الجمهورية الجزائرية
الديمقراطية الشعبية
وزارة العدل

# التجربة الجزائرية في مجال
# التوقيف الإلكتروني

من اعداد :

القاض زينب مامونـي

# مقدمة

تعد الجريمة المعلوماتية من الجرائم المستحدثة التي برزت في الوقت الراهن نتيجة تطور تقنية المعلومات واستغلالها على نحو غير مشروع وبوسائل من شأنها أن تلحق الضرر بمصالح الأفراد والجماعات، ونظرا لخصوصية هذه الجريمة كونها ترتكب في بيئة افتراضية رقمية، فإنه بات من الضروري تطوير أساليب التحقيق الجنائي وإجراءاته بصورة تتلائم مع هذه الخصوصية، وتمكّن جهات التحقيق من كشف الجريمة والتعرف على مرتكبيها، وهو الأمر الذي سعى المشرع الجزائري إلى تجسيده من خلال استحداث نصوص قانونية جديدة أوجد بموجبها قواعد إجرائية تتفق والطبيعة التقنية للجريمة المعلوماتية، ويعتبر التفتيش الالكتروني إحدى هذه الإجراءات التي حملها القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

ويعد التحقيق الجنائي من أهم المراحل التي تأتي في مقدمة محاولات مواجهة الجريمة المعلوماتية وذلك عن طريق وضع آليات وإجراءات تتناسب والطبيعة الخاصة لهذه الجريمة التي تتسم بارتكابها في مسرح الكتروني غير مادي والذي يختلف تماما عن المسرح التقليدي، وكذا إمكانية امتداد آثارها خارج الإقليم الوطني

للدولة، ويشكل التفتيش الالكتروني أهم تلك الإجراءات التي تباشرها سلطات التحقيق في سبيل الكشف عن الحقيقة في الجرائم المعلوماتية والتصدي لها. وانطلاقا مما تقدم، سوف تبحث هذه الورقة البحثية في التحقيق الالكتروني كونه من أكثر الإجراءات استعمالا وأهميته في نطاق الجريمة المعلوماتية.

تفصيلا لما سبق ذكره سوف، نقسم هذا الباب إلى فصلين، ندرس **في الفصل الأول آليات التحقيق في الجرائم الإلكترونية**، وفيه نركّز على إظهار مدى سريان إجراءات التحقيق المألوفة عليها، ثم نبيّن بعدها حاجة هذا النوع الإجرامي المستحدث إلى إجراءات تحقيق جديدة خاصة تتناسب مع طبيعته. أما **الفصل الثاني** فنخصصه لإبراز **القيمة الثبوتية للأدلة المحصلة من الوسائل الإلكترونية** وأثرها على تكوين اقتناع القاضي الجزائي.

# الفصل الأول: ماهية التحقيق الالكتروني

لقد سعى المشرع الجزائري إلى تكريس قواعد إجرائية يمكن للجهات المكلفة بالبحث والتحري عن الجريمة الإلكترونية لاعتماد عليها في الوصول إلى الدليل المناسب في إثباتها.

ولا شك أن هذا الدليل سيتم استخلاصه من البيئة الالكترونية والرقمية التي تعتبر مسرح الجريمة المعلوماتية، مما يجعله يتميز بخصائصها، وهو الأمر الذي يقودنا إلى الحديث عن مسألة القيمة الثبوتية لهذا الدليل ومدى قبوله من طرف القضاء الجزائي، ومدى مشروعيته وتعبيره عن الحقيقة بالنظر إلى ما يمكن أن يتعرض له من التزييف والتحريف. بل حتى مع ضمان مصداقية هذا الدليل ومشروعيته، فتثار مسألة أخرى أكثر أهمية تتعلق بمدى خضوع هذا الدليل ذو الأصالة العلمية للسلطة التقديرية للقاضي الجزائي إعمالا لمبدأ الاقتناع الشخصي للقاضي الجزائي الذي يشكل جوهر أية محاكمة.

## أولا: مفهوم التحقيق الالكتروني

هو مجموعة من الإجراءات تتخذ من أجل الوصول إلى الحقيقة أي اتخاذ الوسائل التي تظهر الحقائق وهو كذلك مجموعة من الإجراءات والأعمال التي يقوم بها المحقق لجمع الأدلة والبيانات اللازمة لكشف الجرائم والتعرف على مرتكبيها والقبض عليه تمهيدا لمحاكمته، ويحتاج المحقق في تنفيذ التحقيق إلى الوسائل

المادية وأخرى معنوية وذلك لما تحتاجه الجريمة الالكترونية من معرفة تامة وإدراك لوسائل تثبت وقوع الجريمة والوصول إلى مرتكبها ونسبتها لهم.

كما يكمن تعريف التحقيق الالكتروني على أنه عبارة عن سلطة يباشرها المحقق لكشف الجريمة والمجرم بالوسائل الالكترونية مستحدثة ضمن نظام جنائي متكامل الأطراف والوسائل معتمدا على الشبكة المعلوماتية وهي ارتباط بين أكثر من حاسب آلي أو نظام معلوماتي للحصول على البيانات وتبادلها مثل الشبكات الخاصة والعامة والشبكة العالمية (الانترنت) وبرامج الملفات الحاسوبية الالكترونية وفقا للقانون .

