مجلة
البحوث والدراسات القضائية والقانونية

إجراءات الاستدلال والتحقيق في الجرائم الإلكترونية وأثرها على صحة الدليل الإلكتروني وحجيته في الإثبات (*)

القاضي. الدكتور/ شمسان حزام علي الذيب

- ورقة عمل قدمت لورشة العمل الخاصة بعنوان: (دور القضاء في مواجهة الجرائم المالية والإلكترونية وفض المنازعات المصرفية) التي أقامتها وزارة العدل وحقوق الإنسان بالتعاون مع جمعية البنوك اليمنية، صنعاء- ٢٠/٢/٢٠٢٥م..

مقدمة:

لقد تزامن مع الاستخدام الواسع للإنترنت في مختلف مناحي الحياة الاجتماعية والتجارية والعلمية والعسكرية ظهور جرائم إلكترونية غير معهودة في طريقة ارتكابها وخطورتها وآثارها على المجتمع، ويتسع مدلول هذه الجرائم ليشمل الجرائم ضد النفس والمال وجرائم التقنية كتخريب البيانات وسرقتها.

وفي ثنايا هذه الورقة العلمية سيتم تناول إجراءات الاستدلال وأعمال التحقيق الابتدائي في الجرائم الإلكترونية بهدف كشف الجريمة ومرتكبها، وبيان مدى مشروعية ما ينتج عنها من أدلة إثبات على تلك الجرائم وحجيتها أمام القضاء، وخلوها من أوجه البطلان، لما له من أثر في إهدار قيمة الدليل الإلكتروني أمام المحاكم. وقبل ذلك كان من اللازم بيان ماهية الجريمة الإلكترونية وخصائصها.

أولًا: ماهية الجريمة الإلكترونية

لقد تزايدت وتيرة ارتكاب الجرائم بزيادة استخدام الوسائل الإلكترونية، التي ساهمت إلى حد كبير في تمكين المجرمين من ارتكاب جرائمهم بكل سهولة ويسر بعيدًا عن الأنظار، فيكفي أن يكون لدى المجرم جهاز حاسوب مرتبط بالإنترنت، ولديه بعض البرامج التي تمكنه من الانتقال من موقع لآخر، ومن حساب لآخر ليقوم بعدها بارتكاب العشرات من الجرائم العادية والإلكترونية وهو جالس على أريكته. والأكثر خطورة حينما يشعر أن يد العدالة لن تطاله لأن القائمين عليها لا يمتلكون القدرة التي تمكنهم من ذلك. وهنا نعرض بإيجاز تعريف هذه الجريمة وبيان خصائصها في الآتي:

تعريف الجريمة الإلكترونية:

تعرف الجريمة الإلكترونية بأنها الجريمة التي يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوبي. وتشمل جميع الجرائم التي يمكن ارتكابها في البيئة الإلكترونية. وهذا التعريف ورد في توصيات مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقد في فيينا سنة ٢٠٠٠م[١].

وتختلف دوافع ارتكاب هذه الجرائم من سعي لتحقيق الفوائد المادية، أو الانتقام من المجني عليه أو لإثبات القدرة على اختراق البيانات والمعلومات، أو لتحقيق أهداف

(١) مؤتمر الأمم المتحدة لمنع الجريمة ومعاقبة المجرمين، فيينا، ١٠- ١٧ نيسان ٢٠٠٠م.

سياسية، وقد تكون عمدية وقد تكون ناشئة عن طريق الخطأ في تفعيل برنامج أو إدارته، كما أن أركان هذه الجرائم هي ذات الأركان وما اختلف سوى وسيلة ارتكابها.

خصائص الجريمة الإلكترونية:

نظرًا لطبيعة الجريمة الإلكترونية وطريقة ارتكابها، فقد جعل ذلك من الضرورة بمكان أن يتم التعامل معها بخصوصية، بحيث لا ينفرد مأمور الضبط القضائي بإجراء التحريات عن الجريمة والجاني لوحده شأنها شأن الجريمة التقليدية، أو حتى عضو النيابة أثناء التحقيق في مثل هذه الجرائم، بل يلزم أن يقوم به فريق للتعاون على إنجاح التحري أو التحقيق. فالتعامل مع المعلومات الرقمية يحتاج لجهود رجل الشرطة والعلوم الجنائية والنيابة والبرمجة وتحليل النظم، إذ ليس بمقدور واحد منهم أن يكون ملمًا بجميع المهارات اللازمة لكشف خبايا الجرائم المتعلقة بالحاسب الآلي والإنترنت[1]. ومن ثم، فلا يكفي أن يقوم بها مأمور الضبط القضائي على انفراد، بل يحتاج إضافة لكونه ذا مهارة وخبرة- لفريق متخصص ليكون بمقدوره تتبع الجريمة ومرتكبها، حتى لا تذهب جهوده سدى، ويتمكن المجرم من إزالة الأدلة ومحو أثرها قبل أن يصل إليها. وترجع أهمية وجود فريق متكامل أثناء جمع الاستدلالات أو التحقيق الابتدائي في الجرائم الإلكترونية لخصائص تميزها عن غيرها، لعل أهمها ما يلي:

أ- أن الجرائم الإلكترونية يتم ارتكابها في إطار افتراضي مفتوح، تتعدد معه طرق وأساليب ارتكاب الجريمة وتتطور بين فينة وأخرى.

ب- أن المجرم الإلكتروني على درجة عالية من الذكاء والمهارة والقدرة على استغلال الثغرات للنفاذ منها، والتخفي من خلالها وإخفاء آثار جريمته، وبالمقابل تحتاج لمواجهتها بقدرات بشرية عالية وكفاءات قادرة على تتبع الجاني، وتحديد موقعه والأجهزة التي يعمل من خلالها، واسترجاع ما تم إتلافه وحذفه من برامج أو وثائق أو ملفات تدل على ارتكابه للجريمة، باستخدام البرامج الإلكترونية التي تمكنه من القيام بذلك.

جـ- أن مسرح الجريمة الإلكترونية ليس بذات المفهوم القانوني المعلوم لمسرح الجريمة التقليدية، بل يختلف عنه اختلافًا كليًا، فمسرح الجريمة الإلكترونية افتراضي، حيزه ونطاقه مفتوح وغير محدد، ومن هنا تظهر مدى الصعوبة الكبيرة

(١) محمد الأمين البشري، الأساليب الحديثة للتعامل مع الجرائم المستحدثة من طرف أجهزة العدالة الجنائية، حلقة علمية منعقدة خلال ١٧- ٢٠١١/١/١٩م، جامعة نايف للعلوم الأمنية الرياض، ٢٠١١م ص٢٩.

التي يواجها مأمورو الضبط القضائي حينما يقومون بجمع المعلومات والبيانات عن تلك الجريمة ومن قام بارتكابها. وفي ذات الوقت، ليس بمقدورهم التحكم به أو السيطرة عليه وعلى مكوناته على غرار ما هو متبع في الجريمة التقليدية، وكل هذا يجعل مهمة مأمور الضبط القضائي في غاية الصعوبة لغير المؤهلين ويتعذر عليه الوصول لنتيجة صحيحة فيما لو ظل يعمل بذات الكيفية التي يتعامل بها مع الجرائم العادية.

د- صعوبة تحديد مكان ارتكاب الجرائم الالكترونية بصورة سريعة أو تحديد زمانها في بعض الحالات، وكذا خروج بعض الوقائع من نطاق عمل رجال الأمن كون الجريمة الإلكترونية يتم ارتكابها عن بعد، وقد يكون ارتكابها من قبل شبكة إجرامية يقيم كل فرد فيها ببلد مختلف، فماذا عسى أن يقوم به مأمور الضبط القضائي في إدارة أمن محافظة أو مديرية لا توجد لديه أدنى مقومات العمل لمواجهة مثل هذه الجرائم، ناهيك عن صعوبات قانونية تجعل من المتعذر على رجل الأمن تتبع جريمة ارتكبت من بلد آخر، في حال عدم التعاون بين البلدان أو وجود اتفاقيات تسهل من عملية التواصل والتنسيق على غرار ما هو حاصل لدى دول الاتحاد الأوروبي، والذي يمنح مأموري الضبط القضائي سرعة التحري والتحقيق والتتبع للمجرم وسرعة القبض عليه، على خلاف واقعنا العربي وما يحيط به من تعقيدات يجعل ذلك من الصعوبة بمكان.

هـ- أن بعض جرائم الإنترنت تقوم بها أجهزة رسمية لدول لأهداف عسكرية أو أمنية أو سياسية أو اقتصادية، ولعلنا نشاهد ونسمع بين فينة وأخرى مثل هذه الوقائع ولا يكاد يخلو منها نظام، وإن اختلفت في ذلك فسيكون من حيث الطريقة والغاية والأثر الذي ينتج عنها، وفي مثل هذه الحالات كيف لمأمور الضبط القضائي أن يقوم بإجراء التحري؟ وكيف لسلطة التحقيق أن تؤدي عملها بالشكل الصحيح؟ في ظل قصور التشريع وانعدام التعاون. وحينها ستكون مثل هذه الجرائم بعيدة عن معاقبة الفاعل والمساعد والشريك والمحرض، وغالبًا ما يكون تأثير هذه الجرائم سياسيًا بين البلدان وتغيب عنها العدالة الجنائية. وهذه من أهم الصعوبات التي تواجه مأموري الضبط القضائي وسلطات التحقيق كتفجير البيجر واللاسلكي في لبنان، وكذا ما يحدث بين روسيا وأمريكا، واستخدام كل منهما للتكنولوجيا للإضرار بالدولة الأخرى، ومثلها وقائع جنائية كثيرة بين أكثر

من دولة ونجد هذا واضحًا رغم الاتفاقيات كما هو الحال في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، لأن تفعيلها بالشكل الصحيح على أرض الواقع ظل حلمًا يأمل الجميع أن يتحول إلى حقيقة، ويبدو من واقع الحال أنه صعب المنال فيما بين بعض البلدان إن لم يكن فيما بين الأغلب منها[1]، رغم أن الموافقة عليها كانت في وقت مبكر.

