Vol. 2, No. 1, pp. 405-423 | 2024
CFORSJ Procedia

دور الأمن السيبراني في موجهة جرائم الاختراقات التي قد تتعرض لها دولة الامارات العربية المتحدة

THE ROLE OF CYBERSECURITY IN CONFRONTING HACKING CRIMES THAT MAY BE EXPOSED TO THE UAE

[i*] Mohammad Ahmad Saeed Alfalasi, [ii] Syahirah Binti Abdul Shukor & [iii] Mahmoud Mohamed Edris

[I, ii, iii] Faculty of Syariah and Law, USIM, Universiti Sains Islam Malaysia, Bandar Baru Nilai

*(Corresponding author) e-mail: M.bin7zaim@gmail.com

ABSTRACT

The study aims to demonstrate the role of cybersecurity in confronting the hacking crimes that the United Arab Emirates may be exposed to by identifying the problematic forms of assault in cyber hacking and assault on the privacy of personal data and information, especially confidential and personal ones, through full or partial access to those secrets related to them. The research relied on the descriptive analytical inductive approach with the aim of reaching objective results that achieve the goal of the study. The research reached an important result, which is that what distinguishes the crime of cyber hacking is that they are crimes that are quickly executed, as in most cases the physical element is only pressing a specific key on the device with the possibility of executing this remotely without requiring presence at the crime scene. The research came out with recommendations, the most important of which is allocating a legal article in the Rumors and Electronic Crimes Law that criminalizes the use of cyber hacking systems in committing the crime and creating a special penalty in the Crimes and Penalties Law for the crime of hacking government information systems.

Keywords: *Security, Cyber, Hacking Crimes, Security Confrontation*

ملخص البحث

تهدف الدراسة إلى بيان دور الأمن السيبراني في موجهة جرائم الاختراقات التي قد تتعرض لها دولة الامارات العربية المتحدة من خلال معرفة إشكالية صور الاعتداء في الاختراقات السيبرانية والاعتداء على خصوصية البيانات والمعلومات الشخصية وخاصة السرية والشخصية منها، عبر الاطلاع الكلي أو الجزئي على تلك الأسرار الخاصة بها، واعتمد البحث على المنهج الوصفي التحليلي الاستقرائي بهدف الوصول الى نتائج موضوعيه تحقق الهدف من الدراسة، وتوصل البحث الى نتيجة هامة هي 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، وخرج البحث بتوصيات اهمها تخصيص مادة قانونية في قانون الشائعات والجرائم الإلكترونية تجرم استخدام أنظمة الاختراق السيبراني في ارتكاب الجريمة واستحداث عقوبة خاصة في قانون الجرائم والعقوبات على جريمة اختراق الأنظمة المعلوماتية الحكومية.

الكلمات المفتاحية: *الأمن، السيبراني، جرائم الاختراقات، المواجهة الأمنية*

مقدمة

إن الأمن السيبراني يحظى اليوم باهتمام متزايد على مستوى عالمي، وذلك بالنظر إلى خطورة التهديدات التي يمثلها انعدام الأمن الإلكتروني على الأفراد والشركات والدول؛ ولهذا فقد أصبح الأمن السيبراني جزءاً لا يتجزأ من الأمن القومي للدول، لذا لا بد لنا من بيان نشأة الامن السيبراني وكيف ظهر هذا المصطلح بشكل موجز ومن ثم توضيح المفهوم من هذا المصطلح.

والأمن 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.

مشكلة الدراسة

تتمثل مشكلة الدراسة في أن ارتكاب الجرائم الماسة بأمن الدولة أصبحت مشكلة تعاني منها جميع دول العالم دون استثناء، وأن الأمن السيبراني هو السبيل التقني الوحدي لمواجهة هذا النوع من الجرائم الخطيرة، إن من أبرز المشكلات القانونية في جريمة الاختراق السيبراني للأنظمة المعلوماتية الخاصة بمؤسسات الدولة التي تعتبر من جرائم أمن الدولة هي أن جريمة الاختراق تختلط مع غيرها من الجرائم الأخرى من حيث محل الجريمة وبعض الأفعال المكونة للركن المادي لجريمة الاختراق، على سبيل المثال هناك خلط بين جريمة الاختراق وجريمة الدخول غير المشروع للمواقع الحكومية السرية الخاصة بأمن الدولة التي تحتوي على اسرار الدفاع والأسرار الأمنية والعسكرية، وخلط بين جريمة الاختراق وجريمة الإتلاف المعلوماتي، حيث أن الاختراق هو الفعل الأول والدخول غير المشروع هو الفعل الثاني والإتلاف هو نتيجة للفعل الثاني، حيث أن المرسوم بقانون اتحادي رقم (34) لسنة 2021 لم يفرق بين هذه الأفعال وأي منها يشكل الجريمة وأي منها يشكل الفعل وأي منها هو النتيجة، وهو ما يتطلب البحث في كل ذلك.

أسئلة الدراسة

1) ما هي جرائم أمن الدولة التي يتم ارتكابها بالفضاء السيبراني؟
2) كيف يسهم المرسوم بقانون اتحادي رقم (34) لسنة 2022 بشأن الشائعات والجرائم الإلكترونية في تعزيز الأمن السيبراني لمواجهة جرائم أمن الدولة؟
3) ماهي آلية واستراتيجية الأمن السيبراني في دولة الإمارات العربية المتحدة الموجهة ضد جرائم أمن الدولة الداخلي والخارجي؟
4) كيف يسهم التعاون الدولي الأمني الإلكتروني في تعزيز الأمن السيبراني ومواجهة جرائم أمن الدولة؟

اهداف الدراسة

1) تحديد جرائم أمن الدولة التي يتم ارتكابها بالفضاء السيبراني.
2) بيان فعالية المرسوم بقانون ارتحادي رقم (34) لسنة 2022 بشأن الشائعات والجرائم الإلكترونية في تعزيز الأمن السيبراني لمواجهة جرائم أمن الدولة.
3) تحليل آلية واستراتيجية الأمن السيبراني في دولة الإمارات العربية المتحدة الموجهة ضد جرائم أمن الدولة الداخلي والخارجي.
4) بيان مدى إسهام التعاون الدولي الأمني الإلكتروني في تعزيز الأمن السيبراني ومواجهة جرائم أمن الدولة.

