Dirasat: Human and Social Sciences, Volume 50, No. 5, Supplement 1, 2023

Deanship of Scientific Research

The Social and Legal Context of Electronic Crime: A Comparative Study between Algerian and Jordanian Legislation

Malika Hadjadj Mustapha [1], ***Amal AbuAnzeh**** [2]

[1] Department of public law, Faculty of Law and Political Science, Ziane Achour University Djelfa17000, Algeria.

[2] Department of public law, School of Law, The University of Jordan, Amman, Jordan.

Received: 10/10/2022
Revised: 19/10/2022
Accepted: 3/11/2022
Published: 30/10/2023

* *Corresponding author:*
a.abuanzeh@ju.edu.jo

Citation: Mustapha, M. H. ., & Abu Anzeh, A. (2023). The Social and Legal Context of Electronic Crime: A Comparative Study between Algerian and Jordanian Legislation. *Dirasat: Human and Social Sciences*, 50(5), 347–364.
https://doi.org/10.35516/hum.v50i5.2681

Abstract

Objectives: The study presents the effects of electronic crime on society when perpetrators exploit electronic media in an attempt to satisfy their aspirations. This study deals with the criminal policy used to confront these crimes and deter their perpetrators by defining their definition and elements, and the penalties prescribed for their perpetrators in Algerian legislation compared to Jordanian legislation.

Methods: The study applied the comparative legal approach, by presenting the legal texts regulating electronic crime, clarifying the terms and conditions that they contain, analyzing and commenting on them, as well as comparing the Jordanian and Algerian legislation approach in the face of electronic crime, describe the strengths and weaknesses of each.

Results: The study reached the awareness of Jordanian and Algerian legislators of the danger of electronic crime on society and their efforts to amend their legal texts. However, the Algerian legislator did not deal with the crime of electronic forgery , whether in the Penal Code or in any special law. Also, the penalties stipulated in the Algerian and Jordanian legislation are not commensurate with the gravity of electronic crime, which may not achieve the main objectives of the penalty with public and private deterrence.

Conclusions: The study concluded that the text of the Algerian Penal Code regulating the crime of forgery should be amended to apply to electronic forgery and the need to reconsider the penalties stipulated in the Algerian and Jordanian legislation for electronic crime perpetrators and the aggravating circumstances thereof.

Keywords: Electronic crime, social context, criminal law, Jordanian law, Algerian law.

السياق الاجتماعي والقانوني للجريمة الإلكترونية: دراسة مقارنة بين التشريع الجزائري والأردني

مليكة حجاج مصطفى [1]، ***أمال عبدالله أبوعنزة*** [2]*

[1] قسم القانون العام، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة، الجزائر.

[2] قسم القانون العام، كلية الحقوق، الجامعة الأردنية، الأردن.

ملخّص

الأهداف: تعرض هذه الدراسة أثر الجرائم الإلكترونية في المجتمع عندما يستغل مرتكبها الوسائط الإلكترونية سعيا إلى إرضاء مطامعهم، وتقف هذه الدراسة على السياسة الجنائية المتبعة لمجابهة هذه الجرائم وردع مرتكبها من خلال تحديد تعريفها وأركانها، والجزاءات المقررة لمرتكبها في التشريع الجزائري مقارنة بالتشريع الأردني.

المنهجية: طبقت الدراسة المنهج القانوني المقارن، وذلك بعرض النصوص القانونية المنظمة للجريمة الإلكترونية، وبيان ما تتضمنه من أحكام وشروط وتحليلها والتعليق عليها، وكذلك مقارنة التشريعين الأردني والجزائري في مواجهة الجرائم الإلكترونية، وبيان نقاط القوة والضعف في كل منهما.

النتائج: توصلت نتائج الدراسة الى إدراك كل من المشرع الأردني والجزائري لخطورة الجرائم الإلكترونية على المجتمع وسعيهم إلى تعديل نصوصهما القانونية بما يتفق مع طبيعة هذه الجرائم، إلا أن المشرع الجزائري لم يعالج جريمة التزوير الإلكتروني سواء في قانون العقوبات أو في أي قانون خاص. كما أن العقوبات المقررة في التشريعين الجزائري والأردني لا تتناسب مع خطورة الجرائم الإلكترونية، الأمر الذي قد لا يحقق أهداف العقوبة الرئيسية بالردع العام والخاص.

الخلاصة: خلصت هذه الدراسة إلى ضرورة تعديل نص قانون العقوبات الجزائري الذي يعرف جريمة التزوير ليصبح قابل للتطبيق على التزوير الإلكتروني، وضرورة إعادة النظر بالنسبة للتشريعين الجزائري والأردني في العقوبات المقررة لمرتكبي الجرائم الإلكترونية والظروف المشددة لها.

الكلمات الدالة: الجرائم الإلكترونية، السياق الاجتماعي، القانون الجنائي، القانون الأردني، القانون الجزائري.

مقدمة

شهد مجال الإعلام والاتصال تطورات كبيرة نتيجة انتشار وسائل التكنولوجيا والابتكارات المستحدثة في النشاطات الإلكترونية، التي أصبحت مقومات ودعائم تطور المجتمعات، ومؤشر مهم في قياس جودة تقديم الخدمات وسرعتها. وعلى الرغم من الايجابيات التي حققتها تقنية المعلومات في جميع المجالات إلا أنه رافقتها العديد من السلبيات نتيجة اساءة استخدام هذه التقنيات المتطورة، أو الانحراف عن الأغراض المخصصة لها، فظهر ما يسمى بالإجرام الالكتروني؛ الغش المعلوماتي؛ جرائم الانترانت؛ والجرائم الإلكترونية. وتعبر جميع هذه التسميات الفقهية عن خطورة هذه الجرائم كونها تهدد مصالح المجتمع الجديرة بالحماية (الخبيزي، 2017، 35 وما يليها)، وتترك أثارا وأضرار كبيرة، قد يصعب إصلاحها، ومن أهم مخاطرها: هدم بناء الأسرة وتفككها، بالإضافة إلى الإساءة بسمعة الأفراد واظهارهم بصورة غير لائقة، والتسبب بالأضرار الاقتصادية للدولة من خلال تدمير النظام الاقتصادي عن طريق التطفل على خصوصيات الدولة وعلى الأموال العامة، كما أنها تشكل خطرًا على سيادة الدولة فمن الممكن أن تؤدي الى حدوث انقلابات سياسية وارتكاب أعمال إرهابية، وبما أن وسيلة التواصل والتسلية والترفيه أصبحت عن طريق التكنولوجيا فإن انتشار تلك الجرائم من شأنه تنشئة جيل فاسد لا يعطي أي اعتبارات لمبادئ الأخلاق والإنسانية، كذلك التسبب بأضرار نفسية للضحية قد تؤدي به للتفكير بإهدار حياته نتيجة خوفه من الابتزاز، ومن الممكن أن يتم إهدار روح الضحية من قبل المجرم ذاته عند عجزه عن تنفيذ تهديداته، أو قيامه بنشر الأخبار الكاذبة وتضليل الناس عن الحقائق، ونشر معلومات مُخلة بالنظام العام والآداب، كذلك إلحاق ضرر بالذمة المالية للشخص ضحية التهديد نتيجة اقدامه على دفع مبالغ ضخمة مقابل التخلص من التهديدات((Sinha & Vidyapeeth, 2018).

ولاحتواء الجرائم الإلكترونية في المجال الفني والقانوني سعت الجهود الدولية إلى سد ثغرات الأنظمة الأمنية، وتحسين تطوير أساليب الحماية الفنية للنظم وبرامج المعلومات، وتحديد أنماط النشاطات الإجرامية وسبل مواجهتها من خلال إبرام العديد من الاتفاقيات كاتفاقية المنظمة العالمية للملكية الفكرية سنة 1967 التي اعتبرت الحاسب الآلي من المصنفات الأدبية والفنية، وأنه إبداع فكري لمصممه ومبتكره لذا لابد من حمايتهم بنصوص قانونية، ومؤتمرات الأمم المتحدة لمكافحة الجريمة ومعاملة المجرمين التي أكدت في دوراتها – كل خمس سنوات- على وجوب حماية الإنسان في حياته الخاصة، وملكيته الفكرية، وحماية نظم المعلومات من خلال التنسيق والتعاون بين أفراد المجتمع الدولي، كما لعب المجلس الأوربي دور مهم في مجال مجابهة الجرائم الإلكترونية بإصدار الاتفاقية الخاصة بجرائم الحاسب الآلي سنة 2000 ودعا الأعضاء إلى ضرورة وضع التشريعات الملائمة، وتعزيز التعاون الدولي خاصة مع تزايد معدلات الجرائم المرتبطة بالتقنية (لطفي، 2019، 89). وفي ظل انتشار الجرائم الإلكترونية وتغلغلها في النشاطات الاقتصادية؛ السياسية، والاجتماعية، ومساسها للمواطن ولأمن الدول وسيادتها واستقرارها، وتهديدها قدسية خصوصية الأفراد، سعت الدول بما في ذلك الأردن والجزائر إلى إيجاد آليات لمجابهة هذا النوع من الجرائم المستحدثة، خاصة وأن القوانين التقليدية اصبحت قاصرة عن الإحاطة بكافة الأنماط الجرمية المستحدثة، نظرا للاختلاف الكبير بين الجرائم التقليدية والجرائم الإلكترونية التي تتسم بالطبيعة اللامادية، وما يترتب على ذلك من تحديات في مجال تطبيق القانون.

مشكلة الدراسة وأسئلتها

الجريمة الإلكترونية ظاهرة حديثة نسبيًا، ومشكلة عالمية يتزايد نموها بتزايد التطور التقني والمعلوماتي. ففي الأردن، أظهرت إحصائيات وحدة الجرائم الإلكترونية التابعة لمديرية البحث الجنائي في مديرية الأمن العام الأردني ارتفاعا في عدد الجرائم الإلكترونية، حيث بلغت 12872 جريمة عام (2021) أحيل منها 6605 إلى القضاء، بينما بلغت 9514 جريمة عام (2020)، و 8483 جريمة في عام (2019). وكانت معظم الجرائم الإلكترونية المرتكبة متصلة بجرائم القدح والذم والتشهير، الإشاعة وخطاب الكراهية وممارسة أعمال الابتزاز، والاحتيال المالي. وغالبية ضحاياها هم من الإناث بنسبة بلغت 75% مقارنة مع الذكور. وبالمثل، في الجزائر، حيث بلغ عدد الجرائم الإلكترونية 4210 جريمة عام (2019). كما شهدت الجرائم الإلكترونية ارتفاعا بلغ ما يقارب 8 آلاف جريمة إلكترونية خلال سنة (2020)؛ إذ سجلت المديرية العامة للأمن الوطني 5163 جريمة إلكترونية. في حين سجلت قيادة الدرك الوطني 1362 جريمة تورط فيها 1028 شخص عام (2021)، (باشوش، 2021). كما أعلنت مصالح أمن ولاية "جيجل" بالجزائر أنها سجلت خلال السّداسي الأوّل من السّنة الجارية (2022) حوالي 134 قضية معلوماتية. تعلقت معظم الجرائم الإلكترونية في الجزائر بالجرائم بالمساس بالأنظمة المعلوماتية، والنصب والاحتيال، والإرهاب المعلوماتي، وإباحية الأطفال، ونشر محتويات تحريضية والجرائم الماسة بالأشخاص كالقذف، السّب، التّهديد، الابتزاز وانتحال الهويّة.

اتبعت الجزائر والأردن سياسة جزائية في مجال الجريمة الإلكترونية من خلال تجريم الأفعال المرتبطة بها، وتحديد آليات العقاب، وأدوات متابعة المجرمين، وكيفية إلقاء القبض عليهم. لذا تكمن مشكلة الدراسة في الاجابة عن الاسئلة التالية:-

1. ما خصائص الجريمة الإلكترونية القانونية والاجتماعية؟
2. ما أهم الأجهزة المسخرة لمجابهة الجريمة الإلكترونية بما يتناسب مع خصائصها وخطورتها؟

3. ما صور النشاط الجرمي المكون للركن المادي في الجريمة الإلكترونية؟
4. ما مدى كفاية العقوبات المقررة لمرتكبي الجريمة الإلكترونية والظروف المشددة لها لتحقيق أهداف العقوبة والحد من الجريمة الإلكترونية؟

أهداف الدراسة

1. تعرُّف خصائص الجريمة الإلكترونية القانونية والاجتماعية؟
2. تعرُّف الأجهزة المسخرة لمجابهة الجريمة الإلكترونية بما يتناسب مع خصائصها وخطورتها؟
3. الكشف عن صور النشاط الجرمي المكون للركن المادي في الجريمة الإلكترونية؟
4. الكشف عن مدى كفاية العقوبات المقررة لمرتكبي الجريمة الإلكترونية والظروف المشددة لها لتحقيق أهداف العقوبة والحد من الجريمة الإلكترونية؟

أهمية الدراسة

أ) الأهمية النظرية: تكسب هذه الدراسة أهميتها النظرية في:-

إلقاء الضوء على أهم الموضوعات التي تهم المجتمع ما بعد الحداثة والتكنولوجيا ألا هو الجريمة الإلكترونية وذلك عن طريق التركيز على أثر الجريمة على المجتمع وبيان القوانين - خاصة الجزائية – التي تسعى إلى مجابهة الجريمة الإلكترونية من خلال تحديد نطاقها، والجزاءات المقررة لمرتكبيها وفق مبدأ الشرعية الذي يعد العمود الفقري للقانون الجزائي وأساسه، وتحليل هذه السياسة، ومعرفة مكامن الغموض والعجز خاصة على مستوى النصوص القانونية، الأمر الذي سياعد على إيجاد الحلول الاستشرافية الممكنة للحد من الجريمة الإلكترونية، ومجابهة خطورتها.

ب) الأهمية التطبيقية: تكسب هذه الدراسة أهميتها التطبيقية في:-

1- خصوصية الجريمة الإلكترونية وسياقها القانوني والاجتماعي، وقلة الوعي القانوني بطرق مواجهتها.

2- دعوة الباحثين إلى إجراء مزيد من الدراسات في مجال الجرائم الإلكترونية والاثار السلبية المرتبطة باستخدام النترنت والأجهزة الإلكترونية الحديثة

3- ستساهم هذه الدراسة في إثراء الجانب المعرفي والفكري عن طريق إثراء المكتبة العربية بدارسات حول موضوع الجرائم الإلكترونية ومقارنتها بين القانونين الجزائري والأردني.

4- تعميم نتائج الدارسة وتوصياتها ليستفيد منها الباحثون والمتخصصون وسلطات التشريع في المجتمع لتعديل القوانين الأردنية والجزائرية لتكون أكثر قدرة على مواجهة وصد مخاطر الجرائم الإلكترونية.

