

الأساليب والاستراتيجيات للحد من الجرائم الإلكترونية في المجتمع الفلسطيني
Methods and Strategies to Reduce Cybercrime in Palestinian Society

ط د/ معاذ عليوي^١، د/ وليد جلعود^٢

^١ جامعة نجم الدين أربكان- تركيا، muath.ilaiwi@gmail.com

^٢ وزارة التربية والتعليم- فلسطين ، wldjaloud@gmail.com

تاريخ الاستلام: 2022/10/23 تاريخ القبول: 2022/11/28 تاريخ النشر: 2022/12/17

Doi: 10.21608/skje.2022.274578

مستخلص البحث:

هدفت هذه الدراسة إلى التعرف على الأساليب والاستراتيجيات المتبعة في المجتمع الفلسطيني للحد من الجرائم الإلكترونية فيه، وسط بيئة خاصةً بالمجتمع الفلسطيني تتمثل بوجود الاحتلال الإسرائيلي، وعدم قيام الدولة الفلسطينية، حيث تم وضع عدة أسئلة تتعلق بالمفهوم الجريمة الإلكترونية وأنوعها وآليات الحد منها في المجتمع الفلسطيني. توصلت الدراسة إلى عدة نتائج أهمها: غياب تطبيق منظومة التشريع الفلسطيني نظراً للحالة الفلسطينية الراهنة التي تمرّ بها سواء من خلال حالة الانقسام التي عطلت اعمال المجلس التشريعي الفلسطيني ودوره عن إصدار القوانين من جهة، وعدم الاستقرار السياسي والاجتماعي داخل البيئة الفلسطينية من جهةٍ أخرى. توصي هذه الدراسة بإجراء الانتخابات في الشارع الفلسطيني بهدف إعادة إحياء دور وعمل المجلس التشريعي الفلسطيني في سن القوانين التشريعية ذات العلاقة بالجريمة الإلكترونية والحد من تفشيها وخطورتها داخل المجتمع. وتخصيص مساقات جامعية تقنية وتطبيقية يتم من خلالها تزويد الطلاب بكافة المهارات والأدوات التكنولوجية للوقاية من مخاطر الجريمة الإلكترونية وتداعياتها السلبية على المجتمع. الكلمات المفتاحية : الجريمة الإلكترونية، المجتمع الفلسطيني، الرقمنة، مكافحة الجريمة الإلكترونية.

Abstract:

This study aimed to identify the methods and strategies used in the Palestinian society to reduce cybercrime in it, amid a special environment for the Palestinian society represented by the presence of the Israeli occupation, and the non-establishment of the Palestinian state, where several questions were developed related to the concept of cybercrime, its types and mechanisms to reduce it in the Palestinian society. The study reached several results, the most important of which are: the absence of the application of the Palestinian legislation system due to the current Palestinian situation it is going through, whether through the state of division that disrupted the work of the Palestinian Legislative Council and its role in issuing laws on the one hand, and the political and social instability within the Palestinian environment on the other hand.

This study recommends holding elections in the Palestinian street with the aim of reviving the role and work of the Palestinian Legislative Council in enacting legislative laws related to cybercrime and reducing its spread and danger within society. And allocating technical and applied university courses through which students are equipped with all the skills and technological tools to prevent the risks of cybercrime and its negative repercussions on society

Keywords cybercrime, Palestinian society, digitalization, combating cybercrime.

مقدمة:

تعتبر الجريمة ظاهرة اجتماعية قديمة تواجدت بتواجد الإنسان، ورافقت المجتمع البشري منذ نشأته، عبر عنها إيميل دور كايم "بالأنومي" وهو خلل وارتباك وبعثرة في العلاقات والسلوك الاجتماعي. ومع تطور المجتمع وظهور الثورة المعلوماتية وخدمة الأنترنت أدى إلى ظهور أنماط جديدة من الجرائم لم تكن مألوفة من قبل، فالمجرمين استفادوا من التقدم التقني للقيام بجرائم تقليدية بوسائل تكنولوجية متطورة، مما جعلها تشكل خطورة على المجتمعات رغم اختلافها، وتعدّها للحدود لتصبح دولية عابرة للقارات من كل الجنسيات.

أما في العصر الحديث فقد أصبحت الجريمة ترتكب بشكل أكثر احترافية عمّا كان عليه سابقاً، فقد أصبحت تعتمد على الذكاء والعقل وليس القوة البدنية كما كان سائداً في العصر القديم، وأصبح الضرر الذي تلحقه هذه الجرائم كبيراً لا يقتصر على

الفرد فقط وإنما يشمل الدول لاسيما وأنها أصبحت تتميز في ظل العولمة بخصائص جديدة عن الجريمة التقليدية سواء من حيث الأثر كالجريمة البيئية مثل النفايات السامة والضارة والنوعية أو من حيث الوسائل والأثار كالجرائم المعلوماتية، ويتضاعف خطر هذه الجرائم كونها لا تعترف بالحدود الجغرافية للدول ولا حتى بالقارات، لأنه مع انتشار شبكة الاتصالات العالمية الأنترنت أمكن ربط أعداد هائلة لا حصر لها من الحواسيب عبر العالم لهذه الشبكة، فقد يكون الجاني في قارة والمجني عليه في قارة أخرى تماماً، وعليه فالجرائم الإلكترونية تقع في أغلب الأحيان عبر حدود دولية كثيرة. فقد تأثر المجتمع الفلسطيني كغيره من المجتمعات الأخرى بشكل كبير بهذا التطور الهائل في مجال الاتصالات وتكنولوجيا المعلومات. حيث تشير العديد من الدراسات والاحصائيات إلى أن هناك نمواً مستمراً ومتسارعاً في أعداد المستخدمين للتكنولوجيا والأنترنت في الأعوام الأخيرة. ووفقاً لتقرير الجهاز المركزي للإحصاء الفلسطيني فإن ٨٢% من الشبان الفلسطينيين يمتلكون المهارات الأساسية اللازمة لاستخدام أدوات التكنولوجيا بما فيها استخدام خدمات الأنترنت.

وعلى الرغم من الجهود الحثيثة والمتواصلة لمكافحة الجريمة الإلكترونية في فلسطين، وإقرار قانون الجرائم الإلكترونية المعدل لعام ٢٠١٨م وإنشاء وحدة الجرائم الإلكترونية، وما أعقبه من افتتاح مركز فلسطين لطوارئ الحاسوب في عام ٢٠١٩، إلا أن العديد من الدراسات والأبحاث العلمية تشير إلى أن هناك زيادة في نسبة الجرائم الإلكترونية في المجتمع الفلسطيني وهذا يعود إلى غياب الوعي التقني والقانوني لدى مستخدمي أدوات تكنولوجيا المعلومات وخصوصاً فئة الشباب

٢. مشكلة الدراسة

إن انتشار تكنولوجيا المعلومات والاتصالات أدى إلى ظهور العديد من أشكال الجريمة الإلكترونية وانتشارها مثل: انتهاك الخصوصية، الاحتيال، الابتزاز، التهديد، سرقة المعلومات وانتحال الشخصية ويمكن تأكيد انتشار الجريمة الإلكترونية بشكل متصاعد وزيادة تأثيرها على الفرد والمجتمع في فلسطين من خلال الرجوع إلى التقارير الصادرة عن جهاز الاحصاء المركزي الفلسطيني، حيث تشير تقارير الشرطة الفلسطينية إلى أن معدل الجريمة الإلكترونية في فلسطين متزايد بشكل كبير.

