AL-NAHRAIN UNIVERSITY
COLLEGE OF LAW
ISSN:3006- 0605 DOI:10.58255

دور المسؤولية المدنية في الحد من الهجمات الإلكترونية (دراسة مقارنة)

The Role of Civil Liability in Reducing Cyber Attacks (A Comparative Study)

أ. م. د. دلال تفكير مراد
كلية القانون – جامعة الكوفة
Assist. Prof. Dr. Dalal Tafkeer Murad
College of Law, University of Kufa
dalalt.alardhi@uokufa.edu.iq

م.م رغد عبد مسلم عبيد الحسناوي
Assist. Lecturer. Raghad Abd Muslim
كلية القانون – جامعة الكوفة
College of Law, University of Kufa
raghada.alhasnawi@student.uokufa.edu.iq

المستخلص في عصر التكنولوجيا الرقمية الذي نعيشه اليوم, تشكل الهجمات الإلكترونية تهديداً متزايداً للأفراد والشركات بل وحتى الحكومات. إذ أن هذه الهجمات اتخذت أشكالاً متعددة, مثل سرقة البيانات, والاختراقات الأمنية, والبرمجيات الخبيثة, والاحتيال الإلكتروني , مما يسبب خسائر مادية ومعنوية جسيمة . وفي هذه السياق, فأن لقواعد المسؤولية المدنية دورًا محوريًا في الحد من هذه الهجمات من خلال توفير إطار قانوني يحمي الحقوق ويحدد المسؤوليات ويعاقب المخالفين فتعد بذلك أداة أساسية لتنظيم العلاقات بين الأفراد والكيانات في الفضاء الالكتروني , حيث تحدد القواعد التي تحكم التعاملات الرقمية وتضمن حماية الخصوصية وسرية البيانات. من خلال نصوص قانونية واضحة, يمكن لقواعد المسؤولية المدنية أن تفرض جزاءات مدنية رادعة على مرتكبي الهجمات الإلكترونية, مما يساهم في ردع المسؤولين عن هذه الهجمات . بالإضافة الى التعويض عن الأضرار التي تلحق بالمتضررين, مما يعزز الثقة في البيئة الرقمية . وباختصار, تعد قواعد المسؤولية المدنية ركيزة أساسية في مكافحة الهجمات الإلكترونية, حيث تعمل على تحقيق التوازن بين التطور التكنولوجي وحماية الحقوق الفردية والجماعية . ومن خلال تطويرها وتحديثها باستمرار لمواكبة التحديات الجديدة, لتكون قواعد المسؤولية المدنية درعًا واقيًا في مواجهة الهجمات الإلكترونية المتزايدة.

الكلمات المفتاحية: الهجمات الإلكترونية , الذكاء الأصطناعي , المسؤولية المدنية , طبيعة المسؤولية , التعويض

Abstract In the digital technology era we live in today, cyberattacks have become an increasing threat to individuals, businesses, and even governments. These attacks take various forms, such as data theft, security breaches, malware, and electronic fraud,

causing significant material and moral losses. In this context, civil liability rules play a pivotal role in mitigating these attacks by providing a legal framework that safeguards rights, defines responsibilities, and penalizes violators. Thus, they serve as an essential tool for regulating relationships between individuals and entities in cyberspace, establishing rules that govern digital interactions and ensuring the protection of privacy and data confidentiality. Through clear legal provisions, civil liability rules can impose deterrent civil penalties on perpetrators of cyberattacks, contributing to the deterrence of those responsible for such attacks. Additionally, they provide compensation for damages suffered by victims, thereby enhancing trust in the digital environment. In summary, civil liability rules are a fundamental pillar in combating cyberattacks, as they strive to balance technological advancement with the protection of individual and collective rights. By continuously developing and updating these rules to keep pace with new challenges, civil liability can serve as a protective shield against the growing threat of cyberattacks.
Keywords:
(cyberattacks, artificial intelligence, civil liability, nature of liability, compensation)

المقدمة

أولاً: جوهر فكرة البحث رغم التقدم الحاصل في التشريعات المدنية ، لا تزال قواعد المسؤولية المدنية تعاني من قصور في مواجهة الهجمات الإلكترونية , والتي ظهرت بسبب التطور التكنولوجي السريع والصعوبة في تحديد المسؤولية المدنية . ويهدف هذا البحث الى تعزيز فعالية قواعد المسؤولية المدنية من خلال تحسين التشريعات النافذة ، وحثها على تطبيق جزاءات رادعة، وضمان تعويض المتضررين ، مع اقتراح آليات حديثة لمواكبة التحديات الرقمية الحديثة.

ثانياً: أهمية البحث يُعد هذا الموضوع بالغ الأهمية حيث يُقدِّم إطارًا قانونيًا يُسهم في حماية الأفراد والمؤسسات من الهجمات الإلكترونية المتصاعدة، كما يعمل على تعزيز الثقة في الفضاء الرقمي عبر تحديد المسؤوليات وضمان حقوق المتضررين من خلال التعويضات المناسبة.

ثالثاً: مشكلة البحث على الرغم من التطورات التشريعية في العديد من الدول لمواجهة الهجمات الإلكترونية , لا يزال هناك قصور في فعالية قواعد المسؤولية المدنية في الحد من هذه الهجمات بشكل كامل .يتمثل هذا القصور في عدة جوانب , منها عدم مواكبة التشريعات للتطورات التكنولوجية السريعة, وصعوبة تحديد المسؤولية القانونية في البيئة الرقمية المعقدة , بالإضافة الى التحديات المتعلقة بتنفيذ القوانين عبر الحدود الدولية .إذا تكمن المشكلة البحثة في التساؤل الرئيسي التالي : كيف لقواعد المسؤولية المدنية أن تكون أكثر فعالية للحد من الهجمات الإلكترونية . مع الأخذ في الاعتبار التحديات التشريعية والفنية المتعلقة بالبيئة الرقمية ؟

رابعاً: منهجية البحث اتخذ البحث المنهج التحليلي وذلك بتحليل النصوص القانونية وتفسيرها وتوضيحها ، والمنهج المقارن حيث سيتم المقارنة بين القانون المدني العراقي والقانون المدني المصري من بين القوانين العربية والقانون المدني الفرنسي من بين القوانين الغربية ، مع التطرق الى بعض القوانين التي عالجت موضوع البحث بقدر تعلقه بالدراسة .

خامسا: خطة البحث تم تنظيم هذه الدراسة على شكل مقدمة ومبحثين , المبحث الاول مفهوم الهجمات الإلكترونية ودور الذكاء الاصطناعي منها .اما في المبحث الثاني فسنتطرق فيه الى مدى كفاية قواعد المسؤولية المدنية للحد من الهجمات الإلكترونية .وبالنسبة للخاتمة فقد تضمن البحث عدة استنتاجات ومقترحات لتعزيز الإطار التشريعي الخاص بمواجهة الهجمات الإلكترونية .

المبحث الاول

مفهوم الهجمات الإلكترونية ودور الذكاء الاصطناعي فيها

تُعد الهجمات الإلكترونية من التحديات الحديثة التي تواجه الأفراد والحكومات والشركات على حد سواء، حيث أصبحت أداة يستخدمها المهاجمون لاستهداف الدول والمؤسسات والأشخاص. يؤدي اللجوء إلى هذه الهجمات إلى إلحاق خسائر كبيرة، سواء كانت مادية أو تقنية، مما يعطل الأعمال ويؤثر سلبًا على العمليات التكنولوجية والمعلوماتية. وقد تتسبب هذه الهجمات في أضرار كارثية للأصول الملموسة، مثل المعدات والمنشآت، مما يجعلها تهديدًا رئيسيًا في العصر الرقمي.

ومع تطور التكنولوجيا، خاصة في مجال الذكاء الاصطناعي، أصبحت الهجمات الإلكترونية أكثر تعقيدًا وخطورة. فالمهاجمون يستخدمون تقنيات متقدمة، مثل الذكاء الاصطناعي، لتنفيذ هجمات يصعب اكتشافها، كالهجمات التلقائية وهجمات التصيد الإلكتروني المدعومة بالذكاء الاصطناعي. هذه التطورات تزيد من سرعة وتكرار الهجمات، كما تجعل من الصعب تحديد هوية المهاجمين بسبب استخدامهم تقنيات متطورة لإخفاء هوياتهم. وان نقص الخبرة التقنية وعدم وجود تشريعات متخصصة في بعض الدول، مثل العراق، يزيد من صعوبة مواجهة هذه الهجمات. لذلك، أصبح من الضروري تعزيز الأمن الإلكتروني واعتماد إجراءات قوية لإدارة المخاطر في ظل التهديدات المتزايدة. ومما تقدم سنناقش ماهية الهجمات الإلكترونية ودور الذكاء الاصطناعي فيها في مطلبين : الأول نبحث فيه التعريف بالهجمات الإلكترونية , أما في المطلب الثاني نحدد دور الذكاء الاصطناعي فيها وعلى النحو التالي:

المطلب الاول

التعريف بالهجمات الإلكترونية

تُعد الهجمات الإلكترونية من أخطر التهديدات في العصر الرقمي، حيث تستهدف الأفراد والشركات عبر وسائل تقنية متطورة. تتنوع هذه الهجمات من حيث أساليبها وأهدافها، مما يستدعي فهمها بشكل دقيق , كونها تتسبب في أضرار كبيره. وفيما يلي سنتعرف على مفهوم الهجمات الإلكترونية وأنواعها الرئيسية. سنتناول في هذا المطلب تعريف الهجمات الإلكترونية وأبرز أنواعها على النحو التالي :

الفرع الاول

تعريف الهجمات الإلكترونية

يُعتبر مصطلح "الهجمات الإلكترونية " مفهومًا حديثًا ارتبط ظهوره بالتطور التكنولوجي الذي شهدته البشرية، وزيادة اعتماد الإنسان على وسائل التكنولوجيا والاتصال. يُطلق على هذا المجال اسم "الفضاء الإلكتروني" أو "السيبراني"،

وهو بيئة افتراضية تشمل أنظمة الكمبيوتر وشبكات الإنترنت. حيث ظهر هذا المصطلح في الثمانينات من القرن الماضي، وتختلف تعريفاته باختلاف الدول ومدى ارتباطها بالعالم الرقمي واستخدامها لتقنيات المعلومات، مثل الحكومات الإلكترونية وشبكات الاتصال السلكية واللاسلكية[١] ,وأن مسألة تعريف الهجمات الإلكترونية (الهجمات السيبرانية) من المسائل المعقدة التي لم يصل الى حد الآن تعريف شامل ومحدد لا فقهاً ولا قانوناً ويعود هذا التعقيد الى اختلاف طبيعة الهجمات وانواع الهجمات المستخدمة ,بالإضافة إلى تباين الادوار والمواقف في مواجهتها, لذا عرف جانب من الفقه الهجمات الإلكترونية (الهجمات السيبرانية) هي "تلك الهجمات التي تشن على الحاسوب والشبكات الإلكترونية بمختلف أنواعها بهدف إلحاق الضرر بها أو سرقة المعلومات الموجودة عليها لأغراض مختلفة شخصية أو اقتصادية أو سياسية"[٢] .

