مجلة العلوم القانونية والسياسية

اسم المقال: التحديات الإجرائية المتصلة بالجرائم المعلوماتية
اسم الكاتب: م.م. صفاء حسن نصيف
رابط ثابت: https://political-encyclopedia.org/index.php/library/1078
تاريخ الاسترداد: 2026/11/01 16:33 +03

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

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

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

التحديات الإجرائية المتصلة بالجرائم 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 تركز 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 تثيرها 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؛ ويثار الإشكال 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 ايجاد 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 اثرها في مكان أو أماكن أخرى متعددة ومن قبل شخص أو اشخاص يحملون جنسيات مختلفة مما يثير 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.

المقدمـــــة

لقد افرز التطور العلمي والتقني في مجال الاتصالات وتكنولوجيا والمعلومات وشبكات الإنترنت 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 بمراكز 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 مواقع التواصل الاجتماعية 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 ومعالمها قبل اكتشافها واعتمادها بشكل أساس على تقنية المعلومات بالإضافة إلى عدم تقيدها 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 المجدي أن نعدل تشريعات أو نستحدث أخرى لاستيعاب هذه الجرائم من غير أن يكون هناك نظام قانوني إجرائي متكامل 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 لتعقّب 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 آخذاً بمبدأ إقليمية القانون الجنائي، ويفضي بالتالي إلى تنازع الاختصاص القضائي بسبب صعوبة تحديد مكان وقوع الجريمة المعلوماتية عبر الوطنية، ومن هنا جاءت فكرة البحث لتسلط الضوء على الجانب الاجرائي للجرائم المعلوماتية[١] وبشكل خاص التحديات الاجرائية التي تثيرها هذه الجرائم في ثلاثة مباحث؛ نخصص الأول منها لبحث مدى قبول الدليل الرقمي في مجال الإثبات الجنائي، ونتناول في الثاني التفتيش في البيئة الرقمية، بينما نبحث في الثالث اشكالية تنازع الاختصاص الجنائي والقانون الواجب التطبيق على هذ الجرائم.

المبحث الأول

اشكالية قبول الدليل الرقمي

تقع الجرائم المعلوماتية على درجة من الصعوبة من حيث اثباتها إذ لا تخلف هذه الجرائم أي أدلة مادية ملموسة كتلك التي تنتج عن الجرائم التقليدية كالسلاح المستخدم والمقذوفات وبصمات الاصابع والاثار وغيرها؛ وفضلاً 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 المحملة 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 اكثر 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 ثنائي ويمكن أن يعتمد عليها في المحكمة" كما عرفه آخرون على نحو أدق بأنه "الدليل المشتق من أو بواسطة النظم البرمجية المعلوماتية الحاسوبية وأجهزة ومعدات الحاسب الآلي أو شبكات الاتصال من خلال إجراءات قانونية وفنية 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]

وبما أن الجرائم المتصلة بالإنترنت تقوم على أساس استخدام تقنيات المعلومات والاتصالات الحديثة فلا يمكن تصور وقوع هذه الجرائم إلا من خلال وسائل واجهزة تسمح باستخدام هذه التقنية؛ ولهذا تشتمل الأدلة الإلكترونية الرقمية بالنظر إلى طبيعتها على نوعين رئيسين : يتمثل الأول بالأدلة المادية المستخدمة في هذه الجرائم كجهاز الحاسب الآلي وأجهزة الهواتف النقالة ووسائل ربط الاجهزة مع بعضها من خلال شبكة الإنترنت (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 أخر 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 بالبيانات المخزنة أو المتنقلة بصيغة رقمية المأخوذة من جهاز الحاسب الآلي وملحقاته وعادة ما تكون بصيغة مجالات أو نبضات مغناطيسية من الممكن تجميعها أو تحليلها باستخدام تطبيقات وتقنيات خاصة؛ وتتعلق 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 اوعية التخزين في الحاسوب الآلي وما في حكمه بشكل نبضات واشارات كهربائية ناتجة عن استخدام لوحة المفاتيح أو غيرها بشكل مجموعات رقمية متكررة من رقمي الصفر والواحد حيث تعبر كل مجموعة الآحاد والاصفار عن بيان أو معلومة بعينها"[٧]؛ ولاستخلاص 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 بحتاً.