اهمية الدراسة

1) **الأهمية النظرية:** تتمثل أهمية الدراسة من الناحية النظرية في أنها تقدم تصور نظري لدور الأمن السيبراني في مواجهة جرائم أمن الدولة، ولا سيما من حيث المفاهيم والخصائص، كما أن الدراسة تبين الإطار النظري للجرائم التي ترتكب ضد أمن الدولة عبر التقنيات الحديثة
2) **الأهمية العلمية:** تظهر أهمية الدراسة من الناحية العلمية في أنها من أولى الدراسات في دولة الإمارات العربية المتحدة التي تتناول دور الأمن السيبراني في مواجهة جرائم أمن الدولة، ولا سيما في ظل المرسوم بقانون اتحادي رقم (34) لسنة 2022 بشأن الشائعات والجرائم الإلكترونية، كما أن الدراسة تعتبر من الدراسة الهامة بالنسبة لطلاب القانون ورجال الأمن السيبراني والمحامين والقضاة ورجال الأمن، حيث يمكن الاستفادة منها في بناء توصيات عليمة تسهم في تعزيز دور الأمن السيبراني في مواجهة جرائم أمن الدولة.

حدود الدراسة

1) النطاق المكاني: تنحصر الدراسة في المساحة الجغرافية لدولة الإمارات العربية المتحدة.
2) النطاق الزماني: منذ عام 2021 وهو العام الذي أصدر به المشرع الإماراتي العديد من التشريعات والتوجيهات الخاصة بتعزيز الأمن السيبراني.
3) النطاق الموضوعي: دور الأمن السيبراني في مواجهة جرائم أمن الدولة.
4) النطاق البشري: رجال الأمن ورجال القانون والطلاب.

منهج الدراسة:

استخدم الباحث المنهجية الوصفية التحليلية لدراسة دور الأمن السيبراني في مواجهة جرائم المساس بأمن الدولة من خلال استخدام التقنيات الحديثة في ارتكاب جرائم أمن الدولة الخارجي، بغية استخلاص حكم المسائل التي لا نجد فيها نصاً أو رأياً أو المسائل التي يشوبها الغموض والاختلاف، وذلك من خلال تحديد أركان جريمة المساس بأمن الدولة من جهة الخارج باستخدام التقنيات الحديثة، وبيان طبيعتها وسبل مواجهتها تشريعيا وأمنياً وتقييم مدى جدوى التشريعات القانونية في مكافحة هذه الجريمة. ووصفها وصفاً دقيقاً والتعبير عنها من خلال النشأة والتطور والوسائل، وذلك من أجل الوصول إلى نتائج وتوصيات تسهم في حل مشكلة الدراسة.

الدراسات السابقة

1. **كتاب بعنوان:" الإرهاب السيبراني[1]"**. أملت تحولات الظاهرة الإرهابية على الدول والمجتمعات يقظة تشريعية مستمرة ودائمة، تشمل مستويات عديدة، بدءاً من تكييف الفعل الإرهابي، وتجفيف المنابع المالية، ومراجعة الجوانب الإجرائية في مكافحة الإرهاب، فضلاً عن تشجيع وتعجيل التصديق و/أو الانضمام إلى الاتفاقات الدولية العالمية والإقليمية ذات الصلة.

ويلاحظ في سياق مكافحة الإرهاب السيبراني، أنه يتعين على الحكومات لضمان التصدي الفعال على مستوى العدالة الجنائية لمخاطر استخدام الإنترنت في أغراض إرهابية، أن تضع سياسات وقوانين وطنية واضحة تتناول أموراً في جملتها: أ) تجريم الأفعال غير القانونية التي يرتكبها الإرهابيون على الإنترنت أو الخدمات ذات الصلة؛ ب) تخويل صلاحيات التحقيق لأجهزة إنفاذ القانون المشاركة في التحقيقات ذات الصلة بالإرهاب؛ ج) التنظيم الرقابي للخدمات المتصلة بالإنترنت (مثل مقدمي خدمات الإنترنت) ومراقبة المحتويات؛ د) تيسير التعاون الدولي: هـ) استحداث إجراءات قضائية وإجراءات إثبات متخصصة؛ و) الحفاظ على المعايير الدولية لحقوق الإنسان[1].

---

[1] الرشيدي، هالة أحمد (2022). الإرهاب السيبراني، القاهرة: دار النهضة العربية، الطبعة الأولى .

[1] استخدام الإنترنت أغراض إرهابية، مرجع سابق ذكره، ص141.

ويعزى الاهتمام بسن التشريعات لمكافحة الجرائم الإرهابية، في حقيقة الأمر، إلى عدة اعتبارات في مقدمتها أن الفراغ التشريعي أو سكوت النص بعبارة أخرى. من شأنه أن يحول دون مثول مرتكبي هذه الجرائم أمام القضاء وتقديمهم للمساءلة، وذلك إعمالاً للمبدأ المستقر في هذا الشأن، وهو مبدأ الشرعية الجنائية، والذي يقضي بأنه لا جريمة ولا عقوبة إلا بنص. كما أن تجريم فعل معينة والمعاقبة عليه لا يضمن فقط التنفيذ الفعال لتدابير مكافحته، بل يرسي، أيضاً، الأساس القانوني الذي تستند إليه كافة هذه التدابير. وفي سياق مكافحة جرائم الإرهاب السيبراني، فإن الغرض من مثل هذه التشريعات ليس تجريم الأنشطة الإرهابية السيبرانية غير المشروعة وفرض العقوبات التي تتناسب معها وحسب (مستوى القمع)، وإنما أيضاً منع وقوع هذه الأنشطة ابتداءً، والتخفيف من آثارها حال وقوعها، وذلك بالقضاء على كافة العوامل التي تيسر ارتكاب هذه الجرائم، بحظر تمويل الإرهابيين وحظر تقديم أي دعم مادي أو تقني لهم على سبيل المثال، وتجريم نشر الأفكار الإرهابية والترويج لها وتمجيدها عبر الإنترنت (مستوى المنع) .

وعلى الرغم من الحداثة النسبية لظاهرة الإرهاب السيبراني، فقد اهتمت بعض الدول بسن التشريعات واتخاذ ما يلزم من تدابير تشريعية وإجرائية ومؤسسية لمكافحتها، وذلك بالنظر إلى أخطارها المحدقة التي باتت تهدد أمن الدول والمجتمعات بشكل شبه يومي. ويلاحظ مع ذلك، إن بعض الدول الأخرى قد لجأت إلى استخدام القوانين الجنائية العامة أو التشريعات المتعلقة بمكافحة الإرهاب أو الجرائم السيبرانية أو مزيج مما سبق لتجريم هذه الأعمال وملاحقة مرتكبيها قضائياً.

