLC, No. 14-3122, United States Court of Appeals for the Seventh Circuit, decided July 20, 2015.

(2) وقد أقرّت المحكمة الفيدرالية لمنطقة مينيسوتا في قضية اختراق بيانات شركة تارغت بأن المؤسسات المالية الشريكة التجارية لتارغت تملك حق المطالبة بالتعويض عن الأضرار اللاحقة بها جراء الاختراق، استناداً إلى مبدأ أن ضررها كان متوقعاً بصورة معقولة:

In re Target Corporation Customer Data Security Breach Litigation, MDL No. 14-2522 (PAM/JJK), United States District Court for the District of Minnesota, December 18, 2014, as cited in Remijas v. Neiman Marcus Group, LLC, No. 14-3122 (7th Cir. 2015); see also In re Target Corporation Customer Data Security Breach Litigation, No. 15-3909, United States Court of Appeals for the Eighth Circuit, decided February 1, 2017, available at: <https://cases.justia.com/federal/appellate-courts/ca8/15-3909/15-3909-2017-02-01.pdf> .

تاريخ اخر زيارة في 2026/6/14

الاعتراف بمسؤولية الشركة تجاههم، ويشترط لقيام هذه المسؤولية أن يكون الضرر اللاحق بهم متوقعاً بصورة معقولة وقت الإخلال، وأن تقوم رابطة سببية وثيقة تربطه بالإخفاق الأمني المنسوب للشركة⁽¹⁾.

ويلاحظ في هذا الإطار أن القضاء الأمريكي يوظف معيار الشخص المعقول في تقدير واجب العناية المستحق للغير، بمعنى أنه يتساءل عما كانت ستفعله شركة أمن سيبراني معقولة في مواجهة المخاطر التي كانت متوقعة وقت الإخلال. ومؤدى ذلك أن نطاق المسؤولية تجاه الغير يتسع كلما كانت المخاطر المحتملة على الغير معروفة للشركة أو كان في مقدورها معرفتها بذل العناية المهنية المعتادة.

أما بالنسبة للقانون الفرنسي، فيتيح القانون المدني فيه إطاراً تحليلياً متكاملًا لمعالجة مسؤولية شركة الأمن السيبراني تجاه الغير، وذلك من خلال قواعد المسؤولية التقصيرية المقررة في المواد (1240) و(1241) من القانون المدني الفرنسي، اللتين تُرسيان المسؤولية على كل من يتسبب بخطئه في إلحاق الضرر بالغير⁽²⁾. وما يميز النظام الفرنسي في هذا الشأن هو أن مفهوم الخطأ الموجب للمسؤولية تجاه الغير لا يقتصر على الإخلال بالتزام تعاقدية، بل يمتد ليشمل كل إخلال بواجب عام للحيطه والحذر يفرضه على الشركة مركزها المتخصص ومعرفتها بالمخاطر التي يتعرض لها الغير من جراء إخفاقها الأمني.

وبالنسبة لفئة عملاء الشركة المتعاقدة الذين تحتفظ هذه الأخيرة ببياناتهم، فإن الحماية المقررة لهم في القانون الفرنسي تجد سندها الإضافي في اللائحة الأوروبية العامة لحماية البيانات، التي تلزم كل جهة تعالج البيانات الشخصية باتخاذ التدابير التقنية والتنظيمية الكافية لضمان أمنها، وتقرر مسؤولية مستقلة تجاه أصحاب البيانات في حال الإخلال بهذه الالتزامات⁽³⁾. ومؤدى ذلك أن شركة الأمن السيبراني

(1) يُنظر في موقف القضاء الأمريكي من اشتراط التوقع المعقول للضرر وقيام الرابطة السببية الوثيقة شرطاً لقيام المسؤولية تجاه المتضررين بصورة غير مباشرة، حيث يُقرر هذا المصدر أن المحاكم الأمريكية تُقيم التمييز بين حالات الفعل الضار المباشر التي يُفترض فيها واجب العناية، وحالات الإهمال غير المباشر التي تشترط فيها وجود علاقة خاصة بين الأطراف أو توقعاً معقولاً للضرر لإقامة المسؤولية.

(2) يُنظر في موقف القضاء الأمريكي من اشتراط التوقع المعقول للضرر وقيام الرابطة السببية الوثيقة شرطاً لقيام المسؤولية تجاه المتضررين بصورة غير مباشرة، حيث يُقرر هذا المصدر أن المحاكم الأمريكية تُقيم التمييز بين حالات الفعل الضار المباشر التي يُفترض فيها واجب العناية، وحالات الإهمال غير المباشر التي تشترط فيها وجود علاقة خاصة بين الأطراف أو توقعاً معقولاً للضرر لإقامة المسؤولية.

(3) نصت المادة (1240) من القانون المدني الفرنسي على أن: "كل فعل أياً كان صادر من شخص يُلحق ضرراً بالغير يلزم من وقع الفعل بخطئه بإصلاح هذا الضرر.. كما نصت المادة (1241) من القانون نفسه على أن: "كل شخص مسؤول عن الضرر الذي تسبب فيه ليس فقط بفعله المباشر، بل أيضاً بإهماله أو تهوره".

(4) ينظر في ذلك: اللائحة الأوروبية العامة لحماية البيانات رقم 679/2016، المادة (82)، التي تُقرر حق كل متضرر مادياً أو معنوياً من انتهاك أحكام اللائحة في الحصول على تعويض من المتحكم في البيانات أو المعالج، مع إمكانية

التي تُسهم في معالجة بيانات أصحابها أو في حماية الأنظمة التي تحتوي عليها، قد تجد نفسها في مواجهة مسؤولية مزدوجة: مسؤولية تقصيرية بموجب القانون المدني، ومسؤولية تنظيمية بموجب اللائحة الأوروبية.

وأما فئة الشركاء التجاريين المتضررين، فيُطبّق القضاء الفرنسي معيار التوقع المعقول للضرر في تحديد نطاق المسؤولية تجاههم، إذ يشترط أن يكون الضرر اللاحق بهم نتيجةً متوقعةً للإخلال الأمني في ضوء ظروف كل حالة. وفيما يتعلق بالفئة الثالثة وهم المتضررون بصورة غير مباشرة، فإن الفقه الفرنسي يتناول هذه الإشكالية في سياق نظرية الضرر المرتد، ويشترط لقيام المسؤولية تجاه هؤلاء أن يكون ضررهم شخصياً ومباشراً وثابتاً، لا مجرد ضرر محتمل أو منعكس⁽¹⁾.

أما على مستوى القانون العراقي، فيُعالج القانون المدني العراقي مسؤولية شركة الأمن السيبراني تجاه الغير في إطار القواعد العامة للمسؤولية التقصيرية المقررة في المادة (204) منه، التي تُقرر أن كل تعدٍ يصيب الغير بأي ضرر يستوجب التعويض⁽²⁾. وفي سياق عقود الأمن السيبراني، يُستخلص الخطأ الموجب للمسؤولية تجاه الغير من إخلال الشركة بواجب عام للحماية والحذر يفرضه عليها مركزها المتخصص، ويتمثل هذا الواجب في اتخاذ التدابير الكافية لمنع امتداد آثار الاختراق الأمني إلى ما يتجاوز نطاق نظام العمل المباشر.

وبالنسبة لفئة عملاء الشركة المتعاقدة الذين تُخزّن بياناتهم في أنظمة هذه الأخيرة، فإن الضرر اللاحق بهم جراء انكشاف بياناتهم أو استغلالها يُعدّ ضرراً مباشراً تترتب عليه المسؤولية التقصيرية لشركة الأمن السيبراني متى ثبت إخلالها بواجب الحماية المنوط بها. وقد أضاف قرار مجلس المفوضين

الإعفاء من المسؤولية إذا أثبت هؤلاء انتفاء مسؤوليتهم عن الحادثة المسببة للضرر. متاح على الرابط: [https://gdpr-](https://gdpr-info.eu/art-82-gdpr)

[info.eu/art-82-gdpr](https://gdpr-info.eu/art-82-gdpr) . تاريخ اخر زيارة في 2026/6/14

⁽¹⁾ يُنظر في مبدأ اشتراط أن يكون الضرر الموجب للتعويض شخصياً ومباشراً في القانون الفرنسي وفي نظرية الضرر المرتد وشروط قيامها:

Cour de cassation, Chambre civile 2, 3 novembre 2011, n° de pourvoi 10-16.036, Publié au bulletin, disponible sur: <https://www.legifrance.gouv.fr> تاريخ اخر زيارة في 2026/6/14

فقد أقرّت محكمة النقض الفرنسية أن الضرر المرتد الذي يصيب الغير لا يتجلى في كامل نطاقه إلا من تاريخ استقرار الضرر الأصلي، مما يؤكد أن المسؤولية تجاه المتضررين بصورة غير مباشرة تستلزم ثبوت الضرر الأصلي المباشر أولاً وقيام رابطة سببية وثيقة تربطه به.

⁽²⁾ تنص المادة (204) من القانون المدني العراقي على أن: " كل تعدٍ يصيب الغير بأي ضرر آخر غير ما ذكر في المواد السابقة يستوجب التعويض".

رقم (33) لسنة 2025 بعداً تنظيمياً لهذه المسؤولية، إذ يلزم الشركات بالإبلاغ عن أي خرق أمني للجهات المختصة، بما يُتيح لأصحاب البيانات المتضررين الاستناد إلى هذا الإخلال التنظيمي دليلاً على توافر ركن الخطأ في دعوى المسؤولية التقصيرية⁽¹⁾.

وأما فئة الشركاء التجاريين والمتضررين بصورة غير مباشرة، فتحكمها المادة (205) من القانون المدني العراقي التي تُقرر أن الضرر الموجب للتعويض يشمل الضرر المادي والضرر الأدبي، بشرط أن يكون الضرر محققاً ومباشراً ومتصلاً برابطة سببية وثيقة بالخطأ المنسوب للشركة⁽²⁾. وفي غياب نص خاص يُنظم توزيع المسؤولية بين شركة الأمن السيبراني وعميلها في مواجهة الغير، تبقى القواعد العامة للمسؤولية التقصيرية هي المرجع الأساسي، مما يُفسح المجال للقاضي العراقي في تقدير نطاق هذه المسؤولية وفق ظروف كل حالة.

تأسيساً على ما سبق، يلاحظ أن ثمة توجهاً مشتركاً نحو الاعتراف بمسؤولية شركة الأمن السيبراني تجاه الغير، غير أن النظم الثلاثة تتباين في آليات تأسيس هذه المسؤولية وتحديد نطاقها. فالقانون الأمريكي يُعَوِّل على مبدأ التوقع المعقول للضرر أداةً لتحديد نطاق واجب العناية المستحق للغير، في حين يستند القانون الفرنسي إلى ازدواجية المصادر بين القواعد المدنية العامة والتنظيمات الخاصة بحماية البيانات لتوسيع نطاق الحماية المقررة للغير. أما القانون العراقي، فيركز على القواعد العامة للمسؤولية التقصيرية مع ما يُضيفه التنظيم الخاص من أدوات إثبات تُيسِّر على الغير المتضرر إقامة دعواه. والقاسم المشترك بين النظم الثلاثة هو أن نطاق مسؤولية الشركة تجاه الغير يتسع كلما كانت الأضرار المحتملة على الغير متوقعة ومعلومة للشركة وقت الإخلال، ويضيق كلما كانت هذه الأضرار بعيدة أو غير متوقعة بصورة معقولة.

وفيما يتعلق بنطاق التعويض المستحق للغير في الأنظمة الثلاثة، يتباين هذا النطاق تبايناً ملحوظاً في ضوء القواعد الحاكمة لكل نظام. ففي القانون الأمريكي، يمتد التعويض ليشمل الأضرار المالية المباشرة الناجمة عن انكشاف البيانات، وتكاليف الحماية المستقبلية، وأضرار سرقة الهوية المحتملة،

(1) قرار مجلس المفوضين في هيئة الاتصالات والإعلام العراقية رقم (33) لسنة 2025، المادة (12/ثانياً/17)، التي تلزم شركات الأمن السيبراني بإعلام الجهات المختصة في حال حدوث أي خرق أمني، بما يُتيح لأصحاب البيانات المتضررين الاستناد إلى هذا الإخلال التنظيمي دليلاً على توافر ركن الخطأ في دعوى المسؤولية التقصيرية.

(2) تنص الفقرة الأولى من المادة (205) من القانون المدني العراقي على أن: "1- يتناول حق التعويض الضرر الأدبي كذلك فكل تعد على الغير في حريته أو في عرضه أو في شرفه أو في سمعته أو في مركزه الاجتماعي أو في اعتباره المالي يجعل المتعدي مسؤولاً عن التعويض". كذلك ينظر: د. عبد المجيد الحكيم. عبد الباقي البكري، القانون المدني وأحكام الالتزام، ج2، وزارة التعليم العالي والبحث العلمي، ص58.

شريطة أن يكون الضرر متوقعاً بصورة معقولة وأن تقوم رابطة سببية وثيقة بينه وبين الإخلال الأمني المنسوب للشركة⁽¹⁾. أما في القانون الفرنسي، فيشترط لقيام التعويض أن يكون الضرر اللاحق بالغير شخصياً ومباشراً وثابتاً وفق ما تقتضيه المادة (1240) من القانون المدني، إذ لا يُعوّض عن الضرر المحتمل أو المنعكس ما لم يستقر وتتحدد معالمه⁽²⁾. وأما في القانون العراقي، فتحكم نطاق التعويض المادة (205) من القانون المدني التي تشترط أن يكون الضرر محققاً ومباشراً ومتصلاً برابطة سببية وثيقة بالخطأ المنسوب للشركة، بما يشمل الضرر المادي والضرر الأدبي على حدٍ سواء⁽³⁾.

المطلب الثاني

المسؤولية الناجمة عن الانتهاك القانوني والتنظيمي

لا تقتصر المسؤولية القانونية لشركات الأمن السيبراني على ما يترتب من آثار في مواجهة العملاء والغير جراء الإخلال بالالتزامات الأساسية، بل تمتد لتشمل بُعداً آخر لا يقل أهمية، يتصل بالانتهاك القانوني والتنظيمي الذي يُخلّ بالنظام العام الرقابي الذي أرسته الدولة في مجال الأمن السيبراني. فشركة الأمن السيبراني لا تعمل في فراغ تنظيمي، بل تمارس نشاطها في ظل منظومة من الالتزامات القانونية والتنظيمية التي تفرضها جهات الرقابة المختصة، وتُحدد من خلالها معايير الأداء المهني ومتطلبات الامتثال الواجبة. والإخلال بهذه الالتزامات يُنشئ مسؤولية مستقلة تختلف في طبيعتها وأساسها عن المسؤولية العقدية أو التقصيرية، إذ هي مسؤولية تنبثق من مخالفة قواعد آمرة وضعتها الدولة لحماية المصلحة العامة لا مجرد مصلحة طرف خاص. وتتشعب هذه المسؤولية على مستويين متميزين؛ فعلى المستوى الأول تقع المسؤولية على الشركة بوصفها شخصاً معنوياً في مواجهة الجهات الرقابية المختصة، إذ يُرتب الانتهاك التنظيمي جزاءات تمس وجودها القانوني وترخيصها في ممارسة النشاط. وعلى

(1) يُنظر في نطاق التعويض المستحق للغير في القانون الأمريكي وامتداده ليشمل الأضرار المستقبلية المحتملة:

Remijas v. Neiman Marcus Group, LLC, No. 14-3122, United States Court of Appeals for the Seventh Circuit, decided July 20, 2015.

Cornell Law School, Legal Information Institute, "Duty of Care", last reviewed March 2026, available at: https://www.law.cornell.edu/wex/duty_of_care. تاريخ اخر زيارة في 2026/6/14

(2) Cour de cassation, Chambre civile 2, 3 novembre 2011, n° de pourvoi 10-16.036, Publié au bulletin, disponible sur: <https://www.legifrance.gouv.fr>. تاريخ اخر زيارة في 2026/6/14

(3) طارق عبد العزيز العبيدي، الضرر الادبي وكيفية إثباته في المسؤولية التقصيرية، دراسة في القانون العراقي، مجلة كلية القانون للعلوم القانونية والسياسية، مجلد 1، عدد 2، 2012، ص 149.

المستوى الثاني تنزل المسؤولية على الأشخاص الطبيعيين المكلفين بالإدارة والتنفيذ الفني داخل الشركة، إذ لا يحول الستار القانوني للشخص المعنوي دون مساءلة من أسهموا بقراراتهم أو إهمالهم في الانتهاك التنظيمي. وعليه يتفرع هذا المطلب إلى فرعين، يتناول الأول المسؤولية القانونية للشركة ككيان معنوي أمام الجهات الرقابية، ويُخصص الثاني للمسؤولية الفردية للإدارة والفنيين.

الفرع الأول

المسؤولية القانونية للشركة ككيان معنوي أمام الجهات الرقابية

تُمثّل مسؤولية شركة الأمن السيبراني ككيان معنوي أمام الجهات الرقابية وجهاً متميزاً من وجوه المسؤولية القانونية، يختلف في طبيعته وأساسه عما سبق دراسته من مسؤولية عقدية أو تقصيرية. فبينما تنشأ هاتان الأخيرتان من الإخلال بالتزام خاص في مواجهة أطراف بعينها، تنبثق المسؤولية الرقابية من مخالفة قواعد أمرة وضعتها الدولة لحماية المصلحة العامة في مجال الأمن الرقمي، وتترتب عليها جزاءات تمس الوجود القانوني للشركة وترخيصها في ممارسة نشاطها. وما يُضفي على هذه المسؤولية خصوصية بالغة هو أن الشركة لا تواجه هنا طرفاً خاصاً يطالب بحق شخصي، وإنما تواجه سلطة عامة تتولى الرقابة على القطاع وتسهر على ضمان مستوى الأمان الرقمي في المجتمع.

أنشأ المشرّع الأمريكي منظومة رقابية متكاملة لمراقبة نشاط شركات الأمن السيبراني وضمان امتثالها للمعايير المهنية المعتمدة، يتصدرها المركز الوطني للتكامل في الأمن السيبراني والاتصالات التابع لوكالة الأمن السيبراني وأمن البنية التحتية. وقد حدّدت المادة (659) من القانون الأمريكي للأمن الداخلي وظائف هذا المركز الرقابية تحديداً دقيقاً، إذ أناطت به مهمة التنسيق متعدد القطاعات في مواجهة مخاطر الأمن السيبراني والحوادث التي قد تترتب على إخفاق مزودي الخدمات الرقمية، فضلاً عن صلاحية تقديم المساعدة الفنية العملية للجهات المتضررة من الحوادث السيبرانية، حيث نصت الفقرة (ج) من النص المذكور على أن: "ان يكون واجهة مدنية فيدرالية للتبادل متعدد الاتجاهات والقطاعات للمعلومات المتعلقة بمؤشرات التهديدات السيبرانية والتدابير الدفاعية ومخاطر الأمن السيبراني والحوادث والتحليلات والتحذيرات للجهات الفيدرالية وغير الفيدرالية"، وكذلك "تقديم المساعدة التقنية العملية ودعم إدارة المخاطر وقدرات الاستجابة للحوادث للجهات الفيدرالية وغير الفيدرالية عند الطلب"⁽¹⁾.

(1) النص باللغة الإنجليزية:

وتتجلى طبيعة المسؤولية الرقابية لشركة الأمن السيبراني في القانون الأمريكي من خلال محورين الأول يتصل بالتزامات الإبلاغ والإخطار التي تفرضها الجهات الرقابية على هذه الشركات، والثاني يتعلق بالجزاء المترتبة على الإخلال بهذه الالتزامات. ففيما يخص المحور الأول، تلتزم شركات الأمن السيبراني بالإبلاغ الفوري عن الحوادث السيبرانية للمركز الوطني، الذي يضطلع بدوره بمهمة تجميع هذه التقارير وتحليلها وتوظيفها في تعزيز الوعي الظرفي بالتهديدات السيبرانية عبر قطاعات البنية التحتية الحيوية، حيث نصت المادة (659/ج/13) من القانون الأمريكي للأمن الداخلي، التي تنص على أن المركز يضطلع بمهمة "استقبال التقارير المتعلقة بالحوادث السيبرانية وتجميعها وتحليلها بما يعزز الوعي الظرفي بالتهديدات السيبرانية عبر قطاعات البنية التحتية الحيوية"⁽¹⁾. وفيما يخص المحور الثاني، تمتد صلاحيات المركز الرقابية لتشمل استخدام سلطة الاستدعاء القضائي في مواجهة الجهات التي تُخفق في الامتثال لمتطلبات الإفصاح، إذ خوّلت المادة (659/ب) مدير المركز صلاحية إصدار أوامر قضائية للحصول على المعلومات اللازمة لتحديد الجهات المعرضة للخطر السيبراني وإخطارها، حيث نصت على أنه: "إذا حدّد المدير نظاماً متصلاً بالإنترنت يعاني من ثغرة أمنية محددة وتعدّر عليه تحديد الجهة المالكة أو المشغلة، جاز له إصدار أمر استدعاء قضائي للحصول على المعلومات اللازمة لتحديد هذه الجهة وإخطارها"⁽²⁾.

6 U.S. Code § 659 (c), National cybersecurity and communications integration center, which provides that the cybersecurity functions of the Center shall include: "being a Federal civilian interface for the multi-directional and cross-sector sharing of information related to cyber threat indicators, defensive measures, cybersecurity risks, incidents, analysis, and warnings for Federal and non-Federal entities" and "upon request, providing operational and timely technical assistance, risk management support, and incident response capabilities to Federal and non-Federal entities".

(1) النص باللغة الإنجليزية:

6 U.S. Code § 659 (c)(13), which provides that the Center shall be responsible for "receiving, aggregating, and analyzing reports related to covered cyber incidents submitted by covered entities in furtherance of enhancing the situational awareness of cybersecurity threats across critical infrastructure sectors".

