المجلة العلمية للتكنولوجيا وعلوم الاعاقة
ISSN: 2682-2873
The Online ISSN : 2682-4256
المجلد06/العـدد: 02 (يونيو2024)، ص ص 119 - 139

سبل وآليات مكافحة الجريمة الإلكترونية في المجتمع العربي

Ways and mechanisms to combat cybercrime in Arab Society

د/ سمير صالحي[1] ،ط د/ سفيان فاسي [2] ،ط د/ محمود تيشوش [3]

[1] جامعة محمد خيضر بسكرة (الجزائر)، Email : samir.salhi@univ-biskra .dz

[2] جامعة محمد خيضر بسكرة (الجزائر)، Email : sofiane.faci@univ-biskra.dz

[3] جامعة محمد خيضر بسكرة (الجزائر)، Email: mahmoud.tichouche@univ-biskra.dz

تاريخ الاستلام: 2024/04/01 تاريخ القبول: 2024/05/23 تاريخ النشر: 2024/06/20
Doi:10.21608/skje.2024.378116

مستخلص البحث

تعتبر الجريمة الإلكترونية من الأشكال الحديثة للاجرائم، التي تعاني منها مؤخرا مختلف دول العالم، نتيجة الانتشار والاستخدام الواسع للتكنولوجية الرقمية، والتي قوامها تكنولوجيا المعلومات والاتصالات الحديثة، لذلك سارعت الكثير منها إلى إيجاد الحلول المناسبة لمكافحتها والتصدي لمخاطرها ومنها بعض الدول العربية التي تبنت استراتيجة رشيدة وفعالة سخرت من خلالها كافة الإمكانيات المادية، واعتمدت في إطارها على سياسة التعاون المتبادل بينها وبين الدول الأجنبية للاستفادة من خبراتها في كيفية التصدي لهذه الظاهرة وتمكنت بفضلها لمواجهة مختلف الجرائم الالكترونية التي تعرضت لها، كما تمكنت في فترة زمنية ووجيزة من التقليل من نسبة وحدة انتشارها.

الكلمات المفتاحية: الجريمة الإلكترونية؛ أشكال الجريمة الالكترونية؛ الأمن الالكتروني؛ مكافحة الجريمة.

المؤلف المرسل: سمير صالحي، Email : samir.salhi@univ-biskra .dz

Abstract:

Cybercrime is one of the modern forms of crimes that various countries of the world suffer from recently, as a result of the widespread and widespread use of digital technology, which is based on modern information and communication technology. Through it, it harnessed all the financial capabilities, and relied within its framework on the policy of mutual cooperation between it and foreign countries to benefit from its experiences in how to address this phenomenon and was able, thanks to it, to confront the various electronic crimes that it was exposed to, and in a short period of time it was able to reduce the percentage of its spread unit.

Keywords: cybercrime; forms of electronic crime; electronic security; The fight against crime.

مقدمة :

عرف المجتمع الحديث تقدما هائلا في درجة التطور التكنولوجي و التقني، خصوصا في مجالات تكنولوجيا الاتصالات و تبادل المعلومات، بحيث أصبحت المعلومات سلعة أو خدمة تباع وتشترى ومصدر قوة اقتصادية وسياسية بالنسبة للمجتمعات التي تحسن جمعها وتنسيقها و استخدامها بحيث تسهم في مضاعفة القدرة على الابتكار والتخطيط في مختلف المجالات مما يؤدي الى دفع عجلة التقدم و التنمية و نتيجة لهذا زاد اهتمام الدول والمجتمعات بتطوير هذا المجال هذا ما أدى إلي توسع الفضاء الالكتروني وتضاعف وزيادة التفاعل ضمنه.

هذا وإن تطور تكنولوجيا المعلومات والاتصالات وزيادة الاعتماد عليها وكذا اتساع التفاعل ضمن الفضاء الالكتروني قد تتجاوز تبعاته وأثاره النواحي الايجابية التنموية لتشمل آثارا سلبية تهدد استقرار و توزان هذه المجتمعات، بحيث أن هذا التطور قد أدى الى تطوير وتحديث الجريمة من حيث الطرق و الأساليب وهذا ما تؤكده "**روى جودسون**" خبيرة بمركز المعلومات الأمريكي بقولها " لقد أصبحت الجريمة أكثر قوة بفضل التقنية الحديثة" (القهوجي، ١٩٩٩، صفحة ٧).

٢. مشكلة الدراسة:-

برزت ظاهرة الجريمة الالكترونية كإحدى أهم الظواهر الاجتماعية الآخذة في النمو والتغلغل داخل المجتمع الحديث، نتيجة الانتشار والاستخدام الواسع للتكنولوجية الرقمية، والتي قوامها تكنولوجيا المعلومات والاتصالات الحديثة، لذلك سارعت الكثير منها إلى إيجاد الحلول المناسبة لمكافحتها والتصدي لمخاطرها ومنها بعض الدول العربية التي تبنت استراتيجية رشيدة وفعالة سخرت من خلالها كافة الإمكانيات المادية، واعتمدت في إطارها على سياسة التعاون المتبادل بينها وبين الدول الأجنبية للاستفادة من خبراتها في كيفية التصدي لهذه الظاهرة وتمكنت بفضلها لمواجهة مختلف الجرائم الالكترونية التي تعرضت لها، كما تمكنت في فترة زمنية ووجيزة من التقليل من نسبة وحدة انتشارها.

ومما سبق سنحاول في هذه الدراسة التطرق لسبل وآليات في مواجهة تحديات الجريمة الالكترونية في المجتمع العربي ؟

وسنتطرق إلى التساؤلات التالية :

- **سبل مواجهة الجرائم الإلكترونية في المجتمع العربي ؟**
- **كيفية حماية نفسك من الجرائم الإلكترونية؟**
- **كيف نتعامل مع الجريمة الالكترونية ؟ دولة قطر أنموذجا.**

٣. أهمية الدراسة:

تعد هذه الجرائم الإلكترونية مرضًا يسبب الفتك بالمجتمعات والعلاقات الإنسانية، ويؤخر من عجلة التقدم والتنمية التي يعيشها العالم مؤخرًا.

