جرائم تقنية المعلومات وجائحة فيروس كورونا بين الواقع والمأمول: دراسة تأصيلية

د. معاذ سليمان الملا
أستاذ القانون الجنائي المساعد
كلية القانون الكويتية العالمية

الملخص

اعتقد الكثير أن هناك انخفاضًا في معدلات الجريمة مع ظهور فايروس كورونا الذي تفشى في كافة دول العالم بسبب فرض التدابير الصحية الوقائية، وهذا صحيح إلى حد ما بالنسبة للجريمة بمفهومها التقليدي، إلا أن جرائم تقنية المعلومات ازدادت معدلاتها تزامنًا مع دعوات المنظمات الدولية والسلطات الحكومية إلى اعتماد التعامل الإلكتروني بدلًا من التعامل التقليدي وأيضا فرض سياسة التباعد الاجتماعي.

نحاول في هذا البحث تحديد العلاقة بين جرائم تقنية المعلومات وجائحة فيروس كورونا المستجد وتأصيلها من خلال طرح عدة موضوعات تكشف لنا ملامح تلك العلاقة، فقمنا باستخدام المنهج التأصيلي، حيث بدأنا ببيان أهمية أدوات تقنية المعلومات ودورها خلال هذه الفترة الاستثنائية، ثم وضَّحنا كيف وظفت تلك الأدوات في خدمة الأنشطة الإجرامية، وبيان حجم خطورتها على أمن الفرد والمجتمع، وانتهينا بعرض آلية المواجهة الجزائية لهذه الأنشطة ومدى كفايتها، وأيضًا دور السلطة التنفيذية التي يناط إليها مهمة تنفيذ تلك الآلية لتحقيق حماية فعالة.

كلمات دالة: جرائم تقنية المعلومات، جائحة كورونا، التعامل الإلكتروني، المشرع، البيانات الشخصية.

المقدمة

أصبح العالم كله في تحدٍ صريح ومواجهة حقيقية ومستمرة لمحاربة فيروس كورونا المستجد (Covid-19)[1]، وهو الفيروس الذي وصفه الكثيرون بالعدو الصغير غير المرئي. وقد تضافرت الجهود العالمية والوطنية لمواجهته منذ اللحظات الأولى لظهوره من أجل الحد من آثاره الخطيرة على بني البشر، حيث راح ضحيته آلاف الأشخاص وتم تسجيل إصابات تُقدر بالملايين في العالم في ظرف شهور قليلة، مما ألزم أكثر من مليار شخص في العالم المكوث في المنازل. هذا إلى جانب تهديده للاقتصاد العالمي، بل وانهياره بسبب إيقاف بعض أهم الأعمال والأنشطة العامة والخاصة، وهو ما حدا بالعديد من الدول إلى تبني سياسة العمل عن بعد، أي الاعتماد على أدوات تقنية المعلومات وشبكة الإنترنت في إتمام الأعمال المختلفة.

أولاً: التعريف بموضوع البحث وأهميته

تبدو أهمية البحث من حيث كونه يناقش تداعيات انتشار فيروس كورونا المستجد على العالم، فهذا الفيروس دفع العديد من الدول إلى تبني سياسة إتمام الأعمال المتنوعة والأنشطة المختلفة عن بعد، وأهمها الأنشطة والخدمات التجارية والمالية التي تقدمها الحكومات والشركات الخاصة عبر التطبيقات الإلكترونية، وهذا بدوره أدى إلى ازدهار التجارة الإلكترونية.

وهذا النظام على الرغم من مميزاته المتعددة التي تتيح للأفراد تحقيق فكرة التوازن بين الحياة الشخصية والحياة المهنية، فضلاً عن مرونة الأداء وسرعة إنجاز الأعمال، إلا أن مساوئه أيضاً عديدة كونه يعتمد بشكل كبير على أدوات تقنية المعلومات، فتكون أعمال الرقابة على سلوكيات المستخدمين عموماً – سواء أكانوا موظفين أم غير موظفين – ضعيفة جداً، إذ يصعب بسط السيطرة عليها، وهو ما يثير نطاق مسؤولية القائمين على الإشراف وآلية رقابتهم على الأداء. كذلك تعتبر فكرة حماية هذه الأدوات من الناحية التقنية ضد مخاطر الاعتداءات السيبرانية المختلفة، وهي من الأمور التي ما زالت تشكل هاجساً لدى العديد من الدول.

(1) عرَّفت منظمة الصحة العالمية فيروس كورونا المستجد بأنه: «فصيلة كبيرة من الفيروسات التي قد تسبب المرض للحيوان والإنسان على حد السواء، وهي عدوى تصيب الجهاز التنفسي، وتتراوح حدته من نزلات البرد الشائعة إلى أمراض أشد وخامة مثل متلازمة الشرق الأوسط التنفسية والمتلازمة التنفسية الحادة الوخيمة (السارس)». راجع الموقع الرسمي لمنظمة الصحة العالمية على الرابط الإلكتروني التالي:
https://www.who.int/ar/emergencies/diseases/novel-coronavirus-2019/advice-for-public/q-a-coronaviruses

ثانياً: مشكلة البحث

اعتقد البعض أن تفشي جائحة فيروس كورونا المستجد في جميع أرجاء العالم أدى إلى انخفاض معدلات الجريمة التقليدية[2]، ولكن الإشكالية تكمن في أن العالم وجد نفسه أمام خانة واحدة وهي الاعتماد الكبير على أدوات تقنية المعلومات وشبكة الإنترنت، وقد رافق ذلك ارتفاع في معدلات الجريمة المرتبطة بها، فهذا الظرف مكّن المجرمين من استغلال هذه الفرصة في تنفيذ الأنشطة الإجرامية المختلفة، وهو ما يشكل تحدياً حقيقياً أمام المجتمعات البشرية لاسيما في ظل غياب التعاون الدولي لمكافحة هذا النوع من الجرائم.

وتبرز مشكلة البحث في عدم استيعاب المشرع الكويتي والأجهزة الحكومية خطورة هذه النوعية من الجرائم وتطورها المستمر على المجتمع الكويتي، خصوصاً بيانات المستخدمين الشخصية التي تعد وقوداً لجرائم تقنية المعلومات، فضلاً عن قلة الوعي لدى المستخدمين أنفسهم أثناء تعاملهم الإلكتروني، وغياب آلية تطبيق استراتيجية الأمن السيبراني خصوصاً في هذه الفترة.

ثالثاً: تساؤلات البحث

نطرح في هذا البحث عدة تساؤلات جوهرية تعتبر الإجابة عنها محددة للأهداف التي نصبو إليها، وهي كالآتي:

1. ما هو دور أدوات تقنية المعلومات وشبكة الإنترنت خلال فترة جائحة فيروس كورونا؟
2. كيف أسيئ استخدام هذه الأدوات؟ وما أسباب ذلك؟
3. ومخاطر ذلك على المستخدمين؟ وما هي ضوابط الاستخدام الصحيح لضمان تقليل تلك المخاطر؟
4. ما هو المقصود بجرائم تقنية المعلومات؟ وما هي النماذج التي برزت أثناء جائحة فيروس كورونا؟

(2) كشف تقرير عالمي نشره موقع تايم دوت كوم الأمريكي عن تراجع معدلات الجرائم في جميع أنحاء العالم مع ظهور فيروس كورونا المستجد، حيث أظهر التقرير أن فرض حظر التجول، ووقف عجلة التجارة، وإغلاق جميع المتاجر الكبرى في العديد من دول العالم أدى إلى هذا التراجع. راجع الرابط الإلكتروني:
https://fox11online.com/news/coronavirus/crime-drops-around-the-world-as-covid-19-keeps-people-inside

5. كيف واجه المشرع والأجهزة الحكومية هذه النوعية من الجرائم؟ وما مدى استيعابهما للتطور المستمر والمخيف لهذه النوعية من الجرائم؟
6. من هو المسؤول عن هذه الجرائم؟ وهل يمكن تصور الخطأ غير العمدي فيها؟
7. هل استفاد المجتمع الكويتي من استراتيجية الأمن السيبراني لعام 2017؟

رابعاً: نطاق البحث

يتحدد نطاق بحثنا من جانبين اثنين: أولهما موضوعي والآخر زمني، فمن حيث النطاق الموضوعي، فإننا سوف نلتزم بعرض مفهوم جرائم تقنية المعلومات، وذلك بعد تناول دورها الفعَّال في حياة المستخدمين ليتسنى لنا بعد ذلك استجلاء دورها السلبي وخطورتها على المستخدمين، أما من حيث النطاق الزمني، فإننا سوف نلتزم بالحديث عن بيان ازدياد جرائم تقنية المعلومات خلال فترة تفشي جائحة كورونا.

خامساً: منهج البحث

اعتمدنا في طرح الدراسة على المنهج التأصيلي، حيث عرضنا في البداية لأهمية دور أدوات تقنية المعلومات خلال فترة تفشي جائحة كورونا، ثم حددنا مصادر خطورة ذلك على المتعاملين عبر شبكة الإنترنت، وكيف استطاع المجرمون توظيف أنشطتهم الإجرامية خلال هذه الفترة، وموقف المشرع الجزائي الكويتي والأجهزة الحكومية تجاه تلك الأنشطة، وصولاً إلى النتائج والتوصيات.

ومن أجل ذلك، فقد قمنا بتقسيم خطة البحث إلى مبحثين اثنين مسبوقين بمطلب تمهيدي، وذلك على النحو الآتي:

مطلب تمهيدي: أهمية أدوات تقنية المعلومات وشبكة الإنترنت في فترة جائحة فيروس كورونا.

المبحث الأول: ملامح سوء استخدام أدوات تقنية المعلومات وشبكة الإنترنت وخطورتها وعوامل انتشارها في فترة جائحة فيروس كورونا.

المبحث الثاني: مكافحة جرائم تقنية المعلومات في التشريع الجزائي الكويتي.

مطلب تمهيدي
أهمية أدوات تقنية المعلومات وشبكة الإنترنت في فترة جائحة فيروس كورونا

لعبت أدوات تقنية المعلومات وشبكة الإنترنت دوراً مهماً خلال فترة تفشي جائحة فيروس كورونا، فهي الملاذ الآمن للأفراد خلال فترة الحظر. وفي هذا المطلب سوف نتحدث عن ارتفاع معدلات استخدام هذه الأدوات وهذا (الفرع الأول)، ثم نعرض دور أدوات تقنية المعلومات في هذه الظروف الاستثنائية (الفرع الثاني).

الفرع الأول
ارتفاع معدلات استخدام أدوات تقنية لمعلومات وشبكة الإنترنت خلال فترة الجائحة

أدت ظروف تفشي جائحة فيروس كورونا المستجد وفرض حظر التجول، وأيضاً الحجر الصحي للمصابين في معظم دول العالم إلى زيادة ملحوظة في عدد مستخدمي حركة مرور البيانات عالمياً على شبكة الإنترنت، بما في ذلك شبكات التواصل الاجتماعي، فقد تغيَّرت السلوكيات الرقمية للمستخدمين منذ بداية تفشي الجائحة، الذين اضطروا إلى التأقلم مع تلك الأدوات المتصلة بهذه الشبكات لإتمام أعمالهم وقضاء حاجياتهم.

أولاً: الأرقام على مستوى العالم

لقد أظهر تقرير الرقمية العالمية Data Reportal لشهر أبريل من عام 2020 أن عدد مستخدمي شبكة الإنترنت في العالم وصل إلى4.57 مليار مستخدم، بواقع زيادة 7% عن أبريل عام 2019، وهم يقضون وقتاً أطول بكثير على أجهزتهم، وهو أمر غير مستغرب بسبب ظروف تفشي الجائحة. فقد أشار التقرير إلى العديد من النتائج التي تدعم دراستنا، وقد أخذنا منه ما يلي[3]:

(3) اعتمد التقرير على محاور أساسية في الربع الأول من عام 2020، وهذه المحاور كان أولها يشير إلى القفزات الهائلة والكبيرة في الأنشطة الرقمية، وجاء المحور الثاني مستعرضاً نتائج استخدام شبكات التواصل الاجتماعي، فيما خصص المحور الثالث لبيان النتائج المتعلقة باستخدام تطبيقات التجارة الإلكترونية، وجاء الرابع مستعرضاً نتائج الوقت الذي يقضيه المستخدمون في الألعاب التفاعلية، وأما الخامس والأخير فكان مخصصاً لعرض بعض الفرص غير المتوقعة للمعلنين الرقميين. راجع الموقع الإلكتروني على الرابط التالي:
https://datareportal.com/reports/digital-2020-april-global-statshot

1. إن مستخدمي منصات شبكات التواصل الاجتماعي بمختلف أنواعها في ازدياد بواقع أكثر من 8% منذ أبريل 2019، حيث بلغ عدد المستخدمين في هذه الفترة 3.81 مليار.
2. ازدياد عدد مستخدمي أجهزة الهواتف المحمولة بواقع 5.16 مليار، بمعدل زيادة 128 مليون مستخدم منذ أبريل عام 2019، أي ما يقارب ثلثي إجمالي سكان العالم.
3. ازدياد استخدام البريد الإلكتروني بمعدل 30% منذ بداية مارس من عام 2020.
4. كشف التقرير أن أكثر من ثلثي مستخدمي الإنترنت الذين تتراوح أعمارهم بين 16 و64 عاماً يقضون وقتاً في ألعاب الفيديو عبر أجهزتهم، وقام المستخدمون بتحميل أكثر من 13 مليار لعبة في الأشهر الثلاثة الأولى من عام 2020، وأنفقوا نحو 17 مليار دولار.
5. ازدياد في معدل التسوق عبر شبكة الإنترنت في أنحاء العالم وفق منظومة التجارة الإلكترونية، حيث أظهر التقرير أن ثلثي مستخدمي شبكة الإنترنت يهتمون أكثر بشراء المواد الاستهلاكية والغذائية من خلال مواقع السوبر ماركت، حيث بلغ معدل نمو عدد زيارات هذه المواقع 251% فقط من 8 إلى 15 أبريل 2020.
6. شهدت العمليات عبر محركات البحث زيادة كبيرة في الموضوعات المتصلة بفيروس كورونا، فقد كان ثالث أكبر نتائج البحث يتم إدخالها عبر محركات موقع جوجل.
7. يتوقع التقرير أن يظل استخدام خدمات الاتصال المرئي وإقامة المؤتمرات عن بعد حتى بعد تفشي الجائحة خصوصاً بعد التجربة الفعلية لها، وأنها ستصبح جزءاً من بيئة الأعمال.

ثانياً: الأرقام في دولة الكويت

تعتبر دولة الكويت من بين الدول التي يشملها التقرير العالمي السالف الذكر، إلا أن نتائج ما بعد فترة تفشي الوباء تأخرت، واعتمد بيانها في بداية يناير من عام 2020 وقد أظهرت أن عدد مستخدمي شبكة الإنترنت في الكويت بلغ 4.200 مليون مستخدم في تلك الفترة. وقد ارتفع بمقدار 24 ألف مستخدم بين 2019 و2020، وبلغ معدل انتشار شبكة الإنترنت 99%.

وازداد عدد معدل مستخدمي شبكات التواصل الاجتماعي نحو 155 ألف مستخدم بين 2019– 2020 ومعدل انتشار شبكات التواصل الاجتماعي 99%. وقد بلغ عدد مستخدمي الهواتف المحمولة في الكويت 7.38 مليون مستخدم في يناير 2020، بزيادة مقدارها 317 ألفاً بين 2019 و2020 ما يعادل 174% من إجمالي عدد السكان[4].

وفيما يتعلق بعمليات التجارة الإلكترونية، فقد ازداد حجمها بعد قرار إغلاق كافة المحال والمجمعات التجارية والمطاعم والمقاهي، وحيث بلغ حجم التسوق عبر شبكة الإنترنت 1.1 مليار دولار منذ بداية تفشي الجائحة، وبلغ عدد الحسابات النشطة في هذا المجال 2.4 مليون حساب، 80% منهم لديهم حسابات مصرفية، بينهم 66% من الشباب، فيما يعتمد 36% من السكان علي الشراء عبر الإنترنت[5].

