International Journal of Advanced Research on Law and Governance
Volume 5, Issue 2, 2023. 176 - 200

Open Access VOL5(2) 2023

The crime of electronic hacking in UAE legislation

Dr. Ibrahim El-Shahat Lotfy

PhD in Law, Faculty of Law, Mansoura University

Abstract:

The world is currently witnessing a technological revolution in the field of information systems and the Internet, the benefits of which have been reaped by humans by facilitating the means of life in various fields. However, this electronic globalization has brought within it new forms of information crimes, including the crime of electronic hacking. Penetration crimes of any website, electronic information system, information network,[1] or information technology means have increased, which is considered a development in advanced criminal methods using modern technology, due to criminals penetrating this information and programs, accessing them, and attacking their content, whether by changing them, or Damaging or stealing it, and the matter becomes more dangerous in the case of electronic hacking on the information systems of state institutions.

Therefore, the UAE criminal legislature - like other modern legislation - worked to protect private data and information, as well as those that affect the state's internal and external security, preserved in the information system, networks, and websites, by criminalizing the hacking of websites, whether this hacking occurred on any website or electronic information system. Or an information network or an information technology means([2]), as well as the crime of hacking into the information systems of state institutions([3]), due to the seriousness and importance of the information that contains state secrets, and the majority of modern penal legislation has considered this crime to be one of the crimes that affect the security

[1] Baha Abu-Shaqra,"Technoethics and Organizing: Exploring Ethical Hacking within a Canadian University",A thesis submitted to the Faculty of Graduate and Postdoctoral Studies in partial fulfillment of the requirements for the MA degree in Communication,Faculty of Arts University of Ottawa,Canada 2015, P.1.

[2] المادة 2 من قانون مكافحة الشائعات والجرائم الإلكترونية الإماراتي رقم (34) لسنة 2021م.

[3] المادة 3 من قانون مكافحة الشائعات والجرائم الإلكترونية الإماراتي رقم (34) لسنة 2021م.

of the state, especially if this crime evolves from accessing data and information to trading in it.

Keywords: Electronic hacking, UAE legislation, Measures and procedures.

Citation: Ibrahim El-Shahat Lotfy, The crime of electronic hacking in UAE legislation, The International Journal of Advanced Research on Law and Governance, Vol.5, Issue 2, 2023.

International Journal of Advanced Research on Law and Governance
Volume 5, Issue 2, 2023. 176 - 200

جريمة الاختراق الإلكتروني في التشريع الإماراتي

إبراهيم الشحات لطفي

دكتوراه في الحقوق، كلية الحقوق، جامعة المنصورة

يشهد العالم في الوقت الحاضر ثورة تكنولوجية في مجال الأنظمة المعلوماتية والإنترنت جنى الإنسان ثمارها من خلال تسهيل سُبل الحياة في مختلف المجالات. غير إنه حملت هذه العولمة الإلكترونية بين ثناياها صوراً جديدة من صور الجرائم المعلوماتية والتي من بينها جريمة الاختراق الإلكتروني؛ فقد زادت جرائم الاختراق لأي موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية معلومات [4] مما يعد تطوراً في الأساليب الإجرامية المتطورة باستخدام التكنولوجيا الحديثة، نظراً لاختراق المجرمين هذه المعلومات والبرامج، والولوج إليها، والاعتداء على محتواها سواء كان ذلك بتغييرها، أو إتلافها، أو سرقتها، كما يزداد الأمر خطورة في حالة الاختراق الإلكتروني الواقع على الأنظمة المعلوماتية الخاصة بمؤسسات الدولة.

لذلك عمل المشرع الجنائي الإماراتي– كبقية التشريعات الحديثة– على حماية البيانات والمعلومات الخاصة وكذلك التي تؤثر على أمن الدولة الداخلي والخارجي المحفوظة في النظام المعلوماتي والشبكات والمواقع الإلكترونية، وذلك من خلال تجريم اختراق المواقع الإلكترونية سواء وقع هذا الاختراق على أي موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية معلومات[5]، كما جرم الاختراق الواقع على الأنظمة المعلوماتية الخاصة بمؤسسات الدولة[6]، نظراً لخطورة وأهمية المعلومات التي تحتوي على أسرار الدولة، كما قد اعتبرت غالبية التشريعات العقابية الحديثة أن هذه الجريمة من الجرائم التي تمس أمن الدولة، خاصة إذا تطورت هذه الجريمة من الاطلاع على البيانات والمعلومات إلى المتاجرة بها.

الكلمات المفتاحية: الاختراق الإلكتروني، التشريع الإماراتي، التدابير والإجراءات.

أهمية البحث:

لقد أدى التطور السريع والمتلاحق لتقنية المعلومات، إلى مضاعفة المخاطر والاعتداءات على الأمن القومي، من خلال ما يُعرف بالتجسس الإلكتروني والإرهاب عن بُعد، ولم يقتصر الاعتداء على القطاع المدني. بل كان لها أكبر الأثر في تطوير أنظمة الحرب الحديثة، وأدى إلى ظهور ما يُسمى بحرب المعلومات لأهداف سياسية وعسكرية، لذلك أصبحت

(4)Baha Abu-Shaqra,"Technoethics and Organizing: Exploring Ethical Hacking within a Canadian University",A thesis submitted to the Faculty of Graduate and Postdoctoral Studies in partial fulfillment of the requirements for the MA degree in Communication,Faculty of Arts University of Ottawa,Canada 2015, P.1.

(5) المادة 2 من قانون مكافحة الشائعات والجرائم الإلكترونية الإماراتي رقم (34) لسنة 2021م.

(6) المادة 3 من قانون مكافحة الشائعات والجرائم الإلكترونية الإماراتي رقم (34) لسنة 2021م.

شبكة المعلومات الدولية مجالًا خ صبًا لن شر أفكار العديد من الأفراد والمجموعات الإرهابية، وو سيلة لترويج أخبار وأمور أخرى قد تحمل في طياتها مساسًا بأمن الدولة، أو بنظام الحكم أو قدحًا في رموز دولية أو سياسية[7].

كما تزداد أهمية هذا البحث إذا ما سلمنا بأنه تمتلك أي دولة في العالم بعض الأسرار التي لا ينبغي لأي شخص أن يقوم بالاطلاع عليها دون إذن أو مســـوغ، وأي اطلاع عليها أو اعتداء، قد يؤدي لحدوث أزمات داخلية وخارجية [8] حيث تؤثر تلك الاعتداءات على أمن الدولة الداخلي والخارجي خاصـــة إذا تطورت هذه الجرائم من مجرد الاطلاع على البيانات والمعلومات إلى المتاجرة بها.

ثالثًا: إشكالية البحث:

يثير البحث عدة إشـــكاليات مهمة لعل أهمها يكمن في حداثة الجرائم الواقعة على أمن الدولة المعلوماتي، وذلك نظرًا لارتباطها بالتقدم التكنولوجي، الأمر الذي يترتب عليه ضرورة تحديد البنيان القانوني لجريمة الاختراق الإلكتروني لا سيما وإنها ت شكل إحدى الجرائم الواقعة على أمن الدولة المعلوماتي، ومدى ا شتراط أن يكون النظام المعلوماتي المخترق محميًا أمنيًّا، أم أن الجريمة تقع كذلك على النظام غير المحمي؟ ومدى نجاح المشـــرع الإماراتي في فرض الحماية الجنائية لهذه المواقع.

رابعا: منهج البحث:

يعتمد الباحث على المنهج الوصفي التحليلي، وذلك بجمع المعلومات المتعلقة بموضوع البحث، ووصفها، وتحليلها، وتشخيصها من مُختلف جوانبها، وأبعادها المختلفة، بهدف التوصل إلى نظرة واضحة عن النظام القانوني لجريمة الاختراق الإلكتروني في التشريع الإماراتي.

خامسا: خطة البحث:

المبحث الأول: أركان جريمة الاختراق الإلكتروني.

المبحث الثاني: العقاب على جريمة الاختراق الإلكتروني.

(7) د. تركي بن عبد الرحمن المويشـــير، بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته، إصـــدارات جامعة نايف العربية للعلوم الأمنية مركز البحوث والدرا سات، جامعة نايف العربية للعلوم الأمنية، مركز الدرا سات والبحوث، الرياض، المملكة العربية السعودية، 2012م، ص39.

(8) Bainbridge. D: Introduction to computer law, fourth edition, London, 2000, P.307.

International Journal of Advanced Research on Law and Governance
Volume 5, Issue 2, 2023. 176 - 200

المبحث الأول

أركان جريمة الاختراق الإلكتروني

تمهيد وتقسيم:

من المسلم به أنه تُعد أركان الجريمة الأساس والأصل لقيام أي جريمة، والمشرع يتطلب لقيام الجريمة توافر أركانها المادي والمعنوي، وبدون هذين الركنين لا تقوم الجريمة، وجريمة الاختراق الإلكتروني؛ كأي جريمة يلزم لتحققها توافر ركنين أحدهما مادي، والآخر معنوي(9)، وهو ما نوضحه من خلال ما يلي:

المطلب الأول

الركن المادي لجريمة الاختراق الإلكتروني

يتكون الركن المادي للجريمة من نشـــاط إجرامي بارتكاب فعل أو الامتناع عن فعل متى كان هذا الارتكاب أو الامتناع مجرماً قانوناً"، وينهض الركن المادي في الجريمة التامة على عناصـــر ثلاثة، هي: الســـلوك الإجرامي، والنتيجة، وعلاقة السببية التي تربط بينهما(10).

