AL HIKMAH RESEARCH & PUBLICATION CENTRE
Al-Hikmah International Journal for Islamic Studies & Human Sciences
E-ISSN: 2637-0581

مجلة الحكمة العالمية
للدراسات الإسلامية والعلوم الإنسانية
العدد 6، الرقم 4، ديسمبر 2023
E-ISSN: 2637-0581

جريمة الأمن السيبراني في انتهاك خصوصية البيانات والمعلومات وتحديد المسؤولية القانونية في دولة الإمارات دراسة وصفيه تحليلية

Cybersecurity Crime in Violating the Privacy of Data and Information and Determining Legal Liability in the UAE: A Descriptive and Analytical Study

محمد حسن مرداد عبيد Mohammed Hassan Merdad Obaid
University Sains Islam Malaysia (USIM)
merdad.24@yahoo.com

نور فضيلة بنت محمد علي Norfadhilah Binti Mohamad Ali
University Sains Islam Malaysia (USIM)
fadhilah.a@usim.edu.my

أحمد زكي بن صلاح Ahmad Zaki Bin Salleh
University Sains Islam Malaysia (USIM)
ahmadzaki@usim.edu.my

Article Progress

Received: 31 Oct 2023
Revised: 21 Nov 2023
Accepted: 8 Dec 2023

*Corresponding Author:
Mohammed Hassan Merdad Obaid

Email:
merdad.24@yahoo.com

ملخص البحث

تهدف الدراسة إلى معرفة الاختراقات والهجمات السيبرانية والاعتداء على الخصوصية المعلوماتية في للبيانات والمعلومات الشخصية وخاصة السرية منها، عبر الاطلاع الكلي أو الجزئي على تلك الأسرار وهذا الاطلاع يكون في ذاته غير مشروع وان يتم من شخص لا يملك قانونا ترخيصاً بالولوج إلى تلك المعلومات، واعتمد البحث على المنهج الوصفي التحليلي الاستقرائي الذي يعتمد على جمع البيانات والحقائق عن الظاهرة وعرض أبعادها من الناحية النظرية والعلمية مع المنهج المقارن لفهم مهام القانون الإلكتروني جراء الاختراقات والانتهاكات التي تتعرض لها المؤسّسات ذات البيانات الخاصة، بهدف الوصول الى نتائج موضوعيه تحقق الهدف من الدراسة، من أهمها هي ما يميز جريمة الاختراق السيبراني هي أنها جرائم سريعة التنفيذ عن بعد دون اشتراط التواجد في مسرح الجريمة وأن الجريمة الالكترونية شكلت عنصر إغراء للمجرمين في إمكانية استغلال التكنولوجيا والتقنية الحديثة خصوصاً عندما يكون الجاني موظفاً يعتمد على الحاسب الآلي في طبيعة عمله بحيث يكون لديها كافة المعلومات اللازمة لتحقيق اختراقات متعددة ومتتالية لأنظمة

الحاسب الآلي، والحاجة لوجود طرق حماية قوية للمعلومات المخزنة في أجهزة الحاسوب أو وسائط نقل البيانات الاكترونية بجدران الحماية، وخرج البحث بتوصيات اهمها تخصيص واستحداث مادة قانونية خاصة في قانون الجرائم الإلكترونية وحماية البيانات، تجرم استخدام أنظمة الاختراق السيبراني في جريمة اختراق الأنظمة المعلوماتية العامة والخاصة.

الكلمات المفتاحية: الأمن السيبراني – المسؤولية القانونية – انتهاك خصوصية – البيانات والمعلومات.

ABSTRACT

The study aims to know about cyber penetrations and attacks on information privacy in personal data and information, especially confidential ones, through complete or partial access to those secrets. This access is illegal if it is done by a person who does not legally have a license to access that information. the research relied on the descriptive analytical inductive approach, which relies on collecting data and facts about the phenomenon and presenting its dimensions theoretically and scientifically with the comparative approach to understand the tasks of electronic law as a result of the hacks and violations suffered by institutions with private data, with the aim of reaching objective results that achieve the goal of the study. The most important of them is that what distinguishes the crime of cyber hacking is that it is a crime that is quickly carried out remotely without requiring presence at the crime scene and that cybercrime constitutes an element of temptation for criminals in the possibility of exploiting technology and modern technology, especially when the perpetrator is an employee who relies on the computer in the nature of his work so that he has all The information necessary to achieve multiple and successive penetrations into computer systems, and the need for strong protection methods for information stored in computers or electronic data transmission media with firewalls, The research came up with recommendations, the most important of which is allocating and creating a special legal article in the Cybercrime and Data Protection Law that criminalizes the use of cyber-hacking systems in hacking public and private information systems.

Keywords: Cybersecurity - Legal Liability - Violation of Privacy - Data and Information.

المقدمة

بداية يوضح الباحث بأن المقصود بالأمن السيبراني هو حماية الأشياء من خلال تكنولوجيا المعلومات المتمثلة في الأجهزة والبرمجيات والأمن السيبراني يعني اتخاذ التدابير اللازمة لحماية الفضاء السيبراني من الهجمات السيبرانية وذلك من خلال مجموعة من الوسائل المستخدمة تقنياً وتنظيمياً وإدارياً في منع الوصول الغير مشروع للمعلومات الإلكترونية ومنع استغلالها بطريقة غير قانونية ونظامية وبذلك فإنه يهدف إلى الحفاظ على استمرارية الأنظمة والمعلومات المتوفرة بها وحمايتها بكل خصوصية وسرية من خلال اتباع التدابير والإجراءات اللازمة لحماية البيانات وننوه بأن مصطلح السيبرانية هو واحد من أكثر المصطلحات تردداً في معجم الأمن الدولي وهي تستخدم مجازا للمتحكم وتعبير التحكم الآلي.

