تدابيـر الضبـط الإداري لمكافحة جـرائـم وسائل التواصل الاجتماعي

د / فوزي محمد صقر

دكتوراه فى القانون العام- جامعة عين شمس

المقدمة

مما لا شك فيه أن الحقوق و الحريات اليوم أضحت مسألة تخص جميع أعضاء المجتمع الدولي ، وقد صدرت من أجلها الكثير من المواثيق الدولية ، وعقدت المؤتمرات وعدلت الدساتير وإن كان من حق الفرد اليوم أن ينعم ببعض الحريات ، فإن تمتعه بها لا يتم بصفة مطلقة ، ودون ضوابط ، فأي حرية وأي حق إذا ما أطلق استعماله لصاحبه انقلب دون شك إلى فوضى، و أثر ذلك على حقوق وحريات الآخرين ، فالتقيد بالنظام ، والالتزام بالضوابط التي تحدثها القوانين والأنظمة هي التي تميز الحرية عن الفوضى ، وهذا الالتزام يُعدُّ سلوكًا حضاريًا ومظهرًا من مظاهر التمدن، ولا شيء فى علم القانون اسمه المطلق.

ولكي لا يساء استعمال الحرية أن تضبط من قبل السلطة العامة وفقا للكيفية التي رسمها القانون وبالضمانات التي قررها و هذا ما يسمى بالضبط الإداري .

وعلى صعيد آخر فقد تباينت الصور الإجرامية لظاهرة الجريمة المعلوماتية وتشعبت أنواعها فلم تعد تهدد العديد من المصالح التقليدية التي تحميها القوانين والتشريعات منذ عصور قديمة ، بل أصبحت تهدد العديد من المصالح والمراكز القانونية التي استحدثتها التقنية المعلوماتية بعد اقترانها بثورتي الاتصالات و المعلومات .

فالمصالح التقليدية التي تحميها كل التشريعات والنظم القانونية منذ زمن بعيد بدأت تتعرض إلى أشكال مستحدثة من الاعتداء بواسطة هذه التقنية الحديثة ، فبعد أن كان الاعتداء على الأموال يتم بواسطة السرقة التقليدية أو النصب، وكانت الثقة فى المحررات الورقية يعتدى عليها بواسطة التزوير، أصبحت هذه الأموال يعتدي عليها عن طريق اختراق الشبكات المعلوماتية وإجراء التحويلات الإلكترونية

من أقصى مشارق الأرض إلى مغاربها فى لحظات معدودة، كما أصبحت تلك الحقوق الثابتة فى الأوعية الورقية يتم الاعتداء عليها فى أوعيتها الإلكترونية المستحدثة عن طريق اختراق الشبكات والأنظمة المعلوماتية دون الحاجة إلى المساس بأي وثائق أو محررات ورقية.

وبعد أن كانت الحياة الخاصة للإنسان تواجه الاعتداء باستراق السمع أو الصورة الفوتوغرافية، أصبحت هذه الخصوصية تُنتهك بواسطة اختراق البريد الالكتروني والحواسب الشخصية ، وقواعد البيانات الخاصة بالتأمين الصحي والمستشفيات ومؤسسات الائتمان والتأمين الاجتماعي.

أما المصالح المستحدثة ، فتتمثل فى استحداث مراكز قانونية أفرزتها الحياة الرقمية الجديدة ، مثل : حقوق الملكية الفكرية على تصميم البرامج المعلوماتية، بالإضافة إلى حقوق الملكية الصناعية ، والاسم التجاري للمواقع الإلكترونية المختلفة ، والحقوق الناتجة عن تشغيلها والخدمات التي تقدمها للعملاء.

فإذا ما تأخرت القوانين والتشريعات اللازمة لمواجهة هذه الظاهرة الإجرامية ، الجديدة فسوف نواجه عشوائية كتلك العشوائية العمرانية – على سبيل المثال- التي نتجت عن تأخر قوانين التطوير العمراني. ومن هنا ظهرت إشكالية البحث .

إشكالية البحث :

تكمن إشكالية البحث فى محاولة الوصول إلى آلية مناسبة وملائمة ومُحكمة لدور سلطات الضبط الإداري داخل الدولة لأجل حماية النظام العام من مخاطر الجرائم الالكترونية وكيفية إيجاد التوازن بين حق الإدارة فى حماية النظام العام وحق الأفراد بممارسة حرياتهم على وسائل التواصل الاجتماعي ، مع وضع التدابير الاحترازية والضمانات الوقائية للحدّ من ارتكاب هذه الجرائم والتي تتسم بالمخاطرة الشديدة على حرمة الحياة الخاصة للأشخاص، بل ولتفادي وقوع مثل هذه الجرائم بالإضافة إلى الحدّ من الجهل بالثقافات القانونية وعدم إساءة استخدام الانترنت

أهداف البحث : يهدف الباحث من خلال هذا البحث إلى الكشف عن بعض الجرائم المتعلقة بشبكة الإنترنت ومعرفة سمات وخصائص مرتكبيها ، وبالتالي لفت انتباه الجهات المختصة سواء التشريعية أو القضائية أو التنفيذية إليها وكذلك توضيح دور سلطات الضبط الإداري فى مواجهة جرائم وسائل التواصل الاجتماعي ، ووضع

التصورات اللازمة لمواجهة تلك الجرائم بالإضافة إلى تسليط الضوء على أهمية التدريب للكوادر القائمة على مكافحة مثل هذه الجرائم المستحدثة .

