خصائص وأنواع الدليل الإلكتروني
في الكويت ودول المقارنة

الباحث/ بندر عقاب جفين كميخ حطاب الدويش

باحث لدرجة الدكتوراه

كلية الحقوق- جامعة عين شمس

(ISSN: 2537- 0758)

خصائص وأنواع الدليل الإلكتروني في الكويت ودول المقارنة

الباحث/ بندر عقاب جفين كميخ حطاب الدويش

ملخص عربي

أن تسارع إيقاع التقدم التكنولوجي والتقني الهائل، وظهور الفضاء الإلكتروني ووسائل الاتصالات الحديثة كالفاكس والإنترنيت وسائر صور الاتصال الإلكتروني عبر الأقمار الصناعية كانوا وسيلة استغلها 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.

ومن حيث ما يرتبط بهشاشة نظام الملاحقة الإجرائية التي تبدو قاصرة على استيعاب هذه الظاهرة الإجرامية الجديدة، سواء على صعيد الملاحقة الجنائية في إطار القوانين الوطنية أم على صعيد الملاحقة الجنائية الدولية، مما أوجب تطوير البنية التشريعية الجنائية الوطنية بذكاء تشريعي مماثل تعكس فيه الدقة الواجبة علي المستوى القانوني وسائر جوانب وأبعاد تلك التقنيات الجديدة، بما يضمن في الأحوال كافة احترام مبدأ شرعية الجرائم والعقوبات من ناحية، ومبدأ الشرعية الإجرائية من ناحية أخرى، وتتكامل فيه في الدور والهدف مع المعاهدات الدولية.

ويعد الإثبات الجنائي بالأدلة الرقمية من أبرز تطورات العصر الحديث، والتي جاءت لتلائم الثورة العلمية والتكنولوجية والتقنية في عصرنا الحالي، والتي تطور معها الفكر الإجرامي الذي صاحب ظهور ما يعرف بالجريمة الإلكترونية ألقى على عاتق القائمين على مكافحة الجريمة في الدولة عبئا شديدا ومهاما جسيمة تفوق القدرات المتاحة لهم و فق أسس وقواعد وإجراءات البحث الجنائي والإثبات الجنائي التقليدي، نظرا لعدم كفاية وعدم ملائمة هذه النظم التقليدية في إثبات تلك الجرائم سواء من الناحيتين القانونية أو التقنية، الشيء الذي ألزم على المشرع أن يتدخل بقوانين تتناسب مع مثل هذه الجرائم.

فكانت هذه التطورات التي عرفتها المعلوميات كفيلة لتجعل الإثبات الجنائي يتأثر من جراء الجرائم التي أفرزتها هذه الثورة المعلوماتية، الأمر الذي جعل من طبيعة الإثبات بالوسائل التقليدية أمر متجاوز.

ولعل هذه الطبيعة غير المرئية للأدلة المتحصلة من الوسائل الإلكترونية تلقى بظلالها على الجهات التي تتعامل مع الجرائم التي تقع بالوسائل الإلكترونية حيث تصعب قدرتهم على فحص واختبار البيانات محل الاشتباه خاصة في حالات التلاعب في برامج الحاسوب، ومن ثم فقد يستحيل عليهم الوصول إلى الجناة .فمن المعلوم أن جهات التحري والتحقيق اعتادت على الاعتماد في جمع الدليل على الوسائل التقليدية للإثبات الجنائي التي تعتمد على الإثبات المادي للجريمة ولكن في محيط الإلكترونيات فالأمر مختلف، فالمتحري أو المحقق لا يستطيع أي منهما تطبيق إجراءات الإثبات التقليدية على المعلومات المعنوية.

summary

The tremendous technological and technical development, cyberspace science and modern means of communication using satellites and electronic transmitters, in carrying out its crimes, which are commercial projects, are considered commercial projects, one country, crimes that have exceeded, and they are commercial and innovative projects that represent a kind of criminal intelligence, use it within the traditional descriptions in national and foreign laws.

And in terms of what is related to the fragility of the procedural prosecution system, which seems limited to absorbing this new criminal phenomenon, whether at the level of criminal prosecution within the framework of national laws or at the level of international criminal prosecution, which necessitated the development of the national criminal legislative structure with similar legislative intelligence that reflects the due accuracy at the level In all cases, the principle of legality of crimes and penalties on the one hand, and the principle of procedural legality on the other hand, is respected in all cases, and is complementary in role and purpose with international treaties.

Criminal evidence with digital evidence is one of the most prominent developments of the modern era, which came to suit the scientific, technological and technical revolution of our time, and with which the criminal thought that accompanied the emergence of what is known as cybercrime has developed, has placed a heavy burden on those in charge of combating crime in the country.

(ISSN: 2537- 0758)

Heavy tasks that exceed the capabilities available to them according to the foundations, rules and procedures of criminal investigation and traditional criminal evidence, due to the inadequacy and inadequacy of these traditional systems in proving these crimes, whether from a legal or technical point of view, which obligated the legislator to intervene with laws commensurate with such crimes.

These developments in informatics were sufficient to make criminal evidence affected by the crimes produced by this information revolution, which made the nature of proof by traditional means transcendental.

Perhaps this invisible nature of the evidence obtained from electronic means casts a shadow on the parties that deal with crimes that occur by electronic means, as it is difficult for them to be able to examine and test the suspected data, especially in cases of tampering with computer programs, and therefore it may be impossible for them to reach the perpetrators. It is well known that investigation and investigation authorities used to rely on traditional means of criminal proof that rely on physical evidence of the crime, but in the vicinity of electronics, the matter is different. Neither of them can apply traditional evidentiary procedures to intangible information.

المقدمة

من المقرر قانوناً أن طلبات الخصوم ودفوعهم في الدعوى لابد لها من الإثبات، وهذا الإثبات يتم من خلال تقديم الدليل المؤيد للحق المدعى به، وينقسم هذا الدليل بدوره إلى نوعين دليل تقليدي، وآخر إلكتروني، ويتسم الدليل الإلكتروني بعدة مزايا تميزه عن الدليل التقليدي، منها تعدد أنواعه وصوره، حيث لا يأتِ الدليل الإلكتروني في صورة واحدة، كما أن له تقسيمات متعددة قدمها الفقه ومؤسسات قانونية مثل وزارة العدل الأميركية، إضافة إلى أن الدليل الإلكتروني يتمتع بجملة من الخصائص التي تميزه عن غيره من الأدلة الأخرى.

وعلى ذلك، فإننا سوف نقوم بتقسيم الدراسة في هذا المبحث إلى مطلبين، نتناول في المطلب الأول بيان أهم الخصائص التي يتميز بها الدليل الإلكتروني، وفي المطلب الثاني نعرض لمعوقات الحصول على الدليل الإلكتروني، وذلك علي النحو التالي بيانه:

المطلب الأول: خصائص الدليل الإلكتروني.
المطلب الثاني: معوقات الحصول على الدليل الإلكتروني.

المطلب الأول
خصائص الدليل الإلكتروني

إن الدليل في العالم المادي عبارة عن جملة من الآثار التي يخلفها المجرم وراءه، ويتم استخلاصها وتحويلها لوسائل إثبات، وهذا بعكس الدليل الرقمي الذي ينشأ أساسا في بيئة رقمية، وتلك البيئة تضفي خصائصها على الدليل، حيث تنتفي في الدليل الإلكتروني صفة المادية، إلى جانب تمتع هذا الدليل الإلكتروني بعدة خصائص تميزه عن غيره من الأدلة المادية الأخرى ومن ثم تجعله ذو طبيعة خاصة بالمقارنة بالدليل التقليدي ويرجع السبب في ذلك إلى كونه جزءاً من البيئة الرقمية بجميع مكوناتها من برمجيات وقطع صلبه وغيرها، وله طبيعة تقنية، ويصنف ضمن الأدلة العلمية، إضافة إلى أنه سريع التطور والتنوع، ويصعب التخلص منه، ومن بين هذه الخصائص تفصيلاً ما يلي[١]:

أولاً: الدليل الإلكتروني دليل عالي التقنية:

تلك الطبيعة تقتضي وجود التوافق بين الدليل والبيئة التي ينشأ فيها، فلا يمكن للتقنية إنتاج دليل مادي مثل بصمة الإصبع أو الشهادة، ولكن ما تنتجه الأجهزة الإلكترونية نبضات رقمية لا يمكن أن تتواجد خارج البيئة التقنية أي العالم الافتراضي مثل شبكات الإنترنت والأقراص الصلبة والمرنة والخوادم وغيرها، وتعد التقنية هي الوعاء الذي يتكون في داخله الدليل الإلكتروني ويقصد بها استخدام الأدوات والآلات والمواد والأساليب ومصادر الطاقة لكي تجعل العمل ميسوراً وأكثر إنتاجيه، وتعتمد الاتصالات الحديثة ومعالجه البيانات علي هذه التقنية خاصة تقنيه الإلكترونيات الرقمية وشبكاتها، والتقنية جزء من العلم وليست بعيدة عنه، وبدون التقنية يصبح العلم مجرد نظريات غير ذات جدوى[٢].

والتقنية الرقمية عالم لا ينتهي من الأرقام التي تتحول في النهاية إلي الأشكال المختلفة من البيانات، وهذه البيانات هي نتاج النشاط الإنساني في هذا الشكل الجديد من التقنيات،

---

[١] د. حاتم أحمد محمد بطيخ– دور الإنترنت في الإثبات، مرجع سابق، ص٣٩٦ وما بعدها.

[٢] د. مصطفى محمد موسى– التحقيق الجنائي في الجرائم الإلكترونية، مطبعه الشرطة، الطبعة الأولى، القاهرة، ٢٠٠٩، ص٢٧.

