Ashur Journal of Legal and political Sciences (AJLSP) is published by the Iraqi Association for Legal Sciences
ISSN: 3005-3269, Vol 3(No.2), pages: 156 -176 (2026)
https://ashurjournal.com/index.php/AJLPS/about

Legislative response to cybercrime in Iraq: A comparative study

Assistant Lecturer. Abeer Jaafar Hattab Al-Jabri

University of Maysan / College of Medicine , eabir.mcm@uomisan.edu.iq

ARTICLE INFORMATION

Received:16 Feb 2026
Accepted:22 Feb 2026
Published:1 Jun 2026

Keywords:

-The crime
-Informatics
-the law

ABSTRACT

The world has witnessed a radical shift towards digitalization, leading to the emergence of new patterns of crime that transcend traditional boundaries of space and time, namely (cybercrime). This type of crime no longer targets individuals alone, but now threatens national security and the economies of countries, which has placed the Iraqi legal system in a real challenge to adapt traditional criminal rules to the nature of digital development and the new patterns that this development has produced in the Criminology, This matter has raised many questions about the nature of that crime and the means required to prove it under Iraqi law and some Arab legislations.

© 2024 , This is an open access article under the cc BY-NC-ND license http://creativecommons.org/licenses/by/4.0/

مجلة آشور للعلوم القانونية والسياسية تصدر عن الجمعية العراقية للعلوم القانونية
المجلد الثالث (العدد الثاني)، الصفحات: 156- 176، (2026) ISSN: 3005-3269
https://ashurjournal.com/index.php/AJLPS/about

المواجهة التشريعية لجرائم المعلوماتية في العراق - دراسة مقارنة

م.م عبير جعفر حطاب الجابري

جامعة ميسان / كلية الطب ، eabir.mcm@uomisan.edu.iq

معلومات المقالة

تاريخ الاستلام : ١٦ شباط ٢٠٢٦
تاريخ القبول : ٢٢ شباط ٢٠٢٦
تاريخ النشر : ١ حزيران ٢٠٢٦

الملخص

شهد العالم تحولاً جذرياً نحو الرقمنة، مما أدى إلى ظهور نمط مستحدث من الجرائم يتجاوز الحدود التقليدية للمكان والزمان، وهي "الجريمة المعلوماتية". هذا النوع من الإجرام لم يعد يستهدف الأفراد فحسب، بل بات يهدد الأمن القومي واقتصاد الدول، مما وضع النظام القانوني أمام تحدٍ حقيقي في مواءمة القواعد الإجرائية التقليدية مع طبيعة التطور الرقمي وما افرزه ذلك التطور من أنماط جديدة في علم الاجرام, الامر الذي اثار تساؤلات عديدة حول طبيعة تلك الجريمة , وما هي الوسائل اللازمة لأثبات تلك الجريمة في التشريع العراقي وبعض التشريعات العربية.

الكلمات المفتاحية:

- الجريمة
- المعلوماتية
- القانون

© 2024 , This is an open access article under the cc BY-NC-ND license http://creativecommons.org/licenses/by/4.0/

المقدمة

أن ظهور شبكة الانترنت وتطورها بهذا الشكل الواسع والمضطرد، وازدياد أعداد المستخدمين للشبكة الالكترونية في العالم بـ(حوالي 4 مليار مستخدم)، جعل الانترنت وسطاً ملائماً للتخطيط ولتنفيذ عدد من الجرائم بعيداً عن رقابة وأعين الجهات الأمنية. فتسارع إيقاع التقدم التكنولوجي والتقني الهائل ، وظهور الفضاء الإلكتروني ووسائل الاتصالات الحديثة كالفاكس والإنترنت وسائر صور الاتصال الإلكتروني عبر الأقمار الصناعية استغله مرتكبو الجرائم الإلكترونية، في تنفيذ جرائمهم التي لم تعد تقتصر على إقليم دولة واحدة ، بل تجاوزت حدود الدول ، وهي جرائم مبتكرة ومستحدثة تمثل ضربا من ضروب الذكاء الإجرامي ، استعصى إدراجها ضمن الأوصاف الجنائية التقليدية في القوانين الجنائية الوطنية والأجنبية ففي الوقت الذي قامت فيه التكنولوجيا على سبيل المثال بتقريب المسافات بين الشعوب، من خلال توفيرها للعديد من وسائل الاتصالات ووسائل التنقل التي لم تكن معروفة من قبل، كـ (الإنترنت) وشبكة المعلومات العالمية (web) ، والبريد الإلكتروني أو الرقمي (E-mail) ، والمجاميع الإخبارية (New Groups) ، ومواقع نقل الملفات (File Transferee Protocol) وغرف المحادثة (Chatting Rooms) ، نجد أن تلك التكنولوجيا أفرزت الكثير من السلبيات، لعل أهمها كان صعوبة احتفاظ الفرد بخصوصياته جراء انتشار الكثير من الوسائل السهلة، والتي يستخدمها أشخاص يعرفون باسم قراصنة الشبكة العنكبوتية(Hackers Internet) ويقومون من خلالها باقتحام خصوصية الفرد رغما عنه ، أو الاعتداء على الاشخاص من خلال استخدام تلك الشبكة المعلوماتية بالسب والقذف والتشهير وغيرها من الافعال التي يجرمها القانون.

اولاً / الدراسات السابقة :

"الجريمة المعلوماتية" للباحثين (محمد علي سالم وحسون عبيد هجيج) المنشور عام 2007 , ركزت دراسة "هذه الدراسة على تأصيل مفهوم الجريمة الإلكترونية كظاهرة قانونية واجتماعية حديثة ظهرت مع تطور تقنيات المعلومات.

رسالة ماجستير: "إجراءات التحقيق في الجريمة الإلكترونية" (بخي فاطمة الزهراء، جامعة المسيلة - الجزائر، 2014) :ركزت على الجوانب الإجرائية في التشريع الجزائري والمقارن، وتناولت كيفية ممارسة سلطات التحقيق لمهامها في الفضاء السيبراني.

رسالة ماجستير: "إثبات الجريمة الإلكترونية" (ثنيان ناصر آل ثنيان، جامعة نايف للعلوم الأمنية، 2012) :انصبت هذه الدراسة على إشكالية الدليل الرقمي وكيفية إثبات الجريمة المعلوماتية.

رسالة ماجستير: "الجرائم الإلكترونية في التشريع الفلسطيني" (يوسف خليل يوسف، الجامعة الإسلامية - غزة، 2013) :تناولت التجربة الفلسطينية في مواجهة هذه الجرائم، وتطرقت لمسائل الضبط والمعاينة.

يتميز بحثنا "المواجهة التشريعية لجرائم المعلوماتية في العراق" عن الدراسات السابقة بتركيزه المباشر على "الفراغ التشريعي "في العراق، حيث قدم المعالجات التي تجعله يغطي فجوات لم تتناولها الدراسات الأخرى بشكل مباشر:

1: التركيز على مشروع القانون العراقي :(2011/2012) بينما ركزت الدراسات السابقة على تشريعات مستقرة (مثل القانون المصري أو الأردني أو الفلسطيني)، قام بحثنا بتفكيك "مسودة "القانون العراقي ونقد ركاكة صياغتها، وبيان تعارضها مع الدستور والمعايير الدولية، مما يجعل بحثك مرجعاً نقدياً للمشرع العراقي.

2: دمج الجانب الموضوعي بالإجرائي في بيئة "غير مقننة :"في حين أن الدراسات السابقة تتحدث غالباً عن قوانين نافذة، فإن بحثنا عالج إشكالية (تطبيق القواعد القديمة على جرائم حديثة) في ظل غياب قانون خاص، وهو تحدٍ قانوني فريد يواجه الممارسة القضائية العراقية حالياً.

3: تأصيل الاختصاص المكاني في غياب قواعد خاصة :عالج بحثنا إشكالية تطبيق القانون الجنائي من حيث المكان بوضوح، منتقداً اعتماد المشرع العراقي على قانون العقوبات التقليدي (1969) في جرائم عابرة للحدود، ومقارناً ذلك بوضوح بالتشريعات المصرية والأردنية التي وضعت قواعد مكانية خاصة للجرائم المعلوماتية.

ثانياً/ اهمية البحث :

تكمن اهمية البحث انه يسعى لتقديم رؤية تحليلية للمشرع العراقي، مؤكداً على أن مواجهة الجريمة المعلوماتية لا تتطلب تشريعاً عقابياً فحسب، بل تستلزم نظاماً إجرائياً مرناً يمنح السلطات التحقيقية صلاحيات تقنية واسعة، مع الحفاظ على الضمانات الدستورية للأفراد، وصولاً إلى منظومة عدالة جنائية رقمية متكاملة.