ويعرض التحليل، في هه الدراسة الخبرات الدولية في مجال مكافحة الإرهاب السيبراني، للاستفادة منها تعميم الممارسات الجيدة من جانب، ولتقييم مدى كفاية هذه الممارسات والخبرات لمعالجة الظاهرة محل التحليل بمختلف صورها ووسائلها وأساليبها.

2. **كتاب :" السويدي، أحمد غانم سيف (2016). المواجهة الجنائية والأمنية للجرائم الماسة بأمن الدولة الداخلي.**[2] لقد اتجهت التشريعات الوضعية إلى وضع قواعد إجرائية خاصة ومستقلة عن الجرائم العادية، وذلك بما يؤدي إلى التوسع في السلطات للجهات القائمة على ضبط هذه الجرائم وتعقبها، وعلى هذا فإن الجرائم الماسة بأمن الدولة الداخلي وجرائم الإرهاب تقرر صلاحيات واسعة لسلطات الضبط والتحقيق والاتهام والمحاكمة، ويرجع خروج هذه الجرائم عن القواعد العامة في الإجراءات الجنائية إلى خطورة مرتكبي هذه الجرائم

[2] السويدي، أحمد غانم سيف (2016). المواجهة الجنائية والأمنية للجرائم الماسة بأمن الدولة الداخلي دبي: أكاديمية شرطة دبي، كلية الدراسات العليا.

واتصالهم بتنظيمات إرهابية قد تساعدهم على طمس الأدلة وسرعة الهروب من العدالة داخل البلاد أو خارجها. ولكن مما يجب أن نشير إليه أن هذه الإجراءات الخاصة يجب أن تكون بالقدر الضروري الذي يتلاءم مع الهدف منها، ومع مراعاة حدود التناسب بين اعتبارات الأمن وحقوق الإنسان، وهذا ما يقتضي منا الحديث عن القواعد الإجرائية لمكافحة جرائم الإرهاب في التشريع المصري، وذلك في مراحلها المختلفة ثم نقوم بإلقاء الضوء على القواعد الإجرائية الخاصة بالإرهاب في بعض التشريعات الأجنبية والعربية، ونعقب على ذلك بموقف الشريعة الإسلامية من القواعد الإجرائية الخاصة بالجرائم الإرهابية.

3. **كتاب**: الأمن القومي الإلكتروني وجرائم المعلومات[3] بين المؤلف 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[4].

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

---

[3] السيد، خالد سامي (2022) : الأمن القومي الإلكتروني وجرائم المعلومات، القاهرة: دار النهضة العربية ، الطبعة الأولى

[4] السيد، خالد سامي (2019). استخدام التقنيات الحديثة بعمليات الأمن المركزي للارتقاء بآليات المواجهة. رسالة دكتوراه. كلية الدراسات العليا. أكاديمية الشرطة. القاهرة.

أفراده بسبب مشكلات نفسية واجتماعية تجلب الحقد في صدر بعض المستخدمين على المجتمع وتجعلهم يخرجون عن القانون من هنا فهي تعطي فرصة ذهبية لأصحاب الفكر المتطرف والجماعات الإرهابية لبث سمومها في المجتمع ونشر أفكار هدامة وقناعات مضللة تتنافي مع المعايير والقيم الأخلاقية والاجتماعية وتمهد الطريق للوقوع في أخطار الانحراف وارتكاب السلوك غير السوي[5]. أيضاً نشر الشائعات من أشد مخاطر إساءة استخدام شبكات التواصل الاجتماعي لأن الشبكات تسهم في انتشار الشائعة وتضخيمها بشكل مبالغ فيه في فترة وجيزة لا تستغرق ساعات مما يترتب عليه إحداث بلبلة وبعض الاضطراب وعدم الاستقرار من خلال شحن الوضع الداخلي وهدم النسيج الوطني، وجعله يعاني من فوضى عارمة نتيجة تناقض الأخبار وتفريق أفراد المجتمع ما بين مصدق ومكذب مما يهدد بنية المجتمع ويسهم في تفكيك نسيجه الوطني[4]. كذلك من أسباب اعتبار نشر الشائعات من أشد مخاطر شبكات التواصل الاجتماعي هي أنها تهدف مباشرة إلى تهديد الأمن الاجتماعي والوطني وتسهم في إحداث بلبلة واضطراب في المجتمع في ضوء استغلال مميزات شبكات التواصل الاجتماعي وعدم إمكانية فرض رقابة عليها في نشر الشائعات المغرضة التي تزعزع الأمن والاستقرار وتجلب حالة من القلق والترقب قد تؤدي إلى ردود أفعال عدائية بين الأفراد والجماعات قد تتفاقم لتحدث حرب أهلية تقضي على الأخضر واليابس.

4. **دراسة:** عقيل، محمد عبد العزيز محمد (2015) التحريض الإلكتروني على الإرهاب – تويتر نموذجاً"[6] هدفت هذه الدراسة إلى توضيح خطورة الجماعات الإرهابية، لأنَّهم أكثر فئات المجرمين استخداماً للتقنيات الحديثة وأكثر استفادة من معطيات الحضارة، فنوعوا الوسائل واستغلوا التقنية المعلوماتية عبر وسائل التواصل الاجتماعي ومواقع الإنترنت والبريد الإلكتروني لتحقيق أهدافهم، واستغلوا التقنية المعلوماتية التي سهلت لهم نشر فكرهم الإرهابي، فأشغلت قضية الإرهاب المجتمعات الإنسانية على اختلاف مللها وشتى اتجاهاتها وتنوع نظمها، وقد نال الدول الإسلامية كغيرها من الدول نصيب من هذا الإرهاب على تفاوت فيما بينها. وقد جاء الدراسة في ثلاثة مباحث، تناولت في المبحث الأول معنى الإرهاب الإلكتروني، وذكر فيه معنى الإرهاب الإلكتروني في اللغة والاصطلاح، وبين خطر الإرهاب الإلكتروني، أمَّا المبحث الثاني فقد تناول وسائل الإرهاب

---

[5] تركي، بن عبد العزيز (2019). توظيف شبكات التواصل الاجتماعي في التوعية الأمنية ضد خطر الشائعات. جامعة نايف العربية الأمنية. الرياض.

[4] هايل، ودعان (2010). التخصص الأمني للرأي العام ضد الشائعات. ندوة دور مؤسسات المجتمع المدني في التوعية الأمنية؟ جامعة نايف العربية للعلوم الأمنية. الرياض

[6] (التحريض الإلكتروني على الإرهاب – تويتر نموذجاً)، رسالة دكتوراه، جامعة الإمام محمد بن سعود الإسلامية، السعودية.

