مجلة العلوم الإنسانية لجامعة أم البواقي
ISSN 1112-9255
المجلد8، العدد 03 – ديسمبر 2021

النشاط الإجرامي في ظل فيروس كورونا كوفيد –19 (تنامي ظاهرة الجريمة الإلكترونية أنموذجا) .

Criminal Activity In Light Of Coronavirus Covid -19 (The Growing Phenomenon Of Cybercrime As A Model)

رضا سيف الدين جلولي*، جامعة ورقلة، الجزائر.
djelloulireda06@gmail.com

تاريخ التسليم:(2020/10/22)، تاريخ المراجعة:(2021/01/02)،تاريخ القبول:(2021/03/13)

ملخص :

تتطرق هذه الدراسة إلى ظاهرة الجريمة الإلكترونية، بالتركيز على أسباب تناميها في ظل فيروس كورونا كوفيد–19 والقطاعات المستهدفة، وقد تم التوصل أن التدابير التي فرض هذا الفيروس على الحكومات والشعوب اتباعها كالزيادة في العمل عن بعد وارتفاع استخدام شبكة الإنترنت والبحث من خلالها حول طرق الوقاية منه، تعد السبب الرئيسي لتنامي الجريمة الإلكترونية، لأنها وفرت البيئة المساعدة لارتكاب هذا النوع من الجرائم،بينما تمثلت القطاعات المستهدفة في: القطاع الصحي والمالي والنفطي ومنصات الفيديو والألعاب الإلكترونية.

الكلمات المفتاحية: الجريمة الإلكترونية، فيروس كورونا كوفيد–19، الهجمات الإلكترونية، الأمن الإلكتروني، الجريمة

Abstract :

This study addresses the phenomenon of Cybercrime, by focusing on the causes of their growth in light of the Coronavirus Covid-19 and the targeted sectors.

The study found that the measures and procedures imposed by the Coronavirus Covid-19 on governments and people especially : Increased Telework, rising use of the Internet and search through it for information about the virus and ways to prevent it, are the main reason behind the increase in cybercrime rates in light of the Coronavirus Covid- 19, Because it provided the enabling environment for committing this type of crime, and The most important sectors targeted were: the health sector, the financial sector, the oil sector, conference platforms, video meetings and chats, electronic gaming platforms.

Keywords : Cybercrime, Coronavirus Covid -19, Cyberattacks, Electronic Security, The Crime..

* المؤلف المراسل: رضا سيف الدين جلولي ، الإيميل: djelloulireda06@gmail.com

مقدمة:

في ظل التطورات المستمرة التي تعرفها ظاهرة الجريمة الإلكترونية وأساليب ودوافع ارتكابها، فإنها تعتبر من أكثر أنواع الجرائم إثارة للانشغالات والتخوفات على المستوى العالمي والقاري والوطني، وخاصة مع الانعكاسات الوخيمة التي من شأنها أن تخلفها على الحكومات والأفراد والشركات والمنظمات، وليس مبالغا القول أنها قد تصل إلى حد تقرير مصيرهم ومستقبلهم، والانتخابات الرئاسية الأمريكية لسنة 2016 وما دار حولها من جدل وجدال حول تدخل روسيا من خلال قراصنة ومخترقين إلكترونيين في التأثير بنتائجها ليس ببعيد.

فظاهرة الجريمة الإلكترونية باتت تشكل هاجسا وتحديا عالميا وإقليميا ووطنيا، اتفقت مختلف الحكومات على بذل الجهود والتعاون فيما بينها لمكافحتها وكبحها من خلال المعاهدات الدولية والإقليمية والمؤتمرات الأممية، والتشريعات الوطنية، والمنظمات المختصة بمكافحة الجرائم بأنواعها.

ومع ذلك، فقد جاء فيروس كورونا كوفيد-19 الذي ظهر في الصين نهاية العام 2019 ليضاعف من حجم خطر وتهديدات هذا النوع من الجرائم، إذ شهدت الهجمات والجرائم الإلكترونية تناميا كبيرا منذ ظهور هذا الفيروس ومع استمراره مقارنة بما كان عليه الأمر قبله.

- إشكالية الدراسة :

على عكس الجرائم التقليدية التي عرفت انخفاضا ملحوظا، شهدت الجريمة الإلكترونية تناميا كبيرا في ظل فيروس كورونا كوفيد-19 و مع استمراره، وذلك بالرغم من الجهود الدولية والإقليمية والوطنية المبذولة لردعها ومكافحتها، وهذا ما يقود إلى طرح الإشكالية التالية : ماهي أسباب تنامي ظاهرة الجريمة الإلكترونية في ظل فيروس كورونا كوفيد-19 رغم الجهود الدولية والإقليمية والوطنية المبذولة لردعها ومكافحتها؟ وماهي القطاعات المستهدفة بالجريمة الإلكترونية في ظل هذا الفيروس؟

- أهداف الدراسة : فضلا عن التعريف بظاهرة الجريمة الإلكترونية والجهود المبذولة دوليا وأوروبيا وعربيا لمكافحتها، تستهدف هذه الدراسة بشكل رئيسي الكشف عن أسباب تنامي هذه الظاهرة خلال أزمة كورونا كوفيد-19 الصحية، و القطاعات المستهدفة والمتضررة، والطريقة التي تعاملت بها الحكومات والمنظمات و الشركات المختلفة وخاصة المستهدفة في مواجهة ذلك.

– منهجية الدراسة : جرى استخدام المنهج الوصفي التحليلي في هذه الدراسة، وذلك من خلال جمع المعلومات والبيانات الخاصة أو ذات الصلة بظاهرة الجريمة الإلكترونية وعلاقة فيروس كورونا كوفيد–19 بتناميها، ومن ثم تفسير وتحليل هذه المعلومات والبيانات من أجل الإجابة على الإشكالية المطروحة وبلوغ أهداف الدراسة.

2 . مدخل مفاهيمي للجريمة الإلكترونية :

للجريمة الإلكترونية كغيرها من الجرائم الأخرى تقليدية أو غير تقليدية، خصائص تتميز بها ودوافع لارتكابها، وفي نفس الوقت هي لاتقل خطورة عن باقي هذه الجرائم من حيث انعكاساتها الوخيمة على المستهدفين سواء أكانوا دولا أو منظمات أو شركات أو أفراد، فتصنيفها ضمن الجرائم في حد ذاته كافي للتأكيد على هذا الأمر.

1.2 تعريف الجريمة الإلكترونية:

اشتقت كلمة الجريمة في اللغة من الجرم وهو التعدي أو الذنب وجمع الكلمة إجرام وجروم وهو الجريمة (الحسيناوي، 2008، ص 21)، والجريمة بوجه عام هي كل فعل أو نشاط يتم بطريقة غير مشروعة، بمعنى أنها تشمل كل نشاط مخالف للقوانين الجزائية النافذة في مختلف دول العالم، وهذا النشاط الإجرامي إذا ما استخدمت فيه وسائط تقنية علمية، أصبح الفعل جريمة إلكترونية (مصري، 2012، ص91)، وهنا يتضح أن الجريمة الإلكترونية تشترك مع الجريمة التقليدية في طبيعة الفعل في كونه مجرما وغير قانوني، ولكنها تختلف معها في الأسلوب ونقصد بذلك أداة ووسيلة ارتكاب الجريمة.