وسوف نقوم بتقسيم هذا البحث إلى مبحثين :

المبحث الأول: سلطات الضبط الإداري على وسائل التواصل الاجتماعي .

المبحث الثاني : الضمانات التشريعية والإدارية لحماية حق الخصوصية فى مجال وسائل التواصل الاجتماعي .

المبحث الأول

سلطات الضبط الإداري على وسائل التواصل الاجتماعي

تقوم نظرية الضبط الإداري بالأساس على مهام رقابية تتولاها جهة الإدارة فى مواجهة نشاط الأفراد؛ حتى لا يكون هذا النشاط سببا فى الإخلال بالنظام العام، فالضبط وإن كان يتمثل فى تقييد نشاط الأفراد حماية للنظام العام، فإن هذا التقييد مبني بنظرنا على رقابة مستمرة تفرضها الإدارة على هذا النشاط حتى لا ينحرف عن الطريق السليم ويصبح ماسا بالنظام العام، وبالتالي لا يمكن الحديث عن التقييد بمعزل عن الرقابة، فهما أمران متلازمان لنجاح سلطات الضبط الإداري فى تأدية مهامها. وفقا للقوانين المطبقة فإن جهات الإدارة العامة المختلفة لها مهام رقابة تجاه العديد من الأنشطة التي مارسها داخل المجتمع لحماية النظام العام الأمن والصحة والسكينة وسوف نقوم بتقسيم هذا المبحث إلى ثلاثة مطالب على النحو التالي:

المطلب الأول

الرقابة الإلكترونية

الفرع الأول: ماهية الرقابة الإلكترونية

تُعدُ الرقابة الإلكترونية من أهم مصادر البحث والتحري التي غالبًا ما يستعان بها فى التقصي سواء التقليدية أو المستحدثة كجرائم وسائل التواصل الاجتماعي [١] والجهات الإدارية المختلفة تمارس مهامها الرقابية تجاه العديد من الأنشطة الإلكترونية، ومن بينها الواقع الإلكتروني، إذ إنه بطبيعته يحتاج لمثل هذه الرقابة للحفاظ على الواقع الأمني أو الأمن المعلوماتي الذي يعد العمود الفقري للواقع الإلكتروني [٢].

وقد عرَّف البعض الرقابة الإلكترونية على أنها: «مراقبة شبكة الاتصالات أو هي العمل الذي يقوم به المراقب باستخدام التقنية الإلكترونية لجميع المعطيات والمعلومات من المشتبه فيه، سواء كان شخصا أو مكانا أو شيئا حسب طبيعته مرتبطا بالزمن لتحقيق غرض أمني أو لأي غرض آخر» [٣].

---

(١) د. نبيلة هبة هروال. الجوانب الإجرائية لجرائم الإنترنت جمع الاستدلالات. دار الفكر الجامعي. الإسكندرية. ٢٠١٢. ص١٩٧.

(٢) د. عزيز ملحم بربر. الشبكات والإنترنت. جامعة نايف العربية للعلوم الأمنية. ٢٠٠٨. ص٣

(٣) د. مصطفى محمد موسى. المراقبة الإلكترونية عبر شبكة الإنترنت بين المراقبة الأمنية التقليدية والإلكترونية. دار الكتب والوثائق المصرية. القاهرة. ٢٠٠٣. ص٣.

كما عرف آخرون المراقبة الإلكترونية بأنها إجراء تحقيق يباشر خلسة، وينتهك سرية الأحاديث الخاصة، تأمر به السلطة القضائية فى الشكل المحدد قانونا بهدف الحصول على دليل غير مادي لجريمة تحقق وقوعها، ويتضمن من ناحية استراق السمع إلى الحديث، ومن ناحية أخرى حفظه بواسطة أجهزة مخصصة لذلك [١].

ويلاحظ من هذه التعريفات أن الرقابة الإلكترونية لها وظيفة وقائية عامة تمارسها الإدارة فى إطار سعيها للمحافظة على النظام العام؛ نظرا لدورها الكبير فى منع وقوع الانحرافات والمخالفات التي تضر بالمصالح المحمية قانونا وتؤثر سلبا على استقرار الأمن العام.