(2) النص باللغة الإنجليزية:

6 U.S. Code § 659 (p)(2)(A), which provides that "if the Director identifies a system connected to the internet with a specific security vulnerability and is unable to identify the entity at risk

ويلاحظ في هذا الإطار أن المسؤولية الرقابية للشركة في القانون الأمريكي لا تتوقف عند حد الجزاء المادي، بل تمتد لتشمل التزامات إيجابية مستمرة تفرض على الشركة التعاون الفعّال مع الجهات الرقابية وتزويدها بالمعلومات الجوهرية في الوقت المناسب. ومؤدى ذلك أن الشركة التي تُخفق في الوفاء بهذه الالتزامات تجد نفسها في مواجهة منظومة متكاملة من الجزاءات، تبدأ بالإنذار وتتم بالغرامات وقد تصل إلى تعليق الترخيص أو إلغائه في الحالات الجسيمة، حيث نصت المادة (681ب/أ/1) من القانون الأمريكي للأمن الداخلي، التي تنص على أن "الجهة المشمولة التي تتعرض لحادثة سيبرانية مشمولة تلتزم بالإبلاغ عنها للوكالة في غضون 72 ساعة من اللحظة التي تعتقد فيها اعتقاداً معقولاً بوقوع الحادثة"، وكذلك المادة (681ب/ج/8) التي تُقرر أن آليات الإنفاذ تشمل "إجراءات الاستحواذ والتعليق والإلغاء" فضلاً عن "غيرها من آليات الإنفاذ المتاحة بما فيها معالجة حالات عدم الامتثال الأخرى"⁽¹⁾.

أما القانون الفرنسي، فيُرسى النظام الفرنسي منظومة رقابية متخصصة تضطلع بها الوكالة الوطنية لأمن نظم المعلومات، التي تتولى الإشراف على نشاط شركات الأمن السيبراني المرخصة والتحقق من استمرار امتثالها للمعايير التي منحت على أساسها التأهيل. وتُشكّل المادة (15) من مرسوم تأهيل منتجات وخدمات الأمن السيبراني الركيزة التشريعية الأساسية لهذه المسؤولية الرقابية، إذ تُخول الوكالة صلاحية التحقق في أي وقت من مدى احترام الشركة للقواعد التي منحت التأهيل على أساسها، وتُلزم الشركة في المقابل بإخطار الوكالة فوراً عن أي تعديل في الظروف التي مُنح التأهيل في ضوءها، فقد نصت المادة (15) من المرسوم الفرنسي على أن "الوكالة الوطنية لأمن نظم المعلومات يجوز لها في أي وقت التحقق من احترام مزود الخدمة للقواعد التي مُنح التأهيل على أساسها، ويلتزم المزود بإخطار الوكالة فوراً عن أي تعديل في الظروف التي مُنح التأهيل في ضوءها، وفي حال الإخلال بالشروط والتحفظات المرتبطة بقرار التأهيل أو تغيير الظروف القانونية أو الواقعية، يجوز للمدير العام للوكالة بعد إتاحة الفرصة للمزود لعرض

that owns or operates such covered device or system, the Director may issue a subpoena for the production of information necessary to identify and notify such entity at risk".

(1) النص باللغة الإنجليزية:

6 U.S. Code § 681b (a)(1)(A), which provides that "a covered entity that experiences a covered cyber incident shall report the covered cyber incident to the Agency not later than 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred"; and § 681b (c)(8)(B), which provides that enforcement mechanisms shall include "acquisition, suspension and debarment procedures" and "other available enforcement mechanisms including other aspects of noncompliance".

ملاحظاته تعليق التأهيل أو إلغاؤه⁽¹⁾.

وتكتسب هذه المسؤولية الرقابية طابعاً مشدداً من خلال ما تُقرره المادة (15) ذاتها من جزاء تعليق التأهيل أو إلغاؤه في حال ثبوت الإخلال بالشروط والتحفظات المرتبطة بقرار التأهيل أو تغيير الظروف القانونية أو الواقعية التي مُنح في ضوءها. وما يُضفي على هذا الجزاء أهمية بالغة في سياق المسؤولية المدنية هو أن تعليق التأهيل أو إلغاؤه لا يقتصر أثره على العلاقة بين الشركة والجهة الرقابية، بل يمتد ليلقي بظلاله على العلاقات التعاقدية القائمة بين الشركة وعملائها، إذ يُجيز لهؤلاء التمسك بقرار التعليق أو الإلغاء دليلاً على توافر ركن الخطأ في دعوى المسؤولية العقدية⁽²⁾.

ويتعزز هذا النظام الرقابي بما تفرضه المادة (10) من المرسوم ذاته من آلية تقييم دورية لخدمات الشركة وفق المعايير الفنية المعتمدة من الوكالة، تشمل مراجعة الوثائق والفحص الميداني وتقييم الكوادر البشرية والتقنية. ومؤدى ذلك أن الشركة تخضع لرقابة مستمرة لا تنتهي بمنح التأهيل، بل تلازمها طوال مدة ممارسة نشاطها، بما يجعل الإخلال بأي متطلب من متطلبات الامتثال مدخلاً للمسؤولية الرقابية،

(1) النص باللغة الفرنسية:

Décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité nationale, article 15, qui dispose que: "L'Agence nationale de la sécurité des systèmes d'information peut s'assurer à tout moment que le prestataire respecte les règles au vu desquelles il a été qualifié. Le prestataire l'informe sans délai de toute modification des circonstances dans lesquelles il a été qualifié. En cas de manquement aux conditions et réserves fixées par la décision de qualification ou en cas de changement des circonstances de droit ou de fait dans lesquelles le prestataire a été qualifié, le directeur général de l'Agence nationale de la sécurité des systèmes d'information peut, après que le prestataire a pu faire valoir ses observations, suspendre ou abroger la qualification".

(2) يُنظر في أثر الجزاء الإداري على المسؤولية المدنية في القانون الفرنسي، إذ يستقر الفقه الفرنسي على أن قرار تعليق التأهيل أو إلغاؤه الصادر عن الجهة الرقابية يُشكّل قرينة على توافر ركن الخطأ في دعوى المسؤولية العقدية، استناداً إلى المبدأ العام المقرر في المادة (1240) من القانون المدني الفرنسي التي تلزم كل من أخلّ بواجبه بإصلاح الضرر الناجم عن إخلاله:

; Code civil français, article 1240, available at: <https://www.legifrance.gouv.fr>

وكذلك: Décret n° 2015-350 du 27 mars 2015, article 15, available at:

<https://www.legifrance.gouv.fr> . تاريخ اخر زيارة في 2026/6/14

حيث تشير المادة (10)، المعدلة بموجب المرسوم رقم 384-2018، التي تنص على أن "خدمات مزود الخدمة تُقيّم وفق قواعد محددة في مرجعيات خاصة بكل نوع من الخدمات، وتُجرى عملية التقييم ميدانياً وعلى الوثائق من قبل مركز تقييم معتمد، وتهدف إلى التحقق من أن المزود يحترم القواعد المقررة، ولا سيما أنه يمتلك الكوادر البشرية الكفوة والوسائل التقنية والمرافق الملائمة لتقديم خدماته"⁽¹⁾.

في العراق، يستند النظام الرقابي على شركات الأمن السيبراني في العراق إلى الإطار التنظيمي الذي أرساه قرار مجلس المفوضين في هيئة الاتصالات والإعلام رقم (33) لسنة 2025، الذي يُشكّل المرجعية التنظيمية الأساسية لتحديد الالتزامات الرقابية الواقعة على عاتق هذه الشركات وتحديد الجزاءات المترتبة على الإخلال بها. وعلى الرغم من أن هذا القرار يندرج في إطاره العام ضمن التنظيم الإداري لقطاع الاتصالات والإعلام، إلا أن أثره يتجاوز هذا الإطار ليمتد إلى تحديد معيار موضوعي لمستوى الأداء المهني المطلوب من شركات الأمن السيبراني، يمكن توظيفه في تقدير المسؤولية المدنية أمام القضاء.

وتتجلى أبرز ملامح المسؤولية الرقابية لشركة الأمن السيبراني في القانون العراقي من خلال الالتزامات التي أوردتها القرار في المادة (12) منه، والتي تشمل مراجعة سياسات الأمان السيبراني بشكل منتظم وتقديم تقارير فصلية عن الأنشطة لضمان تقييم مستمر، فضلاً عن إلزام المرخص له بإعلام الجهات المختصة في حال حدوث أي خرق أمني وفق ما نصت عليه الفقرة (17) من البند (ثانياً) من المادة ذاتها⁽²⁾. ويُرتب الإخلال بهذه الالتزامات مسؤولية إدارية تتمثل في صلاحية الهيئة في تعليق الترخيص أو إلغائه، بما يُفضي إلى آثار قانونية مدنية مباشرة تطل العالقات التعاقدية القائمة بين الشركة وعملائها.

(1) النص باللغة الفرنسية:

Décret n° 2015-350 du 27 mars 2015, article 10, modifié par Décret n°2018-384 du 23 mai 2018, qui dispose que: "Les services fournis par le prestataire sont évalués au regard de règles fixées par des référentiels propres à chaque type de services. L'évaluation est réalisée sur pièce et sur place par un centre d'évaluation agréé. Elle vise à s'assurer que le prestataire respecte les règles prévues par les référentiels mentionnés au premier alinéa, en particulier qu'il dispose du personnel compétent ainsi que des moyens techniques et des locaux adéquats pour fournir ses services".

(2) نصّت الفقرة (6) من المادة (12) من قرار مجلس المفوضين على ان: "التقارير والرصد: تقوم الهيئة بإصدار أدوات التقييم وقياس الالتزام لقياس مدى التزام الجهات بتطبيق الضوابط الأساسية للأمن السيبراني وتقييمها دورياً"، اما الفقرة (12) من المادة ذاتها فقد نصت على ان: "المراجعة والتقييم الدوري ينبغي على المرخص له مراجعة وتقييم سياسات الأمان السيبراني وإجراءاتها بانتظام لضمان الامتثال المستمر وتحسين الأداء وتقديم التقارير الفصلية عن نشاطاته لغرض التقييم



ويُلاحظ في هذا الإطار أن المنظومة الرقابية العراقية لا تزال في طور البناء والتطور، إذ يُشكّل قرار مجلس المفوضين رقم (33) لسنة 2025 الخطوة التأسيسية الأولى نحو إرساء إطار تنظيمي متكامل، غير أنه يظل دون المستوى الذي بلغته النظم المقارنة من حيث تفصيل الجزاءات وآليات تطبيقها. وهو ما يدفع إلى القول بضرورة استكمال هذا الإطار التنظيمي بنصوص أكثر تفصيلاً تُحدد الجزاءات الإدارية بصورة واضحة وتضمن فعالية الرقابة على هذا القطاع الحساس.

يتضح مما سبق، أن ثمة قاسماً مشتركاً يجمعها، يتمثل في الاعتراف بأن شركة الأمن السيبراني لا تخضع لرقابة الأطراف الخاصة وحدها، بل تخضع كذلك لرقابة الجهات العامة المختصة التي تسهر على ضمان مستوى الأمان الرقمي في المجتمع. غير أن النظم الثلاثة تتفاوت في درجة تطور هذه الرقابة وفعاليتها؛ فالنظام الأمريكي يمتاز بشمولية المنظومة الرقابية وتنوع أدواتها من إبلاغ وتحليل واستدعاء قضائي، في حين يتميز النظام الفرنسي بدقة معايير التأهيل وصرامة آليات مراجعتها، أما النظام العراقي فلا يزال في مرحلة التأسيس وإن كان قد وضع اللبنة الأولى نحو منظومة رقابية متكاملة. والمحصلة أن مسؤولية شركة الأمن السيبراني أمام الجهات الرقابية تُعدّ ركناً أساسياً في منظومة المسؤولية القانونية الشاملة لهذه الشركات، لا يمكن فهم هذه المنظومة في كمالها دون استيعاب هذا البُعد الرقابي وما يترتب عليه من آثار مدنية وإدارية متشابكة.

ولا تقتصر آثار الانتهاك التنظيمي على الجزاء الإداري، بل تمتد لثُرتب مسؤولية مدنية مستقلة متى توافرت أركانها الثلاثة. ففي القانون الأمريكي، يتحدد الضرر الناجم عن الانتهاك التنظيمي في الخسائر المالية المباشرة التي يتكبدها العملاء جراء الإخفاق الأمني، وتقوم رابطة السببية متى ثبت أن الامتثال للمعايير التنظيمية كان كفيلاً بمنع وقوع الضرر أو تقليل أثره، ويمتد التعويض ليشمل تكاليف الاستجابة للحادثة والأضرار السمعية القابلة للتقييم المالي⁽¹⁾. أما في القانون الفرنسي، فيُشكّل قرار تعليق

وإعادة التصنيف"، كذلك نصت الفقرة (17) من ذات المادة على أن: "إعلام الجهات المختصة في حال حدوث أي مشكلة فنية أو خلل أمني في أي من النشاطات التي تقدمها هذه الشركات".

⁽¹⁾ يُنظر في نطاق التعويض المستحق في دعاوى الإخفاق الأمني في القانون الأمريكي، إذ استقر القضاء الأمريكي على أن الأضرار القابلة للتعويض لا تقتصر على الخسارة المالية المباشرة، بل تمتد لتشمل تكاليف الحماية المستقبلية وأضرار سرقة الهوية المحتملة وتكاليف مراقبة الائتمان، وذلك متى قامت رابطة سببية معقولة بين الإخفاق الأمني وهذه الأضرار، وقد كرّست محكمة الاستئناف الأمريكية للدائرة السابعة هذا التوجه في قضية ريمياس ضد مجموعة نيومان ماركوس حين اعترفت بحق أصحاب البيانات المسربة في المطالبة بالتعويض عن أضرار الانكشاف المستقبلية رغم عدم تحققها بعد وقت رفع الدعوى:

Remijas v. Neiman Marcus Group, LLC, No. 14-3122, United States Court of Appeals for the Seventh Circuit, decided July 20, 2015, available at:

التأهيل أو إلغائه قرينةً على توافر ركن الخطأ في دعوى المسؤولية المدنية، ويترتب التعويض على الأضرار المباشرة والفورية التي لحقت بالعملاء جراء الانتهاك وفق صريح المادة (1231-4) من القانون المدني الفرنسي. وأما في القانون العراقي، فيُلزم الإخلال بالتزامات الإبلاغ المقررة في قرار مجلس المفوضين رقم (33) لسنة 2025 الشركة بالتعويض متى ثبت أن هذا الإخلال أفضى إلى تفاقم الضرر أو تعدّر تداركه في الوقت المناسب⁽¹⁾.

الفرع الثاني

المسؤولية الفردية للإدارة والفنيين

لا يكفي في تحديد نطاق المسؤولية القانونية لشركات الأمن السيبراني الوقوف عند حدود الشخص المعنوي ومساءلته أمام الجهات الرقابية، إذ كثيراً ما تجد المسؤولية طريقها إلى الأشخاص الطبيعيين الذين يتولون الإدارة أو يضطلعون بالتنفيذ الفني داخل الشركة. فالشركة في نهاية المطاف لا تتصرف من تلقاء ذاتها، وإنما تتجسد إرادتها وقراراتها من خلال أفراد بعينهم، سواء أكانوا في مواقع الإدارة العليا أم في المستويات الفنية التنفيذية. ومن هنا تنشأ إشكالية قانونية جوهرية تتمحور حول مدى إمكانية مساءلة هؤلاء الأفراد مسؤولية شخصية مستقلة عن مسؤولية الشركة، وما هي الشروط التي يجب توافرها لرفع الستار عن الشخص المعنوي والنفوذ إلى الأشخاص الطبيعيين وراءه، وتكتسب هذه المسألة أهمية عملية بالغة في سياق الأمن السيبراني، إذ إن الإخفاق الأمني كثيراً ما يعود في جذوره إلى قرارات فردية صادرة عن مديرين أو إلى تقصير فني مرده إلى أخطاء موظفين متخصصين. ولا يكفي في هذا السياق الاكتفاء بمساءلة الشركة ككيان معنوي، لا سيما حين يكون الضرر ناجماً عن سلوك شخصي يتجاوز حدود الوظيفة أو ينطوي على إهمال جسيم أو قصد إضرار.

<https://law.justia.com/cases/federal/appellate-courts/ca7/14-3122/14-3122-2015-07-20.html>

تاريخ آخر زيارة في 2026/6/14

⁽¹⁾ ويجدر الإشارة إلى أن التنظيم العراقي لنشاط شركات الأمن يفتر إلى نص صريح يُرتب المسؤولية المدنية على الإخلال بالالتزامات التنظيمية في مجال الأمن السيبراني، مما يقتضي الرجوع إلى القواعد العامة للمسؤولية التقصيرية المقررة في المادة (204) من القانون المدني العراقي التي تُقرر أن كل تعدٍ يصيب الغير بأي ضرر يستوجب التعويض، ويمكن توظيف الإخلال بالتزامات الإبلاغ المنصوص عليها في المادة (12/ثانياً/17) من قرار مجلس المفوضين رقم (33) لسنة 2025 دليلاً على توافر ركن الخطأ في دعوى المسؤولية المدنية، لا سيما متى ثبت أن هذا الإخلال أفضى إلى تفاقم الضرر أو تعدّر تداركه في الوقت.

يُعالج القانون الأمريكي مسألة المسؤولية الفردية للإدارة والفنيين في شركات الأمن السيبراني في إطار مبدئين متكاملين: مبدأ المسؤولية الشخصية المستقلة من جهة، ومبدأ رفع الستار عن الشخص المعنوي من جهة أخرى. فوفق المبدأ الأول، يمكن مساءلة المدير أو الفني مسؤولية شخصية متى كان الضرر الواقع ناجماً عن فعله الشخصي المباشر لا عن مجرد قراره بوصفه ممثلاً للشركة، وهو ما يُعبر عنه في القانون الأمريكي بمفهوم المسؤولية الشخصية المستقلة للمدير أو الموظف، القائمة على إخلاله بواجب الأمانة المهنية الذي يفرضه عليه مركزه داخل الشركة⁽¹⁾. ووفق المبدأ الثاني، يجوز رفع الستار عن الشخص المعنوي ومساءلة الأشخاص الطبيعيين وراءه متى ثبت أن الشركة استخدمت غطاءً للتهرب من المسؤولية أو أن ثمة اندماجاً بين شخصية الشركة وأشخاص مسيرتها⁽²⁾.

وفيما يخص المديرين التنفيذيين تحديداً، فقد استقر القضاء الأمريكي على أن المدير الأعلى للأمن المعلوماتي يتحمل مسؤولية شخصية متى ثبت أنه أخفق في اتخاذ التدابير الأمنية الكافية رغم علمه بالمخاطر القائمة، أو أنه أدلى بتصريحات مضللة للمساهمين أو الجهات الرقابية حول مستوى الأمان الفعلي للشركة، ولا يكفي في هذا الشأن الاحتجاج بالصفة الوظيفية ما دام الإخلال شخصياً ومتجاوزاً حدود ما تقتضيه الوظيفة⁽³⁾. وأما على مستوى الفنيين، فإن مسؤوليتهم الشخصية تنشأ حين يثبت أن الخطأ الفني الصادر عنهم يتجاوز حدود الخطأ المهني العادي ليلعب مستوى الإهمال الجسيم أو التعمد، وهو ما يستوجب تطبيق قواعد المسؤولية التقصيرية في مواجهتهم بصورة مستقلة عن مسؤولية الشركة⁽⁴⁾.

(1) يخضع مديرو الشركات لواجبات أمانة تشمل واجب الطاعة وواجب الولاء وواجب العناية، وأن الإخلال بهذه الواجبات يُرتب مسؤولية شخصية مستقلة في مواجهة من لحقه الضرر، ولا يجوز للمدير أن يتذرّع بصفته الوظيفية للتهرب من هذه المسؤولية متى كان إخلاله شخصياً ومباشراً.

Cornell Law School, Legal Information Institute, "Fiduciary Duty", last reviewed March 2026, available at: https://www.law.cornell.edu/wex/fiduciary_duty. تاريخ اخر زيارة في 2026/6/14.

(2) تستلزم المحاكم الأمريكية لتطبيق هذا المبدأ توافر سلوك مخالف جسيم كاختلاط الأموال الشخصية بأموال الشركة أو توظيف الشركة غطاءً للتهرب من المسؤولية، وتتباين معايير تطبيق هذا المبدأ من ولاية إلى أخرى غير أنها تتفق جميعاً على أن الستار القانوني للشخص المعنوي لا يحول دون المساءلة الشخصية متى ثبت الاندماج بين شخصية الشركة وشخصية مسيرتها أو استخدمت الشركة أداة للغش والإضرار بالغير:

Cornell Law School, Legal Information Institute, "Piercing the Corporate Veil", , available at: https://www.law.cornell.edu/wex/piercing_the_corporate_veil. تاريخ اخر زيارة في 2026/6/14.

(3) Cornell Law School, Legal Information Institute, "Piercing the Corporate Veil", , available at: https://www.law.cornell.edu/wex/piercing_the_corporate_veil تاريخ اخر زيارة في 2026/6/14.

(4) تنشأ هذه المسؤولية في مواجهته بصورة مستقلة عن مسؤولية الشركة متى ثبت أن إخفاقه كان شخصياً ومباشراً ولا صلة له بمقتضيات الوظيفة، ويُقاس هذا الإخلال بمعيار ما كان سيفعله الشخص المعقول في نفس الظروف والمركز المهني:

أما القانون الفرنسي، فيضع تمييزاً دقيقاً بين مسؤولية الشركة ككيان معنوي ومسؤولية مسيريهام ومستخدميها، إذ تُشكّل نظرية الخطأ المنفصل عن الوظيفة الركيزة الأساسية التي يقوم عليها نظام المسؤولية الفردية في القانون الفرنسي. فوفق هذه النظرية الراسخة في القضاء الفرنسي، لا يُسأل المدير أو الموظف في مواجهة الغير عن الأخطاء التي يرتكبها في إطار مهامه الوظيفية العادية، إذ تتحمل الشركة المسؤولية عن هذه الأخطاء، بوصفها المتنوع المسؤول عن أعمال تابعيه وفق ما تُقرره المادة (1242) من القانون المدني الفرنسي⁽¹⁾. غير أن هذا الحصن الذي يوفره الغطاء الوظيفي يسقط حين يرتكب المدير أو الموظف خطأً منفصلاً عن وظيفته، بمعنى خطأ لا صلة له بمقتضيات العمل أو ينطوي على نية إضرار أو إهمال جسيم يتجاوز ما يمكن نسبته إلى ممارسة الوظيفة⁽²⁾.

