

تفتيش البيانات المعلوماتية المخزنة كآلية إجرائية: بين اتفاقية بودابست والتشريع الجزائري

الدكتور إدريس قرفلي ، أستاذ محاضر أ ، جامعة محمد خيضر - بسكرة

مقدمة:

كان لثورة تقنية المعلومات انعكاسات واضحة على إثبات الجريمة المعلوماتية مقارنة بالجرائم التقليدية نظرا لطبيعتها وخصائصها، ولعل أهم الصعوبات التي تعترض هيئات مكافحة الجريمة المعلوماتية على المستويين الدولي والداخلي عدم تقيدها بحيز جغرافي محدد، مما يصعب عملية إثباتها ونسبتها لمرتكبها لسهولة التخلص من الأدلة بمحوها أو إتلافها أو التلاعب بالبيانات في ظرف وجيز؛ لوجود برامج لها خاصية الإتلاف والتدمير التلقائي للبيانات بمجرد محاولة جهات المتابعة والتحقيق أو أي شخص غير مصرح له الولوج إليها.

وهو ما جعل عملية الاستدلال والتحقيق عبر البيئة الافتراضية لتعقب المجرمين وتقديمهم للعدالة أمرا بالغ الصعوبة؛ فهو يتطلب مهارات استثنائية في مجال الحاسوب سواء للوصول إلى الجاني أو المحافظة على الدليل الرقمي لضبط الجريمة وإثباتها، ناهيك عن تعارضه مع الضمانات والقيود المقررة قانونا لتمتع محل التفتيش بحرمة قانونية، ومن بين الإجراءات الفنية المتبعة في البحث والتحري لإثبات الجريمة نجد "التفتيش" وهو ما سنعالجه من خلال سعينا للإجابة على الإشكالية الآتية:

ما مدى نجاعة النصوص القانونية التي وضعت على المستويين الدولي(اتفاقية بودابست) والداخلي لتنظيم إجراء التفتيش في مواجهة الجريمة المعلوماتية؟
وقد وضعنا المحاور التالية:

المور الأول: مفهوم التفتفش

عرفت الأنظمة الآائفة فف مراحل تطورها أنواعا من الآآراء اللف تنطو على انتهاك لآقوق الفرد، إلا أن سمو المصلحة العامة للمآمع على مصلحة الفرد جعلها استثناء لاسفما إذا تعلق الأمر بالآرائم المعلوماتفة؛ ومن بفن هذه الآآراء التفتفش آفب بفن بفن بفن تعريفه وخصائصه وطبففته القانونفة ففما فلف:

أولا : تعريف التفتفش

هناك عدة تعريفات فقفة آرففة ورففة للتفتفش نذكر منها؛ تعريفه بأنه "إآراء من إآراء اللفآقف اللف تهدف إلى البآأ أدلة مافة لآنافة أو آنآة لآقف وقوعها فف محل ففتمتع بآرمة المسكن أو الشآص وذلك بهدف إثبات ارتكابها أو نسبفها إلى المآهم وفقا لآراء قانونفة مآددة"⁽¹⁾.

ويعرف أيضا بأنه "البآأ عن الأشياء المتعلقة بالآرمة لضبطها وكل ما ففبفد فف كشف آقفففتها، ففبب أن ففكون للتفتفش سند من القانون"⁽²⁾.

كما عرف بأنه "البآأ فف مستودع سر المآهم عن أشياء فقفد فف كشف الآقفقة ونسبفها إلفه، أو هو الاطلاع على محل منآه القانون آماية آاصة باعآباره مستودع سر صاحبه ففستو فف ذلك أن ففكون المآل سكنا أو ما هو فف آرمة أو أن ففكون شآصا"⁽³⁾.

نآد إلى آانب هذه التعرففات الفقفة الرففة تعريفات أخرى آرففة إلا أنها لا تختلف فف معناها عن الرففة ففما فرفع السبب فف ذلك لأنها مأآوذة منها.

ثانفا : خصائص التفتفش

من آلال التعارف السابقة ففمكن استآلاص أهم خصائص تفتفش نظم الآاسوب والآنترنت وهف:

- 1 إآراء من إآراء اللفآقف : إذ أنه واستنادا للقانون رقم 09/04 المورآ فف 2009 المآضمن القواعد الآاصة للوقافة من الآرائم المآصلة بآناآولآفا الآعلام والاتصال ومكافآتها وآنقفدفا بموجب نص الماده 05 منه؛ واللف آالآنا على الماده 04 نآد أنه فف الفقرة ج ولمآقضىات الآرفبات واللفآقفات القضافة " ففآوز للسلطات القضافة المآآصة وضباط الشرطة القضافة الدآول بفرض التفتفش ولو عن بعد."