وقد تعددت التسميات التي أطلقت على الجريمة الإلكترونية: جريمة إلكترونية، جريمة معلوماتية، جرائم الحاسوب، جرائم الإنترنت، ولكن يبقى أن شكل الجريمة بهم جميعا واحد، وبالتالي فالجريمة الإلكترونية تشمل جميع أنواع الجرائم التي تتم من خلال أو بواسطة الحاسب الآلي منفردا أو متصلا بالإنترنت. (نصار، 2017، ص11)

2.2 الخصائص المميزة للجريمة الإلكترونية:

تنفرد الجريمة الإلكترونية بمجموعة من الخصائص التي تميزها عن غيرها من مفاهيم الجريمة الأخرى، تتمثل أساسا في:

- الحاسب الآلي أداة لارتكابها: تعتبر هذه الخاصية من الخصائص التي تميز الجرائم الإلكترونية عن غيرها من الجرائم الأخرى ولا سيما الجرائم التقليدية، ذلك لأن شبكة الإنترنت هي إحدى التقنيات الحديثة التي أفرزها تطور الحوسبة، ولذلك فإن ارتباطها

بالحاسب الآلي هو أمر لا مفر منه، باعتباره النافذة التي تطل بها تلك الشبكة على العالم الخارجي وإن كنا اليوم نعاصر إمكانية استعمال الإنترنت عبر الهاتف الخلوي. (نصار، 2017، ص 35)

- عابرة للحدود: إذ أن الجريمة الإلكترونية لا تعترف بالحدود الجغرافية، حيث ترتكب من أشخاص يستطيعون أن يخترقوا الزمان والمكان دون الخضوع لحرس الحدود، (عطوش، 2017، ص 29) فالمجرم الإلكتروني يستطيع ارتكاب جريمته في أي بلد من العالم دون الحاجة أن ينتقل إليه أو يتواجد في مكان جريمته.
- سريعة التنفيذ : لا يتطلب تنفيذ الجريمة الإلكترونية الوقت الكبير، فبضغطة زر واحدة على لوحة المفاتيح يمكن أن تنتقل ملايين الدولارات من مكان إلى آخر ، ولكن هذا لا يعني أنها لا تتطلب الإعداد قبل التنفيذ أو استخدام معدات وبرامج معينة. (رسلان، 2016، ص46)
- صعوبة اكتشافها: تتميز الجريمة الإلكترونية بصعوبة اكتشافها وإذا اكتشفت فإن ذلك يكون بمحض الصدفة عادة، ومن أهم الأسباب التي تقف وراء الصعوبة في اكتشاف الجريمة الإلكترونية هي عدم ترك هذه الجريمة لأي أثر خارجي بصورة مرئية. (المومني، 2010، ص 53-54)
- صعوبة إثباتها: تتميز الجرائم الإلكترونية عن الجرائم التقليدية بأنها صعبة الإثبات، وهذا راجع إلى افتقاد وجود الآثار التقليدية للجريمة، وغياب الدليل الفيزيقي (بصمات، تخريب، شواهد مادية)، وسهولة محو الدليل أو تدميره في زمن متناهي القصر، يضاف إلى ذلك نقص خبرة الشرطة والنظام العدلي، وعدم كفاية القوانين القائمة. (رسلان، 2016، ص 47)
- جرائم ناعمة وأقل عنفا في التنفيذ : فالجرائم الإلكترونية عكس الجرائم التقليدية لا تحتاج إلى أدنى مجهود عضلي أو استعمال العنف بل تعتمد على الدراسة الذهنية، والتفكير العلمي المدروس القائم عن معرفة تقنية بالحاسب الآلي. (نصار، 2017، ص 37-38)
- تعاون عدة أشخاص على ارتكابها : حيث تتم الجريمة الإلكترونية من شخص لديه معرفة فنية في مجال الحاسوب، بمساعدة وتعاون في أحيان كثيرة شخص آخر يكون من محيط المؤسسة المجني عليها أو من خارجها لتغطية عملية التلاعب وتحويل المكاسب إليه. (عطوش، 2017، ص 33)

3.2 الدوافع الكامنة وراء ارتكاب الجريمة الإلكترونية :

لكل نوع من أنواع الجرائم المختلفة دوافع محددة لارتكابها، وهذا ينطبق على الجريمة الإلكترونية بل هناك دوافع تشترك فيها هذه الأخيرة مع غيرها من الجرائم، ويمكن حصر أهم الدوافع التي يمكن أن تقف وراء ارتكاب الجرائم الإلكترونية في :

- السعي إلى تحقيق الكسب المادي : تعد محاولات الكسب السريع وجني الأرباح الطائلة دون تعب ولا رأس مال من الدوافع الرئيسية لاختراق الأنظمة الإلكترونية (الحمداني، 2014، ص 69)، ومن الأمثلة على ذلك نذكر قيام مبرمج يعمل لدى شركة ألمانية بالاستيلاء على 22 شريطا ممغنطا تحوي معلومات هامة بخصوص عملاء وإنتاج الشركة، وهدد ببيعها للشركات المنافسة مالم تدفع له فدية مقدارها 200 ألف دولار، وبعد أن قامت الشركة بتحليل الموقف وقدرت أن الخسائر التي يمكن أن تنشأ عن إفشاء محتواها تفوق بكثير المبلغ المطلوب، فضلت دفع المبلغ من أجل استرداد الأشرطة المسروقة. (الديربي و صادق، 2012، ص 50).
- الرغبة في التعلم: كثيرا ما يعلن القراصنة الإلكترونيون أن هدفهم من الوصول إلى المعلومات ودخولهم للشبكات والحواسيب الإلكترونية هو التعلم فقط، فهم يتعاونون في البحث على شكل جماعات ويتقاسمون المعلومات والخبرات التي يحصلون عليها ويستفيدون منها في أنشطة هادفة ولكنها مع ذلك تبقى غير مشروعة، (مجمع البحوث والدراسات،2016، ص28)، وخاصة لكونها تتعدى على حقوق الملكية للآخرين أفرادا أوشركات أومنظمات، وقد تلحق بهم خسائر مادية كبيرة يستحيل تداركها.
- الدوافع السياسية : فالشبكات والأجهزة الأمنية الحكومية في مختلف دول العالم عرضة باستمرار لمحاولات الاختراق الإلكتروني، كذلك يتم استغلال شبكة الإنترنت لنشر أفكار العديد من الأفراد والمجموعات، والترويج لأخبار وأمور أخرى قد تحمل في ثناياها مساسا بأمن الدولة، أو بنظام الحكم، أو قدحا في رموز دولية أو سياسية والإساءة لها بالذم والتشهير. (البقمي، 2008، ص 11)
- الدوافع الإرهابية : امتدت الجريمة الإلكترونية لتشمل صور الجريمة المنظمة، حيث ظهر الإرهاب الإلكتروني على الشبكة، وأخذت الجماعات الإرهابية مواقع لها على الإنترنت تمارس أعمالها من خلالها، كالتحريض على القتل، بالإضافة إلى تعليم صنع المتفجرات والقنابل، علاوة على نشر أفكارها الإرهابية، وأصبحت تقوم بشن عملياتها

الإرهابية عبر الإنترنت من خلال التلاعب بنظم وبيانات نظم خاصة. (البقمي، 2008، ص 11)

