

المراقبة الإلكترونية كإجراء استدلالي في مواجهة الحق في الخصوصية

تاريخ استلام المقال: 2015/10/30 تاريخ قبول المقال للنشر: 2016/09/22

أ.مرنيز فاطمة

جامعة بشار

الملخص:

تعتبر المراقبة من أهم مصادر التحري التي غالبا ما يستهان بها في البحث والتقصي عن الجرائم، سواء التقليدية أو المستحدثة منها كجرائم الانترنت، فهي جزء لا يستغني عنه في أعمال المتحري، إذ تعتبر أسرع الدروب لكشف هذه الأخيرة من الجرائم، وتسمى حينئذ بالمراقبة الإلكترونية.

Abstract :

Monitoring is one of the most important sources of investigation which is often underestimated in research and investigation for the crimes, whether traditional or modern such as online crimes. Monitoring is indispensable in the work of investigators, as it is considered the fastest routes to detect online crimes. The method is called electronic monitoring.

مقدمة:

تعدّ مرحلة جمع الاستدلالات من المراحل الخطرة في إطار عملية بناء الدعوى الجنائية، لذلك نجدّها في إطار النظرية العامة تتخذ موقعها كأول مرحلة يتولاها المشرع والفقّه بدعم قضائي بالرّصد¹.

ولعل الحاجة إلى التنظيم التشريعي لجوانب الاستدلال والتّحري² في حق جرائم الإنترنت ومسائل حماية الحق في الحياة الخاصة أيضا، تجد موجبها في الحاجة إلى توفير معيار مقبول يقيم توازنا بين حقوق وحرّيات الأفراد وحماية خصوصياتهم، وبين موجبات المكافحة وحاجتها إلى قواعد استثنائية تفرضها تحدّيات هذه الجرائم التي تزيد عن تحدّيات غيرها³.

ومن أهم هذه التّحدّيات، سرعة إتلاف الدليل، وطبيعة ما يثبت الجريمة ذاتها من الأدلة في ظل الحاجة للتّدخل السريع لضبط متعلقات الجريمة، إلى جانب إمكانية ارتباط مادة الجريمة أو وسيلتها بأنظمة وأطراف أخرى لا صلة لهم بها، أو شبكات ونظم معلومات خارج الحدود.

¹ - عمر أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، دار النهضة العربية، مصر، 2004، ص 807.

² - لفظي التحري والاستدلال وردا في اللغة بمعنى مشابه، فإذا كان الفعل تحرى يقصد به في اللغة "طلب الأمر"، وكلمة استدلال يقصد بها "طلب أن يدل عليه"، فإن معنى ذلك أن الكلمتين في اللغة تفيدان معنيين لمدلول واحد. عادل عبد العال خراشي، المرجع السابق، ص 15، 16.

³ - سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الانترنت، دار الفكر الجامعي، الإسكندرية، 2006، ص 108.

وتكمن أهمية هذه المرحلة في البحث والتحري عن الجرائم وعن مرتكبيها، وجمع المعلومات عنها، وتحضير المادة اللازمة لتحريك الدعوى العمومية، وبعبارة أخرى تهيئة القضية وتقديمها للنيابة العامة باعتبارها جهة الإدارة والإشراف على الضبط القضائي لتقدير مدى إمكان عرضها على جهات التحقيق أو الحكم حسب الأحوال¹.

وبهذا فإنّ المكافحة الفاعلة قد تتطوي على إهدار لحقوق وحرّيات الأفراد، والتفريط في الضمانات القانونية.

وإمعانا من المشرع والفقهاء الجنائي في الإشادة بالدور الرئيس الذي يقوم به مأمور الضبط القضائي في البحث والتحري، فقد افترض كونه "خط الدفاع الأول ضد الجريمة"² فبرزت مرحلة الاستدلالات في جرائم الإنترنت كأحد أهم المراحل التي يستعان بها لمواجهة الجريمة عبرها. ويترتب على ذلك، أنّه يكمن عمل مأمور الضبط القضائي في لزوم القيام بالبحث عن الجرائم ومرتكبيها عبر شبكة الإنترنت، وحسبما يقرر القانون ذلك، أو ما يصطلح عليه بأساليب التحري الخاصة، وهي مجموع الإجراءات التي يقوم بها المتحري عبر شبكة الإنترنت، بواسطة التغطية الالكترونية الرقمية، وكذلك على أجهزة الحاسب الآلي، وذلك للحصول على بيانات ومعلومات تعريفية أو توضيحية عن الأشخاص أو الأماكن أو الأشياء حسب طبيعتها لضبط جرائم الإنترنت، فهي وسيلة لجمع المعلومات والأدلة³.

وفي هذا الإطار، تعد المراقبة الإلكترونية من أهم وأبرز هذه الأساليب، وهي مسألة تثير إشكالية للبحث حول: ما مفهوم المراقبة الإلكترونية كإجراء استدلالي و ضماناته في مواجهة الحق في الحياة الخاصة للأفراد عبر شبكة الإنترنت؟.