الفرع الثاني

دور أدوات تقنية المعلومات خلال

فترة تفشي جائحة كورونا

بالنظر إلى ما سبق ذكره نجد أن أدوات تقنية المعلومات وشبكة الإنترنت لعبت أدواراً مهمة جداً في حياة المجتمعات البشرية لاسيما خلال فترة تفشي جائحة كورونا التي أثرت على معظم دول العالم[6]، وما صاحب ذلك من اضطرابات وخسائر في بعض البلدان بسبب فرض حظر التجوال وتطبيق سياسة التباعد الاجتماعي، فأدوار هذه التقنية والشبكة تنسجم – وبحق – مع واقع تغير نمط الحياة التي فرضتها ثورة المعلومات والثورة الصناعية الرابعة، واعتمادنا عليها في معظم المجالات التي نمارسها بشكل اعتيادي وغير اعتيادي.

(4) للاطلاع راجع الرابط الإلكتروني التالي:
https://datareportal.com/reports/digital-2020-kuwait

(5) تقرير منشور على موقع صحيفة الأنباء الكويتية بعنوان: بالفيديو.. منصات التسوق الإلكتروني.. «طوق النجاة» للأسواق التجارية. راجع الرابط الإلكتروني التالي:
https://www.alanba.com.kw/ar/economy-news/9566892020--03-16/
بالفيديو–منصات– التسوق–الإلكتروني–طوق–النجاة–للأسواق–التجارية/

(6) Kacper Gradon, Crime in Time of the Plague: Fake news Pandemic and the Challenges to Law-Enforcement and Intelligence community. Society Register, Vol. 4 No. 2 (2020): Postmodern Society and Covid-19 Pandemic: Old, New And Scary, p. 134.
https://pressto.amu.edu.pl/index.php/sr/issue/view/1571

وما ينبغي الإشارة إليه في هذا الصدد هو أن تلك الأدوات استفادت كثيراً من تكنولوجيا الذكاء الاصطناعي والبيانات الضخمة التي دعمت مختلف المجالات[7].

نحاول في هذا الفرع بيان أبرز تلك المجالات وذلك وفق التقسيم الآتي:

أولاً: في مجال الخدمات الطبية والصحية

أسهمت أدوات تقنية المعلومات وشبكة الإنترنت في تطوير مجال الصحة وخدماتها المتنوعة خلال فترة تفشي جائحة كورونا، فنجد أن أدوات تقنية المعلومات على قدر ما مكَّنت هذا المجال من تجميع البيانات والمعلومات من خلال أجهزة الحاسب الآلي وأجهزة التشخيص، فإنها تسهم الآن وعبر تقنيات الذكاء الاصطناعي في تطوير برامج أبحاثها المتنوعة لتتبع انتشار فيروس كورونا من خلال أجهزة تساعد في تشخيص حالة المصابين والمرضى وتطهير المناطق، وأيضاً تسريع عملية إيجاد اللقاح المناسب للحد من انتشاره[8].

ومن الأمثلة المشهودة تطبيقات الهاتف الجوال والسوار الإلكتروني لتتبع المصابين، والروبوت الممرض الذي استعانت به بعض المستشفيات في الصين وإيطاليا للحد من انتشار الفيروس بين الأطقم الطبية. هذا إلى جانب ما تمكنه شبكة الإنترنت من إتاحة المعلومات للجمهور للاستفادة منها في الجانب التوعوي الذي تقدمه الشبكات الطبية عن بعد في جميع أنحاء العالم.

ثانياً: في مجال الأمن ومكافحة الجريمة

تبرز أهمية أدوات تقنية المعلومات وشبكة الإنترنت في مجال الأمن ومكافحة الجريمة من خلال ما تحتويه أنظمتها من قواعد بيانات، يتم تجميعها وتحليلها لدعم القرارات الأمنية،

(7) الذكاء الاصطناعي(Artificial Intelligence :AI) هو طريقة لصنع آلة أو برنامج يتم التحكم بها بواسطة الحاسوب، ويمكن تدريبها وتعليمها لتقوم بأشياء بشكل أفضل وأسرع وأدق مما يفعله الإنسان في الوقت الحالي، ويعتبر الإنسان الآلة (I-Robot) النموذج الأكثر تطبيقاً في واقع الحال، والذكاء الاصطناعي وتطبيقاته المتعددة لا تعمل إلا من خلال تغذيتها بالبيانات الضخمة (Big Data) أي دعمها بكميات ضخمة من المعلومات الشخصية والمهنية التي يمكن تحليلها للكشف عن الأنماط والاتجاهات والأحوال التي تتعلق بسلوك الإنسان وتفاعله من خلال أنشطته المختلفة. وهذا يعني أن البيانات نتاج تراكمي يومي لما يتركه الأفراد من محتويات عبر أدوات تقنية المعلومات وشبكة الإنترنت كالبيانات الشخصية والتعليقات الخاصة بهم، وإلى غير ذلك مما اعتاد ممارسته المستخدمون. للمزيد من التفاصيل، انظر: عبد الله موسى ود.أحمد حبيب بلال، الذكاء الاصطناعي ثورة في تقنيات العصر، ط1، 2019، المجموعة العربية للتدريب والنشر، القاهرة، ص16-113. وانظر حول ذلك أيضاً لدى:
Jerry Kaplan, Artificial Intelligence - What everyone needs to know, Oxford University Press, USA, 2016, Pp1-2 and Pp. 117-118.

(8) عبد الله موسى، ود. أحمد حبيب بلال، مرجع سابق، ص88.

ودعم قنوات المعرفة العلمية والتنبؤ بالمخاطر المستقبلية، وتعزيز الجانب الوقائي ورصد المخالفين والمجرمين وحماية الأنظمة المعلوماتية، وغير ذلك من أدوار مهمة تضمن فعالية حماية المجتمع من داء الجريمة[9]. والسؤال هنا كيف يمكن استفادة المنظومة الأمنية من هذه الأدوات خلال فترة تفشي جائحة كورونا؟

تظهر الاستفادة من استخدام أدوات تقنية المعلومات في تطبيقات الكشف عن مخالفة حظر التجوال عبر أجهزة الهواتف المحمولة، وأيضاً استخدام قبعات أو خوذ تكشف المصابين عن بعد وقد استخدمتها الصين ودولة الإمارات، كذلك تمت الاستفادة منها في توجيه التحذيرات للأشخاص عبر الطائرات المسيرة.

ثالثاً: في مجال التجارة والخدمات

على الرغم مما تسببت به الظروف الحالية من أزمة حادة على الاقتصاد العالمي، وانهيار في أسواق الأوراق المالية، وإغلاق شركات ومؤسسات بسبب تفشي هذا الوباء، إذ يتصور الخبراء الاقتصاديون والماليون أن الاقتصاد العالمي لن يتعافى منها بسرعة، فاضطر الأفراد في معظم دول العالم إلى تغيير سلوكهم وعلى نطاق واسع[10] نحو التجارة الإلكترونية، التي انتعشت في ظل هذه الظروف، فأصبح الأفراد أمام واقع التعامل الإلكتروني لإتمام عمليات التسوق عن بعد والدفع وإجراء العمليات المصرفية والتحويلات المالية وغيرها.

وما يميز هذا الانتعاش أن البضائع التي يقبل عليها المتسوقون تتعلق بالظروف الاستثنائية لجائحة كورونا كشراء مستلزمات الوقاية كالكمامات والقفازات، وأيضاً المواد والمكملات الغذائية. هذا إلى جانب تطور صناعة هذه المستلزمات والأجهزة الطبية، وأيضاً المنافسة الحادة بين شركات الأدوية لصناعة لقاح مضاد للفيروس.

---

(9) تتبع الأجهزة الأمنية أسلوباً جديداً لإنفاذ القانون ومواجهة مختلف التهديدات الإجرامية، وقد أطلق عليها حديثاً وصف الشرطة الاستخباراتية. للمزيد من التفاصيل، انظر: د. ممدوح عبد الحميد عبد المطلب، الشرطة الاستخباراتية – العمل الشرطي القائم على الذكاء الاصطناعي وتحليل المعلومات، ط1، دار النهضة العربية، القاهرة، 2019، ص26 وما بعدها. وانظر أيضاً:

Jerry H. Ratcliffe, Intelligence-Led Policing, Willan Publishing, USA and Canada, 2008, p. 6.

(10) Adam King, The impact of COVID-19 on user behaviour and ecommerce, 31st March 2020.
https://www.ayima.com/blog/the-impact-of-covid-19-on-user-behaviour-and-ecommerce.html

رابعاً: في مجال الإعلام والصحافة

استفادت أجهزة الإعلام والصحافة من أدوات تقنية المعلومات في نقل المحتوى المعلوماتي وبثه أو نشره من أي مكان في العالم وبأسرع وقت ممكن، فضلاً عن اتخاذ المواقع الإلكترونية وشبكات التواصل الاجتماعي منصات لها للتفاعل مع الجمهور سواء بشكل مباشر أو غير مباشر، من خلال تحميل المحتوى الإخباري أو المادة الإعلامية على شبكة الإنترنت وهي كما يصفها البعض بالإعلام الجديد أو الإعلام الإلكتروني، فقد باتت هذه المنصات تحديداً الوسيلة المؤثرة على الأحداث اليومية، حيث أتاحت للأفراد إنشاء هويتهم الافتراضية لنقل أفكارهم ومناقشة مختلف قضاياهم[11].

وقد أسهمت أجهزة الإعلام والصحافة منذ بدء انتشار جائحة كورونا في رصد الأخبار المتعلقة بالفيروس وتفشيه في كافة دول العالم، حيث سخرت أدوات تقنية المعلومات ومنصات شبكة الإنترنت لضمان سرعة نقل تلك الأخبار ونشرها وبثها على نطاق واسع إلى الجمهور في أقاصي العالم، فضلاً عن إسهاماتها في نشر التوعية بمخاطر هذا الوباء والتدابير الصحية اللازمة للتعامل مع هذه الجائحة.

(11) دينا عبد العزيز فهمي، الحماية الجنائية من إساءة استخدام مواقع التواصل الاجتماعي: دراسة مقارنة، ط1، دار النهضة العربية، القاهرة، 2018، ص38 وما بعدها؛ د. علي بن عبد الله الكلباني، الشائعات وخطرها في ظل وسائل الإعلام الجديد، ط1، عالم الكتب، القاهرة، 2017، ص105.

المبحث الأول

ملامح سوء استخدام أدوات تقنية المعلومات وشبكة الإنترنت في فترة تفشي جائحة كورونا

في ظل ظروف تفشي وباء كورونا التي برزت فيها أهمية أدوات تقنية المعلومات وشبكة الإنترنت على النحو السالف ذكره، ظهرت أيضاً ملامح سوء استخدامها، وذلك على النحو الذي يفسر مدى عمق هذه المشكلة.

ولذلك خصصنا هذا المبحث لعرض أهم الأنشطة غير المشروعة خلال فترة تفشي الجائحة وسوف يكون موضوعاً للمطلب الأول، ثم بعد ذلك نستجلي الأسباب المؤدية إليها ومدى خطورتها على أمن الأفراد والمجتمعات في المطلب الثاني.

المطلب الأول

المقصود بسوء استخدام أدوات تقنية المعلومات وشبكة الإنترنت ومظاهرها خلال فترة تفشي جائحة كورونا

ما بدا لنا في هذه الظروف الاستثنائية التي تمر بها دول العالم أجمع ومواجهتها المصيرية لتداعيات تفشي جائحة كورونا، بروز الكثير من المظاهر المعبرة عن سوء استعمال هذه الأدوات.

نحاول في هذا المطلب عرض أهم تلك المظاهر التي تجتمع على استغلال خوف الأشخاص وقلقهم في ظل هذه الظروف ولكن بعد الوقوف على المقصود بسوء استخدام أدوات تقنية المعلومات وشبكة الإنترنت.

الفرع الأول

سوء استخدام أدوات تقنية المعلومات وشبكة الإنترنت ومستقبل أخلاقيات التحكم فيها

من الضرورة بمكان أن نطرح في دراستنا مسألة أخلاقيات استخدام أدوات تقنية المعلومات وشبكة الإنترنت خاصة أن حديثنا سينسحب فيما بعد نحو بيان مسؤولية مستخدمي هذه الأدوات أثناء تفشي وباء كورونا وفرض الحظر، وكيف أن ذلك أدى إلى

ارتفاع نسبة استخدام هذه الأدوات وصاحبها ارتفاع الجريمة عبرها، وهو ما يحتاج إلى تفسير علاقة الإنسان بهذه الآلة من زاوية الأخلاق.

أولاً: سوء الاستخدام تعبير عن التعارض مع القواعد الأخلاقية للاستخدام الصحيح

ما ينبغي إدراكه أن أخلاقيات استخدام أدوات تقنية المعلومات وشبكة الإنترنت إنما تشير إلى حكم استخدام الإنسان لها فيما لو كان استخداماً سيئاً أم حسناً، فالقاعدة التي نعرفها كلما كانت أخلاق المستخدم حسنة كان استخدامه للأداة نافعاً له ولمجتمعه، والعكس صحيح إذا كانت أخلاق المستخدم سيئة كان استخدامه ضاراً عليه وعلى مجتمعه.

ويعني ذلك أن الاستخدام ما هو إلا انعكاس حقيقي لسلوك المستخدم ذاته أي انعكاس لطبيعة البشر وتعاملهم مع أدوات تقنية المعلومات، فعبارة «أنها سلاح ذو حدين» هي إشارة واضحة إلى سلوك المستخدم في كيفية استخدامه لتلك الأدوات. فقد جبلت غريزة البشر على توظيف كل المخترعات أو المبتكرات الجديدة لخدمة غاياته غير المشروعة، ومن بينها أدوات تقنية المعلومات وشبكة الإنترنت التي وضعت البشرية أمام جملة من التحديات الأمنية والقانونية التي تعيق ضبط الفوضى الإلكترونية.

وقد وصف البعض الوضع الذي نعيش فيه بغير المستقر في الفضاء الإلكتروني وأنه مع اعتماد الإنسان على هذه الأدوات وانتشار الجريمة والخطر المستمر عبرها ما سيقودنا إلى انهيار إلكتروني بسبب الانحراف في الاستخدام[12]، إذ يصعب بسط سيطرة فعلية أو حقيقية على أداء المستخدمين لعدم وجود آلية رقابية واضحة على استخدامهم لهذه الأدوات، بحيث تشعرهم بمسؤوليتهم تجاه أنفسهم أو تجاه غيرهم ممن يتعاملون معهم أثناء استخدام تلك الأدوات، ومعنى ذلك أن نطاق البحث في الأخلاقيات المرتبطة ببيئة استخدام تقنية المعلومات وشبكة الإنترنت يكون في ثلاثة مجالات نوردها على النحو الآتي:

1. أخلاقيات المستخدم مع نفسه

أي سلوك المستخدم وأخلاقه مع نفسه عند استخدامه لأدوات تقنية المعلومات وشبكة الإنترنت، فواجبه الأخلاقي إما أن يقوده إلى حسن استخدام تلك الأدوات، وعلى النحو الذي ينفع فيه نفسه ولا يضرها، فيكون رقيباً على ذاته، أو أن تقوده أخلاقه إلى ارتكاب

(12) نديم منصوري، موضوعات في علم اجتماع الإنترنت والتواصل الرقمي، ط1، منتدى المعارف، بيروت، 2019، ص47 وما بعدها. وانظر أيضاً:

Joseph Migga Kizza, Ethical and Social Issues in the Information Age, 6th ed., Springer International Publishing, 2017, p. 9.

سلوكيات تتعارض مع قواعد الأخلاق والقانون بصرف النظر عن غايته التي قد تقتصر عند البعض على التسلية مما قد يعرض نفسه للمسؤولية الاجتماعية والقانونية.