- التهديد والانتقام : فالجريمة الإلكترونية قد تكون بدافع تهديد شخص أو شركة ما، كمثال على ذلك قيام مستخدم باحتجاز الذاكرة المركزية الخاصة بشركة التأمين التي فصل منها كرهينة لديه، و تهديد رئيسه في العمل بأنه إذا حاول أن يلغي بطاقة أجرته من ذاكرة الحاسب الآلي، فإن هذه الأخيرة سوف تدمر تلقائيا عن طريق ما يعرف بالقنابل المنطقية، (الديربي و صادق، 2012، ص 50) كما يعد دافع الانتقام من أخطر الدوافع التي يمكن أن تدفع الشخص إلى ارتكاب جريمة إلكترونية حيث قد يلجأ أحد الموظفين بالاستعداد مسبقا لمثل هذا الموقف، حيث يقوم بزرع برنامج يحمل تعليمات لمسح كافة البيانات في حالة عدم وجود اسمه في كشف الموظفين بالشركة، ويقوم عند فصله بالانتقام من هذه المؤسسة عن طريق تشغيل هذا البرنامج. (نصار، 2017، ص 54)
- قهر النظام وإثبات التفوق : هناك من المخترقين الإلكترونيين دافعه لارتكاب الجرائم الإلكترونية يغلب عليه الرغبة في قهر النظام أكثر من شهوة الحصول على الربح، حيث يميلون إلى إظهار تفوقهم ومستوى ارتقاء براعتهم لدرجة أنه إزاء ظهور أي تقنية مستحدثة فإن مرتكبي هذه الجرائم لديهم شغف بالآلة يحاولون إيجاد الوسيلة إلى تحطيمها بل والتفوق عليها، (رسلان، 2016، ص 43)، وكثيرا ما تلجأ الحكومات والشركات إلى الاستعانة بالمخترقين الإلكترونين وإغرائهم بمكافآت من أجل مساعدتها على تأمين أنظمتها الإلكترونية و اكتشاف نقاط الخلل فيها، وحتى أيضا لمحاربة مجرمين إلكترونين آخرين يستهدفونها.
- التسلية واللهو: عدد ليس بقليل من مخترقي الأنظمة يعتبرون أن عملهم هذا وسيلة للمرح والتسلية وتقضية أكبر وقت ممكن في أنظمة وحواسيب الآخرين، ويكون هذا الإختراق غالبا سلميا ودون أن يحدث تأثير يذكر. (الحمداني، 2014، ص 70)

مما سبق يتبين أن الجريمة الإلكترونية لها دوافع متعددة، تختلف من مجرم إلكتروني إلى آخر ما يجعلنا نميل إلى القول أنه لا يمكن وضع جميع المجرمين أو المخترقين الإلكترونيين ضمن نفس المستوى والصنف، فمن يرتكب جريمة إلكترونية لتحقيق أهداف سياسية وإرهابية أو القيام باختلاسات مالية كبيرة، ليس مثل من يقوم بها لمجرد اللعب واللهو وتمضية الوقت.

3. الجهود المبذولة لمكافحة الجريمة الإلكترونية:

مع تزايد عدد الجرائم الإلكترونية وتطور أساليبها، وارتفاع درجة الخطورة التي باتت تشكلها، أخذت الدول وكذلك المنظمات والشركات سواء المعنية بمكافحة الجريمة بأنواعها المختلفة أو تلك التي يمكن أن تتضرر بالجرائم الإلكترونية في التعامل مع هذه الظاهرة بجدية، وبذل الجهود الرامية إلى مكافحتها وعلى عدة مستويات دوليا، قاريا، إقليميا، وطنيا.

1.3 الجهود الدولية لمكافحة الجريمة الإلكترونية:

نظرا لتباعد المسافات بين الدول فقد اتفقت على استخدام الإنتربول (منظمة الشرطة الجنائية الدولية)، وهي أكبر منظمة شرطية في العالم أنشأت سنة 1923، وتتمثل مهمتها في تقديم المساعدة إلى أجهزة إنفاذ القانون في دول الأعضاء 194 لمكافحة جميع أشكال الإجرام عبر الوطنية، ومنها الجرائم الإلكترونية (المزاهرة،2014، ص 390)، وفي هذا الصدد ترتكز الاستراتيجية الحالية لمنظمة الإنتربول في مكافحة الجريمة الإلكترونية على 05 مسارات عمل هي : (الإنتربول، 2017، ص2)

- تقييم التهديدات وتحليلها ورصد اتجاهاتها: بهدف الكشف عن الجرائم الإلكترونية ومرتكبيها والمجموعات التي تقف وراءها والتوصل إلى نتائج مؤكدة في هذا الشأن.
- الاطلاع على البيانات الرقمية الأصلية والاستفادة منها: تيسير الوصول إلى البيانات المتعلقة بالاعتداءات الإلكترونية والأدوات المفيدة والشركاء لتعزيز جمع البيانات والاستفادة منها بشكل أفضل.
- إدارة الأدلة الرقمية: إدارة الأدلة الرقمية لأغراض التحقيقات والملاحقات القضائية، جمع القرائن وفقا للقانون، وحفظ الأدلة وعرضها بشكل مفهوم ومقبول لدى المحاكم.
- الربط بين المعلومات الإلكترونية والمعلومات الفعلية: اكتشاف العلاقة القائمة بين الآثار الرقمية والمعلومات الفعلية ليتسنى تحديد مكان مرتكبي الجرائم الإلكترونية المحتملين.
- التوحيد والتشغيل البيني : تحسين مستوى العمل سوية على صعيد العمليات والتنسيق على المستوى العالمي والحث على توحيد التشريعات.

بدورها تلعب منظمة الأمم المتحدة دورا مهما في التصدي ومكافحة الجريمة الإلكترونية وتعزيز وتشجيع التعاون الدولي في هذا الشأن، وخاصة من خلال مؤتمراتها المتعلقة بمنع الجريمة والمجرمين التي تعقد كل خمس سنوات. (منذ 2005 أصبحت هذه المؤتمرات تعقد تحت مسمى مؤتمر الأمم المتحدة لمنع الجريمة والعدالة الجنائية).

حيث تم في المؤتمر الأخير المنعقد بالدوحة في قطر سنة 2015 التأكيد بخصوص الجريمة الإلكترونية على ضرورة العمل وبذل الجهود الرامية إلى : (مكتب الأمم المتحدة المعني بالمخدرات والجريمة، 2015، ص 10)

- استكشاف تدابير خاصة تهدف إلى توفير بيئة إلكترونية آمنة ومتينة.
- منع ومكافحة الأنشطة الإجرامية التي تنفذ عبر الإنترنت.
- تعزيز أمن الشبكات الحاسوبية وصون سلامة البنية التحتية ذات الصلة.
- السعي إلى تقديم مساعدة تقنية طويلة الأمد وخدمات لبناء وتدعيم قدرات السلطات الوطنية في التصدي للجرائم الإلكترونية.

وتجدر الإشارة أن الأمم المتحدة وافقت سنة 2019 على إنشاء لجنة خبراء تمثل جميع مناطق العالم لوضع معاهدة دولية لمكافحة الجريمة الإلكترونية. (حدادين، 2019)

2.3 الجهود الأوروبية لمكافحة الجريمة الإلكترونية :

اعتمد المجلس الأوروبي الطابع الدولي للجرائم الإلكترونية منذ العام 1976، وفي سنة 1996 أنشأت اللجنة الأوربية لمشاكل الجريمة (CDPC) لجنة خبراء للتعامل مع الجريمة الإلكترونية، عملت اللجنة بين العامين 1997 و 2000 على مشروع اتفاقية لمكافحة الجريمة الإلكترونية التي اعتمدها البرلمان الأوروبي في الجزء الثاني من جلسته العامة في أفريل 2001، وعرفت باتفاقية مجلس أوروبا حول الجريمة الإلكترونية، وهي أول اتفاقية دولية تسعى لمعالجة الجرائم الإلكترونية عبر التنسيق بين القوانين الوطنية الوطنية وقوانين الدول الأخرى، وقد سعت لتحقيق مايلي : (لبكي، 2013، ص 91-92)

- توحيد عناصر القانون الجزائي المحلي مع الأحكام المتعلقة بالجرائم الإلكترونية.
- توفير الإجراءات القانونية اللازمة للتحري وملاحقة الجرائم المرتكبة إلكترونيا بواسطة الكمبيوتر.
- تعيين نظام سريع وفعال للتعاون الدولي.
- الحفاظ بشكل سريع على البيانات المخزنة على أجهزة الكمبيوتر وحفظها والإفصاح الجزئي عن حركة البيانات المخزنة على الكمبيوتر.
- جمع معلومات عن حركة البيانات وعن إمكانية وجود تدخل في محتواها.
- تحقيق التعاون الدولي في المواضيع التالية: تسليم المجرمين، المساعدة الدولية المتبادلة، إعطاء المعلومات بصورة آلية، إنشاء الولاية القضائية على أي جريمة.