يوكل التفتيش إلى جهات مختصة قانونا ويضم خبراء وفنيين في مجال الحاسوب والانترنت، ويملك هؤلاء المحققون الاستعانة بدورهم بخبراء ومتخصصين أكثر دراية في هذا المجال، حيث يجري التفتيش على يد فريق يتكون من:

- المحقق الرئيسي ويكون ممن لهم الخبرة في التحقيق الجنائي.

- خبراء الحاسوب وشبكات الانترنت الذين يعرفون كيفية التعامل مع مثل هذه الجرائم.

- خبراء ضبط وتحرير الأدلة الرقمية العارفين بأمور تفتيش الحاسوب.

- خبراء الحاسوب الذين يتعاملون مع الأنظمة البرمجية.

- خبراء التصوير والبصمات والرسم التخطيطي^(*).

وهو ما نص عليه المشرع الجزائري في تص المادة 05 في فقرتها الأخيرة؛ حيث أجاز لجهات التحقيق الاستعانة بالخبراء المتخصصين في مجال الحاسوب والنظم المعلوماتية لمساعدتهم في مهمة التفتيش وتزويدهم بالمعلومات الضرورية.

2_ يهدف الى البحث عن أدلة مادية أو معنوية للجريمة وضبطها: فالتفتيش هو إجراء عملي وليس فني كإجراء مظاهرات البصمات، وهو يرمي إلى اكتشاف الجريمة والتأكد من وقوعها ثم كشف ملابساتها وإقامة الدليل عليها، حيث يركز على نقاط أساسية تسبق عملية التفتيش مثل:

- مراعاة مدى أهمية الأجهزة والشبكات المتضررة من الجريمة لعمل الجهة المعتدى عليها.

- مدى حساسية البيانات التي يحتمل سرقتها أو إتلافها.

- مستوى الاختراق الأمني الذي تسبب فيه الجاني.

بعد مراعاة كل ذلك تأتي عملية التفتيش التي تحدد للمحققين نوع الأدلة الواجب البحث عنها.

3_ أن التفتيش يعد قيديا على حرمة أو حصانة الشخص الذاتية: وهو ما كفله التشريع الجزائري عندما حدد الجهات المخولة بالتفتيش، وإجراءاته، وحتى زمنه، مع وجود بعض الاستثناءات المتعلقة بالجريمة المعلوماتية سنوردها في حينها⁽⁴⁾.

4_ أن التفتيش يتم وفقا للإجراءات القانونية المقررة: إذ أن المشرع الجزائري حدد إجراءاته والجهة القائمة عليه وفقا لنصوص قانون الإجراءات الجزائية لاسيما المادتين 12 و18 منه؛ حيث أسندتها لرجال الضبطية القضائية إلى جانب الأجهزة التي استحدثها

المرسوم الرئاسي رقم 183/04 المؤرخ في 08 جمادى الأولى 1425 الموافق ل 26 يونيو 2004 المتضمن استحداث المعهد الوطني للأدلة الجنائية وعلم الإآرام للدرك الوطني وتحديد القانون الأساسي؛ والتي نوردها ضمن الأجهزة المختصة بالتفتيش في الجريمة المعلوماتية في المحور الأخير.

ثالثا: الطبيعة القانونية للتفتيش

يعد التحقيق إآراء من إآراءات التحقيق وليس الاستدلال؛ وهو ما أجمع عليه الفقه الجنائي في فرنسا والعراق والأردن ومصر وحتى الجزائر، وقد ظهرت عدة اتجاهات فقهية لتحديد طبيعة التفتيش⁽⁵⁾ خلصت في نهايتها إلى أن التفتيش هو عمل من أعمال التحقيق الابتدائي الذي يكون بعد تحريك الدعوى العمومية بقصد كشف الحقيقة.

المحور الثاني: محل التفتيش في البيئة الرقمية

يرد التفتيش في نظم المعالجة الآلية للمعلومات على المكونات المادية (HARD WARE) والمكونات المنطقية (SOFTWARE) وعلى شبكات اتصالات بعيدة⁽⁶⁾.

أولا: تفتيش المكونات المادية للحاسوب

لا تثار أي مشكلة في تفتيش المكونات المادية للحاسوب؛ كونها ترد على أشياء مادية الإآراءات الجزائية ورد بالمعنى أن التفتيش يرد على الأشياء وهي تنصرف- على الأرجح - على المكونات المادية؛ وهو ما أكدته المادة 64 من نفس القانون سواء كان الحاسوب وملحقاته المادية موجود في أماكن خاصة أو عامة (المنزل أو محمول باليد أو مقهى الانترنت) شرط أن تراعى فيه الضمانات والقيود القانونية.