2. أخلاقيات المستخدم مع غيره

أي سلوك المستخدم مع من يحيطون به من أشخاص بصرف النظر عن مدى صلته بهم، فهذه الأدوات جعلت الأشخاص يُكوّنون علاقات على الرغم من التباعد الجغرافي أو كما يمكن وصفه بالعلاقات الافتراضية، لذلك يتحتم على المستخدم احترام حقوقهم التي يسهل على البعض انتهاكها مستغلاً ما لهذه الأدوات من إمكانيات عديدة يستطيع بها المرء اختراق أدق تفاصيل حياتهم كحقهم في الخصوصية وحقهم في الكرامة.

3. أخلاقيات المستخدم مع الأداة

أي سلوك الإنسان المستخدم مع الأداة أو الآلة التي يصممها أو يصنعها أو يعالجها من أجل خدمته، فمازال الإنسان حتى يومنا هذا يسعى في أبحاثه إلى تطوير تلك الأدوات عن طريق برمجتها بتكنولوجيا الذكاء الاصطناعي، بحيث تكون ذاتية التحكم أي تتصرف كما يتصرف البشر، فظهرت لنا العديد من الاختراعات على رأسها الروبوت والطائرات دون طيار وغيرها من مخترعات قابلة لأن يتم توظيفها لخدمة الإنسان أو الإضرار به.

ثانياً: الأخلاقيات في بيئة تكنولوجيا الذكاء الاصطناعي

نظراً لعدم وجود مسار دولي متفق عليه بشأن تطوير أدوات تقنية المعلومات وشبكة الإنترنت بشكل ينظم الخارطة الإلكترونية، انتهجت بعض الدول كدول الاتحاد الأوروبي على سبيل المثال وضع استراتيجية لاستخدام تكنولوجيا الذكاء الاصطناعي لتطوير برامج وتطبيقات أنظمة المعلوماتية بمختلف أنواعها وأشكالها، وقد وضعت المفوضية الأوروبية مبادئ توجيهية نشرتها في أبريل 2019، حيث حددت المفوضية الأوروبية أربعة مبادئ أخلاقية إرشادية تستوجب أن يكون البشر هم المتحكمون بها، وليس الآلة ذاتها سنوردها بالترتيب على النحو الآتي[13]:

1. مبدأ احترام الاستقلال الذاتي للإنسان

يقرر هذا المبدأ ضرورة التزام منتجي هذه الأنظمة ومطوريها بمعايير الديمقراطية وسيادة القانون، واحترام حقوق الأشخاص بتمكينهم من ممارسة أنشطتهم دون أي

(13) Independent High -level Expert Group on Artificial Intelligence (AI-HLEG) set up by The European Commission, Ethics Guidelines for Trustworthy AI, European Commission, Brussels, p.11-13.
https://ec.europa.eu/digital-single-market/en/artificial-intelligence

إجبار أو قيد يتعارض مع تلك المعايير.

2. مبدأ منع الضرر

يقرر هذا المبدأ وجوب عدم تسبب أنظمة الذكاء الاصطناعي في الإضرار بالأشخاص سواء في البيئة الشخصية أو حتى في بيئة العمل، فهذه الأدوات يجب أن تكون ضامنة لسلامتهم وحمايتهم من أي تجاوزات تنال من كراماتهم. وينصرف الأمر أيضاً إلى حماية البيئة والكائنات الحية. ويستلزم ذلك أن يكون التطوير تم على أيدي فرق لديها الخبرة والمعرفة في مجال أتمتة الأنظمة، ويجب تعريف المستخدمين بالمخاطر التي يتضمنها النظام وآلية الحد من أثرها لضمان تحقيق المساءلة والشفافية.

3. مبدأ العدالة والإنصاف

يقرر هذا المبدأ أن يكون استخدام أنظمة الذكاء الاصطناعي وتطويرها ضامناً للتوزيع العادل للفوائد والتكاليف في المستوى المعيشي، وضامناً لعدم التحيز والتمييز بين الأفراد وبلوغ العدل المجتمعي، وضامناً أيضاً لتعزيز تكافؤ الفرص في التعليم والسلع والخدمات والتكنولوجيا. لذلك يجب أن تكون هذه الأنظمة مدربة على احترام التناسب والتنافس بين الوسائل وغاياتها.

4. مبدأ القابلية للتفسير

يقرر هذا المبدأ ضرورة تفسير عمليات أنظمة الذكاء الاصطناعي من أجل بناء ثقة المستخدمين فيها، فينبغي أن تكون هذه العمليات شفافة وواضحة من حيث نتائج هذه العمليات والمصطلحات المستخدمة في تلك العمليات، بحيث تمكن المتضررين من الاستفسار عن القرارات الخطأ أو غير الدقيقة التي اتخذتها أنظمة الذكاء الاصطناعي حتى يمكن للمتضرر الطعن عليها.

تعتبر إمارة دبي النموذج العربي الوحيد الذي وضع مبادئ وإرشادات واضحة لاستخدام تكنولوجيا الذكاء الاصطناعي، وهي مشابهة تماماً للمبادئ التوجيهية الأوروبية، حيث تقرر ضرورة أن تكون أنظمة الذكاء الاصطناعي أنظمة عادلة، وتطبق الشفافية وخاضعة للمساءلة وقابلة للفهم[14].

مما تقدم نجد أن فكرة سوء استخدام أدوات تقنية المعلومات وشبكات الإنترنت أمر يتصل بالفرد ذاته وليس بالأدوات أو الآلة، فالأخيرة ما هي إلا وسائل اجتماعية مساعدة

(14) راجع الموقع الإلكتروني لدبي الذكية:
https://www.smartdubai.ae/ar/initiatives/ai-principles-ethics

ومؤثرة في الوقت ذاته إما بالنفع أو الضرر، وذلك بحسب الكيفية التي يراها المستخدم، وبالتالي يمكن تعريف هذه الحالة على أنها: استعمال المستخدم أدوات تقنية المعلومات وشبكة الإنترنت، سواء مع ذاته أو مع غيره أو مع الآلة، بشكل يتعارض مع القواعد الأخلاقية للاستخدام السليم الذي صنعت أو خصصت من أجله.

الفرع الثاني

مظاهر سوء الاستخدام في فترة تفشي جائحة كورونا

يظهر لنا مما سبق أن الإنسان بصفته مستخدماً أو مبرمجاً للأداة هو المسؤول عن تصرفاته أثناء استخدام أدوات تقنية المعلومات وشبكات الإنترنت. والسؤال الذي نطرحه في هذا الفرع هو ما هي مظاهر سوء استعمال هذه الأدوات أثناء تفشي جائحة كورونا ؟

هناك مظاهر عديدة سيئة كان لأدوات تقنية المعلومات دورٌ بارزٌ فيها أثناء تفشي جائحة كورونا سوف نتناولها على النحو الآتي:

أولاً: الترويج لمستلزمات الصحة الوقائية والدوائية المقلدة عبر شبكة الإنترنت

في الوقت الذي أصبحت فيه المجتمعات البشرية بحاجة إلى مستلزمات الوقاية الصحية وسعي الشركات العالمية إلى إنتاج لقاح مضاد للفيروس، استغل البعض النقص الشديد في تلك المستلزمات، حيث قام مجرمون بصناعة مستلزمات مقلدة تتعارض مع معايير السلامة الصحية والدوائية، وذلك بغية جني أرباح طائلة من خلال بيعها للأشخاص عبر المواقع الإلكترونية ومنصات شبكات التواصل الاجتماعي.

وقد أظهر تقرير الشرطة الدولية (الإنتربول) أن مواقع إلكترونية تبيع منتجات طبية غير مشروعة وكمامات مقلدة منتشرة على شبكة الإنترنت ومنصات التواصل الاجتماعي[15].

(15) استطاعت أجهزة إنفاذ القانون للشرطة الدولية (الإنتربول) ضبط كمامات مقلدة ومستحضرات تعقيم لليدين غير مستوفية لمعايير السلامة وأدوية مضادة للفيروسات وهي مستلزمات غير مرخصة، وتبين وجود روابط إعلانية إلكترونية عديدة عبر شبكة الإنترنت ومواقع التواصل الاجتماعي تبيع هذه المواد تحت مسمى منتجات متصلة بكوفيد 19، وقد تم حذف أكثر من 2500 رابط يحيل إلى مواقع إلكترونية وصفحات على وسائل التواصل الاجتماعي وأسواق إلكترونية أخرى تعلن عن هذه المستلزمات عبر هذه القنوات. راجع الموقع الإلكتروني للإنتربول على الرابط التالي:
Interpol Report, Global operation sees a rise in fake medical products related to COVID-19,19 March 2020.
https://www.interpol.int/en/News-and-Events/News/2020/Global-operation-sees-a-rise-in-fake-medical-products-related-to-COVID-19

هذا إلى جانب ما قام به البعض من استغلال رفع أسعار المستلزمات على الأشخاص في الأسواق التقليدية والإلكترونية، وقد لاحظنا ذلك في العديد من الدول ومنها الكويت.

ثانياً: الهجمات الإلكترونية المختلفة عبر شبكة الإنترنت

إن اندفاع مستخدمي أدوات تقنية المعلومات نحو شراء مقتضياتهم عبر شبكة الإنترنت ومنصات شبكات التواصل الاجتماعي، وما يستلزم ذلك بطبيعة الحال من ضرورة إدخال البيانات الشخصية للمستخدمين، بما في ذلك أرقام بطاقاتهم الائتمانية لإتمام إجراءاتهم، وأيضاً تنامي بيئة الأعمال والمؤتمرات عن بعد في القطاعات العامة والخاصة في بعض البلدان واعتمادهم على التراسل الإلكتروني كتطبيق لفكرة التباعد الاجتماعي[16]، أسهم في تعريضهم لهجمات إلكترونية مختلفة[17]، كالاحتيال أو التصيد الإلكتروني وهجمات البرامج الخبيثة واختراقات الأنظمة وغيرها، حيث زادت هذه المخاطر خلال فترة تفشي الجائحة، وتعتبر شبكة الإنترنت الخفي نافذة حقيقية لتلك الاعتداءات[18].

وقد حذرت هيئة شبكة الإنترنت للأسماء المعروفة بـ «الآيكان» من انتشار هذه الأنشطة خصوصاً في هذه الفترة، فقد تم رصد ما يقرب 100 ألف موقع إلكتروني تحت أسماء نطاقات مرتبطة بألفاظ مرتبطة بحاجة كورونا[19].

---

(16) Chi Tran, Recommendations for Ordinary Users from Mitigating Phishing and Cybercrime Risks During COVID-19 Pandemic, Security Research Blog, Writeups , P1. https://ctrsec.io/index.php/12/02/2020/cve-2020-8962-d-link-dir-842-stack-based-buffer-overflow/

(17) بيَّنت «آيكان» في تقرير لها أنه في شهر مارس 2020 فقط، تم تسجيل 100 ألف موقع إلكتروني جديد على الأقل تحت أسماء نطاقات تشمل كلمات مثل «كوفيد» و«كورونا» و«فيروس». راجع الرابط الإلكتروني التالي: تقرير-يحذر-تنامي-الاحتيال-الالكتروني-زمن-كورونا
www.skynewsarabia.com/varieties/1334977-

(18) الإنترنت الخفي إما أن يكون عميقاً وإما أن يكون أعمق، وقد أطلق عليه وصف المظلم، وشبكة الإنترنت الخفي تمثل ما نسبته 90 إلى95%، بينما الشبكة العامة أو الظاهرة التي نستخدمها تشكل الجزء المتبقي أي 5 إلى 10% فأين نحن من هذا العالم وكيف نواجه الأنشطة الإجرامية الخفية، للمزيد من التفاصيل انظر: نديم منصوري، مرجع سابق، ص52. وانظر أيضاً: وليد بن صالح، الإنترنت المظلم والعملات الافتراضية، مجلة كلية القانون الكويتية العالمية، ملحق خاص، أبحاث المؤتمر السنوي الدولي الخامس (الجزء الثاني)، العدد3، أكتوبر 2018، ص 389 وما بعدها. يشير خبراء تقنيون إلى أن هذه الشبكة ساهمت في الأنشطة الإجرامية خلال فترة تفشي جائحة كورونا، انظر هذا التقرير:
IntSights Defend forward, The Cyber Threat Impact of COVID-19 to Global Business, p. 2.

(19) للاطلاع على مزيد من طبيعة وأنواع الهجمات الإلكترونية منذ بداية تفشي جائحة كورونا وتطورات هذه الهجمات، راجع الرابط الإلكتروني التالي:
https://cyware.com/blog/live-updates-covid-19-cybersecurity-alerts-b313

ثالثاً: بث وتداول الشائعات عبر شبكة الإنترنت

الشائعات سلاح لإشعال الحرب النفسية وهي ليست بالأمر الجديد، بل ظلت جزءًا مهماً لها عبر عقود، وقد اكتسبت هذه الظاهرة زخمًا جديدًا في ظل ثورة تكنولوجيا المعلومات التي زادت خطورتها على أمن واستقرار المجتمعات، وتعتبر شبكات التواصل الاجتماعي المنصة الأمثل لتنفيذ مثل هذه الحرب، نظراً لاتساع نطاقها الذي يشمل دول العالم جميعها، حيث تنطلق الشائعات بمجرد بثها على الشبكة ليتم تداولها بنطاق واسع[20]. وهذا الاتساع بطبيعة الحال يرجع إلى إمكانية إنشاء الحسابات الوهمية، إلا أنه ومنذ تفشي هذه الجائحة وانتشار حالة من الذعر والهلع لدى المجتمعات البشرية، استطاع صانعو الشائعات – وبما يحملونه من دوافع سياسية أو مالية أو اجتماعية أو نفسية – استخدام وسائل التواصل الاجتماعي على وجه التحديد في الترويج للأكاذيب والمعلومات المضللة[21]، سواء تعلقت هذه الأكاذيب والمعلومات المضللة بالوباء ذاته، أو الظروف المحيطة به، أو القرارات التي تتخذها السلطات بشأن تدابير مواجهته.

رابعاً: استغلال البيانات الشخصية

البيانات الشخصية هي كل ما يحدد هوية الشخص وسماته، بحيث يجعلها قابلة للتحديد بشكل مباشر أو غير مباشر، سواء في بيئته التقليدية أو الإلكترونية كالاسم والرقم المدني وفصيلة الدم والديانة والبريد الإلكتروني والصور والمقاطع وإلى غير ذلك مما يخصه، فالبيانات الشخصية تعد وقوداً – إن جاز التعبير– للثورة الصناعية الرابعة، نظراً لأهميتها في تغذية الأنظمة الإلكترونية بمختلف أنواعها، فهي جزء من البيانات الضخمة وداعم رئيسي لأنظمة الذكاء الاصطناعي في الآلات الحاسوبية[22].

والجدير ذكره أن الطرق التي استخدمت فيها البيانات الضخمة في أوروبا وبرزت أثناء فترة تفشي كورونا لتنفيذ الخطط الاستراتيجية، ولتتبع المصابين وتقديم المشورة للأفراد عموماً والمصابين خصوصاً[23]، وهذه الطرق اتبعتها بعض دول العالم لمواجهة

(20) علي بن عبد الله الكلباني، مرجع سابق، ص129 وما بعدها.

(21) Kacper Gradon, op, cit, P136.

(22) سامي عبد الصادق، البيانات الشخصية .. الصراع على نفط القرن الحادي والعشرين، كراسات استراتيجية، العدد 287، المجلد رقم27، أبريل 2018، مركز الدراسات السياسية والإستراتيجية، القاهرة، ص12 وما بعدها. وانظر إيهاب خليفة، الذكاء الاصطناعي: ملامح وتداعيات هيمنة الآلات الذكية على حياة البشر، دراسات المستقبل، العدد 6 أبريل 2019، أبو ظبي، دولة الإمارات العربية المتحدة، ص 8 وما بعدها. وانظر حول ذلك أيضاً لدى:

Jerry Kaplan, Op. Cit., p. 117.

(23) J. Scott Marcus, Big data versus COVID-19: opportunities and privacy challenges, 23 March 2020. Blog post.
https://www.bruegel.org/2020/03/big-data-versus-covid-19-opportunities-and-privacy-challenges/

جائحة كورونا ورصد حالات الإصابة.

