HNSJ Humanities & Natural Sciences Journal
ISSN: (e) 2709-0833
www.hnjournal.net

مجلة العلوم الإنسانية والطبيعية
مجلة علمية محكمة (التصنيف: NSP)
معامل التأثير العربي للعام 2024 = 0.44

عنوان البحث

الصور المستحدثة للجريمة الالكترونية

هشام محمد مهيدي صالح[1]، د. محمد هاني فرحات[2]

[1] باحث دكتوراه، الجامعة الإسلامية في لبنان، كلية الحقوق. بريد الكتروني: Real77644@gmail.Com.

[2] تدريسي في الجامعة الاسلامية في لبنان، كلية الحقوق، لبنان، خلده. بريد الكتروني: Mohammad.farhat@iul.edu.lb

HNSJ, 2026, 7(2); https://doi.org/10.53796/hnsj72/7

المعرف العلمي العربي للأبحاث: https://arsri.org/10000/72/7

تاريخ الاستقبال: 2026/01/01م تاريخ القبول: 2026/01/07م تاريخ النشر: 2026/02/01م

المستخلص

يتناول هذا البحث الصور المستحدثة للجريمة الإلكترونية بوصفها نتاجًا مباشرًا للتطور المتسارع في تقنيات المعلومات، وما أفرزه من أنماط إجرامية تستهدف سلامة النظم الإلكترونية والبيانات الرقمية المخزنة فيها، بحيث يغدو النظام ذاته محلًا للاعتداء. ويبرز البحث إشكالية الفراغ التشريعي وصعوبة مواءمة النصوص الجزائية التقليدية مع الخصائص التقنية لهذه الجرائم، لا سيما في السياق العراقي الذي يفتقر إلى قانون نافذ شامل للجرائم الإلكترونية، بما يحدّ من فعالية الحماية الجزائية ويعقّد مهمة القضاء والسياسة الجنائية.

اعتمدت الدراسة المنهج التحليلي في تفكيك أركان الجرائم الواقعة على الأنظمة والبيانات الإلكترونية، والمنهج المقارن من خلال المقارنة بين موقف التشريع العراقي (ولا سيما مشروع قانون الجرائم المعلوماتية لسنة 2011) والتشريع اللبناني (قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي رقم 81 لسنة 2018). وركّزت على جرائم الولوج أو المكوث غير المشروع داخل النظام الإلكتروني، والاعتداء على سلامة النظام، والاعتداء على سلامة البيانات الرقمية، مع بيان صورها وأركانها المادية والمعنوية، والطبيعة القانونية لها بوصفها من "جرائم الخطر" التي قد تتحقق بمجرد السلوك دون اشتراط وقوع ضرر فعلي.

وخلص البحث إلى قصور واضح في المنظومة العراقية لغياب نصوص نافذة متخصصة، مقابل تطور نسبي في التنظيم اللبناني عبر نصوص صريحة ومتكاملة تشمل الفعل التام والشروع وتشديد العقوبة عند تحقق نتائج ضارة. ويوصي البحث بالإسراع في إقرار تشريع عراقي خاص ومحدّث للجرائم الإلكترونية، وإعادة صياغة السياسة العقابية بما يحقق الاتساق بين صور الدخول والبقاء غير المشروع، وتقرير حماية مستقلة للبيانات الرقمية، مع الاستفادة من النموذج اللبناني وتعزيز التأهيل القضائي والتقني لضمان تطبيق فعّال للنصوص.

الكلمات المفتاحية: الجريمة الإلكترونية، الولوج غير المشروع، المكوث غير المشروع، البيانات الرقمية، سلامة النظام الإلكتروني.

RESEARCH TITLE

Newly Emerging Forms of Cybercrime

Abstract

This study examines the newly emerging forms of cybercrime as a direct outcome of the rapid advancement of information technologies, which has led to the proliferation of novel criminal patterns targeting the integrity of electronic systems and the digital data stored within them, rendering the system itself the object of attack. The research highlights the problem of legislative gaps and the difficulty of adapting traditional criminal law provisions to the technical characteristics of these crimes, particularly in the Iraqi context, which lacks a comprehensive and effective cybercrime law, thereby weakening criminal protection and complicating judicial enforcement and criminal policy.

The study adopts an analytical approach to examine the constituent elements of crimes committed against electronic systems and digital data, alongside a comparative approach contrasting the Iraqi legal position—especially the Draft Information Crimes Law of 2011—with the Lebanese legal framework, notably Law No. 81 of 2018 on Electronic Transactions and Personal Data. It focuses on crimes of unlawful access and unlawful stay within electronic systems, as well as crimes infringing the integrity of electronic systems and digital data, clarifying their legal nature, material and moral elements, and classifying them as "crimes of danger" that may be constituted by mere conduct without requiring the occurrence of actual damage.

The study concludes that the Iraqi legal framework suffers from a clear deficiency due to the absence of binding and specialized legislation, in contrast to the relatively advanced Lebanese approach, which provides explicit and integrated criminalization encompassing completed offenses and attempts, with aggravated penalties where harmful consequences arise. Accordingly, the study recommends expediting the enactment of a modern and specialized Iraqi cybercrime law, revising the punitive policy to ensure consistency between unlawful access and unlawful stay where similar criminal results occur, establishing independent criminal protection for digital data, drawing on the Lebanese legislative experience, and enhancing judicial and technical capacity-building to ensure effective enforcement of cybercrime provisions.

Key Words: Cybercrime; unlawful access; unlawful stay; digital data; integrity of electronic systems.

المقدمة

يُعد النظام الالكتروني محلاً للجريمة أو بيئةً حاضنة لها أو أداةً لارتكابها وفي جميع الأحوال فإن أي اعتداء يقع عليه يُشكّل جريمة جزائية تستدعي تدخّل المشرّع من خلال نصوص قانونية خاصة تتناسب مع طبيعة هذه الجرائم ووسائل ارتكابها، فأمام هذا النمط المستحدث من الإجرام لا تبدو النصوص الجزائية الواردة في قانون العقوبات التقليدي أو في بعض التشريعات الخاصة القائمة كافية أو فعّالة بالقدر المطلوب لمواجهته، وإن محاولة تطبيق تلك النصوص التقليدية على الجرائم الالكترونية قد تصطدم بعدد من المعوّقات، تعود في مجملها إلى الخصائص التقنية الفريدة والسمات المميزة للوسائل الالكترونية التي تُرتكب بها هذه الجرائم، يُضاف إلى ذلك أنّ التشريعات التقليدية وُضعت في سياق فكري ينطلق من إدراك الجرائم ذات الطبيعة المادية الملموسة، ما يجعل من العسير اعتمادها كأساس لحماية المعلومات والبيانات المخزّنة ضمن النظم الالكترونية من صور الإجرام المستحدثة التي تستهدفها.

أولًا: أهمية البحث:

تنبع أهمية هذا البحث من كونه يتناول أحد أكثر ميادين الإجرام المعاصر تطورًا وتعقيدًا، والمتمثل بالجرائم الواقعة على الأنظمة الإلكترونية والبيانات الرقمية، والتي باتت تشكّل تهديدًا مباشرًا للأمن المعلوماتي وللمصالح العامة والخاصة على حد سواء، وتزداد أهمية البحث في السياق العراقي على وجه الخصوص، في ظل غياب تشريع جزائي نافذ وشامل ينظم هذه الجرائم، الأمر الذي يفضي إلى فراغ تشريعي يحدّ من فاعلية الحماية الجزائية ويُضعف قدرة القضاء على مواجهة هذا النمط الإجرامي المستحدث، كما تتجلى أهمية البحث في اعتماده المقارنة مع التشريع اللبناني بوصفه نموذجًا تشريعيًا عربيًا متقدمًا نسبيًا في هذا المجال، بما يتيح استخلاص حلول تشريعية قابلة للاستفادة منها عند سن أو تعديل التشريع العراقي.

ثانيًا: إشكالية البحث

تتمحور إشكالية البحث حول التساؤل الرئيس الآتي: إلى أي مدى وفّق المشرّع الجزائي في توفير حماية قانونية فعّالة للنظم الإلكترونية والبيانات الرقمية من خلال تجريم أفعال الولوج والمكوث غير المشروع والاعتداء على سلامة الأنظمة والبيانات، وما مدى كفاية النصوص التقليدية في مواجهة هذا النمط الإجرامي المستحدث؟

ثالثًا: منهجية البحث

اعتمد البحث على المنهج التحليلي من خلال تحليل النصوص الجزائية ذات الصلة بجرائم الأنظمة والبيانات الإلكترونية وبيان أركانها وآثارها القانونية، فضلًا عن المنهج المقارن عبر المقارنة بين موقف التشريع العراقي والتشريع اللبناني، بهدف إبراز أوجه الاتفاق والاختلاف بينهما، وتقييم مدى كفاية كل منهما في توفير الحماية الجزائية المطلوبة، وصولًا إلى استخلاص نتائج علمية وتوصيات تشريعية عملية.