- أول هذه الآثار هي تدمير قيم الأسرة من خلال استغلال أفرادها والإساءة له وصورته التي تؤثر في باقي أسرته لمدة طويلة.

- بحث عن الجرائم الإلكترونية ثاني هذه الآثار هو على المجتمع وهو إيقاع الضرر عليه وعلى الاقتصاد والخصوصيات للأفراد كذلك إيقاع الضرر على الدولة التي يتفكك أفرادها مسببًا أعمال انقلاب عسكرية وحروب أهلية.
- كذلك يسبب انتشار الجرائم الإلكترونية انتاج حيل غير سوي يبرر الجريمة ويرتكبها بأريحية دون النظر إلى خطورة ذلك وتداعياته بسبب زيادة استخدام وسائل التواصل وانتشارها داخل المنزل وبين الجميع من الأطفال إلى الكبار.دون النظر إلى الآثار السلبية التي تسببها مثل هذه الجرائم من مشكلات اجتماعية وصحية للضحايا من نشر معلوماتهم وبياناتهم والأخبار الكاذبة التي تضر بهم وعائلاتهم.
- كثرة استغلال الضحية وابتزازها من أجل الحصول على مال يضر بمصالحه الشخصية وذمته المالية.

٤. مصطلحات الدراسة:-

- **مفهوم الجريمة الالكترونية**

لا يوجد إجماع على تعريف الجريمة الإلكترونية من حيث كيف تعرف أو ما هي الجرائم التي يتضمنها،كما يقول "دير هلست و نيف "هناك غياب لتعريف عام و إطار نظري و متسق في هذا الحقل من الجريمة، و يتراوح تعريف الجريمة الإلكترونية بين الجرائم التي ترتكب بواسطة الحاسوب إلى الجرائم التي ترتكب بأي نوع من المعدات الرقمية، و تعرف الجرائم الالكترونية باختصار على أنها الجرائم التي ترتكب باستخدام الحاسوب و الشبكات و المعدات التقنية مثل الجوال. تتكون الجريمة الإلكترونية من مقطعين هما: الجريمة و الإلكترونية

١.٢تعريف الجريمة من الناحية اللغوية : مشتقة من كلمة الجرم التي تعني التعدي و الذنب و الجمع و إجرام و جروم و هو جرم،يجرم، و إجترم، و أجرم : أذنب و أيضا في

اللغة العربية استخدمت للإشارة إلى أنها الكسب المكروه غير المستحسن،كما يراد منها الحمل على فعل إثم(البدانية، ٢٠١٤، االصفحة ٤) .

التعريف القانوني للجريمة:" السلوك المادي الصادر عن الإنسان و الذي يتعارض مع القانون" و تعرف أيضا على أنها ذلك الفعل الذي يعاقب عليه بموجب القانون أو هي الفعل و الامتناع الذي نص القانون عللا تجريمه و وضع عقوبة جزاءا على ارتكابه.

التعريف النفسي للجريمة: يرى أنصار هذا الاتجاه منهم العالم النفساني "**برت**" أن "التصرفات الإجرامية ما هي إلا الانطلاق للدوافع الغريزية انطلاقا حرا لا يعيقه عائق و يرى أنه من الممكن النظر إلى أنواع الانحراف المختلفة كالسرقة و الاعتداء و الاغتصاب و الجرائم الجنسية و غيرها على أنها تغيرات لغرائز معينة"(ساجي، بوكابوس، ٢٠٢٢).

التعريف الاجتماعي للجريمة : يرى أنها الواقعة الضارة بكيان المجتمع وأمنه. وتعرف الجريمة الالكترونية على أنها كل فعل أو امتناع عبر فعل من مسألة الاعتداء على الموال المعنوية (معطيات الحاسب) يكون ناتجا بطريقة مباشرة وغير مباشرة لتدخل التقنية الالكترونية".(عبابنة، ٢٠٠٥، صفحة ١٧) كما يمكن تعريفها أيضا على أنها كل استخدام في صورة فعل أو امتناع غير مشروع للتقنية المعلوماتية، ويهدف إلى الاعتداء على أي مصلحة مشروعة، سواء أكانت مادية أو معنوية".(المطردي، ٢٣-٢٥ سبتمبر ٢٠١٢، صفحة ١٢).

هذا ويعرفها "عبد الله دغش العجمي"بأنها " كل فعل أو امتناع يتم إعداده أو التخطيط له، ويتم بموجبه استخدام أي نوع من الحواسيب الآلية سواء حاسب شخصي او شبكات الحاسب الآلي أو الإنترنت أو وسائل التواصل الاجتماعي لتسهيل ارتكاب جريمة أو عمل مخالف للقانون، أو تلك التي تقع على الشبكات نفسها عن طريق اختراقها بقصد تخريبها أو تعطيل أو تحريف أو محو البيانات أو البرامج التي تحويها" (العجمي، ٢٠١٤، صفحة ١٤).

وبناءا على التعريفات السابقة يمكن أن نعتبر **الجريمة الالكترونية** على أنها " كل جريمة يمكن ارتكابها بإستخدام نظام أو شبكة حاسوبية أي ترتكب في البيئة الإلكترونية و هي أي فعل غير مصرح به و غير قانوني في البيئة الإلكترونية.أما **المجرم المعلوماتي:** فهو شخص يختلف عن المجرم العادي فلا يمكن أن يكون هذا الشخص جاهلا بتقنيات المعلوماتية الحديثة، فهو يمتلك قدرة فائقة في المهارة التقنية و يستغل مهاراته في اختراق الشبكات و كسر كلمات المرور و يسبح في عالم الشبكات ليحصل على كل ما هو غال و ثمين من البيانات و المعلومات الموجودة في أجهزة الحواسيب و من خلال الشبكات بشكل غير قانوني و غير مشروع.

