مجلة العلوم القانونية – كلية القانون – جامعة المرقب (الخمس–ليبيا)
المجلد الحادي عشر– العدد الثاني – (ديسمبر 2023م)

الحماية الجنائية للمواقع الإلكترونية والأنظمة المعلوماتية للدولة" دراسة مقارنة"

CRIMINAL PROTECTION OF WEBSITES AND STATE INFORMATION SYSTEMS

د. هيفاء عبدالعالي فرج
Hayfa Abdulali faraj
كلية القانون/ جامعة طرابلس
أستاذ مساعد بقسم القانون الجنائي
كلية القانون- جامعة طرابلس (طرابلس–ليبيا)
Email- ***Haifa6371@gmail.com***

تاريخ التقديم 03 نوفمبر 2023م	تاريخ القبول 01 ديسمبر 2023م	تاريخ النشر 04 ديسمبر 2023م

الملخص:

يرتكز موضوع البحث حول الحماية الجنائية للمواقع والأنظمة الإلكترونية الخاصة بالدولة، فبالنظر لخطورة هذا الاعتداء وما يرتبه من ضرر، يفترض إعطاء نوعٍ من الخصوصية لهذا الاعتداء من خلال إضفاء حماية جنائية له، تتمثل في إفراد نصوص لتجريمه، وإقرار عقوبة تتناسب مع الجرم المرتكب، فإن كانت البيانات الخاصة بالأشخاص تقتضي حمايتها من خلال تجريم من يعتدي عليها بدخول غير مشروع أو اعتراض أو تجاوز حق الدخول المسموح به، فمن باب أولى البيانات والمعلومات الموجودة على المواقع الإلكترونية والأنظمة الخاصة بالهيئات العامة والجهات التابعة للدولة لمساسها بمصالح أولى بالرعاية، نحو تعطيل الأعمال الحكومية، والمساس بالأمن المعلوماتي الخاص بالأمن الداخلي أو الخارجي بالدولة، وهذا ما كنا نأمله بإقرار المشرع لقانون رقم (5) لسنة 2022 بشأن الجرائم الإلكترونية الليبي، وقد خلصنا من خلال مقارنة قانوننا في بعض المسائل بالقانونين "الأردني والمصري" أن المشرع الليبي لم يولِ أهمية لحماية المواقع والأنظمة المعلوماتية الخاصة بالدولة من خلال إقرار تجريم خاص لفرضية الاعتداء المتمثل في الدخول غير المشروع أو تجاوز الحد المسموح فيه بالدخول، بل لم يشدد حتى عقوبة هذا الاعتداء حال تحققه على البيانات والمعلومات الخاصة بالدولة.

الكلمات المفتاحية: جريمة الدخول غير المشروع – تجاوز حدود الدخول – جريمة الاعتراض غير القانوني– اصطناع المواقع الإلكترونية.

Abstract*:*

The subject of the research is based on the criminal protection of the state's websites and electronic systems. In view of the seriousness of this violation and the harm it causes, it is assumed that a kind of privacy should be given to this attack by giving it criminal protection, which is represented by providing laws and regulations to criminalize such action, and approving a punishment commensurate with the crime committed.

Also, it is worth mentioning that if Personal data requires protection by criminalizing those who attack it by illegal entry, interception, or bypassing the permissible right of access, It is a fortiori that the data and information found on the websites and systems of public bodies and state-affiliated entities are protected because they correlated to the interests of the most concerned, such as disrupting government work, and compromising Information security related to internal or external security in the country, and this is what we were hoping for when the legislator approved Law No. (5) of 2022 regarding Libyan electronic crimes. We concluded, by comparing our law in some matters with the "Jordanian and Egyptian" laws, that the Libyan legislator did not attach importance to protecting public websites and systems and State-specific information by establishing a special criminalization on the ground of assault represented by illegal entry or exceeding the permissible limit of entry. Indeed, the penalty for this assault was not even mentioned once it was committed against the state's data and information.

Keywords*:* The crime of illegal entry - Exceeding entry limits - The crime of illegal interruption - Fabrication of websites.

مقدمة:

إن ما أفرزه التطور التكنولوجي من وسائل حديثة في العديد من المجالات كان له الأثر البارز في تطور المجتمعات في كافة المناحي، هذا التطور الذي استبان لنا بعديد من الإيجابيات والسلبيات، فلا يكاد يخفى على أحدٍ مدى تغير مجريات ارتكاب الجرائم عن ذي قبل؛ إذ أصبحت تمارس بوسائل وطرق متماشية مع التقدم التكنولوجي بظهور الحواسيب الآلية وشبكة المعلومات الدولية، الأمر الذي أنتج وسائل

جديدة وطرق مبتكرة من الصعب اكتشافها، كما أن ما يتم عن طريق هذه البرامج الحديثة يجعلنا أمام حالة عجز عن حصرها في نطاق محدد؛ لتجاوزها حدود الدولة الواحدة، فهي عابرة للحدود[1].

هذا وقد أصدر المشرّع الليبي قانوناً ألا وهو القانون رقم (5) لسنة 2022 بشأن الجرائم الإلكترونية[2]، كمحاولة منه لتجريم الأفعال التي لم يرد تجريمها بقانون العقوبات والقوانين المكملة له، إعمالاً لمبدأ "لا جريمة ولا عقوبة إلا بنص"، وجاءت المادة الأولى من القانون سالف الذكر في فقرتها رقم (1) بتعريفٍ للجريمة الإلكترونية، على النحو التالي: "كل فعل يُرتكب من خلال استخدام أنظمة الحاسب الآلي، أو شبكة المعلومات الدولية، أو غير ذلك من وسائل تقنية المعلومات، بالمخالفة لأحكام هذا القانون"، وقد أدرجت بهذا القانون العديد من صور الجرائم، كالتحريض على الدعارة، والتعدي على حقوق التأليف، وإنتاج المواد الإباحية وتزويدها، ولعل ما يعنينا بهذا الخصوص الاعتداء على المواقع والأنظمة الإلكترونية للدولة، حيث نصت المادة (46) من مشروع الدستور الليبي 2017 التي جاءت تحت عنوان "الشفافية والحق في المعلومات" على أنه: "تضع الدولة التدابير اللازمة للشفافية، وتضمن حرية تلقي ونقل وتبادل المعلومات، والاطلاع عليها، وتعدد مصادرها، بما لا يمس الأسرار العسكرية، وأسرار الأمن العام، ولوازم إدارة العدالة وحرمة الحياة الخاصة، وما اتفق مع دولة أخرى على اعتباره سرّياً، مع حق الحفاظ على سرية المصدر"، فكما نعلم المعلومات والبيانات التي تخص المؤسسات العامة للدولة كانت مخزنة في مكاتب خاصة وفقاً لأرشفة محددة، وبمقتضى التطور التكنولوجي الحاصل أصبحت كافة الجهات العامة والخاصة تقيد كل معلوماتها وبياناتها في أنظمة معلوماتية خاصة بها وعبر المواقع الإلكترونية، وكما كانت هذه المعلومات بحاجة للحماية عندما كانت ورقية[3] ؛ فهي بحاجة لذات الحماية وربما أكثر؛ لسهولة اختراقها وانتهاك ما يوجد عليها من بيانات إلكترونية تخص الدولة ومؤسساتها العامة.

أهمية البحث:

تكمن أهمية بحثنا في حداثته، فالمشرّع الليبي لم يقر قانوناً للجرائم الإلكترونية إلا من وقت قريب، وقد جاء هذا البحث محاولة لبيان معالم السياسة التي اتبعها المشرّع الليبي في حمايته لمواقع وأنظمة الدولة من الاعتداء عليها، فمن خلال مطالعة نصوص قانون الجرائم الإلكترونية، وكذلك النصوص ذات العلاقة بهذا الموضوع – قانون رقم (4) لسنة 1990 بشأن النظام الوطني للمعلومات والتوثيق، وقانون

1- موسى مسعود إرحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، بحث مقدم إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا – طرابلس،2009،ص 7.

2- قانون رقم 5 لسنة 2022 بشأن مكافحة الجرائم الإلكترونية، منشور بالجريدة الرسمية، ع 1، 2023/1/16.

3 – إسلام مصطفى جمعة مصطفى، جريمة اختراق الأمن السيبراني وحماية استخدام البيانات والمعلومات في القانون المصري، المجلة القانونية" جامعة القاهرة"، 2022،ص 721.

رقم (22) لسنة 2010 بشأن الاتصالات – يمكن لنا أن نتبين مدى الحماية الجنائية التي منحها المشرّع لأنظمة ومواقع الدولة، وذلك بالنظر لخصوصية وخطورة هذا الاعتداء، وما اعترى تلك السياسة من مواطن ضعف، لعلنا نساعد المشرّع في انتقاء سياسة أفضل مما هي عليه.

إشكالية البحث:

حسبما جرى عليه القانون في العديد من الدول هو تشديد عقوبة الجريمة طالما مست مصلحة مباشرة بالدولة، ووفقاً لذلك فإن إصدار قانون الجرائم الإلكترونية يطرح لدينا تساؤلاً مفاده، هل اتبع المشرّع ذات السياسية من خلال إعطاء نوع من الخصوصية في تجريم الاعتداء على مواقع الدولة وأنظمتها الخاصة بها، سواءً بالعبث فيها أو إتلافها أو إفشائها للغير، وذلك من خلال تشديد العقوبة الواجب إيقاعها بحق الشخص الطبيعي؟ أم أنه ساوى بين هذا الاعتداء والاعتداءات الأخرى التي تقع على آحاد الأفراد؟ إلى أي حد تمكن المشرّع من إضفاء الحماية الجنائية اللازمة للمؤسسات والشركات العامة التابعة للدولة حال الاعتداء على أنظمتها وشبكاتها الإلكترونية؟

سنبحث عن إجابة هذه التساؤلات لدى المشرّع الليبي والمصري وكذا الأردني، وذلك من خلال عقد مقارنة بين السياسيات المتبعة، والتي من خلالها نتمكن من معرفة أيهم أوفق تشريعياً، وما الخلل الذي اعترى كلاً منهم.