## ثانيا: آليات التحقيق الالكتروني

نظرا لتطور الكبير الذي شهده العالم في ميدان التكنولوجيات الرقمية، وما أفرزه من أضرار وخيمة تمس بالنظام العام، والذي نتج عنه ظهور نوع مستحدث من الجرائم الذي أصبح يهدد كيان المجتمعات، الأمر الذي دفع بالمشرع الجزائري إلى استحداث أساليب أخرى للبحث والتحري عن الجريمة، من خلال تعديله لقانون الإجراءات الجزائية، وفقا لقانون رقم 06/22 المؤرخ في 20/7/2006وهو ما يسمى بأساليب البحث والتحري الخاصة.

ومما لا شك فيه، أن المشرع حينما أراد توسيع نطاق تطبيق إجراءات التحقيق التقليدية لتطال الجرائم الإلكترونية، فانه يقصد بها تلك الإجراءات التي تثير إشكالات وعقبات عملية تعود إلى خصوصية هذه الجرائم، كالتفتيش، الضبط، المعاينة والخبرة، والتي هي في حاجة إلى تطوير وتحيين لكي تتناسب مع طبيعتها الخاصة وطبيعة الدليل الذي يصلح لإثباتها، أما غيرها من الإجراءات كسماع المتهم أو الشهود، الاستجواب والمواجهة، فإنها مستبعدة نظرا لعدم وجود أية صعوبات في اتخاذها. استرشادا بذلك، فإننا سوف نركّز على دراسة الفئة الأولى من إجراءات التحقيق دون غيرها.

## 1- التفتيش

لم يبق المشرع الجزائري مكتوف الأيدي تجاه المتغيرات التي تحدث في عالم التكنولوجيات الحديثة، بل قام بدوره باستحداث نصوص قانونية جديدة أجاز من خلالها تفتيش المكونات المنطقية والمعطيات المعلوماتية للحاسب، ومن بين هذه النصوص المادة (50) من القانون رقم (90-40) المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها التي تسمح للسلطات القضائية المختصة ولضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة (40) من هذا

القانون، الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها والمعطيات المعلوماتية المخزنة فيها وكذا منظومة تخزين المعلوماتية.

وفي هذا الصدد، نصت الاتفاقية الأوروبية حول الجرائم الالكترونية صراحة على حق الدول الأعضاء في تفتيش النظم المعلوماتية وحثها على تجسيد هذا الحق بكل وضوح في قوانينها الإجرائية لتفادي أي إشكال يمكن أن يثار حول الموضوع، وذلك من خلال المادة (1/91) التي نصت على أنّ **" لكل طرف الحق في سنّ من القوانين ما هو ضروري لتمكين السلطات المختصة من تفتيش أو الدخول إلى:**

**- نظام الحاسب أو جزء منه أو المعلومات المخزنة فيه.**

**-الوسائط التي يتم تخزين معلومات الحاسب بها ما دامت مخزنة في إقليمها.**

ومع تطور تكنولوجيات الإعلام والاتصال لم يعد نطاق الاتصالات محدودا في نطاق إقليم دولة واحدة، بل امتد ليشمل كل أرجاء العالم، خاصة بظهور الانترنت التي تمثل منظومة واسعة جدا من شبكات المعلومات الحاسوبية المتصلة مع بعضها البعض بطريقة لا مركزية، ويدخل في تركيبها ملايين الحواسيب موزعة عبر مختلف دول العالم.

لذلك يثير إخضاع شبكات المعلومات المتصلة بالحاسب الآلي لعملية التفتيش صعوبات كبيرة، تتعلق بالدرجة الأولى بالطبيعة التكنولوجية الرقمية التي تسمح بتوزيع المعلومات التي تحتوي أدلة عبر شبكات حاسوبية في أماكن مجهولة بعيدة تماما عن الموقع المادي للتفتيش، فقد يكون الموقع الفعلي لهذه المعلومات داخل اختصاص قضائي آخر في إقليم دولة واحدة أو في إقليم دولة أو عدة دول أخرى، وهو ما يزيد الأمر تعقيدا باعتبار الشبكة المعلوماتية ممتدة عبر أرجاء العالم.

ومن هنا يثار التساؤل حول مدى جواز امتداد التفتيش إلى الأنظمة المعلوماتية المتصلة بالنظام المأذون بتفتيشه إذا كانت متواجدة في دوائر اختصاص مختلفة.

