

عن فعالية الأمن السيبراني في حماية الفاتورة الإلكترونية *On the effectiveness of cybersecurity in protecting the electronic invoice*



ط.د: إيمان بوزيدي^{*1}

كلية الحقوق والعلوم السياسية، جامعة مولود معمري، (الجزائر)¹

Iman BOUZIDI^{1*},

Faculty of Law and Political Science, University of Mouloud Mammeri Tizi-ouzou,
(ALGERIA)¹

أ.د: مليكة أوباية^{*2}، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، (الجزائر)²

Pr. Malika OUBAYA^{2*},

Faculty of Law and Political Science, University of Mouloud Mammeri Tizi-ouzou,
(ALGERIA)²

تاريخ الاستلام: 2025/04/15 تاريخ القبول للنشر: 2025/06/09 تاريخ النشر: 2025/06/30.



ملخص:

يشهد العالم المعاصر تحولا كبيرا نحو رقمنة المعاملات التجارية وإدارتها نظرا للسمات التي يوفرها الفضاء الرقمي في هذا المجال، وقد أصبحت الفاتورة الإلكترونية مع هذا التحول الاستراتيجي تشكل عنصرا هاما في العمليات التجارية والمالية، ونقلة نوعية في إدارتها، وخطوة رائدة نحو بناء اقتصاد رقمي متكامل. لكن، تبرز المخاطر والتهديدات السيبرانية كأحد العراقيل الكبرى التي تواجه نظام الفاتورة الإلكترونية، الأمر الذي يجعل من توفير الأمن السيبراني عنصرا حاسما في ضمان أمنها وأمن بنيتها التحتية، إلا أن فعاليتها في لعب هذا الدور مرهون بالعديد من العوامل الأساسية المختلفة، وبالكثير من أساليب رفع التحديات التي تواجهها.

الكلمات المفتاحية: الفاتورة الإلكترونية، الجرائم السيبرانية، الأمن السيبراني.

Abstract : The modern world is witnessing a major shift towards the digitization of commercial transactions and their management, thanks to the advantages offered by cyberspace in this field. In this context, the electronic invoice has become a key component of commercial and financial operations, representing a significant milestone in their management and a pioneering step towards building an integrated digital economy.

However, cyber risks and threats emerge as one of the major obstacles facing the electronic invoicing system. This makes cybersecurity a crucial element in ensuring its safety and the security of its infrastructure. Nevertheless, its effectiveness in fulfilling this role depends on various fundamental factors and numerous approaches to overcoming the challenges it faces.

Keywords: Electronic invoice, cybercrime, cybersecurity.

مقدمة:

تتسارع عملية التحول الرقمي والاعتماد على الأنظمة السيبرانية في العديد من المجالات الحيوية في المجتمع المعاصر، ويبرز الحقل التجاري والاقتصادي كأحد الحقول الحيوية التي تتزايد فيها وتيرة هذا التحول، وفي ظل ذلك ظهرت الفاتورة الإلكترونية كأحد الأنظمة الرقمية التي يبدو أن أمر اعتمادها بات من الضروريات الملحة في إطار التوجه نحو بناء الاقتصاديات الرقمية، وهذا نظرا لقدرتها على تحسين الأداء، والتقليل من الجهود البشرية والمالية المبذولة في ظل الفواتير الورقية، ناهيك عن مزاياها الأخرى في حماية البيئة والمستهلك.

ونظرا لطبيعة الفضاء السيبراني وتعقيده، وتحوله في الوقت الراهن إلى ساحة حروب سيبرانية، وبيئة لمختلف الجرائم والتهديدات المعقدة، فإن أنظمة الفواتير الإلكترونية غدت عرضة للعديد من الهجمات السيبرانية المعقدة، التي تضعف من فاعليتها وقدرتها على لعب الأدوار الحيوية التي خصصت من أجله، الأمر الذي يستدعي تحركا فعليا نحو كفالة وضمان حمايتها في إطار أسس ومبادئ وآليات الأمن السيبراني.

تكمن جدوى الأمن السيبراني لحماية الفاتورة الإلكترونية في حماية مختلف البيانات التي تتضمنها، ولاسيما البيانات الشخصية والبيانات ذات الطابع المالي، وذلك بضمان سلامتها من أشكال التلاعب، وضمان سريتها وخصوصيتها، فضلا عن حماية البنية التحتية التشغيلية لأنظمتها، وضمان الاستمرارية في أداء وظائفها وخدماتها، وتبرز أهمية ذلك بالنظر إلى الأبعاد التي يمكن للفضاء السيبراني أن يحققها في إطار وظيفته في حماية الفواتير الإلكترونية.

وكأي حماية لنظام رقمي آخر، يسعى الأمن السيبراني لحماية أنظمة الفاتورة الإلكترونية بالاعتماد على مجموعة من السياسات والإجراءات الاستباقية الشاملة التي تعمل وفق نهج تكاملي ومرن، حيث تتشكل في المقام الأول من آليات قانونية تضع إطارا عاما لهذه الحماية، كما تتشكل في المقام الثاني من آليات ذات طابع تقني وفني قادرة على التكيف مع طبيعة الهجمات السيبرانية وآلياتها، فضلا عن التكيف مع الآثار التي تخلفها بمحاولة التعافي منها بشكل سريع وفعال.

ومع أن الأمن السيبراني يعتبر آلية حاسمة في ضمان حماية الفواتير الإلكترونية ونظمها من مختلف المخاطر والهجمات، إلا أن العقوبات التي تواجهها في ظل ذلك يدعو إلى طرح إشكالية: ما مدى كفاية الإطار القانوني الحالي في ضمان الأمن السيبراني للفاتورة الإلكترونية في ظل التحديات التقنية والتنظيمية التي تفرضها البيئة الرقمية؟

المبحث الأول:

طبيعة الأمن السيبراني للفاتورة الإلكترونية.

تتزايد الأهمية الاستراتيجية للفاتورة الإلكترونية بشكل مطرد مع تزايد وتيرة الرقمنة للقطاعات الحيوية في الدولة المعاصرة، والذي يقابله من ناحية أخرى تزايد المخاطر التي تهدد الفواتير الإلكترونية وتعيق مسار الرقمنة في المجالات الاقتصادية، ليبز الأمن السيبراني كأحد المفاهيم الحديثة لرفع التحديات الأمنية الراهنة لأمن الفاتورة الإلكترونية، وهو من المفاهيم التي تحتاج إلى المزيد من التوضيح والبيان (المطلب الأول)، لتعزيز مكانته وأهميته الاستراتيجية (المطلب الثاني).

المطلب الأول: مفهوم الأمن السيبراني للفاتورة الإلكترونية.

تفرض الطبيعة التقنية للفاتورة الإلكترونية أساليب جديدة لحمايتها وحماية بنيتها التحتية، وذلك من خلال ما يعرف بالأمن السيبراني الذي تعددت واختلفت التعاريف بشأنه، ولا نرى رغم هذه الاختلافات من بد لتقديم تعريف خاص للأمن السيبراني ضمن مفهوم الفاتورة الإلكترونية (الفرع الأول) وتجلية خصائصه بشكل واضح وذلك من واقع طبيعة هذا الأمن وطبيعة إجراءاته (الفرع الثاني).

الفرع الأول: تعريف الأمن السيبراني للفاتورة الإلكترونية.

يستمد الأمن السيبراني للفاتورة الإلكترونية مفهومه من الأمن السيبراني ذاته، ومن طبيعة الفواتير الإلكترونية، وعلى هذا فإنه من الضروري مناقشة مفهوم الأمن السيبراني تشريعا وفقها (أولا)، للوصول بعدها إلى صياغة مناسبة لتعريف الأمن السيبراني للفاتورة الإلكترونية (ثانيا).

أولا: تعريف الأمن السيبراني: تتعدد وتتوغل التعاريف المقدمة لمفهوم الأمن السيبراني وذلك تبعا لاختلاف الرؤى التي ينظر إليه من خلالها، وفيما يلي عرض مقتضب لهذه التعددية التعريفية:

1. التعريف التشريعي: يعرف المشرع الجزائري الأمن السيبراني على أنه: 'مجموع الأدوات والسياسات ومفاهيم الأمن والآليات الأمنية والمبادئ التوجيهية وطرق تسيير المخاطر والأعمال والتكوين والممارسات الجيدة والضمانات والتكنولوجيات التي يمكن استخدامها في حماية الاتصالات الإلكترونية ضد أي حدث من شأنه المساس بتوفر وسلامة وسرية البيانات المخزنة أو المعالجة أو المرسلة'⁽¹⁾.

يعرفه المشرع الأردني أيضا بأنه مجموع: 'الإجراءات المتخذة لحماية الأنظمة والشبكات، والمعلوماتية والبنى التحتية الحرجة من حوادث الأمن السيبراني، والقدرة على استعادة عملها واستمراريتها سواء أكان

(¹) المادة 3/10، قانون رقم 18-04، مؤرخ في 10 مايو 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، ج.ر عدد 27، صادرة في 13 ماي 2018.

الوصول إليها بدون تصريح أو سوء استخدام، أو نتيجة الإخفاق في اتباع الإجراءات الأمنية أو التعرض للخداع الذي يؤدي لذلك⁽¹⁾.

يتضح من خلال هذين التعريفين التشريعيين أن هناك توافقاً مبدئياً في إدراك الأهمية القصوى للأمن السيبراني كأهم ركيزة لحماية الفضاء الرقمي، ومع ذلك فإن التحليل المقارن يكشف بعض الفوارق الجوهرية بين التعريفين: ولعل أهم وأبرز اختلاف بينهما هو تركيز المشرع الأردني على البنية التحتية الحرجة والذي يظهر بعداً استراتيجياً، وهذا ما نجده غائباً في تعريف المشرع الجزائري رغم أهميته البالغة. في مقابل ذلك، أسهب المشرع الجزائري في تحديد مكونات الأمن السيبراني من خلال عرضه للأدوات والآليات الضرورية لتحقيقه، في حين حافظ المشرع الأردني على صيغة أكثر شمولاً تاركا القوس مفتوحاً لكل آلية من شأنها أن تنصب أهدافها ومراميها في تحقيق أمن الفضاء السيبراني.

كما أشار المشرع الأردني أيضاً إلى مسألة استعادة الأنظمة واستمرارية العمل بعد الهجمات، وهو عنصر حيوي في الاستجابة السيبرانية وتخطي الهجمات وآثارها المختلفة سيما تعطيل الخدمة، وهذا ما غاب في تعريف المشرع الجزائري، والذي يتعين تداركه. هذا التحليل المقارن للتعريفين السابقين يكشف أن المشرع الجزائري يركز بشكل خاص على الجوانب الوقائية، في حين أن المشرع الأردني يعكس منظوراً شاملاً يجمع بين الوقاية والاستجابة من جانب، ويشمل جميع البنية التركيبية للفضاء السيبراني والعناصر التي يتعين حمايتها من جانب آخر.