الأدب النظري والدراسات السابقة

يتفق علماء الجريمة على أن الزيادة في جرائم الإنترنت هي نتيجة للتطورات التكنولوجية التي غيرت التفاعل الاجتماعي وسلوك الناس. فالنمو السريع للإنترنت خلق فرصًا جديدة غير مسبوقة للمخالفين. تمثل هذه التطورات تحديات خطيرة للقانون والعدالة الجنائية، وتتحدد موقع ظاهرة الجريمة الإلكترونية في السياقات الأوسع للتغيير الاجتماعي والسياسي والثقافي والاقتصادي. يهتم علم اجتماع الجريمة بالبنى الاجتماعية التي تؤدي إلى الجريمة - "السلوك الفردي لا يتم بناؤه في فراغ" ويحدث في سياق اجتماعي وثقافي معين يجب فحصه عند النظر في النشاطات الجرمية. التوقعات الاجتماعية وهياكل السلطة المحيطة بالأفعال الإجرامية مهمة أيضًا لطبيعة دراسة الجريمة في المجتمع. يحدث العقد الاجتماعي في مجتمع متحضر ويقوم على أساسين هما؛ وجود قواعد أخلاقية تحكم العلاقات بين المواطنين. ووجود حكومة قادرة على تطبيق مثل هذه القواعد. تنص نظرية العقد الاجتماعي على أن "الأخلاق تتكون من مجموعة القواعد التي تحكم كيفية معاملة الناس لبعضهم البعض. سيوافق الأشخاص العقلانيون على القبول، من أجل مصلحتهم المتبادلة، بشرط أن يتبع الآخرون هذه القواعد أيضًا ". يشير هذا العقد إلى أنه لا يوجد رجل له سلطة على آخر وأن لا أحد يعيش فوق القانون. من المفترض أن يحدد المجتمع القواعد لأعضائه، ويجب على كل من هو جزء من هذا المجتمع الالتزام بهذه القواعد. لكي تنجح هذه النظرية، لا يجب ذكر القوانين فحسب، بل يجب تطبيقها أيضًا، وهذا سيمنع أي شخص من أي محاولة لخداع النظام (Yar, 2006; Alsawalqa, 2021, Tutorial, 2022).

أوجدت الشبكة العنكبوتيه والأجهزة التقنية والبرامج والوسائل الرقمية مجالًا عامًا جاذبًا لمشاركة الأفراد، صعب الرقابة، دافعا لانخراط الافراد في الجريمة ضحية وجانيًا، ووفقًا لنظرية المجال العام للفيلسوف وعالم الاجتماع الالماني المعاصر يورغن هابرماس يتكون المجال العام من اجتماع مجموعة من الأفراد لمناقشة القضايا العامة (اجتماعية، سياسية، دينية) فى الأماكن العامة كالمقاهى والنوادي وغيرها، لينتقل في العصر الرقمي من الاماكن العامة الواقعية الى مجال الفضاء الرقمي ولا يعطي للجمهور فرصة حقيقية للمشاركة فى الحوار والتفاعل، ويكون تفاعلهم على الاغلب أحادي الاتجاه. ومن ابرز سمات المجال العام من منظور هابرماس هي المناقشات حول قضية أو موضوع ما، حرية الأفراد المستبعدين من المشاركة في

النقاس والتفاعل الواقعي، والتعبير عن رأيهم، بغض النظر عن مكاناتهم الاجتماعية (المركز الديمقراطي العربي، ٢٠١٨). وقد يدفع تحول الافراد من التفاعل الواقعي إلى التفاعل الرقمي غير المحصن إلى ارتكاب الجريمة الإلكترونية، حيث تُرجع نظرية الضغوط العامة حدوث الجريمة او الانحراف نتيجة الضغوط الناجمة عن البناء الاجتماعي التي لا تتيح للافراد الفرصة لتحقيق أهدافهم المقبولة اجتماعيا، وتحبطهم وتصدر منهم استجابات نفسيه- اجتماعية سلبية من بينها خرق القانون لتحقيق اهدافهم، كاستغلال الثغرات التكنولوجية. بينما تستند نظرية النشاط الروتيني على افتراض أن الجريمة يمكن أن يرتكبها أي شخص لديه الفرصة. تنص النظرية أيضًا على أنه يتم منح الضحايا خيارات بشأن ما إذا كانوا سيقعون ضحايا على نحو أساسي من خلال عدم وضع أنفسهم في مواقف يمكن أن ترتكب فيها جريمة ضدهم، فشبكة الانترنت والوسائل التقنية ووسائل التواصل الاجتماعي لا توفر وسائل الحماية اللازمة لخصوصية الأفراد، وبعض الأفراد المتفاعلين رقميا لا يمتلكون المهارات اللازمة في حماية خصوصيتهم، على البعض الآخر مما يمتلك الخبرة وفنون الاختراق وانتهاك الخصوصية مما يبني فرصة وقوع الجريمة الإلكترونية على اختلاف أشكالها (البداينة، 2014). ويستخدم مفهوم الجريمة الإلكترونية لوصف النشاطات الإجرامية عبر الإنترنت مثل: سرقة الهوية والبيانات، الاحتيال عبر الإنترنت، القرصنة (الوصول غير المصرح به إلى الشبكات)، وخطاب الكراهية، الإرهاب السيبراني، إصابة الأجهزة بالفيروسات، هجمات رفض الخدمة، مشاركة الملفات في انتهاك لحقوق النشر، الطباعة ثلاثية الأبعاد للمنتجات المحظورة، الحرب السيبرانية، المواد الإباحية المتعلقة بالأطفال. تُرتكب الجرائم الإلكترونية باستخدام الهواتف المحمولة وأجهزة الكمبيوتر والماسحات الضوئية والكاميرات الرقمية والأجهزة الإلكترونية الأخرى. ولهذه النشاطات الإجرامية عواقب وخيمة على الصحة الاجتماعية والعقلية والبدنية للأفراد (Yar, 2006; Alsawalqa, 2021).

تأثر المشرع الجزائري بغيره من التشريعات الأجنبية والعربية، في ما يخص القواعد التي أستند إليها لمكافحة الجريمة الإلكترونية حيث اتجه إلى سن نصوص جديدة وخاصة تتعلق بهذا النوع من الجرائم، رغبة منه في تأمين أنظمة المعلومات من اعتداءات المجرمين. كان أول نص تشريعي في المجال الالكتروني هو تعديل قانون العقوبات رقم 09/01 سنة2009 بموجب المواد: 144 مكرر، 144 مكرر 1،. حيث أدرج المشرع عبارة « وسيلة الكترونية أو معلوماتية» لأول مرة. وبعدها قانون رقم 15/04الصادر في 2001/11/10 حيث عدل قانون العقوبات بإضافة القسم السابع مكرر تحت عنوان: المساس بأنظمة المعالجة الآلية للمعطيات وشمل المواد من 399 مكرر 399 مكرر 7 من قانون العقوبات. بالإضافة إلى فرض حماية جنائية على الحياة الخاصة للأفراد والتصدي للاستخدام السيئ لوسائل التكنولوجيا الحديثة بموجب تعديل قانون العقوبات رقم 06/23 سنة2006 وذلك بإضافة المواد 303 مكرر إلى المادة 303 مكرر 3.

اصطلح المشرع الجزائري على تسمية الجريمة الإلكترونية بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وتبنى التعريف الذي جاءت به الاتفاقية الدولية للإجرام المعلوماتي، بموجب المادة الثانية من قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها رقم 09-04 الصادر سنة 2009 الذي عرفها على أنها: "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية ". وبناء على هذا التعريف يتبين أن الجريمة الإلكترونية هي من الجرائم المرتكبة عن طريق أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين، والمرتكبة عن طريق أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية (نبيل، عبد الرؤوف، 2019، 138).

والملاحظ أن المشرع الجزائري عرف الجريمة الإلكترونية بموجب قانون خاص بالإضافة إلى انه عالج أحكامها التجريمية بموجب قانون العقوبات، أما من حيث إجراءات الوقاية منها وسبل مكافحتها، فلقد عالجها بموجب عدة قوانين كقانون الإجراءات الجزائية، وقانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها. على خلاف المشرع الجزائري، نظم المشرع الأردني قواعد الجريمة الإلكترونية بموجب قانون خاص لخصوصية هذه الجريمة، فلقد اصدر في البداية قانون الاتصالات رقم 13 لسنة 1995، ثم قانون جرائم أنظمة المعلومات رقم 30 لسنة 2010، ومن ثم قانون المعاملات الإلكترونية رقم 85 لسنة2001 والمعدل لسنة 2015. أخيرا جاء قانون الجرائم الإلكترونية لسنة 2015 لمعالجة الثغرات والنقص التشريعي في التصدي للجرائم التقليدية التي ترتكب باستخدام نظام المعلومات أو الشبكة الإلكترونية (الزايد، 2011، 32).

وفي إطار دراسة المقارنة بين التشريع الجزائري والأردني، نلاحظ أن القانون الأردني على خلاف القانون الجزائري أطلق على هذه الجريمة مصطلح الجرائم الإلكترونية، وسمى القانون الذي ينظمها قانون الجرائم الإلكترونية لسنة 2015. ولم يعرف هذا الأخير هذه الجريمة تاركا الأمر للفقه، ولعل الحكمة من ذلك هي عدم وجود تعريف متفق عليه لهذه الجريمة (اجتماع مجلس خبراء منطقة التعاون الاقتصادي والتنمية في عام 1994)، وذلك باختلاف النظم القانونية في دول العالم وفكرها القانوني حول حماية المعلومات، فهناك من يرى بأن المعلومات ذات طبيعة خاصة ولا يطبق عليها الشرط المادي الضروري لتعريف الجريمة(أيوب، 2020، 10)، و يرى البعض الآخر أن المعلومات تأخذ قيمة مالية ومادية بصفتها حقا خاصا ينسب لشخص محدد (لدادوة، 2021، 46).

حاول الفقه تعريف الجريمة الإلكترونية، فقد عرفها البعض بأنها: "مجموعة الجرائم المتصلة بعلم المعالجة المنطقية للمعلوماتية"(قورة، 2005،

40). إلا إننا نلاحظ أن هذا التعريف ضيق، لكونه يضيق من نطاق الجرائم الإلكترونية على نحو كبير إذ يتطلب لارتكابها قدرا كبيرا من المعرفة التقنية. لذا، حاول بعض الفقهاء إيجاد تعريف أكثر اتساعا للجرائم الإلكترونية فعرفها بأنها:" كل سلوك إجرامي يتم بمساعدة الحاسب الآلي أو هي كل جريمة تتم في محيط الحاسبات الآلية" (قشقوش، 1992، 89). ووفقا لهذا التعريف تقوم الجريمة الإلكترونية بمجرد استعمال الحاسب الآلي بنشاط إجرامي. باستقراء التعريفات السابقة للجريمة الإلكترونية يتبين أن النظام المعلوماتي والالكتروني هذه الجريمة يلعب دورا أساسيا بها سواء لإتمامها أو كمحل لها(.المناعسة، الزعبي، 2015، 93، أيوب، 7). وبناء على ماسبق، فيمكن تعرف الجريمة الإلكترونية بأنها سلوك غير مشروع يحتمل أن يرتكب على أو عن طريق جهاز حاسوب متصل بنظام معلوماتي.

تعد الجريمة الإلكترونية ذات خصائص تميزها عن غيرها من الجرائم، ويعود ذلك لطبيعتها الخاصة المختلفة عن غيرها من الجرائم التقليدية. فهي جريمة **عابرة للحدود الوطنية**، فقد جعل نظام الإنترنت من معظم دول العالم في حالة اتصال دائم على الخط، وهذا ما يشكل تهديدا عابر للحدود، إذ يمكن من خلال النظام المعلوماتي ارتكاب العديد من الجرائم مثل جرائم التعدي على البيانات والاحتيال المعلوماتي والقرصنة وسرقة الأموال(أيوب، 7). إن عدّ الجريمة الإلكترونية جريمة عابرة للحدود الوطنية يثير التساؤل حول تحديد الاختصاص القضائي والمكاني لملاحقة هذه الجرمية؟ أجاب القانون الأردني عن هذا التساؤل في المادة 17 من قانون الجرائم الإلكترونية التي أجازت إقامة دعوى الحق العام والحق الشخصي على المشتكي عليه أمام القضاء الأردني إذا ارتكبت أي من الجرائم الإلكترونية المنصوص عليها في قانون الجرائم الإلكترونية باستخدام أنظمة معلومات على أرض المملكة الأردنية، أو ألحقت أضرارا بأي من مصالحها أو بأحد المقيمين فيها أو ترتبت آثار الجريمة فيها، كليا أو جزئيا، أو ارتكبت من أحد الأشخاص المقيمين فيها. أما بالنسبة للقانون الجزائري فنجد أنه يخلو من نص خاص ينظم تطبيق القانون الجزائري على الجرائم الإلكترونية من حيث المكان، تاركا الأمر للقواعد العامة بموجب المادة الثالثة من قانون العقوبات " يطبق قانون العقوبات على كافة الجرائم التي ترتكب في أراضي الجمهورية، كما يطبق على الجرائم التي ترتكب في الخارج إذا كانت تدخل في اختصاص المحاكم الجزائية الجزائرية طبقا لأحكام قانون العقوبات حسب مبادئ الاختصاص الذاتي أو الشخصي أو العالمية أو الشامل، وقد يشكل ذلك نقصا تشريعيا نظرا لخصوصية الجرائم الإلكترونية.

إن الجريمة الإلكترونية صعبة الاكتشاف ويسهل إتلاف الدليل المادي الناتج عنها، وأن اكتشفت يكون بمحض الصدفة في غالب الأحيان، بل وبعد وقت طويل من ارتكابها، زد على ذلك أن الجرائم التي لم تكتشف هي أكثر من تلك التي اكتشفت ورفع الستار عنها.(الزايد، 2011، 33). كما تمتاز الجريمة الإلكترونية بأنها من السهل إخفاء معالمها وإتلاف الدليل المادي فيها، حيث يسهل غالبا على الجاني محو أدلة الإدانة في زمن قياسي لا يستغرق ثوان معدودة (رابحي، 2018، 97)، وإن كان يمكن استرجاعة بأجهزة وبرامج خاصة. أيضًا، من الصعب تتبع مرتكبيها، إذ تتسم وسيلة التنفيذ في أغلب الحالات بالطابع التقني الذي يضفي عليها الكثير من التعقيد (يوسف 2011، 157- 158)، فهي تحتاج إلى خبرة فنية يصعب على المحقق التقليدي التعامل معها، لأنها تتطلب إلماما خاص بتقنيات الكمبيوتر ونظم المعلومات(عاقلي،2017، 125). ونظرا لخصوصية الجرائم الإلكترونية وصعوبة الكشف عنها وسهولة إتلاف الدليل المادي فيها، فقد سعت كل من الجزائر والأردن إلى مكافحة هذه الجرائم من خلال استحداث هيئات تسهر على حماية الأفراد والمؤسسات من كل ما تمطره هذه الجرائم من سلبيات.