وتتجلى تطبيقات هذه النظرية في مجال الأمن السيبراني من خلال حالتين رئيسيتين: الأولى تتعلق بالمدير الذي يتخذ قرارات واعية بتخفيض ميزانية الأمن السيبراني برغم علمه بالمخاطر الجسيمة المترتبة على ذلك، إذ يُعدّ هذا القرار خطأً شخصياً منفصلاً عن الوظيفة لانطوائه على استهتار واضح بسلامة الأنظمة والبيانات. والثانية تتعلق بالفني المتخصص الذي يُخفي عمداً معلومات جوهرية عن ثغرات أمنية اكتشفها، إذ يُشكّل هذا الإخفاء خطأً شخصياً موجباً للمسؤولية في مواجهته بصورة مستقلة⁽³⁾.

Cornell Law School, Legal Information Institute, "Negligence", last reviewed July 2023, , available at: <https://www.law.cornell.edu/wex/negligence>. تاريخ اخر زيارة في 2026/6/14

(1) نصت المادة (5/1242) من القانون المدني الفرنسي على أن "أصحاب العمل والموكّلين مسؤولون عن الضرر الذي يحدثه خدمهم وتابعوهم في الوظائف التي كلّفهم بها".

(2) في قضية السيد أ. ضد شركة سوجيبروم، صدر حكم محكمة النقض الفرنسية الدائرة التجارية بتاريخ 18 سبتمبر 2019، وتتعلق وقائع هذه القضية بمدير شركة ارتكب جريمة التواطؤ في إساءة استخدام أموال الشركة لصالح أطراف ثالثة، فأدين جنائياً وطُوبل بالتعويض، فحاول بدوره الرجوع على الشركة لتحمل تبعات أفعاله. وقد رفضت محكمة النقض هذا الطلب مقررّة أن الخطأ الجنائي العمدي للمدير يُشكّل بحكم طبيعته خطأً منفصلاً عن وظيفته يُرتب مسؤوليته الشخصية المستقلة في مواجهة المتضررين، ولا يجوز له التمسك بصفته الوظيفية للتخلص من هذه المسؤولية أو إلزام الشركة بتحمل تبعاتها، إذ إن الخطأ العمدي المتضمن استخداماً غير مشروع لأموال الشركة هو فعل شخصي للمدير يتحمل وحده تبعاته سواء تجاه الغير أو تجاه الشركة التي اعتقد أنه يتصرف باسمها:

Cour de cassation, Chambre commerciale, 18 septembre 2019, n° de pourvoi: 16-26.962, Publié au bulletin, ECLI:FR:CCASS:2019:CO00659, disponible sur: <https://www.legifrance.gouv.fr>. تاريخ اخر زيارة في 2026/6/14

(3) يشير القضاء الفرنسي الى أن المدير الذي يرتكب خطأً ينطوي على نية إضرار أو إهمال جسيم يتجاوز حدود وظيفته يتحمل مسؤولية شخصية مستقلة في مواجهة المتضررين، ولا تحجب هذه المسؤولية الصفة الوظيفية للمدير ولا السائر

وبالنسبة للقانون العراقي، فإنه يستند القانون المدني العراقي في معالجة مسألة المسؤولية الفردية للإدارة والفنيين إلى القواعد العامة التي تحكم مسؤولية التابع والمتبوع، إذ تُقرر المادة (219) منه مسؤولية كل من يستغل مؤسسةً صناعيةً أو تجاريةً عن الضرر الذي يحدثه مستخدموه متى كان ناشئاً عن تعدي وقع منهم أثناء قيامهم بخدماتهم. وتُشكّل هذه المادة الإطار العام الذي يحكم توزيع المسؤولية بين الشركة وموظفيها، إذ تتحمل الشركة المسؤولية في مواجهة المتضرر عن أعمال موظفيها غير المشروعة، مع احتفاظها بحق الرجوع عليهم فيما دفعته من تعويض⁽¹⁾.

غير أن هذا الإطار العام لا يحول دون مساءلة المدير أو الفني مسؤوليةً شخصيةً مستقلة متى كان الخطأ الصادر عنه يتجاوز نطاق وظيفته ليلبغ مستوى الفعل الضار المنفصل عن مقتضيات العمل، وهو ما تستوعبه المادة (204) من القانون المدني العراقي التي تُقرر مسؤولية كل من يتعدى على الغير بأي ضرر⁽²⁾. ويُعزز هذا التوجه ما أشار إليه قرار مجلس المفوضين رقم (33) لسنة 2025 من اشتراطات تتعلق بالكوادر البشرية المؤهلة داخل شركات الأمن السيبراني، إذ يُستفاد من هذه الاشتراطات أن المسؤولية الفردية للفنيين تتوقف على مدى امتلاكهم للمؤهلات المهنية المطلوبة وإخلالهم بمعايير الأداء الواجبة⁽³⁾.

ويُلاحظ في هذا الإطار أن المنظومة القانونية العراقية تفتقر إلى نص صريح يُنظم بصورة خاصة المسؤولية الفردية للمديرين والفنيين في شركات الأمن السيبراني، مما يُبقي هذه المسألة رهينة القواعد العامة وما نتجته من هامش تقديري للقاضي في تحديد نطاق المسؤولية وتوزيعها بين الشركة وموظفيها. وبناءً على ماتقدم يُلاحظ أنّ هناك توجهاً مشتركاً نحو الاعتراف بمسؤولية فردية مستقلة للمديرين والفنيين في شركات الأمن السيبراني، غير أن هذه الأنظمة تتباين في الأداة القانونية التي توصل إلى هذه النتيجة. فالقانون الأمريكي يُركز على الخطأ الشخصي المنفصل عن الوظيفة ويوسع من نطاق مسؤولية

القانوني للشخص المعنوي، وقد استقر هذا المبدأ في القضاء الفرنسي بوصفه ضماناً جوهرياً لحماية الغير من تصرفات المسيرين المتجاوزة لحدود صلاحياتهم:

Cour de cassation, Chambre commerciale, 18 septembre 2019, n° de pourvoi: 16-26.962, précité, disponible sur: <https://www.legifrance.gouv.fr>. تاريخ اخر زيارة في 2026/6/14

(1) ينظر المادة (219) من القانون المدني العراقي.

(2) المادة (204) من القانون المدني العراقي.

(3) المادة (12/12) ثانياً/12 من قرار مجلس المفوضين في هيئة الاتصالات والإعلام العراقية رقم (33) لسنة 2025، التي تنص على أن: "المراجعة والتقييم الدوري: ينبغي على المرخص له مراجعة وتقييم سياسات الأمان السيبراني وإجراءاتها بانتظام لضمان الامتثال المستمر وتحسين الأداء وتقديم التقارير الفصلية عن نشاطاته لغرض التقييم وإعادة التصنيف".

المسؤول الأعلى للأمن المعلوماتي في ضوء التزاماته الرقابية الخاصة، في حين يستند القانون الفرنسي إلى نظرية الخطأ المنفصل المقررة في القضاء المدني بوصفها الضابط الأساسي لتحديد متى تنفصل مسؤولية الفرد عن مسؤولية الشركة. أما القانون العراقي فيركز على القواعد العامة لمسؤولية المتبوع عن أعمال تابعه مع ما تتيحه المادة (204) من إمكانية مساءلة الفرد مسؤوليةً مستقلة. والقاسم المشترك بين النظم الثلاثة هو أن الستار القانوني للشخص المعنوي لا يحول دون المساءلة الشخصية متى بلغ الخطأ الفردي مستوى الإهمال الجسيم أو التعمد أو الانفصال الواضح عن مقتضيات الوظيفة.

ولا تقتصر المسؤولية الفردية على المساءلة القانونية المجردة، بل تمتد لثرتب التزاماً شخصياً بالتعويض متى توافرت أركانه الثلاثة. ففي القانون الأمريكي، يتحدد الضرر القابل للتعويض في مواجهة المدير أو الفني بما لحق العميل أو الغير من خسائر مالية مباشرة جراء الإهمال الشخصي الثابت، وتقوم رابطة السببية متى ثبت أن قرار المدير أو إهمال الفني كان السبب المباشر للإخفاق الأمني، ويُقدَّر التعويض وفق معيار ما كان سيُنجزه المدير المعقول في نفس الظروف والمركز المهني⁽¹⁾. أما في القانون الفرنسي، فيتربط على ثبوت الخطأ المنفصل عن الوظيفة التزام المدير أو الفني بالتعويض الكامل في مواجهة المتضررين بصورة مستقلة عن مسؤولية الشركة، ولا يُخفف هذا الالتزام الستار القانوني للشخص المعنوي ولا الصفة الوظيفية للمدير⁽²⁾. وأما في القانون العراقي، فتحكم نطاق التعويض الفردي المادة (204) من القانون المدني التي تُقرر مسؤولية كل من يتعدى على الغير بأي ضرر، مع مراعاة أن الشركة تحتفظ بحق الرجوع على الموظف المخطئ فيما دفعته من تعويض استناداً إلى المادة (219) من القانون المدني العراقي.

(1) Cornell Law School, Legal Information Institute, "Negligence", last reviewed July 2023, available at: <https://www.law.cornell.edu/wex/negligence> , تاريخ اخر زيارة في 2026/6/14

Cornell Law School, Legal Information Institute, "Fiduciary Duty", last reviewed March 2026, available at: https://www.law.cornell.edu/wex/fiduciary_duty 2026/6/14 تاريخ اخر زيارة في

(2) يستقر الفقه والقضاء الفرنسيان على أن الخطأ المنفصل عن الوظيفة ينطوي على نية إضرار أو إهمال جسيم يتجاوز حدود الوظيفة ويُرتب مسؤوليةً شخصيةً مستقلة لا تحجبها الصفة الوظيفية للمدير:

Cour de cassation, Chambre commerciale, 18 septembre 2019, n° de pourvoi: 16-26.962, Publié au bulletin, ECLI:FR:CCASS:2019:CO00659, disponible sur: <https://www.legifrance.gouv.fr> . تاريخ اخر زيارة في 2026/6/14

المطالب الثالث

التأمين من المسؤولية المدنية لشركات الأمن السيبراني

بين المطلبان السابقان أسباب قيام مسؤولية شركات الأمن السيبراني، سواء نشأت عن الإخلال بالتزاماتها أم عن الانتهاك القانوني والتنظيمي. غير أن قيام المسؤولية لا يجبر الضرر ما لم يجد المضرور ذمة قادرة على الوفاء بالتعويض. وتشتد هذه المسألة في نشاط هذه الشركات الأمرين ضخامة الخسائر التي تخلفها الحوادث السيبرانية (1) وموقع الشركة في شبكة الأنظمة التي تحميها. فهي تتصل بعدد كبير من العملاء، فيمتد أثر الخطأ الواحد في منظومة الحماية إليهم جميعاً في وقت واحد، فيجاوز ما تحتمله ذمتها. ومن هنا تظهر أهمية التأمين من المسؤولية، الذي يعرفه الفقه بأنه عقد بموجبه يؤمن المؤمن المؤمن له من الأضرار التي تلحق به من جراء رجوع الغير عليه بالمسؤولية⁽²⁾. وهو من التأمين من الأضرار محلة دين في ذمة المؤمن له، لأمالٍ مملوك له؛ فيعزز وظيفة المسؤولية في جبر الضرر، بتوزيع تبعته على مجموع المؤمن لهم بدلاً من أن يتحملها واحد منهم.

ويثير تطبيق أداة التوزيع (التأمين) هذه على نشاط شركات الأمن السيبراني مسألتين الأولى مدى قابلية مسؤوليتها للتأمين في ضوء خصوصية الخطر السيبراني والثانية الآثار التي يترتبها هذا التأمين. وعليه نقسم هذا المطلب على فرعين، نبحث في الأول مدى قابلية مسؤولية شركات الأمن السيبراني للتأمين، ونخصص الثاني لآثار هذا التأمين.

الفرع الأول

مدى قابلية مسؤولية شركات الأمن السيبراني للتأمين

لا ينصرف البحث هنا إلى تأمين شركة الأمن السيبراني من الأضرار التي تصيب أنظمتها هي، وإنما إلى تأمين مسؤوليتها تجاه عملائها والغير. ولا يقبل الخطر التأمين إلا إذا توافرت فيه شروط قانونية

(1) بلغ عدد الشكاوى المقدمة إلى مركز شكاوى جرائم الإنترنت التابع لمكتب التحقيقات الفيدرالي الأمريكي سنة 2024 (859,532) شكاوى، وبلغت الخسائر المبلغ عنها نحو (166) مليار دولار، بزيادة قدرها (33) على السنة السابقة. وهي أرقام تقتصر على ما أبلغ عنه، فلا تعكس الحجم الحقيقي للخسائر، على ما ينبه إليه التقرير نفسه.

ينظر: Federal Bureau of Investigation, Internet Crime Report 2024, pp.3-4.

(2) د. عبدالرزاق احمد السنهوري، الوسيط في شرح القانون المدني الجديد، ج7-م2، ص 1641.

يقتضيها كونه محلاً للعقد، وشروط فنية يقتضيها قيام التأمين على تقدير الاحتمالات وقانون الكثرة . وعليه نبحت مدى توافر هذه الشروط في مسؤولية هذه الشركات القانونية أولاً، ثم الفنية ثانياً.

أولاً: من حيث الشروط القانونية للخطر

يشترط في الخطر المؤمن منه أن يكون احتمالياً، وألا يتعلق بمحض إرادة أحد طرفي العقد، وأن يكون مشروعاً. ونعرض لكل شرط في ضوء خصوصية نشاط هذه الشركات.

أ. الاحتمال وتحديد الواقعة المنشئة للضمان

الاحتمال جوهر عقد التأمين، فلا يصح التأمين من خطر تحقق قبل العقد أو كان مستحيل الوقوع. والخطر في التأمين من المسؤولية مركب لا بسيط، إذ لا يكتمل إلا بأمرين: وقوع الفعل الذي تتعقد به مسؤولية المؤمن له، ومطالبة المضرور له بالتعويض⁽¹⁾. ويترتب على هذا التركيب أن بين نشوء الخطر واكتماله زمناً قد يطول، وهو ما يبلغ مداه في النشاط السيبراني. فالاختراق قد يبقى كامناً في أنظمة العمل أشهراً قبل أن يُكتشف⁽²⁾، ثم تمضي مدة أخرى قبل أن يطالب العميل الشركة بالتعويض. فلا يثور الإشكال في أصل الاحتمال⁽³⁾، بل في تحديد الواقعة التي ينعقد بها الضمان: أهى وقوع الإخلال، أم وقوع الاختراق، أم اكتشافه، أم المطالبة به؟

ففي القانون الأمريكي انقسم القضاء، في الوثائق التي تعقد الضمان بوقوع الحادث، بين من يربطه بالتعرض للضرر ومن يربطه بظهوره. وأخذ بعضه بنظرية «التحريك المستمر» التي تمد الضمان إلى كل الوثائق السارية من وقت التعرض إلى وقت الظهور. ولتفادي هذا الاضطراب يلجأ مؤمنو المسؤولية المهنية إلى وثائق تعقد الضمان بالمطالبة المقدمة خلال مدة الوثيقة⁽⁴⁾، وإلى هذا الصنف تنتمي وثائق شركات الأمن السيبراني. غير أن هذا الأساس لا يزيل الإشكال كله. فالشركة التي تنتقل من مؤمن إلى

⁽¹⁾ د. إبراهيم مضحي أبو هلاله ود. فيصل الشقيرات، التزام المؤمن بالتعويض في التأمين من المسؤولية المدنية: دراسة تحليلية تأسيسية في القانون المدني الأردني، مجلة جامعة الحسين بن طلال للبحوث، مج3، ع2، 2017، ص248.

⁽²⁾ Hervé Tsomevou, « L'assurance du risque cyber dans la zone CIMA », Revue de l'ERSUMA, 2022/1, n°16, p.74.

⁽³⁾ لذلك لا نتفق مع القول بأن الخطر السيبراني «غير احتمالي وإنما عشوائي» لأنه لا يخضع لمعيار محدد في تكرار وقوعه، ينظر: أماني تموز عبد الرحمن الخفاجي، الحماية التأمينية للشركات التجارية من المخاطر السيبرانية، رسالة ماجستير، كلية القانون، جامعة ميسان، 2024، ص51. فالعشوائية عين الاحتمال بمعناه القانوني، وما يفتقده هذا الخطر هو قابلية القياس، وهي شرط فني نبخته في البند (ثانياً/ج).

⁽⁴⁾ Michael D. Green & Brooks M. Hanner, "USA", in Ken Oliphant (ed.), Aggregation and Divisibility of Damage, Springer, 2009, pp.421-422.

آخر قد تجد نفسها بلا غطاء عن اختراق وقع في ظل الوثيقة الأولى ولم يُطالب به إلا بعد انتهائها، ما لم تشمله الوثيقة الثانية بأثر رجعي.

أما المشرع الفرنسي فقد حسم المسألة بنص صريح (المادة L.124-5). فقد خيّر الطرفين بين عقد الضمان بالواقعة الضارة أو بالمطالبة، وجعل لكل منهما حكماً. فإذا عُقد بالمطالبة غطى الوقائع السابقة على العقد مهما بعدت، ما لم يثبت المؤمّن أن المؤمّن له كان عالماً بها وقت الاكتتاب. وامتد الضمان إلى مدة لاحقة لا تقل عن خمس سنوات من انتهاء العقد، بحد لا يقل عن حد السنة الأخيرة⁽¹⁾. وهذا الحل يلئم الخطر السيبراني ملائمة ظاهرة: فهو يغطي الاختراق الكامن الذي جهلته الشركة، ويستبعد ما علمت به وكتمته، ويحمي المضرور من انقضاء الوثيقة قبل اكتشاف الضرر.

أما القانون المدني العراقي فأخصّ نصوصه بالمسألة المادة (1004) الواردة في التأمين ضد المسؤولية، إذ نصت على أنه: «لا ينتج التزام المؤمن أثره في التأمين ضد المسؤولية إلا إذا قام المتضرر بمطالبة المستفيد بعد وقوع الحادث الذي نجمت عنه المسؤولية».

ويتبين من هذا النص أن المشرع جعل مطالبة المتضرر شرطاً لنفاذ الضمان، فلا يكفي وقوع الحادث وحده لإلزام المؤمن. غير أنه لم يبيّن ما إذا كان يلزم أن تقع هذه المطالبة، أو الحادث نفسه، خلال مدة الوثيقة.

وإذا كانت هذه المادة تتصل بتحديد الواقعة المنشئة للضمان، فإن المادة (2/984) تتصل بشرط الاحتمال، إذ تحدد مصير الخطر الذي تحقق قبل التعاقد، فقد نصت على أنه: «ويقع عقد التأمين باطلاً، إذا تبين أن الخطر المؤمن ضده كان قد زال أو كان قد تحقق في الوقت الذي تم فيه العقد، وكان أحد الطرفين على الأقل عالماً بذلك».

ومفهوم هذا النص أن تحقق الخطر قبل التعاقد لا يبطل العقد بذاته، وإنما يبطله إذا اقترن بعلم أحد الطرفين على الأقل. فالاختراق الكامن الذي جهله الطرفان وقت التعاقد لا يبطل العقد. أما علم الشركة به

⁽¹⁾ () تنص المادة L.124-5 من تقنين التأمين الفرنسي (Code des assurances)، بصيغتها النافذة منذ 2 تشرين الثاني 2003، على أنه:

« La garantie est, selon le choix des parties, déclenchée soit par le fait dommageable, soit par la réclamation. Toutefois, lorsqu'elle couvre la responsabilité des personnes physiques en dehors de leur activité professionnelle, la garantie est déclenchée par le fait dommageable. Un décret en Conseil d'Etat peut également imposer l'un de ces modes de déclenchement pour d'autres garanties ».

فبيبطله في الشق المتعلق بهذا الاختراق وحده، إعمالاً لقاعدة البطلان الجزئي في المادة (139)، ويبقى العقد صحيحاً فيما عداه.

غير أن هذين النصين لا يحسمان أي الوثيقتين تضمن الاختراق الذي وقع في ظل وثيقة وطولبت عنه الشركة في ظل أخرى، فيبقى الأمر لشروط الوثيقة التي يضعها المؤمن منفرداً. ولذلك نرى أن يتدخل المشرع بنص يقارب الحل الفرنسي: يجيز تحريك الضمان بالمطالبة، ويفرض مدة لاحقة لا يجوز النزول عنها، ويستبعد ما علم به المؤمن له قبل التعاقد.

ب. عدم تعلّق الخطر بمحض إرادة المؤمن له

لا يجوز التأمين من خطر يتوقف تحققه على محض إرادة المؤمن له، لأن تعلقه بإرادته يفقده الاحتمال، ولأن تأمين الشخص من فعله العمدي يخالف النظام العام. ويقتصر هذا الحكم على العمد. فيجوز التأمين من الخطأ غير العمدي، يسيراً كان أو جسيماً، ومن الخطأ العمدي الذي يقع من الغير ولو كان ممن يُسأل عنهم المؤمن له كالتابع⁽¹⁾. ويكتسب هذا التمييز أهمية خاصة في نشاط شركات الأمن السيبراني، لأن كثيراً من أفعالها مقصود في ذاته. فالفحص الاختراقي، وتعديل إعدادات الحماية، وحجب الوصول، أفعال تأتينا الشركة عن قصد، ولا يُتصور أن يُعد كل منها خطأً عمدياً يُسقط الضمان.

وقد واجه القضاء الأمريكي هذه المسألة في قضية Eyeblaster. فقرر أن «الخطأ» في وثيقة الأخطاء المهنية التقنية يشمل الأفعال المقصودة غير الممهلة، ولا يُخرج منه إلا السلوك المتعمّد في عدم مشروعيته، وألزم المؤمن بالدفاع عن المؤمن له⁽²⁾. غير أن الإشكال الأمريكي الأبرز لا يقع في حدود العمد، بل فيما تضيفه الوثائق إليه. فقد درجت على استبعاد الأضرار الناشئة عن الإخلال بتدابير الأمن،

⁽¹⁾ أبو هلاله والشقيرات، المرجع السابق، ص 248-249، ويقران التزام المؤمن بالتعويض «بصرف النظر فيما إذا كان خطأ المؤمن له يسيراً أم جسيماً».