إلا أن المشرع الجزائري استثنى في تعديل القانون رقم 22/06 المؤرخ في 20/12/2006 في المواد (03/45) و (02/47) و (03/64) من قانون الإآراءات الجزائية تطبيق هذه الضمانات فيما يخص الإآراءات المعلوماتية؛ أي أن هذه الضمانات لا تراعى في إآراءات المعلوماتية، ويرجع السبب في ذلك إلى سهولة التلاعب بالأدلة في الإآراءات المعلوماتية، وسهولة التخلص من الأدلة ومحوها أو إتلافها بسرعة كبيرة، ولتوقف الإثبات في هذه الإآراءات على الدليل الرقمي وحده⁽⁷⁾.

ثانيا: تفتيش المكونات المعنوية للحاسوب

اختلف الفقه حول مسألة تفتيش المكونات المعنوية للحاسوب إلى تيارين:

1- التيار الأول يرى عدم التناسب بين الأحكام الاجرائية للتفتيش بمفهومه التقليدي مع طبيعة الجرائم المعلوماتية؛ كونه يقتصر على الماديات المحسوسة دون الكيانات المنطقية.

2 - التيار الثاني يرى إمكانية انسحاب التفتيش بمفهومه التقليدي إلى البرامج والتطبيقات، فالاختلاف في القياس بين الأحجام المادية والمعنوية لا يحول دون تفتيشها⁽⁸⁾.

أما المشرع الجزائري فقد أجاز صراحة تفتيش النظم المعلوماتية بموجب نص المادة 05 من القانون رقم 04/09 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها؛ حيث جاء فيها "يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية، في إطار قانون الاجراءات الجزائية وفي الحالات المنصوص عليها في المادة 04 أعلاه الدخول، بغرض التفتيش، ولو عن بعد، إلى:

- منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها....."

ثالثا: تفتيش الشبكات المعلوماتية المتصلة بالحاسوب

الشبكة المعلوماتية هي اتصال جهازي حاسوب أو أكثر ببعضها سلكيا أو لاسلكيا، فإذا كانوا في نفس الموقع سمي "شبكة محلية"، أما إذا تفرقت تسمى "شبكة بعيدة المدى"، ومع ظهور الانترنت أعطت الاتصال بعدا دوليا⁽⁹⁾.

هنا تثار إشكالية في إجراء التفتيش خاصة ما يتعلق بالاختصاص؛ فهنا نجد أن المشرع الجزائري أجاز صراحة تفتيش نظم المعلومات المتصلة بالحاسوب محل التفتيش، وتسجيل كل البيانات اللازمة كأدلة إثبات ضد المتهم وفقا لنص المادة 05 من القانون 04/09 أعلاه.

كما أن اتفاقية بودابست لسنة 2001 تسمح للدول الأعضاء أن تمد نطاق التفتيش الذي كان محله جهاز كمبيوتر معين أو جزء منه، وأنها تملك أسبابا تدعو للاعتقاد بأن البيانات التي تسعى إليها مخزنة في نظام معلوماتي آخر أو في جزء منه على أرضه، فالسلطات المختصة تملك التوسع العاجل في نطاق التفتيش أو التلوج بطريقة مشابهة لنظام آخر⁽¹⁰⁾.

وأجازت هذه الاتفاقية الأوروبية الدخول بغرض التفتيش إلى أجهزته وشبكات تابعة لدولة أخرى بدون إذنهما في حالتين هما:

1- إذا تعلق التفتيش بمعلومات أو بيانات مباحة للجمهور.

2- إذا رضي صاحب أو حائز هذه المعلومات بهذا التفتيش⁽¹¹⁾.

المحور الثالث: شروط التفتيش

يرتبط التفتيش بإجراء خطير يمس بالحقوق والحريات؛ لذلك حرصت التشريعات المقارنة على إحاطته بشروط وضمانات أساسية لتحقيق التوازن بين مصلحة المجتمع في عقاب الجاني ومصلحة الفرد من خلال حماية حقوقه وحرياته، من هذه الشروط نجد:

أولا: الشروط الشكلية للتفتيش

من بين أبرز هذه الشروط:

1 - إجراء التفتيش بحضور أشخاص محددين قانونا: باعتبار أن التفتيش فيه مساس بحقوق الأفراد من خلال الاطلاع على أسرارهم؛ فقد أوجبت بعض التشريعات ضرورة حضور المشتبه فيه أو بعض الشهود، كما أجازت تشريعات أخرى التفتيش دون حضور أحد⁽¹²⁾.