ثالثاً / مشكلة البحث:

تكمن الإشكالية في قصور النصوص العقابية التقليدية عن استيعاب مفاهيم مثل "الاختراق"، "البيانات المشفرة"، و"التفتيش الافتراضي". كما يبرز تساؤل جوهري حول مدى كفاية مشروع قانون جرائم المعلوماتية العراقي في تنظيم إجراءات التفتيش والضبط والمعاينة، مقارنة بالتشريعات العربية الرائدة التي قطعت شوطاً كبيراً في هذا المضمار.

رابعاً/ منهجية البحث:

تم الاستعانة بالمنهج الوصفي التحليلي: لتحليل نصوص مسودة قانون جرائم المعلوماتية العراقي وتفكيك عناصر الجريمة وخصائصها, كذلك المنهج المقارن: لعقد موازنة بين التشريع العراقي والتشريعات العربية لاستنباط أفضل الممارسات القانونية.

خامساً / نطاق البحث:

يمتد نطاق البحث ليغطي شقي المواجهة التشريعية للجرائم المعلوماتية في العراق؛ حيث يركز الجانب الموضوعي على دراسة سياسة المشرع العراقي في تحديد أركان هذه الجرائم، وتكييفها القانوني، وتناسب العقوبات المقررة لها مع جسامة الاعتداءات الرقمية. كذلك يشمل الجانب الإجرائي، من خلال تحليل القواعد القانونية المنظمة لعمليات الضبط والتحقيق الرقمي، وحجية الأدلة المستمدة من الفضاء السيبراني، مع استقراء مدى توافق هذه الإجراءات مع مقتضيات العدالة الجنائية الرقمية.

سادساً /خطة البحث:

اعتمد الباحث في تقســـيم البحث الى مبحثين : يتناول الأول منه الاطار المفاهيمي للجريمة المعلوماتية من تعريفها وخصائصها اما المبحث الثاني: فقد تم بيان اهم وسائل جمع الأدلة في الجريمة المعلوماتية والتي تشمل التفتيش والضبط والمعاينة.

المبحث الأول

الاطار المفاهيمي للجريمة المعلوماتية

اضحت دراسة الجريمة المعلوماتية ضرورة قانونية ملحة , نظراً لما تثيره تلك الجريمة من إشكالات تتصل بصعوبة حصر مفاهيمها وتعدد خصائصها التي تميزها عن الجريمة التقليدية. فبينما تستند الجريمة التقليدية إلى عناصر مادية ملموســـة واضـــحة الابعاد ، تغوص الجريمة المعلوماتية في عالم مادي ومعنوي , حيث الســـرعة الفائقة، والحدود المتلاشية، والاحترافية العالية.

وبناءً على ما تقدم، ولأجل الإحاطة بالأبعاد النظرية لهذا النوع من الجرائم، يتوجب علينا تفكيك الإطار المفاهيمي لها من خلال الوقوف على تعريفها، تمييزها، وبيان سماتها الجوهرية , وهو ما سنقوم بمعالجته عبر تقسيم هذا المبحث إلى مطلبين أساسيين:

المطلب الاول

ماهية الجريمة المعلوماتية

سوف نقسم هذا المطلب الى ثلاثة فروع سيكون الاول منها : التعريف بالجريمة المعلوماتية ، أما الفرع الثاني فسيكون عن خصائص الجرائم المعلوماتية في حين سيخصص الفرع الثالث الى بيان موضوع الجريمة الالكترونية .

الفرع الاول

التعريف بالجريمة المعلوماتية

أن الجريمة من الناحية القانونية التقليدية هي كل ســـلوك خارجي ايجابيا كان ام ســـلبيا حرمه القانون وقرر له عقابا اذا صـدر عن أنسـان مسـئوول ، وفي اللغة فأن مصـطلح المعلوماتية هو مشـتق من الكلمة الانكليزية (Information) ، فالمعلومة لغة مشـتقة من كلمة" علم "، ودلالتها فيها و تدور بوجه عام حول المعرفة التي يمكن نقلها أو اكتسـابها . وهناك العديد من التعريفات التي سـعت من أجل إدراك المعنى المراد بمصـطلح "المعلوماتية. ولا يوجد إلى يومنا هذا نص قانوني يعطي تعريفا جامعا مانعا للمعلوماتية، ومن جملة التعريفات لهذا المصطلح ، ما أفاض به القانون الفرنسي الصـادر في 1982 الخاص بالاتصـالات السمعية و البصـرية أذ عرفها بأنها" صـوت أو صـور أو وثائق أو بيانات أو رسـائل من أي نوع. وكذلك عرفها قانون الاونسيرال (Uncitral)[1] ، في المادة (2) ، بأنها "النظام الذي يستخدم لإنشاء الرسائل والبيانات أو إرسالها أو إستلامها أو تخزينها لتجهيزها على أي وجه أخر".

بينما عرفها قانون المعاملات الالكترونية الاردني رقم 85 لسنة 2001م ، في المادة (10/2) ، بأنها :" النظام الإلكتروني المستخدم لإنشاء رسائل المعلومات أو إرسالها أو تسلمها أو معالجتها أو تخزينها أو تجهيزها على أي وجه أخر" .

كذلك عرفها قانون إمارة دبي الخاص بالمعاملات والتجارة الإلكتروني رقم 02 لسنة 2002م، في المادة(6/2) ، بأنها:" نظام إلكتروني لإنشاء أو إستخراج أو إرسال أو إستلام أو تخزين أو عرض أو معالجة المعلومات أو الرسائل إلكترونيا". أما مشروع قانون جرائم المعلوماتية العراقي لسنة 2011م ، فأنه قد عرفها في المادة (1/ثاني عشر) بأنها:"البيانات والنصوص والصور والاشكال والاصوات والرموز وقواعد البيانات وبرامج الحاسوب وما شابه ذلك التي تنشأ أو تخزن أو تعالج أو ترسل بالوسائل الالكترونية".وقد عرفها قانون التوقيع الالكتروني والمعاملات الالكترونية رقم 78 لسنة 2012م في المادة (1/ثالثا) بأنها :" البيانات والنصوص والصور والاشكال والاصوات والرموز وما شابه ذلك التي تنشأ او تدمج او تخزن او تعالج او ترسل او تستلم بوسائل الكترونية".

بينما الجريمة المعلوماتية كمصطلح عرفته بعض التشريعات المقارنة ومنها القانون الامريكي"بأنها الاستخدام الغير مصرح به لأنظمة الكومبيوتر المحمية أو ملفات البيانات أو الاستخدام لمتعمد الضار لأجهزة الكومبيوتر أو ملفات البيانات وتتروح خطورة تلك الجريمة ما بين جنحه من الدرجة الثانية وجناية من الدرجة الثالثة" [2]. وعارفها القانون السعودي المعروف بنظام مكافحة الجرائم المعلوماتية بأنها :" أي فعل يرتكب متضمناً أستخدام الحاسب الالي أو الشبكة المعلوماتية بالمخالفة لإحكام هذا النظام"[3]. ويلاحظ أن المشرع المصري في قانون مكافحة جرائم تقنية المعلومات لسنة 2018م ، وبالرغم من النص على تسمية الجريمة الالكترونية في نصوصه (45) ، الا أنه لم يعطي تعريفا لهذه الجريمة ، بل أكتفى بالنص على صورها وأساليب أرتكابها.

ونعتقد أن التعريفات المتقدمة بأنها أنها إنصبت في مجرى واحد معتمده في تعريف نظام المعلومات على تعداد الوظائف التي يقوم بها أو ينجزها هذا النظام والتي تمثل طرق المعالجة المعلوماتية. وهذا ما انتهجه المشرع العراقي في مشروع قانون جرائم المعلوماتية لسنة 2011م، فعلى الرغم من النص على هذه الجرائم في المادة (2) من هذا القانون ، والتي أسماءها بجرائم الحاسوب ، الا أنه لم يعطي لها تعريفا في هذا القانون[4] ، وتجدر الاشارة الى أن مشروع القانون المذكور قد عدد الجرائم الالكترونية التي تقع تحت طائلته على وجه التحديد وعدد مجموعة من العقوبات على استخدام أجهزة الحاسوب فيما--- له علاقة بالعديد من الأنشطة الممنوعة، مثل الاحتيال المالي والاختلاس المادة (7)، وغسيل الأموال المادة (10)، وتعطيل الشبكات المادة (14) ، والمراقبة غير المشروعة المادة (15)، والمادة (16) ، والاعتداءات على الملكية الفكرية المادة (21) .

ونرى مما تقدم بان المشرع لم يتعرض الى جرائم المعلوماتية التي يرتكبها الاحداث ، ومن يتمعن في نصوص المشروع يلمس ركاكة صياغة النصوص القانونية ، ويشعر انها كتبت على عجالة لا ينسجم مع السياسة القانونية التي يتم اعتمادها في الوقت الحاضر ، بالإضافة الى تأكيد الكثير أن أحكام مشروع القانون متعارضة مع القانون الدولي والدستور العراقي، ما ولد العديد من ردود الافعال على المستوى المحلي والدولي[5] ، أدى الى عدم أقراره حتى اليوم.