(ISSN: 2537- 0758)

والذي يتميز بعدم وجود قواعد ثابتة فهو إفراز لأفكار وثقافات لا حصر لها[٣].

ونتج عن سهولة استعمال تقنيه الحاسب الآلي والإنترنت تطويرها وتزويد مستخدميها بالمعلومات والبيانات بسهولة ويسر، فيتميز الدليل الإلكتروني عن باقي أنواع الدليل الجنائي بأنه دليل عالي التقنية نظراً لارتباطه الوثيق بالوسائل الإلكترونية (الحاسب والإنترنت) والأدلة العلمية، ويمتاز بالسعة التخزينية العالمية، فآلة الفيديو الإلكترونية يمكنها تخزين مئات الصور، ودسك صغير يمكنه تخزين مكتبة صغيرة وهكذا[٤].

ولما كان الأمر كذلك، فقد تم استخدام الدليل الرقمي في رصد كافة المعلومات عن الجاني وتحليلها في ذات الوقت، حيث يمكنه تسجيل كافة تحركات الفرد، ويسجل عاداته وسلوكياته وبعض الأمور الشخصية عنه، مما يمكن البحث الجنائي من أن يجد غايته بسهولة أيسر من الدليل المادي. ويرجع ذلك لكون الدليل الرقمي عبارة عن نبضات رقميه تتحول من خلال تقنيات البرمجة إلى الأشكال المختلفة للبيانات التي تمثل النشاط الإنساني الذي تعد الجرائم جزءاً لا يتجزأ منه، فيرتبط الدليل الرقمي ارتباطاً رئيسياً بالبيئة التي خرج منها فينبغي أن يكون جزءاً منها[٥].

ثانياً: الدليل الإلكتروني متطور ومتنوع:

يتميز الدليل الإلكتروني بأنه دليل مرن ومتطور بصوره سريعة على عكس الأدلة المادية التقليدية التي تتميز بالجمود وعدم التطور إلا في صور قليلة منها، بالإضافة إلى أنه دليل متنوع حيث تتشكل كل المعلومات التي يتم إنتاجها في العالم الرقمي من النبضات الإلكترونية، والتي يتم ترجمتها إلى أشكال متنوعة ونصوص وسمعيات ومرئيات والتي تشكل أنواع الدليل الرقمي التي يتم استخلاصها، وتتميز هذه الأنواع بالتنوع في الشكل ولكنها تتحد في المصدر الأساسي لها والنبضات الإلكترونية، وجميع هذه الأشكال يمكن أن تصلح لأن

---

[٣] د. حاتم أحمد محمد بطيخ– دور الإنترنت في الإثبات، مرجع سابق، ص٣٩٧ وما بعدها.

[٤] د. سعيد عبد اللطيف حسن– إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، دار النهضة العربية، القاهرة، (١٩٩٩)، ص١٨.

[٥] د. ممدوح عبد الحميد عبد المطلب– استخدام بروتوكول (TCPIP) في بحث وتحقيق الجرائم على الكمبيوتر، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، مركز البحوث والدراسات، العدد (٤)، المحور الأمني والإداري، المنعقد خلال الفترة ٢٦– ٢٨ إبريل ٢٠٠٣، دبي، الإمارات العربية المتحدة، ٢٠٠٣، ص٦٥٠.

تكون دليلاً للإدانة أو البراءة[٦].

ولقد كان القضاء الأمريكي سباقا في مراعاة هذه الخاصية، حيث جعل سجلات الحاسوب المقبولة استثناءً أمام القضاء إذا كانت معدة في هيئه ملفات وفقا للمادة (٦/٨٠٣) من قواعد الإثبات الفيدرالية، وتعد مقبولة مع التمييز بين عمليه تخزينها وعمليه توالدها[٧].

ثالثاً: الدليل الإلكتروني هو دليل علمي:

الدليل الإلكتروني بصفته دليل معلوماتي يحتاج للبيئة التقنية ليتكون فيها، وعليه فما ينطبق على الأدلة العلمية يطبق على الإلكترونية، إذ يخضع كلاهما لاختبار تجاوبه مع الحقيقة كاملة تطبيقا لقاعدة أن القانون مسعاه العدالة أو العلم فيهدف للحقيقة وعليه فالدليل الإلكتروني يستند للمنطق العلمي ولا يخرج عنه وإلا فقد معناه[٨].

رابعاً: الدليل الإلكتروني يستخلص بأساليب علمية:

يتفق الدليل الإلكتروني مع الدليل العلمي في كل ما يخضع له من قواعد، وهو ما يقتضي ألا يتعارض الدليل الإلكتروني مع القواعد العلمية المستقرة، وقد تفرع عن ذلك قواعد علمية لاستخلاص الدليل الرقمي في الوقائع المجرمة قانونياً، وسميت بعلوم الحاسب الجنائي FORENSIC COMPUTER SCIENCES، ويختص العلم الشرعي للحاسبات بوضع القواعد التي يجب أن يلتزم بها المحققون في حاله القيام بفحص وقائع تمت باستخدام أجهزه التقنيات الرقمية واتصالها بالإنترنت[٩].

فإن فهم مضمون الدليل الإلكتروني يعتمد على استخدام أجهزة خاصة بتجميع وتحليل محتواه، ولذلك فكل ما لا يمكن تحديد وتحليل محتواه بواسطة تلك الأجهزة لا يمكن اعتباره دليلاً إلكترونية وذلك لعدم إمكانية الاستدلال به على معلومة معينة مما يعدم قيمته التدليلية

---

(6) Mark R. Colombell, The legislative response to the evolution of computer verses, 8 RICH, i.1, and TECH 2002.
http//www.low.richmond.edu/ioletv813/article18.htm1.

(7) Eoghan Casy: Digital Evidence Forensics Science Computer and The Internet Computer Crime, OP-CIT, P.9.

(٨) د. ميسون خلف الحمداني، الدليل الرقمي وعلاقته بالمساس بالحق في الخصوصية المعلوماتية أثناء إثبات الجريمة، جامعة النهرين، دولة العراق، ٢٠١٦، ص١٨.

(٩) د. على محمود على حمودة– الأدلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائية، بحث مقدم ضمن أعمال المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، والتي نظمتها شرطة دبي في الفترة ٢٦– ٢٠٠٣/٤/٢٨، دبي، ص٢٢.

(ISSN: 2537- 0758)

في إثبات الجريمة ونسبها إلى الجاني[١٠].

هذا، ولما كانت عملية استخلاص الدليل تمر بثلاثة مراحل هي مرحلة المعاينة، مرحلة التحريز، مرحله المعالجة والتحليل، مرحله تقديم الدليل وعرض النتائج التي تم التوصل إليها في المراحل السابقة وذلك أمام القضاء وبحضور جهات الضبط والادعاء والمتهم ومحاميه. فإنه ينبغي علي الخبير عند تقديم الدليل الإلكتروني للقضاء أن يوضح كيفية استخلاصه وطرق وأساليب معالجته للدليل الرقمي، لكي يتمكن القاضي من الفصل في مدى صلاحية الدليل الرقمي المقدم إليه، وهو ما يتطلب أن يكون القاضي ملماً بالقدر اللازم من المعلومات العلمية والفنية التي تمكنه من تقدير صحة الدليل المستخلص والتأكد من عدم التلاعب به[١١].

خامساً: الدليل الإلكتروني دليل غير ملموس يتميز بالخفاء:

الدليل الإلكتروني ليس دليلاً مادياً ملموساً، فهو- أي الدليل الإلكتروني- تلك المجالات المغناطيسية أو الكهربائية، ومن ثم فإن ترجمة هذا الدليل وإخراجه في شكل مادي ملموس لا يعني أن هذا التجمع يعتبر هو الدليل، بل إن هذه العملية لا تعدو كونها عملية نقل لتلك المجالات من طبيعتها الإلكترونية إلى الهيأة التي يمكن الاستدلال بها على معلومة معينة[١٢].

وبمعنى آخر، إن هذه الأدلة تتميز بكونها أدلة خفية لا يمكن رؤيتها، حيث تتكون من مجموعة نبضات كهربائية ومغناطيسية غير ملموسة، ولا يمكن إدراكها بالحواس الطبيعية للإنسان، أي عدم وجود آثار ماديه يمكن متابعتها، وهي خطيرة وصعبه الاكتشاف من حيث مكان وقوعها أو مكان التعامل معها بسبب اتساع نطاقها وضخامة البيانات، كما هو الشأن في جرائم غسيل الأموال، بينما الأدلة المادية فهي محسوسة مرئية حتى غير الظاهرة منها

---

[١٠] د. محمد الأمين البشري- التحقيق في الجرائم المستحدثة، جامعة نايف العربية للعلوم الأمنية، الرياض، ط١، ٢٠١٤، ص٢٣٧ وما بعدها.

[11] Ralph D. Clifford, Cyber crime The Investigation, prosecution and Defense of a computer crime, Carolina Academic press, USA, 2001, P113. ; Marjie T. and Britz, PHD: Computer Forensics and Cyber crime an introduction, Pearson prentice Hall, USA, 2003, P.137.

[١٢] د. ممدوح عبد المطلب، البحث والتحقيق الجنائي، مرجع سابق، ص ٩٠.

يمكن اكتشافها بواسطة الأجهزة المعدة لذلك بكل سهولة[١٣].