أنواع الجريمة الالكترونية:

لقد تعددت أنواع الجريمة الالكترونية بتعدد مجالاتها و طرقها وأساليبها وفي مايلي أكثر أنواع الجرائم الالكترونية انتشارا (البدانية، ٢٠١٤، الصفحات ٢٣-٢٤) هي :

- **تخريب أو سرقة أو تزوير المعلومات:** وتشمل كل العمليات الالكترونية التي يهدف من خلالها الفاعل إلى نسب معلومات له (السرقة العلمية) أو تزويرها أو تخريب أو تحريف أو إساءة استخدامها.
- **انتهاك الخصوصية:** وهي العمليات الإلكترونية التي تهدف إلى المساس بالطبيعة الخاصة بالأفراد مثل قرصنة الحسابات الشخصية و التجسس وتشهير بالمعلومات الخاصة ونشرها بهدف الإساءة إلى شخصيات معينة.
- **قرصنة البرمجيات و البيانات:** وتشمل عمليات النسخ الغير قانوني للبرمجيات واستخدامها أو بيعها مرة أخرى ومثل ذلك مع البيانات قصد الاستفادة منها بطريقة غير شرعية.
- **نشر المواد الإباحية و التحرش الجنسي:** وتشمل عمليات نشر صور وفيديوهات جنسية خاصة لدى الأطفال و الإناث وكذا نشر الجنس التخيلي (Cyber Six) على الشبكات مثل شبكات التواصل الاجتماعي.

- **برمجة الفيروسات وإرسالها:** وهي تتعلق بإنشاء برمجيات الكترونية بهدف تدمير بيانات أو التحكم فيها وتزييفها ثم إرسالها عبر البريد الالكتروني وهي ما يعرف "القنابل الالكترونية" ونشرها في مواقع التواصل الاجتماعي وغيرها.
- **الاحتيال المالي:** وذلك من خلال قرصنة البنوك و البطاقات الائتمانية بهدف تحصيل الثروة و الربح المالي بطريقة غير مشروعة.
- **الإرهاب الالكتروني:** وذلك من خلال استغلال الأجهزة الالكترونية وشبكاتها في نشر أفكار التطرف ونشر التكتيكات الإرهابية وأسلحته وأهدافه وهو ما يعرف بالإرهاب الالكتروني.
- **المطاردة و الملاحقة و الابتزاز:** وتشمل ملاحقة الذكور للإناث او ملاحقة الشخصيات المعروفة وابتزازهم وسبهم وشتمهم عبر استخدام البريد الالكتروني او مواقع التواصل الاجتماعي.

خصائص الجريمة الإلكترونية:

تتميز الجريمة الالكترونية بمجموعة من الخصائص التي تميزها عن الجريمة العادية ولعل من بين أهم هذه الخصائص:

- نجد مرتكب الجريمة الإلكترونية في الغالب شخص يتميز بالذكاء والدهاء ذو مهارات تقنية عالية ودراية بالأسلوب المستخدم في مجال أنظمة الحاسب الآلي وكيفية تشغيله وكيفية تخزين المعلومات والحصول عليها، في حين أن مرتكب الجريمة التقليدية في – الغالب- شخص أمي بسيط، متوسط التعليم.
- مرتكب الجريمة الإلكترونية– في الغالب– يكون متكيفا اجتماعيا وقادرا ماديا، باعثه من ارتكاب جريمته الرغبة في قهر النظام أكثر من الرغبة في الحصول على الربح أو النفع المادي، في حين أن مرتكب الجريمة التقليدية– غالبا– ما يكون غير متكيف اجتماعيا وباعثه من ارتكابه الجريمة هو النفع المادي السريع(المطردي، ٢٠١٢، صفحة ١٦).

- **جريمة عابرة للقارات:** أي أنها تتخطى الحدود الجغرافية لاتصالها بعالم الانترنت و تقنية المعلومات،حيث قد تتأثر دول كثيرة بهذه الجريمة و في آن واحد بسبب السرعة الفائقة و الهائلة في تنفيذها،فيمكن أن تقع الجريمة في دولة من طرف الجاني و المجني عليه يكون في دولة أخرى و في وقت يسير جدا.
- **صعوبة اكتشاف و إثبات الجريمة الالكترونية:**فالجرائم الالكترونية تتصف بالخفاء أي عدم وجود آثار مادية يمكن متابعتها،و هي خطيرة و صعبة الاكتشاف أو هي صعبة في تحديد مكان وقوعها و مكان التعامل معها بسبب اتساع نطاقها المكاني و ضخامة البيانات،و ترجع صعوبة إثبات الجريمة الالكترونية إلى عدة أمور و أهمها:

- تقع في بيئة الكترونية يتم فيها نقل المعلومات و تداولها بدون مستندات ورقية و لا تترك آثارا مادية.
- صعوبة الاحتفاظ الفني بدليل الجريمة المعلوماتية.
- تحتاج إلى خبرة فنية و الذكاء في ارتكابها و يصعب على المحقق التقليدي التعامل معها.
- تعتمد على الخداع في ارتكابها و التضليل في التعرف على مرتكبيها،و هذا ما يساعد على ازدياد عدم التعرف على مرتكبي الجريمة الالكترونية،مثلا إحجام البنوك و المؤسسات عن الإبلاغ عما يرتكب من جرائم معلوماتية تجنبا للإساءة إلى سمعتها و هز ثقة العملاء،و كذلك إخفاء أسلوب ارتكاب الجريمة خوفا من قيام آخرين بتقليد هذا الأسلوب.
- **وقوع الجريمة المعلوماتية أثناء المعالجة الآلية للبيانات:**حيث أنها قد تقع أثناء عملية المعالجة الآلية للبيانات في أي مرحلة من المراحل الأساسية لتشغيل نظام المعالجة الآلي للبيانات سواء عند مرحلة إدخال البيانات أو أثناء مرحلة المعالجة أو عند إخراج المعلومات.