الفرع الثاني

خصائص الجريمة المعلوماتية

تتميز الجريمة المعلوماتية بمجموعة من الخصائص المميزة لها نوجزها فيما يلي: [6].

1- قلة عدد الحالات التي تم اكتشافها بالفعل مقارنة بما يتم اكتشافه من الجرائم التقليدية.

2- ارتفاع الخسارة الناجمة عن الجرائم المعلوماتية مقارنة بالجرائم التقليدية.

3-عدم اتسام الجريمة المعلوماتية بالعنف الذي تتميز به غيرها من الجرائم التقليدية، حتى أنه يقال أنه لا يوجد شعور حقيقي بعدم الأمان في مواجهة الجريمة المعلوماتية كالذي يوجد بصـــورة دائمة في مواجهة غيرها من الجرائم. فالصـورة التقليدية للمجرم تكاد تختفي في هذه الجرائم بل و على العكس من ذلك فالمجرم المعلوماتي عادة ما يكون ينتمي إلى مستوى اجتماعي مرتفع عن غيره من المجرمين ونادراً يكون محترفا للإجرام أو عائد كما أنه لا ينظر إليه كمجرم بالمعنى المتعارف لهذه الكلمة.

3- غياب الشعور العام بعدم أخلاقية الفعل أو بمساس بمصـالح و قيم يحرص المجتمع على حمايتها بل إن الكثير من العاملين في مجال المعلوماتية لا يجدون حرجا في استعمال الشفرات و الدخول إلى أنظمة الحاسبات الآلية بطريقة غير مشروعة.

4- تقع الجريمة المعلوماتية في مجال المعالجة الآلية للمعلومات وتســـتهدف المعنويات لا الماديات ، وهي بالتالي أقل عنفاً وأكثر صعوبة في الإثبات لأن الجاني مرتكب هذه الجريمة لا يترك وراءه أي أثر مادي خارجي ملموس يمكن فحصه ، وهذا يعسر إجراءات اكتشاف الجريمة ومعرفة مرتكبها ، بخلاف الجريمة التقليدية التي عادة ما تترك وراءها دليلا ماديا أو شـهادة شـهود أو غيرها من أدلة الإثبات ، كما أن موضـوع التفتيش والضـبط قد يتطلب أحيانا امتداده إلى أشخاص آخرين غير المشتبه فيه أو المتهم .

5- الجريمة المعلوماتية ذات بعد دولي ، أي أنها عابرة للحدود ، فهي قد تتجاوز الحدود الجغرافية باعتبار أن تنفيذها يتم عبر الشبكة المعلوماتية ، وبالتالي تعدد الاماكن التي تتعلق بالجريمة وتنازع قوانين الدول الواجبة التطبيق بالإضافة الى اختلاف الاجراءات الجنائية من دولة الى اخرى ( )، وهو ما يثير في كثير من الأحيان تحديات قانونية إدارية فنية ، بل وسياسية بشأن مواجهتها لاسيما فيما يتعلق بإجراءات الملاحقة الجنائية.

المطلب الثاني

خصوصية الجريمة المعلوماتية من الناحية الموضوعية

ان الجريمة المعلوماتية تمتاز بخصـائص تنفرد بها وترسم خطوطاً للتمييز بينها وبين الجرائم الاخرى سبق وان تطرقنا لها , ولا يتوقف الامر على ذلك , اذ تنفرد من حيث الطبيعة القانونية عن الجرائم التقليدية , هذا من جانب ومن جانب اخر يكون لها خصـوصـية من حيث الاختصـاص المكاني , اذ سـبق وصـفها بأنها جريمة عابرة للحدود الوطنية , وهذا الامر يثير اشكالية تحديد مكان وقوع الجريمة ومن ثم تحديد الدولة التي ينهض اختصاصـها في نظر الدعوى فيها , كما لها مظاهر تمييز من حيث اعتبار بعض صور المساهمة فيها جرائم مستقلة.

الفرع الاول

الطبيعة القانونية للجريمة المعلوماتية

في مجال تحديد الطبيعة القانونية للجريمة المعلوماتية تثار مسائل متعددة منها تحديد الطبيعة القانونية للجريمة المعلوماتية من خلال تحديد طبيعة المعلومة من الناحية القانونية , هل هي من قبيل القيم القابلة لاستئثار , ومن ثم يمكن ان تكون محلاً للاعتداءات القانونية عليها, ولما كانت الجرائم المعلوماتية الواردة في مشروع قانون الجريمة المعلوماتية العراقي والقوانين المقارنة لا تقتصر على الجرائم المعلوماتية التي يكون محلها الاعتداء على المعلومة , اذ تشمل صوراً متعددة للجرائم , التي سبق وان تناولها المشرع بالتجريم في قانون العقوبات العراقي [7] , لذا كان لابد من عرض توجهات الفقه في الجرائم المعلوماتية المحضة لو صحت تسميتها , ثم بيان خصوصية الجريمة المعلوماتية بشكل عام.

لقد ظهر اتجاهات في مجال تحديد الطبيعة القانونية , لذا سنتاولها تباعاً :

اولاً : الاتجاه التقليدي : يرى هذا الاتجاه وفقاً للقواعد العامة فأن الاشياء المادية وحدها هي من تقبل الحيازة والاستحواذ , وان محل جريمة السرقة يجب ان يكون مادياً , اي له كيان مادي ملموس حتى يمكن انتقاله وحيازته عند طريق الاختلاس المكون للنشاط الاجرامي في جريمة السرقة , ولما كانت المعلومة ذات طبيعية معنوية , ولا يمكن اعتبارها من القيم القابلة للحيازة والاستحواذ , الا في ضوء حقوق الملكية الفكرية , لذ تستبعد المعلومات ومجرد الافكار من مجال السرقة , مالم تكن مسجلة على اسطوانة او شريط , فاذا ما تم سرقة احدى هاتين الدعامتين الخارجية , فلا تثور مشكلة قانونية في تكييف الواقعة على انها سرقة مال معلوماتي ذو طبيعة مادية , وانما تثور المشكلة عندما نكون امام سرقة مال معلوماتي غير مادي وبالنظر الى ان للمعلومات طبيعة معنوية , لذا فهي غير قابلة للاستحواذ المادي, ولان النتيجة التي يتوصل لها هذا الاتجاه غير منطقية والمتمثلة بعدم العقاب , او عدم تجريم الاستيلاء , يرون ان هذا التجريم يجد اساسه في الظروف التي اقترنت بها الاستيلاء , اي فيما اذا كانت المعلومة على اسطوانة او ما شابه ذلك .

ثانياً : الاتجاه الحديث : تعد المعلومة وفقاً لهذا الاتجاه قيمة قابلة للاستحواذ , اي المعلومة تقيم وفق قيمة السوق متى ما كانت غير محضورة تجارياً , وانها منتج يغض النظر عن دعامتها المادية واستند هذا الاتجاه في اضفاء وصف القيمة على المعلومة لحجتين الاولى :قيمتها الاقتصادية (حيث تقيم المعلومة وفقاً لسعر السوق والثانية علاقة التبني التي تجمع بينها وبين مؤلفها , وبذلك فأن هذا الاتجاه يرى ان المعلومة قيمة ولكن الاختلاف وقع في هل تعد من قبيل القيم المستحدثة اما انها تندرج في مجموعة قيم موجودة من قبل اذ هي مخصصة ومعدة سلفاً من قبيل الاشياء المعنوية , ومن ثم خصائص حق الملكية تنطبق عليها مع مالها من ذاتية وخصوصية من الناحية المدنية والتجارية مع ذلك لا تشكل عائقاً في دخولها ضمن القيم التي يحميها قانون العقوبات[8].

ومن هنا تظهر الطبيعة القانونية لهذه الجريمة من خلال المجال الذي يمكن ان ترتكب فيه والمحل الذي يمكن ان ترتكب عليه , فالتطور السريع في مجال المعلوماتية قد يفسح المجال لاقتناء وسائل الالكترونية تمكن المتجاوزين من ارتكاب

جرائم مختلفة لأن الاجرام المعلوماتي يتعلق بكل سلوك غير مشروع في مجال المعالجة الالية للبيانات او ادخال المعلومات ونقلها ومن ثم يتحتم ضمه الى نطاق القانون الجنائي على الرغم من ان معظم عاجزة عن مواكبة التطور المعلوماتي او ولما يحتويه من فراغ تشريعي في هذا المجال [9].

الفرع الثاني

تطبيق القانون الجنائي من حيث المكان في الجريمة المعلوماتية

ان الذي يميز الجريمة المعلوماتية بأنها غير مقيدة برقعة جغرافية معينة ,مفاد ذلك ان البيئة المعلوماتية التي تحصل فيها هذه الجريمة لا تعترف بالحدود الجغرافية للدول , حيث لا حدود مرئية او ملموسة تعرقل نقل المعلومات عبر الدول المختلفة بعد ظهور شبكات الاتصال , اذ استطاعت ان تربط اعداد من الحاسبات الالية عبر الدول , لذلك اصبح امر الانتحال يسيراً ' لذا هذه الميزة سهلت امكانية ارتكاب الجريمة عن بعد فقد يكون الجاني من دول معينة والمجنى عليه من دولة اخرى .