2. **التعريف الفقهي:** يصف بعض الباحثين الأمن السيبراني بأنه من المصطلحات ذات النطاق الدولي الشامل، ويجسد في صلب جوهره النهج الموجهة لضمان حماية البنية التحتية الرقمية، كما يصفها البعض الآخر بأنها آلية تعمل على التصدي لكافة التهديدات الخبيثة التي تنتهك سلامة وسرية المعلومات الحساسة، أو الرامية إلى الابتزاز، أو تلك التي تسعى إلى المساس بأداء العمليات التجارية المألوفة⁽²⁾. ينظر بعض الباحثين أيضاً إلى الأمن السيبراني باعتباره استراتيجية أمنية تتبناها الأطراف ذات الصلة بهدف إصباح الحماية على سرية وسلامة البيانات وتواجدها، فضلاً عن الحفاظ على الموارد والأنظمة السيبرانية، ويتضمن في ذلك مجموع التعليمات، والنهج، والإجراءات الاحترازية، والتكنولوجيات، والآليات، فضلاً عن تدريب الكوادر البشرية التي تسعى في مجملها إلى تحقيق بيئة سيبرانية آمنة⁽³⁾.

(¹) المادة 2/02، القانون الأردني رقم 16 لسنة 2019، قانون الأمن السيبراني، الصادر بتاريخ 16 أيلول 2019، ج.ر. عدد 5595 لسنة 2019.

(²) فارس عقيل علي الدويري، البيانات الضخمة ودورها في الحد من الجرائم الإلكترونية في ظل استراتيجية الأمن السيبراني، دار الخليج للنشر والتوزيع، الأردن، 2024، ص 72.

(³) (Daniel SCHATZ, Rabih BASHROUSH, Julie WALL, *(Towards a More Representative Definition of Cyber Security)*, Journal of Digital Forensics, Security and Law (JDFSL), Vol.

تعتبر هذه التعاريف الثلاثة عن رغبة ملحة في تأمين الفضاء السيبراني، ووضع أفضل الممارسات لتحقيق ذلك، إلا أن الفوارق بينها جلية، لاسيما في نطاق وأبعاد الحماية، إذ نلمح ميلا في **التعريف الأول** إلى الاهتمام بالبنية التحتية المادية، مع إغفال تام للجوانب الأخرى، بما في ذلك العمليات السيبرانية، فيما نلاحظ في **التعريف الثاني** إغفالا لحماية البنية التحتية، والتركيز بشكل خاص على الخدمات والعمليات السيبرانية، والتي اختزلت بشكل واضح في تلك التي تكتسي طابعا ماليا.

يأتي **التعريف الثالث** لجعل الأمن السيبراني نهجا استراتيجيا متكاملا، فوسع أبعاده ونطاقه حتى كاد يشملها، وأسهب في عرض جوانب هذا النهج ومحاوره الأساسية، لاسيما الإدارية والتقنية والقانونية والبشرية، وهذا ما يجعل منه أجود التعاريف المعروضة وأعمقها في بيان جوهر مفهوم الأمن السيبراني.

ثانيا: تعريف الأمن السيبراني في إطار حماية الفاتورة الإلكترونية: تعرف الفاتورة الإلكترونية على أنها تداول للفاتورة وتخزينها بالاعتماد على الآليات الرقمية والإلكترونية بتعدد أشكالها وأنواعها⁽¹⁾، وبذلك يعتبر الفضاء السيبراني عماد الفاتورة الإلكترونية، فهي تقوم عليه بشكل كامل في كل خطوة من خطواتها، بداية من معالجتها، مروراً بتداولها، ونهاية بتخزينها وحفظها، حيث توظف في ذلك كل البنية التحتية للفضاء السيبراني، بما في ذلك الطبقة المادية والمنطقية، وعلى هذا فإن أمر حمايتها من التهديدات السيبرانية هو شأن أمني سيبراني خالص.

لم يرد تعريف للفاتورة الإلكترونية في التشريع الجزائري، ولم يخص المشرع الجزائر الفاتورة الإلكترونية بتشريع خاص، ولم يضع نظاما شاملا لها رغم اعترافه بها في العديد من النصوص القانونية سيما المادة 11 من المرسوم التنفيذي رقم 05-468⁽²⁾، فالأحكام المتعلقة بالفاتورة الإلكترونية في القانون الجزائري تسري عليها أحكام الفواتير العادية بالإضافة إلى ما تختص به من أحكام التوثيق والتصديق المنصوص عليها في القانون رقم 15-04، الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

علاوة على أن المشرع الجزائري -كما ظهر من استقراء النصوص القانونية ذات الصلة- لم يول الفاتورة الإلكترونية عناية قانونية خاصة وواضحة ضمن منظمة الأمن السيبراني، حيث يغيب الربط الصريح بين الفاتورة كأداة مالية رقمية وبين الحماية القانونية لها ضمن الفضاء السيبراني، لذلك فإن الأمن السيبراني للفاتورة الإلكترونية خاضع في قواعده وأحكامه وآلياته للقواعد المقررة في التشريعات المتعلقة بالأمن السيبراني في التشريع الجزائري، لاسيما القانون رقم 18-07 المؤرخ في 10 يونيو سنة 2018، المتعلق بحماية الأشخاص

12 : No. 2 , Article 8, Association of Digital Forensics, Security and Law (ADFSL), Florida., P.66. <https://commons.erau.edu/jdfsl/vol12/iss2/8/>

¹ (voir: article 02/02/E, DIRECTIVE 2001/115/CE DU CONSEIL du 20 décembre 2001, modifiant la directive 77/388/CEE en vue de simplifier, moderniser et harmoniser les conditions imposées à la facturation en matière de taxe sur la valeur ajoutée, J.O.C.E, L15, 17/01/2002.

⁽²⁾ مرسوم تنفيذي رقم 05-468، مؤرخ في 10 ديسمبر 2005، يحدد شروط تحرير الفاتورة وسند التحويل ووصل التسليم والفاتورة الإجمالية وكيفيات ذلك، ج.ر. عدد 80 الصادرة بتاريخ 11 ديسمبر 2005.

الطبيين في مجال معالجة المعطيات ذات الطابع الشخصي، والقانون رقم 09-04 المؤرخ في 05 غشت سنة 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

وبالتالي رأينا أن نقترح التعريف الآتي لبيان جوهر الأمن السيبراني للفاتورة الإلكترونية باعتباره: مجموع الاستراتيجيات أو النهج والسياسات والإجراءات والآليات التقنية والفنية والقانونية والتنظيمية والبشرية الهادفة إلى حماية الفواتير الإلكترونية حال معالجتها، تداولها، وتخزينها، وذلك من كافة التهديدات السيبرانية، بما في ذلك التهديدات المحتملة التي يمكن أن تطال سلامة وسرية بياناتها، أو تلك التي يمكن أن تستهدف بنيتها التحتية، مادية كانت أم منطقية.

الفرع الثاني: خصائص الأمن السيبراني للفاتورة الإلكترونية.

يتميز الأمن السيبراني للفاتورة الإلكترونية بالعديد من السمات والخصائص، إذ يعتبر أمانا شاملا متكاملًا (أولاً)، يتسم بقدر كبير من المرونة والتكيف مع مختلف المخاطر والتحديات (ثانياً)، فضلا عن تميزه بالطبيعة الاستباقية التي تضمن هذه المرونة والتكيف بشكل كبير (ثالثاً).

أولاً: الشمولية: يعتبر الأمن السيبراني للفاتورة الإلكترونية منظومة شاملة تغطي مختلف طبقاتها التكوينية، وتشمل تدابير تقنية وفنية وقانونية وتنظيمية، إلى جانب الاعتبارات البشرية، وذلك وفق ما أكدت عليه "الاستراتيجية الوطنية للأمن السيبراني لمملكة البحرين" من خلال دمج تلك العناصر ضمن إطار الحوكمة الرشيدة، والمعايير الموحدة، والإدارة الفاعلة، مع تعزيز الشراكة والتعاون على المستوى الوطني والإقليمي والدولي⁽¹⁾.

ثانياً: المرونة: تعد المرونة من صلب مفهوم الأمن السيبراني، إذ يعرفه بعض الفقهاء من منظور هذه الخاصية تحديداً⁽²⁾، والمرونة هي القدرة على مواجهة الأزمات غير المتوقعة والتكيف مع التغيرات، دون اشتراط العودة إلى الوضع السابق⁽³⁾، وتمثل المرونة في أمن الفواتير الإلكترونية القدرة على الاستجابة بفعالية للتحديات السيبرانية والتعافي منها، والتكيف مع آثارها بأساليب أكثر ملاءمة، وتظهر هذه المرونة في التشريع الجزائري من خلال العديد من النصوص الشاملة التي تتضمن بين طياتها معاني الوقاية والاستجابة المتماشي مع مفهوم

(¹) الاستراتيجية الوطنية للأمن السيبراني لمملكة البحرين، المركز الوطني للأمن السيبراني، د.ت.ن، تم الاطلاع عليه بتاريخ 15 نوفمبر 2024، متاح على الرابط: <https://www.ncsc.gov.bh/ar/national-strategy.html>

(²) راجع: منى الأشقر جبور، محمود عارف جبور، الأمن السيبراني والأمن القومي العربي: "واقع ومتطلبات وتحديات"، الفصل الحادي عشر من مؤلف جماعي: الأمن القومي العربي وتحديات الأمن الإقليمي"، المركز العربي للأبحاث ودراسة السياسات، قطر/لبنان، 2023، ص 389.

(³) منتدى أسبار الدولي، معجم المصطلحات الأساسية للدراسات المستقبلية، منتدى أسبار الدولي، الرياض، 2019، ص 139.

المرونة، كنص المادة الأولى من القانون رقم 04-09، والمادة 06/30 من القانون 04-15 المتعلق بالتوقيع والتصديق الإلكترونيين.

ثالثا: الاستباقية: يتميز الأمن السيبراني للفاورة الإلكترونية بخاصية الحماية الاستباقية، والتي يمكن تعريفها ببساطة بناء على التعريف اللغوي لهذا المصطلح⁽¹⁾، على أنها مجموعة الاستعدادات والتحضيرات المبكرة تحسبا لأي هجوم أو حادث سيبراني على الفواتير الإلكترونية وأنظمتها وبنيتها التحتية قبل وقوعه.

