

سبل وآليات مكافحة الجرائم الالكترونية: قراءة في التجربة القطرية (2014-2005)

Ways and mechanisms of combating cybercrime: a reading in the Qatar experience

(2005-2014)

1. فازية خلفوني، fazia khelfouni، أستاذة محاضر (أ)، جامعة مولود معمري- تيزي وزو، fazia.nadia15@gmail.com

تاريخ القبول: 2021/01/13

تاريخ الاستلام: 2020/12/30

ملخص:

تعتبر الجرائم الإلكترونية من أخطر وأحدث الجرائم التي تعاني منها مؤخرا مختلف دول العالم، نتيجة الانتشار والاستخدام الواسع لتكنولوجيا الحديثة في مجال الاتصالات، لذلك سارعت الكثير منها إلى إيجاد الحلول المناسبة لمكافحتها، والتصدي لأخطارها. ومنها الدولة القطرية التي تبنت إستراتيجية رشيدة وفعالة سخرت من خلالها كافة الإمكانيات البشرية، المالية والمادية، واعتمدت في إطارها على سياسة التعاون المتبادل بينها وبين الدول الأجنبية للاستفادة من خبراتها في كيفية التصدي لهذه الظاهرة. وتمكنت بفضلها من مواجهة مختلف الجرائم الالكترونية التي تعرضت لها، كما تمكنت في فترة زمنية وجيزة من التقليل من نسبة وحدّة انتشارها. كلمات مفتاحية: الجرائم الالكترونية، مكافحة الجريمة، جرائم الانترنت، الأمن الالكتروني، التجربة القطرية.

Abstract:

Cybercrime is one of the most dangerous and recent crimes that various countries of the world have recently suffered from, as a result of the widespread and widespread use of modern technology in the field of communication, so many of them rushed to find appropriate solutions to combat them and address their dangers, including the Qatari state that adopted a rational and effective strategy mocked Through it all the human, financial and material capabilities, and within its framework it relied on the policy of mutual cooperation between them and foreign countries to benefit from their experiences in how to address this immaculate nature, and thanks to them, they were able to confront the various electronic crimes that they were exposed to, and in a short period of time they were able to reduce the proportion and severity Spread it.

Keywords: Cybercrimes; Combating crime; Internet crime; Electronic security; Qatar experience.

مقدمة:

تعتبر الجريمة الالكترونية من أخطر وأكثر أنواع الجرائم انتشارا في العالم خصوصا في الآونة الأخيرة، نتيجة التوسع الكبير في استخدام مخرجات العولمة والتقدم التكنولوجي، على رأسها وسائل الاتصالات الحديثة بمختلف أنواعها، والتي تغلغلت واستخدمت في كافة مجالات الحياة الاقتصادية، الاجتماعية، السياسية والثقافية، والتي استغلت من قبل بعض الأشخاص والمؤسسات وحتى الدول استغلالا سلبيا لارتكاب الجرائم الالكترونية بمختلف أشكالها، مستهدفين بذلك الأشخاص العاديين، و النظم السياسية في حد ذاتها، بغية الوصول إلى تحقيق منافع معينة مادية كانت أو معنوية.

عملت العديد من دول العالم في السنوات الأخيرة على استحداث الكثير من الأساليب والتقنيات التي من شأنها الحدّ أو على الأقل التقليل من تفاقم هذه الظاهرة الخطيرة في مختلف المجتمعات، ومن الدول العربية التي عرفت نجاحا في الآليات التي اعتمدها، والتي تمكنت بفضلها من مواجهة الجريمة الالكترونية والخفض من درجة انتشارها، نجد الدولة القطرية التي ركزت في إستراتيجيتها على عملية التكامل والتفاعل بين الجانبين النظري والعملي داخليا وخارجيا، من حيث تأكيدها على اعتماد خطة وطنية تتوافق وظروف بيئتها المحلية من جهة، وعلى الأخذ بمبدأ التعاون الدولي في هذه المسألة من جهة أخرى، مكرسة في ذلك مختلف الإمكانيات البشرية والمادية والمالية اللازمة لتحقيق أعلى مستوى من الفعالية في الأداء الموجه لمواجهة الجريمة الالكترونية ومنع انتشارها.

- الإشكالية: إن ارتفاع مستوى انتشار الجرائم الالكترونية مؤخرا في مختلف دول العالم، دفع بالكثير منها إلى اعتماد العديد من السياسات لمواجهة هذه الظاهرة والحد من انتشارها تجنباً للأضرار الوخيمة الناتجة عنها، ومن هنا فالإشكالية الخاصة بهذه الدراسة تتمثل في: "ما هي الوسائل الكفيلة بمواجهة الجرائم الالكترونية، و كيف تمكنت الدولة القطرية من مكافحتها، والتقليل من حدّة انتشارها؟".

ولقد تفرعت انطلاقاً من هذه الإشكالية، مجموعة من الأسئلة الفرعية التي تتفق وطبيعة الموضوع المتناول، والتي تحتاج إلى إجابات مقنعة لها، حيث تتمثل فيما يلي:

- ما هي أسباب الجريمة الالكترونية، و في ما تتمثل الأضرار الناجمة عنها؟.
- في ما تتمثل المعوقات التي تحول دون القضاء على الجرائم الالكترونية، وما هي السبل الكفيلة لمواجهتها؟.
- كيف واجهت الدولة القطرية مختلف الجرائم الالكترونية التي عرفتها؟.
- أهداف الدراسة: تهدف الدراسة إلى تحقيق مجموعة من الأهداف، تتمثل فيما يلي:
- التعرف على الأسباب المختلفة التي تدفع بالأشخاص والهيئات إلى ارتكاب الجرائم الالكترونية.
- التعرف على كافة الأضرار والنتائج السلبية على الفرد والمجتمع، والناجمة عن الجرائم الالكترونية.
- التعرف على مختلف عوامل وآليات نجاح الحكومة القطرية في مكافحة الجريمة الالكترونية والتقليل من حدّة انتشارها.

- منهجية الدراسة: تم في إطار هذه الدراسة الاعتماد على المنهج الوصفي التحليلي، وذلك من أجل وصف ظاهرة الجرائم الالكترونية في العالم وفي الدولة القطرية، إضافة إلى الاعتماد على كل من الاقتراب أُلنسيقي و اقتراب علاقة الدولة بالمجتمع اللذين تم استخدامهما للحديث عن الإستراتيجية المعتمدة من قبل الدولة القطرية لمكافحة الجريمة الالكترونية، وردود فعل المواطنين حيالها، وكذا الاقتراب السلوكي وذلك في إطار تحليل السلوكيات المختلفة الصادرة عن الهيئات والأشخاص الذين يلجئون إلى ارتكاب الجرائم الالكترونية وتحديد الأسباب التي دفعهم إلى القيام بذلك.

1- الجريمة الالكترونية بين أسباب افتعالها والمخاطر الناجمة عنها:

تتعدد الأسباب التي تدفع بالأشخاص والهيئات إلى ارتكاب الجرائم الالكترونية، غير أن مخاطرها لا تقع فقط على الضحية بل تتعداها لتلحق حتى بالجاني.