وفي هذا الصدد، سمحت الاتفاقية الأوروبية للجرائم الالكترونية لعام 2001 الدول الأعضاء من خلال نص المادة (2/91) بمدّ نطاق التفتيش الذي كان محله جهاز حاسب معين إلى غيره من الأجهزة المرتبطة به في حالة الاستعجال، إذا كان يتواجد بها معلومات أو بيانات مهمة للتحقيق يمكن الولوج إليها من خلال الجهاز محل التفتيش دون أن يشكل ذلك تجاوزا للاختصاص الإقليمي، ولم يتأخر المشرع الجزائري عن التشريعات المذكورة أعلاه، إذ نصّ في المادة5(/2) من القانون رقم (90-40) لسنة 2009 المتعلق بالوقاية من الجرائم المتصلة

بتكنولوجيات الإعلام و الاتصال ومكافحتها بأنه **"... في حالة تفتيش منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزّنة فيها، إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك.**

ومما يتعين الإشارة إليه أيضا، أن المشرع الجزائري استطاع أن يتجاوز مسألة تفتيش المنظومة المعلوماتية عن بعد بصفة نهائية، حينما وسّع في التعديل الأخير لقانون الإجراءات الجزائية اختصاصات ضباط الشرطة القضائية في مجال التحقيق عن الجرائم الإلكترونية، وأجاز إمكانية قيام هذه السلطات بالتفتيش في أي وقت من الليل والنهار، وفي أي مكان على امتداد كافة التراب الوطني.

وفي هذا الصدد، خوّل المشرع الجزائري على غرار التشريعات السابقة سلطات التحقيق والبحث الحق بتفتيش عن بعد الأنظمة المعلوماتية المتصلة أو جزء منها حتى ولو كانت متواجدة خارج الإقليم الوطني، وذلك بنصه في المادة 5(/3) من القانون (40/90) المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة

بتكنولوجيات الإعلام والاتصال ومكافحتها على انه "...**إذا تبين مسبقا أن هذه المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فان الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل**".

الملاحظ في هذه المادة، أن المشرع الجزائري لم يسمح للسلطات القضائية المختصة وضباط الشرطة القضائية بتوسيع نطاق التفتيش الالكتروني ليشمل المعطيات المخزنة في منظومة معلوماتية تقع خارج القطر الوطني، إلا في إطار المساعدة القضائية المتبادلة وفي نطاق الاتفاقيات الدولية المبرمة في مجال ملاحقة الإجرام ألمعلوماتي.

وقد تبنى المشرع الجزائري الإجراءات المستحدثة الخاصة بضبط وتحريز المعلومات والبيانات المعلوماتية وغيرها من الأدلة الرقمية في القانون 04/90 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وذلك بما يتناسب وطبيعتها المادية تحت عنوان حجز المعطيات المعلوماتية في المواد من 60 إلى 70 منه، أما بخصوص المعطيات المحجوزة فقد نصت المادة 80 منه على أنه "**يمكن للسلطة التي تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الاطلاع على**

**المعطيات التي يشكل محتواها جريمة، لاسيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك"**

## 2- المعاينة

تتم المعاينة في الجرائم الإلكترونية كأي جريمة أخرى عن طريق الانتقال إلى مكان وقوع الجريمة، غير أن الانتقال هنا يختلف حسب طبيعة الجريمة الإلكترونية المرتكبة، وإذا كانت الجريمة واقعة على المكونات المادية للأجهزة الالكترونية كجرائم الاعتداء على الحاسب الآلي أو الأشرطة أو الأقراص الممغنطة ، فالانتقال في هذه الحالة يكون ماديا إلى مسرح الجريمة الذي يحوي هذه المكونات لمعاينته والتحفظ على الأشياء التي تعدّ أدلة مادية تدل على وقوع الجريمة وانتسابها لشخص معين، ثم ضبطها وضعها في أحراز مختومة تقدم للنيابة العامة، أما إذا كانت الجريمة واقعة على المكونات غير المادية للأجهزة الإلكترونية أو بواسطتها، كتلك الواقعة على برامج الحاسب وبياناته بواسطة الانترنت فيكون الانتقال للمعاينة هنا افتراضيا أو الكترونيا، ويمكن للمحقق إجراء المعاينة الافتراضية أو الالكترونية بالولوج والانتقال إلى مسرح الجريمة عبر الانترنت انطلاقا من مكتبه بواسطة الحاسب الموضوع تحت تصرفه، أو من خلال مقهى

الانترنت أو إحدى المقرات المزود بخدمات الانترنت، ويتمثل نطاق المعاينة الالكترونية في معاينة **أولا** مكونات الحاسب الآلي من قرص صلب وبرمجيات ونظام المعلومات، **ثانيا** معاينة أنظمة الاتصال بشبكة الانترنت عن طريق فحص مسار الانترنت وفحص الخادم.

## 3- الخبرة التقنية

لقد أصبح انضمام الخبرة التقنية إلى عالم الخبرة القضائية والاستعانة بخبراء مختصين لفحص الأدلة التقنية وتقويم عملية الإثبات الرقمي وتحليل الجريمة الالكترونية أمرا ملحا لا يمكن الاستغناء عنه إذ لا يعقل أن يفصل القاضي في قضايا تقنية المعلومات دون أن يستند إلى الخبرة التقنية في هذا المجال تحقيقا لمبدأ معروف هو "مبدأ التخصص" وإلا كان حكمه معيبا ومطعونا فيه.