أولًا: السلوك الإجرامي في جريمة الاختراق الإلكتروني:

من المسلم به أنه تتخذ الجريمة المعلوماتية من الفضاء الافتراضي مسرحاً لها، مما يجعلها تتميز بخصوصيات تنفرد بها، إلا أن ذلك لا يعني عدم وجود تشابه لها مع الجريمة المرتكبة في العالم التقليدي أو المادي، فهي تشترك بوجود الفعل غير المشروع، ومجرم يقوم بهذا الفعل، وبالتالي لا يختلف مفهوم الركن المادي في الجريمة المعلوماتية عما تقدم. إذ ينطلق مبدأ تحديد الفعل غير المشروع وإعطائه صفة الجريمة بتحديد الركن المادي فيه، فلا جريمة دون ركن مادي، ومع ذلك يتمثل الركن المادي في الجريمة المعلوماتية–عموماً– في السلوك الذي يقوم به الجاني من أجل تحقيق غاية ما، ويحدد له القانون العقاب اللازم، وهو يتباين بتباين الجرائم المرتكبة من قبل الجاني، شـــريطة أن يكون له مظهر خارجي ملموس، غير أن تحديد الركن المادي في الجرائم المعلوماتية تكتنفه العديد من الصعوبات خاصة فيما يتعلق بتحديد النتيجة الإجرامية والرابطة السببية(11).

ويُعد السلوك الإجرامي أهم عناصر الركن المادي لأي جريمة، لأنه يكشف عن سلوك مخالف لإرادة المشرع، ويبدو بمظاهر مادية ملموســـة في العالم الخارجي، ويعني ذلك أن الأفكار داخل النفس لا عقاب عليها. غير إنه لما كان

(9) حكم المحكمة الاتحادية العليا في دولة الإمارات، الدائرة الجزائية، الطعون أرقام 1307، 1308، 1420، 1430 لسنة 2023 جزائي، جلسة 2023/11/7.

(10) انظر المادة (32) من قانون الجرائم والعقوبات الإماراتي رقم 31 لسنة 2021م.

(11) نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، رسالة ماجستير، كلية الحقوق، جامعة الإسكندرية، 2006م، ص45.

الجاني في الجرائم المعلوماتية يختلف عن الجاني في غيرها من الجرائم من حيث كونه ذو خبرة كافية في مجال استخدام التقنيات الحديثة، فإن السلوك الإجرامي الذي سيصدر منه في مجال ارتكاب الجريمة الإلكترونية حتماً سيختلف عن الجاني التقليدي [12]، ويتحقق الركن المادي بفعل الاختراق، وهو ما يختلف عن الدخول بأن الأخير يكون بفتح جهاز الحاسب الآلي أو باستخدام كلمة سر أو رمز أو كود سري، بينما الاختراق يكون بأية وسيلة أخرى، كأن يكون ذلك باستخدام برامج متخصصة لاختراق المواقع والأنظمة المعلوماتية والحسابات الشخصية.

ويتجه البعض من الفقه[13] للقول بأن هناك فرقاً بين الدخول والاختراق، حيث إن الدخول غير المشروع كان يقصد به الدخول من جانب أحد المتعاملين مع المواقع الإلكترونية أو البريد الإلكتروني أو الحساب الخاص أو النظام المعلوماتي الذي يخص الدولة من الموظفين العموميين العاملين لديها، ومن المصرح لهم بالتعامل معها، فيخالف القواعد والتعليمات الخاصة بالدخول أو البقاء، بينما الاختراق فيكون من غير العاملين بالدولة المصرح لهم بالتعامل مع هذه المواقع الإلكترونية أو الحسابات أو النظم المعلوماتية، كأن يكون شخصاً أجنبياً يحاول الدخول إلى هذه المواقع أو الحسابات أو الأنظمة المعلوماتية الحكومية.

ويُلاحظ مما تقدم أن الركن المادي في جريمة الاختراق الإلكتروني يتطلب وجود بيئة رقمية واتصال بالإنترنت، كما يتطلب أيضاً معرفة بداية هذا النشاط والشروع فيه، ونتيجة لذلك نجد أنه قد يقوم مرتكب هذه الجريمة مثلاً بتجهيز جهاز الحاسب الآلي لكي يحقق له حدوث الجريمة، فيقوم بتحميل برنامج اختراق أو أن يقوم بإعداد هذا البرنامج بنفسه، كما يمكن أن يقوم بتلك الجريمة عن طريق إعداد برامج فيروسات تمهيداً لبثها، وبالتالي قد يعاقب الجاني في هذه الجريمة لمجرد التحضير للجريمة، وذلك بشراء برامج التجسس والاختراق ومعدات فك الشفرات وكلمات المرور.

ثانيا: النتيجة الإجرامية وعلاقة السببية:

تُعد النتيجة الإجرامية الأثر المباشر للسلوك الإجرامي غير المشروع، والجريمة المعلوماتية كغيرها من الجرائم التي يُفترض وجود النتيجة الإجرامية فيها كعنصر من عناصر الركن المادي للجريمة، وتختلف النتيجة الإجرامية في الجريمة المعلوماتية بحسب نوع الجريمة المرتكبة، حيث إن الجرائم المعلوماتية تتنوع وتتعدد لذلك فالنتيجة الإجرامية تختلف باختلاف نوع الجريمة المعلوماتية المقترفة. فقد تتمثل النتيجة الإجرامية في الجريمة محل البحث في مجرد الاختراق، أو إحداث أضرار أو تدمير أو إيقاف عن العمل أو تعطيل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة

(12) نبيلة هبة هروال، المرجع السابق، ص45.

(13) د. رامي متولي القاضي، المواجهة الجنائية لجرائم تقنية المعلومات في التشريع المصري في ضوء أحكام القانون 175 لسنة 2018م، مقارناً بالمواثيق الدولية والتشريعات المقارنة، بحث منشور في مجلة البحوث القانونية والاقتصادية، العدد 75، كلية الحقوق، جامعة المنصورة، مارس 2021م، ص1067، 1068.

معلومات أو وسيلة تقنية المعلومات، أو إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أو الحصول على أي بيانات أو معلومات أو خسارة سريتها[14].

فالنتيجة هي الأثر المادي المترتب على القيام بالفعل أو النشاط المادي غير المشروع، وهي أيضًا الأثر القانوني الذي يمثل اعتداءً على الأنظمة المعلوماتية الخاصة بمؤسسات الدولة، وذلك بإحداث أضرار أو تدمير أو إيقاف عن العمل أو تعطيل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية المعلومات، أو إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أي بيانات أو معلومات أو خسارة سريتها أو وقعت الجريمة نتيجة لهجمة إلكترونية[15].

وتُعد علاقة السببية عنصراً مهماً من عناصر الركن المادي للجريمة؛ فهي حلقة وصل بين السلوك الإجرامي والنتيجة الإجرامية، وذلك بأن يثبت أن هذا السلوك هو سبب تلك النتيجة الإجرامية، كذلك فإن علاقة السببية تساهم في تحديد نطاق المسؤولية الجنائية، واستبعاد المسؤولية إذا لم ترتبط النتيجة الإجرامية بالفعل[16].

وقد نستطيع تطبيق القواعد المطبقة على الجرائم العادية على الجرائم المعلوماتية، فيما يتعلق بعلاقة السببية إذا انطبقت عليها، ففي الجريمة محل الدراسة نجد أن فعل يتحقق بالنشاط المادي الصادر عن الجاني وهو ليس في حاجة لاستعمال العنف لتحقق النتيجة إذ تتحقق النتيجة لمجرد إتيانه أحد صور هذا السلوك، وبالتالي فإن رابطة السببية متوافرة بين نشاطه المادي والنتيجة الإجرامية.

ولا شك أن تحديد رابطة السببية في مجال الجرائم المعلوماتية يُعد من المسائل الصعبة والمعقدة بالنظر إلى تعقيدات صناعة الحاسوب وشبكة الإنترنت، وتطور إمكانياتها، وتسارع هذا التطور، إضافة إلى تعدد وتنوع أساليب الاتصال بين الأجهزة الإلكترونية، وتعدد المراحل التي تمر بها الأوامر المدخلة حتى تخرج وتنفذ النتيجة المراد الحصول عليها، كل ذلك سيؤدي حتماً إلى صعوبة تحديد السبب أو الأسباب الحقيقية للإساءات المرتكبة في هذه المسؤولية[17].

كما أن رابطة السببية في الجرائم المعلوماتية أساسية لتحديد نطاق المسؤولية الجنائية في كافة صور جرائم الاختراق الإلكتروني. فالعلاقة التقنية بين مرتكب الجريمة وبين الآلة محل الجريمة المعلوماتية هي الأساس لبيان رابطة السببية في الجرائم المعلوماتية، ويقع عبء إثبات وجود تلك الرابطة من عدمها على النيابة العامة، بما يقدم إليها من أدلة

(14) د. لورنس سعيد أحمد الحوامدة، الجرائم المعلوماتية: أركانها وآلية مكافحتها: دراسة تحليلية مقارنة، بحث منشور في مجلة الميزان للدراسات الإسلامية والقانونية، جامعة العلوم الإسلامية العالمية، عمان، المملكة الأردنية الهاشمية، المجلد الرابع، العدد الأول، يناير 2017م، ص201 وما بعدها.