في الجزائر، استحدث المشرع هيئات وطنية متخصصة في الوقاية من الجرائم الإلكترونية. بداية، استحدث الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها من خلال المرسوم الرئاسي رقم 15 - 261 المؤرخ في سنة 2015، وتمارس الهيئة اختصاصاتها الحصرية تحت رقابة قاض مختص، ومن أهمها مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال. وبموجب المادة 09 من المرسوم الرئاسي رقم 19-172 فإنه من مهام المديرية العامة للهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام والاتصال تبادل المعلومات مع مثيلاتها الأجنبية بغرض تجميع كل المعطيات المتعلقة بتحديد مكان مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والتعرف عليهم(خرشي 2022، 72). كما استحدث المشرع الجزائري بتاريخ 11-06-2015 على مستوى دائرة الاستعمال والتحضير لأركان الجيش الوطني الشعبي مصلحة الدفاع السبراني ومراقبة أمن الأنظمة و أوكلت لها مهمة حماية المنظومات والمنشات الحيوية ضد كل أنواع الجريمة السبيرانية، ومن بين المحاور التي تناولتها الأرضية العملياتية لهذه المصلحة اعتماد التكوين التقني والعلمي لإنتاج الكفاءات والمهارات القادرة على خلق نظام الدفاع السبيراني في كافة نشاطات المؤسسة العسكرية (بوازدية،2019، 82). أما في الأردن، تم إنشاء مركز وطني للاستجابة لحوادث الكمبيوتر، الذي يتبع لمركز تكنولوجيا المعلومات الوطني الذي يعدُّ مرجعية لأمن وسلامة المعلومات والشبكات في المملكة. تتمثل مهمة المركز في دعم البنية التحتية للاتصالات ونظم المعلومات والمحافظة عليها من تهديدات الجرائم الإلكترونية (النوايران، 2019، 179). كما تم إنشاء قسم خاص للجرائم الإلكترونية في مديرية الأمن العام تابع لإدارة البحث الجنائي عام 2008، وذلك لملاحقة هذه الجرائم والتصدي لها. وتم تزويد القسم بالقوى البشرية المؤهلة من مهندسين وفنيين ومبرمجين وبالمعدات والأجهزة اللازمة للقيام بعمله (أيوب، 29). وأخيرا، تم إنشاء مركز لمكافحة الجرائم الإلكترونية في عمان، وذلك بالتعاون مع حلف النيتو عبر برنامج العلم لأجل الأمن والسلام، يهدف هذا المركز إلى تعزيز قدرات الأردن على مواجهة التهديدات الإلكترونية وتنفيذ إستراتجية وطنية في الدفاع الإلكتروني(النوايران، 189).

الدراسات السابقة

أجرى ايوب (2022) دراسة عن اتجاهات القضاة والمحامين نحو تعديل قانون الجرائم الإلكترونية وأثره في الحد من ارتكاب الجريمة في المملكة ألأردنية الهاشمية، وقد خلصت الدراسة إلى أن العقوبات الواردة في قانون الجرائم الإلكترونية غير رادعة وهناك حاجة إلى تعديل هذا القانون بما يتوافق مع التطورات والتقنيات المستحدثة. وتتميز دراستنا عن هذه الدراسة بأنها دراسة موضوعية للسياق القانوني للجريمة الإلكترونية دون الخوض في أراء القضاة والمحامين حول ذلك، كما تميزت بإتباعها المنهج المقارن بين القانونين الأردني والجزائري حول السياق القانوني والاجتماعي لهذه الجريمة.

وتناولت دراسة خرشي (2022) الحديث عن النظام القانوني للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها. وقد ركزت الدراسة على الطبيعة القانونية للهيئة ومهامها باعتبارها من أهم الآليات المستحدثة لمواجهة الجرائم المعلوماتية بالجزائر. ومن أهم نتائج الدراسة هي؛ غياب تكييف واضح ودقيق للهيئة في القانون رقم 09-، كما أن تشكيلة الهيئة سندا للمرسوم الرئاسي رقم 19-172 غير مطابق في مضمونه للإحالة الواردة بالمادة 13 من القانون رقم 09-04 لصدور تنظيم يحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها، الأمر الذي ترك المجال للسلطة التقديرية للسلطة التنفيذية. وتميزت دراستنا بالتركيز على الجوانب القانونية والاجتماعية للجريمة الإلكترونية في التشريعين الجزائري والأردني مع الإشارة على نحو بسيط إلى أهم الأجهزة المؤسساتية المكرسة لمواجهتها في الجزائر كالهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

كما أجرى تشوي وبارتي (Choi & Parti, 2022) دراسة لفهم الجريمة السيبرانية التي تنطوي على تطبيق التشفير في استنباط تدابير وقائية فعالة، بدءًا من سوق العملات المشفرة والشبكة المظلمة إلى اختراق كلمات المرور. ومن خلال النهج التحليلي للعدد الخاص للمجلة الدولية لذكاء الأمن السيبراني والجرائم الإلكترونية، توصلت نتائج الدراسة إلى أنه تقع على الخبراء في علم الجريمة والقانون إجرام مسؤولية معالجة قضية العدالة الجنائية وتوفير فهم أفضل لها للجهات الفاعلة في نظام العدالة الجنائية؛ خاصة المسألة التي تتطلب المعرفة المهنية والتقنية.

وهدفت دراسة الزبن والخرابشة (2021) إلى تعرُّف الجرائم الإلكترونية و مستوى الوعي بخطورتها من وجهة نظر الشباب الجامعي الأردني في جامعة البلقاء التطبيقية كلية الأميرة رحمة الجامعية، وتعرُّف عادات وأنماط استخدام الإنترنت لدى الشباب، وتحديد إن كان هناك فروق تعزى إلى الجنس، والتخصص، والسنة الدراسية، ولتحقيق أهداف الدراسة تم أعداد استبانة تكونت من (43) فقرة، وقد استخدم البحث المنهج الوصفي منهج المسح الاجتماعي بأسلوب العينة، وتكونت عينة الدراسة من (212) طالب وطالبة، تم أجراء الدراسة في شهر تشرين الثاني من عام 2019، تم اختيارهم بطريقة العينة العشوائية، وتم استخدام الإحصاء الوصفي (النسب المئوية) واختبار (ت)، واختبار التباين الأحادي للمتغيرات. وكشفت نتائج الدراسة أن معدل تعرض الطلبة للجرائم الإلكترونية جاء بمستوى منخفض، كما بينت نتائج الدراسة أن 39.15% يقضون من ساعتين إلى أقل من أربع ساعات على الإنترنت، أما أكثر المواقع استخداما فهو الفيس بوك بنسبة 49.06%، و 43.40% يدخلون للمواقع بهدف الترفيه والتسلية، أما مستوى الوعي بالجرائم الإلكترونية فقد جاء مرتفعًا، وأوصت الدراسة بضرورة توعية الطلبة بأهمية استثمار وقتهم عند استخدام الإنترنت لتطوير مهاراتهم، تفعيل النشاطات الرياضية، الثقافية، والترفيهية، لجذب الشباب للحد من الإدمان على مواقع التواصل الاجتماعي، عقد المحاضرات لتوعية بمخاطر الجرائم الإلكترونية.

بينما حللت دراسة ديورا وتشوداساما (Deora & Chudasama, 2021) الجرائم الإلكترونية التي تستهدف الأفراد على الإنترنت وتفحص أيضًا دوافع المجرمين الذين يقومون بمثل هذه الهجمات التي تشمل (التصيد الاحتيالي، والخداع)، المضايقات عبر الإنترنت، سرقة الهوية، البرامج الضارة، القرصنة، وإنكار- جرائم الخدمة. تمثل جرائم الإنترنت تهديدًا لمجتمع اليوم المعتمد على الإنترنت وهي مشكلة كبيرة متنامية. وجدت نتائج الدراسة أن الأشخاص يستخدمون الخدمات المصرفية عبر الإنترنت والتسوق عبر الإنترنت والشبكات الاجتماعية عبر الإنترنت. توفر التكنولوجيا الرقمية فوائد وتوفر بيئة غنية للنشاط الإجرامي لسرقة هوية لسرقة المعلومات الحكومية السري، والمعروفة أيضًا باسم القرصنة. تتضمن بعض الأمثلة القصيرة شراء وبيع البرامج غير القانونية والبرامج الضارة، واختراق الخوادم، وإفساد الأنظمة التي قد تكلف المليارات للأفراد والمؤسسات والحكومة. تشير الجرائم الإلكترونية إلى أي جريمة يتم ارتكابها باستخدام جهاز كمبيوتر أو جهاز إلكتروني، على نحو أساسي عبر الإنترنت. حيث أن الإنترنت لديه العديد من الفرص لاستهلاك المعلومات والوصول إليها. تسببت الهجمات الإلكترونية على نحو أساسي في إلحاق الضرر بالخدمات المصرفية باستخدام بطاقات الائتمان وعمليات الاحتيال في الدفع. تذكر، في أثناء العمل في شركة، يجب على كل شخص تحمل المسؤولية الشخصية لضمان الأمن السيبراني. عليك تحديد أولويات المخاطر التي من المحتمل أن تؤثر والعمل كفريق واحد لإنشاء أقوى دفاع ضد الهجمات الإلكترونية. حددت الدراسة أن الإجراءات الأمنية مطلوبة، إضافة إلى تعرُّف المخاطر المحتملة للإنترنت. يتم اتخاذ خطوات مختلفة لإبطاء الهجمات ولكن للأسف لم تتمكن من تحقيق النجاح. أسباب الهجمات الإلكترونية، 1.البلدان التي لديها أمن إلكتروني ضعيف، 2. المجرمون يستخدمون تقنيات جديدة للهجوم، 3. الجرائم الإلكترونية مع مخططات الأعمال. كل إنسان متصل باستخدام الإنترنت وهذا يجعل العالم صغيرًا. يجب نشر الوعي بشأن

الجرائم الإلكترونية ويجب فرض عقوبات صارمة على مجرمي الإنترنت حتى يترك المجرمون الفكرة لارتكاب أي جريمة. يجب أن يضمن أن القوانين المصاغة يجب أن يتم اتباعها على نحو مناسب.

أما دراسة الجبرة وآخرون (2021) فهدفت بيان أثر الجريمة الإلكترونية على سير المرفق العام الإلكتروني، مع التطرق لأهم التشريعات الأردنية التي تضمنت النصوص القانونية التي جاءت لتوفير الحماية الجزائية للمرفق العام الإلكتروني. ومن خلال المنهج الوصفي، توصلت نتائج الدراسة إلى أن الجريمة الاكترونية من أهم معوقات سير المرفق العام الالكتروني العام، ولها بالغ الأثر في تعطيل سير المرافق العامة لالكترونية. وأن المرفق العام الالكتروني من أهم نتائج التحول الالكتروني الذي تبنته الادارة العامة، لتسيير المرفق العام على نحوه المستحدث. كما ساعدت الادارة الإلكترونية على التخلص من العديد من المشاكل، و التي تتحقق من خالل الخدمة العامة للأفراد، ومنها اختصار الوقت، والسرعة في الحصول على المعلومات والوثائق، و جودة الخدمات. بالاضافة إلى أن المشرع الأردني وضع العديد من النصوص التشريعية لحماية المرفق العام الالكتروني، من الهجمات الإلكترونية المتعددة التي تظهر على صورة جرائم إلكترونية متعددة الصور، كقانون الأمن السيبراني وقانون الجرائم الإلكترونية، إلا أنها لسيت كافية لتوفير الحماية الجزائية الشاملة.

وتناولت دراسة نبيل وعبد الرؤوف (2019) تعريف الجريمة المعلوماتية من الناحية الفقهية والتشريعية، ودراسة أركان الجريمة المعلوماتية من منظور التشريع الجزائري. وقد توصلت الدراسة إلى عدة نتائج أهمها إتباع المشرع الجزائري سياسة مزدوجة للتصدي لظاهرة الإجرام المعلوماتي وذلك بتعديل الجوانب الموضوعية للجريمة المعلوماتية في قانون العقوبات، والإجرائية في قانون الإجراءات الجزائية. وتميزت دراستنا عن هذه الدراسة بالبحث عن العقوبات المقررة لمرتكبي الجرائم الإلكترونية، وأهم الأجهزة المؤسساتية المكرسة لمواجهتها. كما تميزت دراستنا بمقارنة القانون الجزائري حول الجريمة الإلكترونية مع القانون الأردني وبيان أوجه القوة والضعف في كل منهما.

أيضًا، تناولت دراسة سمامعة (2017) الحديث عن جزئية مهمة في الجرائم الإلكترونية وهي مدى خضوعها للأحكام الخاصة بالشروع وفقا لأحكام القانون الأردني، وقد توصلت الدراسة إلى عدة نتائج أهمها ضرورة العقاب على الشروع في الجرائم الإلكترونية لحماية حقوق الأفراد من الخطر الذي قد يلحق بهم حتى ولو لم تتحقق النتيجة التي يهدف الجاني لتحقيقها. وتميزت دراستنا عن هذه الدراسة أنها تحدثت عن السياق القانوني والاجتماعي للجريمة الإلكترونية أركانها والعقوبات المقررة لها، من خلال دراسة تحليلية مقارنة بين التشريعيين الجزائري والأردني، مع الإشارة على نحو سريع الى الشروع بارتكابها.

كما أجرى العجمي (2014) دراسة حول المشكلات العملية والقانونية للجرائم الإلكترونية بهدف بيان التعديلات التشريعية والعملية اللازمة لمواجهة الجريمة الإلكترونية في كل من الأردن والكويت. من خلال النهج المقارن، توصلت نتائج الدراسة إلى أن قواعد التشريع الجزائي في التشريع الكويتي غير كافية لمواجهة الجريمة الإلكترونية وما ينبع عنها من مشكلات وبالمثل في التشريع الاردني.