من هنا جاءت الدراسة الحالية لكي يتبين بصورة أو بأخرى في مدى فاعلية الأليات والاستراتيجيات في مواجهة الجريمة الإلكترونية والتخفيف من أثارها. حيث تكمن مشكلة الدراسة في السؤال الرئيس التالي وهو: ما مدى فاعلية الأساليب والاستراتيجيات التقنية والقانونية للحد من الجرائم الإلكترونية في فلسطين؟ وتتلور أسئلة الدراسة في التالي:

- ماهية الجريمة الإلكترونية؟ ماهي خصائص الجريمة الإلكترونية؟
 - ماهي أنواع الجرائم الإلكترونية؟
 - ماهي التحديات التي تواجه المشرع الفلسطيني للوقاية من الجرائم الإلكترونية في المجتمع الفلسطيني؟
 - ماهي الأساليب والاستراتيجيات للحد من الجرائم الإلكترونية في المجتمع الفلسطيني؟
٣. فروض الدراسة:-

- لا توجد تعريف قانوني يحدد مفهوم الجرائم الإلكترونية في التشريع الفلسطيني.
- لا يوجد تشريعات قانونية خاصة تعاقب مرتكبي الجريمة الإلكترونية في فلسطين.

٤. أهداف الدراسة:

تسعى الدراسة إلى تحقيق الأهداف التالية:

- التعرف إلى مفاهيم الجريمة الإلكترونية.
- إبراز خصائص وأنواع الجريمة الإلكترونية.
- الكشف عن أهم التحديات التي تواجه المشرع الفلسطيني للوقاية من الجرائم الإلكترونية في المجتمع الفلسطيني.
- بيان أهم الأساليب والاستراتيجيات التي تحد من الجرائم الإلكترونية في المجتمع الفلسطيني.

٥. أهمية الدراسة:

- ندرة الدراسات والأبحاث التي تتناول الآليات والاستراتيجيات في مواجهة الجريمة الإلكترونية.
- نأمل أن تنسجم هذه الدراسة في إثراء الأدب النظري بتزويد المكتبة الفلسطينية والمكتبات العربية بهذا النوع من الدراسات.
- مساعدة أصحاب الاختصاص وصانعي القرار في القطاعين الحكومي الفلسطيني باتخاذ الإجراءات المناسبة للحد من الجرائم الإلكترونية ومواجهتها.
- مساعدة أصحاب القرار في المؤسسات التعليمية العامة والخاصة باتخاذ الإجراءات اللازمة لرفع مستوى الوعي ونشر المعرفة اللازمة لمحاربة الجريمة الإلكترونية من خلال المناهج الدراسية وورش العمل والندوات والمؤتمرات الشهرية والسنوية للحيلولة دون تفاقمها خاصة بين فئة الشباب الفلسطيني.
- رفع الوعي الاجتماعي والأسري حول مخاطر الجريمة الإلكترونية والإجراءات اللازمة اتخاذها لمكافحتها والحد منها.

٦. منهجية الدراسة:

اعتمدت هذه الدراسة المنهج الوصفي باعتباره يسعى إلى وصف موضوع الدراسة وصفاً علمياً دقيقاً من حيث واقع الجرائم الإلكترونية، والخصائص التي تمتع بها، كذلك أنواعها، وتحليل أهم التحديات التي تواجه المشرع الفلسطيني للوقاية منها في ضوء الآليات والاستراتيجيات المتبعة من قبل الدوائر الرسمية والغير رسمية في سبيل مواجهتها والحد من مخاطرها التي تواجه جميع أفراد المجتمع.

٧. المفاهيم الأساسية المرتبطة بالدراسة:

سوف نتناول في هذا الإطار المفاهيمي العديد من المفاهيم ذات الصلة بموضوع الدراسة العلمية، والتي تخدم الباحث نفسه وبيئته العلمية، وتكون أسساً علمية نحو تطوير بيئة المجتمع المعرفي والبحثي للباحث نفسه أو للمؤسسات البحثية، وتسهم في إثراء الواقع المعرفي بكل مكوناته ومنها ما يلي:

١١.٧ الجريمة:

لم يعرف المشرع الفلسطيني الجريمة الإلكترونية كون هذه الجريمة حديثة على الساحة الفلسطينية كما لم يتطرق الفقه والقضاء الفلسطيني إلى تعريفها بعد. قبل

الخوض في تعريف الجريمة الإلكترونية، لابد وأن نتطرق إلى معرفة ماهية الجريمة بحد ذاتها بشكل عام فقد عرف القانون التفسيري الفلسطيني الجريمة، ونعني بها لفظة جرم كل فعل أو محاولة أو ترك يستوجب العقوبة بحكم القانون". وتتعدد التعريفات ذات العلاقة بمصطلح الجريمة فمنها طابع فقهي، قانوني، واجتماعي، في هذا الصدد سوف نتناول كل تعريف على حده.

٢.٧ التعريف الفقهي للجريمة:

تعدد التعريفات الفقهية لمصطلح الجريمة، ولكن لا يوجد بينهما اختلاف كبير. فقد عرفها أحد الفقهاء بأنها: "سلوك انساني يرتكب إخلالاً بقواعد القانون الجزائي يترتب عليه المساس بمصلحة يحميها الشارع، ويوقع القضاء على مرتكبه الجزاء الجنائي المناسب. (جرادة، ٢٠١٠، ص ١٠٧). بينما عرفها الأخر بأنها: سلوك انساني ارادي أثم، ينظم أحكامه المشرع ويحدد خصائصه ويرتب عليه نتائج قانونية. (أنور، عبد الرحيم، ١٩٩٤، ص ٧٥).

٣.٧ التعريف القانوني للجريمة:

الجريمة في التصور القضائي القانوني هي: اعتداء أو عدوان على القانون، ولذلك تستحق المحاسبة والمجازاة. (المهيرات، ١٩٩٧، ص ٣١). بينما عرفها البعض الأخر بأنها: فعل أو امتناع يقرر له المشرع جزاءً جنائياً سواء كان هذا الجزاء عقوبة أو تبريراً وقائياً. (أبو عامر، ١٩٩٦، ص ٣٢).

٤.٧ التعريف الاجتماعي للجريمة:

يعرفها (Thosten Selin) بأنها فعل يمكن وصفه بأنه يشكل مخالفة للسلوك الخطر للمجتمع. في حين يعتبر كاره مصطفى بأن الجريمة من الناحية الاجتماعية " كل سلوك مخالف لما ترتضيه الجماعة، وهذا السلوك ضار بالمصالح الاجتماعية وفيه انتهاك لحرمة التقاليد والاعراف ويقتضي الحساب والمساءلة لمرتكبيه. (المهيرات، ١٩٩٧، ص ٣٢-٣٦).

فالجريمة من الناحية الاجتماعية هي كل فعل يتعارض مع ما هو نافع للجماعة وما هو عدل في نظرها، فالجريمة اعتماداً على المفهوم الاجتماعي هي انتهاك للعرف السائد مما يستوجب توقيع الجزاء على منتهكيه، وأنها ذلك الفعل العدائي والمعارض لتمام الجماعة التي يعدها الفرد جماعته الخاصة. (السيد، ١٩٨٥، ص ٩).

