مجلة جامعة الشارقة للعلوم القانونية

اسم المقال: إجراءات التعامل مع مسرح الجريمة الإلكترونية في التشريع الإماراتي "دراسة تحليلية"
اسم الكاتب: سعود عبدالقادر الشاعر
رابط ثابت: https://political-encyclopedia.org/index.php/library/8609
تاريخ الاسترداد: 2026/11/02 02:09 +03

الموسوعة السياسيّة هي مبادرة أكاديمية غير هادفة للربح، تساعد الباحثين والطلاب على الوصول واستخدام وبناء مجموعات أوسع من المحتوى العلمي العربي في مجال علم السياسة واستخدامها في الأرشيف الرقمي الموثوق به لإغناء المحتوى العربي على الإنترنت.
لمزيد من المعلومات حول الموسوعة السياسيّة – Encyclopedia Political، يرجى التواصل على info@political-encyclopedia.org

استخدامكم لأرشيف مكتبة الموسوعة السياسيّة – Encyclopedia Political يعني موافقتك على شروط وأحكام الاستخدام المتاحة على الموقع https://political-encyclopedia.org/terms-of-use

تم الحصول على هذا المقال من موقع مجلة جامعة الشارقة للعلوم القانونية ورفده في مكتبة الموسوعة السياسيّة مستوفياً شروط حقوق الملكية الفكريّة ومتطلبات رخصة المشاع الإبداعي التي ينضوي المقال تحتها.

جامعة الشارقة
UNIVERSITY OF SHARJAH

مجلة جامعة الشارقة

مجلة علمية محكمة

للعلوم القانونية



المجلد 20، العدد 3
ربيع الأول 1443هـ / سبتمبر 2023م

الترقيم الدولي المعياري للدوريات 2616-6526

سبتمبر 2023م **مجلة جامعة الشارقة للعلوم القانونية** المجلد 20 العدد 3

https//:doi.org/10.36394/jls.v20.i3.7

إجراءات التعامل مع مسرح الجريمة الإلكترونية في التشريع الإماراتي "دراسة تحليلية"

سعود عبد القادر الشاعر[1]

تاريخ الاستلام: 25-07-2021 **تاريخ القبول: 28-09-2021**

ملخص البحث:

يهدف البحث إلى دراسة الإجراءات المتبعة عند التعامل مع مسرح الجريمة الإلكترونية وتحليلها، والكيفية التي يجب التعامل بها مع هذا النوع من الجرائم وتكون من خلال مسرح هذه الجريمة ومعاينته والضوابط الواجب مراعاتها عند إجراء المعاينة وآثاره المادية، وكيفية توثيقه ورفع الآثار بالطرق التقنية الحديثة، وفق الأنظمة المتقدمة من تصوير فوتوغرافي ورسم رقمي لمسرح الجريمة، والقياس الرقمي لأبعاد مسرح الجريمة، والأدوات اللازمة للحفاظ على الدليل الرقمي الذي يمكن استخلاصه منه، وذلك في إطار التشريعات والقوانين الخاصة بدولة الإمارات العربية المتحدة، وقد استخدم الباحث المنهج الوصفي التحليلي لوصف الإجراءات المتبعة في مثل هذه الجرائم وتحليلها، وقد توصل الباحث من خلال هذا البحث إلى أن المشرع الإماراتي اتخذ منحى يتوافق مع التطورات المعلوماتية التي أصبحت اليوم تشكل واقعنا المعاش؛ إذ أعطى الحماية القانونية لأدلة الإثبات الإلكترونية وحدد الضوابط التي تحكمها.

الكلمات الدالة: الجريمة الإلكترونية، مسرح الجريمة الإلكترونية، الدليل الإلكتروني، التشريع الإماراتي.

(1) كلية القانون - جامعة عجمان (عجمان - الإمارات العربية المتحدة)

201720185@ajmanuni.ac.ae

20-3.indd 215 9/24/2023 2:32:59 AM

أولاً- المقدمة:

على الرغم من الفوائد التي تم تحقيقها ولا تزال تتحقق كل يوم بفضل التطور الهائل في مجال الإلكترونيات على جميع المستويات في مختلف مجالات الحياة الحديثة، لدرجة أن جميع القطاعات المختلفة تعتمد في أداء عملها بشكل أساسي على استخدام الأنظمة الإلكترونية نظرا لسرعتها ودقتها في جمع المعلومات، مثل التخزين والمعالجة، وكذلك النقل والتبادل بين الأفراد والشركات والمؤسسات المختلفة داخل نفس الدولة أو بين عدة دول. (1)

ومع ذلك، وعلى الرغم من الفوائد الهائلة التي تحققت، فإن هذه الثورة التكنولوجية جاءت مصحوبة بسلسلة من الانعكاسات السلبية والخطيرة من سوء استخدام هذه التكنولوجيا، والتي يحاول البعض استغلالها لارتكاب العديد من الجرائم، كما أن استغلال الإمكانات الهائلة لهذه الابتكارات خلق أشكال أخرى من الجرائم المرتبطة بهذه التقنيات، والتي أصبحت وسائل لارتكاب هذه الجرائم، وقد زادت معدلات هذه الجرائم بشكل كبير في العقدين الماضيين، وأدى ذلك إلى ظهور ظاهرة إجرامية جديدة تسمى الجريمة الإلكترونية.(2)

ويختلف مسرح الجريمة الإلكترونيّة عن مسرح الجريمة التقليديّة، وهو ما يتطلّب إجراءات خاصّة للتعامل مع مسرح الجريمة الإلكترونيّة لأنها تختلف كثيراً عن الجريمة التقليديّة من حيث الوسائل التي تستخدم في ارتكاب الجريمة، كذلك تتميز الجريمة الإلكترونية ببعض الخصوصية كونها تقع داخل الحاسب الآلي أو داخل نظامه.

كما تتميز الجرائم المعلوماتية بصعوبة اكتشافها وإثباتها وذلك يعود إلى أنها لا تخلف آثارا ظاهرة تنصب على البيانات الموجودة في النظم المعلوماتية، فالتحقيق في هذه الجرائم يستوجب استحداث الأساليب العلمية والتقنية ومواكبة التقدم التكنولوجي (3)؛ إذ إنّ الطبع الغالب علي الجرائم الإلكترونية أنها تخترق الحدود، إذ يكفي أن نتصور أن الشخص العامل على الكمبيوتر في واشنطن يستطيع أن يحول مبلغا من المال إلى جاكرتا، مضيفا إليه صفراً أو بضعة أصفار مرتكبا بذلك أخطر الجرائم في اختلاس الأموال وغيرها، أو

(1) جمال، براهيمي (2018)، التحقيق الجنائي في الجرائم الإلكترونية، رسالة دكتوراة، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر.

(2) جفال، يوسف (2017)، التحقيق في الجرائم الإلكترونية، مذكرة مقدمة لنيل شهادة الماستر أكاديمي، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، الجزائر، ص5.

(3) رشيد، بن فريحة (2017)، التحري الجنائي في مسرح الجريمة الإلكترونية، مجلة جامعة القدس المفتوحة للأبحاث والدراسات، العدد الثاني والأربعون (1)، فلسطين، ص53.

20-3.indd 216 9/24/2023 2:32:59 AM

أن يستخدم بعض الفيروسات ليعطب أنظمة حاسوبية بأكملها في بلد آخر. [1]

ونظرا لما يمثله مسرح الجريمة الإلكترونية من أهمية قصوى في الحصول على البيانات والمعلومات لمعرفة مرتكب الجريمة فقد قامت التشريعات بسن القوانين الخاصة بالجرائم الإلكترونية وذلك لتنظيم استخدام شبكة الإنترنت وفرض العقوبات المناسبة لردع مرتكبي هذا النوع من الجرائم، وسوف نتناول في هذا البحث إجراءات التعامل مع مسرح الجريمة الإلكترونية من خلال القانون الإماراتي وبعض القوانين العربية والأجنبية.

أدت الحداثة التي تتميز بها الجريمة الإلكترونية واختلاف النظم القانونية والثقافية بين الدول، إلى عدم الاتفاق على مصطلح موحد للدلالة عليها، وعدم الاتفاق هذا نتج عنه عدم وضع تعريف موحد لهذه الظاهرة الإجرامية، وذلك خشية حصرها في مجال ضيق. [2]

تتكون الجريمة الإلكترونية أو الافتراضية من مقطعين هما الجريمة (crime)، والإلكترونية (cyber)، ويستخدم مصطلح الإلكترونية لوصف فكرة جزء من الحاسب أو عصر المعلومات.

أما الجريمة فهي السلوكيات والأفعال الخارجة على القانون. والجرائم الإلكترونية هي "المخالفات التي ترتكب ضد الأفراد أو المجموعات من الأفراد بدافع الجريمة وبقصد إيذاء سمعة الضحية، أو أذى مادي، أو عقلي للضحية مباشر، أو غير مباشر باستخدام شبكات الاتصالات مثل الإنترنت (مثل غرف الدردشة، والبريد الإلكتروني، والهاتف المحمول). [3]

كما أن للجريمة الإلكترونية عدة مسميات نذكر منها:

1. جرائم الحاسوب والإنترنت
2. جرائم التقنية العالية
3. الجريمة الإلكترونية.
4. الجريمة السايبرية

(1) عوض، محمد محي الدين (1993)، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات، المؤتمر السادس للجمعية المصرية القانون الجنائي، القاهرة، ص 361.

(2) العريان، محمد علي (2004)، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، الإسكندرية، ص 43.

(3) Halder, D., & Jaishankar, K. (2011): Cybercrime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9.

20-3.indd 217 9/24/2023 2:33:00 AM

ويمثل جوهر الجريمة الإلكترونية، أبعد من هذا الوصف، ومع ذلك، فالأعمال ذات الصلة بالحاسوب لأغراض شخصية أو تحقيق مكاسب مالية أو ضرر، بما في ذلك أشكال الجرائم المتصلة بالهوية، والأفعال المتعلقة بمحتويات الحاسوب جميعها تقع ضمن معنى أوسع لمصطلح "الجريمة الإلكترونية"

وتعد الجرائم الإلكترونية هي النوع الشائع من الجرائم في ظل التطور التكنولوجي، إذ إنها تتمتع بالكثير من المميزات بالنسبة للمجرمين والتي تدفعهم إلى ارتكابها، وقد تكون هذه الدوافع ذات طبيعة ربحية بحيث يسعى الجناة إلى تحقيق الربح والحصول على الأموال، أو يكون هدف الجاني هو الرغبة في إثبات ذاته وتحقيق انتصار على تقنيات النظم المعلوماتية [1]. كما يُمكن أيضا أن يكون الدافع لارتكاب هذا النوع من الجرائم تعرض الشخص للتهديد والضغط من الآخرين في مجالات الأعمال التجارية والأخرى الخاصة بالتجسس والمنافسة، أو سعي بعض الموظفين إلى الانتقام من المنشآت، وقد يكون الهدف تهديد الشخص وابتزازه لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعين [2].

وقد تكون الدوافع ذا طبيعة سياسية، إذ تعد الدوافع السياسية من أبرز المحاولات العالمية لاختراق شبكات حكومية في مختلف بقاع العالم، كما إن الأفراد قد يتمكنون من اختراق الأجهزة الأمنية الحكومية، كذلك أصبحت شبكة الإنترنت مجالاً خصباً لنشر أفكار العديد من الأفراد والمجموعات ووسيلة للترويج لأخبار وأمور أخرى قد تحمل في ثناياها مساساً بأمن الدولة أو بنظام الحكم أو قدحاً في رموز دولية أو سياسية والإساءة لها بالذم والتشهير [3].

كما توسعت الجريمة الإلكترونية لتشمل أشكالًا من الجريمة المنظمة، حيث دخل الإرهاب الإلكتروني على شبكة الإنترنت، واستولت الجماعات الإرهابية على صفحات على الإنترنت تمارس من خلالها عملها، مثل التحريض على القتل، بالإضافة إلى تعليم إنتاج المتفجرات والقنابل وتوزيع أفكارهم الإرهابية وشن عملياتهم الإرهابية عبر الإنترنت من خلال التلاعب بالأنظمة والبيانات الخاصة.

(1) البقمي، ناصر بن محمد (2008)، مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربية، سلسلة محاضرات الإمارات تصدر عن مركز الإمارات للدراسات والبحوث الاستراتيجية، العدد 116، ص10.

(2) الملط، أحمد خليفة (2005)، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ص 102.

(3) البقمي، ناصر بن محمد، مرجع سابق، ص11.

20-3.indd 218 9/24/2023 2:33:00 AM

كما عرف الفقيه (Mawre) الجريمة الإلكترونية بأنها الفعل غير المشروع الذي يتورط الحاسب الآلي في ارتكابه. [1]

بينما يعرفها بعض الفقه أنها نشاط إجرامي تستخدم فيه التقنية الإلكترونية، الحاسب الآلي وشبكة الإنترنت، بطريقة مباشرة، أو غير مباشرة كوسيلة لتنفيذ الفعل الإجرامي المستهدف. [2]

ووفقا لاتجاه آخر من الفقه والذي عرفها على أساس موضوع الجريمة بأنها "الجريمة المرتكبة عبر الإنترنت هي الجريمة الناجمة عن إدخال بيانات مزورة في الأنظمة وإساءة استخدام المخرجات إضافة إلى أفعال أخرى تشكل جرائم أكثر تعقيدا من الناحية التقنية مثل تعديل الحاسوب".[3]

كما اهتم جانب آخر من الفقه بمدي توفر المعرفة بتقنيات الحاسوب والمعلومات وعرفها على هذا الأساس وتعتمد هذه التعاريف على أساس توافر المعرفة الفنية بتقنية المعلومات لدى الجاني في الجريمة الإلكترونية، حيث عرفها الأستاذ David Thomson بأنها "أية جريمة يكون متطلبا لاقترافها أن يتوافر لدى فاعلها معرفة بتقنية الحاسب".[4]

كما عرفت الجرائم الإلكترونية بأنها: "الجريمة التي يتم ارتكابها إذا قام شخص ما باستخدام معرفته بالحاسب الآلي بعمل غير قانوني".[5]

ولقد اعتمد هذا الاتجاه في تعريفه للجريمة الإلكترونية على معيار شخصي وهو مدى معرفة الجاني بتقنية المعلومات والإلمام بها، وحيث إن قصور هذه التعاريف واضحة؛ لأن شخصية الجاني لا تكفي لوحدها لتعريف الجريمة الإلكترونية حيث يمكن لشخص عادي غير مؤهل بتقنيات الحاسب الآلي ارتكاب جريمة الغش المعلوماتي أو السرقة المعلوماتية.