٢. الدليل الالكتروني دليل متنوع ومتطور: فلا يعدو أن يكون الدليل الالكتروني سوى قالباً يحوي من مجموعة من البيانات الرقمية منفردة أو مجتمعة تتخذ اشكالاً متنوعة تتضمن نصوصاً مكتوبة أو صوراً ورسومات وسمعيات ومرئيات، تصلح لأن يستند إليها القاضي عند تقرير البراءة أو الإدانة، مستقاة من بيئة متطورة بطبيعتها قابلة لابتكار المزيد من المظاهر الرقمية؛ سيما وأن المبدأ السائد في العالم الرقمي أنه لايزال في بداياته ولم يصل بعد إلى منتهاه وهذا ما يفرض طبيعة التطور في الأدلة المستمدة منه.

٣. الدليل الالكتروني دليل يصعب التخلص منه : وتعد من أهم الخصائص التي يتصف بها الدليل الالكتروني بخلاف الأدلة التقليدية التي غالباً ما تكون قابلة للتخلص منها كبصمات الاصابع وآثار الاقدام أو الشرائط المسجلة والاوراق 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 ازالتها من الحاسوب مرة أخرى من خلال برامج تقنية معينة [٨].

ثانياً. الصعوبات المتعلقة بالدليل الالكتروني :

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

١. الصعوبات الخاصة بالدليل الرقمي نفسه : وتتأتى هذه الصعوبات من البيئة التي يُستمد 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 خصوصا 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 مادية، 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 الاثار المادية للجريمة أن وجدت مما يورث الشك في دلالة الأدلة المستقاة من المعاينة والفحص في هذه الجريمة، ناهيك عن الاسيجة الامنية التي يضربها الجناة حول افعالهم والوسائل التي يلجأون للحيلولة دون كشفها كما لو استخدم الجاني حاسباً أخر 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 مربح ولهذا تتسابق الشركات في تبسيط الاجراءات 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، وربّما تتعقد المسألة أكثر عند استخدام الإنترنت اللاسلكي[١٠].

المطلب الثاني : سلطة القاضي في تقدير الدليل الرقمي

تتفاوت 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 وتأثرها بما تقدم من عوامل على نحو مما يأتي:

أولاً. طبيعة أنظمة الإثبات

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

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 أخر أن دور

القاضي هنا يقتصر فقط على تقدير توافر الشروط التي حددها 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 الاخذ في الإثبات الجنائي وخصوصاً في اطار 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 الاقتناع الذاتي) : وفيه "يترك للقاضي الحرية في أن يؤسس حكمه على أي دليل وفقاً لاقتناعه الشخصي دون أن يُفرض عليه دليل بعينه والاعتراف له بسلطة تقدير قيمة الدليل أو قيمة الأدلة مجتمعة "[١٢]، بمعنى أن للقاضي أن يستمد من الوقائع المعروضة امامه ما يمكن أن يشكل دليلاً من خلال استنتاج قائم على أساس العقل والمنطق، ونجد بأن هذا النظام اكثر اتساقاً مع طبيعة الإثبات الجنائي فالحرية التي يتمتع ضرورية 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 ادوار التحقيق أو المحاكمة وهي الاقرار وشهادة الشهود ومحاضر التحقيق والمحاضر والكشوف الرسمية الأخرى وتقارير الخبراء والفنيين 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 شيوعها 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 اثبات الجريمة ونسبتها إلى المتهم، فيعطي الدور الرئيس في اثبات الجريمة للخبير، ويجعل أهم الأدلة هي القرائن التي تخضع للفحص العلمي الدقيق لاستخراج ما يثبت البراءة أو الإدانة منها"[١٤]؛ والملاحظ هنا أن سلطة القاضي في تقدير الأدلة تنحسر وتتقيد 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 العادية الأخرى كالقرائن والشهادة وغيرها والتي يمارس القاضي بصددها 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 الاساسية التي كفلتها الدساتير والقوانين مما يستلزم أن يكون للقاضي سلطة تخوله 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 الاجزاء المادية (الصلبة) والمعنوية (البرامج) التي يتوسل بها الجاني لتنفيذ جريمته طبعاً عبر شبكة الإنترنت، غير أن الأمر لا يتعلق بهذه المكونات ـ بوصفها اشياء مادية تخضع للقواعد العامة المتعلقة بالدليل المادي العادي ـ 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 ليبني حكمه على اساسها وإلى أي مدى يمكن له قبول الدليل العلمي لإثبات استخدام هذه المكونات في جريمة معلوماتية، هو ما يفرض علينا مناقشة الامور التالية :