- **الجريمة الالكترونية مستحدثة:** تعتبر الجرائم الالكترونية سواء التي تتعرض لها أجهزة الكمبيوتر أو التي تسخر تلك الأجهزة في ارتكابها من الجرائم المستحدثة،فعلى الرغم من المزايا و المنافع الإيجابية المترتبة عن العولمة و ثورة المجتمع الالكتروني إلا أنها ساعدت على ظهور و تعزيز أنواع جديدة من الجرائم من أبرزها جرائم **غسيل الأموال،سرقة الملكيات الفكرية،...الخ.**
- **جرائم ناعمة:** تتميز الجرائم الالكترونية عن الجرائم التقليدية في أنها لا تحتاج إلى أدنى جهد عضلي في ارتكابها بل تعتمد على المجهود الذهني المحكم،و التفكير العلمي المدروس القائم على معرفة تقنية ممتازة بالحاسب الآلي و التعامل السليم بالشبكة على أساس أن الجاني في الجرائم الالكترونية هو إنسان متوافق مع المجتمع و لكنه يقترف هذا النوع من الجرائم بدافع اللهو أو لمجرد إظهار تفوقه على آلة الكمبيوتر أو البرامج التي يشتغل بها.

سبل و آليات مواجهة الجرائم الالكترونية:

سبل مواجهة الجرائم الإلكترونية في المجتمع العربي

وأمام التحديات الكبيرة التي تعيشها المجتمعات المعاصرة بظهور الجريمة الالكترونية وتأثيراتها على مختلف مجالات المجتمع وشرائحه، فإنه من الضروري بما كان البحث عن الحلول الوقائية و العلاجية و التي تسمح بتصدي لأخطار هذا النوع من الجرائم و ذلك بتفعيل مختلف الروابط أو الضوابط الاجتماعية السائدة وتطويرها بما يتناسب مع مختلف خصوصيات الجريمة الالكترونية المعاصرة ، وفي ما يلي **سنحاول عرض بعض أهم الآليات المساعدة** في تحقيق ذلك :

تفعيل دور الأنساق التربوية بالمجتمع:

إن انتقال الجريمة من الواقع الملموس إلى العالم الافتراضي الالكتروني وبالخصوص مواقع التواصل الإجتماعي جعل منها جريمة عابرة للحدود و سريعة النفاذ للمجتمعات فإنه من الضروري على هذه الأخيرة تطوير استراتيجياتها التربوية بما يتوافق مع درجة تطور هذه الجريمة وذلك من أجل تحصين أفراده أخلاقيا و علميا وثقافيا من خلال اعتماد مختلف الأنساق التربوية (الأسرة، المدرسة، المسجد، الجامعة، دور

الشباب، الجمعيات ..الخ) على برامج تربوية و تثقيفية و رياضية تساعد أفراد المجتمع على تفريغ طاقاتهم في الواقع الملموس، وكذا تنشيط أوقات فراغهم وفتح باب الحوار العلمي و الثقافي مع هذه الشريحة سيساهم في بناء شخصية متوازنة يغلب عليها التعقل و الاتزان وهو ما يساهم في تبني الفرد لمضامين مجتمعه و بالتالي ضمان عدم انجراره وراء السلوكيات العدوانية و الإجرامية (عيسات، ٢٠٢٢، الصفحات١٢٥-١٤٥).

حيث تقوم الأسرة ومختلف منظمات المجتمع المدني دورا في مكافحة الجرائم الالكترونية، وذلك بالتنوير بخطورتها والتي تؤدي إلى التهلكة وخاصة فئة الشباب والذين يمكثون ساعات طويلة أمام شاشات الحواسيب و الهواتف الذكية، وحسب دراسة أمريكية التي تقول استخدام الأطفال لتكنولوجيا الحديثة يدفعهم شيئا فشيئا الى ممارسة سلوكات عنيفة مترجمة في الجرائم الالكترونية ومواقع التواصل الإجتماعي بأنواعه نظرا لسهولة افتعالها وصعوبة كشف مرتكبيها . فينبغي التعامل معهم بذكاء لمنعهم لولوج هذه المواقع والعمل على تحويل هذه المواقع من مواقع للممارسة العنف الى مواقع تعليمية تربوية.

كما قوم الجامعة بدور هام من خلال ما تقدمه من معلومات ومعطيات حول كيفية التعامل مع مختلف الخدمات (المواقع الالكترونية) من جهة، وكذا تقديم المساعدات الفنية للشركات، وتقديم برامج المساعدة القانونية في مجال الجريمة الالكترونية لوكالات الأمن الوطني والعدالة الجنائية من جهة أخرى(تقرير مكتب الأمم المتحدة، ٢٠١٢، ص ٣٦١).

تفعيل دور النسق الإعلامي:

يمارس الجانب الإعلامي دورا هاما في توعية وتربية مختلف شرائح المجتمع خصوصا في ظل تطور تكنولوجيا المعلومات و الاتصالات بحيث أصبحت هذه القنوات الإعلامية في كل بيت وعلى الكثير من الأجهزة الالكترونية (حاسوب، هاتف، لوحة ..الخ) وأصبحت من ضروريات الحياة، وبالتالي على الفاعلين في هذا النسق الإعلامي تحمل بعض من المسؤولية في مواجهة أخطار الجريمة الالكترونية خصوصا على الفئات ذات الشخصية الهشة كالأطفال و المراهقين وذلك من خلال إشرافهم على تقديم برامج توعوية بأخطار و تحديات الفضاء الالكتروني على المراهقين و كذا توجيهيه لمساعدة

الأسرة على مرافقة أبنائهم في مرحلة المراهقة و التكفل بقضاياهم ومشاكلهم وهو ما يساهم في تحصينهم من أخطار الجريمة الالكترونية(عيسات، ٢٠٢٢، الصفحات١٢٥-١٤٥).

