Naif Arab University for Security Sciences
Arab Journal for Security Studies
المجلة العربية للدراسات الأمنية
https://journals.nauss.edu.sa/index.php/ajss
AJSS

The Criminal Liability for Illegal Access or Remaining in the Information System: A Study in Comparative Libyan Law

المسؤولية الجنائية للدخول أو البقاء غير المشروع في النظام المعلوماتي: دراسة في القانون الليبي المقارن

ما شاء الله عثمان الزوي
كلية القانون، جامعة بني غازي، ليبيا

Mashaallah Othman Elzwae
Faculty of Law, Benghazi University, Libya.

Received on 30 Apr. 2023, accepted on 20 Aug. 2023, available online on 12 Dec. 2023.

Abstract

Illegal access or remaining in the information system is considered one of the most serious crimes that the information system can face , as it serves as an important precursor to most crimes against the information system and the serious damages and risks that may ensue.

The problem of the study was represented in knowing the extent of the effectiveness of the provisions of the Libyan Cybercrime Law No. 5 of 2022 in confronting forms of illegal entry and illegal stay in the information system.

To achieve this, we have adopted the analytical and comparative approach in the study by analyzing the texts of the Libyan Cybercrime Law and comparing them with other legislation in order to identify its weaknesses and try to find appropriate solutions.The study revealed that the Libyan legislator - unlike the Egyptian legislator - limited the criminalization to the act of illegal entry without staying in the information system, despite its danger to the information system and information security, and the Libyan legislator punishes the perpetrator of the crime, whether he is a natural or legal person, with mild penalties, in addition to its omission of stipulating the severity of the penalty in the event of the availability of certain circumstances contrary to the comparative legislation.

Keywords: *security studies, information criminal, illegal entry crime, illegal survival crime.*

المستخلص

تُعدُّ جريمة الدخول أو البقاء غير المشروع إلى النظام المعلوماتي من أخطر الجرائم التي يتعرض لها النظام المعلوماتي، باعتبارها مقدمةً مهمةً لارتكاب أغلب الجرائم ضده، وما قد يترتب عليها من أضرار ومخاطر جسيمة.

وقد تمثلت إشكالية هذه الدراسة في معرفة مدى نجاعة نصوص قانون الجرائم الإلكترونية الليبي رقم 5 لسنة 2022 في مواجهة صور الدخول غير المشروع والبقاء غير المشروع في النظام المعلوماتي.

ولتحقيق ذلك اتبعنا في الدراسة المنهج التحليلي والمقارن، بتحليل نصوص قانون الجرائم الإلكترونية الليبي ومقارنتها بالتشريع المقارن؛ للوقوف على مواطن الضعف فيها، ومحاولة إيجاد الحلول المناسبة.

وقد أظهرت الدراسة أن المشرع الليبي - على خلاف المشرع المصري - اقتصر في التجريم على فعل الدخول دون البقاء غير المشروع في النظام المعلوماتي، رغم خطورته على النظام المعلوماتي والأمن المعلوماتي، كما أن المشرع الليبي يعاقب مرتكب الجريمة . سواء أكان شخصًا طبيعيًّا أو اعتباريًّا . بعقوبات ضعيفة، فضلًا عن إغفاله النصَّ على تشديد العقوبة في حالة توافر ظروف معينة، خلافًا للتشريع المقارن.

الكلمات المفتاحية: الدراسات الأمنية، المجرم المعلوماتي، جريمة الدخول غير المشروع، جريمة البقاء غير المشروع.

* Corresponding Author: *Mashaallah Othman Elzwae*
Email: msh_m80@yahoo.com
doi: 10.26735/JBNE1836

ونوصي المشرع الليبي بتجريم فعل البقاء في النظام المعلوماتي، والتوسُّع في المسؤولية الجنائية للشخص المعنوي، وتشديد العقوبات على الشخص الطبيعي والمعنوي.

We recommend that the Libyan legislator criminalize the act of staying in the information system, expanding the criminal responsibility of the legal person, and impose stricter penalties on both natural and legal persons.

1. المقدمة

يُعدُّ الأمن المعلوماتي من أهم الركائز التي يرتكز عليها قطاع التجارة والخدمات الإلكترونية بمختلف أنواعها، سواء في القطاع العام أو القطاع الخاص.

ولا شك في أن الأمن المعلوماتي يتطلب ضمان سرية وسلامة البيانات أو المعلومات التي يحويها النظام المعلوماتي والتي تتعلق إما بصاحب النظام المعلوماتي، سواء أكان شخصًا طبيعيًّا أو اعتباريًّا، أو تلك التي تتعلق بالعملاء أو المترددين على الجهات أو المؤسسات المختلفة.

إن انتهاك سرية أو سلامة البيانات أو المعلومات الشخصية يهدد قطاع الخدمات الإلكترونية؛ حيث قد يحجم الكثير من الأشخاص عن الإقبال على تلك الخدمات واستخدامها؛ وهو ما قد يصيب تلك الخدمات أو الاقتصاد في مقتل، ولا سيما تلك التي تعتمد بشكل كبير على الخدمات الإلكترونية التي بدأت في الظهور بوضوح كبديل عن الخدمات التقليدية بالنظر إلى مزاياها المختلفة.

وتتعاظم مخاطر انتهاك الأمن المعلوماتي عندما يتعلق الأمر بأسرار الدفاع للدولة، وتعرضها لمخاطر الإفشاء والاستخدام غير المشروع، وما قد يتعرض له مركز الدولة بين دول العالم المختلفة، وأثر ذلك على علاقتها مع غيرها من الدول.

ولذا يُعدُّ انتهاك سرية الأمن المعلوماتي بالدخول غير المشروع للنظام المعلوماتي من أهم المشكلات التي تحدث في الفضاء الإلكتروني؛ على اعتبار أن هذا الفعل يشكل خطوةً أولى وضروريةً لارتكاب معظم الجرائم الإلكترونية.

ولا غروَ فإن حرمة النظام المعلوماتي لا تقل أهميةً عن حرمة المنزل، فكلاهما محل طمأنينة للشخص ومستودع لأسراره المختلفة، ولا يتحقق انتهاك السرية أو السلامة في كلٍّ منهما إلا عن طريق الدخول غير المشروع أو غير المصرح به من صاحب الحق في ذلك، فالأولى ما هي إلا النسخة المستحدثة للثانية.

وقد تكون حرمة النظام المعلوماتي في عالمنا اليوم أهم من حرمة المنزل أو المكتب، ولا سيما بالنسبة للأشخاص المعنوية، وذلك بالنظر إلى أهمية المعلومات أو البيانات التي يحويها النظام المعلوماتي. وتحقيق الأمن المعلوماتي يستلزم أن يكون الدخول أو البقاء في النظام المعلوماتي مشروعًا أو مرخَّصًا به، سواء من حيث الزمان أو الموضوع؛ لذا نجد أن المشرع الجنائي يكفل الأمن المعلوماتي من خلال التجريم والعقاب لتلك الأفعال؛ متى تمت بشكلٍ غير مشروع، سواء وقعت من شخص طبيعي أو اعتباري، وذلك على الصعيدين المحلي والدولي.

وعليه فقد تدخل المشرع الليبي من خلال قانون الجرائم الإلكترونية الجديد رقم 5 لسنة 2022، وجرَّم فعل الدخول غير المشروع إلى النظام المعلوماتي، وقرر له حزمةً من العقوبات لردع مقترفي الجريمة، وهو ما عليه الحال كذلك في مصر من خلال القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات.

أهمية الدراسة

تتجلى أهمية الدراسة في خطورة أفعال الدخول أو البقاء غير المشروع للنظام المعلوماتي، وما يترتب عليها من آثار؛ حيث تتفق في خطورتها على الأمن المعلوماتي.

ولأهمية تعريف القارئ بهذه الجريمة وأركانها وعقوبتها . سواء للشخص الطبيعي أو الشخص المعنوي . وظروف التشديد فيها، ومخاطرها المختلفة، وكيفية معالجة المشرع الليبي لها.

إشكالية الدراسة

تتمثل إشكالية الدراسة في الوقوف على مدى نجاعة نصوص القانون رقم 5 لسنة 2022 بشأن الجرائم الإلكترونية في ليبيا ومواجهة الدخول أو البقاء غير المشروع في النظام المعلوماتي، بالمقارنة مع التشريع المقارن، ولا سيما في ظل حداثة تجريم هذا الفعل في ليبيا من خلال القانون رقم 5 لسنة 2022، وانعدام وجود دراسات متخصصة في هذا الموضوع في التشريع الليبي.

تساؤلات الدراسة

تثير الدراسة التساؤلات التالية:

هل وفق المشرع الليبي في توفير حماية أمن النظام المعلوماتي ضد مخاطر الدخول، أو البقاء غير المشروع في النظام المعلوماتي؟ وهل جرَّم المشرع الليبي جميع صور الدخول غير المشروع في النظام المعلوماتي؟ وهل جرَّم المشرع الليبي فعل البقاء غير المشروع في النظام المعلوماتي؟

وما مدى فاعلية العقوبات التي يقررها المشرع الليبي لحماية أمن النظام المعلوماتي من الدخول أو البقاء غير المشروع للنظام المعلوماتي، سواء بالنسبة للشخص الطبيعي أو الشخص المعنوي؟

أهداف الدراسة

تهدف الدراسة إلى التعريف بالنظام المعلوماتي، ومخاطر المساس بالأمن المعلوماتي، والتعرض لسرية البيانات أو المعلومات وسلامتها، والتعرف على موقف المشرع الليبي من الدخول أو البقاء غير المشروع في النظام المعلوماتي، سواء من حيث تجريم فعل الدخول، أو البقاء غير المشروع في النظام المعلوماتي، والتعريف بالدخول والبقاء غير المشروع للنظام المعلوماتي وكيفيته، وأركان هذه الجريمة، والعقوبات التي يقررها المشرع الليبي في حالة الدخول، أو البقاء غير المشروع للنظام المعلوماتي، سواء بالنسبة للشخص الطبيعي أو الشخص المعنوي، بالمقارنة مع التشريع المصري.