رابعا: هيكلية البحث

سعيًا لتسليط الضوء على أبرز الصور المستحدثة للجريمة الالكترونية، سنقوم بتقسيم هذا البحث إلى فرعين رئيسين، يُخصص الفرع الأول لدراسة جريمة الولوج أو المكوث غير المشروع داخل النظام الإلكتروني، وجريمة الاعتداء على سلامة النظام الالكتروني وبياناته الرقمية، وذلك على النحو الآتي:

الفرع الاول

جريمة الولوج او المكوث غير المشروع داخل النظام الالكتروني

إنّ الربط بين أجهزة الحاسوب عبر الشبكات الالكترونية، وما يصاحبه من استخدام لأنظمة الخوادم السيرفرات التابعة لمؤسسات الدولة والمؤسسات الخاصة وكذلك الأفراد قد أسهم في تسريع تبادل المعلومات وتيسير الوصول إليها، إلّا أنّ هذا التطوّر التقني رافقته مخاطر جمّة لعلّ أبرزها إمكانية التطفّل أو الدخول غير المشروع إلى تلك الأنظمة، حيث بات من اليسير على أشخاص غير مخوّلين الولوج إلى الخوادم أو البقاء فيها دون ترخيص، مما يشكّل مساسًا بسلامة وأمن النظام الالكتروني[1].

ويقصد بالنظام الالكتروني بأنه: "بيئة تحتوي على عدد من العناصر التي تتفاعل فيما بينها ومع محيطها بهدف جمع البيانات ومعالجتها حاسوبيًا وانتاج وبث المعلومات لمن يحتاجها لصناعة القرارات"[2]، ويتّضح من ذلك أن الغاية الأساسية للنظام الالكتروني تتمثل في إجراء المعالجة الآلية للبيانات، أي تنفيذ سلسلة من العمليات التي تُنجز تلقائيً وتشمل التجميع والتسجيل والإعداد والتعديل والحفظ والاسترجاع، وتكتسب هذه العمليات أهمية خاصة حينما ترتبط بعمليات الربط والتقريب ونقل البيانات ودمجها مع بيانات أخرى، أو تحليلها بغية استخلاص معلومات ذات دلالة معينة، وتقوم المعالجة الآلية على مجموعة من الإجراءات المترابطة والمتسلسلة تبدأ بجمع البيانات وإدخالها إلى الحاسب الآلي، ثم معالجتها وفقًا للبرمجيات المستخدمة وتنتهي بتحليلها وإخراجها في صورة معلومات قابلة للاستفادة منها[3].

تُعد جريمة الولوج أو المكوث غير المشروع داخل النظام الالكتروني من أخطر الصور المستحدثة للجريمة الالكترونية وأكثرها شيوعًا، وذلك لكونها تمثل المدخل الأساسي لارتكاب غالبية الأشكال التقليدية والمستحدثة للجرائم الالكترونية، فغالبًا ما لا يمكن تنفيذ هذه الجرائم إلا بعد النفاذ إلى النظام الالكتروني بشكل غير مشروع، مما يجعل من هذه الجريمة حجر الأساس والخطوة التمهيدية التي تفصل بين الجاني وبقية صور الجريمة الالكترونية، وتمكّنه من ارتكابها لاحقًا[4]، وللوقوف على الجوانب التفصيلية لهذه الجريمة تقتضي الضرورة تناول أركانها تحليلاً، ثم بيان موقف كل من التشريعين العراقي واللبناني منها، وهو ما سيكون محل البحث في الفقرتين التاليتين:

اولًا: اركان جريمة الولوج او المكوث غير المشروع داخل النظام الالكتروني:

يتطلب قيام جريمة الولوج أو المكوث غير المشروع داخل النظام الإلكتروني أن يصدر عن الجاني فعل مادي خارجي يُعبّر من خلاله عن إرادته في انتهاك نظم الحماية الأمنية الموضوعة من قبل مؤسسات الدولة أو الجهات الخاصة أو الأفراد، بهدف حماية أنظمتهم الإلكترونية من محاولات التلاعب أو التعديل أو الإتلاف أو الاطلاع أو الاستحواذ غير المشروع، كما قد يتجسد هذا الفعل في المكوث غير المشروع داخل تلك الأنظمة بقصد تحقيق غايات إجرامية أخرى[5]، وبذلك يتّضح أن جريمة الولوج أو المكوث غير المشروع داخل النظام الإلكتروني تقوم على ركنين أساسيين هما، الركن المادي والركن المعنوي، وذلك على النحو الآتي:

---

[1] د. علاء عبد الباسط خلاف، الحماية الجنائية لوسائل الاتصال الحديثة، بلا دار ومكان نشر، 2004، ص78.

[2] د. عماد الصابغ، نظم المعلومات (ماهيتها ومكوناتها)، ط1، دار الثقافة للنشر والتوزيع، عمان، 2000، ص11.

[3] د. محمد معمر الرازقي و د. محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، 2005، ص83.

[4] محمد مسعود محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، رسالة ماجستير، كلية الحقوق، جامعة الاسكندرية، 2006، ص105.

[5] بلال امين زين الدين، جرائم نظم المعالجة الآلية للبيانات، دار الفكر الجامعي، الاسكندرية، 2008، ص271.

1. **الركن المادي لجريمة الولوج أو المكوث غير المشروع داخل النظام الالكتروني:** يتكوّن الركن المادي لجريمة الولوج أو المكوث غير المشروع داخل النظام الإلكتروني من سلوك إجرامي يتمثّل إما في فعل الولوج غير المشروع إلى النظام الإلكتروني أو إلى جزء منه أو في فعل المكوث غير المشروع داخل ذلك النظام أو أحد أجزائه، ويُعد النظام الإلكتروني عنصراً مفترضاً في هذه الجريمة (وقد سبق بيان المقصود به فلا موجب لتكراره في هذا الموضع)، وعليه فإن الركن المادي لهذه الجريمة يتحقق من خلال ارتكاب أحد السلوكين المذكورين أو كليهما معًا شريطة أن يتم ذلك بصورة غير مشروعة، وهذا ما سنعرضه بإيجاز على النحو الآتي:

أ. **الولوج غير المشروع:** يُعد فعل الولوج غير المشروع إلى النظام الإلكتروني سلوكًا إجراميًا تتوافر به عناصر الركن المادي لهذه الجريمة، وينصرف مفهوم الولوج غير المشروع في السياق الإلكتروني، إلى كل الأفعال التي تتيح النفاذ إلى النظام الإلكتروني ويتحقق ذلك من خلال الوصول إلى البيانات أو المعلومات المخزنة داخل الحاسب الآلي، دون إذن أو موافقة من الشخص المخوّل قانونًا بالإشراف على هذا النظام أو على ما يحتويه من بيانات وخدمات، وقد ذهب جانب من الفقه إلى تشبيه الولوج غير المشروع إلى النظام الإلكتروني بما يشبه النفاذ إلى ذاكرة الإنسان لما ينطوي عليه من اختراق للخصوصية الرقمية، ويشمل هذا الولوج جميع صور التعدي سواء المباشر منها أو غير المباشر، ولا يُقصد بالولوج في هذا الإطار الدخول المادي إلى مكان وجود الحاسب الآلي، وإنما الدخول غير المادي الذي يتحقق من خلال نشاط ذهني وفني يمارسه الجاني داخل ذاكرة النظام دون أن يُباشر فعلًا ماديًا على الجهاز ذاته، كما تفترض هذه الجريمة أن النظام الإلكتروني محل الاعتداء ليس متاحًا لعامة الجمهور، وإنما يكون الولوج إليه مقتصرًا على فئة محددة من الأشخاص المصرّح لهم بذلك بموجب صلاحيات محددة[6].

ومن الجدير بالذكر أن تحقق هذه الجريمة لا يتوقف على اتباع وسيلة أو طريقة معينة للولوج إلى النظام الإلكتروني، إذ يمكن ارتكابها بأي وسيلة كانت ما دامت تؤدي إلى النفاذ غير المشروع، فقد يتم الولوج باستخدام أجهزة أو برمجيات متخصصة تمكّن الجاني من كسر الشفرات الأمنية أو فك رموز قاعدة البيانات، كما قد يتحقق الولوج من خلال استعمال بيانات الدخول الصحيحة الخاصة بشخص مأذون له بالدخول إلى النظام وذلك دون علمه أو رضاه مما يشكّل بدوره اعتداءً على الحق في حماية الأنظمة الإلكترونية[7].