وقد أصبح المستخدمون في ظل فترة تفشي الجائحة محاطين بأساليب الجذب الاختياري للانضمام والتمتع بالخدمات المتنوعة للتطبيقات كالاشتراك على سبيل المثال في موقع زوم لعقد الاجتماعات والمؤتمرات عن بعد أو غيرها من تطبيقات، أو الانضمام جبراً لفئة محددة من المستخدمين وهم المصابون بالوباء أو من هم تحت قيد التقصي الوبائي لتنزيل تطبيقات المراقبة والتتبع عن بعد كالسوار الإلكتروني أو استخدام الخوذة الذكية لرصد الحالات، خصوصاً مع غياب آلية تنفيذ التشريعات المنظمة لهذه المسائل، مما يطرح مشكلة تتعلق بمدى سريان التشريعات الإلكترونية لحماية المتعاملين على الرغم مما تفرضه سلطات الدول من إجراءات استثنائية تتطلب معالجة البيانات الشخصية للجمهور.

إلى جانب ذلك أساء البعض استغلال التطبيقات الإلكترونية التي تجيز للمستخدمين الخروج أثناء فترات حظر التجوال الكلي أو الجزئي لقضاء أعمالهم الضرورية كالذهاب إلى المستشفى أو التسوق في الجمعيات التعاونية، أو غير ذلك مما هو مصرح به من قبل السلطات الحكومية من خلال الولوج إلى الموقع الإلكتروني والحصول على التصريح، إلا أنه يخالف التعليمات بالذهاب إلى موقع على خلاف طلبه.

المطلب الثاني

المخاطر المترتبة على سوء استخدام أدوات تقنية المعلومات وشبكة الإنترنت والبحث في أسبابها

مما لا شك فيه أن سوء استخدام أدوات تقنية المعلومات وشبكة الإنترنت ينجم عنه مخاطر عديدة على حقوق ومصالح الآخرين، وهذه المخاطر تختلف باختلاف الأسباب الناشئة عنها.

وفي هذا المطلب نحاول تحديد تلك المخاطر في الفرع الأول، ثم بعد ذلك نحدد أسباب نشوء تلك المخاطر خلال فترة تفشي جائحة كورونا وهذا هو الفرع الثاني.

الفرع الأول

المخاطر المترتبة على سوء استخدام أدوات تقنية المعلومات وشبكة الإنترنت

إن المخاطر التي تنجم عن سوء استخدام أدوات تقنية المعلومات وشبكة الإنترنت تعتبر تهديداً حقيقياً لمصالح المستخدمين أنفسهم والمجتمع على حد سواء، بل وتمتد أيضاً إلى

المصالح الأساسية المتعلقة بالدولة. لذلك سنقوم بتحديد أهم المخاطر التي لا تختلف عن الوضع الطبيعي ولكنها برزت بشكل أكبر وأخطر أثناء فترة تفشي جائحة كورونا.

أولاً: مخاطر على مصالح المستخدمين

إن جميع الأشخاص معرضون للمخاطر في البيئة الافتراضية، وهذا أمر مسلمٌ به طالما كانوا يتعاملون عبر بياناتهم الشخصية، فالأشخاص المصابون أو المشتبه بهم معرضون للاعتداء على حقهم في الخصوصية بسبب تتبعهم جغرافياً ومراقبتهم عن طريق السوار الإلكتروني، فضلاً عن مطالبتهم بتصوير أنفسهم في أماكن العزل، كذلك استخدام الخوذة الرقمية التي أظهرت في ميادين العمل الأمني مخاوف كثيرة على معالجة بيانات الأشخاص دون موافقتهم، هذا إلى جانب تعرضهم لسرقة بياناتهم المصرفية نتيجة تعاملاتهم الإلكترونية المستمرة عبر تطبيقات الهاتف المحمول أو البريد الإلكتروني.

كذلك فإن هؤلاء معرضون للاحتيال الإلكتروني باتخاذ المجرمين أساليب الهندسة الاجتماعية للإيقاع بضحاياهم لاسيما الأطفال منهم، وبالنسبة للبالغين فإن الجناة ينتهجون الاحتيال البصري من خلال استغلال العلامة التجارية[24]. كذلك استغلال حاجات الناس وخوفهم ببيعهم مستلزمات تتعارض مع معايير السلامة الصحية.

هذا إلى جانب وجود مشكلات كثيرة ينم بعضها عن جهل المستخدمين أنفسهم لبعض الأمور التقنية اللازمة أو الضرورية لتأمين أجهزتهم من الاختراق، وجهل البعض لأخلاقيات التعامل فيها.

ثانياً: مخاطر على مصالح المجتمع

ما ينعكس على الأفراد ينعكس تماماً على مصالح المجتمع الذي يعيشون فيه، ومن المخاطر التي برزت أثناء تفشي الجائحة وعانت منها أيضاً دول العالم مشكلة إطلاق الشائعات وتداولها بين الأفراد خصوصاً عبر تطبيقات التواصل الاجتماعي، فقد كانت الأخبار الكاذبة والمعلومات المضللة التي يتم تداولها عبر شبكات التواصل الاجتماعي، والتي تتناول رصد الإصابات وحالات الوفيات ومصدر الفيروس وطرق انتشاره وطرق العلاج والوقاية من مصادر غير موثوقة، وذلك عبر مقاطع مصورة أو عبر رسائل نصية.

(24) سعى بعض الباحثين إلى وضع بعض الإرشادات الفنية التي تسهم في التخفيف من عمليات الاحتيال الإلكتروني عبر شبكة الإنترنت خلال الحجر الصحي، للمزيد من التفاصيل انظر:
Chi Tran, Op. Cit., p. 3.

كذلك تداول الأخبار المتعلقة بنقص المواد الغذائية في الأسواق، والعجز عن توفيرها يخلق نوعاً من الفوضى بين الجمهور، ومن ثم تزاحمهم في الأسواق والمراكز التجارية بسبب تعليقات يبثها البعض على غير هدى.

ثالثاً: مخاطر على مصالح الدولة

مصالح الدولة الأساسية وأمنها ليسا بمنأى عن الأضرار في هذه الفترة، خصوصاً وأن بعض الأعمال تغيَّرت في هذه الفترة وأصبحت تنفذ عن بعد وأعمال أخرى أوقفت للحد من تفشي الوباء بين الجمهور، فتداول تلك المحتويات عبر وسائل التواصل الاجتماعي من شأنه أن يقوِّض تلك المصالح كالأمن الغذائي على سبيل المثال، فعلى الرغم مما تقوم به السلطات الحكومية من جهود في توفير المواد التموينية أو الأمن الوقائي بشأن توفير الكمامات والقفازات الصحية أو غير ذلك من وجوه الأمن، فإننا نجد بالمقابل تعليقات ومقاطع تنتشر عن نقص هذه المواد وعلى النحو الذي يخلق فيه فوضى بين الجمهور.

والحال كذلك بالنسبة للأمن الصحي وتوفير مستلزمات الوقاية الصحية للجمهور، ناهيك عن تأثير ذلك على من هم في الصفوف الأمامية من موظفين ومتطوعين، فقد يثير هذا المحتوى حالة من الخوف لديهم فيؤدي إلى العزوف عن العمل وعدم الإخلاص في أدائه.

وفي الأمن السيبراني، نجد أن المنظومة التقنية مهددة بالاختراقات من قبل الهاكرز ومثلها اختراق نظام حجز المواعيد، وعلى صعيد الأمن الخارجي نجد مدى تأثير المحتوى المعلوماتي على العلاقات بين الدول، إذ عمد البعض إلى استغلال شبكات التواصل الاجتماعي لإشعال الفتن بين الشعوب بسبب الجاليات العاملة في الدولة.

الفرع الثاني

أسباب نشوء المخاطر خلال فترة جائحة فيروس كورونا

نلتمس مما سبق أن خطورة سوء استعمال أدوات تقنية المعلومات وشبكة الإنترنت النابعة من الأفراد أولاً وآخراً تتمثل في طبيعة المحتوى المعلوماتي الذي يتم بثه وتداوله فيما بينهم على نطاق واسع خصوصاً في هذه الفترة التي تعاني منها المجتمعات البشرية، فما هي الأسباب التي يمكن التعويل عليها في نشوء هذه المخاطر؟

وهناك أسباب كثيرة يمكن التعويل عليها في نشوء هذه المخاطر، إلا أننا سنكتفي بإيراد الأسباب التي برزت لنا خلال فترة تفشي الجائحة، وهي تطبيق حظر التجوال، وعدم تقدير المسؤولية لدى المستخدمين.

أولاً: فرض حظر التجوال

لجأت معظم دول العالم إلى تطبيق حظر التجوال كإجراء يحد من تفشي جائحة كورونا بين الجمهور، وحظر التجوال عبارة عن إجراءات تفرضها سلطات الدولة على الجمهور في منطقة أو مناطق معينة، بحيث تلزمهم بالبقاء في البيوت وحظر خروجهم بشكل كلي أو جزئي، إلا بموجب تصريح محدد يتيح الخروج لبعض العاملين في القطاعات الحيوية أو الخروج لشراء الاحتياجات أو لمراجعة طبية أو غير ذلك مما تحدده السلطات.

وعلى الرغم من أن فرض هذا الحظر يهدف إلى حماية الجمهور من خطر إصابتهم بعدوى الفيروس لاسيما بعد إعلان منظمة الصحة العالمية عن سرعة انتقال الوباء بين الجمهور، إلا أن فرضه حمل معه أيضاً مخاطر كثيرة من بينها سوء استخدام أدوات تقنية المعلومات وشبكة الإنترنت كونها الأدوات التي بدأ جميع المستخدمين في كافة أنحاء العالم يعتمدون عليها في القيام بأنشطتهم المختلفة أثناء فترة الحظر.

ثانياً: عدم الشعور بالمسؤولية خلال فترة تفشي الجائحة

خلال فترة تفشي الوباء ظهرت بعض السلوكيات التي تعكس عدم شعور المستخدمين بالمسؤولية تجاه الكثير من الأمور، ومن بينها بطبيعة الحال أخلاقيات تعاملهم مع أدوات تقنية المعلومات وشبكة الإنترنت، فبعض الأشخاص سواء المختصصون أو غير المختصصين يسارعون إلى تفسير الوباء وطرق العلاج وكيفية الوقاية وإلى غير ذلك من محتوى يقومون بنشره على نطاق واسع عبر تسجيل مصور أو عبر رسائل نصية، لتتضارب بعد ذلك الرؤى لدى من يصلهم المحتوى، وليتم تفسيرها على نحو يختلف عن الواقع.

كذلك تداول المحتوى المعلوماتي الذي يصل من مصادر مجهولة عبر شبكات التواصل الاجتماعي دون تأكد المستخدمين من فحواه، أو على الأقل التحقق من مصدر هذا المحتوى قبل إعادة نشره أو بثه للآخرين، وخطورة ذلك كما قلنا تقع على جهود السلطات الحكومية والعاملين في الصفوف الأمامية.

وينصرف الأمر أيضاً إلى المستخدمين الذين يجهلون بعض الجوانب الفنية ومخاطر هذا الجهل بسبب نقل مواد احتيالية أو الانضمام إلى حسابات مشبوهة أو عدم القدرة على إدارة المجموعات أو الإدلاء ببيانات شخصية غير صحيحة عن طريق تعبئة البيانات الشخصية في الموقع الإلكتروني الخاص بمنح تصاريح الحظر وإلى غير ذلك مما قد يلقي على عاتق المستخدمين مسؤوليات أثناء تعاملهم مع أدوات تقنية المعلومات.

هذا إلى جانب مسؤولية السلطات الحكومية في ضمان احترام حقوق وحريات المستخدمين في البيئة الإلكترونية، ونقصد بذلك البيانات الشخصية للأشخاص المصابين بالفيروس والخاضعين للتقصي الوبائي، وأيضاً العائدين من خارج الكويت والمتعافين من الفيروس، فهؤلاء ملزمون بوضع سوار إلكتروني أثناء فترة الحجز المنزلي وعبر تطبيق «شلونك» في أجهزة الهواتف المحمولة، ويطلب منهم عند تسجيل بياناتهم إرسال صورهم (سيلفي- مباشرة) للتأكد من موhقعهم ويحقق بعدها فريق من صحة هذه الصورة ومطابقتها بواسطة جهاز يبدو أنه مدعم بتكنولوجيا الذكاء الاصطناعي[25].

ويظهر ذلك جلياً في تجربة استخدام السلطات الأمنية خوذة لرصد الحالات المصابة مباشرة، حيث تقيس حرارة أجسام الأشخاص على بعد مسافة معينة[26]، وليس ذلك فحسب؛ بل إن هذه الخوذ يمكن استخدامها في عملية رصد المخالفين من خلال تزويدها بقاعدة بيانات عنهم كالصور والأسماء والأوصاف.

(25) انظر تقريراً بعنوان: «(شلونك).. تطبيق إلزامي للعائدين من الخارج لمراقبة المحجورين ومتابعة المخالطين»، وكالة الأنباء الكويتية (كونا)، نشر على الموقع الإلكتروني للوكالة بتاريخ 2020/4/19، الرابط التالي:
https://www.kuna.net.kw/ArticleDetails.aspx?id=2886637&language=ar

(26) انظر تقريراً بعنوان: «خوذة ذكية لرجال الأمن لكشف قائدي المركبات المُصابين»، صحيفة السياسة، نشر بتاريخ 2020/5/19. راجع الرابط التالي:
al-seyassah.com/ خوذة-ذكية-لرجال-الأمن-لكشف-قائدي-المركبات/

المبحث الثاني
المواجهة الجزائية لجرائم تقنية المعلومات
أثناء فترة تفشي جائحة كورونا

تتطلب المواجهة الجزائية تجريم سوء استخدام أدوات تقنية المعلومات وشبكة الإنترنت، وقد ساير فيها المشرع الكويتي التشريعات العقابية الأخرى في مواجهة جرائم تقنية المعلومات، وذلك من خلال مجموعة من القوانين بعضها تقليدي وبعضها الآخر مستحدث[27].

من هذا المنطلق فقد خصصنا هذا المبحث للتعريف بهذه الجرائم في التشريع الجزائي الكويتي وأنواعها للوقوف على مدى كفاية مواجهتها في التشريعات المعمول بها في الكويت.

المطلب الأول
جرائم تقنية المعلومات أثناء تفشي جائحة كورونا

فيما سبق أكدنا على أن ارتفاع جرائم تقنية المعلومات خلال فترة تفشي الجائحة كان بسبب اعتماد الأشخاص على أدوات تقنية المعلومات وشبكة الإنترنت في إتمام معاملاتهم المختلفة لاسيما أثناء فترة حظر التجوال.

وسوف نحاول تحديد المقصود بهذه الجرائم، ثم بعد ذلك تحديد الأنواع التي ظهرت خلال فترة تفشي الجائحة.

الفرع الأول
مفهوم جرائم تقنية المعلومات ومدى استيعاب تطورها

اختلف الفقهاء خصوصاً في بلداننا العربية بشأن مصطلح ومفهوم الجرائم المرتبطة

(27) واجه المشرع الكويتي جرائم تقنية المعلومات من خلال قوانين موجودة ضمن المدونة الجزائية في التشريع الكويتي كقانون إساءة استعمال أجهزة الاتصالات الهاتفية وأجهزة التنصت وتعديلاته الصادر سنة 2001 وقانون المطبوعات والنشر الصادر سنة 2006 وقانون الاعلام المرئي والمسموع الصادر 2007، ثم أصدر مؤخراً قوانين مستحدثة تدعم تلك القوانين وهي: قانون التعاملات الإلكترونية الصادر سنة 2014، وقانون إنشاء هيئة تنظيم الاتصالات الصادر سنة 2014، وقانون مكافحة جرائم تقنية المعلومات الصادر سنة 2015، وقانون الإعلام الإلكتروني الصادر سنة 2016.

بتقنية المعلومات، حيث تمايزت مصطلحاتهم وتعريفاتهم ضيقاً واتساعاً[28]، وهذا الاختلاف لا يزال قائماً حتى يومنا هذا.