2. منهج الدراسة

تحقيقًا لما سبق فقد اتبعنا المنهج التحليلي والمقارن؛ وذلك بتحليل نصوص قانون الجرائم الإلكترونية الليبي المتعلقة بحماية أمن النظام المعلوماتي من الدخول، أو البقاء غير المشروع في النظام المعلوماتي، ومقارنتها مع التشريع المقارن لبيان أوجه الضعف أو القصور فيها في حماية النظام المعلوماتي من الدخول أو البقاء غير المشروع.

3. المطلب الأول: التعريف بالنظام المعلوماتي

سنحاول من خلال هذا الجزء من الدراسة التعرف على مفهوم النظام المعلوماتي لأهميته، كما يلي:

3. 1 التشريع الليبي

صدر عن المشرع الليبي عدة قوانين حاول من خلالها مواكبة التطور في قطاع تكنولوجيا الاتصالات والمعلومات، ولعل أهمها قانون الجرائم الإلكترونية رقم 5 لسنة 2022، غير أن هذا القانون كان قد خلا من بيان المقصود بالنظام المعلوماتي، وهو ما عليه الحال كذلك في قانون تنظيم الاتصالات رقم 22 لسنة 2010.

وفي المقابل فإن المادة الأولى من القانون رقم 6 لسنة 2022 بشأن المعاملات الإلكترونيةعرفت نظام المعلومات الإلكتروني بأنه «مجموعة برامج أو أجهزة معدة لإنشاء ومعالجة وإدارة البيانات الإلكترونية، أو غير ذلك من الإرشادات الإلكترونية المعبرة عن معلومة أو بيان مفهوم».

3. 2 التشريع المقارن

عرف المشرع المصري النظام المعلوماتي في القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات بأنه «مجموعة برامج وأدوات معدة لغرض إدارة ومعالجة البيانات والمعلومات أو تقديم خدمة معلوماتية» (الجريدة الرسمية، العدد 32 مكرر (ج)، بتاريخ 14 أغسطس 2018، ص. 3 وما بعدها).

أما في فرنسا فقد أغفل المشرع في القانون رقم 17 لسنة 1978 وضعَ تعريفٍ للنظام المعلوماتي (Gassin, 1995, p11).

وفي الإمارات العربية المتحدة خلا المرسوم بقانون اتحادي رقم 34 لسنة 2021 بشأن مكافحة الشائعات والجرائم الإلكترونية من تعريف النظام المعلوماتي، وفي المقابل عرفت المادة الأولى من المرسوم بقانون اتحادي رقم 46 لسنة 2021 بشأن المعاملات الإلكترونية وخدمات الثقة؛ النظام المعلوماتي بأنه «مجموعة برامج معلوماتية، ووسائل تقنية المعلومات المعدة لإنشاء ولمعالجة وإدارة وتخزين وتبادل المعلومات الإلكترونية وما شابه ذلك».

3. 3 الاتفاقيات الدولية

عرفت اتفاقية بودابست بشأن مكافحة الجرائم الإلكترونية لسنة 2001 نظام الكمبيوتر بأنه «أي جهاز أو مجموعة من الأجهزة المتصلة أو ذات الصلة التي يقوم واحد منها أو أكثر، وَفقًا لبرنامج، بالمعالجة الآلية للبيانات».

في حين عرفت اتفاقية الاتحاد الإفريقي بشأن الأمن المعلوماتي وحماية البيانات الشخصية لسنة 2014

النظام المعلوماتي بأنه «أي جهاز إلكتروني أو مغناطيسي أو بصري أو كهروكيميائي، أو أي جهاز عريض النطاق، معزول أو مترابط، يؤدي وظيفة تخزين البيانات، أو مرفق الاتصالات، هذه الاتصالات تتعلق مباشرة، أو تعمل بالاقتران مع جهاز أو أجهزة أخرى».

أما الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 فقد عرفت النظام المعلوماتي بأنه «مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات والمعلومات».

ويَبِين لنا من التعريفات السابقة أن المشرع الليبي لم يضع تعريفًا للنظام المعلوماتي، بخلاف الوضع في التشريعات السابقة؛ حيث أظهر المشرع المصري توسعًا في تعريف النظام المعلوماتي.

كما أن التعريف الوارد في قانون المعاملات الإلكترونية الليبي لا يتسم بالوضوح، وكان ينبغي أن يحدد الأعمال المتعلقة بالبيانات أو المعلومات، كأعمال النقل أو الحفظ أو التخزين أو الإرسال، وغيرها من الأعمال المتعلقة بالبيانات أو المعلومات في الفضاء الإلكتروني.

وكان يفضل حسب وجهة نظرنا لو أن المشرع وضع تعريفًا للنظام المعلوماتي، ولا سيما أنه يشكل محل الجريمة وركنها المفترض، على غرار الوضع في التشريع المصري والاتفاقيات سالفة الذكر، وألَّا يترك المسألة للاجتهاد الفقهي أو القضائي، على أن يكون هذا التعريف موسعًا للنظام المعلوماتي؛ وذلك من أجل توفير حماية أفضل للنظام المعلوماتي ضد مخاطر الدخول أو البقاء غير المشروع.

وعليه فإن النظام المعلوماتي - حسب وجهة نظرنا- هو أي برامج أو أدوات أو وسائل معدة لغرض معالجة البيانات أو المعلومات أو إرسالها واستقبالها، أو تخزينها أو نقلها أو إدارتها، وغير ذلك من الأعمال المرتبطة بالبيانات والمعلومات في الفضاء الإلكتروني باتصال أو بدونه.

4. المطلب الثاني: مخاطر الدخول أو البقاء في النظام المعلوماتي

يعد الدخول أو البقاء في النظام المعلوماتي بشكل غير مشروع من أخطر الجرائم التي تقع على النظم المعلوماتية؛ وذلك بالنظر إلى المخاطر التي تترتب على هذه الجريمة، وعليه سنحاول التعرض لأهم تلك المخاطر كما يلي:

4. 1 انتهاك سرية البيانات أو المعلومات

تؤكد معظم التشريعات الوضعية فضلًا عن السماوية حق الإنسان في السرية أو الحياة الخاصة؛ انطلاقًا من الميثاق العالمي لحقوق الإنسان إلى التشريعات المحلية للدول محل الدراسة، ومن ذلك الإعلان الدستوري في ليبيا الصادر سنة 2011، والمعدل مؤخرًا سنة 2014، الذي أكد السرية وحق الإنسان في حياته الخاصة، والأمر كذلك في الدستور المصري (انظر المادة 12 من الإعلان الدستوري الليبي، والمادة 57 من الدستور المصري لسنة 2014 وتعديلاته).

ويُعدُّ انتهاك سرية البيانات أو المعلومات من أهم المخاطر التي قد يتعرض لها النظام المعلوماتي نتيجة للدخول أو البقاء غير المشروع، وربما يكون هو الهدف الأول للجاني من الدخول غير المشروع إلى النظام المعلوماتي؛ حيث قد يعرض سرية البيانات أو معلومات المستخدم للذيوع أو الإفشاء، وما ينتج عنه من ضرر للمستخدم، سواء أكان ضررًا ماديًّا أم معنويًّا.

وتدقُّ المسألة أكثر إذا تعلق الأمر بما يعرف بالبيانات الشخصية الحساسة للمستخدم، وهي بيانات تتعلق بالأصل العرقي أو الإثني للشخص، أو ميوله الدينية أو النقابية أو السياسية، أو جنسه، أو صحته...إلى آخره (العيداني، 2018، ص. 120) بالنظر إلى طبيعتها وتعلقها بأمور دقيقة ومهمة للشخص، وما قد يترتب على الاطلاع عليها أو إفشائها من مخاطر وأضرار جسيمة، قد تصل إلى إفساد حياة الشخص أو أسرته. غير أن هذه المخاطر في البيئة الإلكترونية لا تتوقف عند الشخص الطبيعي فحسب، بل تمتد كذلك إلى الأشخاص المعنوية، سواء الأشخاص العامة أو الأشخاص الخاصة. بل لعل هذه المخاطر تتعاظم أكثر فأكثر حينما يتعلق الأمر ببيانات أو معلومات شخص من الأشخاص المعنوية العامة أو الخاصة، فبالنسبة للشخص المعنوي العام قد يعرض إفشاء المعلومات والبيانات ثقة الناس في الدولة إلى الاهتزاز وزوال الثقة بين الفرد والإدارة (عبد البر، 1998).

وقد شهدت الفترة الأخيرة تصاعد الهجمات الإلكترونية ضد الأنظمة المعلوماتية المتعلقة بالأشخاص المعنوية العامة للدولة، وذلك لتحقيق أغراض مختلفة، وهو ما يقتضي ضرورة توفير حماية للأنظمة المعلوماتية (Dreyfus، 2020).