(15) المادة 3 من قانون مكافحة الشائعات والجرائم الإلكترونية رقم (34) لسنة 2021م.

(16) د. لورنس سعيد أحمد الحوامدة، المرجع السابق، ص206.

(17) منصور بن صالح السلمي، المسؤولية المدنية لانتهاك الخصوصية في نظام مكافحة جرائم المعلوماتية السعودية، رسالة ماجستير، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، 2010م، ص75، 76.

وبينات واستماع للشهود في مثل هذا النوع من الجرائم المستحدثة، والتي تحتاج إلى أدلة إثبات أخرى تختلف وأدلة الإثبات التقليدية.

المطلب الثاني

الركن المعنوي لجريمة الاختراق الإلكتروني

يُعد الركن المعنوي ركن أســـاســـي في تكوين الجريمة. حيث لا تقوم الجريمة دونه، ويُعتبر الركن المعنوي هو الحالة النفسية للجاني، والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني، ويطلق عليه الركن الأدبي أو الشخصي وهو يعني في الحقيقة الجاني أو المجرم تحديداً، ويُقصد به مدى اتجاه إرادة الجاني إلى ارتكاب الجريمة. فإذا اتجهت إرادته إلى ارتكابها توافر لديه القصد الجنائي وكانت الجريمة عمدية، وإذا لم تتجه تلك الإرادة إلى ارتكابها وتوافر لديه الخطأ غير العمدي كانت الجريمة غير عمدية[18].

أولًا: القصد الجنائي في جريمة الاختراق الإلكتروني:

يكتســـب تحديد الركن المعنوي في الجريمة المعلوماتية بالغ الأهمية بوجه عام، كما هو الحال بالنســـبة للجريمة المرتكبة في العالم المادي، حيث بموجبه يمكن تحديد مناط مساءلة الجاني، وذلك بتحديد القصد الجنائي لديه، الذي بدونه لا يمكن أن يعاقب الشخص المرتكب للفعل.

ولا يتحقق القصد الجنائي في الجريمة محل البحث إلا إذا كان الجاني يعلم بالعناصر الأساسية لقيام هذه الجريمة سواء تعلق ذلك بسلوكه الإجرامي أم بموضوع الاعتداء، فإذا كان الجاني جاهلًا بشيء من ذلك، فلا يتحقق القصد الجنائي، فلا يتحقق القصـــد الجنائي إلا إذا كان الجاني يعلم أنه اخترق عمداً، أو دخل بخطأ غير عمدي موقعًا أو بريداً إلكترونيًا أو حساباً خاصًا أو نظاماً معلوماتيًا يُدار بمعرفة أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة، أو مملوكًا لها، أو يخصها. فالذي يدخل أحد هذه المواقع أو الأنظمة وهو يجهل ذلك، فإنه لا يتوفر القصد الجنائي قبله، وليس كل جهل ينتفي معه القصد الجنائي، بل هناك وقائع يؤثر الجهل بها في القصد، وأخرى لا يتأثر بها القصد.

ويقوم الركن المعنوي في جريمة الاختراق الإلكتروني على أســـاس مجســـد في توافر الإرادة الأثمة لدى الفاعل، وتوجيه هذه الإرادة إلى القيام بعمل غير مشـــروع جرمه القانون، كاختراقه عمداً، أو بخطأ غير عمدي موقعًا أو بريداً إلكترونيًا أو حساباً خاصًا أو نظاماً معلوماتيًا يُدار بمعرفة أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة، أو مملوكًا لها، أو يخصها. كما يجب أن تتوفر النتيجة الإجرامية المترتبة على الأفعال السابقة، فتكتسب إرادة الجاني الصفة الجرمية.

ويُلاحظ أن هذه الجريمة من الجرائم العمدية، حيث يتخذ الركن المعنوي فيها صورة القصد الجنائي العام بعنصريه العلم والإرادة[19]، فيلزم توافر علم الجاني بأن فعله ينصـــب على موقع إلكتروني أو نظام معلومات إلكتروني أو شـــبكة

(18) د. غنام محمد غنام، د. تامر محمد صالح، شرح قانون العقوبات: القسم العام، بدون دار نشر، 2023م، ص97.
(19) د. أشرف توفيق شمس الدين، شرح قانون العقوبات، القسم العام، النظرية العامة للجريمة والعقوبة، طبعة خاصة لطلاب التعليم المفتوح بكلية لحقوق بجامعة بنها، دون دار نشر، 2009م، ص155.

معلومات أو و سيلة تقنية معلومات، أو على موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو و سيلة تقنية معلومات عائدة لمؤسسات الدولة، باعتبار ذلك الموقع أو النظام أو الشبكة أو الوسيلة المحل الذي يحميه المشرع، ولا يؤثر على توافر القصد الجنائي أن يقصد الفاعل الدخول إلى نظام، ثم يترتب على فعله الدخول على نظام آخر؛ لأن ذلك من باب الحيدة عن الهدف التي لا تؤثر على توافر القصد الجنائي، حيث يجهل الفاعل طبيعة فعله المتمثل بالدخول لنظام معلوماتي؛ لأن المجرم المعلوماتي في أغلب الأحوال يتوافر لديه خبرة تكنولوجية في هذا المجال، إلا أنه حال حدوث ذلك ينتفي القصد الجنائي[20].

ثانيا: صور القصد الجنائي في جريمة الاختراق الإلكتروني:

للركن المعنوي صورتان، الصورة الأولى: تتمثل في القصد الجنائي أو العمد، أما الصورة الثانية: فهي تتمثل في الخطأ، وتشترك الصورتان معاً في إرادة السلوك أي أن الجاني يريد السلوك والنتيجة في القصد الجنائي، بينما تختلف الصورتان في إرادة النتيجة حيث يريد الجاني السلوك في الخطأ دون النتيجة[21].

وللقصد الجنائي صورتان: الصورة الأولى: القصد الجنائي العام، إذ يهدف الجاني عند ارتكابه الواقعة الإجرامية مع العلم بعناصرها **إلى** تحقيق غرض معين، بتحقيقه قد تتم الجريمة ويتوافر لها القصد الجنائي العام، ففي جريمة القتل يكون غرض الجاني إزهاق روح المجني عليه، وفي جريمة السرقة يكون غرض الجاني حيازة المال المسروق، وفي جريمة الرشوة يكون غرض الجاني الحصول على منفعة من الراشي، وبالتالي فإن القصد الجنائي العام أمر ضروري ومطلوب في كل الجرائم العمدية.

الصورة الثانية: القصد الجنائي الخاص: إذ يلتقي القصد الخاص مع القصد العام في جميع عناصره، ويزيد عنه في تحديد الإرادة الإجرامية لدى الجاني إما بباعث معين قد يدفعه إلى الجريمة، وإما بنتيجة محددة يريدها، وحكمة هذا التحديد هي الرغبة في توضيح هذه الجريمة وتمييزها عن غيرها من الجرائم التي تشترك معها في بعض العناصر[22]، ويتكون القصد الجنائي الخاص من عنصري العلم والإرادة بالإضافة إلى عنصر ثالث، وهو عنصر الباعث أو الغرض على ارتكاب الجريمة. فالباعث هو العامل النفسي أو القوة الدافعة التي تحرك إرادة الجاني نحو ارتكاب الجريمة[23].

وبالتطبيق على جريمة الاختراق الإلكتروني نجد أن هذه الجريمة يمكن أن تقع عمداً أو بطريق غير عمدي، وإذا كان القصد الجنائي العام يقوم على العلم والإرادة، كما يقوم القصد الجنائي الخاص على العلم والإرادة، فإنه يمتاز عنه بأن

(20) د. عبد الإله محمد النوايسة، جريمة الدخول غير المشروع في تشريعات الجرائم الإلكترونية العربية: دراسة مقارنة، المجلة القانونية والقضائية، السنة (10)، العدد (1)، 2016م، ص47.

(21) د.عمر الشريف، درجات القصد الجنائي، الطبعة الأولى، دار النهضة العربية، القاهرة، 2002م، ص(أ).

(22) د.منصور رحماني، الوجيز في القانون الجنائي العام، فقه، قضايا، دار العلوم للنشر والتوزيع، الجزائر، 2006م، ص112.

(23) د. محمد محرم محمد ود. خالد محمد المهيري، قانون العقوبات الاتحادي لدولة الإمارات العربية المتحدة فقهاً وقضاءً، الطبعة الثانية، الفتح للطباعة والنشر، الإسكندرية، 1992م، ص107.

العلم والإرادة فيه لا يقتصران على أركان الجريمة وعناصرها، وإنما يمتدان بالإضافة إلى ذلك إلى وقائع ليست في ذاتها من أركان الجريمة، وإذا تطلب القانون في جريمة توافر القصد الخاص فمعنى ذلك أنه يتطلب أولًا انصراف العلم والإرادة إلى أركان الجريمة، وبذلك يتوافر القصد العام، ثم يتطلب بعد ذلك انصراف العلم والإرادة إلى وقائع لا تُعد طبقًا للقانون من أركان الجريمة، وبهذا الاتجاه الخاص للعلم والإرادة يقوم القصد الخاص، ولقيام الركن المعنوي في جريمة الاختراق المعلوماتي فإنه، لابد أن يعلم الجاني أنه يرتكب هذه الجريمة من خلال شبكة الإنترنت كأحد الأفعال التي يتضمنها نص التجريم، وأن تتجه إرادته إلى القيام بذلك الفعل[24].