وسنسعى في هذا الفرع إلى تحديد مفهوم جرائم تقنية المعلومات في التشريع الجزائي الكويتي، ثم بعد ذلك نحاول استيعاب مدى تطور هذه النوعية من الجرائم لاسيما بعد ظهور تكنولوجيا الذكاء الاصطناعي كمطور لأداء أدوات تقنية المعلومات.

أولاً: مفهوم جرائم تقنية المعلومات في التشريع الجزائي الكويتي

تحت وصف الجريمة المعلوماتية عرَّف المشرع الكويتي هذه الجرائم في إطار المادة الأولى من القانون رقم 63 لسنة 2015 بشأن مكافحة جرائم تقنية المعلومات، بأنها: «كل فعل يرتكب من خلال استخدام الحاسب الآلي أو الشبكة المعلوماتية، أو غير ذلك من وسائل تقنية المعلومات بالمخالفة لأحكام هذا القانون».

وهذا المسلك غير محمود في حقيقة الأمر كون المشرع قيَّد من نطاق هذه الجرائم، واختزلها في دور الوسيلة في حين أن هذه النوعية من الجرائم أوسع نطاقاً بالنظر إلى الأدوار التي تُؤدي إلى ارتكاب الجريمة، ونلمس هذا القصور في إيراد المشرع مصطلحات عديدة في المادة ذاتها تدخل ضمن نطاق هذه الجرائم سوف نشير إليها لاحقاً.

ومن ناحيتنا فإننا نميل إلى إطلاق مصطلح جرائم تقنية المعلومات على هذه النوعية من الجرائم كونه يستوعب حتى التطور الذي سيلحق بطبيعة هذه الجرائم كما سوف نرى،

(28) مازال الفقه يسعى إلى ضبط مصطلح ومفهوم يتماشيان مع طبيعة الجرائم المرتبطة بتقنية المعلومات، فبالنسبة للمصطلح فمازالت الألفاظ التي يطلقها البعض تتناثر بين الجرائم الإلكترونية والجرائم المعلوماتية والجريمة السيبرانية وإلى غير ذلك من مصطلحات أخرى، والحال كذلك بالنسبة للمفهوم فقد تعددت التعريفات التي تضيق تارة وتتسع تارة أخرى، والحقيقة أن مرجع الاختلاف العميق هو تاريخي أي منذ ظهور الحاسب الآلي كانت المصطلحات والمفاهيم تتماشى مع طبيعة التقنية في هذه الحقبة، ثم اختلفت المصطلحات والمسميات مع ظهور شبكة الإنترنت. انظر: د. علي عبود جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة: دراسة مقارنة، ط1، مكتبة زين الحقوقية، بيروت، 2013، ص75 وما بعدها؛ أسامة أحمد المناعسة وجلال محمد الزعبي، جرائم تقنية نظم المعلومات الإلكترونية: دراسة مقارنة، ط2، دار الثقافة للنشر، عمان، الأردن، 2014، ص66 وما بعدها. وانظر في الفقه المقارن:

Johannes Xingan Li, Cyber Crime and Legal Countermeasures: A Historical Analysis, International Journal of Criminal Justice Sciences (IJCJS), Official Journal of the South Asian Society of Criminology and Victimology (SASCV), July–December 2017, Vol. 12 (2), p. 196; P. Sai Sheela and Nitika Sharma and Bhanu Bharadwaj, Cyber Crime Definition - challenges and the cost, International Journal of Computer & Mathematical Sciences (IJCMS), Volume 3, Issue 2 April 2014, p. 34; Paul Day, Cyber Attack - The truth about digital crime, cyber warfare and government snooping, Carlton Books, UK, 2014, p. 2.

وقد اجتهدنا بتعريفها أنها: «مجموعة من الأنشطة الإيجابية والسلبية التي تكون فيها وسائل تقنية المعلومات أداة لارتكاب الأنشطة الإجرامية أو بيئة لها أو هدفاً لها»[29].

فهذا التعريف يتوافق مع طبيعة هذه الجرائم وخصوصيتها، فمن حيث طبيعتها سنجد أن هذا التعريف ينظر إلى جميع الأدوار التي يمكن أن تتحقق بها الجريمة، سواء من حيث كونها وسيلة؛ أي إذا كانت أدوات تقنية المعلومات وسيلة لتنفيذ الأنشطة الإجرامية، وهي في ذلك تتقارب مع الجرائم التقليدية كجريمة الشائعات على سبيل المثال، أو من حيث كونها بيئة حاضنة للجريمة ونقصد بذلك المحتوى المعلوماتي، الذي يتم تثبيته في أدوات تقنية المعلومات، أو على المواقع والحسابات في شبكة الإنترنت والتي يسهل للمستخدمين تحميلها وتداولها وإتاحتها للغير من ذلك مثلاً جرائم الاحتيال الإلكتروني، أو من حيث كونها هدفاً لتنفيذ النشاط الإجرامي كجريمة اختراق الأنظمة المعلوماتية أو جريمة نشر الفيروسات.

ويمكن تحقق كل هذه الأدوار في واقعة أو بالأحرى جريمة واحدة، كتحميل مادة معلوماتية خبيثة من شبكة الإنترنت على الحاسب الآلي، وإعادة نشرها لاصطياد مستخدمين. ويستوي بعد ذلك أن تكون هذه الجريمة من قبيل الجرائم الواقعة على الأفراد أو على الأموال أو على أمن الدولة، كما يستوي تصنيف هذه الجرائم إلى مستحدثة أو تقليدية.

وفيما يتعلق بخصوصية هذه النوعية من الجرائم، فلو تمعنَّا قليلاً سنجد أن جرائم تقنية المعلومات إنما ترتكز على المحتوى المعلوماتي، سواء أكان هذا المحتوى يتعلق بمصلحة يحميها القانون كالحق في الصورة أو الحق في الملكية، أم كان مادة تخضع للتجريم كالمحتوى الفاضح أو الجنسي.

ثانياً: تطور جرائم تقنية المعلومات

تتميز هذه النوعية من الجرائم بأنها قابلة للتطوير المستمر، فقد استعان المجرمون في دعم أنشطتهم بتكنولوجيا الذكاء الاصطناعي، فالآن لسنا في زمن نتحدث فيه عن جريمة إلكترونية أو جريمة معلوماتية، أو غيرها من مصطلحات لا تتواكب مع التطور التقني الذي نلحظ مؤشراته في أنشطة نجدها تطورت، وأصبحت ذكية بسبب تكنولوجيا الذكاء الاصطناعي، فهي تسهم في تنفيذ الجريمة تحت شعار الآلة وليس البشر فحسب[30]؛ أي

(29) معاذ سليمان الملا، التعليق على أحكام القانون رقم63 لسنة 2015 بشأن مكافحة جرائم تقنية المعلومات، ط1، لجنة التأليف والتعريب، مجلس النشر العلمي، جامعة الكويت، 2019، ص42.

(30) Thomas C. King and Nikita Aggarwal and Maria rosaria Taddeo and Luciano Floridi, Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions, Science and Engineering Ethics, Springer, 2020, p. 90. DOI: 10.1007/s11948-018-00081-0

أن الآلة سترتب نشاطاً إجرامياً دون أي تدخل من الإنسان ذاته[31].

فقدرة هذه التكنولوجيا على تعليم الآلة عن طريق ضخ البيانات الضخمة وتخزينها لضمان استيعاب أكبر قدر ممكن من الأنماط السلوكية المختلفة، بحيث يسهل للآلة وخوارزمياتها قراءة هذه الأنماط لتتمكن الآلة من الاختيار والتنبؤ بالأحداث دون تدخل الإنسان، ونلاحظ ذلك حينما استعان علماء الطب في الصين وبعض البلدان المتقدمة بهذه التكنولوجيا من أجل إيجاد الحلول المناسبة للحد من تفشي جائحة كورونا كاستخدام هذه التكنولوجيا في إيجاد التركيبة الدوائية المناسبة لعلاج كورونا.

ومع ذلك يرى الخبراء في مجال الذكاء الاصطناعي أنه إذا كان من الممكن الاستفادة من هذه التكنولوجيا في تقديم حلول مفيدة، فإن هناك من يستعين بها في ارتكاب جرائم عديدة، فالأمر كما يصفه بالبعض أشبه بالسباق بين الخير والشر للفوز في المعركة[32].

ويمكن للجناة الاعتماد على هذه التكنولوجيا وإعادة توجيه أنشطتهم الإجرامية المختلفة في عمليات الاحتيال الإلكتروني إذ للنظام المدعم بهذه التكنولوجيا مراقبة رسائل البريد الإلكتروني الشخصية للمستخدمين المستهدفين، وتحليل أنماط سلوكهم لاكتشاف طريقة ما لاستهدافهم. وبالتالي يمكن أن تصل البرامج الضارة المستندة إلى إرسال الرسائل من الحسابات الشخصية لتقليد سلوك المستخدم، وفي أسوأ الأحوال، لن يشك المستخدم البسيط أبدًا في أن المحادثة تتم من خلال برنامج شات بوت وسوف يرسل معاملة، ويشارك في أوراق اعتماد بطاقته الائتمانية وأنواع أخرى من المعلومات المالية الشخصية.

ويمكن أيضاً لتكنولوجيا الذكاء الاصطناعي اكتشاف طريقة نقل البيانات من الكاميرات والميكروفونات في الأجهزة لتصبح حالة تجسس إلكتروني تخترق أدق تفاصيل الخصوصية من خلال تتبع المستخدم[33].

---

(31) أثار فقهاء القانون الجنائي منذ زمن ليس ببعيد مشكلة المسؤولية الجزائية إذا ارتكب النشاط الإجرامي بواسطة الآلة. للمزيد من التفاصيل حول هذا الموضوع راجع:

Jerry Kaplan, Op. Cit., p.105; Gabriel Hallevy, Liability for Crimes Involving Artificial Intelligence Systems, Springer, USA, 2015, p. 1.

(32) Thomas C. King and Nikita Aggarwal and Maria rosaria Taddeo and Luciano Floridi, Op. Cit., p. 91. See also: Roman Zhidkov, The Future Impact of AI on Cyber Crime, 14 Feb 2020.
https://becominghuman.ai/the-future-impact-of-ai-on-cyber-crime-f9659cf354a6

(33) Roman Zhidkov, Op. Cit.; Thomas C. King and Nikita Aggarwal and Maria rosaria Taddeo and Luciano Floridi, Op. Cit., p. 94.

وهذا الأمر يضعنا أمام احتمالية الخطر المستمر أو الدائم للهجوم السيبراني، كوننا أصبحنا نعتمد وباستمرار على أدوات تقنية المعلومات وشبكة الإنترنت في القيام بجميع أعمالنا المختلفة خصوصاً في فترة تفشي جائحة كورونا، فالحكومات الإلكترونية التي لم تدرك – حتى الآن– أنها بحاجة فعلاً إلى أن تُطوّر من أدائها لتكون حكومة ذكية عن طريق دعم أنظمتها بتكنولوجيا الذكاء الاصطناعي لحماية أنظمتها الآلية، والتنبؤ بالمخاطر المستقبلية التي يمكن أن تهدد مصالحها الأساسية، والأمر كذلك بالنسبة للشركات والمؤسسات والبنوك وغيرها التي لم تعتمد أيضاً هذه التكنولوجيا في حماية أنظمتها المعلوماتية وقواعد البيانات المخزنة فيها، أو في السحابة الإلكترونية لرصد المخاطر السيبرانية التي يمكن أن تتعرض لها.

وينصرف الأمر أيضاً إلى المستخدم نفسه فعلى الرغم من صعوبة تنبؤه بالمخاطر المحدقة به، إذ ينبغي عليه أن يحرص قدر المستطاع في تعاملاته عبر تلك الأدوات لأنه موضع رصد لنمطه الذي يكون مدخلاً لوقوع ضرر عليه مستقبلاً.

الفرع الثاني

أهم النماذج الإجرامية التي ظهرت أثناء فترة تفشي كورونا

استناداً إلى ما ذكرناه آنفاً، فإن أكثر الأنشطة الإجرامية التي تمت عبر أدوات تقنية المعلومات وشبكة الإنترنت أثناء تفشي جائحة كورونا هي الآتي:

أولاً: جريمة الاحتيال الإلكتروني

عرَّف المشرع الكويتي الاحتيال الإلكتروني في إطار المادة الأولى من القانون رقم 63 لسنة 2015 بشأن مكافحة جرائم تقنية المعلومات، بأنه: «التأثير في نظام إلكتروني مؤتمن أو نظام معلوماتي إلكتروني أو شبكة معلوماتية أو مستند أو سجل إلكتروني أو وسيلة تقنية المعلومات أو نظام أو جهاز حاسب آلي أو توقيع إلكتروني أو معلومات إلكترونية، وذلك عن طريق البرمجة أو الحصول أو الإفصاح أو النقل أو النشر لرقم أو كلمة أو رمز سري أو بيانات سرية أو خاصة أخرى، بقصد الحصول على منفعة دون وجه حق أو الإضرار بالغير».

وقد نص عليها المشرع في البند الخامس من المادة (3) على أنه: «يعاقب بالحبس مدة لا تجاوز ثلاث سنوات وبغرامة لا تقل عن ثلاثة آلاف دينار ولا تجاوز عشرة آلاف دينار، أو إحدى هاتين العقوبتين..5– كل من توصل عن طريق الشبكة المعلوماتية أو باستخدام وسيلة من وسائل تقنية المعلومات إلى الاستيلاء لنفسه أو لغيره على مال أو مستند أو

توقيع على مستند، وذلك باستعمال طريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة متى كان ذلك من شأنه خداع المجني عليه.

فهذا السلوك وفقاً لما ورد في النص قائم على فكرة خداع النظام أو الشبكة، وخداع المستخدمين أيضاً للاستيلاء على أموالهم أو منافع أخرى دون وجه حق. وبالفعل استطاع الجناة استغلال هذه الأدوات في تنفيذ أنشطتهم إما عن طريق إرسال روابط إلكترونية، أو إنشاء حسابات وهمية تبيع المستلزمات الطبية والأدوية المزورة[34].

ومن أنشطة الاحتيال التي ظهرت خلال فترة تفشي وباء كورونا أيضاً قيام بعض الحسابات بعرض شاليهات للتأجير، وذلك من خلال عرض صور ومقاطع ملتقطة للجمهور عبر موقع إلكتروني وبعد الاتفاق على الاختيار يتم إرسال رابط للدفع الإلكتروني ليفاجأ من دفع بأن الموقع قد تم تأجيره لعدة أشخاص.

وقد اعتبر المشرع الكويتي هذه الجريمة عمدية، وهي من قبيل الجنح المعاقب عليها بالحبس والغرامة أو بإحدى هاتين العقوبتين[35].

وهذا النشاط أيضاً مُجرَّم في إطار المادة (37/أ) من القانون رقم 20 لسنة 2014 بشأن المعاملات الإلكترونية، حيث نصت على أنه: «مع عدم الإخلال بأي عقوبة أشد منصوص عليها في قانون آخر يعاقب بالحبس لمدة لا تزيد على ثلاث سنوات وبغرامة لا تقل عن خمسة آلاف دينار ولا تزيد على عشرين ألف دينار أو بإحدى هاتين العقوبتين كل من: .. أ- تعمد الدخول بغير وجه حق إلى نظام المعالجة الإلكترونية أو عطل الوصول إلى هذا النظام أو تسبب في إتلافه أو حصل على أرقام أو بيانات ائتمانية أو غيرها من البطاقات الإلكترونية لاستخدامها للحصول على أموال الغير».

ثانياً: جريمة الدخول غير المشروع

إن النفاذ المتعمد غير المشروع لأجهزة أو أنظمة أو شبكة معلوماتية أو موقع إلكتروني، يُعد من أقدم الأنشطة الإجرامية، ويتحقق هذا السلوك باختراق الأنظمة بالوسائل ذاتها، سواء بشكل جزئي أو كلي أو كان لغرض تحقيق أمر معين من دون تفويض أو تجاوزه.