وتتفاقم هذه المشكلة أكثر إذا تعلق الأمر بأسرار تمس الأمن القومي للدولة بمختلف صنوفه وأنواعه، وما يترتب على ذلك من أضرار جسيمة تلحق بالدولة وعلاقتها بغيرها من الدول من جراء ذلك (الحيوز، 2009).

أما ما يتعلق بالأشخاص المعنوية الخاصة، فقد يترتب على انتهاك سرية البيانات أو المعلومات إفشاء بيانات، أو معلومات تتعلق بأسرار تجارية تخص الشخص المعنوي، وقد تؤثر على وجوده أو استمراره بالمخالفة لقواعد المنافسة المشروعة (حجاج، 2021، ص. 553).

وقد قضت محكمة النقض المصرية بحجب موقعين إلكترونيين، وذكرت الأفعال المكونة للمنافسة غير المشروعة بأنها كل فعل يخالف العادات والأصول المرعيَّة في المعاملات التجارية، ويدخل في ذلك، على وجه الخصوص، الاعتداء على علامات الغير، أو على اسمه التجاري، وكذلك كل فعل أو ادعاء يكون من شأنه إحداث اللبس في المتجر أو في منتجاته، أو إضعاف الثقة في مالكه (نقض تجاري مصري 16 مايو 2022، الطعن رقم 8108 لسنة 91 قضائية).

في حين قضت محكمة النقض الفرنسيَّة بأن المنافسة غير المشروعة تتحقق بعدم الامتثال للوائح في ممارسة النشاط التجاري (Cass. Com., 17 mars 2021, no: 01-10.414).

وهذا فضلًا عن أعمال انتحال الهوية أو سرقتها بالنسبة للأشخاص المعنوية العامة والخاصة، المترتبة على الدخول غير المشروع إلى النظام المعلوماتي، والتي غالبًا ما تستهدف مكانة الشخص المعنوي من الناحية الاقتصادية، والنيل من اسمه في سوق العمل.

ولا شك في أن الاقتصاد الوطني للدولة سيتأثر بخروج تلك الأشخاص المعنوية الخاصة، بالنظر إلى الدور الذي كانت تقوم به في الاقتصاد؛ من أجل رفع كفاءة ومستوى المنتج، والحفاظ على استقرار الأسعار حمايةً للمستهلك.

4. 2 انتهاك سلامة البيانات والمعلومات

لا تقتصر مخاطر الدخول غير المشروع للنظام المعلوماتي على انتهاك سرية البيانات والمعلومات، بل قد يتعرض النظام المعلوماتي نتيجة للدخول أو البقاء غير المشروع إلى انتهاك سلامة البيانات أو المعلومات التي يحتويها النظام.

إذ إن الدخول والبقاء غير المشروع في النظام المعلوماتي لا يقتصر أثره في كثير من الحالات على مجرد الاطلاع غير المشروع على البيانات أو المعلومات أو إفشائها؛ بل قد يترتب على ذلك تعريض سلامة البيانات والمعلومات للخطر. ويلاحظ أن انتهاك البيانات الشخصية هو انتهاك أمني يؤدي إلى فقدان أو تدمير أو تغيير أو الكشف عن البيانات المعالجة (Rouge, 2021) وغيرها، كأعمال المحو الكامل أو الجزئي للبيانات والمعلومات، أو السرقة أو الإتلاف أو التلاعب والتعديل غير المشروع في تلك البيانات أو المعلومات، سواء بالحذف، أو الإضافة، إلى جانب النقل غير المشروع للبيانات والمعلومات.

إذ يستهدف الجاني سلامة البيانات أو المعلومات التي يحتويها النظام المعلوماتي من الدخول أو البقاء غير المشروع، بتخريب النظام المعلوماتي عن طريق إرباك عمل النظام المعلوماتي (رمضان، 2001، ص. 54).

وقد يحدث ذلك لأسباب مختلفة، إما لغرض الانتقام والتشفي من قبل الجاني، أو لتحقيق مكاسب مادية، أو إخفاء الحقيقة في حالات معينة، أو الهروب من العدالة الجنائية بإخفاء الأدلة، أو لإثبات قدرات الجاني وخبرته، وفي المقابل إثبات عجز مشغل النظام المعلوماتي وعدم قدرته على تأمين النظام المعلوماتي من الناحية الفنية أو التقنية.

وفيما يتعلق بمحو البيانات أو المعلومات فقد يتحقق ذلك بشكل جزئي أو كلي، بإزالة البيانات أو المعلومات من على الدعامة أو الملف المثبتة عليه بالطرق الإلكترونية (عبد الإله، 2007، ص. 70) بحيث يتعذر العثور عليها أو استخدامها في المستقبل.

أما سرقة البيانات والمعلومات فتتحقق بأن يأخذ الجاني نسخة من تلك البيانات والمعلومات المثبتة على الدعامة الإلكترونية وإدخالها في حيازته دون التعرض لتلك البيانات أو المعلومات بالإتلاف أو غيره، أو أن يقوم بنقلها من على الدعامة أو الملف المثبتة عليه ومحوها أو إتلافها؛ حيث وجدت على نظام المجني عليه.

في حين أن الإتلاف للبيانات أو المعلومات يتحقق بأي فعل يقوم به الجاني، ويترتب عليه عدم صلاحية تلك البيانات أو المعلومات للاستخدام، كأن يكون ملف البيانات أو المعلومات موجودًا، ولكن لا يمكن على الإطلاق معرفة مضمون البيانات أو المعلومات وما شابه ذلك.

أما التعديل بالحذف والإضافة، فيعني أي عمل يقوم به الجاني، ويترتب عليه التعديل في حقيقة تلك البيانات أو المعلومات، وأن تكون مخالفة للواقع (قارة، 2006، ص. 122) كالتغيير في أسماء الأشخاص المختزنة في النظام المعلوماتي، أو صفاتهم أو مراكزهم، عن طريق الحذف أو الإضافة... إلى آخره.

ويتحقق النقل بأن يقوم الجاني بإرسال البيانات أو المعلومات إلى جهات مختلفة، سواء داخل البلاد أو خارجها، كما يستوي أن يكون النقل كليًا أو جزئيًا، أو أن يكون النقل إلى جهات يعرفها الجاني، أو لا يعرفها ولا تربطه بها أي مصلحة.

والجدير بالذكر أن الجاني في الأعمال السابقة قد يكون من العاملين لدى مشغل النظام المعلوماتي، أو من الذين على صلة به، أو من غيرهم، كما لا يشترط أن تتم الأفعال السابقة في وجود اتصال أو إنترنت أو بدونه.

5. المطلب الثالث: جريمة الدخول غير المشروع في النظام المعلوماتي

5. 1 الدخول غير المشروع

تقتضي طبيعة الدخول أن هذا الفعل لا يمكن أن يتحقق إلا عن طريق فعل إيجابي، ولا يمكن أن يتحقق بطريقة سلبية، أو عن طريق الامتناع.

إن هذه الجريمة تعدُّ من الجرائم الشكلية التي لا يتطلب لقيامها تحقق نتيجة معينة ووقتية لها آثار مستمرة، ولا يتطلب في القائم بها صفة معينة (حمودي، 2016).

ويتحقق الدخول غير المصرح به في جميع الأحوال التي يدخل فيها الجاني إلى النظام المعلوماتي بمختلف الطرق (المومني، 2008، ص. 158) كاستخدام الوسائل التقنية، كالفيروسات أو البرامج الخبيثة (بطيحي، 2019) أو الرسائل التي تتضمن روابط اختراق للنظام المعلوماتي (Salagnon، 2022) والتي يكون من شأنها كسر نظام الحماية والدخول إلى النظام المعلوماتي، أو استخدام كلمة مرور النظام بشكل غير مشروع، ويستوي في ذلك الدخول لكامل النظام أو جزء منه (عباس، 2017) على أن يكون ذلك بطبيعة الحال بدون إذن من صاحب السلطة على النظام.

وهذا يقتضي بطبيعة الحال أن يكون الدخول على هذا النظام محظورًا على الجمهور، ويقتصر الدخول عليه للأشخاص المرخص لهم بذلك، أما إذا كان النظام من النظم المعلوماتية المفتوحة والمتاحة للاستخدام، أو الاطلاع من الجميع، فإن الدخول بدون إذن لا يشكل جريمة، ولا يعد دخولًا غير مشروع للنظام المعلوماتي.

كما هو الحال بالنسبة للأنظمة المفتوحة لمترددي النوادي الرياضية أو الترفيهية، أو تلك الموجودة في مكان العمل أو المؤسسات التعليمية المتاحة للاستخدام من قبل الجميع.

وقضت محكمة النقض الفرنسية بأن لا جريمة في حق من يستفيد من حقوق الوصول إلى البيانات وتعديلها ما دام لم يقم بإخفائها عن باقي مستخدمي النظام المعلوماتي (Cass,Crim7 janvier 2020, N° de pourvoi: 18-84.755).

ولا يشترط لقيام الجريمة أن تكون المعلومات أو البيانات التي يحتويها النظام المعلوماتي سرية، فتقوم الجريمة ولو كانت المعلومات أو البيانات غير سرية (Bitton،2020)؛ حيث إن المشرع يقرر الحماية للنظام ذاته، وليس للبيانات أو المعلومات التي تكون محمية بنصوص أخرى.