سادساً: الدليل الإلكتروني ذو طبيعة رقمية ثنائية:

فالآثار التي يخلفها مستخدم النظام المعلوماتي والتي تضم أية بيانات مرسلة أو مستلمة وآية اتصالات تمت من خلال شبكة الاتصال بشكلها الرقمي، فالبيانات المتوفرة داخل الحاسب أي كانت صورتها تتحول للصيغة الرقمية ويتم ترجمة أي بيانات على الحاسب لنظام ثنائي في تمثيل الأعداد يستوعبه الحاسب الآلي مكون من رقمين (٠، ١)، وتلك الطبيعة لا تتوفر إلا في الدليل الرقمي فالأدلة التقليدية لها مئات الصور ولا تتبع أصل واحد، لذا قد يسهل التلاعب بها[١٤].

سابعاً: الدليل الإلكتروني يصعب التخلص منه بالحذف أو الطمس:

يتميز الدليل الإلكتروني بصعوبة التخلص منه بالمقارنة بالأدلة التقليدية، فالمعلومات التي يتم تخزينها في وسائط التخزين الثابتة والمتحركة من الصعوبة التخلص منها نهائيا حتى وإن تم محوها أو مسحها من خلال أنظمه التشغيل، فبرامج التشغيل تحتفظ بالمعلومات التي تم حذفها في نظام التشغيل ويمكن استرجاعها بواسطة استخدام بعض البرامج الفنية[١٥]. وليس ذلك فحسب بل يمكن أيضاً استخراج نسخ من الأدلة الإلكترونية المطابقة للأصل وتكون لها ذات القيمة العلمية والحجية الثبوتية الشيء الذي لا يتوافر في أنواع الأدلة الأخرى التقليدية مما يشكل ضمانة شديدة الفعالية للحفاظ على الدليل ضد الفقد، والتلف، والتغيير، عن طريق عمل نسخ طبق الأصل من الدليل[١٦].

فهذا النوع من الأدلة يمكن استرجاعه بعد محوه، وإصلاحه بعد إتلافه، وإظهاره بعد إخفائه، مما يؤكد على صعوبة الخلاص منه، فهناك العديد من البرامج الحاسوبية التي وظيفتها استعادة البيانات التي تم حذفها أو إلغائها سواء تم ذلك بالأمر (Delete) وحتى لو تم عمل إعادة تهيئة أو تشكيل القرص الصلب (Hard Disk) باستخدام الأمر (Format) والبرامج التي تم إتلافها أو إخفائها، سواء كانت صورة أو رسوم أو كتابات أو غيرها، مما

---

[١٣] د. ممدوح عبد الحميد– البحث والتحقيق الجنائي، مرجع سابق، ص٨٩.

[١٤] سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير في العلوم القانونية، جامعة الحاج لخضر، باتنة، الجزائر، ٢٠١٣، ص١٢٦.

[15] Kenneth S. Rosenblatt, High- Technology crime investigating Cases Involving computer, ksk publication San Jose, USA, 2003, P.260.

[١٦] د. عمر محمد بن يونس– الإثبات الجنائي عبر الإنترنت، ط١، القاهرة ٢٠١٠، ص٤٥.

(ISSN: 2537- 0758)

يعني صعوبة إخفاء الجاني لجريمته أو التخفي منها عن أعين الأمن والعدالة، طالما تم علم رجال البحث والتحقيق الجنائي بوقوع الجريمة[١٧]. ومن الأمثل على ذلك ما حدث في قضيه إيران– كونترا التي كانت من أولي القضايا التي أبرزت هذه الخاصية في الدليل الرقمي حيث أدرك أحد المسئولين في الحكومة الأمريكية وهو (مستشار الأمن القومي) عدم وجود اتزان في مقارنة الدليل الورقي بالدليل الرقمي، فالدليل الورقي يمكن التخلص منه بتمزيق الورقة التي تحمله في حين أن الدليل الرقمي يمكن استرجاعه حتى ولو تعرض للإزالة، ففي هذه القضية تمكنت الإدارة من استعادة البيانات من خلال استرجاع نظام الحفظ BACKUP للبريد الإلكتروني، فتبين تورط بعض المسئولين بمكتب الرئيس الأمريكي[١٨].

هذا، وتثير هذه الخاصية مسائل هامة مضمونها، أن كل من يحاول أو يساهم في التخلص من الدليل الرقمي بإخفائه أو مسحه أو طمس معالمه، بهدف إعانة الجاني على الفرار من وجه القضاء أو مجرد تمكينه من ذلك يقع تحت طائلة القانون ويعاقب على فعله، وهو يعد التطبيق الفعلي لما نص عليه المشرع المصري في المواد ١٤٠، ١٤١، ١٤٢، ١٤٣، ١٤٤، ١٤٥، ١٤٦ من قانون العقوبات وتعديلاته، وترتبط تلك المواد بالمادتين ٢٥، ٢٦ من قانون الإجراءات الجنائية رقم ١٥٠ لسنة ١٩٥٠ وتعديلاته، واللتان تفرضان على كل شخص أو موظف عام أو مكلف بخدمة عامة علم بوقوع جريمة أن يبلغ النيابة العامة أو أحد مأموري الضبط القضائي.

ومما سبق، فإنه بالإضافة إلى صعوبة إزالة أو محو الدليل الإلكتروني حتى في حالة إصدار أمر من قبل الجاني بإزالته من جهاز الحاسب الآلي، إلا أنه يمكن للخبير التقني المختص إعادة تظهيره من الحاسب الآلي مرة أخرى حتى وإن تم إزالته فعلاً، بينما الدليل المادي يكون عرضه للتلف والإزالة، إذا ما عبث بمسرح الجريمة أو عن طريق الخطأ في تحريز ورفع الآثار المادية للجريمة.

لذا، فيجب إدانة ومعاقبة كل من يقوم بإعداد برامج وهكرات إلكترونية يهدف من ورائها التخلص من الأدلة أو إزالة بيانات الحاسب الآلي أو برمجيات تستخدم في ارتكاب الجريمة، مع ضرورة التأكد من ذلك عن طريق ندب خبير تقني ليقوم بإثبات أن المتهم أو أحد الأشخاص هو من قام بإعداد مثل هذه البرمجيات بهدف إخفاء الأدلة المتعلقة

[١٧] د. ممدوح عبد الحميد عبد المطلب– استخدام بروتوكول (TCPIP)، مرجع سابق، ص٦٤٩.

[١٨] د. عمر محمد أبو بكر – الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص٩٨٢، ٩٨٣.

بالجريمة أو استخدامها في ارتكابها أو مسح وإزالة البيانات المدونة علي جهاز الحاسوب والمتعلقة بالجريمة.

ثامناً: التعامل مع الدليل الإلكتروني يحتاج إلى خبراء وفنيين متخصصين:

تعد إجراءات التحقيق الجنائي العام هي الأساس في التحقيق في جرائم المعلوماتية، كما هو الحال في الجرائم التقليدية الأخرى[١٩]، غير أنها تتميز ببعض الخصوصية في عناصر التحقيق الفرعية والإجراءات الشكلية المتبعة للعناية بمسرح الجريمة وتأمين الأدلة. ففي الوقت الذي تم تجهيز المعامل الجنائية اللازمة للتعامل مع الأدلة المادية، برزت مشكله التعامل مع الأدلة الرقمية كنتيجة حتمية لانتشار تقنية المعلومات في مجال الجريمة مما يستدعي إنشاء معامل ومختبرات خاصة بالإضافة إلى إعداد خبراء فنيين وقانونيين يجمعون بين معرفة التشريعات والنصوص القانونية ومهارة التحقيق[٢٠].

كما يفترض العمل على تطوير الأساليب الخاصة بالتحقيق في جرائم المعلوماتية لأنها جرائم غير تقليديه، وتتميز بطابعها الفني والتقني الخاص، الأمر الذي يتعين معه ضرورة أن تجابه هذه الفئة من الجرائم المعلوماتية بأساليب بحث وتحري وضبط وتحقيق غير تقليديه، والعمل على تدريب أجهزه سلطات إنفاذ العدالة وتطبيق القانون على أساليب وجمع الأدلة والتحقيق الحديث في جرائم المعلوماتية لضمان سلامة الدليل، بل ويذهب البعض إلى أن يوكل مهمة التحقيق في جرائم المعلوماتية لبيوت الخبرة المتخصصة في هذا المجال، خاصة وقد تكونت شركات عالمية حققت النجاح في كثير من الحالات، إلا أن هذا الرأي لم يلق قبولاً لدى الكثيرون حيث يرون خطورة مثل هذا النوع من الإجراء المتمثل في إبعاد أجهزة العدالة الجنائية وتخليها عن دورها في هذا النوع من الجرائم[٢١].

تاسعا: الدليل الإلكتروني يختلف في طبيعته ومضمونه عن الدليل المادي:

فلا تنتج لنا التقنية اعترافاً مكتوباً، أو مالاً ملموساً مثل ما يحدث في جريمة الرشوة مثلاً،

---

[١٩] د. محمد الأمين البشري– التحقيق الجنائي المتكامل، أكاديمية نايف للعلوم الأمنية، الرياض، ١٩٩٧، ص٥٧.

[20] Rosenblatt. K.S. high-Technology Crime (1999): Investigating Cases Involving Computers, San Jose: C.A: K S K Publications, p.21.

[21] Peter Stephenson: Investigating Computer Related Crimes London, C. R. C, 1999, P.73.

(ISSN: 2537- 0758)

كما لا تترك لنا بصمة أصبع كما هو في حالة جرائم السرقة، إلى غير ذلك من الأدلة المادية، فكل ما تنتجه التقنية الحديثة هو نبضات رقميه تتشكل قيمتها في مدى إمكانية تعاملها مع القطع الصلبة المكونة للحاسب الآلي على أية شاكلة تكون، وهذه النبضات تشكل مجموعة البيانات الرقمية التي تتواجد داخل بيئة الحاسب الآلي وشبكاته وفى ذاكرته، وفى الأقراص الصلبة الموجودة بداخله.

