



مجلة العلوم القانونية والسياسية

اسم المقال: التحديات الإجرائية المتصلة بالجرائم المعلوماتية

اسم الكاتب: م.م. صفاء حسن نصيف

رابط ثابت: <https://political-encyclopedia.org/library/1078>

تاريخ الاسترداد: 2025/05/10 18:35 +03

الموسوعة السياسية 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 السياسية – Encyclopedia Political، يرجى التواصل على info@political-encyclopedia.org

استخدامكم لأرشيف مكتبة الموسوعة السياسية – Encyclopedia Political يعني موافقتك على شروط وأحكام الاستخدام

<https://political-encyclopedia.org/terms-of-use>

تم الحصول على هذا المقال من موقع مجلة العلوم القانونية والسياسية جامعة ديالي ورفده في مكتبة الموسوعة السياسية
مستوفياً شروط حقوق الملكية الفكرية ومتطلبات رخصة المنشاع الإبداعي التي يتضمن المقال تحتها.



التحديات الإجرائية المتصلة بجرائم المعلوماتية

Procedural Challenges related to Informatics Crimes

الكلمة المفتاحية : التحديات الإجرائية، الجرائم المعلوماتية

Keywords: *Procedural challenges, informatics crimes.*

م.م. صفاء حسن نصيف

كلية القانون والعلوم السياسية – جامعة ديالى

Assistant Lecturer. *Safa'a Hassan Nisaif*

College of Law and Political Sciences-University of Diyala

E-mail: *safaahassan92@yahoo.com*

ملخص البحث

رافقت التطورات الكبيرة في مجال شبكات الإنترنت والمعلومات انماطاً جرمية مستحدثة وفريدة لم تكن المجتمعات على سابق عهد بها أثارت جدلاً واسعاً ترکز بشكل مباشر حول مدى مرونة واتساع التشريعات العقابية التقليدية لاستيعاب مثل هذه الانماط سيما في الجانب الاجرائي الذي تأتي هذه الدراسة لتسلط الضوء عليه فيما يتعلق بالتحديات الاجرائية التي تشيرها الجرائم المعلوماتية والمتعلقة بمدى مقبولية الدليل الرقمي وخصوصاً تلك البيانات التي لا يمكن التوصل إليها إلا من خلال استخدام تقنيات معينة وتطبيقات خاصة بإشراف خبراء في هذا المجال، ويتوقف مدى حجيتها على طبيعة النظام القضائي القائم والسلطة التقديرية الممنوحة للقاضي، ومدى اعتماد نظام الإثبات العلمي في الإثبات الجنائي؛ ويشار إلى إشكال أيضاً في مجال التفتيش في البيئة الرقمية الافتراضية نظراً لما تتسم به هذا البيئة من طبيعة خاصة وكذلك اتساع مسرح الجريمة المعلوماتية إلى الحد الذي تلغى معه الحدود الإقليمية مما يفرض إيجاد حلولاً قانونية لفرض التفتيش الواقع خارج حدود إقليم الدولة؛ ومن التحديات الأخرى المترتبة على سمة عدم اعتراف الجريمة المعلوماتية بالحدود الإقليمية مشكلة تنازع الاختصاص، في حال وقوع الجريمة في أي مكان فيه حسب موصول بشبكة الإنترنت وتحقق اثراها في مكان أو أماكن أخرى متعددة ومن قبل شخص أو اشخاص يحملون جنسيات مختلفة مما يشير إشكالاً قانونياً في تحديد قبل كل شيء مكان وقوع الجريمة ومن ثم القانون الواجب التطبيق عليها، الأمر الذي يدعو إلى تجاوز القوالب التقليدية واعتماد أسس قانونية مستحدثة جديدة وبما يتلاءم وطبيعة هذه الجرائم.

المقدمة

لقد افرز التطور العلمي والتكنولوجي في مجال الاتصالات وتكنولوجيا المعلومات وشبكات الإنترن特 العديد من الوسائل للبشرية تجعل من نمط حياتها يسير على نحو اسهل وأقل تعقيداً بفضل ما تتسم به من الكفاءة العالية وقدرتها على تجاوز المسافات البعيدة والتعقيدات الإدارية الروتينية وفي مختلف المجالات؛ فلم تدع هذه الوسائل الحديثة مجالاً يمكن أن تسهم فيه بدور أو يمكن أن يستغنى فيه عن دور الإنسان إلا ودخلته؛ سواء على مستوى التعاملات التجارية والمصرفية الإلكترونية كما نلحظ في تطور وازدياد ما يعرف بـمراكز التسوق الإلكترونية أو البنوك الإلكترونية وغيرها، أو على مستوى اساليب الإدارة الحديثة من خلال التحول نحو نظام الإدارة أو الحكومة الإلكترونية أو مستوى الحياة الاجتماعية بشكل عام من خلال م الواقع التواصلي الاجتماعي والمنتديات وغيرها.

لكن بالمقابل افرزت هذه التقنيات الحديثة المرتبطة بشبكة المعلومات والإنترنت انماطاً جرمية مستحدثة وفريدة من نوعها لم تكن المجتمعات على سابق عهد بها تتسم بذات السمات التي تتسم بها هذه التقنيات بالنظر إلى سرعة ارتكابها وسهولة محو أثارها ومعاليمها قبل اكتشافها واعتمادها بشكل أساس على تقنية المعلومات بالإضافة إلى عدم تقييدها بالحدود الإقليمية مما يجعلها ذات طابع دولي وغيرها من المزايا، أثارت هذه الظواهر الاجرامية المستحدثة جدلاً واسعاً تركز بشكل مباشر حول مدى اتساع وفاعلية وجدوى التشريعات الجنائية التقليدية لتجريم مثل هذه الانشطة الجرمية الحديثة، بيد أن الأمر لا يقتصر فقط على الجانب الموضوعي فمن غير المجد أن نعدل تشريعات أو نستحدث أخرى لاستيعاب هذه الجرائم من غير أن يكون هناك نظام قانوني إجرائي متكملاً يسهم بالكشف عن الجريمة والقبض على الجناة ومحاكمتهم، سيما ما يخص إثبات هذه الجرائم من خلال الأدلة الرقمية المعتمدة في ذلك، وآلية مباشرة إجراءات الاستدلال والتحقيق في البيئة الافتراضية لتعقب المجرمين وتقديمهم للمحاكمة؛ يضاف إلى ذلك أن ملاحقة الجناة وكشف جرائمهم عبر الحدود يقتضي من الناحية العملية أن يتم في نطاق إقليم دولة أخرى،

وهو ما يصطدم بمبدأ السيادة الإقليمية للدول آخذًا بمبدأ إقليمية القانون الجنائي، ويفضي بالتالي إلى تنازع الاختصاص القضائي بسبب صعوبة تحديد مكان وقوع الجريمة المعلوماتية عبر الوطنية، ومن هنا جاءت فكرة البحث لسلط الضوء على الجانب الاجرائي للجرائم المعلوماتية^(١) وبشكل خاص التحديات الاجرائية التي تشيرها هذه الجرائم في ثلاثة مباحث؛ شخص الأول منها لبحث مدى قبول الدليل الرقمي في مجال الإثبات الجنائي، وتناول في الثاني التفتيش في البيئة الرقمية، بينما نبحث في الثالث اشكالية تنازع الاختصاص الجنائي والقانون الواجب التطبيق على هذه الجرائم.

المبحث الأول

اشكالية قبول الدليل الرقمي

تقع الجرائم المعلوماتية على درجة من الصعوبة من حيث اثباتها إذ لا تختلف هذه الجرائم أي أدلة مادية ملموسة كتلك التي تنتج عن الجرائم التقليدية كالسلاح المستخدم والمقدوفات وبصمات الاصابع والاثار وغيرها؛ فضلاً عن عدم ترك هذه الجرائم أي اثار مادية نجد أن هناك صعوبات أخرى متعلقة بالدليل الناتج عنها بذاته من حيث صعوبة التوصل إليه في خضم هذا الكم الهائل من البيانات المحمولة على الشبكة، ومن حيث قابليته للتعديل والاخفاء والمحو وغيرها؛ لذا نجد من الضروري أن نبين بدءاً مفهوم هذا الدليل الرقمي والصعوبات الخاصة به قبل أن نحكم عليه ونبين قيمته القانونية.

المطلب الأول : مفهوم الدليل الرقمي والصعوبات المتعلقة به.

أولاً: تعريف الدليل الجنائي الرقمي.

ينصرف مفهوم الدليل الجنائي ابتداءً إلى "الوسائل التي يستعين بها القاضي للوصول إلى الحقيقة التي ينشدها"^(٢)، أو "هو كل ما يتعلق بالواقعة المعروضة على القاضي لإعمال حكم القانون عليها"^(٣)؛ في حين يذهب إلى بعض إلى تعريفه بأنه "كل معنى يدرك من مضمون واقعة تؤدي إلى إثبات البراءة أو الإدانة باستخدام الاسلوب العقلي وإعمال المنطق

في وزن وتقدير تلك الواقعة ليصبح المعنى المستمد منها أكثر دقة ودلالة على البراءة أو الإدانة".^(٤)

أما الدليل الرقمي فيُعرف بأنه "كل بيانات يمكن اعدادها أو تخزينها في شكل رقمي بحيث تمكن الحاسوب من انجاز مهمة ما"^(٥)، وعرفته المنظمة الدولية لأدلة الحاسوب بأنه "المعلومات المخزنة أو المتنقلة في شكل ثانوي ويمكن أن يعتمد عليها في المحكمة" كما عرفه آخرون على نحو أدق بأنه "الدليل المشتق من أو بواسطة النظم البرمجية المعلوماتية الحاسوبية وأجهزة ومعدات الحاسوب الآلي أو شبكات الاتصال من خلال إجراءات قانونية وفية لتقديمها للقضاء بعد تحليلها علمياً أو تفسيرها بشكل نصوص مكتوبة أو رسومات أو صور أو اشكال واصوات لإثبات وقوع جريمة لتقرير البراءة أو الإدانة فيها".^(٦)

و بما أن الجرائم المتصلة بالإنترنت تقوم على أساس استخدام تقنيات المعلومات والاتصالات الحديثة فلا يمكن تصور وقوع هذه الجرائم إلا من خلال وسائل وأجهزة تسمح باستخدام هذه التقنية؛ ولهذا تشتمل الأدلة الإلكترونية الرقمية بالنظر إلى طبيعتها على نوعين رئيسيين : يتمثل الأول بالأدلة المادية المستخدمة في هذه الجرائم كجهاز الحاسوب الآلي وأجهزة الهواتف النقالة ووسائل ربط الأجهزة مع بعضها من خلال شبكة الإنترت (المودم) واقراص التخزين الثابتة والمتحركة وغيرها التي يمكن أن تستخلص منها المعلومة؛ وتأخذ هذه الأدلة حكم الأدلة المادية العادية فقد تكون معبرة بذاتها عن معنى ما لإثبات الواقعة المنظورة أمام القضاء؛ أو قد تحتاج لدليل آخر لإثبات استخدامها في ارتكاب جريمة معينة فلا يجدي ضبط جهاز حاسوب ما أو هاتف نقال ما لم يثبت استخدامه كوسيلة في ارتكاب الجريمة؛ وأما النوع الثاني فهي الأدلة الإلكترونية المعنوية المتمثلة ببيانات المخزنة أو المتنقلة بصيغة رقمية المأخوذة من جهاز الحاسوب الآلي وملحقاته وعادة ما تكون بصيغة مجالات أو نبضات مغناطيسية من الممكن تجميعها أو تحليلها باستخدام تطبيقات وتقنيات خاصة؛ و تتعلق الصعوبات بهذا النوع من الأدلة بشكل كبير بالنظر إلى طبيعتها المعنوية وصعوبة استخلاصها