استغلال طاقات وأفكار الشباب ودمجها في المشاريع التنموية:

إن من بين الأسباب التي تدفع المراهقين لولج عالم الجريمة الالكترونية هو عدم الاهتمام بطاقاتهم و استغلال أفكارهم في الواقع الملموس مما يزيد من شعور عدم تقدير الذات لديهم وبالتالي يتجهون للبحث عن فضاءات أخرى –بما في ذلك الفضاء الالكتروني- لإظهار طاقاتهم وفرضها ولو على حساب ضوابط المجتمع ومعاييره، و بالتالي فإن دمج المراهقين في العملية التنموية من خلال استغلال أفكارهم ومشاركة اقتراحاتهم يعد عاملا مساعدا على ضبط سلوكاتهم وتوجهها نحو تحقيق الأهداف العامة للمجتمع وبالتالي تفعيل ثقافة المواطنة الصحيحة و تعزيز روح الانتماء لديهم (عيسات، ٢٠٢٢، الصفحات١٢٥-١٤٥).

التغذية الروحية و تشجيع الرقابة الذاتية:

إن من بين أسباب ولوج الشباب عالم الإجرام الالكتروني هو وجود الحرية التامة و غياب الرقابة و نقص الوازع الديني والقيم الأخلاقية و المثل العليا وعليه فمن الضروري اهتمام مؤسسات التنشئة الاجتماعية بملء الفراغ الروحي لدى المراهقين بالقيم الروحية الدينية القائمة على الإخلاص في العمل و الصدق في القول و التضامن وخدمة الصالح العام و احترام الضمير الجمعي وهو ما يخلق فهم روح الرقابة الذاتية لتصرفاتهم و سلوكاتهم ويقلل من فرص الانخراط في عالم الجريمة الالكترونية(عيسات، ٢٠٢٢، الصفحات١٢٥-١٤٥).

تفعيل إجراءات النسق القانوني والمبادرات التشريعية و الردعي بما يتوافق مع خصوصيات الجريمة الإلكترونية:

هناك الكثير من الدول لم تطور أنظمتها التشريعية و قوانينها الردعية وأجهزة العدالة بها لكي تتمكن من مجاراة التقدم الحاصل في الجريمة الالكترونية وأساليبها، وهذا لا يتوقف عند التشريعات و النظم القانونية و إنما يشمل أجهزة تطبيق القانون

مثل الشرطة و التحقيق و القضاء وكيفية التعامل مع الأدلة الرقمية على المستوى الوطني و الدولي،(البدانية، سبتمبر ٢٠١٤، صفحة ١٥) وان هذا الضعف المسجل على مستوى أساليب الأجهزة الردعية و الرقابية وكذا التشريعات و النظم القانونية يعد عاملا مساهما في تشجيع أفراد المجتمع على تبني السلوكات الإجرامية دون خوف من الإدانة و العقاب، وعليه فمن الضروري تدعيم المنظومة التشريعية بنصوص قانونية تتجاوب مع تطورات أشكال الجريمة الالكترونية و تعقيداتها وتطوير أساليب الرقابة و الملاحقة وضبط الأدلة و سياسة العقاب الردعي ضد المجرمين المنتهكين للضوابط و القواعد الاجتماعية، بالإضافة إلى النصوص التشريعية التي تشدد على الأسرة تحمل مسؤولياتها اتجاه أبنائها خصوصا المراهقين منهم لمنع كل أشكال الإهمال الذي يؤدي إلى ولوجهم عالم الجريمة بما في ذلك الجريمة الالكترونية.(عبد السلام، ٢٠١٤، صفحة ١٢٨).

- **المبادرات التشريعية:** ومن خلال سن الدول العديد من القوانين الهادفة إلى منع انتشار الجريمة الالكترونية والتقليل من عددها . فعلى سبيل المثال قامت فرنسا في عام ١٩٨٨ بإصدار قانون لمعاقبة الجرائم المعلوماتية (كإتلاف البيانات) .
- كما قامت المملكة العربية السعودية في عام ٢٠١٧ بتأسيس كل من الهيئة الوطنية للأمن السيبراني الهادفة إلى تعزيز أنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات وحماية الأمن الوطني وكذا "الاتحاد السعودي للأمن السيبراني والبرمجة " والذي يهدف إلى بناء القدرات الوطنية في مجال الأمن السيبراني للاستفادة منها في عملية سنّ القوانين والسياسات. المتعلقة به .
- إنشاء مصر للجمعية المصرية لمكافحة جرائم المعلوماتية والانترنت في عام ٢٠٠٤. والتي تعمل على توعية الجمهور بمخاطر هذه الجرائم ووضع إحصائيات حول مدى انتشارها، إضافة إلى المساهمة في تقديم خدمات البلاغ الرقمي.

- **الاتفاقيات والمعاهدات الإقليمية:** سارعت الدول العربية إلى إبرام الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في ٢١ ديسمبر ٢٠١٠، بجامعة الدول العربية، وذلك بهدف إيجاد حلول لمواجهة الجرائم الناتجة عن استخدام التقنيات الحديثة. حيث أكدت على ضرورة التزام الدول التي صادقت عليها بتطبيق مجموع القواعد الإجرائية المتفق عليها، والتي لابد وان تكون متوافقة مع القوانين الداخلية الخاصة بها. والتي تتعلق أساسا بالأبحاث الجنائية وإجراءات التفتيش على المعلومات المخزنة والتجميع الفوري لها أو اعتراض محتواها (لجنة منع الجريمة والعدالة، ص٥).
- **دور الشرطة القضائية:** تمارس الشرطة القضائية دورا مهما في مكافحة الجرائم الالكترونية والحد من انتشارها باعتبارها أحد المنفذين الرئيسيين لبرامج الأمن الوطني الالكتروني.

الوعي ونشر تدابير الوقاية: ويعد هذا من بين الإجراءات المساعدة التي تقلل من حدة انتشار الجرائم الالكترونية، حيث تسمح الحملات التوعوية على المستوى العالمي من التعريف بهذه الجرائم وبالمخاطر التي تنجم عنها وبضرورة عدم افتعالها عبر مختلف وسائل الإعلام التقليدية منها والحديثة. (تقرير مكتب الأمم المتحدة، ٢٠١٢، ص ٣٦١).