أما المشرع الجزائري فقد أوجب ضرورة حصول إجراء التفتيش المتعلق بالساكن وملحقاتها بحضور المشتبه فيه وقت القيام به من طرف الضبطية القضائية، وإذا تعذر ذلك بامتناعه أو أنه كان هاربا يتم استدعاء شاهدين اثنين من غير الموظفين الخاضعين لسلطة ضباط الشرطة القضائية القائمين بالتفتيش حسب المادة 45 من قانون الاجراءات الجزائية.

إلا أن هذا الاجراء استثنى في الجرائم المعلوماتية بموجب القانون 22/06 في الفقرة الأخيرة من المادة أعلاه لذاتية وخصوصية هذا النوع من الجرائم وما يتطلبه من سرية وسرعة في استخلاص الأدلة قبل فقدانها أو التلاعب بها أو إتلافها.

وبالنظر إلى اتفاقية بودابست نجد أنها تناولت إشارة لمسألة الإخطار وذلك في نص المادة 19 في فقرتها 05؛ إذ أن واضعي هذه الاتفاقية بحثوا مسألة معرفة ما إذا كان من المتفق عليه إخطار الأطراف المعنية بالقيام بإجراء تفتيش، ذلك لأن التفتيش في تشريعات بعض الدول الأعضاء لا يقرر الالتزام بالإخطار عن إجراء تفتيش معلوماتي وهذا سيجعل الاتفاقية تدخل شذوذاً أو خروجاً عن تشريعات هذه الدول الأطراف⁽¹³⁾.

من ناحية أخرى فإن بعض الدول ترى أن الإخطار هو عنصر جوهري في إجراء التفتيش؛ لأنه يسمح بالترقية بينه وبين اعتراض البيانات في فترة نقلها والذي يمكن أن يكون سريا بخلاف التفتيش الذي لا يحمل طابع السرية⁽¹⁴⁾.

وعلى العموم فإن مسألة الإخطار وفقا للاتفاقية متروك لتقدير القوانين الداخلية للدول الأطراف فيها، إلا أنه يجب أن نضع في الاعتبار أن جعل نظام الإخطار إلزاميا من شأنه أن يضر بحسن سير التحقيق لذلك توصي الاتفاقية بضرورة إرجاء عملية الإخطار⁽¹⁵⁾.

2 - الميعاد الزمني لاجراء التفتيش: اختلفت التشريعات الاجرائية في وقت تنفيذ التفتيش؛ فمنها من حظر تفتيش المساكن ليلا في أحوال معينة⁽¹⁶⁾ وهذا كضمانة للأفراد في مواجهة سلطة الدولة، ولم تقيد تشريعات أخرى تفتيش المسكن بزمن معين وتركته سلطة في يد القائم بالتفتيش ضمن المدّة المحددة في الإذن⁽¹⁷⁾.

أما التشريع الجزائري فقد حظر تفتيش المساكن وما في حكمها في أوقات معينة، وحدد ميقات تنفيذ هذا الاجراء من الساعة الخامسة صباحا إلى الساعة الثامنة مساء⁽¹⁸⁾، وهناك حالات أجاز فيها الخروج عن هذا الميقات ويصبح في أي ساعة من ساعات النهار والليل عندما يتعلق الأمر بالتحقيق في جرائم معينة كجرائم المخدرات والجريمة المنظمة عبر الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعلومات⁽¹⁹⁾، أو في حالة رضا صاحب السكن صراحة .

ما يستشف من ذلك أن المشرع الجزائري أجاز وكاستثناء في الجريمة المعلوماتية إجراء التفتيش في أي ساعة بناء على إذن مسبق من وكيل الجمهورية المختص.

وبالعودة إلى اتفاقية بودابست نجد أنها تركت هذه التفاصيل الإجرائية لسلطة كل طرف من خلال قوانينه الداخلية وفقا للفقرة الثالثة من المادة 19.