على الرغم من المشرع العراقي قد وضع مشروعاً للجرائم المعلوماتية , وكان هذا المشروع واسعاً بعض الشئ الا انه خلا من قواعد خاصة في مجال تحديد نطاق تطبيق القانون الجنائي العراقي في الجريمة المعلوماتية , الا ان هذا القانون بين في المادة (30) منه مايلي (تطبق القوانين التالية في كل مالم يرد به نص , اولاً : قانون العقوبات العراقي رقم 11 لسنة 19969 , وبذلك يتم العودة لأحكام قانون العقوبات بهذا الخصوص , ووفقاً لقانون العقوبات ت تعد الجريمة واقعة في اقليم العراقي وفقاً للقانون العراقي في حالات معينة بينتها المادة السادسة من قانون العقوبات العراقي مايلي (تسري احكام هذا القانون على جميع الجرائم التي ترتكب في العراق وتعتبر الجريمة المرتكبة في العراق , اذا وقع فيه فعل من الافعال المكونة لها , او اذا تحققت فيه نتيجتها او كان يراد ان تحقق فيه , وفي جميع الاحوال يسري القانون على كل جريمة وقعت كلها او بعضها في العراق ولو كانت مساهمته في الخارج سواء كان فاعلاً او شريكاً) , اي العبرة بوقوع العمل التنفيذي المكون للجريمة – السلوك الاجرامي – فوق اقليم الدولة بصورة كلية او جزئية , ذلك ان العمل المكون للجريمة واعني به السلوك الاجرامي المكون لها , قد يتكون من فعل واحد , وقد يتكون من عدة افعال , اما الاعمال التحضيرية فلا عبرة بها , كذلك لا اهمية للأعمال اللاحقة , والعمل التنفيذي قد يتكون من عدة افعال العبرة بوقوع جزء منه في اقليم الدولة [(10)] .

وعلى خلاف توجه المشرع العراقي في مشروع قانون الجرائم المعلوماتية بين قانون الجرائم الالكترونية المصري نطاق تطبيقه من حيث المكان اذ جاء في المادة الثالثة منه مايلي (مع عدم الاخلال باحكام الباب الاول من قانون العقوبات تسري احكام هذا القانون على كل من ارتكب خارج جمهورية مصر العربية من غير المصريين جريمة من الجرائم المنصوص عليها في هذا القانون , متى كان هذا الفعل معاقباً عليه في الدولة التي وقع تحت اي وصف قانوني , وذلك في الاحوال الاتية :

1.اذا ارتكب الجريمة على متن اي وسيلة من وسائل النقل الجوي او البري وكانت مسجلة في جمهورية مصر العربية او تحمل علمها .

2.اذا كان المجنى عليهم او احدهم مصرياً .

3. اذا تم الاعداد للجريمة او التخطيط او التوجيه او الاشراف عليها او تمويلها في جمهورية .

4.اذا ارتكبت الجريمة بواسطة جماعة اجرامية تمارس انشطة اجرامية في اكثر من دولة من بينها جمهورية مصر العربية.

5.اذا كان من شأن الجريمة الحاق الضرر بأي من مواطني جمهورية مصر العربية او المقيمين فيها , او بأمنها او بأي من مصالحها في الداخل او الخارج .

6.اذا وجد مرتكب الجريمة في جمهورية مصر العربية بعد ارتكابها ولم يتم تسليمه . وكذلك تبنى المشرع الاردني قواعد خاصة في مجال تطبيق القانون من حيث المكان في الجرائم المعلوماتية , اذ اورد نصاً خاصاً في قانون جرائم انظمة المعلومات , اذ جاء في المادة 16 منه ما يلي (يجوز اقامة دعوى الحق العام والحق الشخصي على المشتكى عليه امام القضاء الاردني اذا ارتكبت اي من الجرائم المنصوص عليها في هذا القانون بأستخدام انظمة معلومات داخل المملكة او الحقت اضراراً باي من مصالحها او بأحد المقيمين او ترتيب اثار الجريمة فيها كلياً او جزئياً او ارتكبت من احد الاشخاص المقيمين فيها) .

المبحث الثاني

وسائل جمع الأدلة في الجرائم المعلوماتية

وسائل جمع الأدلة هي مجموعة من الأعمال التي ترى السلطة المختصة ملاءمة القيام بها لكشف الحقيقة بالنسبة لواقعة معينة يهتم بها قانون العقوبات . وحيث إن الاستخدام غير المشروع لتقنية الحاسب الآلي والانترنت رتب العديد من الإشكاليات الإجرائية في مجال إجراءات الملاحقة الجنائية التي تتبع من أجل كشف الجريمة وإقامة الدليل على وقوعها ونسبتها إلى مرتكبيها الذين يستخدمون التقنية المتطورة في ارتكابها وفي إخفاء معالمها وعدم ترك أية آثار مادية دالة عليها ، جميع ذلك أدى إلى تدخل مشرعي بعض الدول لمواجهة هذا النوع من الجرائم من خلال إصدار قوانين خاصة بملاحقتها وتنظيم الإجراءات التي تناسبها دون مساس بحقوق الأفراد وحرياتهم الأساسية.

المطلب الأول

التفتيش في الجرائم المعلوماتية

يعد التفتيش من أهم وأخطر إجراءات التحقيق لمساسه بالحريات الخاصة التي تحميها الدساتير والقوانين ، والتفتيش إجراء قانوني يهدف الى كشف أدلة الجريمة التي وقعت أو المحتمل وقوعها وتزداد خطورة التفتيش بشكل كبير في

الجرائم المعلوماتية والسبب في ذلك يرجع الى أن محل التفتيش فيها هو نظام المعالجة الإلكترونية وهذا النظام ذو طابع غير مادي ، أذ أنه مجرد معلومات الكترونية ليس لها مظهر مادي محسوس في العالم الخارجي كما هو الحال في الجرائم
التقليدية كما أنه قد لا يقتصر على المعلومات الموجودة في كمبيوتر معين ، بل أنه قد يتجاوز الى أنظمة ومعلومات أخرى مرتبطة به ولو أختلف مكان وجودها .

الفرع الأول

تعريف التفتيش في الجرائم المعلوماتية

لم تتضمن التشريعات الجنائية تعريفاً للتفتيش بوجه عام وأنما أكتفت بالنص على أنه وسيلة من وسائل جمع الأدلة [11] لذلك تولى الفقه والقضاء مهمة وضع تعريف للتفتيش فقد عرف فقهاً بتعارف عدة نذكر منها تعريفه بأنه " إجراء من إجراءات التحقيق يقوم به موظف مختص طبقاً للإجراءات المقررة قانوناً في محل يتمتع بالحرمة بهدف الوصول الى أدلة مادية لجناية أو جنحة تحقق وقوعها لإثبات أرتكابها أو نسبتها الى المتهم " [12].
كما عرف بأنه " إجراء تحقيق يقوم به موظف مختص للبحث عن أدلة مادية لجناية أو جنحة وذلك في محل خاص أو لدى شخص وفقاً لأحكام القانون " وعرف أيضاً بأنه " إجراء من إجراءات التحقيق تقوم به سلطة حددها القانون يستهدف البحث عن الأدلة المادية لجناية أو جنحة تحقق وقوعها في محل خاص يتمتع بالحرمة بغض النظر عن أرادة صاحبه " [13] . كما عرف بأنه " البحث في مستودع سر شخص عن أشياء تفيد الكشف عن الجريمة ونسبتها إلى المتهم " [14].
أما تعريف التفتيش قضاءاً فنجد أن محكمة النقض المصرية عرفته بأنه " البحث عن عناصر الحقيقة في مستودع السر فيها " [15].
أما تعريف التفتيش في الجريمة المعلوماتية فقد عرف فقهاً بأنه " البحث عن طريق التفتيش والضبط عن البيانات المخزنة في النظام المعلوماتي للحاسب الآلي أو في دعامة تخزين المعلومات سواء كانت هذه البيانات مخزنة في جهاز واحد أو في منظومة اتصالات " [16] المجلس الأوربي بأنه " إجراء يسمح بجمع الأدلة المخزنة أو المسجلة بشكل ألكتروني " [17]
يتضح من خلال ما تم ذكره من تعاريف للتفتيش أنه لا يختلف في مدلوله القانوني بالنسبة للجرائم المعلوماتية عن مدلوله السائد في فقه الإجراءات الجنائية لذا يمكننا تعريف التفتيش في أطار الجرائم المعلوماتية بأنه " وسيلة من وسائل جمع الأدلة تقوم بها السلطة المختصة بهدف الدخول الى الأنظمة المعلوماتية للبحث في البرامج المستخدمة أو ملفات البيانات المخزنة والوصول الى أدلة تفيد في أثبات الجريمة ونسبتها الى المتهم بارتكابها .

