3007- المسؤولية القانونية عن انتهاك خصوصية البيانات عن طريق الاختراق السيبراني

MOHAMED HASSAN MERDAD OBAID
Faculty of Syariah and Law
Universiti Sains Islam Malaysia (USIM)
merdad.24@yahoo.com

ABSTRACT

تهدف الدراسة إلى بيان إشكالية صور الاعتداء على الخصوصية المعلوماتية: وتتمثل سلوكيات الاعتداء على الخصوصية الفردية في الاطلاع المجرد: محل الاطلاع في هذه الحالة هو معلومات شخصية وخاصة يريد صاحبها إبقاءها سرية، ولما صورة هذا السلوك هو الاطلاع الكلي أو الجزئي على تلك الأسرار الخاصة بحيث يقوم اليقين بالعلم بها وفهمها، فإذا كانت الأسرار بلغة لا يفهمها الفاعل أولا يحسن تحليلها، لم يتحقق الاطلاع إلا بتكامل الصورة وترابط أجزائها فإذا لم يكن ما اطلع عليه الفاعل سوى جزيئات غير مترابطة، غير ذات معنى مفيد لم يتحقق الاطلاع أيضا، وهذا الاطلاع يجب أن يكون في ذاته غير مشروع وان يتم من شخص لا يملك قانونا ترخيصاً بالولوج إلى تلك المعلومات، كما يشترط لتحقق هذه الصورة أن يكون الاطلاع مجردة أي أن يكون قصد الفاعل هو الاطلاع فحسب على تلك المعلومات السرية ومجرد العلم الشخصي بها. وفي نهاية البحث توصلنا لنتيجة هامة ما يميز جريمة الاختراق السيبراني هي أنها جرائم سريعة التنفيذ إذ أنه وفي أغلب الأحيان لا يكون الركن المادي سوى ضغط على مفتاح معين في الجهاز مع إمكان تنفيذ ذلك عن بعد دون اشتراط التواجد في مسرح الجريمة ولهذا فأن الجريمة الالكترونية ولسهولة ارتكابها شكلت عنصر إغراء للمجرمين وإذ أن ارتكابها لا يتعدى سوى توفر إمكانية استغلال التكنولوجيا والتقنية الحديثة خصوصا عندما يكون الجاني موظفا عاما أو في إحدى الشركات التي تعتمد على الحاسب الآلي في طبيعة عملها المتعلق بالمعلومات أو الأموال بحيث يكون لديها كافة المعلومات اللازمة لتحقيق اختراقات متعددة ومتتالية لأنظمة الحاسب الآلي في الشركة وتحقيق أرباح طائلة. ولهذا نشأت الحاجة لوجود طرق حماية قوية للمعلومات المخزنة في أجهزة حاسوب أو وسائط نقل الكترونية ومثال ذلك ما يسمى بجدران الحماية أو الجدران النارية وهي عبرة عن برامج حماية تمنع الاختراق أو الدخول غير المصرح به.

الكلمات المفتاحية: الاختراق السيبراني، الخصوصية، المسؤولية.

1. مقدمة

البيانات هي أغلى ما يمتلكه الإنسان في حياته على مر العصور، لذا سعى إلى جمعها وتسجيلها على وسائط حفظ مختلفة بدءا من جدران المقابر إلى أن تم اختراع الورق في الصين.

وعرفت أولى محاولات تسجيل بيانات في التاريخ على أيدي قدماء المصريين الذين سجلوا حضارتهم على جدران المقابر والمعابد وأوراق البردي، وهذا هو السبب في الإبقاء على حضارتهم محفورة في ذاكرة التاريخ: حضارات عظيمة اندثرت لعدم تسجيلها، لذلك تعتبر المعلومة رمزا من رموز الحضارة الإنسانية على مدى التاريخ، ومعنى أن يفقد الإنسان معلوماته أنه يفقد ذاكرته ومن ثم تضييع حضارته

ولقد اكتسبت البيانات بظهور تكنولوجيا الحواسيب بعدة جديدة أضفي عليها أهمية تفوق ما كانت عليه من قبل، وقد تختلط المعلومات بمفاهيم عدة، مما ينبغي التطرق لتعريفها.