(1) باطلي، غنية (2015)، الجريمة الإلكترونية، دراسة مقارنة، الدار الجزائرية لنشر والتوزيع، الجزائر، ص 22،23.

(2) كحلوش، على (2003)، جرائم الحاسوب وأساليب مواجهتها، مجلة الشرطة، المديرية العامة الأمن الوطني، عدد 42،22، ص 22، نقلا عن يوسف الصغير، الجرائم المرتكبة عبر الإنترنت، رسالة لنيل شهادة الماجيستر 2017 كلية الحقوق، جامعة مولود معمري، تيزي وزو، الجزائر، ص9.

(3) المرجع ذاته.

(4) قشقوش، هدي حامد (2000)، الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت، دار النهضة العربية، القاهرة، ص12.

(5) رستم، هشام محمد فريد (2004)، الجرائم المعلوماتية، مؤتمر القانون والكمبيوتر والإنترنيت، منذ 1 – 5 - 2000 – جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، المجلد الثاني، الطبعة الثالثة، ص 407.

20-3.indd 219 9/24/2023 2:33:00 AM

بينما عرف المشرع الإماراتي الجريمة الإلكترونية في نص المادة الثانية من مرسوم بالقانون الإماراتي الاتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات حيث نصت على أنها " أي فعل عمدي يتوصل فيه بغير وجه حق إلى موقع أو نظام معلوماتي سواء بدخول الموقع أو النظام أو بتجاوز مدخل مصرح به، بهدف حذف، أو تدمير، أو إفشاء، أو إتلاف، أو تغيير، أو إعادة نشر بيانات، أو معلومات". (1)

ويلاحظ على هذا التعريف: أن المشرع الإماراتي قد اعتمد على معيار الجمع بين عدة معايير لتعريف الجريمة الإلكترونية أولها معيار وسيلة الجريمة وهو نظام الاتصالات الإلكتروني أو النظام المعلوماتي، وثانيها معيار موضوع الجريمة المساس بأنظمة المعالجة الآلية للمعطيات بهدف حذف، أو تدمير، أو إفشاء، أو إتلاف، أو تغيير، أو إعادة نشر بيانات، أو معلومات، كما اعتمد المشرع الإماراتي على معيار ثالث في تحديد نطاق الجريمة الإلكترونية، كونه أقر أن الجريمة الإلكترونية ترتكب في نظام معلوماتي أو يسهل ارتكابها عليه، وهذا ما يوسع من نطاق مجال الجرائم الإلكترونية في القانون الإماراتي.

خصائص الجريمة الإلكترونية:

تتميز الجريمة الإلكترونية أو السيبرانية بطبيعة خاصة تميزها عن الجرائم التقليدية؛ لذلك فإن هذا النوع من الجرائم لها سمات وخصائص عديدة، سواء كانت متعلقة بمرتكبيها أو ممن يسمونهم قراصنة الحاسوب، أو بالنسبة لحدود هذا النوع من الجرائم حيث تعتبر ذات بعد عالمي (2).

أولاً- الجريمة الإلكترونية جريمة ذات بعد عالمي (عابرة للحدود):

من أهم السمات المميزة للجريمة السيبرانية أنها تعبر الحدود الجغرافية لارتباطها بعالم الإنترنت وتكنولوجيا المعلومات، حيث قد تتأثر العديد من الدول بهذه الجريمة في نفس الوقت، وبسبب السرعة الهائلة لتنفيذ هذه الجريمة وطريقة تنفيذها وحجم الأموال والأشخاص الذين يتم استهدافهم من خلالها.

للحدود العالمية للجريمة السيبرانية عدة آثار قانونية، من أهمها القانون المطبق عليها والقضاء المختص، سواء كان قانون الدولة التي وقع فيها النشاط الإجرامي، أو الدولة التي

(1) انظر نص المادة (2) من مرسوم بالقانون الإماراتي الاتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات، والمعدل بموجب القانون الاتحادي رقم 12 تاريخ 23/05/2016 والمرسوم بقانون اتحادي رقم 2 تاريخ 24/07/2018

(2) عرب، يونس (2002)، جرائم الكمبيوتر والإنترنت، ورقة عمل مقدمة إلى مؤتمر الأمن العربي، المركز العربي للبحوث والدراسات الجنائية، أبو ظبي 10/12/2002.

20-3.indd 220 9/24/2023 2:33:01 AM

يقع فيها الجاني أو الجاني، أو الدولة التي تعرضت مصالحها للانتهاك.

لذلك، أصبح من الضروري إيجاد الطريقة المثلى للتوفيق بين التشريعات المتعلقة بهذه الجرائم من خلال إبرام المعاهدات الدولية بشأن تسليم المجرمين وإجراءات مكافحة هذه الجرائم.

ولقد قام المشرع الإماراتي بموجب القانون الاتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات بسن أحكام خاصة بالتعاون والمساعدة القضائية والدولية المتبادلة عن طريق المادة (47)، والمادة (49) من هذا القانون.

ثانياً- الصفات الخاصة التي يتمتع بها مرتكبو الجرائم الإلكترونية:

يتميز المجرم الإلكتروني أو المعلوماتي عن غيره من المجرمين العاديين الذين اتجهوا إلى السلوك الإجرامي التقليدي بعدة خصائص والتي ذكرها الأستاذ (Parker) فيما يلي: [1]

1. المجرم الإلكتروني أو المعلوماتي مجرم متخصص ومحترف في تنفيذ جريمته الإلكترونية، حيث إن ارتكابها يتطلب خبرة ومهارة للتغلب على تقنيات حماية أنظمة الحاسوب.
2. خلافا على المجرم العادي المجرم المعلوماتي لا يلجأ إلى العنف في تنفيذ جرائمه، فهو مجرم ذكي يتمتع بالمهارة والمعرفة وبدرجة عالية من الثقافة.
3. يوجد عدة أنواع من المجرمين الإلكترونيين أو المعلوماتيين، فهناك:

أ. مرتكبو الجرائم الإلكترونية بغرض التسلية والمزاح مع الآخرين دون إحداث أي ضرر

ب. مرتكبو الجرائم الإلكترونية بغرض الفضول أو اكتساب الخبرة أو لمجرد القدرة على اختراق هذه الأنظمة ويسمون Hackers.

ج. مرتكبو الجرائم الإلكترونية بغرض الحاق خسائر بالمجني عليهم، دون أن يكون الحصول على مكاسب مالية ضمن هذه الأهداف.

د. مرتكبو الجرائم الإلكترونية الذين يهدفون إلى تحقيق ربح مادي بطريق غير مشروع [2]

(1) الديربي، عبد العال (2013)، الجريمة المعلوماتية – تعريفها – أسبابها وخصائصها، منشور على الموقع التالي http://accronline.com/article_detail.aspx?id=7509، تاريخ أخر زيارة 18/7/2021م.

(2) رحيمة، نمديلي (2017)، خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة، كتاب

20-3.indd 221 9/24/2023 2:33:01 AM

ثالثاً- من أهم الخصائص للجريمة الإلكترونية أنها جريمة صعبة الإثبات

من أهم سمات الجريمة الإلكترونية أو السيبرانية صعوبة إثباتها لأسباب تتعلق بالجاني أو الضحية أو وسائل تنفيذ الجريمة، حيث إن الجريمة تحدث بطريقة منظمة من إقليم دولة تستخدم الإنترنت وقد يكون مصدر خارجي عن الدولة مما يجعل الجريمة صعبة الإثبات، والضحايا غالبًا من المؤسسات العامة أو الخاصة، يترددون في الإبلاغ عنهم لتجنب الإضرار بالسمعة وتقويض الثقة، وكذلك إمكانية إتلاف الأدلة في وقت قياسي. (1)

أنواع الجريمة الإلكترونية:

يُمكن تصنيف أنواع الجرائم الإلكترونية على النحو التالي:

- **هجمات الحرمان من الخدمات:** يُرمز لها بالرمز (DDoS)، وتُنفّذ هذه الهجمات باستخدام مجموعات كبيرة من أجهزة الحاسوب يُتحكَّم بها عن بُعد بواسطة أشخاص يستخدمون نطاق ترددي مشترك، وتهدف هذه الهجمات لإغراق الموقع المستهدف بكميّات هائلة من البيانات في آن واحد، ممّا يُسبّب بطئاً وإعاقةً في وصول المستخدمين للموقع. وقد نص المشرع الإماراتي على هذا النوع من الهجمات في المادة (8) من بموجب القانون الاتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات حيث ذكرت بأنه ".....، كل من أعاق أو عطل الوصول الى شبكة معلوماتية أو موقع الكرتوني أو نظام معلومات الكرتوني". (2)
- **التصيد الاحتيالي:** يُعتبر هذا النوع من الجرائم الإلكترونية الأكثر انتشاراً، وهو إرسال جماعي لرسائل تصل عبر البريد الإلكتروني تحتوي على روابط لمواقع أو مرفقات ضارّة، وبمجرّد نقر المستخدم عليها فإنّه قد يبدأ بتحميل برامج ضارة بجهاز الحاسوب الخاص به. وقد نص المشرع الإماراتي على عقوبة هذا النوع من الجرائم في المادة (10) من القانون السابق ذكره.
- **مجموعات الاستغلال:** يعرّف هذا النوع على أنّه استخدام برامج مصمّمة لاستغلال أيّ أخطاء أو ثغرات أمنية في أجهزة الحاسوب، ويُمكن الحصول على هذه البرامج من شبكة الإنترنت المظلمة، كما يُمكن للقراصنة اختراق مواقع ويب شرعية واستخدامها للإيقاع بضحاياهم.

أعمال مؤتمر الجرائم الإلكترونية المنعقد في طرابلس/ لبنان، ص95.

(1) باطلي، غنية، المرجع السابق، ص 28 – 32.

(2) انظر نص المادة (8) من القانون الاتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

20-3.indd 222 9/24/2023 2:33:01 AM

- **برامج الفدية:** تمنع هذه البرامج صاحب الجهاز من الوصول إلى ملفّاته المخزّنة على محرّك الأقراص الصلبة، ويشترط المجرم على الضحيّة دفع مبلغ مالي كفدية لإتاحة استعادة ملفاته التي يحتاجها. (1)

- **القرصنة:** تُعرّف القرنصة على أنّها وصول غير شرعي إلى بيانات ومعلومات موجودة على أجهزة الحاسوب أو شبكات الإنترنت من خلال استغلال نقاط ضعف وثغرات في هذه الأنظمة.

- **سرقة الهويّة:** يحدث هذا النوع من الجرائم عندما يحصل شخص ما على المعلومات الشخصية لشخص آخر بشكل غير قانونيّ ويستخدمها لأغراض غير شرعية مثل الاحتيال والسرقة.

- **الهندسة الاجتماعية:** يعتمد هذا النوع من الجرائم على العنصر البشري في التلاعب النفسي بالضحية لإرغامها على القيام بأعمال غير قانونية أو إفشاء معلومات سريّة، وهي من الأساليب التي يستخدمها مجرمو الإنترنت للقيام بأعمال الاحتيال.

- **قرصنة البرمجيات:** تُعرّف قرصنة البرمجيات على أنّها إعادة توزيع واستخدام لبرمجيات دون تصريح من الشركة المالكة للبرمجية. (2)

كما تستخدم العديد من الوسائل لتنفيذ الجريمة الإلكترونية وهذا ما سنتناوله في المطلب الثاني والذي ندرس من خلاله أهم الوسائل المستخدمة في ارتكاب الجريمة الإلكترونية.

إن الوسائل التقنية التي قد تستخدم لتدمير أو سرقة مكونات الحاسوب كثيرة ومعقدة في الوقت الحاضر، ولا يُمكن التنبؤ بالوسائل التي قد تستحدثها التكنولوجيا في هذا الشأن، وبناءً على ذلك سوف نقوم بتناول أهم هذه الوسائل على النحو الآتي:

أولاً- الفيروسات (Viruses)

سمي (الفيروس) بهذا الاسم لتشابه آلية عمله مع تلك الفيروسات التي تصيب الكائنات الحية بعدد من الخصائص كخاصية الانتقال بالعدوى وكونه كائناً غريباً يقوم بتغيير حالة

(1) Kate Brush (2020), cybercrime, through the link https://searchsecurity.techtarget.com/definition/cybercrime, last visit 17/7/2021.

(2) VICKY NGO-LAM (24-12-2019) "Cyber Crime: Types, Examples, and What Your Business Can Do", through the link https://www.exabeam.com/information-security/cyber-crime/, last visit 18/7/2021.

20-3.indd 223 9/24/2023 2:33:01 AM

الكائن المصاب إضافة إلى أن الضرر الذي يسبب فيه يجب أن يتم العلاج بإزالته.[1]

تعد الفيروسات من أخطر العوامل المؤثرة على جهاز الحاسوب ويمكن تعريفها وفقًا لتقرير صادر عن المركز الوطني الأمريكي للحاسبات لأنها (تهاجم البرامج التي تصيب أنظمة الكمبيوتر بطريقة مشابهة جدًا للفيروسات التي تصيب الأشخاص).[2]

يمكن أيضًا تعريف فيروس الكمبيوتر بأنه "برنامج يتكون من عدة أجزاء مكتوبة بإحدى لغات البرمجة بطريقة خاصة تسمح له بالتحكم في البرامج الأخرى وقادر على التكرار ويحتاج إلى برنامج وسيط (مثل مضيفه) أو مساحة القرص القابل للتنفيذ". [3]

كما يعد الفيروس برنامجًا مثل أي برنامج آخر موجود على جهاز الكمبيوتر الخاص بك، ولكنه مصمم ليكون قادرًا على التأثير على البرامج الأخرى الموجودة على جهاز الكمبيوتر الخاص بك والتحكم بها. [4]

وتختلف أنواع الفيروسات من حيث الحجم والنوع وطريقة عملها ومستوى الضرر الذي تسببه، بما في ذلك فيروسات محاكاة الحشرات، والفيروسات البطيئة، والفيروسات الخاملة، والفيروسات التطورية، والفيروسات القاتلة، والفيروسات الإسرائيلية، وفيروس السرطان، والفيروسات الجنسية، وإلى جانب هذه الفيروسات، هناك أنواع أخرى ظهرت في مناسبات معينة، منها فيروس مايكل أنجلو الذي انطلق بمناسبة ولادة هذا الرسام، وفيروس ناسا، وفيروس عيد الميلاد، وغيرها ممن يرتبط نشاطهم بفيروس حادثة معينة، مثل بدء تشغيل جهاز مثل الفيروس الباكستاني.