الإلكتروني وهي وسائل التواصل الاجتماعي ومواقع الإنترنت، بينما في المبحث الثالث والأخير فقد استعرض التكييف الفقهي للتحريض الإلكتروني على الإرهاب وحكمه، وذكر تكييف التحريض الإلكتروني على الإرهاب في الفقه وبين حكمه وعقوبته في الفقه. وجاءت الخاتمة مشتملة على أهم النتائج التي توصل إليها الباحث، ومنها أنَّ الإرهاب الإلكتروني يعد جريمة مستجدة نسبياً أخذ يقرع أجراس الخطر في السنوات الأخيرة لتنبيه مجتمعات العصر الراهن بحجم المخاطر وظهور الخسائر الناجمة عنه، كما يصنف الإرهاب الإلكتروني من حيث المعيار التاريخي ضمن الإرهاب المعاصر الذي وجد في عصرنا الحالي ويشمل معظم الحركات الإرهابية الحديثة في القرن العشرين.

تلتقي الدراسة السابقة مع دراستي بأن كليهما يرى أن التحريض الإلكتروني على الأمن هو من جرائم أمن الدولة التي تتطلب المواجهة القانونية والأمنية، ولكن الدراسة السابقة لم تبين آلية التصدي لهذا النوع من الجرائم ودور الأمن السيبراني في ذلك.

5. **دراسة: الهاجري**، راشد رمزان (**2012**)، **بعنوان** (التحريض الإلكتروني المخل بأمن الدولة[7]. تحدثت الدراسة عن كل ما يصدر من الأشخاص في وسائل الاتصالات الحديثة من تحريض على الإخلال بأمن الدولة وتجريم ذلك العمل وتحريمه بالكتاب والسنة والإجماع والأنظمة المرعية في المملكة العربية السعودية وبعض الدول العربية، سواء كان ذلك بالسلوك أو بالاشتراك أو بالشروع، وعقوبة ذلك في الشرع والنظام القانوني. وحُددت الدراسة معالم جريمة التحريض بإحكام من خلال الدراسة، وبين فيها تعريفاً جامعاً لجريمة التحريض الإلكتروني، وهو خلق فكرة الاعتداء على أمن الدولة في ذهن الغير عبر الوسائل المعلوماتية والحث والتشجيع على ذلك لغرض غير مشروع يخل بأمن الدولة، وبث الخوارج أفكارهم في هذه الوسائل بصور عديدة ذكرها الباحث تخالف الشرع والسنة لسهولة استخدامها وسرعة انتشارها وقوة تأثيرها. وأضاف الباحث، أنَّه نتيجة ذلك تتمثل في عدم السمع والطاعة لولاة الأمر وعدم الرجوع للعلماء الربانيين لاهتزاز ثقة الناس بهم بسبب ما يثار حولهم من الشبهات والكذب والافتراء من الخوارج أهل الزيغ والضلال ودعاة الفتنة ثم الخروج عليهم بالتكفير والتفجير وزعزعة الأمن، مشيراً إلى أن عقوبة التحريض في الشرع هي نفس عقوبة الخوارج. وخلصت الدراسة إلى توصيات عدة، منها التأكيد على ترسيخ العقيدة والتوحيد والسنة وعدم الابتداع، حيث إنَّ ذلك سبب جلب كل خير ودفع كل شر وتحقيق الأمن في الدنيا والآخرة، وسبب لحماية الفرد والمجتمع، من الدخول في هذه

[7] الهاجري، راشد رمزان (2012): (التحريض الإلكتروني المخل بأمن الدولة)، رسالة ماجستير، المعهد العالي للقضاء، السعودية.

الأفكار وانتشارها، والتأثر بها، ويأتي ذلك، عبر الدروس والمحاضرات والمؤتمرات والندوات من كبار أهل العلم. وأكد الباحث أيضاً على أهمية حث وتوعية المجتمع بشتى وسائل الإعلام المقروء والمسموع والمرئي من خلال دعوة العلماء والمؤسسات الدينية والوزارات المسؤولة عن التربية والتعليم والثقافة والإعلام وباستخدام التقنية الحديثة ووسائل الاتصال الجديدة، لتصل إلى كل طبقات المجتمع وشرائحه، وتوضيح أخطار التحريض الإلكتروني المخل بأمن الدولة وأعمال الخوارج والإرهابيين وهذا اسمهم الشرعي وليس الفئة الضالة. وطالب الباحث بسرعة محاكمة من يثبت بحقه التحريض الإلكتروني المخل بأمن الدولة، ومعاقبتهم؛ لأنَّ هؤلاء هم سبب تورط كثير من الشباب في أفكار الخوارج والانخراط في الخلايا الإرهابية، وأنَّ سبب هذا كله التحريض الإلكتروني المخل بأمن الدولة.

وتلتقي الدراسة السابقة مع دراستي في نقطة جوهرية، هي أن جريمة التحريض الإلكتروني على جرائم أمن الدولة هي من الجرائم الماسة بأمن الدولة، ولكن الدراسة السابقة لم تبين آصار استخدام الأمن السيبراني في حماية أمن الدولة والتصدي لهذا النوع من الجرائم، وهو الأمر الذي سوف تعمل عليه الدراسة الحالية.

6. **دراسة، هميسي، رضا (2011) بعنوان** (الإعلام الجديد بين حرية التعبير وحماية الأمن الوطني)[8] تناولت الدراسة بيان القيود القانونية الواردة على حرية الرأي والتعبير في وسائل الإعلام الجديد، من خلال دراسة حماية الأمن الوطني كقيد قانوني على ممارسة هذه الحريات، وهي توضح أهمية وسائل الإعلام الجديد كمنصات لممارسة حرية الرأي والتعبير والصحافة في الفضاء الافتراضي، كما تتعرض لتوضيح مفهوم حرية الرأي والتعبير ومفهوم الأمن الوطني، ثم تدرس المسؤولية المترتبة عن إساءة استخدام هذا الحق من خلال إبراز المواجهة القانونية للمساس بالأمن الوطني تحت مسمى حرية التعبير. وتمت هذه الدراسة على ضوء القوانين المنظمة لقطاع الإعلام والصحافة والنشر والمطبوعات، وكذلك في ظل قوانين العقوبات، وقوانين مكافحة الجرائم المعلوماتية، ومكافحة الإرهاب، فضلاً عن الدساتير العربية والمواثيق الدولية لحقوق الإنسان. وهدفت هذه الدراسة إلى توضيح ما يقوم به الإعلام الجديد في ارتكاب أعمال دنيئة، بذريعة حرية التعبير، وذلك من خلال الاستخدام غير المشروع لهذه الوسائل، بهدف المساس بحقوق الآخرين سواء أكانوا أفرادا أم جماعات، والتشهير بهم والطعن في أعراضهم وشرفهم وكشف عوراتهم والتدخل في خصوصياتهم وإلحاق الأذى بهم. ولا يتوقف الأمر عند هذا الحد، وإنَّما قد يمتد إلى استخدام هذه الوسائط لتنفيذ أغراض إجرامية تهدف إلى زعزعة استقرار الدول وتهديد أمنها الوطني وسيادتها، من خلال نشر أخبار ومعلومات زائفة وترويجها بهدف النيل من هيبة الدولة

[8] هميسي، رضا (2011): (الإعلام الجديد بين حرية التعبير وحماية الأمن الوطني)، رسالة ماجستير، جامعة قاصدي مرباح، الجزائر.