حيث تعرف الخبرة الفنية بأنها إجراء من إجراءات التحقيق يتم بموجبه الاستعانة بشخص يتمتع بقدرات فنية ومؤهلات علمية لا تتوافر لدى جهات التحقيق والقضاء، من أجل الكشف عن دليل أو قرينة تفيد في معرفة الحقيقة بشأن وقوع جريمة أو نسبتها إلى المتهم.

وللخبرة الفنية دور كبير في إثبات الجريمة الإلكترونية، لأنها تنير الدرب لسلطات التحقيق والقضاء و سائر الجهات المختصة بالدعوى الجزائية للوصول إلى الحقيقة و تحقيق العدالة

الجنائية، وقد تزايدت الحاجة إلى الخبرة الفنية للتحقيق عن الجرائم الالكتروني في الآونة الأخيرة نظرا للتحولات التكنولوجيا التي مست وسائل الإعلام والاتصال، إذ تعددت أنواع ونماذج الحواسيب وشبكات الاتصال بينها، وأصبحت العلوم والتقنيات المتعلقة بها تنتمي إلى تخصصات علمية وفنية دقيقة ومتشعبة، والتطورات في مجالها سريعة و متلاحقة لدرجة قد يصعب على المتخصص تتبعها واستيعابها.

ولعل إدراك بعض دول العالم لهذه الأهمية، جعلها لا تكتفي بالنصوص التقليدية التي تنظم الخبرة الفنية، وإنما أسرعت إلى تدعيمها بنصوص قانونية جديدة خاصة بالخبرة في مجال جرائم التقنية العالية ولم يتخلف المشرع الجزائري عن هذه التشريعات، إذ نص في المادة (05) الفقرة الأخيرة من القانون رقم (40/90) المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها بأنه **" يمكن للسلطات المكلفة بتفتيش المنظومات المعلوماتية تسخير كل شخص له دارية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية معطيات المعلومات التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لانجاز مهمتها"**

ولم يتوقف المشرع الجزائري عند هذا الحد، بل قام بإنشاء هيئات وأجهزة متخصصة في مواجهة الجرائم الإلكترونية مزودة بوسائل متطورة

وتقنيات عالية، وجعلت من مهامها الأساسية انجاز الخبرات التي تحتاج إليها السلطات القضائية، نذكر منها مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها الذي أنشأته قيادة الدرك الوطني في عام 2009، والمعهد الوطني للبحث في علم التحقيق الجنائي الذي أنشئ بموجب المرسوم الرئاسي رقم (40-234) المؤرخ قي 20ديسمبر2004 وتم تنظيم المصالح والأقسام والمخابر فيه بموجب قرار وازري مشترك مؤرخ في 14-04-2007 والذي تضمن مصلحة الخبرات الخاصة بالدلائل التكنولوجية ونذكر كذلك القسم الخاص بالخبرة الرقمية التابع لنيابة الشرطة العلمية والتقنية بمديرية الشرطة القضائية المتواجد على مستوى المديرية العامة للأمن الوطني، وتمتد مصالحها الى بعض الولايات، والذي يتولى تقديم الخبرة الفنية المتميزة في القضايا ذات الطابع الرقمي، بالإضافة إلى إنشاء مؤخرا ثلاث مخابر جنائية جهوية بشمال البلاد تابعة للأمن الوطني تضمّ عدة أقسام متخصصة بما فيها قسم الأدلة الإلكترونية والرقمية، والتي ستدعّم مستقبلا بثلاث مخابر مماثلة في الجنوب.

## 4- مراقبة الاتصالات الالكترونية واعتراض المراسلات

نجد المشرع الجزائري على غرار العديد من المشرعين لم يقم بتعريف عملية مراقبة الاتصالات الإلكترونية، إلا أننا يمكن أن نعرفها على أساس أنها إجراء تحقيق يباشر خلسة، وتنتهك فيه سرية الأحاديث الخاصة، تأمر السلطة القضائية في الشكل المحدد قانون يهدف الحصول على دليل غير مادي للجريمة المعلوماتية، ويتضمن من ناحية استراق السمع إلى الأحاديث ومن ناحية أخرى حفظه بواسطة أجهزة متخصصة لذلك .

ونجد أن المشرع من خلال قانون 01-06 قد أشار إلى هذا الإجراء دون تقديم تعريف له، بينما في القانون 04-09 في المادة 3 منه قد حدد كيفية مراقبة الاتصالات الإلكترونية **«مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات و الاتصالات يمكن لمقتضيات حماية النظام العام أو المستلزمات التحريات أو التحقيقات القضائية الجارية وفقا للقواعد"** وقد نص القانون رقم 01-06 مؤرخ في 20 فيفري 2006، المتعلق بالوقاية من الفساد و مكافحته ، المعدل و المتمم بموجب القانون رقم 15-11 مؤرخ في 02 أوت 2011 على آليات مكافحة و قمع الجريمة الإلكترونية وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية و تجميع و تسجيل محتواها في حينها والقيام بإجراءات التفتيش و الحجز داخل منظومة معلوماتية وبالتالي فإن مراقبة الاتصالات حددها القانون على سبيل الاستثناء وفي الحالات المحددة حصريا في المادة 4 من القانون 04-09 المتعلق بالوقاية