- المساعدة المتبادلة في جمع حركة المعلومات واعتراضها.
- تحديد الإجراءات المتعلقة بطلبات المساعدة المتبادلة في غياب الاتفاقيات الدولية.

وإلى غاية أكتوبر 2020 بلغ عدد الدول المصادقة والمنظمة إلى هذه الاتفاقية 65 دولة منها دول كثيرة من خارج أوروبا كالولايات المتحدة الأمريكية واليابان وكندا وأستراليا ومن الدول العربية نجد المغرب.(Council Of Europe, 2020)

كما أنشأ المجلس الأوروبي في لكسمبورغ عام 1991 شرطة أوروبية (يوروبول)، لتكون أداة للتنسيق والتعاون بين أجهزة الشرطة الوطنية في الدول الأوروبية المنظمة، ولملاحقة الجناة في الجرائم العابرة للحدود، ومنها بطبيعة الحال الجرائم الالكترونية (المزاهرة، 2014، ص 390) حيث قام اليوروبول بإحداث المركز الأوروبي للجرائم الإلكترونية (EC3) في سنة 2013 بهدف تعزيز استجابة إنفاذ القانون للجرائم الإلكترونية والمساعدة في حماية المواطنين الأوروبيين والشركات والحكومات الأوروبية من الجرائم الإلكترونية (Europol) .

إن وضع أوروبا لاتفاقية دولية وإنشائها مركزا متخصصا لمكافحة الجريمة الإلكترونية، يؤكد من جهة على حجم التهديد والخطر الشديد الذي يشكله هذا من النوع من الجريمة على الدول الأوروبية (حكومات وشركات وأفراد)، ومن جهة أخرى على حرص هذه الدول في التعامل والتعاطي مع قضية الجريمة الإلكترونية بالجدية والصرامة التي تتطلبها.

3.3 الجهود العربية لمكافحة الجريمة الإلكترونية:

لكون الدول العربية ومجتمعاتها كغيرها من دول ومجتمعات العالم ليست بمأمن من التعرض للهجمات والجرائم الإلكترونية، عملت حكوماتها على بذل الجهود ووضع الآليات التي تسمح وتساعد على مكافحة هذه النوع من الجرائم.

و قد تجسد ذلك في إصدار الاتفاقية العربية لمكافحة جرائم تقنية المعلومات سنة 2010 التي تستهدف تعزيز ودعم التعاون بين الدول العربية في مجال مكافحة الجرائم الإلكترونية، والحفاظ على أمن الدول العربية ومجتمعاتها وأفرادها ومصالحها في مواجهة الخطر الذي باتت تمثله هذه الجرائم (جامعة الدول العربية، 2010، ص 1)، ويضاف إلى هذا الجهود الوطنية لكل دولة عربية على حدة، حيث قامت معظمها بسن تشريعات وقوانين لمكافحة الجرائم

الإلكترونية، وكانت الإمارات العربية المتحدة أول دولة عربية تسن قانونا خاصا بهذا النوع من الجرائم، وهو القانون الاتحادي 2006 بشأن مكافحة جرائم تقنية المعلومات. (المزاهرة، 2014، ص 393)

ورغم أن الجهود الدولية والأوروبية والعربية لمكافحة الجريمة الإلكترونية تستحق الإشادة والتثمين، ولكنها في الحقيقة لم تكن كافية لوضع حد لهذه الجرائم والهجمات الإلكترونية، أو حتى على الأقل التقليل من عددها وحجم الخسائر التي سببتها للدول والشركات والأفراد، وهذا ما تؤكده الإحصائيات والتقارير المختصة.

حيث تشير الأرقام إلى ازدياد الهجمات على الأجهزة الإلكترونية في العالم من 500 مليون عام 2003 إلى 12.5 مليار هجوم عام 2010، ومن المتوقع أن يصل عدد هذه الهجمات إلى 50 مليارا عام 2020 (شعيب، 2018) ، وستكلف الجريمة الإلكترونية العالم 6 تريليونات دولار سنويا بحلول عام 2021 في زيادة بنسبة 100٪ عن عام 2015، عندما قدرت تكلفتها السنوية بـ 3 تريليون دولار.(Spajic, 2019)

4. تنامي الجريمة الإلكترونية في ظل فيروس كورونا كوفيد-19

تباينت انعكاسات فيروس كورونا كوفيد-19 على الجريمة، فبينما شهدت الجرائم التقليدية انخفاضا ملحوظا، عرفت الجرائم والهجمات الإلكترونية ارتفاعا كبيرا في معدلاتها، وهذا بحسب ما تؤكده الأرقام والإحصائيات المقدمة من طرف المنظمات الدولية والمؤسسات والشركات المختصة والمعنية بمكافحة هذا النوع من الجرائم.

حيث أعلنت الشرطة الجنائية الدولية الإنتربول Interpol أنه تم تسجيل خلال الأشهر الأربعة الأولى من العام 2020 نحو 907 آلاف رسالة إلكترونية غير مرغوب فيها و737 حادثة ناجمة عن برامج خبيثة و48 ألف رابط لعناوين مواقع إلكترونية ضارة، كلها تتعلق بفيروس كورونا كوفيد-19.(Interpol, 2020, p. 04)

ووفقا لشركة إنسايت IntSights للأمن الإلكتروني، كان هناك ارتفاع كبير في عدد المواقع المستخدمة بأسماء مثل Corona أو Covid لخداع الضحايا للاعتقاد بأنها صفحات رسمية، فخلال عام 2019 تم تسجيل 190 موقع فقط، وفي يناير 2020 وحده، وصل هذا الرقم إلى أكثر من 1400، وخلال فبراير ارتفع إلى ما يزيد عن 5000 قبل أن يتجاوز 38000 في مارس. (الشافعي، 2020)

وكشف تقرير صادر عن شركة مايم كاست Mimecast المختصة في مجال أمن البريد الإلكتروني بعنوان 100 يوم من فيروس كورونا كوفيد-19 عن ارتفاع عدد الجرائم الإلكترونية بنسبة 33 % منذ مطلع العام 2020 حتى نهاية مارس من العام نفسه. (أحمد، 2020)

كما أكد مكتب التحقيقات الفيدرالية الأمريكي FBI أن الجرائم الإلكترونية زادت بنسبة تصل إلى 300 فى المئة منذ بداية فيروس كورونا كوفيد-19، وقال مركز شكاوى جرائم الإنترنت التابع للمكتب الفيدرالى (IC3) إنه أصبح يتلقى ما بين 3000 و 4000 شكوى يوميا تتعلق بالأمن الإلكتروني كل يوم، وذلك مقارنة بمتوسط 1000 شكوى يوميا التى شهدها المركز قبل ظهور فيروس كورونا كوفيد-19.(England, 2020)