المطلب الأول: مفهوم المراقبة الإلكترونية وعلاقته بالحق في الخصوصية

تعتبر المراقبة من أهم مصادر التحري التي غالبا ما يستهان بها في البحث والتقصي عن الجرائم، سواء التقليدية أو المستحدثة منها كجرائم الانترنت، فهي جزء لا يستغني عنه في أعمال رجال البحث والتحري، إذ تعتبر أسرع الدروب لكشف هذه الأخيرة من الجرائم، وتسمى حينئذ بالمراقبة الالكترونية⁴.

¹ - عبد الله اوهابيه، شرح قانون الإجراءات الجزائية الجزائري، دار هونه للطباعة والنشر الجزائر، 2003، ص 184.

² - عمر أبو بكر بن يونس، الجرائم... المرجع السابق، ص 808.

⁽³⁾ - عفيفي كامل عفيفي، المرجع السابق، ص 474.

⁴ - وهي تختلف عن نظام "الوضع تحت المراقبة الالكترونية كأحد الأساليب المبتكرة لتنفيذ العقوبة السالبة للحرية قصيرة المدة خارج أسوار السجن- في الوسط الحر بصورة ما يدعى "السجن في البيت". ويقوم هذا الأسلوب على السماح للمحكوم بالبقاء في منزله، لكن تحركاته محدودة ومراقبة بواسطة جهاز يشبه الساعة أو سوار مثبت في معصمه أو في أسفل قدمه. ومن هنا جاءت تسمية هذا الأسلوب "السوار

ويترتب على ذلك، طرح إشكالية البحث في علاقة هذا الإجراء بالحق في الحياة الخاصة للأفراد، وهو ما يتبين من خلال تحديد المقصود بالحق في الحياة الخاصة (الفرع الأول)، ثم ما هي آليات تنفيذ المراقبة الإلكترونية كإجراء استدلاي في مواجهة هذا الحق (الفرع الثاني) ؟

الفرع الأول: المقصود الحق في الخصوصية

يكاد ينعقد الإجماع على صعوبة التوصل إلى تعريف جامع مانع للحق في الحياة الخاصة أو الخصوصية أو السرية الشخصية كما يسميها البعض¹. لذلك نجد من الأهمية البحث في الدلالة اللغوية ثم المعن الاصطلاحي لهذا الحق.

الخصوصية لغة: يرجع أصل هذه الكلمة في اللغة العربية إلى الفعل خص فيقال خص فلانا بالشيء، بمعنى فضله به وأفرده، ويقال كذلك: خصه بالود أي حبه دون غيره، وخاصة الشيء ما يختص به دون غيره أي ينفرد به، وتعني لفظة الخصوصية في اللغة الانجليزية privacy أي أنها حالة العزلة والانسحاب من صحبة الآخرين²، كما تستخدم لمعان قد تعبر بشكل أو بآخر عن مظاهر معنى هذه الكلمة إن لم يكن مرادفا لها، لتدل على الطمأنينة والسلم والوحدة والانسحاب من الحياة العامة والتفرد.

الخصوصية اصطلاحاً: رغم أن الدساتير والتشريعات الحديثة قد اتفقت على حماية حرمة الحياة الخاصة، إلا أن تعريف هذا الحق ما زال يثير جدلاً وخلافاً في القانون المقارن،

الالكتروني "Le bracelet électronique" "يدعى الوضع تحت المراقبة الالكترونية باللغة الفرنسية، Le placement sous surveillance électronique أي" السجن في البيت La prison à domicile.

Benghozi M, *L'assignation à domicile sous surveillance électronique*, Déviance et Société, 1990, n°1, pp.

59.

يرى كثير من الفقهاء أن المراقبة الالكترونية " تحتل مكاناً متوسطاً ملائماً بين احترام فكرة العقوبة ومفهومها، وبين الغايات المرتبطة بأمن المجتمع، ومعاينة المحكوم عليه، والمشاكل المرتبطة بالوسط العقابي حالياً ". من هؤلاء راجع:

Landreville P, *Surveiller et prévenir. L'assignation à domicile sous surveillance électronique* Déviance et Société, 1987, n° 3, pp. 251-264.

¹ - بن يحي إسماعيل: جرائم التعدي على التجارة الالكترونية، مذكرة ماجستير تخصص قانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة بشار، 2009-2010، ص.52.

² - علي أحمد عبد الزعي: حق الخصوصية في القانون الجنائي، دراسة مقارنة، الطبعة الأولى، المؤسسة الحديثة للكتاب، طرابلس، لبنان، 2006، ص.115، 116.

وقد اتفق الفقه على صعوبة تحديد هذا المضمون بصورة تتلاءم مع مقتضيات العلم القانوني¹.

لكن من منطلق أن لكل إنسان الحق في أن تحترم حياته الخاصة، وأن هذا المبدأ لا يثير خلافا بين أولئك الذين يسعون لتدعيمه، وأن هناك اتفاق عالمي التوجه بشأن هذا الحق الأساسي²، فإنه يمكن تعريف الحق في الخصوصية³، أو ما كما يعرف في النظام اللاتيني بالحق في الحياة الخاصة بأنه حق احترام سرية وخصوصية الأشخاص من أي تدخل مادي أو معنوي، وهو حق عميق الجذور من الوجهة التاريخية⁴.