كيفية حماية نفسك من الجرائم الإلكترونية:

نظرًا لانتشار الجرائم الإلكترونية، قد تتساءل عن وقاية نفسك منها. إليك بعض النصائح البسيطة لحماية جهاز الكمبيوتر الخاص بك وبياناتك الشخصية من الجرائم الإلكترونية:

- **إبقاء البرنامج ونظام التشغيل محدّثَين:** يضمن إبقاء البرنامج ونظام التشغيل لديك محدّثَين استفادتك من أحدث تصحيحات الأمن لحماية جهاز الكمبيوتر الخاص بك.
- **استخدام برنامج مكافحة الفيروسات وإبقائه محدّثًا:** يشكّل استخدام برنامج لمكافحة الفيروسات أو حل شامل لأمن الإنترنت مثل Kaspersky Total Security طريقة ذكية لحماية النظام من الهجمات. يتيح لك برنامج مكافحة

الفيروسات إمكانية فحص التهديدات واكتشافها وإزالتها قبل أن تصبح مشكلة. وجود هذه الحماية يساعد في حماية جهاز الكمبيوتر الخاص بك وبياناتك من الجرائم الإلكترونية، مما يمنحك راحة البال. أبقِ برنامج مكافحة الفيروسات محدَّثًا للحصول على أفضل مستوى من الحماية.

- **استخدام كلمات مرور قوية:**تأكد من استخدام كلمات مرور قوية لا يمكن للأشخاص معرفتها ولا تقم بتسجيلها في أي مكان. يمكنك كذلك استخدم تطبيق مدير كلمات مرور حسن السمعة لإنشاء كلمات مرور قوية بشكل عشوائي لتسهيل الأمر عليك.
- **عدم فتح المرفقات في رسائل البريد الإلكتروني العشوائية أبدًا:**تشكّل مرفقات البريد الإلكتروني في رسائل البريد الإلكتروني العشوائية طريقة تقليدية لإصابة جهاز الكمبيوتر ببرامج ضارة وغيرها من أشكال الجرائم الإلكترونية. لا تفتح أبدًا مرفقًا من مرسِل لا تعرفه.
- **عدم فتح الروابط في رسائل البريد الإلكتروني العشوائية أو على مواقع الويب غير الموثوق بها:**توجد طريقة أخرى يصبح بها الأشخاص ضحايا للجرائم الإلكترونية، وهي فتح الروابط الموجودة في رسائل البريد الإلكتروني العشوائية أو الرسائل الأخرى أو المواقع الإلكترونية غير المألوفة. تجنّب القيام بهذا الأمر للحفاظ على أمنك على الإنترنت.
- **عدم تقديم المعلومات الشخصية إلا إذا كنت آمنًا:**لا تقدم أبدًا بيانات شخصية عبر الهاتف أو عبر البريد الإلكتروني إلى أي جهة ما لم تكن متأكدًا تمامًا من أمان الخط أو البريد الإلكتروني. تأكد من أنك تتحدث إلى الشخص الذي تعتقد أنك تتحدث معه.
- **الاتصال بالشركات مباشرةً بشأن الطلبات المشبوهة:**إذا اتصلت بك شركة وطلبت منك معلومات شخصية أو بيانات، أنه المكالمة بدون إعطائهم شيء، ثم أعد الاتصال بهم مرة أخرى باستخدام الرقم الموجود على الموقع الإلكتروني الرسمي الخاص بهم للتأكد من أنك تتحدث إلهم وليس مع مجرمي الإنترنت. الأفضل كذلك استخدام رقم هاتف مختلف لأن مجرمي الإنترنت يمكنهم إبقاء

الخط مفتوحًا. عندما تعتقد أنك اتصلت بالشركة مجددًا، يمكنهم الادّعاء بأنهم من المصرف أو مؤسسة أخرى تعتقد أنك تتحدث معها.

التنبّه لعناوين مواقع URL التي تزورها:راقب عناوين مواقع URL التي تفتحها. هل تبدو مشروعة؟ تجنب الضغط على الروابط التي تحتوي على عناوين URL غير مألوفة أو التي تبدو كرسالة غير مرغوب فيها. إذا كان منتج أمن الإنترنت لديك يشمل وظائف لضمان أمن المعاملات عبر الإنترنت، فتأكد من تمكينها قبل تنفيذ المعاملات المالية عبر الإنترنت.

- **مراقبة بياناتك المصرفية:**من المهم اكتشاف أنك وقعت ضحية جريمة إلكترونية بسرعة. راقب بياناتك المصرفية واستفسر عن أي معاملات غير مألوفة مع المصرف، ويمكن للمصرف التحقيق فيما إذا كانت احتيالية أم لا.

سيحميك مضاد الفيروسات الجيد من خطر الجرائم الإلكترونية. اعرف معلومات أكثر عن Kaspersky

قراءة في التجربة القطرية لكيفية التعامل مع الجريمة الالكترونية والحد من انتشارها:

رغم خطورة الجرائم الالكترونية وصعوبة إيجاد الحلول المناسبة للحد من انتشارها، فإن إمكانية التقليل منها ليس بالأمر المستحيل.

أساليب مواجهة الجريمة الالكترونية في قطر:

اعتمدت الدولة القطرية على مجموعة من الأساليب والسياسات الداخلية والخارجية بهدف مكافحة الجريمة الالكترونية والتقليل من حدة انتشارها، ومن بين أهم هذه الآليات نجد ما يلي (فازية خلفوني،٢٠٢١، الصفحات ١١-٢٤).

- إصدار قانون مكافحة الجرائم الالكترونية ٢٠١٤، الذي يركز على تحديد مختلف الحالات التي تصنف ضمن الجرائم الالكترونية وتبعات ذلك من ناحية العقوبات التي ستفرض على كل مرتكب لها، ومتابعة الأفراد الذين ينشرون الأخبار غير الصحيحة بقصد تعريض النظام العامل للخطر، وقدرت العقوبة ب ثلاث سنوات سجن وغرامة مالية قدرها ٥٠٠٠٠٠ ألف ريال، مع مضاعفة العقوبة لجريمة التزوير والاحتيال الالكتروني.