تتبلور خاصية الاستباقية في منع الهجمات قبل وقوعها عبر الإجراءات الوقائية والتقنيات التنبؤية كتوظيف الذكاء الاصطناعي⁽²⁾، أو استخدام التعلم البياني الديناميكي غير المتجانس⁽³⁾، كما تتبلور أيضا في إجراءات التعافي من الهجمات⁽⁴⁾ على الفواتير الإلكترونية، وهي مجموع الأعمال والإجراءات التحضيرية لمواجهة الآثار التي تعقب الهجمات السيبرانية في محاولة للحد من تبعاتها أو معالجتها.

ولعل من أبرز الآليات التي تبناها المشرع الجزائري في إطار الاستباقية؛ ما نص عليه من إجراءات التصريح المسبق والترخيص لمعالجة المعطيات⁽⁵⁾، فضلا عن الرقابة والتدقيق⁽⁶⁾ ووضع المعايير في مجال حماية المعطيات⁽⁷⁾، وإنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، التي أسندت إليها مهام تنشيط وتنسيق العمل الوقائي الاستباقي⁽⁸⁾.

(¹) راجع: سامي محمد بونيف، (دور الاستراتيجيات الاستباقية في مواجهة الهجمات السيبرانية: "الردع السيبراني أنموذجا")، المجلة الجزائرية للحقوق والعلوم السياسية، المجلد 04، العدد 01، كلية الحقوق، جامعة أحمد بن يحيى الونشريسي، تيسمسيلت، الجزائر، نوفمبر 2019، ص 152.

(²) (consult: Siva Subrahmanyam BALANTRAPU, *AI for Predictive (Cyber Threat Intelligence)*, *International Journal of Management Education for Sustainable Development*, Vol 7, No 7, 2024. <https://www.ijscds.com/index.php/IJMESD/article/view/590>

(³) (consult: Jun ZHAO, Minglai SHAO, Hong WANG, Xiaomei YU, Bo LI, Xudong LIU, *(Cyber threat prediction using dynamic heterogeneous graph learning)*, *Knowledge-Based Systems*, Volume 240, 15 March 2022. <https://www.sciencedirect.com.sndll.arn.dz/science/article/abs/pii/S0950705121011564>

(⁴) (consult: Meysam TAHMASEBI, *(Beyond Defense: Proactive Approaches to Disaster Recovery and Threat Intelligence in Modern Enterprises)*, *Journal of Information Security*, Vol.15 No.2, April 2024. <https://doi.org/10.4236/jis.2024.152008>

(⁵) راجع المادة 12، قانون رقم 07-18، مؤرخ في 10 يونيو 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي، ج.ر. عدد 34، صادرة في 10 يونيو 2028.

(⁶) راجع: المادة 51-52، قانون رقم 04-15، مؤرخ في 01 فبراير 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج.ر. عدد 06، صادرة في 10 فبراير 2015.

(⁷) راجع: المادة 12/24، قانون رقم 07-18.

(⁸) راجع: المادة 14/أ، قانون رقم 04-09، مؤرخ في 05 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر. عدد 47، صادرة في 16 غشت 2009.

المطلب الثاني: الأولوية الاستراتيجية للأمن السيبراني للفاتورة الإلكترونية.

يحتل الأمن السيبراني للفاتورة الإلكترونية أولوية استراتيجية كبيرة، نظرا لاستخدام الفواتير الإلكترونية على نطاق واسع، الأمر الذي فتح أبعادا عميقة في سياق حمايتها (الفرع الأول)، فضلا عن تقاوم التهديدات السيبرانية وتنوع أساليبها، وخطورة آثارها على الفواتير الإلكترونية، سواء على بياناتها أو على مختلف عناصر بنيتها التحتية (الفرع الثاني).

الفرع الأول: تطور أبعاد الأمن السيبراني للفاتورة الإلكترونية.

يعتبر الأمن السيبراني من الضروريات في مجال حماية أمن وسلامة الفواتير الإلكترونية نظرا لأبعاد أمنها على القطاعات العسكرية الحساسة (أولا)، ونظرا أيضا لارتباط أمنها بمصالح اقتصادية كبرى (ثانيا)، ولما له من آثار اجتماعية مهمة (ثالثا).

أولا: البعد العسكري: يعد التعامل بالفواتير الإلكترونية على خلفية النشاطات التي تقوم بها الجهات العسكرية في الدولة أمر وارد، بل هو أمر محقق في العديد من الدول، كالولايات المتحدة الأمريكية، التي تتعامل قانونا بالفواتير الإلكترونية في قطاع الدفاع⁽¹⁾، ومن هنا تبرز أهمية الأمن السيبراني للفاتورة الإلكترونية في حماية المعاملات العسكرية الحساسة، وتأمين القدرات اللوجستية والدفاعية عبر تأمين سلاسل التوريد من كافة التهديدات السيبرانية.

ثانيا: البعد الاقتصادي: يعتبر الفضاء السيبراني آلية حيوية من آليات تحسين العمليات الإنتاجية، وتسريع العملية الابتكارية، وتنشيط القطاع الاقتصادي، فالإحصائيات تعكس تحولا رقميا مهولا نحو الرقمنة الاقتصادية، كما هو الحال في التجارة الإلكترونية التي تزايد حجمها بين سنة 2013 و 2014 بنحو 20 بالمئة، الأمر الذي يزيد من الأهمية الاقتصادية للأمن السيبراني⁽²⁾، ولاسيما لأغراض حماية الفواتير الإلكترونية نظرا للأدوار الحيوية التي تلعبها.

يسهم الأمن السيبراني للفاتورة الإلكترونية في دعم النمو الاقتصادي، من خلال تعزيز أدورها المتمثلة في زيادة الإيرادات الضريبية والحد من الاقتصاد الموازي⁽³⁾، ورفع من معدلات الاستثمار، وانهاش القطاع

⁽¹⁾ (consult: Financial Management Regulation, Volume 10, Chapter 10, U.S. Department of Defense, USA, January 2016.

https://comptroller.defense.gov/Portals/45/documents/fmr/archive/10arch/10_10_Jan16.pdf

⁽²⁾ سمير بارة، (الأمن السيبراني "cyber Security" في الجزائر: "السياسات والمؤسسات")، المجلة الجزائرية للأمن الإنساني، المجلد 02، العدد 02، جامعة باتنة 1 الحاج لخضر، الجزائر، جويلية 2017، ص 261.

⁽³⁾ محمد منصوري، العيد خيراني، (دور تبني استعمال الفاتورة الإلكترونية في تفعيل التحقيق المصوب في ظل توجه الإدارة الضريبية نحو الرقمنة: "دراسة استطلاعية")، مجلة أبحاث اقتصادية معاصرة، المجلد 07، العدد 01، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة عمار ثليجي، الأغواط، الجزائر، أبريل 2024، ص 331.

التجاري⁽¹⁾، والإخلال بأمنها يهدد أدوارها الحيوية، من خلال تعطيل خدماتها أو الكشف عن بياناتها، مما يؤدي إلى إحداث خسائر مالية كبيرة، ويؤثر على دقة القرارات الاقتصادية.

ثالثا: البعد الاجتماعي: تلزم العديد من التشريعات المستخدمين بتضمين فواتيرهم الإلكترونية العديد من البيانات الشخصية، لاسيما معلومات المشتري، ومعلومات الدافع، وتعليمات الدفع، وتفاصيل الشيء المبوع⁽²⁾، وتهدد مثل هذه المعلومات بأي شكل من أشكال التلاعب بها أو بأنظمة معالجتها، هو انتهاك للخصوصية باعتبارها معلومات شخصية إسمية⁽³⁾، وطريق معبد لشيوع الجرائم المالية كجريمة الاحتيال الإلكتروني⁽⁴⁾.

تعد الفاتورة الإلكترونية كآلية لحماية "المصالح المادية للمستهلك"، ووسيلة إثبات للمعاملات التجارية الضامنة لحقوقه⁽⁵⁾، وهذا ما يجعل من التلاعب بها شكلا من إهدار المصالح والحقوق، مما يبرز أهمية أمنها في تعزيز الثقة ودعم التحول الرقمي المحقق للعديد من المكاسب الاقتصادية والاجتماعية والبيئية.

الفرع الثاني: تفاقم أشكال التهديدات السيبرانية للفاتورة الإلكترونية.

ينجر عن التنوع الكبير لأسلحة الفضاء السيبراني، تعددا كبيرا لأشكال الهجمات السيبرانية على الفاتورة الإلكترونية، ولاسيما على بياناتها من خلال التلاعب بها أو إفشائها (أولا)، أو من خلال استهداف البنية التحتية التشغيلية لها (ثانيا).

أولا: الهجمات على بيانات الفاتورة الإلكترونية. تتخذ الهجمات السيبرانية التي تستهدف بيانات الفاتورة الإلكترونية شكلين رئيسيين هما:

1. **انتهاك سرية البيانات:** تعتبر الفاتورة الإلكترونية من بين المستندات التجارية التي تحمل بين طياتها العديد من البيانات التي تقتضي السرية المعلوماتية⁽¹⁾، والتي قد ينتج الكشف أو الاطلاع عليها آثارا وخيمة، فضلا

(1) نورة حسين، (الفاتورة الإلكترونية آلية لتنشيط الاستثمارات)، مجلة الدراسات القانونية والسياسية، المجلد 05، العدد 02، جامعة عمار ثليجي، الأغواط، الجزائر، جوان 2019، ص ص 137-138.

(2) *(voir; article 06, Directive 2014/55/UE du Parlement européen et du Conseil, du 16 avril 2014, relative à la facturation électronique dans le cadre des marchés publics Texte présentant de l'intérêt pour l'EEE JOUE L 133 du 6 mai 2014, JOUE L 133 du 6 mai 2014.*

(3) عزيزة رابحي، الأسرار المعلوماتية وحمايتها الجزائرية، أطروحة دكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2017-2018، ص 40.

(4) عبد الوهاب عبد الكريم محمد المبارك، (إشكالية المسؤولية القانونية عن جرائم النصب والاحتيال الإلكتروني الواقعة على عملاء البنوك)، المجلة القانونية، المجلد 15، العدد 08، كلية الحقوق، فرع الخرطوم، جامعة القاهرة، مصر، فبراير 2023، ص 1936.

(5) عائشة بوعزم، (فعالية الفاتورة في إطار ممارسات التجارة الإلكترونية على ضوء التشريع الجزائري)، مجلة القانون العقاري والبيئة، المجلد 09، العدد 02، كلية الحقوق والعلوم السياسية، جامعة ابن باديس، مستغانم، جوان 2021، ص ص 05-09.