حيث تستهدف حماية هذا الحق صون كرامة الإنسان واحترام أدميته من خلال عدم التطفل عليه، وعدم انتهاك أسرار ومبادئه وسائر جوانب حياته الخاصة كأحد الحقوق اللصيقة بالشخصية التي تثبت للإنسان، والتي غالبا ما يصعب حصر الجوانب المختلفة لها، والتمييز بحدود واضحة بين ما يعد من الحياة الخاصة للإنسان وما يعد من الحياة العامة له⁵.

وفي هذا الإطار، حظيت الحياة الخاصة للأفراد بحماية دستورية⁶ وقانونية في مختلف تشريعات الدول المتقدمة، كما عُنيت الإعلانات والمواثيق الدولية والإقليمية بحماية هذا الحق.

الفرع الثاني: آليات تنفيذ المراقبة الإلكترونية كإجراء استدلالي

¹ - محمد أمين الشوابكة: جرائم الحاسوب والإنترنت، الجريمة المعلوماتية، الطبعة الأولى، الإصدار الثاني، دار الثقافة، عمان، الأردن، 2006، ص. 58.

² - طارق عثمان: الحماية الجنائية للحياة الخاصة عبر الإنترنت، دراسة مقارنة، مذكرة ماجستير تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2007-2006، ص. 8.

³ - يستخدم الفقه في النظم اللاتينية مصطلح الحق في الحياة الخاصة *la vie prive*، ويطلق مصطلح الحق في الخصوصية *privacy* عند الفقه النظم الانجلوسكونية. محمد أمين الشوابكة: المرجع السابق، ص. 58.

⁴ - عبد الله فكري: جرائم نظم المعلومات، دراسة مقارنة، دار الجامعية الجديدة للنشر، مصر، 2007، ص. 613.

⁵ - محمد أمين الشوابكة: المرجع السابق، ص. 58.

⁶ - اهتم الدستور الجزائري بالحق في الحياة الخاصة من خلال مجموعة من النصوص نذكرها:

تنص المادة 32 من دستور 23 نوفمبر 1996 على ما يلي: "الحريات الأساسية وحقوق الإنسان والمواطن مضمونة، وتكون تراثا مشتركا بين جميع الجزائريين والجزائريات، واجبه أن ينقلوه من جيل إلى جيل كي يحافظوا على سلامته، وعدم انتهاك حرمة".

والمادة 34 منه: "تضمن الدولة عدم انتهاك حرمة الإنسان، ويحظر أي عنف بدني أو معنوي أو أي مساس بالكرامة".

والمادة 35: "يعاقب القانون على المخالفات المرتكبة ضد الحقوق والحريات، وعلى كل ما يمس سلامة الإنسان البدنية والمعنوية".

والمادة 39: "لا يجوز انتهاك حرمة حياة المواطن الخاصة وحرمة شرفه، ويحميها القانون".

والمادة 139: "تحمي السلطة القضائية المجتمع والحريات، وتضمن للجميع ولكل واحد المحافظة على حقوقهم الأساسية".

عملية المراقبة هي عمل أمني أساسي له نظام معلومات، يقوم به المراقب بمراقبة المراقب بالوسائل لتحقيق غرض محدد وتحرير تقارير بالنتيجة.

وتحديدًا المراقبة الأمنية هي العمل الذي يقوم به المراقب باستخدام حواسه لجمع بيانات ومعلومات عن المشتبه فيه، والهدف سواء كان شخصا أو مكانا وشيئا حسب طبيعته، مرتبط بالزمن (التاريخ والوقت) لتحقيق الأمن ولأي غرض آخر، فالمراقب هو فرد الأمن المكلف بالمراقبة، والفرق بينه وبين المراقب واضح فالأول هو ممثل النظام في حين الثاني مخالف للقانون.

أما الوسائل فهي تلك المستخدمة في تتبع حركة الهدف (المشتبه فيه) سواء كانت وسائل نقل أم وسائل اتصال أم وسائل فنية، أما الغرض فهو متعلق بالمطلوب تحقيقه من وضع المراقب (المشتبه فيه) تحت المراقبة، في حين أن تقارير المراقبة فهي الوثائق الهيكلية بنتيجة المراقبة، وحتى تحقق المراقبة أغراضها يجب توفر شروط وقدرات معينة في كل عنصر من تلك العناصر¹.

كما يمكن على ضوء تباين نوعية المراقبة الالكترونية المطلوبة كإجراء، وهي حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية، تأخذ المراقبة الالكترونية إما صورة المراقبة الشخصية (أولا)، أو المراقبة البرمجية (ثانيا).

أولا: المراقبة الشخصية

المراقبة الشخصية هي قيام المرشد أو مأمور الضبط القضائي بنفسه أو من يفوضه في ذلك من مرشدين سريين، لا يكشفون عن هويتهم أو المهام الموكلة إليهم بقصد البحث عن الجرائم ومركبيها عبر الإنترنت، ومثل هذا الإجراء مقبول في القانون بدون تحفظ طالما لم يكن هو تحفيزا أو بحثا من قبل مأمور الضبط القضائي للغير على ارتكاب جريمة بما يضعه في مأزق الفاعل المعنوي أو الشريك بالمساعدة²، أو يضمن القانون مأمور الضبط القضائي سرية من مصادره الإرشادية حيث يكون له فقط صلاحية الكشف عن أسماء من يستعين بهم في البحث عن الجرائم ومركبيها .