وعرفها آخرون بأنها "عبارة عن هجوم يتم شنه من أحد أجهزة الكمبيوتر أو مجموعة من الأجهزة على كمبيوتر آخر أو عدة أجهزة كمبيوتر أو شبكات" [٣] . وعرفته الوكالة الفرنسية بأنه " فضاء لأمن من أنظمة الإعلام التواصل المشكل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية" وعرفه المعهد الوطني للمعايير والتقنية (NIST) بأنه بيئة معلوماتية عالمية تتكون من بنية تحتية متكاملة لأنظمة المعلومات , تشمل شبكات الإنترنيت , وشبكات الاتصالات, وأنظمة الحواسيب ,بالإضافة إلى المعالجات وأجهزة التحكم المدمجة[٤].وبهذا فأن القوانين الفرنسية تهدف الى تعزيز الأمن السيبراني في فرنسا فيما يخص هذه الهجمات من خلال قانون الأمن السيبراني في فرنسا رقم (١١٦٨_٢٠١٣) في نص مادة (٢٢)وتنص "تفرض على مشغلي الخدمات الحيوية (مثل الطاقة والاتصالات) بتعزيز امنهم السيبراني "والمادة (٢٣) " تسمح للحكومة الفرنسية بمراقبة الشبكات لمواجهة التهديدات الإلكترونية "[٥] . أما تعريف الهجمات الإلكترونية، فهي عمليات استغلال لثغرات في أنظمة الكمبيوتر والشبكات، باستخدام برمجيات ضارة تهدف إلى التلاعب بالأنظمة أو سرقة البيانات. تُعد هذه الهجمات تهديدًا كبيرًا في ظل الاعتماد المتزايد على التكنولوجيا[٦]. ومما سبق يمكن الاستنتاج أن التطور التكنولوجي المتسارع وزيادة الاعتماد على استخدام الانترنيت بشكل يومي قد جعل الفضاء الإلكتروني بيئة خصبة للتهديدات الخطيرة مثل الهجمات الإلكترونية أو السيبرانية. فقد أصبحت هذه الهجمات كالبرامج الضارة والتصيد الإلكتروني وغيرها من الاساليب الخبيثة , تشكل خطرًا متزايد على الإفراد والشركات. ويمكن لنا تعريف الهجمات الإلكترونية من الناحية

---

[١]) سامي محمد بونيف , دور الاستراتيجيات الاستباقية في مواجهة الهجمات السيبرانية _ الّردع السيبراني نموذجا , المجلة الجزائرية للحقوق والعلوم السياسية , معهد العلوم القانونية والإدارية , المجلد (٤) , العدد (٧), سنة ٢٠١٩, ص ١٢٣.

[٢]) د. علاء عبد الرزاق محمد السالمي, المدخل الى لأمن السيبراني , الذاكرة للنشر والتوزيع , ط١, بغداد, ٢٠٢٣, ص ١١٨ .

[٣]) عصام السيد , الأمن السيبراني , المركز الأكاديمي للنشر ومكتبة الدراسات العربية للنشر والتوزيع , ٢٠٢٤, ص ٩٢.

[٤]) د. السعيد عبد الحميد إبراهيم , الأمن السيبراني في عالم الميتافيرس الافتراضي , دار العلم والإيمان للنشر والتوزيع , ط١,جمهورية مصر العربية , ٢٠٢٥, ص ١٦و١٧.

[٥]) المادة (٢٢_٢٣) من قانون الأمن السيبراني الفرنسي رقم (١١٦٨_٢٠١٣) .

[٦]) سامي محمد بونيف , مصدر سابق , ص ١٢٤.

المدنية بأنها " فعل غير مشروع يهدف إلى إلحاق ضرر بالغير باستخدام الوسائل التكنولوجية أو الأنظمة المعلوماتية مثل "أجهزة الكمبيوتر والشبكات أو الإنترنيت" والتي تسبب ضرراً للأفراد أو المؤسسات أو الشركات , وتشمل هذه الهجمات أفعالاً مثل "البرمجيات الخبيثة وهجمات حجب الخدمة, وسرقة البيانات " وتخضع هذه الهجمات لأحكام المسؤولية المدنية ويحق للمتضررين المطالبة بالتعويض .

الفرع الثاني

أنواع الهجمات الإلكترونية

مع تزايد الاعتماد على التكنولوجيا ,أصبحت الهجمات الإلكترونية خطرًا يهدد الجميع حيث تعد هذه الهجمات بمثابة استغلال غير مشروع للتكنولوجيا والتي تتنوع بين سرقة المعلومات وتعطيل الأنظمة أو اختراق الخصوصية . وفي هذا السياق نستعرض أبرز أنواع الهجمات الإلكترونية ,وكيفية تأثيرها على الفضاء الرقمي ومنها :

اولا : الهجمات الإلكترونية التي تستهدف الافراد

تُعَد الهجمات الإلكترونية التي تستهدف الأفراد أفعالًا ضارة تُنفَّذ باستخدام الوسائل التكنولوجية، مثل الإنترنت أو الأجهزة الذكية بهدف إلحاق الضرر بفرد معين. تؤدي هذه الهجمات إلى إتلاف المستندات والأنظمة المهمة أو التحكم فيها أو الوصول إليها من خلال اختراق شبكات الكمبيوتر الشخصية. غالبًا ما يتم تنفيذ هذه الهجمات من قبل أفراد أو مجموعات لأغراض شخصية، اقتصادية، أو حتى تدمير المعلومات السرية.

من بين هذه الهجمات، تُستخدَم البرامج الضارة (Malware) التي تتنكر في صورة مرفقات بريد إلكتروني موثوق به أو ملفات مشفرة، مثل الفيروسات وأحصنة طروادة وبرامج التجسس. هذه البرامج تسمح للمهاجمين بالدخول إلى شبكات الكمبيوتر، مما قد يؤدي إلى تعطيل أنظمة تكنولوجيا المعلومات بالكامل[١] .

كما تشمل الهجمات الإلكترونية هجمات حجب الخدمة (DDoS)، التي تستهدف عدة أنظمة كمبيوتر لتعطيل موقع أو شبكة معينة، مما يحجب تجربة المستخدم. على سبيل المثال، يمكن أن تؤدي مئات النوافذ المنبثقة أو الإعلانات المزعجة إلى إرباك المستخدمين وتعطيل الخدمات.

أيضًا، تُعتبر هجمات التصيد الاحتيالي (Phishing) من أكثر الهجمات شيوعًا، حيث يقوم المهاجمون بإرسال رسائل بريد إلكتروني مزيفة تبدو كما لو أنها صادرة من جهات موثوقة، بهدف خداع الضحايا للكشف عن بياناتهم الشخصية أو المالية[١] .

---

[١]) . د. محمد حسن السامرائي , دور القانون الدولي في مكافحة الهجمات السيبرانية , الذاكرة للنشر والتوزيع , بغداد , ٢٠٢٣, ص ٥١. وما المقصود بالهجوم عبر الإنترنيت , مقال , متاح عبرالموقع الإلكتروني , https://www.microsoft.com/ar/security/business/security-101/what-is-a-cyberattack#:~:text=%D8%A7%Dn , تمت الزيارة في ٢٠٢٥/٣/٥ ,الساعة الرابعة عصراً.

بشكل عام، تُعَد الهجمات الإلكترونية التي تستهدف الافراد من أخطر التهديدات في العصر الرقمي، حيث يستغل المهاجمون نقاط الضعف التقنية والنفسية للأفراد لتحقيق أهدافهم غير المشروعة. و يعتمد المهاجمون على أساليب متطورة، مثل التصيد الاحتيالي أو البرامج الضارة، لاستهداف الضحايا بشكل مباشر، مما يجعل هذه الهجمات تهديدًا مستمرًا يتطلب وعيًا أكبر وتدابير أمنية متقدمة للحماية منها.

ثانيا : الهجمات الإلكترونية التي تستهدف الشركات أدى التطور السريع للإنترنت إلى زيادة انتشار الهجمات الإلكترونية التي تستهدف الشركات، حيث تُعَد البرامج الضارة أحد أخطر التهديدات. تستهدف هذه الهجمات البيانات السرية والمعلومات الحساسة للشركات، مما يتسبب في أضرار جسيمة لأنظمتها وشبكاتها. تنتشر البرامج الضارة بسرعة ولا يمكن اكتشافها بسهولة، مما يجعلها تهديدًا كبيرًا للبنية التحتية الرقمية للشركات. يمكن أن تؤدي هذه الهجمات إلى تعطيل العمليات التجارية أو حتى شللها بالكامل. لذلك، أصبحت الحاجة ملحة إلى تطوير أنظمة أمنية متقدمة تعتمد على التعاون بين الدول لاكتشاف البرامج الضارة والتحكم فيها في بيئات الشبكات واسعة النطاق[٢] . والهجمات الإلكترونية التي تستهدف الشركات يمكن أن تستمر لأشهر أو سنوات، حيث يستغل المهاجمون نقاط الضعف في أنظمة الشركات للوصول إلى البيانات الحساسة واستغلالها لأغراض الربح أو التخريب. تؤدي هذه الهجمات إلى خسائر مالية كبيرة، فقدان البيانات، وتضرر سمعة الشركة. مع تزايد تعقيد البيئة الرقمية، أصبحت التهديدات الأمنية أكثر خطورة[٣]، وبهذا يجب على الشركات تعزيز إجراءات الأمان، تدريب الموظفين، وتبني استراتيجيات شاملة لحماية البيانات في الوقت الفعلي.

وفي الأعمال التجارية، غالبًا ما يمتلك المديرون التنفيذيون تصورًا محدودًا لمخاطر الهجمات الإلكترونية، حيث يركزون على التهديدات التقنية المعقدة مثل البرامج الضارة، ويتجاهلون الأخطاء البشرية التي تُعد السبب الرئيسي للأختراقات. يُعزى هذا الإهمال إلى عوامل نفسية مثل الوهم بالسيطرة، مما يدفعهم للاعتقاد بأن التقنيات المتقدمة توفر حماية كاملة. ومع ذلك، فإن أفعالًا بسيطة مثل سوء إدارة كلمات المرور، فتح رسائل بريد إلكتروني مشبوهة، أو إهمال تحديث الأنظمة، تمهد الطريق للهجمات الإلكترونية. ومن الأخطاء الشائعة التي تسهل هذه الهجمات: النقر على روابط ضارة، استخدام كلمات مرور ضعيفة أو مشتركة، مشاركة المعلومات الحساسة بشكل غير آمن، وإهمال

---

[١]) ما معنى الهجمات الالكترونية واشهر الهجمات السيبرانية؟ , مقال , متاح عبر الموقع الإلكتروني ,https://www.it-pillars.com/ar/blog-ar/%D9%85%D8%B9%تمت الزيارة في ٢٠٢٥/٣/٥, الساعة الرابعة ونصف عصراً. د. محمد حسن السامرائي , مصدر سابق , ص ٥١.

[2]) A Study on the Application of Distributed System Technology-Guided Machine Learning in Malware Detection Shi Jin, Zhaofeng Guo, Dongli Liu, YanhuaYangFirstpublished:23February2022,https://doi.org/10.1155/2022/4977898, Academic Editor: Akshi Kumar, This article is part of Special Issue: Advances in Computational Intelligence Techniques for Next Generation Internet of Things.