وتجدر الإشارة إلى أن فيروس الكمبيوتر له إحدى سمات المجرم حيث يختفي كخطوة أولى في وقت معين ثم يبدأ في الظهور كخطوة ثانية ليتم تدميره في الخطوة الثالثة تمامًا مثل المجرم الذي يتولى الإعداد لخطته لارتكاب جريمة وهي تلويث محركات الأقراص أو اتصالات شبكة الكمبيوتر أو البرامج أو الملفات، ويعد انتقاله عبر الإنترنت والبريد الإلكتروني أكثر خطورة، ويمكن أن يكون الفيروس خاصًا بالبرامج، وعندما يقوم المستخدم بتشغيل البرنامج ينتقل إلى القرص الموجود داخل الكمبيوتر ويبدأ في تخريب عمل البرامج

(1) الجنيبهي، ممدوح محمد (2006)، جرائم الأنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، ص71.

(2) الحماد، حسن حماد حميد (2013)، الإتلاف المعلوماتي، بحث منشور في كتاب (نحو معالجات لبعض المستجدات في القانون الجنائي (مجموعة أبحاث معمقة)، ط1، منشورات الحلبي الحقوقية، بيروت، ص135.

(3) مراد، عبد الفتاح، شرح جرائم الكمبيوتر والإنترنت، **الناشر:** خاص- عبد الفتاح مراد، 1900م، ص64.

(4) الجنيبهي، ممدوح محمد، مصدر سابق، ص68.

20-3.indd 224 9/24/2023 2:33:02 AM

أو إتلاف أو محو أو تعديل المعلومات وعندما يظهر فيروس ينتشر كالعدوى إلى برامج أخرى وينتشر بينها. (1)

ثانياً- دودة الكمبيوتر (Worms Computer)

تم استخدام مصطلح "دودة الكمبيوتر" لأول مرة في عام 1975 في رواية "The Rider Shockwave" لجون برونر. في هذه الرواية، يخلق بطل القصة دودة تجمع البيانات. في الأيام الأولى من علوم الكمبيوتر، تم تصميم الديدان لاستغلال نقاط الضعف في النظام. بدلا من إتلاف أجهزة الكمبيوتر المصابة بشكل خطير، استمروا في التكاثر في الخلفية. اليوم، ومع ذلك، فقد تغير الغرض من الديدان الكمبيوتر. اليوم، غالبا ما يستخدمها المهاجمون للوصول الكامل إلى أجهزة الكمبيوتر الخاصة بضحاياهم.

وتكون أجهزة الكمبيوتر المتصلة بشبكة عرضة لأشكال مختلفة من البرامج الضارة، بما في ذلك الديدان الكمبيوتر. دودة الكمبيوتر هي برامج ضارة تستنسخ نفسها وتنتشر عبر اتصالات الشبكة. لا تصيب دودة الكمبيوتر عادة ملفات الكمبيوتر، بل تصيب جهاز كمبيوتر آخر على الشبكة. يتم ذلك عن طريق دودة تكرار نفسها. تقوم الدودة بتمرير هذه القدرة إلى نسختها المتماثلة، مما يسمح لها بإصابة الأنظمة الأخرى بنفس الطريقة. يمكن أيضا العثور على الفرق بين ديدان الكمبيوتر والفيروسات هنا. ديدان الكمبيوتر هي برامج قائمة بذاتها تكرر نفسها وتعمل في الخلفية، في حين تتطلب الفيروسات ملف مضيف لتصيب.(2)

كيفية عمل دودة الكمبيوتر داخل الكمبيوتر المصاب:

من أجل الانتشار، تستخدم ديدان الكمبيوتر نقاط الضعف في الشبكات وتبحث عن باب خلفي لاختراق الشبكة دون أن يلاحظها أحد. وأحيانا تكون الدودة مرفقة برسائل البريد الإلكتروني للتصيد الاحتيالي أو مع الرسائل الفورية. ويحاول مجرمو الإنترنت تمويه الدودة بحيث يكون المستلم على استعداد لتشغيل البرنامج لهذا الغرض، على سبيل المثال، يتم استخدام امتدادات الملفات المزدوجة و / أو اسم بيانات يبدو غير ضار أو عاجل، مثل "الفاتورة". عندما يفتح المستخدم المرفق أو الرابط، سيقوم بتنزيل البرامج الضارة (دودة الكمبيوتر) على الفور في النظام أو توجيهها إلى موقع ويب خطير. في هذه الطريقة، الدودة تجد طريقها إلى نظام المستخدم دون أن يلاحظوا. بمجرد تنفيذها، تبحث الدودة عن

(1) الحلبي، خالد عياد (2011)، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، ط1، دار الثقافة للنشر والتوزيع، الأردن، ص77.

(2) Smith and Matrawy (2009), Computer Worms: Architectures-Evasion-Strategies-and Detection Mechanisms, Journal of Information Assurance and Security 4, p 69-83

20-3.indd 225 9/24/2023 2:33:02 AM

طريقة لتكرار واختراق الأنظمة الأخرى. إحدى طرق القيام بذلك، على سبيل المثال، هي أن ترسل الدودة بريدا إلكترونيا إلى جميع جهات الاتصال الموجودة على الكمبيوتر المصاب، والذي يحتوي على نسخ طبق الأصل من الدودة.

العديد من الديدان الآن ما يعرف باسم الحمولة، وفي هذه الحالة مرفق تجلبه الدودة معها. يمكن أن تحمل الدودة على سبيل المثال، برامج الفدية أو الفيروسات أو البرامج الضارة الأخرى، والتي تسبب تلفا للأنظمة المصابة. ويمكن بعد ذلك، على سبيل المثال، حذف الملفات على جهاز الكمبيوتر أو تشفير الملفات في حالة ابتزاز الضحية، يمكن لدودة الكمبيوتر أيضا تثبيت باب خلفي يمكن استغلاله لاحقا بواسطة برامج ضارة أخرى. هذه الثغرة الأمنية تعطي سيطرة مؤلف الدودة على الكمبيوتر المصاب.

ونظراً لأن الدودة أو مبرمجها يمكنه استخدام قوة الحوسبة للنظام المصاب، فغالبا ما يتم دمجها في الروبوتات. ثم يتم استخدامها من قبل مجرمي الإنترنت، على سبيل المثال لهجمات DDoS أو cyptominig. (1)

ثالثاً- حصان طروادة (horse Trojan)

هي برامج اختراق، وكذلك السمة المميزة لهذا النوع من البرمجيات التي لها القدرة على الانتشار عن طريق نسخ نفسها إلى ملفات أخرى ودخول أماكن سرية ومشفرة، وبالتالي الانتشار داخلها لتحقيق الغرض من تدميرها وتخريبها. (2)

من الصعب اكتشاف أحصنة طروادة لأنها تبدو برامج أو تطبيقات مفيدة ويميل المستخدم إلى تنزيلها. علاوة على ذلك، تمثل أحصنة طروادة في قاعدة البيانات هجوما متطورا لأنه يتم فصل الهجوم إلى قسمين: حقن الشيفرات الخبيثة ثم إعادة تسميتها، وهو أحد أسباب صعوبة تتبع أحصنة طروادة. (3)

يعمل فيروس طروادة عن طريق الاختباء ضمن مجموعة من البرامج المفيدة على ما يبدو. بمجرد التنفيذ أو التثبيت في النظام، سيبدأ هذا النوع من الفيروسات في إصابة الملفات الأخرى في الكمبيوتر. عادة ما يكون فيروس طروادة قادرا على سرقة معلومات

(1) Hornetsecurity (2021), Computer Worm, Article published through link https://www.hornetsecurity.com/en/knowledge-base/computer-worm/, last visit 18/7/2021.

(2) الخن، محمد طارق (2012)، الجريمة المعلوماتية، د.ن، د.م، ص40.

(3) Ghossoon M. Waleed (2014), A Comparison of Trojan Virus Behavior in Linux and Windows Operating Systems, World of Computer Science, and Information Technology Journal (WCSIT), ISSN: 2221-0741, Vol. 1, No. 3, 56-62,

20-3.indd 226 9/24/2023 2:33:02 AM

مهمة من كمبيوتر المستخدم. سيتمكن المطور بعد ذلك من الحصول على مستوى من التحكم في الكمبيوتر من خلال فيروس طروادة [1]. أثناء حدوث هذه الأشياء، سيلاحظ المستخدم أن الكمبيوتر المصاب أصبح بطيئا جدا أو غير متوقع النوافذ المنبثقة دون أي نشاط من المستخدم. في وقت لاحق، سيؤدي ذلك إلى تعطل الكمبيوتر. [2]

أنواع حصان طروادة:

هناك أنواع مختلفة من أحصنة طروادة التي تضر أجهزة كمبيوتر الضحية أو تهدد سلامة البيانات، أو تضعف عمل جهاز الضحية. يتم تضمين أحصنة طروادة متعددة الأغراض أيضا بعض مصنعين الفيروسات خلقت أحصنة طروادة متعددة الوظائف بدلا من حزم طروادة. بعض أنواع أحصنة طروادة كما هو موضح أدناه:

- حصان طروادة لسرقه كلمات المرور (Trojan PSW)
- حصان طروادة الناسخ (Droppers Trojan)
- الجزور الخفية (Rootkits)
- تحميل أحصنة طروادة أخرى (Downloaders Trojan)
- حصان طروادة للتجسس (Spies Trojan)
- حصان طروادة لفتح الأبواب الخلفية (Backdoors) [3]

وتعد أحصنة طروادة لفتح الأبواب الخلفية هي أخطر نوع من طروادة وأيضا الأكثر انتشارا. هذه الأحصنة هي أدوات مساعدة للإدارة عن بعد تفتح الأجهزة المصابة للتحكم الخارجي عبر شبكة LAN أو الإنترنت. وهي تعمل بنفس طريقة برامج الإدارة عن بعد القانونية المستخدمة من قبل administrators system. وهذا يجعل من الصعب اكتشافها.

(1) P2P-Worm.Win32. BlackControl.g, Trojan Programs. [cited; Available from: http://www.securelist.com/en/descriptions/15243378/P2PWorm.Win32.Bla ckControl.g, Aug 20, 2010.

(2) Danchev, D., "The Complete Windows Trojans", cited; Available from: http://www.windowsecurity.com/whitepapers/The_Complete_Windows_Tr ojans_Paper.html. Aug 29, 2005.

(3) ZHU Zhenfang (2015), Study on Computer Trojan Horse Virus and Its Prevention, International Journal of Engineering and Applied Sciences (IJEAS), ISSN: 2394-3661, Volume-2, Issue-8.

20-3.indd 227 9/24/2023 2:33:03 AM

والفرق الوحيد بين أداة الإدارة القانونية والباب الخلفي هو أن الأبواب الخلفية يتم تثبيتها وإطلاقها دون علم أو موافقة مستخدم آلة الضحية.

وبمجرد إطلاق الباب الخلفي، فإنه يراقب النظام المحلي دون علم المستخدم؛ في كثير من الأحيان لن يكون الباب الخلفي مرئيا في سجل البرامج النشطة. بمجرد تثبيت أداة الإدارة عن بعد وإطلاقها بنجاح، يكون جهاز الضحية مفتوحا على مصراعيه. ويمكن أن تشمل وظائف الباب الخلفي الآتي:

- إرسال / استقبال الملفات
- إطلاق / حذف الملفات
- تنفيذ الملفات
- حذف البيانات
- إعادة تشغيل الجهاز[1]

رابعاً- القنابل المنطقية أو الزمنية

يمكن تعريف القنابل النطقية أو الزمنية على إنها برامج صغيرة يتم وضعها بشكل غير قانوني وسري مع برامج أخرى بغرض تدمير وتخريب وتغيير برامج الحاسوب والمعلومات والبيانات في وقت محدد. [2]

من الممكن تعريف القنبلة المنطقية كبرنامج أو جزء من برنامج يتم تنفيذه في نقطة زمنية محددة أو في أي إطار زمني محدد، كيوم، أو سنة. ويتم إدخالها في البرنامج وتنفيذها في جزء صغير من ثانية أو في ثوانٍ أو دقائق وقد يتم ضبط توقيتها لتنفجر بعد سنة كاملة. [3]

وفي هذا الصدد، يتضح لنا أن القنابل المنطقية تظل ثابتة وغير فعالة وبالتالي غير مكتشفة لفترة قد تكون طويلة أو قصيرة، يحددها المؤشر الموجود في برنامج القنبلة، وأن هذا المؤشر لا يقتصر على فترة الوقت، ولكن قد يمتد إلى ما يعرف بتوافر شروط منطقية معينة من برنامج أو ملف معين. هذا حسب الكود المحدد في برنامج القنبلة. إذا حان الوقت أو تم استيفاء هذه الشروط، يبدأ البرنامج في أداء مهامه التخريبية.

(1) P2P-Worm.Win32. BlackControl.g, Trojan Programs, Op. cit. P 57.

(2) الحلبي، خالد عياد، مرجع سابق، ص 86.

(3) الحماد، حسن حماد حميد، مرجع سابق، ص 139.