و- أن الجرائم الإلكترونية تتسم بطابع السرعة في ارتكابها وترتيب آثارها، وتحتاج لسرعة موازية في جمع المعلومات عنها وعن مرتكبها، لأن التأخير من شأنه جعل الجريمة مستمرة وعبئها أكبر على مأموري الضبط القضائي لإيقاف أثرها، وإلا فقد المجتمع الثقة بمنظومة العدالة برمتها، وذلك يمثل خطرًا كبيرًا فيما لو تحقق.

ز- أن المجني عليهم في الجرائم الإلكترونية دورهم سلبي إلى حد كبير، سواءً كانوا أشخاصًا طبيعيين تعرضوا للاستغلال والابتزاز وسرقة البيانات واختراق الحسابات ونقل الفيروسات إليها وهذه تعتبر من أكثر الجرائم المسجلة باليمن، ومع ذلك لا يبادرون للإبلاغ عن الجريمة، والقليل منهم من يبادر للإبلاغ وتقديم الشكوى على الرغم مما قد يلحق به من ضرر. وكل ذلك راجع للعادات والتقاليد والخوف من العار الذي قد يلحق بالشخص المبلغ من الفعل المجرم. ولا يختلف الحال إن كان المجني عليه شركة أو مؤسسة مالية أو بنكًا، فالملاحظ أنهم لا يبادرون لتقديم شكوى خشية تأثير ذلك على سمعته التجارية وثقة المتعاملين به. فظهور واقعة اختراق حسابات أحد البنوك مثلًا قد يدفع العملاء لقطع تعاملاتهم معه، وسحب مدخراتهم لديه لشعورهم بعدم الثقة والأمان على حساباتهم لدى البنك. وغالبًا ما يسعى البنك للتسوية مع العميل المتضرر ودفع ما خسره دون معرفة أحد بذلك، وهذا يجعل مهمة مأمور الضبط القضائي أو المحقق في غاية الصعوبة، حينما يتحفظ المجني عليه عن الإدلاء بما لديه من بيانات ومعلومات عن الجريمة قد تساعد بضبط المجرم.

(١) وقد تمت الموافقة على هذه الاتفاقية من قبل وزراء الداخلية والعدل العرب في الاجتماع المشترك المنعقد بمقر الأمانة العامة للجامعة العربية بالقاهرة في تاريخ ٢١/١٢/٢٠١٠م.

ثانيًا: الأعمال التي تقوم بها سلطة الاستدلال في الجرائم الإلكترونية

تهدف إجراءات الاستدلال للبحث والتحري عن كافة المعلومات المتعلقة بالجريمة ومعرفة فاعلها باستخدام الوسائل القانونية المتاحة.

ولا يختلف الحال بلزوم اتباع الإجراءات القانونية أثناء جمع الاستدلال، سواءً كانت الجريمة تقليدية أو إلكترونية، حتى لا يؤدي تجاوزها أو إغفالها أو مخالفتها إلى إبطال ما ينتج عنها من أدلة إلكترونية لإثبات الجريمة، وتكون بعد ذلك محلًا للطعن بصحتها وإبطال ما ترتب عليها من آثار.

وتتعدَّد إجراءات الاستدلال في الجرائم الإلكترونية ابتداء من تلقي البلاغ، والقيام بأعمال التحري بطريقة تقليدية أو باستخدام الوسائل الإلكترونية للتحقق من صحة البلاغ أو الشكوى، وضبط الأدلة والوثائق والبيانات التي يتم التوصل إليها، وانتهاء بعرض الأوراق على النيابة، والتي يتعين أن يقوم بها المختصون في إطار الضوابط والأصول القانونية والفنية المنظمة لهذا العمل. ونتناول أهم تلك الإجراءات في الآتي:

١. تلقي البلاغات والشكاوى:

تبدأ الاستدلالات مع بداية تلقي المختصين شكوى أو بلاغًا بوقوع جريمة أو باحتمالية وقوعها، سواءً تم تقديم الشكوى أو البلاغ بطريقة إلكترونية من خلال التطبيقات التي يتم إعدادها خصيصًا لذلك أو بطريقة تقليدية. وكما هو معلوم أن القيام بإجراءات الاستدلال في واقعة أو جريمة عادية لا يثير الإشكال، فمأمورو الضبط القضائي صارت لديهم المعرفة والخبرة الكاملة في القيام بمهامهم في مثل هذه الحالة، وجمع المعلومات والأدلة بكفاءة عالية، غير أن الأمر قد اختلف تمامًا في طريقة عملهم مع وقائع جنائية إلكترونية لم يعهدها الكثير من مأموري الضبط القضائي، ولا تتوافر لديهم الخبرة الكافية للتعاطي معها، إضافة إلى أن الشريعة العامة الإجرائية المنظمة لهذه المهام كانت حال صدورها متعلقة بالجرائم التقليدية ولم يدر بخلد المشرع وجود جرائم إلكترونية تحتاج لكثير من المرونة والتنظيم القانوني المواكب. ومن هنا تظهر الإشكاليات أثناء قيام مأموري الضبط القضائي بأعمال البحث والتحري إلكترونيًا فور تلقيهم للبلاغ أو الشكوى، ناهيك عن عدم وجود الكادر المتخصص بعدد كافٍ لمواجهة مثل هذه الجرائم والعمل على جمع الأدلة الإلكترونية بمهنية واحتراف، والحيلولة دون وقوع الجرائم والحد من خطورتها وآثارها بوسائل إلكترونية، تبعًا لطبيعة الواقعة وظروف ارتكابها.

٢. القيام بأعمال المراقبة الإلكترونية والتحري وجمع المعلومات:

ولقيام مأموري الضبط القضائي بأعمال التحري عن الجريمة والمجرم الإلكتروني، فإن لهم القيام بالأعمال التي تتلاءم مع طبيعة تلك الجرائم والبيئة الإلكترونية التي تنشأ فيها. وتختلف هذه الأعمال عما هو متبع في الجرائم التقليدية غالبًا، من حيث الطريقة والوسيلة المستخدمة، وأهم ما يقوم به مأمور الضبط القضائي بهذا الشأن هو تحديد زمان ومكان ارتكاب الجريمة وأماكن مرتكبيها والوسائل المستخدمة في ارتكابها، ومن تعاون أو سهل للمجرمين ارتكاب تلك الأفعال، وذلك من خلال المراقبة الإلكترونية بواسطة برامج التنصت باعتبارها الوسيلة الوحيدة والفاعلة لتحقيق ذلك، بناءً على إذن مسبق من النيابة العامة. ولمأموري الضبط القضائي في سبيل ذلك استخدام البرامج الإلكترونية المتاحة للقيام بأعمال المراقبة بعد الحصول على إذن قضائي بهدف الكشف على الجريمة وجمع الأدلة الإلكترونية المتعلقة بها. وكل ذلك من أجل سلامة وصحة الأدلة التي يتم التوصل إليها لإثبات الجريمة، لأن عدم مراعاة ذلك سيجعل العمل مجردًا من المشروعية لانتهاكه حق الخصوصية الذي تقرر حمايته بالدستور والقوانين النافذة.

- **حالات المراقبة الإلكترونية:** المراقبة إما أن تكون بإذن القضاء أو بدون إذن، وتختلف آثار كل حالة.
- **الإذن القضائي بالمراقبة:**

أ- إصدار الإذن بالمراقبة: لا تكون المراقبة الإلكترونية قانونية إلا بصدور أمر مسبَّب بذلك من القضاء، شأنها في ذلك شأن المراسلات والمخابرات التليفونية. وفي هذا نص قانون الإجراءات الجزائية اليمني في المادة (١٤٨) على أنه: «للنيابة العامة أن تأمر بضبط جميع الخطابات والرسائل، وأن تأمر بمراقبة المحادثات السلكية واللاسلكية، أو إجراء تسجيل لأحاديث تجري في مكان خاص متى كان ذلك لازمًا لكشف الجريمة، وفي جميع الأحوال يكون الأمر مسببًا ولمدة لا تزيد على ثلاثين يومًا». وكان القانون ذاته بالمادة (١٢ــ ٢) قد نص على أن: «حرية المراسلات البريدية والسلكية واللاسلكية وكافة وسائل الاتصال مكفولة وفقًا للدستور، ولا يجوز مراقبتها، أو تفتيشها، أو إفشاء سريتها، أو تأخيرها، أو مصادرتها إلا في الحالات التي يبينها القانون وبأمر من النيابة العامة أو من المحكمة المختصة». ونصت المادة (١٤) من القانون ذاته، على أنه: «لا يجوز المساس بحرية الحياة الخاصة للمواطن في غير الأحوال المصرح بها في القانون

ويعتبر مساسًا بها ارتكاب أحد الأفعال الآتية:١ـ استراق السمع أو تسجيل أو نقل المحادثات التي تجري في مكان خاص، أو عن طريق الهاتف، أو عن طريق جهاز من الأجهزة أيًا كان نوعه.٢ـ الاطلاع على الخطابات أو الرسائل أو البرقيات أو مصادرتها». ولأجل ذلك نصت المادة (١٦) من القانون ذاته، على أنه: «... استثناء من أحكام المادة (٣٧) لا تنقضي بمضي المدة الدعوى الجزائية الماسة بحرية المواطنين أو كرامتهم والتي تتضمن اعتداء على حرية الحياة الخاصة».

وقد حدَّد القانون الجهة التي تملك إصدار أمر المراقبة وضبط المراسلات عادية كانت أو إلكترونية، وحصرها بالنيابة العامة والمحاكم، ولا تملك أي جهة أخرى إصدار أمرٍ بالمراقبة الإلكترونية للبرامج أو المراسلات، كما لا يجوز إصدار ذلك الأمر إلا لغرض كشف واقعة معينة أو التحقيق فيها، وبمواجهة أشخاص مرتبطين بتلك الواقعة الجنائية دون غيرهم. وبالسياق ذاته، فإن النيابة العامة لا تملك إصدار أمر المراقبة على أشخاص لا علاقة لهم بالواقعة التي تحقق فيها.