[3]) pratiques pour réduire les risques cyber menaçant les données , Anthony Seifert (chroniqueur), publié le 14 Avril 2023 .

تحديث البرامج والأنظمة، مما يترك ثغرات أمنية معروفة. بالإضافة إلى ذلك، يمكن أن يؤدي استخدام أجهزة محركات الأقراص (USB) غير آمنة أو غير معروفة المصدر إلى إدخال برامج ضارة أو فقدان بيانات حساسة. لذلك، يجب على الموظفين توخي الحذر واتباع أفضل الممارسات الأمنية لتقليل هذه المخاطر[١] .

ومما تقدم يجب على الشركات التعامل مع الهجمات الإلكترونية كأزمات شاملة، حيث تؤثر على الجوانب التقنية والمالية والقانونية وعلى سمعة الشركة .مما يتطلب ذلك بوجود إدارة من قبل الأشخاص المسؤولين لتقليل من الهجمات والتأثيرات وضمان العمل بنشاط وبسرعة وأمان. وبهذا ينبغي وضع خطط استجابة للأزمات تشمل نقاطًا أساسية مثل تحديد الأدوار والتواصل الفعّال وتقييم الأضرار. كما يجب تعزيز الأمن الإلكتروني عبر استراتيجيات متقدمة وتدريب الموظفين لتقليل تكرار الهجمات.

المطلب الثاني

دور الذكاء الاصطناعي في الهجمات الإلكترونية

يلعب الذكاء الاصطناعي دورًا في تعزيز الهجمات الإلكترونية؛ فمن ناحية، يُستخدم لتطوير برامج ضارة أكثر ذكاءً وقدرة على التكيف ، مثل الهجمات التلقائية والتصيد الذكي، مما يزيد من تعقيد التهديدات. ومن ناحية أخرى، يمكن أن يكون الذكاء الاصطناعي أداة فعالة في مكافحة هذه الهجمات عبر تحليل البيانات الضخمة وتوقع التهديدات قبل حدوثها. ومع ذلك، فإن الاستخدام السلبي لتطبيقات الذكاء الاصطناعي في تعزيز الهجمات يظل تحديًا كبيرًا يتطلب مواجهته بأساليب أكثر تطورًا. نتناول في هذا المطلب تعريف تطبيقات الذكاء الاصطناعي ودورها في تعزيز الهجمات الإلكترونية على النحو التالي:

الفرع الاول

تعريف تطبيقات الذكاء الاصطناعي

الذكاء الاصطناعي هو واحد من أكثر التقنيات التحويلية في العصر الحديث, كما أنه يعتبر من أسرع التكنولوجيات تطورًا ونموًا عند تطبيقه[٢] , وتعد تطبيقات الذكاء الاصطناعي هي المجال التي يهدف إلى تطوير أنظمة كمبيوتر قادرة على أداء مهام بشكل أفضل من البشر مثل التعلم، التفكير المنطقي، واتخاذ القرارات. وتعرف بأنها "مجموعة من التقنيات التي تحاكي العقل البشري من خلال الخوارزميات التي تعالج مشكلات معقدة" [٣]. كما عرف الأمر التنفيذي رقم (١٣٨٥٩) لسنة ٢٠١٩مصطلح "البيانات المفتوحة" هي بيانات متاحة للجمهور ومنظمة بطريقة تسمح باكتشافها واستخدامها بالكامل من قبل المستخدمين النهائيين. أما الذكاء الاصطناعي، فيُعرف بأنه برمجيات أو أجهزة

---

[1]) Réduire le risque d'erreur humaine pour améliorer la protection cyber de l'entreprise : un impératif , Dossier | Publié le 16 octobre 2024 | Mis à jour le 26 décembre 2024 .

[٢]) ماهو الذكاء الاصطناعي , مقال , متاح عبر الموقع الإلكتروني , https://www.sap.com/mena-ar/products/artificial-intelligence/what-is-artificial , تمت الزيارة في ٢٠٢٥/٣/٦, الساعة الثالثة ظهراً.

[٣]) محمد دحماني, الذكاء الاصطناعي كألية لتعزيز الامن السيبراني , جامعة عمار ثليجي _الأغواط , بحث , مجلة الفكر القانوني والسياسي , المجلد السابع ,العدد الثاني , ٢٠٢٣,ص ٦٠٠.

صممها البشر لتقوم بمهام معقدة في العالم الرقمي من خلال إدراك البيئة وجمع المعلومات وتفسير البيانات. تعتمد هذه الأنظمة على تحليل المعطيات واتخاذ أفضل الإجراءات لتحقيق أهداف محددة، باستخدام قواعد رمزية أو نماذج تعلم آلي، مع القدرة على التكيف مع التغيرات البيئية بناءً على التجارب السابقة[١] . ومما تقدم يتم استخدام الذكاء الاصطناعي في مجالات متنوعة، مثل العسكرية، الصناعية، المالية، والتعليم، حيث يُسهم في تحسين الكفاءة واتخاذ القرارات بناءً على تحليل كميات كبيرة من البيانات. رغم اختلاف وجهات النظر حول قدرته للوصول لمستوى الذكاء البشري، إلا أن الذكاء الاصطناعي أصبح جزءًا أساسيًا من حياتنا اليومية.

وبهذا يستغل المهاجمون الذكاء الاصطناعي لتنفيذ هجمات إلكترونية متطورة، مما يمكنهم من تطوير أساليب أكثر تعقيدًا وخطورة. على سبيل المثال، يتم استخدام الذكاء الاصطناعي لإنشاء هجمات تلقائية (Automated Attacks) يمكنها التكيف مع أنظمة الحماية وتجنب الاكتشاف، بالإضافة إلى هجمات التصيد الذكي (Smart Phishing) التي تستهدف الأشخاص بشكل خاص وباستخدام رسائل مخصصة تبدو موثوقة. ومن خلال هذه التقنيات، يتم اختراق أجهزة الكمبيوتر والبنى التحتية لتكنولوجيا المعلومات، مثل شبكات الأمن أو الأنظمة الشخصية والعامة للافراد أو الشركات ، بهدف تخريبها أو تدميرها. يتم ذلك عبر خطط مدروسة بعناية، تشمل استخدام برامج ضارة متطورة (Malware)، خروقات للبريد الإلكتروني، وسرقة المعلومات الحساسة. وهذه الهجمات لا تقتصر على الأضرار التقنية فحسب، بل تمتد إلى التأثيرات المالية والقانونية والسمعية، مما يعرض الأفراد والشركات وحتى الحكومات لخسائر جسيمة. كما أن المهاجمين يعتمدون على تقنيات متقدمة، مثل التعلم الآلي (Machine Learning) وتحليل البيانات الضخمة، لتحسين هجماتهم وجعلها أكثر فعالية[٢] .

لذلك، أصبح من الضروري تعزيز الحماية من هذه التهديدات المتطورة عبر إجراءات أمنية شاملة. تشمل هذه الإجراءات تحديث البرامج والأنظمة بانتظام لسد الثغرات الأمنية، استخدام كلمات مرور قوية ومعقدة، تنفيذ أنظمة كشف التسلل (Intrusion Detection Systems)، وتثقيف المستخدمين حول أفضل الممارسات الأمنية لتقليل احتمالية الوقوع ضحية لهذه الهجمات. وباختصار، يُمثل استخدام الذكاء الاصطناعي في الهجمات الإلكترونية تحديًا كبيرًا يتطلب استجابة متكاملة تجمع بين التقنيات المتقدمة والوعي الأمني لضمان الحماية الفعّالة.

الفرع الثاني

دور الذكاء الاصطناعي في تعزيز الهجمات الإلكترونية

تستخدم تطبيقات الذكاء الاصطناعي لتعزيز الهجمات الإلكترونية من خلال تطوير برامج ضارة ذكية قادرة على التكيف مع أنظمة الحماية وتجنب الاكتشاف. على سبيل المثال، يتم استخدامه في هجمات رفض الخدمة (DDoS) التي تثقل كاهل الأنظمة بطلبات تفوق طاقتها، مما يؤدي إلى تعطيلها. كما يُستخدَم الذكاء الاصطناعي لإنشاء

[١]) د. محمد فتحي محمد إبراهيم , التنظيم التشريعي لتطبيقات الذكاء الاصطناعي , مركز المحمود لتوزيع الكتب القانونية , القاهرة– جمهورية مصر العربية , طبعة٢٠٢٤, ص ٢٥.

[٢]) محمد دحماني , مصدر سابق , ص ٦٠٢و٦٠٣.

برامج ضارة متطورة، مثل أحصنة طروادة، التي تتسلل إلى الأنظمة لتسجيل كلمات المرور أو التجسس على المستخدمين. بالإضافة إلى ذلك، يمكن للذكاء الاصطناعي تحليل بروتوكولات الاتصال واستغلال نقاط الضعف في أنظمة التشغيل لتنفيذ هجمات أكثر تعقيدًا[١]. بالإضافة الى ذلك يستخدم المهاجمون هجوم الوسيط (Man-in-the-Middle)، وهو نوع من الهجمات يُعرف أيضًا بالتنصت، حيث يتدخل المهاجم في عملية التواصل بين طرفين. خلال هذا الهجوم، يتم اعتراض البيانات المتبادلة بين الطرفين، مما يسمح للمهاجم بالتلاعب بالمعلومات أو سرقتها دون أن يلاحظ الأشخاص أي شيء. يُعتبر هذا النوع من الهجمات خطيرًا لأنه يمكن استخدامه لسرقة المعلومات الحساسة، مثل كلمات المرور أو البيانات المالية، مما يتطلب اتخاذ إجراءات أمنية قوية مثل تشفير الاتصالات لمواجهته[٢] . وكذلك يتم استخدام تطبيقات الذكاء الاصطناعي بشكل متزايد من قبل الشركات لتحسين الإنتاجية ومع ذلك يعرضها إلى التهديدات بشكل غير مباشر والذي يتم عن طريق استخدام خوارزميات الذكاء الاصطناعي لأغراض احتيالي مثل تشفير البرامج الضارة أو إنشاء رسائل بريد إلكتروني أو التصيد الاحتيالي أو الهجمات الإلكترونية[٣] .

ونتيجة التطور الهائل للإنترنت والتكنولوجيا، أصبح الفضاء الإلكتروني مساحة حيوية لممارسة الأنشطة البشرية، لكنه أيضًا فتح الباب أمام تهديدات أمنية جديدة لا تقل خطورة عن التهديدات التقليدية. تُعَد التهديدات الإلكترونية هجمات تُنفَّذ باستخدام آليات مثل الإنترنت وأجهزة الحاسب، بهدف إلحاق الضرر بالأنظمة والشبكات أو سرقة المعلومات الحساسة. على عكس الهجمات التقليدية التي تستهدف الأفراد مباشرة، وتركز التهديدات الإلكترونية على التأثير على البنى التحتية الرقمية، مما يهدد أمن الدول وأسلوب حياة المجتمعات. لذلك، أصبحت مواجهة هذه التهديدات أولوية قصوى للدول والمنظمات في ظل التطورات التكنولوجية المتسارعة[٤] . وباختصار، تعد تطبيقات الذكاء الاصطناعي أداة قوية في يد المهاجمين، مما يتطلب تطوير استراتيجيات أمنية متقدمة لمواجهة هذه التهديدات.