وبالرغم من كل المميزات التي تتمتع بها الرقابة الإلكترونية على النشاط الفردي عبر الشبكة العنكبوتية وكافة وسائل التواصل المعاصرة، لم يكن مرحبا بها على الدوام ومن قبل الجميع، إذ إن الجدل الفقهي ساد تجاه القبول بها هذا النظام من عدمه، خصوصا أن جانبا يرى عدم مشروعيته؛ لأنه يعد بمثابة سيف مسلط على الحقوق والحريات الفردية التي يمكن ممارستها من خلال الوسائل الإلكترونية، فى حين يرى آخرون لزوم وجوده كنظام مهم لمحاربة الجريمة الإلكترونية التي تتم عبر وسائل التواصل الاجتماعي والشبكات الإلكترونية الأخرى ومنع انتشارها وتزايدها [٢].

وبهذا الخصوص يرى الباحث أنه ليس من الحكمة ترك الباب مفتوحا دون مراقبة، وليس مع غلقه نهائيا بوضع مراقبة شديدة، إذ يجب أن تتم المراقبة الإلكترونية بشروط، منها أن تكون هذه الجريمة قد أخلت بالنظام العام، ويجب أخذ إذن السلطة القضائية وإشرافهم على ذلك، وفي نهاية الأمر تتوقف قدرة المشرع فى إقامة توازن بين الأمرين.

- خصائص الرقابة الإلكترونية:

أولا - رقابة إدارية:

تمارس الإدارة نوعين من الرقابة، حيث تمارس رقابتها الذاتية على أعمالها، ورقابة أخرى على نشاطات الأفراد ضمن ممارستها لسلطة الضبط الإداري، وهذه

(١) ياسر الأمير فاروق. مراقبة الأحاديث الخاصة فى الإجراءات الجنائية. دار المطبوعات الجامعية. الإسكندرية. ٢٠٠٩. ص ١٥٠.

(٢) د. زينة عبد الله محمد مصطفى. الرقابة الإلكترونية وحرية الرأي والتعبير - دراسة مقارنة بين مصر وإيران. مقال منشور عبر موقع المركز العربي لأبحاث الفضاء الإلكتروني على الرابط التالي:
http://accronline.com/article detail.aspx?id=258

الرقابة أصبحت تتأثر بالتطور الإلكتروني ومع انتقال نشاط الأفراد إلى داخل الواقع الإلكتروني.

ففي فرنسا تم إنشاء هيئة تنظيم الاتصالات الإلكترونية والبريد، بمقتضى القانون الصادر عام ٢٠٠٥ وطبقا للمادة (٤٣٣-١) من قانون الاتصالات الإلكترونية والبريد والمعدل بقانون (ء٣٣/ ٢٠٠١)، وتتولى الهيئة الإشراف والرقابة على المحتوى الرقمي، مع مراعاة عدة اعتبارات، كمقتضيات الحفاظ على النظام العام. كذلك فى ٢٠٠٣هيئة مسؤولة عن تنظيم الاتصالات، وفقا للمادة (٦٧) من هذا القانون والتي تنص: « للسلطات المختصة فى الدولة أن تخضع لإداراتها جميع خدمات وشبكات الصالات أي مشغل أو مقدم خدمة، وأن تستدعي العاملين لديها القائمين على تشغيل وصيانة تلك الخدمات والشبكات، وذلك فى حدوث كارثة طبيعية أو بيئية أو فى الحالات التي تعلن فيها التعبئة العامة طبقا لأحكام القانون (٨٧) لسنة ١٩٦٠ المشار إليه، أو أية حالات أخرى تتعلق بالأمن القومي».

ويرى الباحث أنه يتبين لنا من خلال هذا النص أن جهاز تنظيم الاتصالات يملك سلطة الرقابة على محتوى وسائل التواصل الاجتماعي وعلى الشبكة العنكبوتية بشكل عام، وهذه الرقابة محدودة والغرض منها الحفاظ على الأمن القومي للبلاد، وكذلك النظام العام.

وكذلك - بالإضافة إلى ما سبق - أقام المشرع المصري نوعا من الضبط الإداري الخاص على الشبكات الإلكترونية؛ وذلك من أجل الوقاية من مخاطر هذه الشبكات، ويطلق عليها (إدارة مكافحة جرائم الحاسبات وشبكات المعلومات) أو ما تعرف ب (مباحث الإنترنت)، وقد أنشئت بمقتضى قرار وزير الداخلية). وهي تابعة للإدارة العامة للمعلومات والتوثيق التابعة لوزارة الداخلية، وتضم عدة أقسام [1]: قسم العمليات ويختص بمكافحة الجرائم التي تقع بواسطة الحاسب الآلي فى مجال نظم المعلومات، وقسم التأمين وهو المسؤول عن وضع الخطط والأساليب اللازمة لتأمين الشبكات، وقسم البحوث والمساعدات الفنية ويختص بإعداد البحوث الفنية والقانونية فى مجال تأمين نظم المعلومات.