وتجدر الإشارة هنا أنه يوجد نوع خاص من الولوج غير المشروع يُطلق عليه "الولوج المجرد إلى النظام الإلكتروني"، ويعني ذلك التواجد داخل النظام دون إحداث أي ضرر مادي أو تلاعب في مكوناته، باستثناء الاطلاع على البيانات والمعلومات المخزنة فيه دون غاية محددة أو هدف واضح، مما يُعتبر انتهاكًا لحقوق الخصوصية وأمن المعلومات حتى وإن لم يُترتب عليه تدمير أو تعديل للبيانات[8].

وقد أثار هذا النوع من الولوج المجرد خلافًا في الفقه حول مدى انطباق وصف جريمة الولوج غير المشروع عليه، وقد تباينت الآراء في هذا الصدد حيث اتجه البعض إلى رفض تجريم الولوج المجرد إلى النظام الإلكتروني، خاصة في حالة عدم وجود نية لدى الجاني لارتكاب جريمة تالية على هذا الفعل، ويُبرّر هذا الاتجاه رأيه بالقول إن الولوج المجرد لا يعدو أن يكون وسيلة لعرض القدرات الذهنية والتقنية التي يمتلكها الفاعل، الأمر الذي لا يمكن اعتباره جريمة تستدعي العقاب خاصة إذا لم يُترتب عليه أي ضرر أو تغيير في النظام الإلكتروني نفسه[9].

أما الاتجاه الثاني فيذهب إلى ضرورة تجريم الولوج المجرد إلى النظام الإلكتروني ولو لم يكن ذلك الولوج بقصد

---

[6] د. مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية (دراسة مقارنة)، دار النهضة العربية، القاهرة، 2012، ص50.

[7] د. دلخار صلاح بوتاني، الحماية الجنائية الموضوعية للمعلومات (دراسة مقارنة)، ط1، دار الفكر الجامعي، الاسكندرية، 2016، ص196.

[8] د. محمد سامي الشوا، ثورة المعلومات وانعكاسها على قانون العقوبات، مطابع الهيئة المصرية العامة للكتاب، 2003، ص177.

[9] د. نهلا عبد القادر المومني، الجرائم المعلوماتية، ط2، دار الثقافة للنشر والتوزيع، عمان، 2010، ص156-157.

ارتكاب جريمة لاحقة، إذ يرى هذا الاتجاه أن النشاط الإجرامي لجريمة الولوج غير المشروع يتحقق بمجرد الدخول إلى النظام دون اشتراط الوصول إلى البيانات أو المعلومات أو البرامج التي يحتويها وتُصنّف هذه الجريمة، بحسب هذا الرأي ضمن الجرائم الشكلية التي لا يُشترط لقيامها تحقق نتيجة مادية معينة، ويستند هذا الاتجاه في تبريره إلى أن العلة من تجريم فعل الولوج غير المشروع تكمن في حماية سلامة البيانات والمعلومات والبرمجيات من أي محاولة للوصول غير المصرح به أو العبث بها، وعليه فإن مجرد الولوج المجرد وإن خلا من نية إجرامية لاحقة، يُعد في ذاته تهديدًا محتملاً لسلامة هذه العناصر ويشكل بذلك اعتداءً على الحماية القانونية المقررة للنظم الإلكترونية[10].

ومما تقدّم نرى أن الاتجاه الثاني القائل بضرورة تجريم فعل الولوج المجرد إلى النظام الإلكتروني هو الأرجح من الناحية القانونية، وذلك لأن جريمة الولوج غير المشروع أو غير المصرّح به تُعد من جرائم الخطر، والتي تتحقق نتيجتها الإجرامية بمجرد ارتكاب فعل الولوج دون اشتراط تحقق ضرر فعلي، فالمشرّع من خلال تجريم هذا الفعل يسعى إلى حماية الأنظمة الإلكترونية من احتمالات التهديد أو التلاعب ولو لم يتحقق أثر مادي مباشر، كما أن قيام هذه الجريمة لا يتوقف على نجاح الجاني في الوصول إلى المعطيات أو البيانات التي يتضمنها النظام الإلكتروني، إذ يكفي أن يتم الولوج إليه بصورة غير مشروعة لتتحقق النتيجة الإجرامية باعتبارها قائمة على انتهاك الحماية التقنية والقانونية للنظام.

ب. **المكوث غير المشروع:** إن السلوك الإجرامي المكوّن للركن المادي في الجريمة محل الدراسة قد يتخذ صورة المكوث غير المشروع داخل النظام الإلكتروني، ذلك أن هذه الجريمة يمكن أن تتحقق بارتكاب أحد السلوكين، إما الولوج غير المشروع أو المكوث غير المشروع داخل النظام كما قد تتحقق بارتكاب السلوكين معًا.

ويقصد بالمكوث غير المشروع التواجد داخل النظام الإلكتروني دون إرادة أو إذن من الشخص المخوّل قانونًا بالسيطرة على هذا النظام، ويتجسّد هذا الفعل في استمرار الفاعل بالبقاء داخل النظام بعد أن دخل إليه عرضًا أو عن طريق الخطأ، إذ أن الولوج العَرَضي أو الخاطئ لا يُشكّل بحد ذاته فعلاً معاقبًا عليه قانونًا، نظرًا لانتفاء القصد الجرمي باعتبار أن جريمة الولوج غير المشروع تُعد من الجرائم العمدية التي لا تقوم دون توافر النية الإجرامية، إلا أن الغاية من تجريم فعل "المكوث غير المشروع" تتمثل في معاقبة من يدخل إلى النظام بطريق الخطأ أو الصدفة، ثم تتصرف إرادته بعد العلم بعدم مشروعية وجوده إلى البقاء داخله رغم إدراكه بأن استمراره في التواجد يُشكّل انتهاكًا غير مشروع للنظام[11].

ويأخذ المكوث غير المشروع داخل النظام الإلكتروني صورتين رئيسيتين، الصورة الأولى، أن يتحقق المكوث عقب دخول غير مصرح به إلى النظام، لكن من دون أن يتوافر لدى الفاعل قصد جرمي عند الولوج أي أن الدخول كان نتيجة خطأ أو سهو أو عن طريق المصادفة، غير أن الجريمة تقوم متى ما علم الفاعل بعد دخوله، بأنه داخل نظام لا يملك إذنًا بالدخول إليه ومع ذلك يُصرّ على البقاء فيه ولا يُغادره رغم وجوب ذلك عليه، فالمكوث في هذه الحالة يبدأ لحظة تحقق علم الفاعل بعدم مشروعية وجوده وتثبيت إرادته على الاستمرار في هذا التواجد غير المشروع، أما الصورة الثانية فتتحقق عندما يكون دخول الفاعل إلى النظام الإلكتروني مشروعًا ومأذونًا به من قبل الجهة المسؤولة عن النظام، ولكن هذا الإذن كان مشروطًا بزمن محدد أو بغرض معين فإذا تجاوز الفاعل المدة الزمنية المسموح له بها أو استمر في التواجد في النظام بعد انتهاء الغرض المشروع فإن استمراره يُعد مكوثًا غير مشروع ويستكمل بذلك أركان الفعل المجرَّم[12].

وقد ذهب جانب من الفقه إلى أن الصورة الأخيرة والمتمثلة في دخول الفاعل إلى النظام الإلكتروني بموافقة الجهة

---

[10] د. نائلة عادل محمد فريد قورة، جرائم الحاسب الاقتصادية، مرجع سابق، ص355.

[11] د. شيماء عبد الغني محمد عطاالله، الحماية الجنائية للتعاملات الالكترونية، دار الجامعة الجديد، الاسكندرية، 2007، ص121.

[12] د. دلخار صلاح بوتاني، مرجع سابق، ص207.

المسؤولة عنه لا تُشكّل جريمة المكوث غير المشروع ما دام أن الدخول قد تم بناءً على إذن مشروع، ويستند هذا الرأي إلى أن الغاية من تجريم المكوث غير المشروع داخل النظام الإلكتروني لا تختلف عن الغاية من تجريم الولوج غير المشروع وهي حماية البيانات والبرامج والمعطيات الإلكترونية من الوصول أو الاطلاع من قبل أشخاص غير مخوّلين، وعليه فإن هذه الغاية لا تكون قائمة في الحالة التي يُمنح فيها الإذن بالدخول من قِبل المسؤول عن النظام إذ أن التصريح بالولوج يتضمّن ضمناً الإذن بالاطلاع على محتويات النظام، وبالتالي فإن تجاوز الشخص للمدة الزمنية المحددة لا يجعل من استمراره في التواجد داخل النظام سلوكًا مجرّمًا في إطار جريمة المكوث غير المشروع وإن كان هذا الفعل قد يُشكّل بحسب ذات الرأي، صورة أخرى من صور التجريم مثل استخدام الحاسب الآلي دون تصريح أو ما يُعرف فقهيًا بـ"سرقة وقت الحاسب الآلي"[13].