الفرع الثاني

شروط التفتيش في الجرائم المعلوماتية

نظراً لكون أجراء التفتيش يتضـمن تقييداً للحرية الفردية ويمثل أعتداء على حرمة الحياة الخاصـة فيجب أن تتوافر فيه الضمانات والشروط القانونية اللازمة لصحته ، وفي ظل مشروع قانون جرائم المعلوماتية العراقي لسنة 2011 نجد أن المادة (24/ ثانياً) نصت على التفتيش بأعتباره أجراء من أجراءات جمع الأدلة حيث جاء فيها " لايجوز لجهات التحقيق المباشـرة بإجراءات التفتيش دون أمر من القاضـي المختص " كما نصـت المادة (30) من القانون نفسـه على " تطبق القوانين التالية في كل مالم يرد به نص في هذا القانون : ثانياً : قانون أصول المحاكمات الجزائية رقم (23) لسنة 1971 " . ومن خلال نص المادة (72) وحتى المادة (86) من قانون أصول المحاكمات الجزائية العراقي نجد أن المشرع في هذا القانون نص على إجراء التفتيش وكل مايتعلق بأحكامه بشـكل مفصـل ، وبالاسـتناد الى نص المادة (30) من قانون جرائم المعلوماتية العراقي يمكن تطبيق كل مانص عليه قانون اصـــول المحاكمات الجزائية ولم يرد به نص في هذا القـانون فيمـا يتعلق بـإجراء التفتيش ، ومن خلال نص المـادة (24/ثـانيـاً) والمواد (72 الى 86) من قـانون اصـــول المحاكمات الجزائية يتضـح أن هناك مجموعة من الضـوابط أو الشـروط الشـكلية التي ينبغي مراعاتها في إجراء التفتيش ، ويمكن بيانها بالاتي:

1- صدور أذن بالتفتيش في الجرائم المعلوماتية :

نصت المادة (24/ فـ2) من مشروع قانون جرائم المعلوماتية العراقي فنصت على " لايجوز لجهات التحقيق المباشرة بإجراءات التفتيش دون أمر من القاضي المختص" .

ويشـــترط في الأذن الصـــادر بالتفتيش أن يكون مكتوباً ومؤرخاً وموقعاً عليه وأن يكون واضـــحاً في الغرض منه كأن يحدد في الأمر ضـرورة العثور على سـلاح معين أو كتاب معين أو مال مسـروق أو قد يتضـمن الأمر بالتفتيش مجرد التفتيش للعثور على ماله علاقة بالجريمة [18].

هذا في مجال الجرائم التقليدية ، وهو مايشـــترط في الأذن بالتفتيش في الجرائم المعلوماتية على الرغم من عدم نص مشـروع قانون جرائم المعلوماتية العراقي على ذلك صـراحة ، ولكن بالرجوع الى نص المادة (30 / ثانياً) منه والتي أحالت الى تطبيق أحكام قانون أصـول المحاكمات الجزائية في كل مالم يرد به نص ، فأننا نرى بأن ماورد بشـأن الأذن بالتفتيش وشـــكلياته بالأمكان تطبيقها على الأمر بالتفتيش في الجرائم المعلوماتية ، من حيث الكتابة والتوقيع وتثبيت التأريخ وغير ذلك من الشروط الشكلية التي ينبغي توافرها في أمر التفتيش .

ويشـــترط أن لا يكون الأمر بالتفتيش أمرا عاما ، وإنما يكون الهدف منه محدداً تحديداً دقيقاً وأن يتم وصـــف الأشـــياء المطلوب ضبطها بصـورة تفصـيلية ، بحيث لا يترك ذلك للسلطة التقديرية للجهة المختصـة بتنفيذ الأمر ، وأن لا يكون الأمر بالتفتيش لضـــبط الأشـــياء المتعلقة بالأجهزة الالكترونية التي تحتوي على بيانات شـــخصـــية أو بيانات لا تتعلق بالجريمة ، فهذه الأجهزة يجب أن تكون موصـوفة في أمر التفتيش بصـورة دقيقة فلا يصـدر أمر بالتفتيش مثلا لمجرد

ظنون أو معتقدات بوجود صـور فاضـحة في أحد الأجهزة الالكترونية ، وهذا ما أقتضـى أن يكون منفذ الأمر بالتفتيش ملماً بالجوانب الفنية لهذه الأجهزة واستخداماتها [19].

2- محضر التفتيش في الجرائم المعلوماتية :

يشترط في التفتيش أيضاً في الجرائم المعلوماتية أن ينظم محضراً يثبت فيه ماتم أتخاذه من إجراءات بحيث تتم مراعاة القواعد العامة في محضـر التفتيش في الجرائم التقليدية كأن يكون مكتوباً وأن يثبت فيه تاريخ تنظيمه وأسـم الشـخص الذي قام بتحريره [20] . أما في ظل مشـروع قانون جرائم المعلوماتية العراقي فقد وردت الأشـارة الى هذا الإجراء في نص المادة (26/ ثانياً) التي نصت على " تقوم الجهة التي تتولى جمع الأدلة بما يأتي :

ب : تقديم النسخ الألكترونية أو الورقية من الأدلة مرفقة مع تقرير تفصيلي يبين الإجراءات المتبعة والأدوات والأجهزة التي أسـتخدمت في الحصـول على الدليل أو أسـترجاعه " وهذا مانصـت عليه المادة (33/ ف3) من قانون الجرائم الألكترونية الفلسطيني رقم (16) لسنة 2017 حيث نصت على " أذا أسفر التفتيش عن ضبط أجهزة أو أدوات أو وسائل ذات صلة بالجريمة يتعين على مأمور الضبط القضائي تنظيم محضر بالمضبوطات وعرضها على النيابة العامة "

المطلب الثاني

المعاينة في الجرائم المعلوماتية

تعد المعاينة وسيلة من وسائل جمع الأدلة في مرحلة التحقيق الأبتدائي ، وتظهر أهميتها في أطار الجرائم التقليدية عقب وقوع الجريمة حيث يوجد مسـرح فعلي للجريمة يحتوي على أثار مادية فعلية يتحفظ عليها القائم بالمعاينة لفحصـها وبيان مدى صـحتها في الأثبات ، ألا أن الأمر يختلف في الجرائم المعلوماتية حيث من النادر أن يتخلف عن أرتكابها أثاراً مادية كما قد تطول المدة بين وقوع الجريمة المعلوماتية وبين أكتشـافها مما يعرض الآثار الناجمة عنها الى المحو والتلف أو العبث بها .

الفرع الأول

تعريف المعاينة في الجرائم المعلوماتية

تناولت التشريعات الجنائية المعاينة بوصفها وسيلة من وسائل جمع الأدلة ألا أنها خلت من النص على تعريفها [21] لذلك تولى الفقه مهمة وضـع تعريف للمعاينة فهناك من عرفها بأنها " رؤية بالعين لمكان أو شـخص أو شـئ لأثبات حالته وضـبط كل ما يلزم لكشـف الحقيقة " [22] كما عرفت بأنها " ملاحظة وفحص حي مباشـر لمكان أو شـخص أو شـئ له علاقة بالجريمة لأثبات حالته والكشف والتحفظ على كل ماقد يفيد من الأشياء في كشف الحقيقة ".

فالمعاينة إجراء بمقتضاه ينتقل الشخص المختص الى مكان وقوع الجريمة ليشاهد بنفسه ويجمع

الآثار المتعلقة بالجريمة وكيفية وقوعها وكذلك جمع الأشياء الأخرى التي تفيد في كشف الجريمة،

وتظهر أهمية المعاينة في أنها تنقل للسـلطة المختصـة صـورة مجملة لموقع الجريمة بكل مايحتويه هذا الموقع من تفاصيل سواء تعلقت بمكانه أو وصفه من الداخل أو بيان الآثار الموجودة فيه [23].

الفرع الثاني

محل المعاينة في الجرائم المعلوماتية

على الرغم من الأهمية التي تحتلها المعاينة في مجال كشـــف غموض الجريمة المعلوماتية من خلال أثبات مســـرح الجريمة ألا أنها لاتكون بذات الفاعلية في ضـــبط كافة أدلة هذه الجرائم ، نظراً لوجود طائفة من هذه الجرائم لا تصـــلح بحســـب طبيعتها بأن تكون محلاً للمعاينة ، لذلك ينبغي التمييز في مجال الجرائم المعلوماتية بين مايمكن أن يكون محلاً للمعاينة وبين مالايمكن عده كذلك من مكونات الأجهزة الألكترونية وعلى النحو الآتي :

أولاً: معاينة المكونات المادية :

ومثال هذه الجرائم الأعتداء على أشرطة الحاسبة الألكترونية والكابلات وشاشة العرض الخاصة بها ومفاتيح التشغيل والأقراص وغيرها من المكونات ذات الطابع المادي ، ففي حالة أرتكاب أحدى الجرائم المعلوماتية وكان محل هذه الجريمة مثل هذه المكونات فالأمر لايشـكل أي صـعوبة في أمكانية تقرير مسـرح الجريمة الذي يحتوي هذه المكونات لمعاينتها من قبل الســلطات المختصـــة والتحفظ على مايعتبر منها أدلة مادية تســـاعد على أرتكاب الجريمة ونســـبتها لشخص معين [24].