⁽²⁾ تتلخص وقائع هذه القضية في أن شركة (ايبلاستر) لإدارة الحملات الإعلانية عبر الإنترنت أمنت مسؤوليتها لدى شركة (فيدرال) للتأمين بوثقتين، إحداها للمسؤولية عن الأخطاء والسهو في تقنية المعلومات والشبكات، تضمن الخسارة المالية الناشئة عن فعل خاطئ، وهو فيها الخطأ أو السهو غير المقصود أو الفعل الإهمالي. ثم أقام عليها أحد المستخدمين دعوى زعم فيها أن حاسوبه أصيب ببرنامج تجسس بعد زيارته موقعاً تابعاً لها، فتجمد وضاعت بيانات كان يعمل عليها، ونسب إليها تثبيت برمجياتها على جهازه عمداً ودون إذنه. فرفض المؤمن الدفاع عنها، وأبدته المحكمة الفيدرالية لمنطقة مينيسوتا لأن الدعوى تنسب إليها أفعالاً عمدية لا فعلاً خاطئاً. فألغت محكمة الاستئناف الفيدرالية للدائرة الثامنة هذا الحكم وألزمت المؤمن بالدفاع عنها، مستندة إلى تعريف سابق لها للخطأ في وثائق الأخطاء والسهو التقنية بأنه «يشمل الأفعال العمدية غير الإهمالية، ويستبعد السلوك الخاطئ عمداً». فتثبتت ملفات تعريف الارتباط وتقنيتي (JavaScript) و (Flash) أفعال عمدية، لكن المؤمن لم يثبت أنها خاطئة عمداً. ينظر: United States Court of Appeals for the Eighth Circuit, Eyeblaster, Inc. v. Federal Insurance Co., 613 F.3d 797, 804 (2010). وقد أحالت المحكمة في هذا التعريف إلى حكمها في: United States Court of Appeals for the Eighth Circuit, St. Paul Fire & Marine Insurance Co. v. Compaq Computer Corp., 539 F.3d 809, 815 (2008).

كإغفال المصادقة الثنائية أو التأخر في سد الثغرات⁽¹⁾، حتى صار «الإهمال في مراعاة أمن الحاسوب» من أكثر الاستبعادات شيوعاً⁽²⁾. وفي قضية Cottage Health استند المؤمن إلى استبعاد «عدم اتباع الممارسات الدنيا المطلوبة» ليرفض التغطية ويطلب إبطال الوثيقة. ورأى الفقه في مثل هذا الاستبعاد صورة من «التغطية الوهمية»، ما دامت الوثيقة لا تحدد ماهية الممارسة الدنيا ولا معيارها⁽³⁾. وهذا الاستبعاد إن ضيق التغطية في حق سائر المؤمن لهم، فإنه يكاد يفرغها في حق شركة الأمن السيبراني، لأن الإخلال بتدابير الأمن هو السبب الغالب لمسؤوليتها.

أما المشرع الفرنسي فقد نص في المادة (L.113-1) من قانون التأمين الفرنسي لسنة 1976 على أن: «الخسائر والأضرار التي تحدثها الحوادث الفجائية أو التي يسببها خطأ المؤمن له تقع على عاتق المؤمن، إلا إذا ورد في الوثيقة استبعاد صريح ومحدود. غير أن المؤمن لا يُسأل عن الخسائر والأضرار الناشئة عن خطأ عمدي أو تدليسي من المؤمن له». فقرر الاستبعاد القانوني على هذين الخطأين. والخطأ العمدي يقتضي إرادة الضرر كما وقع لا مجرد إرادة الفعل، في حين يقوم الخطأ التدليسي على مخاطرة إرادية تزيل الاحتمال. ثم نصت المادة (L.121-2/1) من القانون نفسه على أن: «يضمن المؤمن الخسائر والأضرار التي يسببها الأشخاص الذين يكون المؤمن له مسؤولاً عنهم مدنياً بمقتضى المادة (1242) من القانون المدني، أي كانت طبيعة أخطاء هؤلاء الأشخاص وجسامتها»⁽⁴⁾.

(1) NAIC Staff, Report on the Cybersecurity Insurance Market, Memorandum to the Property and Casualty Insurance (C) Committee, November 3, 2023, p.8.

(2) (Sasha Romanosky et al., "Content Analysis of Cyber Insurance Policies: How Do Carriers Price Cyber Risk?", Journal of Cybersecurity, vol.5, no.1, 2019, tyz002, p.7. ومن الاستبعادات الشائعة فيها كذلك الغرامات والجزاءات المالية.

(3) تتلخص وقائع هذه القضية في أن مؤسسة (كوتيج هيلث سيستم) للرعاية الصحية تعرضت لخرق أمني كشف للعموم المعلومات الطبية لآلاف المرضى. فدفعت تعويضات، منها (4.125) مليون دولار تسوية لدعوى جماعية، ثم طالبت مؤمنها شركة (كولومبيا كاجوالتي) باستردادها بموجب وثيقة التأمين السيبراني. فوافق المؤمن أولاً على الدفع مع التحفظ على حقوقه، ثم أقام دعوى يطلب فيها رفض الضمان كله وإبطال الوثيقة. واستند في ذلك إلى استثناء «الإخفاق في اتباع الحد الأدنى من الممارسات المطلوبة»، الذي يُخرج من الضمان الخسارة الناشئة عن إخفاق المؤمن له في «التطبيق المستمر للإجراءات وضوابط المخاطر المحددة في طلب التأمين». واستند أيضاً إلى بيانات غير صحيحة قدمتها المؤمن لها في التقييم الذاتي لضوابط المخاطر، منها أنها تفحص التحديثات الأمنية لأنظمتها وتحافظ عليها بانتظام. فردت المحكمة الفيدرالية لمنطقة وسط كاليفورنيا الدعوى مع حفظ حق إقامتها من جديد، لأن المؤمن أقامها قبل أن يستند إجراءات التسوية البديلة للمنازعات التي تشترطها الوثيقة، فلم تفصل في صحة رفض الضمان. ينظر: United States District Court for the Central District of California, Columbia Casualty Co. v. Cottage Health System, No. 2:15-cv-03432, Order Granting Motion to Dismiss, July 17, 2015, pp.3-4; Deborah L. Johnson, "Demystifying the Elusive Quest for Cyber Insurance Protection: The Need for New Contract Language", 44 Cardozo L. Rev. 2361 (2023), pp.2404-2405.

(4) تنص المادة L.113-1 من تقنين التأمين الفرنسي، بصيغتها النافذة منذ 8 كانون الثاني 1981، على أنه:

أما الاستبعاد الاتفاقي فجاز في حدود ما أجازته الفقرة الأولى من المادة (1-113.L) المتقدمة، أي أن يكون صريحاً محدوداً. فـللمؤمن أن يعلق الضمان على اتخاذ تدبير وقائي، أو أن يستبعده عند الإخلال به، ويقع عليه هو عبء إثبات شروط الاستبعاد. وذلك عملاً بالمادة (2/1353) من القانون المدني الفرنسي لسنة 1804 المعدل، التي نصت على أنه: «وفي المقابل، على من يدعي براءة ذمته أن يثبت الوفاء أو الواقعة التي أدت إلى انقضاء التزامه»⁽¹⁾. ويُستفاد من ذلك أن الاستبعاد العام للإهمال في تدابير الأمن معرض للبطالان لافتقاده التحديد، في حين يصح الاستبعاد المرتبط بتدبير معين، كإغفال المصادقة الثنائية.

أما المشرع العراقي فلم يضع قاعدة عامة للعمد في التأمين من المسؤولية. لكنه قرر في التأمين من الحريق أن المؤمن لا يُسأل عما يحدثه المستفيد «عمداً أو غشاً»، وأنه يُسأل عما يتسبب فيه تابعوه «ولو كانوا متعمدين» (المادة 1000)⁽²⁾. وهو حكم يحسن القياس عليه في التأمين من مسؤولية شركات الأمن السيبراني، لأنها لا تؤدي نشاطها إلا بتابعيها، ولأن علة الحكم، وهي انتفاء تعلق الخطر بإرادة المؤمن له، قائمة فيها⁽³⁾.

Les pertes et les dommages occasionnés par des cas fortuits ou causés par la faute » de l'assuré sont à la charge de l'assureur, sauf exclusion formelle et limitée contenue dans la police

Toutefois, l'assureur ne répond pas des pertes et dommages provenant d'une faute intentionnelle ou dolosive de l'assuré
وتنص الفقرة الأولى من المادة 2-121.L على أنه:

L'assureur est garant des pertes et dommages causés par des personnes dont l'assuré » est civilement responsable en vertu de l'article 1242 du code civil, quelles que soient la nature et la gravité des fautes de ces personnes

وقد أضاف القانون رقم 568-2025 في 23 حزيران 2025 (المادة 3) إلى هذه المادة فقرتين تتعلقان برجوع المؤمن على والدي القاصر. ينظر في شرح المادتين: Jonathan Pouget, La réparation du dommage impliquant une intelligence artificielle, thèse, Aix-Marseille Université, 2019, pp.169-171. وفي الخطأ التدليسي ينظر: Cass. 2e civ., 12 sept. 2013, n°12-24.650.

⁽¹⁾ مستنداً إلى الفقرة الأولى من المادة 1-113.L المتقدم نصها في ، وإلى الفقرة الثانية من المادة 1353 من التقنين المدني الفرنسي في عبء الإثبات، ونصها: « Réciproquement, celui qui se prétend libéré doit justifier le paiement ou le fait qui a produit l'extinction de son obligation ».

⁽²⁾ تنص المادة (1000) من القانون المدني العراقي على أنه: « 1 – يكون المؤمن مسؤولاً عن الحريق الذي وقع قضاءً وقدرًا، أو بسبب خطأ المستفيد، ولا يكون مسؤولاً عن الحريق الذي يحدثه المستفيد عمداً أو غشاً. 2 – ويكون مسؤولاً أيضاً عن الحريق الذي يتسبب فيه تابعو المستفيد، ولو كانوا متعمدين ».

⁽³⁾ ويقتضي ذلك ألا يُسَلَّم بما ذهب إلىه الخفاجي من سقوط حق الشركة في التغطية إذا تعمد تابعها الإضرار (المرجع السابق، ص90-91). فضلاً عن أن قضية Morrisons التي بنت عليها رأيها تتعلق بمسؤولية المتبوع عن فعل تابعه، ولا تتضمن نزاعاً مع مؤمن: WM Morrisons Supermarkets plc v Various Claimants [2020] UKSC

وإذا كان الأصل جواز التأمين من الخطأ الجسيم⁽¹⁾، فإن المؤمن قد يستبعد بشرط في الوثيقة الضرر الناشئ عن عدم اتباع قواعد أمن المعلومات، على نحو ما تقدم في الوثائق الأمريكية. فيُثار السؤال عن صحة هذا الاستبعاد في القانون العراقي.

والنص الأقرب إلى المسألة هو المادة (985). فهي تبطل «الشرط الذي يقضي بسقوط الحق في التأمين بسبب مخالفة القوانين والأنظمة، إلا إذا انطوت هذه المخالفة على جناية أو جنحة عمدية» (الفقرة 1)، و«كل شرط تعسفي آخر، يتبين أنه لم يكن لمخالفته أثر في وقوع الحادث المؤمن منه» (الفقرة 5). غير أنها لا تحمي شركة الأمن من هذا الاستبعاد لسببين. أولهما أنها تتناول السقوط لا الاستبعاد: فالسقوط جزاء يحرم المؤمن له من ضمان خطر داخل في التغطية بسبب إخلاله بالتزام، أما الاستبعاد فيُخرج الخطر من التغطية ابتداءً⁽²⁾. فإذا صاغ المؤمن الإخلال بتدابير الأمن في صورة استبعاد، أفلت من حكمها. وثانيهما أن الفقرة (5) لا تسعف الشركة حتى لو عدّ الشرط من شروط السقوط، لأنها لا تبطل إلا الشرط الذي لم يكن لمخالفته أثر في وقوع الحادث، وإخلال شركة الأمن بتدابير الأمن يكون في الغالب هو سبب الحادث.

ولا يبقى للشركة إلا المادة (167) الخاصة بعقود الإذعان. فهي تجيز للمحكمة أن تعدل الشروط التعسفية أو تعفي الطرف المذعن منها، وتقضي بألا يكون تفسير العبارات الغامضة «ضاراً بمصلحة الطرف المذعن ولو كان دائناً». فتحول بذلك دون الاحتجاج بقاعدة تفسير الشك لمصلحة المدين (المادة 166)، وهي قاعدة تنقلب في التأمين لمصلحة المؤمن بوصفه مديناً بالضمان⁽²⁴⁾⁽³⁾. غير أنها حماية تقديرية لا تعني عن نص يشترط في هذا الاستبعاد أمرين: أن يكون محدداً بتدبير معين، وأن تقوم علاقة سببية بين الإخلال بهذا التدبير ووقوع الحادث. وهو ما نعود إليه عند بحث آثار التأمين.

ج. مشروعية الخطر المؤمن منه

⁽¹⁾ د. طارق عفيفي صادق، الخطر محل التأمين من المسؤولية المدنية في مجال المعلوماتية، ط1، دار الحكمة، القاهرة، 2013، ص337-338.

⁽²⁾ ففي السقوط يكون «الخطر داخل في نطاق الضمان ويستحق عنه التعويض»، لكن المؤمن له يُحرم منه لإخلاله بأحد واجباته: ريم إحسان محمود موسى، الدعوى المباشرة في التأمين من المسؤولية المدنية، رسالة ماجستير، جامعة النجاح الوطنية، نابلس، 2010، ص58-59.

⁽³⁾ تنص المادة (166) من القانون المدني العراقي على أنه: «يفسر الشك في مصلحة المدين». وتنص المادة (167) على أنه: «1 - القبول في عقود الإذعان ينحصر في مجرد التسليم بمشروع عقد ذي نظام مقرر يضعه الموجب ولا يقبل فيه مناقشة. 2 - إذا تم العقد بطريق الإذعان وكان قد تضمن شروطاً تعسفية جاز للمحكمة أن تعدل هذه الشروط أو تعفي الطرف المذعن منها وذلك وفقاً لما تقتضيه به العدالة ويقع باطلاً كل اتفاق على خلاف ذلك. 3 - ولا يجوز أن يكون تفسير العبارات الغامضة في عقود الإذعان ضاراً بمصلحة الطرف المذعن ولو كان دائناً».

يجب أن يكون الخطر المؤمن منه مشروعاً. فلا يجوز التأمين من خطر ينشأ عن نشاط يخالف النظام العام أو الآداب، ولا من جزاء أراد المشرع أن يتحملة المخالف بنفسه. وتثير هذه القاعدة في نشاط شركات الأمن السيبراني ثلاث مسائل: الجزاءات المالية العامة، والجزاءات الخاصة التي تفرضها جهات غير حكومية بموجب العقود، ومبالغ الفدية.

ولا تجري الوثائق الأمريكية على نسق واحد في الجزاءات العامة. فمنها ما يدرج الغرامات التنظيمية ضمن نفقات إدارة حادث الاختراق⁽¹⁾، وأكثرها يستبعد على ما تقدم. أما الجزاءات الخاصة فقد عُرِضت في قضية P.F. Chang's: إذ رفضت المحكمة تغطية الرسوم التي فرضتها شبكات بطاقات الدفع بعد اختراق بيانات الشركة، لأنها التزامات تحملتها الشركة بعقدها مع معالج المدفوعات، والوثيقة تستبعد المسؤولية العقدية⁽²⁾. وهذا الحكم لا يقوم على عدم المشروعية بل على نطاق الوثيقة، فيبقى للطرفين أن يتفقا على تغطية هذه الالتزامات.

وفي الفقه الفرنسي، ومن تأثر به، أن الغرامة الجزائية لا تقبل التأمين لأن العقوبة يجب أن يتحملها المحكوم عليه بنفسه. ويلحق بها الجزاء الإداري لأنه يعاقب على المساس بالنظام العام وإن كان قطاعياً، وقد طُبِّق ذلك صراحة على الجزاءات التي توقعها الجهة التنظيمية على مقدمي خدمات الأمن. أما الفدية فرأى هذا الفقه أن تأمينها يخالف النظام العام قياساً على فدية الاختطاف، لأنه يغري المهاجمين بتكرار الهجمات، وقد يفتح باب التواطؤ بين المؤمن له والمهاجم⁽³⁾. غير أن المشرع الفرنسي حسم الخلاف في

(1) Garrie & Mann, op. cit., p.390

(2) تتلخص وقائع هذه القضية في أن سلسلة مطاعم (بي إف تشانغز) كانت مؤمناً لها لدى شركة (فيدرال) للتأمين، التابعة لمجموعة (تشب)، بوثيقة للتأمين السيبراني. ثم اختُرقت أنظمة الدفع فيها وسُرقت بيانات بطاقات عملائها. فدفع لها المؤمن أكثر من (1.7) مليون دولار عن التحقيق الفني في الاختراق، وعن الدفاع في الدعاوى التي أقامها العملاء وأحد المصارف المصدرة للبطاقات. غير أن المصرف الذي تعاقدت معه لمعالجة مدفوعات البطاقات رجع عليها بنحو (1.93) مليون دولار فرضتها عليه شركة (ماستركارد)، استناداً إلى عقد الخدمات المبرم بينهما، الذي التزمت فيه بأن تعوضه عما يُفرض عليه من رسوم وغرامات. فرفض المؤمن ضمان هذا المبلغ، وأقرته المحكمة الفيدرالية لمنطقة أريزونا على ذلك لأمرين. الأول أن الضرر الماس بالخصوصية المضمون في الوثيقة لا يصيب إلا الشخص الذي اختُرقت سجلاته، وبيانات البطاقات لم تكن من سجلات المصرف بل من سجلات المصارف المصدرة لها. والثاني أن الوثيقة تستبعد المسؤولية التي يتحملها المؤمن له بعقد، ولم يثبت أن الشركة كانت ستسأل عن هذا المبلغ لولا التزامها العقدي. ووصفت المحكمة الطرفين بأنهما متمرسان في التفاوض على الشروط التعاقدية. ينظر United States District Court for the District of Arizona, P.F. Chang's China Bistro, Inc. v. Federal Insurance Co., No. CV-15-01322-PHX-SMM, Order of May 26, 2016, pp.3-4, 9-10, 15-17.

(3) Tsomevou, op. cit., pp.71-72

الفدية: فأجاز تغطية خسائر الاعتداء على أنظمة المعالجة الآلية للبيانات، بشرط أن يقدم المضرور شكوى إلى السلطات المختصة خلال اثنتين وسبعين ساعة من علمه بالاعتداء⁽¹⁾.

وفي القانون المدني العراقي يجد هذا الشرط سنده في المادة (1/984)، التي تجيز أن يكون محلاً للتأمين «كل شيء مشروع يعود على الشخص بنفع من عدم وقوع خطر معين». فلا يجوز التأمين من الغرامة أو المصادرة، لأن العقوبة شخصية، ويبطل التأمين منهما لمخالفته النظام العام⁽²⁾. ومؤدى ذلك أن الجزاءات التنظيمية التي قد تتعرض لها شركة الأمن السيبراني، مما بحثناه في المطلب السابق، تبقى خارج التغطية، ويقتصر التأمين على الشق المدني من مسؤوليتها، وهو ما يفسر قصر هذا المطلب على المسؤولية المدنية.

أما الفدية فلم يتناولها نص. والأقرب عندنا التمييز بين أمرين: الأول تأمين الفدية ذاتها، وهو محل الخلاف، ويخرج من نطاق هذا المطلب لأنه تأمين لخسارة من دفعها لا لمسؤوليته. والثاني تأمين مسؤولية الشركة عن ضرر لحق العميل، ومن عناصره ما دفعه فديةً. وهذا تعويض عن ضرر ناشئ عن إخلال الشركة، لا مكافأة للمهاجم.

ويبقى للقاضي أن يقدّر ما إذا كان دفع الفدية نتيجة طبيعية لهذا الإخلال. وللمشرع أن يقيّد تغطيته بالإبلاغ عن الاعتداء على غرار الحل الفرنسي، بما يتسق مع واجب الإبلاغ الذي قرره قرار مجلس المفوضين رقم (33) لسنة 2025⁽³⁾.

ثانياً: من حيث الشروط الفنية للخطر

لا يكفي أن يقبل الخطر التأمين قانوناً، بل يجب أن يمكن تقديره وفق قانون الكثرة. ويقتضي ذلك أن يكون الخطر متفرقاً، متجانساً، منتظم الوقوع بالنسبة إلى مجموع المؤمن لهم.

⁽¹⁾ تنص المادة L.12-10-1 من تقنين التأمين الفرنسي، الواردة في الفصل العاشر «L'assurance des risques de cyberattaques» والمضافة بالمادة (5) من القانون رقم 22-2023 في 24 كانون الثاني 2023 (قانون توجيه وبرمجة وزارة الداخلية) والنافذة منذ 24 نيسان 2023، على أنه:

« Le versement d'une somme en application de la clause d'un contrat d'assurance visant à indemniser un assuré des pertes et dommages causés par une atteinte à un système de traitement automatisé de données mentionnée aux articles 323-1 à 323-3-1 du code pénal est subordonné au dépôt d'une plainte de la victime auprès des autorités compétentes au plus tard soixante-douze heures après la connaissance de l'atteinte par la victime. Le présent article s'applique uniquement aux personnes morales et aux personnes physiques dans le cadre de leur activité professionnelle ».

⁽²⁾ د. عبدالرزاق احمد السنهوري، المرجع السابق، ص1228

⁽³⁾ تُلزم الفقرة (17) من البند (ثانياً) من المادة (12) من قرار مجلس المفوضين رقم (33) لسنة 2025 شركات الأمن السيبراني بـ«إعلام الجهات المختصة في حال حدوث أي مشكلة فنية أو خرق أمني في أي من النشاطات التي تقدمها».

أ. تفرّق الأخطار

يقتضي قانون الكثرة ألا يتجمع وقوع الأخطار في وقت واحد، ولذلك عسر التأمين من الزلازل والحروب. والخطر السيبراني أقرب إلى هذا الصنف منه إلى الأخطار التقليدية. فتزايد الترابط بين الأنظمة، وشيوع البرمجيات والمعدات الموحدة، والاتجاه المتزايد إلى إسناد خدمات تقنية المعلومات إلى مزودين خارجيين، كلها عوامل لانتشار الهجوم الواحد على نطاق واسع. وتكتسب الجهات التي تؤدي دوراً محورياً في البنى التقنية طابعاً نظامياً⁽¹⁾. وشركة الأمن السيبراني من هذه الجهات: فهي نقطة يتصل بها عملاء كثيرون، فإذا اختُرقت أنظمتها أو أخطأت في إعداد حماية يشترك فيها عملاؤها، انتقل الأثر إليهم جميعاً في وقت واحد، فتتعدد المطالبات الناشئة عن سبب واحد.