2. **الركن المعنوي لجريمة الولوج او المكوث غير المشروع داخل النظام الالكتروني:** تُعد جريمة الولوج أو المكوث غير المشروع داخل النظام الإلكتروني من الجرائم العمدية إذ إن أفعال الولوج أو المكوث التي تنطوي عليها هذه الجريمة تُرتكب من قبل مستخدمي الأنظمة الإلكترونية بصورة متكررة ويومية وفي أحيان كثيرة بشكل مكثف خلال اليوم الواحد، ومن ثمّ لا يمكن تجريم كل فعل ولوج أو مكوث داخل النظام، لأن ذلك من شأنه أن يوقع عدداً كبيراً من مستخدمي الأنظمة الإلكترونية تحت طائلة المسؤولية الجزائية، الأمر الذي يستلزم أن تُصنّف هذه الجريمة ضمن الجرائم العمدية تحقيقاً للتوازن بين مقتضيات حماية الأنظمة الإلكترونية وضرورة ضمان حرية استخدامها من قبل الأفراد[14].

وعليه يتجسد الركن المعنوي في هذه الجريمة في صورة القصد الجنائي العام والذي يتحقق بتوافر عنصري العلم والإرادة، ويُقصد بذلك أن يكون الجاني على علم بأن فعله موجه إلى نظام إلكتروني بما يتضمنه من برامج ومعطيات وليس إلى شيء آخر وأن تنصرف إرادته إلى هذا الفعل تحديداً، كما ينبغي أن يشمل علم الجاني إدراكه بأن ولوجه أو مكوثه داخل النظام تم دون إذن أو تصريح من الجهة المخولة بإدارة هذا النظام، وبالتالي إذا كان الجاني يعتقد اعتقاداً قائماً على أسباب معقولة أن لديه تصريحاً بالدخول أو المكوث داخل النظام، فإن القصد الجنائي ينتفي وتنتفي معه الجريمة لغياب الركن المعنوي، وينطبق ذات الحكم في حالة الدخول العَرَضي أو السهوي أو الناتج عن خطأ غير مقصود إلى النظام الإلكتروني، إلا أنه يُشترط في هذه الحالة أن يغادر الجاني النظام فور علمه بعدم مشروعية دخوله أو مكوثه، فإذا استمر في التواجد داخل النظام رغم علمه بانعدام الإذن اعتُبر حينها قد توفر لديه القصد الجنائي ابتداءً من لحظة تحقق هذا العلم[15].

ومع ذلك فإن توافر عنصر العلم لدى الجاني لا يكفي بمفرده لقيام القصد الجنائي إذ لا بد من اقترانه بعنصر الإرادة أي أن تتجه إرادة الجاني إلى الولوج أو المكوث داخل النظام الإلكتروني بصورة غير مشروعة، وحيث إن جريمة الولوج أو المكوث غير المشروع تُعد من الجرائم الشكلية التي لا يُشترط لقيامها تحقق نتيجة مادية معينة، فإن القصد الجنائي يكتمل بمجرد توجّه إرادة الجاني إلى ارتكاب السلوك الإجرامي المتمثل في الولوج أو المكوث، واستغراقه بجميع عناصره دون الحاجة إلى امتداد هذه الإرادة لتحقيق نتيجة معينة تترتب على ذلك السلوك[16].

وتجدر الإشارة إلى أن جريمة الولوج أو المكوث غير المشروع داخل النظام الإلكتروني لا تقتصر على توافر

---

[13] د. نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية (دراسة نظرية وتطبيقية)، ط1، مشورات الحلبي الحقوقية، بيروت، 2005، ص360.

[14] د. دلخار صلاح بوتاني، مرجع سابق، ص210.

[15] د. نائلة عادل محمد فريد قورة، مرجع سابق، ص3779.

[16] محمد مسعود محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، رسالة ماجستير، كلية الحقوق، جامعة الاسكندرية، 2006، ص128.

القصد الجنائي العام فحسب، بل تستلزم أيضًا وجود قصد جنائي خاص يتمثل في نية الغش أي توجّه إرادة الجاني إلى الإضرار بالغير، غير أنّه لا يُشترط لتحقّق هذا القصد الخاص وقوع الضرر فعلاً طالما أن الجريمة تُصنّف ضمن الجرائم الشكلية التي لا تتطلب تحقق نتيجة مادية معينة، وبالتالي فإن مجرد توافر نية الإضرار ولو لم يُترجم ذلك إلى ضرر فعلي يُعد كافيًا لقيام القصد الجنائي الخاص في هذه الجريمة.

ثانيًا: موقف التشريعين العراقي واللبناني من جريمة الولوج او المكوث غير المشروع داخل النظام الالكتروني:

تُعد هذه الجريمة اعتداءً خطيراً على أمن وسلامة النظم والبيانات الإلكترونية بما يشكل عائقاً كبيراً أمام المستخدمين الشرعيين لهذه التقنية الحديثة، إذ قد يترتب عليها إتلاف أو تدمير معلومات وبيانات رقمية ذات قيمة اقتصادية عالية، كما أن من شأنها أن تُشجّع مرتكبي الجرائم الإلكترونية على ارتكاب صور أكثر خطورة من الجرائم التي تمس سلامة النظم الإلكترونية، الأمر الذي يُحتم تدخل المشرع الجزائي لتوفير الحماية القانونية اللازمة لهذه النظم من خلال تجريم جميع صور الاعتداء التي تُرتكب بحقها وعلى وجه الخصوص تجريم أفعال الولوج أو المكوث غير المشروع داخلها لكونها تمثل البوابة الأساسية التي تُمهد لارتكاب سائر الجرائم الإلكترونية الأخرى.

وبالرجوع إلى موقف التشريعين محل الدراسة يتبين أن المشرع العراقي لم يسن بعد قانوناً خاصاً بالجرائم الإلكترونية، الأمر الذي أفضى إلى وجود قصور واضح في النظام القانوني العراقي في هذا المجال، لا سيما وأن من الصعوبة بمكان مواجهة جريمة الولوج أو المكوث غير المشروع داخل النظم الإلكترونية بالاستناد إلى النصوص الجزائية التقليدية الواردة في قانون العقوبات، فهذه الجريمة تمثل نمطاً إجرامياً مستحدثاً لم يكن في حسبان المشرع عند صياغته لتلك النصوص مما يستوجب تدخلاً تشريعياً عاجلاً لمعالجة هذا الفراغ القانوني، ويُمكن تحقيق ذلك إما من خلال تعديل النصوص القائمة في قانون العقوبات بما يتلاءم مع طبيعة هذه الجريمة أو عن طريق إصدار قانون خاص يتضمّن قواعد جزائية تُواكب التطور التقني وتستوعب أنماط السلوك الإجرامي المستحدث الذي تمثّله هذه الجريمة وسواها من الجرائم الإلكترونية.

ولا بد من الإشارة في هذا السياق إلى أن مشروع قانون الجرائم الإلكترونية العراقي لسنة 2011 تضمّن عدداً من النصوص التي تُجرِّم أفعال الدخول (الولوج) أو البقاء (المكوث) غير المشروع داخل النظم الإلكترونية، ومن بين هذه النصوص المادة (14/ثالثاً) التي نصت على أنه "يعاقب بالحبس مدة لا تزيد على (3) ثلاثة أشهر أو بغرامة لا تقل عن (2000000) مليوني دينار ولا تزيد على (5000000) خمسة ملايين دينار كل من: ... ج: دخل عمداً بدون تصريح موقعاً أو نظاماً معلوماتياً أو اتصل مع نظام الحاسوب أو جزء منه، د: استخدم أو تسبب دون تصريح في استخدام الحاسوب العائد للغير بطريقة مباشرة أو غير مباشرة، هـ: انتفع بدون وجه حق بخدمات الاتصالات من خلال شبكة المعلومات او أحد أجهزة الحاسوب".