منهج البحث:

تقتضي دراسة موضوع البحث تناول نصوص قانون الجرائم الإلكترونية، وكذا القوانين الأخرى التي احتوت نصوصاً تتعلق بذات المسألة –الاعتداء على المواقع والأنظمة الإلكترونية للدولة– بالتحليل، كما سأقارن من خلال تلك النصوص سياسة المشرّع التي انتقاها لحماية مواقع وأنظمة الدولة الإلكترونية، مع ما ورد في بعض القوانين الجنائية، كالقانون الأردني والقانون المصري؛ لذا سيكون المنهج التحليلي والمقارن هو المنهج المتبع في هذا البحث.

خطة البحث:

المطلب الأول:– أوجه الحماية الجنائية للأنظمة والمواقع الإلكترونية للدولة.

المطلب الثاني:– تقييم الحماية الجنائية المقررة للأنظمة والمواقع الإلكترونية للدولة.

المطلب الأول

أوجه الحماية الجنائية المقررة للأنظمة والمواقع الإلكترونية للدولة

قد يتم اختراق بعض الأنظمة والبيانات المعلوماتية من قبل أشخاص غير مصرّح لهم بدخول حسابات بعض الشخصيات أو مواقعهم الإلكترونية، وقد يصرح لهم بالدخول إلا أنهم يتجاوزون الحد

المصرح لهم به، كما قد يتم التنصت على الاتصالات التي تجرى عبر شبكة المعلومات الدولية، ولعل الصورة الأشد خطورة إذا ما وقعت هذه الأفعال على البيانات الحكومية[1]، والمعلومات أو المواقع الخاصة بالدولة، فللمواقع الخاصة بالدولة أهميتها؛ إذ تمثل سيادتها على الفضاء الإلكتروني؛ لذا فإن العدوان عليها يمس بشكل أو بآخر هيبة الدولة[2]، وبناءً على ذلك استلزم الأمر ضرورة تجريم أي اعتداء يمس بالأنظمة الإلكترونية للدولة.

أولاً – الدخول غير المشروع أو تجاوز حدوده:

يتحقق الدخول غير المشروع بالوصول إلى بيانات ومعلومات مخزنة داخل الحاسب الآلي دون رضا المسؤول عنها[3]، ولعل هذه الجريمة تعد مدخل الجرائم الإلكترونية؛ فأغلب هذه الجرائم تقتضي اقتراف فعل الدخول غير المشروع أولاً[4].

وباستقراء نصوص قانون الجرائم الإلكترونية الليبي نجد أن المشرّع قد جرّم الدخول غير المشروع في مادته (11) بأنه: "يعد الدخول لأجهزة وأنظمة الحاسب الآلي أو إلى نظام معلوماتي أو شبكة معلوماتية أو موقع إلكتروني غير مشروع إذا تم الاختراق بشكل متعمد لوسائل وإجراءات الحماية لها بشكل كلي أو جزئي دون تصريح ...".

وبمطالعتنا لهذا النص، نلحظ أن المشرّع الليبي قد توسع في محل الجريمة الذي من الممكن أن يكون موقعاً إلكترونياً أو نظاماً معلوماتياً أو شبكة معلوماتية، إلا أنه لم يضع تعريفات لهذه المصطلحات بالمادة الأولى من القانون المذكور أعلاه، بخلاف المشرّع المصري وكذا الأردني، فقد أُدرج في

1 – لم يرد بقانون الجرائم الإلكترونية الليبي وكذا قانون الجرائم الإلكترونية الأردني أي تعريف للبيانات التي تخص الدولة، بعكس القانون المصري فقد جاءت المادة (1) من قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 بتعريفٍ للبيانات الحكومية بأنها: "بيانات متعلقة بالدولة أو أحد سلطاتها، وأجهزتها أو وحداتها، أو الهيئات العامة، أو الهيئات المستقلة والأجهزة الرقابية، وغيرها من الأشخاص الاعتبارية العامة، وما في حكمها، والمتاحة على الشبكة المعلوماتية أو على أي نظام معلوماتي أو على حاسب أو ما في حكمها".

2– أحمد الضبع، إشكاليات مواجهة الإرهاب بين النظرية والتطبيق، الهيئة المصرية العامة للكتاب،2019، ص 95.

3 – أسامة بن غانم العبيدي، جريمة الدخول غير المشروع إلى النظام المعلوماتي "دراسة قانونية في ضوء القوانين المقارنة"، مجلة دراسات المعلومات، العدد14، 2012، ص 19.

4 – عبدالإله محمد سالم النوايسة، جريمة الدخول غير المشروع في تشريعات الجرائم الإلكترونية العربية "دراسة مقارنة"، المجلة القانونية والقضائية، العدد1،2016،ص 21.

القانونين- قانون الجرائم الإلكترونية الأردني رقم 17 لسنة2023 [1]، وقانون مكافحة جرائم تقنية المعلومات المصري رقم 175لسنة 2018- تعريفاً لهذه المصطلحات، فالموقع الإلكتروني عُرف بأنه : "حيز لإتاحة المعلومات على الشبكة المعلوماتية من خلال عنوان محدد"، وكذا القانون المصري الذي عرف الموقع بأنه: "مجال أو مكان افتراضي له عنوان محدد على شبكة معلوماتية يهدف إلى إتاحة البيانات العامة والخاصة.

أما الحساب الخاص فقد عُرف بأنه: "مجموعة من المعلومات الخاصة بالشخص الطبيعي أو الاعتباري، تخول له دون غيره الحق في الدخول على الخدمات المتاحة أو استخدامها من خلال موقع أو نظام معلوماتي"[2]، والنظام المعلوماتي هو: "مجموعة برامج وأدوات معدة لغرض إدارة ومعالجة البيانات والمعلومات، أو تقديم خدمة معلوماتية"، وفي القانون الأردني عُرف بأنه: "مجموعة البرامج أو التطبيقات أو منصات التواصل الاجتماعي أو الأجهزة أو الأدوات المعدة لإنشاء البيانات أو المعلومات إلكترونياً، أو إرسالها.

ومما تجدر الإشارة إليه أن القانون رقم (4) لسنة 1990 بشأن النظام الوطني للمعلومات والتوثيق قد جرّم في مادته 6/8 استعانة الجاني بأسلوب الحيلة أو الإكراه للحصول على البيانات والمعلومات، إلا أنه لم يتطرق لفرضية الدخول غير المشروع باختراق النظام المعلوماتي، كما أن حدود الحماية الجنائية لا تتعدى ما يحويه النظام الوطني المنصوص عليه بهذا القانون من بيانات ومعلومات، فالحماية الجنائية لا تسري على البيانات والمعلومات المدرجة لدى الجهات الأخرى، كالشركات والمؤسسات العامة [3].

ويُلاحظ أن المشرّع الأردني جاء في قانونه للجرائم الإلكترونية رقم (17) لسنة 2023، بتخصيص نص يتعلق بالاعتداء على الأنظمة الإلكترونية للدولة؛ إذ نصت المادة 4/أ على أنه: "يعاقب كل من دخل أو وصل دون تصريح ... إلى الشبكة المعلوماتية، أو تقنية المعلومات، أو نظام معلومات، أو أي جزء منها، يعود للوزارات، أو الدوائر الحكومية، أو المؤسسات العامة ... واطلع على بيانات، أو معلومات غير متاحة للجمهور، تمس الأمن الوطني أو العلاقات الخارجية للمملكة، أو السلامة العامة، أو

1 – حلَّ هذا القانون – قانون الجرائم الإلكترونية الأردني رقم 17 لسنة 2023، منشور بالجريدة الرسمية، ع 5874، في 2023/8/13 محل قانون الجرائم الإلكترونية السابق رقم 27 لسنة 2015.

2 – بخصوص قانون الجرائم الإلكترونية الأردني لم يعرف الحساب الخاص، ضمن المادة الأولى منه.

3 – لمزيد من الإيضاح يراجع رحاب علي عميش، الجريمة المعلوماتية: دراسة مقارنة بين القانونين الليبي والإماراتي، مجلة معهد دبي القضائي، ع 4،2014، ص 74،75.

الاقتصاد الوطني..."[1]، وقد ورد بذات المادة في فقرتها (ج) نصاً يجرم الدخول غير المشروع عن طريق المواقع الإلكترونية، إلا أن وجه الاختلاف بين الفقرتين "أ، ج" أن المشرّع الأردني في الفقرة "أ" ارتأى تجريم الدخول في حال تمكن الجاني من الاطلاع على معلومات ذات خطورة، موجودة على الشبكة المعلوماتية أو الأنظمة المعلوماتية الخاصة بالجهات العامة التابعة للدولة، أما في الفقرة "ج" فإن المشرّع قد أقر تجريم الدخول غير المشروع للمواقع الإلكترونية وإن لم يتحقق الاطلاع طالما كان هو مبتغى الجاني، ما يعني عدم تحقق هذه الجريمة إذا كان الدخول مجرداً من هدف الاطلاع[2].

أما المشرّع المصري فقد أقر بموجب نص المادة (20) من قانون مكافحة تقنية المعلومات الإلكترونية جريمة الدخول غير المشروع على مواقع الدولة [3]، المتمثل في أي سلوك يأتي به الجاني يمكنه من ولوج الموقع الإلكتروني، أو الحساب الشخصي، أو النظام المعلوماتي، أو الشبكة المعلوماتية، وهذا ما يقتضي ضرورة وجود جهاز كمبيوتر أو أي وسيلة تقنية المعلومات مع الإنترنت تُمكّن الجاني من الدخول للحساب الخاص واختراقه، بغض النظر عن كيفية اختراقه[4] لهذا الحساب أو النظام المعلوماتي، سواءً عن طريق استخدام شبكة الاتصالات الهاتفية، أو بحل الشفرة، أو كلمة السر الحقيقية، في حال لم يكن للجاني حق استخدامها[5].

1 – عُرف التصريح بالمادة الأولى من قانون الجرائم الإلكترونية الأردني بأنه: "الإذن الممنوح من صاحب العلاقة إلى شخص أو أكثر أو للجمهور للدخول أو الوصول إلى نظام المعلومات أو تقنية المعلومات أو الشبكة المعلوماتية أو استخدامها".