وقد ظهر أثر هذا الترابط في القانون الأمريكي في مسألتين:

وحدة الحادث. فالوثائق تحدد حد التغطية لكل حادث، وأغلب المحاكم تأخذ في عد الحوادث بمعيار السبب، فتعد الأضرار حادثاً واحداً إذا نشأت عن سبب مباشر واحد مستمر⁽²⁾. ومؤدى ذلك أن يتزاحم المضرورون من هجوم واحد على حد تغطية واحد قد لا يفي بحقوقهم. ومثاله قضية Home Depot، التي استنفدت فيها الشركة حدود وثائقها السيبرانية البالغة مئة مليون دولار، في حين بلغت التسوية نحو مئة وسبعين مليوناً⁽³⁾.

(1) Sébastien Héon et Didier Parsoire, « La couverture du cyber-risque », Revue d'économie financière, 2017/2, n°126, p.175.

(2) Green & Hanner, op. cit., p.414. وهو المعيار الذي يتجه إليه القضاء بحسب الكاتبين.

(3) رفضت محكمة الاستئناف الفيدرالية للدائرة السادسة رجوع شركة (هوم ديبو) على وثائق المسؤولية العامة الصادرة لها من شركتي (ستيفاست) و(غريت أمريكان) للتأمين. وكان قراصنة قد اخترقوا نظامها الحاسوبي، وسرقوا بيانات بطاقات الدفع لعشرات الملايين من عملائها الذين استعملوا أجهزة الدفع الذاتي في متاجرها. فأقامت عليها المصارف المصدرة للبطاقات دعاوى تطالب فيها بنفقات إلغاء البطاقات وإعادة إصدارها، وبما فاتتها من رسوم وفوائد لقلّة استعمال العملاء لها بعد الاختراق، فسوّتها الشركة بنحو (170) مليون دولار. ولما دفع مؤمنوها السيبرانيون الحد الأقصى لوثائقهم، وهو (100) مليون دولار، طالبت بالباقي بموجب وثائق المسؤولية العامة، بحجة أن ما تحملته المصارف ناشئ عن فقدان الانتفاع ببطاقات الدفع بوصفها أموالاً مادية. فلم تر المحكمة حاجة إلى الفصل في هذه الحجة، لأن الوثائق تستبعد «الأضرار الناشئة عن فقدان البيانات الإلكترونية، أو فقدان الانتفاع بها، أو تلفها، أو إفسادها، أو تعذر الوصول إليها، أو تعذر التعامل معها»، وهذا الاستثناء يمنع الضمان ولو صحت الحجة. فبيانات البطاقات بيانات إلكترونية، وقد فقدت وظيفتها بالاختراق إذ لم يعد ممكناً استعمالها للدفع الآمن، كما تفقد كلمة السر قيمتها متى عرفها المخترق ولو بقيت تتيح لصاحبها الدخول. ولولا الاختراق لما ألغت المصارف البطاقات وأصدرت غيرها، ولا قلّ استعمال العملاء لها. ينظر United States Court of Appeals for the Sixth Circuit, Home Depot, Inc. v. Steadfast Insurance Co., No. 23-3720, decided January 13, 2025, pp.3-12.

الأخطار الكارثية. فالوثائق تستبعد عادة فشل البنى التحتية الحرجة وأعمال الحرب⁽¹⁾. وقد ضيق القضاء استبعاد الحرب فلم يطبقه على هجوم NotPetya ، لأنه ينصرف إلى النزاع المسلح التقليدي⁽²⁾.

أما المشرع الفرنسي فقد حسم مسألة وحدة الحادث بنص أمر المادة (L.124-1-1) ، يُعمل به أيّ كان مضمون العقد. فقد عدّ مجموع الوقائع الضارة الناشئة عن سبب تقني واحد واقعة ضارة واحدة⁽³⁾. وهو حل يحقق اليقين، لكنه يجمع مطالبات المضرورين من الهجوم الواحد في حد تغطية واحد. كما جعل القانون الفرنسي أضرار الحرب خارج الضمان ما لم يُتفق على خلافه المادة (L.121-8)⁽⁴⁾.

ولا يعرف القانون العراقي قاعدة في وحدة الحادث، فيبقى أمرها لشروط الوثيقة وتفسير القاضي في ضوء المادة (3/167). ونرى أن الأخذ بمعيار السبب التقني الواحد، على غرار الحل الفرنسي، أدعى إلى اليقين، بشرط أن يقتصر في التأمين الإلزامي بحد أدنى للتغطية لكل حادث يراعي تعدد المضرورين، وبضمانات تكميلية نببحثها في الفرع الثاني.

⁽¹⁾ ، مع إشارة التقرير إلى أن كثيراً من المؤمنين يستثنون الإرهاب السيبراني من استبعاد NAIC, op. cit., p.8 (1).

⁽²⁾ (Merck & Co. v. Ace Am. Ins. Co., 293 A.3d 535 (N.J. Super. Ct. App. Div. 2023); Johnson, op. cit., pp.2406–2407).

⁽³⁾ تنص الفقرة الأولى من المادة L.124-1-1 من تقنين التأمين الفرنسي، المضافة بالقانون رقم 706-2003 في 1 آب 2003، على أنه:

« Au sens du présent chapitre, constitue un sinistre tout dommage ou ensemble de dommages causés à des tiers, engageant la responsabilité de l'assuré, résultant d'un fait dommageable et ayant donné lieu à une ou plusieurs réclamations. Le fait dommageable est celui qui constitue la cause génératrice du dommage. Un ensemble de faits dommageables ayant la même cause technique est assimilé à un fait dommageable unique. »

⁽⁴⁾ تنص المادة L.121-8 من تقنين التأمين الفرنسي على أنه:

« L'assureur ne répond pas, sauf convention contraire, des pertes et dommages occasionnés soit par la guerre étrangère, soit par la guerre civile, soit par des émeutes ou par des mouvements populaires. »

Lorsque ces risques ne sont pas couverts par le contrat, l'assuré doit prouver que le sinistre résulte d'un fait autre que le fait de guerre étrangère ; il appartient à l'assureur de prouver que le sinistre résulte de la guerre civile, d'émeutes ou de mouvements populaires.

ب. تجانس الأخطار

يقتضي تقدير القسط أن تتجانس الأخطار المجمعة في طبيعتها ومحلها وقيمتها ومدتها، فإن تفاوتت عولج التفاوت بتجزئة الخطر أو بإعادة التأمين. وشركات الأمن السيبراني متباينة تبايناً يعسر معه جمعها في فئة واحدة. فمنها ما يقتصر على الاستشارة أو فحص الثغرات، ومنها ما يتولى إدارة الحماية ومراقبتها على مدار الساعة. ومنها ما يخدم أفراداً ومنشآت صغيرة، ومنها ما يخدم مصارف وجهات حكومية وبنى تحتية حرجية. ولكل صنف من هذه خطر يختلف في احتماله وجسامته.

وفي السوق الأمريكية لم يواكب التسعير هذا التباين. فقد كشف تحليل ملفات التسعير المودعة لدى جهات الرقابة أن المؤمّنين يعتمدون على مصادر خارجية أو على التخمين أو على أسعار المنافسين، وأن معايير الأمن المعترف بها نادراً ما تُعتمد في تقدير الخطر: فلم يُذكر معيار ISO إلا مرة واحدة، ولم يُذكر إطار NIST أصلاً⁽¹⁾.

أما في فرنسا فقد أسهم نظام العلامة المهنية في رسم فئة متجانسة من مقدمي الخدمات. فقد قصر علامة ExpertCyber على من يؤدي خدمات التركيب والصيانة والمساعدة في الأمن السيبراني، بما فيها الاستجابة للحوادث، في مجالات تقنية عامة هي البنية المعلوماتية والاتصالات والمواقع الإلكترونية، واستبعد المجالات المتخصصة كالمعلوماتية الصناعية⁽²⁾. وهو تحديد يتيح للمؤمّن أن يعرف طبيعة الخطر الذي يغطيه.

وفي العراق يزيد صعوبة التصنيف ما نبه إليه الفقه من غياب التنظيم التشريعي للمهن المعلوماتية، وتداخل تخصصاتها، وظهور تخصصات جديدة بتطور القطاع⁽³⁾. غير أن قرار مجلس المفوضين رقم (33) لسنة 2025 نظم نشاط شركات الأمن السيبراني وحدد الإطار العام لواجباتها، فيمكن أن يكون أساساً لتصنيفها. وقد حوّل قانون تنظيم أعمال التأمين رئيس الديوان تحديد فروع التأمين بتعليمات (المادة 4/ثانياً)⁽⁴⁾. فيمكن أفراد فرع لتأمين مسؤولية هذه الشركات، يُقسّم المؤمّن لهم فيه بحسب نوع الخدمة، وقطاع العملاء، ومدى التعامل مع البنى التحتية الحرجية، فيتحقق التجانس داخل كل فئة.

(1) (Romanosky et al., op. cit., pp.12-13).

(2) (GIP ACYMA, op. cit., critères 2.a et 2.b, pp.7-8).

(3) طارق عفيفي صادق، المرجع السابق، ص74-75.

(4) تنص المادة (4) من قانون تنظيم أعمال التأمين (الأمر رقم 10 لسنة 2005)، المنشور في الوقائع العراقية، العدد (3995) في 2005/3/3، على أنه: «أولاً - تقسم أعمال التأمين الى نوعين رئيسيين هما التأمين على الحياة والتأمينات العامة ويدخل في أي منهما كل نشاط يعد في العرف والعادة من أعمال التأمين. ثانياً - تحدد فروع كل نوع من نوعي التأمين بتعليمات يصدرها رئيس الديوان».

ج. انتظام الأخطار وقابليتها للقياس

يشترط أن يكون الخطر منتظم الوقوع، فلا يبلغ من الندرة حداً يتعذر معه الإحصاء، ولا من الكثرة حداً يجعل القسط باهظاً. ولا يُقاس الانتظام بالنسبة إلى مؤمن له بعينه، بل بالنسبة إلى مجموع المؤمن لهم. والخطر السيبراني يفتقر إلى سجل خسائر كافٍ، لحداثه وسرعة تطوره وقلة الإبلاغ عنه.

ويظهر ذلك حتى في أوسع قواعد البيانات الأمريكية. فمركز شكاوى جرائم الإنترنت التابع لمكتب التحقيقات الفيدرالي ينبّه إلى أن ما يسجله من خسائر هجمات القدية لا يشمل خسائر توقف الأعمال والوقت والملفات والمعدات، ولا تكاليف المعالجة، وإلى أن بعض المتضررين لا يبلغون عن خسائرهم أصلاً⁽¹⁾. وإذا كانت أوسع قاعدة بيانات عن الجرائم السيبرانية لا تعكس الخسارة الحقيقية، فإن تسعيراً يقوم عليها لا يكون إلا تقريباً.

وفي الفقه الفرنسي أن غياب نموذج موثوق للتسعير، ولا سيما لنمذجة تراكم الأخطار، جعل معيدي التأمين يتحفظون. فجاءت إعادة التأمين نسبية في أغلبها، مقيدة بحدود لكل حادث أو لكل سنة، بما قد يعوق نمو السوق إن لم تتقدم معرفة الخطر⁽²⁾. وتحفظ معيدي التأمين ينعكس بدوره على المؤمن المباشر، فيضيّق التغطية أو يرفع القسط.

وفي العراق يزداد الأمر صعوبة. فقد نبه الفقه إلى غياب البيانات الإحصائية الكاملة عن الخدمات المعلوماتية ومحترفيها، وعدم وجود جهة تتولى جمعها بانتظام، مما يدفع المؤمنين إلى منح التغطية بحذر وبشروط مقيدة⁽³⁾. غير أن في التشريع العراقي أدوات يمكن البناء عليها:

قانون تنظيم أعمال التأمين: ينظم عمل خبراء تقدير الأضرار والاكتواريين (المادتان 77 و78)، ويلزم مقدمي خدمات التأمين بتزويد الديوان بما يطلبه من بيانات (المادة 87)⁽⁴⁾.

(¹) (Federal Bureau of Investigation, Internet Crime Report 2024, p.10).

(²) (Héon et Parsoire, op. cit., p.178).

(³) طارق عفيفي صادق، المرجع السابق، ص62.

(⁴) تنص المادة (77) من قانون تنظيم أعمال التأمين على أنه: «أولاً – لا يجوز مزاولة أعمال خبير الكشف وتقدير الأضرار إلا ممن يسجل في سجل خبراء الكشف وتقدير الأضرار لدى الديوان، ويصدر رئيس الديوان تعليمات بكيفية مسك هذا السجل وتنظيم التسجيل فيه وتحديد الشروط التي يجب توفرها في الخبير. ثانياً – يجوز للمؤمنين في الحالات التي تقتضي خبرة فنية خاصة أن يستعين بخبراء من غير المسجلين لدى الديوان وعلى المؤمن في مثل هذه الحالات استحصال موافقة الديوان تحريراً».

وتنص المادة (78) منه في البندين (أولاً) و(ثانياً) على أنه: «أولاً – لا يجوز لأي شخص ممارسة أعمال خبراء رياضيات التأمين (الاكتواريين) إلا بعد الحصول على ترخيص من الديوان وفق الأسس والشروط التي يحددها رئيس الديوان بمقتضى تعليمات يصدرها لهذا الغرض. ثانياً – على المؤمن المجاز بممارسة أعمال التأمين على الحياة أو أعمال التأمينات العامة

قرار مجلس المفوضين رقم (33) لسنة 2025: يلزم شركات الأمن السيبراني بإعلام الجهات المختصة بأي مشكلة فنية أو خرق أمني (المادة 12/ثانياً/17). ونرى أن تُجمع هذه البيانات في قاعدة وطنية للحوادث السيبرانية يُتاح للمؤمنين الإفادة منها، فتتوافر بها شروط القياس التي يفقدها هذا الخطر اليوم.

يتبين مما تقدم أن مسؤولية شركات الأمن السيبراني قابلة للتأمين من حيث شروطه القانونية، في حدود استبعاد العمد والجزاءات العامة. وأن الإشكال الأبرز ليس في القانون بل في الوثائق، باستبعادها الإخلال بتدابير الأمن الذي يكاد يفرغ التغطية في حق هذه الشركات. أما قابليتها الفنية فمقيدة بترابط الخطر وتباينه وضعف قياسه. وتنعكس هذه القيود على آثار التأمين في حق المضرور وفي حق الشركة المؤمن لها، وهو ما نبثه في الفرع الثاني.

الفرع الثاني

آثار التأمين من المسؤولية المدنية لشركات الأمن السيبراني

بيّن الفرع الأول مدى قابلية مسؤولية شركات الأمن السيبراني للتأمين، ومن ذلك تحديد الواقعة التي ينشأ بها التزام المؤمن، ومدى صحة ما يرد في الوثائق من استبعاد. ويبقى بعد ذلك بيان ما يرتبه هذا التأمين إذا انعقد.

والأثر الرئيس للتأمين من المسؤولية هو التزام المؤمن بالضمان. وهو التزام يتميز من نظيره في سائر تأمينات الأضرار بأن ثمرته تعود في الحقيقة إلى شخص ثالث ليس طرفاً في العقد، هو المضرور من خطأ الشركة. ولذلك نقصر هذا الفرع عليه. فلا نعود إلى التزامات الشركة تجاه عملائها والجهات الرقابية لسبق بحثها، ولا إلى صحة الاستبعاد لسبق بحثها في الفرع الأول. ولا نعرض لالتزامات الشركة تجاه المؤمن إلا من حيث يحتج المؤمن بالإخلال بها على المضرور.

ونتبع في بحث هذا الالتزام التقسيم المألوف في نظرية الالتزام، فنبحث محله ثم الوفاء به، ونبيّن في كل منهما ما تفرضه طبيعة النشاط السيبراني. فالشركة تخدم عملاء كثيرين بأدوات واحدة، فقد تُلحق

التي تمتد التزاماتها تجاه حملة وثائق التأمين لأكثر من سنة إن يعين أو يعتمد خبير برضايات التأمين مرخص خلال سنتين يوماً من تاريخ منحه الاجازة، على ان يشعر الديوان خلال شهر من تاريخ تعيينه او اعتماده مع بيان اسمه وعنوان عمله ومؤهلاته المهنية».

وتنص المادة (87) منه على أنه: «يلتزم كافة وكلاء التأمين او وكلاء اعادة التأمين والوسطاء وخبراء التأمين وكافة مقدمي خدمات التأمين وفقاً لأحكام هذا القانون بتقديم اية بيانات او معلومات او وثائق يطلبها الديوان خلال المدة التي يحددها».

واقعة واحدة الضرر بهم جميعاً. ومضروورها في الغالب عميل يرتبط بها بعقد. وهي ملزمة بالإبلاغ عن الخرق الأمني متى وقع. وعليه نقسم هذا الفرع على نقطتين: نخصص الأولى لمحل التزام المؤمن بالضمان، والثانية للوفاء به.

أولاً: محل التزام المؤمن بالضمان

يتحدد محل التزام المؤمن بدين المسؤولية الذي يترتب في ذمة المؤمن له تجاه المضرور، في حدود الوثيقة؛ فهو يضمن ما تُسأل عنه الشركة قانوناً، وفي حدود مبلغ التأمين. ويقتضي بيانه تحديد ما يدخل في الضمان، وما يخرج منه، وكيف يعمل حده إذا تعدد المضرورون.

أ. ما يدخل في الضمان: التعويض ونفقات الدفاع

يشمل التزام المؤمن التعويض المستحق للمضرور ونفقات الدفاع في دعوى المسؤولية، وكثيراً ما يؤدي الثانية خدمةً بتعيين المحامي وإدارة الدعوى. ويثور السؤال عن موقع هذه النفقات من الحد: أهى خارجة عنه فيبقى مبلغ التأمين كاملاً للمضرورين، أم داخله فيه فتقتطع منه؟ وتشتد أهميته في مسؤولية شركات الأمن السيبراني، لأن الخرق الواحد يولد دعاوى العملاء والدعاوى الجماعية وتحقيقات الجهات الرقابية؛ ولذلك يشمل ضمان المسؤولية في التأمين السيبراني أتعاب المحامي ومصاريفه إلى جانب تعويض المضرورين.⁽¹⁾

ففي القانون الأمريكي، تضمن وثيقة المسؤولية السيبرانية التعويض ونفقات الدفاع معاً⁽²⁾، وتجري وثائق المسؤولية المهنية في الغالب على إدخال هذه النفقات في الحد، فينقص كل ما يُنفق منها الحد بقدره، بخلاف وثائق المسؤولية العامة للمنشآت التي تجعلها في الغالب خارجة⁽³⁾.

وفي القانون الفرنسي، تنص المادة (5-113 L) من قانون التأمين الفرنسي لسنة 1976 على أنه: «عند تحقق الخطر أو حلول أجل العقد، يجب على المؤمن أن يؤدي في الأجل المتفق عليه الأداء المحدد في

⁽¹⁾ بغدادي شامي، تأمين الخطر السيبراني، بحث منشور في مجلة هيروودوت للعلوم الإنسانية والاجتماعية، المجلد 7، العدد 25، 2023، ص253

⁽²⁾ (Shauhin A. Talesh, Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as "Compliance Managers" for Businesses, Law & Social Inquiry, Vol. 43, No. 2, 2018, p.426)

⁽³⁾ (Katherine J. Henry, Exploring Nevada's Defense Within Limits Laws, Bradley Arant Boult Cummings LLP, January 15, 2025, available at:

<https://www.bradley.com/insights/publications/2025/01/exploring-nevadas-defense-within-limits-laws>1/10/2026 ، تاريخ آخر زيارة في

العقد، ولا يُلزم بما يجاوزه»⁽¹⁾. فالعقد يحدد الأداء، مالا كان أو خدمة، ويرسم حده، ولم يضع المشرع قاعدة عامة لموقع نفقات الدفاع منه. وإنما منعت الفقرة الثانية من المادة (3-124.L) من القانون نفسه المؤمن من أن «يدفع لغير الغير المضرور كل المبلغ المستحق عليه أو بعضه، ما دام هذا الغير لم يُعوّض» عن النتائج المالية للفعل الضار⁽²⁾، وهو نص ينصرف إلى مبلغ التعويض ولا يتناول نفقات الدفاع صراحةً.

ولا يعرف القانون العراقي تنظيمًا خاصاً لهذا التأمين، ولا تتعامل به شركات التأمين العراقية بعد⁽³⁾، فتحكمه القواعد العامة في القانون المدني. فالمادة (1/983) تجعل محل التزام المؤمن «مبلغاً من المال أو إيراداً مرتباً أو أي عوض مالي آخر»، فيتسع للأداء العيني لإدارة الدفاع، والمادة (989) تقيد التعويض بألا يتجاوز «قيمة التأمين»⁽⁴⁾. والنص الحاسم في مسألتنا هو المادة (1006): «لا يجوز للمؤمن أن يدفع لغير المتضرر مبلغ التأمين المتفق عليه كله أو بعضه ما دام المتضرر لم يعوّض عن الضرر الذي أصابه». وعبارته أوسع من النص الفرنسي، إذ تشمل بظاهرها كل ما يُقتطع من «مبلغ التأمين المتفق عليه». لذا نرى أن شرط إدخال نفقات الدفاع في الحد لا يُحتج به على المضرور ما دام لم يُعوّض، لأن ما يُدفع منها للمحامين جزء من هذا المبلغ يُدفع لغيره؛ فإن أرادت الوثيقة تغطيتها دون المساس بحقه، جعلتها فوق الحد.

¹ نص المادة (5-113.L) من قانون التأمين الفرنسي باللغة الفرنسية، بصيغتها المعدلة بالقانون رقم (81-5) في 7 كانون الثاني 1981: «Lors de la réalisation du risque ou à l'échéance du contrat, l'assureur doit exécuter dans le délai convenu la prestation déterminée par le contrat et ne peut payer à un autre que le tiers lésé»⁽²⁾ نص الفقرة الثانية من المادة (3-124.L) من قانون التأمين الفرنسي باللغة الفرنسية، بصيغتها المعدلة بالقانون رقم (1774-2007) في 17 كانون الأول 2007: «L'assureur ne peut payer à un autre que le tiers lésé tout ou partie de la somme due par lui, tant que ce tiers n'a pas été désintéressé, jusqu'à concurrence de ladite somme, des conséquences pécuniaires du fait dommageable ayant entraîné la responsabilité de l'assuré».