عن كونها انتهاكا للحق في الخصوصية، مما يجعل من انتهاك سريتها تصرفا غير مشروع بموجب العديد من التشريعات الدولية والوطنية، ولا سيما اللائحة العامة لحماية البيانات في الاتحاد الأوروبي⁽²⁾، والتوجيه الأوروبي المتعلق بالفاتورة الإلكترونية⁽³⁾، فضلا عن التشريعات الداخلية التي يعتبر القانون 07-18 واحدا منها⁽⁴⁾.

2. **انتهاك سلامة البيانات:** تلعب الفواتير الإلكترونية أدوارا مهمة كونها آلية لحماية المستهلك، وكوسيلة من وسائل الإثبات والتحصيل الضريبي⁽⁵⁾، لكن تبقى هذه الأدوار مرهونة بوجود الفاتورة الإلكترونية وسلامة بياناتها، إذ أن بعض الهجمات السيبرانية قد تستهدفها مباشرة بأساليب متعددة بغرض إتلافها أو تحريفها، مما يمس مصداقتها ويقوض قدرتها على أداء وظائفها المرجوة.

ثانيا: أشكال الهجمات السيبرانية على الفاتورة الإلكترونية: يمكن للهجمات السيبرانية التي تستهدف أنظمة الفواتير الإلكترونية أن تتخذ العديد من الأشكال والصور، وفيما يلي عرض لأهمها وأبرزها:

1. **تهديد البنية التحتية السحابية:** تمكن الحوسبة السحابية المستفيدين من الوصول إلى خدماتها في أي مكان ومن أي جهاز إلكتروني مزود بإمكانية الاتصال بالإنترنت، وهذا بفضل بنية تحتية سحابية ضخمة تتكون من العديد من الموارد التقنية⁽⁶⁾، والفاتورة الإلكترونية هي ضمن هذه الخدمات التي توظف الحوسبة السحابية، على نطاق واسع، وبأساليب متعددة⁽⁷⁾. لذا تستهدف بعض الهجمات السيبرانية البنية التحتية السحابية للفاتورة الإلكترونية، الأمر الذي يترتب عنه آثار خطيرة على سلامتها

¹ (article 07, Directive 2014/55/UE du Parlement européen et du Conseil, du 16 avril 2014, relative à la facturation électronique dans le cadre des marchés publics Texte présentant de l'intérêt pour l'EEE JOUE L 133 du 6 mai 2014, JOUE L 133 du 6 mai 2014.

² (articles 04, 06, 07, Règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (Texte présentant de l'intérêt pour l'EEE), JOUE L 119 du 4.5.2016.

³ (article 08, Directive 2014/55/UE du Parlement européen et du Conseil, Ibid.

⁽⁴⁾ قانون رقم 07-18، سالف الذكر.

⁽⁵⁾ عائشة بوعزم، المرجع السابق، ص ص 05-09.

⁽⁶⁾ خالد بن نصر آل حيان، الحوسبة السحابية: "أساسيات ومبادئ وتطبيقات"، مركز البحوث والدراسات، معهد الإدارة العامة، المملكة العربية السعودية، 2019، ص 79.

⁷ (consult: Marjan GUSEV, Kiril KIROSKI, Sasko RISTOV, (An e-ordering and e-invoicing cloud solution), *Informatyka Ekonomiczna*, Issue 3(29), Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu, Wrocław, Poland, PP. 54-70. URL shortener: <https://2u.pw/A5eGl5h8>

- التشغيلية، وعلى خصائصها، سيما موثوقيتها واستمراريتها⁽¹⁾، ويمكن أن يؤثر بشكل خطير على أداء الخدمة، وعلى موثوقية البيانات، فضلا عما يكابده من خسائر مادية للمؤسسة.
2. **تهديدات واجهة التطبيقات:** تتخذ بعض الهجمات السيبرانية واجهة تطبيقات الفاتورة الإلكترونية كهدف لها، حيث أن هذه الواجهات تعمل على تفاعل المستخدم مع التطبيق، أو تسهل عملية الاتصال بين تطبيقات مستقلة تعمل بشكل منفصل⁽²⁾، والهجوم على آلية عملها، يمكن أن يحدث آثارا مدمرة، أبرزها تعطيل الخدمة⁽³⁾، مما يضعف من فعالية النظام ويزعزع الثقة، ويعرض المستخدم لمخاطر متعددة.
3. **تهديد سلاسل التوريد:** سلاسل التوريد هي تتبع لمسار المواد والمنتجات وإدارتها عبر مراحلها المختلفة بداية من صنعها وصولا إلى المستهلكها⁽⁴⁾، ونظرا لتعدد البروتوكولات والأنظمة المستخدمة في الفواتير الإلكترونية البينية فيها، فإنه من الممكن أن تتفاقم احتمالية الانتهاك بسبب تفاوت مستويات الأمان وتعدد الثغرات الأمنية بين أنظمة أطراف سلاسل التوريد.

المبحث الثاني:

دور الأمن السيبراني في حماية الفاتورة الإلكترونية.

تعتبر الفاتورة الإلكترونية سندا تجاريا حاملا لتفاصيل هامة، وتعد بنيته التحتية عمادها وأساس تشغيلها، وضمنة لتحقيق أهدافها، وعلى هذا، فإن مسألة معالجة قضايا تأمينها سيبرانيا تتطلب مناقشة اعتبارين اثنين: أولهما يتمثل في مختلف الآليات التي يوفرها الأمن السيبراني في حماية الفاتورة الإلكترونية (المطلب الأول)، أما ثانيهما فهو فحص لما يعيق هذه الآليات في إطار قيامها بهذا الدور (المطلب الثاني).

المطلب الأول: آليات الأمن السيبراني في حماية الفاتورة الإلكترونية.

تشكل الاستراتيجية الناجحة لقيام أمن سيبراني فعال في حماية الفاتورة الإلكترونية على نهج متكامل من الإجراءات والأساليب التي تتناسب وطبيعة المخاطر التي تتهددها، وتحتل المواجهة القانونية صدارة هذه الآليات

⁽¹⁾ (consulte Thibaut PROBST, Evaluation et analyse des mécanismes de sécurité des réseaux dans les infrastructures virtuelles de cloud computing, thèse de doctorat en Réseaux et télécommunications, Institut National Polytechnique de Toulouse, université fédérale de toulouse, 2015. P.12.

⁽²⁾ خالد بن ناصر آل حيان، المرجع نفسه، ص 328.

⁽³⁾ أبوها الجفر، ما هو أمان واجهة برمجة التطبيقات (API)؟ 7 ممارسات أمان واجهة برمجة التطبيقات، نشر بتاريخ 06 سبتمبر 2024، تم الاطلاع عليه في 06 نوفمبر 2024، متاح على الرابط:

<https://www.astera.com/ar/type/blog/api-security/>

⁽⁴⁾ مصطفى يوسف كافي، إدارة اللوجستيات: "الإمداد والتوزيع المادي الأخضر"، شركة دار الأكاديميون للنشر والتوزيع، الأردن، 2019، ص 34.

نظرا لما توفره من أساليب ردعية، وبما تضفيه من شرعية على كافة الإجراءات الأخرى (الفرع الأول)، كما أن طبيعة هذه الهجمات تفرض اعتماد أساليب تقنية وفنية مناسبة (الفرع الثاني).

الفرع الأول: الآليات القانونية.

تسمح مختلف التشريعات الموضوعية والإجرائية بردع العديد من صور التهديد التي يمكن أن يمس الفواتير الإلكترونية (أولا)، وذلك إلى جانب الهيكلية المؤسسية أو التنظيمية (ثانيا)، والتعاون القضائي الدولي الذي تفرضه الطبيعة السريعة والعابرة للحدود لهذه الانتهاكات (ثالثا).

أولا: تبني نصوص تشريعية لحماية الفاتورة الإلكترونية: يمكن النظر إلى التشريع كآلية لأمن الفاتورة الإلكترونية سيبرانيا من زاويتين هما:

1. **نطاق الحماية:** تنصب معظم النصوص التشريعية الرامية إلى تحقيق الأمن السيبراني بما في ذلك أمن الفاتورة الإلكترونية في محورين رئيسيين هما:

أ. **حماية البيانات:** تهدف التشريعات الرامية إلى تحقيق الأمن السيبراني للفاتورة الإلكترونية إلى تأمين البيانات عبر اتخاذ العديد من التدابير المتعلقة بكيفية جمع وتخزين ومعالجة البيانات لضمان أمنها وسريتها، ومنع كافة الاعتداءات التي يمكن أن تطالها، بما في ذلك إتلافها أو التلاعب بها أو كشفها⁽¹⁾.

ب. **حماية البنية التحتية:** تضع التشريعات الهادفة إلى تحقيق الأمن السيبراني ضمن أولوياتها أيضا، حماية البنية التحتية لأنظمة الفواتير الإلكترونية، كحماية البنية التحتية السيبرانية على العموم⁽²⁾، وحماية المواقع والتطبيقات والبرامج والمعدات المتعلقة بنظام الفاتورة الإلكترونية⁽³⁾.

2. **قواعد الحماية:** تنقسم معظم النصوص والقواعد القانونية المتعلقة بالأمن السيبراني بما في ذلك أمن الفاتورة الإلكترونية إلى 03 مجموعات أساسية متمثلة فيما يلي⁽⁴⁾:

• **نصوص وقواعد تنظم المبادئ الأساسية للأمن السيبراني، وتحدد مجموع الالتزامات التي تقع على عاتق الجهات ذات الصلة في مجال تحقيق بيئة سيبرانية آمنة⁽⁵⁾.**

(1) ومثالها: قانون رقم 04-15، المؤرخ في 10 نوفمبر 2004، يعدل ويتم الأمر رقم 66-156 المؤرخ في 08 يونيو 1966، المتضمن قانون العقوبات، ج.ر عدد 71، صادرة في 10 نوفمبر 2004، و قانون رقم 18-07، سالف الذكر.

(2) راجع مثلا: المادة 394 مكرر/3، الأمر رقم 66-156، مؤرخ في 08 يونيو 1966، المتضمن قانون العقوبات، المعدل والمتمم. والمادة 177 و 179، من القانون 18-04، سالف الذكر.

(3) راجع: المادة 12، قانون 04-15، سالف الذكر.

(4) راجع: أيمن عبد الله فكري، الجرائم المعلوماتية: "دراسة مقارنة في التشريعات العربية والأجنبية"، مكتبة القانون والاقتصاد، المملكة العربية السعودية، 2014، ص 869.

(5) أبرزها: المواد من 38 إلى 41، قانون رقم 18-07، سالف الذكر، والمواد من 10 إلى 12، قانون 09-04، سالف الذكر، والمواد من 53 إلى 62، قانون 15-04، سالف الذكر.