والتعامل مع الأدلة الإلكترونية الموجودة في هذا المسرح يجب أن يتم على يد خبراء متخصصين في مثل هذا النوع من الجرائم الإلكترونية، نظراً لأن مسرح الجريمة الإلكترونية يختلف– بطبيعة الحال– عن مسرح الجرائم التقليدية مثل جريمة القتل أو السرقة أو الاغتصاب، والتي قد تكون في أغلب الأحوال من الجرائم المستمرة– خاصة إذا كانت جريمة اقتصادية– وقد يكون مسرح الجريمة المعلوماتية مثل مسرح الجرائم التقليدية عندما يكون الغاية منها التخريب أو إتلاف البرامج[٢٢].

ويتميز مسرح الجريمة الإلكترونية بالاتساع العالمي، وهذا الاتساع في مسرح الدليل الإلكتروني، يمكن مستغلي الدليل من تبادل المعرفة الرقمية بسرعة عالية، وبمناطق مختلفة من العالم، مما يساهم في الاستدلال على الجناة أو أفعالهم بسرعة أقل نسبية[٢٣].

عاشراً: الدليل الإلكتروني دليل تحليلي:

نظرا لطبيعة الدليل الإلكتروني المتميزة فمن خلاله يمكن رصد معلومات هامة عن الجاني وتحليل خطواته كاملة، إذ يمكن من خلال الدليل استخلاص تحركات الجاني وعاداته وسلوكياته الإلكترونية وبعض من الأمور الشخصية للجاني، لذا ومن خلال التحقيق

---

[٢٢] **راجع في ذلك:** د. مدحت رمضان– جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية، القاهرة، ٢٠٠٠، ص ٦٠–٦٢. **وراجع أيضاً:**

Vocca, John (2002): Computer Forensics: Computer Crime Scenc Investigation, Hingham, Massa chusetts: Charles River Madia. & Wright, timothy (2000): An Introduction to the field Guide for Investigating Computer Crime, Online available: http//www.security focus.com/infocus //245 (5/9/2003).

مشار إليهم لدى: د. عمر عبد المجيد مصبح– الدليل المادي، مرجع سابق، ص ١٤٣.

[٢٣] منير محمد الجنبيهي، ممدوح محمد والجنبيهي– بروتوكولات وقوانين الإنترنت، دار الفكر العربي، ط١، القاهرة ٢٠١٣، ص٤٦.

الجنائي يكون التعامل مع الدليل الإلكتروني أيسر من الدليل المادي التقليدي[٢٤].

المطلب الثاني
معوقات الحصول على الدليل الإلكتروني

لقد ساهمت العديد من العوامل المحيطة بتقنية المعلومات الإلكترونية بشكل عام في إثارة صعوبات وخلق عقبات جديدة أمام سلطات التحقيق في كشف الجريمة الإلكترونية، فهناك العديد من المعوقات أو المشكلات التي تعترض عمل السلطات المختصة بالضبط والتحقيق وجمع الاستدلالات وتعوق عملية الحصول على الدليل، ومن بين هذه المعوقات المشار إليها ما يتعلق بالجريمة وأطرافها، ومنها ما يتعلق بسلطات الضبط والتحقيق والقضاء، ومنها ما يتعلق بالدليل ذاته، ومنها ما يتعلق بالإجراءات الواجب إتباعها والتشريعات القانونية المنظمة لها، **والتي سنتناولها تفصيلاً في هذا الجانب من الدراسة، من خلال تقسيم الدراسة في هذا المطلب إلى أربعة فروع على النحو التالي بيانه:**

الفرع الأول: المعوقات التي تتعلق بالجريمة وأطرافها.

الفرع الثاني: المعوقات التي تتعلق بسلطات الاستدلال والتحقيق.

الفرع الثالث: المعوقات التي تتعلق بالدليل ذاته.

الفرع الرابع: المعوقات التشريعية والإجرائية.

الفرع الأول
المعوقات التي تتعلق بالجريمة وأطرافها

سوف نقوم بتقسيم الدراسة في هذا الفرع إلى ثلاثة أغصان، نتناول في الغصن الأول المعوقات التي تتعلق بالجريمة، وفي الغصن الثاني المعوقات التي تتعلق بالمجرم، وفي الغصن الثالث المعوقات التي تتعلق بالمجني عليه، **وذلك على النحو التالي بيانه:**

الغصن الأول: معوقات تتعلق بالجريمة.

الغصن الثاني: معوقات تتعلق بالمجرم.

الغصن الثالث: معوقات تتعلق بالمجني عليه.

---

[٢٤] أحمد بن عبد الله الرشودي، حجية الوسائل الإلكترونية في الإثبات الجنائي، دراسة تأصيلية مقارنة تطبيقية، رسالة دكتوراه الفلسفة في العلوم الأمنية، جامعة نايف العربية للعلوم الأمنية، الرياض، ٢٠٠٨، ص٢٥٢.

(ISSN: 2537- 0758)

الغصن الأول
معوقات تتعلق بالجريمة

يختلف مسرح الجريمة الرقمي أو البيئة التي تحوي الجرائم الإلكترونية عن مسرح الجريمة التقليدي، حيث لا تعرف الجريمة الرقمية في العالم الافتراضي أية حواجز مادية، الأمر الذي يزيد عملية البحث والتنقيب عن أدلتها تعقيداً أمام سلطات الضبط والتحقيق[٢٥]، ليس ذلك فحسب بل هناك العديد من المعوقات الأخرى التي ترتبط بالجريمة ذاتها منها سهولة خفاء أدلة الجريمة، ومحو أثارها، وغياب الدليل المرئي المقروء، والقدرة على تدمير الأدلة في زمن قصير جداً، قبل أن تتمكن السلطات من كشف الجريمة والتوصل إلى الأدلة المستخدمة فيها، إضافة إلى ضخامة البيانات والمعلومات المتطلب فحصها، وإمكانية خروجها عن نطاق إقليم الدولة والبعد الجغرافي بين مرتكب الجريمة والضحية، وعدم المعرفة بمكونات الجريمة الإلكترونية المرتكبة عبر الإنترنت من قبل بعض الأطراف، وهو ما يقف حائلاً في الوصول إلى الأدلة[٢٦].

ويهدف الجاني من وراء هذه الأفعال المجرمة خاصة محو آثار الجريمة وأدلتها هو وضع العراقيل أمام سلطات الضبط حتى لا تتمكن هذه السلطات من إدانته أو إقامة الدليل ضده، وبالتالي يستطيع أن يتنصل من مسئوليته عن هذا الفعل الإجرامي وإرجاعه إلى خطأ في نظم الحاسب الآلي وشبكاته، وهو ما حدث في النمسا عندما قام أحد مهربي الأسلحة بإدخال عدد من التعديلات على الأوامر العادية لنظم تشغيل الحاسب الآلي الذي يستخدمه في تدوين عناوين عملائه بحيث يترتب على إدخال إحدى أوامر النسخ أو الطباعة من

---

[٢٥] أ/ عبد الرحمن بحر – معوقات التحقيق في جرائم الإنترنت، دراسة مسحية على ضباط الشرطة بدولة البحرين، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، ١٩٩٩، ص٥١. د. هشام فريد رستم– الجوانب الإجرائية، مرجع سابق، ص٢٠

[٢٦] أ/ عبد الرحمن بحر – معوقات التحقيق في جرائم الإنترنت، دراسة مسحية على ضباط الشرطة بدولة البحرين، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، ١٩٩٩، ص٤٦. أ/ سليمان بن مهجر العنزي– وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير في العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، ٢٠٠٣، ص١١٤.

خلال لوحة المفاتيح محو وتدمير كافة البيانات كاملة[٢٧]، وفي واقعة أخرى شهيرة بدولة الإمارات العربية عندما قام أحد مشغلي الحاسبات بمطالبة المؤسسة التي يعمل بها بتنفيذ مجموعة من المطالب، وإزاء رفض المؤسسة الاستجابة لمطالبه قام بحذف كافة البيانات من على الجهاز الرئيسي للشركة وأقدم على الانتحار مما سبب صعوبة بالغة في استرجاع تلك البيانات التي تم حذفها[٢٨].

الغصن الثاني
معوقات تتعلق بالمجرم

يتميز المجرم المعلوماتي بالذكاء والفطنة والخبرة الفنية وقدرته على التعامل مع الأجهزة الإلكترونية بحرفية وذكاء، كما أنه يتطور بتطور تلك الوسائل الإلكترونية وما يستجد من تقنيات، إضافة إلى قيامه بفرض سياجاً أمنياً على كافة أعماله غير المشروعة قبل ارتكابها حتى لا يقع تحت طائلة القانون، وهو ما يزيد من صعوبة وتعقيد عمل رجال الضبط القضائي في البحث عن الجريمة بالوسائل التقليدية، مثل قيامه بوضع أرقام ومفاتيح سرية تعيق إجراء عملية التفتيش للأجهزة الحاسب الآلي وشبكاته، والوصول إلى البيانات والمعلومات المخزنة إلكترونيا أو المنقولة عبر شبكات الاتصال، كما قد يقوم هؤلاء المجرمون بدس تعليمات خفية بين هذه البيانات أو استخدام رمز أو تشفير لها بحيث يستحيل على غيرهم الاطلاع والوصول إلي الأدلة والبيانات المخزنة[٢٩].