بينما أجرى غاندي وأخرون (Gandhi et al, 2012) دراسة حول الجريمة الإلكترونية في الهند بناءً على تقارير مختلفة من وسائل الإعلام الإخبارية. وتوصلت نتائج الدراسة أن من واجب وسائل الإعلام المطبوعة تثقيف الآباء والشباب غير الحذرين بشأن المخاطر الكامنة في السير في المناطق الخطرة في عالم الإنترنت. كما أصبحت إدارة أمن الفضاء السيبراني بالفعل مكونًا مهمًا في إدارة الأمن القومي وإدارة الأمن العلمي ذات الصلة بالجيش وإدارة الاستخبارات في جميع أنحاء العالم، وأنه من الضروري وضع "سياسة وطنية لإدارة أمن الفضاء الإلكتروني" لتحديد المهام، وتحديد مسؤوليات الوكالات الفردية بهيكل متكامل.

منهجية الدراسة

طبقت الدراسة الحالية المنهج المقارن، يعدُّ المنهج القانوني المقارن أداة لتحسين القانون المحلي والعقيدة القانونية، وطريقة لتجديد النهج المتحجر للمدرسة التفسيرية التي لا تزال مهيمنة على القانون الجزائي وتفسيره. ويتضمن النهج المقارن في الدراسات القانونية والاجتماعية في ثناياه مجموعة أدوات تعددية تحتوي على الفرص المنهجية التالية: البحث في الطريقة الوظيفية في المشكلة الاجتماعية الفعلية، الطريقة التحليلية وهي تحليل المفاهيم والقواعد القانونية (المعقدة)، وثالثًا؛ الطريقة الهيكلية التي ترتكز على إطار القانون أو العناصر التي أعيد بناؤها من خلال نهج تحليلي. والجدير بالذكر، أن نهج القانون قد يستخدم بعض أساليب العلوم الاجتماعية (التاريخية، الاقتصادية، السياسية، الاجتماعية، الأنثروبولوجية) ما لم تكن المعلومات ذات الصلة متاحة بالفعل في نتائج البحث المنشورة. ستكون طرق العلوم الاجتماعية بعد ذلك أداة في سياق إحدى الطرق المقارنة المختارة، للحصول على رؤية كاملة وصحيحة للقانون لأنه يعمل في الممارسة من خلال إجراء تحليل السوابق القضائية المنشورة والعقيدة القانونية. وفي الدراسة الحالية، تم الاستناد الى النصوص القانونية المنظمة للجريمة الإلكترونية في كل من القانون الاردني والجزائري، وبيان ما تتضمنه من أحكام وشروط وتحليلها والتعليق عليها، وتتبع التطور التاريخي في مواجهتها، وكذلك مقارنة منهج التشريعين الأردني والجزائري في

مواجهة الجرائم الإلكترونية، وبيان نقاط القوة والضعف في كل منهما.

المبحث الأول:

اركان الجريمة الإلكترونية

إن دراسة الجريمة الإلكترونية تتطلب دراسة الأركان الأساسية التي تقوم عليها، بما في ذلك الركن الشرعي والمفترض والمادي والمعنوي وبيان مدى تشابهها واختلافها في التشريعين الجزائري والأردني.

المطلب الأول: الركن الشرعي في الجريمة الإلكترونية

لقيام قانون العقوبات بوظيفته في صيانة حقوق الأفراد الأساسية عمدت التشريعات الجزائية إلى إقرار قواعد جوهرية أهمها قاعدة شرعية الجرائم، وهذا ما نص عليه المشرع الجزائري بموجب نص المادة الأولى من قانون العقوبات" لا جريمة ولا عقوبة و لا تدبير من تدابير الأمن إلا بنص قانون"، كما نص عليه المشرع الأردني بموجب نص المادة الثالثة من قانون العقوبات"لا جريمة إلا بنص ولا يقضى بأي عقوبة أو تدبير لم ينص القانون عليهما حين اقتراف الجريمة". وعليه فان تحقق الجريمة الإلكترونية يتطلب الرجوع إلى النص الجزائي. في الجزائر، خص المشرع الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بقسم خاص ضمن قانون العقوبات وهو القسم السابع مكرر من الفصل الثالث الخاص بجرائم الجنايات والجنح ضد الأموال، ويشتمل على ثمانية مواد تهتم بذكر كل أنواع الاعتداءات على الأنظمة الإلكترونية . أما المشرع الأردني فلقد عالج الجرائم الإلكترونية في قانون خاص وهو قانون الجرائم الإلكترونية رقم 27 لسنة 2015. الذي يعدُّ العمود الفقري للتشريع المتخصص بمواجهة الجرائم الإلكترونية ، إضافة إلى أن المشرع أورد نصًا احتياطيًا في قانون الجرائم الإلكترونية لمواجهة أي جريمة ترتكب خلافًا لأحكام القوانين الأخرى بوسائل الكترونية هو نص المادة 15 من ذات القانون التي نصت على أن "أي جريمة معاقب عليها بموجب أي تشريع نافذ ترتكب باستخدام الشبكة الإلكترونية أو أي نظام معلومات أو موقع الكتروني يعاقب عليها بالعقوبة المنصوص عليها في ذلك التشريع"، ومن أمثلة ذلك جريمة الاحتيال الإلكتروني والسرقة الإلكترونية والتزوير الإلكتروني فيطبق عليها أحكام قانون العقوبات. ونظرا لأهمية مبدأ الشرعية في الجرائم الإلكترونية نلاحظ ان خصوصية هذه الأخيرة تفرض على التشريعين محل المقارنة أن تكون دائما ملازمة وملتزمة لمبدأ الشرعية الجنائية،وهو يعد صعبا إلى حد ما، لعدم امتلاك الإمكانيات الفنية والمادية التي يمكن أن تتنبأ بالأفعال الإجرامية الإلكترونية المستقبلية. لذا لابد من السعي إلى اكتساب الخبرات لمواكبة النصوص القانونية لتطور الالكتروني (لدادوة، 2021، 45).

المطلب الثاني: الركن المفترض في الجريمة الإلكترونية

يعد وجود نظام المعالجة الآلية للمعطيات الركن المفترض الذي يلزم تحققه حتى يتمكن البحث في توافر أو عدم توافر أركان أية جريمة من جرائم الاعتداء على هذا النظام، وقد عرف المشرع الجزائري نظام المعالجة الآلية للمعطيات بأنه: "كل نظام أو مجموعة من الأنظمة منفصلة كانت أم متصلة بعضها البعض أو المرتبطة التي يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين"، وهو نفس التعريف الذي جاءت به الاتفاقية الدولية للإجرام المعلوماتي المبرمة ببودابست في 2001 (قارة، 2006، 109). والأمر ذاته بالنسبة للمشرع الأردني، فقد اشترط وجود البيئة الرقمية لقيام الجريمة الإلكترونية، التي قد تكون على شكل نظام معلومات، أو الشبكة الإلكترونية، أو موقع الكتروني، فليس من المتصور دون هذا الركن المفترض أن يكتمل النشاط الجرمي. وقد عرفت المادة الثانية من قانون الجرائم الإلكترونية نظام المعلومات بأنه: "مجموعة البرامج والأدوات المعدة لإنشاء البيانات أو المعلومات الكترونيا، أو إرسالها أو تسلمها أو معالجتها أو تخزينها أو إدارتها أو عرضها بالوسائل الإلكترونية ". كما عرفت ذات المادة الشبكة الإلكترونية بأنها: "ارتباط بين أكثر من نظام معلومات لإتاحة البيانات والمعلومات والحصول عليها"، كما عرفت ذات المادة الموقع الإلكتروني بأنه: "حيز لإتاحة المعلومات على الشبكة الإلكترونية من خلال عنوان محدد". وباستقراء نصوص القانون الجزائري والأردني، نلاحظ أنها لم تحدد طبيعة النظام المرتبط بالمعالجة الآلية للمعطيات أو الوسيلة التقنية لارتكاب الجرائم الإلكترونية على سبيل الحصر بغية توسيع دائرة التجريم، فقد تكون باستخدام الحاسوب أو الهواتف الذكية مثلا (بوبرقيف، 2019، 122).

المطلب الثالث: الركن المادي في الجريمة الإلكترونية

لقيام أي جريمة، يشترط بصفة عامة أن تظهر على نحو مادي إلى العالم الخارجي، فالإرادة المجردة التي لا تصاحبها ماديات تبرز إلى العالم الخارجي لا يعاقب عليها القانون الجنائي بصورة عامة. و بالرجوع إلى التشريعين محل الدراسة، نجد ان الركن المادي للجريمة الإلكترونية يقوم على ثلاثة عناصر: الفعل والنتيجة والعلاقة السببية. ويختلف الركن المادي المكون لكل جريمة على حدا بحسب النموذج القانوني الخاص بها، وعلى هذا النحو سوف نختار أهم الجرائم الإلكترونية المنصوص عليها في كل من التشريع الجزائري والأردني وبيان عناصر الركن المادي لها.

1. جريمة الدخول والتلاعب غير المشروع داخل النظام الالكتروني

في القانون الجزائري نصت المادة 394 مكرر من قانون العقوبات الجزائري أن السلوك الإجرامي المكون للركن المادي ينحصر في الدخول أو البقاء

عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات. والملاحظ أن المشرع الحق فعل الولوج والبقاء غير المصرح به لهذه الجريمة، ويقصد بذلك التواجد داخل النظام المعلوماتي ضد إرادة من له الحق في السيطرة على هذا النظام (طه، 2017، 30). وقد يجتمع الدخول غير المشروع والبقاء غير المشروع معا وذلك في الفرض الذي لا يكون فيه الجاني الحق في الدخول إلى النظام، ويدخل إليه فعلا ضد إرادة من له حق السيطرة عليه، ثم يبقى داخل النظام بعد ذلك، ويتحقق في هذا الفرض الاجتماع المادي للجرائم. لكن قد ترتكب جريمة البقاء من دون الدخول غير المشروع، وذلك على فرض ان يكون للجاني الحق في الدخول إلى النظام ومصرح له بذلك، لكنه يتجاوز حدود هذا الحق والتصريح ويبقى داخل النظام بعد ذلك، مع اتجاه نيته لذلك.

والملاحظ أن جل عمليات الدخول (الاختراق) تتم من خلال برامج متوفرة على الانترانت يمكن لمن له خبرات تقنية أن يستخدمها بشن هجماته على أجهزة الغير (بوازدية، 2019، 79)، وتختلف الأهداف المباشرة للاختراقات، فقد تكون المعلومات هي الهدف المباشر، حيث يسعى المخترق إلى تغيير أو سرقة أو إزالة معلومات معينة، وقد يكون الجهاز هو الهدف المباشر بغض النظر عن المعلومات المخزنة عليه كأن يقوم المخترق بعمليته بقصد إبراز قدراته الاختراقية أو لإثبات وجود ثغرات في الجهاز المخترق (النحوي 2017، 82).

وليس من الضروري أن يقع الدخول إلى كامل النظام المعلوماتي لقيام الركن المادي لجريمة الدخول غير المشروع، بل يكفي أن يتم الدخول إلى جزء منه فأساس قيام الجريمة يهدف إلى حماية نظام المعالجة الآلية للمعطيات بصورة مباشرة (قورة، 2005، 28). وقد أكدت المادة 394 مكرر أعلاه على أن الدخول يتضمن «كل أو جزء من منظومة» للمعالجة الآلية للمعطيات. ويعني الدخول إلى جزء من النظام المعلوماتي الولوج إلى بعض مجالات النظام المعلوماتي كالدخول مثلا إلى برنامج معلوماتي معين أو إلى المعطيات الرقمية المعالجة في النظام(Pradel ,1990, 822).

اعتبر المشرع الجزائري جريمة الدخول غير المشروع من جرائم الخطر بموجب نص المادة 394 مكرر، فهي جريمة شكلية ولا يشترط لقيام الركن المادي فيها تحقق النتيجة الإجرامية بشرط أن يكون فعل الدخول بدون ترخيص مقصودا. ويتحقق السلوك الإجرامي لفعلي الدخول والبقاء بغض النظر عن أية نتيجة أخرى فلا يشترط لقيامهما التقاط المتدخل المعلومات التي يحتويها النظام أو بعضها أو استعمال تلك المعلومات (حجاج، عمرواي، 2020، 85). وعليه فلا مجال لبحث العلاقة السببية بين السلوك والنتيجة بعدّ الجريمة من جرائم الخطر. يؤخذ على المشرع الجزائري في المادة 394 مكرر من قانون العقوبات أنه استخدم عبارة "عن طريق الغش" لأنها توحي بضرورة وجود أجهزة حماية فنية كشرط مسبق للتمتع بالحماية الجزائية ضد الدخول غير المشروع. بمعنى إذا لم تكن الأنظمة الإلكترونية أمنة ولم يحطها أصحابها بأجهزة حماية فنية أو تلك التي لم تزود بهذه الأجهزة الفنية ولم يتم الدخول عن طريق الغش فيكون الدخول مشروعا (Forest, 2017, 65). وبذلك فإن الدخول إلى صندوق البريد الإلكتروني لأحد الأفراد يشكل جريمة الدخول غير المشروع إلى منظومة معلوماتية فقط إذا كان النظام محميا وليس مفتوحا أمام الجمهور، و أن يكون الدخول مخالفا لإرادة صاحب النظام (حجازي، 2002، 28).

وبالرجوع إلى نص المادة 394 مكرر1 من قانون العقوبات نجدها جرمت فعل إدخال الفاعل معطيات إلى النظام المعلوماتي أو إزالتها أو تعديلها بواسطة الغش، ونلاحظ أن المشرع أطلق لفظ المعطيات ولم يقيده بصنف معين. والمعطيات من الناحية الفنية وحتى القانونية لفظ يتسع ليشمل جملة من الأصناف، فيمكن أن تكون بيانات أو معلومات أو حتى برامج خبيثة فيروسات يقوم الفاعل بإدخالها إلى النظام بهدف التجسس وجمع البيانات الخاصة أو إدخال مواد إباحية يتعارض وجودها داخل النظام مع إرادة مالكه أو المسؤول عنه بغرض الإزعاج أو الضرر (العبيدي، 2012، 26، محمود طه، 2017، 304).

في القانون الأردني، جرمت المادة الثالثة من قانون الجرائم الإلكترونية الأردني عملية "الدخول قصدا إلى الشبكة الإلكترونية أو نظام معلومات بأي وسيلة دون تصريح أو بما يخالف أو يجاوز التصريح أو إذا كان الدخول لإلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو توقيف أو تعطيل عمل الشبكة الإلكترونية أو نظام معلومات الشبكة الإلكترونية أو كل من دخل موقع الكتروني لتغييره أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفته أو انتحال شخصية مالكه ".