في ظل الانتشار الكبير للبيانات الحديثة واتجاه دولة الإمارات العربية المتحدة نحو استخدامها في نطاق الحكومة الإلكترونية ومعالجة البيانات الكبيرة، ومنها البيانات الشخصية، أصبح الحديث عن سبل الحماية القانونية للبيانات الخصوصية للأفراد والشركات والجهات الحكومية مطلباً ضرورياً، وعليه نبين في هذا الفصل ماهية البيانات وماهية خصوصيتها وطبيعة البيانات محل الخصوصية من خلال تقسيم البحث إلى ثلاث فقرات على النحو الآتي:

2. أولا: تعريف المسؤولية القانونية

المسؤولية بصفة عامة هي حالة الشخص الذي ارتكب أمراً يستوجب المؤاخذة. فإذا كان هذا الأمر مخالفاً لقواعد الأخلاق فقط، وصفت مسؤوليته بأنها مسؤولية أدبية واقتصرت مؤاخذته مؤاخذة أدبية لا تعدو استهجان المجتمع ذلك المسلك المخالف للأخلاق.

ولكن في حالة ما إذا كان القانون يوجب المؤاخذة على ذلك الأمر أيضاً فإن مسؤولية مرتكبه لا تقف عند حد المسؤولية الأدبية، بل تكون فوق ذلك مسؤولية قانونية تستتبع جزاءً قانونياً (فهيم، 1999).

والأخلاق ولقانون أمران يتمايزان، فالأخلاق تهدف إلى الكمال الذاتي للفرد، في حين أن القانون يرمي إلى إقامة النظام في المجتمع، وهذا الاختلاف في الأهداف بينهما يترتب عليه تباين في المؤيدات التي تفرز قواعدهما، فمؤيد الأخلاق داخلي يقوم على صوت الضمير، في حين أن مؤيد القانون فهو خارجي يقوم على سلطة الدولة ويظهر مؤيد القواعد الأخلاقية في صورة المسؤولية الأدبية بينما يظهر مؤيد القواعد القانونية في صورة المسؤولية القانونية (مسوار، 1992).

3. ثانيا: أنواع المسؤولية القانونية
كما تقدم، تنهض عندما يوجب القانون مؤاخذة شخص ما عن أمر معين قام به، وهي نوعان بارزان، مسؤولية مدنية ومسؤولية جنائية:

3.1 المسؤولية المدنية
تقوم المسؤولية المدنية كلما كان هناك ضرر أصاب شخص ما والجزاء فيها هو التزام المسؤول بتعويض المضرور وهذه المسؤولية نوعان أولهما: المسؤولية العقدية وقوامها وجود التزام تعاقدي نشئ عن عقد صحيح ووقوع اخلال بهذا الالتزام نشأ عنه وقوع ضرر، (إمام، 2002) وثانيهما: المسؤولية التقصيرية وقوامها خطأ ثابت أو مفترض ينشئ التزاماً غير إرادي بين المسؤول والمضرور، وهو الالتزام بالتعويض وتستوجبه المادة (166) من القانون المدني التي تتحدث عن المسؤولية المدنية وعن الفصل الضار بقولها (كل خطأ سبب ضرراً للغير يلزم من ارتكبه بالتعويض) من هنا يمكن تحديد أركان المسؤولية التقصيرية حسب النص المذكور، في الخطأ والضرر والعلاقة السببية بين الضرر والخطأ
توجد عدّة خصائص للمسؤولية المدنية بالمقارنة بالمسؤولية الجنائية أهمها:

1. جزاء المسؤولية المدنية دائماً هو التعويض في حين أن الجزاء المترتب من المسؤولية الجنائية هو عقوبة.
2. المطالب بالجزاء في حالة المسؤولية المدنية هو المضرور، يجوز له الصلح أو التنازل، بينما الأمر يختلف في حالة المسؤولية الجنائية حيث إن الأصل في المطالبة به تكون للنيابة العامة ولا يجوز لها الصلح أو التنازل عنها- أي عن المسؤولية الجنائية- وذلك باعتبارها ممثلة للمجتمع.
3. تنشأ المسؤولية المدنية عن أي عمل غير مشروع، سواء كان هذا العمل منصوصاً عليه في القانون أم لا، بينما يجب لقيام المسؤولية الجنائية أن يكون الفعل الذي يستوجب المساءلة منصوصاً عليه في القانون، ومحدداً له عقوبة، وذلك على أساس مبدأ شرعية الجرائم والعقوبات الذي يقضي بأنه لا جريمة ولا عقوبة بغير النص

على أنه إذا كانت هناك خصائص ذاتية للمسؤولية المدنية بالمقارنة بالمسؤولية الجنائية، فإن ذلك لا يمنع من أن تجتمع كل من المسؤوليتين معاً نتيجة عمل واحد، بمعنى أنه يمكن أن يترتب على العمل الواحد قيام المسؤوليتين معاً، وهذا يعني كذلك أنه لا يوجد تعارض بينهما في الالتقاء، إذ يمكن أن ينشأ عن الفعل الواحد مسؤولية جنائية ومسؤولية مدنية في وقت واحد معاً، كالقتل والسرقة والسب والقذف وفي المقابل يمكن أن توجد مسؤولية دون أخرى (سلطان، 2019).

3.2 المسؤولية الجنائية
يراد بالمسؤولية الجنائية صلاحية الشخص لتحمل الجزاء الجنائي عمّا يرتكب من جرائم إلا أن هذا التعريف غير كاف، لذلك يكون من اللازم لتحديد مفهوم المسؤولية الجنائية التعرض للأمور الآتية:

3.2.1 ظهور المسؤولية الجنائية
لقد كانت القوانين القديمة تخلط بين المسؤولية الجنائية والمسؤولية المدنية، حيث كانت فكرة التعويض وفكرة العقاب مختلطتين، فقد كان جزاء الفعل الضار هو الثأر ثم حلت الدية بعد ذلك محل الثأر فكان الجاني يشتري حق الثأر بدفع مبلغ من المال وبالتالي لم تكن المسؤولية الجنائية نوعاً منفصلاً عن المسؤولية المدنية (تناغو، 1991).
فانفصالها كان ثمرة تطور تاريخي طويل، ولم يظهر التمييز بين المسؤولية الجنائية والمسؤولية المدنية إلا عندما بدأت السلطة في الجماعة أو الدولة ترى أن هناك أفعالاً لا يقتصر خطرها على الفرد أو الأفراد الذي تقع عليهم الجريمة مباشرة، بل تجاوزهم إلى المجتمع في مجموعه، فلا يكفي فيها أداء الديّة للمضرور، بل يجب أن تفرض على مرتكبها عقوبة باسم المجتمع.

3.2.2 مفهوم المسؤولية الجنائية
تنحصر حدود البحث في تحدّيات القانون الدّبلوماسي والقنصلي في العالم المعاصر مع التركيز على الدبلوماسية الإمارتية أُنْمُوذَجًا؛ وبالتّالي فإنّ البحث لن يشير إلى نموذج الدبلوماسية للدّول العربية الأخرى ولا إلى الدّول غير العربية الأخرى.

4. ثالثا: ماهية انتهاك خصوصية البيانات
ان انتشار الحواسيب والأجهزة النقالة والتقنيات العلمية واعتماد المؤسسات الحكومية والخاصة على جودة وكفاءة تلك النظم المعلوماتية قد ادت الى حمايتها من أيدي قراصنة المعلومات والهاكرز والمخترقون وذلك كي لا يتم تسبيب أي فجوات امنية وتعطيل للبيانات الخاصة بمؤسسات الدولة عن طريق الاختراق السيبراني الذي يتم من قبل المجرمين.