ثانيا: الشروط الموضوعية للتفتيش

يمكن تحديد القواعد الموضوعية لتفتيش نظم الحاسوب والانترنت في قسمين هما السبب والمحل تتناولهما تباعا من خلال:

1 - وجود سبب للتفتيش : هناك دائما أسباب وجيهة استدعت من سلطات التحقيق اللجوء إلى هذا الإجراء وأهم هذه الأسباب هي:

* وقوع جريمة معلوماتية: استنادا لمبدأ الشرعية الجنائية فإن وقوع جريمة معلوماتية في التشريع الجزائري يعني مخالفة الفصل السابع من قانون العقوبات هذا كأصل عام، إلا أنه ووفقا للقانون 04/09 أجاز المشرع الجزائري في نص المادة 05 منه لجهات التحقيق اللجوء إلى التفتيش كإجراء وقائي أو في حالة توفر معلومات عن احتمال وقوع

جرائم معينة أوردتها المادة 04 من هذا القانون؛ والتي من بينها الاعتداء على منظومة معلوماتية على نحو يهدد النظام العام.

*الاشتباه في شخص معين أو اتهامه بارتكاب الجريمة أو الاشتراك فيها: أي أن التفتيش لا يكون إلا بعد وجود اتهام موجه ضد شخص معين أو على الأقل توافر دلائل كافية ضده للاعتقاد بارتكابه للجريمة حتى يمكن انتهاك خصوصيته؛ وتفتيش حاسوبه والبرامج الخاصة، وهذا استنادا لنص المادة 46 من قانون الاجراءات الجزائية، ومن الدلائل القوية التي يمكن بها التفتيش تحديد هوية الحاسوب الذي ارتكبت به الجريمة وصاحبه⁽²⁰⁾.

2 - تحديد محل التفتيش: ينصب محل التفتيش في الجرائم المعلوماتية على مكونات الحاسوب المادية والمعنوية وشبكات الاتصال- كما سبق بيانه في المحور الثاني.

ويضيد تحديد محل التفتيش في اشتراط الإذن من عدمه؛ فاستنادا لنص المادة 44 من قانون الاجراءات الجزائري نجد أنه لا يجوز لضباط الشرطة القضائية الدخول إلى المساكن للتفتيش إلا بإذن مكتوب من وكيل الجمهورية أو قاضي التحقيق؛ وهي ضمانات تنسحب على كل الجرائم بما فيها الجريمة المعلوماتية، أما إذا كان المحل عاما كمقاهي الانترنت فإن أغلب التشريعات لا تتطلب الحصول على الإذن⁽²¹⁾.

وبالعودة إلى المشرع الجزائري نجد أنه لم ينظم هذه الجزئية في شقها المتعلق بالجريمة المعلوماتية؛ إذ أنه لم يحدد لنا شرط الحصول على الإذن لتفتيش المنظومة المعلوماتية من عدمه حيث اكتفى القانون رقم 04/09 بالتحدث عن إعلام جهات التحقيق للسلطة القضائية المختصة عند تمديد التفتيش ليشمل منظومة معلوماتية أخرى فقط.

فالمشرع الجزائري وعلى غرار أغلب التشريعات الأخرى لم يقدم لنا حلا بخصوص ضرورة الحصول على إذن خاص لتفتيش المنظومة المعلوماتية أم يكفي بإذن تفتيش المسكن، كما أن إذن التفتيش للمنظومة المعلوماتية هل يكون عاما يشمل كل البيانات الموجودة في الحاسوب أم أنه يجب أن يكون مخصصا ومحددا لجزء من البيانات فقط؛ هذه الإشكالية وجدت خلافا تشريعيًا وقضائيا في الدول الغربية الأكثر تطورا في المجال المعلوماتي كالولايات المتحدة الأمريكية التي استقر رأيها في النهاية على تحديد مجال الإذن بالتفتيش، أي أن إذن التفتيش لا بد أن يكون محدد لمجال البيانات الخاضعة للتفتيش حفاظا على الحياة الخاصة للأفراد.

أما في اتفاقية بودابست فبالرجوع إلى نص المادة 19 منها نجد أن التفتيش لا يكون إلا بعد توافر شرط محدد للحصول على إذن رسمي بالتفتيش؛ ألا وهو الاعتقاد بتوافر بيانات في مكان معين تساعد على إثبات وقوع جريمة جنائية محدد بمقتضى القوانين الداخلية والأحكام الخاصة بالدفاع عن حقوق الإنسان، إلا أنها لم تفصل في مسألة اشتغال الإذن بالتفتيش على كل البيانات الموجودة في الحاسوب أم على جزء فقط؛ وتركت المسألة للقوانين الداخلية للدول الأطراف لتنظيمها. وهو ما ورد في التقرير التفسيري للاتفاقية.