20-3.indd 228 9/24/2023 2:33:03 AM

ولما كان لكل جريمة سواء كانت تقليدية أو الكترونية مسرحا لارتكاب هذه الجريمة والذي يمكن استخلاص بعض الأدلة منه، ونظرا لأهمية ودقة مسرح الجريمة الإلكترونية.

ثانياً- مشكلة البحث:

نظرا للطبيعة الخاصة التي يتميز بها مسرح الجريمة الإلكترونية، وصعوبة الحصول علي الدليل بعكس مسرح الجريمة التقليدية وكذلك كون هذا الدليل هو من الوسائل الإلكترونية فقد تثار حوله العديد من المشكلات فيما إذا كان يمكن قبوله كدليل للإثبات، لأنه من السهل التلاعب بالدليل وتغيير الحقيقة التي يمكن أن يعبر عنها، كذلك تتمثل المشكلة في اختلاف طرق المحافظة على مسرح الجريمة والأدلة مما يصعب معه وضع قاعدة قانونية موحدة تصلح لجميع الأحوال.

وتتمحور مشكلة الدراسة حول تساؤل رئيسي وهو:

1. **ماهي الإجراءات القانونية للتعامل مع مسرح الجريمة الإلكترونية في التشريع الإماراتي؟**

وهناك عدة تساؤلات فرعية وهي:

2. ما الذي يجعل مسرح الجريمة الإلكترونية أكثر تميزا عن مسرح الجريمة التقليدية؟
3. ماهي طرق المحافظة على مسرح الجريمة الإلكترونية وكذلك الأدلة الموجودة به؟
4. كيف تتم معاينة مسرح الجريمة الإلكترونية؟

ثالثاً- أهمية الدراسة

إن دراسة موضوع إجراءات التعامل مع مسرح الجريمة الإلكترونية من الموضوعات الحديثة التي جذبت اهتمام الكثير من الباحثين في عرصنا الحالي نظرا لتطور الوسائل التكنولوجية وبتطور هذه الأخيرة أصبحت للجرائم أبعاد أخرى، إذ ظهرت جرائم تسمى بالجرائم الإلكترونية، تلك التي تعد من الجرائم التي يصعب التحقيق فيها ويجب أن تتوفر عدة وسائل بشرية أو مادية للتحقيق في مسرح الجريمة الرقمية، ومن ثم أردنا أن نسلط الضوء على هذه الإجراءات في مثل هذا النوع من الجرائم الذي يتميز بخصوصيته بالمقارنة مع الجرائم التقليدية.

20-3.indd 229 9/24/2023 2:33:03 AM

رابعاً- محددات البحث

تتمثل حدود البحث فيما يلي:

1. **المجال المكاني**: سوف يقتصر البحث على الحدود المكانية لدولة الإمارات العربية المتحدة والقوانين الخاصة بها.
2. **المجال الزماني**: ستجري هذه الدراسة ابتداء من عام 2021، لكنها ستتنا ول الأوضاع التشريعية السابقة عليها، والاجتهادات القضائية المتعلقة بموضوع إجراءات التعامل مع مسرح الجريمة الإلكترونية.

خامساً- مصطلحات البحث

الجريمة الإلكترونية: يمكن تعريف الجريمة الإلكترونية على أنها أي مخالفة ترتكب ضد أفراد أو جماعات بدافع جرمي و نية الإساءة لسمعة الضحية أو لجسدها أو عقليتها، سواءً كان ذلك بطريقة مباشرة أو غير مباشرة، و أن يتم ذلك باستخدام وسائل الاتصالات الحديثة مثل الإنترنت، غرف الدردشة، البريد الإلكتروني أو المجموعات.

مسرح الجريمة: هو كل محل أو وحدة من منشأة أو رقعة من الأرض تضم بؤرة الجريمة ومركزها بحيث تكون ميداناً لأنشطة الجاني أو الجناة من الفاعلين الأصليين عند ارتكاب الأفعال المؤثمة جنائياً والتي تدخل في عداد الأعمال التنفيذية المكونة للجريمة أو الشروع فيها. (1)

القرصنة (piracy): هي نسخ برامج السوفت وير المؤمنة بدون تصريح.

الإرهاب الإلكتروني (cyberterrorism): هو عبارة عن الهجمات غير القانونية والتهديدات بهجمات إرهابية ضد الحاسوب والمعلومات المخزنة عليهما، لترويع أو إرغام حكومات أو مواطنيها على تقوية الأهداف الاجتماعية أو السياسية للمعتدى.

سادساً- منهج البحث

سيتم الاعتماد على المنهج الوصفي التحليلي؛ من أجل وصف وتحليل الدور الهام لمسرح الجريمة الإلكترونية وكيفية التعامل معه ومع الأدلة الإلكترونية وكذلك تحليل النصوص القانونية ومناقشتها وكذلك الآراء الفقهية بشأن موضوع البحث، ومن ثم التعرف على نقاط القوة ونقاط الضعف، وتقديم التوصيات المتاحة بشأنها.

(1) ممدوح، خالد (2009)، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، ص22.

20-3.indd 230 9/24/2023 2:33:03 AM

سابعاً- خطة البحث

من أجل الإحاطة بموضوع البحث تم تقسيمة إلى مبحثين على النحو التالي:

المبحث الأول: الإجراءات القانونية للتعامل مع مسرح الجريمة الإلكترونية في التشريع الإماراتي

- **المطلب الأول : إجراءات التحري والتحقيق الجنائي وجمع الأدلة في مسرح الجريمة الإلكترونية في التشريع الإماراتي.**
- الفرع الأول: عناصر التحري الجنائي في الجرائم الإلكترونية
- الفرع الثاني: معاينة مسرح الجريمة الإلكترونية
- الفرع الثالث: وسائل التحقيق في الجرائم الإلكترونية
- **المطلب الثاني: حجية الدليل الإلكتروني في الإثبات الجنائي وموقف المشرع الإماراتي منه.**
- الفرع الأول: تقييم صحة الدليل الإلكتروني من التزوير والعبث
- الفرع الثاني: تقييم الدليل الإلكتروني من حيث السلامة الفنية للإجراءات المتبعة في الحصول عليه

المبحث الأول: الإجراءات القانونية للتعامل مع مسرح الجريمة الإلكترونية في التشريع الإماراتي

تمهيد وتقسيم:

لقد تجاوزت الجرائم الإلكترونية الصورة النمطية الموحدة التي تتميز بها الجرائم التقليدية بطبيعتها الكلية والتي حاولت التشريعات الإجرائية التصدي لها، خاصة طرق مكافحتها، لكن جرائم العصر الرقمي الجديد خلقت مشكلة شاملة تبرز كيفية التعامل مع تلك الجرائم التي أجبرت المشرع على تصحيح النقص الموجود في التشريعات الحالية ومحاولة سدّه وذلك وفق عدة معايير أهمها التكنولوجيا العالية في هذه الجريمة، ولإيضاح مضمون هذا المبحث اقتضي تقسيمه إلى مطلبين على النحو التالي:

المطلب الأول: إجراءات التحري الجنائي وجمع الأدلة في مسرح الجريمة الإلكترونية في التشريع الإماراتي

20-3.indd 231 9/24/2023 2:33:04 AM

المطلب الثاني: إجراءات التحقيق في مسرح الجريمة الإلكترونية وتعقب مرتكبو الجرائم الإلكترونية في التشريع الإماراتي

المطلب الأول: إجراءات التحري والتحقيق الجنائي وجمع الأدلة في مسرح الجريمة الإلكترونية في التشريع الإماراتي

وتمهيد وتقسيم:

في حين أن هناك تشابهًا قويًا بين التحقيق في جرائم الإنترنت والتحقيق في الجرائم الأخرى، إلا أنهما يتطلبان عمومًا إجراءات مماثلة مثل المعاينة والتفتيش والشهادة والخبرة بالإضافة إلى جمع الأدلة، وجميعهم يشاركون حقيقة أنهم يسعون للإجابة على تساؤلات المحقق والتي تتمثل في: ماذا حدث؟ وأين؟ وكيف؟ ومن؟ ولماذا؟

تختلف جرائم الإنترنت عن الجرائم الأخرى في سمات معينة، وهذا بالطبع يتطلب تطوير أساليب وإجراءات التحقيق بما يتفق مع هذه الخصوصية، وتمكن المحقق من كشف الجريمة والتعرف على مرتكبيها بالسرعة والدقة اللازمتين. فالتحقيق في هذا النوع من الجرائم يتطلب الرجوع إلى عدد كبير من السجلات المراد عرضها، مثل أدلة الكمبيوتر وملفات سجل عمليات الكمبيوتر، بالإضافة إلى الوصول والاطلاع على كمية كبيرة من سجلات الأجهزة لتكوين خلفية منظمة عن المؤسسة وموظفيها. (1)

مما لا شك فيه أن مثل هذه الجرائم قد غيرت طريقة عمل وكالات التحري والتحقيق، مما أجبرها على التعامل مع مسرح جريمة غير نمطي يقع في عالم افتراضي وفي بيئة معلوماتية تتطلب مهارات وقدرات وتقنيات خاصة قد لا يتوفر معظمها، وإجبارهم على تخصيص فرق متخصصة في مجال تقنية المعلومات ومراقبتها لمكافحة هذه الجرائم. (2)

وعلى المستوى الإجرائي والتحري الجنائي، تشكل الإجراءات التقليدية للفحص البصري والتفتيش واستجواب الشهود وتعيين الخبراء أساس عمل هيئات التحقيق والتحقيق للحصول على أدلة الطب الشرعي والتحقق من الجريمة والقبض على الجناة وتقديمهم للمحاكمة. كما يعد كل من المعاينة والتفتيش والشهادة إحدى طرق جمع الأدلة.

(1) إبراهيم، خالد ممدوح (2009)، الجرائم المعلوماتية، دار الفكر الجامعي، ط1، الإسكندرية، ص 23.

(2) أحمد، سعيد (2005)، الجرائم الإلكترونية وآليات الحصول على الدليل فيها، النشر الذهبي، الطبعة الأولي، ص53.

20-3.indd 232 9/24/2023 2:33:04 AM

الفرع الأول: عناصر التحري الجنائي في الجرائم الإلكترونية

لفهم موضوع فن ومبادئ التحري الجنائي في الجرائم الإلكترونية، تحتاج إلى فهم المبادئ الأساسية للتحقيق، والتي تتطلب مقدمة للعناصر الأساسية للتحقيق. كما تشير عناصر التحقيق أو التحري إلى الإجراءات التي تستخدمها سلطات التحقيق من أجل تطبيق طرق تحقيق ثابتة ومحددة لإثبات الجريمة، ووقوع الجاني وتحديد شخصية الجاني. [1]

وقد حدد المشرع الإماراتي عناصر التحري والتحقيق الجنائي في القانون الاتحادي رقم (35) لسنه 1992 (قانون الإجراءات الجزائية)، حيث نصت المادة رقم (30) على أنه " يقوم مأمورو الضبط القضائي بتقصي الجرائم والبحث عن مرتكبيها وجمع المعلومات والأدلة اللازمة للتحقيق والاتهام".[2]

كما خصص المشرع في حالة الانتهاكات والجرائم الإلكترونية سياسة تنظيمية وضعتها هيئة تنظيم الاتصالات (إدارة النفاذ إلى الإنترنت)، تتم بها عملية اكتشاف المحتوى المحظور وتصنيفه بطريقتين:

1. بشكل رئيسي باستخدام أنظمة تقنية متكاملة مع شبكة المرخص لهم مهيأة ومخصصة لتصنيف واكتشاف المحتوى المحظور.
2. عن طريق البلاغات التي ترد من الجمهور أو من الجهات الحكومية ذوي الاختصاص أو من القضاء أو أية قائمة تحددها الهيئة.

ويتم تحديد نطاق المحتوى المحظور إما عن طريق عنوانه الإلكتروني أو نمط أو بصمة إلكترونية يتم تحديدها للمحتوى أو بأية وسيلة تقنية يمكن استخدامها لتحديد نطاق المحتوى المحظور دون المساس بالمحتوى غير المحظور. [3]

كذلك يكون لمأموري الضبط القضائي من الإدارات الحكومية المختلفة سلطة ملاحقة الجرائم وجمع الأدلة. ويشمل ذلك مأموري الضبط القضائي من إدارة الشرطة، والنيابة العامة والمحاكم الجنائية. وبالإضافة إلى ذلك، وفقا للمادة (32) من قانون الإجراءات

(1) نعيم، سعداني (2013)، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجيستير، في العلوم القانونية، تخصص علوم جنائية، كلية الحقوق والعلوم السياسية- قسم الحقوق- جامعة الحاج لخضر- باتنة، ص 112-111.

(2) انظر نص المادة (30) من القانون الاتحادي رقم (35) رقم 1992م بإصدار قانون الإجراءات الجزائية، الطبعة الثالثة 2017 م، دائرة القضاء بأبو ظبي.

(3) سياسة تنظيمية رقم (3)، إدارة النفاذ الي الإنترنت، الهيئة العامة لتنظيم الاتصالات، نسخة الكترونية رقم 1، الإمارات العربية المتحدة، أبو ظبي، 2017.