وغيرها كما سنرى لاحقاً، وعلى هدي مما سبق يمكن أن نجمل ابرز الخصائص التي يتميز بها الدليل الالكتروني :

١. الدليل الالكتروني دليل علمي تقني: "فالدليل الالكتروني دليل مشتق من بيئة تقنية رقمية تقوم على أساس تخزين البيانات والمعلومات التي تستقبلها أو عية التخزين في الحاسوب الآلي وما في حكمه بشكل نبضات واسارات كهربائية ناتجة عن استخدام لوحة المفاتيح أو غيرها بشكل مجموعات رقمية متكررة من رقمي الصفر والواحد حيث تعبّر كل مجموعة الأحاد والأصفار عن بيان أو معلومة بعينها"^(٧); واستخلاص الدليل من هذه البيئة الرقمية لابد من اتباع ذات القواعد العلمية التي تعتمد عليه الوسائل الأخرى في استخلاص المعلومات أو البيانات وهذا ما يكسب الدليل الرقمي طابعاً علمياً بحثاً.
٢. الدليل الالكتروني دليل متتنوع ومتتطور: فلا يعدو أن يكون الدليل الالكتروني سوى غالباً يحوي من مجموعة من البيانات الرقمية منفردة أو مجتمعة تتحذ أشكالاً متتنوعة تتضمن نصوصاً مكتوبة أو صوراً ورسومات وسمعيات ومرئيات، تصلح لأن يستند إليها القاضي عند تقرير البراءة أو الإدانة، مستقاة من بيئة متطرفة بطبيعتها قابلة لابتکار المزيد من المظاهر الرقمية؛ سيما وأن المبدأ السائد في العالم الرقمي أنه لا يزال في بداياته ولم يصل بعد إلى منتهاه وهذا ما يفرض طبيعة التطور في الأدلة المستمدّة منه.
٣. الدليل الالكتروني دليل يصعب التخلص منه : وتعد من أهم الخصائص التي يتتصف بها الدليل الالكتروني بخلاف الأدلة التقليدية التي غالباً ما تكون قابلة للتخلص منها ك بصمات الأصابع وآثار الأقدام أو الشرائط المسجلة والأوراق وغيرها، بل ومن المستحيل استعادة الدليل المستمد منها بعد إتلافها؛ أما بشأن الأدلة الرقمية فهي على العكس من ذلك تماماً فلا تحول وسائل التخلص من الملفات المعروفة دون استردادها بعد الغائها أو إزالتها من الحاسوب مرة أخرى من خلال برامج تقنية معينة^(٨).

ثانياً. الصعوبات المتعلقة بالدليل الإلكتروني :

تقف أمام مكافحة الجريمة المعلوماتية صعوبات إجرائية كثيرة غير أنها ستفتقر هنا على تلك الصعوبات الخاصة بالدليل الرقمي مرجئين الحديث عن الصعوبات الأخرى كل في محله في المباحث القادمة؛ وفيما يخص الصعوبات الخاصة بالدليل الرقمي فيمكن ارجاعها إلى قسمين يتعلق الأول بالدليل الرقمي ذاته، والآخر بإجراءات الحصول عليه نبينها على النحو التالي :

١. الصعوبات الخاصة بالدليل الرقمي نفسه : وتأتي هذه الصعوبات من البيئة التي يستمد منها هذا الدليل التي تقوم على أساس المعلومات التي تتحرك وتنساب عبر الحواسيب الآلية والشبكات بشكل نبضات الكترونية غير مرئية مما يكسب الدليل الرقمي ميزة التخفي، وليت الأمر يقف عند هذا الحد بل غالباً ما تكون هذه المعلومات مشفرة أو مرمزة يصعب الوصول إليها خصوصاً إذا كانت معلومات خاصة أو خطيرة؛ وعلى الرغم من اعتماد بعض المؤسسات ذات الأنظمة المعلوماتية في حماية هذه الأنظمة على طريق التشفير أو الترميز وغيرها من وسائل الحماية إلا بعض المجرمين المتخصصين قد يتمكنون من اختراق هذه الأنظمة وبالتالي تصبح حمايتها من غير جدوى سيما لو كانوا من العاملين داخل المؤسسة^(٩).

٢. الصعوبات المتعلقة بإجراءات الحصول على الدليل الرقمي: وتأتي في مقدمتها انخفاض مستوى مهارة وخبرة الجهات القائمة على التحقيق فغالباً ما يتم التحقيق في هذه الجرائم من قبل المحققين واعضاء الضبط القضائي الذين يفتقدون للخبرة في مجال التعامل مع الجريمة المعلوماتية، ولهذا انطلقت الدعوات إلى منح صفة الضبطية القضائية للعاملين في مجال تقنية المعلومات سواء كانوا من رجال الأمن أو من المتعاملين مع السلطات المختصة؛ ويضاف إلى ذلك تضاؤل أهمية المعاينة والكشف في الجرائم المعلوماتية نظراً لعدم تركها أي اثر مادي، وكثرة الاشخاص الذين يردون إلى مسرح الجريمة خلال الفترة الواقعة بين وقوع الجريمة وحتى اكتشافها أو التحقيق فيها مما يعطي الجاني الفرصة في

أن يغير أو يتلف الآثار المادية للجريمة أن وجدت مما يورث الشك في دلالة الأدلة المستقاة من المعاينة والفحص في هذه الجريمة، ناهيك عن الإسقاط الامني التي يضرها الجناء حول افعالهم والوسائل التي يلجأون للحيلولة دون كشفها كما لو استخدم الجاني حاسباً آخر غير حاسبه الشخصي أو الحواسيب الموجودة بالأماكن العامة أو في مقاهي الإنترنت لاسيما إذا علمنا أن شبكة الإنترنت تتيح استعمال الخط الواحد من قبل أكثر من شخص في وقت واحد، حيث يعد مجال تقنية المعلومات مجال استثمار مريح ولهذا تتسابق الشركات في تبسيط الإجراءات وتسهيل استخدام البرامج والاجهزة وملحقاتها واقتصار التركيز على الخدمة دون الجانب الامني فلا يطلب من مستخدمي شبكة الإنترنت عبر البطاقات المدفوعة أو مزودي الخدمة بتحديد هوياتهم ما يجعل المراقبة والتعقب للمشتبه فيه أمراً ينطوي على صعوبة كبيرة، وربما تتعقد المسألة أكثر عند استخدام الإنترنت اللاسلكي^(١٠).

المطلب الثاني : سلطة القاضي في تقدير الدليل الرقمي

تفاوت سلطة القاضي الجنائي في تقدير الدليل الرقمي بحسب طبيعة نظام الإثبات المعتمد من جهة وعلى طبيعة الدليل المعروض أمام القضاء من جهة أخرى؛ وسنعرض لمدى هذه السلطة وتأثيرها بما تقدم من عوامل على نحو مما يأتي:

أولاً. طبيعة أنظمة الإثبات

تحتفل سلطة القاضي في تقدير الأدلة المعروضة أمامه تبعاً لاختلاف أنظمة الإثبات المعتمدة في التشريعات من دولة إلى أخرى والتي ترجع إلى نظامين رئيسين وآخر حديث نسبياً، نلخصها كالتالي:

١. نظام الإثبات المقيد (نظام الأدلة القانونية): ونجد فيه "أن المشرع هو الذي يحدد للقاضي الأدلة التي يجوز له قبولها في حالة معينة، ويحظر عليه قبول ما سواها وإن كان يجوز له قبولها في حالة أخرى معينة، وكذلك يحدد المشرف القيمة القانونية للأدلة إذا توافرت شروطها وعندها يلتزم القاضي بالأخذ به وليس له رفضه"^(١١)، بمعنى آخر أن دور

القاضي هنا يقتصر فقط على تقدير توافر الشروط التي حددتها المشرع مسبقاً والحكم بالقيمة القانونية لهذا الدليل في الإثبات، وهذا ما يفرض على المشرع أن يتدخل ويحدد ما يراه أساسياً في واقعة معينة لتنتج المعنى المطلوب لتقرير البراءة أو الإدانة، ونجد أن هذا النظام وإن كان يستقيم إلى حد ما والاثبات المدني إلا أنه لا يمكن الأخذ في الإثبات الجنائي وخصوصاً في إطار الإثبات بالأدلة الرقمية التي تتسم بالتنوع والتطور، فما قد يقرره المشرع من شروط في الدليل الرقمي اليوم قد لا تكون مقبولة أو متخلفة عن ما وصلت إليه التقنية الرقمية مستقبلاً.

٢. نظام الإثبات الحر (نظام الاقتضاء الذاتي) : وفيه "يترك للقاضي الحرية في أن يؤسس حكمه على أي دليل وفقاً لاقتناعه الشخصي دون أن يفرض عليه دليل بعينه والاعتراف له بسلطة تقدير قيمة الدليل أو قيمة الأدلة مجتمعة"^(١٢)، بمعنى أن للقاضي أن يستمد من الواقع المعروضة أمامه ما يمكن أن يشكل دليلاً من خلال استنتاج قائم على أساس العقل والمنطق، ونجد بأن هذا النظام أكثر اتساقاً مع طبيعة الإثبات الجنائي فالحرية التي يتمتع ضروريّة لقابليتها على استيعاب التطورات الحاصلة في الإثبات بالأدلة الرقمية واختلاف انواعه وقيمتها القانونية مما يفرض منح القاضي سلطة وصلاحية تتيح له تقدير كل دليل على حدة، ويسود هذا النظام في اغلب التشريعات الجزائية ومن ضمنها المشرع العراقي حيث تنص المادة (٢١٣/أ) من قانون أصول المحاكمات الجزائية العراقي على أنه: (تحكم المحكمة في الدعوى بناء على اقتناعها الذي تكون لديها من الأدلة المقدمة في أي دور من أدوار التحقيق أو المحاكمة وهي الاقرار وشهادة الشهود ومحاضر التحقيق والمحاضر والكشفوف الرسمية الأخرى وتقارير الخبراء والفنين والقرائن والادلة الأخرى المقررة قانوناً).

والملاحظ على هذا النص أن المشرع العراقي اعطى للمحكمة أن تستمد قناعتها من أي دليل يقدم إليها في مراحل الدعوى وهذا إطلاق يشمل الأدلة الرقمية أيضاً، فالأدلة الواردة في هذا النص ليست على سبيل الحصر كما يرى جانب من الفقه وإنما اقتصر

المشرع عليها بحكم شيوخها وغالبية الاستعانة بها أمام المحاكم، كما أن المشرع عاد وأتى بلفظ عام في ذيل هذه المادة عندما أقر قبول الأدلة الأخرى المقررة قانوناً^(١٣).