المبحث الثاني

مدى كفاية قواعد المسؤولية المدنية للحد من الهجمات الإلكترونية

تعد مسألة تحديد المسؤولية المدنية الناشئة عن الهجمات الإلكترونية من التحديات القانونية المعاصرة التي تتطلب إطارًا قانونيًا واضحًا وفعالًا. وذلك بسبب الطبيعة المعقدة لهذه الهجمات، والتي تتسم بتعدد أبعادها وتأثيراتها على

---

[١])د.محمد علي محمد التوني ,استراتيجية مكافحة الهجمات السيبرانية, دار الفكر الجامعي ,ط١ , الإسكندرية , ٢٠٢٣, ص ٢٥٥ومابعدها

[٢]) د. السعيد عبد الحميد إبراهيم , القوانين والاتفاقيات الدولية في مواجهة مخاطر الهجمات السيبرانية , دار العلم والإيمان للنشر والتوزيع , جمهورية مصر العربية ,ط١, ص ٤١.

[3]) Les risques de l’intelligence artificielle (IA) pour la sécurité,article, Publié le 09/10/2024, https://www.generali.fr/entreprise/actu/risques-IA-pour-securite/ .

[٤]) د.نوران شفيق , أشكال التهديدات الإلكترونية ومصادرها , مقال , متاح عبر الموقع الإلكتروني , https://www.europarabct.com/%D8%A3%D8% , تمت الزيارة في ٢٠٢٥/٣/٧, الساعة الثانية ليلاً.

الأفراد والمجتمعات، سواء على المستوى الاقتصادي أو الاجتماعي أو السياسي. وفي ظل التطور السريع لتقنيات الذكاء الاصطناعي والبرامج الذكية، أصبحت الهجمات الإلكترونية أكثر تواترًا وتعقيدًا، مما يزيد من صعوبة تحديد المسؤولية القانونية عنها. وتنشأ المسؤولية المدنية في هذا السياق من فكرة الإخلال بالالتزام القانوني الذي يؤدي إلى إلحاق الضرر بالغير. وتخضع هذه المسؤولية لأحكام القانون المدني، حيث يحق للمتضررين المطالبة بالتعويض عن الأضرار التي لحقت بهم. ومع ذلك، فإن تحديد طبيعة هذه المسؤولية يعد أمرًا بالغ الأهمية، حيث يمكن أن تكون عقدية إذا نتجت عن إخلال بالتزام تعاقدي، أو تقصيرية إذا نتجت عن إخلال بالتزام قانوني عام بعدم الإضرار بالغير. وفي حالة الهجمات الإلكترونية، تتوقف طبيعة المسؤولية المدنية على عدة عوامل، منها ما إذا كانت ناتجة عن إرادة الأطراف في إطار علاقة عقدية، أو عن إخلال بالتزام قانوني عام. وهذا يستدعي العودة إلى القواعد العامة للمسؤولية المدنية، والتي تحدد الشروط الواجب توافرها لقيام المسؤولية، مثل وجود ضرر وعلاقة سببية بين الفعل الضار والنتيجة.

من ناحية أخرى، تواجه عملية تطبيق هذه الأحكام تحديات تقنية وقانونية كبيرة. فمن الصعب أحيانًا تحديد هوية مرتكبي الهجمات الإلكترونية بسبب طبيعة الإنترنت المعقدة وإمكانية إخفاء الهوية. بالإضافة إلى ذلك، قد تكون هناك صعوبات في إثبات العلاقة السببية بين الهجوم الإلكتروني والضرر الذي وقع، خاصة في حالات الهجمات التي تستخدم تقنيات متطورة مثل الذكاء الاصطناعي. ومما تقدم سنناقش طبيعة المسؤولية المدنية الناتجة عن الهجمات الإلكترونية و مسألة التعويض عنها في مطلبين : الأول نبحث فيه طبيعة الهجمات الإلكترونية هل هي عقدية ام تقصيرية , أما في المطلب الثاني منه نحدد آليات التعويض والعقبات التي تواجه المتضرر في الحصول على التعويض وعلى النحو التالي.

المطلب الاول

طبيعة المسؤولية المدنية الناتجة عن الهجمات الإلكترونية

إن طبيعة المسؤولية المدنية الناتجة عن الهجمات الإلكترونية تتطلب تحليلًا دقيقًا للقواعد العامة للمسؤولية، مع مراعاة التحديات التقنية والقانونية الفريدة التي تطرحها هذه الهجمات. وهذا يتضمن تحديد ما إذا كانت المسؤولية عقدية أم تقصيرية، ووضع آليات فعالة لتحديد المسؤولية وضمان تعويض المتضررين، مما يسهم في تعزيز الأمن الإلكتروني وحماية حقوق الأفراد والمجتمعات. لذا سنبحث في هذا المطلب عن طبيعة المسؤولية المدنية هل هي عقدية ام تقصيرية.

الفرع الاول

الطبيعة العقدية للمسؤولية المدنية الناتجة عن الهجمات الإلكترونية

أن تحديد المسؤولية المدنية العقدية الناتجة عن الهجمات الإلكترونية من المسائل الهامة كونها تنشأ من الإخلال بالالتزام القانوني سواء كان في إطار العقود أو في إطار الاتفاقيات, وفي هذا السياق، يُعد تنفيذ الإدارة القانونية لمشاريع تكنولوجيا المعلومات بالتنسيق مع الفرق التشغيلية أمرًا بالغ الأهمية لاحتواء المخاطر المتزايدة، خاصة في

ظل تزايد التهديدات الإلكترونية. وتتمثل الإدارة القانونية في إيلاء اهتمام خاص للإطار التعاقدي، مع التركيز على البنود التي تحدد طبيعة المسؤوليات والالتزامات بين الأطراف[١].

وأن أحد البنود الأكثر إثارة للنقاش في عقود تكنولوجيا المعلومات هو شرط تحديد المسؤولية, حيث يهدف هذا البند إلى السماح لمقدم الخدمة بالحد من التعويضات التي قد يضطر لدفعها للعميل في حالات عدم الوفاء بالعقد أو سوء الأداء. ومع ذلك، يتطلب هذا البند صياغة دقيقة تتناسب مع طبيعة العلاقة التعاقدية والسياق الذي يتم فيه تنفيذ العقد[٢] . اذ تنص المادة (١٦٨) من القانون المدني العراقي على انه " أذا استحال على الملتزم بالعقد ان ينفذ الالتزام عينا حكم عليه بالتعويض لعدم الوفاء بالتزامه مالم يثبت استحالة التنفيذ قد نشأت عن سبب اجنبي لا يد له فيه وكذلك يكون الحكم اذا تأخر الملتزم في تنفيذ التزامه"[٣] وهذا ما أكدته المادة (٢١٥) من القانون المدني المصري[٤] واما بالنسبة الى التشريع الفرنسي بعد تعديل قانون العقود الفرنسية جاء في المادة (١١٢٢) " يجوز ان ينص القانون أو العقد على مهلة التفكير وهي مهلة لا يجوز لمن وجه اليه الايجاب التعبير عن قبوله قبل انقضائها او على مهلة للعدول هي المهلة التي يمكن لمن تقررت لصالحه الرجوع عن رضائه قبل انقضائها " والمادة (١١٠٤)" يجب التفاوض على العقود وابرامها وتنفيذها بحسن نية يعتبر هذا الحكم من النظام العام "[٥] .وأن هذه النصوص القانونية تركز على الالتزامات التعاقدية والتعويض عند الإخلال بها , لكنها لا تُعتبر كافية في مواجهة الهجمات الإلكترونية كونها تفتقر الى تفاصيل محددة حول مسؤولية الأطراف في حماية الأنظمة والبيانات من الهجمات الإلكترونية .

ومما تقدم نجد بأن هذه المسؤولية تفرض على الأطراف المتعاقدة التزامًا بتبني تدابير أمنية مناسبة لحماية البيانات والأنظمة , وفقاً لما تم الاتفاق عليه في العقد, كحالة الشركة التي تتعاقد مع شركة تركيب أنظمة المراقبة لحمايتها. ففي حالة التقصير في هذه الالتزامات ,او قيام شركة تركيب أنظمة المراقبة بانتهاك خصوصية الشركة أو التلاعب في أنظمة الحماية , فيعتبر الطرف المخل مسؤول مسؤولية مدنية عقدية ويلتزم بالتعويض عن الأضرار الناتجة عن أي هجمات الإلكترونية التي كان يمكن تفاديها . لذا فأن قيام المسؤولية المدنية العقدية أداة قانونية مهمة لتحفيز الشركات والافراد على تعزيز الأمن الإلكتروني والتقيد بالمعايير الوقائية .

وفيما يتعلق بالمسؤولية المدنية العقدية، يمكن أن تأخذ الالتزامات أشكالًا مختلفة منها : الالتزام بالوسائل: هنا يلتزم مقدم الخدمة ببذل كل ما في وسعه لتحقيق النتيجة المطلوبة، دون ضمان تحقيقها. وهذا يشمل واجبات مثل تقديم

---

[١]) د. محمد فتحي محمد إبراهيم , مصدر سابق , ص٢٣وما بعدها .

[2]) Par Haas Avocats ,La clause de responsabilité dans les contrats informatiques , Rédigé par Haas Avocats | Jan 29, 2024 1:47:23 PM, Article available on the website, https://info.haas-avocats.com/droit-digital/la-clause-de-responsabilite-dans-les-contrats-informatiques?hs_amp=true

[٣]) القانون المدني العراقي رقم ٤٠ لسنة ١٩٥١.

[٤]) القانون المدني المصري رقم ١٣١ لسنة ١٩٤٨.

[٥]) قانون العقود الفرنسية رقم ١٣١ لسنة ٢٠١٦ .

المشورة، التوصية، أو التحذير. على سبيل المثال، في حالة الهجمات الإلكترونية، قد يلتزم مقدم الخدمة باتخاذ جميع الإجراءات الوقائية الممكنة، ولكن دون ضمان منع الهجوم بالكامل.

اما الالتزام بالنتيجة: في هذه الحالة، يلتزم مقدم الخدمة بتحقيق نتيجة محددة مسبقًا، مثل الوفاء بموعد نهائي أو تحقيق مستويات خدمة معينة. في سياق الأمن الإلكتروني ، قد يشمل ذلك ضمان عدم اختراق الأنظمة أو تحقيق مستوى معين من الحماية.

الالتزام المعزز بالوسائل (الالتزام بالنتيجة المخففة): هنا يتم تعزيز مسؤولية مقدم الخدمة من خلال عكس عبء الإثبات. إذا لم يتم تحقيق النتيجة المتوقعة، يتحمل مقدم الخدمة مسؤولية إثبات أنه بذل كل ما في وسعه لتجنب الضرر. هذا النوع من الالتزامات مفيد بشكل خاص في حالات الهجمات الإلكترونية، حيث يصعب على العميل إثبات الإهمال من جانب مقدم الخدمة من المهم أن لا يجعل شرط تحديد المسؤولية الالتزام الأساسي للعقد بلا معنى. بمعنى آخر، إذا أدى شرط تحديد المسؤولية إلى إضعاف جوهر العقد أو جعل الالتزام الأساسي غير قابل للتنفيذ، فإنه يعتبر باطلًا. على سبيل المثال، إذا نص العقد على أن مقدم الخدمة غير مسؤول عن أي نوع من الضرر في أي ظرف من الظروف، فإن هذا البند قد يُعتبر غير معقول وغير قابل للتنفيذ.