وعلى ذلك نوضح بانه أدى التقدم التكنولوجي السريع والهائل والغير مسبوق وخصوصاً في تكنولوجيا المعلومات والاتصالات والاهتمام بالبنية التحتية الرقمية وتخزين المعلومات إلى الاهتمام بالبيانات داخل الدول والعمل على تطوير تكنولوجيا الاتصالات الرقمية والمحافظة على خصوصية هذه البيانات من أي أعمال تخريبية تؤدي إلى اختراق خصوصية هذه المعلومات التي تكون غالباً على قدر كبير من الخصوصية والأهمية حيث يستخدم مجرمو الإنترنت أساليب وتطبيقات تسمح لهم بالوصول إلى أنظمة البرامج الخاصة بالمعلومات الرقمية ومما يؤثر ذلك تهديد كبير على الأمن القومي والأمن الاقتصادي داخل الدولة ومن هنا كان الاهتمام بشكل فعّال في وضع الحماية القانونية للفضاء الإلكتروني بشكل عام بهدف الحماية من أي هجمات إلكترونية على تلك المعلومات والبيانات الرقمية العامة والحساسة ولعل اتضح بشكل رئيسي في قانون الجرائم الإلكترونية لدولة الإمارات العربية 2018.

مع ملاحظة بأن تلك الأعمال المتعلقة بالقرصنة الإلكترونية تتنوع بتنوع أهدافها فهناك جرائم ضد الأفراد أو ضد الحكومات أو ضد الملكية الفكرية والأدبية أو قد تستهدف سرقة الأموال أو سرقة المعلومات والبيانات الحساسة فضلاً عن تلك الأعمال قد تستهدف

أيضاً الجوانب الشخصية للإنسان مثل أعمال (التشهير – القذف – التهديد) وانتحال الشخصية والتحريض والابتزاز الإلكتروني (Hilali, 2012). وإزاء ذلك عملت الدول على وضع القوانين اللازمة لحماية الفضاء الإلكتروني وتعد دولة الإمارات العربية من الدول الرائدة في وضع القوانين في هذا الشأن نظراً لكونها دولة تعتمد بشكل كبير على المعلومات والبيانات الإلكترونية (Ramadan, 2008).

ومن هنا سوف نوضح في نطاق بحثنا المسؤوليات القانونية إزاء اختراق خصوصية البيانات والجرائم المعلوماتية. وعملت الدول على وضع اتفاقيات دوليه من أجل حماية خصوصية البيانات والتقليل قدر الإمكان من الجرائم المعلوماتية ولعلى من أهم هذه الاتفاقية هي اتفاقية بودابست الخاصة بالجرائم المعلوماتية حيث تضمنت هذه الاتفاقية اقساماً ثلاثة يتناول القسم الأول مجموعة الجرائم التي تتعرض لها شبكه الإنترنت والقسم الثاني يوضح الإجراءات الجنائية في مواجهة هذه الجرائم والقسم الثالث يوضح التعاون الدولي في مكافحة تلك الجرائم.

مشكلة البحث

ينوه الباحث إلى أنه على الرغم من الإيجابيات الهائلة التي تحققت بفضل تقنية المعلومات فإن تلك الثورة المعلوماتية المتصاعدة قد صاحبتها في المقابل جملة من الانعكاسات السلبية الخطيرة نتيجة سوء الاستخدام ومن بين تلك الانعكاسات المستحدثة ظاهرة الجريمة الرقمية واختراق خصوصية البيانات والتي تصاعدت أخطارها بدورها مما أفرز نوعاً جديداً من الجرائم العابرة للقارات التي لم تعد أخطارها وآثارها محصورة في نطاق دولة بعينها مما أثار بعض التحديات القانونية أمام الأجهزة المعنية بمكافحة الجريمة (Al-Munajjid, 2017).

وفي ضوء ذلك يتضح لنا إشكاليات البحث فيما يخص قواعد حماية الفضاء السيبراني وأمن المعلومات والعمل على حماية خصوصية البيانات سواء كان في البعد الاقتصادي والمتعلق بصناعة تكنولوجيا المعلومات والاتصالات وتطوير البرمجيات أو في مجال

التجارة الإلكترونية من خلال فتح سوق حر على شبكة الإنترنت أو من خلال البعد الأمني المتعلق بأن المعلومات والعمل على منع التهديد السيبراني وخير مثال على ذلك هو مركز تكامل استخبارات التهديد السيبراني بالولايات المتحدة الأمريكية الذي يعمل على التنسيق بين مختلف أجهزة الأمن الأمريكية الأخرى (Mohammed, 2020).

وعلى ذلك تبرز مشكلة البحث في هذا الصدد الحفاظ على مستويات الأمن السيبراني داخل الدولة وعلى وجه الخصوص عندما تكون أعمال الاختراق تدخل في عدة دول وذلك في ظل غياب معايير تحديد المسئوليات إزاء ذلك الاختراق الدولي مما يجعل الصعوبة واضحة في تحديد المسئولية والمتمثلة في معايير تحديد المسئول عن اختراق الأمن السيبراني ووضع كافة القيود والعقوبات الرادعة للحيلولة دون اختراق ذلك المجال (Al-Hafiz, 2016).

وعلى ذلك يتبع الأمن السيبراني نهجا محددا يتكون عادة من عدة طبقات للحماية تثبت في أجهزة الكمبيوتر أو الشبكات أو البرامج أو البيانات التي ينوي المستخدم حمايتها وفي ضوء ما سبق نوضح بان مشكلة موضوع البحث تدور في السرية ومدى التحكم في الولوج إلى البيانات وإتاحتها لمن يسمح لهم فقط و السلامة في معرفة الحفاظ على سلامة البيانات والمعلومات (Al-Nasser, 2020) وحمايتها من الهجمات التخريبية أو السرقة والجاهزية في جميع الأنظمة والخدمات والمعلومات وإتاحتها حسب طلب الشركة أو عملائها وعلى الرغم من إصدار دوله الإمارات العديد من القوانين لحمايه خصوصيه البيانات مثل المرسوم بقانون اتحادي رقم (34) لسنة 2021 بشأن الشائعات والجرائم الإلكترونية وغيره من القوانين المتعلقة بحمايه الخصوصية إلا أن تطور تلك التكنولوجيا وخصوصاً بشكل متقدم أدى إلى ظهور الإشكاليات الخاصة بحمايه البيانات علي المستوى المحلي والمستوى الدولي والعمل على الحفاظ على مستويات الأمن السيبراني داخل الدولة.