ونلاحظ أن المشرع الأردني أسوة بالتشريع الجزائري جعل من صور الجريمة الإلكترونية عملية الدخول إلى الشبكة الإلكترونية أو نظام المعلومات ولم يعرف الدخول. وهذا المنهج الأسلم برأينا؛ لأن تجريم الدخول غير المصرح به للنظام المعلوماتي يرتبط بأمور تقنية متغيرة، ومتطورة فتعريف الدخول قد يحد من التجريم لعجز التعريف عن مجاراة واستيعاب المستجدات التكنولوجية (طه، 2017، 304، أيوب، 36). كما لم يشترط المشرع الأردني أسوة بالتشريع الجزائري أن يتم الدخول بوسيلة بعينها فكل الوسائل سواء، وقد عبر عن ذلك بموجب المادة 1/3 من قانون الجرائم الإلكترونية التي نصت على أن: " كل من دخل قصدا إلى موقع إلكتروني أو نظام معلومات بأي وسيلة". ويستوي في التجريم أن يتم الدخول على نحو مباشر أو غير مباشر كما هو الحال في الدخول عن بعد عن طريق شبكات الاتصالات. كما نلاحظ أن المشرع الأردني اشترط أسوة بالتشريع الجزائري أن يكون الدخول من غير المصرح له أومن يملك التصريح إلا أنه تجاوز حدود التصريح الممنوح له قانونا. وقد عرفت المادة الثانية من قانون الجرائم الإلكترونية التصريح بأنه: "الإذن الممنوح من صاحب العلاقة إلى شخص أو أكثر أو للجمهور للدخول إلى أو استخدام نظام المعلومات أو الشبكة

الإلكترونية بقصد الاطلاع أو إلغاء أو حذف أو إضافة أو تغيير أو إعادة نشر بيانات أو معلومات أو حجب الوصول إليها أو إيقاف عمل الأجهزة أو تغيير موقع الكتروني أو إلغائها أو تعديل محتوياتها".

تطلبت الفقرة ب من المادة الثالثة من قانون الجرائم الإلكترونية لقيام جريمة الدخول غير المصرح به أن يقصد الجاني من دخوله تحقيق أغراض محددة وهي: إلغاء، أو حذف، أو إضافة، أو تدمير، أو إفشاء، أو إتلاف، أو حجب، أو تعديل، أو تغيير، أو نقل، أو نسخ بيانات، أو معلومات، أو توقيف، أو تعطيل عمل الشبكة الإلكترونية أو نظام معلومات الشبكة الإلكترونية . أما الفقرة ج من المادة الثالثة فتطلبت أغراض مختلفة وهي: التغيير، أو الإلغاء، أو الإتلاف، أو التعديل للمحتويات، أو الإشغال، أو انتحال صفته أو انتحال شخصية المالك. مع ملاحظة أن الفقرة أ تجرم الدخول المجرد بدون تحديد الباعث على الدخول، وقد ذكر المشرع أفعال متعددة ومتداخلة أحيانا في المعنى كأغراض للدخول، ويعكس ذلك حرصه على ألا تفلت منه أي حالة من حالات الاعتداء على بيانات ومعلومات من التجريم. والمقصود بالإلغاء الإزالة سواء أكانت على نحو كلي أم جزئي، ولا يختلف مصطلح الحذف عن مصطلح الإلغاء فكلاهما تعني الإزالة. والإتلاف يكون بكل فعل يلحق ضررا بالشيء، أما التدمير فهو خراب شامل، والتغيير له مفهوم أوسع وأشمل فهو يكون بصورة إضافة أو تعديل أو حذف، والنقل يعني تغيير الموضع، والنسخ يتحقق في حالة الحصول على البيانات والمعلومات دون أن يؤدي ذلك إلى فقدان الأصل المنسوخ عنه، والإفشاء يكون بنشر البيانات والمعلومات دون تمييز، والإضافة تعني الزيادة أيا كان شكلها أو نوعها، والحجب يعني التستر والمنع والإخفاء(النوايسة، العدوان،، 2019، 265)، والتعديل يعني التغيير على النظام او المعلومات (الهيتي، 2006، 473)، والتوقيف يكون في حالة المنع والإعاقة عن العمل و التعطيل يعني التخريب أيا كان شكله، والإشغال يعني السيطرة على الموقع أو احتلاله. وانتحال الصفة يعني تصميم موقع يضاهي الموقع الأصلي، وانتحال شخصية المالك يعني إيهام الأخرين بأنه مالك الموقع.

ومن مظاهر الاختلاف بين التشريع الجزائري والأردني، أن المشرع الجزائري استخدم عبارات قليلة لأغراض الإدخال، وهي التخريب،الحذف، التعديل... وذلك بموجب القسم السابع مكرر الخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات من قانون العقوبات، الأمر الذي يضيق من نطاق التجريم.أيضًا، أن المشرع الأردني جرم بموجب الفقرة ب من المادة الثالثة من قانون الجرائم الإلكترونية الدخول بهدف تعطيل أجهزة أو الشبكات عن تأدية عملها بدون أن تتم عملية اختراق تلك الأجهزة، ويتم ذلك بإرسال عدد هائل من الرسائل بطرق فنية معينة إلى الأجهزة أو الشبكات المراد تعطيلها الأمر الذي يعيقها عن تأدية عملها(Perier, 2019: 21))، وهذا ما يتماشى مع مبادئ الاتفاقية الدولية للإجرام المعلوماتي التي جرمت الاعتداء العمدي على سير نظام المعالجة الآلية للمعطيات بموجب المادتان 5 و8.

كما نلاحظ أن المشرع الأردني لم يجرم البقاء غير المصرح به مع جريمة الدخول غير المصرح به إلى النظام الالكتروني، أسوة بنظيره المشرع الجزائري، الأمر الذي يؤدي إلى إفلات مرتكبي هذا الفعل من العقاب احتراما لمبدأ الشرعية. أيضًا نلاحظ أنه لم يشترط المشرع الأردني على خلاف المشرع الجزائري ضرورة توفر أجهزة حماية تقنية للنظام المعلوماتي حتى يعدُّ الدخول غير مشروع، الأمر الذي يوسع من نطاق الحماية الجزائية لهذه الجريمة.

وأخيرا نلاحظ أن المشرع الأردني استخدم لفظ البيانات والمعلومات محل جريمة الإدخال، وقد عرفت المادة الثانية من قانون الجرائم الإلكترونية البيانات بأنها: الأرقام، أو الحروف، أو الرموز، أو الأشكال، أو الأصوات، أو الصور، أو الرسومات التي ليس لها دلالة بذاتها.كما عرفت ذات المادة المعلومات بأنها: البيانات التي تمت معالجتها وأصبح لها دلالة.، وبمقارنة ذلك مع القانون الجزائري فقد استخدم لفظة المعطيات كمحل لجريمة الإدخال.

وبالرجوع كذلك للمادة 12من قانون الجرائم الإلكترونية نجدها جرمت في الفقرة أ و ج منها كل من يدخل قصدا دون تصريح أو بما يخالف أو يجاوز التصريح إلى الشبكة الإلكترونية أو نظام معلومات أو موقع ألكتروني بأي وسيلة كانت بهدف الاطلاع على بيانات او معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للملكة أو السلامة العامة أو الاقتصاد الوطني. كما تطلبت الفقرة ب و د من ذات المادة أن يكون الدخول بقصد إلغاء تلك البيانات أو المعلومات أوإتلافهاأو تدميرها أو تعديلها أو تغييرها أو نقلها أو نسخها او إفشائها. وقد أولى المشرع الأردني اهتمام اكبر ورعاية أكثر بتجريم الدخول قصدا إلى الشبكة الإلكترونية أو نظام المعلومات أو إلى المواقع الإلكترونية للمساس بالأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني. ويعد المحتوى الإلكتروني الغير متاح لعامة الناس هذا محلا للجريمة، وهو الذي يميزها عن جريمة الدخول غير المصرح به المجرد الواردة في المادة الثالثة من قانون الجرائم الإلكترونية. كما انه يتميز المحتوى غير المتاح للجمهور أن يكون مؤمن بوسائل حماية إلكترونية، وطبيعي أن يكون المحتوى محفوظ في موقع أو نظام معلومات أو شبكة معلوماتية حكومية، فكل ما يمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني هو شأن عام، لذا فمن الطبيعي أن الجهات المختصة لا تتيح هذه المعلومات للعامة، وهذا على خلاف المادة الثالثة من قانون الجرائم الإلكترونية (أيوب، 31).

2. جريمة التزوير الالكتروني

لم يستحدث قانون العقوبات الجزائري نصا خاصا بالتزوير المعلوماتي، وجعله يرد على المحررات فقط، وعليه لا يمكن إخضاع أفعال التزوير

المعلوماتي للنصوص العامة للتزوير (عمارة، 2019، 174)، كما هو عليه الحال في التشريع الفرنسي الذي أخضع أفعال التزوير المعلوماتي للنصوص العامة للتزوير وذلك بعد أن قام بتعديله بجعل م التزوير أي دعامة مادية وليس محررا(Gelbstein, E,2005,100, Quemener, M, yves, C, 2010, 13).

بالنسبة للمشرع الأردني، فقد عدل تعريف جريمة التزوير في أخر تعديل له لقانون العقوبات سنة 2022 في المادة 260 منه، حيث أصبح" تحريف مفتعل للحقيقة في الوقائع و البيانات التي يراد اثباتها بصك أو مخطوط أو بيانات نظام معلومات رسمي....". وعليه أصبح نص التجريم في قانون العقوبات لجريمة التزوير يطبق على جريمة التزوير الالكتروني. فبدلا من أن يكون محل هذه الجريمة فقط بيانات مستند أو محرر ورقي، أصبح من الممكن أن يكون أيضًا بيانات نظام معلومات رسمي. والسؤال الذي يمكن طرحه على المشرع الأردني لماذا اقتصر التزوير على بيانات نظام المعلومات مع انه كان بإمكانه إضافة الشبكة الإلكترونية والمواقع الإلكترونية بموجب قانون الجرائم الإلكترونية؟

ومن الجدير بالذكر، أنه قبل تعديل قانون العقوبات حول التزوير الألكتروني، كان النص المطبق في حال ارتكاب هذه الجريمة هو نص المادة الرابعة من قانون الجرائم الإلكترونية الذي جرم التزوير الألكتروني بطريقة غير مباشرة عندما جرم ادخال أو نشر أو استخدام قصدًا برنامجا عن طريق الشبكة الإلكترونية أو باستخدام نظام معلومات لتغيير أو تعديل أو تشويش المعلومات أو البيانات. وبرأينا أنه مع وجود نص صريح في قانون العقوبات يجرم التزوير الألكتروني فليس من الممكن تطبيق نص ضمني موجود في قانون أخر كقانون الجرائم الإلكترونية. خاصة أن نص قانون العقوبات على التزوير الالكتروني عاقب مرتكب هذه الجريمة بعقوبة أشد من العقوبة المنصوص عليها في قانون الجرائم الالكتونية.

يتمثل السلوك لجريمة التزوير الالكتروني في القيام بتحريف وتغيير الحقيقة الذي يعني إظهار الكذب في المعلومات المدرجة في نظام المعلومات بمظهر الحقيقة. يشترط في تحريف الحقيقة أن نكون أمام كذب مفتعل مكتوب، لأن التزوير لا يكون إلا مكتوبًا. أما عن النتيجة الجرمية لهذه الجريمة فهي إلحاق الضرر بالمجني عليه سوء أكان مادي أو معنوي أو اجتماعي، فالضرر ركن موضوعي في جريمة التزوير ولا تقوم الجريمة دون ضرر(السعيد، 2008، 95). وأخيرا يشترط توافر العلاقة السببية، أي أن فعل الفاعل في تغيير حقيقة المعلومات الواردة على نظام المعلومات هو الذي أدى إلى إلحاق الضرر بالمجني عليه.

3. جريمة الذم والقدح والتحقير في المجال الالكتروني

بالرجوع إلى القانون الجزائري، فقد عرفت المادة 296 من قانون العقوبات القذف بأنه: " كل ادعاء بواقعة من شأنها المساس بشرف وعدّ الأشخاص أو الهيئة المدعى عليها بهاو إسنادهم إليهم أو إلى الهيئة ويعاقب على نشر هذا الادعاء أو ذلك الإسناد مباشرة أو بطريق إعادة النشر حتى ولو تم ذلك وجه التشكيك أو إذا قصد به شخص أو هيئة دون ذكر الاسم ولكن كان من الممكن تحديدها من عبارات الحديث أو الصياح أو التهديد أو الكتابة أو المنشورات أو اللافتات أو الإعلانات موضوع الجريمة ". كما نصت المادة 297 من قانون العقوبات على جريمة السب بنصها" يعد سبا كل تعبير أو عبارة تتضمن تحقيرا أو قدحا لا ينطوي على إسناد أي واقعة " والملاحظة التي يمكن أن نستنتجها من خلال نصي المادتين أن المشرع الجزائري لم يتناول فكرة تجريم القذف و السب الالكتروني صراحة وبنص خاص وإنما طبق عليها أحكام جريمة القذف والسب في قانون العقوبات.

ويتمثل السلوك الجرمي لجريمة القذف والسب الالكتروني حسب النموذج القانوني للمادتين296-297 من قانون العقوبات بالادعاء أو الإسناد الذي من شأنه المساس بشرف المجني عليه واعتباره، و يتحقق ذلك بكل صيغة كلامية أو كتابية أو يتحقق أيضًا بكل صيغة تشكيكية من شأنها أن تلقي في أذهان الناس ظنا أو احتمالا ولو بصفة مؤقتة في صحة الأمور المدعاة، وهو ما يمكن أن يتحقق عبر مواقع التواصل الاجتماعي مثلا لاحتوائها على كل طرق النشر الكتابي او الصوتي أو المرئي (لسود، 2019).

على خلاف القانون الجزائري، نظم القانون الأردني جريمة الذم والقدح والتحقير الالكتروني في قانون الجرائم الإلكترونية، فقد نصت المادة 11منه على "يعاقب كل من قام قصدا بإرسال أو إعادة إرسال، أو نشر بيانات أو معلومات عن طريق الشبكة الإلكترونية ، أو الموقع الإلكتروني، أو أي نظام معلومات، تنطوي على ذم أو قدح أو تحقير أي شخص". وباستقراء نص المادة، نلاحظ أن سلوك جريمة الذم أو القدح أو التحقير يقوم بمجرد قيام الفاعل بإرسال أو إعادة إرسال أو نشر أي بيانات أو معلومات تنطوي على المساس بكرامة الأشخاص وشرفهم من خلال نظام المعلومات، أو الشبكة الإلكترونية ، أو الموقع الإلكتروني. ولا يشترط في دلالة المعلومات المرسلة أن تكون صريحة فقد تكون ضمنية(.(المادة 188/1-2 من قانون العقوبات)، وسواء فهم المجني عليه مضمونها أو لم يفهم تقوم الجريمة، فلم يفرق المشرع الأردني في المادة الثانية من قانون الجرائم الإلكترونية بين البيانات أو المعلومات التي تنطوي على الذم والقدح، فالبيانات لا تكون مفهومة وذات دلالة أحيانا إلا اذا تم معالجتها وتحويلها إلى معلومات (أبو رمان، 2018، 217). كما لا يشترط ذكر شخص المعتدى عليه صراحة بل يكفي أن يفهم من هو الشخص المقصود ضمنا (المادة 3/188 من قانون العقوبات). وتتمثل النتيجة الجرمية لهذه الجريمة في المساس بشرف واعتبار المجني عليه ومكانته الاجتماعية حتى ولو على سبيل الشك والاحتمال. مع ضرورة توافر العلاقة السببية بين فعل الفاعل والنتيجة الجرمية.