اما في ما يتعلق بالمسؤولية عن الضرر غير المباشر، والذي يشير إلى الضرر الذي لا يرتبط مباشرة بالضرر الأولي، فإن العقود عادةً ما تستبعد التعويض عن هذا النوع من الضرر. ومع ذلك، يمكن أن يتم التفاوض على شمول الضرر غير المباشر ضمن نطاق المسؤولية التعاقدية، خاصة في حالات الهجمات الإلكترونية التي قد تؤدي إلى أضرار واسعة النطاق [١].

ومما تقدم ، يجب أن تراعي العقود في مجال تكنولوجيا المعلومات، وخاصة تلك المتعلقة بالأمن الإلكتروني ، التوازن بين تحديد المسؤوليات وضمان حماية الأطراف من المخاطر المحتملة. كما يجب أن تكون الصياغة القانونية دقيقة وواضحة لتجنب أي غموض قد يؤدي إلى نزاعات مستقبلية.

الفرع الثاني

الطبيعة التقصيرية للمسؤولية المدنية الناتجة عن الهجمات الإلكترونية

تتمثل المسؤولية المدنية التقصيرية في الحد من الهجمات الإلكترونية في الالتزام العام بعدم الإضرار بالغير، حيث يتحمل الشخص المسؤولية إذا أخل بهذا الالتزام وتسبب في ضرر من خلال هجوم إلكتروني. يشترط لقيام هذه المسؤولية وجود ضرر وعلاقة سببية بين الفعل الضار والنتيجة. وتعد هذه المسؤولية أساسية في حال عدم وجود علاقة عقدية بين الأطراف المتضررة ومرتكبي الهجمات[٢] , وبهذا فأن تحقق المسؤولية التقصيرية بعدم وجود عقد

[1]) Par Haas Avocats, La clause de responsabilité dans les contrats informatiques , Rédigé par Haas Avocats | Jan 29, 2024 1:47:23 PM, Article available on the website, https://info.haas-avocats.com/droit-digital/la-clause-de-responsabilite-dans-les-contrats-informatiques?hs_amp=true .

[٢]) د. محمد صبري السعدي , الواضح في شرح القانون المدني , المدنية العام للالتزامات , مصادر للالتزامات المسؤولية التقصيرية :الفعل المستحق التعويض , دار الهدى , الجزائر , ص ١٦.

يتم مجرد الاخلال بالالتزام العام وهو عدم الاضرار بالغير وبالتالي فأن انتهاك الخصوصية الشخصية عبر الوسائل الرقمية مثل احتراق الحسابات الإلكترونية أو الوصول غير المصرح به إلى الأجهزة الشخصية , يعد عملاً غير مشروع يترتب عليه مسؤولية تقصيرية مدنية توجب تعويض الضرر , حتى لو لم يتصل إلى مستوى الجريمة [١] , كما جاء في نص المادة (٢٠٢) من القانون المدني العراقي والتي نصت" كل فعل ضار بالنفس من قتل او جرح او ضرب او اي نوع اخر من انواع الايذاء يلزم بالتعويضات من احدث الضرر" والمادة (٢٠٤) التي نصت " كل تعدي يصيب الغير باي ضرر اخر غير ما ذكر في المواد السابقة يستوجب التعويض". كما نصت المادة (٢٠٥/أ) على أنه " ١ – يتناول حق التعويض الضرر الادبي كذلك فكل تعد على الغير في حريته او في عرضه او في شرفه او في سمعته او في مركزه الاجتماعي او في اعتباره المالي يجعل المتعدي مسؤولا عن التعويض" [٢] , والمادة (١٦٣) من القانون المدني المصري والتي نصت " كل خطا سبب ضرر يلتزم من أرتكبه بالتعويض"[٣]. اما بالنسبة الى القانون المدني الفرنسي فقد نص في المادة (١٢٤٠) "على ان كل فعل من انسان يحدث ضرراً بالغير يلتزم من وقع هذا الفعل الضار بخطئه ان يعوض هذا الضرر" والمادة (١٢٤١)" يسأل كل شخص عن الضرر الذي سببه ليس فقط فعل ارتكابه بل ايضا بإهماله وعدم تبصره"[٤] ومما تقدم نجد بأن المتسبب ملزماً بالتعويض عن الضرر المادي أو المعنوي الناجم عن انتهاك الخصوصية, دون الحاجة الى إثبات وجود نية الاضرار , إذ يكفي ثبوت التقصير في احترام حدود الحياة الخاصة والخطأ من جانب الشخص المخطئ.

وفي ضوء القواعد العامة للمسؤولية المدنية، يمكن مواجهة الهجمات الإلكترونية عبر آليتي المسؤولية العقدية عند وجود تعاقد مسبق (كعقود حماية البيانات وعقود أنظمة المراقبة)، والمسؤولية التقصيرية عند الإخلال بالواجب العام في الحد من الأضرار الرقمية. الأ أن المسؤولية التقصيرية تتميز بنطاق تعويض أوسع – خاصة في الهجمات الإلكترونية – لشمولها الضرر المعنوي والمادي، بينما تقتصر العقدية على بنود العقد. وقد تترتب المسؤوليتان معاً إذا انتهك الشخص المخطئ التزاماً عقدياً (مثل اتفاقيات الأمن الإلكتروني) وألحق ضرراً بالغير، فيكون مسؤول مسؤولية عقدية أمام الشركة والطرف المتعاقد ومسؤولية تقصيرية أمام المتضرر الغير . وبالتالي، تفعيل هاتين الآليتين معاً يسهم في الحد من الهجمات الإلكترونية عبر الردع القانوني والجبر العادل للضرر.

المطلب الثاني

[١]) زياد بن محمد العتيبي , جرائم السيبرانية المرتكبة عبر الوسائط الرقمية وبيان مفهومها من حيث : أشكالها , خصائصها , أركانها والدافع من أرتكابها , بحث منشور , المجلة الأكاديمية العالمية للدراسات القانونية , المجلد (٣) , العدد(١) , ٢٠٢٠, ص ٦ .

[٢]) القانون المدني العراقي رقم ٤٠ لسنة ١٩٥١.

[٣]) القانون المدني المصري رقم ١٣١ لسنة ١٩٨٤.

[٤]) المادة (١٢٤٠) من القانون المدني الفرنسي لعام ١٨٠٤المعدل ونصها في اللغة الفرنسية L'article stipule : « Tout acte d'un être humain qui cause un préjudice à autrui est tenu de réparer ce préjudice. » والمادة (١٢٤١) من القانون المدني الفرنسي ونصها في اللغة الفرنسية Article (1241) « Comme une personne est responsable du dommage qu'elle a causé, non seulement par le fait qu'elle l'a commis, mais aussi par sa négligence et son imprévoyance. »

التعويض في حالات الهجمات الإلكترونية

إن وضع إطار قانوني قوي وفعال لتحديد المسؤولية المدنية عن الهجمات الإلكترونية يعد أمرًا ضروريًا. هذا الإطار يجب أن يأخذ في الاعتبار الطبيعة الخاصة لهذه الهجمات، ويوفر آلية واضحة لتحديد المسؤولية وضمان حصول المتضررين على التعويض المناسب. كما يجب أن يتضمن أحكامًا خاصة لتجاوز العقبات التقنية والقانونية التي قد تعيق تطبيق القواعد العامة للمسؤولية المدنية في هذا المجال. لذا سنبحث في هذا المطلب عن آليات التعويض في المسؤولية المدنية والعقبات التي تواجه المتضرر في الحصول على التعويض .

الفرع الاول

آليات التعويض في المسؤولية المدنية

يتطلب التعويض عن الأضرار الناتجة عن الهجمات الإلكترونية في المسؤولية المدنية توافر الشروط القانونية اللازمة من (الضرر و الخطأ و العلاقة السببية) وهذا ما سنتناوله تباعا.

اولا: الضرر : اختلفت تعبيرات الفقهاء والقانونيين في تعريف الضرر، حيث استعمل كل منهم اصطلاحًا يختلف عن الآخر: فقيل إنه "اختلال بحق أو مصلحة ذات قيمة للمتضرر" وقيل إنه "ما يصيب الشخص في حقه أو في مصلحة مشروعة له". وعادةً ما يترتب الضرر على وجود خطأ، لكن لا تكفي مجرد ثبوت الخطأ لقيام المسؤولية المدنية؛ بل يجب أن ينتج عن هذا الخطأ ضرر فعلي يصيب المضرور. فإذا لم يتحقق ضرر، فلا مجال للتعويض، إذ يُعد الضرر الركن الثاني للمسؤولية العقدية والتقصيرية بعد الخطأ قسّم القانونيون الضرر إلى نوعين: الضرر المادي: كالخسائر المالية أو تلف البيانات. والضرر الأدبي (المعنوي): كالإضرار بالسمعة أو انتهاك الخصوصية. ويجب التعويض عن كليهما بنفس الشروط، سواءً تعلق الأمر بعدم تنفيذ الالتزام كليًا أو جزئيًا، أو بتأخير في التنفيذ. ويشترط لتحقق وقوع الضرر ثلاثة شروط أن يكون محققًا: أي قد وقع فعلاً، وليس مجرد توقع. وأن يكون شخصيًا ومباشرًا: يصيب المتضرر مباشرة دون وساطة ظروف غير متوقعة. وأن يكون ناتجًا عن فعل المسؤول: أي أن يكون الضرر نتيجة طبيعية للخطأ[١] .

وبالتالي فأن الضرر في نطاق الهجمات الإلكترونية ، يتجلى في صور متعددة، مثل تلف أو سرقة البيانات (ضرر مادي) أو اختراق الخصوصية أو تشويه السمعة (ضرر معنوي) أو تعطيل الخدمات الإلكترونية مما يؤدي إلى خسائر مالية. ويخضع التعويض هنا لنفس الشروط العامة، مع التركيز على إثبات العلاقة السببية بين الهجوم والضرر، وهو ما قد يتطلب خبراء في الأمن الإلكتروني لإثباته. وإن نطاق التعويض في الهجمات الإلكترونية لا يقتصر التعويض على الأضرار المباشرة فحسب، بل قد يشمل أيضًا تكاليف إصلاح الأنظمة المتضررة وتكاليف

[١] بكر بن عبد اللطيف الهبوب , المسئولية العقدية , بحث , مجلة القضائية ,العدد الثالث, محرم , ١٤٣٣هجرية , ص ٢٩٥ومابعدها .

خسائر السمعة التجارية والتعويض عن الانتهاكات القانونية الناتجة عن تسريب البيانات. لكن لا يُسأل المدين عن الأضرار غير المباشرة البعيدة عن فعل الهجوم، إلا في حالات استثنائية تقوم على نظرية تحمل التبعية[١] .