أسئلة البحث

تحدد أسئلة الدراسة بما يلي:

1. ماهية المسؤولية القانونية عن انتهاك خصوصية البيانات؟
2. من هي المؤسسات الحكومية التي من الممكن أن تكون عرضة للهجمات السيبرانية عن طريق الاختراق؟
3. ماهي الإجراءات القانونية الخاصة بحماية المؤسسات من الاختراق عبر الهجمات السيبرانية؟

أهداف البحث

يهدف البحث محل الدراسة في الأتي:

1. بيان ماهية المسؤولية القانونية عن انتهاك خصوصية البيانات.
2. تحديد المؤسسات الحكومية التي من الممكن أن تكون عرضة للهجمات السيبرانية عن طريق الاختراق.
3. البحث في الإجراءات القانونية الخاصة بحماية المؤسسات من الاختراق عبر الهجمات السيبرانية.

أهمية لدراسة

تتمثل أهمية هذا البحث في تناول موضوعاً حيوياً والخاص في جريمة الأمن السيبراني والمسؤولية القانونية في انتهاك خصوصية البيانات والمعلومات في قانون دولة الإمارات حيث يُعد النظام الرقمي من أهم ركائز الإدارية في منظومه الدولة. وتنبثق أهمية البحث من خلال:

- **الأهمية القانونية:** من خلال التعرف على الخصوصية الرقمية والقوانين المحلية والعالمية لتي اهتمت بهذا الحق والتشريعات القانونية الأممية والإماراتية في هذا المجال.

- **الأهمية العلمية:** من حلال أهمية البحث وتزويده للباحثين بمصدر جديد للمكتبة العربية حول الخصوصية الرقمية والمسؤولية القانونية في انتهاك البيانات والمعلومات في المواقع الإلكترونية.

منهج البحث

استخدم الباحث المنهجية الوصفية التحليلية الاستقرائية لتناول دراسة مهام القانون الإلكتروني جراء الاختراقات والانتهاكات التي تتعرض لها المؤسّسات ذات البيانات الخاصة وأمنها السيبراني ليستدل منها على حقائق تعم على الكل، باعتبار أن ما يسري على الجزء يسري على الكل.. ولعل أهم مجالاته ما يتعلق باستقراء اتجاهات أحكام القضاء في موضوع معين لبيان القاعدة التي تحكم الموضوع. للنصوص الواردة في قانون انتهاك الخصوصية في الجرائم الإلكترونية والامن السيبراني من حيث تطبيقات المسؤولية التقصيرية ومن حيث لزوم وجود ركن فعل الإضرار وتوفر وكذا تحليل عناصر المسؤولية القانونية المترتبة على هذا ووصولاً إلى كيفية تحديد الانتهاكات بيان العقوبات للخروج بنتائج وتوصيات تخدم مسار البحث.

الدراسات السابقة

ترتكز الدراسة محل البحث بشأن خصوصية البيانات ولا سيما في الوقت الراهن الذي يشهد تزايدا ملحوظاً لمختلف الأعمال المتعلقة باختراق خصوصية البيانات والآثار السلبية التي قد تنعكس علي البعد الاقتصادي والبعد الأمني في النطاق المحلي للدولة و المستوي العالمي ككل وبذلك نوضح بآن الأمن السيبراني وحماية خصوصية البيانات التي تعمل علي تعزيز حماية أنظمة التقنيات التشغيلية علي كافة الأصعدة والتصدي لهجمات وحوادث أمن المعلومات التي تستهدف المؤسسات علي اختلاف أنواعها والعمل علي توفير بيئة آمنه في مجتمع المعلومات والبيانات والحد من انعكاسات ظاهرة الجرائم الرقمية واختراق خصوصية البيانات والعمل علي وضع الاطار القانوني للأمن السيبراني المتعلق بانتهاك خصوصية

البيانات ووضع المسئوليات القانونية في ظل الاتفاقيات الدولية المنظمة لذلك الشأن الخاص بخصوصية البيانات والأمن السيبراني واذا ما سبق نوضح المعايير والمسئوليات القانونية بخصوصية البيانات والمعايير الدولية في خصوصية البيانات والأمن السيبرانى سواء ذلك علي المستوي الدولي وعلى المستوي دولة الإمارات العربية المتحدة وقد صدر القانون الاتحادي رقم 12 لسنه 2016 بتعديل المرسوم بقانون اتحاد يرقم 5 لسنه 2012 في شأن جرائم تقنيه المعلومات وغيره من القوانين المتعلقة بحمايه الخصوصية ومنع انتهاك البيانات الشخصية عند استخدام الوسائل الحديثة بالإضافة إلي القانون رقم 37 لسنه 1992 في شان العلامات التجارية وتعديلاته وعمل المشرع الإماراتي وفقا للقانون رقم 44 من قانون اللجنة الفيدرالية لدوله الإمارات العربية المتحدة 2021 علي إنشاء مكتب حمايه البيانات لتقديم التوجيه والإشراف علي الامتثال فضلا عن قانون حمايه البيانات رقم 5 لسنه 2020 .