١. مدى قبول مخرجات الحاسب الآلي أو ملحقاته كأدلة جنائية : وتتمثل هذه المخرجات بالبيانات أو المعلومات الموجودة على سطح المكتب في الحاسب الآلي أو المعلومات المثبتة في اقراص ليزرية أو سعات التخزين المختلفة مهما كانت طبيعتها سواء أكانت نصوصاً مكتوبة أو صوراً أو فيديوهات أو غيرها، ولا تثير هذه المخرجات اشكالاً كبيراً في ظل الأنظمة القضائية التي تعتنق مبدأ الاقتناع الذاتي للقاضي كالقضاء العراقي الذي اعتمد على هذه المخرجات كتسجيل مكالمات الهاتف النقال الدائرة بين المشتكي والجناة الموثقة من قبل شركة اثير للاتصالات[١٥]؛ ولكن يبقى في ظل هذه الأنظمة بمقدور القاضي قبول هذه الأدلة أو مناقشتها والاستعانة بالخبرة للتأكد 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 ـ أميركية، ولذلك فإن قبول المستندات المطبوعة لمخرجات الوسائل الإلكترونية التي تتجسد بشكل نبضات أو اشارات ممغنطة يشكل عقبة أمام القضاء لعدم تمكن القاضي أو المحلفين من معاينة الأدلة المتولدة منها أو وضع اليد عليها مما يجعلها أدلة ثانوية وليست أصلية[١٦].

وأزاء هذا الوضع ونظراً لتعاظم دور التقنية المعلومات والوسائل الإلكترونية فقد بادرت تشريعات هذه الدول التي تغيير موقفها السابق وقبلت مخرجات هذه الوسائل كأدلة للإثبات وأن قيدت ذلك ببعض 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 يتعلق 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 نتيجة يسفر عنها استخدام برامج وتطبيقات الكترونية تقنية معينة من قبل المختصين من ذوي الخبرة في هذا المجال تعزز قناعة المحكمة بثبوت واقعة محل شك أو نفيها، ويطلب بناءً على رغبة المحكمة أو بطلب من احد 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، ويبرر اصحاب هذا الرأي توجههم 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 الجناة[١٨].

في حين يفرق رأي أخر 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 أسس علمية دقيقة ولا حرية للقاضي في مناقشة الحقائق العلمية. أما الظروف والملابسات التي وُجد فيها الدليل فأنها 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 الواقعة وملابساتها"[١٩]، وفي ضوء ما تقدم نجد من غير الممكن تجاهل اهمية الدليل الرقمي العلمي كونه الاكثر تناسباً في اثبات الجرائم المعلوماتية في ظل تعقيد الأدلة الناجمة عنها وصعوبة التوصل إليها؛ فإن قيل بأن الدليل الرقمي يقتصر على الاسناد المادي للنشاط الجرمي إلى جهاز الحاسب الآلي أو أي وسيلة من وسائل الاتصال الحديثة بشبكة الإنترنت ولا يتمكن من تحديد شخصية الجاني، رُدَّ على ذلك بأنه من غير المستبعد أن يعلو شان 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 الاطلاع على محل منحه القانون حرمة خاصة لضبط ما عسى قد يوجد فيه مما يفيد في كشف الحقيقة عن جريمة معينة[٢٠]، 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 [٢١]؛ وفي اطار 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 ـ أو ما في حكمه ـ موصول بشبكات الاتصال يتمكن من خلاله الجاني من بلوغ غاياته، فإلى أي مدى تَصلُح مكونات الحاسب الآلي للتفتيش ؟ والى أي مدى يمكن تفتيش شبكات الاتصال بالحاسب الآلي ؟ هذا ما سنحاول الاجابة عليه فيما يأتي:

المطلب الأول : مدى صلاحية مكونات الحاسب الآلي للتفتيش

من المعلوم أن جهاز الحاسب الآلي يتكون من مركبات مادية واخرى معنوية، وفي صدد تفتيش الحاسب الآلي نجد أن مركبات الحاسب الآلي المادية وما يلحق بها من اجهزة وكذلك المعلومات المخزنة في أوعية التخزين الثابتة كالقرص الصلب في جهاز الحاسب الآلي أو الأوعية المنفصلة كالأقراص المرنة وغيرها، لا تثير إشكالاً فهذه المركبات المادية بل