وسمعتها والمساس بالنظام العام فيها، وهو ما تلجأ إليه الجماعات المتطرفة باستخدام شبكة الإنترنت. وقد توصلت الدراسة إلى العديد من النتائج، أهمها أن تطور مفهوم الأمن الوطني ولم يعد يقتصر في الوقت الراهن على القدرات العسكرية أو الدفاعية وإنَّما أصبح ينظر إليه بمفهومه الشامل الذي يتضمن الجوانب الاقتصادية والاجتماعية والسياسية لحماية أمن الدولة والحفاظ على كيانها، كما إنَّ نشر معلومات وأخبار مضللة على وسائل الإعلام الجديد بهدف زعزعة نظام الحكم، يعدُّ مساساً خطيراً بالأمن الوطني وبسيادة الدول، وهو لا يدخل البتة في خانة ممارسة حريات التعبير، لأنَّ الحفاظ على النظام العام والمصالح العليا في الدولة، وصون سيادتها واستقلالها، وتترتب المسؤولية الجزائية عن المساس بالأمن الوطني، عند إساءة ممارسة حريات الرأي والتعبير، حيث تسلط عقوبات سالبة للحرية وغرامات مالية على مرتكبي الجرائم التعبيرية، فضلاً عن العقوبات الإدارية، المتمثلة في وقف الطبع، أو سحب المطبوعة، أو وقف البث، أو تعليقه لفترة محدودة.

وتلتقي الدراسة السابقة مع الدراسة الحالية في أنها تبين آلية ووسائل استخدام التقنيات الحديثة في ارتكاب الجرائم الماسة بأمن الدولة، ولكنها لم تذكر دور الأمن السيبراني في مكافحة هذه الجريمة وهو ما سيتم تحليله في هذه الدراسة.

7. **دراسة:" الصيفي،** عبد الفتاح مصطفى (**2016**): (التحريض على الجريمة الإرهابية ووضعه من النظرية العامة للمساهمة الجنائية – دراسة مقارنة[9] هدفت هذه الدراسة إلى دراسة التحريض على الجريمة الإرهابية ووضعه من المساهمة الجنائية، متبعاً في ذلك المنهج التحليلي التأصيلي المقارن، وقد قسم الباحث دراسته إلى ثلاثة أبواب، تناولت وضع التحريض من النظرية العامة للمساهمة الجنائية، وعناصر التحريض وما يثيره من مشاكل قانونية. وقد توصل الباحث إلى أنَّ المشرّع المصري لم يكن دقيقاً في استعماله للمصطلحات الخاصة بموضوع التحريض، فيما يتعلق بمصطلح الشريك، حيث استعمل هذا اللفظ بطريقة أثارت الخلاف والجدل بين الفقهاء، ورأى الباحث أن المقنن كان في غنى عن هذا كله، لو أنَّه استعمل مصطلح (المساهم) كاسم جنس تندرج تحته درجتان (الاشتراك) والفاعل الأصلي أو الفاعل مع غيره).

تلتقي الدراسة السابقة مع دراستي في أنها تبين آلية التحريض لارتكاب الجرائم الماسة بأمن الدولة عبر التقنيات الحديثة، ولكنها تختلف عنها من حيث سياق التناول القانوني والتقني والأمني، حيث أن الدراسة السابقة لم

---

[9] الصيفي، عبد الفتاح مصطفى (2016): (التحريض على الجريمة الإرهابية ووضعه من النظرية العامة للمساهمة الجنائية)، رسالة دكتوراه، كلية الحقوق، جامعة الإسكندرية.

تبين دور الأمن السيبراني في مواجهة جريمة التحريض على ارتكاب جرائم أمن الدولة، وهو ما سيتم العمل عليه في هذه الدراسة.

8. **دراسة: العلاونة،** حاتم سليم (**2012**): (دور التواصل الاجتماعي في تحريض المواطنين للمشاركة في الحراك الجماهيري)[10]. هدفت هذه الدراسة إلى التعرف على دور مواقع التواصل الاجتماعي، في تحريض المواطنين الأردنيين للمشاركة في فعاليات الحراك الجماهيري، المطالب بالإصلاح السياسي والاقتصادي والاجتماعي، كهدف رئيس لهذه الدراسة، وذلك باستخدام منهج المسح الإعلامي بشقيه الوصفي والتحليلي، حيث أتاحت مواقع التواصل الاجتماعي المجال لمنظمي فعاليات هذا الحراك الجماهيري، للمشاركة والتفاعل مع الأحداث، على مستوى التحفيز وتحريك الرأي العام. وقد جاءت الدراسة في ثلاثة مباحث، تناولت في المبحث الأول التعريف بشبكات التواصل الاجتماعي ونشأتها وتطورها، وخصائصها ومميزاتها، وأنواعها. أما المبحث الثاني فقد تناولت فيه تأثير شبكات التواصل الاجتماعي على وسائل الإعلامي بوصفها أدوات جاذبة، وما هي التحديات والصعوبات التي تواجه شبكات التواصل الاجتماعي. بينما في المبحث الثالث فقد استعرضت دور شبكات التواصل الاجتماعي في التغيير السياسي.

وتلتقي الدراسة السابقة مع دراستي بأنها تبين آلية استخدام التقنيات الحديثة في ارتكاب جرائم أمن الدولة، ويمكن الاستفادة منها في الإطار النظري للدراسة التي نحن بصددها، وإن الدراسة السابقة يعتريها النقص والغموض في بعض جزئياتها، ولا سيما أنها لم تتطرق لدور الأمن السيبراني في مواجهة هذا النوع من الجرائم وهو ما سيتم التركيز عليه وتوضيحه في هذه الدراسة.