٥.٧ الجريمة الإلكترونية:

لقد تعددت ألفاظ ومفردات وصيغ ومصطلحات التعريف بالجريمة الإلكترونية فأطلق على الجريمة الإلكترونية، جرائم الكمبيوتر والأترنت، وجرائم الحاسب الآلي (Computer crimes) وجرائم التقنية العالية (High –Tech Crim's) والجرائم الرقمنة (Digital Crim's) والسيبر كرايم (Crim's Cyber) وجريمة أصحاب الباقات البيضاء (White Collar) والجرائم الناعمة (Crim's Soft) والجرائم النظيفة (Color Clean Crim's). (البعادي، ٢٠١٢، ص ٤).

تعددت الآراء بشأن تعريف الجريمة الإلكترونية، كل رأي يتبنى مفهوماً بالنظر إلى الزوايا التي يراها، فهناك من جانب من الفقه عرفها من زاوية فنية، أخرى قانونية، وهناك جانب آخر يرى تعريفها بالنظر إلى وسيلة ارتكابها أو موضوعها أو حسب توافر المعرفة بتقنية المعلومات لدى مرتكبها أو استناداً لمعايير أخرى حسب العاملين بها. وهذا ما حدا بالأمم المتحدة في مدونتها بشأن الجريمة المعلوماتية إلى عدم التوصل لتعريف متفق عليه دولياً.

وعلى الرغم من صعوبة وضع تعريفٍ لظاهرة الجريمة الإلكترونية وحصرها في مجال ضيق، إلا أن مكتب تميم التقنية في الولايات المتحدة الأمريكية عرفها من خلال تعريف الحاسب الآلي بأنها: "الجرائم التي تقوم فيها بيانات الحاسب الآلي والبرامج المعلوماتية بدور رئيسي". كما عرفت أيضاً بأنها: نشاط جنائي يمثل اعتداء برامج وبيانات الحاسب الإلكتروني". وعرفت أيضاً بأنها: "كل استخدام في صورة فعل أو امتناع غير مشروع للتقنية المعلوماتية، ويهدف إلى الاعتداء على أي مصلحة أو امتناع غير مشروع سواء أكانت مادية أو معنوية". (يس، ٢٠١٦، ص ٧).

بينما في المقابل، يرى البعض الآخر بأنها كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به تتعلق بالمعالجة الآلية للبيانات ونقلها كون التقنية فيها تكون إما وسيلة تستخدم في ارتكاب الفعل أو البيئة والوسط الذي يحدث فيه الجرم أو يكون الهدف أو الغاية لارتكاب الفعل المجرم، أي أن الوسيط يكون آلة تقنية كجهاز الحاسب الآلي الذي يكون دوماً وسيلة للفعل الإجرامي الإلكتروني دون إهمال بعض الأجهزة التقنية الأخرى كالجيل الثالث للهواتف المحمولة، ولاسيما مع الانتشار الواسع لاستخدامات الأترنت الذي حول العالم إلى قرية صغيرة بإعتباره وسيلة اتصالات عالمية تعتمد على البرامج

المعلوماتية الحديثة في ضبط مختلف البيانات والمعطيات والمعلوماتية الدقيقة. (يس، ٢٠١٦، ص٧-٨).

يرى الباحثين بأن هناك تعريفات متعددة متعلقة بالجريمة أو الجريمة الإلكترونية أو الجريمة عبر الكمبيوتر، والانترنت أو جرائم تقنية المعلومات أو جرائم أصحاب الباقات البيضاء. فالجريمة الإلكترونية تعرف بأنها: جريمة تتعلق بالكيانات المعنوية ذات القيمة المادية أو القيمة المعنوية بهدف الحصول على المعلومات ذات العلاقة بالأجهزة والأشخاص بشكل مباشر.

٨. خصائص الجريمة الإلكترونية:

تختلف الجريمة الإلكترونية عن الجريمة التقليدية من حيث خصائصها، فالجريمة الإلكترونية لم تظهر إلا في عصر الحاسب الآلي والانترنت، كون هذه الجرائم حديثة ومتطورة فإن لها خصائص منفردة تتميز بها عن غيرها من الجرائم من الجرائم التقليدية، ومن أهم هذه الخصائص أن الجرائم الإلكترونية تتطلب وجود جهاز إلكتروني ومعرفة كيفية استخدامه، كما أن هذه الجرائم لا حدود لها وبنفس الوقت هذه الجرائم صعبة الاثبات والاكتشاف، ولذلك فهي مغرية للمجرمين وفي ضوء ما سبق سوف نتناول هذه الخصائص بالتفصيل ولعل أهمها ما يلي:

١٠.٨ يتطلب لارتكابها وجود جهاز إلكتروني ومعرفة بتقنية استخدامه:

بدون الجهاز الإلكتروني تنتفي الجريمة الإلكترونية وتتطلب هذه الجريمة دراية كافية وخبرة فائقة بالكمبيوتر والانترنت في بعض الجرائم، أو معرفة بسلوكيات الفعل المرتكب في الجرائم البسيطة منها، كما أنها لا تمتاز بالعنف وأغلب الجرائم الإلكترونية ترتكب عبر الإنترنت. (القاضي، ٢٠١١، ص٥٢-٥٣).

ولذلك فإن ما يميز الجريمة الإلكترونية عن غيرها من الجرائم أنها تتطلب وجود علم كافي بالجوانب الفنية والتقنية لاستخدام الحاسوب والانترنت، وتعتبر العلاقة بين مدى الدراية بالجوانب الفنية والتقنية للحاسوب وبين الجريمة الإلكترونية علاقة طردية، فكلما زادت الخبرة لدى الأفراد بمعرفة تقنية الحاسوب، زاد احتمال استخدام خبرتهم بشكل غير مشروع. (عبابنة، ٢٠٠٩، ص٣٦).

٢.٨ موضوع الاعتداء هو معطيات الجهاز الإلكتروني:

تعد البيانات والمعلومات على الحاسب الآلي هي موضوع الجرائم الإلكترونية، فهذه البيانات يمكن تخزينها ونقلها من جهاز لآخر عبر الوسائط الصلبة أو المرنة أو عبر البريد الإلكتروني، ولذلك فهي تعتبر مكونات معنوية نقبل الحيابة والنقل، ويمكن سرقة وإتلافه ولذلك يجب أن يكون هذا المال محل حماية من قبل القانون الجزائي. (الحلي، ٢٠١١، ص ٥٥).

وعليه فإذا كان موضوع الاعتداء هو الحاسب الآلي أو شاشته أو أحد مكوناته المادية، فإنه هذه الحالة يصلح تطبيق قانون العقوبات الفلسطيني، أما لو كان موضوع الاعتداء هو معطيات الحاسوب من البيانات والمعلومات فنحن هنا بصدد جريمة إلكترونية وتحتاج إلى نصوص أكثر دقة لمعالجتها. (العفيفي، عبدالعال، ٢٠١٣، ص ١٥). ولذلك فإن البيانات والمعلومات الحاسوبية تعد مالمأ قابل للحيابة والنقل وله قيمه مادية، وقد نص المشرع الأردني في المادة ٣٤ من القانون المدني الأردني بأن " كل شيء يمكن حيابته مادياً ومعنوياً والانتفاع به انتفاعاً مشروعاً ولا تخرج عن التعامل بطبيعته أو بحكم القانون يصبح أن يكون الجريمة الإلكترونية لا حدود لها* .