أما عن الإثبات في توافر الركن المعنوي؛ فهو يقع على عاتق النيابة العامة، والمحكمة المختصة بالنظر في مثل هذا النوع من الجرائم، والمحكمة صاحبة الاصلاحية بتقدير وجود سوء النية من عدمها، ووزن البينات، وتمحيصها بما لها من صلاحية باعتبارها صاحبة القرار النهائي بالفصل في الدعاوى المرفوعة أمامها، وعليه؛ فلا يتريث المشرع لإنزال العقاب إلى أن تتحقق النتيجة الإجرامية. بل يبادر ويعجله ليرجع التجريم إلى لحظة مبكرة تُعتبر فيها الجريمة قد تمت عندها، ولو لم تكن كذلك في الحقيقية، فالمشرع وبالنظر لخطورة الجرائم مبكرة الاتمام في محيط الجرائم الماسة بأمن الدولة المعلوماتي رأى ضرورة شمول السلوك المكون لها بالعقاب على الرغم من أنه لم يصل بعد إلى حد الفعل الذي يضر بصورة مباشرة بالمصلحة المحمية في نطاق تلك الجرائم كما في حالة الاتفاق على ارتكاب جريمة ماسة بأمن الدولة المعلوماتي لأن هذه الصورة لا تدخل في نطاق التجريم والعقاب طبقًا للقواعد العامة.

ولما كانت جرائم الاختراق الإلكتروني شُكل تحديًا كبيرًا يواجه المشرع الجنائي في كافة المجتمعات، نظرًا لضخامة الأضرار التي قد تنجم عن مثل تلك الجرائم، والتي قد تصل إلى حد انهيار مجتمع بأكمله؛ الأمر الذي أدى إلى الحاجة الملحة لمواجهة هذه الجرائم بقواعد خاصة تتميز بالشدة والردع. لذلك خص المشرع العقابي هذه الجرائم بسياسة جزائية تختلف عن الجرائم الأخرى، ويأتي ذلك من منطلق خطورة هذه الجرائم، وأهمية المصلحة التي يستهدف المشرع حمايتها، لذلك اعتمد المشرع على السياسة التحوطية، وقد ظهر ذلك بوضوح في بعض الجوانب المتعلقة بالركن المادي والركن المعنوي لجريمة الاختراق الإلكتروني.

(24) منصور بن صالح السلمي، المرجع السابق، ص78.

المبحث الثاني

العقاب على جريمة الاختراق الإلكتروني

تمهيد وتقسيم:

نص المشرع الإماراتي على مجموعة من العقوبات المقررة لجريمة الاختراق الإلكتروني، وقد تكون هذه العقوبات عقوبات أ صلية، وقد تكون عقوبات تكميلية، وبالإ ضافة إلى هذه العقوبات نص الم شرع أي ضًا على مجموعة من التدابير والإجراءات التحفظية التي يمكن اتخاذها ضد مرتكبي جرائم الاختراق الإلكتروني.

المطلب الأول: العقوبات الأصلية والتكميلية المقررة.

المطلب الثاني: التدابير والإجراءات التحفظية.

المطلب الأول

العقوبات الأصلية والتكميلية المقررة

أولًا: العقوبات الأصلية المقررة:

تعرف العقوبات الأصلية بأنها العقوبات التي فرضها المشرع كجزاء أساسي جزاء للجريمة، ويُمكن الحكم بها دون الحكم بأي عقوبة أخرى[25]. وقيل إنها العقوبات التي يجوز الحكم بها بـ صفة أ صلية أ سا سية كجزاء عن جريمة معينة، ويتوقف عليها التق سيم الثلاثي للجرائم، وهي منفردة أي بغير أن يكون الحكم بها مُعلقًا على الحكم بعقوبة أخرى، ولا يمكن تنفيذ هذه العقوبات إلا إذا قُضـــي بها في الحكم[26]، وقد نص عليها المشـــرع الاتحادي في المادة (67) من قانون الجرائم والعقوبات[27].

كما قرر الم شرع الإماراتي أن تطبيق العقوبات المذ صوص عليها في المر سوم بقانون اتحادي رقم (34) لـ سنة 2021م في شأن مكافحة الشائعات والجرائم الإلكترونية الإماراتي لا تخل بتطبيق أية عقوبة أشد ينص عليها قانون الجرائم والعقوبات، أو أي قانون آخر[28]. كما يشدد القانون الإماراتي من عقوبة الجريمة عندما تُرتكب من الموظفين المسئولين عن

(25) خالد ســـليمان عبد الله الحمادي، جريمة الدخول غير المشـــروع إلى النظام المعلوماتي في القانون القطري: دراســـة مقارنة، رسالة ماجستير، كلية القانون، جامعة قطر، دولة قطر، 2019م، ص104.

(26) د. أحمد فتحي سرور، الو سيط في قانون العقوبات، القـ سم العام، الطبعة الـ ساد سة، مطورة ومحدثة، دار النهـ ضة العربية، القاهرة، 2015م، ص380.

(27) المادة 67 من قانون الجرائم والعقوبات الإماراتي.

(28) المادة 72 من قانون مكافحة الشائعات والجرائم الإلكترونية رقم (34) لسنة 2021م.

الأنظمة[29]، وشـــدد القانون الإماراتي العقوبة إذا ما ارتكب الجاني أي جريمة منصـــوص عليها في هذا المرســـوم بقانون لحساب أو لمصلحة دولة أجنبية أو أي جماعة معادية أو جماعة إرهابية أو تنظيم غير مشروع[30].

وتتضح معالم تطبيق قاعدة التناسب بين الجريمة والعقوبة، والتدرج في العقوبة من خلال ما نص عليه المشرع الإماراتي في معاقبة الجاني على جريمة الاختراق الإلكتروني عموماً فيما يلي:[31]:

1. عقوبة الحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تزيد على ثلاثمائة ألف درهم، أو بإحدى هاتين العقوبتين، لكل من اخترق موقع إلكتروني أو نظام معلومات إلكتروني أو شـــبكة معلومات أو وســـيلة تقنية معلومات.

2. تكون العقوبة الحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن مائة وخمسون ألف درهم ولا تزيد على خمسمائة ألف درهم، أو بإحدى هاتين العقوبتين، إذا ترتب على الاختراق إحداث أضرار أو تدمير أو إيقاف عن العمل أو تعطيل موقع إلكتروني أو نظام معلومات إلكتروني أو شـــبكة معلومات أو وســـيلة تقنية المعلومات، أو إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أو الحصول على أي بيانات أو معلومات أو خسارة سريتها.

3. تكون العقوبة الحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن مائتي ألف درهم ولا تزيد على خمسمائة ألف درهم، أو بإحدى هاتين العقوبتين، إذا كان الاختراق بغرض الحصول على البيانات أو المعلومات لتحقيق غرض غير مشروع.

وفيما يتعلق بصورة هذه الجريمة إذا ما ارتكبت ضد الأنظمة المعلوماتية الخاصة بمؤسسات الدولة، فيما يلي:[32]:

1. عقوبة السجن المؤقت والغرامة التي لا تقل عن مائتي ألف درهم ولا تزيد على خمسمائة ألف درهم، لكل من اخترق موقع إلكتروني أو نظام معلومات إلكتروني أو شـــبكة معلومات أو وســـيلة تقنية معلومات عائدة لمؤسسات الدولة.

2. تكون العقوبة السجن مدة لا تقل عن خمس سنوات والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تزيد على مليون وخمسمائة ألف درهم، إذا ترتب على الاختراق إحداث أضرار أو تدمير أو إيقاف عن العمل أو تعطيل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية المعلومات، أو إلغاء

(29) المادة 1/60 من قانون مكافحة الشائعات والجرائم الإلكترونية رقم (34) لسنة 2021م.
(30) المادة 3/60 من قانون مكافحة الشائعات والجرائم الإلكترونية رقم (34) لسنة 2021م.
(31) المادة 3 من قانون مكافحة الشائعات والجرائم الإلكترونية رقم (34) لسنة 2021م.
(32) المادة 3 من قانون مكافحة الشائعات والجرائم الإلكترونية رقم (34) لسنة 2021م.

أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أي بيانات أو معلومات أو خسارة سريتها أو وقعت الجريمة نتيجة لهجمة إلكترونية.

3. وتكون العقوبة السجن مدة لا تقل عن سنوات والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تزيد على مليون وخمسمائة ألف درهم، إذا كان الاختراق بغرض الحصول على البيانات أو المعلومات الخاصة بتلك الجهات المنصوص عليها بالفقرة الأولى من هذه المادة.

ثانيا: العقوبات التكميلية المقررة:

إن العقوبة التكميلية هي عقوبة ثانوية لا يمكن الحكم بها بمفردها بل لابد من وجود عقوبة أخرى أصلية، وترتبط العقوبة التكميلية بنوع معين من الجرائم، ولا توقع إلا إذا نطق بها القاضي، وتدخل في نطاق سلطته التقديرية، ويرجع في نصوص القانون في جواز أو وجوب توقيعها [33].