وفي إطار الدراسة التحليلية بين التشريعين الجزائري والأردني نلاحظ أن المشرع الجزائري قيد تحريك الدعوى العمومية في جريمة القذف على الإدعاء بالحق الشخصي، وان صفح الضحية يضع حد للمتابعة الجزائية، وهذا ما نصت عليه المادة 298 من قانون العقوباتفي القانون الأردني في

حين نلاحظ خلو قانون الجرائم الإلكترونية الأردني من النص على شرط تعليق تحريك الدعوى الذم والقدح والتحقير على الإدعاء بالحق الشخصي. وعيه فقد ترددت الإجتهادات القضائية حول ذلك، بداية اتجهت في قراراتها إلى أنه على الرغم من تطلب المشرع الأردني الإدعاء بالحق الشخصي لتحريك دعوى الحق العام في جرائم الذم والقدح والتحقير التقليدية (المادة 364 من قانون العقوبات) إلا أنه لم يشترط ذلك في الجرائم المرتكبة عبر الوسائل الإلكترونية، ولو أراد المشرع ذلك لنص عليه صراحة (محكمة بداية عمان بصفتها الإستئنافية بقرارها رقم 2630 تاريخ 2020/11/29). إلا أن محكمة التمييز في قرارها رقم1381 بتاريخ 2021/7/27 حسمت الأمر، وقررت أنه لو أراد المشرع عدم تطلب اتخاذ صفة الإدعاء بالحق الشخصي لجريمة الذم والقدح والتحقير الإلكتروني "لأفصح عن غايته تلك كما فعل بخصوص العقوبة، لذلك لا بد من الرجوع إلى قانون العقوبات بصفته موطن القواعد العامة في تحديد ماهية وأركان وعناصر جرائم الذم والقدح والتحقير وطريقة ملاحقتها، خاصة وأن الوسائل الإلكترونية ما هي إلا وسائل جديدة للنشر ولا يمكن أن تكون بحد ذاتها مانعًا من تطبيق الأحكام العامة الواردة في قانون العقوبات، طالما لم ينص عليها النص الخاص الوارد في المادة (11) من قانون الجرائم الإلكترونية ". بما أن جريمة الذم والقدح والتحقير من الجرائم المعلقة على الإدعاء بالحق الشخصي، فإنه ينطبق عليها الفقرة الأولى من نص المادة 52/أ من قانون العقوبات الأردني أي تسقط دعوى الحق العام تبعا لإسقاط الحق الشخصي.

بالرجوع إلى نص المادة 296 من قانون العقوبات الجزائري نجد أنها اشترطت العلنية لقيام هذه الجريمة وذكرت وسائلها وهي القول أو الجهر بالقول أو الكتابة أو التهديد أو المنشورات أو اللافتات أو الإعلانات موضوع الجريمة التي كلها تتحقق عبر مواقع التواصل الاجتماعي على سبيل المثال بعدّها عالم افتراضي.

أما في القانون الأردني، يخلو قانون الجرائم الإلكترونية الأردني من النص على شرط العلنية لقيام جريمة الذم والقدح والتحقير الألكتروني. ومع غياب النص اجتهد القضاء في ذلك، فقررت لمحكمة بداية مأدبا بصفتها الاستئنافية بقرارها رقم (2019/995) تاريخ 2019/10/29 على عدم أهمية هذا الشرط، حيث قضت "بأن الجرم المسند للمشتكى عليه هو جرم مخالفة المادة 11 من قانون الجرائم الإلكترونية وهو نص خاص قد ورد بقانون خاص نظم العلاقة الإلكترونية بين الأفراد وأية مراسلات تتم من خلالها وأي تجاوز لهذه العلاقة، وحيث لم يرد في متن المادة أي إشارة، أو تصريح لوجوب العلانية لقيام المساءلة الجزائية بحق المشتكى عليه الذي يعد مخلا بهذه العلاقة بأي فعل إلكتروني، ولا يمكن القول بعدّ العلانية ركنا من أركانه كجرم ولا مجال لتطبيق المادة 188من قانون العقوبات التي أوجبت العلانية ركنا أساسيا لهذا الجرم، وحيث ورد نص خاص وهو أولى بالتطبيق". وسندا لهذا القرار فإنه بمجرد قيام الفاعل بإرسال أو نشر بيانات أو معلومات عن طريق الشبكة الإلكترونية أو الموقع الالكتروني أو أي نظام معلومات تنطوي على الذم أو القدح أو التحقير تقوم الجريمة، وذلك على خلاف المادة 189 من قانون العقوبات الأردني التي اشترطت العلنية لقيام جريمة الذم والقدح (النوايسة،2017، 265، المناعسة، الزعبي، 2015، 335). وقبول هذا التوجه أي عدم تطلب العلانية لقيام جريمتي الذم والقدح المرتكبة عبر الوسائل الإلكترونية قد يفسر برغبة المشرع الأردني بتوسيع نطاق الحماية الجزائية للجرائم الإلكترونية نظرا لخصوصية طبيعة ارتكابها في عالم افتراضي يحتاج إلى تقنية عالية.

إلا انه بالنسبة للبعض(مصاروة، 2021، 97)فإن هذا التوسع قد يؤدي إلى اختلال مبدأ التناسب بين العقوبة والجريمة، فمن يقوم بذم أو قدح شخص برسالة مرسلة عبر (الواتس آب) أو (الماسنجر) أو (التويتر)، أو غيرها من مواقع التواصل الاجتماعي أي بدون علنية بحيث لم يشاهدها إلا الطرفان فقط ستكون عقوبته أشد ممن ذم أو قدح شخص في مجلس يحضره عشرة أشخاص مثلا، رغم ما لهذه الواقعة من مساس بالمكانة الاجتماعية للمعتدى عليه، والنيل من كرامته وشرفه واعتباره. ويؤيد الباحث هذا الرأي، ويرى أن العلنية شرط أساسي لقيام جريمة الذم والقدح والألكتروني، ومن الممكن أن نستند في ذلك على قرار محكمة التمييز السابق ذكره لسنة 2021 بحيث لو أراد المشرع عدم تطلب العلنية "لأفصح عن غايته تلك كما فعل بخصوص العقوبة، لذلك لا بد من الرجوع إلى قانون العقوبات بصفته موطن القواعد العامة في تحديد ماهية وأركان وعناصر هذه الجريمة".

المطلب الرابع: الركن المعنوي في الجريمة الإلكترونية

يعد الركن المعنوي الجانب الشخصي أو النفسي للجريمة فلا تقوم الجريمة بمجرد قيام الواقعة المادية وفق نموذجها القانوني، بل لا بد من أن تصدر الواقعة عن إرادة فاعلها وترتبط بها ارتباطًا معنويًا أو أدبيًا. وقد تطلب كل من القانون الجزائري والأردني القصد العام في جميع الجرائم الإلكترونية، كما تطلبا القصد الخاص في بعضها. يرتبط الركن المعنوي في إطاره العام بالجريمة الإلكترونية بوجوب علم الفاعل أن الفعل الذي يقوم به ينصب على نظام المعالجة الآلية للمعطيات بما يتضمنه من معلومات وبرامج حسب النصوص الخاصة بالجريمة الإلكترونية في قانون العقوبات الجزائري (خلاف، 2012، 337). كما أكد قانون الجرائم الإلكترونية الأردني في مواده على ضرورة أن يكون الفاعل عالما بأنه يدخل لموقع إلكتروني أو نظام معلومات، أو شبكة إلكترونية، وأنه غير مصرح له في الدخول.

كما يجب أن يعلم الفاعل بالنتيجة الجرمية لفعله والعلاقة السببية بينهما. فمثلا في جريمة التزوير الالكتروني يجب أن يدرك الفاعل انه يغير حقيقة المعلومات المدرجة على نظام معلومات رسمي، وإن من شأن هذا التغيير أن يترتب عليه ضرر يلحق بالأفراد أو الصالح العام(رستم،1995، 237).

أيضًا يجب أن تتجه إرادة الفاعل إلى القيام بالفعل المكون للجريمة الإلكترونية، وأن تكون إرادة حرّة وواعية. أيضًا يجب أن تتجه إرادة الفاعل إلى تحقيق نتيجة الجريمة الإلكترونية، فمثلا في جريمة الذم والقدح الالكتروني يجب أن تتجه إرادة الفاعل من وراء فعله الذي ينطوي على إسناد واقعة إلى المجني عليه إلى المساس بكرامته وشرفه ومكانته الاجتماعية، سواء أكان قصده مباشرا أو احتماليا بأن يتوقع هذه النتيجة ويقبل بها ويقبل بالمخاطرة. ونلاحظ أن كل من القانون الأردني والجزائري قد قصرا نطاق الحماية الجنائية للجريمة الإلكترونية على وجود القصد الجرمي لدى الجاني، فيشترط أن تكون الجريمة مقصودة، مما يشير أنه لا يسأل الفاعل عن الجريمة الإلكترونية إذا كان فعله ينطوي على خطأ سواء في صورة إهمال، أم قلة احتراز، أم عدم مراعاة القوانين والأنظمة (عبد الستار، 2010، 48)، الأمر الذي قد يضيق من نطاق الحماية الجزائية لهذه الجرائم بما لا يتناسب مع خطورتها.

إلى جانب توفر القصد الجنائي العام في جميع الجرائم الإلكترونية دون أي استثناء، اشترط المشرع الجزائري والأردني توفر القصد الخاص في بعض الجرائم الإلكترونية. فاستعمل المشرع الجزائري عبارة "عن طريق الغش" في المادة394 التي نظمت جريمة الدخول والتلاعب غير المشروع داخل النظام الالكتروني (التجسس) (بوخزة، 2012، 62). كما يجب أن يكون الدخول بقصد تحقيق الأغراض المحددة في ذات المادة التي تم شرحها سابقا في الركن المادي للجريمة.

في القانون الأردني لم يتطلب المشرع القصد الخاص في الفقرة أ من المادة الثالثة من قانون الجرائم الإلكترونية التي جرمت الدخول غير المصرح به للنظام المعلوماتي أو الشبكة الإلكترونية أو الموقع الألكتروني، إلا أنه تطلب ذلك في الفقرة ب و ج من ذات المادة، وهو أن يكون الدخول بقصد تحقيق الأغراض المحددة في ذات المادة التي تم شرحها سابقا في الركن المادي للجريمة. كما تطلبت المادة 12-أ و ج من ذات القانون القصد الخاص الذي يتمثل في أن تكون الغاية من الدخول غير المصرح به للنظام المعلوماتي أو الشبكة الإلكترونية أو الموقع الألكتروني "الاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للملكة أو السلامة العامة أو الاقتصاد الوطني". أما الفقرتان ب و د فقد تطلبتا إضافة للقصد السابق أن يكون الدخول لتحقيق أغراض محددة التي تم شرحها سابقا في الركن المادي للجريمة.وهناك بعض التشريعات رتبت على توفر القصد الخاص تشديد العقوبة كالدنمارك واستراليا والنرويج متى كان الفعل الإجرامي يسبب ضررا للغير مقابل الحصول على ربح مالي غير مشروع(.(André, 2018, 255).

المبحث الثاني:

السياسة العقابية للحد من الجريمة الإلكترونية في التشريعين الجزائري والأردني

يظهر الأثر التهديدي لقانون العقوبات من خلال الأوامر والنواهي بأحكامه، فتكون باعثا أو مانعا لهم من إتيان الفعل المحظور جنائيا، وفي حالة انتهاك هذه الأوامر والنواهي يتعرض مرتكبها لجزاء جنائي قد يستهدف حياته أو حريته أو ذمته المالية، ويطلق عليه العقوبة، ويمكن تشديدها حسب خطورة الجريمة وتأثيرها على الضحية والشهود و والمجتمع.

المطلب الأول: العقوبات الأصلية والتكميلية

تقتضي السياسة الجزائية في مجال العقاب إقرار عقوبات أصلية وتكميلية على مرتكبي الجرائم الإلكترونية. وباستقراء النصوص المتعلقة بالجرائم الماسة بالأنظمة الإلكترونية في التشريع الجزائري يتبين لنا وجود تدرج داخل النظام العقابي. هذا التدرج في العقوبات يحدد الخطورة الإجرامية التي قدرها المشرع لهذه التصرفات، إذ نجد سلم الخطورة يتضمن ثلاث درجات للعقوبة، بداية عاقبت المادة 394 مكرر من قانون العقوبات حالة الدخول والبقاء بالغش بالحبس من 3 أشهر إلى سنة و الغرامة المالية من 50000 دج إلى 100000 دج في،ثم عاقبت المادة 394 مكرر1 من قانون العقوبات بالحبس من ستة أشهر إلى ثلاث سنوات وغرامة من 500000 دج إلى 2000000 دج الاعتداء العمدي على المعطيات الموجودة داخل النظام، أخيرا، عاقبت المادة 394 مكرر 2 من قانون العقوبات استخدام المعطيات في ارتكاب الجرائم الماسة بالأنظمة الإلكترونية وكذا حيازة أو إفشاء أو نشر أو استعمال المعطيات المتحصل عليها من إحدى الجرائم الماسة بالأنظمة الإلكترونية بالحبس من شهرين إلى ثلاث سنوات وغرامة من 1000000 دج إلى 5000000 دج.

وفي جريمة القذف عاقب المشرع الجزائري مرتكبها بعقوبة بسيطة وهي الحبس من شهرين إلى ستة أشهر وبغرامة من 25.000 دج إلى 50.000 دج أو بإحدى العقوبتين. ويعاقب المشرع الجزائري السب إذا كان موجه إلى شخص أو أكثر بسبب انتماءهم إلى مجموعة عرقية أو مذهبية أوالى دين معين بالحبس من خمسة أيام إلى ستة أشهر وبغرامة من 5.000 إلى 50.000 دج أو بإحدى هاتين العقوبتين.