ب- تسبيب الأمر الصادر بالمراقبة: كما اشتراط القانون في أمر المراقبة أن يكون مسببًا، كضمانة لمن صدر بحقه الأمر. وقد أكد على ذلك قانون الإجراءات الجزائية بالمادة (١٤٨) والتي تنص على أنه: «... وفي جميع الأحوال يجب أن يكون الأمر مسببًا». وقد وضع القانون حدًا زمنيًا لنفاذ الأمر بالمراقبة حتى لا يظل شبحًا يطارد الأفراد إلى ما لا نهاية، فقيَّد قرار المراقبة بثلاثين يومًا من تاريخ إصداره. ويسري هذا الحكم بذاته على المراقبة الإلكترونية. وقد جاء اشتراط المشرع اليمني صدور الأمر القضائي بالمراقبة بهدف حماية الحرية الخاصة للأفراد، وحتى تكون الأدلة الناتجة عنها مشروعة، بعد أن صار إثبات الجرائم بأية وسيلة من وسائل الإثبات ممكنًا بما فيها الدليل المستمد من المراقبة الإلكترونية.

وإذا كان القانون قد خلا من أي نص ينظم عمل مورِّد خدمة الإنترنت بحماية الحق في الخصوصية بمواجهة السلطة العامة، فإنه بالرجوع لقانون الإجراءات الجزائية نجد أنه قد تضمَّن إلزامًا بضمان سريتها، ويدخل في ذلك التراسل الإلكتروني كوسيلة من وسائل الاتصال بالغير، وإعماله في مواجهة الإدارة، بحيث لا يكون لها الاطلاع على مراسلات الأشخاص، إلا وفق ضوابط قانونية شأنها شأن غيرها من المراسلات حماية للحق بالخصوصية قبل الإدارة والسلطة العامة.

جـ- حالات إصدار الإذن بالمراقبة: لا يجوز لمأموري الضبط القضائي القيام بالمراقبة الإلكترونية للبرامج والمراسلات، أو انتهاك سريتها، أو الاطلاع عليها، أو الكشف عن المعلومة أو الرسالة إلا في الأحوال المبينة بالقانون وبإذن القضاء، لضرورات تتعلق بالنظام العام والأمن القومي، والوقاية من الجرائم، وحماية حقوق وحريات الآخرين، وفقًا لما نص عليه قانون الإجراءات الجزائية اليمني بالمادة (١٤٨) بأنه: «للنيابة العامة أن تأمر بضبط جميع الخطابات والرسائل والصحف والمطبوعات لدى مكاتب البرق وأن تأمر بمراقبة المحادثات السلكية واللاسلكية أو إجراء تسجيل لأحاديث تجري في مكان خاص متى كان ذلك لازمًا لكشف الجريمة وفي جميع الأحوال يكون الأمر مسببًا ولمدة لا تزيد على ثلاثين يومًا».

وإذا كانت تلك الحالات التي نص عليها القانون يجوز فيها المراقبة الإلكترونية بعد صدور إذن القضاء، فهناك حالة أخرى تجوز فيها المراقبة ونشر محتواها أو الاطلاع عليها، وذلك في حال موافقة وقبول صاحب الحساب الإلكتروني[١]، ما لم يكن في ذلك انتهاك لخصوصية المتعاملين مع ذلك الشخص فإنه يلزم الحصول على إذن القضاء وفقًا للقواعد العامة للقيام بتلك المراقبة، ليكون ما يتوصل إليه مأمور الضبط القضائي من أدلة إلكترونية مشروعة وقانونية.

- وسيلة المراقبة الإلكترونية:

تتم المراقبة عادة من خلال برامج لا علاقة لها بملفات وبرامج الشخص المراقب، وليس بمقدور الأشخاص العاديين إدراكها، على خلاف من يعمل بنظام الحاسوب وله إدراك به، فإنه يسهل عليه اكتشاف أنه تحت المراقبة من قبل مؤسسات ضبط قضائي تستخدم تلك الملفات لتفتيش حاسوبه، وقد تكون معرفته بتلك المراقبة مصادفة، سواء كانت بهدف الكشف عن جريمة والتحري عنها، أو لغيره من الأسباب[٢]. ولعل أول ما يجب أن يقوم به المحققون مع كل أعمال تخريبية هو اقتفاء الأثر من خلال المراسلات الإلكترونية التي استقبلها المعتدى عليه، والبحث عن رقم الجهاز[٣]، وتحديد موقعه،

(١) إيمان محمد طاهر، الحماية المدنية لمستخدمي البريد الإلكتروني، مجلة الرافدين للحقوق، المجلد ١٢، العدد ٥٤، لسنة ٢٠١٢، صـ ١٤٨.

(٢) فتحي محمد أنور عزت، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية للمجتمع المعلوماتي، الطبعة الثالثة، منشأة المعارف، الإسكندرية، مصر، ٢٠١٠، صـ ٦٤٣.

(٣) وعنوان IP مسؤول عن التراسل عبر الشبكة، وإيصال تلك المراسلات لوجهتها، وتحديد من أين أرسلت الرسالة الإلكترونية لاشتماله على بيان المنطقة الجغرافية ومزود الخدمة والحاسوب الذي تم استخدامه لإرسالها.

لمعرفة الجاني الذي قام بتلك الأعمال، ويمكن لمزود خدمة الإنترنت أن يراقب المشترك، كما يمكن للشركة التي تقدّم خدمة الاتصال الهاتفي أن تراقبه إن توافرت لديها أجهزة وبرامج خاصة لذلك[1]. وتلك المراقبة تعد مشروعة طالما روعي فيها أحكام القانون، وتمت بناءً على إذن القضاء.

- تجاوز حدود المراقبة:

يتعارض تجاوز مأموري الضبط القضائي والخبراء المكلفين بإجراء المراقبة الإلكترونية مع حرمة الحياة الخاصة، ويمثل مخالفة للقانون، يكون معه للمتضرر رفع الدعاوى المدنية بالتعويض لمخالفة عملهم أحكام القانون، وانتقالهم من العمل المشروع إلى غير المشروع، لأنه ليس لمأمور الضبط القضائي المأذون له بالمراقبة أن يطلع أو يراقب سائر البرامج ونظم المعلومات التي يحتويها الحاسب الآلي وتخرج عن محل الإذن بالمراقبة، وهذا إذا كان أمر المراقبة محصورًا ببرنامج إلكتروني محدَّد دون ما عداه من برامج أُخرى لا ترتبط به. أما إذا كان شاملًا فله مراقبة كل ذلك.

- **المراقبة الإلكترونية بغير إذن القضاء:** لقد أصبح اعتراض ومراقبة التراسل إلكترونيًا عبر الإنترنت وكشف مضمونه ممكنًا عبر مقدم الخدمة، أو من خلال برامج قادرة على تحقيق ذلك تستخدمها جهة الإدارة أو رب العمل.

أ- المراقبة الإلكترونية من قبل الإدارة: لا تعد سريةً المراسلات والتواصل إلكترونيًا بين الأفراد وتمتعهم بالحق بالخصوصية مطلقًا، إذ للسلطات العامة في الدولة أن تقوم بواجباتها نحو المجتمع بحمايته والحيلولة دون الإضرار به، وهي في سبيل قيامها بواجباتها ومهامها تراقب سلامة استخدام تلك الوسائل الإلكترونية مراقبة ظاهرية لحماية الأفراد وحرياتهم من أي انتهاكات لضبط السلم والأمن العام. دون أن تقوم بما يعد خروجًا على ذلك ويدخل في إطار المراقبة القضائية، فهذه تحتاج لإذن القضاء، وفي حال خالفت ذلك وتجاوزت في مراقبتها أحكام القانون، بما يتعارض مع حرمة الحياة الخاصة، فإنها تعد منتهكة لحق الشخص المراقب، واستحقاقه للتعويض عن أية أضرار لحقت به، ما لم يكن قابلًا وموافقًا على مراقبته إلكترونيًا. وإذا أسفرت تلك المراقبة عن كشف جريمة من غير جرائم الشكوى فإن لمأمور الضبط القضائي القيام بكافة الإجراءات اللازمة لضبط

(١) خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، ٢٠١١م، صـ ٢٠٥- ٢٠٦.

الجريمة ومرتكبها وأخذ الإذن من النيابة لتفتيش سائر حساباته الإلكترونية لضبط أي أدلة متعلقة بتلك الجريمة ومعرفة المتعاونين فيها.

ويقتضي ذلك عدم جواز مراقبة البرامج والمراسلات الإلكترونية من قبل الجهات الحكومية، إلا لضرورة تتعلق بالنظام العام، أو الوقاية من الجرائم وحماية الحقوق والحريات، ولا يتم الكشف عن محتوى تلك البرامج والوسائل الإلكترونية إلا بالطرق التي أوردها القانون. ولا يعني وجود الحق في الخصوصية وسرية التراسل أنه حق مطلق، بل مقيد في حال أذن القضاء بمراقبته، أو مراقبة الإدارة في الأحوال التي أجاز لها القانون، وفي حال تجاوزت مراقبة الشخص بمعرفة مراسلاته التي يجريها دون علمه ورغبته، بما يمثل مساسًا بخصوصيات الفرد، فإن مشروعية الدليل المتحصل عليه من خلال تلك المراقبة في التشريع اليمني ستكون محل نظر.

ب- المراقبة الإلكترونية للعمال في أماكن العمل: أعطى القانون لأرباب العمل والشركات سلطة الإشراف والرقابة على العاملين لديهم، بما في ذلك مراقبة الوسائل الإلكترونية المستخدمة لتقديم الخدمات للعملاء والتواصل معهم، بعد أن صار استخدامها ضروريًا وحتميًا في مجال التجارة، ولم يعد بمقدور أي شركة أن تمارس عملها بدونها، لما لها من فاعليته في تبادل المعلومات، وقلة التكاليف فيما بين العاملين مع بعضهم، أو مع إدارة المنشأة، أو في التواصل مع العملاء، وحتى لا يسيء أحد العاملين استخدامه في إرسال رسائل تحمل فيروسات أو تهديدًا أو تعديًا على حقوق الملكية الفكرية، أو تتضمن تحرشًا جنسيًا أو قدحًا أو ذمًا أو تهريبًا للأسرار الخاصة بالعمل، مما يوقع الشركة أو رب العمل في مساءلات قانونية، أو يلحق به خسائر في عمله وسمعته التجارية، فإنه يكون له مراقبة البرنامج الإلكتروني المستخدم في نطاق المشروع[1]، لأن حرية العامل بمراسلاته أثناء العمل ليست مطلقة، بل هي مقيدة بما ليس فيه إساءة للغير باستعمالها، والمحافظة على أسرار العمل وعدم إفشائها كأهم واجب في عمله، وتكفل المراقبة عدم مخالفة ذلك الالتزام.