2 – حسن فضيل خليف، جريمة الدخول غير المشروع إلى النظام المعلوماتي والتعدي على محتوياته "دراسة مقارنة"، رسالة ماجستير، جامعة جرش،2016،ص 70.

3 – من الملاحظ أن هذه الجريمة تحديداً وردت بنص المادة 2/29 مكافحة الإرهاب، في حال الدخول غير المشروع للمواقع الإلكترونية التابعة للحكومة، بهدف الحصول على البيانات، أو المعلومات الموجودة عليها، أو الاطلاع عليها، أو تغييرها، أو محوها، أو إتلافها، أو تزوير محتواها الموجود بها، وكل ما ارتكب بغرض الترويج للأفكار أو المعتقدات الداعية إلى ارتكاب أعمال إرهابية، أو لبث ما يهدف إلى تضليل السلطات الأمنية، أو للتأثير على سير العدالة في شأن أية جريمة إرهابية. قانون مكافحة الإرهاب رقم (94) لسنة 2015، منشور بالجريدة الرسمية، ع 33 (مكرر)، في 15 أغسطس،2015.

4 – عُرف الاختراق بموجب نص المادة 2/1 من قانون الجرائم الإلكترونية الليبي بأنه: "هو القدرة على الوصول إلى أي وسيلة تقنية لمعلومات بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاصة".

5 – مدحت عبدالحليم رمضان، الحماية الجنائية للتجارة الإلكترونية" دراسة مقارنة"، دار النهضة العربية،2012، ص 50،51.

هذا ولم يقصر المشرّع المصري صور الاعتداء بالدخول عمداً إلى النظام المعلوماتي، بل أضاف إليها الدخول بطريق الخطأ نتيجةً لإهمال الجاني أو تقصيره، وقد ربط المشرّع تجريم الدخول الخطأ إلى الحساب أو الموقع الإلكتروني أو النظام المعلوماتي بالبقاء بهذا الحساب، ويفهم من ذلك عدم مساءلة الجاني في حالة الدخول بطريق الخطأ والخروج على الفور من ذاك النظام، فضلاً عن ذلك أضاف المشرّع الاختراق كأحد صور الاعتداء ضمن نص المادة ذاته.

أما عن تجاوز حدود الدخول فتتحقق هذه الصورة في حال إذا ما كان مصرحاً لشخص ما بالدخول للحساب الخاص بالدولة، إلا أن دخوله لهذا الحساب محدد زمنياً أو موضوعياً أو مكانياً[1]، وهذا الشخص لم يتقيد بهذه الحدود وتجاوزها؛ أي خالف الحدود المصرح له بها، فالبقاء في النظام المعلوماتي قد يسبقه دخول مشروع، إلا أن المستخدم المصرح له بالدخول قد تجاوز الوقت المحدد له [2]، أو قد يطلع على بيانات غير مصرح له بالاطلاع عليها، وبهذا الخصوص فإن تحديد تجاوز الحق المصرح به في الدخول من حيث الزمان أو مستوى الدخول ثم إدراجها بقانون مكافحة الجرائم الإلكترونية المصري – نص المادة 20– أما قانونا الجرائم الإلكترونية الليبي والأردني فقد اكتفيا بذكر عبارة (أو يجاوز، أو يخالف التصريح)، دون أن يبينا حدود هذه المخالفة زمانياً أو موضوعياً.

ولا يشترط في هذه الصورة وسابقتها –الدخول غير المشروع– تحقق نتيجة معينة، فالجريمة تتحقق بمجرد تجاوز حدود الحق المصرح به في الدخول أو الدخول غير المشروع، باستثناء ما ورد بنص المادة الرابعة من قانون الجرائم الإلكترونية الأخير 2023 [3]، التي اشترطت لتحقق الدخول غير المشروع أو تجاوز حدود الدخول بضرورة الاطلاع، فقد جاء نص المادة كالتالي: "يعاقب كل من دخل أو وصل دون تصريح أو بما يخالف أو يجاوز التصريح ..... واطلع على بيانات ومعلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة...".

1 – رامي متولي القاضي، المواجهة الجنائية لجرائم تقنية المعلومات في التشريع المصري في ضوء أحكام القانون 175 لسنة 2018 م. مقارناً بالمواثيق الدولية والتشريعات المقارن، مجلة البحوث القانونية والاقتصادية، العدد75، 2021، ص 1039.

2 – ما شاء الله الزوي، الحماية الجنائية للبيانات الإلكترونية في القانون الليبي والمقارن، مجلة العلوم الشرعية والقانونية، العدد1،2018،ص166.

3 – وفقاً لقانون الجرائم الإلكترونية الأردني رقم 27 لسنة 2015 كانت العبارة المدرجة بنص المادة 12 الخاصة بالدخول غير المشروع أو تجاوز حدود الدخول للمواقع والأنظمة الخاصة بالدولة هي (بهدف الاطلاع على البيانات...).

وقد قرر المشرّع الليبي لجريمة الدخول للأنظمة المعلوماتية أو شبكة المعلومات –في حال اختراق وسائل وإجراءات الحماية بشكل كلي أو جزئي سواءً بدون تصريح أو مخالفةً لأحكام التصريح– عقوبة الحبس مدة لا تزيد عن سنة، أو الغرامة التي لا تقل عن 100 ولا تزيد عن 500 دينار، أو العقوبتين معاً.

وفيما يتعلق بالقانون الأردني فقد قرر معاقبة من يدخل دون تصريح أو بما يجاوز التصريح إلى الشبكة المعلوماتية أو نظام المعلومات ويطلع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو السلامة العامة أو الاقتصاد الوطني –أي ما يمس بالدولة– بالحبس مدة لا تقل عن 6 أشهر ولا تزيد عن ثلاث سنوات وبغرامة لا تقل عن 2500 دينار ولا تزيد على 25000دينار[1] .

أما المادة (20) من قانون مكافحة جرائم تقنية المعلومات المصري فقد قضت بمعاقبة كل من يدخل عمداً، أو دخل بخطأ غير عمدي وبقي بدون وجه حق، أو تجاوز الحد المخول له بالدخول، بالحبس مدة لا تقل عن عامين وغرامة لا تقل عن 50 ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى العقوبتين.

ومما تجدر الإشارة إليه أن كلاً من المشرّع الليبي والمصري وكذا الأردني ارتأوا تشديد العقوبة في حال توافر قصد خاص فضلاً عن القصد الجنائي العام المتمثل في توافر علم الجاني بدخوله لنظام معلوماتي أو موقع إلكتروني أو حساب خاص، واتجاه إرادته لهذا الدخول أو تجاوز حق الدخول المصرح له به – واطلاعه على البيانات والمعلومات بالأردن–، فوفقاً للمادة 2/12 من قانون الجرائم الإلكترونية الليبي إذا كان قصد الدخول هو إلغاء البيانات أو حذفها، وتتحقق هذه الحالة بإزالة كافة البيانات الموجودة على حسابات أو مواقع الدولة[2]، أو إضافة أو تدمير ما هو موجود على الحساب أو الموقع الإلكتروني وجعله

1 – من بين ما تم تعديله بموجب قانون الجرائم الإلكترونية الأردني الأخير هذه العقوبة، فقد كانت أخف من ذلك في القانون السابق– قانون الجرائم الإلكترونية الأردني رقم 27 لسنة 2015– إذ نصت المادة 12 على أنه: "يعاقب كل من دخل قصداً دون تصريح أو بما يخالف أو يجاوز التصريح إلى الشبكة المعلوماتية أو نظام معلومات بأي وسيلة كانت بهدف الاطلاع على بيانات أو معلومات بأي وسيلة كانت... بالحبس مدة لا تقل عن 4 أشهر وغرامة لا تقل عن 500 دينار ولا تزيد عن 5000دينار".

2 – دلال لطيف الزبيدي، جريمة الاعتداء على المواقع الإلكترونية، مجلة جامعة بابل للعلوم الإنسانية، العدد9، 2018، ص 401.

غير صالح للاستعمال[1]، أو إفشاء أو حجب أو نقل أو تعديل أو نسخ البيانات بنسخ ما يحتويه الحساب الخاص أو الموقع أو النظام المعلوماتي وحفظها بأي وسيلة إلكترونية أخرى، بما يمكن الحصول على صورة من البيانات الأصلية[2]، أو تعطيل عمل نظام معلوماتي أو تغيير موقع إلكتروني، أو انتحال شخصية مالك الموقع أو الشبكة المعلوماتية أو النظام المعلوماتي، تشدد العقوبة في حق الجاني وتصبح الحبس مدة لا تقل عن سنة وغرامة لا تقل عن 500 دينار و لا تزيد عن خمسة آلاف دينار.

وحسبما جاء في المادة 4/ب من قانون الجرائم الإلكترونية الأردني إذا كان هذا الدخول بغرض إلغاء البيانات أو المعلومات، أو إتلافها، أو تدميرها، أو تعديلها، أو نقلها، أو نسخها، أو نشرها، أو إعادة نشرها، أو خسارة سريتها، أو تشفيرها، أو إضافتها، أو حذفها، أو حجبها، أو إفشائها، أو التقاطها، فتكون العقوبة الأشغال الشاقة المؤقتة التي تتراوح مدتها بين ثلاث سنوات كحد أدنى، وخمس عشرة سنة كحد أقصى، والغرامة التي لا تقل عن 5000 دينار ولا تزيد عن 25000 دينار.

أما المشرّع المصري فقد شدَّد العقوبة وفقاً للمادة 2/20 في حالتين فقط، هما إذا كان قصد الجاني من وراء الدخول هو الاعتراض، أو الحصول بدون وجه حق على بيانات أو معلومات حكومية.

ومن الملاحظ أن العقوبة تغلّظ في حق الجاني بمجرد توافر أي من القصود المذكورة أعلاه؛ إذ لا يشترط لذلك تحقق ما قصده الجاني من وراء دخوله غير المشروع أو تجاوز حقه في الدخول.