- نصوص تشمل القواعد التنظيمية والإجرائية ومختلف المعايير المتعلقة بالأمن السيبراني، لاسيما أمن الفاتورة الإلكترونية، فضلا عن تعيين وتنظيم الجهات الرقابية، والقواعد الإجرائية المتعلقة بتطبيق القواعد الموضوعية⁽¹⁾.
- نصوص تتعلق بالقواعد الموضوعية التي تركز الحماية المدنية والجنائية، وبالأخص تلك المتعلقة بتحديد السلوكيات محل التجريم والعقوبات المقررة لها، والتي تحدد نطاق المسؤولية والمساءلة المترتبة عنها⁽²⁾.
- ثانيا: استحداث إطار مؤسسي لحماية الفاتورة الإلكترونية: تعني الهيكلية المؤسسية إنشاء جهات متخصصة بتطبيق معايير الأمن السيبراني الخاصة بالفاتورة الإلكترونية، ومكافحة الجرائم الإلكترونية، وتشكل هذه الهياكل محورا أساسيا في حماية الأنظمة والبنية التحتية، والتصدي للتهديدات السيبرانية، مع الاضطلاع بأدوار توعوية وتعزيز التعاون الدولي، ومن أمثلة هذه الهياكل: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها⁽³⁾، السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي⁽⁴⁾.
- ثالثا: التعاون القضائي الدولي لحماية الفاتورة الإلكترونية: لا يعرف الفضاء السيبراني وما يرتكب فيه من انتهاكات وجرائم متعلقة بالفاتورة الإلكترونية حدا سياديا للدول، فهي جرائم عابرة للحدود الإقليمية التقليدية، الأمر الذي يثير العديد من التحديات الأمنية، لذا فإن التنسيق الدولي يعتبر من أهم السبل القانونية لمواجهتها، وذلك عبر آليات التعاون القضائي الدولي كالمساعدة في إطار البحث والتحري المتعلقة بهذه الجرائم وكشف منفذها⁽⁵⁾.

الفرع الثاني: الآليات التقنية والفنية.

- تقرض الطبيعة التقنية للفاتورة الإلكترونية وطبيعة الهجمات التي تتهددها، اللجوء إلى أساليب تقنية متنوعة من أجل التحقق من هوية المستخدمين، ومن موثوقية الفواتير ذاتها (أولا)، ومن أجل ضمان أمن أنظمتها ومضامينها واستدامة الاستقرار الأمني فيها (ثانيا).
- أولا: آليات التحقق: يوفر الأمن السيبراني آليات مختلفة للتحقق من هوية المستخدمين، وضمن موثوقية الفواتير الإلكترونية، ومن أبرز هذه الآليات نجد:

1. التحقق الثنائي: نظرا لإمكانية تخمين كلمات المرور من قبل منفذي الهجمات السيبرانية، فإنه من الواجب أن تكون هناك حماية ثنائية لتعزيز التحقق من الهوية، وذلك من خلال مرحلتين مختلفتين: أولهما هو إدخال

(1) أنظر فيها: المواد من 05 إلى 09، قانون رقم 09-04، والمواد من 10 إلى 14، قانون 04-15.

(2) أبرزها: المواد من 394 مكرر إلى 394 مكرر 7، أمر رقم 66-156.

(3) راجع في ذلك: المواد 13 و 14، قانون رقم 04-09.

(4) راجع: المواد من 22 إلى 31، قانون رقم 07-18.

(5) راجع في ذلك: المادة 16، قانون رقم 04-09، سالف الذكر.

كلمة المرور أو أي رقم سري يعرفه المستخدم، وثانيهما هي إدخال رمز لمرة واحدة يتم إرساله من خلال آليات اتصال مختلفة، كرقم الهاتف أو رسالة على البريد الإلكتروني⁽¹⁾.

2. **التوقيع الإلكتروني:** هو آلية إلكترونية للتوثيق، ترتبط فيها البيانات ببعضها البعض منطقياً⁽²⁾، ودورها في الفاتورة الإلكترونية هو ضمان موثوقيتها، وذلك عبر إنشاء قيمة رقمية مدمجة يطلق عليها اسم "هاش"، وفي حالة وجود أي شكل من أشكال التلاعب في الفاتورة الإلكترونية فإن التوقيع الإلكتروني لن يكون صحيحاً، لأن قيمة "الهاش" حينها لن تكون مطابقة لقيمتها حال إنشائها⁽³⁾.

ثانياً: **آليات حماية النظام:** حماية الأنظمة والبيانات قد يتطلب تقنيات كثيرة، وفيما يلي عرض لأهمها وأكثرها شيوعاً.

1. **نظام التشفير:** نظام التشفير عموماً هو وسيلة لتحويل البيانات إلى صيغة غير قابلة للفهم وذلك عبر توظيف بعض الآليات الخاصة، بهدف حمايتها من الوصول غير المصرح به⁽⁴⁾، وتستعمل من أجل ذلك العديد من التقنيات والأنظمة، وتبرز تقنية التشفير بالمفتاح الخاص كأحد التقنية التي يتم توظيفها في حماية بيانات الفاتورة الإلكترونية حال تداولها أو تخزينها، حيث تشفر بيانات الفاتورة الإلكترونية بمفتاح عام يمتلكه المرسل، ومفتاح خاص يتحده لمتلقي بيانات الفاتورة الإلكترونية لفك شفرتها⁽⁵⁾، وقد اعتمد المشرع الجزائري هذا النظام في التشفير ضمن أحكام التوقيع والتصديق الإلكترونيين⁽⁶⁾.

2. **الجدران النارية:** هي بمثابة جدار عازل يفصل بين الشبكة الداخلية للمؤسسة أو النظام وبين الشبكة الخارجية كالإنترنت، ويحول دونها ودون التهديدات التي يمكن أن تأتي من هذه الأخيرة⁽⁷⁾، فهي آلية حماية لمختلف نظم الفواتير الإلكترونية من أي تهديد خارجي.

3. **التحديثات الأمنية:** تعتبر التحديثات الأمنية من بين العناصر الأساسية لتحقيق الأمن السيبراني للفاتورة الإلكترونية. إذ هدفها الرئيس هو معالجة وسد الفراغات الأمنية التي قد تنتج عن خلل في مختلف الأنظمة

⁽¹⁾ (Sebastian FLORCZAK , Adrian JASIAK, Izabela SZCZYGIEL, **(Two-factor authentication (2FA) comparison of methods and applications)**, *Advances in Web Development Journal*, Vol. 1, N.03, Patryk Organiściak, Rzeszów University of Technology, 2023, P.27. URL shortener: <https://2u.pw/Qwk3c3tb>

⁽²⁾ المادة 1/02، قانون رقم 15-04، سالف الذكر.

⁽³⁾ أنظر: مصطفى يوسف كافي، النقود والبنوك الإلكترونية في ظل التقنيات الحديثة، دار مؤسسة رسلان للطباعة والنشر والتوزيع، سوريا، 2011، ص 200.

⁽⁴⁾ عبد الصبور عبد القوي علي المصري، التجارة الإلكترونية والقانون، دار العلوم للنشر والتوزيع، القاهرة، 2010، ص 115.

⁽⁵⁾ راجع: عصمت عبد المجيد بكر، دور التقنيات العلمية في تطور العقد، دار الكتب العلمية، لبنان، 2015، ص 432.

⁽⁶⁾ راجع: المادة 8/02-9، قانون 15-04، سالف الذكر.

⁽⁷⁾ حسن طاهر داود، أمن شبكات المعلومات، مركز البحوث، معهد الإدارة العامة، المملكة العربية السعودية، 2004، ص 260.

والبرامج، فهي ضرورية للحفاظ على سلامة الأنظمة⁽¹⁾، إذ أن عدم التعامل معها بحسم يمكن أن يعرض أنظمة الفواتير الإلكترونية للعديد من المخاطر السيبرانية.

المطلب الثاني: تحديات الأمن السيبراني في حماية الفاتورة الإلكترونية.

يعتبر الأمن السيبراني من الآليات الأكثر فعالية في مواجهة كل الهجمات والتهديدات التي تستهدف نظام الفاتورة الإلكترونية، إلا أن ثمة جملة من العقبات والتحديات المختلفة التي تواجهها، والتي قد تسهم في تقليص فعاليتها، ولاسيما تلك العقبات والإشكالية القانونية (الفرع الأول)، فضلا عن بعض التحديات التقنية والفنية التي تثيرها أنظمة التأمين السيبراني (الفرع الثاني).

الفرع الأول: التحديات القانونية.

يواجه الأمن السيبراني للفاتورة الإلكترونية العديد من التحديات القانونية نظرا لطبيعة الانتهاكات التي تواجهها والبيئة السيبرانية المعقدة، إذ تؤثر بشكل واضح على مدى قدرة النصوص العقابية على الردع، وكأهم هذه العقبات والتحديات نجد: إشكاليات التجريم والعقاب (أولا)، وإشكالية إنفاذ القوانين (ثانيا).

أولا: إشكاليات التجريم والعقاب: يمكن أن نتناول إشكاليات التجريم والعقاب من خلال العناصر التالية:

1. **إشكاليات الركن الشرعي:** تكمن الإشكاليات التي تثار في هذا الركن ضمن إطار الفاتورة الإلكترونية فيما يلي:

أ. **عدم التجريم:** لا يمكن متابعة ومعاينة الأشخاص الذين يرتكبون أفعالا ضارة على الفضاء السيبراني أو من خلاله إلا إذا قامت السلطة التشريعية بسن قوانين خاصة تجرم هذه الأفعال، وهذا استنادا إلى مبدأ الشرعية الجنائية القاضي بآلا جريمة ولا عقوبة بدون نص واضح⁽²⁾، وأمام الفراغ التشريعي الذي يشوب قوانين الجريمة السيبرانية ولاسيما تلك المتعلقة بالانتهاكات الماسة بالفاتورة الإلكترونية، فإن تعزيز حمايتها وحماية ضحاياها جنائيا ضد مختلف المخاطر السيبرانية يبقى أمرا معقدا.

ب. **ازدواجية نص التجريم:** ففي ظل القانون الأردني للمعاملات الإلكترونية رقم 85 -الملغى- نجد أن المشرع الأردني قد نص في المادة 38 منه على المعاقبة على الأفعال التي تشكل جريمة في التشريع المعمول به بعقوبة من 03 أشهر إلى سنة، وبغرامة من 3000 إلى 10000 دينار، ثم أعطى الأولوية للنص المشدد سواء في المادة 38 أو في نص التجريم في التشريع التقليدي المعمول به⁽³⁾، وفي حالة تزوير أو إتلاف المحررات

(1) مانيش أغروال، أليكس كامبو، إيريك بيرس، أمن المعلومات وإدارة مخاطر تقنية المعلومات، ترجمة: "جعفر بن أحمد العلوان"، مركز البحوث والدراسات، معهد الإدارة العامة، المملكة العربية السعودية، 2018، ص 492.