تهديد خصوصيّة الأفراد ازداد بشكل يبعث على القلق في ظل المجتمع المعلوماتي خاصة مع انتشار بنوك المعلومات (الموني، 2018)، حيث تعتمد اليوم الكثير من المؤسسات والشركات عليها لما لها من قدرات هائلة تجعلها قادرة على عمليّة دمج وتخزين ومعالجة واسترجاع ونقل كم رهيب من بيانات خاصة بأفراد المجتمع في قطاعاته المختلفة وخاصة العاملين في هذه المؤسسات أو الشركات (عفيفي، 2015).

ويمكن تعريف بنوك المعلومات، بأنها تلك التي تقوم بعملية تخزين المعلومات بطريقة تسمح بتقديم معلومات أو بيانات عن الأفراد بصورة تمكن من التعرف على أشخاصهم سواء من خلال أسمائهم أو بأي وسيلة أخرى، أو بعبارة أخرى، تعني تلك البنوك بتكوين قاعدة بيانات تفيد موضوعاً معيناً وتهدف لخدمة غرض معين ومعالجتها بواسطة أجهزة الحاسبات الإلكترونيّة لإخراجها في صورة معلومات تفيد مستخدمين MSen مختلفين في أغراض متعددة (قايد، 2016).

صور الاعتداء على الخصوصية المعلوماتية: وتتمثل سلوكيات الاعتداء على الخصوصية الفردية في الآتي: اولا الاطلاع المجرد: محل الاطلاع في هذه الحالة هو معلومات شخصية وخاصة يريد صاحبها إبقاءها سرية، ولما صورة هذا السلوك هو الاطلاع الكلي أو الجزئي على تلك الأسرار الخاصة بحيث يقوم اليقين بالعلم بها وفهمها، فإذا كانت الأسرار بلغة لا يفهمها الفاعل أولا يحسن تحليلها، لم يتحقق الاطلاع إلا بتكامل الصورة وترابط أجزائها فإذا لم يكن ما اطلع عليه الفاعل سوى جزيئات غير مترابطة، غير ذات معنى مفيد لم يتحقق الاطلاع أيضا، وهذا الاطلاع يجب أن يكون في ذاته غير مشروع وان يتم من شخص لا يملك قانونا ترخيصاً بالولوج إلى تلك المعلومات، كما يشترط لتحقق هذه الصورة أن يكون الاطلاع مجردة أي أن يكون قصد الفاعل هو الاطلاع فحسب على تلك المعلومات السرية ومجرد العلم الشخصي بها (العزام، 2009).

ومثال ذلك أن يقوم الشخص العالم بأوجه الدخول إلى أنظمة الغير بالتسلل إلى أنظمة الحاسب الآلي لشخص آخر وإعطائه الأوامر اللازمة بفتح ملفات الشخص المعتدى عليه والاطلاع عليها عن طريق المشاهدة على شاشة عرض جهازه هو، إن هذا الفعل يشكل خرق للسرية والخصوصية وذلك أن السر إنما جعل سرا لكونه يخفي ما لا يرغب الإنسان في إظهاره لعلة شخصية قد تتعلق بسلوك أو مصلحة إذا أفشت عادت بالضرر على صاحبها (شقيري، 2018).

الاطلاع بقصد الافشاء: في هذه الحالة لا يكون الاطلاع على الأسرار الخاصة المخزنة في الحاسب مجردة وإنما لتحقيق غرض او هدف معين وهو إنشاء تلك الأسرار.

يقوم بهذا السلوك إما الشخص المتاح له بحكم عمله الاطلاع على المعلومات والبيانات الخاصة السرية، كموظف في مستشفى او دائرة الأحوال المدنية أو محكمة، وهذا ما يسمى بإفشاء الأسرار المهنية هذا إذا كانت اسرار خاصة في حين إذا كانت بيانات إسمية عموما لا تتصف بالسرية هنا يفرق بين سلوكي الاعتداء عليها أدناه فيما يتعلق بإفشاء الأسرار.