من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

ونظرا لثبوت نجاعة هذا الإجراء في تعقب الدليل و إثبات الجرائم الإلكترونية، فقد أوصت الاتفاقية الأوروبية حول الجرائم الإلكترونية لعام 2001 من خلال نص المادة (12) جميع الدول الأعضاء بضرورة تبني اجراء اعتراض المراسلات والمراقبة الإلكترونية للاتصالات في تشريعاتها الإجرائية الداخلية ضمن اجراءات البحث والتحري ولم يتخلف المشرع الجزائري عن هاته الدول، بل تدخل بموجب قانون الإجراءات الجزائية رقم (22/60) المؤرخ في 2006/09/20 المعدل و المتمم فاستحدث لهذا الإجراء الفصل الرابع كاملا تحت عنوان " اعتراض المراسلات وتسجيل الأصوات والتقاط صور وتناول فيه المقصود بهذا الإجراء، نطاقه وضمانات استخدامه. ثم عززه بالقانون رقم (40/90) المؤرخ 5 أوت 2009يعتبر إجراء من إجراءات التحري المستحدثة والذي يقصد به التتبع السري والمتواصل للمرسلات الخاصة بالمشتبه به ودون علمه ذلك باعتبار إجراء تحقيقي يباشر خلسة وتنهك فيه سرية الأحاديث الخاصة تأمر به السلطات القضائية في الشكل المحدد قانونا بهدف الحصول على دليل مادي للجريمة، والتي تستخدمها في مواجهة الإجرام الخطير، وتتم عبر وسائل الاتصال السلكية واللاسلكية.

ووفقا لنص المادة 65مكرر5 من قانون إجراءات الجزائية فان اعتراض لم يقتصر فقط على المكالمات الهاتفية، بل تم توسيعه إلى مختلف أنواع الاتصال السلكية واللاسلكية أما بخصوص أداة الاعتراض فإن المشرع لم يحدد وسيلة معينة فقد تكون تقليدية أو مستحدثة.

لكن رغم أن أسلوب اعتراض المراسلات السلكية واللاسلكية دون علم أصحابها قد اثبت جدارته في كشف وإثبات الكثير من الجرائم الغامضة كتلك المتعلقة بالجرائم الإلكترونية، فهو في الوقت نفسه يمثل انتهاكا خطيرا لحرمة الحياة الخاصة للإفراد، واعتداء صارخا على سرية مراسلاتهم واتصالاتهم التي كفلتها معظم الدساتير والتشريعات العقابية بالحماية ولتحقيق التوازن بين ضرورة التحقيق التي تفرضها المصلحة العامة واحترام الحياة الخاصة التي تفرضها المصلحة الفردية، تمت إحاطة عملية الاعتراض بعدد من القيود القانونية التي تضمن عدم تعسف السلطات العامة وتصون الحرية الفردية. والتي نلخصها **في:**

*** الحصول على إذن مسبق من الجهات القضائية المختصة** المتمثلة عادة في وكيل الجمهورية أثناء مرحلة التحقيق الابتدائي أو قاضي التحقيق في مرحلة التحقيق القضائيين أجلا للجوء إلى عملية اعتراض او مراقبة المراسلات.

*** تسبيب أمر اللجوء الى اعتراض أو مراقبة المراسلات.**

*** تحديد الجرائم محل الاعتراض والمراقبة.**

* سرية الاجراءات وكتمان السر المهني.

## 5- التسرب الالكتروني

يعد التسرب من إجراءات البحث والتحقيق الجديدة التي أرستها معظم تشريعات العالم الحديثة لمواجهة الجرائم الإلكترونية وقد كانت اتفاقية منظمة الأمم المتحدة المتعلقة بمكافحة الجريمة المنظمة سباقة الى احتواء هذا الإجراء بنصها في المادة (20) على أساليب التحري الخاصة بما فيه التسرب الذي عبّرت عنه ب «**الأعمال المستترة**".

أما المشرع الجزائري فقد تبني بدوره هذا الإجراء، مباشرة عقب تصديق الدولة الجزائرية على اتفاقية منظمة الأمم المتحدة أعلاه بموجب المرسوم الرئاسي رقم (05/02) المؤرخ في 02/02/2002 بتحفظ واتفاقية مكافحة الفساد بتاريخ2004/04/19 وقد ورد النص على هذا الأسلوب لأول مرة بالجزائر بمناسبة صدور القانون رقم(01/06) المتعلق بالوقاية من الفساد ومكافحته في عام 2006، الذي نص في المادة (56) على أنه" **من أجل تسهيل جمع الأدلة المتعلقة بالجرائم المنصوص عليها في هذا القانون يمكن اللجوء إلى التسليم المراقب واتباع أساليب تحري خاصة كالترصد الإلكتروني**

**أو الاختراق على النحو المناسب وبإذن من السلطة القضائية المختصة "**

ولكن نظرا للغموض الذي انتاب هذا النص بخصوص المقصود بالاختراق أو التسرب شروطه وآليات مباشرته، بقي هذا الإجراء جامدا وبدون مفعول إلى أن تم تعديل قانون الإجراءات الجزائية بموجب قانون(22/60) المؤرخ في 20/12/2006، أين تم تحديد معالم إجراء التسرب من خلال تعريف هوتحديد ضوابطه والآثار المترتبة عنه.