9. **دراسة بعنوان:" المسؤولية المدنية لمزودي الخدمة في الأمن السيبراني".**[11] وتهدف هذه الدراسة للكشف عن المسؤولية المدنية لمزودي الخدمة في الأمن السيبراني، من خلال أربعة فصول وخاتمة ونتائج وتوصيات، تم استخدام المنهج الوصفي والمنهج التحليلي في هذه الدراسة والمنهج المقارن للمقارنة بين القوانين المختلفة، تتمثل مشكلة الدراسة في بيان المسؤولية المدنية لمزودي الخدمة في الأمن السيبراني من خلال الرجوع للقوانين ذات العلاقة. وقد توصلت الدراسة لعدد من النتائج منها: أن المشرع الأردني لم يعالج في قانون الأمن السيبراني المسائل التقنية والفنية لحادث الأمن السيبراني من حيث الطبيعة والأثر والتصنيف. الأمر الذي من شأنه التأثير

---

[10] العلاونة، حاتم سليم (2012): (دور التواصل الاجتماعي في تحريض المواطنين للمشاركة في الحراك الجماهيري)، رسالة ماجستير، جامعة اليرموك، الأردن.

[11] العوايشة، آلاء فراس شحادة (2022)، **المسؤولية المدنية لمزودي الخدمة في الأمن السيبراني**، مجلة جامعة عمان العربية للبحوث – سلسلة البحوث القانونية، جامعة عمان العربية – عمادة البحث العلمي والدراسات العليا، المجلد/العدد: مج4, ع2

على الضمان للحماية التي تم إقرارها أو المرجوة في الأمن السيبراني وسلامة الفضاء السيبراني في الأردن. وكذلك الاستفادة من طاقات تقنيات معلومات واتصالات الأمن السيبراني، في جميع المستويات وقد أوصت الدراسة بضرورة أن تسمح قوانين بعض الدول أن يتم اللجوء للدعاوى أو للطلبات لوقف بث المضمون التقني غير المشروع، وأن يتم، بدقة، تحديد الإجراءات الواجب إتباعها لسحبه، أو لمنع وصوله لمستخدمي الشبكة.

10. **دراسة بعنوان:" أشكال انتهاك الفضاء السيبراني ووسائلها وأثارها".**[12] ويتناول البحث موضوع أشكال انتهاك الفضاء السيبراني ووسائلها وأثارها وقد تمثلت مشكلة البحث في التساؤل الرئيس "ما أشكال انتهاك الفضاء السيبراني ووسائلها وأثارها؟" وقد هدف البحث إلى التعرف على مفهوم الفضاء السيبراني ومفهوم انتهاك الفضاء السيبراني، والتعرف على أشكال جرائم انتهاك الفضاء السيبراني، وتحديد وسائل الإجرام في انتهاك الفضاء السيبراني، وبيان تصنيف المجرمين منتهكي الفضاء السيبراني، والتعرف على الآثار المترتبة على جرائم انتهاك الفضاء السيبراني وقد استخدم الباحث المنهج الوصفي الاستقرائي التحليلي وهو الأنسب للدراسات القانونية الذي يحقق أهداف الدراسة، "وهو المنهج الذي يبدأ بالجزئيات ليصل منها إلى قوانين عامة، ويعتمد على التحقيق بالملاحظة المنظمة الخاضعة للتحليل والتحكم في المتغيرات المختلفة ومن أبرز النتائج التي توصلت إليها الدراسة عدم وجود لائحة تنفيذية للمواد القانونية في النظام السعودي لتوضيح النصوص وعدم إلمام بعض أفراد المجتمع ونقص الوعي والإلمام بالانتهاكات السيبرانية، مما جعلهم عرضة لارتكابها أو وقوعهم ضحية لاستغلال المنتهكين لهم وارتكاب الجرائم تجاههم وأن سبب تنامي الانتهاكات السيبرانية يعود إلى العمل بنظرية ازدواجية القانون الداخلي الذي لا يتماشى مع القانون الدولي، ولكن هذا قد ينطبق على قوانين معينة ولكن يجب أن يتوافقا في الفضاء السيبراني، وذلك لكون الضرر يقع على كافة الدول، وأن هذه الانتهاكات قد تعدت مرحلة حدود الدولة لوحدها في مواجهة أخطار الفضاء السيبراني. ومن التوصيات التي توصلت إليها البحث ضرورة وجود اتفاقيات دولية تتفق عليها الدول فيما يتعلق بالفضاء السيبراني لتحديد المسؤولية ومعاقبة من يرتكب الانتهاكات وتسليمه للعدالة، لأن الانتهاكات السيبرانية تجاوزت الاعتبارات الجغرافية والموضوعية وضرورة تعزيز التعاون الدولي لمكافحة الانتهاكات السيبراني وتحديد المسؤولية لمن يقف خلفها من أفراد أو دول مع مراعاة مبادئ حقوق الإنسان والحريات ويجب أن يعي كل فرد داخل الوطن أن تعزيز الأمن السيبراني ليس مسؤولية الدولة ورجال الأمن بل تشمل المسؤولية أفراد المجتمع، بل

---

[12] ناصر، محمد (2023). **أشكال انتهاك الفضاء السيبراني ووسائلها وأثارها، مجلة الندوة للدراسات القانونية**، اللمغرب: المجلد/العدد: ع40

كل فرد له دور في حماية الفضاء السيبراني وذلك من خلال معرفة ماهيته ومتعلقات وكيفية تجنب الوقوع بأشكالها المختلفة.

الإطار النظري:

ظهر الأمن السيبراني كمشروع بحث في سبعينيات القرن الماضي، حينما طرح الباحث بوب توماس برنامج كمبيوتر أُطلق عليه اسم(Creeper) ، وقد تمكّن هذا البرنامج من التحرك عبر شبكة(ARPANET) ، ثمّ طرح راي توملينسون برنامج(Reaper) ، لمطاردة وحذف(Creeper) ، من خلال تعقّب مساراته، وعليه كان (Reaper) أول برنامج ذاتي النسخ لمكافحة الفيروسات، حيث اعتُبر عندها أول دودة حاسوب تُلاحق الفيروسات في الكمبيوتر وتقضي عليها ، ومع ازدياد الاعتماد على أجهزة الكمبيوتر ونمو الشبكات وانتشارها، ازدادت المناقشات حول أمن الكمبيوتر وأهميته ما بين عام 1972–1974م، وكان من الضروري تحديد نقاط الضعف، لذا أقرت الحكومات بأهمية الأمن الإلكتروني، وأنّ الوصول غير المصرح به إلى البيانات والأنظمة يمكن أن يكون له عواقب كارثية، أُنشئ العديد من مشاريع الأمن المبكر من قِبل الجهات المختلفة من معاهد، وجامعات، وجهات حكومية، ففي عام 1979 م رُصدت أول عملية اختراق فعلية لشركة تطوير أنظمة تشغيل من قِبل كيفين مينتيك البالغ من العمر 16 عامًا، إذ قام بنسخ البرامج وتوزيعها ما أدّى إلى سجنه، ليصبح بعدها مديرًا لشركة .(Mintick Security Consulting)