٣. نظام الإثبات العلمي : وهو "نظام يقوم على أساس الاستعانة بأساليب الفنية التي كشف عنها العلم الحديث في إثبات الجريمة ونسبتها إلى المتهم، فيعطي الدور الرئيس في إثبات الجريمة للخبر، ويجعل أهم الأدلة هي القرآن التي تخضع للفحص العلمي الدقيق لاستخراج ما يثبت البراءة أو الإدانة منها"^(١٤)؛ والملاحظ هنا أن سلطة القاضي في تقدير الأدلة تنحصر وتقتيد إلى حد كبير ذلك بالاستغناء عن عملية الاستدلال المنطقي والعقلي التي يقوم بها القاضي والاستعانة باستدلال علمي يقوم على أساس قواعد علمية وفنية متعلقة بفرع من فروع المعرفة ومن بينها طبعاً تقنية المعلومات؛ لكن نجد أنه من غير الممكن استبعاد مبدأ الاقتناع الشخصي تماماً من عملية الإثبات، فقد ينعدم الدليل العلمي وهنا لا مناص من اللجوء إلى الأدلة العادلة الأخرى كالقرآن والشهادة وغيرها والتي يمارس القاضي بتصديقها سلطتها التقديرية كاملة، فضلاً عن ذلك نجد أن هناك مساحة لسلطة القاضي في تقدير الخبرة وتقدير الدليل العلمي الناجم عنها حتى في ظل التشريعات التي تأخذ بنظام الإثبات العلمي؛ فليس كل دليل علمي مقبول قانوناً في الإثبات، فقد تظهر أدلة علمية دقيقة جداً من حيث مطابقتها للحقيقة بفضل التطورات العلمية والتقنية وفي المجالات كافة لكنها قد تصطدم بالمبادئ العامة والحقوق الأساسية التي كفلتها الدساتير والقوانين مما يتلزم أن يكون للقاضي سلطة تحوله تحديد ما يمكن قبوله من الأدلة العلمية أمام المحكمة من عدم ذلك.

ثانياً. طبيعة الدليل الرقمي.

يستمد الدليل الرقمي من المركبات المادية للحاسب الآلي وملحقاته ويقصد بها الأجزاء المادية (الصلبة) والمعنوية (البرامج) التي يتوصل بها الجاني لتنفيذ جريمته طبعاً عبر شبكة الإنترنت، غير أن الأمر لا يتعلق بهذه المكونات - بوصفها أشياء مادية تخضع للقواعد العامة المتعلقة بالدليل المادي العادي – قدر تعلقه بإثبات الانشطة الجرمية التي تمت من

خلالها والذي لا يتم إلا بواسطة مخرجات الحاسب الآلي وملحقاته أو من خلال الأدلة العلمية والتي لا يمكن التوصل إليها إلا من خلال فحص نظام الاتصال بالإنترنت، فإلى أي مدى يمكن للقاضي أن يستند إلى هذه المخرجات لبني حكمه على أساسها وإلى أي مدى يمكن له قبول الدليل العلمي لإثبات استخدام هذه المكونات في جريمة معلوماتية، هو ما يفرض علينا مناقشة الأمور التالية :

١. مدى قبول مخرجات الحاسب الآلي أو ملحقاته كأدلة جنائية : وتمثل هذه المخرجات بالبيانات أو المعلومات الموجودة على سطح المكتب في الحاسب الآلي أو المعلومات المثبتة في أقراص ليزرية أو ساعات التخزين المختلفة مهما كانت طبيعتها سواءً أكانت نصوصاً مكتوبة أو صوراً أو فيديوهات أو غيرها، ولا تشير هذه المخرجات أشكالاً كبيرةً في ظل الأنظمة القضائية التي تعتقد مبدأ الاقتضاء الذاتي للقاضي كالقضاء العراقي الذي اعتمد على هذه المخرجات كتسجيل مكالمات الهاتف النقال الدائرة بين المشتكي والجناة المؤثقة من قبل شركة اثير للاتصالات^(١٥)؛ ولكن يبقى في ظل هذه الأنظمة بمقدور القاضي قبول هذه الأدلة أو مناقشتها والاستعانة بالخبرة لتأكد من مدى صدقيتها أو ومطابقتها للحقيقة ورفضها أن لم يتحقق ذلك؛ ولكن قد يتعقد الأمر في ظل الأنظمة التي تعتمد الإثبات بالشهادة كمبدأ اساسي كالأنظمة الانجلو – أميركية، ولذلك فإن قبول المستندات المطبوعة لمخرجات الوسائل الإلكترونية التي تتجسد بشكل نبضات أو اشارات ممغنطة يشكل عقبة أمام القضاء لعدم تمكן القاضي أو المحلفين من معاينة الأدلة المتولدة منها أو وضع اليد عليها مما يجعلها أدلة ثانوية وليس أصلية^(١٦).
وأزاء هذا الوضع ونظرًا لتعاظم دور التقنية المعلوماتية والوسائل الإلكترونية فقد بادرت تشريعات هذه الدول التي تغير موقفها السابق وقبلت مخرجات هذه الوسائل كأدلة للإثبات وأن قيدت ذلك بعض الشروط.^(١٧)
٢. قيمة الدليل العلمي في الإثبات الجنائي : قد يستمد الدليل الرقمي من الحاسب الآلي أو ملحقاته من خلال استخراج أو استرداد البيانات أو المعلومات وتجسيدها بصيغة معينة

يمكن معها للمحكمة أن تقف على مدى مطابقتها للحقيقة، وقد يتعلّق الدليل الرقمي بواقعة معينة لا يمكن التوصل إليها إلا بفحص نظام الاتصال بالإنترنت من خلال برامج وتطبيقات معينة؛ لذا فالدليل العلمي الرقمي هنا ليس سوى نتائج يسفر عنها استخدام برامج وتطبيقات الكترونية تقنية معينة من قبل المختصين من ذوي الخبرة في هذا المجال تعزز قناعة المحكمة بشبهة واقعة محل شك أو نفيها، ويطلب بناءً على رغبة المحكمة أو بطلب من أحد الخصوم.

وأما بخصوص القيمة القانونية للدليل العلمي الرقمي في الإثبات فيرى بعض الباحثين اعطاء هذا الدليل دلالة قانونية قاطعة ويدعو إلى اعتماده من قبل المحكمة كدليل كافي لإثبات الإدانة أو البراءة ولو جاء مفرداً من غير أدلة أخرى تدعمه، ويبعد أصحاب هذا الرأي توجّههم هذا بالنظر إلى صعوبة استخلاص الأدلة في البيئة الرقمية من جهة ونقص الكوادر المتخصصة وانخفاض كفاءتها من جهة أخرى، فضلاً عن أن القول بخلاف ذلك يؤدي إلى افلات الكثير من الجنحة^(١٨).

في حين يفرق رأي آخر بين أمرين "الأول هو القيمة القانونية القاطعة للدليل، والأمر الثاني هو الظروف والملابسات التي وُجد فيها الدليل. فتقدير القاضي لا يتناول الأمر الأول لأن قيمة الدليل تقوم على أساس علمية دقيقة ولا حرية للقاضي في مناقشة الحقائق العلمية. أما الظروف والملابسات التي وُجد فيها الدليل فإنها تدخل في نطاق السلطة التقديرية الشخصية للقاضي؛ فهي من طبيعة عمله بحيث يمكن أن يطرح هذا الدليل رغم قطعيته من الناحية العلمية عندما يلاحظ القاضي أن وجوده لا يستقيم مع ظروف الواقعه وملابساتها"^(١٩)، وفي ضوء ما تقدم نجد من غير الممكن تجاهل أهمية الدليل الرقمي العلمي كونه الأكثر تناسباً في إثبات الجرائم المعلوماتية في ظل تعقيد الأدلة الناجمة عنها وصعوبة التوصل إليها؛ فإن قيل بأن الدليل الرقمي يقتصر على الاستناد المادي للنشاط الجرمي إلى جهاز الحاسب الآلي أو أي وسيلة من وسائل الاتصال الحديثة بشبكة الإنترت ولا يمكن من تحديد شخصية الجاني، ردّ على ذلك بأنه من غير المستبعد أن يعلو شأن الأدلة الرقمية كغيرها من

الأدلة العلمية كالبصمة الوراثية وغيرها فقد يتمكن الدليل الرقمي مستقبلاً من ذلك سيما ونحن في بيئة معلوماتية رقمية يعد التطور من أبرز سماتها؛ ولا يعني هذا بأي حال حرمان القاضي من سلطته التقديرية التي قد تكون لازمة لتشذيب الدليل الرقمي وتطويعه بما يضمن أن تكون الحقيقة العلمية قضائية أيضاً.

المبحث الثاني

التفتيش في البيئة الرقمية

يقصد بالتفتيش ابتداءً الإطلاع على محل منحه القانون حرمة خاصة لضبط ما عسى قد يوجد فيه مما يفيد في كشف الحقيقة عن جريمة معينة^(٣٠)، أو عبارة عن إجراء من إجراءات التحقيق التي تهدف إلى البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة بهدف إثبات ارتكابها أو نسبتها إلى متهم ما وفقاً لإجراءات محددة^(٣١)؛ وفي إطار الجريمة المعلوماتية ينصرف التفتيش إلى الولوج إلى مكونات الحاسب الآلي وملحقاته للبحث عن ما يتصل بجريمة معلوماتية وقعت أو يفيد في الكشف عنها، وكما هو معلوم فإن قوام الجريمة المعلوماتية هو جهاز حاسب آلي - أو ما في حكمه - موصول بشبكات الاتصال يمكن من خلاله الجاني من بلوغ غاياته، فإلى أي مدى تصلح مكونات الحاسب الآلي للتفتيش؟ وإلى أي مدى يمكن تفتيش شبكات الاتصال بالحاسوب الآلي؟ وهذا ما سنحاول الإجابة عليه فيما يأتي:

المطلب الأول : مدى صلاحية مكونات الحاسب الآلي للتفتيش

من المعلوم أن جهاز الحاسوب الآلي يتكون من مركبات مادية و أخرى معنوية، وفي صدد تفتيش الحاسوب الآلي نجد أن مركبات الحاسوب الآلي المادية وما يلحق بها من اجهزة وكذلك المعلومات المخزنة في أوعية التخزين الثابتة كالقرص الصلب في جهاز الحاسوب الآلي أو الأوعية المنفصلة كالأقراص المرنّة وغيرها، لا تشير إشكالاً لهذه المركبات المادية بل

والمعلومات أيضاً متى اتخدت مظهراً مادياً ملمساً تخضع للقواعد الاجرائية العامة في التفتيش وذلك بحسب المكان أو الحيز الذي توجد فيه، فيحكمها ما يحكم الاماكن والأشخاص أن هي وجدت في منزل المتهم أو ملحقاته أو في أماكن عامة، أو وجدت في الحيز الشخصي للمتهم.^(٢٢)

ولكن الفقه اختلف بشأن التفتيش عندما يرد على المكونات المعنية المتمثلة بالبيانات بمختلف أشكالها المستخرجة من جهاز الحاسب الآلي من خلال تقنيات فنية معقدة؛ فيذهب رأي إلى "جواز ضبط البيانات على مختلف انواعها ويجد هذا الرأي أساسه في أن القوانين الاجرائية غالباً ما تنص على ضبط أي شيء يمكن أن يسهم في كشف الحقيقة عن جريمة ما، وهذا النص من الاتساع ما يسمح بتفسيره على نحو يشمل البيانات المخزنة أو تلك المعالجة الكترونياً"^(٢٣)؛ كنص المادة (٤٨٧) من القانون الكندي التي "تمنح سلطة اصدار إذن الضبط لأي شيء طالما توافرت أسس معقولة للاعتقاد بأن جريمة قد وقعت أو يشتبه في وقوعها أو أن هناك نية ارتكاب جريمة بواسطته أو سوف ينتج دليلاً على وقوع الجريمة". وكذلك المشرع اليوناني الذي خول سلطات التحقيق امكانية القيان بأي شيء ضروري لجمع وحماية الدليل الجنائي بموجب المادة (٢٥١) من قانون الإجراءات الجنائية^(٢٤)؛ ونجد من مثل هذا النص كذلك في قانون أصول المحاكمات الجزائية العراقي حيث تقضي المادة (٧٨) من هذا القانون على أنه : (لا يجوز التفتيش إلا بحثاً عن الاشياء التي أُجري التفتيش من أجلها).