ولكن هل عدم وجود حماية تقنية للنظام المعلوماتي يعني أنه متاح للجميع دون إذن، ولا يتمتع بالحماية القانونية؟

لم ينص المشرع صراحة لقيام الجريمة أن يكون النظام محميًّا بالوسائل الفنية أو التقنية، وسكت المشرع عن هذه المسألة.

ويذهب البعض إلى أن الحماية تقتصر على النظم المعلوماتية المعززة بأساليب حماية فنية ضد الدخول غير المشروع، على اعتبار أن القانون لا يوفر حماية إلا لمن اتخذ الحيطة والحذر لحماية النظام، ما يدل على نيته في عدم السماح بالدخول للنظام بدون إذن، وهذا ما يقتضيه المنطق والعدالة. (الهيتي، 2007)

ويرى الباحث أنه لئن كان وجود كلمة مرور أو قفل للنظام يدل على أن صاحب السلطة على النظام يحظر دخوله بدون إذن منه، فإن عدم وجود كلمة مرور لا تعني بالضرورة أنه متاح، أو يسمح للغير بدخوله بدون إذن، فعدم وجود كلمة مرور قد يكون سببه أن النظام تم اختراقه دون انتباه من صاحبه، أو عدم قدرته على وضع كلمة مرور...إلى آخره.

وعليه فإن الأمر يقاس حسب قصد صاحب النظام، وليس بالنظر إلى وجود كلمة المرور من عدمها، ويمكن مقاربة ذلك على المنزل، فحرمة المنزل مصونة حتى ولو كان باب المنزل بدون قفل، بل حتى ولو كان من غير باب، فالدخول للمنزل محظور قانونًا إلا بإذن صاحبه أو في الأحوال التي يجيزها القانون.

كما أن النص التشريعي- كما سبق القول - ورد عامًّا دون اشتراط وجود وسائل حماية فنية أو تقنية للنظام، ومن ثم لا محل لتقييد عموم النص، إلا بنص يُقيد، والقول بخلاف ذلك يجافي التفسير المنطقي والسليم للنص.

5. 2 مدى استلزام القصد الجنائي في الدخول إلى النظام المعلوماتي

لئن كان المشرع الليبي لم ينص صراحة في قانون الجرائم الإلكترونية على تطلب القصد الجنائي لقيام الجريمة؛ حيث قضت المادة 11 من القانون 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، أو بما يخالف التصريح»، إلا أن ذلك يفهم بداهة وَفقًا للقواعد العامة في قانون العقوبات؛ حيث إن الجنح لا عقاب عليها إذا وقعت عن طريق الخطأ إلا إذا نص المشرع على ذلك صراحة، وهو ما لم يفعله المشرع (المادة 62 من قانون العقوبات الليبي).

وعليه فإن جريمة الدخول غير المشروع في القانون الليبي تعد من الجرائم العمدية، ولا محل لقيامها إذا وقعت عن طريق الخطأ.

وعلى خلاف ذلك نجد أن المشرع المصري في المادة 14 من القانون رقم 175 لسنة 2018 نصَّ على «كل من دخل عمدًا، أو دخل بخطأ غير عمدي وبقي بدون وجه حق، على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه» ويفهم من ذلك أن المشرع المصري يجرم الدخول العمدي وغير العمدي للنظام المعلوماتي، وغاية الأمر أن المشرع المصري يتطلب للعقاب على الدخول غير العمدي أن يقترن ببقاء الجاني في النظام المعلوماتي.

أضف إلى ذلك أن الدخول عن طريق الخطأ إلى النظام يترتب عليه ذات النتائج التي يمكن أن تترتب على الدخول المتعمد، وهي الاطلاع أو الإفشاء غير المشروع للبيانات أو المعلومات أو إتلافها أو نقلها...إلى آخره.

وعليه فمن الصواب في نظرنا الاتجاه السابق للمشرع المصري، وكان يتعين على المشرع الليبي الأخذ بنهج المشرع المصري في هذا الشأن.

5. 3 ربط تجريم الدخول بتوافر قصد جنائي خاص

لم يتطلب المشرع في التشريعين الليبي من خلال المادة 11 والمصري من خلال المادة 14 لتجريم الدخول للنظام المعلوماتي؛ أن يكون الدخول قد تم لتحقيق غاية معينة أي قصد معين.

وحسنًا فعل المشرع بذلك من عدم ربط تجريم الدخول غير المشروع إلى النظام بتوافر قصد خاص، لأنه ينطوي على تضييق غير مبرر للنص، ولعدم استيعابه للحالات التي يتم فيها الدخول غير المشروع للنظام المعلوماتي بدون توفر القصد الخاص.

ومن الجدير الإشارة إلى أن المشرعين جعلا القصد من الدخول ظرفًا مشددًا للعقوبة وليس عنصرًا لازمًا لقيام الجريمة، ونعني بذلك أن يكون فعل الدخول في التشريع الليبي قد تم بقصد إلغاء أو حذف أو إضافة أوتدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو نقل أو نسخ بيانات، أوتعطيل عمل نظام معلومات، أو تغيير موقع إلكتروني أو إلغائه أو إتلافه أو تعديل محتوياته، أوانتحال شخصية مالكه.

أما في التشريع المصري فيشترط أن يكون الفعل قد تم بقصد الإخلال بالنظام العام، أو تعريض سلامة المجتمع وأمنه للخطر، أو الإضرار بالأمن القومى للبلاد أو بمركزها الاقتصادى، أو منع أو عرقلة ممارسة السلطات العامة لأعمالها، أو تعطيل أحكام الدستور أو القوانين أو اللوائح، أو الإضرار بالوحدة الوطنية والسلام الاجتماعى.

ويلاحظ أن كلا المشرعين استخدم كلمة «الدخول» وقد أغفلا مصطلح الاتصال، ونظن أن هذا المصطلح الأخير كان ينبغي النصُّ عليه للابتعاد عن المشكلات الفنية التي قد يثيرها مصطلح الدخول، إلى جانب أن الدخول قد لا يتطلب الاتصال بالإنترنت، أما الاتصال؛ فيتطلب حتمًا استخدام الإنترنت أو أي وسيلة اتصال أخرى كالإنترانت وغيرها من الوسائل، كما أن مصطلح الاتصال بلا شك يستوعب حالات التجسس على المعلومات والبيانات التي يحويها النظام المعلوماتي دون تحقق الدخول في حال تم ذلك بأي وسيلة كانت.

وغني عن البيان أن الجريمة تقوم بغض النظر عن الباعث على ارتكابها؛ إذ يستوي أن يكون الباعث شريفًا أو غير شريف، وعلى هذا الأساس أدانت محكمة النقض الفرنسيَّة صحفيًا نشر على صفحته ثغرات اختراق أمن نظام معلوماتي، رغم أنه فعل ذلك لإطلاع الجمهور على الثغرات الأمنيَّة والحصول على سبق صحفي (Cass. Crim 27 Oct.2009, n°09-82.346).

5. 4 تجاوز حدود الدخول المصرح به

قد يحدث أن يكون الجاني قد دخل إلى النظام بإذن من صاحب السلطة عليه إلا أنه تجاوز حدود الدخول من حيث الزمان أو الموضوع (إبراهيم، 2015).

5. 5 تجاوز حدود الدخول من حيث الزمن

قد يحدث أن يكون الجاني قد تحصل على الموافقة بالدخول إلا أنه تجاوز حدود هذا الدخول من حيث الزمان، ويذهب البعض إلى أن تجاوز حدود الدخول يتحقق عن طريق التجاوز من حيث الموضوع لا من حيث الزمن (عباوي، 2016).

ونرى أنه يتحقق تجاوز حدود الدخول من حيث الوقت، كأن يكون قد سمح له بالدخول مرةً واحدةً فقط إلا أنه أعاد الدخول أكثر من مرة خلافًا للمرة التي سمح له فيها بالدخول، بحيث تمكن من الاطلاع على رسائل أو معلومات وصلت في نفس الوقت إلى النظام. ويتحقق ذلك أيضًا في الحالة التي يسمح بها للشخص بالدخول لمدة معينة، إلا أنه يتجاوز هذه المدة بما يخالف الإذن.

5. 6 تجاوز حدود الدخول من حيث الموضوع

قد يسمح صاحب السلطة على النظام لأحد الأشخاص بالدخول إلى جزء معين للاطلاع على ما يحتويه من ملفات دون غيره، إلا أنه يتجاوز حدود هذا الإذن، ويدخل على ملفات أخرى بالمخالفة لحدود الإذن الممنوح له.

ولا شك في أن الدخول في الحالات السابقة وإن كان قد تم بموافقة أو إذن صاحب السلطة على النظام، فإنه يبقى دخولًا غير مشروع؛ لأنه خالف حدود الإذن أو الموافقة، وتتحقق من خلالها علة تجريم المشرع للدخول غير المشروع للنظام.

5. 7 الموقف التشريعي من تجاوز حدود الدخول

أكد المشرع المصري صراحة من خلال المادة 15 من قانون مكافحة جرائم تقنية المعلومات على حالة تجاوز حدود الدخول المصرح به، أما في ليبيا فيفهم من صياغة المادة 11 من قانون الجرائم الإلكترونية أنها تتناول حالة تجاوز حدود الدخول المصرح به؛ حيث نصَّت على أنه «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، أو بما يخالف التصريح».

وعليه يفهم من عبارة «بما يخالف التصريح» أنها تتناول حالة تجاوز حدود الدخول للنظام المعلوماتي، بمعنى أن يدخل الشخص للنظام المعلوماتي بطريقة مخالفة للتصريح، سواء من حيث الزمان أو الموضوع.