وتجدر الإشارة إلى أن نصوص التجريم الحديثة لا تنطبق على هذه الحالة؛ لأن جل القوانين تصدت لهذه الجريمة بنصوص عقابية كافية وحددت من خلالها بنيان الجريمة والتي لابد أن يكون الإفشاء من طرف موظف أو مستخدم كشرط مفترض.

بينما محل البحث هو من يتوصل إلى تلك المعلومات السرية الالكترونية بخبرته ودرايته بأنظمة المعلومات لتحقيق اختراقات او اتصالات بعدية او مباشرة مع الحاسوب الموجودة به تلك الأسرار بحيث يتمكن من الاطلاع عليها وإفشائها.

ويمكن أن يشكل الحاسب الآلي وسيلة أكثر فعالية في نشر الأسرار بشمولية وتوسع كبيرين وبسرعة وكفاءة عاليتين؛ ويتحقق ذلك باستخدام قنوات الاتصال المتعددة التي تتيحها انظمة الاتصالات المعلوماتية الحديثة، مع ظهور الانترنت بشكل خاص. ثالثا الابتزاز يمثل التهديد بالاستغلال غير المشروع للأسرار الشخصية، حيث يستغل الفاعل ما يتحصل عليه من معلومات الكترونية سرية وذات علاقة بالحياة الشخصية للأفراد في تحقيق منافع مادية أو معنوية، وذلك بتهديد صاحب الأسرار بإفشائها أو فضح أمرها في حال عدم تحقيق مطالبه، ولابد أن يكون لهذا الشخص القدرة على تنفيذ تهديداته (العزام، 2020).

رابعاً الاحتفاظ بنسخة: قد يتم التوصل إلى المعلومات السرية الالكترونية بكل سهولة ونسخها بسرعة فائقة، والخطورة تكمن هنا في إمكانية استخدام تلك المعلومات السرية الخاصة في المستقبل لتحقيق أغراض غير مشروعة. فكل اشكال الاعتداء الواقعة على سرية الخصوصية المعلوماتية ترتكب بطبيعة الحال بوسائل تقنية معلوماتية سهلت وبشكل كبير في ذلك الأمر الذي يتطلب دراسة مختصرة عن هته الوسائل، والمتمثلة في عناصر النظم المعلوماتية.

تعد التكنولوجيا الحديثة وتقنيات الذكاء الاصطناعي من الميادين الحديثة التي تستقطب اهتمام العلماء والباحثين في هذا المجال والتي تشهد تطورات عديدة مستمرة ، وقد اثرت في عدة ظواهر في هذا القرن الحديث ، كما انها أدت الى ظهور تطبيقات وبرامج جديدة تتميز بالتنوع والابتكار المستمر، حيث ان استخدام التكنولوجيا تعد من الركائز الأساسية والتي تعتمد عليها اغلب الدول في العصر الحالي الحديث، وذلك لكونها مفعمة بالعديد من الفوائد الكبيرة منها؛ سرعة نقل وتبادل المعلومات والبيانات وذلك بتوفير الوقت والجهد ، حيث ان هذه النظم المعلوماتية أصبحت اليوم مستودع ضخم يضم العديد من البيانات المتعلقة بالمعلومات الشخصية وتضم كذلك البيانات الاقتصادية والمالية والأمنية المتعلقة بمؤسسات الدولة.

ففي الآونة الأخيرة اتجهت التطبيقات الحديثة لتقنيات المعلومات لاستخدام الذكاء الاصطناعي والأنظمة الذكية في عالم الإدارة، المال والأعمال، والامن الشرطي والحروب النفسية وكذا الاستفادة من قدرة تلك النظم الذكية وتطبيقاتها على اتخاذ