والمعلومات أيضاً متى اتخذت مظهراً مادياً ملموساً تخضع للقواعد الاجرائية العامة في التفتيش وذلك بحسب المكان أو الحيز الذي توجد فيه، فيحكمها ما يحكم الاماكن والاشخاص أن هي وجدت في منزل المتهم أو وملحقاته أو في أماكن عامة، أو وجدت في الحيز الشخصي للمتهم.[٢٢]

ولكن الفقه اختلف بشأن التفتيش عندما يرد على المكونات المعنوية 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 أخر إلى "عدم انطباق المفهوم المادي على بيانات الحاسب الآلي غير المرئية، ويرى ذلك نقصاً تشريعياً 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 أخر 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 الاشياء المادية التي يمكن أن تكون محلاً للتفتيش، أسوة بالطاقة الكهربائية التي عدتها اغلب التشريعات من قبيل الاشياء 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 الدعامات التي يمكن أن تحملها مهما كان شكلها؛ وتبنى هذا الاتجاه المشرع الالماني إذ اشترط أن تكون الأدلة المضبوطة ملموسة وذلك بمقتضى المادة (٩٤) من قانون الاجراءات الجنائية[٢٨]. ويعد هذا الرأي في تقديرنا من اكثر 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 واستخراجه بهيئة أو شكل مادي يمكن تقديمه وأثباته أمام القضاء، على أن ذلك لا يغني 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 الاخذ بالآراء 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 تُستغل فيها لارتكاب جرائم معلوماتية معينة كالسرقة والاتلاف والتزوير والاختراق والبقاء غير المصرح فيه وغيرها؛ ويستدل على ذلك بموقف المشرع الفرنسي الذي عاقب على الافعال 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 الالية لمعطيات الحاسب الآلي وشددت العقوبة إذا نتج عن هذا البقاء تعديل البيانات الموجودة داخل النظام أو إفساد وظيفته"[٢٩].

المطلب الثاني : تفتيش شبكات الاتصال بالحاسب الآلي

قد يطال التفتيش أماكن أخرى غير مكان حاسوب المتهم وذلك في اطار 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 موصول بشبكة الإنترنت مما يطرح تساؤلاً حول مدى خضوع شبكات الاتصال للتفتيش، وهذا ما يفرض التمييز بين الفروض التالية:

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

لا يثير هذا الفرض إشكالاً كبيراً طالما أن الاماكن التي وُجد فيها حاسب المتهم أو الحاسب الاخر المرتبط به الذي قد يطاله التفتيش خاضع لنظام قانوني واحد، وتكاد تجمع التشريعات الاجرائية ـ سواء بالنسبة للقواعد الاجرائية العامة أو القواعد الاجرائية الخاصة بالجرائم المعلوماتية ـ على جواز امتداد التفتيش لمناطق أخرى غير واردة في أمر للتفتيش ولو وقع ذلك بدون إذن صادر من جهة مختصة ولكنها تقيدها بضوابط معينة، وقد تبنت معظم التشريعات هذا الاتجاه ومنها قانون اصول تحقيق الجنايات البلجيكي لسنة ٢٠٠٠ الذي أجاز امتداد التفتيش إلى نظام معلوماتي أخر 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 بحاسوب غير المتهم يتم الدخول إليها من خلال الحاسب الأصلي محل التفتيش[٣٠].

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 أخر 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 الدواة عبر شبكات الاتصال بهدف تضليل وعرقلة سير التحقيقات، واختلف الفقه أزاء هذا الوضع وانقسم إلى أراء متعددة واختلفت التشريعات تبعاً لذلك؛ فذهب رأي إلى "جواز امتداد التفتيش الالكتروني 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 تثيره من معوقات أمام التفتيش؛ إذ يؤدي انتظار الحصول على الإذن من الدولة التي أمتد إليها التفتيش قد يؤدي إلى افراغ 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 لايزال يصطدم بمبدأ السيادة الذي يعد مثل هذا الأمر انتهاكاً صريحاً له.