حيث عرفت المادة 65مكرر12من قانون إجراءات الجزائية التسرب على أنه **" قيام ضابط أو عون شرطة قضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم ويسمح لضابط أو عون الشرطة القضائية أن يستعمل لهذا الغرض، هوية مستعارة وأن يرتكب عند الضرورة الأفعال المذكورة في المادة 65 مكرر14 أدناه، ولايجوز تحت طائلة البطلان أن تشكل هذه الأفعال تحريضا على ارتكاب الجرائم"**

وبالتالي نستخلص من هذه المادة، أن التسرب هو قيام ضابط أو عون الشرطة القضائية بمراقبة المشتبه في ارتكاب جناية أو جنحة بإيهامهم أنه فاعل أصلي بغرض كشف الحقيقة، ويبطل هذا الإجراء إذا كان الهدف منه التحريض على ارتكاب الجريمة .كما نص المشرع الجزائري على التسرب في قانون مكافحة الفساد باستخدام مصطلح اختراق للدلالة عنه وبالإشارة إليه فقط باعتباره من إجراءات التحري.

# 6- انتاج المعطيات المعلوماتية

إن عملية إنتاج المعطيات المعلوماتية هو إجراء يفرضه القانون على مقدم خدمات الانترنت يلتزم من خلاله بموافاة السلطات المختصة بالبحث والتحقيق بكل المعطيات أو البيانات المعلوماتية المتعلقة بالمشتركين وخدماتهم، غير بيانات المرور أو المحتوى الموجودة بحوزته أو تحت سيطرته، من أجل استعمالها لأغراض التحقيق.

وقد تناولت اتفاقية بودابست الخاصة بمكافحة الجرائم المعلوماتية هذا الإجراء ضمنا لإجراءات المستحدثة في مجال البحث والتحقيق عن الجرائم الإلكترونية في المادة (81) منها تحت عنوان **" الأمر بإنتاج معطيات معل ومات L'injonction de produire"** أوجبت على كل طرف في الاتفاقية تبني الإجراءات التشريعية وإجراءات أخرى التي يراها ضرورية من اجل تأهيل سلطاته المختصة بأن تأمر:

أ- كل شخص على أرضه بإرسال معطيات معلوماتية معينة في حوزته أو تحت سيطرته، والمخزنة في نظامه ألمعلوماتي، أو في دعامة تخزين معلوماتية.

ب - كل مزود خدمات الذي يقدم خدماته على ارض ذلك الطرف من اجل إرسال المعطيات

المتعلقة بالمشتركين وخدماتهم التي في حوزته أو تحت سيطرته

والجدير بالذكر انه رغم أهمية عملية إنتاج البيانات المعلوماتية في التحقيق والبحث عن الجرائم الإلكترونية، باعتباره إجراء جديد يتناسب وطبيعة الدليل المعلوماتي، وتقتضيه السرعة المطلوبة التي يفرضها الحفاظ على الأدلة الإلكترونية من التلاعب، إلا أن المشرع الجزائري مثله مثل معظم دول العالم أغفل النص على هذا الإجراء ضمن إجراءات التحري المستحدثة، وعليه ينبغي التنبيه إلى هذا الفراغ والعمل لتدارك الوضع مستقبلا.

## الفصل الثاني: سلبيات وايجابيات التحقيق الالكتروني

إن الجرائم الإلكترونية من الأنماط الإجرامية الجديدة التي فجرتها حديثا ثورة تقنية المعلومات والاتصالات عن بعد، و التي تتميز بخصائص مختلفة تماما عن الجرائم التقليدية، وأنها من المستجدات التي لم تكن معروفة في القانون الجزائي بشقيه الموضوعي والإجرائي، من ثمة فأي محاولة للتعامل إجرائيا مع هذا النمط الإجرامي الجديد في إطار عملية البحث والتحقيق سوف يخلق إشكالات إجرائية أمام السلطات المكلفة بهذه العملية.

# أولا: سلبيات التحقيق الالكتروني

يعد من أهم سلبيات التحقيق الالكتروني الإشكالات في القصور الذي يعتري النصوص الجزائية الإجرائية القائمة في مواجهة مثل هذه الجرائم، لأن أحكام هذه النصوص إنما وضعت لتحكم الإجراءات المتعلقة بجرائم تقليدية لا توجد صعوبات في إثباتها أو التحقيق فيها مع خضوعها لمبدأ حرية القاضي الجزائي في الاقتناع.