(١) انظر قرار وزير الداخلية. رقم (١٣٥٠٧) لسنة ٢٠٠٢. وكذلك د. رامي محمود الجالي. التنظيم القانوني لحرية الصحافة الإلكترونية. دار الجامعة الجديدة. الإسكندرية. ٢٠١٩. ص ٢٧١.

ثانيا - رقابة قضائية:

يمكن أن تتم الرقابة القضائية على وسائل التواصل الاجتماعي أو على الشبكات الإلكترونية بشكل عام من خلال مقدمي خدمات الإنترنت، يأتي هذا فى حدود ضيقة؛ وذلك لتحقيق المصلحة العامة وعدم الإخلال بالنظام العام.

وفي فرنسا تنص المادة (٦) من القانون (٥٧٥) لسنة ٢٠٠٤ المتعلقة بالثقة فى الاقتصاد الرقمي، وتم تعديله بالقانون (ء١١٨/ ٢٠١٣) الصادر عام ٢٠١٣، على أن: «مقدمي خدمات النقل والتخزين للمعلومات على الخط (يقصد متعهد الإيواء) غير خاضعين لالتزام عام بالرقابة على المعلومات المنقولة والمخزونة، ولا التزام بالبحث عن الأفعال والأنشطة غير المشروعة، إلا أن هذا لا يمنع من إجراء رقابة هادفة ومؤقتة بناء على طلب من السلطة القضائية؛ وذلك لتحقيق المصلحة العامة أو حال ارتكاب عنصري أو انتهاك الكرامة الإنسانية أو نشر صور جنسية جرائم ضد الإنسانية أو وجود تمييز للأطفال»[١].

ثالثا - رقابة أمنية:

إن الرقابة التي تمارسها جهات الضبط الإداري الأمني أو الإدارات الأمنية على سلوك ونشاط الأفراد داخل الواقع الإلكتروني، هي رقابة إدارية بالنظر إلى صفة القائمين عليها والجهة التي تتولاها، كما أن هذه الرقابة ليست تقليدية، وإنما رقابة جديدة مرتبطة بالتطور الإلكتروني، وهذه الرقابة هدفها المحافظة على الأمن العام من كل ما يهدده داخل الواقع الإلكتروني، لذلك توصف هذه الرقابة بأنها إدارية، إلكترونية، أمنية.[٢]

رابعا - رقابة وقائية :

تعد الرقابة وقائية فى حال كانت تهدف لمنع وقوع الضرر أو الخطأ؛ أي الحيلولة دون تحقيق هذا الخطأ أو الضرر، لذلك تسمى هذه الرقابة بالرقابة المسبقة ويرى الباحث أن الرقابة الوقائية التي تتم ممارستها على نشاط الأفراد الإلكتروني تعد رقابة وقائية وليست علاجية، أي سابقة وليست لاحقة ؛ لأن الهدف من هذه الرقابة هو من الإخلال بالنظام العام ومنع كل ما يهدده .

(١) ( )رامي محمود الجالي. التنظيم القانوني لحرية الصحافة الإلكترونية. المرجع السابق. ص ٢٧١.

(٢) ( )مصطفى جمال حنفي زينو. دور الضبط الإداري فى مجال الجرائم الإلكترونية المخلة بالأمن العام. رسالة ماجستير . كلية الحقوق . جامعة الأزهر . غزة . ٢٠١٧. ص ١٦٤.

الفرع الثاني
آليات الرقابة الإلكترونية

فى إطار مكافحة جرائم وسائل التواصل الاجتماعي والجرائم الإلكترونية التي تخل بالنظام العام، لابد السلطات الضبط من اتباع عدة إجراءات عند المراقبة الإلكترونية لكشف الجرائم وجمع التحريات، والاستعانة بالأجهزة الفنية المتطورة والأساليب العلمية الحديثة بات أمراً ضرورياً فى المراقبة الإلكترونية، بشرط موافقة السلطة القضائية، ومن هذه الإجراءات التي تستعمل:

أولاً - اعتراض المراسلات الإلكترونية :

يمكن لسلطات الضبط مراقبة المراسلات الإلكترونية وفحصها، التي تتم عن طريق وسائل التواصل الاجتماعي أو عن طريق البريد الإلكتروني، وهي جميع الرسائل والطرود والبرقيات.

ثانيًا - مراقبة المكالمات وتسجيل الأصوات :

يمكن مراقبة الأحاديث وتسجيلها وكل الاتصالات التي تشمل كل أدوات الاتصال السلكية أو اللاسلكية.