القرارات الخاصة بالظواهر الخارجية في المجتمع مثل القدرة على الحسابات والقدرة على قيادة السيارة بدون سائق وغيرها من الأمور الأخرى.
ومع ظهور الكثير من أنواع كيانات الذكاء الاصطناعي والتي أصبحت تحاكي السلوك البشري ظهر نوع جديد من الجرائم هي الجرائم التي تتم عبر الهجمات السيبرانية.
ومنذ بروز هذه التكنولوجيا الإلكترونية والمعلوماتية في فجر الألفية الثالثة، راحت المجتمعات تتغير تغيرًا سريعًا وجذريًا، حيث أدت الأهمية المتزايدة للمعرفة إلى جانب العولمة والآثار المترتبة على التطوّر التكنولوجي في عصر الثورة الصناعية الرابعة إلى إيجاد عالم مختلف تمامًا. ذلك أنّ هذه الثورة الصناعية الرابعة التي تختلف عن الثورات السابقة في شدتها وتعقيدها واتساع نطاقها، بحكم استنادها في جوهرها إلى ظاهرة تكنولوجية جديدة اسمها التحول الرقمي أي اندماج التكنولوجيات الرقمية وتغلغلها السريع في البنية التحتية لكل شركة ومؤسسة وحكومة.

أفرز التقدم التقني - رغم إيجابياته الكثيرة- العديد من السلبيات، حيث أساء البعض استخدام الإمكانيات التي تقدمها شبكة المعلومات الدولية في ارتكاب أفعال تندرج تحت طائلة القانون، والجرائم التي ترتكب عبر شبكة المعلومات الدولية بعضها تقليدي، وبعضها الآخر مستحدث أي جرائم موجودة من قبل ولكن تطورت مع دخول التكنولوجيا الحديثة والذكاء الاصطناعي، فظهرت تحويرات لتبدو وكأنها جرائم جديدة.
الا ان هذه التقنيات الالكترونية قد ظهرت عليها تهديدات ومخاطر من قبل قراصنة المعلومات يستهدفون فيها الأنظمة الأمنية والتي تمس الامن القومي، حيث ان التهديدات التي تتعرض لها البيانات والمعلومات المخزنة الكترونية باتت في خطر يهدد سلامتها وسريتها، وذلك نتيجة لسوء استخدام هذه التكنولوجيا الحديثة عن طريق الاختراق والهجوم الذي يحصل ضد الامن السيبراني والذي يوضع لحمايته.
ويشترط أن يتحقق السلوك الإجرامي بغير رضاء المجني عليه أو دون إذنه. ومن ثم تعد هذه الجريمة إحدى صور انتهاك الحق في الخصوصية أو الاعتداء على حرمة الحياة الخاصة (الجندي، 2017).
تتحقق هذه الصورة الإجرامية بتعطيل أو إعاقة النظام المعلوماتي عن القيام بوظائفه المعتادة، إذ يترتب على ذلك توقف النظام عن العمل بشكلٍ تامٍ أو تباطؤ واضطراب في عمله مما يؤدي إلى إصدار نتائج غير صحيحة ومخالفة للحالة المعهودة لعمل النظام، ولو لم ينتج عن ذلك توقف تام للعمل في النظام، وتعرف جريمة تعطيل أو إعاقة النظام بأنها "الاعتداء على نظم المعالجة الآلية للمعلومات بمنعها من أداء وظائفها بصورة تامة أو إجراء تعديل في تلك الوظائف (صالح، 2013) هي "كل فعل يتسبب في توقف أو تباطؤ أو ارتباك عمل نظام المعالجة ومن ثم ينتج ذلك تغيير في حالة عمل النظام (طه، 1999).
إن محل السلوك الإجرامي هو اعتراض المعلومات، وهي كل ما يمكن تخزينه ومعالجته وتوليده ونقله باستخدام وسائل تقنية المعلومات وبوجه خاص الكتابة والصور الثابتة والمتحركة والصوت والأرقام والحروف والرموز والإشارات وغيرها
والمعلومات الالكترونية: هي أي معلومات يمكن تخزينها ومعالجتها وتوليدها ونقلها بوسائل تقنية المعلومات وبوجه خاص الكتابة والصور والصوت والأرقام والحروف والرموز والإشارات وغيرها
والبيانات: البيانات والمعلومات الالكترونية، كل ما يمكن تخزينه أو معالجته او إنشاؤه أو نقله باستخدام وسيلة تقنية المعلومات، وبوجه خاص الكتابة أو الصور أو الصوت أو الأرقام أو الحروف او الرموز أو الإشارات وغيرها او كل ما يمكن إنشاؤه أو تخزينه أو معالجته أو تخليقه او نقله او مشاركته او نسخه، بواسطة تقنية المعلومات، كالأرقام والأكراد والشفرات والحروف والرموز والإشارات والصور والأصوات، وما في حكمها وأيضاً كل ما هو متداول عن طريق شبكة معلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها: وشبكة معلوماتية: مجموعة من الأجهزة او نظم المعلومات تكون مرتبطة معاً، ويمكنها تبادل المعلومات والاتصالات فيما بينها، ومنها الشبكات الخاصة والعامة وشبكات المعلومات الدولية، والتطبيقات المستخدمة عليها