1-1- أسباب الجرائم الالكترونية:

تعتبر الجرائم الالكترونية من أحدث وأخطر الجرائم المرتكبة في الوقت الحالي، نظرا لارتباطها بالتقدم التكنولوجي السريع الذي مس وسائل الاتصالات الحديثة، والتي أصبحت تمثل فضاء مناسباً لممارسة مختلف أنواع الجرائم الالكترونية التي تترجم في "تلك السلوكيات غير المشروعة أو غير الأخلاقية أو غير المصرح بها، والتي تتعلق بالمعالجة الآلية للبيانات أو نقلها"¹، ومن بين الأسباب التي تدفع بالمجرمين إلى ارتكاب الجرائم الالكترونية، نجد ما يلي:

- الأسباب النفسية: لقد ساعد التطور التكنولوجي السريع في مجال تقنيات الاتصالات بعض الأشخاص إلى التوجه نحو ارتكاب الجرائم الالكترونية بمختلف أنواعها، خصوصا مع انتشارها الواسع في مختلف دول العالم المتقدمة منها والسائرة في طريق النمو، إلى جانب أثمانها المعقولة التي سمحت لأغلب سكان العالم بامتلاكهم لجهاز متطور، بعدما كان يوجد 20 حاسوباً فقط على المستوى العالمي في سنة 1983 من جهة²، أو بسبب معاناتهم من بعض المشاكل والضغوطات النفسية التي تدفعهم إلى إفراغ طاقاتهم السلبية في سلوكيات عنيفة تترجم في عمليات التهديد، الابتزاز، التزوير والتشهير بالأشخاص، والسرقه وإتلاف البيانات من خلال الدخول غير القانوني لنظم المعلومات والحسابات الشخصية للأفراد، وذلك عن طريق الاستيلاء على المعلومات بغية إتلافها أو تعطيلها أو الحصول على أرباح معينة من جهة أخرى³، أو بسبب الفضول والرغبة في اكتشاف كل جديد له علاقة بهذه التقنيات بغية التغلغل فيلا خباياها وكشف أسرارها التحكم فيها، حتى وإن لم تكن لديهم أي نية في ارتكاب الجرائم وإلحاق الضرر بالأشخاص أو المؤسسات، وبغض النظر عن المستوى المعيشي أو الاجتماعي الذي يتميزون به، إذ يمكن أن يكون الشخص متكيفا اجتماعيا وقادرا ماديا، باعثة من ارتكاب الجريمة الرغبة في قهر النظام، أكثر من الرغبة في الحصول على الربح أو النفع المادي⁴.

- الأسباب الاقتصادية والاجتماعية: تمثل سوء الظروف الاقتصادية والاجتماعية للفرد أو المجتمع، أحد الأسباب الرئيسية التي تؤدي إلى ارتكاب الجرائم الالكترونية، وذلك في سبيل الحصول على بعض المزايا المادية والمالية، حيث يتم في إطار ذلك العمل على إتلاف أنظمة المعلومات لحسابات شخصية أو لمؤسسات مالية بغية نهب وتحويل مبالغ معينة إلى حساباتهم الشخصية، ففي سنة 2003 مثلا تم سرقة أرقام 8 ملايين بطاقة ائتمان من شركة تجارية في الولايات المتحدة الأمريكية، إلى جانب ما كشفتته شركة (كاسبرسكي لاب) في روسيا المتخصصة في مجال الأمن الالكتروني، بتعرض النظام المصرفي اللبناني مثلا لأحد الفيروسات الالكترونية التي طالت حسابات الآلاف من الزبائن⁵، والتي تعتبر جرائم سهلة من ناحية التنفيذ وصعبة في ناحية اكتشاف مرتكبيها، لذلك يميل الكثير من الأشخاص إلى إلحاق الضرر بالآخرين الكترونيا، حيث يحول ذلك دون تعرضهم لأي نوع من أنواع الصدمات أو النزاعات المباشرة التي قد تؤدي بحياتهم إلى الهلاك أو بسمعتهم إلى الهاوية، وتجنهم الكثير من التكاليف المالية، المادية والبشرية التي تستخدم في ارتكاب الجرائم التقليدية، والتي تتميز في معظمها بسهولة عملية اكتشاف المسؤولين عن ارتكابها واقتفاء أثرهم.

- التنشئة الأسرية والاجتماعية السيئة: تعتبر التنشئة الأسرية والاجتماعية التي ينشأ عليها الطفل، المحدد الرئيسي للسلوكيات التي يمارسها في مراحل معينة من عمره كفترات المراهقة أو ما بعدها، فإذا كانت التربية والتنشئة سليمة كانت النتيجة ايجابية وكان سلوكه صحيحا، وعلى العكس من ذلك إذا عانى الشخص في طفولته من سوء التربية، فإن ذلك سينعكس سلبا على تصرفاته مستقبلا، كان يلجأ إلى ارتكاب العنف بمختلف أنواعه ومنها الجرائم الالكترونية التي تعتبر بالنسبة له متنفسا يستطيع من خلالها التعبير عن النقص والحرمان الذي عاشه في صغره، لاسيما وأنها جرائم بسيطة من حيث الافتعال نظرا للانتشار الواسع لتكنولوجيا الاتصالات الحديثة، حيث أصبحت في متناول الجميع

وشملت حتى الأطفال الذين يتأثرون بها بدرجة كبيرة جدا، لذلك فالسلوكيات العنيفة التي يقوم بها في فترات معينة تفترض تحليل العلاقات الاجتماعية التي كان هذا الشخص طرفا فيها⁶، والتي كان لابد للعائلة أن تتفطن لها وتحول دون إقحامه فيها، حتى لا تكون مستقبلا سببا في توجيهه نحو ممارسة السلوكيات غير القانونية التي تضره هو شخصا وتضر من حوله أيضا في مختلف الجوانب المادية، المالية والمعنوية.

- الأسباب أو الدوافع السياسية: تمثل الظروف السياسية للبلاد أحد الأسباب التي تدفع بالأفراد والمؤسسات إلى ارتكاب الجرائم الالكترونية، وذلك بهدف زعزعة استقرار النظام، إما بسبب سوء الأحوال الاقتصادية، أو بسبب الأطماع الخارجية في خيرات بلد معين، حيث يتم استغلال تقنيات الاتصالات الحديثة لاستخدام قدرات هجومية ودفاعية بغاية إفساد نظم المعلومات والشبكات والبنى التحتية⁷ والتي من شأنها زعزعة الاستقرار والإخلال بالسير الحسن للشؤون العامة للبلاد، أو العمل على تخريب أنظمة معلوماتها الالكترونية عبر ضخ أنواع مختلفة من الفيروسات، وفي هذا الإطار صرحت الولايات المتحدة الأمريكية في سنة 2000، عن تعرضها لعملية هجوم من طرف أحد الفلبينيين مسّت أجهزة الحواسيب الآلية، وذلك من خلال نشر فيروس خطير يعمل على إتلاف المعلومات في هذه الأجهزة سمي بـ فيروس (love bug)⁸، أي أن هذه الجرائم أصبحت تمثل شكلا جديدا من أشكال الاستعمار غير المباشر، والذي لا يتطلب موارد بشرية ومالية ومادية كبيرة مقارنة بالحروب التقليدية المباشرة، وبالتالي فالجريمة الالكترونية لا تمثل مشكلا داخليا بل هي عابرة للحدود، وبالمقابل تتطلب حلولاً دولية، تجعل كل دولة تلتزم بحماية مجتمعاتها ضدّ جرائم التقنية⁹. أدخل هنا محتوى العنوان الفرعي الأول، أدخل هنا محتوى العنوان الفرعي الأول، أدخل هنا محتوى العنوان الفرعي الأول، أدخل هنا محتوى العنوان الفرعي الأول، أدخل هنا محتوى العنوان الفرعي الأول.