وحسنًا فعل المشرع بذلك على اعتبار أنه يوفر حماية أفضل للنظام المعلوماتي ضد مخاطر الدخول غير المشروع؛ حيث يستوعب كافة صور الدخول غير المشروع للنظام المعلوماتي.

5. 8 تجريم فعل البقاء غير المشروع في النظام المعلوماتي

لا يقل فعل البقاء خطورة عن فعل الدخول غير المشروع، وقد اختلفت السياسة التجريمة بشأنه، وهو ما سنحاول بيانه كما يلي:

5. 9 مفهوم البقاء غير المشروع في النظام المعلوماتي

فعل البقاء يشكل جريمةً شكليةً ومستمرةً (ابن مسعود، 2017، ص. 486) ويتحقق البقاء غير المشروع في جميع الأحوال التي يبقى فيها الشخص داخل النظام المعلوماتي بالمخالفة لإذن من صاحب السلطة على النظام المعلوماتي أو بدونه.

ولا مشكلة إذا كان الدخول منذ البداية غير مشروع، فلا ضرر من عدم تجريم فعل البقاء، وإنما تظهر المشكلة عندما يكون دخول الشخص قد تحقق بشكل مشروع، بمعنى أن لديه إذنًا أو تصريحًا بالدخول دون البقاء، ففي هذه الحالة تظهر أهمية تجريم فعل البقاء بشكل مستقل عن فعل الدخول.

ومن صور البقاء غير المشروع أن يمتنع الشخص عمدًا عن الخروج من النظام بعد دخوله بشكل مشروع، رغم التنبيه عليه بعدم البقاء، كأن يكون الغرض من السماح له بالدخول مجرد الاطلاع على بعض المعلومات، وأن يخرج بعد ذلك على الفور، إلا أنه يفضل البقاء، أو أن يتظاهر بالخروج، ويظل قابعًا في النظام ولا يخرج منه؛ لتحقيق أغراض مختلفة.

ويستوي أن يكون البقاء قد تم باستخدام العنف أو التهديد أو الحيلة... إلى آخره؛ إذ إن البقاء غير المشروع في النظام المعلوماتي يتحقق متى تم ضد إرادة صاحب السلطة على النظام.

ثانيًا: الموقف التشريعي من البقاء غير المشروع في النظام المعلوماتي

ورد النصُّ على تجريم هذه الصورة لدى المشرع المصري من خلال المادة 14، في حين أغفل المشرع الليبي النصَّ على هذه الصورة رغم خطورتها.

ولعل الصواب ما ذهب إليه المشرع المصري؛ وذلك لخطورة فعل البقاء الذي لا تقل خطورته عن فعل الدخول غير المشروع؛ إذ يؤدي إلى تحقيق ذات العلة التي من أجلها جرَّم المشرع فعل الدخول غير المشروع إلى النظام.

إن النصوص الحالية في التشريع الليبي بلا شك لا تستوعب حالة البقاء غير المشروع، سواء سبقه دخول غير مشروع أو دخول مشروع، وهذا ما يتفق مع الفهم والتفسير الصحيح للنصوص الحالية.

وتجدر الإشارة إلى أن هذه الصورة قد ورد النصُّ عليها صراحةً في المادة 29 من اتفاقية الاتحاد الإفريقي للأمن المعلوماتي وحماية البيانات الشخصية، وكذلك المادة السادسة من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

6. المطلب الرابع: عقوبة الدخول أو البقاء في النظام المعلوماتي

6. 1 الفرع الأول: عقوبة الشخص الطبيعي

يعاقب المشرع في التشريعين محل الدراسة على الجريمة بعقوبات أصلية إلى جانب عقوبة المصادرة، وهو ما سنحاول بيانه كما يلي:

6. 2 العقوبات الأصلية

عقوبة الجريمة في صورتها البسيطة

يعاقب المشرع الليبي من خلال المادة 12 من قانون الجرائم الإلكترونية على الجريمة في صورتها البسيطة بعقوبة الحبس مدة لا تزيد على سنة، أو الغرامة التي لا تقل عن 100 دينار، ولا تزيد على 500 دينار، أو بالعقوبتين معًا.

أما المشرع المصري فيعاقب على الجريمة من خلال المادة 14 من قانون مكافحة جرائم تقنية المعلومات بعقوبة الحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه، ولا تزيد على مائة ألف جنيه، أو بإحدى هاتين العقوبتين.

وعليه فإن المشرع قد منح القاضي سلطةً تقديريةً في اختيار العقوبة المناسبة باختيار إحدى العقوبتين أو الجمع بينهما، وحسنًا فعل المشرع بذلك تماشيًا مع حسن السياسة الجنائية والتفريد العقابي.

غير أنه يتضح لنا مما سبق ضعف العقوبة المقررة في التشريع الليبي من حيث مقدارها، ونظن أن المشرع المصري كان أكثر توفيقًا من المشرع الليبي؛ إذ إن العقوبات الواردة في التشريع الليبي لا تتناسب ألبتة مع خطورة الفعل، وما قد يترتب عليه من آثار، ومن المعلوم أنه ينبغي أن يكون هناك تناسب بين الفعل والعقوبة؛ حتى تكون العقوبة أكثر ردعًا.

6. 3 عقوبة الجريمة في صورتها المشددة

يشدد المشرع الليبي وَفقًا للمادة 12 من قانون الجرائم الإلكترونية العقوبة، بحيث تكون الحبس مدة لا تقل عن سنة، أو غرامة لا تقل عن 500 دينار ولا تزيد على 5000 دينار، أو إحدى هاتين العقوبتين إذا كان الدخول بقصد إلغاء أو حذف أو إضافة أوتدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو نقل أو نسخ بيانات، أو تعطيل عمل نظام معلومات، أو تغيير موقع إلكتروني، أو إلغائه أو إتلافه، أو تعديل محتوياته، أوانتحال شخصية مالكه.

وتكون العقوبة السجن والغرامة التي لا تقل عن 10,000 عشرة آلاف دينار إذا نجم عن الدخول إعاقة عمل النظام المعلوماتي، أو تعطيل الشبكة المعلوماتية أو عمل الموقع الإلكتروني، أو إفساد المحتويات.

وفي مصر يشدد المشرع العقوبة إذا نتج عن الدخول إتلاف أو محو أو تغيير أو نسخ، أو إعادة نشر للبيانات أو المعلومات الموجودة على النظام المعلوماتي، وتكون العقوبة الحبس مدة لا تقل عن سنتين، وغرامة لا تقل عن مائة ألف جنيه، ولا تجاوز مئتي ألف جنيه، أو

بإحدى هاتين العقوبتين. كما يشدد المشرع المصري العقوبة وَفقًا للمادة 14 من قانون مكافحة جرائم تقنية المعلومات أكثر، بحيث تكون السجن المشدد إذا كانت الجريمة قد ارتكبت بغرض الإخلال بالنظام العام أو تعريض سلامة المجتمع وأمنه للخطر، أو الإضرار بالأمن القومى للبلاد، أو بمركزها الاقتصادى، أو منع أو عرقلة ممارسة السلطات العامة لأعمالها، أو تعطيل أحكام الدستور أو القوانين أو اللوائح، أو الإضرار بالوحدة الوطنية والسلام الاجتماعى.

ويفهم مما سبق أن المشرع الليبي لا يتطلب تحقق نتيجة معينة لتشديد العقوبة، وإنما يكفي أن يكون الفعل قد تم بقصد تحقيق نتيجة معينة، خلافًا للمشرع المصري الذي يتطلب لتشديد العقوبة أن ينتج عن الفعل نتيجة معينة على النحو السابق.

ونظن أن المشرع الليبي كان أكثر توفيقًا من المشرع المصري من هذه الناحية، غير أنه ومع ذلك نرى أن المشرع المصري كان أكثر توفيقًا من المشرع الليبي في العقوبات المقررة، على اعتبار أن العقوبة الواردة في التشريع الليبي حتى في حالة تشديد العقوبة لا تزال ضعيفة، ولا تتناسب مع خطورة الفعل، وما قد يترتب عليه من مخاطر أو أضرار.

إضافة إلى أن المشرع الليبي أغفل النصَّ على العديد من ظروف التشديد الواردة في التشريع المصري على النحو السابق بيانه.

ومن ناحية أخرى نرى أنه من الأفضل أن تكون عقوبة الحبس وجوبيَّة في هذه الحالات؛ وذلك بالنظر إلى خطورة الجريمة والآثار المترتبة عليها، خلافًا للحالة الأولى.

6. 4 عدم النصِّ على بعض ظروف التشديد

أغفل المشرع الليبي تشديد العقوبة عند توافر العديد من الظروف، كما في الحالات التي فيها يقع الفعل من أحد العاملين في تلك الجهات أو قصد ارتكاب جريمة أخرى (خليفة، 2018، ص. 69-70) أو تلك التي يكون فيها الدخول إلى نظام معلوماتي تابع للدولة (المادة 323-1 من قانون العقوبات الفرنسي) أو أحد الأجهزة الأمنية بها، أو عن طريق جماعة منظمة، أو استغلال الجاني لسلطته ونفوذه في ارتكاب الجريمة، فمن غير المنطقي عدم تشديد المشرع الليبي للعقوبة في مثل هذه الحالات، وجعلها ذات عقوبة الفعل بدون توافر هذه الظروف.