5. الخاتمة

تناولت الدراسة الوسائل التشريعية للمسؤولية الجنائية عن انتهاك الخصوصية على الأنظمة المعلوماتية:

5.1 النتائج

1) مع تزايد استخدام أنظمة الذكاء الاصطناعي والتي أصبحت بين يدينا في عصرنا هذا، نتوقع من خلال الدراسة التي سنقوم بها بأن البيانات والبرمجيات الخاصة في أنظمة الذكاء الاصطناعي هي محل الاعتداء في تلك الجرائم السيبرانية وقراصنة المعلومات يقومون باختراق تلك النظم والبرمجيات والبيانات الإلكترونية.

2) استحداث قانون مرن يتواكب مع الجرائم الإلكترونية والأمن السيبراني والتي يتوقع أن تكون بصورة طردية مع المشكلة الخاصة بالبحث، أي انه يمكن الاستنتاج من خلال البحث على ضرورة التعديل على قانون الجرائم الإلكترونية بصورة مستمرة، أي كل ما ظهرت أنواع جديدة من الجرائم كل ما تم إدراج نصوص عقابية وتجريميه لها، حيث ان المشرع الإماراتي والذي تطرقنا به بصورة بحته قد اظهر في سياقه وأوضح الجرائم والعقوبات المطبقة والتي نص عليها عند ارتكاب قراصنة المعلومات لهذه الجرائم ، كما أنَّ ذات القانون قد بين واستحدث مفاهيم جديدة ومنها الروبوت الإلكتروني والاختراق والهجمات الإلكترونية والسيبرانية والتي تم تكن موضحة في التشريع الإماراتي القديم من المرسوم الاتحادي رقم 5 لسنة 2012.
3) من النتائج والحلول التي قد يتم التوصل لها لموضوع الأمن السيبراني وتدمير الأنظمة الإلكترونية من قبل قراصنة المعلومات هي ابتكار جدار حماية بواسطة برمجيات ورموز مشفرة أمنية يحد من اختراق البشر العاديين وقراصنة المعلومات المحترفين.
4) بالنسبة للتنبؤ بالجريمة قبل وقوعها.. سنتوصل إلى ما يعرف " بالشرطة التنبؤية " والتي تجمع حلول التنبؤ وتقي من حدوث الجرائم سواء كانت إلكترونية أم عادية وذلك باستخدام تقنيات المعلومات المختلفة وأنظمة الذكاء الاصطناعي بإمكانات تحليلية قوية ومجموعة غنية من البيانات المتكاملة المستمدة من تطبيقات نظم المعلومات والخوارزميات، وتقوم فكرة هذه الأنظمة على تزويد الأجهزة الأمنية بوسائل التكنلوجيا الذكية وتحقيق أفضل استخدام للأشخاص والمعلومات المتوفرة لمراقبة اتجاهات الجريمة وقياسها ومن ثم التنبؤ بها قبل وقوعها.
5) أن جريمة الاختراق وما يتبعها من جرائم الكترونية، لا يمكن أن تتم إلا عن طريق هذه الشبكة فالمعلومات المدونة في الحاسوب الخاص، الذي لم يرتبط بالإنترنت لا يمكن اختراقه.
6) ما يميز جريمة الاختراق السيبراني هي أنها جرائم سريعة التنفيذ إذ أنه وفي أغلب الأحيان لا يكون الركن المادي سوى ضغط على مفتاح معين في الجهاز مع إمكان تنفيذ ذلك عن بعد دون اشتراط التواجد في مسرح الجريمة ولهذا فأن الجريمة الالكترونية ولسهولة ارتكابها شكلت عنصر إغراء للمجرمين وإذ أن ارتكابها لا يتعدى سوى توفر إمكانية استغلال التكنولوجيا والتقنية الحديثة خصوصا عندما يكون الجاني موظفا عاما أو في إحدى الشركات التي تعتمد على الحاسب الآلي في طبيعة عملها المتعلق بالمعلومات أو الأموال بحيث يكون لديها كافة المعلومات اللازمة لتحقيق اختراقات متعددة ومتتالية لأنظمة الحاسب الآلي في الشركة وتحقيق أرباح طائلة. ولهذا نشأت الحاجة لوجود طرق حماية قوية للمعلومات المخزنة في أجهزة حاسوب أو وسائط نقل الكترونية ومثال ذلك ما يسمى بجدران الحماية أو الجدران النارية وهي عبرة عن برامج حماية تمنع الاختراق أو الدخول غير المصرح به.