ازدادت الهجمات الإلكترونية والتهديدات الجاسوسية في فترة الثمانينات، وظهرت مصطلحات جديدة مثل فيروسات الحاسوب(Trojan Horse) ، لذا حدّدت وزارة الدفاع الأمريكية معايير لتقييم نظام الكمبيوتر الموثوق به عام 1985 م. ومع ذلك في عام 1986 م، اخترُقت بوابة الإنترنت في كاليفورنيا، وتمّ تهكير 400 جهاز كمبيوتر عسكري، بالإضافة إلى الأجهزة المركزية في مقر البنتاغون، وذلك بهدف بيع المعلومات. وبعدها في عام 1987 م انطلق أول برنامج تجاري لمكافحة الفيروسات، ثمّ توالت شركات تطوير برامج مكافحة الفيروسات في الظهور عام 1988 م، وشهد هذا العقد تأسيس أول منتدى إلكتروني مخصص لأمن مكافحة الفيروسات، بالإضافة إلى تأسيس مطبعة مكافحة الفيروسات، لحماية بيانات مستخدمي الفضاء السيبراني من أي قرصنة إلكترونية إجرامية، وهو ما مهّد لظهور الأمن السيبراني.

كما ان دولة الامارات العربية المتحدة قد اولت اهتمام كبير في هذا المجال وكان له الأولوية في السنوات القليلة الماضية، فقد سعت جاهدة بأن تحقق إنجازات عالمية كبيرة وتكون في صدارة أبرز المؤشرات الدولية في هذا المجال، فقد تم عمل استراتيجية وطنية للأمن السيبراني وتهدف من خلالها الى خلق بيئة سيبرانية امنة وصلبة تساعد على تمكين الافراد من تحقيق طموحاتهم وذلك من خلال وضع ستين مبادرة ضمن خمس محاور، وقد تم إطلاق النسخة المحدثة في عام 2019 من قبل الهيئة العامة لتنظيم قطاع الاتصالات.

كما وانه قد اعتمد مجلس الوزراء إنشاء مجلس الأمن السيبراني بتاريخ 29 نوفمبر 2020 برئاسة رئيس الأمن السيبراني لحكومة الإمارات ويتبع مجلس الوزراء، ويضم في عضويته عددا من الجهات الاتحادية والمحلية في الدولة، بهدف تطوير استراتيجية وطنية للأمن السيبراني وتعزيزه في كافة القطاعات الحيوية. حيث ان الدولة قد حققت تقدم نوعي فريد في مؤشر الامن السيبراني العالمي فقد تبوأت دولة الامارات المركز الخامس عالمياً وذلك وفق التقرير الصادر عن الاتحاد الدولي للاتصالات التابع للأمم المتحدة حيث قفزت من المرتبة الثالثة والثلاثين عام 2019 إلى المرتبة الخامسة عام 2020؛ لتكون بذلك ضمن أفضل دول العالم في تحقيق الأمن الإلكتروني.

لم تميز التشريعات الجنائية القديمة بين الجرائم الواقعة على أمن الدولة من جهة الخارج والجرائم القائمة على الإخلال بالأمن الداخلي، أما التشريعات الجنائية الحديثة فقد ميزت بين الجرائم الماسة بأمن الدولة من جهة الخارج والجرائم الماسة بأمن الدولة من جهة الداخل، وذلك لما يكون بينهما من خلاف حول طبيعة الحق المعتدى عليه في درجة الجسامة. ويعتبر الأمن من الضروريات الرئيسية لوجود المجتمع واستقراره، فحاجة الإنسان له تعادل حاجته للطعام والشراب والمسكن، وهو أهم ما يلزم الإنسان في حياته، حيث أن الأمن شرط لتحقيق الاستقرار والحياة الهادئة، وهو مظهر لسيادة القانون والنظام، وفي ظل مفهوم الأمن الشامل على مستوى الفرد أو الجماعة أو الدولة، فإن الأمن يستوعب الحياة الإنسانية والقيم والفكر والبيئة المحيطة بها .

فالجرائم الماسة بأمن الدولة من جهة الخارج تقع على الدولة في علاقتها مع الدول الأخرى، ويراد منه الاعتداء على استقلالها، أو زعزعة كيانها في محيطها الدولي، أو الإساءة لعلاقتها بالدول الأخرى، أو إعانة

عدوها عليها. ولا شك أن الاعتداء على أمن الدولة يعد من أكبر الجرائم لأن له خطورة كبيرة على الأمن والاستقرار، لذلك انصرفت عناية الشرائع المختلفة إلى فرض عقوبات مشددة على مرتكبي هذه الجرائم.

وكانت جرائم أمن الدولة– سابقاً– من جهة الخارج ترتكب بالوسائل التقليدية المتاحة، أما في عصرنا الحالي وفي ظل التطور الهائل للتقنيات الحديثة ووسائل الاتصالات المتعددة التي تعمل في أغلبها عن طريق شبكة الإنترنت، حيث أفرز التطور العلمي والتكنلوجي الذي يعد أحد أهم مظاهر العصر الحديث ثورة في الاتصالات والمعلومات، وأصبح ارتكاب الجرائم الماسة بأمن الدولة من جهة الخارج باستخدام هذه التقنيات أكثر سهولة وفعالية.

ونظراً لخطورة تلك الجرائم والوسائل الحديثة التي تستخدم لارتكابها، كان لزاماً على المشرع الاتحادي إيجاد نظام تشريعي خاص لمواجهة الجرائم الماسة بأمن الدولة من جهة الخارج باستخدام التقنيات الحديثة، وهذا الأمر يتطلب أيضاً استراتيجية أمنية موازية للنظام التشريعي وداعمة له من أجل مواجهة الجرائم الماسة بأمن الدولة من جهة الخارج باستخدام التقنيات الحديثة .