ثانيا : الخطأ : بالرغم من وجود بعض الصعوبات في تحديد مفهوم الخطأ – نظراً لاختلاف طبيعته بين نطاقي المسؤولية العقدية والمسؤولية التقصيرية – إلا أن ذلك لا يعني استحالة وضع تعريف محدد له. ويظهر هذا الاختلاف جلياً في أن الخطأ في المسؤولية العقدية يتميز بسهولة التحديد نسبياً كونه ينشأ في إطار رابطة قانونية قائمة بين طرفين (العقد) ويتمثل في أن أي تجاوز للحدود المرسومة لهذه العلاقة التعاقدية هو في جوهره إخلال بالالتزامات الناشئة عن العقد . اما الخطأ في المسؤولية التقصيرية يكتنفه قدر أكبر من التعقيد كونه ينشأ في غياب أي رابطة قانونية مسبقة بين الأطراف. وبهذا تعددت التعريفات الفقهية له: عند بعض الفقهاء: فعرف الخطأ بأنه "عدم التنفيذ أو التأخر في تنفيذ الالتزام" عند آخرين: يمثل "إخلالاً بالتزام قانوني عام" . وففي الفقه الفرنسي: عُرف بأنه "الإخلال بالتزام سابق"[٢] . وبهذا تتميز المسؤولية العقدية عن المسؤولية التقصيرية من حيث شروط الأهلية المطلوبة لتحميل الشخص المسؤولية. ففي المسؤولية العقدية، يشترط أن يكون الشخص كامل الأهلية، أي أن يكون قد بلغ سن الرشد القانوني (تمام الثامنة عشرة) كما جاء في نص المادة (١٠٦) من القانون المدني العراقي التي نصت على أن " سن الرشد هي ثماني عشرة سنة كاملة"[٣] ، وذلك لأنها تقوم على الإخلال بالتزام ناشئ عن عقد، مما يتطلب إدراكًا كاملًا لطبيعة الالتزامات التعاقدية وآثارها. أما في المسؤولية التقصيرية، فيكفي أن يكون الشخص مُميِّزًا، أي قادرًا على التمييز بين النافع والضار، لأن أساس هذه المسؤولية هو ارتكاب عمل ضار (مثل التعدي على الغير أو الإضرار بممتلكاته)، بغض النظر عن وجود عقد بين الطرفين. فالمسؤولية التقصيرية تنشأ عن الأفعال غير المشروعة التي تسبب ضررًا للآخرين، سواء أكانت متعمدة أم ناتجة عن إهمال[٤] . وتختلف التشريعات القانونية حول مدى إمكانية مساءلة الشخص غير المميز أو غير المدرك إذا تسبب في إلحاق الضرر بالآخرين، وذلك نظراً لارتباط المسؤولية التقصيرية بمدى إدراك الفعل الضار وقدرة الشخص على التمييز. ففي التشريع العراقي، فقد اختلف الفقهاء

---

[١]) د. عبد الرزاق احمد السنهوري، الوسيط في شرح القانون المدني الجديد، نظرية الالتزام بوجه عام مصادر الالتزام، الجلد ١، ط٣، منشورات الحلبي الحقوقية، لبنان، ص٧٣٤. و بكر بن عبد اللطيف الهبوب , مصدر سابق , ص ٢٩٦ومابعدها . وجاء في نص المادة (٢) من قانون حماية البيانات الشخصية المصري رقم (١٥١) لسنة ٢٠٢٠والتي نصت على " تحديد نطاق تطبيق القانون على جميع الجهات التي تتعامل مع البيانات الشخصية " والمادة (٥) " تفرض عقوبات على انتهاك حماية البيانات ". واما في التشريع الفرنسي فقد نص في قانون حماية البيانات الشخصية الفرنسي رقم (٧٨_١٧) في المادة (١) " تحمي خصوصية الأفراد في التعامل مع البيانات الشخصية ." والمادة (٣٤) " تفرض عقوبات على انتهاك حماية البيانات .. ".

[٢]) أشوق دهيمي , أحكام التعويض عن الضرر في المسؤولية العقدية , رسالة ماجستير في العلوم القانونية , جامعة الحاج لخضر باتنه , كلية الحقوق والعلوم السياسية قسم الحقوق , ٢٠١٣, ص ٣٦.

[٣]) القانون المدني العراقي رقم ٤٠ لسنة ١٩٥١ .

[٤]) حسين عامر , عبد الرحيم عامر , المسئولية المدنية التقصيرية والعقدية , ط٢ , دار المعارف , ١٩٧٩, ص ١٥ .

في تفسير نصوص القانون المدني العراقي ، وخاصة المادتين (١٨٦) و (١٩١)[١] ، حيث يرى بعضهم أن المادة (١٨٦) تشترط الإدراك لقيام المسؤولية، بينما لا يشترط ذلك في المادة (١٩١). إلا أن هذا التعارض غير حقيقي في الواقع، إذ أن المشرع العراقي قد أخذ بمنهج وسط، حيث جعل مسؤولية الصغير مسؤولية أصلية مخففة، أي أنها قائمة لكنها تخضع لاعتبارات خاصة تتعلق بعدم اكتمال الأهلية. أما في التشريع المصري: أخذ المشرع موقفاً مخففاً، حيث جعل مسؤولية الصغير غير المميز مسؤولية جوازية، أي أنها ليست أصلية بل تخضع لتقدير القاضي بناءً على ظروف الواقعة[٢] .وفي التشريع الفرنسي: يشترط أن يكون الفاعل مدركاً ومميزاً حتى يمكن تحميله المسؤولية التقصيرية، حيث أن الإدراك شرط أساسي لقيام الخطأ الموجب للتعويض[٣] .

ومما تقدم نجد بأن في عصر التكنولوجيا، تبرز إشكاليات جديدة تتعلق بالمسؤولية القانونية، خاصة في حالات الهجمات الإلكترونية مثل الاختراقات أو نشر البرمجيات الخبيثة أو سرقة البيانات. هنا يمكن تطبيق كلا نوعي المسؤولية العقدية ، إذا وقع الاختراق بسبب إخلال أحد الأطراف (مثل موفر الخدمة) بالتزاماته التعاقدية (كحماية البيانات وفقًا لعقد الخصوصية).المسؤولية التقصيرية: إذا قام شخص (حتى لو كان قاصرًا مميزًا) بهجوم إلكتروني متسببًا في ضرر للغير، فيُطالب بالتعويض حتى لو لم يكن هناك عقد بينه وبين الشخص المضرور .

ثالثا : العلاقة السببية : تعد العلاقة السببية ركناً جوهرياً في قيام المسؤولية المدنية، سواءً كانت عقدية أم تقصيرية. فلا تكفي مجرد ثبوت الخطأ أو الضرر، بل يجب أن يكون هناك رابط سببي مباشر بين الخطأ المرتكب والضرر الحاصل وبهذا لا تقوم المسؤولية المدنية إلا بوجود الضرر و الخطأ و العلاقة السببية، ولكن قد تتحقق المسؤولية أحياناً بدون الخطأ (كالمسؤولية العقدية المطلقة أو مسؤولية حارس الأشياء)، بينما لا تتحقق أحياناً أخرى رغم وجود الخطأ إذا انعدمت السببية. لذا، يبقى إثبات الرابطة السببية عاملاً حاسماً في تحديد المسؤولية وتعويض المتضرر[٤] . وتعرف العلاقة السببية بأنها " العلاقة التي يكون فيها عنصر الخطأ هو الذي أحدث الضرر المباشرة وأن الأخير نتيجة مباشرة مترتبة على الأول" [٥] . وتعد العلاقة السببية في المسؤولية المدنية ركناً محورياً، لكنها لا تقوم إلا على السبب المنتج الفعّال، أي ذلك السبب المباشر والمؤثر في إحداث الضرر، دون الأخذ بالأسباب العارضة التي لا تؤدي بطبيعتها إلى النتيجة الضارة. فالمحاكم لا تعتد إلا بالسبب المباشر الذي يمكن نسبته إلى الخطأ، بحيث يكون

---

[١]) نصت المادة (١/١٨٦) " اذا اتلف احد مال غيره أو انقص قيمته مباشرة أو تسببا يكون ضامنا، اذا كان في احداثه هذا الضرر قد تعمد أو تعدى" ونصت المادة (١٩١) " اذا اتلف الصبي مميز أو غير مميز او من في حكمهما مال غيره. لزمه الضمان في ماله وإذا تعذر الحصول على التعويض من أموال من وقع منه الضرر ان كان صبيا غير مميز او مجنون جاز للمحكمة أن تلزم الولي أو القيم او الوصي بمبلغ التعويض على أن يكون لهذا الرجوع بما دفعه على من وقع منه الضرر.....".

[٢]) القانون المدني المصري رقم ١٣١ لسنة ١٩٨٤.

[٣]) د. حسن علي ذنون، المبسوط في شرح القانون المدني، الخطأ، ج٢، ط١, دار وائل للنشر، الاردن،٢٠٠٦، ص١٣٠.

[٤]) د. عبد الرزاق أحمد السنهوري , الوسيط في شرح القانون المدني الجديد نظرية الالتزام بوجه عام مصادر الالتزام , دار النشر للجامعات المصرية , القاهرة , ١٩٥٢, ص ٨٧٢.

[٥])السيد عبدالوهاب عرفة, المسئولية المدنية,المجلد ٢,المسئولية التقصيرية,الناشر المكتب الفني للموسوعات القانونية,الاسكندرية,ص٧١.

هو العامل الحاسم في وقوع الضرر إذا تعددت الأسباب وكان أحدها خطأً منتجاً (مثل إهمال الشركة في تأمين البيانات)، بينما كان الآخر عرضياً (مثل هجوم إلكتروني معقد)، فإن المسؤولية تقع على من كان خطأه مباشراً ومؤثراً. أما إذا كانت الأسباب مستقلة (مثل قرصنة خارجية أو إهمال داخلي)، فيتم توزيع المسؤولية حسب درجة تأثير كل سبب. وتعتمد المحاكم على الرابطة السببية المباشرة، فإذا ثبت أن الخطأ (كعدم استخدام تشفير البيانات) كان كفيلاً بجعل الضرر متوقعاً، قامت المسؤولية. أما إذا تدخل سبب أجنبي (مثل هجوم إلكتروني معقد غير متوقع)، فقد تنقطع السببية[١] .اما في حالات الهجمات الإلكترونية، قد تتداخل الأسباب، مثل: إهمال المؤسسة في تأمين أنظمتها (سبب منتج) وتطور أدوات القرصنة (سبب خارجي).فهنا، تُحمَّل المسؤولية على الطرف المهمل، ما لم يكن الهجوم استثنائياً وغير متوقع.

الفرع الثاني

العقبات التي تواجه المتضرر في الحصول على التعويض

لقد عرف الفقهاء التعويض بأنه "مبلغ نقدي أو عيني يعادل قيمة الضرر الواقع، سواء تمثل في خسارة مباشرة أو فقدان كسب متوقع". ويشترط في التعويض أن يكون متناسباً مع الضرر دون إفراط أو تفريط، حيث يدور وجوده وعدمه مع وجود الضرر وعدمه . وبالتالي فأن في مجال الهجمات الإلكترونية، يواجه المتضررون صعوبات عديدة في الحصول على تعويض عادل، أهمها: ١- صعوبة إثبات العلاقة السببية بين الهجوم والضرر ٢- تعقيدات تحديد هوية المهاجم الحقيقي ٣- عدم وضوح الجهة القضائية المختصة وصعوبة فهم الجوانب المعقدة للهجمات الألكترونية ٤- التحديات التقنية في تقدير حجم الأضرار غير المادية [٢] .