وفي هذا أوجب قانون العمل اليمني بالمادة (٩٠) على العامل أن يلتزم بالمحافظة على أسرار العمل، وفي حال إخلاله بذلك الواجب يجوز لرب العمل أن ينهي العقد من

(١) عبد الله بن ناصر بن أحمد العمري، الحماية الجنائية للبريد الإلكتروني، رسالة ماجستير غير منشورة، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، الرياض، ٢٠١٠، صـ٧٥.

جانبه بدون إشعار كتابي، أو تحمل الأجر المقرَّر عن فترة الإنذار، مادة (٣٥/ ١ـ ي) من القانون ذاته، وأن يوقع عليه العقوبة الملائمة، بما فيها عقوبة الفصل من العمل مادة (٩٣) من القانون ذاته. لكل ذلك يجوز لرب العمل مراقبة العمال، على اعتبار أن النظام المعلوماتي الذي يستعمله العامل مملوك للشركة.

ولتلافي تلك الإشكالات تتجه الشركات الحديثة لوضع قواعد لموظفيها بإعلامهم بأن الحسابات الإلكترونية والاتصال بالإنترنت يعتبر ملكًا للشركة، وأن لها حق المراقبة الإلكترونية لكل موظف بما يحفظ مصالح الشركة ويحول دون الإضرار بها. أما في حال عدم إعلام العامل بالمراقبة فالأصل حماية حقه في الخصوصية بمراسلاته الإلكترونية أثناء عمله، وقصر جواز مراقبة رب العمل في حالة الخشية من وقوع الضرر من تلك المراسلات، وقيام المبررات الدالة على ذلك وبالبناء على ذلك تم اكتشاف جريمة إلكترونية ارتكبها العامل أثناء عمله، وسمح رب العمل لمأموري الضبط القضائي بالمراقبة الإلكترونية وجمع الأدلة المتعلقة بتلك لجريمة، فإن تلك المراقبة ستكون مشروعة والدليل الناشئ عنها صحيح، ولو لم يصدر أمر من القضاء بذلك.

٣- القيام بإجراء المعاينة بطريقة الإلكترونية:

وذلك من خلال اطلاع مأمور الضبط القضائي على البرنامج الإلكتروني المستخدم في ارتكاب الجريمة، وتجميع محتوياته من المراسلات والصور والفيديوهات التي يعثر عليها في ذلك البرنامج، والمتعلقة بالجريمة والقيام بنسخها وحفظها تمهيدًا لعرضها على النيابة العامة لاتخاذ ما تراه في ذلك، وهذا وفقًا لمقتضى نص المادة (٩٢) إجراءات جزائية. والمعاينة التي يقوم بها مأمورو الضبط تكون في حدود المعاينة الظاهرية للموقع أو الحساب الإلكتروني بحسب ما يتاح له ذلك دون حاجة للدخول إلى البيانات والمعلومات المشفرة، فهذه لا تعد معاينة، بل تعد تفتيشاً إلكترونيًا يحتاج معه مأمور الضبط لإذن قضائي، لأن عدم مراعاة ذلك من شأنه أن يجعل الدليل الذي يتم التوصل إليه مثارًا للطعن ببطلانه وعدم مشروعيته.

أما بخصوص المتابعة العادية لشبكة الإنترنت من قبل مأموري الضبط القضائي فإنه لا يلزم معها الإذن بذلك، لأن تلك الشبكة متاح للجميع استخدامها، ومطالعة ما يكتب من خلالها، ومشاهدة الأفلام والبرامج والصور، ومتى ما وجد مأمور الضبط القضائي جريمة وضبط الدليل عليها أثناء قيامه بذلك، فهو صحيح ولا يسري إليه البطلان لعدم حصول الإذن.

٤- ضبط الأدلة المادية والبيانات والوثائق الإلكترونية:

يقوم مأمور الضبط القضائي بضبط ما يظهر له وما يتوصل إليه من وثائق إلكترونية أو عادية أو أجهزة حاسوب أو تلفونات متعلقة بالجريمة الإلكترونية ومرتكبيها، وله كذلك ضبط الفلاشات والهارد والقرص المدمج والمودم والطابعة وأي وسائل متعلقة بها، وله القيام بضبط البيانات الإلكترونية وحفظ نسخة منها، سواءً كانت ملفات أو صورًا أو فيديوهات أو مراسلات وعرضها على النيابة العامة بصورة صحيحة دون عبث بمحتواها.

ويلزم لصحة وسلامة هذا الإجراء من قبل مأمور الضبط القضائي أن يكون بمناسبة عمله واطلاعه على الجريمة بناءً على ذلك، كما لو كان مكلفًا بأعمال مراقبة اعتيادية وحدثت جريمة فله ضبط الأدلة باعتبارها واقعة تلبس إلكتروني، أما إذا لم تكن في هذه الحالة وكانت أثناء قيامه بالتفتيش أو المراقبة الإلكترونية فيلزم لصحة ذلك الإجراء وسلامة ما ينتج عنه من أدلة إلكترونية أن يكون بناء على إذن النيابة وإلا كان باطلًا وما ترتب عليه من آثر.

٥- التفتيش الالكتروني:

ويكون لمأمور الضبط القضائي تفتيش الحسابات الإلكترونية والبرامج إذا تحققت شروط التفتيش من وقوع جريمة ونسبتها لمتهم محدد وتوافرت مسوّغات كافية على أن تفتيش الحساب الإلكتروني التابع لذلك الشخص من شأنه أن يوصل إلى الأدلة والبيانات المثبتة للجريمة محل التفتيش، ومعرفة الحقيقة المتعلقة بها وبمرتكبيها. وإذا كان مأمور الضبط القضائي مأذونًا له بتفتيش حساب إلكتروني معين أو جهاز حاسوب بذاته، وكان ذلك الحساب مرتبطًا بحسابات إلكترونية أخرى يلزم التفتيش عليها حتى يتم الإحاطة بمحتواها وما فيها من أدلة، فإن لمأمور الضبط القضائي تفتيش تلك الحسابات أو الأجهزة الإلكترونية بناء على إذن بتفتيشها، ولا يكتفي بالإذن السابق، وهذا إذا كانت داخل البلد وبالإمكان التفتيش عليها بصورة مباشرة، أما إذا كانت تلك الحسابات الإلكترونية خارج البلد، فإنه يلزم كذلك الحصول على إذن النيابة بتفتيش تلك الحسابات عن بعد، ليكون ما يتوصل إليه مأمور الضبط القضائي من أدلة مشروعة وقانونية، حتى وإن كان التفتيش على حسابات خارج البلد طالما ارتبطت بالجريمة الواقعة داخل البلد وأمتد أثرها إليه. وفي حال تجاوز مأمورو الضبط القضائي ذلك فإن التفتيش يكون باطلًا وما يتوصل إليه من أدله سيكون باطلًا كذلك.

أما إذا كان مأمور الضبط القضائي يقوم بالتفتيش في شبكة الإنترنت عمومًا، فإنه

لا يلزم الإذن له بالتفتيش فيها، لأن تلك الشبكة متاح للجميع استخدامها والدخول فيها، ومتى عثر مأمور الضبط القضائي على أي دليل أثناء قيامة بذلك فهو صحيح ولا يسري إليه البطلان لعدم الإذن بالتفتيش.

- تجاوز حدود التفتيش:

وفي حال ما إذا كان مأمور الضبط القضائي مأذونًا له بالتفتيش على حسابات إلكترونية أو برامج محددة، وتجاوز حدود ذلك الإذن بالتفتيش لحسابات وبرامج أخرى، فإن ذلك التجاوز يعد انتهاكًا للحق بالخصوصية وحرمة الحياة الخاصة ومخالفًا لأحكام القانون، ويساءل عن ذلك التجاوز جنائيًا ومدنيًا بالتعويض عن الأضرار. ناهيك عن عدم مشروعية ما يتوصل إليه من أدلة إلكترونية ناتجة عن ذلك التفتيش الباطل.

ثالثًا: إجراءات التحقيق في الجرائم الإلكترونية

للنيابة العامة في سبيل جمع الأدلة الإلكترونية عن الجريمة ومعرفة مرتكبيها أن تقوم بالإجراءات الكفيلة بتحقيق ذلك، ولها سلطة واسعة للوصول لتلك النتيجة بما فيها استخدام الوسائل الإلكترونية والاستعانة بالخبراء أثناء التحقيق بهذه الجرائم لتسهيل مهمتها وتجاوز أي صعوبات وعوائق، وتلك الإجراءات التي يكون للنيابة العامة القيام بها وهي بصدد القيام بوظيفتها إزاء الجرائم الإلكترونية لا تختلف كثيرًا عما يتم من إجراءات في الجرائم التقليدية، وإن كانت تتميز بطريقة إجرائها والوسائل المستخدمة لجمع الأدلة، ولعل أهمها ما يلي:

١- القيام بعمل المعاينة في الجرائم الإلكترونية:

للنيابة العامة القيام بمعاينة الحسابات والبرامج الإلكترونية لمعرفة ما تحتويه من وثائق وملفات ومعطيات قد تفيد في الوصول للحقيقة وكشف الغموض الناشئ عن الجريمة الإلكترونية وتحديد مرتكبيها، ولها في سبيل ذلك الاستعانة بالخبراء لتحديد الأجهزة والحسابات التي تتم معاينة محتواها من برامج ورسائل ووسائط تخزين وأقراص وأجهزة إلكترونية مرتبطة ومتصلة بها، بما يمكنها من الإحاطة بمسرح الجريمة وتوثيق وحفظ الأدلة الإلكترونية التي يتوصل إليها. وإذا كانت المعاينة تتشابه مع التفتيش إلا أن المراد منها حصر المحتوى الظاهر لتلك الحسابات دون الغوص في تفاصيلها وتجميع كل مفرداتها، لأنه قد لا تكون تلك الحسابات أو البرامج هي المحل الحقيقي للجريمة أو

الوسيلة المستخدمة لارتكابها، وتكون في حسابات إلكترونية أخرى هي الأولى بالفحص والتدقيق لما تحويه من بيانات ومعلومات متعلقة بالجريمة محل التحقيق.