٣.٨ الجريمة الإلكترونية لا حدود لها:

لأن أغلب الجرائم الإلكترونية ترتكب عبر الأنترنت فإنها تتسم بالطابع الدولي حيث تقع هذه الجرائم فيكون المجرم في دولة والمجني عليه في دولة أخرى، ويمكن أن يكون الضرر قد حدث في دولة تالفة أو في عدة دول مثل: اختراق المواقع والأجهزة هو إتلافها، وسرقة البيانات والمعلومات والأموال، كل ذلك جعل مكافحة الجرائم الإلكترونية أمراً عسيراً ولذلك لتعدد الأماكن التي تتعلق بالجريمة وتنازع قوانين الدولة الواجبة للتطبيق، واختلاف الإجراءات الجزائية من دولة لأخرى، وصعوبة ملاحقة الجناة كل ذلك يتطلب تعاون ودي للقبض على الجناة وتقديمهم للمحاكم المختصة بنظر النزاع. (عبابنة، ٢٠٠٩، ص ٣٥).

فالتحقيق في الجرائم الإلكترونية يتطلب إجراءات وأعمال للتحقيق خارج حدود الدولة مثل: تفتيش المواقع الإلكترونية أو تفتيش الأجهزة الإلكترونية والمادية

* المادة ٥٤ من القانون الأردني رقم (٤٣) لسنة ١٩٧٦ مشار إليه في الموقع الرسمي للنشريات الأردنية، ديوان التشريع والرأي.

للعثور على البيانات أو المعلومات، أو إلقاء القبض على المطلوبين، أو معاينة مسرح الجريمة. وكل ذلك يحتاج إلى تعاون دولي ملموس على أرض الواقع. (القاضي، ٢٠١١، ص٥٣).

يرى الباحثين بناءً على ما تقدم بوجود التعاون الدولي بهدف ملاحقة ومتابعة المجرمين الإلكترونيين، مع إعطاء أهمية كبرى للإنتربول الدولي بشأن القبض على المجرمين الإلكترونيين وتسليمهم إلى الجهات القانونية المختصة، والعمل على تفعيل نتائج ومخرجات المؤتمرات والندوات الدولية للخروج باتفاقيات دولية تعالج مسائل تفاقم الجرائم الإلكترونية ومكافحتها والحيلولة دون تفاقمها.

٤.٨ الجرائم الإلكترونية صعبة الاكتشاف أو الإثبات:

ومما جعل الجرائم الإلكترونية صعبة الاكتشاف والاثبات البُعد الجغرافي بين الجاني والمجني عليه كما ذكرنا، واستخدام الجاني وسائل فنية حديثة في جرمه، كما أن هذه الجرائم ترتكب في وقت سريع ومن يتم محو أثرها في وقت أسرع لا تتعدى الثواني، ومما يزيد الأمر صعوبة عدم وجود خبرة لدى ضباط التحقيق في مثل هذه الجرائم خاصة من ناحية التحقيق والبحث على الأدلة والتحفيز عليها، ومن الصعوبات التي تواجه اثبات هذه الجرائم عدم اقتناع القضاة بكثير من الجرائم المستحدثة في هذا المجال. (المناعسة وآخرون، ٢٠١٠، ص١٠٦-١٠٧).

حيث تعد هذه الخاصية من الخصائص التي تتميز بها الجريمة الإلكترونية عن غيرها، فقد انتشرت مكاتب تقوم بأعمال السرقة والقرصنة من خلالها يقوم بعض الأشخاص باستئجار قرصنة محترفين لسرقة بيانات الشركات العالمية مقابل مبالغ مالية، ومن ثم يتم بيعها لأشخاص مستفيدين، وكل هذه الأعمال غير مشروعة، وأن من الأسباب الكامنة في صعوبة واكتشاف واثبات هذه الجرائم عدم تقديم شكاوى من قبل أصحاب الشركات التي يتم اختراقها وذلك خوفاً على سمعة الشركة وعلى المستثمرين فيها. (المؤمنى، ٢٠١٠، ص٥٤).

يتضح مما سبق، بإننا بحاجة إلى توظيف خبراء تقنيين في هذا المجال والعمل على تدريب ضباط التحقيق ليكون لديهم القدرة على معرفة الأدلة الإلكترونية والحفاظ عليها، والأهم من ذلك أن يتم تطوير التشريع الفلسطيني ليستطيع مواكبة هذا التطور

الإجرائي، وكذلك عقد المزيد من الدورات التدريبية للقضاة في الدول الأكثر خبرة في هذا المجال ليتسنى لهم معرفة مدى خطورة مثل هذه الجرائم على صعيد الفرد والمجتمع.

٥.٨ الجرائم الإلكترونية جرائم الأذكاء:

تعتبر الجرائم الإلكترونية جرائم مُغرية لسرعة تنفيذها، وسهولة محو أدلة الإدانة فيها، فهي تنفذ عن بُعد دون التواجد في مسرح الجريمة، ولا تتطلب سوى ضغط مفتاح معين في الجهاز لتنفيذها. ومن مغريات هذه الجرائم المكاسب المادية الضخمة التي تحققها في وقت معين، خاصة الموظفين الذين يعملون في الشركات التي تعتمد على النظام الإلكتروني في عملها، فمن السهل لديهم اختراق الأجهزة والبرامج وتحقيق مساعيهم دون أن يعترضهم أي عائق نظراً لخبرتهم وتجاربهم في هذا المجال. (المناعسة وآخرون، ٢٠١٠، ص ١٠٧).

٦.٨ أنواع الجرائم الإلكترونية:

إن للجرائم الإلكترونية أنواعاً كثيرة لا يمكن حصرها إذ لم يوضع لها معايير محددة من أجل تصنيفها بصورة قاطعة، وهذا عائد إلى التطور المستمر لشبكة المعلومات العالمية والخدمات التي تقدمها. وقد تضاربت آراء فقهاء القانون الدولي من أجل تحديد أنواع جرائم الأنترنت، وتعددت التصنيفات فهناك من عدّها بحسب موضوع الجريمة، وأخر قسمها حسب طريقة ارتكابها. ونتيجة لذلك الاختلاف القانوني بين فقهاء القانون حول العالم إلا أن هناك محاولات مستمرة من أجل تقسيمها بصورة إجرائية. ويمكن تقسيم الجريمة الإلكترونية في جانبها القانوني إلى نوعين وهما: (الشبلي، ٢٠١٩: ٨٧).

■ الجرائم التي تستعمل فيها الوسائل التكنولوجية من أجل القيام بالفعل الإجرامي مثل: تزوير الأموال عن طريق الماسح الضوئي فهذا النوع له إطاره القانوني في معظم التشريعات العالمية.

■ الجرائم التي تستخدم التقانة الحديثة لارتكابها: وذلك عن طريق شبكة الأنترنت كإنشاء المواقع الإباحية، أو الانضمام إلى مجموعات إرهابية. أو المتاجرة بالسلاح أو المخدرات، أو المتاجرة بأسرار الناس عن طريق اختراق مواقعهم، أو أجهزة الكمبيوتر الشخصية باستخدام بطاقات الائتمان.

وهناك من فقهاء القانون من حاول تصنيف الجرائم الإلكترونية بحسب علاقتها بالجرائم التقليدية إلى خمسة أنواع رئيسية وهما: (الشبلي، ٢٠١٩: ٨٧).

■ يتمثل في الجرائم الإلكترونية المنصوص عليها في قانون العقوبات متى ارتكبت باستعمال شبكة المعلومات العالمية.