(2) عبد العال الديربي، محمد صادق إسماعيل، الجرائم الإلكترونية: "دراسة قانونية قضائية مقارنة"، المركز القومي للإصدارات القانونية، القاهرة، 2012، ص 148.

(3) أيمن عبد الله فكري، المرجع السابق، ص 909.

التجارية بما في ذلك الفاتورة، نجد ازدواجه في التجريم؛ تجريم بمقتضى قانون المعاملات الإلكترونية، وتجريم بمقتضى القانون التقليدي ساري المفعول.

2. صعوبة تحديد أركان للجريمة الأخرى:

إلى جانب الركن الشرعي، تثار العديد من الإشكاليات في تحديد الأركان الأخرى لجرائم الاعتداء على الفاتورة الإلكترونية، ويمكن أن نسوق ذلك على النحو الآتي:

أ. **الركن المادي:** تتحدد الإشكاليات المثارة في هذا الإطار من خلال العناصر التالية:

- **السلوك الإجرامي:** يختلف السلوك الإجرامي في الجرائم التقليدية عن نظيرتها الإلكترونية، إذ يتطلب في الأخيرة نوعا من الاحترافية التقنية، فيكون عالما ومدركا لبعض التقنيات أو الفنيات الإلكترونية⁽¹⁾، فلا يمكن تصور هجوم إلكتروني -فيروسي مثلا- على الفاتورة الإلكترونية من هاو أم عديم الخبرة، علاوة على كون السلوك الإجرامي فيها غير مادي⁽²⁾، مما يعقد من عملية تحديده.
- **النتيجة الإجرامية:** يشكل تحديد النتيجة الإجرامية في الجرائم السيبرانية تحديا كبيرا، ذلك أن الجريمة السيبرانية تقع في بيئة رقمية، مما يصعب الفصل بين السلوك الإجرامي السيبراني وتأثيراته على الواقع المادي، وبالتالي يؤثر على مدى اكتمال عناصر الجريمة في العالم السيبراني، وتتجلى هذه المعضلة بشكل واضح في الجرائم الماسة بالفاتورة الإلكترونية، حيث يكون السلوك الإجرامي في هذه الحالة تاما في بيئة سيبرانية، إلا أن نتائجها قد لا تتجلى إلا في الفضاء المادي؛
- **العلاقة السببية:** يكتمل عنصر السلوك الإجرامي والعلاقة السببية في العالم الافتراضي، فيما تكتمل النتيجة الإجرامية في العالم المادي، الأمر الذي يصعب عملية ربط النتيجة بالسلوك الإجرامي بشكل مباشر، وعلاوة على ذلك، تقوم الجريمة السيبرانية على فكرة النتيجة المحتملة⁽³⁾، وهذه الفكرة فيها تباين فقهي كبير، وتناقض في أحكام القضاء بشأنها⁽⁴⁾، الأمر الذي يعقد من مسألة وضوح العلاقة السببية في غالبية الجرائم السيبرانية بما في ذلك جرائم الفاتورة الإلكترونية.

ب. **الركن المعنوي:** تحدث العديد من الإشكاليات القانونية في تحديد القصد الجنائي لجرائم الفاتورة الإلكترونية، شأنها شأن بقية الجرائم السيبرانية الأخرى، فالفقه يتجه إلى القول بأصلية القصد الجنائي العمدي في الجرائم السيبرانية على العموم، ويرى بعض الفقه أيضا أن الخطأ غير العمدي يمكن أن يكون أساسا للقصد الجنائي

(1) إبراهيم محمد بن حمود الزندان، الجرائم الإلكترونية من منظور الشريعة الإسلامية وأحكامها في القانون القطري والقانون اليمني: "دراسة مقارنة"، رسالة ماجستير، قسم الدراسات الإسلامية، جامعة فطاني، 2018، ص ص 30-31.

(2) عماد مفلح الحسبان، عز الدين أحمد النعيمي، عدنان محمد الضمور، باير طالب الخزاعلة، الجرائم المستحدثة: "المعلوماتية. الإلكترونية. السيبرانية"، دار الخليج للنشر والتوزيع، الأردن، 2024، ص 191.

(3) إبراهيم محمد بن حمود الزندان، المرجع نفسه، ص ص 31-32.

(4) ساهر إبراهيم الوليد، (النتيجة المحتملة وموقعها من الإثم الجنائي: "دراسة مقارنة")، مجلة البحوث القانونية والاقتصادية، المجلد 09، العدد 68، كلية الحقوق، جامعة المنصورة، مصر، أبريل 2019، ص 247 (المقدمة).

عند تحقق الجريمة بغير قصد، فيما أنتقد هذا الرأي عندما يتعلق الأمر بالجرائم الإلكترونية، إلا إذا قامت المسؤولية التقصيرية، أو افضى نشاط الفرد إلى وقوع جريمة دون قصد منه⁽¹⁾.

ويثير هذا الوضع العديد من الإشكاليات القانونية، فافتراض القصد الجنائي العمدي وجعله أصلاً، يمكن أن يفضي إلى الإخلال بمقتضيات العدالة، ولا سيما مبدأ البراءة الذي يقضي ببراءة المتهم حتى تثبت إدانته بأدلة تقدمها جهة الادعاء، وافتراض النية الإجرامية هو عكس ما يقره المبدأ، ووضع المتهم في دائرة افتراض الإدانة التي قد لا يتمكن من إثبات عكسها، علاوة على ذلك، يمكن أيضاً لقيام المسؤولية الجنائية عن الخطأ غير العمدي القائم على المسؤولية التقصيرية أن يثير إشكاليات عدة، أبرزها عدم القدرة على إثبات المسؤولية التقصيرية في كل الأحوال نظراً للطبيعة المعقدة للجرائم الإلكترونية.

تثار إشكالية أخرى في الجرائم المتعلقة بالفواتير الإلكترونية عندما يتم تأسيس المتابعة الجنائية فيها بناء على القوانين التقليدية، فجريمة تزوير المحررات الرسمية أو العرفية تقتضي قصداً جنائياً مباشراً، بعنصري العلم والإرادة، مع قصد جنائي خاص وهو استعمال المحرر فيما زور لأجله⁽²⁾، وهذا الوضع يثير عدة إشكاليات في التلاعب ببيانات الفواتير الإلكترونية، ذلك أن الطبيعة التقنية للفواتير الإلكترونية وأنظمتها قد لا تتمكن من تحديد المسؤول المباشر عن هذا التلاعب، وفي حالة إسناد المسؤولية لطرف، فإنه يعقّبها إشكالية إثبات النية الإجرامية.

ثانياً: إشكاليات التنفيذ.

1. إشكالية الاختصاص القضائي: تعد الجرائم السيبرانية جرائم عابرة للحدود، بفعل الترابط الحاصل بين المجتمعات في الفضاء السيبراني خارج نطاق السيادة الوطنية، مما يثير تحديات قانونية عديدة، أبرزها مسألة الاختصاص القضائي⁽³⁾، التي تثار في الجرائم المتعلقة بالفواتير الإلكترونية شأنها شأن سائر الجرائم السيبرانية الأخرى، نظراً لصعوبة تكييفها ضمن القواعد الإجرائية التقليدية، مما يستدعي حلاً قانونية أكثر تناسبا مع الطبيعة المعقدة لهذه الجرائم⁽⁴⁾.

(1) إبراهيم محمد بن حمود الزنداني، المرجع نفسه، ص 35.

(2) محمد أمين صبحي، (الطبيعة القانونية لجريمة التزوير في المحررات)، مجلة القانون العام الجزائري والمقارن، المجلد 03، العدد 02، جامعة جيلالي اليابس، سيدي بلعباس، جوان 2017، ص ص 71-72.

(3) ميرفت محمد حبابية، مكافحة الجريمة الإلكترونية: "دراسة مقارنة في التشريع الجزائري والفلسطيني"، دار اليازوري العلمية للنشر والتوزيع، الأردن، 2023، ص 41.

(4) خالد حسن أحمد لطفي، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2019، ص 83.

2. **إشكالية الإثبات:** تعتبر مسألة الإثبات من أبرز التحديات التي تواجه الجهود الرامية إلى مكافحة الجرائم الإلكترونية، وذلك نظرا لتعقيد البيئة السيبرانية، وتطور أساليب التخفي، حيث يصعب الكشف عن الجناة أو ربطهم بالأفعال المجرمة، نظرا للإشكاليات التي تواجه الأدلة الرقمية، إذ إنها قد تكون غير مرئية أو يصعب الوصول إليها، ويمكن أن يتم محوها أو تدميرها بسهولة من قبل الجناة الذين يتمتعون بقدرات تقنية متقدمة، فضلا عن صعوبة جمعها وتحليلها بسبب السرية العالية التي تتمتع بها بيئة الإنترنت، والتي تمنع الكشف المبكر عن تفاصيل الجريمة⁽¹⁾.

الفرع الثاني: التحديات التقنية والفنية.

تبرز التحديات التقنية والفنية كأحدى العقبات التي تواجه فعالية الأمن السيبراني للفاتورة الإلكترونية، إذ يمكن في هذا الإطار ألا تتوفر الأساليب التقنية اللازمة لتوفير بيئة آمنة، وقد يسمح الطابع الإجرائي المعقد للأمن السيبراني بالتأثير سلبا على نظام الفاتورة الإلكترونية، ومن أبرز التحديات في هذا السياق نجد:

1. **التكلفة المرتفعة:** تعود التكلفة المرتفعة للأمن السيبراني في نظام الفاتورة الإلكترونية إلى المتطلبات التي يتعين توفيرها في هذا المجال، وإلى توسع نطاق هذه الحماية، فتأمين الفاتورة الإلكترونية يقتضي توفير التكنولوجيا المناسبة لذلك، فضلا عن تكلفة الصيانة والمراقبة الدورية، بالإضافة إلى توفير العنصر البشري وتدريبه بشكل دوري، وتكاليف التنسيق والامتثال لسياسات الأمن السيبراني التي تقرها الدولة.

تشير الإحصائيات العامة إلى أن حجم الإنفاق على الأمن السيبراني في الشرق الأوسط قد يصل مع حلول عام 2026 إلى 35.4 مليار دولار⁽²⁾، كما أوضح **سعد القرني** الرئيس التنفيذي للأمن السيبراني في شركة **ملاء المالية** أن حجم التكلفة اللازمة لرفع كفاءة الأمن السيبراني لشركة مالية ناشئة قد تتراوح ما بين 03 إلى 05 بالمئة من رأس المال، تبعا لحجم الأصول والبيانات المحمية⁽³⁾.