ولكن هل يشدد المشرع الليبي والمصري من العقوبة إذا ترتب على الجريمة تعريض الآخرين لخطر الوفاة، أو الإصابة بعاهة أو تشويه، أو منع مواجهة كارثة تشكل خطرًا على سلامة الأشخاص؟

أغفل المشرع في التشريعين الليبي والمصري النصَّ على تشديد العقوبة في مثل هذه الحالات، وفي المقابل فقد تدخل المشرع الفرنسي حديثًا بموجب القانون رقم 22 لسنة 2023) (Loi n° 2023-22 du 24 janvier 2023 (d'orientation et de programmation du ministère de l'intérieur.

وأضاف إلى قانون العقوبات المادة 323-4-2 ونصَّ على تشديد العقوبة في مثل هذه الحالات، وذلك بأن يترتب على الجريمة تعريض الآخرين لخطر مباشر كالوفاة أو تشويه أو إعاقة دائمة، أو عرقلة خدمات الإنقاذ التي تهدف إلى إنقاذ شخص من خطر وشيك، أو مواجهة كارثة تشكل خطرًا على سلامة الأشخاص.

وكان يتعين على المشرع في التشريعين الليبي والمصري تشديد العقوبة في مثل هذه الحالات؛ وذلك نظرًا لخطورتها ولخطورة الجاني والجريمة، الأمر الذي يستدعي تشديد العقوبة.

6. 5 عقوبة الشروع في الجريمة

أغفل المشرع الليبي وضع نصٍّ خاصٍّ بعقوبة الشروع في الجرائم الإلكترونية في قانون الجرائم الإلكترونية، وهذا يعني خضوعها لقواعد قانون العقوبات التي تجعل من عقوبة الشروع أقل من عقوبة الجريمة التامة.

حيث تنص المادة 60 من قانون العقوبات على أن "يعاقب على الشروع في الجناية بالعقوبات الآتية إلا إذا نصَّ القانون على خلاف ذلك بالسجن المؤبد إذا كانت عقوبة الجناية الإعدام، وبالسجن الذي لا تقل مدته عن ثماني سنوات إذا كانت عقوبة الجناية السجن المؤبد، وفي الأحوال الأخرى يحكم بعقوبة السجن، مع خفض حديها إلى النصف.

أما المادة 61 من قانون العقوبات فتنص على أن «يعاقب على الشروع في الجنح بالعقوبات المقررة للجنحة الكاملة، مع خفض حديها إلى النصف».

ومن المعلوم فإنه وَفقًا للمادة 12 من قانون الجرائم الإلكترونية فإن المشرع قد يعاقب على جريمة الدخول غير المشروع بعقوبات جناية أو جنحة، حسب النتيجة المترتبة على الجريمة.

وفي المقابل نجد أن المادة 40 من قانون مكافحة جرائم تقنية المعلومات المصري تعاقب على الشروع بما لا يجاوز نصف الحد الأقصى للعقوبة المقررة للجريمة.

غير أن عقوبة الشروع في التشريعين الليبي والمصري أضعف من عقوبة الشروع في التشريع الفرنسي؛ حيث يسوِّي المشرع الفرنسي بين جريمة الدخول، أو البقاء في النظام أو الشروع فيها من حيث العقوبة (المادة 323-7 من قانون العقوبات الفرنسي).

لذلك كان يتعين على المشرع الليبي النصُّ صراحةً على عقوبة الشروع في قانون الجرائم الإلكترونية، وجعلها هي ذاتها عقوبة الجريمة التامة.

6. 6 المصادرة في التشريع الليبي

تقرر المادة 50 من قانون الجرائم الإلكترونية أنه مع عدم الإخلال بحقوق الغير حسن النية يحكم في جميع الأحوال بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب الجريمة أو الأموال المتحصلة منها.

6. 7 المصادرة في التشريع المقارن

نصَّ المشرع المصري على عقوبات تبعية تطبق عند ارتكاب الجريمة، فالمادة 38 تقرر أنه مع عدم الإخلال بحقوق الغير حسن النية، على المحكمة في حالة الحكم بالإدانة، أن تقضي بمصادرة الأدوات والآلات والمعدات والأجهزة، مما لا يجوز حيازتها قانونًا، أو غيرها مما يكون قد استخدم فى ارتكاب الجريمة، أو سهل أو أسهم فى ارتكابها، كما تقرر المادة 39 من ذات القانون أنه يجوز للمحكمة إذا قضت بالإدانة على أحد الموظفين العموميين، لارتكابه الجريمة في أثناء تأديته لوظيفته؛ أن تقضي بعزله مؤقتًا من وظيفته، إلا فى الحالات المشار إليها فى المادة (34) من هذا القانون، فيكون العزل وجوبيًا (وهي حالات توافر ظروف التشديد).

ويتضح مما سبق أن المشرع الليبي كان موَفقًا عندما قرر المصادرة - في جميع الأحوال - للأجهزة والبرامج والوسائل المستخدمة في ارتكاب الجريمة أو الأموال المتحصلة منها، أي سواء كان الحكم الصادر بالبراءة أو الإدانة، وذلك كتدبير احترازي، في حين أن المشرع المصري لا يقرر المصادرة إلا عند الحكم بالإدانة كعقوبة تبعية، فضلًا عن أن المشرع المصري يوسِّع نطاق المصادرة؛ ليشمل ليس فقط المستخدمة في الجريمة، بل كذلك التي سهَّلت أو أسهمت في ارتكابها.

وتجدر الإشارة إلى أنه وعلى خلاف الوضع في التشريع المصري فقد أغفل المشرع الليبي النصَّ على عقوبة العزل، وذلك إذا قضت المحكمة بالإدانة على أحد الموظفين العموميين لارتكابه الجريمة في أثناء وبسبب تأديته لوظيفته.

فارتكاب الموظف العمومي للجريمة يجعله حقيقًا بتشديد العقوبة عليه وعزله من الوظيفة التي لم يحترمها وأخل بالثقة الممنوحة له.

6. 8 عقوبة الشخص المعنوي

عقوبة المسؤول عن الإدارة الفعليَّة للشخص المعنوي

خلت قواعد قانون العقوبات الليبي من تقرير مبدأ المسئولية الجنائية للشخص المعنوي بشكلٍ عام، وذلك تماشيًا مع الاتجاه التقليدي في تقرير المسؤولية الجنائية للشخص المعنوي؛ وذلك على خلاف الوضع في التشريعات المقارنة، مثل: التشريع الفرنسي والتشريع الجزائري... إلى آخره.

يقرر المشرع الليبي من خلال المادة 48 عقوبة الحبس مدة لا تقل عن سنة للمسؤول عن الإدارة الفعليَّة للشخص المعنوي؛ إذا ارتكبت الجريمة بواسطة أحد العاملين لديه باسمه ولصالحه، متى وقعت الجريمة بسبب إخلاله بواجبات وظيفته.

وهذا يعني عدم قيام المسؤولية في غير تلك الحالات، كأن تتم الجريمة لمصلحة الشخص المعنوي دون ارتكابها من أحد العاملين بالشخص المعنوي.. إلى آخره.

وفي المقابل تقرر المادة 36 من قانون مكافحة جرائم تقنية المعلومات في مصر معاقبة المسؤول عن الإدارة الفعلية للشخص المعنوي في الأحوال التي ترتكب فيها الجريمة باسم الشخص المعنوي ولحسابه، إذا ثبت علمه بالجريمة، أو سهل ارتكابها تحقيقًا لمصلحة له أو لغيره؛ بذات عقوبة الفاعل الأصلي.

يتضح لنا مما سبق أن المشرع المصري لم يتطلب لمعاقبة المسؤول عن الإدارة الفعلية للشخص المعنوي أن تكون الجريمة قد ارتكبت بواسطة أحد العاملين لدى الشخص المعنوي باسمه ولصالحه، وأن تكون الجريمة وقعت بسبب إخلاله بواجبات وظيفته.

بل اكتفى المشرع المصري لمعاقبة المسؤول عن الإدارة الفعلية للشخص المعنوي بثبوت علمه بالجريمة، أو تسهيل ارتكابها تحقيقًا لمصلحته أو مصلحة غيره، وهذا يعني أن المشرع المصري يوسِّع من نطاق مسئولية الشخص المسؤول عن الإدارة الفعليَّة، في حين يضيِّق المشرع الليبي من تلك المسؤولية.

فضلًا عن ذلك فإن المشرع المصري . وعلى النحو السابق بيانه، وخلافًا للمشرع الليبي - يتشدد في عقوبة المسؤول عن الإدارة الفعلية للشخص المعنوي، ويتضح ذلك من خلال مقدار العقوبات التي يقررها المشرع المصري.

ونظن أن المشرع المصري كان أكثر توفيقًا من المشرع الليبي في تقرير الأحكام السابقة، غير أن المشرع في التشريعين الليبي والمصري يتطلب لقيام مسؤولية الشخص المعنوي أن تكون الجريمة قد تمَّت باسم الشخص المعنوي ولحسابه، ومن ثم لا محل لقيام المسؤولية في الأحوال التي تتم فيها الجريمة لحساب الشخص المعنوي دون أن تتم باسمه، إلى غير ذلك من الحالات.

ويقرر المشرع المصري من خلال المادة 37 من قانون مكافحة جرائم تقنية المعلومات أنه لا يترتب على تقرير مسؤولية الإدارة الفعلية للشخص الاعتبارى استبعاد المسؤولية الجنائية للأشخاص الطبيعيين الفاعلين الأصليين أو الشركاء؛ عن ذات الوقائع التى تقوم بها الجريمة.