ثالثًا - فحص بصمة الصوت :

وهو فحص فيزيائي لمتخصص فى الأصوات، ويقوم على فحص النطق والتخاطب من متخصص فى النطق والتخاطب مع استخدام جهاز قياس ذبذبات الصوت.[١]

رابعًا - استخدام التقنيات عن طريق الحاسب الآلي :

من الوسائل والتقنيات الحديثة التي يعتمد عليها سلطات الضبط الإداري هو الاعتماد على جهاز يركب فى المركبة يرسل ويستقبل الإشارات، ومن خلال تلك الإشارات يمكن التعرف على مكان وجود المركبة، ويتم استقبال هذه الإشارات عن طريق الحاسب الآلي وبطريقة إلكترونية، وتتم متابعة المركبة، وكذلك عن طريق الحاسب الآلي يمكن رسم صور المتهم أو المشتبه به بواسطة الحاسب الآلي وفقا لبرامج إلكترونية معدة لهذا الغرض، وكذلك استخدام نظام الخرائط الإلكتروني عن طريق

(١) حسن علي شاهين. التحريات الأمنية فى مجال الضبط الإداري فى مصر وفرنسا. دار النهضة العربية.٢٠١٥. ص ٢٩٥.

الحاسب الآلي، ويعد هذا النظام أحد التقنيات العلمية الحديثة التي أثبتت نجاحها فى التصدي للجرائم الحديثة، وكذلك استعمال برنامج (1000. S. C .D) الذي يقوم بفحص وتعقب رسائل البريد الإلكتروني المرسلة و الواردة عبر أي حساب، وقد طور هذا البرنامج من قبل مكتب التحقيق الفيدرالي (F.B.I. حيث تتم المراقبة عبر هذا البرنامج بعد استئذان المحكمة. (١)

خامسا- فحص مكونات الحاسب الآلي: الكمبيوتر مكون من قطع صلبة وقطع مرنة ويمكن السلطات الضبط الإداري فحص القرص الصلب، فحص البرمجيات، فحص النظام المعلوماتي، وفحص نظام ذاكرة التخزين. سادسا- فحص نظام الاتصال بالإنترنت:

يتم فحص النظام الأمني للشبكات، فحص بروتوكول الإنترنت، وفحص الخادم أو الملقم، ويعمل الخادم علي ربط أعضاء الشبكة العنكبوتية بغرف التداول (٢).

ومما تقدم ذكره يتضح لنا أن سلطات الضبط الإداري تستعمل تقنيات حديثة عند إجراءات المراقبة الإلكترونية، وهذ الإجراءات هي بالغة الخطورة؛ لأنها تمس حرمة الحياة الخاصة، إذ يجب على من يقوم بهذا الإجراءات أن يكون لديه الخبرة الكافية، ويجب حفظ السر المهني من أجل المحافظة على حقوق الآخرين وحرياتهم، وقبل البدء بأي إجراء يجب الحصول على موافقة السلطة القضائية.

- حالات اللجوء إلى المراقبة الإلكترونية: (٣)

يمكن اللجوء إلى المراقبة الإلكترونية إذا توافرت إحدى الحالات الآتية: ١- الوقاية من الأفعال الموصوفة بجرائم التخريب وجرائم الإرهاب والجرائم التي تخل بأمن الدولة ونظامها العام والآداب العامة. - فى حالة توفر معلومات عن احتمال اعتداء على منظومة حاسوبية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني. ٣- لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية. ٤ - فى إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة كما هو منصوص عليه فى بعض القوانين الدولية.

(١) راشد محمد الشحي. الرقابة القضائية على قرارات الضبط الإداري فى الحكومة الإلكترونية. أطروحة دكتوراه. كلية الحقوق. جامعة القاهرة. ٢٠٠١ - ١٢٧ - ١٢٩ ص ٢٠٠١

(٢) راشد محمد الشحي. الرقابة القضائية على قرارات الضبط الإداري فى الحكومة الإلكترونية. المرجع السابق . صـ٢١٦

(٣) محمد علي سويلم. مكافحة الجرائم الإلكترونية - دراسة مقارنة بالدراسات العربية والأجنبية. دار المطبوعات الجامعية . الاسكندرية . ط١ . ٢٠١٩ . ص ٧٤٥.

ومن الإجراءات الرقابية الأخرى تستعمل السلطات السوار الإلكتروني، ولكن هذا الإجراء يستخدم بعد حدوث الجريمة؛ أي ليس وقائيا .

- السوار الإلكتروني :

أسهمت التقنيات الحديثة بتطوير كافة مناحي الحياة، فلا شك أن الجريمة قد تطورت بشكل كبير بفضل التقنيات الحديثة، وكذلك تطورت الأساليب الضبطية لكشف الجريمة بفضل هذه التقنيات.

وبسبب تلك التقنيات بدأت الأنظمة العقابية المعاصرة تجد بدائل للعقوبات السالبة للحرية قصيرة المدة، ومنها الوضع تحت المراقبة الإلكترونية، وهو البديل المستحدث فى السياسة العقابية، ويعد أحد أهم وأبرز تطبيقات التطور العلمي العقابي الذي أظهر ضرورة إيجاد بدائل لهذي العقوبات بغير الأساليب العقابية التقليدية .