■ دعم الأنشطة الإجرامية: ويتعلق الأمر بما تلعبه الشبكة من دور في دعم جرائم غسل الأموال، والمخدرات، والإتجار بالأسلحة، واستعمال الشبكة كسوق للترويج غير المشروع في المجالات غير المشروعة.

■ جرائم الدخول في نظام المعالجة الألية للمعطيات: وتقع الجريمة على البيانات والمعلومات المكونة للحاسوب وتغييرها أو تعديلها، أو حذفها مِمَّا يغير مجرى عمل الحاسوب.

■ جرائم الاتصال: وتشمل كل ما يرتبط بشبكات الهاتف، وما يمكن أن يقع عليها من انتهاكات باستغلال ثغرات شبكة الأنترنت.

■ الجرائم المتعلقة بالاعتداء على حقوق الملكية الفكرية: تتمثل في عمليات نسخ البرامج دون وجه حق، وسرقة حقوق الملكية المعروضة على الشبكة دون إذن من صاحبها وبطبيعتها وتسويقها واستغلالها بأي صورة طبقاً لقانون حماية الملكية الفكرية.

في العصر الحديث المعاصر الذي نعيشه تعد وسائل التواصل الاجتماعي بمختلف أشكالها من أخطر أنواع الجرائم التي غزت جميع الأسر العربية، ومعها انتفت صفة الخصوصية فلم يعد هناك أي مكان للخصوصية بل أصبح كل شيء متاحاً ومنتهكاً بنفس الوقت، مِمَّا يتطلب وضع حد للتوازن بين الحفاظ على حق الفرد بالتعبير عن نفسه وحماية خصوصيته وبين حق المجتمع الذي هو جزء أساسي منه.

٩.التحديات والاساليب والاستراتيجيات للحد من الجرائم الإلكترونية في المجتمع الفلسطيني:

هناك عدة تحديات تواجه المشرع الفلسطيني خلال معالجته ومحاربه للجرائم الإلكترونية في المجتمع الفلسطيني، تتعلق بالبيئة الفلسطينية، وخصوصيتها، وتواجد الاحتلال الإسرائيلي، وغيرها من التحديات، والتي تتمثل بما يلي:-

- عدم تفعيل الحماية القانونية لخصوصية المواطنين: فغياب مثل هذه المنظومة يؤدي إلى تشجيع ممارسة الجريمة الإلكترونية في الشارع الفلسطيني، فمن حق أي شخص أن يعيش بعيداً عن أي قيود اجتماعية مسلطة عليه، وتؤدي إلى كشفه امام المجتمع بطريقة تنهك خصوصيته وحقوقه الإنسانية (قوراي، وآخرون، ٢٠١٧، ص ١٣).
- غياب منظومة التشريع الفلسطيني: وذلك بسبب حالة الانقسام الفلسطيني الداخلي، والتي أدت الى غياب التشريع الفلسطيني، وتعطل اعمال المجلس التشريعي الفلسطيني.
- غياب آليات الرقابة المجتمعية: والتي تهدف إلى منع سلوكيات الأشخاص غير المرغوب فهم من ممارستهم للجرائم الإلكترونية بحق غيرهم، وأهم شرط لعمل هذه الرقابة هو القدرة على التنبؤ بقيام الفرد بمثل هذه السلوكيات (زيوش، بومدفع، ٢٠٢١، ص ٥).
- فقدان السيطرة الاجتماعية والسياسية: حيث يتعذر على الحكومات، لا سيما في البيئات غير المستقرة كاليئة الفلسطينية، السيطرة على كافة المواقع والاعمال الإلكترونية سياسياً واجتماعياً، الامر الذي يؤدي إلى تشكل مناخ مناسب للجريمة الإلكترونية بشكلٍ يصعب على المشرع الفلسطيني مقاومته والحد منه (العفيفي، ايمن، ٢٠١٣، ص ٢٥).
- التصادم مع منظمات المجتمع المدني: فقد تؤدي بعض التشريعات الحكومية الناظمة للجرائم الإلكترونية على حدوث صدامات مع منظمات المجتمع المدني بذرائع تقييد الحريات وما شابه ذلك، الامر الذي يؤدي إلى تعطيل هذه التشريعات، أو إعادة النظر بها، وبالتالي منح الوقت لتفشي الجريمة الإلكترونية في المجتمع الفلسطيني.
- غياب التمكين الأمني للتصدي للجريمة الإلكترونية: فعدم وجود منظمة امنية تمكن جهات الاختصاص من الإمساك بالقائمين خلف الجريمة الإلكترونية، وتمكهم من الإفلات من العقاب نظراً لخصوصية الحالة الفلسطينية، فإن ذلك يحد من الوقاية من الجريمة الإلكترونية في المجتمع الفلسطيني (الزعابي، ٢٠٢١، ص ٣٣).

- غياب تطبيق قانون الجرائم الإلكترونية: مع ان المشرع الفلسطيني قد أقر قانوناً للجريمة الإلكترونية، إلا ان تطبيقاته غائبة في البيئة الفلسطينية بشكل عام، وذلك لخصوصية الحالة الفلسطينية، والتحكم الإسرائيلي بمنافذ الانترنت، وحصرت تطبيق القانون على بعض القضايا السياسية، ممّا أدى إلى غياب تطبيق هذا القانون. والتمرد عليه من قبل عدة الجهات داخل الشارع الفلسطيني (جلعود، ٢٠١٣، ص ٣٥).
 - غياب التشبيك الدولي في محاربة الجريمة الإلكترونية: فعدم تظافر الجهود المحلية في الفلسطينية مع الجهود الدولية في محاربة الجريمة الإلكترونية، وإيجاد نظام قانوني مقاوم لها يؤدي إلى استمرارية انتشارها في المجتمع الفلسطيني. فالوضع السياسي للبيئة الفلسطينية يحول دون ذلك (خالد، ٢٠١٦، ص ٢٩).
 - عدم تطبيق برامج للتوعية التقنية ضد الجريمة الإلكترونية: وهو أمر يتعلق بوزارة الاتصالات الفلسطينية والجامعات ووزارة التربية والتعليم، بحيث يتوجب عليها تطبيق مثل هذه البرامج لخلق وعي اجتماعي ومجتمعي حول الجريمة الإلكترونية، ممّا يسهل على المشرع الفلسطيني من تطبيق مخرجاته القانونية في البيئة الفلسطينية (الجعبري، عمرو، ٢٠١٩، ص ٤٧).
 - تعددية القوانين والتشريعات المعمول بها في البيئة الفلسطينية: حيث يسري في فلسطين عدة قوانين وتشريعات قد تؤدي إلى عرقلة مقاومة الجريمة الإلكترونية. كالقانون البريطاني والعثماني والأردني والمصري والإسرائيلي، وهو شأن قد يؤدي إلى خلخلة المنظومة القانونية في فلسطين (العفيفي، ايمن، ٢٠١٣، ص ١٣).
- تعيق هذه التحديات السابقة الذكر، وغيرها، المشرع الفلسطيني في مقاومة الجريمة الإلكترونية. والحد منها في المجتمع الفلسطيني. وهي تحديات تحمل شيئاً من الخصوصية التي تتعلق بالبيئة الفلسطينية، نظراً لوجود الاحتلال الإسرائيلي، وغياب ملامح الدولة الفلسطينية، والسيطرة شبه مطلقة على المقدرات الفلسطينية من قبل الاحتلال الإسرائيلي، ممّا يؤدي إلى خلق الكثير من التحديات، وفي مختلف مجالات العمل الفلسطينية، السياسية والاقتصادية والاجتماعية والثقافية والتقنية والقانونية.