في حين يرى رأي أخر بأن التفتيش الالكتروني خارج حدود إقليم الدولة لا يمكن أن يتم إلا في إطار اتفاقيات دولية خاصة ثنائية أو عامة تجيز هذا الامتداد أو على الاقل بعد الحصول على الإذن، ويسود هذا الرأي في الفقه الالماني.[٣٢]

في حين سلك اتجاه أخر طريقاً وسطاً فهو أقر بدءاً عدم جواز التفتيش الالكتروني خارج حدود الاقليم كمبدأ عام إلا بعد الحصول على إذن، إلا أنه أورد بعض الاستثناءات لضرورات معينة يقتضيها التفتيش، واخذ بهذا لاتجاه المجلس الاوروبي 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 التوسع فيها وضمان عدم الاعتداء على الحريات الشخصية ولا ضير من أن تتم عملية التفتيش والضبط أمام انظار ومراقبة الجهات القضائية في الدولة التي تمتد غليها أعمال التفتيش الالكتروني أو على الاقل إحاطتها علماً بذلك.

ثالثاً: التنصت والمراقبة الإلكترونية لشبكات الاتصال :

بالرغم من كونها تشكل انتهاكاً صريحاً للحريات الفردية إلا اننا نجد معظم التشريعات تجيزها بضوابط معينة كضرورة استحصال 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 لضرورات 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 حددها المشرع وفقاً لقواعد وإجراءات محددة"[٣٦]. وهذا ما يقتضي من المشرع الوطني أن يحدد مسبقاً الافعال المجرمة والعقوبات المقررة لها متى ما وقعت ضمن نطاق معين يتمثل بحدود إقليم الدولة الخاضعة لقوانينها النافذة وفقاً لمبدأ الإقليمية، وتخضع هذه الافعال بدورها لاختصاص المحاكم الوطنية التي تنبسط ولايتها لتشمل كل الدعاوى الناشئة عن تلك الافعال المجرمة على هذا الإقليم، وبالمقابل عدم سريان قانون الدولة وسلطان محاكمها خارج إقليمها كأصل عام، إلا على سبيل الاستثناء وفق ما تقتضيه ضرورات حماية مصالح 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 الجرمية 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 الافعال المكونة للسلوك الجرمي في الجريمة التقليدية بشكل عام والجريمة المعلوماتية بوجه خاص التي يعتبر الغاؤها وعدم تقيدها بالحدود الإقليمية من ابرز سماتها، الأمر الذي يثير 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 الاجرائي فيما يتعلق بتحديد المحكمة المختصة ولا يمتد إلى الجانب الموضوعي لخضوع كامل إقليم لقانون عقابي موضوعي واحد.

إلا أن الأمر قد يدق ويتعقد اكثر في حال التنازع الدولي واتساع نطاق وقوع الجريمة ليشمل اكثر من دولة واكثر 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 وتشريعاً في هذا الصدد بهدف تقييمها وبيان مزاياها ومثالبها، نتطرق من بعدها للإشكاليات المتعلقة بتحديد الاختصاص والحلول المقترحة 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 اقدم المبادئ وأكثرها شيوعاً على مستوى التشريعات، ويفترض هذا المبدأ المعاقبة على كل الجرائم الواقعة على إقليم الدولة بغض النظر عن جنسية مرتكبيها؛ ولكن ما يُثار التساؤل بشأنه هو وفقاً لأي قاعدة أو معيار تعد الجريمة مرتكبة على إقليم ما ؟

اختلف الفقه بهذا الشأن وانقسم إلى اكثر من رأي، فذهب رأي إلى "اعتماد مكان تحقق النشاط أو السلوك الإجرامي معياراً بتحديد مكان وقوع الجريمة وليس مكان تحقق اثارها أو النتيجة الجرمية، ويبرر انصار هذا الاتجاه رأيهم بأن معيار مكان تحقق النتيجة الجرمية يعد معياراً واسعاً مرناً 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 الاثار الجرمية 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 أتاه 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 الاثار أو النتيجة الجرمية كمعيار لتحديد مكان وقوع الجريمة؛ فمما يؤخذ على الاتجاه السابق كونه "لا يعير اهتماماً للمكان الذي تحقق 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 جسامة الضرر كأساس لتقدير التعويض ولا عبرة بخطورة الفعل أو درجة الخطأ؛ كذلك يعد حصول الضرر شرطاً أساسياً لقيام المسؤولية المدنية، فتنفى هذه المسؤولية متى ما انتفى الضرر، ومن ثَم 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 مظهر 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 الاخذ 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 يتلافى 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 تحققت فيه النتيجة أو الذي من المتوقع أو من المنتظر تحققها 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 اطار الجرائم المعلوماتية العابرة للحدود قد لا يقدم مبدأ الإقليمية

حلولاً مناسبة لمشكلة الاختصاص إذا ما اخذنا بعين الاعتبار ما تتسم به الجريمة المعلوماتية من امكانية كبيرة لتفّرق عناصرها في اكثر مكان مما يزيد المسألة تعقيداً إذا ما تمسكت كل دولة وقع على اقليمها عنصر من عناصر الجريمة بمبدأ اقليمية القاعدة الجنائية.