بينما ذهب رأي آخر إلى "عدم انطباق المفهوم المادي على بيانات الحاسب الآلي غير المرئية، ويرى ذلك نصاً تشرعياً يستلزم التعديل والنص صراحة على أن يشمل التفتيش المواد والبيانات المعالجة الكترونياً عن طريق الحاسب الآلي، بحيث تصبح الغاية الجديدة من التفتيش بعد التطور التقني وثورة الاتصالات لا تقتصر على الأدلة المادية بل تشمل أيضاً البيانات المعالجة عبر الحاسب الآلي".^(٢٥).

ففي التشريع الأمريكي على سبيل المثال تقضي المادة (٣٤) من القواعد الفيدرالية الخاصة بالإجراءات الجنائية الصادرة سنة ١٩٧٠ بعد تعديلها بمد نطاق التفتيش ليشمل ضمن ما يشمل أجهزة الحاسب الآلي وأوعية التخزين والبريد الإلكتروني والصوتي والمنقول عن طريق الفاكس؛ فضلاً عن أن الاتفاقية الأوروبية للجريمة الافتراضية (اتفاقية بودابست) تقضي في المادة (١٩) منها بإلزام الدول الأطراف في هذه الاتفاقية بضرورة تبني التدابير والإجراءات التشريعية التي تخول السلطات المختصة ولوج البيئة المعلوماتية، وذلك من أجل تيسير إثبات هذه الجرائم.^(٢٦)

ويذهب رأي آخر إلى أنه "يجب الرجوع في تحديد مدلول الشيء إلى العلوم الطبيعية، حيث تتمثل المادة في هذه العلوم بكل ما يشغل حيزاً مادياً في فراغ معين ويمكن قياس ذلك الحيز والتحكم فيه، وهو ما ينطبق على بيانات الحاسب الآلي، لذا فهي تعد من الأشياء المادية التي يمكن أن تكون محلاً للتفتيش، أسوة بالطاقة الكهربائية التي عدتها اغلب التشريعات من قبيل الأشياء المادية التي يمكن أن تكون محلاً لجريمة السرقة".^(٢٧)

في حين نأى جانب من الفقه عن البحث في دلالات النصوص والخوض في تفسيراتها وانطلق من منظور واقعي الذي يتطلب بطبيعة الحال أن تتخذ هذه البيانات شكلاً مادياً كي يتم ضبطها وتقديمها للقضاء، وبالتالي فهو يرى أن التفتيش يقع على مكونات الحاسب الآلي ويشمل أيضاً البيانات مضافة إلى الدعامتين التي يمكن أن تحملها مهما كان شكلها؛ وتبني هذا الاتجاه المشرع الألماني إذ اشترط أن تكون الأدلة المضبوطة ملموسة وذلك بمقتضى المادة (٩٤) من قانون الإجراءات الجنائية^(٢٨). ويعد هذا الرأي في تقديرينا من أكثر الآراء اتساقاً والبيئة التي يتم التفتيش فيها، فلا مبرر من الاقتصار على الأدلة المادية في التفتيش طالما بالإمكان أن يوجد دليل معنوي يؤدي إلى كشف الحقيقة في جريمة معلوماتية معينة يمكن التوصل إليه من خلال اتباع تقنيات فنية معينة واستخراجها بهيئة أو شكل مادي يمكن تقديمها وأثباتها أمام القضاء، على أن ذلك لا يعني طبعاً عن معالجة القصور التشريعي لموضوع

التفتيش في الجرائم المعلوماتية خصوصاً ما يتعلق بتحديد الضوابط الشكلية والموضوعية ومحل التفتيش وبما يتلاءم وطبيعة هذه الجرائم.

ويرى آخرون أن الأخذ بالأراء التي تجيز أن يقع التفتيش على بيانات الحاسب الآلي فيه اعتداء على حقوق الملكية الفكرية لمالك الحاسب الآلي، إذ سيأتي التفتيش على مركبات الحاسب الآلي المعنوية بما فيها من معلومات وبرمجيات وبيانات التي قد تكون خاضعة للحماية الجنائية لحق المؤلف.

بينما يذهب رأي إلى "أن هذه البرمجيات والبيانات إن كانت مبتكرة فمن الطبيعي أن تخضع للحماية الجنائية لكن ما نحن بصدده إثباته هنا هو استخدام هذه البرمجيات التي يمكن أن تستغل فيها لارتكاب جرائم معلوماتية معينة كالسرقة والاتلاف والتزوير والاختراق والبقاء غير المصرح فيه وغيرها؛ ويستدل على ذلك بموقف المشرع الفرنسي الذي عاقب على الأفعال غير المشروعة التي تقع على البيانات المعالجة إلكترونياً في قانون العقوبات لسنة ١٩٩٤ بعيداً عن قانون حماية الملكية الفكرية حيث قضت الفقرة الأولى من المادة (٣٢٣) بتجريم الدخول أو البقاء غير المشروع في نظام المعالجة الآلية لمعطيات الحاسب الآلي وشددت العقوبة إذا نتج عن هذا البقاء تعديل البيانات الموجودة داخل النظام أو إفساد وظيفته".^(٢٩)

المطلب الثاني : تفتيش شبكات الاتصال بالحاسوب الآلي

قد يطال التفتيش أماكن أخرى غير مكان حاسوب المتهم وذلك في إطار السعي وراء البيانات التي يمكن أن تنتشر خلال الشبكة إلى أماكن بعيدة بفضل تقنيات الاتصال والمعلومات، فقد اتاحت هذه التقنيات لسلطات الضبط القضائي الكشف عن بعد عن محتويات أي حاسوب متصل بشبكة الإنترنت مما يطرح تساؤلاً حول مدى خضوع شبكات الاتصال للتفتيش، وهذا ما يفرض التمييز بين الفروض التالية:

أولاً : اتصال حاسب المتهم بحاسب آخر أو نهاية طرفية موجودة داخل إقليم الدولة:

لا يشير هذا الفرض إشكالاً كبيراً طالما أن الأماكن التي وُجد فيها حاسب المتهم أو الحاسب الآخر المرتبط به الذي قد يطاله التفتيش خاضع لنظام قانوني واحد، وتکاد تجمع التشريعات الاجرائية - سواء بالنسبة للقواعد الاجرائية العامة أو القواعد الاجرائية الخاصة بالجرائم المعلوماتية - على جواز امتداد التفتيش لمناطق أخرى غير واردة في أمر التفتيش ولو وقع ذلك بدون إذن صادر من جهة مختصة ولكنها تقيدها بضوابط معينة، وقد تبنت معظم التشريعات هذا الاتجاه ومنها قانون اصول تحقيق الجنائيات البلجيكي لسنة ٢٠٠٠ الذي أجاز امتداد التفتيش إلى نظام معلوماتي آخر غير مكان البحث الأصلي، ولكن ليس بصورة مطلقة وإنما بقيود معينة، يمكن إجمالها في أن تكون ثمة ضرورة لكشف الحقيقة فيما يخص الجريمة موضوع البحث أو أن تكون الأدلة معرضة لمخاطر معينة كالإتلاف أو التدمير وما شابه، كما وأقرت الاتفاقية الأوروبية للجرائم المعلوماتية ذلك متى كانت المعلومات المخزنة بمحاسوب غير المتهم يتم الدخول إليها من خلال الحاسب الأصلي محل التفتيش^(٣).

وبالانتقال إلى موقف المشرع العراقي نجد مثل هذا الجواز بامتداد التفتيش ولو خارج منطقة اختصاص القاضي بمقتضى المادة (٨٥) من قانون اصول المحاكمات الجزائية العراقي على أن يراجع قاضي التحقيق المختص في تلك المنطقة، وفي الحالات المستعجلة يمكن تنفيذ أمر التفتيش بشكل مباشر ثم يتم اخبار القاضي المراد تنفيذ أمر التفتيش في منطقته، ونجد بأن هذه حالة الضرورة والاستعجال التي استلزمت قيامها اغلب التشريعات قائمة خصوصاً في إطار الجرائم المعلوماتية وذلك لسهولة محو وإتلاف أو نقل البيانات محل التفتيش الذي قد يصل الحال فيها إلى إتلاف الحاسب الآلي نفسه الذي يحتوي مثل هذه البيانات مما يفرض السرعة في التعامل مع هذه الجرائم التي قد يقف الحصول على الإذن بالتفتيش حائلاً دون ذلك.

ثانياً : اتصال حاسب المتهم بحاسب آخر أو نهاية طرفية موجودة خارج إقليم الدولة :
قد يمتد التفتيش في إطار الجرائم المعلوماتية إلى خارج حدود إقليم الدولة، وذلك بفضل تقنية المعلومات التي تتيح للجناة تخزين بياناتهم ومعلوماتهم خارج حدود الدولة عبر شبكات الاتصال بهدف تضليل وعرقلة سير التحقيقات، واحتلّ الفقه أراء هذا الوضع وانقسم إلى أراء متعددة واحتلّت التشريعات تبعاً لذلك؛ فذهب رأي إلى "جواز امتداد التفتيش الإلكتروني خارج حدود إقليم الدولة دون الحاجة إلى استئذان الدولة التي امتد التفتيش عبر شبكة الاتصال فيها والحواسيب المرتبطة بها منطلقاً في ذلك من الواقع التي تفرضه الجريمة المعلوماتية وما تشيره من معوقات أمام التفتيش؛ إذ يؤدي انتظار الحصول على الإذن من الدولة التي امتد إليها التفتيش قد يؤدي إلى افراج التفتيش من مضمونه نظراً لتمكن الجناة من محو الأدلة وإخفاء معالم جرائمهم"^(٣١).