قام الباحث بالاطلاع على مجموعة من الدراسات السابقة التي تغطي الفترة الزمنية (2015–2019) فيما يتعلق بمرسوم بقانون اتحادي رقم 5 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات وتعديلاته وخاصة المسؤوليات القانونية على المؤسسات جراء اخترق خصوصية البيانات: مشروع مقترح للإمارات العربية المتحدة. وقد خلص الباحث الى مجموعة من الدراسات التي تدعم مسار البحث وهي:

دراسة بعنوان "**الأمن القومي الإلكتروني وجرائم المعلومات**"(Al-Sayed, 2021) حيث بينت هذه الدراسة أنه في عصرنا الحاضر الذي يشهد ثورة معلوماتية ضخمة حيث تتسابق العلوم والاكتشافات في الظهور في كل يوم يشرق صاحبه معلنة بذلك منافسة قوية وحادة في هذا المجال، ففي بداية الأمر ظهرت الشبكة العنكبوتية (الإنترنت) باستخداماتها المحدودة غير أنها توسعت وانتشرت انتشاراً سريعاً وفي وقت قياسي وأصبح مستخدميها من جميع الفئات العمرية وعلى مختلف مستويات تعليمهم، وبذلك فتحت الأبواب المغلقة ودق ناقوس الخطر؛ حيث أن هذه الشبكة بقيت بدون حراسة وبدون قيود أو حدود لردع الأعمال السيئة التي مصدرها دائماً البشر. فشبكات التواصل الاجتماعي

يمكن أن تستخدم في إثارة الفوضى والشغب وتحقيق الانفلات الأمني من خلال بث شائعات مغرضة تتهم الحكومات بارتكاب أخطاء متعمدة أو إساءة استخدام السلطة أو عدم العناية بحقوق الشعب مما قد يؤدي إلى الاضطرابات والقلاقل الداخلية التي تزعزع الأمن والاستقرار كما حدث فيما يسمى بثورات الربيع العربي، حيث استخدمت شبكات التواصل الاجتماعي في إحداث فوضي وبلبلة ونشر شائعات وأخبار مغلوطة ومحاولات لبث الفتن بين فئات المجتمع الواحد كان لها بالغ الأثر في تقويض الأنظمة الحاكمة وإشاعة الفوضى والاضطراب وزعزعة الأمن الداخلي فقد تسهم إساءة استخدام شبكات التواصل الاجتماعي في زعزعة الأمن والاستقرار عن طريق ترويع وإفزاع الأفراد وإشاعة الفوضى وتهديد حالة الأمن والاستقرار وزعزعة الطمأنينة وبث روح الكراهية بين مختلف طبقات المجتمع أو منع السلطات العامة من ممارسة صلاحياتها أو تعطيل تطبيق الدستور والقوانين وتقويض النظام العام ما يترتب عليه تشتيت الجهود وانخفاض الروح المعنوية، بالإضافة إلى الانتقام من المجتمع وتهديد أمن وسلامة أفراده بسبب مشكلات نفسية واجتماعية تجلب الحقد في صدر بعض المستخدمين على المجتمع وتجعلهم يخرجون عن القانون. ومن خلال هذه الدراسة يتضح أنها لم تأتي بشكل مباشر بمعلومات حول مهام القانون الإلكتروني جراء الاختراقات التي تتعرض لها المؤسّسات ذات البيانات الخاصة وأمنها السيبراني، وهذا يعتبر نقص بها والدراسة الحالية سوف تكمل النقص الذي يعتري هذه الدراسة.

دراسة بعنوان:" **الجرائم الإلكترونية ومخاطرها**" (Al-Rahbani, 2020) وبينت الدراسة أنه لا شك بأن مفهوم الجريمة الإلكترونية يتشابه إلى حد ما الجرائم التقليدية من حيث أطراف الجريمة، كمجرم ذي دافع لارتكاب الجريمة، والضحية التي ربما تتحول من تقليدية إلى ضحية إلكترونية، ومن حيث الأدوات المستخدمة. وليس هناك إجماع على تعريف الجرائم الإلكترونية من حيث كيف تعرف؟ أو ما هي الجرائم التي تضمنتها الجريمة الإلكترونية؟ كما أن تعريف الجرائم التي ترتكب بأي نوع من المعدات والأجهزة الرقمية. وبينت أيضاً انه عرف الفقه الجريمة بما يلي: "الجريمة هي كل فعل أو امتناع جرم المشرع إتيانه

في نص من النصوص الجنائية، وقرر له عقوبة أو تدبير وقائياً بسبب ما يحدثه من اضطراب اجتماعي ويكون هذا الفعل أو الامتناع صادراً عن شخص أهل للمساءلة الجنائية". والجريمة تستلزم وجود نص تشريعي وهذا هو الركن المادي وتستلزم إضافة إلى ذلك بحث المسؤولية الجنائية بحيث لا يسأل هذا الشخص عن هذا الفعل أو الترك إلا إذا قام به بإرادة واختيار وهذا هو الركن المعنوي. وهذه الدراسة تلتقي مع الدراسة الحالية من حيث الموضوع حيث أنها تبين ماهية الجرائم الإلكترونية وكيفية التعامل معها، وإن الدراسة الحالية سوف تكمل النقص في هذه الدراسة وتتناول في كافة جوانبها مهام القانون الإلكتروني جراء الاختراقات التي تتعرض لها المؤسّسات ذات البيانات الخاصة وأمنها السيبراني وفق المرسوم بقانون اتحادي رقم (34) لسنة 2021 بشأن الشائعات والجرائم الإلكترونية.