ثانياً : مبدأ شخصية القاعدة الجنائية:

ويراد به "تطبيق القانون الجنائي في الدولة على كل من يحمل جنسيتها ولو ارتكب جريمته خارج اقليمها؛ 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 الاجنبية حتى مع وجود اتفاقيات التعاون القضائي الدولية بحكم ارتفاع عدد الدول المرتبطة بشبكة الإنترنت قياساً بتلك المنضمة إلى مثل هذه الاتفاقيات؛ كما قد يؤدي تطبيق هذا المبدأ إلى محاكمة المتهم اكثر من مرة في دولته بحكم جنسيته وخارج دولته استناداً لمبدأ الإقليمية 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 اساسية لتلك الدولة، أياً كان مكان ارتكابها أو جنسية مرتكبها"[٨]؛ ويلعب هذا المبدأ دوراً مكملاً لمبدأ الإقليمية حيث تحرص الدول على المعاقبة واخضاع 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.[٤٣]

رابعاً : مبدأ عالمية القانون الجنائي:

ويراد به "تطبيق القانون الجنائي للدولة على كل جريمة يقبض على مرتكبها في إقليم الدولة أياً كان الإقليم الذي ارتكبت فيه وأياً كانت جنسية مرتكبها"[٤٤]؛ 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 الاجنبية وغيرها.

المطلب الثاني : الاشكاليات المتعلقة بالاختصاص والحلول المقترحة 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 وتتحقق آثاره في مكان أخر أو أماكن متعددة في دولة اجنبية ثالثة، ومن ثَم تكون هذه الجرائم من حيث المبدأ خارج أية رقابة أو سيطرة من أية جهة، بحيث لا يمكن القول بخضوعها لاختصاص قانون جنائي معين، ومما يثير 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 الاساسية في تلك الدول.

ففي إحدى الحالات "تمكن شاب روسي من الدخول من غير إذن على الحاسب الرئيسي الخاص بمصرف سيتي بنك في الولايات المتحدة الاميركية وقام بتجنيد العديد من المتواطئين معه لفتح حسابات مصرفية في شتى انحاء العالم، ثم اصدر تعليمات إلى حاسوب البنك بتحويل الاموال إلى تلك الحسابات؛ وفي واقعة أخرى تمكن 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 الرئيسة المقدمة لخدمة الإنترنت وذلك كله بهدف تشجيع شراء اسهم إحدى الشركات الاميركية التي كانت تباع في بورصة (*Nasdaq*) وكانت هذه الرسائل تبشر بارتفاع قيمة هذه الاسهم 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 التجريم واختلافها من دولة إلى أخرى ومن الأمثلة التي يسوقها الفقه على ذلك "الدعاية للقنّب الهندي (الخشخاش) فهي أمر غير محظور في بعض البلدان كما هو الحال في هولندا، وفي المقابل يعد مثل هذا السلوك مما يجرّمه 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 الوقائع 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 الجاني الذي يرتكب جريمته في الخارج وتنفيذ الأحكام الاجنبية؛ 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 آنفاً أن الجرائم المعلوماتية لا تتقيد بحدود سوى تلك التي تتقيد 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 القوالب

القانونية التقليدية واعتماد أسس جديدة في تحديد الاختصاص تتلاءم وطبيعة هذه الجرائم في اطار 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 كمحل للنشاط الإجرامي أو محل لتحقق الاثار 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 ينبئ 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 يتنازع فيها الاختصاص بشكل عام فمن الممكن اللجوء إلى فكرة الاختصاص الاصلي والاختصاص الاحتياطي أو الثانوي الذي يلجأ إليه في حال تعذر الاخذ بقانون الاختصاص الاصلي وفقاً لقواعد عامة يتم الاتفاق عليها في ضوء الاتفاقية المقترحة بهذا الشأن، فتعطى الأولوية مثلاً إلى قانون محل تحقق اثار 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 الاجنبية.