كما يتميز هذا النوع من الجناة بذكاء عالي جداً وقدرة على الهرب والمراوغة والتفنن في وضع واكتشاف أساليب متطورة للهرب من قبضة العدالة، وطمس معالم الجريمة، ومحو كافة أثارها، والبعد عن دائرة الشك والاتهام، إذ يقوم الجاني بوضع عقبات فنية لإعاقة ومنع

---

[٢٧] د. هشام فريد رستم– الجرائم المعلوماتية (أصول التحقيق الجنائي الفني)، بحث منشور بمجلة الأمن والقانون، العدد الثاني، دبي ١٩٩٩، ص٤٣٠.

[٢٨] أ/ خالد الستاني– أمن المعلومات وتحليل المخاطر، ورقة عمل مقدمة إلى ندوة فيروسات الحاسب الآلي، التي عقدها معهد التنمية الإدارية بالمجمع الثقافي بإمارة أبو ظبي، دولة الأمارات العربية المتحدة، في ١٩٩٦/٩/٢٣.

[٢٩] د. هشام فريد رستم– الجوانب الإجرائية، مرجع سابق، ص٢٢. أ/ أسامة أحمد المناعسة، جلال محمد الهوواشة، صايل فضل– جرائم الحاسب الآلي والإنترنت، الطبعة الأولي، دار وائل للنشر، لبنان– بيروت، ٢٠٠١، ص٢٩٣ وما بعدها.

(ISSN: 2537- 0758)

الوصول للدليل وكشف جريمته وضبط أدلتها باستخدام تقنيات التشفير[٣٠] أو كلمة السر، وذلك بقصد حجب المعلومة عن التداول العام، ومنع الغير بما فيه أجهزة الرقابة من الوصول غير المشروع إلى البيانات والمعلومات المخزنة أو التلاعب فيها، وقد كشفت التحقيقات التي أجريت في ألمانيا على بعض الجرائم الإلكترونية عن وجود العديد من الصعوبات التي واجهت سلطات التحقيق نتيجة استخدام مرتكبي هذه الجرائم لتقنيات خاصة كالتشفير والترميز لإعاقة الوصول إلى الأدلة التي تدينهم كوسيلة لمنع ضبطهم والقبض عليهم[٣١].

أضف إلى ذلك، أنه من بين الصعوبات التي تواجه سلطات التحقيق والاستدلال أثناء عملية جمع الأدلة الجنائية الإلكترونية من مسرح الجريمة وهي قدرة الجناة على إخفاء الهوية، أي إخفاء المستخدم لهويته، وهو ما يشكل تحديا أمنيا عندما يتم إخفاء الهوية دون أن يبذل الفاعل في ذلك مجهودا، فهو يستطيع التخلص من التهمة الموجهة إليه من خلال

---

[٣٠] التشفير هو غلق أو تشويش لخط البيانات من خلال لوغاريتمات أو خوارزميات بحيث لا يمكن لشخص ثالث قراءتها.

[٣١] ومن الأمثلة التي لجأ فيها الجاني إلى أسلوب التشفير، كوسيلة لمنع ضبطه والقبض عليه، الواقعة التي حدثت في الولايات المتحدة عام ١٩٩٦، حيث كان المشتبه به مشغلا للوحة إعلانات bbs، وبعد الوصول إلى جهاز الحاسب الشخصي الذي يستخدمه في إدارة اللوحة الإلكترونية، حاول محققو الشرطة العثور على كلمة المرور الخاصة بالمشتبه به، فقاموا بأخذ نسخة احتياطية من محتويات القرص الصلب، وقاموا بكتابة برنامج يحاول تشغيل النسخة الاحتياطية، وبعد فحص ملف المستفيدين استطاع المحققون الوصول بسهوله إلى أسماء المستفيدين وأرقامهم، ولكن لم يتمكنوا من العثور على كلمة المرور الخاصة بالمشتبه به، خاصة وأنها كانت مشفرة، ولولا تشفير كلمة المرور لأمكن إضافة مستفيد جديد بكلمة مرور جديدة، ثم تتبع هذه الكلمة داخل قاعدة بيانات المستفيدين حتى يتم معرفة مكانها، ولكن التشفير حال دون ذلك. وللوصول إلى كلمة المرور قام المحققون بإنشاء رقمين جديدين من أرقام المستفيدين، لهم نفس كلمة المرور، ولكنهم يختلفون في أسماؤهم، وبهذه الطريقة وبتتبع كلمتي المرور المتشابهتين أمكن العثور على مكان وجود كلمات المرور على القرص الصلب، ووضع المحققون يدهم على كلمة المرور الخاصة بالمتهم في ملف المستفيدين، ثم قاموا بإحلال كلمة المرور السابق استخدامها مع المستفيدين الوهميين مكان كلمة المرور الخاصة بالمشغل وهي مشفرة كما هي دون تعديل أو تغيير، وبذلك أمكن الدخول إلى الحاسب باستخدام اسم المشغل مع كلمة المرور الخاصة بالمستفيد الوهمي. م/ حسن طاهر داود– جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، الطبعة الأولى، الرياض، ٢٠٠٠، ص٢٣٣وما بعدها.

الادعاء بعدم مسؤوليته عن فعل الإخفاء، وقد يستخدم المجرمون جهدا بسيطا من الإجراءات لإخفاء هوياتهم من الشبكة لجعل أنشطتهم التي يقومون بها مجهولة الهوية من أجل محاولة الإفلات من إجراءات الاعتقال، ومن هذه الإجراءات التي يستخدمها المجرمون استخدام جهاز حاسب آلي من مقهى عام للإنترنت، وفي مقابل ذلك توجد العديد من البرامج والتطبيقات المختلفة التي تعمل على إخفاء هوية المستخدم عند دخوله لشبكة المعلومات، وهو ما يزيد من هذه الصعوبة لدى عضو سلطة التحقيق أو الخبير الإلكتروني عند تحليل الأدلة التي تم العثور عليها وتجميعها[٣٢].

ومن ناحية أخرى، قدرة الجناة على إخفاء المعلومات، فهي صعوبة أخرى تضاف إلى تحديات سلطة التحقيق والخبير الإلكتروني في الجريمة الإلكترونية، وهي تتم من أجل وضع هذه المعلومات المشبوهة أو المخالفة خارج نطاق الاطلاع من الأشخاص وسلطات الضبط والتحقيق، وقد تجتمع هذه الصعوبات في الشبكة بين إخفاء هوية المستخدم والمعلومات أو البيانات، مما يجعل الأمر معقدا وفي غاية الصعوبة لكشف ومعرفة الفاعل في مثل هذه الجرائم، إلا أنه توجد بعض البرامج التي تمكن سلطات التحقيق والخبير الإلكتروني من فك شفرات تلك الصعوبات وتعمل هذه البرامج على استعادة كافة المعلومات والبيانات المخفية في الشبكات منها البرنامج المعروف باسم ماروتوكي Marutukku[٣٣].

الغصن الثالث

معوقات تتعلق بالمجني عليه

تعد من قبيل المعوقات التي تواجه سلطات الضبط والتحقيق عدم تقدير المسئولين بالمؤسسات والشركات لخطورة الجرائم المعلوماتية، وضعف الجانب التوعوي لإرشاد المستخدمين إلى خطورة تلك الجرائم، حيث تقوم عدد من المؤسسات بالعمل على تقديم خدمات أسرع لعملائها وتتسابق في تسهيل إجراءات الحصول عليها وزيادة المنتجات، واقتصار تركيزها على مجرد تقديم الخدمة بدون عوائق، وذلك دون النظر إلى ما يترتب على تلك الخدمة أو السرعة في تقديمها من مشكلات أمنية مستقبلية[٣٤]، حيث لا يهم مزود

---

[٣٢] د. حازم محمد حنفي، الدليل الإلكتروني ودوره في المجال الجنائي، مرجع سابق، ص٨٢.

[٣٣] د. حازم محمد حنفي، الدليل الإلكتروني ودوره في المجال الجنائي، مرجع سابق، ص٨٣.

[٣٤] أ/ باسم الحمادي– إثبات جرائم الإنترنت صعب، بحث منشور عبر الانترنت بتاريخ ٧ محرم ١٩٢٣هـ، دولة الرياض، ص١٤، على موقع www.alrivadh.com.sa.

(ISSN: 2537- 0758)

الخدمة معرفة هوية مستخدمي خدمة الإنترنت أكثر من تقديم الخدمة، وزيادة عدد المستخدمين، ورفع كفاءة الشبكات وتطويرها باستمرار، كما أن الإحجام عن الإبلاغ عن الأشخاص الميسورين أو صغار السن، خوفاً من المجتمع المحيط بهم وخشية الفضيحة وعدم الظهور بمظهر مشين أمام الآخرين يعد معوقاً من المعوقات التي تحول دون إجراء التحقيق والحصول على الأدلة نظراً لما يتركه من انطباع بإهمال تلك الجهات المتضررة وفقدان ثقة الأفراد فيها وقلة خبرتها وعدم وعيها الأمني[٣٥].

الفرع الثاني
المعوقات التي تتعلق بسلطات الاستدلال والتحقيق

لقد واجهت سلطات الضبط والتحقيق والقضاء عدداً من المعوقات التي ترجع إلى شخص المحقق ذاته وعدم إمكانية التعامل بالوسائل الاستدلالية والإجرائية التقليدية مع هذه النوعية الحديثة من الجرائم التكنولوجية، ومنها عدم توافر الخبرة والكفاءة البشرية التي تؤهلهم لإجراء عملية التحقيق والبحث عن الأدلة، وعدم الاهتمام بمتابعة كل ما هو جديد في عالم الجريمة الافتراضي الرقمي، والتهيب من استخدام الحاسب الآلي، والتهيب من شبكة الإنترنت[٣٦]، ولم يكن في بداية استخدام أنظمة الحاسب الآلي أساليب للرقابة وضوابط للمراجعة والتدقيق على العمليات والتطبيقات، وعدم وجود وسائل فنية لاكتشاف وتتبع مسار العمليات[٣٧].