وهذا السلوك- كما أشرنا سابقاً - تحقق فعلاً في الكويت من خلال حادثة اختراق نظام تصاريح الخروج في فترات الحظر. وقد ميَّز المشرع في هذه الجريمة بين

(34) Insights Defend forward, Op. Cit., pp. 23-.

(35) معاذ سليمان الملا، مرجع سابق، ص85 وما بعدها.

صورتين بسيطة وأخرى مشددة[36]، أما الصورة البسيطة وهي جريمة الدخول غير المشروع دون أي مقاصد يحملها الجاني سوى الدخول للنظام، وهي من قبيل الجنح وقد أدرجها المشرع في المادة (2) من القانون رقم 63 لسنة 2015 بشأن مكافحة جرائم تقنية المعلومات، التي نصت على أنه: «يعاقب بالحبس مدة لا تجاوز ستة أشهر وبغرامة لا تقل عن خمسمائة دينار ولا تجاوز ألفي دينار أو بإحدى هاتين العقوبتين، كل من ارتكب دخولاً غير مشروع إلى جهاز حاسب آلي أو إلى نظامه أو إلى نظام معالجة إلكترونية للبيانات أو إلى نظام إلكتروني مؤتمن أو إلى شبكة معلوماتية. فإذا ترتب على هذا الدخول إلغاء أو حذف أو إتلاف أو تدمير أو إفشاء أو تغيير أو إعادة نشر بيانات أو معلومات، فتكون العقوبة الحبس مدة لا تجاوز سنتين والغرامة التي لا تقل عن ألفي دينار ولا تجاوز خمسة آلاف دينار أو بإحدى هاتين العقوبتين. فإذا كانت البيانات أو المعلومات شخصية تكون العقوبة الحبس مدة لا تجاوز ثلاث سنوات والغرامة التي لا تقل عن ثلاثة آلاف دينار ولا تجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين».

أما الصورة المشددة فقد اعتبرها المشرع من قبيل الجنح تارة، ومن قبيل الجنايات تارة أخرى، وقد أدرجها في المادة (3/1) من القانون ذاته، حيث نصت على أنه: «يُعاقب بالحبس مدة لا تجاوز ثلاث سنوات وبغرامة لا تقل عن ثلاثة آلاف دينار ولا تجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين كل من: 1- ارتكب دخولاً غير مشروع إلى موقع أو نظام معلوماتي مباشرة أو عن طريق الشبكة المعلوماتية، أو بإحدى وسائل تقنية المعلومات بقصد الحصول على بيانات أو معلومات حكومية سرية بحكم القانون. فإذا ترتب على هذا الدخول إلغاء أو حذف أو إتلاف أو تدمير أو إفشاء أو تغيير أو إعادة نشر بيانات أو معلومات، تكون العقوبة الحبس مدة لا تجاوز عشر سنوات والغرامة التي لا تقل عن خمسة آلاف دينار ولا تجاوز عشرين ألف دينار أو بإحدى هاتين العقوبتين. ويسري هذا الحكم على البيانات والمعلومات المتعلقة بحسابات عملاء المنشآت المصرفية..».

ولاحظنا أن هذا النشاط مُجرَّم أيضاً في إطار المادة (37/أ) من القانون رقم 20 لسنة 2014 بشأن المعاملات الإلكترونية المشار إليها سابقاً. لذلك يمكن القول بأن هذا السلوك هو أحد أهم نماذج جرائم تقنية المعلومات، حيث إنه بوابة لأنشطة إجرامية أخرى كتزوير المستندات أو إتلافها أو الاطلاع على المعلومات أو إفشائها، أو غير ذلك من الأنشطة التي تعقب الدخول إلى النظام المعلوماتي.

وقد نص المشرع في المادة (11) من قانون مكافحة جرائم تقنية المعلومات، على إنزال عقوبة الحبس أو الغرامة التي يحكم بها عن نصف حدها الأقصى إذا اقترنت هذه الجرائم أو غيرها بأفعال تتصل بالعصابات المنظمة.

(36) معاذ سليمان الملا، مرجع سابق، ص71 وما بعدها.

ثالثاً: جريمة نشر الشائعات عبر شبكات التواصل الاجتماعي

الشائعات في بيئة تقنية المعلومات وشبكة الإنترنت عبارة عن مجموعة من المعلومات أياً كان شكلها (صورة، صوت، نص، مقطع مسجل)، تتضمن أخباراً صحيحة أو غير صحيحة أو الاثنين معاً تناقش موضوعات تتصل بأنشطة عديدة يمارسها أفراد المجتمع في مجالات الحياة العادية كالمجال السياسي والمجال الاقتصادي والمجال الاجتماعي والمجال الثقافي والمجال الديني وإلى غير ذلك من مجالات أخرى، وتصدر هذه المعلومات من جهات مجهولة أو معلومة ولكنها غير موثوقة عن طريق وسائل متعددة، من بينها وسائل التواصل الاجتماعي، ويكون من شأنها أن تؤثر على الرأي العام.

والشائعات – كما ذكرنا سابقاً – من بين المظاهر السلبية والخطيرة في آن واحد على الأمن بكافة مستوياته، وقد ظهرت خطورتها بشكل أوضح خلال فترة تفشي الجائحة عبر وسائل التواصل الاجتماعي.

وقد جرَّم المشرع الكويتي نشر الشائعات عبر أدوات تقنية المعلومات وشبكة الإنترنت في إطار المادة (15) من القانون رقم 31 لسنة 1970 بشأن تعديل بعض أحكام قانون الجزاء الكويتي الصادر سنة 1960، فقد نصت هذه المادة على أنه: «يعاقب بالحبس المؤقت الذي لا تقل مدته عن ثلاث سنوات كل كويتي أو مستوطن في الكويت أذاع عمداً في الخارج أخباراً أو بيانات أو إشاعات كاذبة أو مغرضة حول الأوضاع الداخلية للبلاد، وكان من شأن ذلك إضعاف الثقة المالية بالدولة أو هيبتها واعتبارها، أو باشر بأية طريقة كانت نشاطاً من شأنه الإضرار بالمصالح القومية للبلاد».

رابعاً: جريمة التزوير الإلكتروني

أثناء فترات الحظر لاحظنا قيام بعض المستخدمين بالحصول على تصريح للخروج أثناء فترات الحظر الكلي والجزئي سواء كان مصدر التصريح وزارة التجارة أو وزارة الداخلية بالتنسيق مع هيئة المعلومات المدنية، وذلك للذهاب إلى الأماكن المحددة حصراً في التطبيق أو الموقع الإلكتروني المخصص بإصدار تلك التصاريح، ليتضح بعد ذلك قيام بعضهم وعلى خلاف الحقيقة بزيارة أقاربه أو أي مكان آخر غير الوجهة التي قام بإدخالها بالتطبيق، وعلى النحو الذي يخالف فيه عمداً تعليمات السلطات الحكومية التي بدورها ألزمت المصرح لهم بضرورة التسجيل في الوجهات التي تم تحديدها.

والسؤال هنا هل يمكن اعتبار هذا السلوك تزويراً إلكترونياً كون ما قام به المستخدم عمداً بإدخال بيانات على خلاف الحقيقة وفي غير ما هو ما صرح له؟

نص البند الثاني من المادة (3) من القانون رقم 63 لسنة 2015 بشأن مكافحة جرائم تقنية المعلومات على أنه: «يعاقب بالحبس مدة لا تجاوز ثلاث سنوات وبغرامة لا تقل عن ثلاثة آلاف ولا تجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين كل من: ...2- زوَّر أو أتلف مستنداً أو سجلاً أو توقيعاً إلكترونياً أو نظام معالجة إلكترونية للبيانات أو نظام إلكتروني مؤتمن أو موقعاً أو نظام حاسب آلي أو نظاماً إلكترونياً بطريق الاصطناع أو التغيير أو التحوير أو بأي طريقة أخرى، باستخدام وسيلة من وسائل تقنية المعلومات. فإذا وقع التزوير على مستند رسمي أو بنكي أو بيانات حكومية أو بنكية إلكترونية تكون العقوبة الحبس مدة لا تجاوز سبع سنوات وبغرامة لا تقل عن خمسة آلاف دينار ولا تجاوز ثلاثين ألف دينار أو بإحدى هاتين العقوبتين».

إلى جانب ذلك جرَّم المشرع التزوير الإلكتروني في البندين (ج) و(د) من المادة (37) من قانون المعاملات الإلكترونية رقم 20 لسنة 2014، التي نصت على أنه: «مع عدم الإخلال بأي عقوبة أشد منصوص عليها في قانون آخر، يعاقب بالحبس لمدة لا تزيد على ثلاث سنوات وبغرامة لا تقل عن خمسة آلاف دينار ولا تزيد على عشرين ألف دينار أو بإحدى هاتين العقوبتين كل من:.ج- أتلف أو عيَّب توقيعاً أو نظاماً أو أداة توقيع أو مستنداً أو سجلاً إلكترونياً أو زوَّر شيئاً من ذلك بطريق الاصطناع أو التعديل أو التحوير أو بأي طريقة أخرى. د- استعمل توقيعاً أو أداة توقيع أو مستنداً أو سجلاً إلكترونياً معيباً أو مزوراً مع علمه بذلك».

واستناداً إلى هذه النصوص نجد أن سلوك إدخال بيانات في نظام المعالجة الإلكترونية على أنها بيانات حقيقية، ومن ثم اتجاه الفاعل إلى استعمالها على النحو الذي يغاير الحقيقة وهو استعمال التصريح في غير ما صرح من أجله، يُشكّل تزويراً معنوياً كون المستخدم قام بالإدلاء ببيانات غير صحيحة عن طريق إدخالها بنظام التصاريح، وهي بيانات تخالف حقيقة الوجهة التي سيذهب إليها[37]، ومن ثم استعمال هذا التصريح أو عدم استعماله سيخضعه للأحكام السالفة الذكر، فضلاً عن تدابير أخرى تتخذها السلطات الحكومية، وهو حظر استخدام التصريح عن طريق وضع «بلوك» على المستخدمين المخالفين[38].

(37) معاذ سليمان الملا، مرجع سابق، ص81.

(38) مقال منشور على موقع جريدة الجريدة الكويتية بعنوان/ وزارة الداخلية: «بلوك» لمخالفي التصريح الطبي، منشور بتاريخ 20-05-2020.
https://www.aljarida.com/articles/1589897478017924600

- **صعوبة إثبات جرائم تقنية المعلومات**

واجهت جرائم تقنية المعلومات صعوبات عملية كثيرة من بينها صعوبة إثبات وقائعها وضبط مرتكبيها، خصوصاً إذا نفذت الاعتداءات خارج إقليم دولة الكويت لأن فكرة التعاون الدولي لمكافحة هذه النوعية من الجرائم مازالت عقيمة هذا من ناحية، ومن ناحية أخرى ضعف الشق الإجرائي لمكافحة هذه النوعية من الجرائم في القانون رقم 63 لسنة 2015 بشأن مكافحة جرائم تقنية المعلومات، حيث اقتصر فيها المشرع على المادة (15) بشأن تحديد من لهم صفة الضبط القضائي، والمادة (17) بشأن اختصاص النيابة العامة بالتحقيق والتصرف والادعاء في هذه الجرائم.

أما إجراءات الضبط والتفتيش، فقد اكتفى المشرع بتطبيق الأحكام الواردة في قانون الإجراءات والمحاكمات الجزائية الصادر سنة 1960، وهو ما يصطدم عملياً مع طبيعة هذه النوعية من الجرائم فيما يتعلق بالدليل المتحصل منها[39].

المطلب الثاني

فرضيات المسؤولية الجزائية الناشئة عن جرائم تقنية المعلومات وملامح القصور في المعالجة التشريعية

ينشأ عن ارتكاب الأنشطة الإجرامية السابقة قيام مسؤولية جزائية ضد المستخدمين، طبيعيين كانوا أن اعتباريين، وهي أنشطة تتعلق بالمحتوى المعلوماتي التي عرفها المشرع في إطار المادة الأولى من قانون مكافحة جرائم تقنية المعلومات لسنة 2015 وقانون المعاملات الإلكترونية لسنة 2014، بأنها: «إنشاء أو إدخال أو استرجاع أو إرسال أو استلام أو استخراج أو تخزين أو عرض أو معالجة المعلومات أو الرسائل إلكترونياً».

وسنعرض في فرعين فرضيات المسؤولية الجزائية عن تلك الأنشطة وذلك على ضوء ما لاحظناه خلال فترة تفشي الجائحة، وموقف المشرع الجزائي الكويتي في ترتيب هذه المسؤولية وتحديد أوجه القصور فيها.

الفرع الأول

مسؤولية الشخص الطبيعي (المستخدم)

المستخدم قد يُسأل جزائياً إذا ارتكب أحد الأنشطة الإجرامية المشار إليها بطريقة عمدية، ولكن هل يمكن مساءلته إذا ارتكب الجريمة بطريقة غير عمدية؟

(39) معاذ سليمان الملا، مرجع سابق، ص229 وما بعدها.

أولاً: المسؤولية عن الجريمة العمدية

لا خلاف على مساءلة المستخدم جزائياً إذا تعمد لوحده ارتكاب أحد الأنشطة الإجرامية السابقة، إذ يتحمل العقوبة المنصوص عليها في إطار القانونين اللذين أشرنا إليهما، ولا خلاف أيضاً على تحمل كل من ساهم معه في اقتراف هذه الأنشطة، فيُعاقب معه بوصفه فاعلاً أصلياً أو شريكاً فيها.

وفي حالة تعدد الجناة في جرائم الشائعات عن طريق شبكات التواصل الاجتماعي، فإنه لابد من التفرقة في آلية عمل التطبيقات الإلكترونية فيما بينها، فتطبيق «تويتر» على سبيل المثال يختلف تماماً عن تطبيق «الواتساب»، فالأول من التطبيقات التي تتصف بالطابع العلني، إذ من خلالها يتم التواصل مع الجمهور بصورة مباشرة، وقد اعتبرت محكمة التمييز الكويتية في العديد من الأحكام أن تطبيق «تويتر» من قبيل الأماكن العامة[40]، بينما يعد تطبيق «واتساب» من التطبيقات التي اعتبرتها محكمة التمييز بأنه لا يتحقق معها الطابع العلني، وبمعنى آخر فإنها تعد من التطبيقات المغلقة، فهي بالتالي في حكم المراسلات الخاصة[41].

وقد اعتبر التطبيق الأخير «واتساب» من أكثر التطبيقات التي تم تداول الشائعات فيها، ويعتبر المستخدم أو المستخدمون (المجموعة) مسؤولين جميعاً – بما في ذلك مدير المجموعة – عن طبيعة المحتوى المُجرَّم متى علموا بهذا المحتوى، ولم يتخذوا حياله أي تصرف يوقف أثره كمسحه على سبيل المثال، أو تحذير صاحبه بعدم إرسال مثل هذه المحتويات، أو نصحه بعدم إعادة نشره مرة أخرى وتحري الدقة في المعلومات، أو استبعاده من المجموعة وهو أقصى إجراء ممكن أن يتخذه مدير المجموعة، بحيث يدلل على رفضه ورفض المجموعة للمحتوى، وذلك من باب المسؤولية الاجتماعية التي تتطلب الإحساس بخطورة ذلك على أمن الأفراد والمجتمع لاسيما خلال فترة تفشي جائحة كورونا.

ثانياً: المسؤولية عن الخطأ غير العمدي

ولكن ما حكم من يخطئ أثناء استخدام هذه الأدوات وتطبيقاتها، كالمستخدم الذي لا يذهب إلى الموقع الذي أدلى به في تصريح الخروج أثناء الإذن، أو ذهب إلى الموقع ونسي تأكيد حضوره للمكان، أو قام بإعادة نشر أو بث محتوى دون أن يطلع على فحواه أو اطلع عليه ولكن دون التدقيق في تفاصيله، أو عدم ملاحظة مدير المجموعة للمحتويات

(40) مثلها طعن تمييز رقم 2016/538 جزائي3، وطعن تمييز رقم 2015/1039 جزائي3.
(41) طعن تمييز رقم 2017/144 جزائي2.