20-3.indd 233 9/24/2023 2:33:04 AM

الجزائيـة، يصـرح لجهـات مختلفـة أخـرى جمـع الأدلـة فـي التحقيقـات الجنائيـة، مثـل:

- ضباط القوات المسلحة
- شرطة الحدود
- خفر السواحل
- ضباط الإدارة العامة للإقامة وشؤون الأجانب
- مفتشو البلديات
- وزارة الصحة ووقاية المجتمع. [1]

الفرع الثاني: معاينة مسرح الجريمة الإلكترونية

مسـرح الجريمـة هـو مفتـاح حـل أي لغـز جريمـة، وهـو حجـر الزاويـة الأول والأهـم لبدايـة حـل هـذه الجريمـة. فـي بعـض الأحيـان بجانـب المسـرح الرئيسـي يوجـد أكثـر مـن مـكان لمسـرح الحـادث وهـذه الأماكـن هـي الأماكـن التـي تـم فيهـا التحضيـر وإعـداد الجرائـم [2]، أو الأماكـن التـي تحتـوي علـى آثـار جرائمهـم. ويقصـد بالمعاينـة الرؤيـة بالعيـن المجـردة، والغـرض منـه مشـاهدة ووصـف مسـرح الجريمـة. [3]

إن معاينـة وتفتيـش مسـرح الجريمـة هـو عمـل متخصـص للغايـة يتطلـب سـنوات مـن الخبـرة العمليـة مصحوبـة بالتعليـم والتدريـب المسـتمر

ويلـزم قبـل وصـول المحققيـن والفنييـن إلـى مسـرح الجريمـة، يجـب إعـداد خطـة عمـل شـاملة وفـق الخطـوات التاليـة:

1. تجهيز المواد والمغلفات اللازمة لسفن الجريمة الرقمية بمختلف أحجامها وأشكالها.
2. تحضير النموذج الأولي لتسجيل المستندات المطلوبة للفحص

(1) الموقع الرسمي لحكومة دولة الإمارات العربية المتحدة، معلومات وخدمات، العدل والسلامة والقانون، إجراءات التقاضي، الدعاوى الجزائية، تتبع الجرائم وجمع الأدلة، من خلال اللينك https://u.ae/ar-ae/informa-tion-and-services/justice-safety-and-the-law/litigation-procedures/criminal-cases، تاريخ أخر زيارة 20/7/2021م.

(2) فرج، هشام عبد الحميد (2004 م) معاينة مسرح الجريمة. الطبعة الأولى، مطابع اللواء الحديثة، القاهرة، مصر.

(3) العجرفي، علي بن حامد (1987)، إجراءات جمع الأدلة ودورها في كشف الجريمة، الطبعة الثالثة، دون دار نشر، الرياض، السعودية.

20-3.indd 234 9/24/2023 2:33:04 AM

3. تأكد من أن جميع المهنيين والفنيين يفهمون شكل الأدلة والتعامل الصحيح معها
4. تقييم النتائج القانونية لعمليات التفتيش على مسرح الجريمة الرقمية.
5. بحث متوقع عن التأثير المادي لمسرح الجريمة الرقمية
6. حدد المسؤول قبل وصوله إلى مسرح الجريمة.
7. القيام بإعداد مهام الطاقم الأساسية قبل الوصول.
8. تقييم مهام الطاقم المطلوبة للتعامل بنجاح مع مسرح الجريمة. (1)

كما أن هناك ضوابط يجب تطبيقها عند إجراء المعاينة لمسرح الجريمة الإلكترونية وهي كما يلي:

1. تصوير الكمبيوتر والأجهزة الطرفية الخاصة به، وأيضا يجب تسجيل الوقت والتاريخ والمكان الذي تم فيه التقاط الصورة.
2. إبلاغ الفريق الذي سيجري التفتيش مقدمًا من أجل الاستعداد من الناحية الفنية والعملية حتى يمكن وضع خطة مناسبة للحصول على الأدلة الجنائية فور التفتيش.
3. إعداد خطة التفتيش مرفق بها رسومات توضيحية وإجراء مراجعة شاملة للتأكد من تنفيذها بالكامل.
4. الانتباه إلى كيفية إعداد النظام.
5. الانتباه لإثبات حالة التوصيلات والكابلات لجميع مكونات النظام، بحيث يمكنك مقارنتها وتحليلها لاحقًا عند تقديم سؤال للمحكمة.
6. قبل إجراء الاختبار، لا ترسل أي مواد إعلامية من مسرح الجريمة للتأكد من أن البيئة الخارجية لموقع الكمبيوتر لا تحتوي على أي مجالات مغناطيسية قد تتسبب في حذف البيانات المسجلة.
7. الاحتفاظ بالورق المهمل أو الممزق، وورق الكربون المستخدم، والأشرطة غير الصحيحة، والمعلومات غير المرغوب فيها على الأقراص المدمجة، وقم بإزالة بصمات الأصابع المتعلقة بالجريمة منها.

(1) هلال، محمد رضوان (2014)، كيفية التعامل التقني والآمن مع أوعية الجريمة الرقمية في مسرح الجريمة لضامن حيدة الدليل المستخلص، المجلة العربية الدولية للمعلوماتية، المجلد الثالث، العدد الخامس.

20-3.indd 235 9/24/2023 2:33:04 AM

8. الاحتفاظ بملفات الإدخال والإخراج الورقية للكمبيوتر المتعلقة بالجريمة

9. حصر عمليات التفتيش على الباحثين والمحققين الذين لديهم قدرات علمية وخبرة فنية في مجال الكمبيوتر. (1)

وقد قضت المحكمة الإتحادية العليا في دولة الإمارات العربية المتحدة بأن: "لما كانت المواد 35/36/40 من قانون الإجراءات الجزائية الاتحادي 35/1992 (توجب على مأموري الضبط القضائي ومرؤوسيهم أن يحصلوا على الإيضاحات، وإجراء المعاينة اللازمة لتسهيل الوقائع التي تبلغ إليهم أو التي يعلمون بها بأية كيفية كانت وأن يثبتوا الإجراءات التي يقومون بها في محاضر موقع عليها منهم؛ يبين بها وقت اتخاذ الإجراءات ومكان حصولها). (2)

الفرع الثالث: وسائل التحقيق في الجرائم الإلكترونية

للجرائم الإلكترونية طابعها الخاص، فالتحقيق يتطلب معرفة كاملة ووعيًا بوسائل الجريمة، ومن ثم حل الغموض والوصول إلى الفاعل، وعند التحقيق في جريمة (3)، يجب على المحقق الامتثال للقانون، والتشريعات، واللوائح المفسرة، والتقنية. المبادئ التي تضمن الشرعية وتسهل الوصول إلى الجاني، ولكن كيف يمكن إثبات جريمة الكمبيوتر؟ هذا سؤال يحدد الإطار الذي سيعمل فيه ضابط الضبطية العدلية. سبق أن ذكر أن فريق التحقيق في جرائم الكمبيوتر والإنترنت يمكنه العثور على أدلة رقمية في مسرح الجريمة الإلكترونية وسط كمية هائلة من البيانات، وهي عقبة يمكن أن تمنع استخراج الأدلة، ولكن هناك العديد من البرامج التي يمكن أن تؤدي دورًا رئيسًا في مساعدة فريق التحقيق على الإسراع في جمع المزيد من الأدلة، وهناك طرق للمساعدة، من أهمها:

أولاً- الوسائل المادية:

هي الأدوات الفنية التي غالبا ما تستخدم في بنية نظم المعلومات والتي يمكن باستخدامها تنفيذ أساليب وإجراءات التحقيق المختلفة والتي تثبت وقوع الجريمة وتساعد على تحديد شخصية مرتكبها وفي هذه الحالة أباح المشرع الإماراتي لمأمور الضبط القضائي بالتفتيش

(1) Taylor Robert (1992), computer crime, in criminal investigation, edited by Charles Swanson, N. Chamelin, Hill Inc. 5th edition, p450.

(2) الطعن رقم 133 لسنة 17 قانون جزائي، جلسة 27/1/1996، مكتب فني 18، رقم الجزء 1، ص2 اتحادية عليا.

(3) السرحاني، محمد بن نصير محمد (2004)، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت، بحث مقدم استكمالا لمتطلبات الحصول على درجة الماجستير في قسم العلوم الشرطية، تخصص القيادة الأمنية، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، قسم العلوم الشرطية، الرياض، ص63.

20-3.indd 236 9/24/2023 2:33:05 AM

ورصد أدوات الجريمة في نص المادة (71) من قانون الإجراءات الجزائية الإماراتي رقم (35) لسنة 1992 حيث نصت المادة علي أنه " ينتقل عضو النيابة العامة إلى أي مكان ليثبت حالة الأشخاص والأماكن والأشياء المتصلة بالجريمة وكل ما يلزم إثبات حالته"، وكذلك نصت المادة (72) من ذات القانون علي أنه " لعضو النيابة العامة تفتيش منزل المتهم بناء علي تهمة موجهه إليه بارتكاب جريمة أو باشتراكه في ارتكابها، وله أن يفتش أي مكان ويضبط فيه أو أية أوراق أو أسلحة وكل ما يحتمل أنه استعمل في ارتكاب الجريمة أو نتج منها أو وقعت عليه وكذلك كل ما يفيد في كشف الحقيقة".[1] ومن أهمها:

1. **عناوينIP، والبريد الإلكتروني، وبرامج المحادثة:** عنوان الإنترنت هو المسؤول عن توصيل حزم البيانات عبر شبكة الإنترنت وتوجيهها إلى أهدافها وهو بشبه إلى حد كبير عنوان البريد العادي وفي حالة وجود أية مشكلة أو أية أعمال تخريبية فان أول ما يجب أن يقوم به المحقق هو البحث عن رقم الجهاز وتحديد موقعه لمعرفة الجاني الذي قام بتلك الأعمال غير القانونية، ويمكن لمزود خدمة الإنترنت أن يراقب المشترك كما يمكن للشبكة التي تقدم خدمة الاتصال الهاتفي أن تراقبه أيضا إذا ما توافرت لديها أجهزة وبرامج خاصة لذلك. [2]

2. **الجدار الناري (Firewall):** أثناء العمل على هذه المهمة، تقوم هذه البرامج بتوثيق عمليات الاتصال الداخلي والخارجي وإنشاء سجلات توضح مصدر كل اتصال والغرض منه، بحيث يتم حفظ هذه السجلات كملفات مرجعية يمكن الرجوع إليها وقراءتها في أي وقت.

3. **برامج التتبع:** تحدد هذه البرامج محاولات الاختراق وتزود المستخدم الذي تم اختراق جهازه ببيان شامل يتضمن اسم الحدث وتاريخ حدوثه وعنوان IP الذي حدث الاختراق من خلاله واسم مزود خدمة الإنترنت Hacker ISP المضيف وأرقام الدخول والخروج الخاصة به على الإنترنت وغيرها من المعلومات.

4. **أدوات الضبط:** وهي الأدوات التي تعتبر تدابير مادية تساعد في السيطرة على جرائم المعلومات، على سبيل المثال برامج الأمن، وأدوات التدقيق، وأدوات مراقبة مستخدمي الشبكة، وبرامج التنصت على الشبكة، والتقارير التي تم إنشاؤها

(1) انظر نص المادتين (72-71) من القانون الاتحادي رقم (35) رقم 1992م بإصدار قانون الإجراءات الجزائية، مرجع سابق.

(2) العنزي، سليمان ابن مهجع (2003)، وسائل التحقق في جرائم نظم المعلومات، رسالة ماجستير في العلوم الشرطية، كلية الدراسات العليا جامعة نايف العربية للعلوم الأمنية، الرياض، ص99.

20-3.indd 237 9/24/2023 2:33:05 AM

بواسطة أنظمة أمان البيانات، وبرامج التصفح وقواعد البيانات الاحتياطية. (1)

5. **أدوات فحص ومراقبة الشبكات:** وتستخدم في فحص بروتوكول IP/TCP وذلك معرفة ما قد يصيب الشبكة من مشاكل ومعرفة العمليات التي تتعرض لها ومن هذه الأدوات أداة (ARP)، برنامج (TPUT VISUAL)، كذلك أداة (STAT NET).

ثانياً- الوسائل الإجرائية:

يقصد بها الإجراءات التي باستخدامها يتم تنفيذ طرق التحقيق الثابتة والمحددة والمتغيرة وغير المحددة التي تثبت وقوع الجريمة وتحدد شخصية مرتكبها ومنها:

1. **اقتفاء الأثر(التتبع):** من أكثر الأشياء التي يخشاها مجرمو الإنترنت هي تتبعهم عندما يقوموا بارتكاب جريمة. كما أن هناك العديد من الوثائق المنشورة على موقع المخترق، والتي تحتوي على العديد من النصائح، أولها اقتراح، يتغلب على غطائك. سيتم بالتأكيد القبض على المتسللين إذا لم يمحوا آثارهم، حتى إذا تم تنفيذ عملية التسلل بشكل صحيح، فمن الضروري تتبع الآثار بعدة طرق، سواء كان ذلك عن طريق البريد الإلكتروني أو من خلال تتبع أثر الجهاز الذي يستخدم للتسلل. (2)

2. **التحقق من تشغيل الأنظمة الإلكترونية وطرق الحماية:** عند التحقيق في جرائم المعلومات مثل جرائم معلومات الشبكة، يجب أن يكون المحققون على دراية بنظام المعلومات والشبكات المكونة له والتطبيقات والخدمات المقدمة للعملاء. كما يجب مراجعة تشغيل وإدارة نظام المعلومات كقاعدة بيانات، وكذلك خطة حمايته، وفهم تصنيف مواد النظام، والمستفيدين، والملفات، والبرامج، والموارد العامة، ودرجة تزامن المعدات، والوقت من اليوم للسماح باستخدام كلمات المرور، ونطاق السلطة المخصصة للمستفيدين، وإجراءات الموظفين، وطرق النسخ الاحتياطي، واستخدام برامج الحماية كموارد وبرامج لرصد المستفيدين، ومعالجة البيانات، وتسجيل الحوادث، والإخفاقات. بالإضافة إلى فهم جودة برنامج الحماية وأساليب عمله وكذلك من أمن البيانات بالإضافة إلى الاستفادة من التقارير التي يصدرها النظام وتقارير جدار الحماية، يمكنك أيضًا الوصول إلى النظام. (3)

---

(1) المرجع نفسه.

(2) الفيل، علي عدنان (2012)، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية (دراسة مقارنة)، دون طبعة، المكتب الجامعي الحديث، بدون بلد نشر، صفحة 67.

(3) المرجع نفسه، ص 78-77.