ومع أن هذه الإحصائيات لا تشير مباشرة إلى حجم الإنفاق على أمن الفاتورة الإلكترونية، إلا أن تزايد التوجه نحو تبنيها، يوحي بأن تكلفة تأمينها لن تكون خفيفة الوطأة على الدول والشركات، لأنها لا تختلف كثيرا عن تأمين الأصول والبيانات الأخرى للشركات أو الدول، وكل ذلك يزيد من حجم الإنفاق مما قد يفضي إلى وجود ثغرات أمنية كبيرة نتيجة محاولة تقليص حجم ميزانية الأمن السيبراني للفواتير الإلكترونية.

(¹) البركة الطيبي، (إشكالية الإثبات في الجرائم الإلكترونية)، مجلة آفاق علمية، المجلد 11، العدد 01، جامعة تامنغست، الجزائر، أبريل 2019، ص 280.

(²) الأمن السيبراني يستحوذ على 3.3 مليارات دولار من انفاق الشرق الأوسط عام 2024، نشر بتاريخ 27 مارس 2024، تم الاطلاع عليه في 15 نوفمبر 2024، متاح على الرابط: <https://linksshortcut.com/NByiU>

(³) نقلا عن: "ملاء المالية": تكلفة الأمن السيبراني لشركة ناشئة تتراوح بين 3 و5% من رأس المال، نشر بتاريخ 02 أكتوبر 2024، تم الاطلاع عليه في 15 نوفمبر 2024، متاح على الرابط: <https://2u.pw/Dfn0SSUL>

2. **نقص الخبرة الفنية:** يواجه أمن نظام الفاتورة الإلكترونية عقبة أخرى تتمثل في ضعف الخبرة ونقص الخبراء في مجال الأمن السيبراني، إذ تشير الأبحاث والدراسات إلى أن ثمة فراغ ونقص عالمي كبير في عدد خبراء الأمن السيبراني، علاوة على أن ثلث هؤلاء يتركون وظائفهم في هذا المجال لأسباب مختلفة، فضلا عن أن 30 بالمئة منهم يخططون لذلك على مدى سنة أو سنتين⁽¹⁾.

3. **التأثير على الأداء:** قد تقضي بعض تقنيات وإجراءات الأمن السيبراني إلى تحديات تشغيلية كبيرة، كتعطيل أو بطء أداء أنظمة الفواتير الإلكترونية، ويعود ذلك إلى العديد من الأسباب، فقد تعود إلى وجود خلل في عنصر الأمان ذاته، ومثال ذلك ما حدث بالتحديث الذي أنزلته شركة "كراود سترايك" والذي أفضى إلى اضطرابات تشغيلية كبيرة في شركات الطيران والمؤسسات المصرفية وخدمات الرعاية الصحية⁽²⁾، أو إلى طبيعة الإجراء نفسه، كأعمال التحديثات وإجراءات التشفير وبرامج مكافحة الفيروسات التي تبطئ من أداء الأنظمة.

خاتمة:

يتبين من خلال هذه الدراسة أن فعالية الأمن السيبراني يمثل عاملا أساسيا في حماية الفواتير الإلكترونية من التهديدات السيبرانية المزيدة، حيث يضمن سلامة البيانات واستمرار العمليات، وقد توصلنا إلى النتائج التالية:

- الأمن السيبراني يمثل إطارا استراتيجيا لحماية الفواتير الإلكترونية من التهديدات السيبرانية، وذلك نظرا لتطافر مختلف الأساليب والآليات التقنية والتشريعية والتنظيمية.
- الفاتورة الإلكترونية تستند أساسا على الفضاء السيبراني، وترتبط به عضويا، مما يجعل أي تهديد سيبراني موجه إليها بمثابة تهديد للنظام المالي والمعاملات التجارية.
- يتضح من التشريعات المقارنة (التشريع الأردني والجزائري) أن هناك تفاوت في تحديد مكونات الأمن السيبراني وعناصره الأساسية، مما يؤثر على الحماية القانونية المتعلقة بالفواتير الإلكترونية.
- يفقر الإطار القانوني الجزائري الحالي إلى تشريعات خاصة تنظم الفواتير الإلكترونية بشكل دقيق، فضلا عن غياب نصوص صريحة تحدد عناصر الأمن السيبراني لها.
- تعقيد الجرائم السيبرانية التي تهدد أمن الفواتير الإلكترونية يثير العديد من الإشكاليات التشريعية ضمن القواعد القانونية التقليدية مما يجعل أمر مواجهتها صعبا للغاية.

⁽¹⁾ محمد سناجلة، أزمة الأمن السيبراني تتفاقم في العالم وتزداد سوءا بسبب مشكلة جديدة، نشر بتاريخ 29 جوان 2022، تم الاطلاع

عليه في 15 نوفمبر 2024، متاح على الرابط: <https://2u.pw/i9oismvZ>

⁽²⁾ "أكبر عطل في تاريخ تكنولوجيا المعلومات" .. دروس وتحذيرات للمستقبل، نشر بتاريخ 20 يوليو 2024، تم الاطلاع عليه في

16 نوفمبر 2024، متاح على الرابط: <https://www.masrimes.com/413190>

- نقص الكوادر البشرية المتخصصة في مجال حماية الأمن السيبراني للفواتير الإلكترونية، وتعد أنظمة الحماية التي تزيد من احتمالية التهاون في تطبيقها، أو تأثر على المنظمات التي تحميها. ومن أجل ذلك نقترح ما يلي:
- ضرورة وضع تشريع خاص ينظم أحكام الفواتير الإلكترونية في الجزائر، وإنشاء منظومة لها تمكن الجهات الرقابة من فرض رقابتها على كافة الشروط والمعايير المطلوبة إلكترونياً.
- سن تشريعات خاصة لحماية الفاتورة الإلكترونية سيبرانيا تتناسب مع طبيعة الانتهاكات والجرائم التي قد تتعرض لها، مع التزام الدقة في بيان صورها وأركانها، وبيان محكم للعقوبات المقررة لكل جريمة بشكل مستقل، مع ضمان انسجامها مع مبادئ العدالة الجنائية وأسس حقوق وحريات الأفراد من جهة، وبينها وبين النصوص العقابية الأخرى لتفادي الوقوع في ازدواجية التجريم من جهة ثانية.
- استحداث إطار قانوني واضح لطرق وآليات التحقيق الجنائي في جرائم الفاتورة الإلكترونية ضمن قانون إجرائي متعلق بكافة الجرائم السيبرانية، وبيان سليم للإجراءات وطرق البحث والاستدلال، ومعايير قبولها أمام الجهات القضائية، مع توفير الآليات الفنية والتقنية لتحقيق ذلك، بالإضافة إلى تكوين جهات إنفاذ القانون للتعامل وفهم وتفسير الأدلة الرقمية.
- وضع المعايير الفنية والتقنية للأمن السيبراني، وإلزام الشركات وأصحاب المصلحة بنظمها من خلال إصدار قرارات وتنظيمات تلزم الأعوان الاقتصاديين والتجار الإلكترونيين باستخدامها والالتزام بها حال إنشاء أو تبادل الفواتير الإلكترونية مع مراعاة توحيد هذه المعايير من خلال إنشاء منظومة موحدة للفاتورة الإلكترونية.
- إنشاء جهات رقابية تعنى بالتدقيق والفحص الرقمي لأنظمة الفواتير الإلكترونية وذلك من خلال إنشاء مفتشيات أو مصالح على مستوى إدارات الضرائب والجمارك والتي تقوم برقابة دورية على المؤسسات للتحقق من توافق أنظمتها للمعايير المطلوبة.
- دعم التعاون الدولي لمكافحة الجرائم المتعلقة بالفواتير الإلكترونية من خلال آليات التعاون القضائي، أو من خلال أقطاب أو هيكل متخصصة لتبادل المعلومات والبيانات بشكل سريع عبر المعاهدات والاتفاقيات الثنائية أو الجماعية.
- التركيز على العنصر البشري، من خلال التدريبات الدورية والتأطيرات النظرية لتقليص حجم الهجمات التي يتسبب فيها العنصر البشري (الموظفين)، وذلك من خلال إنشاء معاهد متخصصة في مجال الأمن السيبراني على المستوى الوطني، والتعاون بين الجامعات والمؤسسات البحثية.

قائمة المراجع والمصادر:

أولاً: المصادر باللغة العربية:

1. الكتب:

1. أيمن عبد الله فكري، الجرائم المعلوماتية: "دراسة مقارنة في التشريعات العربية والأجنبية"، مكتبة القانون والاقتصاد، المملكة العربية السعودية، 2014.
2. حسن طاهر داود، أمن شبكات المعلومات، مركز البحوث، معهد الإدارة العامة، المملكة العربية السعودية، 2004.
3. خالد بن نصر آل حيان، الحوسبة السحابية: "أساسيات ومبادئ وتطبيقات"، مركز البحوث والدراسات، معهد الإدارة العامة، المملكة العربية السعودية، 2019.
4. خالد حسن أحمد لطفي، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2019.
5. عبد الصبور عبد القوي علي المصري، التجارة الإلكترونية والقانون، دار العلوم للنشر والتوزيع، القاهرة، 2010.
6. عبد العال الديربي، محمد صادق إسماعيل، الجرائم الإلكترونية: "دراسة قانونية قضائية مقارنة"، المركز القومي للإصدارات القانونية، القاهرة، 2012.
7. عصمت عبد المجيد بكر، دور التقنيات العلمية في تطور العقد، دار الكتب العلمية، لبنان، 2015.
8. فارس عقيل علي الدويري، البيانات الضخمة ودورها في الحد من الجرائم الإلكترونية في ظل استراتيجية الأمن السيبراني، دار الخليج للنشر والتوزيع، الأردن، 2024.
9. مانيش أغروال، أليكس كامبو، إيريك بيرس، أمن المعلومات وإدارة مخاطر تقنية المعلومات، ترجمة: "جعفر بن أحمد العلوان"، مركز البحوث والدراسات، معهد الإدارة العامة، المملكة العربية السعودية، 2018.
10. مصطفى يوسف كافي، إدارة اللوجستيات: "الإمداد والتوزيع المادي الأخضر"، شركة دار الأكاديميون للنشر والتوزيع، الأردن، 2019.
11. مصطفى يوسف كافي، النقود والبنوك الإلكترونية في ظل التقنيات الحديثة، دار مؤسسة رسلان للطباعة والنشر والتوزيع، سوريا، 2011.
12. منتدى أسبار الدولي، معجم المصطلحات الأساسية للدراسات المستقبلية، منتدى أسبار الدولي، الرياض، 2019.
13. منى الأشقر جبور، محمود عارف جبور، الأمن السيبراني والأمن القومي العربي: "واقع ومتطلبات وتحديات"، الفصل الحادي عشر من مؤلف جماعي: الأمن القومي العربي وتحديات الأمن الإقليمي"، المركز العربي للأبحاث ودراسة السياسات، قطر/لبنان، 2023.