٢- ندب الخبير التقني في الجرائم الإلكترونية:

تعد استعانة النيابة العامة بالخبراء للكشف عن الجرائم الإلكترونية من أهم إجراءات التحقيق بهدف الوصول للأدلة الإلكترونية وتجميعها والتأكد من صحتها والحفاظ عليها. وهذا حق للنيابة العامة خولها القانون في المسائل الفنية الغامضة التي يدق فيها على عضو النيابة معرفة وإدراك تفاصيل تلك الوقائع أو حتى معرفتها والوصول إليها. كما أن لعضو النيابة الاستعانة بخبير تقني لتجاوز كلمات المرور وفك تشفير الحسابات الإلكترونية، حتى يستطيع القيام بالمعاينة أو التفتيش للحسابات أو البرامج الإلكترونية والإحاطة بتفاصيل الجريمة وإثباتها، وحتى يقوم بجمع الأدلة الإلكترونية بطريقة صحيحة وحفظها من الضياع والتبديد. وهنا تظهر أهمية الاستعانة بالخبير التقني أثناء التحقيق لما له من دور في جمع الأدلة وفقًا لما تقضي به المادة (١٣٠) إجراءات جزائية، تمهيدًا لتقديمها للمحكمة بعد ذلك.

٣- القيام بأعمال التفتيش الإلكتروني والضبط:

وفي هذا الإجراء تقوم النيابة العامة بصورة مباشرة أو من خلال الاستعانة بالخبراء التقنيين بأعمال التفتيش للحسابات الإلكترونية أو البرامج أو الأقراص المدمجة أو أجهزة الحاسوب أو الهاتف، سواءً كان ذلك التفتيش للمحتوى على أدوات وأجهزة محجوزة لدى النيابة، أو حتى من خلال التفتيش إلكترونيًا عن بعد باستخدام أجهزة وبرامج حديثة للقيام بذلك. وفي هذا نصت المادة (٢٥) من قانون مكافحة الاتجار بالبشر[١]، على سريان أحكامه على كل من ارتكب جريمة من جرائم الاتجار بالبشر ولو كان خارج حدود اليمن أيًا كانت جنسيته، ومن جهة أخرى، أكَّدَت المادة (٢٦) من ذات القانون على امتداد اختصاص سلطة الاستدلال والنيابة والمحكمة في كافة الجرائم التي نص عليها قانون الاتجار بالبشر، ليشمل ذلك القيام بكافة الإجراءات بما فيها التفتيش والمراقبة الإلكترونية وسائر إجراءات التحقيق.

ويعد التفتيش من قبل النيابة العامة في هذه الجرائم ذا أهمية كبيرة، فمن خلاله يكون بمقدورها جمع الأدلة الإلكترونية المخزنة، سواءً كانت وثائق أو صورًا أو تسجيلات

(١) وهو القانون رقم ١ لسنة ٢٠١٨م بشأن مكافحة الاتجار بالبشر، والصادر في ١١ يناير ٢٠١٨م.

أو بيانات أو معلومات أيًا كانت طريقة عملها وتدوينها على ذلك الحساب لإثبات وقوع الجريمة ونسبتها لمن قام بارتكابها، سواءً كانت جريمة عادية أو إلكترونية، ولا يختلف هذا الإجراء الذي تقوم به النيابة إلا من حيث الوسيلة والطريقة المستخدمة، وإلا فما نص عليه قانون الإجراءات الجزائية يكفي لتقوم النيابة بذلك في الجرائم الإلكترونية، طالما توافرت مبررات القيام به من اتهام شخص محدَّد بارتكاب جريمة وكان ممكنًا ضبط أشياء تفيد في كشف غموضها.

- شروط تفتيش الحسابات والبرامج الإلكترونية:

أ- **وقوع جريمة:** لابد لصحة إجراء التفتيش أن نكون بصدد جريمة إلكترونية واقعة بالفعل سواءً كانت جسيمة أو غير جسيمة كالتهديد الذي يمثل اعتداءً على حق الإنسان في الأمان والاطمئنان[1]، أو بارتكاب جريمة القتل كاعتداء على حقه في الحياة، كتلك الواقعة التي قام فيها شخص بقتل زوجته عمدًا عن طريق البريد الإلكتروني، حينما كانت تعاني من مرض، وتم وضعها تحت جهاز (المونيتور)، فاخترق الزوج في أقل من ساعة الشبكة المعلوماتية للمستشفى، وغيَّر الوصفة الطبية الخاصة بها والواردة في البريد الإلكتروني الخاص بالمستشفى على نحو قاتل، وحينما أُعطيت الأدوية من قبل الممرضة ماتت المريضة، واعتبر القضاء أن الممرضة لم تكن سوى وسيلة في ارتكاب الجريمة، وأدان الزوج بجريمة القتل العمد، لأنه تعمد الدخول لنظام المعالجة الآلية للبيانات وغيَّر في المعلومات بقصد قتل زوجته[2].

ب-**اتهام شخص محدَّد بارتكاب جريمة إلكترونية:** بأن تتوافر في حق الشخص المراد تفتيشه دلائل كافية بأنه قد ارتكب أو ساهم بارتكاب جريمة إلكترونية أو

(١) وفي واقعة تلبس بجريمة إلكترونية قام متهم بالأردن عام ٢٠٠٤م بتهديد العاملين بدائرة المخابرات باستخدام العنف، برسالة وجهها من موقعه الإلكتروني للموقع الخاص بتلك الدائرة، فتمكن بعدها البحث الجنائي من متابعة مسار المراسلات، وصولًا لبروتوكول الإنترنت، ورصدت تردد المتهم على أحد المقاهي في العاصمة عمان، من خلال تشغيل بريده الإلكتروني على عدد من أجهزة ذلك المقهى، فراقبت الدخول إلى بروتوكولات الأجهزة في المقهى، حتى قام المتهم بزيارته واستخدام أحد الأجهزة، فتم إلقاء القبض عليه متلبسًا بكتابة الرسائل الإلكترونية، وأسندت له أمام المحكمة تهمة التهديد باستخدام العنف، بهدف الإخلال بالنظام العام، وتعريض سلامة المجتمع وأمنه للخطر. مشار لدى: عادل عزام سقف الحيط، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الإلكترونية، الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان، الأردن، ٢٠١٥م، صـ٢٣٦.

(٢) عبد الفتاح بيومي حجازي، الجريمة في عصر العولمة، دار الفكر الجامعي، الإسكندرية، مصر، ٢٠٠٧م، صـ١٥٢.

شارك فيها، كتلك الواقعة التي قام بها أحد العاملين في إحدى الشركات بإدخال نظام تدمير للمعلومات الموجودة في البريد الإلكتروني الخاص بالشركة، بعد أن تم إقصاؤه من عمله[1]. ويكون إثبات الوقائع المجرمة من خلال تحديد جهاز الحاسوب المستخدم وربط هوية المشتبه به بذلك الجهاز الذي ارتكبت منه الجريمة، ومعرفة ما إذا كان شخصًا آخر قد اخترق الحساب الإلكتروني، وانتحل بيانات صاحبه ونفذ الجريمة من خلاله.

جـ- توافر مسوغّات التفتيش: كما يجب توافر مسوّغات كافية لتفتيش الحساب أو البرنامج الإلكتروني بما يوصل للأدلة والبيانات المثبتة للجريمة محل التفتيش، وإلا امتنع التفتيش وبطلت أية إجراءات أو آثار تترتب عليه.

ومما ينبغي أن يراعى في هذا الجانب، أن التفتيش الإلكتروني لا يتقيد بذات طريقة إجراء التفتيش العادي كعدم القيام به قبل شروق الشمس وبعد غروبها وفقًا للمادة (١٤٤) إجراءات جزائية، لأن الجرائم المرتكبة إلكترونيًا قد تتم في أي زمن من ليل أو نهار، وإعمال تلك القواعد يؤدي لضياع الأدلة وصعوبة العثور عليها إذا تم تأجيل التفتيش، بل على العكس من ذلك فطبيعتها تقتضي سرعة البحث عنها وعن مرتكبها والتفتيش عنها في أي وقت، وهو ما استدعى التدخل لوضع ضوابط وإجراءات تلائم هذا النوع من الأفعال المجرمة في مشروع قانون مكافحة جرائم التقنية، غير ما تضمنته القواعد والشروط المنصوص عليها في القانون المنظم لإجراءات التفتيش العادية.

- طرق التفتيش الإلكتروني وآثاره:

هناك طريقتان للتفتيش الإلكتروني، إحداهما تقليدية والأخرى حديثة، وهما كما يلي:

أ - **الطريقة التقليدية للتفتيش الإلكتروني:** وتتم حينما يعطي المتهم بإرادته للقائم بالتفتيش رمز الدخول (user name) لحسابه الإلكتروني، أو بناءً على طلب المحقق، ليقوم بفتح جهاز الحاسوب الخاص بالمتهم، وأي جهاز آخر مرتبط بشبكة الإنترنت، ودخول الحساب الإلكتروني لتفتيش محتواه وفتح الرسائل المخزنة فيه، سواء كانت صادرة أو واردة أو محفوظة، وعندما يعثر على الرسالة المطلوبة أو أي ملف باعتباره الدليل الذي يتم البحث عنه يتم نقله لدعامة أخرى مثل الأقراص الممغنطة أو أي وسيلة مناسبة، أو

(١) عدي جبار هادي، الحماية الجزائية للبريد الإلكتروني، بحث منشور في مجلة رسالة الحقوق، جامعة كربلاء، السنة الثانية، العدد الثالث، ٢٠١٠م، صـ ١٧٦.

طباعته على ورق، أما إذا كان المتهم قد حذف الملف أو الرسالة وهذا وارد لإخفاء دليل الواقعة، فإنه بإمكان المحقق أن يعود لملفات حفظ الرسائل وسلة المحذوفات التي توجد بها الرسالة، وقد يتوصل المحقِّق بهذه الطريقة لقراءتها واستخراجها وحفظها.