إن مأمور الضبط القضائي في نظام الإرشاد الجنائي عبر الانترنت يمكن أن يقوم بذاته بدور المرشد أو أن يكلف غيرهم من هم على الإيصال بالإنترنت حيث أنه لا يحتاج إلى لا يحتاج إلى مجهود مادي كبير يبذل في هذا الإطار، فكل ما عليه فعله هو الحصول على إذن

¹-مصطفى محمد موسى المراقبة الالكترونية عبر الانترنت، دراسة مقارنة، دار الكتب القانونية، مصر، 2005. ص 6، 7.

²- عمر أبو بكر بن يون: الجرائم، المرجع السابق، ص 840.

رسمي بمباشرة مهامه عبر الإنترنت ثم الجلوس على حاسوب على اتصال بالإنترنت أو ربما حاسوبه الشخصي.

ويلزم أن يتضمن الإذن الرسمي بمباشرة مهام البحث عن الجرائم ومرتكبيها مساحة يكتب فيها رقم الحاسوب وصلاحيته للعمل وخلوه من العوائق التكنولوجية واحتوائه على برمجيات أصلية وليست منسوخة، تذكر أيضا أرقامها المسلسلة رقم وتاريخ الترخيص بها وجهة إصدارها¹ إلى غير من البيانات اللازمة.

فإذا ما تم كل ذلك، فإنه يشرع في الولوج إلى الإنترنت سعيا وراء الكشف عن الجرائم ومرتكيها بآليات مختلفة، فله أن يلج إلى قاعات الدردشة أو حلقات النقاش أو استخدام برمجيات الاتصال المباشر المستقلة والتتكر عبر الانترنت في هيئات مختلفة واتخاذ أسماء مستعارة وتناول الأحاديث المختلفة.

وبشكل عام الظهور بمظهر طبيعي كما لو كان فعلا ذلك الشخص الطبيعي الذي يجالس الغير سعيا إلى إضاعة الوقت والهروب من الملل، فالحديث يستمر عاديا، فليس للمرشد الجنائي دفع الغير إلى ارتكاب الجريمة، وإنما يظل يتداول أحاديث عادية إلى اللحظة التي يبرز فيها مشروع إجرامي من قبل الغير كأن يكون هناك حديث في إحدى حلقات النقاش حول دعارة أطفال أو كلام يدور حول كيفية قام أحدهم باختراق شبكات أو بث فيروسات... الخ، ففي هذه الأحوال يكون للمرشد الجنائي القيام بتقصي المعلومات كأن يقوم سؤال الهاكر عن كيفية اقتحامه لموقع ما أو السؤال عن كيفية قيام الشخص ببث الفيروس عبر الإنترنت إذا ادعى أحدهم ذلك... الخ.

وهنا يقوم المرشد الجنائي باتخاذ إجراءات توصيل مثل هذه المعلومات إلى جهة الضبط القضائي التي تباشر عملها في ضبط وإحضار المجرم وجريمته، وهي تعمل في ذلك مستخدمة برمجيات معينة تقودها إلى مسار مزود الإنترنت²، الذي يتحرك فيه مرتكب الجريمة أو أن تقوم جهة الضبط القضائي باستدراج المجرم حال تعرفها على نواياه¹.

¹ - نبيلة هبة هروال: الجوانب الإجرائية لجرائم الانترنت، في مرحلة جمع الاستدلالات (دراسة مقارنة)، الطبعة الأولى، دار الفكر الجامعي، مصر، 2006، ص. 196.

² - المادة 11 من القانون رقم 04-09 المؤرخ في 05 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها) : " مع مراعاة طبيعة ونوعية الخدمات، يلتزم مقدمو الخدمات بحفظ:

أ- المعطيات التي تسمح بالتعرف على مستعملي الخدمة،

ب- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال،

ج- الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال،

ثانيا: المراقبة البرمجية.

ويقصد المراقبة البرمجية مراقبة شبكة الاتصالات، أو العمل الذي يقوم به المراقب (بكسر القاف) باستخدام التقنية الإلكترونية لجمع بيانات ومعلومات عن المشتبه فيه سواء أكان شخصا أو مكانا أو شيئا حسب طبيعته مرتبط بالزمن (التاريخ والوقت) لتحقيق غرض أمني أو لأي غرض آخر².

فالمراقبة الإلكترونية هي الأخرى وسيلة من وسائل جمع البيانات والمعلومات عن المشتبه فيه، يقوم بها مراقب إلكتروني، يتمثل في مأمور ضبط قضائي ذي كفاءة تقنية عالية تتماشى مع نوع الجريمة التي يتعامل معها، مستخدما في ذلك التقنية الإلكترونية وعبر شبكة الإنترنت، كأن يراقب أحد الهكرة ممن قام باختراق الحاسب الآلي الخاص بالمجني عليه، أو يقوم بإعداد صندوق بريد إلكتروني مستنسخ لمراقبة المشتبه فيه عند إرساله أو استقباله لصور داعة للأطفال عبر الإنترنت.