والملاحظ أن هذه العقوبات بسيطة مقارنة بخطورة الأفعال التي تهدد مصالح المجتمع في المجال المعلوماتي لذا لابد من المشرع أن يزيد من العقوبات المقررة للجريمةالإلكترونيةللحد من خطورتها(براهيمي 2016، 137).

في القانون الأردني، عاقب المشرع على جريمة الدخول والتلاعب في شبكة المعلومات أو نظام المعلومات في الفقرة أ من المادة الثالثة من قانون

الجرائم الإلكترونية بالحبس مدة لا تقل عن أسبوع ولا تزيد على ثلاثة أشهر أو بغرامة مالية لا تقل عن 100 مائة دينار ولا تزيد على 200 مائتي دينار أوبكلتا العقوبتين. كما عاقبت الفقرة أ و ج من المادة 12 من ذات القانون على جريمة الدخول والتلاعب في شبكة المعلومات أو نظام المعلومات أو موقع ألكتروني بهدف الاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني، أو العلاقات الخارجية للمملكة، أو السلامة العامة، أو الاقتصاد الوطني بالحبس مدة لا تقل عن أربعة أشهر وبغرامة لا تقل عن (500) خمسمائة دينار، ووضع المشرع حد أقصى للغرامة في الفقرة أ من نص التجريم بأن لا تزيد على (5000) خمسة آلاف دينار.

كما عاقب المشرع في المادة 11 من قانون الجرائم الإلكترونية جريمة الذم والقدح أو التحقير بالحبس مدة لا تقل عن ثلاثة أشهر وغرامة لا تقل عن 100 مائة دينار ولا تزيد على 2000 الف دينار. وأخيرا، عاقب المشرع في المواد 262،263 من قانون العقوبات مرتكب تزوير بيانات نظام المعلومات الرسمي إذا كان موظفا عاما بالأشغال المؤقتة بما لا يقل عن خمس سنوات. أما إذا ارتكب التزوير من مواطن عادي فتكون العقوبة الأشغال المؤقتة أو الاعتقال بموجب نص المادة 265 من ذات القانون. والملاحظ إن هذه العقوبات بسيطة مقارنة بالأفعال الخطيرة التي تعبر عن خطورة إجرامية تمس خصوصية الأفراد و المؤسسات.

ومما تجدر الإشارة إليه، أن جريمتي التجسس الإلكتروني والذم والقدح أو التحقير الالكتروني يمكن أن تكونا محلا للاشتراك الجرمي الأصلي والتبعي وفقا للأحكام العامة في قانون العقوبات. وقد خرج قانون الجرائم الإلكترونية الأردني على الأحكام العامة في الاشتراك الجرمي، وساوى بين عقوبة الاشتراك الأصلي والتبعي، فوفقا للمادة 14 يعاقب كل من قام قصدا بالاشتراك، أو التدخل، أو التحريض على ارتكاب أي من الجرائم المنصوص عليها في هذا القانون بالعقوبة المحددة فيه لمرتكبها. وأسوة بالقانون الأردني نص المشرع الجزائري على نص خاص حول الاشتراك الجرمي للجرائم الإلكترونية بموجب المادة 394 مكرر 3 من قانون العقوبات.

وفي الأخير، نلاحظ أن المشرع الأردني ترك معاقبة الشروع في الجرائم الإلكترونية للقواعد العامة في قانون العقوبات، فيعاقب دائما على الشروع في الجنايات الإلكترونية سندا للمادة 68 من قانون العقوبات. ولا يعاقب على الشروع بجنح الجرائم الإلكترونية لعدم وجود نص صريح بذلك سندا للمادة 71 من ذات القانون. وتنقسم جنح الجرائم الإلكترونية إلى قسمين جنح تستهدف الشبكة الإلكترونية، وجنح تتم بواسطة أنظمة المعلومات. يرى البعض أن الحكمة من عدم معاقبة الشروع في الجنح الإلكترونية صعوبة تحديد وقت ومكان ارتكاب الجريمة الإلكترونية (ابراهيم، 2009،82)، وصعوبة أظهار الركن المادي لهذه الجرائم كجريمة الذم والقدح فإما أن تقع كاملة أو لا تقع (الدلالعة،2005، 100 وما بعدها). إلا أن البعض الأخر يرد على هذا الأمر بالقول أن العديد من الجنح الإلكترونية تقبل فكرة الشروع كونه يمكن إظهار الركن المادي بها كجنحة الدخول إلى موقع الكتروني بدون تصريح أو الدخول بهدف الإطلاع المنصوص عليها في المادة 3 بجميع فقراتها والمادة (12/أو ج) من قانون الجرائم الإلكترونية. ذلك لأن الأعمال السابقة على إتمام هذه الجرائم وكذلك الأدوات التي أعدها الجاني لإنجاز فعله -كشراء برامج اختراق، وبرامج فيروسات، ومعدات التقاط الإشارات، وبرامج فك الشفرات، جميعها يمكن المعاقبة عليها(سمامعة، 2017، 66)، إذا أثبتت النيابة أن إرادة الجاني قد اتجهت عبر هذه التجهيزات إلى استهداف نظام المعلومات إما بقصد اختراقه فحسب، أو بقصد اختراقه وتخريبه (النوايسة،،2017، 265).

على خلاف المشرع الأردني، نص المشرع الجزائري بموجب المادة 394 مكرر 07 من قانون العقوبات على معاقبة الشروع في ارتكاب الجنح المنصوص عليها في القسم السابع المعنون بجرائم المساس بأنظمة المعالجة الآلية للمعطيات بالعقوبات المقررة للجنحة ذاتها. بذلك خرج المشرع عن القواعد العامة بغية توسيع الحماية الجزائية للجرائم الإلكترونية .

إن عدم تجريم الشروع في الجنح الإلكترونية في القانون الأردني قد يؤدي إلى ثغرات في نظام العقاب كونه لا يحمي المعطيات المخزنة والمتداولة عبر نظم المعلومات الإلكترونية والرقمية على نحو يخالف متطلبات الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2012 التي صادقت عليها الأردن بموجب القانون رقم 19 لسنة 2012 التي تطلبت المعاقبة على الشروع على الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية (٢/١/١٩).كما أن عدم التجريم للشروع لا يراعي الطبيعة الخاصة للجريمة الإلكترونية التي ترتكب باستخدام الأجهزة التقنية الحديثة ولا يأخذ بعين الاعتبار زيادة التعاملات من خلال الإنترنت ونشاط التجارة الإلكترونية، خاصة وأن نسبة كبيرة من الأفراد والشركات والجهات المختلفة خسرتٍ كبيرة بسبب التعامل بالوسائل الإلكترونية (سمامعة،67). إضافة للعقوبات الأصلية التي فرضها القانون الجزائري والأردني على مرتكبي الجرائم الإلكترونية، فقد قاما بالنص على عقوبات تكميلية.

في القانون الجزائري، نصت المادة 394 مكرر 3 قانون العقوبات على العقوبات التكميلية إلى جانب العقوبات الأصلية أهمها المصادرة، و إغلاق المواقع التي تكون محلا لجريمة من الجرائم الماسة بالأنظمة الإلكترونية (طه، 2017، 304). أما في القانون الأردني، تحكم المحكمة المختصة بالمصادرة، وإغلاق المحل الذي ارتكبت فيه الجريمة. ويقصد بالمصادرة نزع ملكية شيء ثبتت صلته بالجريمة المرتكبة، وإضافته إلى أملاك الدولة دون مقابل، والمصادرة تكون عقوبة تكميلية عندما ترد على شيء يباح حيازته وتداوله، ولا يحكم بها في هذه الحالة إلا تبعا للحكم بعقوبة أصلية، وتكون المصادرة تدبيرا احترازية متى وقعت على شيء تعد حيازته أو تداوله جريمة وتكون في هذه الحالة وجوبية، وقد جعلت المادة 13/ج من قانون الجرائم الإلكترونية

الحكم بالمصادرة أمرا جوازيا للمحكمة وجاء فيها "أن للمحكمة المختصة الحكم بمصادرة الأجهزة والأدوات والوسائل والمواد وتوقيف أو تعطيل عمل أي نظام معلومات أو موقع إلكتروني مستخدم في ارتكاب أي من الجرائم المنصوص عليها أو يشملها هذا القانون".

المطلب الثاني: الظروف المشددة لمرتكبي الجرائم الإلكترونية في ظل التشريعين الجزائري والأردني

تتطلب السياسة الجزائية ضرورة تشديد العقاب لمرتكبي الجرائم الإلكترونية في حالة المساس أكثر بالمصالح الجديرة بالحماية و لخطورتهم الإجرامية، وهذا ما تبناه المشرع الجزائري. في القانون الجزائري، شدد المشرع من عقوبة الدخول أو البقاء بدون ترخيص في نظام المعالجة الآلية. بموجب الفقرة الثانية من المادة 394 مكرر من قانون العقوبات بمضاعفة العقوبة إذا ترتب على ذلك حذف أو تغيير المعطيات المنظومة أو ترتب عن الأفعال المذكورة تخريب نظام اشتغال المنظومة بعقوبة الحبس من 6 أشهر إلى سنتين والغرامة من 50.000 دج إلى 150.000 دج (دردور 2013، 304).

كما شدد العقوبات إذا كان القذف الموجه إلى شخص أو أكثر بسبب انتماءهم إلى مجموعة عرقية أو مذهبية ا والى دين معين من شهر إلى سنة أو بغرامة مالية 10.000الى 100.000 أو بإحدى العقوبتين فقط إذا كان الغرض هو التحريض على الكراهية بين المواطنين وتشدد عقوبة السب إلى الحبس من شهر إلى ثلاثة أشهر وبغرامة من 10.00 دج و 25.000. ونلاحظ من خلال هذه العقوبات سواء كانت بسيطة أو مشددة هي عقوبات بسيطة جدا مقارنة بخطورة الأفعال الإجرامية خاصة إذا تمت عبر الوسائل الالكتروني فليس من المعقول أن نعاقب شخص بالغرامة المالية فقط قيامه بالتحريض وبث الكراهية بين المواطنين عبر وسائل التواصل الاجتماعي، ولعل هذا ما تفطن له المشرع الجزائري من خلال سن القانون رقم 20-05 لسنة 2020 المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتها الذي عاقب بموجب المادة 30 منه بالحبس من ستة أشهر إلى ثلاث سنوات، وبغرامة من 60.000الى 300.000 دج كل من يقوم بجميع أشكال التعبير التي تنشر أو تشجع أو تبرر التمييز وكذا تلك التي تتضمن أسلوب الازدراء أو الاهانة أو العداء أو البغض أو العنف للموجهة إلى شخص من الأشخاص على أساس الجنس أو العرق أو اللون أو النسب أو الأصل القومي أو ألاثني أو العرقي أو اللغة أو الانتماء الجغرافي أو الإعاقة أو الحالة الصحية. وفي اعتقادنا انه لابد من حذف المادة 298 الفقرة الثانية من قانون العقوبات لارتباطها بقانون الوقاية من التمييز وخطاب الكراهية ومكافحتها لأنه في كل الأحوال سوف تطبق أحكامه وفق قاعدة الخاص يقيد العام.

في القانون الأردني، كما شدد المشرع في المادة 16 من قانون الجرائم الإلكترونية عقوبة الجرائم المنصوص عليها في هذا القانون بأن ضاعف العقوبة في حالة التكرار، والتكرار المقصود هنا تكرار الجرائم الإلكترونية وليس التكرار المقصود في قانون العقوبات في المواد من 102-105. أيضًا، شدد المشرع العقوبات إذا كان القصد الخاص من الدخول إلى النظام الألكتروني أو الشبكة الإلكترونية أو الموقع الألكتروني تحقيق الأغراض المنصوص عليها بموجب الفقرة ب و د من المادة الثالثة من قانون الجرائم الإلكترونية، بأن تصبح الحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد عن سنة وبغرامة لا تقل عن 200 مائتي دينار ولا تزيد على 1000 ألف دينار. كما شدد المشرع العقوبات إذا كان القصد الخاص من الدخول إلى النظام الألكتروني أو الشبكة الإلكترونية أو الموقع الألكتروني الذي يمس الأمن الوطني أو العلاقات الخارجية للملكة أو السلامة العامة أو الاقتصاد الوطني بقصد تحقيق الأغراض المنصوص عليها بموجب الفقرة ب و د من المادة 12 من ذات القانون، بأن تصبح الأشغال الشاقة المؤقتة وبغرامة لا تقل عن 1000 ألف دينار ولا تزيد على 5000 خمسة ألاف دينار.

الخاتمة

تعدُّ الجريمة الإلكترونية من الجرائم التي يصعب الكشف عنها ويسهل إتلاف الدليل المادي فيها، لذلك فقد استحدثت كل من الجزائر والأردن هيئات ومراكز للوقاية من هذه الجرائم ومكافحتها والكشف عنها وملاحقة مرتكبيها. إن الجريمة الإلكترونية من الجرائم العابرة للحدود الوطنية، لذلك نظم قانون الجرائم الإلكترونية الأردني قواعد الاختصاص القضائي والمكاني لهذه الجريمة ها على خلاف ذلك، لم يخصص القانون الجزائري نصا ينظم ذلك. لم يشترط القانون الأردني في عملية الدخول للنظام المعلوماتي ضرورة توفر أجهزة حماية تقنية كشرط مسبق للتمتع بالحماية الجزائية، على خلاف القانون الجزائري الذي تطلب أن يكون الدخول للنظام المعلوماتي عن طريق الغش.