ودراسة تناولت "**الوجيز في الجرائم الإلكترونية**" (Darragh, 2022) بينت الدراسة أنه تتميز الجريمة الإلكترونية عن الجريمة التقليدية في تعريفها وخصائصها وأركانها، فهي من الجرائم الحديثة التي لها طبيعة خاصة تختلف عن بقية الجرائم، وتعرف هذه الجرائم بالعديد من المسمّيات كالجرائم المعلوماتية، وجرائم تقنية المعلومات وجرائم السيبرانية، وجرائم الحاسوب والإنترنت أو الجرائم الإلكترونية ونظراً لحداثة الجرائم الإلكترونية فلا يوجد لها تعريفاً جامعاً وشاملاً نتيجة للتطور المستمر والمتسارع لتكنولوجيا المعلومات والاتصالات الحديثة، فالجرائم الإلكترونية لشكل أعمالاً إجراميةً غير شرعية ترتكب باستخدام الأجهزة الإلكترونية كأداة فاعلة، أو على الحاسوب والأنظمة الإلكترونية الأخرى كمحل وهدف للجريمة وقد تعددت التسميات بشأن هذه الظاهرة الإجرامية، فأحياناً تسمى جرائم تقنية المعلومات، ومرة أخرى تسمى جرائم الحاسوب والإنترنت، ومرة ثالثة جرائم السيبرانية، ونلاحظ أن جميع تلك التسميات تحمل ذات المضمون بحيث يمكن تسميتها بالجريمة الإلكترونية هذا ولم يستقر الفقه على تعريف موحد للجريمة الإلكترونية كونها مرتبطة بتكنولوجيا المعلومات والتقنيات الحديثة، لذلك تعددت التعريفات الفقهية بهذا الخصوص، فقد عرفها الفقه الفرنسي على أنها: "مجموعة من الأفعال المرتبطة بالمعلوماتية والتي يمكن أن تكون جديرة

بالعقاب"(4)، وقد عرفها البعض الآخر بأنها: "أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية والجريمة التي تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية" وهذه الدراسة تفيدنا في مجال الإطار النظري للدراسة الحالية من خلال بيان طبيعة الاختراق والأمن السبراني وفق أحكام المرسوم بقانون اتحادي رقم (34) لسنة 2021.

وبحث **"الجرائم الإلكترونية"** (Al-Badaina, 2014) وتناول خلالها الجرائم الالكترونية من حيث المفهوم والاسباب بيت ان الجريمة الإلكترونية أو الافتراضية (crimes cyber)تتكون من مقطعين هما الجريمة (crime) والإلكترونية (cyber) ويستخدم مصطلح الإلكترونية لوصف فكرة جزء من الحاسب أو عصر المعلومات. أما الجريمة فهي السلوكيات والأفعال الخارجة على القانون. والجرائم الإلكترونية هي " المخالفات التي ترتكب ضد الأفراد أو المجموعات من الأفراد بدافع الجريمة وبقصد إيذاء سمعة الضحية أو أذى مادي او عقلي للضحية مباشر او غير مباشر باستخدام شبكات الاتصالات مثل الإنترنت (مثل غرف الدردشة، والبريد الإلكتروني، والموبايل (.Taishankar&Halder 2011) ويمثل جوهر الجريمة الإلكترونية. أبعد من هذا الوصف، ومع ذلك، فالأعمال ذات الصلة بالحاسوب لأغراض شخصية أو تحقيق مكاسب مالية أو ضرر، بما في ذلك أشكال الجرائم المتصلة بالهوية، والأفعال المتعلقة بمحتويات الكمبيوتر جميعها تقع ضمن معنى أوسع لمصطلح "الجريمة الإلكترونية". (2013)، كما تتناول أسباب الجريمة الإلكترونية، حيث تم تصنيف هذه الأسباب على ثلاثة مستويات من النظم هي: النظام الشخصي، والنظام الوسيط والنظام الكلي. فقد انطلقت من أن الجرائم الإلكترونية هي الأفعال الإجرامية التي ترتكب بواسطة الحاسب أو النطاق التقني مثل الإنترنت والشبكات، أو التي يكون فيها الحاسب والحيز التقني مستهدف للجريمة الإلكترونية. وتشمل الجرائم الإلكترونية ضمن هذا التحديد وليس حصرا على (الإرهاب الإلكتروني، والاحتيال وسرقة الهوية، والملاحقة والتحرش، وبريد النفايات، والفيروسات، وشم كلمات السر، والقنابل الذكية. وتتلخص أسباب الجرائم

الإلكترونية بانها ظاهرة اجتماعية متوافقة مع انتقال المجتمعات إلى المجتمع الرقمي، حيث انتقل نشاط الناس من الواقع الفعلي (المادي) إلى الواقع الافتراضي، وهي جريمة عابرة للحدود الوطنية. وقد سهل انتشار الجرائم الإلكترونية سهولة الوصول للمستهدفين وانخفاض الكلفة، والغفلة في تنفيذها وضعف الرقابة والسرعة في تنفيذها وتوظيف الاتصالات والتفاعلات في ارتكابها، وقلة الخطورة على الجناة، وسرعة الكسب غير المشروع، والفرص المتاحة لارتكابها، والضغوط الشخصية والعامة على الجناة، وضعف الرقابة عامة. كما ساهمت عوامل التحضر السريع، والبطالة والرغبة بسرعة الثراء، وضعف التشريعات وضعف أدوات الحماية، وتوافر الفرصة لارتكابها وغياب الحراسة التقنية في انتشارها. وينفذها شباب يسعون للشهرة أو مجرمون محترفون يسعون للكسب والثراء، أو الإرهاب الذي يتربص بالدول العربية والإسلامية.