20-3.indd 238 9/24/2023 2:33:05 AM

المطلب الثاني: حجية الدليل الإلكتروني في الإثبات الجنائي وموقف المشرع الإماراتي منه

تمهيد وتقسيم:

مجرد الحصول على الأدلة الإلكترونية وتقديمها إلى القضاء لا يكفي لاستخدامها كدليل إدانة، لأن الطبيعة التقنية للأدلة الإلكترونية تسمح بالتلاعب بمحتوياتها بشكل يشوه الحقائق، ولا يوجد شخص غير محترف يكون قادر على علم بالعبث. بالإضافة إلى أن معدل الخطأ في الإجراء له دليل صادق على الإبلاغ عن الحقيقة، لذلك يبدو طبيعيًا في هذا النوع من الأدلة، لذلك تتكون فكرة الشك في مصداقية الأدلة الإلكترونية كدليل جنائي. (1)

الفرع الأول: تقييم صحة الدليل الإلكتروني من التزوير والعبث

هناك طرق عديدة لضمان عدم العبث بسلامة الدليل الإلكتروني، ومنها: (2)

فكرة التحليل الرقمي التناظري والتي تتمثل في مقارنة الأدلة الرقمية المقدمة إلى القضاء بالأصل المُدرج في الآلة الرقمية لتحديد مدى العبث بالنسخة المستخرجة، وكذلك استخدام الكمبيوتر يلعب جانب المعلومات الفنية لمحتوى الأدلة دورًا مهمًا، ويستخدم هذا العلم أيضًا للكشف عن مدى التلاعب بمحتوى الأدلة.

تُستخدم عمليات حسابية خاصة تسمى الخوارزميات وتستخدم هذه التقنية عندما يتعذر الحصول على النسخة الأصلية من الدليل الرقمي، أو في حالة العبث بالنسخة الأصلية، من الممكن التأكد من الحصول على الأدلة الرقمية من التشوهات والتغييرات باستخدام هذه العمليات الحسابية.

يعد استخدام الأدلة المحايدة نوعًا من الأدلة الرقمية المخزنة في بيئة افتراضية، والتي لا علاقة لها بالموضوع الجنائي، ولكنها تساعد في ضمان سلامة الأدلة الرقمية المتوقعة دون أي تعديل في نظام الكمبيوتر. (3)

لا شك أن الخبرة الفنية في هذه الحالة تؤدي دورًا مهمًا في التحقق من سلامة الأدلة الرقمية. إذا كانت الخبرة الفنية ذات أهمية كبيرة في مجال استخراج الأدلة الرقمية، فسيكون لها نفس الدور في التحقق من المصداقية وتقييم المصداقية. بدون أي تلاعب، يمكن للقضاة

(1) الحلبي، خالد عياد، مرجع سابق، ص 246.

(2) نعيم، سعداني، مرجع سابق، ص 217.

(3) الحلبي، خالد عياد، مرجع سابق، ص 264

20-3.indd 239 9/24/2023 2:33:06 AM

الذين يفتقرون إلى المعلومات والثقافة أن يكونوا بمثابة واجبات قضائية. والمجرمون الذين يستخدمون المعرفة المهنية في هذه الأمور ليسوا فقط لإكمال الأدلة، ولكن أيضًا للتحقق من مصداقيتهم في مجال معالجة المعلومات. ولضمان يقين الأدلة.

وقد ألزم المشرع الإماراتي الخبير بالقيام بمهمة الخبرة بنفسه بدون توكيل غيره أو تفويضه وذلك لعدم التلاعب في النتائج وضمان مصداقيتها وفقا للمادة لمادة (11 / 2) من القانون رقم 7 لسنة 2012 في شأن تنظيم مهنة الخبرة أمام الجهات القضائية، وتطابقها المادة (14 / 2) من لائحته التنفيذية رقم 6 لسنة 2014،والمادة (6 / 2) من القرار الوزاري رقم 116 لسنة 2015م بشأن ميثاق عمل الخبراء الفنيين والتي تضمنت وجوب تنفيذ الخبير القضائي المهام الموكلة إليه بنفسه في حدود المهمة المكلف بها، والمادة (4 / 3) من قرار رئيس دائرة القضاء في أبوظبي رقم 10 لسنة 2015م بشأن مدونة سلوك الخبراء. (1)

الفرع الثاني: تقييم الدليل الإلكتروني من حيث السلامة الفنية للإجراءات المتبعة في الحصول عليه

بشكل عام، يتطلب الحصول على الأدلة الرقمية اتباع بعض الإجراءات الفنية، وقد أشرنا بالفعل إلى أن هذه الإجراءات قد ترتكب أخطاء وقد تشكك في سلامة النتائج. لذلك، في هذا الصدد، يمكن استخدام ما يعرف بـ (test por) كوسيلة لضمان سلامة الإجراءات المتبعة للحصول على البراهين الرقمية، كدليل على مصداقيتها من حيث الأدلة المنتجة، فحص الميناء هو طريقة عن بُعد للتحقق مما إذا كان المنفذ مفتوحًا أم مغلقًا. إنه مفيد للمحققين الذين يرغبون في التحقق من إعادة توجيه المنفذ والتحقق مما إذا كان الخادم أو البرنامج قيد التشغيل أو ما إذا كان جدار الحماية يحظر منافذ معينة، لذلك سنعرض بإيجاز الخطوات التالية للتأكد أن هذه البرامج سليمة من الناحية الفنية: (2)

أ. إخضاع الأداة المستخدمة لعدة تجارب للتأكد من دقتها في إعطاء النتائج المبتغاة، وذلك باتباع اختبارين رئيسين هما:

- **اختبار السلبيات الزائفة:** ومفاد هذا الاختبار أن تخضع الأداة المستخدمة في الحصول على الدليل لاختبار يبين مدى قدرتها على عرض كافة البيانات المتعلقة بالدليل الرقمي، وأنه لا يتم إغفال بيانات مهمة عنه.

(1) صدر القرار عن وزير العدل بتاريخ: 30 / 3 / 2015م وفقا للمادة 34 من القانون الاتحادي رقم 7 لسنة 2012، المذكور أعلاه، وتم نشر القرار في الجريدة الرسمية لدولة الإمارات العربية المتحدة، العدد 578، ص 625.

(2) مدين، محمود (2020)، فن التحقيق والإثبات في الجرائم الإلكترونية، كتاب للنشر والتوزيع، الطبعة الأولي، القاهرة، مصر، ص 472.

20-3.indd 240 9/24/2023 2:33:06 AM

- **اختيار الإيجابيات الزائفة:** ومفاد ذلك أن تخضع الأداة المستخدمة في الحصول على الدليل الرقمي اختبار في يمكن من التأكد من أن هذه الأداة لا تعرض بيانات إضافية جديدة، وبذلك يتم من خلال هذين الاختبارين التأكد من أن الأداة المستخدمة عرضت كل البيانات المتعلقة بالدليل الرقمي وفي ذات الوقت لم تضف إليها أي بيان جديد، وهذا يعطي للنتائج المقدمة عن طريق تلك الآلة مصداقية في التدليل على الواقع.[1]

ب. الاعتماد على الأدوات التي أثبتت البحوث العلمية كفاءتها في تقديم نتائج أفضل:

وفي إطار مشروعية الأدلة الإلكترونية، نجد أن قانون الإجراءات الجنائية الفرنسي رغم أنه لم يتضمن أي نصوص تتعلق بمبدأ الأمانة أو النزاهة في البحث عن الحقيقة، إلا أن الفقه والقضاء كانا بجانب هذا المبدأ سواء في مجال التنقيب عن الجرائم التقليدية، أم في مجال التنقيب في جرائم الحاسوب والإنترنت، كان يستخدم أعضاء الضابطة العدلية طرقا معلوماتية في أعمال التنصت على المحادثات الهاتفية.

يشير رأي قضائي فرنسي إلى أن الأجهزة القضائية قد قبلت استخدام الأساليب العلمية الحديثة لإجراء البحث والاستكشاف عن الجرائم على أساس أن أدلة الطب الشرعي، بما في ذلك الأدلة التي تم الحصول عليها من أجهزة الكمبيوتر والإنترنت، يتم الحصول عليها بطريقة قانونية وعادلة. وكذلك في سويسرا وبلجيكا. وفي المملكة المتحدة، حصلت الشرطة على موافقة إحدى المشتكين لتركيب جهاز مراقبة على خط هاتفها. واستدعى صاحب الشكوى الشرطة عدة مرات للاشتباه في ارتكاب جريمة. تم تسجيل هذه المكالمات الهاتفية، بما في ذلك موضوع اتهام المدعى عليه بالذنب، لكن القاضي استبعد هذه التسجيلات على أساس أنها تمت أثناء المصيدة المفخخة. وفي هولندا، إذا كانت بيانات الكمبيوتر المسجلة في ملف الشرطة غير قانونية، هذا من شأنه أن يؤدي إلى الاستنتاج والاستنتاج هو أنه يجب حذف البيانات ولا يمكن استخدامها كدليل جنائي كمبدأ استبعاد الأدلة غير القانونية. [2]

أما في اليابان فقد أصدرت محكمة مقاطعة (KOFV) حكما أقرت فيه مشروعية التنصت للبحث عن الدليل، حيث ضرورة التحريات، وإمكانية استخدام الإجراءات في التحريات تكون مأخوذة بعين الاعتبار، لكن الفقه الياباني، يرى أن الأدلة الجنائية التي يتم الحصول عليها بطرق مشروعة يجب أن تكون مستبعدة سواء كانت تقليدية أم أدلة حاسوب أم أدلة إنترنت.

(1) الحلبي، خالد عياد، مرجع سابق، ص 251.

(2) مدين، محمود (2020)، مرجع سابق، ص 472.

20-3.indd 241 9/24/2023 2:33:06 AM

وبالنسبة للمشرع الإماراتي فقد نصت المادة 17 مكرر من قانون الإثبات في المعاملات المدنية والتجارية على انه "يعتبر توقيعاً الكترونياً كل أحرف، أو أرقام، أو رموز، أو إشارات، أو صور، أو أصوات لها طابع منفرد تسمح بتحديد شخص صاحب التوقيع وتمييزه عن غيره على النحو الوارد في قانون المعاملات والتجارة الإلكترونية." (1)

كما وتضمن نص المادة رقم 4 من القانون الاتحادي رقم (1) لسنه 2006 بشأن المعاملات والتجارة الإلكترونية تأكيدا على الأثر القانوني للرسالة الإلكترونية وحجتها حيث جاء فيها: (2)

1. لا تفقد الرسالة الإلكترونية أثرها القانوني أو قابليتها للتنفيذ لمجرد أنها جاءت في شكل الكتروني.
2. لا تفقد المعلومات المثبتة في الرسالة الإلكترونية حجتها القانونية حتى وأن وردت موجزة متى كان الاطلاع على تفاصيل تلك المعلومات متاحا ضمن النظام الإلكتروني الخاص بمنشئها، وتمت الإشارة في الرسالة إلى كيفية الاطلاع عليها.

إذا استوفى الدليل الإلكتروني الشروط السابقة فيما يتعلق بمقاومته للتلاعب وسلامة الأخطاء، فلا يمكن رفضه بناءً على تقدير القاضي. من الضروري التنفيذ إلى الحد الذي يتم فيه التشكيك في الأدلة. وهذا شيء لا يمكن للقاضي تحديده. طالما أن الأدلة تفي بشروط السلامة، فإن دور القاضي يقتصر على مراجعة مدى ملاءمة الدليل. وتشكل أساس معتقدات القاضي دورًا مهمًا. (3)

ووفقا للمادة العاشرة من القانون الاتحادي رقم (1) لسنه 2006 بشأن المعاملات والتجارة الإلكترونية تكون الرسالة الإلكترونية أو التوقيع الإلكتروني مقبولا كدليل في الإثبات وإن لم تكن تلك الرسالة أو ذلك التوقيع أصليا في شكله الأصلي طالما كانت الرسالة أو التوقيع الإلكتروني أفضل دليل يتوقع بدرجه مقبولة أن يحصل عليه الشخص الذي يستشهد به، وما لم يثبت العكس يفترض أن السجل الإلكتروني الصحيح لم يتغير منذ أن أنشئ.

وتنص المادة العاشرة من القانون نفسه والتي تتعلق بقبول وحجيه البينة الإلكترونية

(1) انظر نص المادة رقم 17 مكرر من قانون الإثبات في المعاملات المدنية والتجارية رقم (10) لسنة 1992 والمعدل بموجب القانون رقم (36) لسنة 2006م.

(2) انظر نص المادة رقم (4) من القانون الاتحادي رقم (1) لسنة 2006 بشأن بشأن المعاملات والتجارة الإلكترونية

(3) محمد، هلال عبد الله (2008)، حجية مخرجات الكمبيوتر في المواد الجنائية، الطبعة الثانية، دار النهضة العربية، ص95.

20-3.indd 242 9/24/2023 2:33:06 AM

علـى أن:

1. **لا يحول دون قبول الرسالة الإلكترونية أو التوقيع الإلكتروني كدليل إثبات:**

- أن تكون الرسالة أو التوقيع قد جاء في شكل إلكتروني.
- أن تكـون الرسـالة أو التوقيـع ليـس أصليـا أو فـي شـكله الأصلـي، متـى كانـت هـذه الرسـالة أو التوقيـع الإلكترونـي أفضـل دليـل يتوقـع بدرجـه معقولـه أن يحصـل عليـه الشـخص الـذي يستشـهد بـه.

2. **في تقدير حجيه المعلومات الإلكترونية في الإثبات، تراعى العناصر الآتية:**

- مـدى إمكانيـه الاعتـداد بالطريقـة التـي تـم بهـا تنفيـذ واحـده أو أكثـر مـن عمليـات إدخـال المعلومـات، أو إنشـائها، أو تجهيزهـا، أو تخزينهـا، أو تقديمهـا، أو أرسـالها.
- مدى إمكانيه الاعتداد بالطريقة التي استخدمت في المحافظة على سلامه المعلومات.
- مدى إمكانيه الاعتداد بمصدر المعلومات إذا كان معروفاً.
- أي عنصر أخر يتصل بالموضوع.

3. **مالم يتم إثبات عكس ذلك، يفترض أن التوقيع الإلكتروني المحمي:**

- يمكن الاعتداد به.
- هو توقيع الشخص الذي تكون له صله به.
- قـد وضعـه ذلـك الشـخص بنيـه توقيـع أو اعتمـاد الرسـالة الإلكترونيـة المنسـوب إلـه إصداراهـا.
- لم يتغير منذ أن أنشئ. [1]

وبذلـك نجـد أن المشـرع الإماراتـي اتخـذ منحـى يتوافـق مـع التطـورات المعلوماتيـة التـي أصبحـت اليـوم تشـكل واقعنـا المعـاش حيـث اعطـى الحمايـة القانونيـة للمراسـلات الإلكترونيـة وحـدد الضوابـط التـي تحكمهـا مـن خـلال تنظيـم التشـريعات المشـار إليهـا أعـلاه. [2]

(1) انظر نص المادة (10) من القانون الاتحادي رقم (1) لسنه 2006 بشأن المعاملات والتجارة الإلكترونية.