ويشترط في كل هذا، أن يحصل على إذن من ذلك المجني عليه، أو من الجهة القضائية المختصة³، كالحصول على أمر بتلك المراقبة من المحكمة.

ومن جهة، فإن المشتبه فيه المراقب من طرف مأمور الضبط القضائي هو شبكة الاتصالات، وذلك عن طريق مراقبة الشخص الذي أساء استخدام مواقع الإنترنت أو البريد الإلكتروني، إذا تم من خلالها مراقبة اتصالاته الإلكترونية المشتبه فيها، أي تلك التي تتم عن طريق الإنترنت بما في ذلك مراسلات البريد الإلكتروني⁴.

ومن جهة ثانية، فإن التقنية المستخدمة في هذه المراقبة هي التقنية الإلكترونية، والتي تعني مجموعة الأجهزة المتكاملة مع بعضها لغرض تشغيل مجموعة من البيانات المتعلقة بالمجرمين أو المشتبه فيهم وقف برنامج موضوع مسبقا لتحديدهم من أجل ضبطهم وتفتيشهم وجمع الأدلة قبلهم لإثبات إدانتهم وتقديمهم إلى المحاكمة⁵.

- ونذكر بعض النماذج عن تقنيات المراقبة الإلكترونية:

د- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها،

هـ- المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها..."

¹- عمر أبو بكر بن يونس، الجرائم ...، المرجع السابق، ص 839.

²- نفس المرجع السابق، ص 192

³- المادة 4 من القانون 04-09 المتضمن القواعد الخاصة بتكنولوجيات الإعلام والاتصال ومكافحتها: "...لا يجوز إجراء عمليات المراقبة

في الحالات المذكورة ... إلا بإذن مكتوب من السلطة القضائية المختصة..."

⁴- نبيلة هبة هروال، المرجع السابق، ص 199.

⁵- مصطفى محمد مرسي، المرجع السابق، ص 205.

- **تقنية برنامج كارنيوز:** هذه التقنية طورتها إدارة المعلومات التابعة لمكتب التحقيقات الفيدرالي F.B.I، وذلك من أجل تعقب وفحص رسائل البريد الإلكتروني المرسله والواردة عبر أي حاسب خادم تستخدمه أي شركة تقوم بتوفير خدمة الإنترنت ويشتهر في أن تيار الوسائل المار عبر خدماتها يحمل معلومات عن جرائم جنائية.

لا يتم تنفيذ هذه العملية إلا بعد استئذان المحكمة المختصة بوضع أجهزة تلك الشركة تحت المراقبة.

إلا أن هذه التقنية قد اعتبرت بأنها تخترق الحق في الخصوصية، ولذلك أصدر القضاء الأمريكي خلال الأسبوع الثاني من شهر أغسطس /أوت 2000 حكماً يلزم مكتب التحقيق الفيدرالي بإذاعة التسجيلات والمعلومات التي يحصل عليها من عمليات التصنت على رسائل البريد الإلكتروني لمستخدمي شبكة الانترنت 10 أيام لتنفيذ الحكم وذات الشأن بالنسبة للكونجرس الأمريكي¹.

ولكن وبالرغم من ذلك فقد حققت هذه التقنية نجاحات كبيرة في تعقب المجرمين، ولقد أصبح يطلق على هذه التقنية بعد 11 سبتمبر 2001 ، تقنية 1000 " DCS " وأصبحت تختص بمتابعة القضايا المتعلقة بالأمن القومي والتصدي لأي محاولة لتنفيذ هجمات داخل الولايات المتحدة الأمريكية، وقد تمكن مكتب التحقيقات الفيدرالية بفضل هذه التقنية من تقديم قرائن أدانت قائد ميليشيات كانت تستخدم الإنترنت للتراسل، وللتخطيط للدخول إلى المنشآت العسكرية لسرقة متفجرات وتفجير محطات الطاقة الموجودة جنوب شرق الولايات المتحدة الأمريكية².

- **تقنية تعقب المواقع الإباحية أو ما يسمى ببرنامج " نوبد شرطة الإنترنت ":** وهو برنامج يبحث عن الصور الجنسية المخلة على أنظمة الكمبيوتر التي تعمل ببرامج تشغيل "ويندوز" الحديث وبلغ الهيئات الحكومية عنها بهدف تطهير الشبكة من المواقع الإباحية والجنسية، وهو يصل إلى تلك الأخيرة على شكل دورة إلكترونية ملحقه برسالة إلكترونية بعنوان " ساعدونا لإنهاء المواقع الإباحية " ³.

المطلب الثاني: اثر المراقبة الإلكترونية كإجراء استدلاي في مواجهة الحق في الخصوصية

¹-نبيلة هبة هروال، المرجع السابق، ص.201.

²- مصطفى محمد مرسي، المراقبة الإلكترونية...، المرجع السابق، ص.202.

³- نفس المرجع السابق، ص.217.

إن البحث في الإطار القانوني للمراقبة الالكترونية كإجراء استدلاي في مواجهة الحق في الخصوصية عبر شبكة الإنترنت، يقتضي تحديد نطاق هذا الحق عبر شبكة الإنترنت (الفرع الأول)، ثم البحث في ضمانات تنفيذ هذا الإجراء (الفرع الثاني).