كما يُلاحظ أن العقوبات التكميلية هي العقوبات التي يوقعها القاضي وجوبًا أو جوزًا، بالإضافة إلى العقوبة الأصلية، فلا يحكم بها بمفردها [34]، ومن الأمثلة على العقوبات التكميلية عقوبة المصادرة [35]، وهي تُعد إحدى العقوبات المالية التي تتخذ من الذمة المالية في حق المحكوم عليه محلًا لها، وهي عبارة عن نزع ملكية المال من صاحبه جبراً عنه، وإضافته إلى ملكية الدولة دون مقابل، وتُعرف المصادرة في اصطلاح الفقه القانوني بأنها:" إجراء القصد منه تمليك الدولة بموجب حكم قضائي كل أموال المحكوم عليه أو بعضها، أو تمليكها أصلًا، أو المضرور استثناءً بموجب ذلك الحكم أموالًا مضبوطة ذات صلة بجريمة، قهراً عن صاحبها، وبغير مقابل"[36].

ومن المُلاحظ في هذا الصدد أن المشرع الاتحادي لدولة الإمارات العربية قد نص على عقوبة المصادرة، فأجاز في غير الأحوال التي يوجب فيها القانون الحكم بالمصادرة، حيث أجاز المشرع الإماراتي للمحكمة عند الحكم بالإدانة، أن تقضي بمصادرة الأشياء والأموال المضبوطة التي استعملت في الجريمة، أو كان من شأنها أن تستعمل فيها، أو كانت محلًا لها، أو التي تحصلت منها، وذلك كله دون الإخلال بحقوق غير حسن النية[37].

وبالإضافة إلى ذلك نصت المادة 56 من قانون مكافحة الشائعات والجرائم الإلكترونية على أنه: "مع عدم الإخلال بحقوق الغير حسن النية، وفي حال الإدانة يحكم بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا المرسوم بقانون أو الأموال المتحصلة منها، وبحذف المعلومات أو البيانات"، ولعل من

(33) د. هدى قشقوش، شرح قانون العقوبات–القسم العام، دار النهضة العربية، القاهرة، 2010، ص384، 385.

(34) د. أحمد شوقي عمر أبو خطوة، المبادئ العامة في قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، 2013م، ص565.

(35) د. هدى قشقوش، المرجع السابق، ذات الموضع.

(36) د. أحمد شوقي عمر أبو خطوة، المرجع السابق، ص571

(37) المادة 83 من قانون الجرائم والعقوبات الإماراتي رقم 31 لسنة 2021م.

مصادرة جميع الأموال المتحصلة من مثل هذه الجريمة في أنها تتناسب جزئياً مع الباعث من الجريمة الذي يكون في الغالب مالياً[38].

ومن ناحية أخرى استبعدت المادة 56 من قانون مكافحة الشائعات والجرائم الإلكترونية رقم (34) لسنة 2021م المصادرة الخاصة للغير حسن النية، كما استبعدته كذلك نص المادة (83) من قانون الجرائم والعقوبات رقم 31 لسنة 2021م، والمقصود بالغير حسن النية: هو كل من كان غير مساهم بالجريمة أو عالماً بارتكابها، أي كل من لا يعد فاعلًا أو شريكًا فيها، وحسن نيته تعني ألا يتوافر لديه قصد أو خطأ بالنسبة إلى ارتكاب الجريمة؛ لذلك لا يستحق عقوبته عن شيء لا يعلمه[39].

(38) د. رامي متولي القاضي، الحماية الجنائية للمرأة من الاتجار بها في ضوء أحكام القانون رقم 64 لسنة 2010، المؤتمر الدولي السنوي الثامن عشر لكلية الحقوق جامعة المنصورة، تحت عنوان "المرأة... والقانون" في الفترة من 15-16 أبريل 2018م، ص44.

(39) أسماء علي سالم راشد الشامسي، جرائم الاعتداء على حرمة الحياة الخاصة للأشخاص في ظل المرسوم بقانون رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات "دراسة مقارنة"، رسالة ماجستير، كلية القانون، جامعة الإمارات العربية المتحدة، دولة الإمارات العربية المتحدة، 2018م، ص97.

المطلب الثاني

التدابير والإجراءات التحفظية

يُقصد بالتدابير الجنائية أو الاحترازية مجموعة من الإجراءات القانونية التي تؤخذ لمواجهة خطورة إجرامية كامنة في شخص مرتكب جريمة، لمنعه من ارتكاب جرائم في المستقبل، ومفاد هذا التعريف بأن التدابير تقتضيها مصلحة المجتمع في مكافحة الإجرام، لذلك هي تثبت على من ثبت أنه مصـــدر خطر على المجتمع، كما تهدف إلى حماية الجاني وتهذيبه، وإ صلاحه[40]، وتتنوع التدابير والإجراءات التحفظية الواردة في قانون مكافحة الـ شائعات والجرائم الإلكترونية رقم (34) لـسنة 2021م إلى تدابير وإجراءات تحفظية يمكن اتخاذها بـشأن المواقع الإلكترونية التي اُستخدمت في ارتكاب الجريمة أو كانت مســرحًا لها، وقد تكون تلك التدابير في مواجهة مرتكبي تلك الجرائم، وهذا ما نوضـــحه من خلال بيان ما يلي ذلك شرحًا وتفصيلًا:

أولًا: التدابير الجزائية بشأن المواقع الإلكترونية:

من بين التدابير والإجراءات التحفظية التي نص عليها المـ شرع الإماراتي بـ شأن المواقع الإلكترونية تدبير حجب الموقع الإلكتروني، فقد قرر المشرع الإماراتي بمقتضى المرسوم بقانون اتحادي رقم (34) لسنة 2021م أنه يجوز للمحكمة عند الحكم بالإدانة في أي جريمة من الجرائم المنصوص عليها بهذا المرسوم بقانون أن تقضي بحجب الموقع المخالف حجبًا كليًا أو جزئيًا للمدة التي تقررها المحكمة[41].

كما أجاز المشـــرع الإماراتي كذلك للنائب العام متى قامت أدلة على قيام موقع إلكتروني يُبث من داخل الدولة أو خارجها، بو ضع أي عبارات أو أرقام أو صور أو أفلام أو أي مواد دعائية، أو ما في حكمها بما يُعد جريمة من الجرائم المنصـــوص عليها في المادة (71) من هذا المرســـوم بقانون، أو يشـــكل تهديدًا للأمن الوطني أو يعرض أمن الدولة أو اقتصـــادها الوطني للخطر، أن يأمر بحجب الموقع أو المواقع محل البث، كلما أمكن تحقيق ذلك فنيًا أو إصـــدار أي من الأوامر المنصوص عليها بهذا المرسوم بقانون[42].

والجدير بالذكر أن المشـــرع الإماراتي قد حدد الجرائم الماســـة بأمن الدولة بمقتضـــى هذا القانون بأنها: الجرائم الواردة في المواد (3)، (5)، (7)، (11) البند 3، (12) البند (3)، (13)، (19)، (20)، (21)، (22)، (23)، (24)، (25)، (26)، (27)، (28)، (47) الفقرة الثانية، (52)، (53)، (55)، من هذا المر سوم بقانون من الجرائم الما سة بأمن الدولة. كما تعتبر من الجرائم الما سة بأمن الدولة، أي جريمة منصوص عليها في هذا المر سوم بقانون إذا ارتكبت لحساب

(40) د. محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص وفقًا لأحدث التعديلات التشريعية، الطبعة الخامسة، طبعة نادي القضاة، 2018م، ص984.

(41) المادة 59 من قانون مكافحة الشائعات والجرائم الإلكترونية رقم (34) لسنة 2021م.

(42) المادة 66 من قانون مكافحة الشائعات والجرائم الإلكترونية رقم (34) لسنة 2021م.

أو لمصلحة دولة أجنبية أو أي جماعة إرهابية أو عصابة أو تنظيم أو منظمة أو هيئة غير مشروعة[43]. كما قرر المشرع الإماراتي بمقتضى المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية الإماراتي أنه يجوز للمحكمة عند الحكم بالإدانة في أي جريمة من الجرائم المنصوص عليها بهذا المرسوم بقانون إغلاق الموقع المخالف إغلاقًا كليًا أو جزئيًا متى أمكن ذلك فنيًا"[44].

ويُلاحظ أن اصطلاحي الحجب والإزالة متمايزين، وليسا مترادفين، فلكل منهما مفهومه الخاص، وإن كان كلاهما يشترك في أنهما عبارة عن إجراءات فنية تهدف إلى تقييد الوصول إلى الموقع الإلكتروني أو إلى المعلومات أو المواد المستضافة عليه، وما يمايز بينهما أن حجب المواقع الإلكترونية هو إجراء يستهدف منع عرض محتوى معين من على شبكة الإنترنت، ويقوم به مزود خدمة الإنترنت– مقدم الخدمة، أما إزالة المحتوى فهو إجراء لإزالة أو حذف محتوى الموقع أو صفحة أو صفحات منه، وعادة ما يُوجه طلب إزالة المحتوى إلى مشغلي مواقع الإنترنت– مستضيفي محتوى المواقع، وهو ما يقود إلى القول بأن الحجب يشمل الموقع بجميع صفحاته، في حين أن الإزالة تستهدف محتوى أو صفحة خاصة من صفحات الموقع، ولا تشمل الموقع بأكمله[45].