(2) محامي جرائم الكترونية (2020)، مقال بعنوان مدى حجية المراسلات الإلكترونية في الإثبات وفق التشريع الإماراتي، منشور بالموقع الإلكتروني https://cutt.us/EWI0lK، تاريخ أخر زيارة 20/7/2021م.

20-3.indd 243 9/24/2023 2:33:06 AM

الخاتمة:

بعد استعراضنا بالبحث والدراسة لموضوع إجراءات التعامل مع مسرح الجريمة الإلكترونية في التشريع الإماراتي أصبح لدينا فهم واضح لدرجة التغيير التي تؤثر في مجال العلوم الجنائية ومدي تأثرها بالتطور التكنولوجي، وخاصة تطبيق التكنولوجيا الإلكترونية. لقد جربنا كل ما راجعناه لإعطاء الشخصية أكبر عدد ممكن من الميزات الفنية والتقنية البحث القانوني بالاعتماد على مزيج من المصطلحات القانونية والعلمية وكل هذا لتسليط الضوء على تقدم البحث وخاصة في أعمال البحث والتحقيق في مجال التقاضي الجنائي لفترة طويلة لها خصائص المادية التقليدية، لكن الجريمة تتأثر بتطور نمط الحياة في العصر. وتسارع تكنولوجيا المعلومات في تطوير المفاهيم والإجراءات القانونية الحديثة بهدف تطويرها والبحث والتحقيق في مجال الجريمة الإلكترونية، بغرض ملاحقة الجناة والمجرمين للتأكد من أن استخدام تكنولوجيا المعلومات لن يكون خارج نطاق السيطرة وكان هدفها الرئيسي هو خدمة المصالح المعرفية للمجتمع والشعب. وقد توصل الباحث إلى مجموعة من النتائج والتوصيات التي تتمثل في:

أولاً- نتائج البحث:

1. اتضح لنا في نطاق مفهوم الجرائم الإلكترونية أن التعريفات التي أوردها الفقه قد امتازت بالتعدد والاختلاف ضيقاً واتساعا تبعاً للمعايير والمنطلقات المستندة إليها، فمنها ما اعتمد أصحابها على معيار الوسيلة المستخدمة في ارتكاب الجريمة، وآخرون اعتمدوا معيار موضوع الجريمة ذاتها، ومنهم من اعتمد معايير مختلطة جمعت بين المعيارين السابقين.

2. إن عالم تقنية المعلومات عالم لا حدود له وفي تطور متسارع بشكل مذهل، ففي كل يوم يرفدنا بابتكارات جديدة.

3. إن للجرائم الإلكترونية طبيعة خاصة، إذ تمتاز بقدرتها على التحرك في مجال فضائي واسع لا توقفه حدود الدول وسيادتها الإقليمية، حيث يُمكن لجريمة تقنية المعلومات أن تقع في مكان وتُنتج آثارها في مكان أو أماكن أخرى خارج الدول.

4. إن الوسائل الفنية التي قد تستخدم لتدمير مكونات الحاسوب كثيرة ومعقدة في الوقت الحاضر، ولا يُمكن التنبؤ بالوسائل التي قد تستحدثها التكنولوجيا في هذا الشأن.

5. صعوبة إثبات جرائم تقنية المعلومات؛ بسبب صعوبة الاحتفاظ الفني بآثارها إن وجدت، والحرفية الفنية العالية التي تتطلبها من أجل الكشف عنها، وهذا ما يعرقل عمل رجال التحقيق الذين تعودوا على التعامل مع الجرائم التقليدية.

20-3.indd 244 9/24/2023 2:33:07 AM

6. اتضح لنا من خلال هذا البحث أهمية مسرح الجريمة الإلكترونية وأنها تختلف عن مسرح الجريمة التقليدية من حيث صعوبة الحصول على الأدلة وكذلك صعوبة إثبات حجية الأدلة المستخرجة منها أمام القضاء.

7. توصلنا أن المشرع الإماراتي اتخذ منحى يتوافق مع التطورات المعلوماتية التي أصبحت اليوم تشكل واقعنا المعاش حيث أعطى الحماية القانونية للمراسلات الإلكترونية وحدد الضوابط التي تحكمها.

ثانياً- التوصيات:

1. ضرورة تأهيل المختصين بالتصدي للجريمة الإلكترونية بالتقنية الحديثة للتعامل مع مسرح الجريمة الإلكتروني، وتدريبهم على فهم مضامين البلاغات المرتبطة في جرائم تقنية المعلومات واستيعاب معطيات مسرح الجريمة، والتعامل مع الأدلة المتحصلة من الوسائل الإلكترونية.

2. ضرورة توفير التقنيات الحديثة وما يستجد منها للتعامل مع مسرح الجريمة الإلكترونية.

3. عقد الدورات التدريبية لمن لهم اهتمام رسمي واختصاص بالجريمة الإلكترونية للتعريف بتقنياتها وكيفية التعامل معها.

4. ضرورة صدور قانون ينظم إجراءات الضبط والتفتيش للكيانات المعنوية للحاسب الآلي، ونظم تقنية المعلومات، يأخذ في الاعتبار خصائص جرائم تقنية المعلومات من حيث سرعة إخفاء الدليل وتدميره وعدم ترك آثار مادية.

5. ضرورة النص في قانون الإجراءات الجزائية الاتحادي بدولة الإمارات قواعد لتنظيم إجراءات الضبط في جرائم تقنية المعلومات، ويعطي مأموري الضبط القضائي سلطة استخدام كافة الوسائل الممكنة للضبط المشروع عن طريق الشبكة الإلكترونية.

6. ضرورة تزويد مختبرات الجريمة الإلكترونية بالبرامج والأجهزة التقنية الحديثة التي تكشف عن الجرائم الالكترونية.

7. إعطاء اختصاص البحث والتحري والمعاينة في العالم الافتراضي إلى سلطة مختصة في جرائم تقنية المعلومات.

20-3.indd 245 9/24/2023 2:33:07 AM

قائمة المصادر والمراجع:

أولاً: المراجع العربية:

إبراهيم، خالد ممدوح (2009). الجرائم المعلوماتية. دار الفكر الجامعي.

أحمد، سعيد (2005). الجرائم الإلكترونية وآليات الحصول على الدليل فيها. النشر الذهبي.

باطلي، غنية (2015). الجريمة الإلكترونية، دراسة مقارنة. الدار الجزائرية لنشر والتوزيع. ص 22،23.

البقمي، ناصر بن محمد (2008). مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربية، سلسلة محاضرات الإمارات تصدر عن مركز الإمارات للدراسات والبحوث الاستراتيجية، (116)، ص10.

جفال، يوسف (2017). التحقيق في الجرائم الإلكترونية [مذكرة الماجيستير، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف].

جمال، براهيمي (2018). التحقيق الجنائي في الجرائم الإلكترونية [رسالة دكتوراة، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو].

الجنيبهي، ممدوح محمد (2006). جرائم الأنترنت والحاسب الآلي ووسائل مكافحتها. دار الفكر الجامعي. ص71.

الحلبي، خالد عياد (2011). إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت. دار الثقافة للنشر والتوزيع.

الحماد، حسن حماد حميد (2013). الإتلاف المعلوماتي. بحث منشور في كتاب (نحو معالجات لبعض المستجدات في القانون الجنائي (مجموعة أبحاث معمقة). منشورات الحلبي الحقوقية. ص135.

الخن، محمد طارق (2012). الجريمة المعلوماتية.

الديربي، عبد العال (2013). الجريمة المعلوماتية – تعريفها – أسبابها وخصائصها. منشور على الموقع التالي http://accronline.com/article_detail.aspx?id=7509، تاريخ أخر زيارة 18/7/2021م.

رحيمة، نمديلي (2017). خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة. كتاب أعمال مؤتمر الجرائم الإلكترونية. طرابلس، لبنان، ص95.

رستم، هشام محمد فريد (2004، ماي). الجرائم المعلوماتية. مؤتمر القانون والكمبيوتر والإنترنيت 2000، جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، المجلد الثاني، الطبعة الثالثة، ص 407.

رشيد، بن فريحة (2017). التحري الجنائي في مسرح الجريمة الإلكترونية. مجلة جامعة القدس المفتوحة للأبحاث والدراسات، *1*(42)، ص53.

السرحاني، محمد بن نصير محمد (2004). مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت [رسالة الماجيستر، جامعة نايف العربية للعلوم الأمنية].

سياسة تنظيمية رقم (3). إدارة النفاذ إلى الإنترنت، الهيئة العامة لتنظيم الاتصالات، نسخة الكترونية رقم 1، الإمارات العربية المتحدة، أبو ظبي، 2017.

العجرفي، علي بن حامد (1987). إجراءات جمع الأدلة ودورها في كشف الجريمة (ط3).

عرب، يونس (2002). جرائم الكمبيوتر والإنترنت [ورقة عمل]. مؤتمر الأمن العربي، المركز العربي للبحوث

20-3.indd 246 9/24/2023 2:33:08 AM

والدراسات الجنائية، أبو ظبي، الإمارات العربية المتحدة. 10- 12 فيفري.

العريان، محمد علي (2004). الجرائم المعلوماتية. دار الجامعة الجديدة للنشر. ص 43.

العنزي، سليمان ابن مهجع (2003). وسائل التحقق في جرائم نظم المعلومات [رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية].

عوض، محمد محي الدين (1993). مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات.

فرج، هشام عبد الحميد (2004). معاينة مسرح الجريمة. مطابع اللواء الحديثة.

الفيل، علي عدنان (2012). إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية (دراسة مقارنة). المكتب الجامعي الحديث.

القانون الاتحادي رقم (1) لسنه 2006 بشأن المعاملات والتجارة الإلكترونية.

القانون الاتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

القانون الاتحادي رقم 7 لسنة 2012، المذكور أعلاه، وتم نشر القرار في الجريدة الرسمية لدولة الإمارات العربية المتحدة- العدد 578، ص 625.

القانون الاتحادي رقم (35) رقم 1992م بإصدار قانون الإجراءات الجزائية، الطبعة الثالثة 2017 م، دائرة القضاء بأبو ظبي.

القانون الاتحادي رقم (35) رقم 1992م بإصدار قانون الإجراءات الجزائية، مرجع سابق.

قانون الإثبات في المعاملات المدنية والتجارية رقم (10) لسنة 1992 والمعدل بموجب القانون رقم (36) لسنة 2006م.

قشقوش، هدي حامد (2000). الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت. دار النهضة العربية. ص12.

كحلوش، على (2003). جرائم الحاسوب وأساليب مواجهتها، مجلة الشرطة، المديرية العامة الأمن الوطني، عدد *42*، *22*، ص *22*، نقلا عن يوسف الصغير، الجرائم المرتكبة عبر الإنترنت [رسالة الماجيستر، جامعة مولود معمري].

المادة رقم (4) من القانون الاتحادي رقم (1) لسنة 2006 بشأن بشأن المعاملات والتجارة الإلكترونية

المؤتمر السادس للجمعية المصرية القانون الجنائي 1993، القاهرة، مصر. ص 361.

محامي جرائم الكترونية (2020). مقال بعنوان مدى حجية المراسلات الإلكترونية في الإثبات وفق التشريع الإماراتي، منشور بالموقع الإلكتروني https://cutt.us/EWI0lK، تاريخ أخر زيارة 20/7/2021م.

محمد، هلال عبد الله (2008). حجية مخرجات الكمبيوتر في المواد الجنائية (ط2). دار النهضة العربية.

مدين، محمود (2020). فن التحقيق والإثبات في الجرائم الإلكترونية. كتاب للنشر والتوزيع.

مراد، عبد الفتاح (د.ت.). شرح جرائم الكمبيوتر والإنترنت.

الملط، أحمد خليفة (2005). الجرائم المعلوماتية. دار الفكر الجامعي. ص 102.

ممدوح، خالد (2009). فن التحقيق الجنائي في الجرائم الإلكترونية. دار الفكر الجامعي.

الموقع الرسمي لحكومة دولة الإمارات العربية المتحدة، معلومات وخدمات، العدل والسلامة والقانون،

20-3.indd 247 9/24/2023 2:33:08 AM

إجـراءات التقـاضي، الدعـاوى الجزائيـة، تتبـع الجرائـم وجمـع الأدلـة، مـن خـلال اللينـك https://u.ae/ar-ae/information-and-services/justice-safety-and-the-law/litigation-procedures/criminal-cases-، تاريـخ أخـر زيـارة 20/7/2021م.

نعيـم، سـعداني (2013). آليـات البحـث والتحري عن الجريمة المعلوماتيـة في القانون الجزائـري [مذكرة مقدمة لنيل شـهادة الماجيسـتير، كلية الحقوق والعلوم السياسـية- جامعة الحاج لخضـر- باتنة].

هـلال، محمـد رضـوان (2014). كيفيـة التعامـل التقني والآمن مـع أوعية الجريمـة الرقمية في مـسرح الجريمة لضامن حيدة الدليل المسـتخلص. المجلـة العربية الدولية للمعلوماتيـة، *3*(5). https://doi.org/10.12816/0029001

ثانياً: المراجع الأجنبية:

Brush, K. (2020). *Cybercrime*. through the link https://searchsecurity.techtarget.com/definition/cybercrime, last visit 17/7/2021.

Danchev, D., (2005). *The Complete Windows Trojans*. cited; Available from: http://www.windowsecurity.com/whitepapers/The_Complete_Windows_Trojans_Paper.html. Aug 29, 2005.