يقوم الوضع تحت المراقبة الإلكترونية على تنفيذ العقوبة بطريقة مبتكرة خارج أسوار السجن فى الوسط الحر بصورة ما يسمى (السجن فى البيت)، يتضمن هذا الأسلوب نظاما إلكترونيا للمراقبة عن بعد، بموجبه يمكن التأكد عن وجود أو غياب الشخص عن المكان المخصص لإقامته بموجب حكم قضائي، حيث يسمح للمحكوم عليه بالبقاء فى منزله لتكون تحركاته محدودة ومراقبة بمساعدة جهاز مثبت فى معصمه أو أسفل قدمه (السوار الإلكتروني).

ويسمى أيضا نظام المراقبة الإلكترونية أو الحبس فى البيت، ويمكن تعريفه بأنه إلزام المحكوم عليه أو المحبوس مؤقتا بالإقامة فى منزله أو محل إقامته خلال ساعات محددة بحيث تتم متابعة الشخص الخاضع للمراقبة إلكترونيا[١].

أدخل الوضع تحت المراقبة الإلكترونية تاريخيا إلى التشريعات العقابية أول مرة فى الولايات المتحدة الأمريكية، وتم تطبيقه عام ١٩٨٧ فى ولاية فلوريدا أو المكسيك الجديدة، وكذلك فى عام ١٩٨٧ طبقت كندا هذا النظام، أما إنجلترا فتبنت الوضع عام ١٩٨٩، والسويد عام ١٩٩٤، وهولندا عام ١٩٩٥، وبلجيكا واستراليا عام ١٩٩٧، وقد أدخل المشرع الفرنسي الوضع تحت المراقبة الإلكترونية إلى النظام العقابي من خلال

(١) د. عمر سالم، المراقبة الالكترونية طريقة حديثة لتنفيذ العقوبة السالبة للحرية خارج السجن، دار النهضة العربية، القاهرة، ص .

القانون رقم (٩٧-١١٥٩) فى عام ١٩٩٧[١].

أما الدول العربية فكانت الجزائر أول من طبق هذا النظام بموجب القانون (١٥-١٧) فى عام ٢٠١٥[٢].

وكذلك فى المغرب فتح العمل بنظام السوار الإلكتروني، حيث جاء منصوصا عليه فى مسودة قانون المسطرة الجنائية ، حيث جاءت الفصول (١ - ٧٩ و ٢ - ٧٩ و ٣ - ٧٩) منظمة للهيكلية العامة لهذه التقنية، وتم تطبيق هذه المراقبة عام ٢٠١٨[٣].

وفي الإمارات تم تطبيق هذا النظام والعمل به بعد استحداث المشرع مرسوما بقانون اتحادي رقم (١٧) لسنة ٢٠١٨، وتم تنفيذ هذا النظام بعد (٦) أشهر من إصدار هذا المرسوم).[٤]

وكذلك استعملت دائرة صحة أبي ظبي السوار الإلكتروني للمصابين بفيروس كورونا فى العزل المنزلي، ونوهت الدائرة إلى أن السوار الإلكتروني مخصص للمصابين الذين تنطبق عليهم معايير برنامج العزل المنزلي ولا يوجد تطبيق مرتبط بالسوار الالكتروني ولا يمكن فتحه من قبل المريض ويتم فتحه عن طريق الفريق المختص بعد التعافي من المرض).[٥]

خصائص السوار الإلكتروني : مقاوم للماء ، الحرارة ، الرطوبة ، الغبار، الاهتزازات ، الذبذبات ، والصدمات. - مقاوم للتمزق والقطع والفتح. - مقاوم للأشعة فوق البنفسجية، ويتحمل قوة الضغط. - قابل للشحن بواسطة شاحن خاص به. - ضد الحساسية، ويحتوي على عازل مصنوع من القماش يفصله عن بشرة المتهم.

---

(١) د. صفاء أوتاني. الوضع تحت المراقبة الإلكترونية (السوار الإلكتروني فى السياسة العقابية الفرنسية. مجلة جامعة دمشق للعلوم الاقتصادية والقانونية. المجلد ٤٥. العدد ١. ٢٠٠٩. ص ١٢٩.

(٢) د عبد الهادي درار. نظام المراقبة الإلكترونية فى ظل تطورات النظم الإجرائية الجزائية بموجب الأمر (١٥-٢٠). مجلة الدراسات والبحوث القانونية. العدد . ص ١٤٤.

(٣) د. عبد الإله المتوكل . المجلة الإلكترونية للأبحاث القانونية . العدد ٢. ٢٠١٨. ص ٤٨.

(٤) مركز الخليج للدراسات . نشر المقال بتاريخ ٢٠١٩/٥/٤ تم الاطلاع بتاريخ ٢٠٢٠/٣/٢١ انظر الرابط الالكتروني http://www.alkhaleej.ae/alkhaleej/pageleac98b9b-176d-44fd-881d-4c1d295cd24a.