وتأخذ الجرائم الماسة بأمن الدولة من جهة الخارج والتي تستخدم فيها التقنيات الحديثة أشكالاً متعددة، فمنها جرائم التخابر لدى دولة أجنبية أو من يمثلها أو تسريب أسرار الدفاع أو إرسال صور وخرائط عن المواقع الحساسة عبر التقنيات الحديثة.

وقد تنبه المشرع الإماراتي لخطورة هذه الجرائم على أمن الدولة من جهة الخارج، وأصدر تشريعاً جنائياً خاصاً لمواجهة جرائم تقنية المعلومات بكافة أشكالها وهو المرسوم بقانون رقم (34) لسنة 2022 ، بشأن مكافحة جرائم تقنية المعلومات. واعتبر المشرع الإماراتي في هذا القانون أن تقنية المعلومات الحديثة ووسائلها بما فيها التطبيقات الذكية ومواقع التواصل الاجتماعي وأجهزة الاتصالات المتطورة هي الوسائل التي تستخدم لارتكاب الجرائم الماسة بأمن الدولة من جهة الخارج .

ويعتبر المشرع الإماراتي من أوائل المشرعين الذين أيقنوا خطورة وسائل تقنية المعلومات واستعمالها كوسيلة للإضرار بأمن واستقرار الدولة من جهة الخارج، وجاء ذلك تماشياً مع ما تشهده دولة الإمارات العربية المتحدة من تطور تقني هائل ومواكبة التشريعات الإماراتية لكافة أشكال التطورات التقنية لتحصين الدولة والمجتمع من الآثار السلبية لوسائل تقنية المعلومات والتي من الممكن أن تكون وسيلة يستخدمها العابثون

وأفراد التنظيمات الإرهابية المتطرفة للعبث بالأمن والاستقرار في دولة الإمارات العربية المتحدة . وإيماناً من المشرع الإماراتي بضرورة الحفاظ على أمن الدولة من جهة الخارج فقد سن مواد قانونية تشدد العقوبة على مرتكبي الجرائم الماسة بأمن الدولة من جهة الخارج باستخدام التقنيات الحديثة وهذا ما سيكون محور بحثنا هذا

ومن خلال التعقيب على الدرسات السابقة والتركيز على أوجه الشبه والاختلاف وما هو الجديد التي ستقدمه هذا الدراسة والاطار النظري للدراسة لبيان **دور الأمن السيبراني في موجهة جرائم الاختراقات التي قد تتعرض لها دولة الامارات العربية المتحدة**، ومعرفة مفهوم الامن السيبراني وماهية **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/ 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.

ثانياً/ 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.

1- قيام المشرع الإماراتي بتحديد أنواع أنظمة الاختراق السيبراني للأنظمة المعلوماتية الحكومية.

References

Al-Rashīdī, Hālā Ahmad (2022). *Al-Irhab al-Saybrānī*, Cairo: Dār al-Nahḍah al-‘Arabīyah, 1st ed.

Al-Suwaidī, Aḥmad Ghānim Sayf (2016). *Al-Muwājaha al-Jinā’īyah wa al-Amnīyah li-l-Jarā’im al-Māsah bi-Amn al-Dawlah al-Dākhilī*, Dubai: Dubai Police Academy, Graduate Studies College.

Al-Sayyid, Khālid Sāmī (2022). *Al-Amn al-Qaumī al-Ilktronī wa Jarā’im al-Ma‘lūmāt*, Cairo: Dār al-Nahḍah al-‘Arabīyah, 1st ed.

Al-Sayyid, Khālid Sāmī (2019). *Istikhdām al-Taqanāt al-Ḥadīthah bi-‘Amalīyāt al-Amn al-Markazī*

li-l-Irtiqā' bi-Ālīyāt al-Muwājaha, Doctoral Dissertation, Graduate Studies College, Police Academy, Cairo.

Tūrkī, Bin ʻAbd al-ʻAzīz (2019). *Tawẓīf Shabakat al-Tawāṣul al-Ijtimāʻī fī al-Tawʻīyah al-Amnīyah ḍidd Khaṭar al-Shā'ī'āt*, Naif Arab University for Security Sciences, Riyadh.

(4) Hāyl, Wadiʻān (2010). *Al-Takhāṣuṣ al-Amnī li-Ra'y al-ʻĀm ḍidd al-Shā'ī'āt*, Symposium on the Role of Civil Society Institutions in Security Awareness, Naif Arab University for Security Sciences, Riyadh.

Al-Ḥarīẓī, Khuṭr al-Ilktronī ʻalā al-Irhab – Twitter Namūdhajan, Doctoral Dissertation, Imam Muhammad bin Saud Islamic University, Saudi Arabia.

Al-Hājirī, Rāshid Ramzān (2012). *Al-Taḥrīẓ al-Ilktronī al-Mukhl bi-Amn al-Dawlah*, Master's Thesis, High Institute of Judiciary, Saudi Arabia.

Himīsī, Riḍā (2011). *Al-Iʻlām al-Jadīd Bayna Ḥurīyat al-Taʻbīr wa Ḥimāyat al-Amn al-Waṭanī*, Master's Thesis, Qāṣidī Murbaḥ University, Algeria.

Al-Ṣayfī, ʻAbd al-Fattāḥ Muṣṭafā (2016). *Al-Taḥrīẓ ʻalā al-Jarīmah al-Irhābīyah wa Wādʻuhu min al-Nazariyyah al-ʻĀmah li-l-Mushārakah al-Jinā'īyah*, Doctoral Dissertation, Faculty of Law, Alexandria University.

Al-ʻAlāwanah, Ḥātim Salīm (2012). *Dawr al-Tawāṣul al-Ijtimāʻī fī Taḥrīẓ al-Muwāṭinīn li-l-Mushārakah fī al-Ḥarak al-Jamāhīrī*, Master's Thesis, Yarmouk University, Jordan.

Al-ʻAwāyishah, Ālā' Firās Shaḥādah (2022). *Al-Mas'ūlīyah al-Madaniyyah li-Muzawidī al-Khidmah fī al-Amn al-Saybrānī*, *Majallat Jāmiʻat ʻAmman al-ʻArabīyah li-l-Buḥūth - Silsilat al-Buḥūth al-Qānūnīyah*, University of Amman, College of Graduate Studies and Scientific Research, Vol. 4, Issue 2.

Nāṣir, Muḥammad (2023). *Ashkāl Intihāk al-Faḍā' al-Saybrānī wa Wasā'iluhā wa Āthāruhā*, *Majallat al-Nadwah li-l-Dirāsāt al-Qānūnīyah*, Morocco: Vol. 40.