14. ميرفت محمد حبابية، مكافحة الجريمة الإلكترونية: "دراسة مقارنة في التشريع الجزائري والفلسطيني"، دار اليازوري العلمية للنشر والتوزيع، الأردن، 2023.

II. الرسائل الجامعية:

أ. رسائل الدكتوراه:

عزيزة رابحي، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة دكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2017-2018.

ب. رسائل الماجستير:

إبراهيم محمد بن حمود الزنداني، الجرائم الإلكترونية من منظور الشريعة الإسلامية وأحكامها في القانون القطري والقانون اليمني: "دراسة مقارنة"، رسالة ماجستير، قسم الدراسات الإسلامية، جامعة فطاني، 2018.

III. المقالات:

1. البركة الطيبي، (إشكالية الإثبات في الجرائم الإلكترونية)، مجلة آفاق علمية، المجلد 11، العدد 01، جامعة تامنغست، الجزائر، أبريل 2019، ص ص 266-284.

2. سامي محمد بونيف، (دور الاستراتيجيات الاستباقية في مواجهة الهجمات السيبرانية: "الردع السيبراني أنموذجاً")، المجلة الجزائرية للحقوق والعلوم السياسية، المجلد 04، العدد 01، كلية الحقوق، جامعة أحمد بن يحيى الونشريسي، تيسمسيلت، الجزائر، نوفمبر 2019، ص ص 121-135.

3. ساهر إبراهيم الوليد، (النتيجة المحتملة وموقعها من الإثم الجنائي: "دراسة مقارنة")، مجلة البحوث القانونية والاقتصادية، المجلد 09، العدد 68، كلية الحقوق، جامعة المنصورة، مصر، أبريل 2019، ص ص 247-304.

4. سمير بارة، (الأمن السيبراني "cyber Security" في الجزائر: "السياسات والمؤسسات")، المجلة الجزائرية للأمن الإنساني، المجلد 02، العدد 02، جامعة باتنة 1 الحاج لخضر، الجزائر، جويلية 2017، ص ص 255-280.

5. عائشة بوعزم، (فعالية الفاتورة في إطار ممارسات التجارة الإلكترونية على ضوء التشريع الجزائري)، مجلة القانون العقاري والبيئة، المجلد 09، العدد 02، كلية الحقوق والعلوم السياسية، جامعة ابن باديس، مستغانم، جوان 2021، ص ص 128-145.

6. عبد الوهاب عبد الكريم محمد المبارك، (إشكالية المسؤولية القانونية عن جرائم النصب والاحتيال الإلكتروني الواقعة على عملاء البنوك)، المجلة القانونية، المجلد 15، العدد 08، كلية الحقوق، فرع الخرطوم، جامعة القاهرة، مصر، فبراير 2023، ص ص 1919-1948.

7. محمد أمين صبحي، (الطبيعة القانونية لجريمة التزوير في المحررات)، مجلة القانون العام الجزائري والمقارن، المجلد 03، العدد 02، جامعة جيلالي اليابس، سيدي بلعباس، جوان 2017، ص ص 49-73.

8. محمد منصوري، العيد خيراني، (دور تبني استعمال الفاتورة الإلكترونية في تفعيل التحقيق المصوب في ظل توجه الإدارة الضريبية نحو الرقمنة: "دراسة استطلاعية")، مجلة أبحاث اقتصادية معاصرة، المجلد 07، العدد 01، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة عمار ثليجي، الأغواط، الجزائر، أبريل 2024، ص ص 313-332.

9. نؤارة حسين، (الفوترة الإلكترونية آلية لتنشيط الاستثمارات)، مجلة الدراسات القانونية والسياسية، المجلد 05، العدد 02، جامعة عمار ثليجي، الأغواط، الجزائر، جوان 2019، ص ص 126-139.

IV. النصوص القانونية:

أ. النصوص القانونية الجزائرية:

1. قانون رقم 04-15، المؤرخ في 10 نوفمبر 2004، يعدل ويتم الأمر رقم 66-156 المؤرخ في 08 يونيو 1966، المتضمن قانون العقوبات، ج.ر عدد 71، صادرة في 10 نوفمبر 2004.
2. قانون رقم 09-04، مؤرخ في 05 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر عدد 47، صادرة في 16 غشت 2009.
3. قانون رقم 15-04، مؤرخ في 01 فبراير 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكتروني، ج.ر عدد 06، صادرة في 10 فبراير 2015.
4. قانون رقم 18-04، مؤرخ في 10 مايو 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، ج.ر عدد 27، صادرة في 13 ماي 2018.
5. قانون رقم 18-07، مؤرخ في 10 يونيو 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي، ج.ر عدد 34، صادرة في 10 يونيو 2018.

ب. النصوص القانونية الأجنبية:

القانون الأردني رقم 16 لسنة 2019، قانون الأمن السيبراني، الصادر بتاريخ 16 أيلول 2019، ج.ر عدد 5595 لسنة 2019.

V. المواقع الإلكترونية:

1. "أكبر عطل في تاريخ تكنولوجيا المعلومات" .. دروس وتحذيرات للمستقبل، نشر بتاريخ 20 يوليو 2024، تم الاطلاع عليه في 16 نوفمبر 2024، متاح على الرابط: <https://www.masrimes.com/413190>
2. "ملاءة المالية": تكلفة الأمن السيبراني لشركة ناشئة تتراوح بين 3 و5% من رأس المال، نشر بتاريخ 02 أكتوبر 2024، تم الاطلاع عليه في 15 نوفمبر 2024، متاح على الرابط: <https://2u.pw/Dfn0SSUL>
3. اببها الجفر، ما هو أمان واجهة برمجة التطبيقات (API)؟ 7 ممارسات أمان واجهة برمجة التطبيقات، نشر بتاريخ 06 سبتمبر 2024، تم الاطلاع عليه في 06 نوفمبر 2024، على الساعة 16:17، متاح على الرابط: <https://www.astera.com/ar/type/blog/api-security/>

4. الاستراتيجية الوطنية للأمن السيبراني لمملكة البحرين، المركز الوطني للأمن السيبراني، د.ت.ن، تم الاطلاع عليه بتاريخ 15 نوفمبر 2024، متاح على الرابط: <https://www.ncsc.gov.bh/ar/national-strategy.html>.

5. الأمن السيبراني يستحوذ على 3.3 مليارات دولار من انفاق الشرق الأوسط عام 2024، نشر بتاريخ 27 مارس 2024، تم الاطلاع عليه في 15 نوفمبر 2024، متاح على الرابط: <https://linksshortcut.com/NByiU>.

6. محمد سناجلة، أزمة الأمن السيبراني تتفاقم في العالم وتزداد سوءا بسبب مشكلة جديدة، نشر بتاريخ 29 جوان 2022، تم الاطلاع عليه في 15 نوفمبر 2024، متاح على الرابط: <https://2u.pw/i9oismvZ>.

ثانيا: المصادر الأجنبية:

I. Article :

1. Daniel SCHATZ, Rabih BASHROUSH, Julie WALL, (**Towards a More Representative Definition of Cyber Security**), *Journal of Digital Forensics, Security and Law (JDFSL)*, Vol. 12 : No. 2 , Article 8, Association of Digital Forensics, Security and Law (ADFSL), Florida. <https://commons.erau.edu/jdfsl/vol12/iss2/8/>
2. Sebastian FLORCZAK , Adrian JASIAK, Izabela SZCZYGIEL, (**Two-factor authentication (2FA) comparison of methods and applications**), *Advances in Web Development Journal*, Vol. 1, N.03, Patryk Organiściak, Rzeszów University of Technology, 2023, P.27. URL shortener: <https://2u.pw/Qwk3c3tb>
3. Jun ZHAO, Minglai SHAO, Hong WANG, Xiaomei YU, Bo LI, Xudong LIU, (**Cyber threat prediction using dynamic heterogeneous graph learning**), *Knowledge-Based Systems*, Volume 240, 15 March 2022. <https://www.sciencedirect.com.sndll.arn.dz/science/article/abs/pii/S0950705121011564>
4. Marjan GUSEV, Kiril KIROSKI, Sasko RISTOV, (**An e-ordering and e-invoicing cloud solution**), *Informatyka Ekonomiczna*, Issue 3(29), Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu, Wrocław, Poland, PP. 54-70. URL shortener: <https://2u.pw/A5eGl5h8>
5. Meysam TAHMASEBI, (**Beyond Defense: Proactive Approaches to Disaster Recovery and Threat Intelligence in Modern Enterprises**), *Journal of Information Security*, Vol.15 No.2, April 2024. <https://doi.org/10.4236/jis.2024.152008>
6. Siva Subrahmanyam BALANTRAPU, (**AI for Predictive Cyber Threat Intelligence**), *International Journal of Management Education for Sustainable Development*, Vol 7, No 7, 2024. <https://www.ijscds.com/index.php/IJMESD/article/view/590>
7. Financial Management Regulation, Volume 10, Chapter 10, U.S. Department of Defense, USA January 2016. https://comptroller.defense.gov/Portals/45/documents/fmr/archive/10arch/10_10_Jan16.pdf

II. Theses:

Thibaut PROBST, Evaluation et analyse des mécanismes de sécurité des réseaux dans les infrastructures virtuelles de cloud computing, thèse de doctorat en Réseaux et télécommunications, Institut National Polytechnique de Toulouse, université federale de toulouse, 2015. P.12

III. textes juridiques:

1. **DIRECTIVE 2001/115/CE** DU CONSEIL du 20 décembre 2001, modifiant la directive 77/388/CEE en vue de simplifier, moderniser et harmoniser les conditions imposées à la facturation en matière de taxe sur la valeur ajoutée, J.O.C.E, L15, 17/01/2002.
2. **Directive 2014/55/UE** du Parlement européen et du Conseil, du 16 avril 2014, relative à la facturation électronique dans le cadre des marchés publics Texte présentant de l'intérêt pour l'EEE JOUE L 133 du 6 mai 2014, JOUE L 133 du 6 mai 2014.



3. *Directive 2014/55/UE du Parlement européen et du Conseil, du 16 avril 2014, relative à la facturation électronique dans le cadre des marchés publics Texte présentant de l'intérêt pour l'EEE JOUE L 133 du 6 mai 2014, JOUE L 133 du 6 mai 2014.*
4. *Règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (Texte présentant de l'intérêt pour l'EEE), JOUE L 119 du 4.5.2016.*