- التدريب الوظيفي للتعامل مع الهجمات الالكترونية، من خلال تدريب الموظفين في مختلف المجالات لكيفية التعامل معها من خلال التدرب على توفير الحماية لمختلف الأنظمة من جهة، والعمل على كشف وإحباط الجرائم قبل حدوثها من جهة أخرى.
- إنشاء مراكز مكافحة الجريمة الالكترونية، والتي تعنى بتحقيق هذه الغاية على أرض الواقع، كإنشا المركز الوطني لأمن المعلومات بالتعاون مع معهد هندسة البرمجيات في جامعة كار جيني ميلان الأمريكية في ديسمبر عام ٢٠٠٥، بهدف مواجهة تهديدات الجريمة الالكترونية وتحديات الأمن السيبراني واعتماده كوسيلة لبناء مقدرات التعامل مع معلومات البنية التحتية الحرجة لدولة قطر.
- كما تم أيضا تأسيس الفريق القطري للاستجابة لطوارئ الحاسب عام ٢٠٠٥ من طرف وزارة الاتصالات وتكنولوجيا المعلومات بالتعاون مع جامعة ميلون كارن يجي والتي تعرف باسم " كيوسرت "(منظمة غير ربحية تعمل على الإلمام باحتياجات الدولة القطرية في مجال أمن المعلومات).
- العمل على حماية المؤسسات المالية من الجرائم الالكترونية التي تتعرض لها المؤسسات المالية والنقدية في الدولة القطرة سواء كان ذلك من ناحية الخطورة أو العدد.، وفي هذا الصدد قام مصرف قطر مثلا عام ٢٠١٠ بوضع مجموعة من العمليات والإجراءات الوقائية التي من شأنها حماية المنظمة المصرفية.
- التركيز على مبدأ التعاون، قد أوضح أحد الخبراء المتخصصين في مكتب الأمم المتحدة لمكافحة الجرائم في هذا الشأن، أن الجرائم الالكترونية هي جريمة القرون اللاحقة، وفي هذا الإطار تم التعاون مع قاعدة الأنتربول الدولية للجرائم الالكترونية المرتكبة ضد الأطفال، وهي التجربة الأولى من نوعها عربيا، حيث تم تشكيل فريق يضم في عضويته كلا من إدارات البحث الجنائي

والتعاون الدولي وشرطة الأحداث ومركز الحماية والتأهيل الاجتماعي ويتم في إطاره اعتماد دورات تدريبية لتحليل الصور والأفلام، والقائم على معلومات أكثر من ١٤٠ دولة مشتركة.

النتائج المحققة للسياسة القطرية في مواجهة الجريمة الالكترونية:

تعتبر التجربة التي اعتمدتها الدولة القطرية في مكافحة الجريمة الالكترونية من أنجح التجارب التي عرفتها البلدان العربية، رغم أنها أكثر من أكثر البلدان عرضة للهجمات الالكترونية نتيجة الاستخدام المكثف والكبير للتكنولوجيا الحديثة، حيث بلغ عدد مستخدمي الانترنت بها إلى أكثر من ٣٤.٨ بالمائة في سنة ٢٠١٤،لتصل بعد عامين إلى ما يعادل ٤٠ بالمائة، حيث لم يمنعها هذا من مواجهة الجريمة الالكترونية والتقليل من مستوى انتشارها وذلك نتيجة عملية التوازن بين ظروف ومتطلبات بيئتها الداخلية والمستجدات الحاصلة في العالم بخصوص وضع وتطور الجريمة الالكترونية وسبل مواجهتها.

إن نجاح الدولة القطرية في الحصول والإبقاء على الترتيب الأول خليجيا وعالميا في مجال الأمن الالكتروني دليل كاف على فعالية الإستراتجية التي اعتمدتها منذ سنة ٢٠٠٥، حيث تمكنت في هذه الفترة من مواجهة الجرائم المختلفة التالية(فازية خلفوني،٢٠٢١، الصفحات ١١-٢٤).

- كشف جرائم استخدام البطاقات الائتمانية التي كانت منتشرة بكثرة في قطر.
- تمكن فريق الأمن السيبراني القطري في عام ٢٠١٤ من كشف ومعالجة١٤ مليون سجل معلومات تعرضت للتهديد والاحتيال، في قطاع التعليم، الطاقة والمؤسسات المالية.
- كشف ومعالجة ٢ مليون إصابة شملت الشبكات المنزلية والشركات إضافة إلى العمل على توجيه أزيد من ٣٠٠٠٠ تحذير بالتهديد المحتمل خاصة من خلال مواقع التواصل الاجتماعي

وهنا يتبين أن الإستراتيجية الترشيدية التي اعتمدتها الدولة القطرية ساعدتها في تحقيق نتائج جد إيجابية واجهت من خلالها الجرائم الالكترونية التي كانت منتشرة، الأمر الذي جعلها تحتل المراتب الأولى في درجة التمتع بالأمن السيبراني.

فلقد عرفت الدولة القطرية منذ بداية استخدامها لتكنولوجيا الاتصالات التفاعلية، انتشارا ملحوظا لظاهرة الجرائم الالكترونية، غير أنها تمكنت وفي ظرف وجيز من احتوائها ومنع تفاقمها، وذلك بفضل سياسة التكامل والتعاون الداخلي والخارجي، إلى جانب إستراتجيتها الوطنية التي استثمرت فيها كافة مواردها المالية والبشرية لتحقيق ذلك على أرض الواقع، من خلال تظافر كافة الجهود السياسية والمدنية لمواجهة الجريمة الالكترونية والتقليل من حدة انتشارها تجنبا للأضرار النفسية والمادية والمالية التي يمكن أن يمكن أن تلحق بالفاعل والضحية على حد السواء .فكلما كان استخدام التقنيات الحديثة لتكنولوجيا الاتصالات استخداما غير عقلاني، كلما أدى ذلك إلى توجه الأشخاص نحو ارتكاب الجرائم الالكترونية سواء كان ذلك عن قصد أو عن غير قصد، مخلفا نتائج جد وخيمة على المستوى الشخصي وعلى مستوى المجتمع ككل. الأمر الذي يتطلب اعتماد سياسة رشيدة وفعالة في مكافحة الجريمة الالكترونية في قطر، إلى جانب التركيز على تفعيل استراتيجية التكامل الداخلي والخارجي التي اعتمدها الدولة القطرية والتي ساعدت كثيرا في مواجهة الجريمة الالكترونية والتقليل من حدة انتشارها.