5.2 التوصيات

1) قيام المشرع الإماراتي بتعريف الهجوم السيبراني والاختراق السيبراني في نص المادة الأولى من المرسوم بقانون اتحادي رقم (34) لسنة 2011.
2) تخصيص مادة قانونية في قانون الشائعات والجرائم الإلكترونية تجرم استخدام أنظمة الاختراق في ارتكاب الجريمة.
3) استحداث عقوبة خاصة في قانون الجرائم والعقوبات على جريمة اختراق الأنظمة المعلوماتية الحكومية.
4) قيام المشرع الإماراتي بتحديد أنواع أنظمة الاختراق السيبراني للأنظمة المعلوماتية الحكومية.

المراجع

Afifi, K. A. (2015) *Assault on electronic data*. Cairo: Dar Al-Nahda Al-Arabiya.
Al-Ahwani, H. E. K. (2014). *Cybercrime*. Cairo: Dar Al-Nahda Al-Arabiya.
Al-Azzam, S. M. (2009). *Al-Wajeez in cybercrime*. University of Jordan Library Department.
Al-Azzam, S. M. (2020). *Al-Wajeez in cybercrime*. Amman: Wael Publishing House.
Al-Mouni, N. A. Q. (2018). *Cybercrime*. Cairo: Dar Al-Nahda Al-Arabiya.
Fahim, A. S. (1999). *The general theory of criminal responsibility for crimes of persons and status*. Basra: Al-Haddad Press
Imam, M. K. E. (2002), *The basis of criminal responsibility in positive law and Islamic law* [Unpublished PhD thesis]. Faculty of Law Library.
Maswar, H. W. (1992). *The general theory of commitment, part I: sources of commitment*. Damascus: New Edition.
Mohamed, A. (1980). *Penal code, general section*. Alexandria: University Press.
Hatata, M. N. (1975). *Social defense between Sharia and law*. Cairo: Wahba Library.

Qaid, O. A. (2016). *Cybercrime and information technology*. Cairo: Dar Al-Nahda Al-Arabiya.
Saleh, S. R. Y. (2013). *Criminal policy in the face of information crimes (an analytical study)* [PhD thesis]. Koya University.
Shuqairi, H. M. (2018). *Information confidentiality: its legal controls and rulings*. Beirut: Islamic Publishing House.
Sultan, A. (1990). *The general theory of commitment, part one: sources of commitment*. Cairo: Dar Al-Maaref.
Taha, A. H. (2000). *Crimes arising from the use of computers* [PhD thesis]. Tanta University.
Tanago, S. A. S. (1991). *The theory of commitment*. Alexandria: Knowledge Foundation.