ب- إجبار المتهم على بيان شفرة الدخول للحساب الإلكتروني: أن إجبار المتهم على بيان شفرة الدخول للحساب الإلكتروني، حتى يتمكن المحقق من معرفة محتوى ذلك الحساب محل خلاف؟ فبعض رجال الفقه يرون بأن مالك الحاسوب أو مستغله ملزم بتزويد القائم بالتفتيش بكلمة السر، على اعتبار أن مفتاح الدخول للحاسوب كمفتاح دخول المنزل فيقاس عليه، وإذا امتنع صاحب الحساب عن الإدلاء بكلمة السر أمكن إجباره على ذلك من قبل المفتش بأمر قضائي[1]، من أجل الوصول لدليل الإدانة ضد مرتكب الأعمال المجرمة وتتبع مصدر الرسائل. ويؤخذ على هذا القول قياسه تفتيش البرامج الإلكترونية وجهاز الحاسوب بتفتيش المنازل والأشياء المادية وهو قياس غير منطقي، لأنه إذا أمكن إجبار المتهم على تسليم مفتاح الدار وامتنع أمكن دخوله بكسر الأقفال الموضوعة على مداخله، وهذا غير متصور في حال امتنع المتهم عن إعطاء كلمة سر حسابه الإلكتروني، وقد لا تجدي معه أي وسيلة لإجباره على إعطاء الرقم السري، وحينها ستكون الطريقة الثانية هي المثلى بالاستعانة بخبير لكسر شفرة الحساب لمراقبة واستقراء محتواه بناء على إذن قضائي. كما أن ذلك الرأي مجاف للعدالة، لأن في إجبار المتهم على كشف الرقم السري لحسابه الإلكتروني والإدلاء به للنيابة أو طباعة الملفات المخزنة بداخله فيه إجبار له على تقديم دليل ضد نفسه، وهو ما لم يقل به أحد ولا يقبل به القضاء، لأن للمتهم الحق في الكلام والإدلاء ببيانات التشفير إن رغب بكامل إرادته، وله حق الامتناع، دون أن تملك النيابة أو المحكمة إجباره على الإدلاء ببيانات التشفير.

ج- إجبار الشاهد على تقديم الرقم السري للحساب الإلكتروني: أما عن جواز إجبار الشاهد المعلوماتي على البوح برمز دخول الحاسوب إن كان الجهاز محميًا برمز سري؟ فإن الجائز إجباره بأمر قضائي على كشف مفتاح شفرة المعلومات المخزنة بنظام الحاسب الآلي[2]، حينما يتولى مراقبة ذلك الحساب. إذ الواجب عليه قانونًا موافاة النيابة والمحكمة بالمعلومات التي توصَّل إليها وتعلقت بالقضية محل الخبرة، وإذا أخل بذلك الواجب فهو مستحق للعقاب وفقًا للقواعد العامة. إضافة لذلك، فإن المحكمة إذا لم تطمئن لتقريره ورغبت بالتحقق، فلها أخذ الرقم السري من ذلك الخبير وإعطاؤه لآخر، وليس له الامتناع

(١) جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، مصر، ٢٠٠٢م، صـ١٠٥.

(٢) مرجع سابق، صـ١٠٥.

عن ذلك، لأن امتناعه غير مبرر وفيه تضليل للعدالة في حال لم يكن صادقًا بنقل البيانات التي توصل إليها من خلال المراقبة أو التفتيش للمحتوى. ولذا أجاز قانون الإجراءات الجزائية بالمادة (٣٣٢) للمحكمة أن تطلب أي شخص كان ولو بإحضاره قهرًا، أو الأمر لأي شخص بتقديم شيء بحيازته إذا كانت فيه مصلحة أو يفيد بكشف الحقيقة. ويدخل الرقم السري للحساب الإلكتروني في هذا الإطار إن كان فيه ما يفيد بمعرفة الحقيقة.

د- الطريقة الثانية للتفتيش الإلكتروني الاستعانة بخبير معلوماتي: وتكون الاستعانة بخبير وفق الإجراءات وفي الأحوال التي تتحقق معها مبررات الاستعانة به، وقد نظمها المشرع اليمني في المواد (٢٠٧- ٢١٦) من قانون الإجراءات الجزائية، فجعل من حق النيابة العامة أن تطلب من أي شخص له خبرة فنية إبداء الرأي في مسألة متعلقة بالتحقيق، وعلى الخبير حلف اليمين أمام المحقق قبل مباشرته العمل[١]. وذلك حينما لا يقبل المتهم إعطاء المحقق رمز الدخول إلى الحساب الخاص به، فيكون اللجوء للخبرة الفنية[٢] لفك الشفرة باستخدام البرامج التي تؤدي إلى ذلك، بعد أن ترجح عدم جواز إجبار المتهم على فك شفرة الدخول، أو إلزامه بالإفصاح والكشف عن أكواد الدخول وكلمات السر، لتنافى ذلك مع حقه في الصمت والامتناع عن الإجابة. وحتى يكون عمل الخبير مشروعًا لابد أن يكون مكلفًا بذلك من قبل النيابة وإلا كان الدليل المتحصل عليه من عمل الخبرة غير مشروع، ولا تملك المحكمة أن تستند إليه في حكمها وتكوين قناعتها، وإلا كان حكمها مشوبًا بعيب مخالفة القانون ومآله النقض.

الأثر المترتب على التفتيش: قد ينتج عن التفتيش الإلكتروني الوصول للأدلة التي تقود إلى الجريمة ومعرفة الجاني. وفي حال وجد القائم بالتفتيش أدلة إلكترونية تشير لارتكاب جرائم أُخرى غير التي قام بالتفتيش من أجلها، فله حينها ضبط تلك الأدلة الإلكترونية المتعلقة بتلك الجرائم، وتكون حالة التلبس قائمة في حق من قام عليه ذلك الدليل لظهورها عرضًا أثناء التفتيش، ما دام أنه لم يكن في تفتيشه متجاوزًا للغرض من التفتيش. وهو ما أجازه المشرع لسلطة التحقيق بضبط أي شيء توافرت الأسس المعقولة للاعتقاد بأنه متصل بالجريمة الإلكترونية محل التفتيش، وفي هذا نصت المادة (١٣٧) إجراءات جزائية، على أنه «لا يجوز التفتيش إلا للبحث عن الأشياء والآثار الخاصة بالجريمة التي يجري التحقيق بشأنها ولا يتجاوز إلى سواها إلا إذا ظهرت عرضًا

(١) نص المادة ٢٠٧/أ ـ ب من قانون الإجراءات الجزائية اليمني.

(٢) والخبير الإلكتروني شخص تعمق بدراسة الأعمال الإلكترونية، وتخصَّص في أدائه فترة زمنية طويلة، حتى صار قادرًا على إبداء الرأي في الأمور المتصلة بذلك العمل. للمزيد انظر: فتحي محمد أنور عزت، مرجع سابق، صـ ١٠٣.

أثناء التفتيش أشياء تعد حيازتها جريمة أو تفيد في كشف الحقيقة عن جريمة أخرى، فيجوز لمن يقوم بالتفتيش ضبطها وإثباتها في المحضر».

حق المتهم بالاستعانة بخبير تقني: والاستعانة بالخبرة التقنية ليست حكرًا على النيابة أو المحكمة، بل للمتهم بجريمة إلكترونية أن يستعين بخبير تقني أثناء المحاكمة لتفنيد ما قدّم في حقه من أدلة إلكترونية وتقارير فنية، وعرض ما لديه من أدلة دفاع لإثبات براءته. وعدم استجابة المحكمة له في ذلك يجعل حكمها معيبًا لإخلالها بحقه في الدفاع ودحض ما قدمه الادعاء من أدلة إثبات.

٤- الطلب من الجهة المزودة لخدمة الإنترنت بالبيانات المتعلقة بالجريمة:

لا تتوقف معرفة بيانات المتهم ومكان إقامته على ما يقوم به الخبير التقني من بحث، فقد يتم التعرف على تلك البيانات عبر الجهة المزودة لخدمة الإنترنت بناء على طلب بذلك، لأنه بمقدور مزود الخدمة مراقبة المشترك ومعرفة هويته، ومن خلال ذلك تستطيع النيابة إثبات تراسله الذي يحمل في طياته واقعة مجرمة. وحينها تتمكن النيابة العامة من تتبع الدليل في الحساب الإلكتروني وتفتيشه وتحريز ما فيه من أدلة واستخراجها عن طريق طباعتها وتحويلها لنسخ ورقية.

٥- ضبط الأدلة المادية والبيانات والوثائق الإلكترونية:

تقوم النيابة العامة بضبط ما يظهر عن الجريمة الإلكترونية، سواء كانت مادية كالأوراق وأجهزة الحاسوب والتلفون وأجهزة الحفظ كالفلاشات والهارد والقرص المدمج والمودم والطابعة ونحوها مما اتصل بالجريمة وتعلق بها. كما أن للنيابة ضبط البيانات الإلكترونية وحفظ نسخ منها، سواءً كانت عبارة عن وثائق أو ملفات أو صور أو فيديوهات أو مراسلات، والمحافظة عليها حتى تقديمها للمحكمة.

أما إذا تم ضبط تلك الأدلة من قبل مأمور الضبط القضائي فيلزم لصحة هذا الإجراء أن يكون بمناسبة عمله واطلاعه على الجريمة، كما لو كان مكلفًا بأعمال مراقبة اعتيادية وحدثت جريمة فله القيام بضبط الأدلة باعتبارها واقعة تلبس إلكتروني، أما إذا لم تكن في هذه الحالة وكانت أثناء قيامه بالتفتيش فيلزم لصحة ذلك الإجراء وسلامة ما نتج عنه من أدلة أن يكون بناء على إذن النيابة وإلا كان باطلًا وما ترتب عليه من آثار.

٦- سماع الشهود في الجرائم الإلكترونية وتدوينها في محاضر رسمية:

وهؤلاء الشهود يتم سماعهم من قبل النيابة العامة بهدف معرفة حقيقة الأشياء والمستندات الإلكترونية وصلتها بالجريمة والمجرم، وقد يدلي بهذه الشهادة خبراء تم تكليفهم لفحص المحتوى الإلكتروني إذا غمضت فيه وقائع أو ملابسات معينة، أو من قبل مأموري الضبط القضائي حينما تأذن لهم النيابة العامة بإجراء المراقبة الإلكترونية وتتبع المجرم، لأنه إضافة لما يقوم به من مهام بحدود اختصاصه وعمله تسمع النيابة لما يدلي به من توضيحات وتفصيلات عن الجريمة ومرتكبها، وكذا الاستدلال بشهاداته أمام المحكمة عن تلك الجريمة كدليل لا يستغنى عنه.