الفرع الأول: نطاق الحق في الخصوصية عبر شبكة الإنترنت

بداية يقتضي تحديد المقصود بالخصوصية المعلوماتية، بحث موضوع شبكة الإنترنت وعلاقتها بالحياة الخاصة للأفراد، ويتجلى ذلك من خلال ما شهدته الإنترنت بتزايد الاتجاه من قبل الحكومات والهيئات والشركات والأفراد نحو نشر وحفظ الملفات والبطاقات الخاصة بهم على حاسباتهم الآلية المتصلة بالإنترنت¹. وقد شهدت شبكة الإنترنت نماء التوجه نحو جمع البيانات المتوفرة في العالم الحقيقي باعتبارها تصبح أكثر سهولة في بيئة الإنترنت من حيث قدرة الوصول إليها، وأكثر ملائمة للتبويب بسبب تقنيات الحوسبة وأسهل للتبادل في ضوء وسائل تبادل المعلومات بكل أشكالها التي إتاحتها الإنترنت وبرمجيات التصفح والتبادل والنقل، فالبيئة التي تمر عبرها رحلة البيانات المتبادلة تغيرت بسبب الإنترنت².

غير أن ذلك وسع من المخاطر التي تهدد الحياة الخاصة نتيجة تقنية المعلومة المتقدمة، ويتجلى هذا الأثر في أمرين:

أولاً: الإنترنت تشكل أكبر آلة لجمع وحفظ ومعالجة البيانات الشخصية

توفر في مجال شبكة الإنترنت العديد من الوسائل لجمع وحفظ ومعالجة البيانات الشخصية للأفراد نذكر على سبيل المثال:

1- البرمجيات المتوفرة لدى مزود خدمات الإنترنت لرقابة إبحار مستخدمي الإنترنت التي تسجل عناوين المواقع التي يزورها المستخدم، تاريخ ومدة استخدام الإنترنت، و ذا تدخلات المستخدم كالتي يقوم بها مثلاً في منتديات الحوار أو قاعات الدردشة³، كما قد تتضمن بيانات حول الوقت الذي تم قضاؤه في كل صفحة، البيانات التي أرسلت واستقبلت، ويتم تسجيل هذه البيانات من قبل مزودي خدمات الإنترنت في ملفات تعرف "، ويتم الاحتفاظ بها لعدة شهور fichier .log

2- برامج الرقابة والتتبع التي تستخدمها محركات البحث لتسجيل تحركات المستخدم عبر الإنترنت، والمواضيع التي تهتم، والمواقع التي يتصل بها، كما تقوم هذه البرامج بتحليل هذه

¹ - أسامة عبد الله بلقايد : الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة العربية، مصر 1994 ، ص 61

² - محمد حسين منصور : المسؤولية الالكترونية، دار الجامعة الجديدة، بدون طبعة، مصر، 2007 ، ص 307

³ - يونس عرب: " المخاطر التي تهدد الخصوصية وخصوصية البيانات في العصر الرقمي، ص6

<http://www.arablaw.org/privacy%20&20%security.htm>

البيانات لمعرفة ميول المستخدم وعادات التسوق لديه، وهذه البيانات من شأنها أن تشكل عند حملها بيانا بأنشطة المستخدم.

3_ استمارات الاستبيان التي تتضمنها مواقع الانترنت، وتقترح تعبئتها من طرف المستخدمين سواء بصورة اختيارية أو جبرية للمرور إلى باقي جوانب وخدمات المواقع، وتتضمن هذه الاستمارات جملة من البيانات الشخصية كعنوان البريد الإلكتروني للمستخدم، رقم الهاتف، اسم ولقب المستخدم ومهنته وسنه وحالته الاجتماعية، وأحيانا اهتمامات الشخص، أما مواقع البيع التي تم فيها إجراء عمليات الدفع، فإنها تتطلب أرقام بطاقات الائتمان ونوعها وتاريخ انتهاء صلاحيتها¹

4. الوسائل التقنية التي تستخدمها المواقع الإلكترونية لتتبع المعلومة الشخصية للمستخدمين، من أشهرها ما يعرف برسائل "الكوكيز" مع أنها اتبعت ابتداء لغرض غير جرمي، إلا أنها مثلت وسيلة مهمة لملاحقة واقتفاء اثر مستخدمي الانترنت، وجمع المعلومات عنهم، وتحليلها لغايات الدراسات التسويقية على الخط، ولم تكن هذه المعلومات بعيدة عن الاستغلال في أغراض غير مشروعة أو على الأقل لا علم لصاحبها بها.

إن هذه البيانات التي يتم جمعها عبر وسائل تقنية مختلفة تشكل بعد جمعها بيانا بأنشطة الفرد، وفي مرحلة من المراحل تصبح عند جمع شتاتها وتحليلها خاصة مع قيام برمجيات ذكية بذلك، مادة تكشف تفاصيل كثيرة قد لا يرغب الشخص بكشفها، وبنفس الوقت تصبح هذه البيانات محلا للبيع من جهة لأخرى لغايات الأعمال والأنشطة، كما ارتكبت العديد من جهات الرقابة أنشطة إساءة استخدام البيانات الشخصية التي كان في الغالب الهدف منها سياسيا أو اقتصاديا، لهذا كانت البيانات المستهدفة هي بيانات المعارضة السياسية والصحفيين وناشطي حقوق الإنسان، وهو ما اقتضى تزايد النشاط الدولي لحماية البيانات الشخصية².