وكذلك نصّت المادة (15) من ذات مشروع القانون على تجريم أفعال تمسّ بأمن وسلامة النظم الإلكترونية والتي نصت على أنه "أولاً: يعاقب بالحبس وبغرامة لا تقل عن (1000000) عشرة ملايين دينار ولا تزيد على (15000000) خمسة عشر مليون دينار كل من: أ: تجاوز عمداً نطاق التصريح المخول به أو أعترض أية معلومات خلال عمليات تبادلها، ب: تنصت او راقب البيانات والمعلومات المخزنة او المتبادلة في نظم المعلومات، ثانيا: تكون العقوبة الحبس مدة لا تقل عن (4) اربع سنوات وبغرامة لا تقل عن (15000000) خمسة عشر مليون دينار ولا تزيد على (25000000) خمسة وعشرين مليون دينار إذا نشأ عن الفعل المنصوص عليه في البند (اولا) من هذه المادة حذف أو تدمير أو تغيير أو تعييب أو تعطيل أو إعادة نشر بيانات ومعلومات تعود للغير بغير وجه حق"[(17)].

[(17)] للمزيد حول مسودة مشروع قانون الجرائم المعلوماتية العراقي لسنة 2011، ينظر الموقع الإلكتروني الرسمي لقناة السومرية العراقية، الرابط الإلكتروني: www.alsumaria.tv . تاريخ الزيارة 2024/8/13.

ومن خلال النصوص المتقدّمة يتبيّن أن المشرّع العراقي في مشروع قانون الجرائم الإلكترونية قد شدّد العقوبة على فعل البقاء غير المشروع داخل النظام الإلكتروني، في حال ترتّب عليه حذف أو تدمير أو تعديل أو تشويه أو تعطيل أو إعادة نشر بيانات أو معلومات تعود للغير من دون وجه حق، غير أنّ ما يُؤخذ على المشرّع في هذا السياق هو اقتصاره في تشديد العقوبة على حالة البقاء غير المشروع فقط، دون أن يشمل بذلك حالة الدخول غير المشروع إلى النظام، رغم أن النتائج ذاتها قد تنشأ عن الفعلين معاً، وعليه فإن من المأمول أن يتنبّه المشرّع إلى هذا القصور، وأن يعمل على معالجته عند مناقشة مشروع القانون والتصويت عليه من خلال تشديد العقوبة على كلٍّ من فعلي الدخول والبقاء غير المشروع متى ما ترتّب عليهما أيٌّ من النتائج الجرمية المشار إليها.

أمّا بالنسبة للمشرّع اللبناني فقد حرص على تجريم فعلي الولوج والمكوث غير المشروعين داخل النظام الإلكتروني، بل إنه ذهب إلى أبعد من ذلك فنصّ صراحةً على تجريم الشروع (المحاولة) في ارتكاب هذين الفعلين أيضاً وذلك بموجب أحكام قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي رقم (81) لسنة 2018 النافذ، وقد ورد هذا التجريم في المادة (110) من القانون المذكور، تنص على أنه "يعاقب بالحبس من ثلاث اشهر إلى سنتين وبالغرامة من مليون إلى عشرين مليون ليرة لبنانية او بإحدى هاتين العقوبتين كل من اقدم، بنية الغش، على الوصول او الولوج إلى نظام معلوماتي بكامله او في جزء منه او على المكوث فيه، تشدد العقوبة إلى الحبس من ستة اشهر إلى ثلاث سنوات والغرامة من مليونين إلى اربعين مليون ليرة، إذا نتج عن العمل الغاء البيانات الرقمية او البرامج المعلوماتية او نسخها او تعديلها او المساس بعمل النظام المعلوماتي".

وقد أكّد المشرّع اللبناني في المادة (115) من القانون ذاته على أن العقوبة المقرّرة لجريمة الدخول أو البقاء غير المشروع داخل النظام الإلكتروني تشمل أيضاً الشروع في ارتكاب هذه الجريمة حيث نصّ صراحةً على معاقبة المحاولة بالعقوبة ذاتها المقرّرة للفعل التام، وفي هذا السياق ذهب جانب من الفقه اللبناني إلى أن إدراج هذه المادة لم يكن ضرورياً، طالما أن المشرّع قد تضمّن في نص التجريم ذاته مصطلح "المحاولة"، مما يُغني بحسب هذا الرأي عن النص المستقل ويُجنّب التكرار التشريعي غير المبرّر[18].

الفرع الثاني

جريمة الاعتداء على سلامة النظام الالكتروني وبياناته الرقمية

تُعد جريمة الاعتداء على سلامة الأنظمة الإلكترونية وبياناتها الرقمية من أبرز الآثار السلبية التي أفرزتها ثورة تكنولوجيا المعلومات، إذ تُشكّل تهديدًا جوهريًا في نطاق البيئة التقنية المعاصرة، ويتجسد هذا التهديد من خلال المساس بسلامة النظام الإلكتروني ذاته أو من خلال الاعتداء على البيانات الرقمية المخزنة ضمنه، مما يؤدي إلى اضطراب في أداء أنظمة التشغيل الإلكترونية ويُحدث خللًا في وظائفها بصرف النظر عن الجهة التي تعتمد عليها تلك الأنظمة، ويتم ارتكاب هذه الجريمة عادة عبر شبكة الإنترنت سواء من خلال الإخلال بالوظائف التشغيلية لأجهزة الحاسوب أو التعدي على البيانات والبرامج المخزنة أو المتبادلة إلكترونيًا أو من خلال التلاعب بالمعلومات أو إتلافها أو حذفها أو تعديلها أو تشويه نتائجها أو التسبب في إعاقة عمل الأنظمة الإلكترونية وتعطيل سير أدائها.

وبناءً على ما تقدّم سيتم في هذا الفرع تناول جريمة الاعتداء على سلامة النظام الإلكتروني وجريمة الاعتداء على سلامة البيانات الرقمية مع بيان الأركان المكوّنة لكلٍ منهما، وذلك من خلال فقرتين، على النحو الآتي:

[18] د. سمير عالية، الجرائم الالكترونية في القانون الجديد (رقم2018/81) ط1، منشورات الحلبي الحقوقية، 2020، ص147.

اولا: جريمة الاعتداء على سلامة النظام الالكتروني:

يقصد بهذه الجريمة الاعتداء الذي يقع على المعطيات الإلكترونية الموجودة خارج النظام الإلكتروني والتي تُساهم في تحقيق نتيجة محددة تتمثّل في المعالجة الآلية لتلك المعطيات، فجريمة الاعتداء على سلامة الأنظمة الإلكترونية من خلال تخريبها أو تدميرها من شأنها أن تعيق سير هذه الأنظمة وتُفقدها صلاحيتها للاستخدام الوظيفي المطلوب[19]، وبما أن هذه الجريمة تُعد من الجرائم العمدية فإن من الضروري بيان ركنها المادي أولًا ثم التطرق إلى ركنها المعنوي، وذلك على النحو الآتي:

1. **الركن المادي لجريمة الاعتداء على سلامة النظام الالكتروني:** يمتد فعل الاعتداء في نطاق الأنظمة الإلكترونية ليشمل المكونات المادية للنظام الإلكتروني أو مكوناته المعنوية كأن يقع الاعتداء على أجهزة الحاسب الآلي بأكملها أو على جزء منها، ويتمثّل الركن المادي في هذه الجريمة في إلحاق الضرر بالنظام الإلكتروني سواء بتخريبه أو جعله غير صالح للاستخدام، ولا يُشترط أن يكون فعل الاعتداء تامًا لتحقيق الجريمة إذ يكفي أن يكون جزئيًا ما دام من شأنه التأثير على صلاحية النظام للاستعمال أو التسبب في تعطيله بأي وسيلة كانت[20].

تتخذ الأفعال المكوّنة للركن المادي في هذه الجريمة والتي تمس سلامة النظام الإلكتروني صورتين رئيسيتين، الصورة الأولى هي التعطيل أو الإعاقة ويقصد بها منع النظام من أداء عمله كليًا أو جزئيًا ويتحقق ذلك بفعل يؤدي إلى إرباك النظام وتعطيله عن أداء وظائفه المختلفة، وقد تنجم عملية التعطيل أو الإعاقة عن الاعتداء على المكونات المادية للأنظمة الإلكترونية، مثل تحطيم الأقراص الصلبة أو قطع شبكة الاتصال أو قد تكون ناتجة عن الاعتداء على المكونات البرمجية والمنطقية لتلك الأنظمة كالمعلومات الرقمية والبرامج[21]، كما يمكن أن تكون عملية التعطيل أو الإعاقة دائمة كما في حالة إدخال فيروس تدميري أو مؤقتة لفترات محددة كإدخال فيروس زمني مبرمج يؤدي إلى شل النظام الإلكتروني عند بدء تشغيله أو عند استخدام أحد البرامج التطبيقية[22].

أما الصورة الثانية فهي الإفساد ويُقصد به كل فعل يجعل النظام الإلكتروني غير صالح للاستخدام السليم وذلك بإعطائه نتائج تختلف عن تلك التي كان من المفترض الحصول عليها، وتتعدد وسائل الإفساد منها استخدام القنبلة الإلكترونية التي تُدخل معلومات تتكاثر داخل الأنظمة الإلكترونية مما يجعلها غير صالحة للاستخدام أو استخدام فيروس حصان طروادة[23].