Ghossoon, M. W. (2014). A Comparison of Trojan Virus Behavior in Linux and Windows Operating Systems. *World of Computer Science, and Information Technology Journal (WCSIT)*, *1*(3), 56-62. ISSN: 2221-0741

Halder, D., & Jaishankar, K. (2011). *Cybercrime and the Victimization of Women: Laws, Rights, and Regulations*. Hershey. IGI Global. ISBN 978-1-60960-830-9.

Hornetsecurity (2021). *Computer Worm*. Article published through link https://www.hornetsecurity.com/en/knowledge-base/computer-worm/, last visit 18/7/2021.

Ngo-Lam, V. (2019). *Cyber Crime: Types, Examples, and What Your Business Can Do*. through the link https://www.exabeam.com/information-security/cyber-crime/, last visit 18/7/2021.

P2P-Worm.Win32. BlackControl.g, Trojan Programs. [cited; Available from: http://www.securelist.com/en/descriptions/15243378/P2PWorm.Win32.Bla ckControl.g, Aug 20, 2010.

Robert, T. (1992). *Computer crime, in criminal investigation* (5th ed.). edited by Charles Swanson. N. Chamelin, Hill Inc. p450.

Smith, & Matrawy (2009). Computer Worms: Architectures-Evasion-Strategies-and Detection Mechanisms. *Journal of Information Assurance and Security*, *4*, p 69-83

Zhenfang, Z. (2015). Study on Computer Trojan Horse Virus and Its Prevention. *International Journal of Engineering and Applied Sciences (IJEAS)*, *2*(8). ISSN: 2394-3661.

20-3.indd 248 9/24/2023 2:33:09 AM

Romanized Arabic References: **الترجمة الصوتية لمصادر ومراجع اللغة العربية:**

’ibrāhym khālida mamdūḥa 2009). aljarā’ima alma‘lūmātiyyata dāru alfikri aljāmi‘iyyi

a’aḥamdun sa‘īda 2005). aljarā’ima al’ilikturwniyyata wa{liyyāti alḥuṣūli ‘alā al-dalyli fīhā al-nashru al-dhahabiyyu

bāṭiliyyun ghaniyyata 2015). aljarīmata al’ilikturwniyyata dirāsata muqāranatin al-dāru aljazā’iriyyatu linashrin wa-l-tawzī‘i ṣ 2322 ،.

albaqamiyyu nāṣara bn muḥammadu 2008). mukāfaḥata aljarā’imi alma‘lūmātiyyati wataṭbīqātihā fī dū’ali majlisi al-ta‘āwuni lidū’ala alkhalījī al‘arabiyyati silslata muḥāḍarāti al’imārāti taṣduru ‘an markazi al’imārāti lil-dirāsāti wa-l-buḥwthi al-astrātyjya 116) ،ṣ

jaffālun yūsf 2017). al-taḥqīqa fī aljarā’imi al’ilikturwniyyati mudhakkirata al-mājystyr kulliyyata alḥuqwqi wa-l-‘ulūmi al-sīāsiyyati jāmi‘ata muḥammada bwḍyāf

jamālun brāhymy 2018). al-taḥqīqa aljinā’iyya fī aljarā’imi al’ilikturwniyyati risālata duktūrātin kulliyyata alḥuqwqi wa-l-‘ulūmi al-sīāsiyyati jāmi‘ata mawlūda mu‘ammarī tīzī wuzū’a

al-jnybhy mamdūḥa muḥammada 2006). jarā’ima al-’āntrnt wa-l-ḥāsiba al{liyya wawasā’ila mukāfaḥatihā dāru alfikri aljāmi‘iyyi ṣ

alḥalbiyyu khālida ‘ayyādu 2011). ijrā’āti al-taḥarrī wa-l-taḥqīqi fī jarā’imi alḥāswbi wa-l-’intrnt dāru al-thaqāfati lil-nashra wa-l-tawzī‘a

alḥammādu ḥusna ḥammāda ḥamīda 2013). al’itlāafa alma‘lūmātiyya baḥthu manshūru fī kitābi naḥwa mu‘ālajātin liba‘ḍi almustajaddāti fī alqānūni aljinā’iyyi majmū‘ata abḥāthi m‘mqa manshūrāti alḥalbiyyi alḥuqūqiyyati ṣ

ulkhinna muḥammada ṭāriqi 2012). aljarīmata alma‘lūmātiyyata

al-dayrabiyyu ‘abda al‘āli 2013). aljarīmata alma‘lūmātiyyata – ta‘rīfahā – a’asabbābahā wkhṣā’iṣhā manshūrun ‘alā almawqi‘i al-tālī http:// accronline. com / article_detail. aspx? id = 7509 ،tārīkha a’akkhara zīārata 18 / 7 / 2021m.

raḥīmatun nmdyly 2017). khuṣūṣiyyata aljarīmati al’ilikturwniyyati fī alqānūni aljazā’iriyyi wa-l-qawānīni almuqāranati kitābu a’a‘māli mu’utamari aljarā’imi al’ilikturwniyyati ṭarābulusun lubnānun ṣ

rustum hishāma muḥammada farīda 2004 ،miyya aljarā’ima alma‘lūmātiyyata mu’utamaru alqānūni wa-l-kambīūtiri wa-l-’intrnyt 2000 ،jāmi‘ata al’imārāti al‘arabiyyati almuttaḥidati kulliyyata al-sharī’ati wa-l-qānūni almujallada al-thānī al-ṭab‘ata al-thālithata ṣ 407.

rashydun bn faryḥata 2017). al-taḥarrī aljinā’iyya fī masraḥi aljarīmati al’ilikturwniyyati majallatu jāmi‘ati alqudsi almaftūḥati lil-’ābḥātha wa-l-dirāsāti 1(42) ،ṣ

al-sirḥāniyyu muḥammada bn naṣīri muḥammadi 2004). mahārāti al-taḥqīqi aljinā’iyyi alfanniyyi

20-3.indd 249 9/24/2023 2:33:09 AM

fī jarā'imi alḥāswbi wa-l-'intrnt risālata al-mājystr jāmi'ata nāyifi al'arabiyyati lil-'ulūma al'a'amniyyata

sīāsatu tanẓīmiyyatu raqmi 3). idārata al-nafādhi ilā al-'intrnt alhay'iata al'āmmata litanẓīma alittiṣālāti nuskhata al-ktrwnya raqma 1 ،al'imārāti al'arabiyyati almuttaḥidati a'abū ẓaby 2017.

al'ajrafiyyu 'uliya bn ḥāmidu 1987). ijrā'āti jam'i al'a'adillati wadawrihā fī kashfi aljarīmati ṭ

'arabun yūnisa 2002). jarā'ima alkambīūtiri wa-l-'intrnt waraqata 'amali mu'utamara al'a'amni al'arabiyyi almarkaza al'arabiyya lil-buḥwtha wa-l-dirāsāti aljinā'iyyati a'abū ẓaby al'imārāti al'arabiyyati almuttaḥidati 10- 12 fayafrī

al'uryāni muḥammada 'allī 2004). aljarā'ima alma'lūmātiyyata dāru aljāmi'ati aljadīdati lil-nashra ṣ 43.

al'anaziyyu salīmāni ibna mahja'i 2003). wasā'ila al-taḥaqquqi fī jarā'imi naẓmi alma'lūmāti risālata mājistīrin jāmi'ata nāyifi al'arabiyyati lil-'ulūma al'a'amniyyata

'iwaḍa muḥammada muḥḥī al-dayyini 1993). mushakkalāti al-sīāsati aljinā'iyyati almu'āṣirati fī jarā'imi naẓmi alma'lūmāti

farajun hishāma 'abdi alḥamīdi 2004). mu'āyanata masraḥi aljarīmati maṭābi'u al-liwā'i alḥadythati

alfīlu 'uliya 'adanāni 2012). ijrā'āti al-taḥarrī wajam'i al'a'adillati wa-l-taḥqīqi alibtidā'iyyi fī aljarīmati alma'lūmātiyyati dirāsata muqāranati almaktaba aljāmi'iyya alḥadytha

alqānūnu alittiḥādiyyu raqma 1) lisinnahu 2006 bisha'ani almu'āmalāti wa-l-tijārati al'ilikturwniyyati

alqānūnu alittiḥādiyyu raqma 5) lisanata 2012 fī sha'ani mukāfaḥati jarā'imi tiqniyyati alma'lūmāti

alqānūnu alittiḥādiyyu raqma 7 lasinatin 2012 ،almadhkūra a'lāahu watamma nashru alqarāri fī aljarīdati al-rasmiyyati lidawlata al'imārāti al'arabiyyati almuttaḥida#i- al'adada 578 ،ṣ 625.

alqānūnu alittiḥādiyyu raqma 35) raqma 1992m bi'iṣdāri qānūni al'ijrā'āti aljazā'iyyati al-ṭab'ata al-thālithata 2017 m dā'irata alqaḍā'i bi'a'abawin ẓaby

alqānūnu alittiḥādiyyu raqma 35) raqma 1992m bi'iṣdāri qānūni al'ijrā'āti aljazā'iyyati marji'a sābiqa

qānūnu al'ithbāti fī almu'āmalāti almadaniyyati wa-l-tijāriyyati raqma 10) lisanata 1992 wa-l-mu'addala bimūjibi alqānūni raqma 36) lisanata 2006m.

qshqwsh hady ḥāmida 2000). alḥimāyata aljinā'iyyata lil-tijārata al'ilikturwniyyata 'abiru al-'intrnt dāru al-nahḍati al'arabiyyati ṣ

kḥlwsh 'alā 2003). jarā'ima alḥāswbi wa'a'asālībi mūājahatihā majallata al-shurṭati almudīriyyata al'āmmata al'a'amina alwaṭaniyya 'adada 42 ،22 ،ṣ 22 ،naqalā 'an yūsf al-ṣaghīra aljarā'ima almurtakibata 'abiru al-'intrnt risālata al-mājystr jāmi'ata mawlūda mu'ammarī

20-3.indd 250 9/24/2023 2:33:10 AM

almāddatu raqma 4) mina alqānūni alittiḥādiyyi raqma 1) lisanata 2006 bisha'anin bisha'ani almu'āmalāti wa-l-tijārati al'ilikturwniyyati

almu'utamaru al-sādsu lil-jam'iyyata almiṣriyyata alqānūna aljinā'iyya 1993 ،alqāhirata miṣrun ṣ 361.

maḥāmmiyyu jarā'imi al-ktrwnya 2020). maqālun bi'unwāni mudā ḥujjiyyati almurāsilāti al'ilikturwniyyati fī al'ithbāti wafuqi al-tashrī'a al-'imārāty manshūrun bi-l-mawqi'i al'ilikturwniyyi https:// cutt. us / EWI0lK ،tārīkha a'akkhara zīārata 20 / 7 / 2021m.

muḥammadun halāala 'abdi Allāhi 2008). ḥujjiyyata makhrajāti alkambīūtiri fī almawāddi aljinā'iyyati ṭ dāra al-nahḍati al'arabiyyati

madīnun maḥmūda 2020). fanna al-taḥqīqi wa-l-'ithbāti fī aljarā'imi al'ilikturwniyyati kitābun lil-nashra wa-l-tawzī'a

murādun 'abda alfattāḥi d t). sharaḥa jarā'imu alkambīūtiri wa-l-'intrnt

almuluṭu a'aḥamida khalīfatu 2005). aljarā'ima alma'lūmātiyyata dāru alfikri aljāmi'iyyi ṣ 102.

mamdūḥun khālida 2009). fanna al-taḥqīqi aljinā'iyyi fī aljarā'imi al'ilikturwniyyati dāru alfikri aljāmi'iyyi

almawqi'u al-rasmiyyu liḥukūmata dawlati al'imārāti al'arabiyyati almuttaḥidati ma'lūmātin wakhidmātin al'adla wa-l-salāamata wa-l-qānūna ijrā'āti al-taqāḍī al-da'āwā aljazā'iyyata tatba'u aljarā'imu wajam'u al'a'adillati min khilāla al-lynk https:// u. ae / ar- ae / information- and- services / justice- safety- and- the- law / litigation- procedures / criminal-cases- ،tārīkha a'akkhara zīārata 20 / 7 / 2021m.

na'īmun sa'dāniyya 2013). āliyyāti albaḥthi wa-l-taḥarrī 'ani aljarīmati alma'lūmātiyyati fī alqānūni aljazā'iriyyi mudhakkirata muqaddimatin linabla shahādati al-mājystyr kulliyyata alḥuqwqi wa-l-'ulūmi al-sīāsiyya#i- jāmi'ata alḥājji likhaḍira bātna

halāalun muḥammada riḍwāni 2014). kayfiyyata al-ta'āmuli al-tiqniyyi wa-l-{mini ma'a a'aw'iyati aljarīmati al-raqmiyyati fī masraḥi aljarīmati liḍāmina ḥaydati al-dalyli almustakhlaṣi almajallatu al'arabiyyatu al-dawliyyatu lil-ma'lūmātiyyata 3(5). https:// doi. org / 10. 12816 / 0029001

20-3.indd 251 9/24/2023 2:33:10 AM

Procedures for dealing with the cybercrime scene in the UAE legislation: An analytical study

Saud Abdelqader Al-Shaer[1]

Abstract:

This research aims to study and analyze the procedures followed when dealing with the scene of cybercrime and the way this type of crimes must be handled. The process is carried out through the scene of the concerned crime, taking into consideration the controls that must be observed during inspection as well as the crime's physical effects, the way it is documented and the modern technical methods used to pick up traces. These methods include the advanced systems of photography and electronic drawing of the crime scene, the digital measurement of the dimensions of the scene, and the tools necessary to preserve the digital evidence that can be extracted from it, based on the UAE laws and legislations. The researcher has used the descriptive analytical approach to describe and analyze the procedures used in such crimes. He concluded that the Emirati legislator adopted an approach that is compatible with informational developments that have become part of everyday life reality. It gave legal protection to electronic evidence and specified the controls that govern it.

Keywords: electronic crime, electronic crime scene, electronic evidence, UAE legislation.

(1) College of Law - Ajman University (Ajman - U.A.E.)
201720185@ajmanuni.ac.ae

20-3.indd 252 9/24/2023 2:33:10 AM