ويُلاحظ كذلك أن المشرع الإماراتي قد أجاز للمحكمة عند الحكم بالإدانة في أي جريمة من الجرائم المنصوص عليها بهذا المرسوم بقانون أن تقضي بإغلاق الموقع المخالف إغلاقًا كليًا أو جزئيًا متى أمكن ذلك فنيًا، كما أجاز حجب الموقع المخالف حجبًا كليًا أو جزئيًا للمدة التي تقررها المحكمة، وبالتالي يؤكد المشرع بهذا التوجه على وجود فارق بين حجب المواقع الإلكترونية، وإلغاؤها.

ثانيا: التدابير الجزائية بشأن مرتكبي جريمة الاختراق الإلكتروني:

من بين التدابير الجزائية بشأن مرتكبي جريمة الاختراق الإلكتروني إجراء الأمر بوضع المحكوم عليه تحت الإشراف أو المراقبة الإلكترونية أو حرمانه من استخدام أي شبكة معلوماتية، أو نظام المعلومات الإلكتروني، أو أي وسيلة تقنية معلومات أخرى، أو وضعه في مأوى علاجي أو مركز تأهيل للمدة التي تراها المحكمة مناسبة[46].

وما تجب الإشارة إليه أن المشرع الإماراتي كان ينص بمقتضى المادة 42 من القانون الاتحادي رقم 5 لسنة 2012م في شأن مكافحة جرائم تقنية المعلومات المعدلة بالمرسوم بقانون اتحادي رقم 2 لسنة 2018م على الحكم بإبعاد الأجنبي الذي يحكم عليه بعقوبة الجناية في أي من الجرائم المنصوص عليها في هذه القوانين، غير إنه بصدور المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية الحالي –الذي ألغى القانون آنف الذكر– لم يقرر هذا الحكم، ولم ينص على إجراء طرد أو بإبعاد كل أجنبي غير مرغوب فيه الذي يُشكل ووجوده خطراً

(43) المادة 71 من قانون مكافحة الشائعات والجرائم الإلكترونية رقم (34) لسنة 2021م.
(44) المادة 2/59 قانون مكافحة الشائعات والجرائم الإلكترونية رقم (34) لسنة 2021م.
(45) د. عمر أبو الفتوح عبد العظيم الحمامي، حجب المواقع الإلكترونية: دراسة جنائية مقارنة، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنوفية، العدد 50، أكتوبر 2019م، ص405 وما بعدها.
(46) المادة 1/59من قانون مكافحة الشائعات والجرائم الإلكترونية رقم (34) لسنة 2021م.

على النظام العام أو الأمن، أو الذي قام بأنشطة تتعارض مع المصالح العليا للبلاد أو التي من شأنها المساس بالسلم الاجتماعي أو الآداب العامة[47]، ومع ذلك نجد المشرع قد نص على هذا الإجراء بمقتضى نص المادة 126 من قانون الجرائم والعقوبات[48].

وفي هذا الصدد يُفرق البعض من الفقه بين اصطلاحي الإبعاد والطرد، **فالاصطلاح الأول** هو إجراء إداري تصدره سلطات الدولة في حق الأجنبي المقيم على إقليمها لكي يغادرها خلال مدة معينة، وإلا تعرض للجزء الجنائي، والإخراج بالقوة، بينما **الاصطلاح الثاني** إجراء شرطي بحت يتم تحت إشراف الشرطة، ويتخذ دائماً شكل التدبير الأمني الحال والتقديري، ويُعد الطرد إجراءاً أمنياً للحفاظ على الأمن العام، ويتمثل الهدف من الطرد في حماية المصلحة العليا للبلاد[49].

ويرى الباحث أنه سواء أكان الاصطلاح هو الطرد أم الإبعاد فهو حق وواجب للدولة تلجأ إليه في حالة مخالفة الأجنبي للأحكام الواردة بقانون مكافحة الشائعات والجرائم الإلكترونية الإماراتي، لا سيما وأن يكون قد ارتكب إحدى الجرائم الواقعة على الأنظمة المعلوماتية الخاصة بالدولة، حيث إن وجوده يُشكل خطراً على النظام العام أو الأمن، خاصة وأن تلك الأنشطة تتعارض مع المصالح العليا للبلاد أو التي من شأنها المساس بالسلم الاجتماعي.

وفي نهاية هذا البحث نجد أن موضوع جريمة الاختراق الإلكتروني هو موضوع شائك ومرتبط بمجال يعرف تطوراً سريعاً يمس كرامة الأشخاص، وينعكس أيضاً بلا شك سلباً على حقوقهم، وينتقل من تهديد كيان الأمر في بعض الحالات إلى المعاملات الاقتصادية لكبريات الدول، فالجرائم المستحدثة عموماً والجرائم محل الدراسة على وجه الخصوص أصبحت تكلف الدول خسائر مادية مرتفعة.

ولا شك أن المصلحة الجديرة بالحماية فيما يتعلق بجرائم الاختراق الإلكتروني لا سيما اختراق الأنظمة المعلوماتية الخاصة بمؤسسات الدولة والتي من أجلها أسبغ المشرع صفة التجريم والعقاب على كل سلوك ينطوي على تعريض مصالح الدولة وأمنها ونظامها المعلوماتي للخطر–تتمثل في حماية النظام السياسي للدولة، والحفاظ على وجودها وبقائها، وأمنها، وسلطاتها، وكذلك الحفاظ على الكيان الاجتماعي والاقتصادي للدولة.

ويعد الإطار القانوني لتجريم الاختراق المعلوماتي في دولة الإمارات خطوة أولى مهمة في حماية المجتمع والبنية التحتية الرقمية من تهديد القرصنة، حيث يوفر المشرع الإماراتي من خلال قانون مكافحة الشائعات والجرائم الإلكترونية رقم (34) لسنة 2021م، بالإضافة إلى الأحكام والنصوص القانونية ذات الصلة أساساً قانونياً قوياً لإنفاذ القانون ضد مرتكبي جرائم الاختراق، ومع ذلك، لا يزال تطبيق القانون السيبراني في دولة الإمارات والعالم العربي بوجه عام يواجه العديد من التحديات التي يتعين التغلب عليها.

(47) المادة 73 من قانون مكافحة الشائعات والجرائم الإلكترونية رقم (34) لسنة 2021م.
(48) المادة 126 من قانون الجرائم والعقوبات رقم 131 لسنة 2021م.
(49) د. عزوز ابتسام، إبعاد وطرد الأجانب كآلية للحد من الهجرة غير الشرعية، بحث منشور في مجلة الحقوق والحريات، المجلد التاسع، العدد الثاني، الجزائر، 2021م، ص205.

إذ يُشكل الاختراق المتزايد للأنظمة المعلوماتية أو المواقع الإلكترونية تعقيداً كبيراً لمؤسسات الدولة، الأمر الذي يتطلب معه تعاوناً وثيقًا بين مختلف المؤسسات الحكومية والخاصة، بالإضافة إلى التعاون الدولي للتغلب على عمليات الاختراق التي تتم عبر الحدود. كما يتطلب ذلك أيضًا التنفيذ الفعال للقانون السيبراني من خلال إجراء تغييرات وتحديثات مستمرة في الإطار القانوني، وزيادة الوعي العام بالأمن السيبراني، ولن تتمكن الدول من مواجهة ذلك إلا من خلال اتباع منهج شامل ومستدام فعال في التعامل مع تهديد القرصنة في عالم رقمي دائم التغير(50).

كما أن متطلبات العدالة الجزائية تفرض على الأجهزة الحكومية بشكل عام، والأجهزة المسؤولة عن تتبع الجرائم وضبطها والتحقيق فيها بشكل خاص أن تتحمل مسؤولياتها نحو اكتشاف المجرمين وضبطهم ومحاكمتهم، ومثل هذا الأمر يقتضي توفير الإمكانات التقنية اللازمة، سواء في عملية التحقيق أو الكشف والاستدلال عن الجرائم، لاسيما بعد أن تطورت ليس فقط أساليب الكشف عن الجرائم، وإنما أيضاً تطور أساليب ارتكاب الجرائم، وظهور أنماط جديدة من الجرائم ما كانت التشريعات لتعرفها من قبل، إلا بعد أن ظهرت وسائل متطورة تمكن المجرمين ارتكاب جرائمهم بأساليب وطرق غير معهودةً.

وما تجب الإشارة إليه أن طرق وآليات الحماية من جرائم الاختراق الإلكتروني لا سيما جريمة اختراق الأنظمة المعلوماتية الخاصة بمؤسسات الدولة مختلفة ومتعددة حسب طبيعة وموارد كل دولة على حدة، لكن يبقى الهدف الرئيس هو ردع المجرم المعلوماتي لتغيير سلوكه، سواء من خلال اللجوء إلى الأمن الرقمي، والذي يُعتبر الحل الأنجح نظراً لما يمتاز به من خصائص تركز على ماهية المعلومات والبيانات وسلامتها وسريتها، أو من خلال كافة الطرق الوقائية والعلاجية التي تنبني على تكوين الشباب والمجتمعات في الوسط المعلوماتي وإحساسهم بمخاطره، وهي مسؤولية تقع على عاتق الدولة في إطار بنائها لمجتمع المعلومات، ثم في المقابل لكافة القوانين التي صاغها المشرع.