وهناك حالة أخرى لتشديد عقوبة الدخول لأنظمة ومواقع الدولة وذلك بحسب ما ينجم عن الدخول أو تجاوز حدوده من نتائج؛ أي بحسب الضرر المتحقق، فإذا تمكن الجاني من وراء دخوله لهذه الأنظمة إعاقة عملها، أو تعطيل الشبكة المعلوماتية أو عمل المواقع الإلكترونية، أو أفسد ما تحتويه، فستكون عقوبته السجن والغرامة التي لا تقل عن عشرة آلاف دينار– المادة 3/12 من قانون الجرائم الإلكترونية الليبي–، أما القانون المصري فقد شدد العقوبة إذا ما نجم عن الدخول المتعمد أو بطريق الخطأ إتلاف البيانات أو المعلومات، أو الحساب الخاص، أو النظام المعلوماتي، أو البريد الإلكتروني، أو تدمير أو تشويه أو تغيير أو تسجيل ما فيه من بيانات، أو إعادة نشر محتوى أو إلغاء ما به كلياً أو جزئياً؛ فتكون العقوبة السجن والغرامة التي لا تقل عن مليون جنيه ولا تتجاوز 5 ملايين جنيه.

1– المرجع نفسه، الصفحة نفسها.

2 - أحمد طلعت عبدالحكيم، السياسة الجنائية في مواجهة جرائم تقنية المعلومات في ضوء القانون المصري رقم (175) لسنة 2018، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 2022، ص117.

ويُلاحظ في إطار تشديد العقوبة أن المشرّع الأردني قرر بموجب نص مادته 4/ب، د – قانون مكافحة الجرائم الإلكترونية رقم 17السنة2023–[1]، تشديدها إذ ما نجم عن الدخول غير المصرح به أو تجاوز حدوده النتيجة التي ابتغى الجاني تحققها من وراء دخوله "إلغاء البيانات، إتلافها، تدميرها، تعديلها، تغييرها، نقلها، نسخها، التقاطها، إفشائها، حذفها، خسارة سريتها، تشفيرها، حجبها"، فبتحقق أيٍّ من هذه النتائج يعاقب الجاني بالأشغال المؤقتة مدة لا تقل عن خمس سنوات، والغرامة 25000 دينار، هذا ما يعني أن المشرّع رفع من الحد الأدنى للعقوبة السالبة للحرية، وجعل الغرامة من حد واحد فقط.

وقد خُصصت المادة 40 من قانون مكافحة جرائم تقنية المعلومات المصري لتحديد عقوبة من يشرع في ارتكاب إحدى الجرائم الواردة بهذا القانون وذلك بمعاقبته بذات العقوبة المقررة للجريمة التامة، والأمر ذاته ينطبق على قانون الجرائم الإلكترونية الأردني الذي نص في مادته 4/ه على أنه: "يعاقب على الشروع في الجرائم المنصوص عليها في هذه المادة بالعقوبة المقررة للجرائم ذاتها"، أما قانون الجرائم الإلكترونية الليبي فلم ينص على عقوبة من يشرع بالدخول غير المشروع للأنظمة والمواقع.

ثانياً– الاعتراض غير القانوني:

يتحقق الاعتراض باستخدام وسائل معينة لالتقاط الانبعاثات الكهرومغناطيسية الناتجة عن نظام معلوماتي أو حاسب آلي، هذه الانبعاثات لا تعد بيانات، إلا أنه من الجائز إعادة بنائها في صورة بيانات[2].

وقد جُرم الاعتراض في قانون الجرائم الإلكترونية الليبي بموجب نص المادة 13 التي جاءت تحت عنوان: "الاعتراض أو التعرض" بأنه: "يعاقب .... كل من اعترض نظاماً معلوماتياً بقصد الحصول على بيانات رقمية أو للربط مع أنظمة إلكترونية أخرى"، وبهذا الخصوص جاءت المادة الأولى وعرفته– الاعتراض– بأنه: "مشاهدة البيانات أو المعلومات أو الحصول عليها"، أما المشرّع المصري فقد عرف الاعتراض في المادة الأولى بشكل يكاد يكون أكثر شمولاً مما ورد بالقانون الليبي؛ إذ نص في مادته الأولى على أن الاعتراض هو: "مشاهدة البيانات أو المعلومات أو الحصول عليها، بغرض التنصت، أو التعطيل، أو التخزين، أو النسخ، أو التسجيل، أو تغيير المحتوى، أو إساءة الاستخدام، أو تعديل المسار، أو إعادة التوجيه، وذلك لأسباب غير مشروعة ودون وجه حق"، وتتحقق جريمة الاعتراض غير

1 – مما يجدر التنويه إليه أن قانون الجرائم الإلكترونية رقم 27 لسنة 2015 في نص مادته 12/ب– د لم يشدد العقوبة بناءً على تحقق نتيجة إجرامية معينة، فقد اكتفى بتغليظ العقوبة بمجرد توافر القصد الخاص؛ لذا فإن ذات العقوبة المقررة في حال توافر القصد الخاص تنطبق سواءً تحققت النتيجة أم لم تتحقق وفقاً لهذا القانون.

2 – هلالي عبد اللاه أحمد، جرائم المعلومات التقليدية والمستحدثة وتطبيقاتها في النظام البحريني، 2013، ص255، مشار إليه عند عبد الإله النوايسي، المرجع السابق، ص 59.

المشروع – حسب ما جاءت بنص المادة 16 – في حال ما قام الجاني باعتراض أي معلومات أو ما هو متداول عن طريق الشبكات المعلوماتية؛ فالاعتراض يتحقق بمجرد مشاهدة أو سماع البيانات والحصول عليها حتى ولو لم يتم تحميلها أو تصويرها[1]، ولعل النص المقابل لذلك في قانون الجرائم الإلكترونية الأردني، هو نص المادة 7، حيث جرم المشرّع فيه – المادة1/7 – من يعترض عمداً خط سير البيانات، أو يلتقط محتواها، أو يعيق أو يشطب أو يسجل أي محتوى، سواءً أكان مرسلاً عن طريق شبكة المعلومات أو نظام معلومات، أو كانت هذه البيانات متبادلة داخل ذات الشبكة أو النظام، ونص في م 3/7 على تشديد العقوبة إذا كان محل الاعتراض معلومات وبيانات تخص جهة رسمية، بخلاف القانونين المصري والليبي؛ إذ حدد كلٌّ منهما لهذه الجريمة عقوبة واحدة أياً كان محل هذا الاعتداء، سواءً بيانات تخص الأفراد أم تخص الدولة[2].

ويُلاحظ أن المشرّع الليبي لم يكتفِ بنص الاعتراض، وإنما أفرد نص المادة 47 لجريمة التنصت، جاء فيها: "يُعاقب بـــ... كل من تنصت لصالح نفسه أو لصالح غيره على الاتصالات التي تجرى عبر شبكة المعلومات الدولية أو أي وسيلة إلكترونية أخرى، وتكون العقوبة ... إذا كان التنصت بقصد الحصول على أسرار حكومية أو أمنية أو عسكرية أو مصرفية ..." .

وباستقراء نص المادة 2/47 من قانون الجرائم الإلكترونية الليبي نلاحظ أن المشرّع قرر تغليظ العقوبة في حال ما كان التنصت غير المشروع بقصد الحصول على أسرار حكومية أو أمنية أو عسكرية أو مصرفية؛ إذ يعاقب الجاني في هذه الحالة بالسجن الذي يتراوح بين ثلاث سنوات كحد أدنى إلى 15 سنة كحد أقصى، فضلاً عن ذلك أقر المشرّع تشديد العقوبة أكثر في حال تحقق نتيجة من وراء هذا التنصت، ألا وهي نشر الأسرار التي تحصل عليها الجاني، فعقوبته في هذه الحالة هي السجن المؤبد.

ومما يجدر التنويه إليه أن قانون رقم (22) لسنة 2010 بشأن الاتصالات قد تطرق في مادته (35) إلى جريمة إساءة استخدام شبكة المعلومات؛ إذ نصت هذه المادة على أنه: "يعاقب بالحبس مدة لا تقل عن (6) أشهر وغرامة لا تقل عن (3) آلاف دينار ولا تزيد عن خمسة آلاف دينار وسحب الترخيص ومصادرة الآلات والأجهزة المستخدمة وذلك لكل من أساء استخدام شبكة المعلومات الدولية في نشر معلومات أو بيانات تمس الأمن السياسي أو الاقتصادي أو الاجتماعي ...".

1 – رامي متولي، المرجع السابق، ص1045.

2 – وفقا لنص المادة 17 من قانون مكافحة جرائم تقنية المعلومات المصري فإن عقوبة جريمة الاعتراض هي الحبس مدة لا تقل عن سنة، وغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتين وخمسين ألف جنيه، وبإحدى هاتين العقوبتين، بينما حُددت لها وفقاً لقانون الجرائم الإلكترونية الليبي بموجب نص المادة 13 عقوبة الحبس مدة لا تقل عن سنة وبغرامة لا تقل عن 1000 ألف دينار ولا تزيد عن 5000آلاف دينار.

ثالثاً- تعطيل الأعمال الحكومية:

أضفى المشرّع الليبي حماية جنائية خاصة للأعمال الحكومية من العبث بها إلكترونياً، بأن نصَّ في المادة (34) من قانون الجرائم الإلكترونية على جريمة تعطيل الأعمال الحكومية باستخدام أي نظام معلوماتي أو موقع إلكتروني، أو من خلال الحساب الخاص بهذه الجهة الحكومية، وأسبغ على الجريمة وصف الجناية؛ وذلك بأن قرر معاقبة الجاني بالسجن الذي يتراوح بين 3 سنوات ولا يزيد عن 15 سنة، وغرامة لا تقل عن 10000ولا تزيد عن 100000 في حال تعطيله للأعمال الحكومية أو عرقل عملها بأي وسيلة إلكترونية. وفي هذا الصدد لم ينص قانونا الجرائم الإلكترونية الأردني والمصري على هذه الجريمة بنص خاص ضمن نصوص قوانينهما.