ومن التشريعات التي اخذت بهذا الرأي المشرع الفرنسي في المادة (١٧) من قانون الأمن الداخلي الفرنسي التي اجازت لقاضي التحقيق اخذ نسخة من البيانات التي يحتاجها للكشف عن جريمة معلوماتية ما دون انتظار الحصول على الإذن، وقضى قانون التحقيق البلجيكي بمثل ذلك؛ ونلاحظ بأن هذا الاتجاه من الفقه يحاول أن يؤسس لقواعد جديدة في ظل المتغيرات الحاصلة في مسرح الجريمة والطبيعة الافتراضية الرقمية التي يتسم بها. إلا أنه لا يزال يصطدم بمبدأ السيادة الذي يعد مثل هذا الأمر انتهاكاً صريحاً له.

في حين يرى رأي آخر بأن التفتيش الإلكتروني خارج حدود إقليم الدولة لا يمكن أن يتم إلا في إطار اتفاقيات دولية خاصة ثنائية أو عامة تجيز هذا الامتداد أو على الأقل بعد الحصول على الإذن، ويسود هذا الرأي في الفقه الألماني.^(٣٢)

في حين سلك اتجاه آخر طريقاً وسطاً فهو أقر بدءاً عدم جواز التفتيش الإلكتروني خارج حدود الإقليم كمبدأ عام إلا بعد الحصول على إذن، إلا أنه أورد بعض الاستثناءات لظروف معينة يقتضيها التفتيش، وأخذ بهذا لاتجاه المجلس الأوروبي في الاتفاقية الخاصة بالجريمة المعلوماتية الموقعة في بودابست عام ٢٠٠١ حيث قضت المادة (١٧) بجواز

التفتيش والضبط في اجهزة وشبكات تابعة لدولة أخرى بدون أذنها في حالتين، الأولى : إذا تعلق التفتيش بمعلومات أو بيانات متاحة للجمهور؛ والثانية : إذا رضي صاحب الشأن أو حائز هذه البيانات بهذا التفتيش^(٣٣)، كما درجت المحاكم في اميركا على جواز التحلل من قاعدة الاستئذان إذا كان لدى مأمور الضبط القضائي شك في أن إعمال هذه القاعدة من شأنه أن يعيق فعلياً سير التحقيق أو من المتوقع أن تنجم عنه خطورة ما^(٣٤).

ونجد أن ايراد بعض الاستثناءات على القاعدة العامة بلزوم الحصول على موافقة أو إذن قد يكون ضرورياً للحول دون إفلات الجناة ولكن بشرط عدم التوسيع فيها وضمان عدم الاعتداء على الحريات الشخصية ولا ضير من أن تتم عملية التفتيش والضبط أمام انتظار ومراقبة الجهات القضائية في الدولة التي تمتد إليها أعمال التفتيش الالكتروني أو على الأقل إحاطتها علمًا بذلك.

ثالثاً: التنصت والمراقبة الإلكترونية لشبكات الاتصال :

بالرغم من كونها تشكل انتهاكاً صريحاً للحريات الفردية إلا اننا نجد معظم التشريعات تجيزها بضوابط معينة كضرورة استحصلال إذن من القاضي، وظهور ما يفيد تورط الجاني بجرائم خطيرة، ومن بين التشريعات تلك القانون الفرنسي الصادر ١٩٩١ الذي أجاز اعتراض شبكات الاتصال بما في ذلك شبكة المعلومات لمراقبة المكالمات والمراسلات المختلفة؛ وقضى على نحو من ذلك كل من القانون الاميركي والمصري وغيرها.^(٣٥)

أما بالنسبة لموقف المشرع العراقي فقد خلا قانون اصول المحاكمات الجزائية من النص على هذا الجواز، ولكن بالرجوع إلى الدستور العراقي نجده وبموجب المادة (٤٠) منه قد كفل من حيث المبدأ منه حرية الاتصالات والمراسلات البريدية والبرقية والهاتفية والإلكترونية وغيرها، لكنه مع ذلك أجاز مراقبتها والتنصت عليها أو الكشف عليها لظروفات قانونية أو أمنية، على أن يكون ذلك بقرار قضائي.

المبحث الثالث

الاختصاص في الجرائم المعلوماتية

يقصد بالاختصاص القضائي "السلطة التي يقررها القانون للقضاء في أن ينظر دعاوى معينة حددتها المشرع وفقاً لقواعد وإجراءات محددة"^(٣٦). وهذا ما يقتضي من المشرع الوطني أن يحدد مسبقاً الأفعال المجرمة والعقوبات المقررة لها متى ما وقعت ضمن نطاق معين يتمثل بحدود إقليم الدولة الخاضعة لقوانينها النافذة وفقاً لمبدأ الإقليمية، وتحظى هذه الأفعال بدورها لاختصاص المحاكم الوطنية التي تنبسط ولائيتها لتشمل كل الدعاوى الناشئة عن تلك الأفعال المجرمة على هذا الإقليم، وبال مقابل عدم سريان قانون الدولة وسلطان محاكمها خارج إقليمها كأصل عام، إلا على سبيل الاستثناء وفق ما تقتضيه ضرورات حماية صالح الدولة العليا أو ضرورات التعاون الدولي لمكافحة الجريمة.

ويتحدد القانون الواجب التطبيق في المكان الذي تقع فيه الجريمة الذي يكون هو ذاته مكان تحقق نتائجها الجنائية في الغالب الأعم من الحالات، بيد أن الأمر قد لا يسير على هذا النحو فقد تتجزأ عناصر الركن المادي للجريمة؛ فيقع السلوك الجرمي في مكان يختلف عن مكان تحقق نتائجها، بل وقد تتعدد أماكن وقوع الأفعال المكونة للسلوك الجرمي في الجريمة التقليدية بشكل عام والجريمة المعلوماتية بوجه خاص التي يعتبر الغايتها وعدم تقديرها بالحدود الإقليمية من ابرز سماتها، الأمر الذي يشير إشكالاً وتنازعاً في تحديد الاختصاص بنظر هذه الجرائم سواء على المستوى الدولي أو الداخلي، غير أن التنازع على المستوى الداخلي من السهولة التغلب عليه بالرجوع إلى القواعد القانونية التي نص عليها المشرع لمواجهة مثل هذه الحالات من التنازع، كما يقتصر التنازع الداخلي على الجانب الاجرامي فيما يتعلق بتحديد المحكمة المختصة ولا يمتد إلى الجانب الموضوعي لخضوع كامل إقليم لقانون عقابي موضوعي واحد.

إلا أن الأمر قد يدق ويعتقد أكثر في حال التنازع الدولي واتساع نطاق وقوع الجريمة ليشمل أكثر من دولة وأكثر من نظام قانوني عقابي معين، وقبل الخوض في موضوع تحديد الاختصاص في الجرائم المعلوماتية العابرة للحدود، نود أن نستعرض ابتداءً للمذاهب الفقهية والمبادئ المستقرة فقهاً وتشريعياً في هذا الصدد بهدف تقييمها وبيان مزاياها ومتالبها، نتطرق من بعدها للإشكاليات المتعلقة بتحديد الاختصاص والحلول المقترنة بخصوصها.

المطلب الأول : المبادئ العامة في تحديد الاختصاص

تحكم مسألة تحديد الاختصاص وتطبيق القواعد الجنائية من حيث المكان ثلاثة مبادئ رئيسية مستقرة في معظم التشريعات الجنائية المقارنة نبحثها على نحو مما يأتي :

أولاً : مبدأ إقليمية القاعدة الجنائية:

ويعد من أقدم المبادئ وأكثراها شيوعاً على مستوى التشريعات، ويفترض هذا المبدأ المعاقبة على كل الجرائم الواقعة على إقليم الدولة بغض النظر عن جنسية مرتكبيها؛ ولكن ما يثار التساؤل بشأنه هو وفقاً لأي قاعدة أو معيار تعد الجريمة مرتكبة على إقليم ما ؟

اختلف الفقه بهذا الشأن وانقسم إلى أكثر من رأي، فذهب رأي إلى "اعتماد مكان تحقق النشاط أو السلوك الإجرامي معياراً بتحديد مكان وقوع الجريمة وليس مكان تتحقق اثارها أو النتيجة الجنائية، ويرى أنصار هذا الاتجاه رأيهم بأن معيار مكان تتحقق النتيجة الجنائية يعد معياراً واسعاً مناً وتكتنفه بعض الصعوبات لاسيما في حال تعدد أماكن وقوع اثار السلوك الإجرامي، كما أن اعتماد معيار السلوك الإجرامي من شأنه تيسير عملية الإثبات وجمع الأدلة بحكم قرب المحكمة من مسرح الجريمة، يضاف إلى ذلك سهولة تنفيذ الأحكام وملاحقة الجناة، كما أن من شأن تطبيق قانون الدولة التي تحقق في نطاقها الضرر أو الآثار الجنائية لا يتفق واعتبارات العدالة نظراً لجهل الجاني بهذا القانون الذي يتم إعماله بحقه، وفي الغالب ليس ممكناً العلم به؛ إذ حينما أقدم على ارتكاب الفعل الذي أتاها يعتقد مشروعيته وفقاً لقانون البلد الذي وقع فيه السلوك، وإذا به غير ذلك من منظور قانون البلد الذي تحقق فيه الضرر^(٣٧).

إلا أن هذا الاتجاه قد تعرض لانتقادات عديدة انطلق منها المعارضون في ترجيحهم معيار مكان تحقق الآثار أو النتيجة الجرمية كمعيار لتحديد مكان وقوع الجريمة؛ فمما يؤخذ على الاتجاه السابق كونه "لا يغير اهتماماً للمكان الذي تتحقق فيه الضرر أو أثر النشاط الإجرامي الذي كان الجاني يسعى إلى تحقيقه فيه، فالآثار الضارة هي التي تبعث الفزع في نفوس الناس، في حين أن مكان وقوع السلوك لا يعدو أن يكون مصدر الضرر ليس إلا؛ كما أن تمام الجريمة لا يكون إلا في المكان الذي ظهرت فيه آثارها الضارة التي كان الجاني يقصدها أو يرغب في تحقيقها؛ كما يؤخذ في الحسبان جسامنة الضرر كأساس لتقدير التعويض ولا عبرة بخطورة الفعل أو درجة الخطأ؛ كذلك يعد حصول الضرر شرطاً أساسياً لقيام المسؤولية المدنية، فتنفي هذه المسؤولية متى ما انتفى الضرر، ومن ثم لا مصلحة للمدعي في الدعوى، ما يجعلها بالتالي غير مقبولة، كذلك يمتاز هذا الاتجاه في نظر المدافعين عنه بأنه أكثر واقعية على اعتبار أن الضرر له مظاهر خارجي ملموس خلافاً للنشاط الذي قد لا يكون كذلك متى ما اتخذ صورة الامتناع أو السلوك السلبي، غير أن هذا الاتجاه لم يسلم بدوره من النقد، ذلك بأن الأخذ به يفضي إلى عدم تجريم الشروع إذا لم تتحقق النتيجة، وكذلك عدم العقاب على ما يُعرف بالجريمة الشكلية أو جرائم السلوك المجرد^(٣٨).