١٠. الأساليب والاستراتيجيات للحد من الجرائم الإلكترونية في المجتمع الفلسطيني:

نظراً لخطورة الجرائم الإلكترونية على المجتمعات، فإنه يلقي على عاتق مؤسساتها الرسمية وغير الرسمية، والأطر الاجتماعية والمجتمعية والمدنية فيه القيام بعدة خطوات واستراتيجيات لمجابهة الجريمة الإلكترونية، ومن أهمها ما يلي:-

- ضبط وتحديد المقصد الدقيق للجريمة الإلكترونية: فنظراً لتعددية أساليب الجريمة الإلكترونية، واختلاف أنواعها واساليبها، فإنه يجب على الأطر الرسمية ضبط هذا المفهوم، والعمل على حصر الجريمة الإلكترونية ضمن إطار مفاهيمي شامل للجريمة الإلكترونية، بحيث يعد ذلك أولى استراتيجيات الحد من الجريمة الإلكترونية (نجم الدين، ٢٠٢١، ص ٣٣).
- تشريع قانون لمكافحة الجريمة الإلكترونية واحترام الخصوصية الرقمية للمواطن: وذلك عبر العمل على بناء قانون عصري وحديث لمجابهة الجريمة الإلكترونية ومكافحتها يستند على جميع جوانب وأركان وعناصر هذه الجريمة، ويكون قابلاً للتطور والبناء عليه مستقبلاً، وله ارتباطات تشريعية أخرى مع القانون الدولي (الزعابي، ٢٠٢١، ص ٤٥).
- وضع استراتيجية للبناء الأمني والمعلوماتي للأفراد والمؤسسات: وهي استراتيجية تلقى على عاتق الأجهزة الأمنية والشرطية في الدولة، والمؤسسات التقنية والرقمية فيها، عبر تحصين الافراد والجماعات في المجتمع من خطر الجريمة الإلكترونية، وزيادة الوعي المعلوماتي والتقني حولها (زيوش، بومدفع، ٢٠٢١، ص ٥).
- وضع استراتيجية توعوية للانتباه لخطورة الجريمة الإلكترونية: بحيث تتكفل بها وزارة التربية والثقافة ووزارة الاتصالات، عبر القيام بحملة دعائية للتوعية من خطورة الجريمة الإلكترونية، وتعريف المجتمع على أنواعها واساليبها وأهدافها ووسائل تنفيذها. وهي استراتيجية بنائية وضرورية للحد من انتشار مثل هذه الجرائم الرقمية (الجعبري، عمرو، ٢٠١٩، ص ١٧).
- التوعية حول المخاطر الاقتصادية والاجتماعية للجريمة الإلكترونية: وذلك عبر ربط خطر الجريمة الإلكترونية بالنشاط الاقتصادي والاجتماعي للمجتمع، كونه النشاط الذي يلامس حاجيات المجتمعات، ويعمل على تنمية مداركها

حول أي خطر يهدد نشاطاتها الاقتصادية والاجتماعية (المشهداني، ٢٠١٥، ص٣٧).

• تعزيز اطر التعاون الدولي لمكافحة الجريمة الإلكترونية: فوضع استراتيجيات محلية دون ربطها مع الأطر الدولية في مكافحة الجريمة الإلكترونية ستكون غير مجدية، كون أن الجريمة الإلكترونية عابرة للحدود والدول (يس، ٢٠١٦، ص٩).

• التشهير بالمجرم الإلكتروني امام المجتمع: وذلك لتحذير المجتمع منه، وتعريفهم على اساليبه، مع أن مثل هذه الاستراتيجيات قد تنتهك خصوصية الفرد، لكنها ضرورية لتعريف المجتمع على هؤلاء المجرمين (العفيفي، ايمن، ٢٠١٣، ص١١).

• تفعيل دور وسائل الاعلام للحديث عن مخاطر الجريمة الإلكترونية: وهي استراتيجية تتكامل مع استراتيجيات التوعية السابقة الذكر، لكنها بشكلٍ أضخم وأكثر كثافة لإبقاء الموضوع ضمن وعي المواطن بشكلٍ مستمر (قوراي، وآخرون، ٢٠١٧، ص٢٧).

• تطوير فريق وطني لمكافحة الجريمة الإلكترونية: وذلك بإيعازٍ من الدوائر السياسية العليا في الدولة، عبر استقطاب الكوادر البشرية المناسبة لذلك، وتدريبها على سبل مجابهة الجريمة الإلكترونية ومعالجتها (المليحي، ٢٠١٩، ص٣٣).

• تعزيز ثقافة الرقابة المجتمعية على الجرائم الالكترونية: وهي استراتيجية جماعية اجتماعية يتشارك فيها جميع الافراد والجماعات في الدولة، وذلك لمساندة الفرق الرقمية والوطنية، وتفعيل المشاركة المجتمعية في التصدي للجرائم الإلكترونية (زيوش، بومدفع، ٢٠٢١، ص٤١).

تمثل هذه الاستراتيجيات، وغيرها، أبرز الوسائل والأساليب للحد من انتشار الجريمة الالكترونية في أي مجتمع، لكنها تكون أكثر حدةً في المجتمع الفلسطيني، نظراً لخصوصيته السياسية والاجتماعية والاقتصادية، بوجود الاحتلال الإسرائيلي، وغياب ملامح الدولة، واستخدام إسرائيل لمثل هذه الوسائل في محاربتها للمجتمع الفلسطيني.

لذلك، فإن على دوائر صنع القرار في الشارع الفلسطيني الانتباه لخطر هذه الجريمة، ومكافحتها بكافة السبل والوسائل.

١١. الدراسات السابقة:

سوف يتناول الباحثون العديد من الدراسات العلمية السابقة ذات الصلة بموضوع الدراسة، وهي على النحو الآتي:

نجم الدين، سامر، (٢٠٢١)

هدفت الدراسة إلى تسليط الضوء على مفهوم الجريمة المنظمة الإلكترونية وتفرقتها عن الجريمة الإلكترونية التقليدية، إضافة إلى أنها تهدف للتعرف على طريقة تعاطي المشرع الفلسطيني مع الجريمة المنظمة الإلكترونية، ومدى إفراد خصوصية لها في التشريع النافذ من خلال توضيح أثارها المباشرة وغير المباشرة على المجتمع المستهدف والمجتمعات بشكل عام. ومن أجل دراسة هذا الموضوع أتبع الباحث المنهج الوصفي التحليلي من خلال القيام بوصف الإشكالية موضوع البحث وتحليل النصوص القانونية ذات العلاقة التي تناولت الموضوع وربطها ببعضها البعض ومحاولة التوصل إلى الحلول اللازمة لحل الإشكالية. توصلت الدراسة إلى مجموعة من النتائج أهمها ما يلي: لم يكن التنظيم القانوني للمشرع الفلسطيني الخاص بالجرائم الإلكترونية كافياً لإزالة الغموض والتوضيح. وتوصي الدراسة بضرورة النفي بوضوح من قبل المشرع الفلسطيني في الإقرار بقانون الخاص بالجرائم الإلكترونية على الجريمة المنظمة الإلكترونية، وتوضيح أركانها والعقوبات عليها بشكل يزيل الغموض أو الالتباس.