الخاتمـــــة

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 والانظمة القانونية التقليدية، تعاظمت معه الحاجة لتدخل تشريعي لمعالجة الاوضاع 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 بحتة، متطورة ومتنوعة، ولا يمكن التخلص منها بسهولة إذا ما استخدمت التطبيقات المناسبة التي تمكننا 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، وبإمكانه 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 وخصوصاً في حال اتصال حاسب المتهم بحاسب آلي أخر 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 اطار دولي، فلا يمكن القول بانطباق قانون عقابي دون أخر إذا كانت الجريمة اساساً لا تعرف حدوداً جغرافية من جهة، ولاختلاف معايير تحديد وقوع الجريمة على مستوى التشريعات العقابية الوطنية من جهة أخرى، مما يضفي بعداً دولياً لهذه الاشكالية يفرض معها حلاً 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. لزوم 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 المناظرة 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 اقل تقدير التوسع في عقد الاتفاقيات الإقليمية أو الثنائية لإيجاد حلول لهذه الاشكالية؛ طبعاً بعد سد الفراغ التشريعي ـموضوعياً وإجرائياًـ في مجال الإجرام المعلوماتي بالنسبة للدول التي لا يوجد فيها قانون عقابي خاص بالجرائم المعلوماتية ومن بينها المشرع العراقي.

الهـــوامـــش

(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 انها 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، اما محل الاعتداء فهي مصالح محمية جنائياً اصلاً على مر الازمان كالأموال والشرف والاعتبار وغيرها ويطلق عليها تسمية (اجرام غير معلوماتي عبر شبكة الإنترنت)؛ اما النوع الثاني فتضم انواعاً 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 بصدد الجانب الاجرائي لهذه الجرائم خصوصا فيما يتعلق بالتفتيش والاختصاص التي يثار 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 الاجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، ١٩٩٨،ص:٢٣ وما بعدها؛ كذلك : د. صالح احمد البربري، دور الشرطة في مكافحة جرائم الإنترنت في اطار الاتفاقية الاوربية . الموقعة في بودابست في٢٠٠١/١١/٢٣، *arablawinfo.com*.

(٢) رمسيس بهنام، المحاكمة والطعن في الأحكام، منشاة المعارف، القاهرة،١٩٩٣، ص:٥٨

(٣) احمد فتحي سرور، الوسيط في قانون الاجراءات الجنائية، دار النهضة العربية، القاهرة، ٢٠١٠، ص٢٣.

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

(٥) عائشة بن قارة مصطفى، حجية الدليل الالكتروني 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 الإنترنت، دار النهضة العربية، القاهرة، ٢٠٠٩، ص:٥٣٤ وما بعدها.

(٩) عبدالفتاح بيومي حجازي، مصدر سابق،ص:٧٨

(١٠) د. هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية (على ضوء اتفاقية بودابست الموقعة في ٢٣ نوفمبر ٢٠٠١)، الطبعة الأولى، دار النهضة العربية . القاهرة، ٢٠٠٦، ص١٦٠.

(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 الكومبيوتر والجرائم المرتكبة عبر الإنترنت، 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:٦٠٤

(١٨) د. عبدالفتاح بيومي حجازي، مصدر سابق، ص٩٢.

(١٩) د. فتحي محمد انور عزت، مصدر سابق،ص٦١٢.

(٢٠) سعيد حسب الله عبدالله، شرح قانون اصول المحاكمات الجزائية، دار الاثير للطباعة والنشر،الموصل،٢٠٠٥،ص٢٠٠.

(٢١) د. عبدالفتاح بيومي حجازي، مصدر سابق،ص:١٩٢.

(٢٢) د.هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة . أسيوط، ١٩٩٤،ص٦٤.

(٢٣) د. هلالي عبدالإله، تفتيش نظم الحاسب 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،ص٣٧٨ ومابعدها

(25) Pirgoff (Donald.k) computer crimes and other crimes against information technology in canda :rev intern de.pen 1993.p241.