ثانيا :عجز الانترنت عن ضمان سرية ما ينقل عبرها من بيانات .

¹ - نفس المرجع السابق، ص8

19- تم كشف النقاب عن تطوير وكالة التحقيقات الفدرالية برنامجا في عام 2000 يدعى الملتهم "كارينفور" لديه القدرة على التجسس على كافة الاتصالات والتبادلات عبر الانترنت(مصطفى محمد موسى: المراقبة الإلكترونية عبر الانترنت، دار الكتب القانونية، مصر، 2005، ص210. كما تنتشر في الولايات المتحدة الأمريكية شركات تدعى شركات اكتشاف الأدلة والقرائن الإلكترونية، وهي تضم محققين شرطة متقاعدين وخبراء في الإعلام الآلي وعلماء النفس، تقوم هذه الشركات بتسهيل عملها بالبحث والتحري في الوثائق الإلكترونية باعتبار أن هذه الوثائق تترك وراءها أثرا لا يمحي، ويمكن بالتالي استعادتها مهما اجتهد الفاعل في محوها و لقد طورت هذه الشركات العديد من برامج البحث في ذاكرة الحاسب الآلي عن الرسائل المحاة والمعلومات المصاحبة لها. انظر نفس المرجع السابق، ص214.

سهلت الانترنت عن طريق وسائل تبادل البيانات التي أتاحتها، من تنقل البيانات الشخصية من دولة إلى دولة، ومن منظمة لمنظمة، ومن جهة عمل لأخرى، ومن فرد إلى مؤسسة دون قيد، وبكل اللغات¹.

غير أن ذلك خلق مشكلة أمنية تمثلت في عدم قدرة شبكات الاتصال على توفير أمان مطلق وكامل لسرية ما ينقل عبرها من بيانات.

وأمام هذه التحديات التي أضحت تهدد الحق في الخصوصية المعلوماتية، فإن استحداث المراقبة الإلكترونية كإجراء استدلالي عبر شبكة الإنترنت ومدى مساهمته بهذا الحق، يثير مسألة البحث في شروط تنفيذ هذا الإجراء.

الفرع الثاني: ضمانات المراقبة الإلكترونية كإجراء استدلالي

عملية المراقبة هي وضع شخص أو مكان أو حادث تحت ملاحظة ونظر رجال الأمن بصورة ليس من شأنها إحساس الغير بمباشرتها لتسجيل كل ما عساه يحدث من تصرفات غير قانونية قد تقع من الأفراد، ويكون من شأنها أن تخل بالأمن أو النظام العام في المجتمع على أن تجري المراقبة في إطار من الشرعية لجمع التحريات بشأن قضية ما لتقديمها كدليل على صحة الجريمة.

ويستند مجال تطبيق هذا الإجراء في التشريع الجزائري إلى القانون 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، حيث تنص المادة الثالثة منه: "مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية وفقا للقواعد النصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية".

وباعتبار أن للأحاديث الشخصية والاتصالات الخاصة حرمة تستمد من حرمة الحياة الخاصة لصاحبها، وتضمن حرمتها وحمايتها ضد أي مساس بسريتها فإن الحالات التي يسمح باللجوء إلى المراقبة الإلكترونية بموجب هذا القانون، واستنادا على نص المادة 4 الفقرة ج هي: "لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية".

¹ أيونس عرب: المرجع السابق، ص5

كما تقتضي التحريات والتحقيقات في إطار مراقبة الاتصالات عبر الشبكة الاستعانة بمزود الخدمات بموجب المادة 10 من القانون 04-09 المتضمن القواعد الخاصة بتكنولوجيات الإعلام والاتصال ومكافحتها والتي تنص: "...يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 أدناه، تحت تصرف السلطات المذكورة..."

لكن الإشكال الذي يطرح في هذا الصدد حول ما مدى التزام المتدخل المهني بسر المهنة باعتبار أن المهني أو مقدم خدمة الانترنت لا ينتمي إلى فئة الموظفين، وماذا لو كان من شأن إفشاء الأسرار التحقيق في الجرائم؟

يجيب الفقه أنه من منطلق الالتزامات التي تقع على عاتق مزود خدمة الانترنت، فإنه ملزم بإفشاء أسرار الاتصالات عبر شبكة الانترنت لرجال الضبط القضائي إذا كانت هذه المعلومات تفيد في الكشف عن الحقيقة بخصوص تحقيق جنائي قائم، إذ يرى جانب من الفقه ضرورة إدخال المتدخلين المهنيين على شبكة الانترنت في دائرة الدفاع عن الانترنت ومكافحة الإجرام عبرها¹.