(٥) انظر صحيفة البيان الإماراتية - نشر الخبر بتاريخ ٢٠٢٠/٦/٢ انظر هذا الرابط
https : / / www . albayan .ae / across - the - uae / news - and -report

المطلب الثاني
الحظر الإلكتروني

يمثل إجراء الحظر أو المنع أحد التدابير التي تلجأ إليها سلطات الضبط الإداري منذ القدم لمنع الأفراد من القيام ببعض الأنشطة المحظورة التي تهدد النظام العام، وقد استمرت هذ التدابير تجاه الأنشطة الجديدة للأفراد، وبدأت سلطات الضبط الإداري فى مختلف دول العالم باستعمال وسيلة الحظر على الأنشطة الإلكترونية وكل ما يتعلق فى الشبكة العنكبوتية على مستوى نشر الأفكار والمعلومات والبيانات وتأسيس الحسابات الشخصية والمواقع والصفحات والبرامج المختلفة التي تخل بالنظام العام، وقد تكلمنا عن موضوع الحظر الإلكتروني بشكل موجز فيما سبق فى الفصل الأول، وسنبينه بشكل مفصل .

يمكن أن يعرف الحظر الإلكتروني بأنه: إجراء تهدف من خلاله السلطة الرسمية إلى حظر نشاط أو محتوى أو أفكار يتم نشرها على شبكة الإنترنت من خلال وسائل التواصل الاجتماعي، ويعد الغرض من اتخاذ هذا الإجراء هو حماية النظام العام).[١]

وفي المقابل فإن تدابير الحظر الإلكتروني ظلت محل جدل أيضا فى ظل التطور التقني فى المجال الإلكتروني وعلاقته بالنظام العام .

ونستدل على ذلك بقرار الإدارة الأمريكية الأخير القاضي بالحظر الإلكتروني داخل الطائرات أثناء الرحلات ، بيد أن هذا الحظر لا يعد من إجراءات الضبط الموجهة نحو نشاط الأفراد داخل الواقع الإلكتروني ، وإنما يمكن اعتباره إجراء ضبطيا تمارسه إدارة الطيران الأمريكية فى مواجهة الركاب عند صعودهم للطائرات، وذلك من خلال منعهم من حمل الأجهزة الإلكترونية داخل الطائرات أثناء تحليقها فى الجو؛ تحقيقا للسلامة الأمنية ومنع الحوادث الإرهابية.[٢]

---

(١) سامي حسن نجم الحمداني، حسين طلال مال الله العزاوي. دور الضبط الإدارية الإلكتروني فى مكافحة الشائعات المخلة بالأمن العام. كلية الحقوق والعلوم السياسية . جامعة كركوك .٢٠١٩، ص ٢٨.

(٢) ( ) مصطفى جمال حنفي. دور الضبط الاداري فى مجال الجرائم الإلكترونية المخلة بالأمن العام. مرجع سابق . ص ١٨٧.

اولاً: تطبيقات الحظر الإلكتروني:

هناك فرق بين الحظر والحجب، فالحظر يعني المنع، والحجب يعني الفصل أو القطع التام، وهو أشمل من الحظر، وبعض الدراسات تشير إلى أن الحظر لا يختلف عن الحجب ، فحظر المواقع الإلكترونية يعني حجبها، غير أنه قد يأتي الحجب الإلكتروني فى مواضع أخرى بمعنى قطع خدمة الإنترنت أو قطع الاتصال لضرورات أمنية، وليس بمعنى حظر النشاط الإلكتروني.

فى بعض الأحيان تضطر الدولة إلى أن توجه سلطات الضبط الإداري بحجب خدمة الإنترنت لمنع تفاقم الخطر والتأثير السلبي على النظام العام.

ويمكن تعريف الحجب الإلكتروني بأنه: «عبارة عن قطع خدمة الإنترنت لمنع الاتصال بالشبكة من قبل الأفراد، وللحيلولة دون التواصل فيما بينهم عبر الإنترنت» [١]

ويعرف أيضا بأنه: إجراء تقوم به الأجهزة المختصة بمساعدة مقدمي الخدمات الوسيطة عادة، تمنع من خلاله المستخدمين فى نطاق جغرافي معين من الوصول إلى موقع أو أكثر من وسائل التواصل الاجتماعي، بصفة دائمة أو مؤقتة، من أجل حماية النظام العام بمختلف عناصره [٢].

ويرى الباحث أن على الدول أن لا تفرض تدابير الحظر والحجب لوسائل التواصل الاجتماعي والشبكات بشكل عام، إلا إذا كانت فعلا ملمة بالنظام العام وتهدد أمن الدولة، فحينئذ يتم الحظر بالقدر الضروري، حيث إن احترام حقوق الإنسان وحمايتها خارج شبكة الإنترنت يمتد إلى داخل الإنترنت أيضا، لا سيما أن الحق فى حرية التعبير مكفول فى جميع المواثيق والتشريعات الدولية.