³ د. هالة صلاح الحديثي، قواعد التأمين عن الأخطار الإلكترونية (دراسة تحليلية)، بحث منشور في مجلة الباحث العربي، المجلد 1، العدد 1، 2020، ص 25. كذلك ينظر: كفاء علي عيسى أبو رغيف وإبتسام عباس عبد الحسن هادي، تأثير التأمين السيبراني في مخاطر شركات التأمين: دراسة تطبيقية على عينة من شركات التأمين العالمية، بحث منشور في Journal Port Science Research، جامعة أروك، المجلد 9، العدد 3، 2026، ص 700.

⁴ تنص المادة (1/983) من القانون المدني العراقي رقم (40) لسنة 1951 على أن: «التأمين، عقد به يلتزم المؤمن أن يؤدي إلى المؤمن له أو إلى المستفيد مبلغاً من المال أو إيراداً مرتباً أو أي عوض مالي آخر، في حالة وقوع الحادث المؤمن ضده، وذلك في مقابل أقساط أو أية دفعة مالية أخرى يؤديها المؤمن له للمؤمن». وتنص المادة (989) منه على أن: «يلتزم المؤمن بتعويض المستفيد عن الضرر الناشئ من وقوع الخطر المؤمن ضده، على ألا يتجاوز ذلك قيمة التأمين».

ب. ما يخرج عن الضمان: ما تلتزم به الشركة بالعقد زائداً على مسؤوليتها القانونية

يضمن التأمين من المسؤولية ما يرتبه القانون على المؤمن له من مسؤولية، عقدية كانت أو تقصيرية، لا ما يتطوع بتحملة زيادةً عليها؛ فالمؤمن حسب القسط على المسؤولية كما ينظمها القانون، وهو أجنبي عن عقد الشركة مع عميلها. وللمسألة شأن خاص هنا، لأن مضرور الشركة في الغالب عميلها، وقد تتضمن عقودها ضمان عدم وقوع الاختراق أو تعويض العميل عن كل ما يتكبده أياً كان سببه. على أن الفصيل مجاوزة الالتزام لما يقرره القانون لا مصدره؛ فقد عدّ جانب من الفقه إخلال المؤسسة بالتزامات السرية مما يضمنه التأمين السيبراني، سواء اكتتبتها بعقد أو فرضها عليها القانون⁽¹⁾.

وقد ضبط القضاء الأمريكي هذا المعيار في تفسيره شرط استبعاد المسؤولية التعاقدية، الذي يستبعد ما يلتزم به المؤمن له بسبب تحمله المسؤولية في عقد، ويستثنى ما كان سيُسأل عنه دونه. ففي قضية (إوينغ للإنشاءات ضد أميريشور للتأمين) لعام 2014، أكدت المحكمة العليا لولاية تكساس أن «تحمل المسؤولية يعني أن المؤمن له تحمّل مسؤولية عن أضرار تجاوز المسؤولية التي كانت ستقع عليه وفقاً للقانون العام»⁽²⁾، وأن تعهد المقاول بأداء عمله على الوجه الصحيح، دون زيادة، لا يوسّع واجب العناية الذي يقع عليه⁽³⁾. فتعهد الشركة بالعناية المهنية الواجبة لا يُخرج مسؤوليتها من الضمان، أما ضمانها نتيجةً بعينها أو تعويض كل خسارة فيخرج منه بقدر ما يزيد على مسؤوليتها القانونية؛ ومن تطبيقاته في التأمين السيبراني قضية (P.F. Chang's) التي سبقت الإشارة إليها في الفرع الأول.

وفي القانون الفرنسي، تحكم المسألة قاعدة نسبية أثر العقد، إذ تنص المادة (1199) من القانون المدني الفرنسي لسنة 1804 المعدل على أنه: «لا ينشئ العقد التزامات إلا بين أطرافه. ولا يجوز للغير أن يطالب بتنفيذ العقد ولا أن يُجبر على تنفيذه...»⁽⁴⁾؛ فلا تلزم المؤمن التعهدات التي تزيد بها الشركة مسؤوليتها ما لم يقبلها في الوثيقة، وتخضع الشروط التي تستبعد صراحةً للمادة (L.113-1) التي سبق بحثها في الفرع الأول.

¹ (بغدادى شامبي، مصدر السابق، ص253).

⁽²⁾ Ewing Construction Co. v. Amerisure Insurance Co., 420 S.W.3d 30, 36 (Tex. 2014).

⁽³⁾ Ibid., pp.37-38.

⁽⁴⁾ نص المادة (1199) من القانون المدني الفرنسي باللغة الفرنسية، بصيغتها المعدلة بالمرسوم بقانون رقم (2016-131) في 10 شباط 2016: «Le contrat ne crée d'obligations qu'entre les parties. Les tiers ne peuvent ni demander l'exécution du contrat ni se voir contraints de l'exécuter, sous réserve des dispositions de la présente section et de celles du chapitre III du titre IV».

وفي القانون العراقي، تجيز المادة (1/259) من القانون المدني «الاتفاق على أن يتحمل المدين تبعة الحادث الفجائي والقوة القاهرة». فإذا تعهدت الشركة بتبعة الهجوم الذي لا يمكن توقعه ولا دفعه، كانت مسؤوليتها في هذا القدر اتفاقية لا قانونية، فلا يضمنها المؤمن ما لم تشملها الوثيقة. ونرى أنها إن أبرمت هذا الاتفاق أثناء سريان الوثيقة زادت الخطر المؤمن منه، فيلزمها إخطار المؤمن به وفق المادة (1/986ج)⁽¹⁾.

ج. حدود الضمان عند تعدد المضرورين من واقعة واحدة

إذا تعدد المضرورون من واقعة واحدة وجاوزت مطالباتهم مبلغ التأمين، ثارت مسألتان: هل تُعد مطالباتهم حادثاً واحداً يقابله حد واحد؟ وكيف يُقسم الحد بينهم إذا لم يكفهم؟ وهذه هي المشكلة النموذجية في مسؤولية شركات الأمن السيبراني، لأنها تخدم عملاء كثيرين بأدوات واحدة، فقد يصيبهم الخلل الواحد جميعاً؛ ومن ذلك أن تحديثاً برمجياً واحداً أصدرته شركة الأمن السيبراني (CrowdStrike) في تموز 2024 أصاب نحو 8.5 ملايين جهاز يعمل بنظام ويندوز⁽²⁾.

ففي القانون الأمريكي، قضت المحكمة العليا لولاية تكساس في قضية (تكساس فارمرز للتأمين ضد سوريانو) لعام 1994 بأن المؤمن الذي يواجه مطالبات لا يكفيها المبلغ «يجوز له أن يبرم تسوية معقولة مع أحد المطالبين، ولو استنفدت هذه التسوية المبلغ المتاح للوفاء بالمطالبات الأخرى أو أنقصته»⁽³⁾. وهذا يفتح باب السباق بين المضرورين، وقد نبهت المحكمة العليا الأمريكية في قضية (ستيت فارم ضد تاشاير) لعام 1967 إلى أن أول من يحصل منهم على حكم أو تسوية «قد يستأثر بالمبلغ كله أو بحصة غير متناسبة منه»، وأقرت لجوء المؤمن إلى دعوى التزامم لقسمة المبلغ بين المطالبين⁽⁴⁾؛ فحماية المضرورين المتعددين هناك إجرائية في الغالب.

وفي القانون الفرنسي، حسمت المادة (L.124-1-1) من قانون التأمين الفرنسي لسنة 1976 المسألة الأولى، إذ تنص على أنه: «يُعد حادثاً... كل ضرر أو مجموعة أضرار تلحق بالغير وتقيم مسؤولية المؤمن له، وتنتج عن فعل ضار، وتؤدي إلى مطالبة أو أكثر... وتُعد مجموعة الأفعال الضارة ذات السبب

⁽¹⁾ وتنص المادة (1/986ج) منه على أن يلتزم المؤمن له: «أن يخطر المؤمن بما يطرأ أثناء العقد من أحوال من شأنها أن تؤدي إلى زيادة هذه المخاطر».

⁽²⁾ Microsoft, Helping our customers through the CrowdStrike outage, Official Microsoft Blog, July 20, 2024, available at: <https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage.2/10/2026> ، تاريخ آخر زيارة في 2/10/2026

⁽³⁾ Texas Farmers Insurance Co. v. Soriano, 881 S.W.2d 312, 315 (Tex. 1994).

⁽⁴⁾ State Farm Fire & Casualty Co. v. Tashire, 386 U.S. 523, 533. (1967)



الفني الواحد بمنزلة فعل ضار واحد»⁽¹⁾. فالخلل الفني الواحد الذي يصيب عملاء الشركة جميعاً حادث واحد يقابله حد واحد، ولو تعددت المطالبات وتفرقت في الزمن. ولم يضع المشرع قاعدة لقسمة الحد بين المضرورين، والمادة (L.124-3) تمنع الوفاء لغير المضرور دون أن تفضل بين المضرورين أنفسهم.

وفي القانون العراقي، تجعل المادة (989) قيمة التأمين سقفاً لا يجوز تجاوزه⁽²⁾، ولا نص يجمع المطالبات الناشئة عن سبب واحد كالنص الفرنسي، ولا قاعدة لقسمة المبلغ بين المضرورين. ونرى أن المرجع في ذلك المادة (2/260): «جميع الدائنين متساوون في هذا الضمان إلا من كان له منهم حق التقدم طبقاً للقانون»، فيقتسمون المبلغ قسمة غرماء كلٌ بنسبة حقه، مع براءة ذمة المؤمن الذي يوفي من تقدم منهم بحسن نية وهو لا يعلم بغيرهم⁽³⁾. فإذا أصاب الخلل الواحد عملاء الشركة اقتسموا حداً واحداً، ولذلك تتوقف فاعلية هذا التأمين في حماية المضرورين على كفاية حده.

ثانياً: الوفاء بالتزام المؤمن بالضمان

يوفي المؤمن بالتزامه للمضرور لا للمؤمن له، إذ يمنعه النقصان العراقي والفرنسي اللذان سبق بيانهما من الوفاء لغيره قبل تعويضه. ويقتضي بيان الوفاء تحديد صاحب الحق في المطالبة وطريقها، ثم الدفع التي يحتج بها المؤمن عليه؛ ويفرق الفقه فيها بين الدفع السابقة على الحادث فيُحتج بها على المضرور، واللاحقة له فلا يُحتج بها⁽⁴⁾.

أ. الموفى له: المضرور ودعواه المباشرة، ومركز العميل المتعاقد

المضرور أجنبي عن عقد التأمين، فلا يطالب المؤمن في الأصل إلا باسم المؤمن له بالدعوى غير المباشرة، فيزاحمه دائنو المؤمن له في حصيلتها؛ ولذلك قررت التشريعات الحماية له دعوى مباشرة يرفعها باسمه ويستأثر بحصيلتها. ومضرور شركة الأمن السيبراني في الغالب عميلها المتعاقد معها، وهو

¹ نص المادة (L.124-1-1) من قانون التأمين الفرنسي باللغة الفرنسية، المضافة بالقانون رقم (706-2003) في 1 آب 2003: «Au sens du présent chapitre, constitue un sinistre tout dommage ou ensemble de dommages causés à des tiers, engageant la responsabilité de l'assuré, résultant d'un fait dommageable et ayant donné lieu à une ou plusieurs réclamations. Le fait dommageable est celui qui constitue la cause génératrice du dommage. Un ensemble de faits dommageables ayant la même cause technique est assimilé à un fait dommageable unique».

² د. هالة صلاح الحديثي، مصدر السابق، ص24.

³ سمية مكريش، الدعوى المباشرة في التأمين من المسؤولية، بحث منشور في مجلة العلوم الإنسانية، جامعة الإخوة منتوري قسنطينة 1، العدد 46، المجلد أ، 2016، ص508.

⁴ المصدر السابق، ص509.

مع ذلك أجنبي عن عقد التأمين، فلا يحول عقده مع الشركة دون انتفاعه بالدعوى المباشرة حيث يقررها القانون.

ففي القانون الأمريكي، الأصل شرط «لا دعوى» الذي يمنع مقاضاة المؤمن قبل أن يتحدد التزام المؤمن له نهائياً بحكم أو باتفاق بينه وبين المطالب والمؤمن، وقد عرضت المحكمة العليا الأمريكية هذا الشرط في قضية (واطسن ضد شركة تأمين مسؤولية أرباب العمل) لعام 1954⁽¹⁾. ولا يتجاوز المضرور هذا الأصل إلا بنص، كقانون ولاية لويزيانا الذي يجيز الدعوى المباشرة، لكنه قصرها بعد تعديلات سنة 2024 على حالات محددة، منها إفلاس المؤمن له أو إفساره أو وفاته أو تعذر إعلانه⁽²⁾.

وفي القانون الفرنسي، تنص الفقرة الأولى من المادة (L.124-3) من قانون التأمين الفرنسي لسنة 1976 على أن: «لغير المضرور حق الدعوى المباشرة على المؤمن الضامن للمسؤولية المدنية للشخص المسؤول»⁽³⁾. وقد أضيفت هذه الفقرة سنة 2007، وكانت المادة قبلها مقصورة على منع الوفاء لغير المضرور، ومع ذلك كان قضاء محكمة النقض يقر الدعوى المباشرة، فلم تكن الإضافة إلا تقنياً له⁽⁴⁾.

¹ (Watson v. Employers Liability Assurance Corp., 348 U.S. 66, 68 (1954): "No action shall lie against the company unless, as a condition precedent thereto, the insured shall have fully complied with all the terms of this policy, nor until the amount of the insured's obligation to pay shall have been finally determined either by judgment against the insured after actual trial or by written agreement of the insured, the claimant and the company".

² (نص الفقرة (B)(1) من المادة (22:1269) من القوانين المنقحة لولاية لويزيانا باللغة الإنجليزية، بصيغتها المعدلة سنة 2024: "The injured person or, if deceased, the persons identified in Civil Code Articles 2315.1 and 2315.2, shall have no right of direct action against the insurer unless at least one of the following applies: (a) The insured files for bankruptcy in a court of competent jurisdiction or when proceedings to adjudge an insured bankrupt have been commenced before a court of competent jurisdiction. (b) The insured is insolvent. (c) Service of citation or other process has been attempted without success or the insured defendant refuses to answer or otherwise defend the action within one hundred eighty days of ... service. ... (f) The insured is deceased

³ (نص الفقرة الأولى من المادة (L.124-3) من قانون التأمين الفرنسي باللغة الفرنسية، المضافة بالقانون رقم (2007-1774) في 17 كانون الأول 2007: « Le tiers lésé dispose d'un droit d'action directe à l'encontre » «.de l'assureur garantissant la responsabilité civile de la personne responsable

⁴ (Franck Riester, Rapport fait au nom de la Commission des affaires économiques, de l'environnement et du territoire sur le projet de loi portant diverses dispositions d'adaptation au droit communautaire dans les domaines économique et financier, Assemblée nationale, n° 406, 13 novembre 2007, p.16.

ولا يعرف القانون المدني العراقي نصاً يقرر الدعوى المباشرة صراحةً، وإنما منعت المادة (1006) المؤمن من الوفاء لغير المضرور قبل تعويضه، وهي نظير النص الفرنسي الذي أقر القضاء في ظله الدعوى المباشرة قبل تقنينها. وقد قرر المشرع العراقي هذه الدعوى صراحةً في تأمين حوادث السيارات، إذ تنص المادة (14) من قانون التأمين الإلزامي من حوادث السيارات رقم (52) لسنة 1980 على أن «يكتسب المتضرر حقاً مباشراً قبل المؤمن ولا يحتج عليه بالحالات المنصوص عليها في المادة (8) من هذا القانون». فإن لم يُعترف للمضرور بها في غير ذلك، بقيت له الدعوى غير المباشرة وفق المادة (261) من القانون المدني، وعيها أن «كل فائدة تنتج من استعمال هذه الحقوق تدخل في أموال المدين وتكون ضماناً لجميع دائنيه» بحكم المادة (262). ونرى أن المادة (1006)، وقد خصصت مبلغ التأمين للمضرور، تقتضي الاعتراف له بحق مباشر عليه، وهو ما تحتاجه حماية عملاء شركات الأمن السيبراني، ويحسن أن يقرره المشرع صراحةً.

ب. الدفع السابقة على الحادث

يتلقى المضرور حقه من عقد التأمين على حاله يوم الحادث، فيُحتج عليه بما نشأ قبله من دفع، كبطلان العقد، ووقف الضمان لعدم دفع القسط، وخروج الواقعة عن نطاق الضمان وحدوده. وأبرز هذه الدفع في التأمين السيبراني الدفع بكذب البيانات المتعلقة بتدابير الأمن؛ لأن المؤمن يقدر الخطر من استمارة الطلب، وهي استبيان يجيب عنه طالب التأمين بنفسه⁽¹⁾، وقد يشترط عليه تدابير حماية محددة يُخفّض التعويض أو يُرفض إن لم يلتزم بها⁽²⁾. وتقلب في شركة الأمن السيبراني صورة التفاوت المعهودة في المعرفة بين طرفي العقد؛ فهي أعلم بأمن أنظمتها من المؤمن، فيقل عذرها فيما تقرره منه خطأً.

ففي القانون الأمريكي، ينص قانون ولاية لويزيانا على أن الدعوى المباشرة «تخضع لجميع الشروط المشروعة في الوثيقة أو العقد، وللدفع التي يجوز للمؤمن أن يتمسك بها في دعوى مباشرة يرفعها المؤمن له»⁽³⁾؛ فلا يملك المضرور أكثر مما يملكه المؤمن له.

(1) Daniel Woods, Ioannis Agrafiotis, Jason R. C. Nurse and Sadie Creese, Mapping the coverage of security controls in cyber insurance proposal forms, Journal of Internet Services and Applications, Vol. 8, No. 8, 2017, p.1.

(2) د. محمد سعيد إسماعيل، التأمين الإلكتروني ضد المخاطر السيبرانية: المشكلات القانونية والحلول المقترحة – دراسة في القانون القطري والمقارن، بحث منشور في المجلة الدولية للقانون، جامعة قطر، المجلد العاشر، العدد الثالث (عدد خاص)، 2021، ص224.

(3) It is the intent of this Section that any action brought under the provisions of this Section shall be subject to all of the lawful conditions of the policy or contract and the defenses which

وفي القانون الفرنسي، تنص المادة (L.112-6) على أنه: «يجوز للمؤمن أن يحتج على حامل الوثيقة أو على الغير الذي يتمسك بالانتفاع بها بالدفع التي يجوز الاحتجاج بها على المكتتب الأصلي»⁽¹⁾، ومنها بطلان العقد الذي تقضي به المادة (L.113-8) في حالة الكتمان أو البيان الكاذب العمدي من جانب المؤمن له، إذا كان من شأن هذا الكتمان أو البيان الكاذب أن يغير موضوع الخطر أو ينقص من تقدير المؤمن له⁽²⁾.

وفي القانون العراقي، توجب المادة (1/986/ب) على المؤمن له أن يقرر وقت إبرام العقد كل الظروف المعلومة له التي يهم المؤمن معرفتها، و«يعتبر مهماً في هذا الشأن الوقائع التي جعلها المؤمن محل أسئلة مكتوبة»، وتجزئ المادة (1/987) للمؤمن طلب فسخ العقد إذا تعمد المؤمن له كتمان أمر أو قدم عن عمد بياناً كاذباً يغير موضوع الخطر أو يقلل أهميته في نظره. ولما كان هذا الإخلال سابقاً على الحادث، فإنه يُحتج به على المضرور؛ فتغدو أسئلة الاستمارة عن تدابير الأمن هي المقياس الذي يُوزن به صدق الشركة.

ج. الدفع اللاحقة للحادث

أما ما ينشأ بعد الحادث من إخلال المؤمن له، كالتأخر في إخطار المؤمن أو الإقرار بالمسؤولية دون رضاه، فالأصل في التشريعات الحمائية ألا يُحتج به على المضرور، لأن حقه ثبت بوقوع الحادث فلا يضار بفعل لاحق لا يد له فيه. ولهذه المسألة في نشاطنا بعدد خاص؛ فشركة الأمن السيبراني ملزمة بالإبلاغ عن الخرق للجهات الرقابية وللعلاء على ما سبق بيانه، وقد يبدو الإبلاغ إقراراً بالمسؤولية يخالف شرط عدم الإقرار الشائع في الوثائق.

could be urged by the insurer to a direct action brought by the insured, provided the terms and conditions of such policy or contract are not in violation of the laws of this state".

¹ نص المادة (L.112-6) من قانون التأمين الفرنسي باللغة الفرنسية: «L'assureur peut opposer au porteur de la police ou au tiers qui en invoque le bénéfice les exceptions opposables au souscripteur originaire».

² نص الفقرة الأولى من المادة (L.113-8) من قانون التأمين الفرنسي باللغة الفرنسية، بصيغتها المعدلة بالقانون رقم (5-81) في 7 كانون الثاني 1981: «Indépendamment des causes ordinaires de nullité, et sous réserve des dispositions de l'article L. 132-26, le contrat d'assurance est nul en cas de réticence ou de fausse déclaration intentionnelle de la part de l'assuré, quand cette réticence ou cette fausse déclaration change l'objet du risque ou en diminue l'opinion pour l'assureur, alors même que le risque omis ou dénaturé par l'assuré a été sans influence sur le sinistre».

ففي القانون الأمريكي، قد يُحتج على المضرور بشروط الإبلاغ في الوثيقة؛ فقد قضت المحكمة العليا لولاية لويزيانا في قضية (غورمان ضد مدينة أوبلوساس) لعام 2014 بأن «إعمال شروط الوثيقة المتعلقة بتقديم المطالبات والإبلاغ عنها لا يحرم الغير المضرور من حق الدعوى بموجب قانون الدعوى المباشرة»⁽¹⁾، فأجازت الاحتجاج عليه بشرط الإبلاغ في وثائق المطالبة المقدمة، وهي الصيغة التي تجري عليها وثائق المسؤولية السيبرانية في الغالب على ما سبق في الفرع الأول.