وهناك من المشكلات ما يتعلق بالنواحي الفنية، كنقص الخبرة والمهارة الفنية المطلوبة للتحقيق والبحث عن أدلة هذا النوع من الجرائم الحديثة، ونقص المهارة الفنية في استخدام الحاسب الآلي والإنترنت، وعدم المعرفة بأساليب ارتكاب هذا النوع من الجرائم الرقمية، وعدم المعرفة بالمصطلحات العلمية الإنجليزية المتداولة بين الخبراء الفنيين والعاملين في مجال الحاسب الآلي والتي تستخدم في برمجة الحاسب الآلي ومكوناته، خاصة وأنها أصبحت

---

[٣٥] **راجع في ذلك:** د. طارق عبد الله الشدي– آلية البناء لنظم المعلومات، دار الوطن للطباعة والنشر، الرياض، ١٤٢٣هـ، ص٢١٠. أ/ عبد الرحمن بحر– معوقات التحقيق في جرائم الإنترنت، مرجع سابق، ص٣٩. أ/ باسم الحمادي– إثبات جرائم الإنترنت، مرجع سابق، ص١٤.

[٣٦] أ/ سليمان بن مهجر العنزي– وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير في العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، ٢٠٠٣، ص١١٩.

[٣٧] د. هشام فريد رستم– الجوانب الإجرائية، مرجع سابق، ص١٨.

الطابع المميز لمحادثاتهم وأساليب التفاهم معهم، كما أنهم قاموا بوضع لغة جديدة تميزهم عن غيرهم تعرف بلغة Acronyms وهي عبارة عن مصطلحات وعبارات إنجليزية فنية تم صياغتها بأحرف لاتينية وتتميز بتجددها وتطورها، الأمر الذي جعل قراصنة الإنترنت ومعتادي الإجرام المعلوماتي يطلقون على أنفسهم وصفة النخبة، ويطلقون على رجال السلطة ومكافحة الجريمة وتطبيق القانون وصف الضعفاء أو القاصرين[٣٨].

لذا، فقد بدأ عدد من الأجهزة الأمنية والقضائية في جلب كوادر فنية من المتخصصين في تكنولوجيا وبرمجيات الحاسب الآلي وشبكاته ليعاونوها في كشف الجريمة والتوصل إلى أدلتها، بالإضافة إلى العمل على تدريب رجال من الشرطة والقانون على علوم الحاسب الآلي وشبكاته، وإيفاد بعثات خارجية لتلقي عدد من الدورات التدريبية، وإنشاء أقسام وأجهزة معاونة وتابعة لجهاز الشرطة تكون على استعداد تام ومعرفة بعلوم الحاسب الآلي وطرق مكافحة الجريمة الإلكترونية، وعلى الرغم من ذلك لا تزال تلك الأجهزة غير قادرة على مواكبة التطور السريع في تكنولوجيا الحاسب الآلي وبرمجياته، **وبالتالي عدم التوصل إلى سبل كشف الجريمة المعلوماتية نظراً لوجود عدة أسباب من أهمها[٣٩]:**

- قد تكون الميزانية المرصودة لتدريب كوادر بشرية من رجال الأمن غير كافية لجلب النخبة من المتميزة في مجال تقنية الحاسب الآلي وبرمجياته وشبكاته، خاصة وأن شركات ومؤسسات القطاع الخاص تبذل قصارى جهدها وتنفق الكثير من أجل التوصل إلى هذه النخبة وتجنيدها للعمل لديها.
- عدم تفرغ أجهزة الأمن والقضاء تماماً للجرائم الرقمية وحدها، بل هناك العديد من المجالات الأخرى والمتنوعة التي يجب تغطيتها بالدعم والعناية والتي تنال أهمية خاصة لديها.
- ضعف خبرة الأجهزة الأمنية في التعامل مع هذا النوع من الجرائم ويرجع السبب في

---

[٣٨] راجع د. محمد الأمين البشري– التحقيق في جرائم الحاسب الآلي، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة، في الفترة من ١– ٢٠٠٠/٥/٣، الطبعة الثالثة، ٢٠٠٤، ص١٠٧٠ وما بعدها.

[٣٩] راجع د. محمد الأمين البشري– التحقيق في جرائم الحاسب الآلي، المرجع السابق، ص١٠٧٢ وما بعدها. د. هشام محمد فريد رستم– الجوانب الإجرائية، مرجع سابق، ص٢٢. **وراجع أيضاً:**

Peter Tillers: Introduction to program on Artificial Intelligence N.Y. Yeshiva, University press, 1999, p117.

(ISSN: 2537- 0758)

ذلك لما يتميز به جرائم الحاسب الآلي والإنترنت من حداثة وقلة اكتشافها، على عكس ما يتميز به مرتكبوا هذا النوع من الجرائم الإلكترونية من ذكاء وخبرة فنية وتقنية وسرعة في التكيف مع التقنيات المتغيرة والبيانات المختلفة لها.

- صعوبة حصر أساليب ارتكاب جرائم الحاسب الآلي والإنترنت وصورها وأنماطها بسبب سرعة انتشار أجهزة الحاسب الآلي وشبكاته وتنوع برامجه وأنظمته الأمر الذي يصعب معه تدريب كوادر فنية من المحققين ورجال الأمن لمكافحة تلك الجريمة.

ولعلاج هذه المشكلات والتوصل إلى وضع أسلوب لمكافحة جرائم الحاسب الآلي والإنترنت، والتغلب على ما يستجد من عراقيل ومعوقات يصعب على الأجهزة الأمنية والقضائية التغلب عليها، فقد انقسمت أراء رجال الفقه والقانون في هذا الشأن إلى اتجاهين[٤٠]:

- **الاتجاه الأول:** يرى أنصاره ضرورة أن توكل مهمة الكشف عن جرائم الحاسب الآلي والإنترنت والبحث عن أدلتها وضبطها والتحقيق فيها إلى بيوت خبرة متخصصة في هذا المجال الفني عالي التقنية لا سيما مع وجود شركات عالمية متخصصة حققت نجاحات كثيرة في مجال مكافحة الجريمة الإلكترونية.
- **الاتجاه الثاني:** ويرى أنصاره ضرورة أن تقوم الأجهزة الأمنية الحكومية بتحمل مسئوليتها وفقا لمقتضيات العدالة الجنائية تجاه الكشف عن الجريمة ومكافحتها وضبط الجناة وتحقيق العدالة المنشودة، وتحمل توفير الإمكانيات المادية والمعنوية والكوادر البشرية المتخصصة اللازمة للحد من جرائم الحاسب الآلي والإنترنت والعمل على مكافحتها.

ونحن من جانبنا، نتفق وأنصار الاتجاه الأول، مع ضرورة الاهتمام بتوفير الدعم اللازم لتطوير وتجهيز العناصر الفنية المدربة، والعمل على إنشاء جهاز أو قطاع خاص لمكافحة جرائم الحاسب الآلي والإنترنت تكون مهمته التفرغ لتدريب كوادر شرطية

---

[٤٠] د. حسين الغافري– السياسة الجنائية، مرجع سابق، ص٤١١. أ/ أسامة أحمد المناعسة– جرائم الحاسب الآلي والإنترنت، مرجع سابق، ص٢٩٠ وما بعدها. **وراجع أيضاً:**

United Nation: United Nation Manual on the prevention and control of Computer–Related crime: Vienna 1999.

وقضائية فنية تجمع بين الخبرة الفنية والكفاءة المهنية، والتفرغ لمواكبة التطور السريع في تكنولوجيا الحاسب الآلي وشبكات الإنترنت ومواجهة الأنماط الإجرامية الحديثة والمتطورة وأساليب التلاعب المحاسبي المعقدة التي تستخدم في ارتكاب جرائم الحاسب الآلي والإنترنت.

الفرع الثالث
المعوقات التي تتعلق بالدليل ذاته

هناك مشكلات تعيق عمل سلطات الضبط والتحري في الحصول على الأدلة المتعلقة بجرائم الحاسب الآلي والإنترنت، تتعلق بشكل الدليل المستخرج ذاته، حيث يتميز الدليل الرقمي– البيانات والمعلومات– المستخرج من وسائل التقنية بالحداثة والتطور، فالدليل الرقمي هو مجموعة من المعلومات والبيانات المسجلة إلكترونياً، بكثافة بالغة، وبصورة مرمزة (على شكل رموز) غالباً داخل محتوى عبارة عن دعائم أو وسائط للتخزين ممغنطة، لا يترك التعديل فيها أي أثر، ولا يمكن للإنسان قراءتها إلا من خلال الآلة نفسها وبالتقنية نفسها[٤١]، أو هو الدليل الذي يجد له أساساً في العالم الافتراضي ويقود إلى الجريمة، فهو ذلك الجزء المؤسس على الاستعانة بتقنية المعالجة التقنية للمعلومات، والذي يؤدي إلى قناعة قاضي الموضوع بثبوت ارتكاب شخص ما لجريمة عبر الإنترنت[٤٢].