صعوبات الاستدلال و الإثبات في الجرائم الإلكترونى تتميز الجريمة الالكترونية عن الجريمة التقليدية بكونها ترتكب في بيئة افت ارضية غير مادية عبر نبضات وذبذبات إلكترونية رقمية غير محسوسة، وتمحى آثارها بمجرد نقرة بسيطة على لوحة مفاتيح الحاسب، و في وقت قياسي قد يكون جزءًا من الثانية. مما يعطيها طابع خاص ليس فقط في طريقة ارتكابها، وإنما حتى في الوسيلة التي ترتكب بها، وهو ما قد يشكل صعوبات في اكتشاف الجريمة الالكترونية.

يعد اكتشاف الجريمة الالكترونية من التحديات الحقيقية التي تعيق رجال الضبطية القضائية عن المواجهة الفعالة لها، والتي يرجع سببها إلى عدة اعتبارات، منها ما يتعلق بغياب الآثار

المادية للجريمة، لأن الجريمة الالكترونية ترتكب عادة في بيئة افت ارضية تقنية لا تترك أية آثار مادية محسوسة تدّ ل على الجريمة أو مرتكبها، ومنها ما هو ارجع إلى سهولة إخفاء ومحو الدليل، إذ يكفي الضغط على زر في لوحة الاستخدام لزوال ملفات أو حتى قواعد بيانات وأنظمة بأكملها كما أن الامتناع عن التبليغ بوقوع الجريمة الالكترونية، ونقص الخبرة و المعرفة الفنية لدى سلطات الاستدلال والإثبات تحول بد ورها دون اكتشاف هذا النوع المستحدث من الجريمة.

- غياب الآثار الماد ية للجريمة و سهولة محو الدليل فالجريمة الالكترونية من الجرائم المستحدثة التي لا تترك شهودا يمكن الاستدلال بأقوالهم ولا بصمات يمكن تحليلها أو أدلة مادية يمكن فحصها، إنما تقع في بيئة الكترونية افتراضية عن طريق نقل معلومات رقمية و تداولها بواسطة ذبذبات الكترون ية غير مرئية.

-غياب الآثار المادية للجريمة و سهولة محو الدليل

- صعوبة اكتشاف هوية المجرم الالكتروني والتي تعتبر من بين المسائلة الشائكة التي تعرقل عملية التحقيق في الجرائم الالكترونية صعوبة تحديد مكان

تواجد جهاز الحاسب الآلي مصدر النشاط الإجرامي، والذي يسمح من خلاله الكشف عن المجرم.

- تميز المجرم الالكتروني عن المجرم العادي بالذكاء و المعرفة الفنية الواسعة ، وهذه الخصلة تمكنه من التخطيط جيدا لجريمته قبل أن يقدم على ارتكابها، وإحاطتها بأساليب أمنية وتدابير الحماية الفنية التي تحول دون كشف أمره وتعيق مهمة أجهزة الاستدلال والتحقيق في الوصول إلى الدليل.

في السياق ذاته تبين أن الإجراءات الجديدة لاستخلاص الدليل في البيئة الالكترونية قد تشكل خطرا كبير يهدد الحق في الخصوصية، نظرا لما تتيحه لسلطات التحقيق من إمكانية الاطلاع على أسرار خاصة بأشخاص قد لا يكون لهم يد في الجريمة، مما جعل المشرع يحرص كل الحرص على حصر اللجوء إلى هذه الإجراءات في الحالات التي تستدعي ضرورة التحقيق والتحري الى ذلك، كما أحاطها بجملة من الضمانات القانونية التي يتعين على المحقق احترامها عند استعماله لهذه الإجراءات.

وقد أظهرت الدراسة كذلك أنه من المشكلات التي تواجه سلطات البحث و التحقيق ما يتعلق بالقيمة القانونية للأدلة الالكترونية

المتحصل عليها في عملية الإثبات الجنائي أو بمعنى أخر مدى قبول هذه الأدلة كوسيلة إثبات من طرف القاضي الجزائي، إذ أن عملية استخلاص الدليل الالكتروني سواء بالطرق الإجرائية التقليدية أو المستحدثة ليست بالسهولة بما كان، بل تعيقها في غالب الأحيان صعوبات تتعلق إما بالطبيعة التكوينية للدليل الالكتروني أو بالعامل البشري. كما أن مجرد وجود دليل يثبت وقوع الجريمة ونسبتها الى شخص معين قد لا يكفى للتعويل عليه، بل يلزم أن يكون لهذا الدليل قيمة قانونية، التي تتوقف على مسألتين أساسيتين، الأولى هي مشروعية الدليل، والثانية هي حجيته على الوقائع المراد إثباتها.

فالأدلة الإلكترونية وإن كانت تتمتع بقيمة علمية قاطعة في الدلالة على الحقائق التي تتضمنها، إلا أن ذلك لا يغني عنها ان تكون مشروعة، سواء من حيث الوجود، بان تكون من ضمن الأدلة المقبولة قانونا كوسيلة إثبات. أو من حيث التحصيل، وذلك بان يتم الحصول عليها بالطرق القانونية وأن تقدم للمحكمة على الهيئة نفسها التي تم جمعها عليها، بدون أن يطرأ عليها أي تغيير أو تحريف خلال فترة حفظه.