ومما تقدم يبقى التعويض الجزاء الطبيعي للمسؤولية، لكن تطبيقه في الهجمات الإلكترونية يواجه تحديات عملية كبيرة تقلل من فعاليته في تحقيق العدالة للمتضررين.

وبالتالي تصنف الهجمات الإلكترونية إلى ثلاثة مستويات رئيسية: بسيطة يقوم بها أفراد باستخدام أدوات متاحة، ومتوسطة تتطلب خبرة تقنية متخصصة، ومعقدة تحتاج إلى فرق محترفة وتمويل ضخم. وتعتمد فعالية هذه الهجمات بشكل أساسي على وجود ثغرات أمنية في الأنظمة المستهدفة، حيث تزداد خطورتها مع ارتفاع درجة تعقيدها.

---

[١])السيد خلف محمد,دعوى التعويض عن المسئولية التقصيرية,الناشر المركز القومي للإصدارات القانونية,ط١,القاهرة,٢٠٠٧,ص٧١ومابعدها

[٢]) بيطار صابرينة , التعويض في نطاق المسؤولية المدنية في القانون الجزائري , رسالة ماجستير في القانون الخاص الأساسي, وزارة التعليم العالي والبحث العلمي جامعة أحمد دراية_ إدرار, كلية الحقوق العلوم السياسية, ٢٠١٥, ص ١١ ومابعدها . وكما جاء في قانون مكافحة جرائم تقنية المعلومات المصري (قانون الجرائم الإلكترونية رقم ١٧٥لسنة ٢٠١٨,في المادة (٢) والتي تنص "تعاقب على الاختراق غير المصرح به للأنظمة المعلوماتية ..." والمادة (٧) والتي جاء فيها " تعاقب على إنشاء أو استخدام مواقع إلكترونية لأغراض إجرامية..." والمادة (٢٥) التي نصت على " تعاقب على انتهاك خصوصية الأفراد عبر وسائل تقنية المعلومات .." وكذلك جاء في التشريع الفرنسي في قانون العقوبات الفرنسي على نصوص متعلقه بالجرائم الإلكترونية في نص المادة (٣٢٣_١) " التي تعاقب على الدخول غير المصرح به الى الأنظمة المعلوماتية .." والمادة (٢٣٢_٣) " تعاقب على إعاقة عمل الأنظمة المعلوماتية (مثل هجمات حجب الخدمة DdoS).

وبهذا تواجه الأنظمة الإلكترونية العديد من نقاط الضعف، أهمها الأخطاء البرمجية الكامنة في ملايين أسطر الأكواد، والثغرات في المكونات المادية للأجهزة، بالإضافة إلى طبيعة الإنترنت المفتوحة التي تفتقر للتشفير الكامل. هذه الثغرات تتيح للمهاجمين فرصاً مختلفة حسب مستوى تطورهم وقدراتهم [١] . كذلك نقص الخبرات في مواجهة التهديدات الإلكترونية حيث يعاني سوق الأمن الرقمي من نقص الكوادر المؤهلة للتعامل مع الهجمات المتقدمة، مما يزيد من صعوبة التصدي لها. وبالتالي تعد حماية البيانات الإلكترونية حجر الأساس للحفاظ على استقرار الأعمال وخصوصية الأفراد، وذلك للأسباب التالية : لضمان استمرارية العمليات من أي اختراق أو توقف للأنظمة قد يتسبب في خسائر مالية كبيرة وتعطيل الخدمات. وكذلك الحفاظ على ثقة العملاء والشركاء في عدم تسريب البيانات الشخصية أو المالية التي تسبب فقد في الثقة وفي المؤسسات ويتسبب في أضرار قانونية وسمعية. وأخيراً منع الاستغلال والابتزاز الإلكتروني حيث تساعد هذه الاجراءات في تقليل من مخاطر الهجمات التي تستهدف سرقة المعلومات أو تشفيرها[٢] وأن صعوبة إثبات الضرر في كل هذه التحديات وفي طبيعة الأضرار الغير الملموسة وفي الكثير من الأحيان تكمن الصعوبة ايضا في تقدير الخسائر المستقبلية الناتجة عن تسريب البيانات وعدم وجود معايير واضحة لتقدير الأضرار المعنوية والتكلفة العالية للخبراء والتقنيين اللازمين لإثبات الضرر[٣] .وبهذا نوصي المشرع العراقي بأدراج مادة جديدة في القانون المدني لحماية الأشخاص من الهجمات الإلكترونية مقتبسة من نصوص المواد (٢٠٢_٢٠٥) من القانون المدني العراقي وتكون بالصياغة التالية " ١_كل فعل ضار بالبيانات أو الأنظمة الإلكترونية، سواءً كان اختراقًا أو سرقةً أو تلفًا أو تشفيرًا دون وجه حق، أو أي نوع آخر من الهجمات الرقمية التي تسبب ضررًا ماديًا أو معنويًا، يلزم مرتكبه بالتعويض عما أحدثه من أضرار.٢_ يكون حق التعويض عن الضرر المادي والأدبي الناجم عن الهجمات الإلكترونية، بما في ذلك انتهاك خصوصية الأفراد أو سرقة بياناتهم الشخصية أو المالية، أو الإضرار بسمعة الأشخاص أو المؤسسات عبر الوسائل الرقمية، أو تعطيل الخدمات الإلكترونية الحيوية، مما يجعل الفاعل مسؤولًا عن التعويض.٣_ ويجوز الحكم بالتعويض للأفراد أو الشركات المتضررة، وكذلك للورثة في حال تسبب الاعتداء الإلكتروني في وفاة الضحية أو أضرار جسيمة تلحق بهم. ٤_ لا ينتقل حق التعويض عن الضرر الأدبي أو المادي الناتج عن الهجمات الإلكترونية إلى الغير إلا إذا تم تحديد قيمته بموجب اتفاق مكتوب أو حكم قضائي نهائي. ٥_تُراعى في تقدير التعويض طبيعة الضرر، سواء كان ملموسًا أو

---

[١] د. نوران شفيق, آثار الهجمات الإلكترونية وخطورتها , كلية الاقتصاد والعلوم السياسية , جامعة القاهرة, يوليو ١٢, ٢٠١٨,المركز الأوربي لدراسات مكافحة الإرهاب والاستخبارات , مقال , متاح عبر الموقع الإلكتروني , https://www.europarabct.com/%D8%A2%D8%, تمت الزيارة في ٢٠٢٥/٣/٢٠, الساعة الثالثة ليلاً.

[٢] امل عباس عبيد , الأمن السيبراني : التحديات وأهمية حماية البيانات الإلكترونية , مقال , متاح عبر الموقع الإلكتروني, https://uomus.edu.iq/NewColl.aspx?colid=25&newid=25642 , تمت الزيارة في ٢٠٢٥/٣/٢٤, الساعة الرابعة ليلاً.

[٣] د. نوران شفيق, آثار الهجمات الإلكترونية وخطورتها , كلية الاقتصاد والعلوم السياسية , جامعة القاهرة, يوليو ١٢, ٢٠١٨,المركز الأوربي لدراسات مكافحة الإرهاب والاستخبارات , مقال , متاح عبر الموقع الإلكتروني , https://www.europarabct.com/%D8%A2%D8%, تمت الزيارة في ٢٠٢٥/٣/٢٤, الساعة الرابعة ليلاً.

غير ملموس، بما في ذلك الخسائر المستقبلية المحتملة الناتجة عن انتهاك البيانات أو فقدان الثقة، مع الأخذ بعين الاعتبار التكلفة الفنية والقانونية لإثبات الضرر وإصلاحه".

ومما تقدم نجد بأن من الضروري في ظل الهجمات الإلكترونية تعزيز الوعي الأمني واعتماد أحدث التقنيات للتصدي للهجمات. كما أن الاستثمار في تدريب الكوادر وتطوير أنظمة الحماية سيحد من المخاطر ويضمن بيئة رقمية أكثر أماناً للجميع.

الخاتمة

بعد الانتهاء من البحث في موضوع دور المسؤولية المدنية في الحد من الهجمات الإلكترونية دراسة مقارنة توصلنا إلى مجموعة من الاستنتاجات والتوصيات التي رأينا انها ضرورية ولابد من الإشارة إليها كما يأتي.

أولاً: الاستنتاجات

١. ارتبط ظهور مصطلح "الهجمات الإلكترونية" بالتطور التكنولوجي الهائل واعتماد الإنسان المتزايد على وسائل الاتصال الرقمية. يعرف المجال الذي تتم فيه هذه الهجمات باسم "الفضاء السيبراني"، وهو بيئة افتراضية تشمل أنظمة الحواسيب وشبكات الإنترنت، وقد بدأ استخدام هذا المصطلح بشكل بارز منذ ثمانينيات القرن العشرين.

٢. تشكل الهجمات الإلكترونية تهديدًا كبيرًا للأفراد والمؤسسات والدول على حد سواء، حيث تُستخدم كأداة من قبل الجهات الخبيثة لاستهداف البنى التحتية والأنظمة الحساسة وسرقة البيانات، مما يجعلها أداة فعالة في الصراعات الحديثة.

٣. تواجه بعض الدول، مثل العراق، صعوبات في التصدي للهجمات الإلكترونية بسبب نقص الخبرة التقنية وعدم وجود تشريعات كافية. وهذا يستدعي تعزيز الأمن السيبراني ووضع استراتيجيات متكاملة لإدارة المخاطر في ظل التهديدات المتطورة.

٤. أصبح الذكاء الاصطناعي أداة متقدمة في يد المهاجمين، حيث يُستخدم لتطوير برامج ضارة ذكية قادرة على التكيف مع أنظمة الحماية وتجنب الكشف. ومن الأمثلة على ذلك هجمات حجب الخدمة (DDoS)، التي تهدف إلى إرباك الأنظمة من خلال إغراقها بكميات هائلة من الطلبات الوهمية، مما يؤدي إلى تعطيلها بالكامل.

٥. تختلف المسؤولية الناتجة عن الهجمات الإلكترونية بين: المسؤولية عقدية: إذا نتج الضرر عن إخلال بالتزام تعاقدي (مثل عقد حماية البيانات).وبين المسؤولية تقصيرية: إذا نتج الضرر عن إخلال بالتزام قانوني عام (مثل الإضرار بالغير دون وجود عقد).

٦. كما أن التعويض يحقق غايتين رئيسيتين ، هي الردع عن طريق معاقبة الجاني ومنعه من تكرار أفعاله الضارة. والتعويض المادي والأدبي ، بإصلاح الضرر الذي لحق بالمتضررين ، سواء كان ماديًا (مثل الخسائر المالية) أو معنويًا (مثل انتهاك الخصوصية).