ولما كانت المعلومات والبيانات المستخرجة من شبكات المعلومات، تعتبر من البيانات المتحركة، وتوجد العديد من التطبيقات التي تعمل على تحميل الملفات من الجهاز أو وسيلة تقنية المعلومات إلى الشبكة العالمية للمعلومات، ويمكن من خلالها الحصول على نسخة من تلك المعلومات أو البيانات من قبل أي شخص آخر عن طريق الشبكة ذاتها، ورغم ذلك فإن عضو سلطة التحقيق أو الخبير التقني المنتدب يواجه العديد من الصعوبات عند جمع الأدلة الإلكترونية من شبكات المعلومات والتي تتعلق بالدليل الإلكتروني ذاته، **إضافة إلى الصعوبات التي تم ذكرها سابقا وهي:**

---

[٤١] د. جميل عبد الباقي الصغير– الجوانب الإجرائية، مرجع سابق، ص٨٠. وللمؤلف أيضاً– أدلة الإثبات الجنائي والتكنولوجيا الحديثة، مرجع سابق، ص١٤. د. خالد حازم إبراهيم– دور الأجهزة الأمنية في الإثبات الجنائي في الجرائم المتعلقة بشبكة المعلومات الدولية (الإنترنت)، دراسة مقارنة، القاهرة، ٢٠١٤، ص٣٦٢.

[٤٢] د. عمر أبو بكر يونس– الإثبات الجنائي عبر الإنترنت، مرجع سابق، ص٥. د. حسين بن سعيد الغافري– السياسة الجنائية، مرجع سابق، ص٤١٥.

(ISSN: 2537- 0758)

أولا– طبيعة شبكة المعلومات هي عبارة عن اتصال لأكثر من شبكة وجهاز: ونتيجة لذلك توزعت مسارح الجريمة وكذلك الأدلة الإلكترونية في عدة أماكن مختلفة مما يؤدي إلى صعوبات عملية وتشريعية في آن واحد، خاصة مع اختلاف نصوص القوانين بين تلك الأماكن، ففي أغلب الأحيان إذا وجدت أدلة في دولة أخرى لا يمكن الحصول عليها حتى مع اتخاذ إجراءات دولية تسهل عملية تبادل تلك الأدلة الإلكترونية وذلك لأن معظم هذه الإجراءات معقدة، كما أنها ليست عملية إلا عند وقوع إحدى الجرائم الخطيرة والتي حينها يتم استدعاء المعلومات بصورة رسمية من الدول الأخرى.

ثانيا– طبيعة المعلومات والبيانات الإلكترونية ذاتها: حيث إنها يمكن أن تخضع للمحو أو التغيير بسهولة، لذا يصبح من الضروري جمعها والتحفظ عليها بسرعة كلما أمكن ذلك، ورغم أن مرور تلك المعلومات والبيانات في الشبكات لا يستغرق إلا أجزاء من الثانية وهي فترة قصيرة جدا، وكذلك حجم تلك المعلومات والبيانات الكبير والمتزايد بشكل لحظي، فإنه يصبح من غير الممكن التحفظ على المعلومات والبيانات لوقت طويل. وبالإضافة لذلك، فإذا ما توافرت فرصة المعرفة والمهارة لدى المجرم، فإنه يقوم بإتلاف الأدلة أو تعديلها أو محوها من أجل الهروب من يد العدالة وتبرئة ساحته من الأدلة التي تدينه.

ثالثا– نقص الخبرة الفنية حول هذه الشبكات وذلك لتنوعها واختلافها من شبكة لأخرى: وهو ما يصعب من مهمة الخبير الذي لا يمكن أن يكون ملما بالتعامل مع جميع أنواع الشبكات واختلافها، وهو ما يتطلب أشخاصا أكثر يمتلكون الكفاءة للتعامل مع التقنية والحصول منها على الأدلة.

رابعا– حجم البيانات الكبيرة التي تستخدم في التحقيق والمستخرجة من أنظمة الأجهزة محل التحقيق: فعند القيام بإجراءات التحقيق المختلفة والبحث عن الأدلة، فإن ذلك يتم في كم كبير من المعلومات والبيانات الإلكترونية وهو ما يحتاج لجهد كبير ومهارة عالية[٤٣].

وعلى الجانب الآخر، فإننا نلاحظ وبدقة نقص في المعرفة التقنية الحديثة والمتجددة لدى القائمين بالبحث والتحقيق في هذه الجرائم، مما يجعل منهم غير قادرين على أداء واجبهم على الوجه المطلوب، إذ أن نقص الخبرة والكفاءة، سواء في أجهزة الشرطة أو الادعاء يعد من الأسباب الرئيسية للإخفاق في كشف الجرائم الإلكترونية وجمع أدلتها،

[٤٣] د. ممدوح عبد الحميد عبد المطلب– البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر الإنترنت– المحلة الكبرى– دار الكتب القانونية، القاهرة، ٢٠٠٦، ص١٢٠.

ويظهر ذلك بشكل واضح في الدول التي لا تزال تتعامل مع هذه الجرائم بإجراءات البحث والتحقيق التقليدية، وتفتقر سلطاتها الضبطية والقضائية للأجهزة التقنية المتطورة في متابعة الجرائم الإلكترونية وضبط أدلتها، وبديهيا أنه في حالة عدم توافر التأهيل والخبرة وشُحِّ الإمكانيات التقنية على وجه الخصوص، فلا يمكن أن نتصور أي وجه للتعامل مع هذه الجرائم، وبالتالي ستكون النتائج سلبية لا محالة.

لذا، فإن حداثة الدليل الرقمي تثير نوعين من المشكلات:

النوع الأول: يتمثل فيما تواجهه سلطات الضبط والتحري من معوقات في التعامل مع هذا المحتوى الإلكتروني وإثبات وقوع الجريمة وجمع أدلتها وتتبع أثر مرتكبيها، ومدى إمكانية إجبار الجاني أو المتهم على تقديم الدليل والكشف عن الرقم السري لجهاز الحاسب الآلي الخاص به، ومدى إمكانية السيطرة على الجاني ومنعه من محاولة تدمير البيانات والمعلومات أثناء عملية التفتيش[٤٤].

أما النوع الثاني: فيتمثل في شكل المعلومات الرقمية المسجلة إلكترونياً، ومدى إمكانية قبولها لدى جهات التحقيق والمحاكمة كدليل إثبات[٤٥].

ونظراً لما يتمتع به الدليل الرقمي من حداثة وتطور وما تتمتع به الجريمة من طبيعة افتراضية الأمر الذي تكون معه الأجهزة الأمنية والقضائية في حاجه إلى محققين وخبراء فنيين في مجال الشبكات والأدلة وتكنولوجيا المعلومات والاتصالات للتعامل مع مسرح الجريمة الرقمي الذي لا يرتبط بالمحيط المادي لمسرح الجريمة، حيث يتم جمعه من عدد كبير من أجهزة الحواسب الموجودة بمسرح الجريمة أو المتنقلة خارج نطاق مسرح الجريمة أو الدولة طالما أنها مرتبطة بالجريمة عن طريق شبكات إلكترونية، وهو ما يحتاج إلى وقت طويل قد تتعرض معه العديد من الأدلة للفقد والضياع والتلف، وحتى في حالة الوصول للدليل تواجه أيضا مشكلة القانون الواجب التطبيق عليها، وهو ما يحتاج إلى رجال ضبط قضائي ومحققين لديهم مهارة فنية عالية وخبراء في البحث عن الدليل المستخرج من

---

[٤٤] د. سامح محمد عبد الحكم– جرائم الإنترنت الواقعة على الأشخاص في إطار التشريع البحريني، دراسة مقارنة بالتشريع المصري، الطبعة الثانية، دار النهضة العربية، القاهرة، ٢٠٠٧، ص٣.

[٤٥] د. هشام فريد رستم، الجوانب الإجرائية في الجرائم المعلوماتية– مكتبة الآلات الحديثة، أسيوط، ١٩٩٤، ص١٨. **وراجع أيضاً:**

Urlich Sieber: The spreading danger of computer crime, Business week, 20 April 1991, P.92.

(ISSN: 2537- 0758)

الحاسب الآلي والإنترنت وتحليله وتقديمه للقاضي للفصل في النزاع[٤٦].

وبالتالي، فإنه يتعين على الدولة أن تضع برنامج تدريب وتأهيل لرجال الشرطة على أساليب الوقاية من جرائم الإنترنت والحاسب الآلي، ووضع التدابير المانعة لوقوعها، والقيام بالتحري عما ارتكب منها وكشفها، وأيضا كيفية التعامل مع الأدلة وضبطها، والاستعانة بذوي التخصصات الدقيقة المتعمقة في أنظمة الحاسب الآلي والإنترنت وشبكات الاتصال الأخرى، كما يجب عليها عقد دورات تدريبية وبرامج تأهيل للمحققين ورجال القضاء ليكونوا على دراية ومعرفة بكافة الأساليب الإجرامية الحديثة وسبل مواجهتها وطرق استخلاص الدليل من تلك الجرائم[٤٧].

الفرع الرابع
المعوقات التشريعية والإجرائية

يمكن القول أن التطور التكنولوجي قد أفرز في مجال تكنولوجيا المعلومات العديد من الجرائم التقنية ذات الطبيعة الخاصة التي تسببت في فرض الكثير من المعوقات أمام جهات الضبط التقليدية نظراً لسرعة، ومرونة طرق ارتكابها، وتمثلت هذه المعوقات في إجراءات الاستدلال، والضبط، والتحقيق، واعتراض المراسلات والاتصالات للبحث عن الأدلة، والتأكد من صحتها، وتحديد سلطة الاختصاص[٤٨].

إضافة إلى أن ندرة التشريعات واختلافها بين الدول يثير العديد من المشكلات التي تعوق عملية ضبط تلك الجريمة، وجمع أدلتها خاصة فيما يتعلق بشروط قبول تلك الأدلة المستخرجة من الوسائل الإلكترونية، وإتباع الإجراءات اللازمة للتوصل إليها مثل التفتيش العابر للحدود[٤٩].