رابعاً- اصطناع المواقع والحسابات الخاصة والبريد الإلكتروني:

يقصد بالاصطناع إظهار الشيء من العدم أو إعداد شيء لم يكن موجوداً[1]، وقد نص المشرّع المصري على هذه الجريمة بموجب نص مادته 24، ففي حال اصطناع الموقع أو البريد الإلكتروني أو الحساب الخاص ونسبته لأحد الاشخاص الاعتبارية العامة يسأل الجاني عن جريمة اصطناع المواقع، وقد انتهج المشرّع الأردني ذات النهج بتجريمه لذات السلوك في المادة الخامسة منه، والمتمثل في قيام الجاني بإنشاء أو اصطناع برنامج أو تطبيق أو موقع إلكتروني أو بريد إلكتروني ونسبته زوراً إلى جهة رسمية أو موظف عام أو بانتحال هويته بحكم وظيفته.

وبناءً على ذلك فالجريمة تتحقق بالاصطناع سواءً كان محله موقعاً أو بريداً إلكترونياً، أو حساباً خاصاً، ونسبته زوراً للشخص الاعتباري العام – وفقاً للقانون المصري- أو جهة رسمية أو موظف عام – القانون الأردني.

وقد أسبغ كلٌّ من المشرّع الأردني وكذلك المصري على هذه الجريمة وصف الجناية؛ فالعقوبة المقررة لها بالمادة5/ج الأشغال الشاقة المؤقتة، والغرامة التي لا تقل عن 15 ألف دينار ولا تزيد عن 45 ألف دينار، وبهذا الخصوص قرر لها المشرّع المصري في مادته 3/24عقوبة السجن والغرامة التي لا تقل عن مائة ألف جنيه، ولا تزيد عن ثلاثمائة ألف جنيه.

خامساً- الظروف المشددة:

وفي معرض حديثنا عن تشديد العقوبة فإن قانون مكافحة جرائم تقنية المعلومات المصري قد أدرج بنص مادته (34) حالات محددة تشدد فيهما العقوبة؛ إذ نص هذا القانون على أنه: "إذا وقعت أي جريمة من الجرائم المنصوص عليها في هذا القانون بغرض الإخلال بالنظام العام أو تعريض سلامة المجتمع

1 – أحمد طلعت عبدالحكيم، المرجع السابق، ص179.

وأمنه للخطر، أو الإضرار بالأمن القومي للبلاد أو بمركزها الاقتصادي، أو منع أو عرقلة ممارسة السلطات العامة لأعمالها، أو تعطيل أحكام الدستور أو القوانين أو اللوائح أو الإضرار بالوحدة الوطنية والسلام الاجتماعي تكون العقوبة السجن المشدد".

ما يفهم من هذا النص أن العقوبة تشدد في حق الجاني إذا ارتُكبت إحدى الجرائم الواردة بهذا القانون، كجريمة الدخول غير المشروع للمواقع الإلكترونية أو الأنظمة المعلوماتية الخاصة بالدولة، أو تجاوز الحد المصرح بدخولها إذا كان غرضه الإخلال بالنظام العام أو تعريض سلامة المجتمع وأمنه للخطر وإن لم يتحقق أي ضرر جراء ذلك، أو بهدف الإضرار بالأمن القومي للبلاد المتمثل حسبما جاء بقانون مكافحة جرائم تقنية المعلومات المصري في : "كل ما يتصل باستقلال واستقرار وأمن الوطن ووحدته وسلامة أراضيه، وما يتعلق بشؤون رئاسة الجمهورية ومجلس الدفاع الوطني ومجلس الأمن القومي ووزارة الداخلية، والمخابرات العامة وهيئة الرقابة الإدارية، والأجهزة التابعة لتلك الجهات"، وكذلك في حال ما كان مبتغى الجاني الإضرار بالمركز الاقتصادي للدولة أو منع وعرقلة ممارسة الدولة لأعمالها من خلال تعطيل السلطات التشريعية أو التنفيذية أو القضائية من ممارسة أعمالها، أو منع المؤسسات التعليمية من ممارسة أعمالها[1]. فضلاً عن ذلك تُغلظ العقوبة في حق الجاني إذا ما ارتكب إحدى الجرائم المنصوص عليها بهذا القانون، وكان يهدف من وراء ارتكاب جريمته تعطيل العمل بأحكام الدستور أو القوانين أو اللوائح أو الأضرار بالوحدة الوطنية والسلام الاجتماعي.

ونشير في هذا المقام إلى أن المشرّع الأردني نصَّ على جملة من الظروف المشددة الخاصة بالجرائم الإلكترونية بموجب نص مادته 28، فضاعف العقوبة في حال ارتكاب الجريمة من قبل من استغل وظيفته أو عمله أو الصلاحيات الممنوحة له، وكذلك إذا ما تعدد المجني عليهم، وفي حال تكرار ارتكاب الجريمة، أو إذا ما ارتكبت لمصلحة دولة أجنبية أو تنظيم غير مشروع.

وفي إطار حديثنا عما ورد من جزاءات في قانون الجرائم الإلكترونية الليبي، نلاحظ أن المشرّع خصص للمصادرة وغلق المحل نص المادة 50، الذي قضى فيه بمصادرة جميع الأجهزة والمعدات أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم الواردة بهذا القانون، كجريمة الدخول غير المشروع للأنظمة المعلوماتية الخاصة بالدولة بقصد تعطيل البيانات أو إتلافها أو تعطيل عمل النظام المعلوماتي، فضلاً عن ذلك تصادر الأموال التي تحصل عليها الجاني من وراء ارتكاب جريمته، بشرط مراعاة حقوق الغير حسني النية.

1 – رامي متولي، المرجع السابق، ص1160.

كما أوجب ذات النص غلق المحل أو الموقع الذي ترتكب فيه جريمة من الجرائم الواردة بهذا القانون، طالما ارتكبت الجريمة بعلم مالك المحل، وهذا الإغلاق قد يكون كلياً أو محدداً بفترة معينة حسبما تقدره المحكمة، بخلاف المشرّع الأردني الذي حدده بفترة معينة – المادة4/31– لا تقل عن ثلاثة أشهر ولا تزيد عن سنة.

أما فيما يتعلق بالمصادرة فقد أوردها المشرّع المصري في قانون مكافحة تقنية المعلومات في المادة (38)، التي قضت بمصادرة الأدوات والآلات والمعدات والأجهزة مما لا يجوز حيازتها قانوناً– أي أن حيازتها غير مشروعة–، أو غيرها، مما يكون قد استُخدم في ارتكاب الجريمة، أو سهّل أو أسهم في ارتكابها، ولعل ما جاء في قانون الجرائم الإلكترونية الأردني– المادة 1/31– ليس ببعيد عما أقره القانون المصري فيما يتعلق بمصادرة الأجهزة والأدوات والوسائل والمواد المستخدمة في ارتكاب أي من الجرائم المنصوص عليها بهذا القانون، فضلاً عن مصادرة الأموال المتحصلة من تلك الجريمة .

سادساً– العزل من الوظيفة:

ويلاحظ في هذا الشأن أن المشرّع المصري نص على عقوبة العزل من الوظيفة، التي عرفها بأنها: "الحرمان من الوظيفة والمرتبات المقررة لها" – نص المادة 1/26 من قانون العقوبات المصري–؛ إذ أوجبت المادة 39 من قانون مكافحة جرائم تقنية المعلومات المصري عزل الموظف العمومي من وظيفته عزلاً مؤقتاً، في حال ارتكابه جريمة من الجرائم الواردة بهذا القانون أثناء وبسبب تأدية وظيفته، وبناءً على ذلك فإن عقوبة العزل في هذه الحالة عقوبة جوازية، ولمحكمة الموضوع أن تكتفي بالعقوبة الأصلية المقررة للجريمة دون أن تقضي في حكمها بعقوبة العزل، كما لها سلطة الحكم بها، وفي هذه الحالة يجب أن تنطق بها صراحةً في حكمها، ووفقاً للقواعد العامة فإن مدة العزل لا تقل عن سنة ولا تزيد عن ست سنوات – المادة 2/26من قانون العقوبات المصري–، ويكون العزل وجوبياً في حال ارتكاب الموظف العام إحدى الجرائم الواردة بهذا القانون– كجريمة الاعتداء على المواقع الإلكترونية للدولة– مع توافر أي من الظروف المشددة الواردة بالمادة 34 المتمثلة في ارتكاب الجريمة إخلالاً بالنظام العام، أو تعريض سلامة المجتمع وأمنه للخطر، أو الإضرار بالأمن القومي للبلاد، أو منع أو عرقلة ممارسة السلطات العامة لأعمالها، أو تعطيل أحكام الدستور والقوانين أو اللوائح، أو الإضرار بالوحدة الوطنية والسلام الاجتماعي، ففي حال اقتران الجريمة الإلكترونية مع أي من هذه الظروف يعزل الموظف العام من وظيفته عزلاً مؤبداً كعقوبة تبعية في هذه الحالة، ويحرم بموجبه من الالتحاق بوظيفة عامة طوال حياته.

هذا ولم يتطرق قانون الجرائم الإلكترونية الليبي لمثل هذه العقوبة ضمن نصوص مواده، إلا أن هذه العقوبة تطبق بحق الجاني باعتبارها إحدى العقوبات التبعية الواردة بقانون العقوبات الليبي تحديداً نص المادة 2/33، فالمحكوم عليه سيحرم من حقوقه المدنية التي منها صلاحيته للبقاء في الوظيفة العامة، وهذا الحرمان قد يكون دائماً في حالة الحكم عليه بالسجن المؤبد أو السجن لمدة عشر سنوات أو أكثر، وقد يكون حرماناً مؤقتاً في حالة الحكم عليه بالسجن

لمدة ثلاث سنوات أو أكثر؛ إذ سيحرم في هذه الحالة من ممارسة وظيفته العامة مدة تنفيذ العقوبة، ومدة بعد ذلك لا تقل عن سنة ولا تزيد عن خمس سنوات (المادة 34 من قانون العقوبات الليبي).