في حين أغفل المشرع الليبي في قانون الجرائم الإلكترونية النصَّ على ذلك صراحةً، ونرى أنه يتعين على المشرع الليبي تأكيد ذات الأحكام صراحةً في قانون الجرائم الإلكترونية، كي لا تكون مساءلة الشخص المعنوي مبررًا لعدم قيام مسؤولية الشخص الطبيعي.

ولا سيما أن هذا الحكم قد ورد النصُّ عليه صراحةً كذلك في المادة 20 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، والمادة 30 من اتفاقية الاتحاد الإفريقي للأمن المعلوماتي وحماية البيانات الشخصية، والمادة 12 من اتفاقية بودابست لمكافحة الجرائم الإلكترونية.

وتجدر الإشارة إلى أن المشرع الليبي توسَّع في نطاق المسؤولية الجنائية للشخص المعنوي في القانون رقم 6 لسنة 2022 بشأن المعاملات الإلكترونية على النحو الوارد في القانون رقم 5 لسنة 2022 بشأن الجرائم الإلكترونية؛ حيث تنص المادة 82 من قانون المعاملات الإلكترونية على أنه «مع عدم الإخلال بالمسؤولية الجنائية الشخصية لمرتكب الجريمة.يُعاقب الممثل القانوني للشخص الاعتباري العقوبات ذاتها المقررة عن الأفعال التي ترتكب بالمخالفة لأحكام هذا القانون، إذا ثبت أن إخلاله بواجبات وظيفته أسهم في وقوع الجريمة، ويكون الشخص الاعتباري مسؤولًا بالتضامن عما يحكم به من عقوبات مالية أو تعويضات إذا ارتكبت الجريمة لحسابه أو باسمه أو لصالحه».

إن الأحكام السابقة في المادة 82 لا تفي بالمطلوب في تقرير المسؤولية الجنائية للأشخاص المعنوية، إلا أنها توسع من نطاق المسؤولية الجنائية للشخص المعنوي خلافًا لقانون الجرائم الإلكترونية، ولعل التوسع في نطاق المسؤولية الجنائية للشخص المعنوي في قانون مكافحة الجرائم الإلكترونية أولى وأهم من قانون المعاملات الإلكترونية؛ وذلك بالنظر لخطورة الجرائم المنصوص عليها في هذا القانون، وأهمية المصالح والحقوق التي تمس بها تلك الجرائم، وذلك بالمقارنة مع حجم وطبيعة الجرائم التي نصَّ عليها قانون المعاملات الإلكترونية.

وعلى الرغم من تقارب صدور القانونين في التاريخ، وهو ما يفترض معه أن تكون سياسة المشرع واحدة تجاه تقرير المسؤولية الجنائية للشخص المعنوي، وألا تختلف المعايير في تقرير تلك المسؤولية؛ فإن المشرع الليبي انتهج سياسة جنائية دون معايير واضحة، تبرر سبب المغايرة في أحكام المسؤولية الجنائية للشخص المعنوي في قانون الجرائم الإلكترونية وقانون المعاملات الإلكترونية.

6. 9 عقوبة كيان الشخص المعنوي نفسه

حل الشخص المعنوي

يوجب المشرع الليبي على المحكمة أن تقضي بحل الشخص المعنوي، إذا ثبت لها أن الغرض الحقيقي من إنشائه هو ارتكاب جريمة من الجرائم الإلكترونية.

وفي المقابل يجعل المشرع المصري من حل الشخص المعنوي عقوبةً جوازيةً للمحكمة، إلى جانب إلغاء الترخيص في حالة العود إلى ارتكاب الجريمة.

ونظن أن المشرع المصري كان أكثر توفيقًا من المشرع الليبي في تقرير الأحكام السابقة؛ حيث إن المشرع الليبي وإن جعل عقوبة الحل وجوبية، غير أنه يقصرها على حالة واحده فقط دون غيرها، وهي حالة أن يكون القصد من إنشاء الشخص المعنوي ارتكاب جريمة من الجرائم الإلكترونية، ومن ثم لا تطبق العقوبة في الحالات الأخرى، كأن تكون الجريمة قد ارتكبت باسم الشخص المعنوي ولحسابه...إلى آخره.

6. 10 الوقف أو إلغاء الترخيص والغلق ونشر الحكم

أغفل المشرع الليبي تقرير عقوبة وقف الشخص المعنوي عن العمل لمدة أو مدد معينة، أو إلغاء الترخيص الممنوح للشخص المعنوي.

وفي المقابل يقرر المشرع المصري من خلال المادة 36 من قانون مكافحة جرائم تقنية المعلومات عقوبة الوقف مدة لا تزيد على سنة كعقوبة بسيطة للجريمة، وإلغاء الترخيص في أحوال العَوْد.

بالإضافة إلى ذلك فقد أغفل المشرع الليبي تقرير عقوبة نشر الحكم بالإدانة في قانون الجرائم الإلكترونية، وعلى خلاف ذلك يقرر المشرع المصري صراحةً عقوبة نشر الحكم بالإدانة على نفقة الشخص المعنوي.

وبالرجوع إلى القواعد العامة في قانون العقوبات الليبي نجد أن المشرع يقرر عقوبة نشر الحكم بالإدانة في أحوال معينة، ليس من ضمنها - بطبيعة الحال - جريمة الدخول أو البقاء في النظام المعلوماتي (المواد: 39، 340، 367 من قانون العقوبات الليبي).

ولا شك في أن نشر الحكم بالإدانة من العقوبات المهمة في تحقيق الردع بالنسبة للشخص المعنوي؛ إذ تصيب سمعة الشخص في بيئة العمل، ومن المعلوم أن الشخص المعنوي يعتمد كثيرًا على سمعته في بيئة العمل لجذب الزبائن أو العملاء.

وتجدر الإشارة إلى أنه قد ورد النصُّ على هذه العقوبة في المادة 31 من اتفاقية الاتحاد الإفريقي للأمن المعلوماتي وحماية البيانات الشخصية.

6. 11 العقوبات الأخرى

أغفل المشرع في التشريعين الليبي والمصري النصَّ على بعض العقوبات، منها عقوبة الغرامة على الشخص المعنوي نفسه ككيان مستقل، فعقوبة الغرامة هي الأمثل والأكثر ردعًا للشخص المعنوي، فالشخص المعنوي غالبًا ما يكون الهدف من تأسيسه تحقيق الربح، فيعامل بنقيض قصده أو هدفه، ومن ثم يكون الجزاء من جنس العمل.

ولذلك نجد أن المادة 31 من اتفاقية الاتحاد الإفريقي للأمن المعلوماتي وحماية البيانات الشخصية أكدت ضرورة أن تكون عقوبة الغرامة من ضمن العقوبات المقررة على الشخص المعنوي، وهو ما أكدته كذلك المادة 13 من اتفاقية بوادبست لمكافحة الجرائم الإلكترونية، والمادة 323-6 من قانون العقوبات الفرنسي.

فضلًا عن بعض العقوبات الأخرى التي نصَّ عليها المشرع في بعض التشريعات المقارنة، كعقوبة الحظر من مزاولة بعض الأنشطة، وحظر إصدار الشيكات، والحرمان من دعوة الجمهور إلى الادخار، والاستبعاد من الأسواق... إلى آخره (المواد 131-47 إلى 131-49 من قانون العقوبات الفرنسي).

ولا شك في أن هذه العقوبات مهمة في تحقيق الردع للشخص المعنوي؛ لكونها تمس بنشاطه وقدرته على العمل، وكان ينبغي للمشرع في التشريعين الليبي والمصري النصُّ عليها في إطار مكافحة الجرائم الإلكترونية.

ويلاحظ أن المشرع في التشريعين الليبي والمصري قد أغفل تشديد العقوبة بالنظر إلى صفة المجني عليه، وذلك بأن يكون من الأشخاص المعنوية العامة، ونظن أنه كان ينبغي للمشرع النصَّ على تشديد العقوبة في مثل هذه الحالات، فمن غير المنطقي ألا تشدد العقوبة في مثل هذه الحالات، وذلك بالنظر إلى الآثار المترتبة على الجريمة إذا ما قورنت بالاعتداء على الأشخاص المعنوية الخاصة أو الأفراد، وهذا ما يتفق مع التفريد العقابي وحسن السياسة الجنائية.

كما أن المشرع الليبي أغفل النص على تشديد العقوبة في الأحوال التي ترتكب فيها الجريمة لغرض الإخلال بالنظام العام أو تعريض سلامة المجتمع 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. ونظن أنه كان يتعين على المشرع الليبي النصُّ على تشديد العقوبة في مثل هذه الحالات؛ على اعتبار أن علة التشديد متوافرة، إعمالًا للتفريد العقابي.

كما تجدر الإشارة إلى أن المشرع الليبي قد جانبه الصواب - حسب وجهة نظرنا - بإغفاله النص على الإعفاء من العقوبة صراحة في قانون الجرائم الإلكترونية.

إن عدم النص صراحة على الإعفاء في قانون الجرائم الإلكترونية يعني الرجوع إلى القواعد العامة في قانون العقوبات، ونجد أن المشرع يقرر الإعفاء من العقوبة في جرائم معينة ليس من بينها الجريمة محل الدراسة.

وغني عن البيان أنه وَفقًا للقواعد العامة في قانون العقوبات (المادة 270) فإن المشرع الليبي يقرر الإعفاء من العقوبة في بعض الحالات؛ لوجود صلة القرابة، كالزوجة التي تساعد زوجها في الفرار من العدالة الجنائية.