٧. لكي يتحقق التعويض في إطار المسؤولية المدنية، يجب توافر ثلاثة أركان أساسية: هي الضرر: أي أذى مادي أو معنوي لحق بالمتضرر . والخطأ: سواء كان عمديًا (مثل الاختراق المتعمد) أو إهمالًا (مثل عدم تأمين البيانات). وكذلك عنصر العلاقة السببية: أن يكون الخطأ هو السبب المباشر في وقوع الضرر.

ثانياً: التوصيات

١. ضرورة تعزيز التعليم والتوعية الأمنية من خلال دعوة الحكومات والمجتمع المدني إلى تعزيز التعليم الأمني الإلكتروني للأفراد والمؤسسات، وبناء ثقافة الثقة والأمانة بين الجهات الفاعلة في المجتمع. كما نوصي بإدراج مادة "الأمن الإلكتروني " أو "مكافحة الهجمات الإلكترونية" ضمن المناهج التعليمية في المراحل المتوسطة والإعدادية، لخلق جيل واعٍ بمخاطر الفضاء الرقمي وقادر على حماية نفسه ومجتمعه.

٢. نوجه نداءً إلى المشرع العراقي بضرورة: تطوير التشريعات والقوانين وإكمال تشريع قانون الجرائم الإلكترونية الحالي ليشمل جميع صور الاعتداءات الرقمية الحديثة. وإصدار قانون خاص باسم "قانون مكافحة الهجمات الإلكترونية"، يوضح تعريف هذه الهجمات، صورها، والإجراءات القانونية والمدنية للتصدي لها. بالإضافة الى تعديل القانون المدني العراقي الحالي وإضافة مواد تعالج المسؤولية المدنية الناشئة عن الأضرار الإلكترونية ، وتضمن تعويض المتضررين دون إفلات المُتسببون في الضرر من العقاب.

٣. نوصي بضرورة إنشاء هيئة وطنية للأمن الإلكتروني أو السيبراني و بتشكيل من "المجلس الوطني للأمن السيبراني" كهيئة وطنية تعنى بـ: حماية البنى التحتية الرقمية والبيانات الحساسة. وتطوير استراتيجيات الرد السريع على الهجمات الإلكترونية العابرة للحدود. والتعاون مع الجهات الدولية لمتابعة التهديدات الإلكترونية الحديثة.

٤. نوصي بـ: تفعيل دور القضاء في مكافحة الانتهاكات الإلكترونية وإدراج نصوص قانونية واضحة تمنح القضاة أدوات فعالة في تطبيق النصوص القانونية وجبر الضرر وإعادة الحقوق الى المتضررين. وكذلك تدريب القضاة على فهم طبيعة الهجمات الرقمية وإثباتها قانونيًا. والعمل على إنشاء محاكم متخصصة في الهجمات الإلكترونية لضمان محاكمة عادلة وسريعة.

٥. العمل على تعزيز التعاون الوطني والدولي والتنسيق بين الحكومة والقطاع الخاص لتبادل الخبرات وتطوير أنظمة الحماية. بالإضافة الى الانضمام إلى الاتفاقيات التي تعنى بمكافحة الهجمات الالكترونية، مثل اتفاقية بودابست وإنشاء مراكز مراقبة إقليمية للإنذار المبكر عن الهجمات الإلكترونية .

٦. نوصي بضرورة ضمان فعالية المسؤولية المدنية في الحد من الهجمات الإلكترونية على إثبات العلاقة السببية بين الفعل الضار والضرر الناتج. وعلى تحديد التعويضات العادلة (المادية والمعنوية) للمتضررين. لتحقيق الردع العام عبر جزاءات مدنية رادعة تتناسب مع خطورة البيئة الرقمية.

٧. وكما نوصي بضرورة زيادة الاستثمارات في مجال الأمن الإلكتروني وخاصة في ظل التطورات المتسارعة للهجمات الإلكترونية , واعتماد منهجيات شاملة وفعالة لإدارة المخاطر. حيث تشهد الفترة الحالية ظهور أنماط جديده ومتطورة

من الهجمات الإلكترونية التي تستهدف بشكل متزايد الحقوق المكتسبة والمصالح الحيوية باستخدام أحدث التقنيات الرقمية.

مصادر البحث

اولا/ باللغة العربية

- د. السعيد عبد الحميد إبراهيم , الأمن السيبراني في عالم الميتافيرس الافتراضي , دار العلم والإيمان للنشر والتوزيع , ط١,جمهورية مصر العربية , ٢٠٢٥.
- د. السعيد عبد الحميد إبراهيم , القوانين والاتفاقيات الدولية في مواجهة مخاطر الهجمات السيبرانية , دار العلم والإيمان للنشر والتوزيع , جمهورية مصر العربية ,ط١.
- السيد عبد الوهاب عرفة , المسئولية المدنية , المجلد الثاني , المسئولية التقصيرية , الناشر المكتب الفني للموسوعات القانونية , الاسكندرية.
- السيد خلف محمد , دعوى التعويض عن المسئولية التقصيرية , الناشر المركز القومي للإصدارات القانونية , ط١, القاهرة , ٢٠٠٧.
- أشوق دهيمي , أحكام التعويض عن الضرر في المسؤولية العقدية , رسالة ماجستير في العلوم القانونية , جامعة الحاج لخضر باتنه , كلية الحقوق والعلوم السياسية قسم الحقوق , ٢٠١٣.
- امل عباس عبيد , الأمن السيبراني : التحديات وأهمية حماية البيانات الإلكترونية , مقال , متاح عبر الموقع الإلكتروني, https://uomus.edu.iq/NewColl.aspx?colid=25&newid=25642.
- بكر بن عبد اللطيف الهبوب , المسئولية العقدية , بحث , مجلة القضائية ,العدد الثالث, محرم , ١٤٣٣هجرية.
- بيطار صابرينة , التعويض في نطاق المسؤولية المدنية في القانون الجزائري , رسالة ماجستير في القانون الخاص الأساسي, وزارة التعليم العالي والبحث العلمي جامعة أحمد دراية_ إدرار, كلية الحقوق العلوم السياسية, ٢٠١٥.
- د. حسن علي ذنون، المبسوط في شرح القانون المدني، الخطأ، ج٢، ط١, دار وائل للنشر، الاردن،٢٠٠٦.
- حسين عامر , عبد الرحيم عامر , المسئولية المدنية التقصيرية والعقدية , ط٢ , دار المعارف , ١٩٧٩.
- زياد بن محمد العتيبي,جرائم السيبرانية المرتكبة عبر الوسائط الرقمية وبيان مفهومها من حيث: أشكالها , خصائصها, أركانها والدافع من أرتكابها,بحث منشور,المجلة الأكاديمية العالمية للدراسات القانونية,المجلد(٣), العدد(١) , ٢٠٢٠.
- سامي محمد بونيف , دور الاستراتيجيات الاستباقية في مواجهة الهجمات السيبرانية _ الّردع السيبراني نموذجا , المجلة الجزائرية للحقوق والعلوم السياسية , معهد العلوم القانونية والإدارية , المجلد (٤) , العدد (٧), سنة ٢٠١٩.
- د. عبد الرزاق احمد السنهوري، الوسيط في شرح القانون المدني الجديد، نظرية الالتزام بوجه عام مصادر الالتزام، الجلد ١، ط٣، منشورات الحلبي الحقوقية، لبنان.
- د. عبد الرزاق أحمد السنهوري , الوسيط في شرح القانون المدني الجديد نظرية الالتزام بوجه عام مصادر الالتزام , دار النشر للجامعات المصرية , القاهرة , ١٩٥٢.
- د. علاء عبد الرزاق محمد السالمي, المدخل الى لأمن السيبراني , الذاكرة للنشر والتوزيع , ط١, بغداد, ٢٠٢٣.
- عصام السيد , الأمن السيبراني , المركز الأكاديمي للنشر ومكتبة الدراسات العربية للنشر والتوزيع , ٢٠٢٤.

- د. محمد حسن السامرائي , دور القانون الدولي في مكافحة الهجمات السيبرانية , الذاكرة للنشر والتوزيع , بغداد , ٢٠٢٣, ص ٥١. وما المقصود بالهجوم عبر الإنترنيت , مقال , متاح عبرالموقع الإلكتروني , https://www.microsoft.com/ar/security/business/security-101/what-is-a-cyberattack#:~:text=%D8%A7%Dn.
- محمد دحماني, الذكاء الاصطناعي كألية لتعزيز الامن السيبراني , جامعة عمار ثليجي _الأغواط , بحث , مجلة الفكر القانوني والسياسي , المجلد السابع ,العدد الثاني , ٢٠٢٣.
- د. محمد فتحي محمد إبراهيم , التنظيم التشريعي لتطبيقات الذكاء الاصطناعي , مركز المحمود لتوزيع الكتب القانونية , القاهرة-جمهورية مصر العربية , طبعة٢٠٢٤.
- د. محمد علي محمد التوني,استراتيجية مكافحة الهجمات السيبرانية,دار الفكر الجامعي ,ط١, الإسكندرية , ٢٠٢٣.
- د. محمد صبري السعدي , الواضح في شرح القانون المدني , المدنية العام للالتزامات , مصادر للالتزامات المسؤولية التقصيرية :الفعل المستحق التعويض , دار الهدى , الجزائر.
- د. نوران شفيق , أشكال التهديدات الإلكترونية ومصادرها , مقال , متاح عبر الموقع الإلكتروني , https://www.europarabct.com/%D8%A3%D8%.
- د. نوران شفيق, آثار الهجمات الإلكترونية وخطورتها , كلية الاقتصاد والعلوم السياسية , جامعة القاهرة, يوليو ١٢, ٢٠١٨,المركز الأوربي لدراسات مكافحة الإرهاب والاستخبارات , مقال , متاح عبر الموقع الإلكتروني , https://www.europarabct.com/%D8%A2%D8%.
- القانون المدني العراقي رقم ٤٠ لسنة ١٩٥١.
- القانون المدني المصري رقم ١٣١ لسنة ١٩٤٨.
- قانون الأمن السيبراني الفرنسي رقم (٢٠١٨_١١٦٨) .
- قانون العقود الفرنسية رقم ١٣١ لسنة ٢٠١٦ .

ثانيا/ باللغة الاجنبية

-pratiques pour réduire les risques cyber menaçant les données , Anthony Seifert (chroniqueur), publié le 14 Avril 2023 .

- Réduire le risque d'erreur humaine pour améliorer la protection cyber de l'entreprise : un impératif , Dossier | Publié le 16 octobre 2024 | Mis à jour le 26 décembre 2024 .

- Les risques de l'intelligence artificielle (IA) pour la sécurité,article, Publié le 09/10/2024, https://www.generali.fr/entreprise/actu/risques-IA-pour-securite/ .

- Par Haas Avocats ,- La clause de responsabilité dans les contrats informatiques , Rédigé par Haas Avocats | Jan 29, 2024 1:47:23 PM, Article available on the website, https://info.haas-avocats.com/droit-digital/la-clause-de-responsabilite-dans-les-contrats-informatiques?hs_amp=true.

- Par Haas Avocats, La clause de responsabilité dans les contrats informatiques , Rédigé par Haas Avocats | Jan 29, 2024 1:47:23 PM, Article available on the website, https://info.haas-avocats.com/droit-digital/la-clause-de-responsabilite-dans-les-contrats-informatiques?hs_amp=true.