ومما يجدر الإشارة إليه أن هناك رأيًا فقهيًا ميز بين مصطلحي الإعاقة والإفساد إذ يرى أن لكل منهما معنى يكمل الآخر، فالنص يتناول من خلالهما كافة الوسائل المستخدمة للاعتداء على سلامة النظام الإلكتروني، ففعل التعطيل أو الإعاقة يشمل الأفعال الموجهة بشكل مباشر إلى النظام وذلك بهدف منعه من أداء وظائفه ويترتب عليه تعطيل مؤقت، أما الإفساد فيتمثل في الأحوال التي ينتج عنها تعطيل النظام عن أداء وظائفه بحيث يصبح غير صالح للاستخدام[24].

---

[19] د. محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت (دراسة مقارنة)، دار النهضة العربية، القاهرة، 2009، ص495.

[20] د. عمر ابو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة الكترونيًا (دراسة مقارنة)، دار النهضة العربية، القاهرة، 2010، ص985.

[21] طعباش امين، الحماية الجنائية للمعاملات الالكترونية، ط1، مكتبة الوفاء القانونية، الاسكندرية، 2015، ص66.

[22] د. رشيدة بوكر، الحماية الجزائية للتعاملات الالكترونية، ط1، منشورات الحلبي الحقوقية، بيروت، 2020، ص90.

[23] آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، ط2، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2007، ص118-119.

[24] د. نائلة عادل محمد فريد قورة، مرجع سابق، ص222.

2. **الركن المعنوي لجريمة الاعتداء على سلامة النظام الالكتروني:** لا يكفي لقيام الجريمة قانونًا مجرد توافر الركن المادي فيها بل يجب أن تكون هناك رابطة نفسية بين السلوك الإجرامي والنتائج المترتبة عليه وبين الجاني وتُعرف هذه الرابطة بالركن المعنوي، فجريمة إعاقة أو إفساد النظام الإلكتروني تُعد من الجرائم العمدية التي يتخذ ركنها المعنوي صورة القصد الجزائي العام المتمثل في عنصرَي العلم والإرادة، ولتتحقق عناصر الركن المعنوي، يجب أن يعلم الجاني أنه يقوم بفعل الإعاقة أو الإفساد وأن هذا الفعل من شأنه التأثير على أداء وظيفة النظام الإلكتروني، وأن ذلك يتم دون رضا صاحب الحق في السيطرة على النظام، كما يجب أن تتجه إرادته نحو ارتكاب الفعل وتحقيق النتيجة الضارة إذ تُعتبر نية الضرر متوافرة قانونًا لدى الجاني متى علم أن سلوكه يضر أو قد يضر بالغير، ومن ثم فإن الضرر هو الهدف الذي يسعى إليه الجاني من وراء ارتكابه للجريمة[25].

وبالرجوع إلى موقف المشرّعين العراقي واللبناني من جريمة الاعتداء على سلامة النظام الإلكتروني يُلاحظ أن المشرّع العراقي لم يتناول هذه الجريمة صراحةً في التشريعات النافذة باستثناء ما ورد في مشروع قانون جرائم المعلوماتية لسنة 2011، حيث نصت المادة (14/ثانيًا) منه على أن "يعاقب بالحبس مدة لا تقل عن (3) ثلاث سنوات وبغرامة لا تقل عن (15000000) خمسة عشر مليون دينار ولا تزيد على (25000000) خمسة وعشرون مليون دينار او بإحدى هاتين العقوبتين كل من عطل عمدًا أجهزة الحاسوب وبرامجه وشبكات المعلومات المخصصة للمنفعة العامة او اتلفها او عاق عملها".

في حين نصّت الفقرة (ثالثًا) من المادة ذاتها على أن "يعاقب بالحبس مدة لا تزيد على (3) ثلاثة اشهر او بغرامة لا تقل عن (2000000) مليوني دينار ولا تزيد على (5000000) خمسة ملايين دينار كل من: أ- عهدت اليه مهمة تشغيل او الاشراف على جهاز الحاسوب فتسبب عمدًا في اتلاف او تعطيل او اعاقة او تعييب أجهزة الحاسوب او انظمته او برامجه او شبكاته وما في حكمها، ب- تطفل او ازعج او اتصل بمستخدمي أجهزة الحاسوب وشبكة المعلومات بدون تصريح او اعاقة استخدامها من منتفعيها...".

وباستقراء النصوص القانونية المشار إليها يتضح أن المشرّع العراقي قد ميّز بين صورتين لجريمة الاعتداء على سلامة النظام الإلكتروني، إذ اعتبرها بصورتها البسيطة متى ما وقعت على نظام إلكتروني يُستخدم لتحقيق منفعة خاصة، بينما اعتبرها بصورتها المشددة إذا وقعت على نظام إلكتروني مخصص لتحقيق منفعة عامة، كما هو الحال في الاعتداءات التي تمس سلامة الأنظمة الإلكترونية التابعة للمؤسسات العامة في الدولة.

أما بالنسبة للمشرّع اللبناني فقد جرّم فعل الاعتداء على سلامة النظام الإلكتروني بصورة صريحة وذلك بموجب قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي رقم (81) لسنة 2018 النافذ، حيث نصّت المادة (111) منه على أن "يعاقب بالحبس من ستة اشهر إلى ثلاث سنوات وبالغرامة من ثلاثة ملايين إلى مئتي مليون ليرة لبنانية او بإحدى هاتين العقوبتين كل من اقدم بنية الغش وباي وسيلة على اعاقة عمل نظام معلوماتي او على افساده".

في حين نصّت المادة (113) من القانون ذاته على أن "كل من اعاقة او شوش او عطل قصدًا وباي وسيلة، من خلال الشبكة المعلوماتية او أحد أجهزة الحاسب الآلي وما في حكمها، الوصول إلى الخدمة او الدخول إلى الأجهزة او البرامج او مصادر البيانات او المعلومات يعاقب بالحبس من ثلاثة اشهر إلى سنتين وبالغرامة من مليونين إلى ثلاثين مليون ليرة لبنانية او بإحدى هاتين العقوبتين"، وقد أكّد المشرّع اللبناني في المادة (115) من القانون ذاته على تجريم

[25] د. محمود محمود مصطفى، شرح قانون العقوبات القسم الخاص، ط8، مطبعة جامعة القاهرة، القاهرة، 1984، ص649.

محاولة الاعتداء على سلامة النظام الإلكتروني، حيث قرر لها ذات العقوبة المقرّرة للجريمة التامة المنصوص عليها في المادتين اعلاه.

علمًا أن الجريمة المنصوص عليها في المادة (113) من قانون المعاملات الإلكترونية تختلف عن تلك الواردة في المادة (111) من القانون ذاته، إذ إن الجريمة الأولى تتعلق بالاعتداء على البنية التحتية للشبكة الإلكترونية أو على أجهزة الحاسب الآلي، في حين تنصرف الجريمة الثانية إلى الاعتداء على سلامة النظام الإلكتروني وأداء وظائفه بما يشمل ما يحتويه من معالجة آلية للبيانات والمعلومات[26].

ثانيا: جريمة الاعتداء على سلامة البيانات الرقمية:

ويقصد بجريمة الاعتداء على البيانات الرقمية كل سلوك من شأنه التأثير على تلك البيانات على نحو يؤدي إلى زوال قيمتها الاقتصادية أو إنقاصها وذلك من خلال الإضرار بكفاءتها أو بقدرتها على أداء الغرض الذي أُعدّت له، فإذا ترتب على الفعل فقدان البيانات الرقمية لقيمتها أو نقصانها فإن ذلك يُعد اعتداءً يُشكّل جريمة معاقباً عليها بموجب أحكام القانون[27]، وتُعرّف هذه الجريمة بأنها "افناء او تغيير شامل للبيانات المعالجة آليًا سواء بالمحو او التعديل او التبديل، يؤدي إلى عدم صلاحية هذه البيانات وضياع قيمتها وجعلها غير صالحة للغرض الذي خصصت من أجله"[28].