ومن جهة أخرى المتدخل المهني ملتزم بعدم مراقبة الاتصالات الالكترونية للمشاركين²، لأن البيانات الشخصية المتعلقة بمستخدمي الانترنت تدخل في إطار الحق في الخصوصية، لذا لا يجوز لمقدمي الخدمات أن يقوم بمراقبة الاتصالات بزرع برامج معينة، ولا يتعارض ذلك مع حق مزود الخدمات في معرفة أماكن الأجهزة المتراصة وفقا لما يعرف بروتوكول الانترنت³.

أما على مستوى التشريع، فبالرجوع إلى نص المادة 10 في فقرتها الأخيرة والتي تنص: "... ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق". على أن الأمر لم يقف عند هذا الحد، فالإشكال الذي يطرح أيضا في هذا الإطار: هل يجوز لمقدمي الخدمات مراقبة النظام بدون إذن قضائي؟

¹ عمر محمد أبو بكر بن يونس: الجرائم...، المرجع السابق، ص. 710.

² شيماء عبد الغني محمد عطا الله: الحماية الجنائية للتعاملات الالكترونية، دار الجامعة الجديدة، الإسكندرية، 2007، ص. 217.

³ نفس المرجع السابق، ص. 219.

تأسيسا على ما سبق ذكره، فإن قاعدة التزام هذا المتدخل بعدم مراقبة الاتصالات الإلكترونية للمشاركين في إطار نشاطه، قد وردت استثناءات عليها تتمثل في:

1/ حالة المراقبة المعتادة لعمل الشبكة لأنها تسمح باكتشاف الجرائم المرتكبة عبر الشبكة.

2/ المراقبة بناء على شكوى من المشترك¹.

خاتمة :

خلاصة القول أن الجريمة المرتكبة عبر شبكة الإنترنت تشكل إحدى الجرائم المستحدثة التي تتطلب وسائل ومعينات تكنولوجية أثناء البحث والتحري وفي المقابل، لا يعني ذلك إلغاء القواعد التقليدية العامة، ومن بينها تلك القواعد التي تتصل بسلامة الإجراءات القانونية الشكلية التي قد يكون أي تجاوز لها سبب من أسباب بطلانها.

وترتب على ذلك، أن تكريس حرمة الحق في الحياة الخاصة في مواجهة الرقابة الإلكترونية عبر شبكة الانترنت كإجراء أوجبه مقتضيات التحريات والتحقيقات القضائية هي وسيلة لمحاكمة الإجرام عبر الإنترنت على المستوى الدولي.

ونقتضي أن يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية، مع وجوب تشديد الرقابة على القائم بهذا الإجراء، حتى لا يمتد الأمر إلى ارتكاب تجاوزات تشكل في حد ذاتها جرائم ماسة بخصوصية الاتصالات الخاصة عبر الشبكة وهذا وفقا للقيود والضوابط المنصوص عليها.

كما يجب أن يراعى التأهيل والتكوين لدى مأمور الضبط بصفته مراقب الكتروني، ولا يجوز إجراء المراقبة الإلكترونية إلا بإذن مكتوب من السلطة القضائية المختصة.

قائمة المراجع:

أسامة عبد قايّد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة العربية، مصر 1994.

سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الانترنت، دار الفكر الجامعي، الإسكندرية، 2006.

عبد الله اوهابيه، شرح قانون الإجراءات الجزائية الجزائري، دار هونه للطباعة والنشر الجزائر، 2003.

مصر، 2004. عمر أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، دار النهضة العربية،

محمد أمين الشوابكة، جرائم الحاسوب والإنترنت، الجريمة المعلوماتية، الطبعة الأولى، الإصدار الثاني، دار الثقافة، عمان، الأردن، 2006.

محمد منصور منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة، بدون طبعة، مصر، 2007.

يونس عرب، "المخاطر التي تهدد الخصوصية وخصوصية البيانات في العصر الرقمي".

¹ شيماء عبد الغني محمد عطا الله : المرجع السابق، ص224.

[http:// www.arablawn.org/privacy%20&20%security.htm](http://www.arablawn.org/privacy%20&20%security.htm)

شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الالكترونية، دار الجامعة الجديدة، الإسكندرية، 2007.

نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت، في مرحلة جمع الاستدلالات (دراسة مقارنة)، الطبعة الأولى، دار الفكر الجامعي، مصر ، 2006.

مصطفى محمد مرسى، المراقبة الالكترونية عبر الانترنت، دراسة مقارنة، دار الكتب القانونية، مصر، 2005.

محمد حسين منصور، المسؤولية الالكترونية، دار الجامعة الجديدة، بدون طبعة، مصر، 2007 .

طارق عثمان، الحماية الجنائية للحياة الخاصة عبر الانترنت، دراسة مقارنة، مذكرة ماجستير، كلية الحقوق، جامعة محمد خيضر بسكرة، 2006-2007.

القانون رقم 04-09 المؤرخ في 14 شعبان 1430 هـ الموافق لـ 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات والإعلام والاتصال ومكافحتها، ج.ر العدد 47 بتاريخ 16 أوت 2009، ومتاح على الموقع: www.joradp.dz

Benghozi M, *L'assignation à domicile sous surveillance électronique*, Déviance et Société, 1990, n°1.

Landreville P, *Surveiller et prévenir. L'assignation à domicile sous surveillance électronique* Déviance et Société, 1987, n° 3.