2-1- الأضرار الناجمة عن الجرائم الإلكترونية:

إنّ الأضرار التي تنتج عن الجرائم الالكترونية، تشمل جميع المجالات دون أي استثناء، ويمكن عرض ذلك فيما يلي:

- الخسائر المالية للمؤسسات والشركات: لقد كبدت الجرائم الالكترونية التي مسّت الأنظمة والمواقع الالكترونية للمؤسسات خسائر مالية كبيرة جراء السطو على حساباتها وحسابات المتعاملين معها، إذ يتم سنويا تسجيل خسارة ما يقارب 160 مليار دولار في قطاع الأعمال الذي يتعرض لانتهاك وسرقة حقوق الملكية الفكرية¹⁰، رغم حاجة المؤسسات إلى استخدام الأموال التي تم نهبها في الرفع من مستوى إنتاجيتها، والتحسين في نوعية خدماتها، وقد أفادت دراسة قامت بها شركة (SYMANTEC) حول معدل الخسائر التي كبدتها بسبب الجرائم الالكترونية التي مسّت الأنظمة والبرامج المعلوماتية لعام 2011، ما يعادل 114 مليار دولار مقابل 431 مليون ضحية¹¹، وهي خسائر جدّ مرتفعة مقارنة بقيمة الأموال التي صرفت من أجل إنتاج هذه البرامج وتشغيلها، خاصة وأن هذه الجرائم لا تatal الأموال الخاصة بالشركة فقط، بل تتعدى ذلك لسرقة أموال المتعاملين معها، ففي عام 2010 مثلا صرحت العديد من الشركات الكبرى المتخصصة في مجال صناعة أنظمة البرمجيات الالكترونية تعرضها للعديد من الهجمات الالكترونية، كالهجمة التي تعرضت لها إحدى الشركات الكبرى لمحركات البحث الالكتروني، والتي تسببت في الدخول إلى الحسابات البريدية للعمال، وكشف الأرقام السرية غير المؤمنة كفاية¹².

- الخسائر الاقتصادية للدولة: تعد الجرائم الالكترونية من أخطر الجرائم التي تسبب خسائر اقتصادية كبيرة للدول، تؤثر سلبا على تطورها واستقرارها الاجتماعي، حيث يعمل الكثير من المجرمين على سرقة الأموال وتحويلها من حسابات معينة إلى أخرى دون أي حدود أو موانع لذلك، نظرا لسهولة اقتحام أنظمة الأجهزة الالكترونية للدول، التي تكون غير مؤمنة بالقدر الكافي الذي يمكنها من التصدي للهجمات الالكترونية الهادفة إلى سرقة الأموال، حيث أفادت دراسة نشرت

بتاريخ 9 يوليو عام 2014، أن جرائم الانترنت كبدت الاقتصاد العالمي خسائر وخيمة، تعادل سنويا ما قيمته 445 مليار دولار¹³، وهي خسائر جد ضخمة، كان العالم في غنى عنها قبل الولوج إلى عالم تكنولوجيا الاتصالات الحديثة رغم أهميتها في تسهيل وتفعيل الحياة المهنية للدول، وهي مبالغ مالية كان ينبغي استثمارها في تحريك عجلة التنمية. وإحداث التطورات والتحسينات في القطاعات الاقتصادية والاجتماعية والسياسية للدول، وقد أنفقت بريطانيا مثلا في عام 2012، ما يعادل 100 مليار دولار على مشروع الأمن الالكتروني بعدما صرفت 63 مليار دولار في عام 2011¹⁴، وهذا بعد إدراكها لحجم الأضرار الاقتصادية التي تكبدها اقتصادها بسبب الجرائم الالكترونية، والتي اعتبرت أن أهم خطوة للحلول دون تعرضها لمثل هذه الهجمات هو إنشاء ترسان أمنية قوية مضادة لكل محاولة لاختراق أنظمة حواسيبها ونهب أموالها.

- الإخلال بالحياة الشخصية للفرد: تؤدي الجرائم الالكترونية في أغلب الأحيان إلى الإضرار بالحياة النفسية والمادية للأفراد، نظرا لسهولة اقتحام حساباتهم التي تكون في أكثرها غير مزودة بأنظمة أمن وحماية كافية تحول دون الوصول إليها والتخريب فيها، حيث يستخدم مرتكبها كل أنواع الجرائم المخلة بالحياة كاستعمال الألفاظ البذيئة، والسلوكيات اللااخلاقية كالسب والشتم والتحرش الجنسي الذي يعتبر من أكثر الجرائم انتشارا، خصوصا في السنوات الأخيرة والذي مسّ حتى الأطفال بغض النظر عن نوع جنسهم، وتعتبر مواقع التواصل الاجتماعي في مقدمتها الفيسبوك، من أكثر المواقع التي يستغلها المجرمون لارتكاب الجرائم الالكترونية، نظرا لسهولة استخدامها من جهة، وسهولة إخفاء هوياتهم الحقيقية من جهة أخرى، ومن أكثر العمليات الإجرامية الممارسة من خلالها نجد عمليات التهديد والتشهير، وقد أفادت دراسة قام بها موقع "أرقام ديجيتال"، في هذا الإطار أن عدد ضحايا الجرائم الالكترونية التي حدثت بسبب اختراق حسابات الفيسبوك قد وصل إلى 105 ضحية في اليوم¹⁵، وهي أرقام جد مخيفة تعكس مدى خطورة هذه المواقع على سلامة مستعملها، لاسيما منهم فئتي الشباب والأطفال الذين يكونون أكثر عرضة لهذه الجرائم، نظرا لنقص أو غياب مستوى الوعي لديهم بمدى خطورة السلوكيات العنيفة التي يقومون بها، وببشاعة الأضرار التي يلحقونها بأنفسهم وبغيرهم.

- الإخلال بالمنظومة الأخلاقية والقيمية للمجتمع: إنّ التأثير السلبي للجرائم الالكترونية لا يتوقف عند الجوانب المادية والمالية للمجتمع، إنما يتعداه ليشمل حتى القيم الأخلاقية للأفراد ومن ثم للمجتمع، إذ أن أغلب المجرمين يميلون إلى إفساد أخلاق الآخرين وإلحاق الأضرار النفسية أو المادية المخلة بالحياة، خصوصا ما تعلق بفئة النساء اللواتي يتعرضن لانتهاك حرمتهم وخصوصيتهم عبر الحسابات الشخصية لهن، وقد أفادت في هذا الإطار دراسة قام بها الاتحاد الأوروبي عام 2014، أن أربعة بالمائة من النساء اللواتي يتراوح عمرهن بين 18 و 29 سنة، تم ملاحقتهن من خلال الفضاء السيبراني (Cyberstalking)¹⁶، أو أنهم يعملون على تعليم ضحاياهم لطرق ممارسة الجرائم وإشراكهم في تنفيذها، كدفعهم إلى تعاطي المخدرات بمختلف أنواعها لاسيما منها المخدرات الرقمية، وقد نوهت الهيئة الدولية لمراقبة المخدرات إلى ذلك من خلال تقرير لها صدر عام 2000، إلى أن تكنولوجيا الاتصالات الحديثة ستصبح سببا في اللجوء إلى ممارسة الأنشطة غير المشروعة والتي لها علاقة بالمخدرات¹⁷.

2- تحديات مكافحة الجرائم الالكترونية، وسبل تجاوزها:

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

2-1- تحديات ومعوقات مجابهة الجرائم الالكترونية: من بين أكثر التحديات التي تواجه الدول في محاولتها التقليل من الجرائم الالكترونية ومكافحتها ما يلي:

- صعوبة اقتفاء أثر الجريمة الالكترونية: يعد البحث عن الجريمة الالكترونية أو الفاعل الذي ارتكبها، من اكبر المعوقات التي تحول أو تصعب من مهمة الأفراد أو الهيئات المعنية في محاولة اكتشافها وفرض العقوبات اللازمة على مرتكبيها، وذلك بسبب سهولة إزالة ومسح أي دليل حولها في وقت زمني قصير، إلى جانب صعوبة التعرف على المجرم وتحديد هويته الحقيقية نظرا لاعتماده على أسماء وصور ومستعارة، إضافة إلى مشكل عدم إمكانية تتبعه والاحتفاظ الفني بآثار الجريمة إن وجدت، فليست هناك أموال أو مجوهرات مفقودة، إنما هي أرقام تتغير في السجلات¹⁸ حيث لا يتطلب الأمر خبرة كبيرة في مجال الأجهزة الالكترونية لكشف الجريمة أو فاعلها، إذ يسهل كثيرا على أي شخص لديه خبرة قصيرة أو اطلاع كافي على كيفية استخدام تقنيات تكنولوجيا الاتصالات الحديثة، أن يخفي أي أثر للجريمة المرتكبة.
- عدم الإبلاغ عن الجريمة الالكترونية: بمعنى عزوف بعض الأفراد والمؤسسات عن عدم رفع الشكاوى للسلطات المعنية للتبليغ عن الأضرار المادية والمعنوية التي لحقت بهم، من طرف المجرمين الذين الحقوا بهم الأذى عن طريق الأجهزة الالكترونية، إما خوفا من ردود فعل مرتكبي الجريمة، أو خوفا على سمعتهم ومكانتهم في المجتمع لاسيما إن كانت الضحية امرأة. فهي تصدم بواقع بعض المجتمعات التي تضعها على الهامش وتجعل سمعتها فوق أي اعتبار، حتى وإن تعرضت لأبشع صور التعنيف المادي واللامادي ومنها الجريمة الالكترونية.
- استغراق وقت طويل في الإبلاغ عن الجريمة: تعتبر السرعة التي تتميز بها تكنولوجيا الاتصالات الحديثة في نقل وتبادل الأفكار والمعلومات، إحدى أهم الخصائص التي يستغلها المجرمين في ارتكاب الجرائم الالكترونية، وإلحاق الضرر المعنوي والمادي بالآخرين، حيث لا يتطلب افتعالها أو محو آثارها وقتا طويلا، لاسيما وإن تزامن ذلك مع تردد الضحية أو عدم إبلاغها عن الجريمة في حينها، حيث تعطي بذلك الفرصة و الوقت الكافي للمجرمين لمسح أي دليل تركوه حول ما قاموا به من أفعال أو حول ما صدر عنهم من أقوال ضد الضحية.
- حجم التكلفة اللازمة لكشف الجريمة: يتطلب الكشف عن الجرائم الالكترونية ومرتكبيها، إمكانيات ضخمة من الموارد البشرية المؤهلة، رؤوس الأموال والأجهزة المتطورة، خصوصا في دول العالم الثالث التي تعاني من نقص أو عدم توفرها على هذه الموارد، لاسيما ما تعلق بالأجهزة الحديثة التي تتغير وتتطور بسرعة كبيرة يصعب على هذه الدول اقتناؤها من ناحية، والتحكم فيها وفي طرق استخدامها، أو إصلاحها في حالة تعطلها، الأمر الذي يحول دون وصولها إلى كشف الجرائم الالكترونية كلها، والذي يعطي الفرصة للمجرمين من أجل المضي في سلوكياتهم اللا أخلاقية وإلحاق الأذى بالآخرين عبر هذه التقنيات.
- ضعف التعاون والتنسيق الدولي: رغم كثرة الاتفاقيات والمعاهدات الدولية التي تم إبرامها بخصوص مكافحة الجرائم الالكترونية، إلا أن مسألة التعاون الدولي ضعيف من ناحية التطبيق العملي، إذ أن أغلب الاتفاقيات التي يتم إبرامها على المستوى العالمي، تنفرد كل دولة بتطبيق قراراتها وفقا لخصوصية نظامها وبيئتها المحلية، ما يجعلها تصطدم في الكثير من الأحيان مع ما تم الاتفاق عليه في إطار تلك الاتفاقيات، خصوصا ما تعلق بتسليم المجرمين ومعاقبتهم، إذ لا يمكن لأي دولة أن تقوم بعمليات التفتيش حول الجريمة الالكترونية المرتكبة في بلدان أخرى، دون الحصول على موافقة سلطاتها الوطنية، كما أن إجراءات تسليم المجرمين معقدة وتستلزم وقتا طويلا لإتمامها، وذلك احتراماً لمبدأ السيادة الوطنية للدولة¹⁹.
- 2-2- آليات وسبل مواجهة الجرائم الالكترونية: من بين الأساليب والآليات التي يمكن الاعتماد عليها لمواجهة الجرائم الالكترونية، نجد ما يلي:

- المبادرات التشريعية: سارعت مختلف دول العالم بمجرد بروز، ومن ثم انتشار ظاهرة الجرائم الالكترونية إلى سنّ العديد من القوانين الهادفة إلى منع انتشارها والتقليل من عددها، حيث قامت فرنسا مثلاً في عام 1988 بإصدار القانون

الخاص ببعض الجرائم المعلوماتية كإتلاف البيانات، أو الدخول بطرق غير قانونية إلى أنظمة المعالجة الآلية²⁰، كما قامت السعودية في عام 2017 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 به²¹، إلى جانب إنشاء مصر للجمعية المصرية لمكافحة جرائم المعلوماتية والانترنت المصرية في عام 2004، والتي تعمل على توعية الجمهور بمخاطر هذه الجرائم، ووضع إحصائيات حول مدى انتشارها، إضافة إلى المساهمة في تقديم خدمات البلاغ الرقمي²².

- **الاتفاقيات والمعاهدات الدولية والإقليمية:** عملت الكثير من الدول والمنظمات على عقد العديد من الاتفاقيات التي تساهم في مكافحة الجرائم الالكترونية، وقد كانت الأمم المتحدة السباقة إلى ذلك، حيث أصدرت في سنة 1999، القرار رقم 99-23 المتعلق بمنع الجريمة والعدالة الجنائية²³ ونفس المبادرة قامت بها أوروبا من خلال ما يعرف باتفاقية بودابست، التي تم عقدها في 23 نوفمبر 2001 بالعاصمة المجرية بودابست، وتعتبر من أهم الاتفاقيات الدولية التي أبرمت بخصوص الجرائم السيبرانية من خلال التنسيق بين مختلف التشريعات الوطنية، وذلك بالتركيز على القواعد الموضوعية للجرائم، إجراءات التحقيق وآليات التعاون الدولي²⁴، كما سارعت أيضا الدول العربية إلى إبرام اتفاقية العربية لمكافحة جرائم تقنية المعلومات في 21 ديسمبر 2010، 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 لا بد وأن تكون متوافقة مع القوانين الداخلية الخاصة بها، والتي تتعلق أساسا بالأبحاث الجنائية وإجراءات التفتيش على المعلومات المخزنة، والتجميع الفوري لها أو اعتراض محتوياتها²⁵.

- **الوعي ونشر تدابير الوقاية:** يعتبر العمل على نشر ثقافة الوعي والوقاية من الجرائم الالكترونية من أهم الإجراءات المساعدة في التقليل من حدة انتشارها، حيث تسمح حملات التوعية على المستوى العالمي من التعريف بهذه الجرائم وبالمخاطر التي تنجم عنها، وبضرورة عدم افتعالها عبر مختلف وسائل الإعلام التقليدية منها والحديثة، وقد نوهت الولايات المتحدة الأمريكية في هذا السياق إلى أن أهمية تثقيف الجمهور وتوعيته، يعد إستراتيجية أساسية في الوقاية من أي نوع من أنواع الجريمة²⁶، فكلما أدرك الفرد خطورة الأضرار النفسية والمادية التي يتعرض لها الضحية ومرتكب الجريمة، كلما ابتعد عن هذا السلوك، لذلك اعتمدت الكثير من الدول عبر مختلف ربوع العالم إجراءات التوعية من أجل التقليل من عدد الجرائم المرتكبة، كالحملة التي قام بها مشغل الاتصالات في أوروبا الشرقية (KYIVSTAR) عام 2020 تحت شعار: "أخبر طفلك عن أمان الانترنت"²⁷، كسبيل لتوعية الأطفال بمخاطر تكنولوجيا الاتصالات الحديثة من طرف أوليائهم، والعمل على إبعادهم قدر المستطاع عن استخدامها في غير ما يفيدهم.