لهذا ظهر اتجاه فقهي ثالث حاول أن يتلافي الانتقادات التي تعرضت إليها الاتجاهات السابقة ويقضي هذا الاتجاه بأن مكان وقوع الجريمة يتحدد في كل مكان وقع فيه عنصر من العناصر المكونة للجريمة وبالتالي فهو يشمل مكان حصول النشاط أو السلوك الإجرامي، وكذلك المكان الذي تتحقق فيه النتيجة أو الذي من المتوقع أو من المنتظر تتحققها فيه^(٣٩)، ونجد لهذا الاتجاه تطبيقاته في اغلب التشريعات المقارنة كقانون العقوبات الفرنسي والمصري والعراقي^(٤٠).

وعلى الرغم مما يحسب لهذا الاتجاه من افضلية فيما يتعلق بتوسيع نطاق الحماية الجنائية واعطاء مبدأ الإقليمية المرونة الكافية ليشمل كل العناصر الجرمية الواقعة على إقليم الدولة، ولكن بالمقابل وفي إطار الجرائم المعلوماتية العابرة للحدود قد لا يقدم مبدأ الإقليمية

حلولاًً مناسبة لمشكلة الاختصاص إذا ما أخذنا بعين الاعتبار ما تتسم به الجريمة المعلوماتية من امكانية كبيرة لتفرق عناصرها في أكثر مكان مما يزيد المسألة تعقيداً إذا ما تمسكت كل دولة وقع على إقليمها عنصر من عناصر الجريمة بمبدأ إقليمية القاعدة الجنائية.

ثانياً : مبدأ شخصية القاعدة الجنائية:

ويراد به "تطبيق القانون الجنائي في الدولة على كل من يحمل جنسيتها ولو ارتكب جريمته خارج إقليمها؛ وكان هذا المبدأ قديماً هو الأصل في تطبيق القانون الجنائي من حيث المكان ثم تحولت القوانين عنه تدريجياً إلى مبدأ الإقليمية"^(٤١).

وعلى الرغم من سهولة تطبيق هذا المبدأ لارتباطه بجنسية مرتكب الجريمة بعيداً عن مكان وقوعها أو مكان تحقق اثارها الجرمية إلا أنه يصطدم بالكثير من المعوقات منها ما يتعلق بالإجراءات الطويلة الخاصة بتنفيذ الأحكام الأجنبية حتى مع وجود اتفاقيات التعاون القضائي الدولي بحكم ارتفاع عدد الدول المرتبطة بشبكة الإنترنت قياساً بذلك المنضمة إلى مثل هذه الاتفاقيات؛ كما قد يؤدي تطبيق هذا المبدأ إلى محاكمة المتهم أكثر من مرة في دولته بحكم جنسيته وخارج دولته استناداً لمبدأ إقليمية خصوصاً عندما يقع السلوك الإجرامي في دولة وتمتد اثاره إلى دولة أخرى.^(٤٢)

ثالثاً : مبدأ عينية القاعدة الجنائية:

ويراد به "تطبيق القانون الجنائي للدولة على كل جريمة تمس مصلحة أساسية لتلك الدولة، أيًّا كان مكان ارتكابها أو جنسية مرتكبها"^(٤٣)؛ ويلعب هذا المبدأ دوراً مكملاً لمبدأ الإقليمية حيث تحرص الدول على المعاقبة واصطدام تلك الجرائم التي تقع خارج إقليمها ولكنها تمس مصالحها العليا ولا تتوقع من تلك التي وقعت فيها ابداء ذات الاهتمام بالمعاقبة عليها، ويجد هذا المبدأ في الكثير من التشريعات ومن بينها قانون العقوبات العراقي.^(٤٤)

رابعاً : مبدأ عالمية القانون الجنائي:

ويراد به "تطبيق القانون الجنائي للدولة على كل جريمة يقبض على مرتكبها في إقليم الدولة أيًّا كانإقليم الذي ارتكبت فيه وأيًّا كانت جنسية مرتكبها"^(٤٥)؛ ويأتي هذا المبدأ في

اطار التعاون الدولي في مكافحة بعض الجرائم المجمع على خطورتها من قبل المجتمع الدولي ومن امثلتها جرائم الاتجار بالمخدرات والرقيق والاطفال وكذلك تعطيل خطوط المواصلات وغيرها، ويمتاز هذا المبدأ باتساع نطاقه وسهولة تطبيقه لتوافق الدول على تطبيقه من غير أن يثير اشكاليات فيما يتعلق بالاختصاص أو تنفيذ الأحكام الأجنبية وغيرها.

المطلب الثاني : الاشكاليات المتعلقة بالاختصاص والحلول المقترنة بشأنها :

تتسم الجرائم المعلوماتية بطبيعة خاصة تميزها عن غيرها من الجرائم، فكما هو معلوم أن الوسيلة الاساسية التي تمكن من ارتكاب هذه الجرائم هي شبكة المعلومات (الإنترنت) التي لا تتقيد بحدود ولا تختص بدولة دون غيرها؛ فمن الممكن أن يقع السلوك الإجرامي لهذه الجرائم في أي مكان أو بالأحرى من أي حاسب موصول بهذه الشبكة يعود لشخص يحمل جنسية ما في دول أجنبية لا يحمل جنسيتها وتحقيق آثاره في مكان آخر أو أماكن متعددة في دولة أجنبية ثالثة، ومن ثم تكون هذه الجرائم من حيث المبدأ خارج أية رقابة أو سيطرة من أية جهة، بحيث لا يمكن القول بخضوعها لاختصاص قانون جنائي معين، ومما يشير حتماً اشكالية في تحديد القانون الواجب التطبيق على هذه الجرائم، اخذين بالاعتبار إجماع الدول على إعطاء قانونها الوطني الاختصاص إذا امتدت اثار السلوك الإجرامي إلى إقليمها أو مست المصالح الأساسية في تلك الدول.

ففي إحدى الحالات "تمكن شاب روسي من الدخول من غير إذن على الحاسب الرئيسي الخاص بمصرف ستي بنك في الولايات المتحدة الأميركيّة وقام بتجنييد العديد من المتواطئين معه لفتح حسابات مصرفيّة في شتى أنحاء العالم، ثم اصدر تعليمات إلى حاسوب البنك بتحويل الأموال إلى تلك الحسابات؛ وفي واقعة أخرى تمكّن شخصان مقيمان في ملبورن في استراليا بإرسال ملايين الرسائل الإلكترونية على عناوين في الولايات المتحدة واستراليا بالإضافة إلى قيامهما بوضع عدة رسائل على لوحات الرسائل لدى الشركات الرئيصة المقدمة لخدمة الإنترنت وذلك كله بهدف تشجيع شراء أسهم إحدى الشركات الأميركيّة التي كانت تباع في بورصة Nasdaq) وكانت هذه الرسائل تبشر بارتفاع قيمة هذه الأسهم بنسبة

عالية جداً مما أدى إلى ازدياد في حجم تداولها وتضاعف اسعارها وتحقيق ارباح طائلة جراء التلاعب في الاسواق المالية، بالإضافة إلى تعطل اجهزة الحاسب الآلي في كلا البلدين بسبب الكم الهائل من الرسائل الإلكترونية^(٤٥).

ومما يزيد الاشكال تعقيداً تباين معايير التحريم واختلافها من دولة إلى أخرى ومن الأمثلة التي يسوقها الفقه على ذلك "الدعائية للقنب الهندي (الخشحاش) فهي أمر غير محظوظ في بعض البلدان كما هو الحال في هولندا، وفي المقابل يعد مثل هذا السلوك مما يحرّمه القانون وغير مسموح به في بلدان أخرى بما فيها فرنسا مثلاً. والأمر ذاته ينسحب على المراهنات على كرة القدم، فهي غير مشروعة في بلد كفرنسا، وجائزة في بلدان أخرى كما هو الحال في إنجلترا^(٤٦)، ففي هذه الواقع وغيرها ومع تميزها بالعالمية فإن الحلول المقترحة في سبيل مكافحتها لا يمكن أن تأتي إلا في إطار دولي؛ هذا وعلى فرض ايجاد حلولاً قانونية لمشكلة الاختصاص فإنه تبقى هناك مشكلة تفاوت امكانيات وتقنيات ضبط الجريمة ومراقبتها من دولة إلى أخرى، وكذلك الاجراءات الطويلة والمعقدة المتعلقة بمحاكمة الجنائي الذي يرتكب جريمته في الخارج وتنفيذ الأحكام الجنائية؛ في الوقت الذي تعتبر السرعة الفائقة من مميزات هذه الجريمة مما يفرض حلولاً إجراءات تقع على ذات الدرجة من السرعة والمرونة لمواجهة هذا النوع من الجرائم.

أما بشأن الحلول المقترحة للتصدي لمشكلة الاختصاص في الجرائم المعلوماتية فنجد بدايةً ضرورة تدخل التنظيم القانوني الدولي في موضوع تحديد الاختصاص لا أن يترك الأمر لاجتهادات الفقه والقضاء على المستوى الداخلي فمن الطبيعي أن تلجأ كل دولة إلى اعطاء قوانينها الاختصاص في نظر هذه الجرائم إذا مست مصالحها مما يفاقم من مشكلة تحديد الاختصاص؛ فكما مرّ بنا آنفًا أن الجرائم المعلوماتية لا تتقييد بحدود سوى تلك التي تتقييد بها شبكة الإنترنت نفسها ما يضفي على هذه الجرائم بعداً دولياً يستلزم والحال هذه أن تكون المواجهة الجنائية على نفس المستوى، ولا سبيل إلى ذلك إلا من خلال تجاوز القواعد

القانونية التقليدية واعتماد أسس جديدة في تحديد الاختصاص تتماًءم وطبيعة هذه الجرائم في إطار اتفاقيات دولية عامة.

ويتراءى لنا بدءاً ضرورة التفرقة في تحديد الاختصاص بين الجرائم المعلوماتية بحسب المصالح التي يقع الاعتداء عليها، فكلما كانت هذه المصالح تهم الجماعة الدولية بشكل عام ومحل اجماع على تجريمها من قبلها عُقد فيها الاختصاص لقانون أي دولة يتم فيها ضبط الجريمة ك محل للنشاط الإجرامي أو محل لتحقق الآثار أو يتم فيها ضبط الجاني على أساس مبدأ الاختصاص الشامل أو العالمي على غرار بعض الجرائم التقليدية التي يثبت فيها للدول مثل هذا الاختصاص، وفي حال مست هذه الجرائم مصالح دولة بعينها دون غيرها أو مست مصالحها الحيوية على نحو ينبع بمخاطر كبيرة كالهجمات الإلكترونية على المواقع الحكومية الحساسة وغيرها أُعطي قانون تلك الدولة الاختصاص للنظر في مثل هذه الجرائم.

أما فيما يتعلق بالجرائم الأخرى التي تقع على مصالح متعددة من غير ما سبق وتتعدد فيها أماكن تحقق آثار الجريمة أو يتanax فيها الاختصاص بشكل عام فمن الممكن اللجوء إلى فكرة الاختصاص الاصلي والاختصاص الاحتياطي أو الثانوي الذي يلتجأ إليه في حال تعذر الأخذ بقانون الاختصاص الاصلي وفقاً لقواعد عامة يتم الاتفاق عليها في ضوء الاتفاقية المقترحة بهذا الشأن، فتعطى الأولوية مثلاً إلى قانون محل تحقق آثار الجريمة أو المحل المتوقع أن تشكل خطورة على مصالحه الحيوية أو مكان ضبطها أو ضبط المجرم وهكذا، دون أن نغفل عن ضرورة أن تنظم وتبسط أن أمكننا القول هذه الاتفاقية الاجراءات الخاصة بمحاكمة الاجنبي وتنفيذ الأحكام الجنائية.