وفيما يتعلق بقانون الجرائم الإلكترونية الأردني فمن خلال مطالعة نصوصه يتضح لنا عدم إيراده لعقوبة العزل ضمن نصوص مواده، إلا أن ذلك لا يعني عدم إمكان إيقاع هذه العقوبة، فقد وردت عقوبة عزل الموظف من وظيفته بموجب المادة (171) من نظام الخدمة المدنية رقم (82) لسنة 2013، وقد حدد المشرّع الأردني في المادة 171/أ الحالات التي تؤدي إلى عزل الموظف العام، ومنها في حال الحكم على الموظف العام بارتكاب جناية، وفي حال الحكم على الموظف العام بعقوبة مقيدة للحرية لمدة تزيد عن ستة أشهر.

سابعاً- الإعفاء من العقاب:

بالنظر لخطورة الجرائم الإلكترونية وبالأخص الجرائم التي تمثل اعتداءً على الدولة من خلال الاعتداء على بياناتها ومعلوماتها الخاصة ونشرها أو حذفها، وفي محاولة للتقليل من ارتكاب هذه الجرائم ومكافحتها التي لا تحقق من خلال تشديد العقوبة في حق الجناة فقط، وإنما يجب وضع نظام يقر نوعاً من تخفيف العقوبة في حق الجناة أو إعفاؤهم منها في حالات محددة، ولأهمية الإعفاء كوسيلة لمكافحة الجريمة والتقليل من حدتها تنبه المشرّع المصري وأدرج في نص المادة 41 على أنه: "يعفى من العقوبات المقررة للجرائم المنصوص عليها في هذا القانون، كل من بادر من الجناة أو الشركاء إلى إبلاغ السلطات القضائية أو السلطات العامة بما يعلمه عنها قبل البدء في تنفيذ الجريمة وقبل كشفها. ويجوز للمحكمة الإعفاء من العقوبة أو التخفيف منها إذا حصل البلاغ بعد كشف الجريمة وقبل التصرف في التحقيق فيها، إذا مكن الجاني أو الشريك في أثناء التحقيق السلطات المختصة من القبض على مرتكبي الجريمة الآخرين، أو على ضبط الأموال موضوع الجريمة، أو أعان أثناء البحث والتحقيق على كشف الحقيقة فيها، أو على القبض على مرتكبي جريمة أخرى مماثلة لهذا النوع والخطورة..."، وما يمكن ملاحظته من هذا النص أن المشرّع المصري قرر الإعفاء من العقاب المقرر للجريمة في حالتين، تتمثل الحالة الأولى في فرضية الإبلاغ عن الجريمة قبل البدء في تنفيذها وقبل كشفها من قبل السلطات المختصة، أما الحالة الثانية التي يجوز فيها الإعفاء من العقوبة أو تخفيفها فتتمثل في فرضية الابلاغ عن الجريمة بعد ما اكتشف أمرها من السلطات التي تمكنت باستعانة الجاني من القبض على الجناة الآخرين في هذه الجريمة أو في جريمة أخرى مماثلة، أو ضبط الأموال موضوع الجريمة، أو تمكنت من كشف الحقيقة بخصوص الجريمة عن طريق معاونة الجاني لها.

المطلب الثاني

تقييم الحماية الجنائية المقررة للمواقع والأنظمة الإلكترونية

سيتضمن هذا المطلب ما اعترى السياسة التشريعية التي انتهجها كلٌّ من المشرّع الليبي والأردني والمصري من مثالب، وكذلك ما امتاز به كلٌّ منهم من أوجه حماية للمواقع والأنظمة الإلكترونية الخاصة بالدولة، وذلك من خلال اتباع التقسيم السابق ذاته.

أولاً- جريمة الدخول غير المشروع وتجاوز حدود الدخول:

لعل ما نود الإشارة إليه أولاً قبل الحديث عن الجريمة هو تعريف بعض المصطلحات؛ فبمطالعتنا لنص المادة الأولى من قانون الجرائم الإلكترونية الليبي، لاحظنا خلو هذا القانون من تعريفٍ لبعض المصطلحات التي تعد محلاً للجريمة الإلكترونية، ما يعد عيباً في القانون، فعدم إيضاح بعض المصطلحات بتعريف لها، قد يسبب اختلاط معناها مع غيرها، فكما لاحظنا فيما سبق أن كلاً من القانون الأردني وكذا المصري أدرجا في المادة الأولى تعريفاً لعدد من المصطلحات التي تجنبنا التناقض وعدم الوضوح.

أما عن جريمة الدخول وتجاوز حدوده، فما لاحظناه على نص المادة 12 من قانون الجرائم الإلكترونية الليبي أنه جاء بصيغة عامة دون أن يحدد لنا صفة المجني عليه من هذا الاعتداء – الدخول غير المشروع-، هل هو شخص عادي أم جهة من الجهات الاعتبارية كالشركات والمؤسسات العامة أو الشركات الخاصة؟ وهذا ما يجعلنا نعطي لهذا النص صفة العمومية وانسحاب تطبيقه بغض النظر عن الجهة المعتدى على بياناتها الخاصة، طالما لا يوجد نص آخر بهذا القانون يعطي بعضاً من صفة الخصوصية للاعتداءات التي تمس بالجهات العامة ومؤسسات الدولة.

وهذا بخلاف كلٍّ من المشرّع الأردني، و المشرّع المصري، اللذين أحاطا البيانات والمعلومات الخاصة بالدولة بقدرٍ من الحماية؛ إذ نصّا على تجريم الدخول غير المشروع وتجاوز حدود الدخول المصرح به للأنظمة المعلوماتية الخاصة بالدولة بنص خاص غير النص المتعلق بفرضية الاعتداء على المواقع أو الأنظمة الخاصة بالأفراد – المادة الثالثة من قانون الجرائم الإلكترونية الأردني، ونص المادة الرابعة عشرة من قانون مكافحة جرائم تقنية المعلومات المصري- وذلك بالنظر للمصلحة المعتدى عليها، التي تعد ذات أهمية تستوجب تخصيص نص لها، وعدم شمولها مع النص المتعلق بحماية الأنظمة المعلوماتية الخاصة بالأفراد؛ لذا كان الأولى بالمشرّع الليبي أن يقتفي أثر التشريعين المصري والأردني[1]، بأن يفرد لهذا الاعتداء – الدخول غير المشروع وتجاوز حدود الأنظمة المعلوماتية والمواقع الخاصة بالدولة- نصاً خاصاً.

وكما لاحظنا فيما سبق أن المشرّع المصري لم يجرم الدخول العمدي غير المشروع، بل جرم فضلاً عن ذلك الدخول بطريق الخطأ مع البقاء في النظام، وقد وفق المشرّع المصري بتجريمه لهذه الصورة من الدخول – الدخول بطريق الخطأ مع البقاء في الموقع أو النظام- بعكس القانونين الليبي والأردني اللذين اقتصرا على صورة واحدة للدخول، ألا وهي الدخول العمدي غير المشروع ؛ فلتحقيق أكبر قدر من الحماية للبيانات والمعلومات التي يحويها النظام المعلوماتي أو الموقع الإلكتروني يفترض تجريم البقاء غير المشروع في ذاك النظام أو الموقع باعتباره لا يقل خطورة عن الدخول غير المشروع؛

1 – مما يجدر التنويه إليه أن قانون الجرائم الإلكترونية الأردني رقم 27 لسنة 2015، أفرد لهذا الاعتداء نصاً خاصاً ألا وهو نص المادة 12 منه.

إذ يترتب على هذا البقاء في النظام أو الموقع المساس بسرية البيانات وسلامتها[1]، وهناك من يرى عدم المساواة في العقوبة بين الصورتين؛ إذ يفترض إقرار عقوبة أقل لحالة الدخول غير العمدي [2]، ومع تقديرنا لهذا الرأي إلا أننا لا نتفق معه؛ فسبب تجريم هذه الصورة ليس بسبب الدخول غير العمدي للنظام المعلوماتي، وإنما السبب هو البقاء في هذا النظام أو الموقع أو الحساب، فعبارة المشرّع واضحة وصريحة في الربط بين الدخول غير العمدي والبقاء الذي يتصور فيه تغيير في نية الجاني؛ أي أن بقاءها لا يفترض فيه إلا صورة العمد لا الخطأ.

كما أن ما يحسب للمشرع المصري أنه حدد لنا تجاوز الحد المصرح به بالقيد الزمني والمكاني، في حين غفل المشرّع الليبي وكذلك الأردني عن هذه المسألة؛ إذ اكتفيا بتجاوز حدود الدخول المصرح به فقط، وكان من المفترض تحديد قيد التجاوز حتى يعد الجاني فعلاً تجاوز الحد المصرح به له؛ إلا أنه من بين المآخذ على هذا القانون إدراجه للاختراق وكأنه فعل يختلف عن الدخول، وعلى الرغم من رأي البعض بأنه ثمة اختلاف بينهما؛ لكون الدخول يتحقق بفتح جهاز حاسب آلي أو استخدام رمز أو كود، وأن الاختراق يتحقق بوسيلة أخرى كاستخدام برامج متخصصة لاختراق المواقع[3]، فإننا لا نرى أي فارق بين الاثنين؛ فالاختراق هو ذاته الدخول[4].

أما عن العقوبة المقررة لجريمة الدخول غير المشروع بنص المادة 12، فما يعيب سياسة المشرّع الليبي في هذا الشأن، أنه قرر للجريمة عقوبة واحدة بغض النظر عما كان الاعتداء واقع على موقع أو حساب أو نظام معلوماتي خاص بالأفراد أو خاص بالمؤسسات الحكومية أو الجهات الاعتبارية العامة، ولعل الجريمة تعد أشد خطورة إذا ما تم الاعتداء على نظامها المعلوماتي أو موقعها الإلكتروني بالدخول إليه دخولاً غير مشروع أو تجاوز حدود الدخول المشروع؛ بالنظر لأهمية البيانات والمعلومات الموجودة عليه، وخطورة ما تحتويه، فضلاً عن خطورة الجاني الذي تسلل إلى هذا النظام أو الموقع وتمكن من اختراق نظام من المفترض أن حمايته المشددة

1 – ما شاء الله الزوي، المرجع السابق، ص 194.