التي يبثها الأفراد المنضمون للمجموعة، أو إعادة نشر رابط إلكتروني احتيالي، أو غير ذلك مما أثبته الواقع العلمي لاسيما أثناء تفشي الجائحة ؟

لم يشأ المشرع الكويتي تناول هذه المسألة في إطار القوانين المتعلقة بتقنية المعلومات، فقد أحال حكمها إلى القواعد العامة وتحديداً ما ورد في المادة (44) من قانون الجزاء التي تناولت حكم الخطأ غير العمدي، وقد نصت على أنه: «يُعد الخطأ غير العمدي متوافراً إذا تصرف الفاعل، عند ارتكاب الفعل، على النحو الذي لا يؤتيه الشخص المعتاد إذا وجد في ظروفه، بأن اتصف فعله بالرعونة أو التفريط أو الإهمال أو عدم الانتباه أو عدم مراعاة اللوائح. ويعد الفاعل متصرفاً على هذا النحو إذا لم يتوقع، عند ارتكاب الفعل، النتائج التي كان في استطاعة الشخص المعتاد أن يتوقعها فلم يحل دون حدوثها من أجل ذلك، أو توقعها ولكنه اعتمد على مهارته ليحول دون حدوثها فحدثت رغم ذلك».

واستناداً لهذا النص، فإن الخطأ غير العمدي سلوك ينحرف فيه الشخص عن قواعد الحرص الواجب اتباعه لدرء نتيجة يعاقب عليها القانون، وبتطبيق ذلك على موضوع دراستنا، فإن صور الخطأ غير العمدي تنسجم مع طبيعة الأخطاء المترتبة أثناء استخدام أدوات تقنية المعلومات وشبكة الإنترنت، فعدم الاحتياط على سبيل المثال يمكن تصوره بقيام المستخدم بإعادة نشر محتوى مُجرَّم لم يطلع عليه، وهو سلوك يتسم بنقص الحذر الواجب اتباعه، وأيضاً يمكن تصور الرعونة من خلال قيام المستخدم بعدم تحري الدقة في نقل الخبر أو الحدث، وهذا سلوك يتسم بسوء تقدير أو جهل من قبل المستخدم، أو الإهمال برمي السوار الإلكتروني وعدم تسليمه أو الاحتفاظ به مما يوقعه ضحية بسبب بياناته المخزنة فيه، أو عدم الالتزام بوجوب التأكيد على الموقع الذي حدده المستخدم لاستخراج التصريح أثناء الحظر، أو غير ذلك من التصرفات الأخرى التي ظهرت من واقع استخدام بعض الأفراد لأدوات تقنية المعلومات وشبكة الإنترنت أثناء فترة تفشي جائحة كورونا.

وما نلاحظه أن المشرع الكويتي لم يتدخل لتجريم الخطأ غير العمدي في بيئة تقنية المعلومات سوى أنه أشار إلى بيئة الدفع الإلكتروني في الفقرة الثانية من المادة (30) من قانون المعلومات الإلكترونية، التي نصت على أنه: «ويعتبر العميل مسؤولاً عن استعمال غير مشروع لحسابه بواسطة الدفع الإلكتروني، إذا ثبت أن إهماله قد أدى أو أسهم في ذلك بصورة رئيسية، وأن المؤسسة قد قامت بواجبها للحيلولة دون أي استعمال غير مشروع لذلك الحساب».

ولم يشر المشرع ضمن هذا القانون إلى أي عقوبة مستحقة على المستخدم حال خطئه بشكل غير عمدي حتى أنه لم يشر إلى تطبيق القواعد العامة، وهو ما يعد –في رأينا –

ثغرة قانونية تستوجب تدخله بالنص صراحة على تجريم الخطأ غير العمدي لاسيما مع خطورة بعض نتائجها على الأفراد والمجتمع.

الفرع الثاني

مسؤولية الشخص الاعتباري

الشخص الاعتباري هو شخصية قانونية تعترف بها معظم تشريعات دول العالم وبمسؤوليتها الجزائية تجاه الأفعال التي تنشأ عنها خصوصاً في البيئة الإلكترونية التي ازداد دورها في إدارة أعمال الدولة وخدماتها تحت مسمى الحكومة الإلكترونية، أو في إدارة الأعمال الخاصة كشركات ومؤسسات القطاع الخاص.

وقد تناول المشرع الكويتي تعريف مزود الخدمة في بيئة شبكات الاتصالات في المادة الأولى من القانون رقم 37 لسنة 2014 بشأن إنشاء هيئة تنظيم الاتصالات، حيث عرَّفه بأنه: « الشخص الذي يرخص له بتقديم خدمة أو أكثر من خدمات الاتصالات للجمهور، أو يرخص له بإدارة أو إنشاء أو تشغيل شبكة اتصالات أو خدمة إنترنت لتوفير خدمات الاتصالات للجمهور، ويشمل مقدمي المعلومات أو المحتوى الذي يقدم بواسطة شبكة الاتصالات».

وعرَّفه أيضاً في المادة الأولى من قانون التعاملات الإلكترونية بأنه: «الجهة التي تقوم بمهمة مزود خدمات فيما يتعلق بإنتاج أو معالجة أو إرسال أو حفظ ذلك المستند أو السجل الإلكتروني وغير ذلك من الخدمات المتعلقة بها».

والسؤال الذي نطرحه في هذا المقام ما هو نطاق المسؤولية الجزائية للشخص الاعتباري في بيئة المعالجة الآلية للبيانات؟ وما هي الالتزامات التي ترتب مسؤولية الشخص الاعتباري في بيئة المعالجة الإلكترونية؟ وكيف يمكن تقدير هذه الالتزامات في مجملها خلال فترة تفشي جائحة كورونا؟ ففيما يتعلق بالشق الأول من السؤال فقد نصت المادة (14) من قانون مكافحة جرائم تقنية المعلومات على أنه: «مع عدم الإخلال بالمسؤولية الشخصية لمرتكب الجريمة، يعاقب الممثل القانوني للشخص الاعتباري بذات العقوبات المالية المقررة عن الأفعال التي ترتكب بالمخالفة لأحكام هذا القانون، إذا ثبت أن إخلاله بواجبات وظيفته أسهم في وقوع الجريمة مع علمه بذلك. ويكون الشخص الاعتباري مسؤولاً عما يحكم به من عقوبات مالية أو تعويضات إذا ارتكبت الجريمة لحسابه أو باسمه أو لصالحه».

وهذا النص يتوافق تماماً من حيث صياغته مع ما جاء في نص المادة (39) من قانون

المعاملات الإلكترونية وأيضاً نص المادة (83) من قانون تنظيم هيئة الاتصالات وتقنية المعلومات[42]. فمن واقع قراءة النصوص المعمول بها في بيئة تقنية المعلومات وشبكات الاتصالات، نجد أن المشرع الكويتي يتجه إلى التضييق في تقرير المسؤولية الجزائية للأشخاص الاعتبارية، إذ يرى أن ارتكاب أي جريمة من الجرائم المنصوص عليها في التشريعات المتعلقة بتقنية المعلومات لحساب أو لمصلحة الشخص الاعتباري هو في الحقيقة من ممثليه أو أعضائه أي الشخص الطبيعي.

وبالتالي فإننا أمام مسؤوليتين مباشرة وأخرى غير مباشرة، أما المسؤولية المباشرة فتعني مسؤولية الممثل القانوني أو المدير الفعلي للشخص الاعتباري الذي أسهمت أفعاله في ارتكابها لحساب الشخص الاعتباري أو لمصلحته، وأما إذا ارتكبها لحسابه أو لمصلحته الخاصة، فهنا يكون مسؤولاً عنها شخصياً ولا علاقة للشخص الاعتباري بذلك.

أما المسؤولية غير المباشرة للشخص الاعتباري، فهي مسؤوليته غير الجزائية التي يتحمل فيها هذا الشخص الوفاء بما يحكم من عقوبات مالية وتعويضات مع ضمان حقه في الرجوع إلى ممثله أو الموظف لما قام به من أخطاء بالمخالفة لأحكام هذه القوانين.

وعلى الرغم من اختلاف طبيعة الالتزامات التي يمارسها الشخص الاعتباري، سواء أكان الشخص عاماً أم خاصاً في بيئة تقنية المعلومات، إلا أنها تجتمع في أن الشخص الاعتباري بقدر ما هو ملزم بتوفير الخدمات والإمكانات للأفراد في بيئة تقنية المعلومات وشبكة الإنترنت، فهو ملزمٌ أيضاً بتوفير حماية لحقوقهم ومصالحهم في البيئة ذاتها. وفي هذا الجانب يمكن إيضاح الالتزامات بالتقسيم الآتي:

أولاً: في قانون المعاملات الإلكترونية

وهذه الالتزامات وردت بوضوح في إطار المادة (35)، حيث نصت على أنه: «يحظر على الجهات المذكورة في المادة (32) ما يلي:

1- جمع أو تسجيل أو تجهيز أي بيانات أو معلومات شخصية من تلك المنصوص

(42) نظم المشرع الكويتي مسؤولية الشخص الاعتباري في الجرائم المتصلة بالإعلام الإلكتروني، وذلك في إطار المادة (17) من القانون رقم 8 لسنة 2016 بشأن الإعلام الإلكتروني، وقد نصت على أن: «يكون المدير المسؤول عن الموقع أو الوسيلة الإعلامية الإلكترونية مسؤولاً عما يتضمنه المحتوى من مخالفات لأحكام هذا القانون، ويجب عليه تحري الدقة والمصداقية في كل ما ينشره من أخبار أو معلومات أو بيانات، كما يجب عليه أن ينشر وبدون مقابل أي رد أو تصحيح أو تكذيب يرد إليه بصورة مباشرة أو غير مباشرة من الوزارة أو الجهات الحكومية الأخرى أو من أي شخص اعتباري أو طبيعي أو من يمثله قانوناً ورد اسمه أو أشير إليه في كتابة أو رسم أو رمز تم نشره بالموقع أو الوسيلة الإعلامية الإلكترونية وذلك في التاريخ الذي تحدده الجهة المعنية أو ذوي الشأن وفي ذات مكان النشر والطريقة ذاتها والأسلوب واللغة والحجم الذي نشرت به المادة موضوع الرد أو التصحيح أو التكذيب».

عليها في المادة (32) بأساليب أو طرق غير مشروعة، أو بغير رضاء الشخص أو من ينوب عنه.

2- استخدام البيانات أو المعلومات الشخصية المشار إليها والمسجلة لديها بسجلاتها أو بأنظمة معلوماتها في غير الأغراض التي جمعت من أجلها.

وتلتزم تلك الجهات بالآتي:

1- التحقق من دقة البيانات أو المعلومات الشخصية الواردة في المادة (32) والمسجلة لديها بأنظمة المعلومات والمتعلقة بالأشخاص واستكمالها وتحديثها بانتظام.

2- اتخاذ التدابير المناسبة لحماية البيانات والمعلومات الشخصية المشار إليها في المادة (32) من كل ما يعرضها للفقد أو التلف أو الإفشاء أو استبدالها ببيانات غير صحيحة أو إدخال معلومات على خلاف الحقيقة».

نستفيد من هذا النص أن المشرع أراد أن يفرض على الجهات التي تتعامل في بيئة تقنية المعلومات، وهم الذين ورد ذكرهم في إطار المادة (32) من القانون ذاته[43]، أن تلتزم بمراعاة حقوق المستخدمين أثناء معالجة بياناتهم الشخصية، والتي تبدأ بضرورة الحصول على موافقتهم بمعالجة بياناتهم الشخصية، وضرورة طلب تحديثها وحمايتها من مخاطر الفقد أو التلف أو غير ذلك مما ورد في النص، وقد وضعت اللائحة التنفيذية القرار رقم 48 لسنة 2014 إيضاحاً لآلية معالجة البيانات عملاً بأحكام هذا القانون، حيث تناولت أحكاماً تتعلق بعدة تدابير بمعالجة البيانات الشخصية كحفظ واسترجاع المستندات والسجلات الإلكترونية، وأيضاً ضوابط التعامل وخدمات التوقيع الإلكتروني وآلية إصدار التراخيص لمزاولة الخدمات الإلكترونية ومراقبة أنشطة مزودي تلك الخدمات، والإشراف عليها والإجراءات المتعلقة بتنظيم الاطلاع والمحو والتعديل على البيانات والمعلومات الشخصية[44].

(43) نصت المادة (32) من قانون المعاملات الإلكترونية على أنه: «لا يجوز في غير الأحوال المصرح بها قانوناً- للجهات الحكومية أو الهيئات أو المؤسسات العامة أو الشركات أو الجهات غير الحكومية أو العاملين بها الاطلاع دون وجه حق أو إفشاء أو نشر أية بيانات أو معلومات شخصية مسجلة في سجلات أو أنظمة المعالجة الإلكترونية المتعلقة بالشؤون الوظيفية أو بالسيرة الاجتماعية أو بالحالة الصحية أو بعناصر الذمة المالية للأشخاص أو غير ذلك من البيانات الشخصية المسجلة لدى أي من الجهات المبينة في هذه البيانات أو المعلومات أو من ينوب عنه قانوناً، أو بقرار قضائي مسبب. وتلتزم الجهات المبينة في الفقرة الأولى من هذه المادة ببيان الغرض من جمع البيانات المذكورة، وأن يتم جمع تلك البيانات والمعلومات في حدود ذلك الغرض».

(44) للمزيد من التفاصيل راجع القرار رقم 48 لسنة 2014 بشأن اللائحة التنفيذية للقانون رقم 20 لسنة 2014 بشأن التعاملات الإلكترونية

http://reqaba.com/ArticleDetail.aspx?id=45079

ثانياً: في قانون تنظيم هيئة الاتصالات وتقنية المعلومات

حدَّد قانون تنظيم هيئة الاتصالات وتقنية المعلومات دور الهيئة باعتبارها جهة مستقلة في مراقبة المرخص له (مزود الخدمة) والإشراف على أدائه، هذا إلى جانب دورها في تنفيذ المبادرات التي نصت عليها الاستراتيجية الوطنية للأمن السيبراني، وذلك استناداً للمادة الثالثة من القانون ذاته لضمان حسن الأداء وحماية المستخدمين، يمكن إيضاح ملامح الرقابة والإشراف على مزود الخدمة بما يأتي[45]:

1- ما نصت عليه المادة (47) من أنه يجب على المرخص له بتقديم خدمات الاتصالات أن ينشئ قسماً خاصاً لتلقي شكاوى المستفيدين والمشتركين وتلافي الإشكالات التي تتعلق بمستوى الخدمة ونوعيتها أو طريقة تقديمها.

2- بموجب المادة (49) يجب على مزود الخدمة إزالة أي مخالفة لشروط الرخصة أو أي خلاف موجود بين مزود الخدمة والمستفيدين بشأن مستوى الخدمة، وذلك خلال 90 يوماً من تاريخ إخطار المزود من قبل الهيئة.

5- بموجب المادة (50) يجب على المرخص له أن يقدم تقريراً سنوياً عن الجوانب الفنية والإدارية والمالية التي تضمن تقديم المستوى المطلوب للمستفيدين. ويجوز للهيئة استناداً لنص المادة (54) أن تتحقق من هذه الالتزامات.

8- يلتزم المرخص له بموجب المادة (52) بالاتفاق مع الهيئة على وضع القواعد والإجراءات التي يجب اتباعها عند تلقي المرخص له لشكاوى الإزعاج، وإجراءات التحقق من هذه الشكاوى، والقواعد اللازمة لتقليل اتصالات الإزعاج بشكل عام.

نستشف من جميع هذه التدابير في حقيقة الأمر أن هناك أمرين ينبغي على مزود الخدمة الالتزام بهما في مواجهة المستخدم: أولهما التزام أخلاقي، أي الالتزام بأخلاقيات العمل المشروع الذي يتطلب حماية حقوق المستخدمين، كالحق في الخصوصية والحق في الاطلاع والحق في تداول المعلومات وغيرها من حقوق في هذه البيئة. وثانيهما التزام فني يتطلب اتخاذ كافة الشروط الفنية أو الأمنية التي تضمن عدم اختراق الأنظمة الحاسوبية وحماية البيانات المخزنة فيها.