الخاتمة

تأتي هذه الدراسة في خضم المتغيرات التي نجمت عن التطورات الهائلة في مجال تقنية المعلومات ونظم الاتصال الحديثة، فأصبحنا على اعتاب عالم جديد ذو طابع رقمي يستعصي على اغلب القواعد والأنظمة القانونية التقليدية، تعاظمت معه الحاجة لتدخل تشريعي لمعالجة الوضع القانونية المترتبة على ظاهرة المعلوماتية، ومنها ما يتعلق بالسياسة الجنائية في مواجهة الجرائم التي تعتمد على مثل هذه التقنيات سواء من الناحية الموضوعية أو الاجرائية، ولقد أتى البحث على أهم الاشكاليات الاجرائية المتصلة بالجرائم المعلوماتية وتوصلنا من خلاله إلى جملة من الاستنتاجات والتوصيات نوردها استكمالاً للفائدة من البحث على نحو ما يأتي :

أولاً: الاستنتاجات

١. يعتمد إثبات الجرائم المعلوماتية إلى حد كبير على أدلة لا يمكن استخلاصها إلا بإتباع ذات القواعد التي تحكم التقنية المعلوماتية، مما يجعل هذه الأدلة أدلة علمية بالدرجة الأساس يتوقف مدى حجيتها على السلطة الممنوحة للقاضي في تقديرها وعلى طبيعة نظام الإثبات المعتمد من قبل القضاء.
٢. تتصف الأدلة الرقمية بذات الصفات التي تتصف بها التقنية الرقمية ذاتها من حيث كونها أدلة علمية بحثة، متطورة ومتنوعة، ولا يمكن التخلص منها بسهولة إذا ما استخدمت التطبيقات المناسبة التي تمكنا من استعادتها، بل بالعكس قد يعد التخلص منها أو محاولة ذلك من قبل الجاني دليلاً يصب ضد مصلحته.
٣. لا يعني اعتماد الإثبات بالأدلة العلمية ومن بينها الأدلة الرقمية الغاء دور القاضي، فإذا كان الدليل العلمي قاطعاً فيما يتوصل إليه من حقائق علمية، إلا أن للقاضي مناقشة الظروف والملابسات التي وُجد فيها ذلك الدليل، ويامكانه طرح ذلك الدليل رغم قطعيته، إذا لم يكن بالإمكان أن تعد هذه الحقائق العلمية حقائق قضائية أيضاً.

٤. عدم الاتساق بين القواعد الاجرائية التقليدية الخاصة بالتفتيش وطبيعة البيئة الافتراضية، وذلك لاختلاف ما تتعامل معه الجهات القائمة بالتحقيق فيما يخص طبيعة مسرح الجريمة المعلوماتية بحكم عدم تركه لأي اثار مادية وتضاؤل دور الانتقال والمعاينة لهذا المسرح، وكذلك طبيعة الأدلة الرقمية وما تتطلبه عملية استخلاصها من تقنيات وخبرات فنية عالية.

٥. يقف مبدأ سيادة الدولة عائقاً أمام التفتيش في الجرائم المعلوماتية خصوصاً في حال اتصال حاسب المتهم بحاسب آلي آخر يقع خارج حدود إقليم الدولة يلجأ إليه الجاني لإخفاء معالم جريمته أو العمليات الرقمية التي قام بها لإخفائها عن سلطات التحقيق، مما يستلزم الحصول على الموافقات قبل الشروع بتفتيش هذه الحواسيب ما يستغرق وقتاً طويلاً على خلاف ما يحتاجه التفتيش والضبط في مثل هذه الجرائم التي تتسم بالسرعة وقابليتها للإخفاء بوقت قصير جداً.

٦. لا يمكن تصور حلولاً قانونية لإشكالية تنازع الاختصاص مالم تأتي هذه الحلول في إطار دولي، فلا يمكن القول بانطباق قانون عقابي دون آخر إذا كانت الجريمة أساساً لا تعرف حدوداً جغرافية من جهة، ولا اختلاف معايير تحديد وقوع الجريمة على مستوى التشريعات العقابية الوطنية من جهة أخرى، مما يضفي بعداً دولياً لهذه الإشكالية يفرض معها حالاً على ذات المستوى.

ثانياً : التوصيات :

١. ضرورة تدخل المشرع بالتنظيم القانوني لموضوع الإثبات بالأدلة الرقمية وتحديد حجيتها وقيمتها القانونية، وتحديد الوسائل والطرق التي تمكن القاضي من التأكد من سلامة الدليل وشروط قبوله.

٢. نزوم افراد المشرع لأحكام خاصة بالتفتيش في البيئة الافتراضية تحدد الاشياء القابلة للتفتيش وكيفية تحريز الأدلة وضبطها، وضرورة مراعاة الأحكام المستحدثة في هذا الصدد الضمانات الدستورية والقانونية للحق في السرية والخصوصية.

٣. استحداث جهات واقسام خاصة ضمن الجهات القائمة على التفتيش أو جهاز الشرطة تختص بالتفتيش في هذه الجرائم، والعمل على تأهيل الأشخاص القائمين على التحقيق على التعامل مع هذا النوع من الجرائم على المستوى الداخلي، وعلى المستوى الدولي أيضاً فيما يخص التعاون مع الاجهزة الم対اظرة في الدول الأخرى في مجال تبادل المعلومات والتعاون الامني لمكافحة الجريمة.

٤. السعي نحو إيجاد اتفاق دولي يتولى تنظيم موضوع الاختصاص في الجرائم المعلوماتية أو على أقل تقدير التوسع في عقد الاتفاقيات الإقليمية أو الشائكة لإيجاد حلول لهذه الاشكالية؛ طبعاً بعد سد الفراغ التشريعي موضوعياً وإجرائياً في مجال الإجرام المعلوماتي بالنسبة للدول التي لا يوجد فيها قانون عقابي خاص بالجرائم المعلوماتية ومن بينها المشرع العراقي.

الهوا مش

- (١) يفرق بعض الباحثين في إطار الجرائم المعلوماتية بين نوعين : ويرى بأن الأول وأن كان يشمل صور مستحدثة من صور الاعتداء باستخدام الحاسوب والإنترنت إلا أنها تقع على مصالح محمية جنائياً بالنصوص العقابية التقليدية، أي أن طرق الاعتداء فقط هي المستحدثة في هذا النوع من الجرائم لأنها تتم عن طريق التقنية المعلوماتية بعد أن كانت ترتكب بالسلوك المادي الملموس، أما محل الاعتداء فهي مصالح محمية جنائياً أصلاً على مر الأزمان كالأموال والشرف والاعتبار وغيرها وبطريق عليها تسمية (جرائم غير معلوماتي عبر شبكة الإنترت)؛ أما النوع الثاني فتضم أنواعاً أخرى من الاعتداءات تقع بطرق مستحدثة على مصالح مستحدثة أيضاً لم تعرفها القواعد التقليدية كالشبكات المعلوماتية التي تتعرض للاختراق أو التعطيل أو الاضرار وهي تمثل المعنى الدقيق للجرائم المعلوماتية عبر شبكة الإنترنت. وطالما أن أساس التفرقة بين النوعين موضوعي ونحن هنا بقصد الجانب الاجرامي لهذه الجرائم خصوصاً فيما يتعلق بالتفتيش والاختصاص التي يشار فيها الاشكال بناءً طبيعة هذه الجرائم من حيث كونها عابرة للحدود لذا يفضل الباحث استخدام تسمية "الجرائم المعلوماتية" على التسميات الأخرى النظر إلى اتساع مدلولها ليشمل ما تقدم من تسميات وانواع. وللمزيد من التفاصيل ينظر : جميل عبد الباقي الصغير، الجوانب الاجرامية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، ١٩٩٨، ص: ٢٣؛ وما بعدها؛ كذلك : د. صالح احمد البربرى، دور الشرطة في مكافحة جرائم الإنترت في إطار الاتفاقية الأوربية. الموقعة في بودابست في ٢٣/١١/٢٠٠١ .arablawinfo.com

(٢) رمسيس بنهام، المحاكمة والطعن في الأحكام، منشأة المعارف، القاهرة، ١٩٩٣ ، ص: ٥٨.

(٣) احمد فتحي سرور، الوسيط في قانون الاجراءات الجنائية، دار النهضة العربية، القاهرة، ٢٠١٠ ، ص: ٢٣.

(٤) عبدالفتاح بيومي حجازي، مبادئ الاجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، ٢٠٠٧ ، ص: ٥٨.

(٥) عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة، الاسكندرية، ٢٠١٠ ، ص: ٥١.

(٦) حنان ريحان مبارك المضحكي، الجرائم المعلوماتية، منشورات الحلبي الحقوقية، ط١، بيروت، ٢٠١٤ ، ص: ٣٥٥.

- (٧) د. فتحي محمد انور عزت، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية للمجتمع المعلوماتي، ط٢، دار النهضة العربية، القاهرة، ٢٠١٠، ص: ٤٨.
- (٨) د. فتحي محمد انور عزت، مصدر سابق، ص: ٦٥٤. ينظر أيضاً حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنٽ، دار النهضة العربية، القاهرة، ٢٠٠٩، ص: ٥٣٤ وما بعدها.
- (٩) عبدالفتاح بيومي حجازي، مصدر سابق، ص: ٧٨.
- (١٠) د. هلالٰي عبد اللهٰ أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية (على ضوء اتفاقية بودابست الموقعة في ٢٣ نوفمبر ٢٠٠١)، الطبعة الأولى، دار النهضة العربية . القاهرة، ٢٠٠٦، ص: ١٦٠.
- (١١) د. جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، مجلة العلوم القانونية والاقتصادية، العدد الأول، كلية الحقوق، جامعة عين شمس، ٢٠٠٧، ص: ٩.
- (١٢) حسين بن سعيد الغافري، مصدر سابق، ص: ٥٩٩.
- (١٣) د. براء منذر كمال عبداللطيف، شرح قانون اصول المحاكمات الجزائية، ط٥، مطبعة يادكار، السليمانية، ٢٠١٦ ، ص: ٢٩٠.
- (١٤) سعيد عبداللطيف حسن، اثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنٽ، دار النهضة العربية، ط١، القاهرة، ١٩٩٩، ص: ١٤٦.
- (١٥) للمزيد من التفاصيل ينظر : سلمان عبيد عبدالله، المبادئ العامة في قرارات الهيئة الموسعة والهيئة العامة في محكمة التمييز الاتحادية، الجزء الأول، ط١، المكتبة الوطنية، بغداد، ٢٠١٢ ، ص: ٨٦.
- (١٦) حسين بن سعيد الغافري، مصدر سابق، ص: ٦٠٢.
- (١٧) للاطلاع على مواقف هذه التشريعات ينظر : حسين بن سعيد الغافري، مصدر سابق، ص: ٤٠٦.
- (١٨) د. عبدالفتاح بيومي حجازي، مصدر سابق، ص: ٩٢.
- (١٩) د. فتحي محمد انور عزت، مصدر سابق، ص: ٦١٢.
- (٢٠) سعيد حسب الله عبدالله، شرح قانون اصول المحاكمات الجزائية، دار الاثير للطباعة والنشر، الموصل، ٢٠٠٥، ص: ٢٠٠.
- (٢١) د. عبدالفتاح بيومي حجازي، مصدر سابق، ص: ١٩٢.