ويمكن للأجهزة الأمنية تطوير قدراتها من خلال استخدام تقنيات الذكاء الاصطناعي في كشف الجرائم لا سيما المعلوماتية منها، حيث يُستخدم الذكاء الاصطناعي في مجموعة واسعة من المهام الأمنية والكشف عن الجريمة، والوقاية منها(51) باستخدام هذه الأنظمة بإمكانات تحليلية قوية ومجموعة غنية من البيانات المتكاملة المستمدة من تطبيقات نظم المعلومات، وتقوم فكرة هذه الأنظمة على تزويد الأجهزة الأمنية بالوسائل التكنولوجية والذكية بتحقيق أفضل استخدام للأشخاص والمعلومات المتوفرة لمراقبة اتجاهات الجريمة وقياسها والتنبؤ بها(52).

(50) Jay Sadikin Abdul Azis Mandala Putra,"hacking as a challenge for change and the development of cyber law in Indonesia", Jurnal Ilmu Hukum Tambun Bungai 8(2):344-355,December 2023,P.353.

(51) Strom ,Kevin,Research on the Impact of Technology on Policing Strategy in the 21st Century, Final Report, NCJ 251140,Affiliation: National Institute of Justice, May 2016,P.48, on the following website https://content.govdelivery.com/accounts/USDOJOJP/bulletins/1c9d005,Accessed 10/12/2023 at 12.00 Pm.

(52) د. عمار ياسر البابلي، دور أنظمة الذكاء الاصطناعي في التنبؤ بالجريمة، مجلة الفكر الشرطي، القيادة العامة لشرطة الشارقة، مركز بحوث الشرطة، المجلد 28، العدد 110، يوليو، 2019، ص61.

ولا شـــك أن تجهيز وتحفيز البنية النظامية لمواكبة تحديات تقنيات الذكاء الاصـــطناعي أصـــبحت ملحة لما لتلك الأخيرة من تأثير اقتصادي كبير، بحسبان ما سوف يؤدي إليه إدخال إنترنت الأشياء من تبعات على مستوى التوظيف والاستهلاك، مما قد يجلب العديد من المخاطر الاقتصادية بشأن التسريح الجماعي للموظفين ذوي المؤهلات المنخفضة. كما ستفتح هذه التقنيات مجالًا تنافسيًا رهيبًا بين الشركات الصناعية، بحكم ما سوف تسمح به تقنية التسجيل الموزعة أو الكتل المتسلسلة من تخزين ومعالجة للمعلومات بالنسبة لجميع أنواع القطاعات ومواقع الإنترنت، وما ستوفره من توسع في مجموعة متنوعة من الخدمات الإلكترونية، في مجالات اقتصادية واجتماعية عديدة[53].

وبالإضافة إلى ما سبق بيانه تم استخدام التقنيات الذكية التي تعمل بالذكاء الاصطناعي في عملية التحليل الجنائي، والبحث عن الأدلة والسمات الحيوية، كبصمة الوجه والإصبع والعين والصوت، فقد تم استخدام نظام **AFIS** كنظام آلي للتعرف على بصمات الأصابع باستخدام الخوارزميات، حيث يقوم هذا النظام بتخزين البصمات وتصنيفها، والبحث فيها ومعالجتها بسرعة ودقة عالية، كما تم استخدام نظام بصمة العين المعروف باسم **Iris Scan**، بالإضافة إلى ما يُعرف ببصمة المخ للتعرف على الجناة في الجرائم التي يتم ارتكابها[54].

وما تجب الإشـــارة إليه في هذا المقام أنه إذا كان للذكاء الاصـــطناعي أهمية كبرى في آليات اكتشـــاف وردع الجريمة وهوية مرتكبيها، وتخزين البيانات والأدلة التي يتم الحصول عليها من مسرح الجريمة خلال فترة زمنية محددة[55]، وذلك باستخدام الكاميرات الذكية لرصد مرتكبي الجرائم والتعرف عليهم وتحليل البيانات المسجلة للتعرف على سمات معينة، لتتبع والقبض على المجرمين أو الهاربين من العدالة. غير إنه يُخشى من إساءة استخدام واستغلال هذه البيانات الشخصية في التنميط الإلكتروني. بالإضافة إلى خاصية توقع ارتكاب الجرائم في المستقبل للوقاية من الجرائم باستخدام الذكاء الاصطناعي، وبالتالي الوقاية من الخطورة الإجرامية واحتمال ارتكاب جريمة في المستقبل[56].

53() د. أحمد لطفي السيد، انعكاسات تقنية الذكاء الاصطناعي على نظرية المسؤولية الجنائية: دراسة تأصيلية مقارنة، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنصورة، العدد 80، 2022، ص250.

(54)Rughani, Parag,Artificial Intelligence Based Digital Forensics Framework, in:Gujarat Forensic Sciences University Gandhinagar,International Journal of Advanced Research in Computer Science, Vol.8, No.8, 2017,P.11.

(55)Karimi, Abbas and Others,Cybercrime Detection Using Semi-Supervised Neural Network, in:Computer Science Journal of Moldova" (CSJM), Vol.29, No.2(86),2021, P. 156.

56() د. ياسر محمد اللمعي، المسؤولية الجنائية عن أعمال الذكاء الاصطناعي ما بين الواقع والمأمول: دراسة تحليلية استشرافية، مؤتمر: الجوانب القانونية والاقتصادية للذكاء الاصطناعي وتكنولوجيا المعلومات، كلية الحقوق، جامعة المنصورة، مصر، الفترة من 23-24 مايو 2021، ص8.

الخاتمة:

فر ضت دولة الإمارات العربية المتحدة قوانين ت ساعد على حماية المواطن بالدرجة الأولى، ويظهر ذلك جليًا من الن صوص الت شريعية الواردة في قانون الجرائم والعقوبات الإماراتي رقم 31 ل سنة 2021، وكذلك قانون مكافحة الـ شائعات والجرائم الإلكترونية رقم (34) لسنة 2021، وذلك من خلال النصوص التشريعية بشأن حماية البيانات والمعلومات الخاصة وكذلك التي تؤثر على أمن الدولة الداخلي والخارجي المحفوظة في النظام المعلوماتي والشبكات والمواقع الإلكترونية.

ولم يكتف المشـــرع الإماراتي بما قرره من حماية خاصـــة للأفراد، بل جرم كذلك الاختراق الواقع على الأنظمة المعلوماتية الخا صة بمؤ سـ سات الدولة، نظرًا لخطورة وأهمية المعلومات التي تحتوي على أ سرار الدولة، كما قد اعتبرت غالبية الت شريعات العقابية الحديثة أن هذه الجريمة من الجرائم التي تمس أمن الدولة، خا صة إذا تطورت هذه الجريمة من الاطلاع على البيانات والمعلومات إلى المتاجرة بها.

أولًا: **نتائج البحث**:

1. لقد سعى المـشرع الإماراتي إلى تجريم الاختراق الإلكتروني، وذلك من خلال ن صه على تجريم اختراق أي موقع إلكتروني أو نظام معلومات إلكتروني أو شـــبكة معلومات أو وســـيلة تقنية معلومات، كما جرم ما يترتب على الاختراق من إحداث أ ضرار أو تدمير أو إيقاف عن العمل أو تعطيل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو و سيلة تقنية المعلومات، أو إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو ن سخ أو ن شر أو إعادة ن شر أو الحـ صول على أي بيانات أو معلومات أو خـ سارة سريتها، ولم يفت عليه كذلك تجريم الاختراق إذا كان بغرض الحصول على البيانات أو المعلومات لتحقيق غرض غير مشروع.
2. خصص المشرع الإماراتي ن صًا مستقلًا لتجريم اختراق الأنظمة المعلوماتية الخاصة بمؤ سسات الدولة، وذلك من أجل توفير نوع من الحماية اللازمة لجميع و سائل وأنظمة التقنية المعلوماتية الخا صة بالدولة من شبكات سلكية ولا سلكية وأجهزة ومعدات وبيانات وبرامج، وكذلك المعلومات المخزنة أو المعالجة أو المولدة أو المخلقة على أي نظام معلوماتي خاص بالدولة، وما في حكمه، سواء كان الاختراق لموقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية معلومات عائدة لمؤسسات الدولة.
3. عاقب المشرع الإماراتي على جريمة الاختراق الإلكتروني بعقوبات أصلية وأخرى تكميلية، حيث تتراوح العقوبات الأصـــلية المقررة لجريمة الاختراق الإلكتروني ما بين عقوبتي الحبس والغرامة، كما فرض المشـــرع الإماراتي عقوبة المـ صادرة كعقوبة تكميلية يجوز توقيعها على الجاني في حالة الإدانة مع عدم الإخلال بحقوق الغير حـ سن النية، مع بحذف المعلومات أو البيانات.
4. بالإضـــافة إلى ما قرره المشـــرع الإماراتي من عقوبات أصـــلية وأخرى تكميلية لمرتكبي جريمة الاختراق الإلكتروني؛ فقد قرر المشـــرع مجموعة من التدابير الجزائية والتي تتنوع إلى تدابير وإجراءات تحفظية يمكن

اتخاذها بشأن المواقع الإلكترونية التي استُخدمت في ارتكاب الجريمة أو كانت مسرحًا لها كحجب الموقع المخالف حجبًا كليًا أو جزئيًا للمدة التي تقررها المحكمة، وكذلك إغلاق الموقع المخالف إغلاقًا كليًا أو جزئيًا متى أمكن ذلك فنيًا، وقد تكون تلك التدابير في مواجهة مرتكبي تلك الجرائم كالأمر بوضع المحكوم عليه تحت الإشراف أو المراقبة الإلكترونية أو حرمانه من استخدام أي شبكة معلوماتية، أو نظام المعلومات الإلكتروني، أو أي وسيلة تقنية معلومات أخرى، أو وضعه في مأوى علاجي أو مركز تأهيل للمدة التي تراها المحكمة مناسبة، وكذلك إبعاد الأجنبي.