وبالتالي فإن إخلال مزود الخدمة بالالتزامات بموجب التشريعات الإلكترونية، ستنشأ عنه مسؤوليته الجزائية والمدنية عملاً بأحكام المواد (14) و(39) و(83) المشار إليها سابقاً.

(45) للمزيد من التفاصيل راجع الموقع الإلكتروني للهيئة على الرابط التالي:
https://citra.gov.kw/sites/Ar/Pages/cybersecurity.aspx

الفرع الثالث

تقدير الالتزامات أثناء فترة تفشي جائحة كورونا وضمانات الحماية

إن تقدير تحمل الالتزامات أثناء تفشي جائحة كورونا لا تقتصر فقط على الشخص الاعتباري بقدر ما تشمل أيضاً المستخدم ذاته، الذي يُلقى عليه العبء الأكبر أثناء استعماله لأدوات تقنية المعلومات، ونقصد بذلك أن يراعي المستخدم الحد الأدنى للحيطة والحذر بالنسبة للشخص العادي، في تعامله مع الآخرين، إذ ينبغي عليه أن يتحرى الدقة في المحتوى الذي يستقبله بأي طريقة كانت على جهازه، فقد يكون المحتوى محلاً للتجريم وقد يكون مسؤولاً عنه، كما أن تحقق الخطأ غير العمدي بصوره المتمثلة في الإهمال أو عدم الاحتياط أو الرعونة أو عدم التزامه باللوائح أمرٌ واردٌ في هذه الفرضيات.

أما بالنسبة للشخص الاعتباري، فالدولة ممثلة بحكومتها الإلكترونية يلقى على عاتقها حماية البيانات الشخصية للمستخدمين التي يتم تخزينها فتكون ضمن قواعد البيانات لأنظمتها، فوزارة الصحة ملزمة بحماية البيانات الشخصية للمصابين، حيث ألزمت من هم تحت قيد التقصي الوبائي بارتداء السوار الإلكتروني، وتصوير أنفسهم وإرسال الصور عبر تطبيق (شلونك) لمتابعة مدى التزامهم بالحجر.

كذلك الأمر بالنسبة لوزارة الداخلية التي حاولت أن تضع الخوذة الإلكترونية كأداة لرصد حرارة المصابين، وكذلك البيانات التي يدخلها الأشخاص للحصول على تصريح للخروج أثناء فترات الحظر، ووزارة التجارة التي خصصت تطبيقاً لحجز مواعيد الزيارة إلى الجمعيات التعاونية، وهذه الأنظمة وما تحتويه من قواعد بيانات معرضة للاختراق والعبث في المحتوى المعلوماتي المخزن فيه.

وهذا يتم– بطبيعة الحال – وفقا للخطة الاستراتيجية الوطنية للأمن السيبراني التي تشرف عليها الهيئة العامة للاتصالات وتقنية المعلومات، والتي يُلقى عليها عبء تأمين البنية التحتية للحكومة الإلكترونية، فضلاً عن دورها في تأمين معالجة البيانات الشخصية. ويلاحظ على أن دور الهيئة في هذه المرحلة لم يكن بالمستوى المطلوب، خصوصاً في عملية اختراق الموقع الخاص بتصاريح خروج أثناء فترة الحظر وهو خير دليل على ذلك، فضلاً عن ضعف الجانب التوعوي في استخدام تقنية المعلومات لاسيما مع الاعتماد الكلي على هذه الأدوات، إذ يتطلب أن تمارس دوراً ملحوظاً يبث الطمأنينة إلى المستخدمين بشأن التعاملات الإلكترونية.

وينصرف الأمر كذلك إلى الشخص الاعتباري في القطاع الخاص كالمتاجر ومواقع

التوصيل والبنوك وغيرها من المواقع، التي تعالج باستمرار البيانات الشخصية للمستهلكين عبر تطبيقاتها الإلكترونية. ففيما يتعلق بعمليات الدفع الإلكتروني، نصت المادة (29 – ب) من قانون المعاملات الإلكترونية الصادر سنة 2014 على قيام المؤسسات المالية التي تمارس الدفع الإلكتروني بتقديم خدمات مأمونة للعملاء والحفاظ على السرية المصرفية وفقاً للمعايير القانونية.

وفيما يتعلق بالخصوصية، فقد حظرت المادة (32) من قانون التعاملات الإلكترونية على الجهات الحكومية أو الهيئات أو المؤسسات العامة أو الشركات أو الجهات غير الحكومية أو العاملين الاطلاع على البيانات الشخصية للمستخدمين في غير الأحوال المصرح لها بذلك، وهذا التصريح يستلزم تحديد الغرض من تلك البيانات.

وفيما يتعلق بحق الاطلاع فقد أجازت المادة (33) من القانون ذاته للمستخدمين طلب الاطلاع على بياناتهم الشخصية المخزنة لدى الجهات الحكومية وغير الحكومية بمجرد تقديم طلب من المستخدم بذلك، وينبغي لتلك الجهات الاستجابة للطلبات المقدمة، وقد استثنى المشرع من ذلك البيانات المخزنة لدى الجهات الحكومية متى تعلقت باعتبارات أمنية.

واشترطت المادة (34) لتقديم البيانات الشخصية للجهة الطالبة ممن ورد ذكرهم في المادة (32) أن توافق الجهة المطلوب منها تقديم البيانات، وأن تحدد صفة الطالب والغرض من هذا الطلب وأي شروط أخرى تجدها مناسبة، إذ يجوز لها رفض الطلبات، وللجهة الطالبة التظلم من ذلك خلال ثلاثين يوماً من تاريخ الرفض. كما بيَّنت المادة نفسها عدم جواز استخدام البيانات الشخصية في غير الغرض الذي تمت الموافقة على تقديمه.

أما المادة (35) فقد أشرنا إليها سابقاً، حيث تناولت عدة التزامات يجب على مزود الخدمة الالتزام بها عند معالجة البيانات الشخصية للمستخدمين. وأما المادة (36) وتتعلق بحق المستخدمين في محو بياناتهم الشخصية، أو تعديلها لدى المعالجين الذين ورد ذكرهم في المادة (32) وفق الضوابط التي وردت في القرار رقم 48 لسنة 2014 الخاص باللائحة التنفيذية للقانون رقم 20 لسنة 2014 بشأن المعاملات الإلكترونية.

مما تقدم فإن جميع ما ذكرناه يشكل ضمانة حقيقية لمن تمت معالجة بياناتهم، سواء في الجهات التابعة للقطاع العام أو القطاع الخاص، ويكون للمستخدمين حق الاستناد إليها في مواجهة مزود الخدمات خصوصاً المصابون بفيروس كورونا أو من هم تحت قيد التقصي الوبائي، فيجوز لهم استناداً إلى هذا القانون الاطلاع على بياناتهم الشخصية أو تعديلها أو محوها أو طلبها أو غير ذلك من صور المعالجة الآلية للبيانات، وذلك وفقاً للضوابط التي رسمها القانون.

الخاتمة

في ختام دراستنا فقد حرصنا أن يكون الواقع والمأمول عنواناً وهدفاً لدراستنا، فالواقع أننا توصلنا إلى ما يجسد أهمية استخدام أدوات تقنية المعلومات وآثارها الخطيرة أثناء فترة تفشي جائحة كورونا، أما المأمول فقد عرضنا فيه بعض التوصيات التي نرى فيها أهمية لمعالجة بعض الثغرات القانونية وتعزيز الجانب الوقائي لمواجهة هذه الجرائم.

أولاً: أهم النتائج

1. تعتبر أدوات تقنية المعلومات وشبكة الإنترنت وتكنولوجيا الذكاء الاصطناعي من الأدوات الرئيسة التي تم الاستعانة بها لمواجهة فيروس كورونا، وأثبتت فاعليتها من حيث التطبيق كالسوار الإلكتروني والخوذة الإلكترونية وأجهزة فحص كورونا.

2. ينبغي الأخذ في الاعتبار أن المستخدمين عموماً والمصابين بفيروس كورونا خصوصاً معرضون لخطر الاعتداء على حقوقهم ومصالحهم بصفة دائمة نتيجة معالجة بياناتهم الشخصية وأول هذه الحقوق انتهاكاً هو حقهم في الخصوصية.

3. عالمياً ارتفعت نسبة جرائم تقنية المعلومات أثناء تفشي جائحة كورونا بسبب اعتماد سكان العالم بأسره على أدوات تقنية المعلومات وشبكة الإنترنت في القيام بأعمالهم المختلفة، والأنشطة الأكثر انتشاراً في العالم وفي الكويت هي أنشطة الاحتيال الإلكتروني وجرائم الشائعات عبر شبكات التواصل الاجتماعي.

4. جرائم تقنية المعلومات في طريقها إلى الجريمة الذكية بسبب تكنولوجيا الذكاء الاصطناعي التي سيتم استخدامها من قبل المجرمين، والمشرع الكويتي حتى الآن لم يُجرّم الأخطاء غير العمدية التي يمكن أن تتحقق.

5. تعتبر مواجهة هذه الأنشطة الإجرامية خصوصاً خلال فترة تفشي جائحة كورونا من المسؤوليات المشتركة، فهي تتطلب أولاً وعي المستخدم أثناء استخدامه لتلك الأدوات واستيعاب خطورتها عليه وعلى غيره.

6. سياسة حماية البيانات الشخصية في التشريع الكويتي تحتاج إلى إيضاح أكثر، فالمستخدمون وبعض الجهات يجهلون أهميتها.

7. كلما كانت خطة الأمن السيبراني محكمة إشرافاً وتنفيذاً قلت التهديدات السيبرانية والعكس صحيح.

8. على الرغم من وجود استراتيجية أمن سيبراني في الكويت 2020/2017، إلا أنها لم تكن فاعلة بالشكل الذي يتوجب أن تكون عليه خلال هذه الفترة، كما أنها لم تتناول في بنودها ما يعني بتكنولوجيا الذكاء الاصطناعي وإنترنت الأشياء والبيانات الضخمة.

ثانياً: التوصيات

1. نوصي المشرع الكويتي باعتماد لائحة مخصصة لحماية البيانات الشخصية ولائحة أخلاقيات لاستخدام التكنولوجيا الحديثة، وبموجبها تصاغ التشريعات بشكل أوضح، بحيث تحدد حقوق وواجبات المتعاملين والمسؤوليات المترتبة عليها.

2. نوصي المشرع الكويتي بتجريم صور الأخطاء غير العمدية عبر أدوات تقنية المعلومات لطالما سلمنا بأن الجرائم غير العمدية لا تجرم إلا بنص خاص.

3. ضرورة معالجة الجوانب الإجرائية لمكافحة هذه النوعية من الجرائم.

4. نوصي المشرع الكويتي بدعوة الحكومة إلى تفعيل آليات تطبيق استراتيجية الأمن السيبراني، ودعوتها أيضاً إلى ضرورة استكمال إجراءات الانتقال الذكي لخدمات الحكومة الإلكترونية والالتفات إلى تعزيز الجوانب الوقائية من مخاطر الجريمة الذكية.

المراجع

أولاً: باللغة العربية

- أسامة أحمد المناعسة وجلال محمد الزعبي، جرائم تقنية نظم المعلومات الإلكترونية: دراسة مقارنة، ط2، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2014.
- إيهاب خليفة، الذكاء الاصطناعي: ملامح وتداعيات هيمنة الآلات الذكية على حياة البشر، دراسات المستقبل، أبو ظبي، الإمارات العربية المتحدة، العدد 6، أبريل 2019،
- دينا عبد العزيز فهمي، الحماية الجنائية من إساءة استخدام مواقع التواصل الاجتماعي: دراسة مقارنة، ط1، دار النهضة العربية، القاهرة، 2018.
- وليد بن صالح، الإنترنت المظلم والعملات الافتراضية، ورقة عمل بحثية مقدمة في مؤتمر (التحديات المعاصرة للضمانات القانونية في عالم متغير)، مجلة كلية القانون الكويتية العالمية، ملحق خاص، الجزء الثاني، العدد 3، أكتوبر 2018.
- ممدوح عبد الحميد عبد المطلب، الشرطة الاستخباراتية – العمل الشرطي القائم على الذكاء الاصطناعي وتحليل المعلومات، ط1، دار النهضة العربية، القاهرة، 2019.
- معاذ سليمان الملا، التعليق على أحكام القانون رقم 63 لسنة 2015 بشأن مكافحة جرائم تقنية المعلومات، ط1، لجنة التأليف والتعريب، مجلس النشر العلمي، جامعة الكويت، 2019.
- نديم منصوري، موضوعات في علم اجتماع الإنترنت والتواصل الرقمي، ط1، منتدى المعارف، بيروت، 2019.
- سامي عبد الصادق، البيانات الشخصية .. الصراع على نفط القرن الحادي والعشرين، كراسات استراتيجية، مركز الدراسات السياسية والاستراتيجية، القاهرة، العدد287، المجلد 27، أبريل2018.
- عبد الله موسى ود. أحمد حبيب بلال، الذكاء الاصطناعي ثورة في تقنيات العصر، ط1، المجموعة العربية للتدريب والنشر، القاهرة، 2019.
- علي بن عبد الله الكلباني، الشائعات وخطرها في ظل وسائل الإعلام الجديد، ط1، عالم الكتب، القاهرة، 2017.
- علي عبود جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة: دراسة مقارنة، ط1، مكتبة زين الحقوقية، بيروت، 2013..

ثانياً: باللغة الأجنبية

- Adam King, The impact of COVID-19 on user behaviour and ecommerce, 31st March 2020. https://www.ayima.com/blog/the-impact-of-covid-19-on-user-behaviour-and-ecommerce.html.
- Gabriel Hallevy, Liability for Crimes Involving Artificial Intelligence Systems, Springer, USA, 2015.
- Independent High -level Expert Group on Artificial Intelligence (Ai-Hleg) set up by The European Commission, Ethics Guidelines for Trustworthy AI, European Commission, Brussels. https://ec.europa.eu/digital-single-market/en/artificial-intelligence.
- Jerry H. Ratcliffe, Intelligence-Led Policing, Willan Publishing, USA and Canada, 2008.
- Jerry Kaplan, Artificial Intelligence- What everyone needs to know, Oxford University Press, USA, 2016.
- Johannes Xingan Li, Cyber Crime and Legal Countermeasures: A Historical Analysis, International Journal of Criminal Justice Sciences (IJCJS), Official Journal of the South Asian Society of Criminology and Victimology (SASCV), July–December 2017, Vol. 12 (2).
- Joseph Migga Kizza, Ethical and Social Issues in the Information Age, 6 ed-, Springer International Publishing, 2017.
- Kacper Gradon, Crime in Time of the Plague: Fake news Pandemic and the Challenges to Law-Enforcement and Intelligence community. Society Register, Vol. 4 No. 2 (2020): Postmodern Society and Covid-19 Pandemic: Old, New and Scary. https://pressto.amu.edu.pl/index.php/sr/issue/view/1571.
- P. Sai Sheela and Nitika Sharma and Bhanu Bharadwaj, Cyber Crime-Definition - challenges and the cost, International Journal of Computer & Mathematical Sciences (IJCMS), Volume 3, Issue 2 April 2014.

- Paul Day, Cyber Attack- The truth about digital crime, cyber warfare and government snooping, 2014, Carlton Books.
- Roman Zhidkov, The Future Impact of AI on Cyber Crime, 14 Feb 2020. https://becominghuman.ai/the-future-impact-of-ai-on-cyber-crime-f9659cf354a6.
- Thomas C. King and Nikita Aggarwal and Maria rosaria Taddeo and Luciano Floridi, Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions, Science and Engineering Ethics (2020). DOI: 10.1007/s11948-018-00081-0.

ثالثاً: أهم مواقع الإنترنت

- https://datareportal.com/reports/digital-2020-april-global-statshot
- https://datareportal.com/reports/digital-2020-kuwait
- https://www.alanba.com.kw/ar/economy-news/956689/16-03-2020-
- https://www.smartdubai.ae/ar/initiatives/ai-principles-ethics

المحتوى