2 – وليد سمير المعدواي، مكافحة جرائم تقنية المعلومات و الإرهاب الإلكتروني وفقاً لأحدث التشريعات المصرية، القيادة العامة لشرطة الشارقة، مركز بحوث الشرطة، العدد 2020،114،ص 217.

3 – رامي متولي القاضي، المرجع السابق، ص 1097.

4 – بمناسبة الحديث عن الاختراق، نص قانون الجرائم الإلكترونية الليبي في المادة 11 منه على أنه: "يعد الدخول لأجهزة وأنظمة الحاسب الآلي أو إلى نظام معلوماتي ... إذا تم الاختراق بشكل متعمد لوسائل وإجراءات الحماية لها بشكل كلي أو جزئي دون تصريح أو بما يخالف التصريح"، وكأن هذين المصطلحين لهما نفس المعنى..

(1)، أو كان مصرحاً له بدخول النظام إلا أنه تجاوز ما صُرّح له به، كأن يكون قد دخل لأنظمة شديدة الخطورة تمس أمن الدولة غير مسموح له بدخولها.

وبمناسبة الحديث عن هذا الاعتداء نجد أن المشرّع المصري والأردني لم يغفلا عن توفير حماية خاصة لأجهزة وأنظمة الدولة؛ إذ أوجبا تشديد عقوبة جريمة الدخول غير المشروع في حال ما كانت بسبب الاعتراض- الالتقاط بالأردن-، فالعقوبة المقررة للدخول غير المشروع إذا ما كان بقصد الاعتراض وفقاً لنص المادة 2/20 من قانون مكافحة تقنية المعلومات المصري هي السجن والغرامة التي لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه، ووفقاً لنص المادة 4/ب من قانون الجرائم الإلكترونية الأردني هي الأشغال المؤقتة وغرامة لا تقل عن 5000 دينار ولا تزيد عن 25000 دينار، ولعل المشرّع الأردني كان الأوفق حسب رأينا وذلك بتغليظه للعقوبة أكثر من ذلك إذا ما تمكن الجاني فعلاً من اعتراض البيانات والمعلومات فعقوبته في هذه الحالة بناءً على نص المادة سالفة الذكر هي الأشغال المؤقتة مدة لا تقل عن خمس سنوات والغرامة 25000 دينار.

ويُلاحظ أن المشرّع الليبي جاء بفرضيتين لتشديد عقوبة جريمة الدخول غير المشروع وتجاوزه في نص المادة 2،3/12 قانون الجرائم الإلكترونية، تتحقق الأولى بالنظر إلى قصد الجاني من وراء دخوله للنظام المعلوماتي، بينما تعتمد الثانية على النتائج المتحققة من وراء هذا الدخول التي قصرها المشرّع حسبما نرى على أخطر النتائج ألا وهي تعطيل النظام المعلوماتي أو إعاقته أو افساد محتوى النظام أو الشبكة المعلوماتية؛ لذا فقد أحاطها المشرّع بحماية أكثر وذلك بجعل العقوبة في مصاف الجنايات، وهذا التقسيم حسب اعتقادنا يُحسب للمشرع الليبي مقارنةً بالتشريع المصري الذي قصر القصد على الاعتراض أو الحصول بدون وجه على بيانات ومعلومات حكومية، وجاء في فقرة أخرى وشدد العقوبة بناءً على تحقق نتائج الإتلاف أو تدمير أو تشويه أو النسخ أو تسجيل أو إعادة النشر أو إلغاء البيانات كليا أو جزئياً.

وفيما يتعلق بسياسة المشرّع الليبي في التشديد بناءً على قصد الجاني من وراء الدخول تحديداً قصد إفشاء المعلومات أو البيانات، يثار لدينا تساؤل مفاده: إذا دخل الجاني بقصد إفشاء أسرار تتعلق بالدولة، فهل سيعاقب وفقاً للعقوبة المقررة بموجب نص المادة 2/12؟

بمطالعتنا لنصوص قانون الجرائم الإلكترونية، نلاحظ أن هذا الأخير احتوى بالفقرة الثانية من نص المادة 49 التي أحالت إلى قانون العقوبات لتطبيق العقوبة الأشد، وقد تضمن قانون العقوبات الليبي بموجب نص المادة 2/171 عقوبة لمن يحصل على سر يتعلق بالدفاع أو ما يماثله بقصد إفشائه يعاقب بالإعدام.

1 - ماشاء الله الزوي، المرجع السابق، ص163.

وبخصوص الشروع في جريمة الدخول غير المشروع أو تجاوز حدود الدخول، لنا أن نتساءل هل يتصور الشروع في هاتين الجريمتين؟ حقيقةً لا نتصور تحقق الشروع في إحدى هاتين الصورتين، باعتبار أن الجريمة تعد كاملة بمجرد الدخول أو تجاوز الحد المصرح فيه للجاني بالدخول دون تطلب تحقق نتيجة معينة من وراء ذلك، باستثناء ما ورد بنص المادة 4/ أ من قانون الجرائم الإلكترونية الأردني التي قيدت تحقق الجريمة – الدخول غير المشروع– باطلاع الجاني على البيانات والمعلومات.

ثانياً– جريمة الاعتراض غير القانوني:

بخصوص هذه الجريمة يحسب للمشرع الأردني تشديده لعقوبة جريمة الاعتراض في حال وقوع الاعتراض على بيانات ومعلومات خاصة بالدولة، في حين ساوى المشرّع الليبي والمصري عقوبة جريمة الاعتراض أياً كان محله، سواءً كان بيانات ومعلومات خاصة بالدولة أم خاصة بالأفراد، وكان من المفترض إعمالاً لإقرار حماية جنائية تتناسب مع أهمية بيانات الدولة تشديد العقوبة مثلما فعل المشرّع الأردني، وقد أضفى المشرّع الليبي حماية جنائية للاتصالات التي تجرى عبر شبكة المعلومات الدولية أو أي وسيلة إلكترونية أخرى في حال التنصت عليها[1]، وهذا بخلاف القانون المصري الذي اكتفى بنص واحد لتجريم الاعتراض الذي يحوي التنصت، والواقع أن هناك من يرى ضرورة تخصيص نص للتنصت – كما فعل المشرّع الليبي– وعدم اشتماله مع جريمة أخرى، كما فعل المشرّع المصري الذي دمج الجرائم تحت نطاق تعريف الاعتراض[2]، إلا أننا نرى خلاف ذلك ؛ فنص الاعتراض يحوي بذاته التنصت، ولعل تعريف المشرّع الليبي للاعتراض أو الالتقاط دليل على ذلك؛ إذ عرفه بأنه: "مشاهدة البيانات أو المعلومات أو الحصول عليه " وهذا ما يفسر لدينا بأن التنصت من طرق الحصول على المعلومات والبيانات؛ فما الداعي لإفراد هكذا نص، ضمن نصوص قانوننا الليبي.

ثالثا– جريمة تعطيل الأعمال الحكومية:

هذه الجريمة التي وردت بنص صريح في قانون الجرائم الإلكترونية الليبي وفقاً لنص المادة 34، يثار لدينا تساؤل بخصوصها هو: لماذا أفرد المشرّع الليبي لصورة هذا الاعتداء نصاً خاصاً؟ إذ كان يمكن دمج هذه الصورة ضمن نص المادة (12) من ذات القانون، فتعطيل العمل الحكومي عادةً ما يتحقق بالدخول غير المشروع للبيانات والمواقع الخاصة به، أو بمخالفة الحدود المسموح بها في هذا الدخول، ولعل سبب تخصيص نص لهذه الصورة كون أن المشرّع الليبي لم يتطرق للاعتداءات الماسة بالجهات

1 – التنصت هو" فعل استراق السماع لمحادثات صوتية ترسل عبر الشبكة الإلكترونية عمداً بدون وجه حق"، محمد علي أبو علي، جريمة التنصت الإلكتروني، مجلة الباحث للدراسات القانونية والقضائية، العدد 46، 2022، ص 211.

2 – المرجع نفسه، ص219.

الاعتبارية العامة بشكل صريح في المادة (12)، فحسبما أوضحنا أن ما ورد بها هو تجريم لأنماط معينة من الأفعال بدون تحديد الجهة المعتدى عليها، هل هي شخص عادي أو جهة من الجهات الحكومية.

كما أن نص المادة 2/12 من القانون الليبي قد غلظ العقوبة في حق الجاني إذا كان قصده تعطيل عمل نظام معلومات، وهذا ما يطرح لدينا تساؤل آخر، وهو: ما الفرق بين تعطيل عمل نظام معلومات وتعطيل عمل حكومي باستخدام أي نظام معلوماتي؟ ألا يعد ما ذكر بنص المادة 2/12 أكثر توسعاً لإمكانية تحقق التعطيل في أي نظام حكومي يمس مصالح الدولة، وليس العمل فقط.

رابعاً- جريمة اصطناع المواقع الإلكترونية:

من أوجه الحماية التي أقرها كلٌّ من المشرّع المصري والأردني تخصيص نص خاص لتجريم اصطناع المواقع والبريد الإلكتروني، أما عن مشرعنا الليبي فلعل من بين أوجه قصور الحماية الجنائية بقانون الجرائم الإلكترونية أنه لم يدرج هذه الجريمة ضمن نصوص قانونه رغم ارتكاب هذا الفعل - الاصطناع- بشكل ملحوظ وخطورته لصعوبة الكشف عن هوية من يصطنع الحسابات والمواقع؛ إلا أنه إذا تمعنا النظر في نصوص قانوننا الليبي سنجده ضمن صور تشديد عقوبة جريمة الدخول غير المشروع وتجاوز حدود الدخول بناءً على توافر قصد معين ألا وهو انتحال شخصية مالك الحساب أو الموقع، وحسب اعتقادنا هذا القصد تحديداً يتقارب مع جريمة اصطناع المواقع ونسبتها لشخص اعتباري عام، فلماذا لم يفرد قانوننا لهذا الفعل نصاً يجرمه؛ وعدم جعله مجرد قصد تشدد به عقوبة جريمة الدخول غير المشروع والتجاوز، ومن جانب آخر إذا تمسكنا بحرفية مصطلحي "الاصطناع، الانتحال" نجد قصوراً في كلٍ من القانون الأردني والمصري وكذا الليبي الذي جاء بالانتحال ضمن ظروف تشديد عقوبة جريمة الدخول غير المشروع، ووجه القصور في الاصطناع يكمن في كونه عبارة عن إنشاء شيء من العدم باصطناع موقع أو بريد لا وجود مسبق له، والحقيقة أحياناً الجاني لا يصطنع الموقع بل يكتفي بانتحال شخصية مالكه - يستوي ذلك بدخول مشروع أو غير مشروع-، بالمقابل هناك قصور في الاكتفاء بالانتحال فالجاني قد لا ينتحل شخصية مالك الحساب أو الموقع بل ينشئ حساب لاوجود له مسبقاً؛ فلتحقيق حماية شاملة من هكذا اعتداء يفترض تجريم الفعلين معاً .