وتتباين جريمة الاعتداء على سلامة البيانات الرقمية عن الجريمة السابقة التي تتمثل في الاعتداء على سلامة النظام الالكتروني ذاته من حيث محل الحماية القانونية، فبينما تنصرف الجريمة الأولى إلى حماية هيكل النظام الالكتروني ووظائفه فإن جريمة الاعتداء على سلامة البيانات الرقمية تتركز على البيانات المخزنة داخل ذلك النظام والتي تُعد جزءًا منه، ويتمثل محل هذه الجريمة في المعطيات التي أُدخلت إلى النظام الالكتروني لغرض معالجتها إلكترونيًا، وتحولت نتيجة ذلك إلى بيانات رقمية، أما المعطيات التي لم تُدخل بعد إلى النظام الالكتروني، أو التي أُدخلت دون أن تُباشَر بشأنها أي عملية معالجة فإنها لا تندرج ضمن نطاق الحماية الجزائية لهذه الجريمة، في المقابل فإن المعطيات التي تم إدخالها إلى النظام وبدأت إجراءات معالجتها أو كانت في طريقها للمعالجة فإنها تُعد محمية قانونًا حتى وإن لم تبدأ المعالجة فعليًا ما دامت دخلت في دائرة التعامل الإلكتروني داخل النظام[29]، ويتكوَّن البنيان القانوني لجريمة الاعتداء على سلامة البيانات الرقمية من ركنين أساسيين، الركن المادي والركن المعنوي، وهو ما سيتم بيانه بإيجاز على النحو الآتي:

1. **الركن المادي لجريمة الاعتداء على سلامة البيانات الرقمية:** يتجسّد السلوك الإجرامي المكوّن للركن المادي في جريمة الاعتداء على سلامة البيانات الرقمية من خلال عدة صور من الأفعال تُعدّ أبرزها، الإدخال والمحو والتعديل، ويُعد تحقق أحد هذه الأفعال كافيًا لقيام الركن المادي للجريمة إذ لا يُشترط اجتماعها مجتمعةً بل يكفي أن يقع أحدها بصورة تامة ومؤثرة في سلامة البيانات محل الحماية، ويُقصد بالإدخال "اضافة معطيات جديدة لم تكن موجودة من قبل على

---

[26] د. سمير عالية، مرجع سابق، ص167.

[27] د. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الاول، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، القاهرة، 1992، ص153.

[28] د. هبه حسين محمد زايد، الحماية الجنائية للصفقات الالكترونية (دراسة مقارنة)، دار الكتب القانونية، مصر، 2015، ص75.

[29] د. سمير عالية، مرجع سابق، ص163.

الدعامة الخاصة سواء كانت خالية او كان يوجد بها معطيات، وذلك بهدف التشويش على صحة البيانات والمعلومات المخزنة داخل النظام المعلوماتي، وتغذية النظام بمعلومات خاطئة او زائدة فيه لم تكن موجودة من قبل"[30].

علمًا بأن فعل الإدخال غير المشروع للمعطيات والبيانات لا يؤدي بالضرورة في جميع الحالات إلى تعديل في ذاكرة النظام الالكتروني، بل قد ينتج عنه أحيانًا تعديل البيانات ذاتها أو حتى تدميرها، ومن الأمثلة على ذلك إدخال برامج خبيثة تُعرف بالقنابل المنطقية والزمنية، ويقصد بالقنبلة المنطقية نوعًا معينًا من الفيروسات التي تنشط بمجرد حدوث واقعة معينة، مثل تشغيل النظام أو إتمام إجراء محدد داخله أما القنبلة الزمنية فهي فيروس يُفعَّل في تاريخ معين وينتج عنه تأثيرات في أوقات محددة بالساعة واليوم والسنة، ويُميّز هذا الفعل عموماً بكونه يُرتكب في الغالب من قبل المسؤول أو الموظف المختص بالقسم الالكتروني، نظراً لما يمتلكه من معرفة وخبرة تمكنه من تنفيذ هذا النوع من التعديات والتلاعب غير المشروع بفعالية[31].

ومن الأفعال الأخرى التي تشكل الركن المادي لهذه الجريمة، فعل المحو (الإزالة) ويُقصد به "ازالة جزء من المعطيات المسجلة على دعامة والموجودة داخل النظام، او تحطيم تلك الدعامة او نقل وتخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة"[32]، ومن الأمثلة الواقعية على فعل المحو قيام مجموعة من الأشخاص بالاستيلاء على مبلغ (61,000) دولارًا أرسلته إحدى شركات التأمين إلى أحد المراكز الطبية، حيث قام هؤلاء بإنشاء حسابات وهمية خاصة بهم وأودعوا فيها المبلغ المالي ثم قاموا بحذف هذه الحسابات من سجلات الحاسب الآلي التابعة للمركز الطبي، ما أدى إلى إخفاء أثر العملية المالية وارتكاب جريمة تزوير وتلاعب بالبيانات الرقمية[33].

فضلًا عن الفعلين السابقين يوجد فعل آخر يُشكل ركنًا ماديًا من أركان جريمة الاعتداء على سلامة البيانات الرقمية وهو فعل التعديل، ويُقصد به "اجراء نوع من التشفير غير المشروع للمعطيات والبيانات المخزنة داخل النظام المعلوماتي، واستبدالها بمعطيات وبيانات جديدة باستخدام أحد وظائف الحاسب الآلي، فالنشاط الاجرامي المتمثل بالتعديل يعني تغيير المعطيات المعالجة الكترونيًا والمخزنة داخل النظام المعلوماتي واستبدالها بمعطيات أخرى جديدة"[34].

2. **الركن المعنوي لجريمة الاعتداء على سلامة البيانات الرقمية:** يشترط لتحقق جريمة الاعتداء على سلامة البيانات الرقمية توافر القصد الجزائي العام الذي يتألف من العلم والإرادة، فلا بد أن يكون الجاني على علم بأن السلوك الذي يقوم به سواء كان إدخالًا أو إزالةً أو تعديلًا هو فعل غير مشروع، كما يجب أن يكون مدركًا بأنه يعتدي على صاحب الحق في المعطيات والبيانات موضوع الاعتداء، إضافة إلى ذلك يجب أن تتجه إرادته نحو ارتكاب هذه الأفعال بقصد مباشر ودون موافقة أو رضا من صاحب الحق أو من يملك حق السيطرة عليها[35].

وبالرجوع إلى موقف المشرعين في العراق ولبنان من جريمة الاعتداء على سلامة البيانات الرقمية، يتبيّن أن التشريع العراقي يفتقر إلى نص صريح ونافذ يعالج هذه الجريمة بشكل مباشر، باستثناء ما ورد في المادة (15/أولًا) من

---

[30] د. علي عبدالقادر القهوجي، الحماية الجنائية للبيانات المعالجة الكترونيًا (دراسة مقارنة)، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، المجلد الثاني، كلية الشريعة والقانون، جامعة الامارات العربية المتحدة، 2000، ص559.

[31] د. رشيدة بوكر، مرجع سابق، ص98.

[32] د. محمد عبيد الكعبي، مرجع سابق، ص211.

[33] د. عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي (دراسة متعمقة في القانون المعلوماتي)، ط1، دار الفكر الجامعي، الاسكندرية، 2006، ص384.

[34] د. جميل عبد الباقي الصغير، مرجع سابق، ص34.

[35] د. علي عبدالقادر القهوجي، مرجع سابق، ص60.

مشروع قانون الجرائم المعلوماتية لسنة 2011، والتي نصّت على أن "يعاقب بالحبس وبغرامة لا تقل عن (10000000) عشرة ملايين دينار ولا تزيد على (15000000) خمسة عشر مليون دينار كل من : أ- تجاوز عمدًا نطاق التصريح المخول به او اعترض اية معلومات خلال عمليات تبادلها، ب- تنصت او راقب البيانات والمعلومات المخزنة او المتبادلة في نظم المعلومات".

وقد شدد المشرع العقوبة في الفقرة (ثانيًا) من ذات المادة، حيث فرض الحبس لمدة لا تقل عن أربع سنوات، وبغرامة مالية لا تقل عن خمسة عشر مليون دينار عراقي، إذا نتج عن الفعل المنصوص عليه في الفقرة (أولًا) من هذه المادة حذف أو تدمير أو تغيير أو تعييب أو تعطيل أو إعادة نشر بيانات ومعلومات تعود للغير دون وجه حق.

أما بالنسبة للمشرع اللبناني، فقد نصّ قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي رقم (81) لسنة 2018، الذي يُعتبر نافذًا، على تجريم فعل الاعتداء على سلامة البيانات الرقمية صراحةً في مادته رقم (112)، والتي جاء فيها ما يلي: "يعاقب بالحبس من ستة اشهر إلى ثلاث سنوات وبالغرامة من ثلاثة ملايين إلى مئتي مليون ليرة لبنانية او بإحدى هاتين العقوبتين كل من ادخل بيانات رقمية، بنية الغش، في نظام معلوماتي وكل من الغى او عدل، بنية الغش، البيانات الرقمية التي يتضمنها النظام المعلوماتي".