---

(46) Jody R. and Westby. Project Chair& Editor, international Guide to Combating Cybercrime, Op-Cit, p87.

(٤٧) د. حاتم بطيخ– دور الإنترنت في الإثبات، مرجع سابق، ص٥١٢.

(48) Jody R. and Westby. Project Chair& Editor, international Guide to Combating Cybercrime, Op-Cit, p89.

(٤٩) د. جميل عبد الباقي الصغير– الجوانب الإجرائية للجرائم المتعلقة بالإنترنت– دار النهضة العربية، القاهرة، ٢٠٠١، ص٨٢ وما بعدها. د. حاتم بطيخ– دور الإنترنت في الإثبات، مرجع سابق، ص٥١٢، د. حسين بن سعيد بن سيف الغافري– السياسة الجنائية في مواجهة جرائم الإنترنت، رسالة دكتوراه، جامعة عين شمس، بدون سنة نشر، ص٤١٤.

وهو الأمر الذي دعا فقهاء القانون للمطالبة بسن تشريعات حديثة تكون أكثر مرونة، وتتوافق مع جرائم التقنية المعلوماتية المتطورة، وتقيم التوازن بين حماية الحقوق والحريات الخاصة للأفراد والحقوق العامة للمجتمع، وتطوير قواعد وإجراءات جمع الأدلة.

كما أنه من الصعوبة تطبيق القواعد القانونية التقليدية الداخلية للدولة على الجرائم الإلكترونية التي تقع علي أرضها، كما لا يمكن تطبيقها على الجرائم التي تحدث أيضاً خارج نطاق إقليمها، فهناك أنواع من الجرائم تتعدد أماكن ارتكابها داخل الدولة الواحدة، أو يمتد نطاقها ليشمل الكثير من الدول عبر شبكة الإنترنت، الأمر الذي يتعذر معه اتخاذ الإجراءات التقليدية المحلية لجمع الأدلة بالنسبة لها، أو قد تصاب تلك الإجراءات بعدم المشروعية.

وهو ما أقره الفقه الألماني حيث شكك في إمكانية الدخول إلى أنظمة تقنية المعلومات لدى الحاسبات الأخرى التي توجد بالخارج بغرض ضبط الأدلة من بيانات ومعلومات مخزنة بها دون وجود اتفاق بين الدول المعنية ينظم تلك الإجراءات، ويقول الفقه في ذلك أن اتخاذ مثل هذه الإجراءات دون وجود اتفاق مسبق بين الدول يعد خرقاً لسيادة كل دولة على إقليمها، ويخالف الاتفاقيات الثنائية الخاصة بإمكانية التعاون في مجال العدالة القضائية[٥٠].

ويعتبر موضوع الإثبات بالوسائل الحديثة أو ما أطلق عليه الدليل الإلكتروني أحد أهم الموضوعات التي شغلت الرأي العام على المستويين الدولي والمحلي، ويرجع السبب في ذلك إلى التطور المستمر الذي تحظى به وسائل تقنية المعلومات وانعكس ذلك على الدليل الإلكتروني وأدوات استخلاصه من الأجهزة والوسائل والشبكات الإلكترونية.

ولا شك في أن الدليل الإلكتروني يحتاج في سبيل الوصول إليه واستخلاصه استخلاصًا صحيحًا إلى خبراء، وفنيين متخصصين في مجال تكنولوجيا المعلومات، ويخضع هذا الدليل كغيره من الأدلة التقليدية في قبوله لسلطة القاضي ومدى تأثير هذا الدليل في قناعته الوجدانية.

ومن أجل ذلك فقد خصصنا هذه الدراسة لتناول موضوع غاية في الأهمية يتعلق بمدى مشروعية الدليل الإلكتروني في الإثبات أمام القاضي الجنائي والإداري، وتناولنا هذا

(50) Mohrenschlager "Manfred": Computer crimes and other crimes against, OP Cit, P.351- 352.

(ISSN: 2537- 0758)

الموضوع من وجهة نظر المشرع الكويتي والمصري، وبعض التشريعات المقارنة، واعتمدنا في ذلك على بعض النصوص التقليدية والقواعد العامة في الإثبات، وما استقر لدى الفقه والقضاء من مبادئ، خاصة وأن أغلب هذه التشريعات لم تتطرق لتنظيم قواعد وبإجراءات الإثبات بالوسائل الإلكترونية بشكل كامل إلا في بعض الجزئيات المتفرقة على نحو ما عرضنا.

وقد توصلنا في هذا البحث إلى عدد من النتائج الهامة، والتي أهمها الآتي:

أولاً: النتائج:

١- تطور شكل الجريمة والمجرمين بتطور وسائل التقنية المعلوماتية ودخولها في شتى المجالات الحياتية، واستغلالها في تحقيق أغراضهم الإجرامية غير المشروعة.

٢- إن الجريمة الإلكترونية تحتاج إلى خبراء وفنيين متخصصين في مجال تقنية المعلومات للتعامل معها، ومعاونة السلطات المختصة في كشفها.

٣- تطور شكل الدليل بتطور وسائل التقنية المعلوماتية التي انعكست علي الجريمة والسلوكيات الإجرامية، وظهر ما يسمى بالدليل الإلكتروني أو الرقمي الذي أثر في نظرية الإثبات بشكل عام.

٤- يقصد بالدليل الإلكتروني أو الرقمي مجموعة البيانات المخزنة بشكل كهرومغناطيسي على القرص الصلب بالحاسب الآلي أو شبكة المعلومات، والذي يتم استخلاصه بإجراءات فنية تحكمها إجراءات قانونية بهدف ترجمة تلك البيانات وتقديمها كدليل إثبات لنفي أو إثبات فعل ما بحق صاحبه.

٥- يعد الدليل الإلكتروني هو الوسيلة التي من خلالها يتوصل إلى حقيقة الجرائم التي ترتكب الوسائل الإلكترونية أو التي تقع على هذه الوسائل.

قائمة المراجع

أولاً: المراجع العربية:-

- **د. أحمد بن عبد الله الرشودي**، حجية الوسائل الإلكترونية في الإثبات الجنائي، دراسة تأصيلية مقارنة تطبيقية، رسالة دكتوراه الفلسفة في العلوم الأمنية، جامعة نايف العربية للعلوم الأمنية، الرياض، ٢٠٠٨
- **د. حاتم أحمد محمد بطيخ**، دور الإنترنت في الإثبات أمام القاضي الجنائي والإداري، رسالة دكتوراه، كلية الحقوق– جامعة عين شمس، ٢٠١٧.
- **د. سامح محمد عبد الحكم–** جرائم الإنترنت الواقعة على الأشخاص في إطار التشريع البحريني، دراسة مقارنة بالتشريع المصري، الطبعة الثانية، دار النهضة العربية، القاهرة، ٢٠٠٧
- **د. سعيد عبد اللطيف حسن**– إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، دار النهضة العربية، القاهرة، (١٩٩٩)
- **سعيداني نعيم**، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير في العلوم القانونية، جامعة الحاج لخضر، باتنة، الجزائر، ٢٠١٣،
- **سليمان بن مهجر العنزي–** وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير في العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، ٢٠٠٣
- **عبد الرحمن بحر–** معوقات التحقيق في جرائم الإنترنت، دراسة مسحية على ضباط الشرطة بدولة البحرين، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، ١٩٩٩
- **د. على محمود على حمودة**– الأدلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائية، بحث مقدم ضمن أعمال المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، والتي نظمتها شرطة دبي في الفترة ٢٦– ٢٠٠٣/٤/٢٨، دبي
- **د. عمر محمد بن يونس**– الإثبات الجنائي عبر الإنترنت، ط١، القاهرة ٢٠١٠
- **د. محمد الأمين البشري–** التحقيق الجنائي المتكامل، أكاديمية نايف للعلوم الأمنية، الرياض، ١٩٩٧
- **د. محمد الأمين البشري**– التحقيق في الجرائم المستحدثة، جامعة نايف العربية للعلوم الأمنية، الرياض، ط١، ٢٠١٤

(ISSN: 2537- 0758)

- **د. مدحت رمضان–** جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية، القاهرة، ٢٠٠٠
- **د. مصطفى محمد موسى–** التحقيق الجنائي في الجرائم الإلكترونية، مطبعه الشرطة، الطبعة الأولى، القاهرة، ٢٠٠٩
- **د. ممدوح عبد الحميد عبد المطلب**– استخدام بروتوكول (TCPIP) في بحث وتحقيق الجرائم على الكمبيوتر، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، مركز البحوث والدراسات، العدد (٤)، المحور الأمني والإداري، المنعقد خلال الفترة ٢٦– ٢٨ إبريل ٢٠٠٣، دبي، الإمارات العربية المتحدة، ٢٠٠٣
- **د. منير محمد الجنبيهي**، ممدوح محمد والجنبيهي– بروتوكولات وقوانين الإنترنت، دار الفكر العربي، ط١، القاهرة ٢٠١٣
- **د. ميسون خلف الحمداني**، الدليل الرقمي وعلاقته بالمساس بالحق في الخصوصية المعلوماتية أثناء إثبات الجريمة، جامعة النهرين، دولة العراق، ٢٠١٦

ثانياً: **المراجع الأجنبية**:-

- Kenneth S. Rosenblatt, High- Technology crime investigating Cases Involving computer, ksk publication San Jose, USA, 2003
- Mark R. Colombell, The legislative response to the evolution of computer verses, 8 RICH, i.1, and TECH 2002
- Peter Stephenson: Investigating Computer Related Crimes London, C. R. C, 1999.