(٢٦) جميل عبد الباقي الصغير، الجوانب الاجرائية للجرائم المتعلقة بالإنترنت، مصدر سابق،ص:٤٥؛ كذلك ينظر د. عمر بن يونس، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي "المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسيب وصولاً إلى الدليل الإلكتروني في التحقيقات الجنائية"، الطبعة الأولى، ٢٠٠٤ . ٢٠٠٥، ص٢٠١

(٢٧) د. هلالي عبد اللاه، مصدر سابق،ص:٨٨

(28) Mohrenschlager(manfrred): 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:٤١.

(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، اكاديمية الدراسات العليا، طرابلس،٢٠٠٩،ص:١٢.

(٣٢) د. عبدالله حسين محمود، سرقة المعلومات في الحاسب الآلي، دار النهضة العربية، القاهرة، ص٣٧٦.

(٣٣) حسين بن سعيد الغافري، مصدر سابق،ص:٤٨٥.

(٣٤) أ.د. موسى مسعود أرحومة، مصدر سابق،ص١٢.

(٣٥) للمزيد من التفاصيل ينظر:د.هلالي عبدالإله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي،مصدر سابق،ص٨٠؛ 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، ص٥٣٥.

(٣٧) أ.د.موسى مسعود أرحومة، مصدر سابق،ص:١٤.

(٣٨) ا.د.علي حسين الخلف ود. سلطان الشاوي، المبادئ العامة في قانون العقوبات، مكتبة السنهوري، بغداد، ٢٠١٠، ص٩٧.

(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:٦٤٤.

(٤٦) د. جميل عبدالباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، ص:٤٣.

المصـــــادر

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 ـ 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 الباقي الصغير، الجوانب الاجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، ١٩٩٨.

٥. حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت، دار النهضة العربية، القاهرة، ٢٠٠٩.

٦. حنان ريحان مبارك المضحكي، الجرائم المعلوماتية، منشورات الحلبي الحقوقية، ط١، بيروت، ٢٠١٤.

٧. رمسيس بهنام، المحاكمة والطعن في الأحكام، منشاة المعارف، القاهرة،١٩٩٣.

٨. سعيد حسب الله عبدالله، شرح قانون اصول المحاكمات الجزائية، دار الاثير للطباعة والنشر،الموصل،٢٠٠٥.

٩. سعيد عبداللطيف حسن، اثبات جرائم الكومبيوتر والجرائم المرتكبة عبر الإنترنت، 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 البربري، دور الشرطة في مكافحة جرائم الإنترنت في اطار الاتفاقية الاوربية ـ الموقعة في بودابست في٢٠٠١/١١/٢٣، *arablawinfo.com*.

١٢. عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة، الاسكندرية، ٢٠١٠.

١٣. د. عبدالله حسين محمود، سرقة المعلومات في الحاسب الآلي، دار النهضة العربية، القاهرة،١٩٩٨.

١٤.عبدالفتاح بيومي حجازي، مبادئ الاجراءات الجنائية في جرائم الكومبيوتر والإنترنت، دار الكتب القانونية،مصر،٢٠٠٧.
١٥.عبد القادر قهوجي، الحماية الجنائية للبيانات المعالجة الكترونياً، مؤتمر كلية الشريعة والقانون، جامعة الامارات، ٢٠٠٠.
١٦.د.علي حسين الخلف ود. سلطان الشاوي، المبادئ العامة في قانون العقوبات، مكتبة السنهوري، بغداد، ٢٠١٠.
١٧.د. عمر بن يونس، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي "المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسيب وصولاً إلى الدليل الإلكتروني في التحقيقات الجنائية"، الطبعة الأولى، ٢٠٠٥.
١٨.د. فتحي محمد انور عزت، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية للمجتمع المعلوماتي،ط٢،دار النهضة العربية، القاهرة، ٢٠١٠.
١٩.د.محمود نجيب حسني، شرح قانون الاجراءات الجائية، ط٣،دار النهضة العربية، القاهرة، ١٩٩٨.
٢٠.د.هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة . أسيوط، ١٩٩٤.
٢١.د.هلالي عبدالإله أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية (على ضوء اتفاقية بودابست الموقعة في ٢٣ نوفمبر ٢٠٠١)، الطبعة الأولى، دار النهضة العربية . القاهرة، ٢٠٠٦ .
٢٢.د.هلالي عبدالإله، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي،دار النهضة العربية،القاهرة،١٩٩٧.

ثانياً: البحوث والمجلات

١. د. جميل عبد الباقي 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، اكاديمية 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.