- **التنشئة الأسرية والاجتماعية:** تلعب الأسرة ومختلف التنظيمات التي تنطوي في إطار المجتمع المدني دورا هاما في مكافحة الجرائم الالكترونية، وذلك عبر التنويه المستمر بخطورة هذه الجرائم التي تؤدي بمرتكبيها وبالمجتمع ككل إلى التهلكة، لاسيما وأن اغلب مفتعلها هم من فئة الشباب الذين يعيشون فترات المراهقة التي تؤثر على الكثيرين منهم بطريقة سلبية، خصوصا إن كانوا يعانون من بعض المشاكل الاجتماعية أو الاقتصادية التي تدفعهم إلى المكوث ساعات طويلة أمام شاشات الحواسيب أو الهواتف النقالة، وهو الشيء الذي يمثل اكبر مخاوف الأولياء حسب دراسة استطلاعية تم إجراؤها في الولايات المتحدة الأمريكية بخصوص الاستخدام الكبير للأطفال والشباب لتقنيات تكنولوجيا الاتصالات الحديثة التي تؤثر سلبا على خبراتهم الاجتماعية وصدقاتهم²⁸، والتي تدفع بهم شيئا فشيئا إلى ممارسة السلوكيات العنيفة المترجمة في الجرائم الالكترونية نظرا لسهولة افتعالها وصعوبة كشف مرتكبها، لذلك ينبغي التعامل

معهم بنوع من الحكمة والذكاء للوصول إلى منعهم من الولوج إلى المواقع التعليمية لمثل هذه الجرائم، والعمل على تحويل هذه المواقع من مصادر لممارسة العنف إلى ميدان تربوي وتعليمي، حيث يمكن أن يكون التطور التقني في مجال الاتصالات أحد العوامل الرئيسية التي تستثمر في الميدان التربوي، وهو الشيء الذي لفت انتباه التربويين وجذبهم إليه²⁹.

- دور الجامعة: تعتبر الجامعات ومعاهد التعليم العالي من أكثر وأهم الهيئات المساهمة في منع الجريمة الالكترونية والتقليل من انتشارها، خصوصا تلك الجامعات التي تتوفر على التخصصات المعنية بمجال التقنيات والتكنولوجيات الحديثة، حيث يقوم الأساتذة في إطار ذلك بتلقين الطلبة الدروس التي تساهم في تعريفهم بالتقنيات المستخدمة في مجال الاتصالات الحديثة، وتعليمهم كيفية استخدامها وكيفية حماية الحسابات والأنظمة الالكترونية، إلى جانب تقديم مختلف المعلومات والمعطيات حول كيفية التعامل مع مختلف الخدمات (المواقع الالكترونية)، وتقديم المساعدات الفنية للشركات الصغيرة والمتوسطة للطرق التي يجب اعتمادها من أجل تحليل محتوى البرمجيات من جهة، وتقديم برامج المساعدة القانونية في مجال الجريمة الالكترونية لوكالات الأمن الوطني والعدالة الجنائية من جهة أخرى، إلى جانب دورها المهم في إعطاء المقترحات حول صياغة وتعديل التشريعات³⁰، وذلك بالتركيز على ضرورة تقديم تقارير دورية ومستمرة بشأن آخر التطورات والمستجدات في مجال تطور تقنيات تكنولوجيا الاتصالات الحديثة.

- مسؤولي ومقدمي خدمات الانترنت: يعتبر الأشخاص أو المؤسسات التي تدير المواقع الالكترونية، ويقومون من خلالها بتقديم مختلف الخدمات إلى الزبائن، من بين العناصر الأساسية المساهمة في التقليل أو الحد من انتشار الجرائم الالكترونية، وذلك من خلال ما يقومون به من عمليات الإبلاغ وتعميد طرق ووسائل الولوج إلى المواقع المحظورة قانونيا، والتي تمنح الفرصة لكشف المتلاعبين بهذه المواقع، كالإجراء الذي قامت به إحدى شركات مواقع التواصل الاجتماعي التي أبلغت عن خمسة من أكثر وأخطر مزودي أدوات إرسال الرسائل الالكترونية الطفيلية الشرسة³¹ وهو إجراء من شأنه الحيلولة دون المقدرة على تخطي أنظمة الأمان المعتمدة، وبالتالي التقليل من عدد الجرائم الالكترونية المرتكبة.

- دور الشرطة القضائية: تلعب الشرطة القضائية دورا هاما جدا في مكافحة الجرائم الالكترونية والحد من انتشارها، باعتبارها أحد المنفذين الرئيسيين لبرامج الأمن الوطني الالكتروني، من خلال متابعة ومعاينة مرتكبي الجرائم، عبر ما يصلها من شكاوى وبلاغات من الضحايا، فقد قامت إدارة المباحث الالكترونية في القيادة العامة لشرطة دبي مثلا في ظرف ثلاث سنوات ثلاث متتالية (2016.2017.2018) بمعالجة 2606 قضية متعلقة بالجرائم التي تضمنت عمليات الاحتيال والابتزاز، إضافة إلى قرصنة واختراق بعض الشركات³²، غير أن الشرطة القضائية لا يمكنها الوصول إلى كشف الجرائم الالكترونية والعمل على معالجتها دون وجود مساعدة أفراد المجتمع لها، من خلال العمل المستمر على تزويدها بمختلف المعلومات حول الجريمة، والإبلاغ عنها في حينها، الشيء الذي سيساهم في بناء إستراتيجية واحدة لمكافحة هذه الجرائم والحد من انتشارها.

3- 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.

3-1- أساليب مواجهة الجريمة الالكترونية في قطر:

لقد اعتمدت الدولة القطرية على مجموعة من الأساليب والسياسات الداخلية والخارجية بهدف مكافحة

الجريمة الالكترونية والتقليل من حدّة انتشارها، ومن بين أهم هذه الآليات نجد ما يلي:

- إصدار قانون مكافحة الجرائم الالكترونية 2014: قامت الحكومة القطرية الحكومة القطرية بهدف التخفيف من

حدّة وعدد الجرائم الالكترونية المرتكبة ضدّ المواطنين والسلطات، بالعمل على إصدار قانون في عام 2014، يهدف إلى

تجسيد هذه الغاية على أرض الواقع، من خلال التركيز على تحديد مختلف الحالات التي تصنف ضمن الجرائم الالكترونية وتبعات ذلك من ناحية العقوبات التي ستفرض على كل مرتكب لها، حيث ينص هذا القانون على متابعة الأفراد الذين ينشرون معلومات وأخبار غير صحيحة بقصد تعريض النظام العام للخطر من جهة، وكذا كافة المعلومات التي تقوض المبادئ أو القيم الاجتماعية من جهة أخرى³³، حيث عمل هذا القانون على تحديد مختلف أنواع الجرائم الالكترونية التي يمكن ارتكابها، وكذا العقوبات المختلفة التي ستسلط على مرتكبها حسب نوعية وجسامة الجرم المرتكب، كجريمة التعدي على أنظمة وبرامج وشبكات المعلومات والمواقع الالكترونية، والتي حددت عقوبتها ب ثلاث سنوات حبس وغرامة مالية قدرها 500000 ألف ريال، وذلك في حالة الدخول إلى الأجهزة الخاصة بالدولة، وتكون هذه العقوبة مضاعفة في حال الحصول على المعلومات والبيانات حولها، وقد حددت العقوبة المتعلقة بجريمة التزوير والاحتيال الالكتروني ب عشر سنوات حبس و 2000000 ألف ريال، في حال التزوير المتعلق بمحرر الكتروني رسمي واستعماله عن قصد، إلى جانب الحكم ب ثلاث سنوات حبس و غرامة مالية قدرها 100000 ألف ريال في حالة تزوير محرر الكتروني غير رسمي والقيام باستعماله.