وسماع الشهادة قد يتم بصورة مباشرة من الشاهد، وقد يتم سماعها عن بعد، وفي هذه الحالة الأخيرة يحتاج لتعديل تشريعي ليكون صحيحًا خاليًا من أي مطعن في صحته وسلامة القيام به قانونًا[1]. وغالبًا ما يكون الشاهد بمثل هذه الجرائم متخصصًا بتقنية المعلومات وشبكات الاتصال لما له من خبرة في نظام المعالجة الآلية للبيانات.

٧ـ استجواب المتهم بارتكاب جريمة إلكترونية:

كما أن للنيابة في حال معرفة المتهم أو المشتبه به في ارتكاب جريمة إلكترونية أن تقوم باستجوابه عن تلك الوقائع، وفقًا لما رسمه قانون الإجراءات الجزائية، إذ لا يختلف الأمر في هذه الحالة، بيد أن الإشكال يكمن حينما يكون المتهم في بلد آخر، إذ يتعذر على النيابة القيام بذلك الإجراء بصورة مباشرة وتحتاج للتعاون مع ذلك البلد، مع ما يصاحب هذا المسلك من صعوبات واقعية وقانونية.

ويعد الاستجواب من أهم إجراءات التحقيق الذي تقوم به النيابة العامة ويحتاج العضو المحقق حينما يقوم باستجواب المتهم بجريمة إلكترونية أن يكون ملمًا بطرق ووسائل ارتكابها حتى يؤتي الاستجواب نتيجته في مواجهة المتهم بالأدلة الإلكترونية التي توصل إليها المحقق. كما يلزم تمكين المتهم من الإدلاء بأقواله بحرية تامة بعد إحاطته علمًا بالتهمة المنسوبة له حتى يكون الاستجواب قانونيًا ولا يتطرق إليه البطلان.

(١) وقد تضمن النظام الأساسي لمحكمة الجنايات الدولية جواز سماع شهادة الشهود بطريقة إلكترونية، رغم خطورة الجرائم وجسامتها.

رابعًا: الصعوبات التي تواجه سلطة الاستدلال والتحقيق بشأن الجرائم الإلكترونية

تتعدد الصعوبات القانونية والواقعية التي تواجه سلطة الاستدلال والنيابة العامة أثناء قيامها بأعمال التحري والتحقيق في الجرائم المعلوماتية، ويمكن بيان أهمها في الآتي:

١- قصور التشريع الإجرائي والعقابي:

من خلال استقراء نصوص التشريع اليمني المنظم للإجراءات الجزائية والقوانين العقابية نجد القصور واضحًا، فقانون أنظمة الدفع المالية والمصرفية رقم (٤٠) لسنة ٢٠٠٦م لم يرد فيه سوى نصوص عقابية على بعض الجرائم. في حين عاقبت المادة (١٠/ب) من قانون مكافحة الاتجار بالبشر بالحبس والغرامة من أنشأ أو استخدم موقعًا إلكترونيًا أو نشر معلومات على الشبكة المعلوماتية بقصد ارتكاب جريمة من جرائم الاتجار بالبشر، مع الحكم بإغلاق الموقع نهائيًا ومصادرة الأموال المتحصلة. وعاقبت المادة (١٥/١، ٢، ٣) من ذات القانون المحرض والشريك وكذلك الشروع في تلك الجرائم. كما عاقبت المادة (١٧) كل من علم بهذه الجرائم ولم يبلغ عنها، وأكد على امتداد اختصاص سلطة الاستدلال والتحقيق والمحاكمة في اليمن لتلك الجرائم بالمادة (٢٦). ومن خلال ذلك نجد أن قانون مكافحة الاتجار بالبشر قد ورد فيه التنظيم مكتملًا للإجراءات والعقوبات بخصوص جرائم الاتجار بالبشر، بما فيها الجرائم الإلكترونية، وتحتاج بقية الجرائم لتنظيم مماثل، وهو ما تضمنه مشروع قانون مكافحة جرائم التقنية الذي لم ير النور بعد. وبالعودة لقانون الإجراءات الجزائية نجد أنه لم يرد فيه نص بإجراءات التحقيق في الجرائم الإلكترونية، ومع ذلك نجد النيابة العامة تعمل حقها في تفسير النصوص التي وردت في مجملها عامة للتعامل مع كافة الجرائم أيًا كانت طبيعتها ووسيلة ارتكابها، وتقوم بكافة الإجراءات الآنف ذكرها، وهي بصدد التحقيق في الجرائم الإلكترونية دون الخروج على مبدأ الشرعية الإجرائية وهي محقة في ذلك. وبالرغم مما سلف تظل تلك النصوص بحاجة لتعديل وتطوير لمضامينها بما يواكب المتغيرات.

ولا يقتصر الأمر على ذلك فالجريمة الإلكترونية قد لا يتوقف نطاقها وأثرها على مستوى وطني، بل يمتد لمستوى دولي، وهذا يستلزم تتبعها والتحقيق فيها بأكثر من مكان والتعاون مع البلدان الأخرى لمجابهة هذه الجريمة من خلال إبرام الاتفاقيات الملزمة بهذا الشأن.

٢- اختلاف الجريمة والأدلة المثبتة لها:

فالدليل الذي يلزم تقديمه للمحكمة هو دليل رقمي يتم استخراجه بطريقة إلكترونية، ونظرًا لكون المجرم الإلكتروني يتمتع بدرجة عالية من الذكاء والمهارة، فقد يقوم بمسح كافة الأدلة من الدعامات الإلكترونية التي تحتوي على دليل ارتكابه للجريمة أو تدل عليها بوقت قياسي، وحينها ستكون المهمة أكثر صعوبة للبحث عنها والوصول إليها.

٣- ضعف التأهيل والتدريب وعدم إلمام المحقق بالجوانب الفنية والتقنية بأجهزة الحاسوب والإنترنت:

والتي تمثل وسيلة ارتكاب الجرائم الإلكترونية ومسرحًا لها في ذات الوقت، وعدم معرفته بطريقة عمل شبكات الإنترنت التي يتم ارتكاب الكثير من الجرائم بواسطتها، فالجرائم غير مرئية ومنفذها مجهول الهوية غالبًا. وانعدام الدورات التدريبية التي يتلقاها مأمور الضبط القضائي وعضو النيابة حول الإنترنت وأجهزة الحاسوب والشبكات وطرق ووسائل استخدامها في ارتكاب الجرائم، وتعريفه بمكونات الحاسوب ووسائط التخزين وأنظمة التشغيل والتطبيقات المختلفة والبرمجيات المستخدمة في المواقع وتبادل الرسائل ونقل الملفات وبرامج الحماية وآلية عمل كل ذلك بهدف تأهيله وتدريبه ليتمكن من جمع الأدلة وحفظها بالشكل الصحيح. ناهيك عن عدم وجود العدد الكافي من المتخصصين والكفاءات البشرية المؤهلة من مأموري الضبط القضائي وأعضاء النيابة العامة للمكافحة والتحقيق في هذه الجرائم، وعدم وجود قضاء متخصص لنظر الجرائم المعلوماتية.

خامسًا: حجية الدليل الإلكتروني الناشئ عن جمع الاستدلال وإجراءات التحقيق

لعلنا ندرك بأن وجود أي مخالفة للقانون الإجرائي بصدد جريمة تقليدية قد يجعل البطلان نتيجة حتمية لتلك الإجراءات وما نتج عنها من أدلة، والحال لا يختلف بالنسبة للجريمة الإلكترونية، فإذا كانت الإجراءات في إطار القانون فإن الدليل الناشئ عنها سيكون مشروعًا وقانونيًا وذا حجية أمام القضاء، والعكس صحيح ويؤدي إلى استبعاد الدليل غير المشروع من الإثبات.

١- شروط قبول الدليل الإلكتروني:

وتتمثل الشروط القانونية في الدليل الإلكتروني ليكون محلًا للقبول من القضاء في الآتي:

أ- **مشروعية الدليل الإلكتروني:** وتعد مشروعية الدليل الإلكتروني ضمانة للأشخاص وحماية لحرياتهم وحقوقهم ضد أي تجاوز من قبل مأمور الضبط القضائي أو سلطة التحقيق، فإذا كان عملها موافقًا للقانون حال قيامها بجمع الأدلة بالتتبع أو المراقبة أو التفتيش، فإن ذلك يجعل الدليل صحيحًا وسليمًا من أي بطلان، ويعول عليه القضاء في أحكامه. أما إذا كان الدليل قد تم الوصول إليه واستخلاصه إلكترونيًا بطريقة غير مشروعة ومخالفة لما رسمه القانون، فإنه سيكون دليلًا غير مقبول قانونًا وقضاءً، ويتولد لدى القاضي الجنائي شعور بالشك في كونه معبرًا عن الحقيقة. فمثلًا إذا أسفر قيام مأمور الضبط القضائي بمراقبة إلكترونية لرسائل شخص ما دون إذن النيابة العامة عن اكتشاف جريمة أو الاطلاع عليها أو تجميع أدلتها فإنها ستكون غير صحيحة ولا مقبولة لقيامها على إجراءات غير قانونية ويكون مآلها البطلان من قبل القضاء إعمالًا لمبدأ الشرعية الإجرائية، ذلك أن حرية القاضي في تكوين قناعته ليست مطلقة، بل لابد أن يكون الدليل الذي يبني عليه قناعته مشروعًا وإلا كان الحكم محلًا للنقض من محاكم أعلى درجة.

كما أن القاضي الجنائي وفقًا للتشريع اليمني ليس مقيدًا بدليل معين، بل يختار من بين ما يطرح عليه ما يراه صالحًا للوصول إلى الحقيقة ولو كان دليلًا إلكترونيًا تم استخلاصه بطريقة مشروعة، إذ لا يوجد في القانون ما يمنع القاضي من قبول الدليل الإلكتروني، ومن ثم، تعد الأدلة الرقمية مشروعة من حيث الوجود القانوني، ويبقى للقاضي تقدير حجيتها طالما روعي بجمعها واستخلاصها إلكترونيًا الشروط القانونية من وجود جريمة وصدور إذن قضائي وانتفى إكراه المتهم باعتبار ذلك الإجراء الباطل يمتد أثره لما تلاه من إجراءات.