خاتـمة:

وعلى ضوء ما سبق و نظرا لطبيعة الجريمة الالكترونية الخاصة وبيئتها غير المحسوسة تظهر لنا جليا صعوبة المهام التي تؤديها السلطات الأمنية والقضائية للكشف عن مرتكبيها.وايضا إلى خصوصية المجتمعات العربية المحافظة والمتكتمة عن الجرائم التي تحدث ضد أفرادها وأسرها تزيد من أثر الجريمة المعلوماتية السلبي.كما نجد جرائم شبكات التواصل الاجتماعي ذات بعد دولي ولا تحدها الأوطان أو الأقاليم مما يتطلب التعاون الدولي للحد منها.

مقترحات الدراسة:

ومن بين الاقتراحات التي يمكن تقديمها بشأن مكافحة الجرائم الالكترونية والتقليل من حدة انتشارها ما يلي:

- ضرورة توفير آليات وسبل الرقابة الفعلية والمستمرة لتقنيات تكنولوجيا الاتصالات الحديثة على مستوى العائلة والمجتمع. وذلك توعية الأشخاص بكل مكان عن أسباب حدوث الجرائم وكيفية تنفيذها،فو سائل الإعلام له دور هام في توعية المواطنين عن مدى خطورة الجرائم الإلكترونية، كما يجب الإشارة أيضاً إلى كيفية التعامل معها والحماية منها. مع تجنب نشر أي صور شخصية أو معلومات شخصية على مواقع التواصل الاجتماعي أو أي مواقع أخرى، وذلك حتى لا تتعرض للسرقة ومن ثم الابتزاز من قبل مرتكبي الجرائم الإلكترونية.
- عدم كشف كلمات المرور لأي حساب على موقع معين بالإنترنت، كما يجب أيضاً تغييرها باستمرارلضمان عدم وقوعها في الأيدي الخاطئة.
- التأكيد على ضرورة تشديد وتطبيق العقوبة ضد مرتكبي الجرائم الالكترونية.
- الإكثار من حملات التوعية بمخاطر الجرائم الالكترونية على الجاني والضحية، خصوصا على مستوى المؤسسات التربوية والتعليمية.
- التأكيد على أهمية التنشئة الأسرية والاجتماعية للأفراد (الأطفال)، حتى لا تنعكس التربية السيئة سلبا على سلوكاتهم مستقبلا، ودفعهم إلى ارتكاب الجرائم الالكترونية.
- العمل على فتح دورات تدريبية ولتكوين متخصصين في كيفية استخدام التقنيات الحديثة من جهة ولكيفية الوقاية من الجرائم الالكترونية ومواجهتها.
- تفعيل دور النسق الإعلامي في توعية وتربية مختلف شرائح المجتمع خصوصا في ظل تطور تكنولوجيا المعلومات و الاتصالات السمعية والبصرية.

قائمة المراجع :

- البدانية، ذياب موسى (٢٠١٤).**الجرائم الالكترونية- المفهوم و الأسباب،** الملتقى العلمي الجرائم المستحدثة في ظل المتغيرات و التحولات الإقليمية و الدولية، كلية العلوم الإستراتيجية، عمان، الأردن.

- بوبكر المطردي،مفتاح.(٢٥-٢٣ سبتمبر ٢٠١٢).**الجريمة الالكترونية و التغلب على تحدياتها**، المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية .
- تقرير مكتب الأمم المتحدة(٢٠١٢).
- خلفوني فازية (٢٠٢١). **سبل وآليات مكافحة الجرائم الإلكترونية قراءة في التجربة القطرية (٢٠٠٥-٢٠١٤)**، مجلة التميز الفكري في العلوم الاجتماعية والإنسانية، جامعة الطارف، الصفحات ١١-٢٤.

- ساجي فوزية، بوكابوس عبد القادر(٢٠٢٢). **ظاهرة الجريمة،المفهوم و الأسباب و الأشكال**، مجلة أبحاث، المجاد٧العدد١٠.
- سي حمدي عبد المؤمن، قيرة سعاد(٢٠٢٢). **الجريمة الالكترونية و آليات التصدي لها في القانون الجزائري**، مجلة البيان للدراسات القانونية و السياسية ،المجلد٧،العدد١، الصفحات ٦٢،٦١.

- عبابنة، محمد أحمد.(٢٠٠٥)**جرائم الحاسوب وابعادها الدولية**، دار الثقافة، عمان، الأردن.

- عبد السلام،خالد(٢٠١٤) **عوامل الانحراف الاجتماعي لدى الشباب الجزائري و استراتيجيات التكفل و العلاج**، مجلة دراسات نفسية وتربوية، (ع١٣)، مخبر تطوير الممارسات النفسية و التربوية، جامعة سطيف، الجزائر.

- عبد القادر القهوجي، علي.(١٩٩٩). **الحماية الجنائية لبرامج الحاسب الآلي**، الدار الجامعية للطباعة و النشر، بيروت .

- العمري عيسات(٢٠٢٢). عبد الرؤوف بوعزة، **الجريمة الالكترونية لدى المراهقين**، دوافع إلاقبال وآليات الضبط الاجتماعي، مجلة علوم الإنسان و المجتمع، جامعة بسكرة، المجلد ١١ العدد ٠١، الصفحات ١٢٥-١٤٥.