زيوشي، سعيد. بومدفع، الطاهر. (٢٠٢١)

يهدف هذا المقال إلى تسليط الضوء على الظاهرة الإجرامية الإلكترونية وأليات الرقابة المجتمعية التي سيفرضها المجتمع من أجل التفادي في الوقوع في مثل هذا النوع من الجرائم. حيث تشهد الجزائر موجة من التغيرات على كافة الجوانب لاسيما التقنية والتكنولوجية منها، الأمر الذي أدى إلى انتشار كبير للإنترنت الذي توفره شركات خاصة كما توفره شركات اتصالات الجزائر. توصلت الدراسة إلى مجموعة من النتائج أهمها ما يلي: رفع درجة الوعي لدى كل الأفراد فهم في غير مأمّن من برائن المجرمين إذا تم التراخي عن المراقبة أو التخلي عن الدور المنوط بهم.

الجعبري، مهند. عمرو، بلال. (٢٠٢٠).

هدفت الدراسة إلى قياس فاعلية الوعي التقني والقانوني في مواجهة الجريمة الإلكترونية والتخفيف من أثارها لدى طلبة جامعة الخليل. اعتمد الباحثان على المنهج شبه التجريبي (المجموعة الواحدة). باستخدام القياس القبلي والبُعدي. اشتملت عينة الدراسة على عينة طبقية مكونة من ٧٦ طالباً وطالبة من طلبة جامعة الخليل التحقوا في مساق تطبيقات تكنولوجيا في العام الأكاديمي ٢٠١٨-٢٠١٩.

وقد خلصت الدراسة إلى وجود فروق ذات دلالة إحصائية في متوسطات التطبيقيتين القبلي والبُعدي للجانب التقني والجانب القانوني لصالح التطبيق البُعدي وهذا يدل على فاعلية البرنامج المطبق في رفع مستوى معرفة طلبة جامعة الخليل في الجانب التقني والقانوني للحد من الجرائم الإلكترونية، فقد بلغ حجم تأثير البرنامج المطبق (٠,٦٤) بالنسبة للجانب التقني و(٠,١٤) للجانب القانوني. وقد أوصى الباحثان بضرورة رفع مستوى المعرفة التقني والقانوني عن طريق برامج تدريبية هادفة، وموجهة للأجيال الشابة من خلال المناهج المدرسية والجامعية، إضافة إلى تكثيف محاضرات التوعية وورش العمل ذات العلاقة من قبل جهات الاختصاص.

المایل، عبد السلام وآخرون. (٢٠١٩).

هدفت الدراسة إلى إلقاء الضوء على الجريمة الإلكترونية في الفضاء الإلكتروني والاسباب الدافعة إلى ارتكاب الجريمة، واقتراح بعض الحلول التي من شأنها الحد من هذه الظاهرة ومكافحتها. فقد استخدم المنهج الوصفي من خلال الكتب والمقالات والدوريات العلمية والأبحاث التي تناولت الموضوع قيد الدراسة. وقد توصلت الدراسة إلى مجموعة من النتائج أهمها ما يلي: تعد التشريعات والقوانين عاملاً مهماً في مواجهة الجريمة الإلكترونية (المعلوماتية) التي ترتكب في الفضاء الإلكتروني، وكذلك قصور مؤسسات التعليم والمجتمع المدني في القيام بالدور التوعوي والوقائي في مكافحة تلك الجرائم، وأن مكافحة الجرائم المعلوماتية في ليبيا مازالت بلا غطاء تشريعي يحددها ويحرم كافة صورها. وأوصت الدراسة بضرورة تدخل المشرع القانوني لمواجهة الجريمة الإلكترونية التي ترتكب في الفضاء الإلكتروني.

الشبلي، عبد الله. (٢٠١٩).

هدف الدراسة إلى تحديد مفهوم الجريمة الإلكترونية وخصائصها، ودور التشريع العماني في إيجاد الحلول المناسبة لها، ومن أجل تحقيق هدف الدراسة الرئيس فقد تم استخدام المنهج القانوني الوصفي وتوصلت الدراسة إلى أن المشرع العماني استطاع مواكبة التقدم الحضاري من خلال تطوير القوانين التي تكافح الجرائم بصورة عامة والجرائم الإلكترونية وتقنية المعلومات على وجه الخصوص من خلال منظومة قانونية متكاملة إذ تتراوح تلك العقوبات بين الغرامة المالية والعقوبات السالبة للحرية. حيث توصل الباحث إلى جملة من التوصيات منها ما يلي: توعية المجتمع بخطورة الجرائم الإلكترونية وأساليب ارتكابها وتأثيرها الأخلاقي على الفرد والمجتمع وطرق الوقاية منها.

١.١١ التعقيب على الدراسات السابقة:

تم الاستفادة من الدراسات السابقة في معرفة وصياغة تساؤلات ومشكلة الدراسة التي نحن بصددتها، ولكن تختلف هذه الدراسة عن باقي الدراسات السابقة كونها تعمل على التركيز على دراسة توضيح مفهوم الجريمة الإلكترونية أنواعها وخصائصها والتحديات المرتبطة بها، ثم توضيح أهم الآليات والاستراتيجيات للحد من الجرائم الإلكترونية، وانطلاقاً من نتائج الدراسات السابقة ومن الإطار النظري الذي تتناوله الدراسة الحالية واتساقاً مع ما سبق من أهمية موضوع الدراسة الحالية، فقد جاءت هذه الدراسة لتبيان خطورة الجريمة الإلكترونية في المجتمع الفلسطيني وضرورة العمل المجتمعي للحد منها ومكافحتها حتى يتسنى لنا بناء مجتمع خالٍ إلى حدٍ ما من الجرائم أياً كان نوعها، فالجرائم تضعف المجتمعات وتخلُّ بأمنها واستقرارها الداخلي، وتعيق أبنائها عن التقدم والبناء في كافة المجالات.

١٢ نتائج الدراسة:

➤ غياب تطبيق منظومة التشريع الفلسطيني نظراً للحالة الفلسطينية الراهنة التي تمرُّ بها سواء من خلال حالة الانقسام والتشظي التي عطلت أعمال المجلس التشريعي الفلسطيني ودوره عن إصدار القوانين من جهة، وعدم الاستقرار السياسي والاجتماعي داخل البيئة الفلسطينية خاصة ما بعد العام

٢٠٠٧ وحتى وقتنا الحاضر والذي أدى إلى غياب منظومة تشريعية قانونية فاعلة تؤدي دورها على أكمل وجه.

- غياب التوعية القانونية والمجتمعية المشتركة ما بين الوزارات المؤسسات التعليمية الفلسطينية العليا سواء بين الجامعات أو المعاهد، ممّا أدى إلى تفشي ظاهرة الجريمة الإلكترونية بين صفوف الشباب الجامعي.
- تعدد القوانين المتداولة داخل الشارع الفلسطيني، فمن الصعب على المشرع الفلسطيني التفرد بقانون واحد لمقاومة الجرائم الإلكترونية أو إيجاد حلٍ لها ممّا أدى إلى خلخلة في المنظومة التشريعية القانونية الفلسطينية.