علماً بأن المشرع اللبناني قد عاقب، بموجب المادة (115) من ذات القانون، على محاولة جريمة الاعتداء على سلامة البيانات الرقمية بالعقوبة ذاتها المقررة للجريمة التامة المنصوص عليها في المادة (112).

وتجدر الإشارة أخيرًا إلى أن المشرع اللبناني أورد في قانون المعاملات الإلكترونية نصًا تجريميًا عامًا تنطبق أحكامه على جميع الجرائم المتعلقة بالأنظمة والبيانات المعلوماتية، وذلك بموجب المادة (114) التي نصت على أن "يعاقب بالحبس من ستة اشهر إلى ثلاث سنوات وبالغرامة من ثلاثة ملايين إلى مئتي مليون ليرة لبنانية او بإحدى هاتين العقوبتين كل من استورد او انتج او حاز او قدم او وضع في التصرف او نشر، دون سبب مشروع، جهازًا او برنامجًا معلوماتيًا او اي بيانات معدة او مكيفة، بهدف اقتراف اي من الجرائم المنصوص عليها في المواد السابقة من هذا الفصل".

من كل ما تقدم يتضح أن المشرع اللبناني قد أرسى حماية جزائية واضحة ومتكاملة للنظم الالكتروني والبيانات الرقمية المخزنة فيها حيث جرّم كافة الأفعال التي تشكل مساسًا بسلامة النظم والبيانات الالكترونية، وهذا يتناقض مع المشرع العراقي الذي أغفل حتى الآن وضع نصوص قانونية صريحة تضمن الحماية الجزائية اللازمة للنظم والبيانات الالكترونية، وبناءً عليه نهيب بالمشرع العراقي السير على النهج الذي تبناه المشرع اللبناني في تجريم الأفعال التي تمس سلامة النظم والبيانات الالكترونية، وذلك من خلال الإسراع في إنجاز التعديلات المطلوبة على مشروع قانون الجرائم الالكترونية المقدم من الحكومة العراقية إلى مجلس النواب منذ عام 2011، فعلى الرغم من مرور فترة طويلة لم يُقر المجلس هذا المشروع بصيغة قانون ملزم حتى تاريخ إعداد هذا البحث.

الخاتمة

أولًا: الاستنتاجات

1. تُعد جرائم الولوج والمكوث غير المشروع والاعتداء على سلامة الأنظمة والبيانات الإلكترونية من أخطر صور الإجرام المستحدث، لكونها تمس البنية التحتية للمعلومات وأمنها.

2. كشفت الدراسة عن قصور واضح في التشريع العراقي لعدم وجود قانون نافذ خاص بالجرائم الإلكترونية، وعدم ملاءمة النصوص التقليدية الواردة في قانون العقوبات لمواجهة هذه الجرائم ذات الطبيعة التقنية.

3. تبيّن أن مشروع قانون الجرائم الإلكترونية العراقي لسنة 2011، رغم تضمّنه نصوصًا تجريمية مهمة، إلا أنه لا يزال غير كافٍ من حيث الشمول والدقة والتوازن العقابي.

4. أظهر التشريع اللبناني، ولا سيما قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي لسنة 2018، تطورًا ملحوظًا في تجريم أفعال الاعتداء على الأنظمة والبيانات الإلكترونية، من خلال نصوص واضحة ومتكاملة تشمل الفعل التام والشروع.

5. أثبتت المقارنة أن التجربة التشريعية اللبنانية تشكّل نموذجًا صالحًا للاسترشاد به عند بناء الإطار القانوني العراقي المنشود.

ثانيًا: التوصيات

1. ضرورة الإسراع في إقرار قانون خاص بالجرائم الإلكترونية في العراق، يراعي الخصائص التقنية لهذا النوع من الجرائم ويواكب التطور التكنولوجي المتسارع.

2. إعادة النظر في مشروع قانون الجرائم الإلكترونية لسنة 2011، ولا سيما فيما يتعلق بتوحيد السياسة العقابية بين فعلي الولوج والمكوث غير المشروع متى ما ترتبت عليهما نتائج جرمية متشابهة.

3. تبني نصوص جزائية صريحة تجرّم الاعتداء على سلامة البيانات الرقمية بوصفها محلًا مستقلًا للحماية الجنائية.

4. الإفادة من التجربة التشريعية اللبنانية في تنظيم الجرائم الإلكترونية، خصوصًا في مجال تجريم الشروع وتوسيع نطاق الحماية الوقائية للنظم والبيانات الإلكترونية.

5. تعزيز التأهيل القضائي والتقني للقضاة وأعضاء الادعاء العام بما يضمن حسن تطبيق النصوص الجزائية المتعلقة بالجرائم الإلكترونية.

قائمة المراجع:

أبو الفتوح عبد العظيم الحمامي، عمر .(2010) *الحماية الجنائية للمعلومات المسجلة إلكترونيًا (دراسة مقارنة)* .القاهرة: دار النهضة العربية.

بوكر، رشيدة .(2020) *الحماية الجزائية للتعاملات الإلكترونية* .ط1. بيروت: منشورات الحلبي الحقوقية.

بوتاني، دلخار صلاح .(2016) *الحماية الجنائية الموضوعية للمعلومات (دراسة مقارنة)* .ط1. الإسكندرية: دار الفكر الجامعي.

حجازي، عبد الفتاح بيومي .(2006) *مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي (دراسة متعمقة في القانون المعلوماتي)* .ط1. الإسكندرية: دار الفكر الجامعي.

خليفة، محمد مسعود محمد .(2006) *الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن* .رسالة ماجستير، كلية الحقوق، جامعة الإسكندرية.

خلاف، علاء عبد الباسط .(2004) *الحماية الجنائية لوسائل الاتصال الحديثة* .بدون دار نشر وبدون مكان نشر.

رمضان، مدحت عبد الحليم .(2012) *الحماية الجنائية للتجارة الإلكترونية (دراسة مقارنة)* .القاهرة: دار النهضة العربية.

زين الدين، بلال أمين .(2008) *جرائم نظم المعالجة الآلية للبيانات* .الإسكندرية: دار الفكر الجامعي.

زايد، هبة حسين محمد .(2015) *الحماية الجنائية للصفقات الإلكترونية (دراسة مقارنة)* .مصر: دار الكتب القانونية.

الصابغ، عماد .(2000) *نظم المعلومات (ماهيتها ومكوناتها)* .ط1. عمّان: دار الثقافة للنشر والتوزيع.

الصغير، جميل عبد الباقي .(1992) *القانون الجنائي والتكنولوجيا الحديثة: الجرائم الناشئة عن استخدام الحاسب الآلي* . القاهرة: دار النهضة العربية.

عالية، سمير .(2020) *الجرائم الإلكترونية في القانون الجديد رقم .(81/2018)* ط1. بيروت: منشورات الحلبي الحقوقية.

قارة، آمال .(2007) *الحماية الجزائية للمعلوماتية في التشريع الجزائري* .ط2. الجزائر: دار هومة للطباعة والنشر والتوزيع.

قورة، نائلة عادل محمد فريد .(2005) *جرائم الحاسب الآلي الاقتصادية (دراسة نظرية وتطبيقية)* .ط1. بيروت: منشورات الحلبي الحقوقية.

الكعبي، محمد عبيد .(2009) *الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت (دراسة مقارنة)* .القاهرة: دار النهضة العربية.

القهوجي، علي عبد القادر .(2000) *الحماية الجنائية للبيانات المعالجة إلكترونيًا (دراسة مقارنة)* .بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة.

المومني، نهلا عبد القادر .(2010) *الجرائم المعلوماتية* .ط2. عمّان: دار الثقافة للنشر والتوزيع.

مصطفى، محمود محمود .(1984) *شرح قانون العقوبات – القسم الخاص* .ط8. القاهرة: مطبعة جامعة القاهرة.

الشوا، محمد سامي .(2003) *ثورة المعلومات وانعكاسها على قانون العقوبات* .القاهرة: مطابع الهيئة المصرية العامة للكتاب.

عطاالله، شيماء عبد الغني محمد .(2007) *الحماية الجنائية للتعاملات الإلكترونية* .الإسكندرية: دار الجامعة الجديدة.

طعباش، أمين .(2015) *الحماية الجنائية للمعاملات الإلكترونية* .ط1. الإسكندرية: مكتبة الوفاء القانونية.

الرازقي، محمد معمر، وعبابنة، محمود أحمد .(2005) *جرائم الحاسوب وأبعادها الدولية* .عمّان: دار الثقافة للنشر والتوزيع.

قناة السومرية العراقية .(2024) *مسودة مشروع قانون الجرائم المعلوماتية العراقي لسنة 2011* .متاح على: www.alsumaria.tv

(تاريخ الاطلاع: 13 أغسطس 2024).