1.4 العوامل التي أدت إلى تنامي الجريمة الإلكترونية في ظل فيروس كورونا كوفيد-19 :

هناك عوامل محددة لا اختلاف حولها كانت هي السبب الرئيس في ارتفاع عدد الجرائم والهجمات الإلكترونية خلال أزمة كورونا كوفيد-19 الصحية، تتمثل أساسا في:(خليفة، 2020)

- التوسع في العمل عن بعد: فالتوسع في إنشاء شبكات تسمح بدخول الموظفين إلى قواعد بيانات الشركات عن بعد، مع زيادة كبيرة في الطلب على دخول هذه الشبكات من قبل الموظفين وضعف ثقافة الأمن الإلكتروني لدى كثير منهم، واستخدامهم لأجهزة كمبيوتر شخصية قد تحتوي على برامج غير أصلية أو غير محدثة، يجعل عمل المخترقين أمرا سهلا، نظرا لتنوع الأهداف التي يمكن إصابتها، وكثرة الثغرات التي يمكن استغلالها.
- صعوبة تأمين بيئة الأعمال الإلكترونية: في ظل حالة عدم اليقين التي تسيطر على البشرية، وضعف الإجراءات الإلكترونية الأمنية، وتطبيق الحجر الصحي أيضا على مسؤولي قطاع تكنولوجيا المعلومات في الشركات، وصعوبة السيطرة على البيئة الإلكترونية الخاصة بالشركة، والتي تشمل موظفين غير معلوم حجم الثغرات الإلكترونية التي يقعون فيها، فإن ذلك يمثل بيئة مثالية للمخترقين لتحقيق أهدافهم، ويصعب بشكل كبير من مهمة مكافحة الاختراق.
- زيادة الاعتماد على تطبيقات التواصل الاجتماعي: مع توجه كثير من الأفراد لتطبيق مفهوم Social Distance أو المسافة الاجتماعية، زاد اعتمادهم على المحادثات الافتراضية من خلال تطبيقات التواصل الاجتماعي ومكالمات الفيديو، فأصبحوا بمثابة أهداف للمخترقين، إما لسرقة معلومات شخصية بهدف بيعها أو تشفيرها للابتزاز

المالي، أو السيطرة على أجهزتهم الشخصية لاستخدامها من خلال شبكات بوت نت Botnet في شن هجمات إلكترونية على الشركات والمؤسسات والحكومات.

- زيادة فترة استخدام شبكة الإنترنت : أصبح معدل استهلاك الإنترنت أكبر من ذي قبل، وزادت فترة التواجد، سواء للعمل أو التعليم أو الترفيه أو التواصل الاجتماعي، فمثلا أعلنت شركة فودافون أن نسبة الزيادة في تحميل البيانات الخاصة بها وصلت إلى 50% في بعض البلدان، كما زاد استهلاك الإنترنت في بعض البلدان مثل إيطاليا بنسبة 30%، وزاد استهلاك الولايات المتحدة الأمريكية حتى 22 مارس أي قبل أن تستحوذ على المرتبة الأولى من حيث عدد الإصابات بفيروس كورونا كوفيد-19 بنسبة 18%، وبالتالي فإن زيادة فترة التواجد على الإنترنت تعني زيادة معدل التعرض للهجمات الإلكترونية أيضا.
- استغلال المخاوف والقلق البشري: استغل المخترقون المخاوف والقلق البشري في تنفيذ عمليات الاختراق الإلكتروني، حيث يقوم كثير من الأفراد بالبحث عن معلومات عبر الإنترنت حول فيروس كورونا كوفيد-19 ، بهدف معرفة مزيد من المعلومات حول هذا الفيروس والأعراض المرضية المرتبطة به والتعليمات الصحية الضرورية لتفادي الإصابة، وكذلك المعلومات حول أعداد الحالات الجديدة المصابة بالمرض، فقام المخترقون بإنشاء مواقع إلكترونية خادعة، تعمل بمثابة فخ إلكتروني للزوار، فبمجرد دخول الأفراد إلى أحدها تتم إما سرقة بياناتهم الشخصية بهدف بيعها عبر الإنترنت، أو اختراق الأجهزة الشخصية الخاصة بهم.

مما تقدم يتضح أن الواقع والتدابير التي فرضها فيروس كورونا كوفيد-19 على البشرية (تطبيق التباعد الاجتماعي، التعليم والعمل عن بعد، زيادة استخدام شبكة الإنترنت والبحث من خلالها على معلومات حول الفيروس المستجد وطرق الوقاية والتعافي منه...إلخ)، أتاح للمخترقين والمجرمين الإلكترونيين البيئة المناسبة والمساعدة للقيام بجرائمهم وهجماتهم الإلكترونية، وهو ما عملوا على عدم تفويته، وكان النتيجة بذلك تزايد معدلات الجرائم والهجمات الإلكترونية بشكل كبير خلال أزمة فيروس كورونا كوفيد-19 الصحية.

2.4 القطاعات المستهدفة بالجريمة الإلكترونية في ظل فيروس كورونا كوفيد-19 :

ظهر جليا أن هناك قطاعات هي الأكثر استهدافا بالجرائم والهجمات الإلكترونية من غيرها خلال أزمة كورونا كوفيد -19 الصحية، وهي :

- القطاع الصحي : يعد قطاع الرعاية الصحية أكثر القطاعات تعرضا للهجمات والجرائم الإلكترونية خلال فيروس كورونا كوفيد-19، حيث جرى استهداف المستشفيات والمراكز الطبية والمؤسسات العامة في مختلف أنحاء العالم من خلال برامج الفدية بصورة أساسية، فنظرا لحاجة أطقم الرعاية الصحية إلى بنية تحتية رقمية لمواجهة أزمة كورونا كوفيد-19، عمل المخترقون على استغلال هذه الثغرة، ظنا منهم أن المؤسسات الصحية ستضطر إلى الدفع لاستعادة أنظمتها، كما انتهز المخترقون أيضا أزمة الرعاية الصحية لبيع الأدوات الطبية المزيفة، وشمل ذلك عمليات احتيال عديدة تورط فيها أفراد وكيانات تنتحل صفة المسؤولين الحكوميين، وتدعي هذه الكيانات توصلها إلى اكتشافات جديدة عن فيروس كورونا كوفيد-19 وتروج لمبيعات أو منتجات طبية وهمية، وأبلغ المكتب الوطني للاستخبارات الاحتيالية في المملكة المتحدة عن خسائر 1.6 مليون جنية إسترليني بسبب الاحتيال المرتبط بفيروس كورونا كوفيد-19، إذ دفعت ضحية واحدة 000 15 جنيه استرليني لشراء أقنعة وهمية، (مؤسسة دبي للمستقبل، 2020، ص 4) من جانبها أشارت منظمة الصحة العالمية في عدة تقارير صادرة عنها في نهاية أفريل 2020، إلى تزايد الهجمات الإلكترونية المرتبطة بفيروس كورونا كوفيد-19 التي كانت عرضة لها، لتصبح عدة أضعاف مستواها وقت بداية تفشي الفيروس، وقد تركزت هذه الهجمات في ثلاثة اتجاهات : الهجوم على البنية المعلوماتية للمنظمة، واختراق الحسابات الإلكترونية للعاملين في مجال مكافحة فيروس كورونا كوفيد-19 من أطباء وصيادلة وأفراد طواقم طبية وباحثين بيولوجيين ومسئولين في شركات أدوية، وتزوير حسابات إلكترونية باسم الصندوق التضامني للاستجابة ضد فيروس كورونا كوفيد-19، ويتمثل الهدف من ذلك في الحصول على معلومات بشأن الفيروس أو الأدوية التي تعالج أعراضه، أو تتعلق باللقاحات المحتملة للقضاء عليه، ومن ثم يمكن لهؤلاء المخترقين بيع هذه المعلومات لدول وأجهزة مخابرات وشركات كبرى التي تتسابق فيما بينها للحصول على هذا اللقاح .(مركز المستقبل للأبحاث والدراسات المتقدمة، 2020)
- القطاع المالي : تضرر القطاع المالي بشدة من الهجمات والجرائم الإلكترونية في ظل فيروس كورونا كوفيد-19، ولهذا حذرت المصارف المركزية من المحتالين الذين يسعون لاختراق الحسابات المصرفية (البيان الإلكتروني، 2020)، ونشرت مجموعة العمل الدولي FATF وهي منظمة حكومية دولية رقابية تضع المعايير الدولية لمكافحة غسيل الأموال،