خامساً- الظروف المشددة:

كما رأينا فإن من ضمن أوجه الحماية التي قررها المشرّع المصري تغليظ العقوبة في حال توافر إحدى الظروف المشددة بالمادة 34، وما يعنينا في هذا الإطار هو الحديث عن الظرف المشدد المتعلق بمنع وعرقلة ممارسة الدولة لأعمالها، فكأنه يتوافق مع ما ورد بقانون الجرائم الإلكترونية الليبي فيما يتعلق بتعطيل العمل الحكومي أو عرقلته باستعمال أي وسيلة إلكترونية، التي قرر لها المشرّع عقوبة السجن وغرامة لا تقل عن

10000 دينار ولا تزيد عن 100000 دينار، وما يحسب للقانون المصري أنه جعل هذا المبتغى ظرفاً مشدداً لعقوبة أي جريمة من جرائم هذا القانون، كجريمة الاعتداء على مواقع وأنظمة الدولة .

سادساً- الإعفاء من العقاب:

بالنظر لما يرتبه إيراد نص كهذا في الكشف عن الجريمة، كنا نأمل من المشرّع الليبي أن يضمنه ضمن نصوص مواده، وإن كان لدينا وجهة نظر بخصوص قانون الجرائم الإلكترونية المصري، تحديداً فيما يتعلق بالحالة الأولى من الإعفاء من العقاب عن الجريمة التي اشترطت أن يكون قبل الشروع في تنفيذ أي فعل منها، وهو ما لا يمكن تحققه؛ فأي سلوك يأتي به الجاني قبل هذه المرحلة -الشروع في التنفيذ- لا يعاقب عنه أصلاً؛ لذا فلا مجال للحديث عن الإعفاء[1].

ويُلاحظ بالاطلاع على نصوص قانون الجرائم الإلكترونية الأردني، أن المشرّع لم يضمن نصوص مواده الإعفاء من العقاب؛ إلا أنه قرر سياسة لعلها الأوفق حسب رأينا، وذلك بتخفيض العقوبة المنصوص عليها في أي جريمة من هذه الجرائم إلى النصف في حال ما أدلى الجاني بمعلومات عن أية جريمة من الجرائم المنصوص عليها في هذا القانون قبل إحالتها للمدعي العام، طالما كان من شأن هذه المعلومات الكشف عن الجريمة أو مرتكبها أو القبض عليه.

الخاتمة

وصلنا إلى نهاية بحثنا حول الحماية الجنائية للمواقع والأنظمة الإلكترونية للدولة، وتبين لنا من خلال عرضنا لأوجه الحماية التي قررها مشرعنا الليبي بموجب قانونه الذي أصدره مؤخراً وجود العديد من أوجه القصور فيما قرره، لعل أهمها عدم إيلائه أهمية لصورة الدخول غير المشروع، أو تجاوز الحد المصرح به لدخول المواقع الخاصة بالدولة، من حيث إدراجها بنص خاص وتشديد العقوبة في حق من يدخل أو يتجاوز حد الدخول المسموح به، بخلاف كلٍ من القانون الأردني والمصري اللذين اعتنيا بإضفاء الحماية المناسبة لمواقع وأنظمة الدولة، وذلك بتخصيص نص يجرم الدخول وتجاوز حدوده لمواقع الدولة.

كما يحسب للمشرع المصري عدم اكتفائه بالدخول العمدي للنظام المعلوماتي أو الحساب أو الموقع الإلكتروني الخاص بالدولة، وذلك بتجريم صورة الدخول غير العمدي لهذا النظام والبقاء فيه، وقد كان من الأجدر بالمشرّع الليبي إقرار هذه الصورة مع الدخول العمدي لتصور تحقق هذه الفرضية.

1 - حورية محمد عبدالرحيم، مدى إمكانية تطبيق الإعفاء الوجوبي من عقوبة الجرائم المرتكبة ضد شخصية الدولة، مجلة كلية القانون، جامعة طرابلس، العددين8،7، 2023، ص200.

أما عن جريمة تعطيل الأعمال الحكومية الواردة بنص المادة (47) من قانون الجرائم الإلكترونية الليبي، فإننا نرى أنه كان من الأجدر بالمشرّع الليبي أن يدرجها ضمن الظروف المشددة للاعتداء على مواقع وأنظمة الدولة الإلكترونية، وحسناً فعل المشرّع المصري بإدراجه لها (تعطيل الأعمال الحكومية) ضمن الظروف المشددة لأي جريمة من الجرائم الواردة بقانونه، كجريمة الاعتداء على المواقع والأنظمة الإلكترونية للدولة. ولأهمية تنظيم الإعفاء عن العقوبة لفاعليته في مكافحة الجريمة كان من الأجدر بالمشرّع الليبي إقرار نص يُعفي الجاني من العقوبة أو تخفيفها.

لذا نوصي بتعديل قانون الجرائم الإلكترونية الليبي بتخصيص نص يجرم أفعال الاعتداء التي تمس المواقع والأنظمة الإلكترونية الخاصة بالدولة، من خلال تجريم الدخول غير المشروع – الدخول العمدي والدخول بطريق الخطأ في حال البقاء في النظام أو الموقع الإلكتروني– وتجاوز الحد المسموح به في الدخول، وإقرار عقوبة تتناسب مع جسامة وخطورة هذا الاعتداء، فضلاً عن تشديد العقوبة في حالات محددة سواءً حسب قصد الجاني من دخوله، أو وفقاً للنتيجة الإجرامية المتحققة من الدخول أو التجاوز.

كما أننا نرى ضرورة تخصيص نص في قانوننا الليبي يجرم اصطناع المواقع والأنظمة الإلكترونية الخاصة بالدولة، أو انتحال شخصية مالكيها.

قائمة بأهم المراجع

أولاً– الكتب:

1– أحمد الضبع، إشكاليات مواجهة الإرهاب بين النظرية والتطبيق، الهيئة المصرية العامة للكتاب، 2019.

2– مدحت عبدالحليم رمضان، الحماية الجنائية للتجارة الإلكترونية "دراسة مقارنة"، دار النهضة العربية، 2012.

ثانياً– الرسائل العلمية:

1– أحمد طلعت عبدالحكيم، السياسة الجنائية في مواجهة جرائم تقنية المعلومات في ضوء القانون المصري رقم 175لسنة 2018، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 2022.

2– حسن فضيل خليف، جريمة الدخول غير المشروع إلى النظام المعلوماتي والتعدي على محتوياته" دراسة مقارنة"، رسالة ماجستير، جامعة جرش،2016.

ثالثاً– البحوث والمقالات:

1– إسلام مصطفى جمعة مصطفى، جريمة اختراق الأمن السيبراني وحماية استخدام البيانات والمعلومات في القانون المصري، المجلة القانونية" جامعة القاهرة"، 2022.

2– حورية محمد عبدالرحيم، مدى إمكانية تطبيق الإعفاء الوجوبي من عقوبة الجرائم المرتكبة ضد شخصية الدولة، مجلة كلية القانون جامعة طرابلس، العددين 7،8، 2023.

3- دلال لطيف الزبيدي، جريمة الاعتداء على المواقع الإلكترونية، مجلة جامعة بابل للعلوم الإنسانية، العدد 9، 2018.

4- رامي متولي القاضي، المواجهة الجنائية لجرائم تقنية المعلومات في التشريع المصري في ضوء أحكام القانون 175 لسنة 2018م. مقارناً بالمواثيق الدولية والتشريعات المقارن، مجلة البحوث القانونية والاقتصادية، العدد75، 2021.

5- رحاب علي عميش، الجريمة المعلوماتية: دراسة مقارنة بين القانونين الليبي والإماراتي، مجلة معهد دبي القضائي، ع 4، 2014.

6- ما شاء الله الزوي، الحماية الجنائية للبيانات الإلكترونية في القانون الليبي والمقارن، مجلة العلوم الشرعية والقانونية، العدد1، 2018.

7- موسى مسعود ارحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، بحث مقدم إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا – طرابلس،2009

8- وليد سمير المعدواي، مكافحة جرائم تقنية المعلومات والإرهاب الإلكتروني وفقاً لأحدث التشريعات المصرية، القيادة العامة لشرطة الشارقة، مركز بحوث الشرطة، العدد 114، 2020.

رابعاً- القوانين:

1- قانون رقم 4 لسنة 1990 بشأن النظام الوطني للمعلومات والتوثيق، منشور على الموقع:
https://security-legislation.ly/ar/1aw/101056

2- قانون رقم 22 لسنة 2010 بشأن الاتصالات منشور بالجريدة الرسمية، ع 10، في 28يناير 2010.

3- قانون الجرائم الإلكترونية الأردني رقم 17 لسنة2023، منشور بالجريدة الرسمية، ع 5874، في 2023/8/13.

4- قانون مكافحة الإرهاب رقم 94 لسنة 2015، منشور بالجريدة الرسمية، ع 33(مكرر)، في 15 أغسطس،2015

5- قانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات المصري، منشور بالجريدة الرسمية،ع 32مكرر(ج)، في 14 أغسطس 2018.

6- قانون رقم 5 لسنة 2022 بشأن مكافحة الجرائم الإلكترونية الليبي، منشور بالجريدة الرسمية،ع1، 2023/1/16.