المحور الرابع: الأجهزة المكلفة بالتفتيش

نتيجة لتنامي ظاهرة الإجرام المعلوماتي بمختلف أشكاله لجأت الكثير من التشريعات المقارنة إلى استحداث أجهزة متخصصة لمكافحة الجرائم المعلوماتية؛ تتولى مهمة التحري عن جرائم العالم الافتراضي منها ما يعمل على المستوى الداخلي للدول ومنها ما يعمل على المستوى الدولي، ونتيجة لكون المدخلة تمس التشريع الجزائري واتفاقية بودابست فسأقتصر بحثي على هذين المجالين من خلال مايلي:

أولا: الأجهزة المختصة بالتفتيش استنادا لاتفاقية بودابست

لم تنص اتفاقية بودابست على إنشاء جهاز محدد ومشارك يختص بالتحقيق والمتابعة وإنما اكتفت بالتأكيد على ضرورة التعاون الدولي للدول الأعضاء في مكافحة الجرائم المعلوماتية العابرة لحدود تلك الدول وما يستتبعها من تسليم للمجرمين والمساعدة القضائية المتبادلة... وغيرها⁽²²⁾.

إلا أن الملفت للانتباه في هذا السياق أنها أوردت في الفصل الأخير من الاتفاقية وتحديدًا في النقطة المتعلقة "بالمساعدة المتبادلة في مجال سلطات التحقيق" المنصوص عليها في المواد من 31 إلى 34 والتي تكون الجريمة المعلوماتية فيها تتجاوز حدود دولة من الدول الأطراف ضرورة" إنشاء شبكة طوارئ دائمة لتفعيل المساعدة المتبادلة".

وترجع أصول هذا الإجراء إلى قرار الدول الثماني الكبار إقامة نقطة مراقبة دائمة للإنترنت تعمل 24 ساعة كل 24 ساعة تقوم بإعطاء إنذار بمجرد تسرب أحد القرصنة إلى الشبكة وبمجرد إطلاق صفارة الإنذار يتحرك على الفور نخبة من خبراء الأخصائيين في عالم الإنترنت لتحديد مكان المشتبه فيه باتباع أثره الإلكتروني وفقاً لآجال نشاطه الإجرامي.

ومن بين الأهداف التي يسعى مجلس التعاون الأوروبي لتحقيقها وضع نظام للتفتيش عن بعد TELEPERQUISITION حيث يستطيع ضابط الشرطة المعلوماتية تفتيش جهاز الكمبيوتر المشبوه عن بعد، وتوسيع مفهوم جريمة الإنترنت بحيث يجرم كل شخص يدخل دون ترخيص أي شبكة معلومات غير مخصصة للجمهور.

هذه الشبكة تعمل 24/24 على مدار 07 أيام في الأسبوع دون توقف، مهمتها

التحقيق والقيام بالإجراءات التالية:

- تقديم المشورات التقنية
 - التحفظ على البيانات
 - تجميع الأدلة وتقديم معلومات ذات طابع قانوني، وتحديد أماكن المشتبه فيهم⁽²³⁾
- وتعتبر هذه الشبكة أهم الطرق المنصوص عليها في الاتفاقية لمواجهة الجرائم المعلوماتية لأنها تضمن أفضل الوسائل الناجحة في مواجهة هذا الإجرام، كما أنها تسهل عمل أجهزته المتابعة والتحقيق لكل دولة من الدول الأعضاء لأنها تشكل نقطة اتصال دائمة تضمن توفير الارشادات التقنية، والتحفظ على البيانات، وتجميع الأدلة، وإعطاء المعلومات ذات الابع القانوني، وتحديد أماكن المشتبه فيهم⁽²⁴⁾.
- وجدير بالذكر أن لكل طرف الحرية في تحديد مكان أو موقع نقطة الاتصال الخاصة به والجهاز المكلف بها؛ فبعض الأطراف يضع نقطة الاتصال داخل هيكل السلطة المركزية المسؤولة عن المساعدة المتبادلة (كوزارة العدل أو الداخلية مثلا). والبعض الآخر قد يربطها بجهاز الشرطة المتخصص لمكافحة الإجرام المعلوماتي، أو يتم ربط نقطة الاتصال بجهاز إداري.

فالاتفاقية لم تحدد جهاز معين لهذه المهمة بل حددت أهداف هذه الشبكة وهو توفير الارشادات والنصائح التقنية لصد أي هجوم معلوماتي كإجراء وقائي أو تحديد مصدره وتسهيل التحقيق والقبض على الجاني كإجراء ردعي، كما شددت الاتفاقية في الفقرة الأخيرة من نص المادة 35 على ضرورة توفير كل نقطة اتصال للمعدات اللازمة لسهولة تشغيلها كالتليفونات والفاكسات والأجهزة المعلوماتية الحديثة، وتدريب أعضاء كل طاقم بوصفه جزء من الفريق في الشبكة لتسهيل التعامل المنسق مع أي جريمة معلوماتية.