تقريرا يوجز المخاطر المختلفة التي تواجهها الشركات نتيجة أزمة كورونا كوفيد-19، التي شملت حدوث زيادة في عمليات الاحتيال، بما في ذلك انتحال هوية المسؤولين و انتشار عمليات الاحتيال الاستثمارية وزيادة الجرائم الإلكترونية، وتنامي إساءة استخدام الخدمات المالية عبر الإنترنت والأصول الافتراضية لنقل الأموال غير المشروعة وإخفائها. (Rosenstein, 2020)

- القطاع النفطي : يعد القطاع النفطي أحد أكثر القطاعات تضررا من الهجمات والجرائم الإلكترونية في ظل فيروس كورونا كوفيد-19 وخاصة في منطقة الشرق الأوسط وشمال إفريقيا، فقد تعرضت شركات عديدة في كثير من الدول مثل الولايات المتحدة الأمريكية وماليزيا وإيران وسلطنة عمان والإمارات العربية المتحدة والمملكة العربية السعودية، إلى رسائل بريد إلكتروني مخادعة لإيهام مستقبليها أنها مرسلة من شركة نفط وغاز حقيقية في مصر، وهي شركة حكومية تسمى الشركة الهندسية للصناعات البترولية والكيماوية إنبي، وسعى المخترقون إلى الحصول على تفاصيل حساسة عن الأفراد وإنتاج النفط، كي يبيعوها بعد ذلك على الإنترنت المظلم Dark Web . (مؤسسة دبي للمستقبل،2020، ص 6)
- منصات مؤتمرات واجتماعات ومحادثات الفيديو : منصات مؤتمرات واجتماعات ومحادثات الفيديو كانت من بين الأهداف المفضلة للمخترقين خلال أزمة كورونا كوفيد-19، إذ ظهرت فيها بعض الثغرات الأمنية، مثل منصة زووم Zoom، التي شهدت انضمام بعض الأشخاص عشوائيا إلى اجتماعات الفيديو وتعطيله بمحتوى غير مرغوب به، أو نشر فيديوهات مسجلة لم يتم حفظها في مساحات تخزين سحابية آمنة، وتم نشرها بعد ذلك على شبكة الإنترنت، وشمل ذلك اجتماعات عمل خاصة، ومحادثات شخصية بين عائلات وأصدقاء. (البيان الإلكتروني، 2020)
- منصات الألعاب الإلكترونية: كانت منصات الألعاب الإلكترونية بدورها هدفا للهجمات والجرائم الإكترونية خلال فيروس كورونا كوفيد-19، فعلى سبيل المثال سعى المخترقون إلى اختراق شبكة نينتدو Nintendo للحصول على معلومات مالية شخصية، مستغلين زيادة عدد الحسابات عليها، بسبب شعبية بعض ألعابها الجماعية: مثل لعبة أنيمال كروسينج Animal Crossing التي تتيح للأشخاص الاتصال ببعضهم افتراضيا، ولذا عطلت الشبكة القدرة على تسجيل الدخول إلى الحسابات من خلال معرف شبكة نينتدو Nintendo. (مؤسسة دبي للمستقبل،2020، ص 7)

وعليه نستنتج أن تركز معظم الجرائم والهجمات الإلكترونية على قطاعات محددة خلال أزمة كورونا كوفيد-19 الصحة لم يكن بمحض الصدفة، بل هو راجع إلى إدراك المجرمين والمخترقين الإلكترونيين بأن هذه القطاعات تسمح لهم أكثر من غيرها بتحقيق غايتهم الرئيسية والنهائية وتحديدا ما يتعلق بالكسب المادي.

3.4 إجراءات وردود فعل الحكومات والمنظمات والشركات على تنامي الجريمة الإلكترونية في ظل فيروس كورونا كوفيد-19 :

دفع تزايد عدد الجرائم والهجمات الإلكترونية خلال أزمة كورونا كوفيد-19 الصحية، العديد من الحكومات والمنظمات والشركات إلى الإعلان عن جملة من الإجراءات والجهود التي ستتخذها وتبذلها لمواجهة الجريمة الإلكترونية وكبحها في ظل استمرار هذه الأزمة و الواقع والتدابير التي فرضتها على البشرية جمعاء.

– منظمة الشرطة الجنائية الدولية الإنتربول : أعلن الإنتربول كرد فعل على تنامي الجرائم الإلكترونية خلال أزمة كورونا كوفيد-19 الصحية عن جملة من الإجراءات والتدابير تمثلت في : (الإنتربول، 2020، ص 2)

- إعداد برنامج الإنتربول العالمي لمكافحة الجريمة الإلكترونية.
- قيادة الإجراءات العالمية التي تتخذها أجهزة إنفاذ القانون لمكافحة التهديدات الإلكترونية التي تستغل تفشي فيروس كورونا كوفيد-19.
- تعميم نشرات بنفسجية (الغرض منها توفير معلومات عما يستخدمه المجرمون من أساليب إجرامية وأغراض وأجهزة ووسائل إخفاء) من أجل تنبيه البلدان الأعضاء إلى التهديدات الإلكترونية الجديدة والشديدة الخطورة.
- إعطاء إرشادات تقنية للمنظمات ضحية الاعتداءات الإلكترونية لمساعدتها في جهود التعافي التي تبذلها.
- التعاون مع مجموعة خبراء في مجال الأمن الإلكتروني عبر الإنترنت.
- عقد اجتماعات افتراضية في حالات الطوارئ مع الجهات المعنية منها رؤساء الوحدات الوطنية والإقليمية لمكافحة الجريمة الإلكترونية والشركاء من القطاع الخاص، من أجل تزويد البلدان الأعضاء بخدمات متكيفة مع احتياجاتها لمنع الجريمة الإلكترونية وكشفها والتحقيق فيها.