١٣. التوصيات:

- إجراء الانتخابات في الشارع الفلسطيني بهدف إعادة إحياء دور وعمل المجلس التشريعي الفلسطيني في سن القوانين التشريعية ذات العلاقة بالجريمة الإلكترونية والحد من تفشيها وخطورتها داخل المجتمع.
- تخصيص ورش عمل لكافة الطلاب بمختلف مراحلهم الجامعية للتعرف على ماهية الجرائم الإلكترونية وخطورتها، وهذا لن يتم إلا من خلال التنسيق والتعاون بين كافة مؤسسات المجتمع المدني والوزارات ذات العلاقة بالشأن لكي يتم الوقوف على مخاطرها والحد من تفاقمها.
- تخصيص مساقات جامعية تقنية وتطبيقية يتم من خلالها تزويد الطلاب بكافة المهارات والأدوات التكنولوجية، للوقاية من مخاطر الجريمة الإلكترونية وتدابيرها السلبية على جميع أفراد المجتمع.
- تفعيل قانون الجرائم الإلكترونية من خلال إعداد قضاة ومحامين ومختصين وتدريبهم بشكل كافٍ على الوقوف على تداعيات ومخاطر الجريمة الإلكترونية داخل المجتمع الفلسطيني.
- تفعيل دور اللجان والمؤسسات المجتمعية والأمنية بدورها المجتمعي الرقابي والأمني في نشر الوعي بين كافة شرائح المجتمع كافة من خلال عقد المؤتمرات والندوات التوعوية للحد من مخاطر الجريمة الإلكترونية داخل الشارع الفلسطيني.

١٤. قائمة المراجع:

أولاً: قائمة الكتب:

- أبو عامر، محمد. (١٩٩٦). مبادئ علم الإجرام والعقاب. بيروت: الدار الجامعية.
 - أنور، يسر. عبد الرحيم، أمال. (١٩٩٤). أصول علمي الاجرام والعقاب. ج ١. القاهرة: دار النهضة العربية.
 - جرادة، عبد القادر. (٢٠١٠). مبادئ قانون العقوبات الفلسطيني الجريمة والمجرم. المجلد (١). غزة: مكتبة أفاق
 - الحلبي، خالد. (٢٠١١). إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت. ط١. عمان: دار الثقافة للنشر والتوزيع.
 - السيد، رمضان. (١٩٨٥). الجريمة والانحراف من منظور الاجتماعي. الإسكندرية: المكتب الجامعي الحديث.
 - عبابنة، محمود. (٢٠٠٩). جرائم الحاسوب وأبعادها الدولية. ط١. عمان: دار الثقافة للنشر والتوزيع.
 - القاضي، رامي. (٢٠١١). مكافحة الجرائم المعلوماتية. ط١. القاهرة: دار النهضة العربية.
 - المناعسة، أسامة وآخرون. (٢٠١٠). تقنية نظم المعلومات الإلكترونية. ط١. عمان: دار الثقافة للنشر والتوزيع.
 - المهيرات، بركات. (١٩٩٧). جغرافيا الجريمة علم الإجرام الكارتوجرافي. ط١. الأردن: مكتبة الجلاوي.
 - المؤمني، نهلا. (٢٠١٠). الجرائم المعلوماتية. ط٢. عمان: دار الثقافة للنشر والتوزيع.
- ثانياً: المقالات العلمية:

- الجعبري، مهند، عمرو، بلال، (٢٠٢٠). "فاعلية برامج التوعية التقنية والقانونية في مواجهة الجريمة الإلكترونية من وجهة نظر طلبة جامعة الخليل - فلسطين". مجلة جامعة الخليل للبحوث. مجلد (٩). ص١٢٩-١٥٦. الرابط الإلكتروني:

<http://dspace.hebron.edu/xmlui/bitstream/handle/123456789/1128/v9-130-156.pdf?sequence=1&isAllowed>

- الزعابي، سلطان. (٢٠٢١). "آليات مكافحة الجريمة الإلكترونية بالإمارات العربية المتحدة". *مجلة القانون المغربي*، ع ٤٦. ص ٣٠١-٣٢٧. الرابط الإلكتروني: <https://search.mandumah.com/Record/1158259/Description#tabnav>
- زيوش، سعيد، بومدفع، الطاهر. (٢٠٢١). "الجريمة الإلكترونية وآليات الرقابة المجتمعية في الجزائر". *المجلة الجزائرية للعلوم الاجتماعية والانسانية*، مج ٩، ع ٢. ص ٢٣٠-٢٥٣. الرابط الإلكتروني: <https://www.asjp.cerist.dz/en/downArticle/259/9/2/174599>
- الشبلي، عبد الله. (٢٠١٩). "الجريمة الإلكترونية في سلطنة عُمان: التحديات والحلول القانونية". *مجلة العلوم الاقتصادية والادارية والقانونية*. مج ٣، ع ٢٤. ص ٨٣-٩٨. الرابط الإلكتروني: <https://search.mandumah.com/Record/1038161/Description#tabnav>
- المايل، عبد السلام وآخرون. (٢٠١٩). "الجريمة الإلكترونية في الفضاء الإلكتروني: المفهوم - الأسباب - سبل المكافحة مع التعرض لحالة ليبيا". *مجلة أفاق للبحوث والدراسات*. ع ٤٤. ص ٢٤٢-٢٥٥. الرابط الإلكتروني: <https://search.mandumah.com/Search/Results?lookfor>
- المشهداني، أكرم. (٢٠١٥). "الجرائم الإلكترونية: التحديات والمعالجة". *مجلة الدراسات المالية والمصرفية*، مج ٢٣، ع ١. ص ٢٣-٢٨. الرابط الإلكتروني: <https://search.mandumah.com/Record/741850>
- المليحي، عبد الحميد. (٢٠١٩). "الجريمة الإلكترونية: مدخل إلى الإطار المفاهيمي". *مجلة المنارة للدراسات القانونية والإدارية*. مج ١٩. عدد خاص. ص ١٤٥-١٥٩. الرابط الإلكتروني: <https://search.mandumah.com/Record/1058654>
- نجم الدين، سامر. (٢٠٢١). "الجريمة المنظمة الإلكترونية: دراسة تحليلية في التشريع الفلسطيني". *مجلة الجامعة الإسلامية للدراسات الشرعية والقانونية*، مج ٢٩، ع ٢. ص ٩٣-١١٥.

- يس، خالد. (٢٠١٦). "الجهود الدولية لمكافحة الجرائم الإلكترونية". مجلة الدراسات العليا، مج ٤، ع ١٤. ص ١-٣٠. الرابط الإلكتروني :
<https://search.mandumah.com/Record/790745>.

ثالثاً: رسائل الماجستير:

- جلعود، وليد، (٢٠١٣). دور الحرب الإلكترونية في الصراع العربي الإسرائيلي، رسالة ماجستير غير منشورة. كلية الدراسات العليا. جامعة النجاح الوطنية. نابلس.
- العفيفي، يوسف، أيمن، عبد العال، (٢٠٢١). الجرائم الإلكترونية في التشريع الفلسطيني: دراسة تحليلية. رسالة ماجستير. كلية الشريعة والقانون. الجامعة الإسلامية: غزة.

رابعاً: الملتقيات العلمية:

- البعادي، أحمد. (٢٠١٢). دعاوى الجرائم الإلكترونية وأدلة اثباتها في التشريعات العربية بين الواقع والمأمول. ورقة مقدم إلى المؤتمر الثالث لرؤساء المحاكم العليا بالدول العربية ٢٢-٢٥ سبتمبر ٢٠١٢. إدارة الدراسات والبحوث- الخرطوم.
- قوراري. سليمان وآخرون، (٢٠١٧). دور التربية والتوجيه في الحماية والوقاية من الجرائم الإلكترونية. ورقة مقدم إلى المؤتمر الدولي الرابع عشر للجرائم الإلكترونية. مركز جيل البحث العلمي. الجزائر.