ثانيا: الأجهزة المختصة بالتفتيش في التشريع الجزائري

بالعودة إلى الوضع في بلادنا نجد أن الخصوصية التي تتميز بها الجريمة المعلوماتية؛ كان الأمر لازماً لتوفير كفاءات وكوادر وأجهزة متخصصة تعنى بالبحث والتحري عن الجريمة المعلوماتية، سواء على مستوى جهاز الشرطة أو الدرك الوطني

1 - على مستوى جهاز الشرطة: نجد أن المديرية العامة للأمن الوطني أنشأت المخبر المركزي للشرطة العلمية بشاطونيف بالجزائر العاصمة، ومخبرين جهويين بكل من قسنطينة وهران، تحتوي هذه المخابر الثلاثة على فروع تقنية من بينها خلية الإعلام الآلي.

كما يوجد على مستوى مراكز الأمن التولائي فرق متخصصة مهمتها التحقيق في الجرائم المعلوماتية وتعمل بالتنسيق مع المخابر الثلاثة السابقة الذكر.

2 - على مستوى الدرك الوطني: يوجد بالمعهد الوطني للأدلة الجنائية وعلم الإجرام ببوشاوي التابع للقيادة العامة للدرك الوطني قسم الإعلام والالكترونيك الذي يختص بالتحقيق في الجرائم المعلوماتية.

بالإضافة إلى المعهد الوطني للأدلة الجنائية نجد أيضا مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها ببنر مراد رايس والتابع لمديرية الأمن العمومي للدرك الوطني وهو قيد الإنشاء⁽²⁵⁾.

الخاتمة:

خلصنا في هذه الدراسة المتواضعة إلى أن تفتيش البيانات المعلوماتية المخزنة كآلية إجرائية له أهمية بالغة في الكشف عن الجريمة المعلوماتية وإثباتها، إلا أن تحقيق ذلك يتطلب قواعد إجرائية متكاملة، وكفاءات وكوادر مكونة ومدربة على أعلى مستوى وفقا للتقنيات المتطورة سواء على المستوى الداخلي أو الدولي.

وقد أولت كل من اتفاقية بودابست والتشريع الجزائري أهمية بهذه المسألة؛ حيث خصصت الاتفاقية نصوص قانونية لتنظيم إجراء التفتيش (المادة 19 تحديدا) وللتعاون الدولي في مجال سلطات التحقيق (المواد من 31 إلى 34 من الاتفاقية)، أما التشريع الجزائري فقد استحدث القانون رقم 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها؛ حيث أورد تنظيم لإجراء التفتيش ولو عن بعد وفقا لنص المادة 05 منه، واستحدثت أجهزة متخصصة بالبحث والتحري في الجريمة المعلوماتية.

إلا أن هذه الجهود تبقى غير كافية مقارنة بالتطور والتوسع السريع والخطير للجريمة المعلوماتية؛ حيث تصطدم الجهود الدولية والداخلية لمكافحة هذه الجريمة بسيادة الدول لامتدادها لأكثر من دولة مما يصعب إجراء التحقيقات والمتابعة. كما أن تأهيل الأجهزة الأمنية المكلفة بالمتابعة والتحقيق يتطلب تكويننا خاصا ومؤهلات كبيرة وتكنولوجيا عالية المستوى تحتاج إلى أموال وجهود دولية متضافرة. المقترحات:

- من الحلول المقترحة في هذا المجال نجد على مستوى القانون الداخلي ضرورة انضمام الجزائر إلى الاتفاقيات الدولية لتعزيز التعاون القضائي والأمني لمواجهة التحديات الإجرائية الناجمة عن الطبيعة الخاصة للجريمة المعلوماتية. - ضرورة تعاون مقدمي خدمات الإعلام الآلي مع جهات التحقيق من خلال التبليغ وتقديم الخدمات التي تسهل عملهم وتجعله أكثر فاعلية ونجاعة، وهذا من شأنه ربح الكثير من الوقت والجهد؛ كما يمتد هذا التعاون إلى المجني عليهم والشهود وغيرهم من مستخدمي تكنولوجيا المعلومات لكي تكون المعلومة متاحة للاستخدام أمام القضاء. - وجوب تحقيق التناسب والتوازن بين السلطات الممنوحة لجهة التحقيق لاسيما إجراء التفتيش وما يستتبعه من إجراءات قسرية من جهة وبين حقوق المشتبه فيهم والضمانات الممنوحة لهم من جهة ثانية؛ لمنع المساس بحقوق الأفراد وحررياتهم التي كفلها لهم الدستور، وذلك بإخضاع الاجراءات برمتها لرقابة القضاء وهو ما أغفلته اتفاقية بودابست التي لم تتحدث عن الضمانات بشكل محدد بخلاف الاتفاقية الأوروبية لحقوق الانسان وقضائها اللاحق مثل (قضية مالون وقضية الفوردي وقضية لمبرت وقضية كورسلين).