وقد أشار القانون أيضا إلى الجرائم المتعلقة بالتعدي على حقوق الملكية كحقوق المؤلف والحقوق المجاورة، والتي تمثلت عقوبتها بثلاث سنوات حبس وغرامة مالية تقدر ب 500 ألف ريال، في حين تمثلت العقوبة الخاصة على بمرتكي الجرائم الالكترونية المتعلقة ببطاقة التعامل الالكتروني الفردية ب ثلاث سنوات حبس وغرامة مالية تقدر ب 200 ألف ريال، أو بإحدى هذه العقوبات في حالة التسهيل أو الحصول على بيانات وأرقام البطاقة أو العمل على تزويرها. - التدريب الوظيفي للتعامل مع الهجمات الالكترونية: أدركت الدولة القطرية جليا أن أهم آلية لمكافحة الجريمة الالكترونية، هي تدريب الموظفين في مختلف المجالات لكيفية التعامل معها من خلال التدريب على توفير الحماية لمختلف الأنظمة من جهة، والعمل على كشف الجرائم قبل حدوثها، والعمل إحباطها بمجرد اكتشافها من جهة أخرى، وبذلك عملت على تنظيم تمارين خاصة بحماية البنى التحتية، شملت أكثر من 20 مؤسسة حكومية وخاصة، كان الهدف منها هو رفع المهارات الخاصة بموظفي الحواسيب الآلية للتعامل مع الهجمات الالكترونية، وذلك من خلال مواجهة هجمات حقيقية والعمل على إيجاد الحل المناسب لها، وقد شملت هذه التمارين القطاعات الحيوية للدولة كالطاقة، القطاع المصرفي والمواصلات، وقد شارك في إطار هذه المبادرة أزيد من 120 موظفا مختصا في مجال الأمن السيبراني والحاسب الآلي، وبفضل هذه الإستراتيجية تمكنت الدولة القطرية من تخفيف عدد الجرائم الالكترونية إلى حد كبير جدا، فقد أصبحت ضمن قائمة الدول البيضاء من ناحية البريد غير المرغوب به في عام 2013، بعدما كانت تصنف ضمن القائمة السوداء في عام 2010³⁴.

- إنشاء مراكز مكافحة الجريمة الالكترونية: عملت قطر في إطار مكافحة الجريمة الالكترونية على إنشاء مراكز تعنى بتحقيق هذه الغاية على أرض الواقع، كإنشاء (المركز الوطني لأمن المعلومات) بالتعاون مع معهد هندسة البرمجيات في جامعة كار جيني ميلان الأمريكية في ديسمبر من عام 2005، بهدف مواجهة تهديدات الجريمة الالكترونية وتحديات الأمن السيبراني من جهة، واعتماده كوسيلة لبناء مقدرات التعامل مع معلومات البنى التحتية الحرجة في قطر من جهة أخرى، وقد أصبح هذا المركز مسئولاً عن أمن واحتياجات حماية معلومات الأمة القطرية، وتأمين المجتمع المحلي وتوجيهه نحو إيجابيات التقنيات وتقليل المخاطر، وتقديم المعلومات القيمة بشأن حماية الأمن السيبراني.

كما تم أيضا تأسيس مركز آخر من طرف وزارة الداخلية، زود بأحدث التقنيات والأجهزة لكشف الجريمة الالكترونية، وقد ساعد في كشف الكثير من الجرائم المتعلقة بالتشهير والسب والتجسس الصناعي والقرصنة الالكترونية. إلى جانب _ تأسيس الفريق القطري للاستجابة لطوارئ الحاسب عام 2005 من طرف وزارة الاتصالات وتكنولوجيا المعلومات، وذلك بالتعاون مع جامعة (ميلون كارن يجي)، حيث يعرف هذا الفريق باسم "كيوسرت"، وهو منظمة غير ربحية، يعمل على الإلمام باحتياجات الدولة القطرية في مجال امن المعلومات، وعلى نشر الثقة الرقمية بين مختلف شرائح المجتمع³⁵.

- العمل على حماية المؤسسات المالية: تعتبر الجرائم الالكترونية المالية من أكثر الجرائم التي تعرضت لها المؤسسات المالية والنقدية في الدولة القطرية سواء كان ذلك من ناحية الخطورة أو العدد، لذلك أولت الحكومة لهذا المجال أهمية كبيرة من اجل حمايتها، والحد من انتشارها وتغلغلها داخل أقسامها المختلفة وإلحاق الضرر بها وبالمعاملين معها، خاصة وان الدولة القطرية معروفة بالانتشار الواسع لاستخدام التقنيات الحديثة لتكنولوجيا الاتصالات، حيث يمتلك أكثر من 96 بالمائة من سكان قطر جهاز كمبيوتر محمول، و 71 بالمائة يمتلكون الهواتف الذكية، ووفقا لذلك فإن نسبة الأفراد الذين يستخدمون اشتراك الانترنت في عام 2008 مثلا قد وصل إلى 38 بالمائة ليرتفع ارتفاعا ملحوظا عام 2013 ليصل إلى 85 بالمائة، وهو ما يعكس العدد الكبير من الجرائم الالكترونية المرتكبة في قطر، خصوصا المالية منها والتي بلغت نسبتها 9.64 بالمائة من إجمالي سكان قطر³⁶، كما طالت هذه الجرائم أيضا الدولة، كالهجمة الالكترونية التي حدثت خلال عامي 2012 و2013، والتي كان الهدف منها ضرب الكيان القطري ودول الخليج العربي ككل.

إن الانتشار الواسع للجرائم الالكترونية المالية، استدعى ضرورة العمل على تأمين وحماية المؤسسات المالية والنقدية المختلفة، وفي هذا الإطار قام مصرف قطر مثلا، في عام 2010 بوضع مجموعة من العمليات والإجراءات الوقائية التي من شأنها حماية المنظومة المصرفية، والتي يجب على المؤسسات المالية الالتزام بها والعمل على تطبيقها بدقة بغية كشف ومنع مختلف الأنشطة الممكن حدوثها والمتعلقة بعمليات تحويل الأموال وتمويل الإرهاب، وذلك من خلال منع سوء استخدام التطورات التكنولوجية في إطار غسيل الأموال، والعمل على تصنيف العملاء الذين يتم التعامل معهم³⁷.

- التركيز على مبدأ التعاون: تعد مكافحة الجرائم الالكترونية عملية جدّ معقدة نظرا لصعوبة كشف هوية مرتكبيها في الوقت المناسب، خاصة وأنها لا تحدد بالمدى الزمني والجغرافي للدولة المعنية، لذلك لا يمكن لأي دولة الانفراد والعمل بصفة مستقلة عن غيرها من الدول الأخرى على المستوى العالمي، في محاولة مكافحة الجريمة الالكترونية ومنع انتشارها، وقد أوضح أحد الخبراء المتخصصين في مكتب الأمم المتحدة لمكافحة الجرائم في هذا الشأن، أن الجرائم الالكترونية هي جريمة القرون اللاحقة³⁸ إذ يصعب كثيرا التحكم فيها أمام التطورات التكنولوجية التي يعرفها مجال الاتصالات التفاعلية اليوم، خاصة وان الدولة القطرية تعتبر من أكثر الدول التي تعرف انتشارا واسعا في استخدام الانترنت، حيث احتلت المرتبة 26 عالميا من حيث مؤشر القوة التكنولوجية، وذلك بنسبة مائة بالمائة من حيث استخدام المواطنين له³⁹، وهذا الأمر يعكس بصورة جلية النسبة المرتفعة جدا في امتلاك المجتمع القطري للوسائل والأجهزة الالكترونية الحديثة التي تسهل عمليات ارتكاب الجرائم الالكترونية بمختلف أشكالها، وهو ما يستدعي تضافر جهود كل الدول ماديا ومعنويا لمواجهة هذه الظاهرة وتلافي أضرارها، وفي هذا الإطار تم التعاون مع قاعدة الأنتربول الدولية للجرائم الالكترونية المرتكبة ضد الأطفال، وهي التجربة الأولى من نوعها عربيا، حيث تم تشكيل فريق وطني 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 140 دولة مشتركة⁴⁰.