من مظاهر الاختلاف بين التشريع الجزائري والأردني أن هذا الأخير جرم بموجب المادة الثالثة من قانون الجرائم الإلكترونية الدخول بهدف تعطيل أجهزة أو شبكات عن تأدية عملها، وهذا ما يتماشى مع مبادئ الاتفاقية الدولية للإجرام المعلوماتي التي جرمت الاعتداء العمدي على سير نظام المعالجة الآلية للمعطيات. ومن ناحية أخرى، اعتبر القانون الأردني والجزائري جريمة الدخول غير المشروع إلى النظام الالكتروني من الجرائم الشكلية التي لا يشترط لقيام الركن المادي فيها تحقق النتيجة الإجرامية. علاوة على ذلك، لم يجرم المشرع الأردني البقاء غير المصرح به في النظام الإلكتروني، أسوة بنظيره المشرع الجزائري، الأمر الذي يؤدي إلى إفلات مرتكبي هذا الفعل من العقاب احتراما لمبدأ الشرعية. وجرم المشرع الأردني التزوير الالكتروني بموجب تعديل قانون العقوبات سنة 2022 في المادة 260 منه، عندما عدل تعريف جريمة التزوير بحيث أصبح محلها يشمل بيانات نظام المعلومات الرسمي. على خلاف ذلك لم يعالج المشرع الجزائري جريمة التزوير المعلوماتي سواء في قانون العقوبات أو في أي قانون خاص. خرج المشرع الأردني والجزائري عن القواعد العامة في التجريم والعقاب المطبقة في حالة الاشتراك الجرمي، بأن عاقبا الاشتراك، أو التدخل، أو التحريض على

ارتكاب أي من الجرائم الإلكترونية بالعقوبة المحددة لمرتكبها، بينما أحسن المشرع الجزائري بمعاقبة الشروع على ارتكاب جنح المساس بأنظمة المعالجة الآلية للمعطيات بالعقوبات المقررة للجنحة ذاتها. على خلاف المشرع الأردني الذي لم ينص على معاقبة الشروع في الجنح الإلكترونية المجرمة بموجب قانون الجرائم الإلكترونية أو أي قانون أخر. لقد تبنى التشريع الجزائري والأردني تشديد العقوبات على مرتكبي الجريمة الإلكترونية في حالة زيادة الخطورة الإجرامية التي تهدد المصالح الجديرة بالحماية، إلا أن هذه العقوبات ما زالت تتسم بالبساطة وعدم تناسبها مع الأفعال الإجرامية المكونة للجريمة الإلكترونية، الأمر الذي قد لا يحقق أهداف العقوبة الرئيسية بالردع العام والخاص.

التوصيات:

1- نوصي المشرع الجزائري إلغاء نص المادة الثانية من من قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها رقم 09-04 سنة 2009 الذي يعرف الجريمة الإلكترونية، وترك الأمر للفقه نظرا لصعوبة إيجاد تعريف دقيق وجامع ومانع لها.

2- نوصي المشرع الجزائري أسوة بالمشرع الأردني، بإضافة نص صريح يحدد قواعد الاختصاص المكاني للجريمة الإلكترونية، بأن يكون القانون الجزائري واجب التطبيق إذا ارتكبت أي من الجرائم الإلكترونية المنصوص عليها في قانون العقوبات باستخدام أنظمة معلومات على أرض الجزائر أو ألحقت أضرارا بأي من مصالحها أو بأحد المقيمين فيها أو ترتبت آثار الجريمة فيها، كليا أو جزئيا، أو ارتكبت من أحد الأشخاص المقيمين فيها.

3- نوصي المشرع الجزائري أسوة بنظيره المشرع الأردني بتجريم الدخول لنظام معلومات بغية تعطيل أجهزة أو شبكات عن تأدية عملها.

4- نوصي المشرع الجزائري أسوة بنظيره المشرع الأردني بتعديل القصد الخاص لجريمة الدخول غير المصرح به للنظام المعلوماتي، حتى لا يفلت الفاعل من العقاب في أي حالة من حالات الاعتداء على المعطيات من العقاب، وذلك بداية بإلغاء عبارة "عن طريق الغش"، ثم إضافة غايات أخرى للدخول وهي: الإلغاء أو الإضافة أو التدمير والإفشاء أو إتلاف أو حجب أو تغيير أو نقل أو نسخ المعطيات،أو الدخول للنظام بغية انتحال صفته أو انتحال شخصية مالكه.

5- نوصي المشرع الأردني بتجريم البقاء غير المصرح به في النظام الإلكتروني أو الشبكة المعلوماتية أو الموقع الإلكتروني، أسوة بنظيره المشرع الجزائري.

6- تعديل نص قانون العقوبات الجزائري الذي يعرف جريمة التزوير، ليصبح قابل للتطبيق على التزوير المعلوماتي، وذلك على النحو التالي: "كل تغيير للحقيقة بطريق الغش في مكتوب أو في أي نظام معلوماتي".

7- نوصي المشرع الأردني بالنص صراحة على معاقبة الشروع في الجنح الإلكترونية التي تضمنها قانون الجرائم الإلكترونية أو أي قانون أخر، أسوة بما فعله المشرع الجزائري وبما يتفق مع متطلبات الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2012.

8- مد نطاق الحماية الجزائية في القانون الأردني والجزائري، وتجريم الحالات التي تقع فيها الجرائم الإلكترونية نتيجة الإهمال أو التقصير أو الخطأ نظرا لخطورة هذه الجرائم والأضرار التي قد تسببها.

9- ضرورة إعادة النظر بالنسبة للتشريعين الجزائري والأردني في العقوبات المقررة لمرتكبي الجرائمالإلكترونية و الظروف المشددة لها، كونها بسيطة ولا تعكس جسامة الأفعال المكونة لهذه الجرائم، فمثلا لابد من تعديل نص المادة (12/أ و د) من قانون الجرائم الإلكترونية الأردني وذلك بتشديد عقوبة الدخول غير المشروع على البيانات والمعلومات غير المتاحة للجمهور وتمس الأمن الوطني بهدف الإطلاع عليها، بحيث يتم رفع الحد الأدنى والأعلى للعقوبة الجنائية لاسيما أن أفعاله قد تتخذ صور نسخ أو إفشاء أو إتلاف بيانات سرية تخص الدولة.

المصادروالمراجع

إبراهيم، خ. (2009). *الجرائم المعلوماتية*. دار الفكر الجامعي.

الخبيزي، ب. (2017). *الجرائم الإلكترونية من وجهة نظر اجتماعية*. القاهرة: دريم بوك للنشر والتوزيع.

الدلالعة، س. (2005). *الحماية القانونية الدولية والوطنية لتكنولوجيا المعلومات، "برامج وأنظمة الحاسب الآلي"*: دراسة مقارنة. جامعة آل البيت.

رستم، ه. (1995). *قانون العقوبات ومخاطر تقنية المعلومات*. أسيوط: مكتبة الآلات الكاتبة.

السعيد، ك. (2008). *شرح قانون العقوبات (الجرائم المضرة بالمصلحة العامة)*. عمان: دار الثقافة، عمان.

طه، م. (2017). *المواجهة التشريعية لجرائم الكمبيوتر والانترانت*. مصر: دار الفكر والقانون.

عبد الستار، ف. (2010). *النظرية العامة للخطأ غير العمدي*. القاهرة: دار النهضة العربية.

قارة، أ. (2006). *الحماية الجنائية للمعلوماتية في التشريع الجزائري*. (ط1). دار هومة.
قشقوش، هـ. (1992). *جرائم الحاسب الإلكتروني في التشريع المقارن. القاهرة:* دار النهضة العربية.
قورة، ن. (2005). *جرائم الحاسب الآلي الاقتصادية*. (ط1). بيروت: منشورات الحلبي الحقوقية.
لطفي، خ. (2019). *الدليل الرقمي ودوره في إثبات الجريمة الإلكترونية*. الاسكندرية: دار الفكر الجامعي.
المناعسة، أ.، والزعبي، ج. (2014). *جرائم تقنية نظم المعلومات الإلكترونية:* دراسة مقارنة. (ط2). عمان: دار الثقافة.
النوايسة، ع. (2017). *جرائم تكنولوجيا المعلومات، شرح الأحكام الموضوعية في قانون الجرائم الإلكترونية*. عمان: دار وائل للنشر.
الهيتي، م. (2006). *جرائم الحاسوب*. عمان: دار المناهج للنشر والتوزيع.
يوسف، أ. (2011). *الجريمة الإلكترونية والإلكترونية والجهود الدولية والمحلية لمكافحة جرائم الكومبيوتر والانترنت*. (ط1). الاسكندرية: مكتبة الوفاء القانونية للنشر.
أبو رمان، م. (2018). *التنظيم القانوني لجريمة الذم الإلكتروني في التشريع الأردني. مجلة دراسات، جامعة عمار ثلجي بالأغواط*، (264).
الجبرة، ع.، العراسي، س.، والمناصير، ص. (2021). أثر الجريمة الإلكترونية على سير المرافق العامة الإلكترونية في التشريع الأردني. *مجلة الزرقاء للبحوث والدراسات الانسانية*، 21(2)، 346- 366.
الزبن، غ.، والخرابشة، ع. (2021). الجرائم الإلكترونية ومستوى الوعي بخطورتها: دراسة ميدانية على عينة من الشباب الجامعي الأردني. *مجلة الجامعة الاسلامية للدراسات الانسانية*، 29(2)، 230 – 248.
براهيمي، ج. (2016). مكافحة الجرائم الإلكترونية في التشريع الجزائري. المجلة النقدية للقانون والعلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، (2).
بوازدية، ج. (2019). الإستراتيجية في مواجهة الجرائم السيبرانية التحديات والأفاق المستقبلية. *مجلة العلوم القانونية والسياسية*، 10(1).
بوبرقيف، ع. (2019). *مفهوم أنظمة المعالجة الآلية للمعطيات في الجرائم المحددة في المواد 394 مكرر 394 مكرر 2من قانون العقوبات. مجلة الدراسات والبحوث القانونية*، 4(1).
حجاج، م.، وعمرواي، م. (2020). حماية الحق في الخصوصية عبر الانترانت: دراسة وصفية تحليلية وفق قانون العقوبات. *مجلة دراسات وأبحاث*، 12(3).
خرشي، إ. (2022). النظام القانوني للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها. *مجلة الأبحاث القانونية والسياسية*، 4(1).
خلاف، ب. (2012). التنظيم القانوني للجريمة الإلكترونية في الجزائر. *مجلة العلوم القانونية والاجتماعية*، 6(2).
سمامعة، خ. (2017). الشروع في الجرائم الإلكترونية وفقا لأحكام القانون الأردني: دراسة تحليلية مقارنة. *المجلة الأردنية في القانون والعلوم السياسية*، 9(4).
العبيدي، أ. (2012). جريمة الدخول غير المشروع إلى النظام المعلوماتي. *مجلة دراسات المعلومات*، (14).
لسود م، (2019). التكييف القانوني لجريمة القذف عبر مواقع التواصل الاجتماعي في التشريع الجزائري. *مجلة الدراسات القانونية والسياسية*، 5(1).
مصاروة، س. (2021). إشكالية تطبيق النصوص الناظمة لجرائم الذم والقدح والتحقير الإلكترونية في التشريع الأردني: دراسة تحليلية. المجلة الأردنية في القانون والعلوم السياسية، 13(4).
نبيل، و.، وعبد الرؤوف، ز. (2019). الجريمة الإلكترونية في التشريع الجزائري. *مجلة العلوم القانونية والاجتماعية*، 4(3).
الزايد، إ. (2011). *نطاق المسؤولية الجزائية عن جرائم الذم والقدح والتحقير المرتكبة من خلال المواقع الإلكترونية. رسالة ماجستر غير منشورة*، جامعة الشرق الأوسط، عمان.
بوخزة، ع. (2012). *الحماية الجزائية من الجريمة الإلكترونية في التشريع الجزائري. رسالة ماجستر في القانون الجنائي*، كلية الحقوق، جامعة وهران.
دردور، ن. (2012). *جرائم الإلكترونية على ضوء القانون الجزائري والمقارن. رسالة ماجستير في القانون الجنائي*، كلية الحقوق، جامعة منتوري، قسنطينة.
رابحي، ع. (2018). *الأسرار الإلكترونية وحمايتها الجزائية. أطروحة لنيل شهادة الدكتوراه*، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان.
لدادوة، ع. (2021). *مدى ملاءمة نصوص قانون الجرائم الإلكترونية الأردنية للأحكام العامة لقانون العقوبات. رسالة ماجستر في القانون العام*، جامعة الشرق الأوسط، عمان.
أيوب، إ. (2020). *اتجاهات القضاة والمحامين نحو تعديل قانون الجرائم الإلكترونية واثره في الحد من ارتكاب الجريمة. اطروحة دكتوراه*، دراسة ميدانية في المملكة الأردنية الهاشمية،جامعة مؤتة، كلية الدراسات العليا، الأردن.
البداينة، ذ. (2018). الجرائم الإلكترونية: المفهوم والأسباب. *الملتقى العلمي: الجرائم المستحدثة في ظل المتغيرات والمتحولات الاقليمية والدولية*، الأردن.
النوايران، ث. (2019). الجرائم الإلكترونية وطرق الحد منها: تجربة الأردن. *المؤتمر الدولي الأول لمكافحة الجرائم الإلكترونية، جامعة الإمام محمد بن سعود الإسلامية، كلية الحاسب والمعلومات، المملكة العربية السعودية.*
عاقلي، ف. (2017). الجريمة الإلكترونية وإجراءات مواجهتها من خلال تشريع الجزائري. *أعمال المؤتمر الدولي الرابع عشر، الموسوم بعنوان: الجرائم الإلكترونية، المنعقد بطرابلس، لبنان.*

References

Alsawalqa, R. O. (2021). Cyberbullying, social stigma, and self-esteem: the impact of COVID-19 on students from East and Southeast Asia at the University of Jordan. *Heliyon*, *7*(4). https://doi.org/10.1016/j.heliyon.2021.e0671

André, C. (2019). *Droit pénal spécial*. Dalloz.

Choi, S., & Parti, K. (2022). Understanding the Challenges of Cryptography-Related Cybercrime and Its Investigation. https://vc.bridgew.edu/ijcic/vol5/iss2/1

Deora, R. S., & Chudasama, D. (2021). Brief study of cybercrime on the internet. *Journal of communication engineering & Systems*, *11*(1), 1-6.

Forest, D. (2017). *Droit des logiciels gualina*. France.

Gandhi, V. K., & Thanjavur, T. N. S. I. (2012). An overview study on cybercrimes in internet. *Journal of Information Engineering and Applications*, *2*(1), 1-5.

Kurbalija, J., & Gelbstein, E. (2005). *Gouvernance de l'internet: enjeux, acteurs et fractures*. DiploFoundation.

Van Hoecke, M. (2013). Methodology of comparative legal research. *Pravovedenie*, 121.

Perier, B. (2019). *Responsabilité pénale*. France: Dalloz.

Pradel, J. (1990). Les infractions relatives à l'informatique. *Revue internationale de droit comparé*, *42*(2), 815-828.

Quéméner, M., & Charpenel, Y. (2010). Cybercriminalité. *Droit pénal appliqué, Paris: Economica, coll. Pratique du droit*, 7.

Sinha,R., & Vidyapeeth, N. (2018). Socia Impact of Cyber Crime: A Sociological Analysis. *International Journal of Management, IT & Engineering*, 10(1), 254-259. http://dx.doi.org/10.13140/RG.2.2.20922.93126.

Yar, M. (2013). Cybercrime and society. *Cybercrime and Society*, 1-232.