الهوامش:

- (1) خالد ممدوح ابراهيم - فن التحقيق الجنائي في الجرائم الالكترونية - دار الفكر الجامعي - 2009 - ص 07.
- (2) المرجع نفسه - ص.07
- (3) محمد الطوالبية - التفتيش الجنائي على نظم الحاسوب والانترنت - عالم الكتاب الحديث - الأردن - 2004 ص.11
- (*) للتفصيل أكثر أنظر: عبد الله حسين محمود - إجراءات جمع الأدلة في الجريمة المعلوماتية - مؤتمر الجوانب القانونية والأمنية للعمليات الالكترونية - دبي - 2003 - ص.612
- (4) إبراهيم الدسوقي عطية - الأمن المعلوماتي - دار الجامعة الجديدة - الاسكندرية - 2009 - ص.371
- (5) محمد الطوالبية - مرجع سابق - ص. (14-17)

- (6) إبراهيم الدسوقي عطية - مرجع سابق - ص.380
- (7) من الضمانات القانونية: حضور المشتبه فيه أثناء التفتيش أو من ينوبه - تحديد وقت التفتيش - رضا المشتبه فيه بالتفتيش.
- (8) سعيداني نعيم - آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري - مذكرة ماجستير - جامعة الحاج لخضر - باتنة - 2012/2013 - ص.145
- (9) هلائي عبد اللاه أحمد - تفتيش نظم الحاسوب الآلي وضمانات المتهم المعلوماتية - دراسة مقارنة - دار النهضة العربية - القاهرة - 2006 - ص.76
- (10) إبراهيم الدسوقي عطية - مرجع سابق - ص.386
- (11) هلائي عبد اللاه أحمد - اتفاقية بودابست لمكافحة جرائم المعلوماتية - دار النهضة العربية - القاهرة - 2007 - ص.240
- (12) من التشريعات التي تلزم حضور المشتبه فيه أو الشهود: التشريع المغربي) المادة 81 من قانون المسطرة الجنائية المغربي. (الأردني) المواد 85-84-83-36 من أصول المحاكمات الجزائية الأردني - (ومن التشريعات التي لا تلزم الحضور نجد: التشريع المصري) المادة 92 من قانون الاجراءات الجزائية المصري. (الإماراتي) المادة 73).
- (13) هلائي عبد اللاه أحمد - اتفاقية بودابست - مرجع سابق - ص.256
- (14) أنظر المواد 20 و 21 من اتفاقية بودابست لسنة 2001
- (15) هلائي عبد اللاه أحمد - اتفاقية بودابست - مرجع سابق - ص.257
- (16) أنظر مثلا التشريع الكويتي) المادة 85 من قانون أصول كويتي - والتشريع القطري) المادة (59) ، المغربي) المادة (64) ، الفرنسي) المادة 59 من قانون الاجراءات الجزائية.
- (17) أنظر مثلا: التشريع البريطاني) المادة 2/05 من قانون الشرطة والأدلة الجنائية البريطاني لسنة 1984).
- (18) المادة 47 من قانون الاجراءات الجزائية الجزائري.
- (19) وهي الجرائم المنصوص عليها في المواد من 342 إلى 348 من قانون العقوبات الجزائري.
- (20) سعيداني نعيم - آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري - مذكرة ماجستير - جامعة الحاج لخضر - باتنة - 2012/2013 - ص.155
- (21) حسن محمد الطوالبه - مرجع سابق - ص.82
- (22) أنظر المواد من 23 إلى 30 من اتفاقية بودابست لسنة 2001
- (23) المادة 35 من اتفاقية بودابست لسنة 2001
- (24) هلائي عبد اللاه أحمد - اتفاقية بودابست لمكافحة جرائم المعلوماتية - مرجع سابق - ص.389
- (25) عبيداني نعيم - آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري - مذكرة ماجستير - جامعة الحاج لخضر - باتنة - 2012/2013 - ص.107