ثانياً : معاينة المكونات الغير مادية :

وتمتاز هذه الجرائم بأنها تقع على برامج الجهاز الألكتروني وبياناته وكل ماهو غير مادي ومحســـوس وفي هذا النوع من الجرائم تظهر الصعوبة في صلاحية مسرح هذه الجرائم كمحل يمكن معاينته .

وتتمثل هذه الصعوبة في أمرين :

1- قلة الآثار المادية التي التي يمكن أن تتخلف عن هذا النوع من الجرائم .

2- الأعداد الكبيرة من الأشخاص الذين قد يترددون على مسرح الجريمة خلال المدة بين أرتكاب الجريمة والكشف عنها والتي غالباً ماتكون طويلة نســـبياً الأمر الذي يمكن من أحداث تغييرات أو عبث بالأثار المادية أو زوال بعضـــها وهو مايلقي بالغموض على الدليل الذي يمكن الحصول عليه من إجراء المعاينة [25].

المطلب الثالث

الضبط في الجرائم المعلوماتية

للإحاطة بموضـوع الضـبط باعتباره وسـيلة من وسـائل جمع الأدلة في الجرائم المعلوماتية سـوف نقسـم هذا المطلب الى فرعين نتناول في الفرع الأول تعريف الضبط في الجرائم المعلوماتية ونخصص الفرع الثاني لتحديد محل الضبط في الجرائم المعلوماتية وعلى النحو الآتي :

الفرع الأول

تعريف الضبط في الجرائم المعلوماتية

يمكن تعريف الضـبط بصـفة عامة بأنه " وضـع اليد على شـئ يتصـل بجريمة وقعت ويفيد في كشـف الحقيقة عنها وعن مرتكبيها سواء كان هذا الشـئ عقاراً أو منقولاً ، وقد يرد الضـبط على الأشـخاص وهو مايصـطلح على تسميته بالقبض " [26].

ويعد الضـبط وسـيلة من وسـائل جمع الأدلة شـأنه في ذلك شـأن التفتيش يهدف للتوصـل الى الأدلة التي تفيد في كشـف الجريمة ، وأن كان في بعض الأحيان يعتبر نتيجة للتفتيش ، ألا أنه يمكن أن يتخذ كإجراء مسـتقل دون اللجوء الى التفتيش حيث قد يؤدي اليه كشـف محل الحادث ، كما يمكن أن يكون نتيجة لما يقدمه الشـهود أو المتهمون من أشـياء ، لذلك فأن للضـبط قواعده وشـروطه التي التي تلتزم السـلطة المختصـة بها فهو لايجوز الا في الأشـياء التي تسـاعد على أظهار الحقيقة كالأسـلحة والأدوات التي أستخدمت في أرتكاب الجريمة وملابس الجاني أو المجني عليه فيما اذا وجدت عليها أثار الجريمة من دماء وغيرها ، وأهم مايميز الضـبط عن التفتيش هو أن الضـبط لا يتعدى بواسطته على السرية أذ هو يمس حقوقاً مالية فحسب كحق الملكية والحيازة ففي هذه الحالة يجري الضبط دون تفتيش كما لو وقع الضبط على أشياء مكشوفة لا توجد في محل يتمتع بالسرية ، أما التفتيش الذي غايته الضبط فهو الذي يمس حرمة السر [27] .

أما في ظل التشـريعات الخاصـة بالجرائم المعلوماتية ، فقد نص مشـروع قانون جرائم المعلوماتية العراقي لسـنة 2011 على إجراء الضـبط في المادة (24 / ثالثاً) التي نصـت على " يتولى قاضـي التحقيق أو المحقق المباشـرة في إجراءات الضـبط ... " ونصـت المادة (26) على " أولاً - للقاضـي المختص مايأتي : ضـبط أجهزة الحاسـوب أو جزء منها أو الواسطة التي خزنت فيها البيانات ونقلها الى جهة التحقيق لتحليلها ودراستها وله نسخها دون نقل النظام وأزالة البيانات المانعة من الدخول الى الحاسوب دون ألحاق الضرر بالنظام أو المساس بسلامة البيانات والبرامج المخزنة فيه " .

وهذا ماسـار عليه المشـرع الفلسـطيني في قانون الجرائم الألكترونية الفلسـطيني رقم (16) لسـنة 2017 ألا أنه كان أكثر تفصـيلاً في بيانه لأحكام الضـبط في الجرائم الألكترونية عما كانت عليه المعالجة في مشـروع قانون جرائم المعلوماتية العراقي حيث جاءت المادة (34) من قانون الجرائم الألكترونية الفلسـطيني معالجة لكل مايتعلق بإجراء الضـبط أبتداءاً من السلطة المختصـة بإجراءه وبيان محل الضبط ووسائل التحفظ على الأشياء محل الضبط الى ضرورة تدوين محضر بما تم ضبطه [28].

الفرع الثاني

محل الضبط في الجرائم المعلوماتية

ينبغي التمييز في محل الضـــبط في الجرائم المعلوماتية فيما أذا كان هذا المحل يتمثل في المكونات المادية للأجهزة الألكترونية أو يتمثل في المكونات المعنوية اوالغير مادية لهذه الأجهزة :

أولاً : ضبط المكونات المادية :

الأصـل في الضـبط أنه يرد على الأشـياء المادية التي تصـلح لوضـع اليد عليها ، ولهذا لا يثير ضـبط المكونات المادية للأجهزة الألكترونية وملحقاتها أيه إشكالية باعتبارها أشياء مادية ، وبالتالي يجوز ضبط الأسلاك ومفاتيح التشغيل وحدة الإدخال والمودم ووحدة الذاكرة ووحدة التحكم ، وبما في ذلك المخرجات الموجودة في صـــورة مخرجات ورقية أو وسـائط وأوعية التخزين المادية كالأقراص والأشـرطة المغناطيسـية ، حيث يتم ضـبط الأداة أو الوسـيط الذي يتم فيه التخزين .

ثانياً : ضبط المكونات المعنوية :

أثار موضـوع ضـبط المكونات المعنوية للأجهزة الألكترونية خلافاً واسـعاً بين الفقهاء حيث ذهب رأي منهم الى القول بأن الكيانات المعنوية لاتصـلح أن تكون محلاً للضـبط والسـبب في ذلك أن نصـوص القوانين الإجرائية تشـترط الطابع المادي الملموس في هذه الكيانات لكي تصلح أن تكون محلاً للضبط [29].

وذهب اتجاه ثاني إلى أن مفهوم الضبط يمكن أن يمتد ليشمل المكونات المعنوية الإلكترونية ، ويجد هذا الاتجاه تجسيده التشـريعي في قوانين بعض الدول مثل كندا واليونان والولايات المتحدة الأمريكية التي قضـت بإعطاء سـلطات التحقيق مكنة القيام بأي شـــيء يكون ضـــروريا لجمع الأدلة وحمايتها ، بما في ذلك المكونات المعنوية ، وإن كان لا يتصـــور ضـبطها باعتبارها أشـياء غير محسـوسـة ، فإنه من الممكن ضـبطها إذا أصـبح لها كيان مادي ، كضـبط القطعة الصـلبة كأداة تخزينية للدليل و المعلومات والبيانات المراد ضـبطها على ورق أو تسـجيلها في أشـرطة أو أقراص أو نسـخها في ملفات ، إذ في هذه الحالة تتحول المكونات المعنوية إلى أشـــياء مرئية ومقروءة وتكتســـب كيانا ماديا يمكن بواســـطته ضـبطها ونقلها من مكان لأخر ، والقول نفسـه يطبق بشـان الرسـائل الالكترونية ، فللمحقق أن يضـبط الرسـائل المخزنة بالبريد الالكتروني عن طريق طباعة الرسالة التي يريد ضبطها ، أو تسجيلها في ملف أو قرص .

وهناك اتجاه ثالث وأخير يرى أنصـــاره بأنه لا فائدة من تطبيق نصـــوص الإجراءات الحالية المتعلقة بالضـــبط على البيانات المعالجة إلكترونيا بصـورتها المجردة عن دعامتها المادية ، بل لابد من تدخل المشـرّع لتوسـيع دائرة الأشـياء التي يمكن أن يرد عليها الضبط ، ليشمل البيانات المعالجة بصورتها غير الملموسة[30] .