وبحث" **جريمة الاختراق الإلكتروني" للكاتب**" (Swailem, 2021) حيث تناول الحرب الالكترونية في الفضاء السيبراني حيث اوضح ان الفضاء السيبراني والطيف الكهرومغناطيسي جزءً من العمليات العسكرية الحديثة، حيث تستخدم القوات العسكرية أنواعا عديدة من الأجهزة الإلكترونية المتصلة بالشبكة وأنظمة اتصالات المعلومات في ساحة المعركة. ويعد استخدام هذه الأنظمة المتصلة بالشبكة ضروريا لتحقيق التفوق التشغيلي. على الصعيد الآخر، تساهم الحرب الإلكترونية في الطيف الكهرومغناطيسي في تحقيق التفوق المعلوماتي ونجاح العمليات العسكرية باستخدام التكتيكات والتقنيات والإجراءات الهجومية والدفاعية. إلى جانب ذلك، تعمل أنظمة اتصالات المعلومات الإلكترونية المتصلة بالشبكة في الفضاء السيبراني والطيف الكهرومغناطيسي، وتخلق بيئة عمليات عسكرية مشتركة متداخلة. هذه البيئة هي المجال الكهرومغناطيسي السيبراني. في هذا المجال، يتم إجراء عمليات كهرومغناطيسية إلكترونية متزامنة ومتكاملة. وتعتبر الحرب الإلكترونية التي تُستخدم ضد أنظمة اتصالات المعلومات الشبكية للعدو، أو لحماية أنظمتنا المماثلة، هي القدرة الرئيسية لهذه العمليات.

بحث" **الأمن السـيبراني**" (Cyber Security, 2017) بين الباحث ان هناك العديد من الخيارات لدولة تريد تحسـين أمنها السـيبراني، وبالتعاون مع مختلف الوكالات الدولية، لأنه من الصـعب إدانة الجاني بسـبب اختلاف القوانين بين الدول الأخرى، ولأن طبيعة الإنترنت تخلق مسـألة الاختصـاص القضـائي حول مكان ارتكاب الجريمة، حيث يمكن لأي شـخص يجلس في جزء من العالم الاعتداء على العالم ككل. الى جانب ذلك، تختلف القوانين من دولة إلى أخرى ويصـعب القبض على المهاجم إذا بدأ الجريمة من دولة مختلفة ويصـعب معاقبة الجاني إذا كان قانون تلك الدولة مختلفا في حالة معينة. لذلك، يجب أن يوفر القانون المعياري الحماية ضـد جرائم الإنترنت وأن يحمي المعلومات والبنية التحتية الوطنية والحقوق المتعلقة بالممتلكات الفردية. فعلى سـبيل المثال، تعرضـت دولة الإمارات العربية المتحدة لهجمات سـيبرانية عديدة في السـنوات الاخيرة الماضـية نتيجة انتشـار الإنترنت واسـتخدام الأنظمة القائمة على الإنترنت في البنية التحتية الحيوية. لذلك، تم تكليف اتفاقية بشـأن القانون السـيبراني من قبل دولة الإمارات العربية المتحدة بصـفتها دولة موقعة وافقت على افتتاح الاتفاقية. وقررت الولاية القضـائية في وقت لاحق تنفيذ قانون جديد من خلال رؤية نمو الجريمة الإلكترونية في جميع أنحاء العالم حيث كان الجناة يهربون بسـهولة بعد ارتكاب الجريمة. ومن ثم تم تشـكيل الاختصـاص القضـائي لتطبيق قانون لمراقبة مثل هذه الأعمال.

بحث" **أمن المعلومات**" (Shackelford, Scott J, 2017) في قضية اختيار الآلية المناسبة لتسوية النزاعات القائمة بين شركات التكنولوجيا الفائقة وشركائها ومورديها وعملائها وأصحاب المصلحة الآخرين في قضايا معقدة تتعلق ببراءات الاختراع وحقوق الملكية الفكرية، وقرصنة المنتجات، والتزوير، والإنترنت والأمن السيبراني، والعديد من القضايا المتعلقة بالتسويق والحقوق الإقليمية لبيع المنتجات العلمية. وأشار الباحثون أنه عندما تنشأ مثل هذه النزاعات يجب على الشركات أن تكون مستعدة لتسويتها مع آلية حل النزاع الأكثر ملاءمة. وتبين من قبل الباحثين أن التحكيم الإلكتروني هو الآلية المناسبة

والمفضلة للنزاعات عالية التقنية على المستويات الدولية لصعوبة معالجة هذه القضايا في المحاكم التقليدية.

بحث" **الأمن الإلكتروني السيبراني**" (Imranuddin, 2017) حيث تناول خلالها قواعد المسؤولية في قوانين الإنترنت الحالية في دولة الإمارات العربية المتحدة. ويتضمن ذلك شرحًا موجزًا لكل قانون. الحالات المثيرة للجرائم الإلكترونية جنبًا إلى جنب مع توضيح كيفية تأثير وجود القوانين السيبرانية أو عدم وجودها على محاكمة الأفراد المعنيين. تم توضيح سيناريو وضع قوانين للتعامل مع الحالات الصعبة المقاضاة. استمرارًا لذلك، دراسة مقارنة لهذه القوانين والقوانين الموجودة في الدول المتقدمة تقنيًا مثل الولايات المتحدة الأمريكية وإنجلترا ودول أخرى. هناك تركيز خاص على إنجلترا لأنها من أوائل الدول التي طبقت قوانين الإنترنت ردًا على الجرائم الإلكترونية. أخيرًا، تم تضمين خطوات موحية يمكن أن تحسن بشكل كبير من السيطرة على الجرائم الإلكترونية، خاصة في المناطق سريعة التطور مثل الإمارات العربية المتحدة. لطالما كانت الإمارات العربية المتحدة سلبية إلى حد ما عندما يتعلق الأمر بالتعاون الدولي في مجال الأمن، القوة الدافعة الرئيسية للبحث هي الأهمية المتزايدة باستمرار للأمن السيبراني في جميع أنحاء العالم، وخاصة في الإمارات العربية المتحدة.