– الولايات المتحدة الأمريكية : أعلنت مجموعة من أعضاء مجلس الشيوخ الأمريكي الجمهوريين عن تقديم مشروع قانون للخصوصية ينظم البيانات التي جمعتها تطبيقات التتبع والتعقب الخاصة بأزمة كورونا كوفيد–19، وبموجب قانون حماية بيانات المستهلك خلال فيروس كورونا كوفيد–19 المطروح سيتاح للأمريكيين مزيد من الشفافية والاختيار والتحكم حول مكان وكيفية استخدام بياناتهم الشخصية. (مؤسسة دبي للمستقبل،2020، ص 9)

– أوروبا : كشفت المفوضية الأوروبية في 24 جويلية 2020 عن الاستراتيجية الجديدة للإتحاد الأوروبي بخصوص الأمن الداخلي والخارجي للفترة 2020–2025، التي من أهم الركائز والأولويات التي تضمنتها نجد الأمن الإلكتروني، حيث أعلنت المفوضية زيادة جهودها للتعامل مع العدد المتنامي من الهجمات الإلكترونية التي تزداد تعقيدا بشكل متسارع، (Nicolás, 2020) كما أكدت مفوضة الشؤون الداخلية الأوروبية يلفا يوهانسون Ylva Johansson على الحاجة الملحة لتكثيف جهود الإتحاد الأوروبي لمكافحة الجريمة الإلكترونية والدور الأساسي لليوروبول في هذه الجهود في ظل تزايد عدد الجرائم الإلكترونية بفعل فيروس كورونا كوفيد–19. (Europol, 2020)

– الصين : أكدت الحكومة الصينية على لسان تشاو ليجيان Zhao Lijian ، المتحدث باسم وزارة الخارجية الصينية أنها ستتخذ إجراءات صارمة ضد أي شكل من أشكال الجرائم والهجمات الإلكترونية وستعزز الإجراءات لحماية أمنها الإلكتروني، كما دعت إلى مزيد من التعاون الدولي لحماية الأمن الإلكتروني. (شبكة الجزيرة الإعلامية، 2020)

– الشرق الأوسط وشمال إفريقيا : أعلن مكتب الأمم المتحدة المعني بالمخدرات والجريمة لمنطقة الشرق الأوسط وشمال إفريقيا في برنامجه لمكافحة الجريمة الإلكترونية عن عدد من الإجراءات والتدابير لتعزيز قدرات دول المنطقة على مواجهة الجريمة الإلكترونية في ظل فيروس كورونا كوفيد–19 : (مكتب الأمم المتحدة المعني بالمخدرات والجريمة بالشرق الأوسط وشمال إفريقيا، 2020، ص 12)

- الارتقاء بمستوى الأمن التكنولوجي بالبنية التحتية الحيوية على المستوى الوطني.
- تطوير إجراءات التشغيل الموحدة لضمان استجابة رقمية مثلى.
- توفير تدريبات معترف بها دوليا للمستجيبين الأوائل والمسؤولين بالحكومات.
- شراء معدات طب شرعي إلكتروني لضمان كفاءة التحقيق عن الهجمات الإلكترونية في الوضع الحالي.

- تقييم الاحتياجات والتنسيق الإقليمي لتقديم الدعم.
- تحقيقات الجرائم الإلكترونية المتخصصة لمنع المزيد من الهجمات الإلكترونية.
- استجابة الطب الشرعي الإلكتروني لمواقع الجرائم المختلفة أو تتبع البيانات.
- مراجعة واستشارات تشريعية.
- دعم التعاون الدولي.
- حملات توعية بمواقع التواصل الاجتماعي عن مشكلات محددة ذات صلة بالفيروس.

– منظمة الصحة العالمية : أعلنت منظمة الصحة العالمية قيام خبراءها وعامليها التقنيين بالعمل على الحد من محاولات الاختراق التي تتعرض لها وتغيير نظامها المعلوماتي في اتجاه أكثر أمنا (مركز المستقبل للأبحاث والدراسات المتقدمة، 2020)، كما قدمت المنظمة من خلالها موقعها الإلكتروني الرسمي مجموعة من النصائح والإرشادات للمستخدمين لتجنب تعرضهم للاحتيال والخداع الإلكتروني من قبل من ينتحلون صفة المنظمة أو أحد موظفيها.

– مؤسسات الخدمات المالية : لجئت مؤسسات الخدمات المالية إلى تطبيق تقنيات الذكاء الاصطناعي وتحليلات البيانات في الوقت الحقيقي لتأسيس نظام للإنذار المبكر لمواجهة الاحتيال على معاملات بطاقات الائتمان، وقد أثبت التطبيق السليم والوقائي للذكاء الاصطناعي أهميته خلال فترة تفشي فيروس كورونا كوفيد–19، مع ارتفاع مستويات الحماية من الأنشطة الاحتيالية بمعدل 40% مقارنة بالفترة السابقة. (Oertli, 2020)

– شركة جوجل Google: أطلقت شركة جوجل Google بالتعاون مع شبكة مكافحة الجرائم الإلكترونية وهي منظمة غير ربحية تركز على مساعدة ضحايا الاحتيال عبر الإنترنت، موقعا لمساعدة المستخدمين في كشف عمليات الاحتيال التي تأخذ أشكالا متعددة مثل الفحوصات الزائفة، أو عرض اللقاحات المزيفة، أو غيرها من المعلومات الطبية المخادعة المتصلة بفيروس كورونا كوفيد–19. (محمد، 2020)

خاتمة:

تمثل الجرائم الإلكترونية تحديا حقيقيا أمام الدول والمنظمات والأجهزة المعنية بمكافحة الجريمة بأنواعها، بفعل الخصوصيات التي تتميز بها من حيث صعوبة اكتشافها وإثباتها وتتبع مرتكبيها وتجاوزها لعاملي الحدود وبعد المسافات، وفي ظل فيروس كورونا كوفيد–19 عرفت الجريمة الإلكترونية ازديادا وارتفاعا كبيرا في معدلاتها، وهو ما جعل الحكومات ومجتمعاتها في

مختلف دول العالم تواجه مشكلتين في غاية الصعوبة والتعقيد خلال وقت واحد، مشكلة كورونا كوفيد-19 وخطر الهجمات والجرائم الإلكترونية.

وقد تبين من خلال ما جاء في هذه الدراسة أن التدابير التي فرضها فيروس كورونا كوفيد-19 المتمثلة في تطبيق مبدأ التباعد الاجتماعي والعمل والتعليم عن بعد وزيادة استخدام شبكة الإنترنت وبحث الناس من خلالها على معلومات حول الفيروس المستجد وكيفية حماية أنفسهم منه، أدت كلها إلى زيادة وبشكل كبير جدا عدد الأهداف السهلة وغير المؤمنة إلكترونيا، ووفرت فرصة لا تعوض للمخترقين والمجرمين الإلكترونيين للقيام بجرائمهم وهجماتهم الإلكترونية، وهو ما حدث بالفعل، كما ظهر أيضا أن أهم القطاعات المستهدفة بالهجمات والجرائم الإلكترونية في ظل فيروس كورونا كوفيد-19 تمثلث في كل من : القطاع الصحي، القطاع المالي، القطاع النفطي، منصات مؤتمرات واجتماعات ومحادثات الفيديو ، منصات الألعاب الإلكترونية، وهذا ما نجده منطقي بالنظر إلى دوافع المخترقين والمجرمين الإلكترونين التي تعلقت أساسا بتحقيق الكسب المادي.

ورغم أن الحكومات والمنظمات والشركات لم تقف موقف المتفرج أمام تزايد عدد الهجمات والجرائم الإلكترونية خلال أزمة كورونا كوفيد-19، بل وضعت إجراءات وقائية واحترازية وأكدت مضاعفة الجهود لمكافحة هذه الهجمات والجرائم، ولكن مع ذلك فنجاح هذه الإجراءات والجهود ونجاعتها في وقف والحد من الجرائم والهجمات الإلكترونية مع استمرار فيروس كورونا كوفيد-19 والتدابير التي فرضها غير مضمون، ليس لسبب سوى لأن المجرمين والقراصنة الإلكترونيين قد أثبتوا في السابق حتى قبل ظهور الفيروس قدرتهم على التكيف والتفوق على أي إجراءات أو جهود تضعها ضدهم الدول والشركات لحماية أمنها الإلكتروني .