ب- **أن يكون الدليل الإلكتروني يقينيًا وغير قابل للشك:** لأن القاضي الجنائي لا يمكن أن يصدر حكمه بالإدانة إلا بدليل يقيني، والشك في الدليل يفسر لمصلحة المتهم وفقًا للقواعد العامة، كما لو أهمل المفتش بحفظ الأدلة والبيانات المتحصلة إلكترونيًا، ولم يقم بتحريزها بطريقة صحيحة فنتج عن ذلك تعرُّضها للعبث

والضياع، فذلك يولد الشك بصحتها وسلامتها. وللمحكمة الاستعانة بخبير للتحقق من سلامة الدليل الإلكتروني وعدم العبث بمضمونه ومحتواه.

جـ- أن يطرح الدليل الإلكتروني على بساط البحث والنقاش لكي يكون بمقدور المتهم تقديم ما لديه من أدله تدحض ذلك الدليل، بما فيها استعانته بالخبرة التقنية. فالقاضي لن يستمد قناعته إلا من أدلة عرضت عليه، إعمالًا لمبدأ المواجهة، حتى لا يكون حكمه قائمًا على علمه الشخصي ومن خارج ما حواه الملف.

٢- تقدير القيمة القانونية للدليل الإلكتروني:

يخضع تقدير قيمة الدليل الإلكتروني لقاضي الموضوع فله أن يصدر حكمه بناءً على ذلك الدليل، وله أن يهدره طالما بنى ذلك على تسبيب سائغ ومقبول. غير أن مما يثار في مسألة تقدير القاضي الجنائي لقيمة الدليل الإلكتروني أنه قد لا يكون ملمًا بتفاصيل تلك الأدلة وطريقة جمعها، باعتبارها أدلة رقمية قد يصعب عليه إدراك تفاصيلها، ويمكن القول هنا بأن سلطة القاضي تضيق في تقدير الدليل الإلكتروني الناتج عن أعمال الخبرة من قبل المتخصصين في هذه البرامج والتقنيات، لأن القاضي لن يكون بمقدوره الإلمام بدقائق الأمور الفنية والتقنية التي لا يدركها سوى متخصص بهذا المجال. ولا يجوز للقاضي أن يضع نفسه محل الخبير في مسألة فنية وعليه الاستعانة به، وللخبير أن يقوم بمهمته باستخدام الأساليب العلمية اللازمة لتحقيق ذلك، ويخضع تقريره لتقدير المحكمة في نطاق ضيق طالما بني على أسباب منطقية وسائغة وإلا كان حكمها محلًا للنقض. في حين يرى البعض بأن من الضرورة إعطاء قوة إلزامية لتقرير الخبير التقني على سند من القول إن القاضي إذا رفض رأي الخبير فقد تعارض مع نفسه، حينما أراد أن يفصل بمسألة سبق أن اعترف في بادئ الأمر بأن الخبير يتمتع فيها بمعرفة ودراية تفوق معرفته الشخصية[١]. ومع ذلك، يظل القول بخضوع تقرير الخبير لتقدير المحكمة وسلطتها التقديرية هو الأولى بالقبول في مثل هذه الحالة، شريطة أن يكون القاضي لديه إلمام كاف بالمسائل التقنية، حتى يكون بمقدوره مناقشة التقرير والرد على ما تضمنه من بيانات ومعلومات لا يتفق محتواها مع روح العدالة والقانون، ليكون رأيه فيها قائمًا على أسس علمية وقانونية.

(١) عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي «دراسة مقارنة»، رسالة ماجستير، جامعة الإسكندرية، كلية الحقوق، السنة الجامعية ٢٠٠٩م، صـ٩١.

٣ -رقابة محكمة النقض على قبول وتقدير القاضي الجنائي للدليل الإلكتروني:

من حيث المبدأ ليس للقاضي الجنائي أن يرفض الدليل لمجرد كونه دليلًا إلكترونيًا، وله سلطة تقدير ذلك الدليل بالأخذ بما يراه مقنعًا ويقينيًا وطرح ما عداه، إعمالًا لمبدأ الاقتناع القضائي المستقر عليه في القضاء، غير أن هذا الاقتناع ليس مجردًا أو مطلقًا، بل يلزم أن يكون مؤصلًا ومؤسسًا بطريقة قانونية من خلال الأسباب التي يعرضها القاضي في حيثيات حكمه، والتي يجيب من خلالها عن الأساس القانوني الذي بني عليه ذلك الحكم، ومن هنا يكون ما حكم به القاضي محل نظر المحكمة الأعلى درجة إن كان موافقًا للقانون من عدمه.

ومما ينبغي الإشارة إليه، أن تقديم أدلة الإثبات الإلكترونية أمام محاكم أول درجة لا يكفي، بل لا بد من إيجاد الوسائل المناسبة لحفظ تلك الأدلة ليسهل الرجوع إليها أمام محكمة الاستئناف والنقض، كلما اقتضى الأمر ذلك، لأن تعرضها للتلف أو العبث قد ينهي حجيتها أمام القضاء ويشكل مدخلًا للتشكيك بصحتها أمام محاكم ثاني درجة، أو في حال إعادة النظر بالقضية إذا نقض الحكم بعد الطعن فيه. وهذا يقتضي توفير إدارات بإمكانات مادية وبشرية وأجهزة حديثة لحفظ تلك الأدلة على مستوى المحاكم الاستئنافية كمرحلة أولى، لتعمم تلك الإدارات على مستوى المحاكم الابتدائية، بهدف تحقيق العدالة وإرساء دعائمها.

المقترحـــــــــات

من خلال هذه الورقة العلمية، يمكن أن نخلص إلى بعض المقترحات:

- التسريع بإقرار وإصدار مشروع قانون مكافحة جرائم تقنية المعلومات لتجاوز أوجه القصور الحالية.
- إنشاء وتفعيل أقسام مكافحة جرائم المعلوماتية بإدارات البحث والأمن بالمحافظات والمديريات والمصالح لتتولى إجراءات جمع الاستدلالات في تلك الجرائم ورفدها بالكفاءات.
- ندعو وزارة الداخلية والسلطة القضائية لاستقطاب الكوادر المؤهلة بمجال الحاسوب والإنترنت ليكونوا ضمن العاملين للاستفادة من قدراتهم ومهاراتهم في مواجهة الإجرام الإلكتروني ضبطًا وتحقيقًا ومحاكمة.
- ضرورة تأهيل القضاة تأهيلًا علميًا وعمليًا باستخدام الوسائل الحديثة وآلية عملها والأدلة الإلكترونية المستخرجة منها، لتكون لديهم القدرة على إدارة المنازعة وامتلاك زمام تسييرها ومناقشة الأدلة والتقارير والطعون المثارة بشأنها باعتبارها من واجبات القاضي، نظرًا لما تثيره هذه الجرائم من إشكالات لا تقل في تأثيرها عن غياب النص القانوني، ونقص معرفة القاضي بهذا المجال يجعله أمام دليل غير مألوف يثير لديه الشك وقد يحمله ذلك على طرحه وعدم الاستناد إليه.
- إضافة المقررات المتعلقة بالجرائم الإلكترونية في مناهج معهد القضاء وأكاديمية الشرطة وكليات القانون في الجامعات الحكومية والخاصة كمواد أساسية.
- إنشاء إدارة مختصة بالمسائل التقنية تابعة لوزارة العدل وحقوق الإنسان أو مصلحة الخبراء- بعد إنشائها- يسهل تأهيلها والتعامل معها ليسهل على النيابة والمحاكم الاستعانة بها فيما قد يُثار من مطاعن حول الأدلة الإلكترونية التي يطعن بصحتها.
- نوصي بتدريب رجال التحقيق والضبط القضائي ومن لهم صلة بتلك الأدلة تجميعًا وحفظًا، وكذا تأهيل المحامين وأساتذة القانون والمتعاملين بهذه الوسائل من التجار والإدارات الرسمية حول التعامل الإلكتروني ومخاطره وضوابطه القانونية ليتمكنوا من إدراكها وفهمها واستيعاب الإشكالات الناتجة عنها، لأن صدور تشريعات مواكبة وتأهيل القضاة لا يكفي ليستقيم الأمر، بل يلزم إعداد الفرد للتعامل بهذه الوسائل والتقنيات المرتبطة بها.

قائمة المراجع والمصادر

- إيمان محمد طاهر، الحماية المدنية لمستخدمي البريد الإلكتروني، مجلة الرافدين للحقوق، المجلد ١٢، العدد ٥٤، لسنة ٢٠١٢م.
- جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، مصر، ٢٠٠٢م.
- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، ٢٠١١م.
- عادل عزام سقف الحيط، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الإلكترونية، الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان، الأردن، ٢٠١٥م.
- عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي «دراسة مقارنة»، رسالة ماجستير، جامعة الإسكندرية، كلية الحقوق، السنة الجامعية ٢٠٠٩م.
- عبد الفتاح بيومي حجازي، الجريمة في عصر العولمة، دار الفكر الجامعي، الإسكندرية، مصر، ٢٠٠٧م.
- عبد الله بن ناصر بن أحمد العمري، الحماية الجنائية للبريد الإلكتروني، رسالة ماجستير غير منشورة، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، الرياض، ٢٠١٠م.
- عدي جبار هادي، الحماية الجزائية للبريد الإلكتروني، بحث منشور في مجلة رسالة الحقوق، جامعة كربلاء، السنة الثانية، العدد الثالث، ٢٠١٠م.
- فتحي محمد أنور عزت.
- فتحي محمد أنور عزت، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية للمجتمع المعلوماتي، الطبعة الثالثة، منشأة المعارف، الإسكندرية، مصر، ٢٠١٠م.
- قانون الإجراءات الجزائية اليمني.
- قانون مكافحة الاتجار بالبشر، والصادر في ١١ يناير ٢٠١٨م.
- محمد الأمين البشري، الأساليب الحديثة للتعامل مع الجرائم المستحدثة من طرف أجهزة العدالة الجنائية، حلقة علمية منعقدة خلال ١٧- ٢٠١١/١/١٩م، جامعة نايف للعلوم الأمنية الرياض، ٢٠١١م.