وهذه الدراسة تتناول **جريمة اختراق الأمن السيبراني في انتهاك خصوصية البيانات والمعلومات في قانون دولة الإمارات العربية**، وتم دراسة مفهوم الامن السيبراني ومعرفة ماهية البيانات والمعلومات الالكترونية وبيان المسؤولية القانونية تجاه انتهاك خصوصية هذه البيانات والمعلومات وصور الاعتداء على هذه الخصوصية ومعرفة القصد الجنائي لانتهاك خصوصية البيانات، والذي خرج بمجموعة من النتائج وتوصيات تساهم في الحد من هذه الانتهاك الخطير والتي يمكن تفصيلها في التالي:

أولاً/ الامن السيبراني:

قوانين الأمن الإلكتروني أو كما تسمى غالباً بـ «**الأمن السيبراني**» هي لوائح تشتمل على توجيهات متخصصة لحماية تقنية المعلومات وأنظمة الحاسب بغرض إجبار الشركات

والمؤسسات على حماية أنظمتها ومعلوماتها من الهجمات الإلكترونية مثل الفيروسات والديدان وأحصنة طروادة والتصيد وهجمات رفض الخدمة (DOS) والوصول غير المصرح به كسرقة الملكية الفكرية أو المعلومات السرية وهجمات نظام التحكم وغيرها. هناك العديد من التدابير المتاحة لمنع الهجمات الإلكترونية. تشمل هذه التدابير في الأمن السيبراني بناء سياسات وضوابط وأنظمة مثل إنشاء جدران الحماية وبرامج مكافحة الفيروسات وأنظمة كشف التسلل والوقاية منها والتشفير وكلمات المرور في عمليات تسجيل الدخول. كانت ولازالت هناك محاولات لتحسين الأمن السيبراني من خلال التنظيم والجهود التعاونية بين الحكومة والقطاع الخاص لتشجيع التحسينات الطوعية للأمن السيبراني. لاحظ مسؤولين ومنظمين الصناعة، بما في ذلك المنظمون والشركاء المصرفيون المخاطر الناجمة عن الأمن السيبراني وبدأوا يخططون للبدء في إدراج الأمن السيبراني كجانب من جوانب الاختبارات التنظيمية (PwC, 2015).

حيث يعد الهجوم السيبراني واحدًا من أحدث أنواع الأخطار الرقمية التي تواجه الإنسان في وقتنا الحالي، وفيه يتعرض الشخص أو الجهة أو المؤسسة أو حتى الدولة إلى هجمات إلكترونية الغرض منها تعطيل أو تدمير أو الدخول الغير مصرح إلى بيانات ذات قيمة أو حساسة للجهة أو الطرف الذي يتعرض للهجوم، وقد تحدث الهجمات الإلكترونية للأشخاص لا بسبب قيمة البيانات أو المعلومات التي يمتلكونها، ولكن بسبب كونهم حلقة وصل بين أطراف أخرى ذات قيمة يصعب الوصول إليهم، أو كونهم يمتلكون صلاحية للوصول إلى أجهزة وتقنيات يصعب اختراقها بطريقة مباشرة، وهو ذاته ما حدث لإحدى العيادات الجامعية في ألمانيا عندما تم اختراق نظامها بشكل كامل بسبب وجود ثغرة تكنولوجية في إحدى أجهزتها المستخدمة[1].

[1] Do Business Academy. (2023). Cybersecurity: its concept, characteristics, and most common types of threats. For more details, see the following website:
https://www.e3melbusiness.com/blog/cyber-security

ثانياً/ البيانات والمعلومات الالكترونية:

هي أي معلومات يمكن تخزينها ومعالجتها وتوليدها ونقلها بوسائل تقنية المعلومات وبوجه خاص الكتابة والصور والصوت والأرقام والحروف والرموز والإشارات وغيرها، وأن 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 (Janan. 2007).

ثالثاً/ التكنولوجيا الحديثة وتقنيات الذكاء الاصطناعي:

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 (Al-Sharnoubi et al. 2022).

وأفرز التقدم التقني – رغم إيجابياتها 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 التكنلوجيا الحديثة عن طريق الاختراق والهجوم الذي يحصل ضد الامن السيبراني والذي يوضع لحمايته.

رابعاً/ 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 (Fahim, 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 (Meswar, 1992).

أنواع المسؤولية القانونية:

كما تقدم، تنهض عندما يوجب القانون مؤاخذة شـــخص ما عن أمر معين قام به، وهي نوعان بارزان، مسؤولية مدنية ومسؤولية جنائية:

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، (Imam, 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، وتوجد عدّة خصائص للمسؤولية المدنية بالمقارنة بالمسؤولية الجنائية أهمها (Sultan, 2019):

أ. جزاء المسـؤولية المدنية دائماً هو التعويض في حين أن الجزاء المترتب من المسـؤولية الجنائية هو عقوبة.

ب. 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.

ج. 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.

2. **المسؤولية الجنائية:** ويراد 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:

- **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 (Tanago, 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.
- **مفهوم المسؤولية الجنائية:** للمسؤولية الجنائية بوجه عام مفهومان، فهي إما مسؤولية **بالقوة** أو مسؤولية بالفعل، والمفهوم الأول مجرد أما الثاني فواقعي، ويراد بالمفهوم الأول صلاحية الشخص لأنه يتحمل تبعة سلوكه، والمسؤولية بهذا المعنى صفة في الشخص أو حالة تلازمه سواء وقع منه ما يقتضي المساءلة أو لم يقع منه شيء بعد. أما المفهوم الثاني فيراد به تحميل الشخص تبعة سلوك صدر منه حقيقة، والمسؤولية بهذا المعنى ليست مجرد صفة أو حالة قائمة بالشخص، ولكنها فضلاً عن ذلك جزاء، فالمفهوم الثاني إذن يستغرق الأول- أو يفترضه- بحكم اللزوم العقلي، لأنه لا يتصور تحميل شخص تبعة سلوك أتاه إلَّا إذا كان أهلاً لتحمل هذه التبعة وهذا يتطلب أن يكون ممن توجه إليه أحكام القانون الجنائي.