الخاتمة

يُعد التطور الرقمي الهائل سلاحاً ذا حدين, فبقدر ما ساهم في تقريب المسافات، أفرز نمطاً إجرامياً مبتكراً يتسم بالذكاء والعابرة للحدود .وقد كشـــف هذا البحث أن الجريمة المعلوماتية لم تعد مجرد اعتداء رقمي تقني، بل باتت تحدياً قانونياً يمس صلب النظام الإجرائي القانوني، الامر الذي يتطلب من المشرع استجابة تشريعية مرنة تتجاوز فضاء النصوص التقليدية الجامدة .

ان حماية الفضـاء الإلكتروني العراقي تستوجب موازنة دقيقة بين منح السلطات التحقيقية صـلاحيات تقنية واسعة وبين الحفاظ على الحقوق والحريات الدستورية للأفراد.

وخلصـــت الدراســـة إلى أن الجريمة المعلوماتية تمتاز بخصـــائص فريدة، فهي أقل عنفاً مادياً لكنها أكثر جســـامة في خسائرها وصعوبة في إثباتها، حيث لا يترك الجاني خلفه آثاراً ملموسة يمكن فحصها بالوسائل التقليدية .كما أن طبيعتها العابرة للحدود الوطنية تفرض واقعاً يتجاوز السيادة الإقليمية للدول، مما يجعل من تحديد الاختصاص القضائي وتطبيق القانون الجنائي معضلة قانونية وفنية تستدعي تعاوناً دولياً وتشريعاً وطنياً متطوراً.

وفي ختام دراستنا لموضوع الجريمة المعلوماتية نستعرض أهم النتائج والمقترحات التي توصلت اليه الدراسة:

اولاً/ الاستنتاجات:

1. خلص البحث إلى أن المشـرع العراقي لا يزال يعتمد على نصـوص "قانون العقوبات لعام 1969" التي تفتقر للقدرة على تكييف الأفعال الإلكترونية المستحدثة (مثل الاختراق، والبيانات المشفرة)، مما يضع مبدأ "لا جريمة ولا عقوبة إلا بنص" في موضع تساؤل.

2 .خلص البحث الى أن مسـودة قانون جرائم المعلوماتية (2011) تعاني من ركاكة في الصـياغة، وافتقارها لتعريفات قانونية دقيقة للجرائم، مما يجعلها غير صـالحة للتطبيق العملي وتتعارض في بعض جوانبها مع الدسـتور والمعايير الدولية.

3. أن قواعد التفتيش والضـبط والمعاينة المعتمدة حالياً (بموجب قانون أصـول المحاكمات الجزائية لعام 1971) غير قادرة على التعامل مع "الأدلة المعنوية" (البيانات الرقمية غير الملموسـة)، إذ إن هذه القواعد صُـممت للتعامل مع أدلة مادية ملموسة

4. وجود فجوة قانونية تتعلق بـ "جرائم عابرة للحدود"، حيث يعجز القانون العراقي الحالي عن تحديد الاختصـاص المكاني بوضـوح في الجرائم التي يرتكبها أجانب من الخارج ضـد مصـالح عراقية أو العكس، بعكس التشـريعات المصرية والأردنية التي وضعت قواعد مكانية خاصة لهذه الجرائم.

ثانياً/ المقترحات :

1. " التفتيش الافتراضي" : بدلاً من التفتيش التقليدي، يجب اقتراح تشريع يسمح بـ "التفتيش الافتراضي" الذي يتيح للسلطات الوصول إلى البيانات المخزنة في السحابة الإلكترونية (Cloud Computing) أو في خوادم خارج الحدود الوطنية، مع وضع ضوابط قانونية مشددة لضمان الخصوصية.

2. " خبير رقمي ": تجاوز الاعتماد على خبير المحاكم التقليدي، واقتراح تأسـيس "وحدة تحقيق جنائي رقمي" متخصصة تتبع السلطة القضائية مباشرة، تمتلك صلاحيات تقنية حصرية لجمع الأدلة الإلكترونية قبل تلفها، مع منحها صفة مأمور الضبط القضائي التقني.

3. " التوسـع في مفهوم مسـرح الجريمة": تقديم مقترح قانوني لتوسـيع مفهوم "مسـرح الجريمة" ليشـمل الفضـاء السيبراني، واعتبار المعالجة الآلية للبيانات والشبكات "أماكن" تخضع لحرمة القانون، وتسهيل إجراءات معاينتها دون اشتراط مادي ملموس.

4. بما أن معظم الدراسـات السـابقة اقتصـرت على المقارنة العربية، يكمن تقديم مقترح لانضـمام العراق إلى "اتفاقية بودابسـت" للجرائم السـيبرانية لتوحيد إجراءات التعاون الدولي في تبادل الأدلة الرقمية، وهو ما يحل إشـكالية الاختصاص المكاني التي يعاني منها العراق حالياً.

5. مقترح بإنشاء "هيئة رقابة مستقلة" تشرف على إجراءات التفتيش والضبط الرقمي للتأكد من عدم انتهاك خصوصية الأفراد أثناء جمع الأدلة .

ـ الهوامش:

[1] ـ لجنة الأمم المتحدة للقانون التجاري الدولي، هي هيئة قانونية ذات عضوية عالمية متخصصة في إصلاح القانون التجاري على النطاق العالمي منذ ما يزيد على 50 سنة. وتتمثل مهمة الأونسيترال في عصرنة ومواءمة القواعد المتعلقة بالأعمال التجارية الدولية.

2 - أنظر القانون الامريكي رقم 1223 لسنة 1986م ، الخاص بمواجهة جرائم الكومبيوتر ، مشار اليه في كتاب رامي متولي القاضي ، مكافحة جرائم المعلوماتية ،ط1،دار النهضة العربية ، 2011م،ص23.

3 - المادة (18) من نظام مكافحة الجرائم المعلوماتية السعودي رقم م/17 لسنة 1428 ه ، والمشار اليه على الرابط الالكتروني www.boe.gov.sa.

4 - عرفت منظمة التعاون الاقتصادي (OECD) و الخاص باستبيان الغش المعلوماتي عام 1982 و الذي أوردته بلجيكا في تقريرها بأن الجرائم المعلوماتية هي " :كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية و المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية".

5 - أنظر التقرير الخاص بمنظمة HUMAN RIGHTS WACH المنشور على الموقع الالكتروني https://www.hrw.org/sites/default/files/reports/iraq0712arForUpload.pdf

6 - د. محمد على العريان ، الجرائم المعلوماتية ، دار الجامعة الجديدة للنشر ، الإسكندرية ، 2004 ، ص37 .

[7] ينظر نص المواد (3 , 4 ,5 ,6 , 7) من مشروع الجرائم المعلوماتية لسنة 2012 .

[8]- محمد عبد الله ابو بكر سلامة , جرائم الكمبيوتر والانترنت , منشاة المعارف , الاسكندرية , 2006 , ص 92 ,93

[9] - محمد علي سالم ,حسون عبيد هجيج ,الجريمة المعلوماتية مجلة جامعة بابل للعلوم الانسانية ,المجلد 14 ,العد 2 , 2007 , ص 91 .

[10] د.علي حسين خلف , د .سلطان الشاوي ,المبادئ العامة في قانون العقوبات ,مكتبة السنهوري ,بيروت , 2015 , ص 94 ,95 .

[11] . مثل قانون أصول المحاكمات الجزائية العراقي رقم (23) لسنة 1971 في المواد (72 الى 86) و قانون الأجراءات الجنائية المصري رقم (150) لسنة 1950 في المواد (91 الى 94) ومشروع قانون جرائم المعلوماتية العراقي لسنة 2011 في المادة (24) وقانون الجرائم الألكترونية الفلسطيني رقم (16) لسنة 2017 في المادة (33) .

[12] - د. عفيفي كامل عفيفي ، جرائم الكمبيوتر ، بدون ناشر ، بدون مكان نشر ، ص 338 .

[13] - د. حامد راشد ، أحكام تفتيش المسكن في التشريعات الاجرائية العربية ، منشأة المعارف ، الأسكندرية ، 2008 ، ص 20 .

[14] - د. مأمون محمد سلامة ، الإجراءات الجنائية في التشريع الليبي ، الجزء الأول ، ط 1 ، منشورات الجامعة ، 1971، ص481 .

[15] - نقض مصري 1959/3/31 ، أحكام النقض س 10 رقم 87 ص 391 في 1962/12/17 س 13 رقم 205 ص 853 .

[16] - د. نديم محمد حسن الترزي ، سلطات النيابة العامة في الجرائم المعلوماتية ، بحث منشور في مجلة الأندلس العدد 13 المجلد 15 لسنة 2017 ، ص 321 .

[17] - علي عدنان الفيل ، أجراءات التحري وجمع الأدلة والتحقيق الأبتدائي في الجريمة المعلوماتية ، المكتب الجامعي الحديث ، 2012، ص 39 .

[18] - د. عبد الأمير العكيلي ، أجراءات التحري وجمع الأدلة والتحقيق ، ط1، مطبعة المعارف ، بغداد ، 1971 ، ص 77.