وعلى خلاف الوضع في التشريع الليبي يقرر المشرع المصري صراحةً من خلال المادة 41 من قانون مكافحة جرائم تقنية المعلومات؛ الإعفاء من العقوبات وجوبيًا لكل من بادر من الجناة أو الشركاء إلى إبلاغ السلطات القضائية أو السلطات العامة بما يعلمه عنها قبل البدء فى تنفيذ الجريمة وقبل كشفها.

ومع ذلك يجوز 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 ضبط الأموال موضوع الجريمة، أو أعان أثناء البحث والتحقيق على كشف الحقيقة فيها، أو على القبض على مرتكبي جريمة أخرى مماثله لهذا النوع والخطورة (ولا يخل الإعفاء بوجوب الحكم برد المال المتحصل من الجريمة (المادة 41 من قانون مكافحة جرائم تقنية المعلومات المصري).

ولعله من الصواب في نظرنا ما ذهب إليه المشرع المصري من تقرير الإعفاء من العقوبة، على اعتبار أن ذلك من حسن السياسة الجنائية، وذلك للحيلولة دون تمام الجريمة أو الكشف عن مرتكبيها، ففي بعض الحالات قد يكون من الصعوبة الكشف عن الجريمة أو أشخاص مقترفيها إلا من خلال تعاون بعض المتهمين بارتكابها، خاصة وأن الجرائم الإلكترونية تتسم بصعوبة إثباتها في الكثير من الأحيان، وذلك بالنظر إلى بيئة وأساليب ارتكابها.

7. الخاتمة

تناولنا في هذا البحث موضوع السياسة الجنائية للمشرع الليبي في مكافحة الدخول أو البقاء غير المشروع في النظام المعلوماتي، وقد خلصنا من هذه الدراسة إلى مجموعة من النتائج والتوصيات:

7. 1 النتائج:

- كشفت الدراسة أن المشرع الليبي لم ينص على تجريم صورة البقاء غير المشروع في النظام المعلوماتي.
- أبانت الدراسة أن المشرع الليبي لا يجرِّم الدخول في صورة الخطأ غير العمدي، ويقتصر التجريم على الدخول العمدي فقط.
- كشفت الدراسة عن ضعف العقوبات التي يقررها المشرع الليبي لجريمة الدخول غير المشروع للنظام المعلوماتي، سواء في صورتها

البسيطة أو المشددة، أو في حالة الشروع، كما أغفل النص على الكثير من ظروف التشديد، وذلك خلافًا للوضع في التشريع المصري.

- أبانت الدراسة أن المشرع الليبي يضيق من نطاق مسؤولية المسؤول عن الإدارة الفعلية للشخص المعنوي؛ وذلك على خلاف الوضع في التشريع المصري، كما أن المشرع الليبي - ويجاريه في ذلك المشرع المصري - قد أغفل النص على العديد من العقوبات المهمة للشخص المعنوي التي نص عليها التشريع المقارن.

8. التوصيات:

- نقترح على المشرع الليبي تجريم فعل البقاء غير المشروع في النظام المعلوماتي؛ على اعتبار أن هذا الفعل لا يقل خطورة عن فعل الدخول غير المشروع للنظام المعلوماتي.
- نقترح على المشرع الليبي النص صراحة على تجريم فعل الدخول عن طريق الخطأ إلى النظام المعلوماتي، في الأحوال التي يبقى فيها الجاني في النظام المعلوماتي ويرفض الخروج منه، بالنظر إلى شيوع وقوع هذه الصورة في الفضاء الإلكتروني، وتترتب عليها نفس النتيجة المترتبة على فعل الدخول العمدي غير المشروع للنظام المعلوماتي.
- نأمل من المشرع الليبي رفع عقوبة الجريمة، سواء في صورتها البسيطة أو المشددة أو في حالة الشروع، بالإضافة إلى النص على بعض ظروف التشديد، ولا سيما تلك المتعلقة بالموظف العام عند ارتكابه الجريمة، والتوسيع من نطاق المسؤولية الجنائية للشخص المسؤول عن الإدارة الفعلية للشخص المعنوي، والتأكيد صراحة على أن مسؤولية المسؤول عن الإدارة الفعلية للشخص المعنوي لا تمنع من قيام مسؤولية الشخص الطبيعي المرتكب للوقائع محل الجريمة.
- حث المشرع الليبي على سرعة التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، والتوقيع ثم التصديق على اتفاقية الاتحاد الإفريقي للأمن السيبراني وحماية البيانات الشخصية.

الإفصاح عن تضارب المصالح

يعلن المؤلف أنه ليس لديه أي تضارب في المصالح للمقالة المنشورة.

الإفصاح عن تمويل البحث

يعلن (المؤلف) أن البحث المنشور لم يتلقَ منحة مالية من أية جهة تمويل في القطاعات العامة أو التجارية أو المؤسسات غير الربحية.

المصادر والمراجع

أولًا: المراجع العربية

إبراهيم، مدحت محمد عبد العزيز،(2015) الجرائم المعلوماتية الواقعة على النظام المعلوماتي، دار النهضة العربية، القاهرة، الطبعة الأولى.

بطيحي، نسمة (2019) جريمة الدخول أو البقاء غير المشروع إلى النظام المعلوماتي، مجلة الفقه القانوني والسياسي، المجلد 1، العدد 1.

حجاج، مليكة، (2021) الحماية الجزائية للأسرار التجارية في التشريع الجزائري، مجلة العلوم القانونية والاجتماعية، جامعة زيان عاشور - الجلفة، الجزائر، المجلد السادس، العدد الثالث.

حمودي، ناصر (2016)، الحماية الجنائية لنظم المعالجة الآلية للمعطيات في التشريع الجزائري، المجلة الأكاديمية للبحث القانوني، المجلد الرابع عشر، العدد الثاني.

الحيوز، محمد عودة (2009)، الجرائم الواقعة على أمن الدولة وجرائم الإرهاب، دار الثقافة للنشر والتوزيع، عمان - الأردن، الطبعة الأولى.

خليفة، محمد، (2007) الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة للنشر والتوزيع، الإسكندرية.

خليفة، محمد،(2018) دراسة نقدية لنصوص جرائم أنظمة المعالجة الآلية للمعطيات في قانون العقوبات الجزائري، المجلة النقدية للقانون والعلوم السياسية،المجلد الثالث عشر، العدد الأول.

رمضان، مدحت، (2001) الحماية الجنائية للتجارة الإلكترونية، (دراسة مقارنة)، دار النهضة العربية، القاهرة.

عباس، كريمة، (2017) جرائم المساس بأنظمة المعالجة الآلية للمعطيات، مجلة البيان للدراسات القانونية والسياسية، العدد الرابع، ديسمبر.

عباوي، نجاة،(2016) الاختلافات التشريعية في تجريم الدخول غير المصرح به إلى أنظمة المعلومات، مجلة القانون والعلوم السياسية، المجلد الثاني، العدد الأول.

عبد الإله، هلالي،(2007) اتفاقية بودابست لمكافحة الجرائم المعلوماتية، (معلقًا عليها)، دار النهضة العربية، القاهرة، الطبعة الأولى.

عبد البر، فاروق، (1998) دور مجلس الدولة المصري في حماية حريات الموظف العام، بدون ناشر.

العيداني، محمد يوسف زروق، (2018) حماية المعطيات الشخصية في الجزائر على ضوء القانون رقم 18-07 (المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة البيانات ذات الطابع الشخصي)، مجلة معالم للدراسات القانونية والسياسية، العدد الخامس.

قارة، آمال (2006)، الحماية الجزائية للمعلوماتية في القانون الجزائري، دار هومة، الجزائر.

ابن مسعود،أحمد، (2017)، جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري، مجلة الحقوق والعلوم الإنسانية، المجلد العاشر، العدد الأول.

المومني، نهلا عبد القادر،(2008) الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان - الأردن، الطبعة الأولى.

الهيتي، محمد حماد مرهج، (2014) الجريمة المعلوماتية نماذج من تطبيقاتها، دراسة مقارنة في التشريع الإماراتي والسعودي والبحريني والقطري والعماني، دار الكتب القانونية، القاهرة.

ثانيًا: المراجع الأجنبية

BittonAvi: (2020) piratage informatique: délits d'accès ou maintien frauduleux dans un stad, le 28 octobre, https://www.village-justice.com/articles/piratage-informatique-delits-acces-maintien-frauduleux-dans-systeme-traitement,36903.html.

Dreyfus Nathalie: (2020) blog, carrières, accès client... la sécurité informatique des pouvoirs publics estinquiétante, 18 mai, https://www.village-justice.com/articles/blog-carrieres-acces-client-securite-informatique-des-pouvoirs-publics-inquiete,35391.html.

GassinRymond: (1995) ,fraude informatique, Dalloz, Paris

Rouge ,Olivier de Maison (2021): la sécurit énumérique des données professionnelles juridiques et judiciaires, 4 février, https://www.village-justice.com/articles/securite-numerique-des-donnees-professionnelles-juridiques-judiciaires-par,37946.html.

Salagnon Charlyves: (2022): Les arnaques aux faux ordres de virement (fovi): quels recours-enindemnisation pour les victimes ?, 10 juin, https://www.village-justice.com/articles/les-arnaques-aux-faux-ordres-virement-fovi-quels-recours-indemnisation-pour-les,42895.html.