- (٢٢) د. هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة .
أسيوط، ١٩٩٤، ص ٦٤.
- (٢٣) د. هلالی عبدالإله، تفتيش نظم الحاسوب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية، القاهرة، ١٩٩٧، ص: ٨٢ كذلك د. حسين الغافري مصدر سابق، ص: ٤٧٧ .
- (٢٤) للمزيد من التفاصيل ينظر د. عبدالفتاح بيومي حجازي، ص ٣٧٨ وما بعدها
- (25) Pirgoff (Donald.k) computer crimes and other crimes against information technology in canda :rev intern de.pen 1993.p241.
- (٢٦) جميل عبد الباقى الصغير، الجوانب الاجرامية للمعلوماتية بالإنترنت، مصدر سابق، ص: ٤٥؛ كذلك ينظر د. عمر بن يونس، الإجراءات الجنائية عبر الإنترت في القانون الأمريكي "المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسيب وصولاً إلى الدليل الإلكتروني في التحقيقات الجنائية"، الطبعة الأولى، ٢٠٠٤ . ٢٠٠٥ . ٢٠٠٤ ، ص ١
- (٢٧) د. هلالی عبد الله، مصدر سابق، ص: ٨٨ .
- (28) Mohrenschlager(manfred): computer crimes and other crimes against information technology in canda :rev intern de.pen 1993.p351.
- (٢٩) عبد القادر قهوجي ،الحماية الجنائية للبيانات المعالجة الكترونياً، مؤتمر كلية الشريعة والقانون، جامعة الامارات، ٢٠٠٠ ، ص: ٤ .
- (٣٠) د. محمد ابو العلا عقيدة، التحقيق وجمع الأدلة في مجال الجرائم المعلوماتية، المؤتمر العلمي الأول حول الجوانب القانونية والامنية للعمليات الإلكترونية، دبي، ٢٠٠٣ ، ص: ٣٤ .
- (٣١) أ.د. موسى مسعود أرحومة، الجريمة المعلوماتية عبر الوطنية، بحث مقدم إلى مؤتمر المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، ٢٠٠٩ ، ص: ١٢ .
- (٣٢) د. عبدالله حسين محمود، سرقة المعلومات في الحاسوب الآلي، دار النهضة العربية، القاهرة، ص ٣٧٦ .
- (٣٣) حسين بن سعيد الغافري، مصدر سابق، ص: ٤٨٥ .
- (٣٤) أ.د. موسى مسعود أرحومة، مصدر سابق، ص: ١٢ .
- (٣٥) للمزيد من التفاصيل ينظر: د. هلالی عبدالإله أحمد، تفتيش نظم الحاسوب الآلي وضمانات المتهم المعلوماتي، مصدر سابق، ص ٨٠؛ حسين بن سعيد الغافري، مصدر سابق، ص: ٤٨٦؛ د. عبدالفتاح بيومي

- حجازي، مصدر سابق، ص: ٣٨٤ د. محمود نجيب حسني، شرح قانون الاجراءات الجائية، ط٣، دار النهضة العربية، القاهرة، ١٩٩٨، ص: ٣٢٣.
- (٣٦) د. أحمد عبدالكريم سلامة، قانون حماية البيئة . دراسة تأصيلية في الأنظمة الوطنية والاتفاقية، الطبعة الأولى، منشورات جامعة الملك سعود، ١٩٩٧ ، ص ٥٣٥.
- (٣٧) أ.د.موسى مسعود أرجومة، مصدر سابق، ص: ١٤ .
- (٣٨) ا.د.علي حسين الخلف ود. سلطان الشاوي، المبادئ العامة في قانون العقوبات، مكتبة السنهوري، بغداد، ٢٠١٠ ، ص ٩٧ .
- (٣٩) ينظر المادة (٦) من قانون العقوبات العراقي؛ وللمزيد من التفاصيل ينظر : حسين بن سعيد الغافري، مصدر سابق، ص: ٥٧٨؛ ا.د. علي حسين الخلف ود. سلطان الشاوي، مصدر سابق، ص: ٩٧ .
- (٤٠) ينظر المادة (١٠) من قانون العقوبات العراقي.
- (٤١) د. جميل عبدالباقي الصغير، الجوانب الاجرائية للجرائم المتعلقة بالإنترنت، مصدر سابق، ص: ٦٠ .
- (٤٢) د.علي حسين الخلف ود.سلطان الشاوي، مصدر سابق، ص: ١٠١ .
- (٤٣) ينظر المادة (٩) من قانون العقوبات العراقي.
- (٤٤) ينظر المادة (١٣) من قانون العقوبات العراقي.
- (٤٥) حسين بن سعيد الغافري، مصدر سابق، ص: ٤٤ .
- (٤٦) د. جميل عبدالباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، ص: ٤٣ .

المصادر

أولاً: الكتب القانونية

١. احمد فتحي سرور، الوسيط في قانون الاجراءات الجنائية، دار النهضة العربية، القاهرة، ٢٠١٠.
٢. د. أحمد عبدالكريم سلامة، قانون حماية البيئة. دراسة تأصيلية في الأنظمة الوطنية والاتفاقية، الطبعة الأولى، منشورات جامعة الملك سعود، ١٩٩٧.
٣. د.براء منذر كمال عبداللطيف، شرح قانون اصول المحاكمات الجزائية، ط٥، مطبعة يادكار، السليمانية، ٢٠١٦.
٤. جميل عبد الباقى الصغير، الجوانب الاجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، ١٩٩٨.
٥. حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترت، دار النهضة العربية، القاهرة، ٢٠٠٩.
٦. حنان ريحان مبارك المضحكي، الجرائم المعلوماتية، منشورات الحلبي الحقوقية، ط١، بيروت، ٢٠١٤.
٧. رسيس بنهام، المحاكمة والطعن في الأحكام، منشأة المعارف، القاهرة، ١٩٩٣.
٨. سعيد حسب الله عبدالله، شرح قانون اصول المحاكمات الجزائية، دار الاثير للطباعة والنشر، الموصل، ٢٠٠٥.
٩. سعيد عبداللطيف حسن، ثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترت، دار النهضة العربية، ط١، القاهرة، ١٩٩٩.
١٠. سلمان عبيد عبدالله، المبادئ العامة في قرارات الهيئة الموسعة والهيئة العامة في محكمة التمييز الاتحادية، الجزء الأول، ط١، المكتبة الوطنية، بغداد، ٢٠١٢.
١١. د. صالح احمد البريري، دور الشرطة في مكافحة جرائم الإنترت في إطار الاتفاقية الأوروبية. الموقعة في بودابست في ٢٣/١١/٢٠٠١. arablawinfo.com
١٢. عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة، الاسكندرية، ٢٠١٠.
١٣. د. عبدالله حسين محمود، سرقة المعلومات في الحاسوب الآلي، دار النهضة العربية، القاهرة، ١٩٩٨.

٤. عبدالفتاح بيومي حجازي، مبادئ الاجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، ٢٠٠٧.
٥. عبد القادر قهوجي، الحماية الجنائية للبيانات المعالجة الكترونياً، مؤتمر كلية الشريعة والقانون، جامعة الإمارات، ٢٠٠٠.
٦. د. علي حسين الخلف ود. سلطان الشاوي، المبادئ العامة في قانون العقوبات، مكتبة السنهاوري، بغداد، ٢٠١٠.
٧. د. عمر بن يونس، الإجراءات الجنائية عبر الإنترت في القانون الأمريكي "المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسيب وصولاً إلى الدليل الإلكتروني في التحقيقات الجنائية"، الطعة الأولى، ٢٠٠٥.
٨. د. فتحي محمد انور عزت، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية للمجتمع المعلوماتي، ط٢، دار النهضة العربية، القاهرة، ٢٠١٠.
٩. د. محمود نجيب حسني، شرح قانون الاجراءات الجنائية، ط٣، دار النهضة العربية، القاهرة، ١٩٩٨.
١٠. د. هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة . أسيوط، ١٩٩٤.
١١. د. هلالي عبدالله أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية (على ضوء اتفاقية بودابست الموقعة في ٢٣ نوفمبر ٢٠٠١)، الطبعة الأولى، دار النهضة العربية . القاهرة، ٢٠٠٦ .
١٢. د. هلالي عبدالله، تفتيش نظم الحاسوب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية، القاهرة، ١٩٩٧ .
- ثانياً: البحوث والمجلات
١. د. جميل عبد الباقى الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، مجلة العلوم القانونية والاقتصادية، العدد الأول، كلية الحقوق، جامعة عين شمس، ٢٠٠٧ .
 ٢. د. محمد ابو العلا عقيدة، التحقيق وجمع الأدلة في مجال الجرائم المعلوماتية، المؤتمر العلمي الأول حول الجوانب القانونية والامنية للعمليات الإلكترونية، دبي، ٢٠٠٣ .
 ٣. أ.د. موسى مسعود أرحومة، الجريمة المعلوماتية عبر الوطنية، بحث مقدم إلى مؤتمر المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، ٢٠٠٩ .

ثالثاً: المصادر الاجنبية

1. *Pirg off (Donald.k) computer crimes and other crimes against information technology in Canada :rev intern de. Pen 1993.p241*
2. *Mohrenschlager (manfrred): computer crimes and other crimes against information technology in Canada :rev intern de. pen 1993.p351.*

Procedural Challenges related to Informatics Crimes

Assistant Lecturer. Safa'a Hassan Nisaif

College of Law and Political Sciences-University of Diyala

Abstract

Major developments in the field of Internet and information networks have been accompanied with unique and novel criminal patterns that communities were not familiar with before . They raised massive controversy focused directly on the extent of the flexibility and breadth of traditional punitive legislations to accommodate such patterns. Especially in the procedural aspect that this study shed the lights on concerning the procedural challenges raised by the IT, Cyber, crimes to the extent of admissibility for digital evidence . Especially the data that cannot be reached only by the use of certain techniques and applications under the supervision of experts in this area.

Its authenticity depends on the nature of the current judicial system and the discretionary power granted to the judge, and the extent to which system of scientific proof is reliable in Criminal evidence;

The problem also raised in the inspection field of virtual digital environment due to the special character of such environment. In addition, the breadth of informatics crime scene to the extent that territorial boundaries are canceled which enforce finding legal solutions to impose an inspection outside the borders of the State's territory; and other challenges are raised out of the fact that cyber crime does not recognize the territorial boundaries for the competence conflict in the event of having the crime happened in any place plugged into the Internet and their impact is realized in other multiple places or by a person or people with different nationalities raising a legal problem in determining the crime scene. Then, the applicable law calling for neglecting the traditional stereotypes and adopting new and innovative legal basis to suit the nature of these crimes.