وفي القانون الفرنسي، توجب المادة (R.124-1) أن تنص وثائق تأمين المسؤولية المدنية على أنه «لا يُحتج على المضرورين أو ذوي حقوقهم بأي سقوط يستند إلى إخلال المؤمن له بالتزاماته بعد الحادث»⁽²⁾. وتجيز المادة (L.124-2) للمؤمن أن يشترط عدم الاحتجاج عليه بأي إقرار بالمسؤولية أو صلح يتم دون تدخله، لكنها تنص على أن «الإقرار بمادية واقعة لا يجوز أن يُعد اعترافاً بالمسؤولية»⁽³⁾؛ فإبلاغ الشركة عن الخرق إقرار بواقعة مادية لا يسقط به حقها في الضمان.

وفي القانون العراقي، لا نص عاماً كالنص الفرنسي يمنع الاحتجاج على المضرور بالدفع اللاحقة للحادث، وإنما أبطلت المادة (2/985) الشرط الذي يقضي بسقوط حق المؤمن له بسبب تأخره في إعلان الحادث إلى السلطات أو في تقديم المستندات «إذا تبين من الظروف أن التأخر كان لعذر مقبول»، وأجازت المادة (1005) الاتفاق على إعفاء المؤمن من الضمان إذا أقر المستفيد للمتضرر بالمسؤولية دون رضاه، ومنعت التمسك به «إذا كان ما أقر به المستفيد مقتصرًا على واقعة مادية». فإبلاغ الشركة عن الخرق تنفيذًا لالتزامها القانوني إقرار بواقعة مادية لا يسقط حقها. ونرى أن حماية عملاء الشركة تقتضي تقرير قاعدة عامة كالفرنسية تمنع الاحتجاج عليهم بالدفع اللاحقة للحادث.

(1) Gorman v. City of Opelousas, 148 So. 3d 888, 896 (La. 2014).

(2) نص الفقرة الأولى من المادة (R.124-1) من قانون التأمين الفرنسي باللغة الفرنسية: « Les polices d'assurance garantissant des risques de responsabilité civile doivent prévoir qu'en ce qui concerne cette garantie aucune déchéance motivée par un manquement de l'assuré à ses obligations commis postérieurement au sinistre ne sera opposable aux personnes lésées ou à leurs ayants droit ».

(3) نص المادة (L.124-2) من قانون التأمين الفرنسي باللغة الفرنسية: « L'assureur peut stipuler qu'aucune reconnaissance de responsabilité, aucune transaction, intervenues en dehors de lui, ne lui sont opposables. L'aveu de la matérialité d'un fait ne peut être assimilé à la reconnaissance d'une responsabilité ».



الخاتمة



الخاتمة

بعد أن استوفت هذه الدراسة بيان المسؤولية المدنية لشركات الأمن السيبراني في (دراسة مقارنة)، خلصت إلى جملة من النتائج والمقترحات يمكن بيانها على النحو الآتي:

أولاً: النتائج

1. تبين أن الأنظمة القانونية الثلاثة تفتقر التي تناولتها الدراسة إلى تعريف تشريعي لشركات الأمن السيبراني ، بوصفها شخصاً معنوياً متميزاً، إذ اكتفت تشريعاتها بتعريف النشاط والوظيفة دون الكيان، وهو قصور مفاهيمي حقيقي يُعقّد تحديد القواعد الواجبة التطبيق ويُضعف الأساس القانوني لدعوى المسؤولية المدنية أمام القضاء .
2. تتمتع شركات الأمن السيبراني بطبيعة قانونية مزدوجة لا يمكن إغفال أي من بُعديها عند تكييفها قانونياً، فهي من حيث التأسيس والتنظيم أشخاص معنوية خاصة تخضع لقواعد القانون المدني والتجاري، فإنها ومن حيث الوظيفة تمثل كيانات تمارس صلاحيات ذات طابع سيادي جزئي بتفويض من الدولة لا بحق أصيل، وهذا التفويض هو الذي يُشَدّد معيار العناية الواجبة في مواجهتها دون أن يُخرجها من دائرة القانون الخاص.
3. أتضح لنا اختلاف التزام شركات الأمن السيبراني اختلافاً جوهرياً عن التزام شركات تقنية المعلومات من حيث طبيعته ونطاقه، إذ يتجاوز في كثير من الحالات حدود التزام بذل العناية ليقترّب من التزام تحقيق النتيجة كلما تضمّن العقد تحديداً واضحاً لمستوى الحماية الأمنية المطلوب، وهو ما يُقلب عبء الإثبات في دعوى المسؤولية المدنية بحيث يكفي للمضرور إثبات عدم تحقق النتيجة لا إثبات تقصير الشركة..
4. لا تقتصر مسؤولية شركات الأمن السيبراني على الإطار التعاقدى الثنائي مع العميل، بل تمتد لتشمل المسؤولية التقصيرية تجاه الغير الذي يتضرر من الإخفاقات الأمنية، والمسؤولية الإدارية أمام الجهات الرقابية عند انتهاك الالتزامات التنظيمية، والمسؤولية الفردية للمديرين والفنيين متى بلغ خطأهم الشخصي درجة الإهمال الجسيم أو تجاوز حدود الوظيفة، وهذا التعدد في مستويات المسؤولية يعكس خصوصية هذا النشاط وارتباطه بالمصلحة العامة الرقمية.
5. أظهرت المقارنة بين الأنظمة الثلاثة أن النظام الفرنسي هو الأكثر تطوراً في تنظيم نشاط شركات الأمن السيبراني من خلال نظام التأهيل والاعتماد الذي تشرف عليه الوكالة الوطنية لأمن نظم المعلومات، في حين يتسم النظام الأمريكي بتعدد جهات التنظيم وتشتت الأطر القانونية بتعدد



القطاعات، أما النظام العراقي فلا يزال في طور بناء منظومته المؤسسية رغم أن اللائحة رقم 33 لسنة 2025 مثلت خطوة تشريعية مهمة في هذا الاتجاه.

6. يفتقر القانون المدني العراقي إلى نص صريح يُحدد طبيعة التزام شركات الأمن السيبراني ويُميز بين التزام بذل العناية والتزام تحقيق النتيجة في عقود الحماية الرقمية، مما يؤدي إلى اضطراب في تطبيق قواعد الإثبات وعدم اليقين في تقدير التعويض، وهو فراغ تشريعي يستوجب معالجة عاجلة.

7. كشفت الدراسة أن الخطأ المهني في نشاط شركات الأمن السيبراني يتسم بخصوصية تقنية تجعل إثباته أمراً عسيراً على المضرور العادي، مما يُرجّح اعتماد معيار موضوعي مشدّد في تقييم سلوك هذه الشركات يستند إلى معايير الممارسة المهنية المعتمدة دولياً كإطار عمل المعهد الوطني للمعايير والتكنولوجيا الأمريكي، لا إلى المعيار الذاتي للشخص المعقول العادي.

8. يُشكّل الالتزام بالإفصاح عن المخاطر السيبرانية والإبلاغ عن الحوادث التزاماً قانونياً مستقلاً وليس مجرد التزام تبعي، وإخلال شركة الأمن السيبراني بهذا الالتزام يُرتّب مسؤوليتها المدنية بصورة مستقلة عن المسؤولية الناجمة عن الإخفاق الأمني الفعلي، وهو ما أكدته التشريعات المقارنة الثلاثة وإن تفاوتت في درجة صراحة النص عليه.

9. أثبتت الدراسة أن المسؤولية الفردية للمديرين والفنيين في شركات الأمن السيبراني لا تقوم عند مجرد وقوع الإخفاق الأمني، بل تستلزم إثبات خطأ شخصي منفصل عن الوظيفة يبلغ درجة الإهمال الجسيم أو يتضمن قصداً في الإضرار، وهو معيار تتبناه الأنظمة الثلاثة وإن اختلفت في تسميته وآليات تطبيقه.

10. تكشف مقارنة الأنظمة الثلاثة أن ثمة توجهاً دولياً متنامياً نحو توسيع نطاق مسؤولية شركات الأمن السيبراني وتشديد معاييرها استجابةً لتصاعد المخاطر الرقمية وتوسع نطاق الأضرار الناجمة عن الإخفاقات الأمنية، وهو توجه ينبغي للمشروع العراقي مواكبته لا سيما في ضوء التوسع المتسارع في الاعتماد على الأنظمة الرقمية في المعاملات الحكومية والتجارية والمصرفية.



ثانياً: المقترحات

1. دعوة المشرّع العراقي إلى تعديل أحكام التأمين ضد المسؤولية في القانون المدني رقم 40 لسنة 1951، بإضافة المواد الآتية بعد المادة (1006). واستعملت فيها لفظ «المستفيد» لأنه لفظ المواد (1004-1006) نفسها:

أ. المادة الأولى المقترحة - تحريك الضمان:

(يجوز الاتفاق في التأمين ضد المسؤولية على أن ينعقد الضمان بمطالبة المتضرر خلال مدة العقد. وعندئذ يشمل الضمان الحوادث السابقة على إبرامه ما لم يثبت المؤمن أن المستفيد كان عالماً بها وقت التعاقد. ويمتد إلى المطالبات التي تُقدّم خلال خمس سنوات من انتهاء العقد عن حوادث وقعت قبل انتهائه، بحد لا يقل عن حد السنة الأخيرة. ويقع باطلاً كل اتفاق على إنقاص هذه المدة).

ب. المادة الثانية المقترحة - الاستبعادات المتصلة بالأمن والفدية:

(لا يصح الشرط الذي يستبعد من الضمان الضرر الناشئ عن إخلال المستفيد بتدابير أمن المعلومات إلا إذا حدد التدبير المطلوب تحديداً واضحاً، وكان الإخلال به سبباً في وقوع الحادث. ولا يلتزم المؤمن بضمان ما يُدفع فديةً بسبب اعتداء على نظام معلوماتي إلا إذا أبلغت الجهات المختصة بالاعتداء خلال اثنتين وسبعين ساعة من العلم به).

ج. المادة الثالثة المقترحة - وحدة الحادث وتعدد المتضررين:

(تُعدّ الأضرار الناشئة عن سبب تقني واحد حادثاً واحداً في تطبيق حد التأمين. وإذا تعدد المتضررون ولم يكف مبلغ التأمين لتعويضهم، قُسم بينهم بنسبة حقوقهم، وتبرأ ذمة المؤمن إذا أوفى بحسن نية لمن تقدم منهم قبل علمه بغيره).

ز. المادة الرابعة المقترحة - حق المتضرر المباشر:

(للمتضرر حق مباشر قبل المؤمن في حدود مبلغ التأمين. ولا يُحتج عليه بالدفع التي تنشأ بعد وقوع الحادث، مع حفظ حق المؤمن في الرجوع بها على المستفيد. ولا تُقتطع نفقات الدفاع في دعوى المسؤولية من مبلغ التأمين ما دام المتضرر لم يُعوّض).

2. نقترح تعديل اللائحة التنظيمية رقم 33 لسنة 2025 الصادرة عن هيئة الإعلام والاتصالات بإضافة المواد الآتية:

المادة الأولى المقترحة - تعريف شركة الأمن السيبراني بأنها :



(تُعدّ شركة الأمن السيبراني في تطبيق أحكام هذه اللائحة كل شخص معنوي يُنشأ وفق الأحكام القانونية ويُمنح رخصة لمزاولة نشاط مهني محدد يتمثل في تقديم خدمات حماية وتأمين الأنظمة الرقمية، الشبكات والبيانات. ويخضع هذا الكيان في مزاولة نشاطه لأحكام القوانين ذات الصلة، ويتحمل المسؤولية القانونية الكاملة عن أي إخلال بالتزاماته تجاه العملاء أو الأطراف المتضررة).

المادة الثانية المقترحة - طبيعة الالتزام:

(يُعدّ التزام شركة الأمن السيبراني التزاماً بتحقيق نتيجة فيما يخص المستويات الأمنية المحددة صراحةً في العقد كمستويات كشف التهديدات وزمن الاستجابة ودرجة الوقاية، ويكفي لقيام المسؤولية المدنية في هذه الحالة عدم تحقق النتيجة المتفق عليها ما لم تثبت الشركة وجود سبب أجنبي. أما فيما لم يُحدده العقد من مستويات أمنية ، فيُعدّ التزام الشركة التزاماً ببذل عناية مهنية مشددة تُقاس وفق المعايير الفنية الدولية المعتمدة).

المادة الثالثة المقترحة - الإفصاح عن الحوادث:

(تلتزم شركة الأمن السيبراني بالإفصاح الفوري لعملائها وللجهة الرقابية المختصة عن أي حادثة سيبرانية تمس أمن بياناتهم أو تؤثر في استمرارية خدماتهم، وذلك خلال مدة لا تتجاوز اثنتين وسبعين ساعة من اكتشافها. ويترتب على الإخلال بهذا الالتزام مسؤولية مدنية مستقلة عن المسؤولية الناجمة عن الحادثة ذاتها، يُقدّر فيها التعويض على أساس الأضرار الناجمة عن التأخير في الإفصاح).

المادة الرابعة المقترحة - التأمين الإلزامي:

(تلتزم شركة الأمن السيبراني العاملة في حماية القطاعات الحيوية كالقطاع المصرفي وقطاع الطاقة وقطاع الاتصالات بالحصول على تأمين إلزامي من المسؤولية المدنية بحد أدنى تحدده الجهة الرقابية المختصة بحسب حجم الشركة ونطاق عملها، وذلك ضماناً لحق المتضررين في التعويض الفعلي حتى في حال إعسار الشركة أو توقفها عن النشاط).

3. دعوة المشرّع العراقي الى تعديل قانون الشركات رقم 21 لسنة 1997 المعدل بإضافة المادة الآتية:

(يُسأل المدير المفوض للأمن المعلوماتي في شركة الأمن السيبراني ، في مسؤوليته الشخصية ، عن الأضرار الناجمة عن إهماله الجسيم أو تجاوزه الصريح للمعايير المهنية المعتمدة، وذلك بصرف النظر عن مسؤولية الشركة بوصفها شخصاً معنوياً مستقلاً. وللمتضرر المطالبة بالتعويض في مواجهة الشركة والمدير معاً أو أيهما، مع احتفاظ الشركة بحق الرجوع على المدير المخطئ فيما أدته من تعويض وفق أحكام المادة (219) من القانون المدني).



4. دعوة المشرّع العراقي إلى إصدار قانون خاص يُنشئ دائرة قضائية متخصصة في النزاعات الرقمية والسيبرانية على أن يتضمن المادة الآتية:

(تختص الدائرة القضائية المتخصصة في النزاعات الرقمية بالفصل في الدعاوى المدنية الناجمة عن الإخلال بعقود الأمن السيبراني وما يترتب عليها من مسؤولية، مع إمكانية الاستعانة بخبراء فنيين معتمدين من هيئة الإعلام والاتصالات للبت في المسائل التقنية المرتبطة بالنزاع، وتسري على إجراءاتها أحكام قانون المرافعات المدنية مع مراعاة خصوصية الدليل الرقمي وإجراءات حفظه وإثباته).



المصادر

المراجع

أولاً: المعاجم

- 1- ابو الفضل جمال الدين محمد بن مكرم بن منظور الافريقي المصري، لسان العرب، ابن منظور، ج2، مادة شرك، دار الحديث، القاهرة، الطبعة المنقحة، 2013.
- 2- المعجم الوسيط، مجمع اللغة العربية بالقاهرة، الطبعة الثانية، القاهرة، مادة أمن، 1972.

ثانياً: الكتب القانونية

1. د. أنور سلطان، مصادر الالتزام في القانون المدني، ط10، دار الثقافة للنشر والتوزيع، عمان، 2018.
2. أيمن ابراهيم العشماوي، مفهوم العقد وتطوره، دراسة مقارنة، دار النهضة العربية، القاهرة، 2002.
3. حازم الشمري، توظيف القوة السيبرانية في استراتيجيات الدول الكبرى، دار انكي للنشر والتوزيع، بغداد، 2022.
4. حسام الدين كامل الاهواني، مصادر الالتزام، دار النهضة العربية، مصر، 1991- 1992.
5. د. حسن علي الذنون، شرح القانون المدني، أصول الالتزام، مطبعة المعارف، بغداد، 1970.
6. د. حسين الماحي، الشركات التجارية، دار النهضة العربية، القاهرة، 2010.
7. د. حيدر فالح سليمان، مقدمة في الامن السيبراني، ط1، الذاكرة للنشر والتوزيع، العراق - بغداد، 2024.
8. خالد جمال احمد حسن، الالتزام بالإعلام قبل التعاقد، دراسة مقارنة، دار النهضة العربية، القاهرة، 1996.
9. د. سعيداني نعيم، الحماية القانونية للحق في الخصوصية المعلوماتية (دراسة مقارنة)، ط1، المؤسسة الحديثة للكتاب، لبنان - بيروت، 2022.
10. زاهية حورية سي يوسف، المسؤولية المدنية للمنتوج، دار هومه للطباعة والنشر، الجزائر، 2009.
11. د. طارق عفيفي صادق، الخطر محل التأمين من المسؤولية المدنية في مجال المعلوماتية، ط1، دار الحكمة، القاهرة، 2013.
12. د. عبد الحي حجازي، النظرية العامة للالتزام، ج3، احكام الالتزام، مطبعة نهضة مصر، 1953.
13. د. عبد الرزاق أحمد السنهوري، الوسيط في شرح القانون المدني، ج7، م2: عقود الغرر (عقود المقامرة والرهان والمرتب مدى الحياة وعقد التأمين)، دار إحياء التراث العربي، بيروت، 1964.

14. عبد القادر الاقصاوي، الالتزام بضمان السلامة في العقود، ط1، دار الفكر العربي، مصر، 2010.
15. د. عبد المجيد الحكيم، عبد الباقي البكري، محمد طه البشير، القانون المدني وأحكام الالتزام، ج2، وزارة التعليم العالي والبحث العلمي، بغداد،
16. د. عبد المنعم فرج صدة، احكام الالتزام، شركة مكتبة ومطبعة مصطفى البابي الحلبي وأولاده، دون مكان نشر، 1965.
17. د. عبد الفتاح محمود كيلاني، مدى المسؤولية القانونية لمقدمي خدمات الانترنت، دار الجامعة الجديدة، الإسكندرية، 2011.
18. علي محيي الدين القرة داغي، مبدأ الرضا في العقود، ج1، ط3، دار البشائر، 2008.
19. علي علي سليمان، النظرية العامة للالتزام، مصادر الالتزام في القانون المدني الجزائري، ط5، ديوان المطبوعات الجامعية، 2003.
20. علي محمد دهب، التشفير وأمن المعلومات، كلية دراسات الحاسوب والإحصاء، جامعة كردفان، بلا طبعة، بلا سنة نشر.
21. د. محمد أحمد سلامة مشعل، الحق في محو البيانات الشخصية (دراسة تحليلية في ضوء لائحة حماية البيانات بالاتحاد الأوروبي GDPR وأحكام المحاكم الأوروبية)، بلا سنة نشر.
22. د. محمد حسين منصور، المسؤولية الالكترونية، دار الجامعة الجديدة، مصر، 2007.
23. محمد دغمان، الزامية العقد، ط2، مجلد1، منشورات زين الحقوقية، 2018.
24. محمد عبد الظاهر حسين، المسؤولية القانونية في مجال شبكات الانترنت، دار النهضة العربية، القاهرة، 2002.
25. د. محمد مصطفى زرباني، الشركات التجارية، دراسة في النشأة التعاقدية والنظام القانوني، المطبعة العالمية، 2020.
26. محفوظ لشعب، المبادئ العامة للقانون الجزائري، ط5، ديوان المطبوعات الجامعية، الجزائر، 2011.
27. منذر الفضل، الوسيط في شرح القانون المدني، دار نارس، أربيل، 2006.
28. د. مصطفى الخطيب، الموجز في النظرية العامة للالتزامات، مطبعة قرطبة، دون مكان نشر، 2019.
29. مصطفى أحمد أبو الخير، الشركات العسكرية والأمنية الدولية الخاصة، دراسة قانونية سياسية، ط1، اترك للطباعة والنشر والتوزيع، القاهرة، 2008.
30. فارس حامد عبد الكريم، المعيار القانوني، ط1، بلا دار ومكان نشر، 2009.
31. د. نشوان أحمد المجر، التشفير وأمنية المعلومات، ط2، دار الكتب اليمنية للطباعة والنشر والتوزيع، صنعاء، 2018.



32. وليد الزبيدي، القرصنة على الانترنت والحاسوب، ط1، دار أسامة للنشر والتوزيع، الأردن – عمان، دون سنة نشر.

ثالثاً: الأطاريح والرسائل الجامعية

1. أماني تموز عبد الرحمن الخفاجي، الحماية التأمينية للشركات التجارية من المخاطر السيبرانية، رسالة ماجستير، كلية القانون، جامعة ميسان، 2024.
2. السيد بدوي، نحو نظرية عامة لمبدأ حسن النية في المعاملات المدنية، أطروحة دكتوراة، كلية الحقوق، جامعة القاهرة، 1989.
3. سلطان فياض محمد السكر، جريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية في التشريع الأردني، رسالة ماجستير مقدمة لكلية الحقوق – جامعة الشرق الأوسط، 2022.
4. ريم إحسان محمود موسى، الدعوى المباشرة في التأمين من المسؤولية المدنية، رسالة ماجستير، جامعة النجاح الوطنية، نابلس، 2010.
5. علي عبد الأمير عبيد، المسؤولية الجنائية الناشئة عن انتهاكات الشركات السيبرانية الخاصة في النزاعات المسلحة، رسالة ماجستير، معهد المعلمين للدراسات العليا/قسم القانون، 2024.
6. هديل خضير كاظم البديري، المعقولية في الالتزام العقدي، دراسة مقارنة، رسالة ماجستير، كلية القانون، جامعة كربلاء، 2018.