ثانيًا: توصيات البحث:

1. نقترح أن ينص المشرع الإماراتي على الطرد والإبعاد للأجنبي في المرسوم بقانون اتحادي رقم (34) لسنة 2021م في شأن مكافحة الشائعات والجرائم الإلكترونية كما نصت عليه بعض التشريعات العربية كالمشرع العُماني، وذلك في حالة إدانته في جريمة الاختراق الإلكتروني لا سيما إذا كان الاختراق واقعًا على الأنظمة المعلوماتية الخاصة بمؤسسات الدولة باعتبار أن هذا الإجراء حق وواجب للدولة تلجأ إليه في حالة مخالفة الأجنبي للأحكام الواردة مكافحة الشائعات والجرائم الإلكترونية، لا سيما وأن وجوده بعد ارتكابه لهذه الجريمة يُشكل خطرًا على النظام العام أو الأمن، خاصة وأن تلك الأنشطة تتعارض مع المصالح العليا للبلاد أو التي من شأنها المساس بالسلم الاجتماعي.

2. يقترح الباحث على المشرع الإماراتي أن ينظم مسألة التدابير والإجراءات التحفظية كما نظمها المشرع المصري، وذلك بتبني أمر المنع من السفر وترقب الوصول ضمن القانون الاتحادي رقم 34 لسنة 2021م في شأن مكافحة الشائعات والجرائم الإلكترونية.

3. يقترح الباحث إضافة مادة في المرسوم بقانون اتحادي رقم (34) لسنة 2021م في شأن مكافحة الشائعات والجرائم الإلكترونية الإماراتي تلزم الشركات المزودة لخدمات الاتصالات بالاحتفاظ بـ سجلات الدخول والخروج (Log Files) لمدة مناسبة، وذلك لسهولة تتبع مجرمي الإنترنت.

4. نوصي المشرع الإماراتي على وجه الخصوص والتشريعات العربية على وجه العموم بتجريم تصنيع أو استيراد أو الإعلان عن الأجهزة التي تستخدم في التجسس والاختراق للأنظمة المعلوماتية أو المواقع الإلكترونية والتي من شأنها الاعتداء على الحياة الخاصة بكافة عناصرها، سواء بالتصوير أو النقل أو الاعتراض أو تسجيل المحادثات والاتصالات، وذلك على هدى ما تبناه المشرع الفرنسي من أجل فرض مزيد من الحماية الجزائية للحق في الخصوصية.

5. من أجل كشـــف جريمة الاختراق الإلكتروني، والاهتداء إلى مرتكبها وملاحقته قضـــائياً، فإن ذلك يتطلب استراتيجيات تحقيق وتدريب مهارات خاصة، تسمح باستيعاب ومواجهة التقنيات المعلوماتية المتطورة، من حيث الأنظمة والبرامج، وطبيعة الجريمة لاكتشاف أساليب التلاعب التي تستخدم في ارتكاب هذه الجرائم عادة.

قائمة بأهم المراجع

أولًا: المراجع العامة:

1. د. أحمد شوقي عمر أبو خطوة، المبادئ العامة في قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، 2013م.
2. د. أحمد فتحي سرور، الوسيط في قانون العقوبات، القسم العام، الطبعة السادسة، مطورة ومحدثة، دار النهضة العربية، القاهرة، 2015م.
3. د. غنام محمد غنام، د. تامر محمد صالح، شرح قانون العقوبات: القسم العام، بدون دار نشر، 2022م/2023م.
4. د. محمد محرم محمد ود. خالد محمد المهيري، قانون العقوبات الاتحادي لدولة الإمارات العربية المتحدة فقها وقضاء، الطبعة الثانية، الفتح للطباعة والنشر، الإسكندرية، 1992م.
5. د. محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص وفقًا لأحدث التعديلات التشريعية، الطبعة الخامسة، طبعة نادي القضاة، 2018م.
6. د. هدى قشقوش، شرح قانون العقوبات–القسم العام، دار النهضة العربية، القاهرة، 2010م.

ثانيا: المراجع المتخصصة:

1. تركي بن عبد الرحمن المويشير، بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته، إصدارات جامعة نايف العربية للعلوم الأمنية مركز البحوث والدراسات، جامعة نايف العربية للعلوم الأمنية، مركز الدراسات والبحوث، الرياض، المملكة العربية السعودية، 2012م.
2. د.عمر الشريف، درجات القصد الجنائي، الطبعة الأولى، دار النهضة العربية، القاهرة، 2002م.

ثالثًا: الرسائل العلمية:

1. أسماء علي سالم راشد الشامسي، جرائم الاعتداء على حرمة الحياة الخاصة للأشخاص في ظل المرسوم بقانون رقم 5 لسنة 2012م بشأن مكافحة جرائم تقنية المعلومات:"دراسة مقارنة"، رسالة ماجستير، كلية القانون، جامعة الإمارات العربية المتحدة، دولة الإمارات العربية المتحدة، 2018م.

2. خالد سـليمان عبد الله الحمادي، جريمة الدخول غير المشـروع إلى النظام المعلوماتي في القانون القطري: دراسة مقارنة، رسالة ماجستير، كلية القانون، جامعة قطر، 2019م.
3. منصـور بن صـالح السـلمي، المسـؤولية المدنية لانتهاك الخصـوصـية في نظام مكافحة جرائم المعلوماتية السـعودية، رسـالة ماجسـتير، كلية الدراسـات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، 2010م.
4. نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، رسالة ماجستير، كلية الحقوق، جامعة الإسكندرية، 2006م.

رابعا: المجلات والبحوث:

1. د. رامي متولي القاضـي، المواجهة الجنائية لجرائم تقنية المعلومات في التشـريع المصـري في ضـوء أحكام القانون 175 لسـنة 2018م، مجلة البحوث القانونية والاقتصـادية، كلية الحقوق، جامعة المنصورة، ع 75، مارس2021م.
2. . عبد الإله محمد النوايسـة، جريمة الدخول غير المشـروع في تشـريعات الجرائم الإلكترونية العربية: دراسة مقارنة، المجلة القانونية والقضائية، السنة (10)، العدد (1)، 2016م.
3. د. عزوز ابتسـام، إبعاد وطرد الأجانب كآلية للحد من الهجرة غير الشـرعية، بحث منشـور في مجلة الحقوق والحريات، المجلد التاسع، العدد الثاني، الجزائر، 2021م.
4. د. عمر أبو الفتوح عبد العظيم الحمامي، حجب المواقع الإلكترونية: دراسـة جنائية مقارنة، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنوفية، العدد 50، أكتوبر 2019م.
5. د. لورنس سـعيد أحمد الحوامدة، الجرائم المعلوماتية: أركانها وآلية مكافحتها: دراسـة تحليلية مقارنة، مجلة الميزان للدراسـات الإسـلامية والقانونية، جامعة العلوم الإسـلامية العالمية، عمان، المملكة الأردنية الهاشمية، المجلد الرابع، العدد الأول، يناير 2017م.

خامسا: المؤتمرات:

1. د. رامي متولي القاضـــي، الحماية الجنائية للمرأة من الاتجار بها في ضـــوء أحكام القانون رقم 64 لسـنة 2010 ، المؤتمر الدولي السـنوي الثامن عشـر لكلية الحقوق جامعة المنصـورة، تحت عنوان "المرأة... والقانون" في الفترة من 15-16 أبريل 2018م.

سادسا: المراجع باللغة الإنجليزية:

1. Baha Abu-Shaqra,"Technoethics and Organizing: Exploring Ethical Hacking within a Canadian University",A thesis submitted to the Faculty of Graduate and Postdoctoral Studies in partial fulfillment of the requirements for the MA degree in Communication,Faculty of Arts University of Ottawa,Canada 2015.
2. Bainbridge. D: Introduction to computer law, fourth edition, London, 2000.
3. Jay Sadikin Abdul Azis Mandala Putra,"hacking as a challenge for change and the development of cyber law in Indonesia", Jurnal Ilmu Hukum Tambun Bungai 8(2):344-355,December 2023.
4. Karimi, Abbas and Others,Cybercrime Detection Using Semi-Supervised Neural Network, in:Computer Science Journal of Moldova" (CSJM), Vol.29, No.2(86),2021.
5. Rughani, Parag,Artificial Intelligence Based Digital Forensics Framework, in:Gujarat Forensic Sciences University Gandhinagar,International Journal of Advanced Research in Computer Science, Vol.8, No.8, 2017.
6. Strom ,Kevin,Research on the Impact of Technology on Policing Strategy in the 21st Century, Final Report, NCJ 251140,Affiliation: National Institute of Justice, May 2016,P.48, on the following website:https://content.govdelivery.com/accounts/USDOJOJP/bulletins/1c9d005,Accessed 10/12/2023 at 12.00 Pm.