2-3- النتائج المحققة للسياسة القطرية في مواجهة الجريمة الالكترونية:

تعتبر التجربة أو السياسة التي اعتمدها الدولة القطرية في مكافحة الجريمة الالكترونية من انجح التجارب التي عرفتھا البلدان العربية، رغم أنها من أكثر البلدان عرضة للهجمات الالكترونية نتيجة الاستخدام المكثف والكبير للتكنولوجيا الحديثة، حيث وصل استخدام الانترنت بها إلى أكثر من 34,8 بالمائة في سنة 2014، لتصل بعد عامين فقط إلى ما يعادل 45 بالمائة، وتخص هذه النسب نشاطات الحياة اليومية للمواطنين كاستخدام مواقع التواصل الاجتماعي، البريد الالكتروني، والمواقع الخاصة بالدولة المتصلة بالمجالات الحيوية كالصحة، التعليم، المواصلات إلى جانب تدعيم قطاع الأعمال أيضا بالأسلوب الحديث للتجارة المتمثل في التجارة الالكترونية⁴¹، حيث لم يمنعه ذلك 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، حيث حصدت في العديد من السنوات المراتب الأولى في مجال الأمن والسلامة الالكترونية، وفق تقرير مؤتمر السلام العالمي الذي صنّفها في المرتبة الأولى خليجيا وعربيا، كما احتلت أيضا المرتبة 30 عالميا سنتي 2016 و2017 من ناحية التمتع بالأمن، وهو ما يفسر نجاح الإستراتيجية التي اعتمدها منذ سنة 2005، والتي سخرت لها مختلف الإمكانيات المادية، المالية والبشرية، والتي جعلتها مرة أخرى تفتك المركز الأول في تمتع مجتمعيها بالسلامة من الجريمة الالكترونية في عام 2015، وهو نفس المركز الذي بقيت محتفظة به أيضا في عام 2019⁴².

إن نجاح الدولة القطرية في الحصول والإبقاء على الترتيب الأول خليجيا وعالميا في مجال الأمن الالكتروني، دليل كاف على فعالية الإستراتيجية التي اعتمدها منذ سنة 2005 والتي حصدت ثمارها في السنوات اللاحقة، فقد تمكنت حسب تصريح المختصين في إدارة مكافحة الجرائم الالكترونية بوزارة الداخلية القطرية، أن جميع الجرائم الالكترونية التي وقعت باستخدام البطاقات الائتمانية قد تم ضبطها بنسبة 100/100⁴³، والتي تعد من أكثر أنواع الجرائم المرتكبة والمنتشرة في مختلف دول العالم، والتي عانت منها الحكومة القطرية التي عملت جاهدة على كشفها، وإفشالها قبل حدوثها وإلحاق الضرر بمالكها الأصليين، إلى جانب تمكّنها من إحباط العديد من جرائم القرصنة المفتعلة عبر أجهزة الحاسوب⁴⁴، كما تمكن فريق الأمن السيبراني القطري في عام 2014 من كشف ومعالجة 14 مليون سجل معلومات تعرضت للتهديد والاحتيال، وذلك بنسبة 17 بالمائة بالنسبة لقطاع التعليم، ونفس النسبة سجلت على مستوى قطاع الطاقة، والمؤسسات المالية، في حين قدرت النسبة الخاصة بالإعلام بـ 46 بالمائة، إلى جانب كشف ومعالجة 2 مليون إصابة شملت الشبكات المنزلية والشركات، إضافة إلى العمل على توجيه أزيد من 30000 تحذير بالتهديد المحتمل⁴⁵، خاصة من خلال مواقع التواصل الاجتماعي والتي تعتبر من أكثر المواقع استخداما في مجال الجريمة الالكترونية في قطر على اعتبار أنها مفتوحة للجميع، ولا تتطلب مستوى تعليمي عالي من ناحية استخدامها، كما أنها مفتوحة على جميع أنحاء العالم، حيث يتصفحها يوميا أزيد من 45 بالمائة على الأقل مرة في اليوم⁴⁶، وهو ما يعكس الكم الهائل من الجرائم الالكترونية التي عانت منها المجتمع القطري، والتي تمكنت الحكومة بفضل الإستراتيجية الرشيدة التي اعتمدها من تحقيق نتائج جد ايجابية واجهت من خلالها مختلف الجرائم الالكترونية التي كان محضرا لها، وتمكنت من إفشالها قبل حدوثها، الشيء الذي جعلها تحتل المراتب الأولى عالميا في درجة التمتع بالأمن السيبراني.

نتائج الدراسة:

لقد 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 إستراتيجيتها الوطنية التي استثمرت فيها كافة مواردها المالية والبشرية لتحقيق ذلك على أرض الواقع، من خلال تضافر كافة الجهود السياسية والمدنية لمواجهة الجريمة الالكترونية والتقليل من حدة انتشارها، تجنباً للأضرار النفسية والمادية والمالية التي يمكن أن تلحق بالفاعل والضحية على حد سواء، 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 وفعاليتها من خلال الإكثار من حملات التوعية والأساليب العقابية التي قللت كثيرا من معدل انتشار الجرائم الالكترونية في قطر، إلى جانب التركيز على تفعيل إستراتيجية التكامل الداخلي والخارجي التي اعتمدتها الدولة القطرية، والتي ساعدت كثيرا في مواجهة الجريمة الالكترونية، والتقليل من حدة انتشارها.

الاقتراحات: من 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.
- 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 سلوكياتهم مستقبلا، ودفعهم إلى ارتكاب الجرائم الالكترونية.
- العمل على فتح دورات تدريبية ولتكوين متخصصين في كيفية استخدام التقنيات الحديثة من جهة، وكيفية الوقاية من الجرائم الالكترونية ومواجهتها.

خاتمة:

انطلاقا مما سبق ذكره، يمكن القول بأن تكنولوجيا الاتصالات الحديثة ورغم أهميتها في تسهيل مختلف شؤون الحياة الاجتماعية، السياسية، الثقافية والاقتصادية، إلا أن سوء استخدامها يؤدي إلى أضرار وخيمة على الفرد والمجتمع ككل، وتعد الجريمة الالكترونية إحدى أخطر وأكثر السلوكيات الممارسة عبر هذه التقنيات المتطورة، والتي طالت الأشخاص، المؤسسات وحتى الحكومات، الشيء الذي دفع بالعديد من دول العالم إلى البحث عن استراتيجيات معينة بهدف التقليل من انتشارها وتفادي أثارها السلبية، ومنها الدولة القطرية التي اعتمدت سياسة ناجعة منذ بروز هذه الظاهرة فيها، حيث تمكنت من خلالها من إبطال العديد من محاولات ارتكاب الجرائم الالكترونية قبل حدوثها، وقللت كثيرا من مستوى انتشارها في الفترة الممتدة من عام 2005 وإلى غاية عام 2014.

- العمل على إيجاد إستراتيجية تعاونية دولية واضحة، بشأن إجراءات مكافحة الجريمة الالكترونية، وكيفية التعامل مع مرتكبيها.

الهوامش:

- ¹ محمد حجازي، جرائم الحاسبات والانترنت: الجرائم المعلوماتية، 2005، ص 10.
- ² Jiansheng Liang, criminalité informatique, école nationale supérieure des sciences de l'information et des bibliothèques, 1999, p17.
- ³ سعيد بن سالم البادي وآخرون، الجريمة الالكترونية في المجتمع الخليجي وكيفية مواجهتها، عمان: مجلس تعاون دول الخليج العربية، (د.ت.ن)، ص 28.
- ⁴ مفتاح بوبكر المطردي، "الجريمة الالكترونية والتغلب على تحدياتها"، المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية، جمهورية السودان، 23-25 سبتمبر 2012، ص 16.
- ⁵ اللجنة الاقتصادية والاجتماعية لغربي أسيا: الاسكوا (2013)، "نشرة تكنولوجيا المعلومات والاتصالات للتنمية في المنطقة العربية"، ع. 18، الأمم المتحدة: نيويورك، 2013، ص 28.
- ⁶ Michel Maffesoli, Essais sur la violence, librairie des méridiens, Paris, 1984, p47.
- ⁷ نورة شلوش، "القرصنة الالكترونية في الفضاء السيبراني: التهديد المتصاعد لأمن الدول"، مجلة مركز بابل للدراسات الإنسانية، ع. 2، المجلد 8، 2012، العراق، ص 195.
- ⁸ المطردي، مرجع سابق الذكر، ص 23.
- ⁹ Melissa Halhaway, programme de préparation a la lutte contre la cybercriminalité: étude de référence et indice, Arlington : Potomac Institute for Policy studies, 2015, p13.
- ¹⁰ بن سالم البادي وآخرون، مرجع سابق الذكر، ص 30.
- ¹¹ محمد بوزينة أمنة، "إجراءات التحري الخاصة في مجال الجرائم المعلوماتية دراسة تحليلية لأحكام قانون الإجراءات الجزائية وقانون الوقاية من جرائم الإعلام"، الملتقى الوطني حول: آليات مكافحة الجرائم الالكترونية في التشريع الجزائري، الجزائر، 29 مارس 2017، ص 59.
- ¹² office on drugs and crime, « rapport étude détaillée sur la cybercriminalité », 2013, USA : new York, 2013, p17.
- ¹³ بن سالم البادي وآخرون، مرجع سابق الذكر، ص 30.
- ¹⁴ الأمير عبد القادر حفوفة و حسام غرداين، "الجريمة الالكترونية واليات التصدي لها"، أعمال الملتقى الوطني: آليات مكافحة الجرائم الالكترونية في التشريع الجزائري، الجزائر، 29 مارس 2017، ص 94.
- ¹⁵ المرجع نفسه.
- ¹⁶ اللجنة الاقتصادية والاجتماعية لغربي أسيا: الاسكوا، "تقرير مكتب الأمم المتحدة المعني بالمخدرات والجريمة"، 2013، ص 3.
- ¹⁷ لجنة منع الجريمة والعدالة الجنائية، "تدابير فعالة لمنع ومكافحة الجريمة ذات الصلة بالحاسوب"، الدورة 11، الأمم المتحدة: فيينا، 2002، ص 5.
- ¹⁸ محمود صالح العادلي، "الجرائم المعلوماتية: ماهيتها وصورها"، ورشة العمل الإقليمية حول: تطوير التشريعات في مجال مكافحة الجرائم الالكترونية. مسقط، 2-4 ابريل 2006، ص 7.
- ¹⁹ Marco Gercke, comprendre la cybercriminalité, guide pour les pays en développement, Genève : union internationale des télécommunications, 2009, p10.
- ²⁰ التنظيم القانوني والجرائم الالكترونية ما بين امن المعلومات وتقييد الحريات، القاهرة: مركز هورودو لدعم التعبير الرقمي، 2018، ص 21.
- ²¹ عدنان مصطفى البار و خالد علي المرحي، "امن المعلومات والأمن السيبراني"، 2018، ص 9، تم الاسترجاع من الرابط: www.kau.edu.sa (consulté le 18/02/2020)
- ²² عبد الله دغش العجمي، "المشكلات العملية والقانونية للجرائم الالكترونية دراسة مقارنة"، (كلية الحقوق، جامعة الشرق الأوسط، الأردن، 2014)، ص 105.
- ²³ لجنة منع الجريمة والعدالة الجنائية، مرجع سابق الذكر، ص 5.

- ²⁴ اللجنة الاقتصادية والاجتماعية لغربي آسيا: الاسكوا، "الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية: توصيات سياسية"، الأمم المتحدة: نيويورك، 2015، ص 10.
- ²⁵ هشام ملاطي، "خصوصية القواعد الإجرائية للجرائم المعلوماتية- محاولة لمقاربة مدى ملائمة القانون الوطني مع المعايير الدولية"، سلسلة ندوات محكمة الاستئناف بالرباط، ع.7، 2014، ص 83؛
- ²⁶ تقرير مكتب الأمم المتحدة المعني بالمخدرات والجريمة، مرجع سابق الذكر، ص 329.
- ²⁷ المرجع نفسه، ص 332.
- ²⁸ Noémie Girard, *risque reliés à l'utilisation de la tablette électronique: vision holistique pour une prévention efficace*, paris : université Québec, 2016, p31.
- ²⁹ أديب خضور، دور الإعلام التربوي في مكافحة المخدرات: كيف يعالج الإعلام العربي مشكلة المخدرات دراسة ميدانية، الجزائر، دار الأيام للطباعة والنشر، 1999، ص 5.
- ³⁰ تقرير مكتب الأمم المتحدة المعني بالمخدرات والجريمة، مرجع سابق الذكر، ص 361.
- ³¹ المرجع نفسه، ص 346.
- ³² إخلاص شذوذ، "6 تحديات تعطل إثبات الجريمة الالكترونية.....ضحايا: نعرف المجرمين ولا دليل قاطعاً"، 2019، ص 1، تم الاسترجاع من <http://cybearena.com> (consulté le 01/03/2020).
- ³³ القانون رقم 14، المتعلق بمكافحة الجرائم الالكترونية في قطر، الجريدة الرسمية، ع.15، 2014.
- ³⁴ الهاشي، "تدريب 20 مؤسسة للتعامل مع الهجمات الالكترونية"، حزمة قوانين لحماية الأفراد من المخاطر الالكترونية قريبا"، 2013، ص 1، تم الاسترجاع من الرابط:
- www.raya.com » news (consulté le 18/01/2020).
- ³⁵ محمد نعمان، "الأمن السيبراني يعالج 14 مليون سجلا الكترونيا تعرضت للتهديد والاحتيال"، 2015، ص 1، تم الاسترجاع من الرابط:
- www.motc.gov.qa/cyber-security (consulté le 22/02/2020).
- ³⁶ تقرير الإعلام الاجتماعي العربي، "الجريمة الالكترونية في المجتمع الخليجي وكيفية مواجهتها"، عمان: مجمع البحوث والدراسات، 2016، ص 38.
- ³⁷ بوعلي حمدي بوجلطية، "الإرهاب الالكتروني وطرق مواجهته على المستوى العربي: دراسة للتجربتين السعودية والقطرية"، مجلة الأكاديمية للدراسات الاجتماعية والإنسانية، ع.16، 2016، ص 186.
- ³⁸ عبيد صالح حسن، "سياسة المشرع الإماراتي لمواجهة الجرائم الالكترونية"، مجلة الفكر الشرطي، ع.95، المجلد 24، 2015، ص 29.
- ³⁹ سعيد حبيب، "قطر الرابعة عالميا بالبنية التحتية الالكترونية"، ص 1، 2020، تم الاسترجاع من الرابط:
- www.aljazeera.net (consulté le 10/02/2020).
- ⁴⁰ "فريق وطني لمواجهة الجرائم الالكترونية، جريدة الوطن القطرية"، 2018، ص 5، تم الاسترجاع من الرابط:
- www.al-watan.com (consulté le 12/01/2020).
- ⁴¹ وزارة الاتصالات وتكنولوجيا المعلومات، تقرير حول: "الاتجاهات الناشئة لتكنولوجيا المعلومات والاتصالات في قطر"، 2014، ص 6.
- ⁴² عماد مراد، مؤثر دولي: قطر الأولى عالميا في الأمن والأمان، ص 1، 2019، تم الاسترجاع من الرابط:
- www.aljazeera.net (consulté le 16/03/2020).
- ⁴³ محمد أبو حجر، "ضبط جميع جرائم سرقة البطاقات الائتمانية"، ص 4، 2019، تم الاسترجاع من الرابط:
- www.al-watan.com (consulté le 22/01/2020).
- ⁴⁴ مسفر الأحبابي، "جهود متواصلة لحماية المجتمع من الجريمة"، ص 1، 2012، تم الاسترجاع من الرابط:
- www.mohamoon-qa.com (consulté le 22/01/2020).
- ⁴⁵ محمد نعمان، "الأمن السيبراني يعالج 14 مليون سجلا الكترونيا تعرضت للتهديد والاحتيال"، ص 1، 2015، تم الاسترجاع من الرابط:
- www.motc.gov.qa/cyber-security (consulté le 22/02/2020).
- ⁴⁶ وزارة الاتصالات وتكنولوجيا المعلومات، "تقرير حول: المشهد الرقمي في دولة قطر الأسر والأفراد"، 2014، ص 16.