رابعاً: البحوث والمقالات:

1. د. إبراهيم مضحي أبو هلاله ود. فيصل الشقيرات، التزام المؤمن بالتعويض في التأمين من المسؤولية المدنية: دراسة تحليلية تأصيلية في القانون المدني الأردني، مجلة جامعة الحسين بن طلال للبحوث، المجلد 3، العدد 2، 2017.
2. أحمد هشام فواز العمري، المسؤولية المدنية لمقدمي خدمات الامن السيبراني، أبحاث الدراسات العليا، كلية الحقوق، جامعة المنصورة، مجلد15، عدد35، 2025.
3. د. أمل شافعي و د. ام السعد شافعي، التأسيس للحق في حماية البيانات الشخصية كحق مستقل عن الحق في الخصوصية في تشريع الاتحاد الأوروبي، جامعة الحاج لخضر - باتنة 1، بحث مقدم ال مجلة الباحث القانوني، المجلد 01، العدد 02، 2022.
4. بغدادي شامي، تأمين الخطر السيبراني، مجلة هيرودوت للعلوم الإنسانية والاجتماعية، المجلد 7، العدد 25، 2023.
5. دحموش فايزة. جغام محمد، شركات الحراسة الخاصة وخدمات الامن العمومي، دراسات وابحاث المجلة العربية للأبحاث والدراسات في العلوم الإنسانية والاجتماعية، مجلد14، عدد3، 2022.

6. زوليخة حيمر، مسؤولية المدين العقدية عن فعل الغير، دراسة تحليلية، حوليات جامعة قاملة للعلوم الاجتماعية والإنسانية، قالمه، عدد 1، 2024.
7. سمية مكربش، الدعوى المباشرة في التأمين من المسؤولية، مجلة العلوم الإنسانية، جامعة الإخوة منتوري قسنطينة 1، المجلد أ، العدد 46، 2016.
8. د. عادل موسى عوض جاب الله، وسائل حماية الامن السيبراني (دراسة فقهية تأصيلية مقارنة بالنظم المعاصرة)، بحث منشور في المجلة العلمية في كلية الشريعة والقانون بأسسيوط، جامعة الازهر، العدد 34، ج 3، 2022.
9. طارق عبد العزيز العبيدي، الضرر الادبي وكيفية إثباته في المسؤولية التقصيرية، دراسة في القانون العراقي، مجلة كلية القانون للعلوم القانونية والسياسية، مجلد 1، عدد 2، 2012.
10. كفاء علي عيسى أبورغيف وإبتسام عباس عبد الحسن هادي، تأثير التأمين السيبراني في مخاطر شركات التأمين: دراسة تطبيقية على عينة من شركات التأمين العالمية، Journal Port Science Research، جامعة أوروک، المجلد 9، العدد 3، 2026.
11. محمد سعيد إسماعيل، التأمين الإلكتروني ضد المخاطر السيبرانية: المشكلات القانونية والحلول المقترحة - دراسة في القانون القطري والمقارن، المجلة الدولية للقانون، جامعة قطر، المجلد 10، العدد 3 (عدد خاص)، 2021.
12. مصطفى إبراهيم سلمان الشمري، الامن السيبراني واثره في الامن الوطني العراقي، مجلة العلوم القانونية والسياسية، كلية القانون والعلوم السياسية، جامعة ديالى، العدد 1، مجلد 10، 2021.
13. د. هالة صلاح الحديثي، قواعد التأمين عن الأخطار الإلكترونية (دراسة تحليلية)، مجلة الباحث العربي، المجلد 1، العدد 1، 2020.
14. د. هبة رمضان رجب، الحماية القانونية للبيانات الشخصية في عصر التكنولوجيا الرقمية، بلا عدد، بلا سنة.
15. د. وليد مرزة حمزة المخزومي. محمد خزعل عباس، أمن الفضاء السيبراني، قراءة في المفهوم القانوني، مجلة العلوم القانونية، مجلد 37، ج 2، 2023.



خامساً: التشريعات الدولية

1. اللائحة العامة لحماية البيانات الاوربية (GDPR) .

سادساً: التشريعات الوطنية

1. القانون المدني العراقي رقم (40) لسنة 1951 المعدل.
2. قانون التأمين الإلزامي من حوادث السيارات رقم (52) لسنة 1980.
3. قانون التجارة العراقي رقم 30 لسنة 1984.
4. قانون الشركات العراقي رقم 21 لسنة 1997.
5. دستور جمهورية العراق لسنة 2005.
6. قانون تنظيم أعمال التأمين (الأمر رقم 10 لسنة 2005)، الوقائع العراقية، العدد (3995) في 2005/3/3.
7. قانون حماية المستهلك رقم 1 لسنة 2010.
8. اللائحة التنظيمية الخاصة بتنظيم عمل الشركات المختصة في خدمات الأمن السيبراني العراقي رقم 33 لسنة 2025.

المصادر الأجنبية

First: Books and Academic Monographs

- 1- Michel Séjean (dir.), Code de la Cybersécurité Annoté & commenté, 2e éd., Dalloz, Paris, 2024.
- 2- Philippe Malaurie, Laurent Aynès et Philippe Stoffel-Munck, Droit des obligations, LGDJ, Paris, 2020.
- 3- Alexandre Cruquenaire, La cybersécurité dans les contrats informatiques, Larcier, 2022.
- 4- Guillaume Harry, IAM – Gestion des identités et des accès : Protégez vos systèmes d'information, Éditions ENI, 2021.
- 5- American Law Institute, Restatement (Second) of Contracts, St. Paul, 1981.
- 6- Michael D. Green & Brooks M. Hanner, "USA", in Ken Oliphant (ed.), Aggregation and Divisibility of Damage, Springer, Vienna, 2009.



- 7- Jonathan Pouget, La réparation du dommage impliquant une intelligence artificielle, thèse de doctorat, Aix-Marseille Université, 2019.

Second: Research Articles and Peer-Reviewed Journals

- 1- Kristen E. Eichensehr, "Public-Private Cybersecurity", Texas Law Review, Vol. 95, No. 3, 2017.
- 2- Charlotte A. Tschider, "Locking Down 'Reasonable' Cybersecurity Duty", Yale Law & Policy Review, Vol. 41, No. 2, 2023.
- 3- Randy E. Barnett, "Four Senses of the Public Law-Private Law Distinction", Harvard Journal of Law & Public Policy, Vol. 9, 1986.
- 4- Hervé Jacquemin, "Contrats informatiques", Revue du Droit des Technologies de l'information, n° 35, 2009.
- 5- Dan Craigen, Nadia Diakun-Thibault, and Randy Purse, "Defining Cybersecurity", Technology Innovation Management Review, 2014.
- 6- Mohit Sharma, Sajud E., Naranjan Goklani, Krishna Chaubey, "Public-Private Partnerships in Cybersecurity: A Strategic Approach to National Threat Management", Journal of Electrical Systems, Vol. 21, No. 1, 2025.
- 7- Rachel Brandenburger & Jill Ottenberg, "Looking backwards to move forwards: The role of history in current US antitrust enforcement", Journal of Antitrust Enforcement, Vol. 11, No. 2, July 2023.
- 8- Devika Sharma, Sandeep Reddy, Hamza Shahid, "Cybersecurity Obligations for Critical Infrastructure: Emerging Legal Norms, Enforcement Gaps, and Governance Challenges", Legal Studies in Digital Age, Vol. 2, No. 3, 2023.
- 9- Arina Alexei, Anatolie Alexei, "The Difference Between Cyber Security vs Information Security", Journal of Engineering Science, Vol. XXIX, No. 4, 2022.
- 10- Cristian MACSIM, "Legal Person Subject to Civil Law", Vol. 9, Issue 1, 2021.
- 11- Mariarosaria Taddeo, "Is Cybersecurity a Public Good?", Vol. 29, 2019.
- 12- Daniel Chibuike Okoro, "An Evaluation of Cybersecurity Frameworks and Privacy Regulations for Companies in the Digital Age: A Legal Approach", American Journal of Economics and Business Administration, Vol. 25, Issue 4, 2025.
- 13- Md Nazrul Islam Khan, Md Soyeb Rabbi, "Cybercrime, Legal Accountability, and Contractual Risk: A Systematic Review of

- Jurisprudence and Protective Frameworks”, American Journal of Advanced Technology and Engineering Solutions, Vol. 4, Issue 1, 2024.
- 14- Guillaume Harry, “IAM Gestion des identités et des accès: concepts et états de l’art”, HAL, Archive Ouverte, 2013.
 - 15- Rishita Maheshwari, “The Intersection of Data Privacy and Competition Law: Analyzing Big Tech’s Market Dominance”, SSRN Working Paper No. 5214841, April 2025.
 - 16- Yasmine Budustour & Leen Budustour, “The Doctrine of Separate Legal Personality and Its Significance in International Business”, SSRN Electronic Journal, 2023.
 - 17- Philippe VITEL and Henrik BLIDDAL, “French Cyber Security and Defence: An Overview”, Vitel & Bliddal, Vol. 32, 2015.
 - 18- C. Warren Axelrod, “Using Contracts to Reduce Cybersecurity Risks”, CrossTalk, July/August 2017.
 - 19- Adejoke T. Odebade, Elhadj Benkhelifa, “A Comparative Study of National Cyber Security Strategies of Ten Nations”.
 - 20- Paweł Zając, “The Liability of Entities Providing Services by Electronic Means for Digital Content”, 2021.
 - 21- Louise Marie Hurel, “Private Authority and the Political Economy of Private Companies in Cybersecurity Crises and Conflicts”.
 - 22- California Consumer Privacy Act (CCPA) – Summary and Guidance, Jones Day, 2020.
 - 23- Olivier Iteanu, «Cybersécurité: une obligation de résultat?», disponible sur: <https://www.iteanu.law/en/cybersecurite-une-obligation-de-resultat/> .
 - 24- Jeff Kosseff, "Defining Cybersecurity Law", Iowa Law Review, Vol. 103, No. 3, 2018.
 - 25- Md Nazrul Islam Khan & Debashish Goswami, "Cybercrime and Contractual Liability: A Systematic Review of Legal Precedents and Risk Mitigation Frameworks", Journal of Sustainable Development and Policy, Vol. 1, No. 1, 2025.
 - 26- Isaac Ijuo, Chizoba Okonkwo, Chinenye Umekwe, Ajibola Yusuff & Julius Samson, "Cybersecurity Law: Individual Rights, Corporate Liability, Compliance, and Operational Resilience", ResearchGate, 2025.
 - 27- Jukka Ruohonen, "A Systematic Literature Review on the NIS2 Directive", arXiv:2412.08084, 2024.



- 28- Adebola Folorunso, Ifeoluwa Wada, Bunmi Samuel & Viqaruddin Mohammed, "Security compliance and its implication for cybersecurity", World Journal of Advanced Research and Reviews, Vol. 24, No. 1, 2024.
- 29- Rostand Gervais Tsomevou, « L'assurance du risque cyber dans la zone CIMA », Revue de l'ERSUMA, n° 16, 2022/1.
- 30- Sasha Romanosky, Lillian Ablon, Andreas Kuehn & Therese Jones, "Content Analysis of Cyber Insurance Policies: How Do Carriers Price Cyber Risk?", Journal of Cybersecurity, Vol. 5, No. 1, 2019.
- 31- Deborah L. Johnson, "Demystifying the Elusive Quest for Cyber Insurance Protection: The Need for New Contract Language", Cardozo Law Review, Vol. 44, No. 6, 2023.
- 32- Daniel Garrie & Michael Mann, "Cyber-Security Insurance: Navigating the Landscape of a Growing Field", The John Marshall Journal of Information Technology & Privacy Law, Vol. 31, No. 3, 2014.
- 33- Sébastien Héon & Didier Parsoire, « La couverture du cyber-risque », Revue d'économie financière, n° 126, 2017/2.
- 34- Shauhin A. Talesh, "Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as 'Compliance Managers' for Businesses", Law & Social Inquiry, Vol. 43, No. 2, 2018.
- 35- Daniel Woods, Ioannis Agrafiotis, Jason R. C. Nurse & Sadie Creese, "Mapping the coverage of security controls in cyber insurance proposal forms", Journal of Internet Services and Applications, Vol. 8, 2017

Third: Case Law

- 1- Supreme Court of the United States, *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997).
- 2- United States Court of Appeals for the Third Circuit, *FTC v. Wyndham Worldwide Corporation*, No. 14-3514, decided August 24, 2015.
- 3- United States Court of Appeals for the Seventh Circuit, *Remijas v. Neiman Marcus Group, LLC*, No. 14-3122, decided July 20, 2015.
- 4- United States District Court for the District of Minnesota, *In re Target Corporation Customer Data Security Breach Litigation*, MDL No. 14-2522, December 18, 2014.



- 5- United States Court of Appeals for the Eighth Circuit, In re Target Corporation Customer Data Security Breach Litigation, No. 15-3909, decided February 1, 2017.
- 6- United States Court of Appeals for the Eighth Circuit, Eyeblaster, Inc. v. Federal Insurance Co., 613 F.3d 797 (2010).
- 7- United States Court of Appeals for the Eighth Circuit, St. Paul Fire & Marine Insurance Co. v. Compaq Computer Corp., 539 F.3d 809 (2008).
- 8- United States District Court for the Central District of California, Columbia Casualty Co. v. Cottage Health System, No. 2:15-cv-03432, July 17, 2015.
- 9- United States District Court for the District of Arizona, P.F. Chang's China Bistro, Inc. v. Federal Insurance Co., No. CV-15-01322-PHX-SMM, May 26, 2016.
- 10- United States Court of Appeals for the Sixth Circuit, Home Depot, Inc. v. Steadfast Insurance Co., No. 23-3720, decided January 13, 2025.
- 11- Superior Court of New Jersey, Appellate Division, Merck & Co. v. Ace American Insurance Co., 293 A.3d 535 (2023).
- 12- Supreme Court of Texas, Ewing Construction Co. v. Amerisure Insurance Co., 420 S.W.3d 30 (2014).
- 13- Supreme Court of Texas, Texas Farmers Insurance Co. v. Soriano, 881 S.W.2d 312 (1994).
- 14- Supreme Court of the United States, State Farm Fire & Casualty Co. v. Tashire, 386 U.S. 523 (1967).
- 15- Supreme Court of the United States, Watson v. Employers Liability Assurance Corp., 348 U.S. 66 (1954).
- 16- Supreme Court of Louisiana, Gorman v. City of Opelousas, 148 So. 3d 888 (2014).
- 17- Cour de cassation, Chambre civile, 20 mai 1936, arrêt Mercier, Gazette du Palais 1936.
- 18- Cour de cassation, Chambre civile 2, 3 novembre 2011, n° de pourvoi 10-16.036.
- 19- Cour de cassation, Chambre civile 2, 12 septembre 2013, n° de pourvoi 12-24.650.
- 20- Cour de cassation, Chambre commerciale, 18 septembre 2019, n° de pourvoi 16-26.962, ECLI:FR:CCASS:2019:CO00659.
- 21- Cour de cassation, Chambre commerciale, 1er juin 2022, n° 20-19.476.



- 22- Cour d'appel de Rennes, 3e chambre commerciale, 19 novembre 2024, n° 23/04627.
- 23- Supreme Court of the United Kingdom, WM Morrison Supermarkets plc v Various Claimants [2020] UKSC 12.

Fourth: Legislation, Regulations and Official Documents

American:

- 1- Title 6 of the United States Code (6 U.S.C.), Homeland Security Act of 2002, as amended.
- 2- Sherman Antitrust Act of 1890, as amended 2004.
- 3- Clayton Antitrust Act of 1914, as amended.
- 4- California Consumer Privacy Act (CCPA), as amended 2023.
- 5- NIST Special Publication 800-145, The NIST Definition of Cloud Computing, September 2011.
- 6- NIST Special Publication 800-12 Rev. 1, An Introduction to Information Security, June 2017.
- 7- DEPARTMENT OF HOMELAND SECURITY, Cybersecurity and Infrastructure Security Agency, Federal Register, Vol. 89, No. 66, April 4, 2024.
- 8- Mississippi House of Representatives Bill No. (HB 1541) of 2014.
- 9- Federal Acquisition Regulation (FAR), 48 C.F.R. Chapter 1, including § 39.101 and § 52.204-21, as amended.
- 10- National Institute of Standards and Technology, The NIST Cybersecurity Framework (CSF) 2.0, NIST CSWP 29, February 26, 2024.
- 11- Louisiana Revised Statutes, La. R.S. 22:1269 (Direct Action Statute), as amended 2024.
- 12- Federal Bureau of Investigation, Internet Crime Complaint Center (IC3), Internet Crime Report 2024.
- 13- NAIC Staff, Report on the Cybersecurity Insurance Market, Memorandum to the Property and Casualty Insurance (C) Committee, November 3, 2023.

French:

- 1- Décret n° 2015-350 du 27 mars 2015 relatif à la qualification des prestataires de services de confiance pour la sécurité des systèmes d'information.
- 2- Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN), telle que modifiée.



- 3- Code de commerce français.
- 4- Loi n° 96-659 du 26 juillet 1996 de réglementation des télécommunications.
- 5- Code civil, tel que modifié notamment par l'ordonnance n° 2016-131 du 10 février 2016.
- 6- Code des assurances, tel que modifié notamment par la loi n° 2023-22 du 24 janvier 2023.
- 7- Arrêté du 18 septembre 2018 portant approbation du cahier des clauses simplifiées de cybersécurité, JORF n° 0223 du 27 septembre 2018.
- 8- ANSSI, Référentiel d'exigences applicables aux prestataires de service de confiance qualifiés, version 2.0, 2015.
- 9- Franck Riester, Rapport fait au nom de la Commission des affaires économiques, de l'environnement et du territoire sur le projet de loi portant diverses dispositions d'adaptation au droit communautaire dans les domaines économique et financier, Assemblée nationale, n° 406, 13 novembre 2007.
- 10- GIP ACYMA (Cybermalveillance.gouv.fr), Label ExpertCyber : Recueil des critères d'évaluation des candidatures, version 3.1, novembre 2025.

European:

- 1- Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 (NIS2 Directive).
- 2- Règlement (UE) 2016/679 du Parlement européen et du Conseil (RGPD).

Fifth: Electronic Websites

- 1- The website of the U.S. National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, 2018, available at: NIST Cybersecurity Framework. (https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11-arabic-translation?utm_source=).
- 2- The official website of the French National Institute of Statistics and Economic Studies (INSEE), available at: INSEE Official Website. (https://www.insee.fr/fr/metadonnees/definition/c1251?utm_source=).
- 3- The official website of the U.S. Federal Trade Commission (FTC), available at: FTC Antitrust Laws Guide. (https://www.ftc.gov/advice-guidance/competition-guidance/guide-antitrust-laws/antitrust-laws?utm_source=).



- 4- Cybermalveillance.gouv.fr, Label ExpertCyber et prestataires de cybersécurité, available at: <https://www.cybermalveillance.gouv.fr/tous-nos-contenus/label-expertcyber/questions-reponses-faq>
- 5- ANSSI, « ANSSI – A driving force of the European Public-Private Partnership on cybersecurity », 3 août 2016.
- 6- Autorité de la concurrence, Missions: Enforcing competition rules – Combating cartels and abuses of dominant position, available at: <https://www.autoritedelaconcurrence.fr/en/missions>
- 7- Booz Allen Hamilton, "Booz Allen to help US Cyber Command boost cybersecurity", July 13, 2016, available at: <https://www.boozallen.com/e/media/press-release/booz-allen-to-help-us-cyber-command-boost-cyber-security.html>
- 8- DataGuard, "What is the Difference Between IT and Cyber Security?", 2023, available at: <https://www.dataguard.com/blog/what-is-the-difference-between-it-and-cyber-security>
- 9- SANS Institute, Information Security Resources, available at: <https://www.sans.org/information-security>
- 10- Kinza Yasar, "What is information technology (IT)?", TechTarget, May 9, 2024, available at: <https://www.techtarget.com/searchdatacenter/definition/IT>
- 11- Katherine J. Henry, "Exploring Nevada's Defense Within Limits Laws", Bradley Arant Boult Cummings LLP, January 15, 2025, available at: <https://www.bradley.com/insights/publications/2025/01/exploring-nevadas-defense-within-limits-laws>
- 12- Microsoft, "Helping our customers through the CrowdStrike outage", Official Microsoft Blog, July 20, 2024, available at: <https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/>



- 13- Cornell Law School, Legal Information Institute, "Breach of Contract", available at: https://www.law.cornell.edu/wex/breach_of_contract
- 14- Cornell Law School, Legal Information Institute, "Duty of Care", available at: https://www.law.cornell.edu/wex/duty_of_care
- 15- Cornell Law School, Legal Information Institute, "Fiduciary Duty", available at: https://www.law.cornell.edu/wex/fiduciary_duty
- 16- Cornell Law School, Legal Information Institute, "Negligence", available at: <https://www.law.cornell.edu/wex/negligence>
- 17- Cornell Law School, Legal Information Institute, "Piercing the Corporate Veil", available at: https://www.law.cornell.edu/wex/piercing_the_corporate_vei

Abstract

Cybersecurity companies possess a legal nature that does not readily conform to the conventional models recognized in private law. Although they take the form of private commercial entities, their activities relate to the protection of national digital security, a function historically monopolized by the state. This gives their activities a quasi-public character that bears upon the nature of their obligations and the standards applicable to their civil liability. This issue has become increasingly significant in light of the rapid expansion of reliance on digital systems in governmental, commercial, and banking transactions, as these companies have become key actors within the digital security ecosystem whose legal role cannot be overlooked. Nevertheless, specific civil-law regulation governing their liability remains absent in most comparative legal systems, particularly under Iraqi law, which continues to subject such disputes to the general rules of civil liability, despite the limitations of those rules in accommodating the distinctive nature of this activity.

This research examines a number of interrelated legal issues in this context. First, it addresses the legal characterization of these companies, the requirements for establishing their legal status, and the characteristics that distinguish them from other technical service providers. Second, it examines the legal foundations of their obligations, whether primary obligations relating to the protection of systems and data or secondary obligations relating to disclosure and regulatory compliance. Third, it considers the distinction between an obligation of means and an obligation of result, and the direct consequences of this distinction for the standard of fault, the burden of proof, and the scope of compensation in relation to clients, third parties, and regulatory authorities alike. Ultimately, the research identifies legislative gaps in Iraqi civil law and proposes legislative solutions informed by comparative experience and adapted to the particularities of the Iraqi legal system and the requirements of the evolving digital environme

Republic of Iraq
The Ministry of Higher Education
and scientific research
Al- Qadisiya University
Collage of Law



Civil Liability of Cybersecurity Companies (A Comparative Study)

A thesis submitted by the student

Ahmed Shaker Abdul

To the Council of the College of Law - Al-Qadisiyah University
As part of the requirements for obtaining a Master's degree in
Private Law

Supervised by

Assist. Prof. Dr. Safaa Mutab Al-Khuzai

2026 AD

1448 AH