قائمة المراجع :

أولا- المراجع باللغة العربية:

- البقمي، ناصر، مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربية،(أبو ظبي :مركز الإمارات للدراسات والبحوث الإستراتيجية ،2008) .

- الديربي، عبد العال و صادق، محمد الجرائم الإلكترونية :دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والإنترنت،(القاهرة :المركز القومي للإصدارات القانونية، 2012).

– الحمداني، بشرى، القرصنة الإلكترونية أسلحة الحرب الحديثة،(عمان :دار أسامة للنشر والتوزيع،2014) .
– الحسيناوي، علي، جرائم الحاسوب والإنترنت،(عمان :دار اليازوري، 2008).
– المومني، نهلا، الجرائم المعلوماتية،(عمان :دار الثقافة للنشر والتوزيع، ط2، 2010).
– المزاهرة، منال، تكنولوجيا الاتصال والمعلومات،(عمان :دار المسيرة للنشر والتوزيع، 2014).
– مجمع البحوث والدراسات،الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها،(نزوى : أكاديمية السلطان قابوس لعلوم الشرطة،2016).
– مصري، عبد الصبور، التنظيم القانوني للتجارة الإلكترونية،(الرياض :مكتبة القانون والاقتصاد،2012) .
– نصار، غادة، الإرهاب والجريمة الإلكترونية،(القاهرة :العربي للنشر والتوزي، 2017).
– عطوش، ضرغام، جريمة التجسس المعلوماتي :دراسة مقارنة،(القاهرة :المركز العربي للنشر والتوزيع، 2017)
– رسلان، أيمن، الجرائم المعلوماتية في دولة الإمارات والوطن العربي،(دبي :قنديل للطباعة والنشر والتوزيع، 2016).
– لبكي، جورج، المعاهدات الدولية للإنترنت :حقائق وتحديات، مجلة الجيش اللبناني، العدد83، يناير 2013.
– الإنتربول، الاستراتيجية الشاملة لمكافحة الجريمة الإلكترونية، (ليون: الإنتربول، 2017).
– الإنتربول، التهديدات السيبرية المترتبة بكوفيد 19–في العالم،(ليون: الإنتربول،2020) .
– جامعة الدول العربية،الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، (القاهرة: جامعة الدول العربية، 2010).
– مؤسسة دبي للمستقبل، اتجاهات المستقبل: الأمن السيبراني،(دبي: مؤسسة دبي للمستقبل، 2020).
– مكتب الأمم المتحدة المعني بالمخدرات والجريمة بالشرق الأوسط وشمال إفريقيا، كوفيد–19 : تحليل التهديدات الإلكترونية، (مكتب الأمم المتحدة المعني بالمخدرات والجريمة،2020).
– مكتب الأمم المتحدة المعني بالمخدرات والجريمة ، مؤتمر الأمم المتحدة الثالث عشر لمنع الجريمة والعدالة الجنائية،(الدوحة: مكتب الأمم المتحدة المعني بالمخدرات والجريمة، 2015).

– أحمد، داليا السيد (06 سبتمبر 2020)، لماذا تصاعد خطر الهجمات الإلكترونية في ظل وباء كورونا، الرابط الإلكتروني : https://bit.ly/2SRJEvl تم الاطلاع بتاريخ :(2020/10/14).
– البيان الإلكتروني (21 جوان 2020)، دبي للمستقبل : توجهات عالمية لتعزيز الأمن الرقمي وتبني الذكاء الاصطناعي لحماية القطاعات، الرابط الإلكتروني : https://bit.ly/343ve1w تم الاطلاع بتاريخ :(2020/10/15).
– الشافعي، هايدي (12 جوان 2020)، أشكال ومعدلات الجريمة في زمن كورونا، الرابط الإلكتروني : https://marsad.ecsstudies.com/32507/ تم الاطلاع بتاريخ : (2020/10/14).
– حدادين، غيث (28 ديسمبر 2019)، الأمم المتحدة تقر تشكيل لجنة مكافحة الجرائم الإلكترونية، الرابط الإلكتروني : https://bit.ly/3734zDW تم الاطلاع بتاريخ : (2020/10/11).
– محمد، ناريمان (28 ماي 2020)، جوجل تطلق موقعا لمحاربة الاحتيال الإلكتروني، الرابط الإلكتروني: https://bit.ly/2SVwddA تم الاطلاع بتاريخ : (2020/10/16).
– مركز المستقبل للأبحاث والدراسات المتقدمة، (07 ماي 2020)، لصوص الحظر :كيف أثر منع التجول على جرائم ما بعد كورونا في الإقليم؟، الرابط الإلكتروني : https://bit.ly/3lSaWxQ تم الاطلاع بتاريخ : (2020/10/15).
– شبكة الجزيرة الإعلامية (09 أفريل 2020)، للتجسس أو الانتقام؟ القراصنة يستهدفون الصين ومنظمة الصحة العالمية، الرابط الإلكتروني: https://bit.ly/3j8mlbq تم الاطلاع بتاريخ : (2020/10/16).
– شعيب، جيهان(30 سبتمبر 2018)، بيع البيانات.. تهديد لأمن المجتمع، الرابط الإلكتروني : https://bit.ly/37gAIYI تم الاطلاع بتاريخ :(2020/10/18).
– خليفة، إيهاب (07 أفريل 2020)، الأمن المعلوماتي : لماذا تصاعدت التهديدات الإلكترونية مع انتشار كورونا، الرابط الإلكتروني : https://bit.ly/3dBwQCX تم الاطلاع بتاريخ : (2020/10/15).

ثانيا– المراجع باللغة الأجنبية :

- Interpol, Cybercrime : Covid-19 Impact, (Lyon: Interpol,2020).
- Council Of Europe. (2020, October 11). Chart Of Signatures And Ratifications Of Treaty 185 : Convention On Cybercrime, Url : https://bit.ly/3dCyOmr (Consulted 11/10/2020).
- England, R. (2020, April 20). FBI Sees Cybercrime Reports Increase Fourfold During COVID-19 Outbreak, Url :

https://www.entrepreneur.com/article/349509(Consulted 14/10/2020).
- Europol. (2020, October 05). Covid-19 Sparks Upward Trend In Cybercrime,Url : https://www.europol.europa.eu/newsroom/news/covid-19-sparks-upward-trend-in-cybercrime(Consulted 15/10/2020).
- Europol. (N.D.). European Cybercrime Centre - Ec3 : Combating Crime In A Digital Age, Url : https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3(Consulted 11/10/2020).
- Nicolás, E. (2020, July 27). EU Five-Year Security Plan To Focus On Critical Infrastructure, Url : https://euobserver.com/justice/149030(Consulted 15/10/2020).
- Oertli, K. (2020, August 20). How Digital Innovations Helped Banks Adapt During Covid-19, Url : https://www.weforum.org/agenda/2020/08/how-digital-innovations-helped-banks-adapt-during-covid-19/(Consulted 16/10/2020).
- Rosenstein, P. (2020, May 04). Covid-19 Raises Financial Crime Risks, Report Says, Url : https://www.law360.com/articles/1270188/covid-19-raises-financial-crime-risks-report-says(Consulted 15/10/2020).
- Spajic , Damjan .(2019,December 04). Cybercrime Statistics That Will Make You Change Your Password, Url : https://kommandotech.com/statistics/cybercrime-statistics/(Consulted 18/10/2020).