[19] - د. مفتاح بو بكر المطردي ، لجريمة الإلكترونية، ورقة عمل مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية، السودان، 2012.، ص 47 .

[20] - تنظر المادة (82) من قانون أصول المحاكمات الجزائية العراقي النافذ رقم 23 لسنة 1971.

[21] - منها قانون أصول المحاكمات الجزائية العراقي رقم (23) لسنة 1971 و قانون الأجراءات الجنائية المصري رقم (150) لسنة 1950 في المادة (90) منه .

[22] - د. عفيفي كامل غفيفي ، مصدر سابق ، ص 333 .

[23] د. نديم محمد حسن الترزي ، مصدر سابق ، ص 312 .

[24] - د. عفيفي كامل غفيفي ، مصدر سابق ، ص 336 .

[25] - ثنيان ناصر آل ثنيان ، أثبات الجريمة الألكترونية ، رسالة ماجستير مقدمة الى كلية الدراسات العليا – جامعة نايف للعلوم الأمنية ، 2012 ، ص57 .

[26] - بخي فاطمة الزهراء ، إجراءات التحقيق في الجريمة الالكترونية , رسالة ماجستير ,كلية الحقوق والعلوم السياسية , جامعة المسيلة , الجزائر ,2014.ص 79 .

[27] - د.صالح عبد الزهرة الحسون ، أحكام التفتيش وآثاره في القانون العراقي ،ط1،بغداد , 1979 ، ص 70 .

[28] - تنظر المادة (34) من قانون الجرائم الألكترونية الفلسطيني رقم (16) لسنة 2017 .

[29] - يوسف خليل يوسف ، الجرائم الألكترونية في التشريع الفلسطيني ، رسالة ماجستير مقدمة الى كلية الشريعة والقانون – الجامعة الأسلامية – غزة ، 2013 ، ص،124 .

[30] - د. مفتاح بو بكر المطردي ، مصد سابق ، ص 46 .

المصادر

أولا/ الكتب باللغة العربية :

1. د. حامد راشد ، أحكام تفتيش المسكن في التشريعات الاجرائية العربية ، منشأة المعارف ، الأسكندرية .
2 .رامي متولي القاضي ، مكافحة جرائم المعلوماتية ،ط1،دار النهضة العربية ، 2011.
3. د.صالح عبد الزهرة الحسون ، أحكام التفتيش وآثاره في القانون العراقي ،ط1،بغداد , 1979 .
4. د.علي حسين خلف , د .سلطان الشاوي ,المبادئ العامة في قانون العقوبات ,مكتبة السنهوري ,بيروت , 2015.
5 .علي عدنان الفيل ، أجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية ، المكتب الجامعي الحديث، 2012.
6. د. عبد الأمير العكيلي ، إجراءات التحري وجمع الأدلة والتحقيق ، ط1، مطبعة المعارف ، بغداد ، 1971 .
7. د. عفيفي كامل عفيفي ، جرائم الكمبيوتر ، بدون ناشر ، بدون مكان نشر.
8. د. مأمون محمد سلامة ، الإجراءات الجنائية في التشريع الليبي ، الجزء الأول ، ط 1 ، منشورات الجامعة ، 1971.
9. د. محمد على العريان ، الجرائم المعلوماتية ، دار الجامعة الجديدة للنشر ، الإسكندرية ، 2004.
10. محمد عبد الله ابو بكر سلامة , جرائم الكمبيوتر والانترنت , منشاة المعارف , الاسكندرية , 2006 .

ثانياً /الرسائل والاطاريح:

1. بخي فاطمة الزهراء ، إجراءات التحقيق في الجريمة الالكترونية , رسالة ماجستير ,كلية الحقوق والعلوم السياسية , جامعة المسيلة , الجزائر ,2014.
2. ثنيان ناصر آل ثنيان ، أثبات الجريمة الإلكترونية ، رسالة ماجستير مقدمة الى كلية الدراسات العليا – جامعة نايف للعلوم الأمنية ، 2012.
3. يوسف خليل يوسف ، الجرائم الإلكترونية في التشريع الفلسطيني ، رسالة ماجستير مقدمة الى كلية الشريعة والقانون – الجامعة الإسلامية – غزة ، 2013.

ثالثا /البحوث :

1. محمد علي سالم ,حسون عبيد هجيج ,الجريمة المعلوماتية مجلة جامعة بابل للعلوم الانسانية ,المجلد 14 ,العد 2 , 2007 .
2. د. مفتاح بو بكر المطردي ، الجريمة الإلكترونية، ورقة عمل مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية، السودان، .2012،
3 .د. نديم محمد حسن الترزي ، سلطات النيابة العامة في الجرائم المعلوماتية ، بحث منشور في مجلة الأندلس العدد 13 المجلد 15 لسنة 2017 .

رابعاً /القوانين :

1 .القانون الامريكي رقم 1223 لسنة 1986.
2. مشروع الجرائم المعلوماتية العراقي لسنة 2012 .
3. قانون أصول المحاكمات الجزائية العراقي رقم (23) لسنة 1971) .
4. قانون الإجراءات الجنائية المصري رقم (150) لسنة 1950 .
5. قانون الجرائم الإلكترونية الفلسطيني رقم (16) لسنة 2017) .

خامساً /المواقع الالكترونية :

1 -التقرير الخاص بمنظمة HUMAN RIGHTS WACH المنشور على الموقع الالكتروني

https://www.hrw.org/sites/default/files/reports/iraq0712arForUpload.pdf

2- نظام مكافحة الجرائم المعلوماتية السعودي رقم م/17 لسنة 1428 ، والمشار اليه على الرابط الالكتروني .www.boe.gov.sa

Sources

First / Books in Arabic:

1. Dr. Hamed Rashed, Provisions for Searching a Residence in Arab Procedural Legislations, Al-Maaref Establishment, Alexandria.

2. Rami Metwally Al-Qadi, Combating Cybercrime, 1st ed., Dar Al-Nahda Al-Arabiya, 2011.

3. Dr. Saleh Abdul-Zahra Al-Hassoun, Provisions for Search and its Effects in Iraqi Law, 1st ed., Baghdad, 1979.

4. Dr. Ali Hussein Khalaf, Dr. Sultan Al-Shawi, General Principles of Penal Law, Al-Sanhouri Library, Beirut, 2015.

5. Ali Adnan Al-Feel, Procedures for Investigation, Evidence Collection, and Preliminary Investigation in Cybercrime, Modern University Office, 2012.

6. Dr. Abdul-Amir Al-Akeeli, Procedures for Investigation, Evidence Collection, and Investigation, 1st ed., Al-Maaref Press, Baghdad, 1971.

7. Dr. Afifi Kamel Afifi, Computer Crimes, no publisher, no place of publication.

8. Dr. Mamoun Muhammad Salama, Criminal Procedures in Libyan Legislation, Part One, 1st ed., University Publications, 1971.

9. Dr. Muhammad Ali Al-Aryan, Cybercrimes, Dar Al-Jami'a Al-Jadeeda Publishing House, Alexandria, 2004.

10. Muhammad Abdullah Abu Bakr Salama, Computer and Internet Crimes, Mansha'at Al-Ma'arif, Alexandria, 2006.

Second/ Theses and Dissertations:

1. Bakhi Fatima Al-Zahra, Procedures for Investigating Cybercrime, Master's Thesis, Faculty of Law and Political Science, University of M'sila, Algeria, 2014.

2. Thunayyan Nasser Al Thunayyan, Proving Cybercrime, Master's Thesis submitted to the College of Graduate Studies, Naif Arab University for Security Sciences, 2012.

3. Yousef Khalil Yousef, Cybercrimes in Palestinian Legislation, Master's Thesis submitted to the College of Sharia and Law, Islamic University of Gaza, 2013.

Third/ Research:

1. Muhammad Ali Salem and Hassoun Obeid Hajij, Cybercrime, Journal of Babylon University for Humanities, Volume 14, Issue 2, 2007.

2. Dr. Muftah Abu Bakr Al-Mutardi, Cybercrime, Working Paper presented at the Third Conference of Presidents of Supreme Courts in Arab States, Sudan, 2012.

3. Dr. Nadeem Muhammad Hassan Al-Tarzi, The Powers of the Public Prosecution in Cybercrimes, Research published in Al-Andalus Journal, Issue 13, Volume 15, 2017.

Fourth/ Laws:

1. US Law No. 1223 of 1986.

2. Iraqi Cybercrime Bill of 2012.

3. Iraqi Criminal Procedure Code No. (23) of 1971.

4. Egyptian Criminal Procedure Code No. (150) of 1950.

5. Palestinian Cybercrime Law No. (16) of 2017.

Fifth /Websites:

1. The Human Rights Watch report published on the website https://www.hrw.org/sites/default/files/reports/iraq0712arForUpload.pdf

2. Saudi Anti-Cybercrime Law No. M/17 of 1428, referenced at www.boe.gov.sa.