## ثانيا: ايجابيات التحقيق الالكتروني

تفاديا لإفلات المجرم الالكتروني من المتابعة الجزائية و العقاب، بادر المشرع في الكثير من الدول إلى إعادة النظر في بعض القواعد الإجرائية المتعلقة باستخلاص الدليل كالتفتيش و الضبط وجعلها صائغة الاستعمال في مجال البيئة الرقمية الالكترونية. فضلا عن استحداث قواعد إجرائية أخرى تتلاءم مع الطبيعة الخاصة التي يتميز بها هذا النوع من الجرائم، كالمراقبة الالكترونية واعتراض المراسلات والتسرب الالكتروني، وهو ما أقدم عليه المشرع الجزائري من خلال تعديل قانون الإجراءات الجزائية في عام 2006، وإصداره القانون رقم (40/90) المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

# الخـــــــــــــــاتـــمة

لا يكفي الاعتماد على التشريعات القائمة لتجاوز الصعوبات الإجرائية التي تثيرها عملية البحث والتحقيق في الجرائم الالكترونية بل لا بد من تدعيمها بنصوص خاصة حديثة تتضمن إجراءات تحقيق ملائمة مع طبيعة هذا الشكل الجديد من الإجرام، ومسايرة للمتغيرات او للتطوارت الحاصلة في تقنيات وأساليب ارتكابها. كما فعل المشرع الجزائري من خلال القانون رقم (90-40) المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. حينما استحدث تقنيات ومعالم جديدة توضح القواعد الإجرائية في مجال تحريك ومباشرة الدعوى الجزائية و اتباع آثار المجرم الالكتروني من خلال تحديد الترتيبات التقنية للمراقبة الإلكترونية، وكيفية تفتيش المنظومة المعلوماتية عن بعد، ثم إجراءات حجز المعطيات الإلكترونية، ورسم معالم الاختصاص القضائي تحسبا للطابع الدولي الذي تكتسيه الجرائم الإلكترونية.

ضرورة تكثيف التعاون والتنسيق الدولي بين الدول من اجل تطوير وتوحيد التشريعات الجزائية الموضوعية والإجرائية

التي تعنى بمكافحة الجرائم الإلكترونية، عن طريق إبرام اتفاقيات دولية وإقليمية ثنائية ومتعددة الأطراف في هذا المجال، أو الانضمام إلى الاتفاقيات المبرمة في هذا الخصوص ضرورة اعتماد سياسة واضحة وفعالة بخصوص التعاون الأمني المتبادل والمساعدة القضائية والفنية بين الدول في مجال مكافحة الجريمة الإلكترونية، من خلال تبني إجراءات التحقيق والمتابعة الجزائية السريعة والمناسبة، وخلق قنوات اتصال ثنائية أو متعددة الأطراف تسمح للسلطات القائمة على التحقيق، الاتصال بسهولة بمثيلتها الأجنبية والتنسيق معها. أو التدخل السريع للتحقيق في إقليم دولة أجنبية دون ان يشكل ذلك مساسا بسيادة هذه الدولة.

دعوة الدول العربية إلى إنشاء منظمة شرطة عربية تهتم بالتنسيق الامني في مجال مكافحة الجرائم المعلوماتية عبر الانترنت؛ مع تشجيع قيام اتحادات عربية تهتم بالتصدي لجرائم الانترنت وتفعيل دور المنظمات والإدارات والحكومات العربية في مواجهة هذه الجرائم عن طريق نظام الأمن الوقائي.

ضرورة إنشاء وحدات أمن وأجهزة قضائية متخصصة في مكافحة الجرائم الإلكترونية، يكون لديهم الإلمام الكافي بالجوانب التقنية والفنية لمتابعة وكشف وضبط تلك الجرائم ومرتكبيها، مع إخضاعهم لبرامج تدريبية خاصة

دورية، تساعدهم على تحيين وتحديث معارفهم وخبراتهم وإطلاعهم بآخر المستجدات الحاصلة مجال التقنية المعلوماتية.

إتاحة الفرصة للمواطنين للمشاركة في مكافحة الجرائم الالكترونية من خلال إنشاء خطوط ومواقع اتصال خضراء تعمل على مدار الساعة، وتسمح لأي كان بالإبلاغ عن بعد بوقوع جريمة الكترونية دون قيد أو شرط.

ضرورة نشر الوعي في أوساط المجتمع بالمخاطر الاقتصادية والاجتماعية والنفسية وغيرها الناجمة عن الاستخدامات غير المشروعة وغبر الآمنة للأنترنت، وبما يترتب عنها من انعكاسات سلبية على حياة الفرد والمجتمع.

تفعيل دور المجتمع المدني والحراك الجمعوي المؤهل في التحسيس والوقاية من الوقوع في الممارسات الخاطئة او السلوكيات الإجرامية عبر شبكة الانترنت.

كما يتعين إدخال مادة "أخلاقيات استخدام الانترنت" ضمن المناهج الدراسية في التعليم ما قبل الجامعي.