خامساً/ 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. **و**تهديد خصوصيّة الأفراد ازداد بشكل يبعث على القلق في ظل المجتمع المعلوماتي خاصة مع انتشار بنوك المعلومات (Al-Moni, 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 (Afifi, 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 (Qayed, 2016).

صور الاعتداء على الخصوصية المعلوماتية: تتمثل سلوكيات الاعتداء على الخصوصية الفردية في الآتي:

- **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 (Al-Azzam, 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 (Shaqiri, 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. ويقوم 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.

يمكن 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 (Al-Azzam, 2020).

سادساً/ القصد الجنائي لانتهاك خصوصية البيانات:

يشترط 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 (Al-Jundi, 2017). وتتحقق 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 (Saleh, 2013)، هي "كل فعل يتسبب في توقف أو تباطؤ أو ارتباك عمل نظام المعالجة ومن ثم ينتج ذلك تغيير في حالة عمل النظام (Taha, 1999). وإن 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.

الخاتمة:

تناولت الدراسة الوسائل التشريعية للمسؤولية الجنائية عن انتهاك الخصوصية على الأنظمة المعلوماتية وخرجت بمجمعه من النتائج وتوصيات يمكن ذكر أهمها فيما يلي:

أولاً/ النتائج:

1) 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.
2) 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 .
3) 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 .

4) 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.

5) 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 .

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.

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 تحرم 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

شكر وتقدير Acknowledgments

يتقدم الباحثون بالشكر إلى الجامعة العلوم الإسلامية الماليزية (**USIM**)، لإعطاء بيئة مواتية لإجراء وبناء فكرة هذا المقال.

تضارب المصالح Conflict Of Interests

يعلن ويعترف الباحثون بعدم وجود تنافس في المصالح المالية أو الشخصية أو غيرها فيما تتعلق بكتابة هذا المقال.

مساهمات الباحثين Authors' Contributions

صمم الباحثون هذه الدراسة كلها سويا.

قائمة المصادر والمراجع:

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.

Al-Badaina, Dhiab. (2014). *Cybercrime: concept and causes*. (PhD dissertation), Amman: Al-Ahliyya Amman University.

Al-Hafiz, Basil Mohammed. (2016). *Electronic crimes in the United Arab Emirates*, Dubai: United Arab Emirates.

Al-Mouni, N. A. Q. (2018). *Cybercrime*. Cairo: Dar Al-Nahda Al-Arabiya.

Al-Munajjid, Marwan Jassim. (2017). *Information technology crimes in the United Arab Emirates*. Dubai: United Arab Emirates.

Al-Nasser, Hamad Mohammed. (2020). *A guide to combating cybercrime in UAE law*. Dubai: United Arab Emirates.

Al-Sharnoubi, Mahmoud. Rehab, Ahmed Abdel Fattah. Karim, Abu Al-Majd. (2022). *Technology and artificial intelligence in tourism guidance: challenges and opportunities*. Laya Tourism and Hotels Magazine. Mansoura University, 11(5). 483-553.

Cyber Security Products and Services. (2017). Itgovernance.co.uk. Retrieved 25 November 2016, from http://www.itgovernance.co.uk/cyber-security-solutions.aspx

Darraj, Abdullah Ismail. (2022). *Al-Wajeez in Cybercrime*. Amman: Dar Al-Thaqafa for Publishing and Distribution.

Do Business Academy. (2023). *Cybersecurity: its concept, characteristics, and most common types of threats*. For more details, see the following website: https://www.e3melbusiness.com/blog/cyber-security

Fahim, A. S. (1999). *The general theory of criminal responsibility for crimes of persons and status*. Basra: Al-Haddad Press

Hatata, M. N. (1975). *Social defense between Sharia and law*. Cairo: Wahba Library.

Hilali, Abdullah Ahmed. (2012). *Budapest Convention on Cybercrime*. 1st edition. C3. Cairo: Dar Al Nahda Al Arabiya.

Imam, M. K. E. (2002), *The basis of criminal responsibility in positive law and Islamic law* [Unpublished PhD thesis]. Faculty of Law Library.

Imranuddin, Mohammed, (2017). "*A Study of Cyber Laws in the United Arab Emirates*" Thesis. Rochester Institute of Technology.

Jinan Sadiq Abdul Razzaq. (2007). *Electronic documents in institutions and information centers*. College of Education Journal. Issue (4).

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.

Mohammed, Hamdan Nasser. (2020). *Practical applications of the Anti-Cybercrime Law*. Dubai: United Arab Emirates.

Mr. Khaled Sami. (2021). *National cyber security and information crimes*. Cairo: Dar Al Nahda Al Arabiya.

PWC. (2017). Cyber: Think risk, not IT" (PDF). pwc. Financial Services Regulatory Practice, April, **(**2015**)**. https://www.pwc.com/us/en/financial-services/regulatory-services/publications/assets/cyberrisk.pdf

Qaid, O. A. (2016). *Cybercrime and information technology*. Cairo: Dar Al-Nahda Al-Arabiya.

Rahbani, Shafiq. (2020). *Cybercrime and its risks*. First edition. Amman: Dar Al-Thaqafa for Publishing and Distribution.

Ramadan, Mohammed Kamel. (2008). *Explaining information crimes*. Alexandria: Dar Al-Maaref at the University.

Saleh, S. R. Y. (2013). *Criminal policy in the face of information crimes (an analytical study)* [PhD thesis]. Koya University.

Shackelford, Scott J., The Law of Cyber Peace (July 5, 2016). Chicago Journal of International Law, 2017, Kelley School of Business Research Paper No. 16-56, Available at SSRN: https://ssrn.com/abstract=2805061 or http://dx.doi.org/10.2139/ssrn.2805061

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.

Sweilem, Asma Aqib (2021). *Electronic hacking crime*, (Master Thesis) Ajman: Ajman University.UAE.

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.