ثانيا - احترام الحقوق والحريات وعدم جواز الحظر المطلق فى إجراءات الحظر:

إن حظر وسائل التواصل الاجتماعي بالرغم من كونه مبررا فى حالات معينة، إلا أن عدم تقييد ممارسته قد يحوله إلى إجراء مكبل للحريات المرتبطة بتلك الوسائل.

---

(١) مصطفى جمال حنفي، المرجع السابق ،ص ١٨٩.

(2) Conseil de l'Europe, l'Étude comparative sur le blocage, le filtrageet le retrait de contenusil-legauxsur internet, Lausanne, 2017, pp. 03-04.

وإذا وجدت سلطات الضبط الإداري أن هناك مخالفات للنظام العام، فيمكن أن يكون الحظر بصفة مؤقتة، ولا يمكن أن نجد تبريرا لحظر موقع معين بشكل مطلق ودائم.

وهنا ينبغي أن تميز بين القرارات الصادرة التي تفرض حظرا مؤقتا وتلك التي تفرض حظرا دائما، أي هناك فرق بين الحظر والحجب، فالأولى تكون مؤقتة وتزول بعد مدة، فإذا ما وجد ما يدعو أن يكون التنظيم الضبطي مؤقتا يمكن أن يكون تنظيما متشددا؛ لأنه دعت إليه ظروف خاصة قد تبه، ولأن الغرض قد يزول بعد فترة قصيرة، أما إذا كان التنظيم الضبطي بشكل دائم ومستقر يجب أن يكون أقل شدة لأنه تهديد دائم للحقوق والحريات.

وتطبيقا لذلك، فإن القضاء يراعي الاعتبارات الزمنية التي تحيط بسلطات الضبط الإداري من ناحيتين: تقدير مدى خطورة الظروف الزمنية وما يحدث بسببها من أخطار على الأمن أو النظام العام، وتقدير المدى الزمني المناسب لإجراءات الضبط الإداري).[1]

وفي قرار محكمة القضاء الإداري لمجلس الدولة المصري يظهر بوضوح مبدأ عدم جواز تطبيق الحظر المطلق للحرية في إجراءات حجب وسائل التواصل الاجتماعي، الذي اعتبر أن استعمال وسائل التواصل الاجتماعي هو الأصل، والتعبير بات من الحقوق الأصيلة للأفراد[2]

وفي حكم آخر قضت المحكمة الإدارية العليا أنه: «ولئن كانت التشريعات المصرية - بما فيها قانون تنظيم الاتصالات - لم تحدد الحالات التي تستدعي حجب المواقع الإلكترونية، إلا أن ذلك لا يخل بحق الأجهزة الحكومية والجهاز القومي لتنظيم الاتصالات في حجب بعض المواقع على الشبكة الدولية للإنترنت حينما يكون هناك مساس بالأمن القومي أو المصالح العليا للدولة، وذلك بما لتلك الأجهزة من سلطة في مجال الضبط الإداري لحماية النظام العام بمفهومه المثلث: الأمن العام والصحة العامة والسكينة العامة للمواطنين ، وذلك تحت رقابة القضاء. ويتعين التفرقة في هذا الصدد بين التعدي على الحق الفردي للأشخاص والتعدي على المجتمع وأمنه وأمانه،

(١) عبد الرؤف هاشم بسيوني. نظرية الضبط الإداري في النظم الوضعية المعاصرة والشريعة الإسلامية. دار الفكر الجامعي. الإسكندرية. ط١، ٢٠٠٧، ص ١٨٨.

(٢) مجلس الدولة المصري. محكمة القضاء الإداري. قضية رقم ٥٧٩٣٣ لسنة ٦٨ ق. بتاريخ ٢٠١٥/٨/٢٥

وإن كان كلاهما تلفظه الشرائع ونصوص الدستور والقانون، بيد أن المساس بالحق الشخصي كفل دفعه ولوج سبيل التقاضي جنائيا أو مدنا أو كليهما معا، حسبما ألمحت إليه المادة (٧٩) من قانون تنظيم الاتصالات، أما حال المساس بأمن المجتمع وأمانه فلا يدرؤه إلا أن يوصد منبع هذا الخطر مؤقتا كان على شبكة الإنترنت أو غيره»[١].

ثالثا- احترام مبدأ التناسب فى إجراءات حظر وسائل التواصل الاجتماعي:

يجب أن تكون الإجراءات متناسبة مع مدى حجم الاضطراب الذي تهدف الإدارة إلى تفاديه، ويقدر التناسب بقدر جسامة التهديدات التي تخشى منه على النظام العام، فمن غير المعقول أن تكون شدة الإجراءات الضابطة أكثر من الشدة التي يراد اتقاؤها بهذا الإجراء. ولذلك يجب على سلطات الضبط أن تستعمل التدابير الملائمة لمواجهة الإخلال بالنظام العام دون أن تنال من الحقوق والحريات بالتعطيل أو التضييق.

تأسيسا لذلك، يفرض القضاء الإداري على سلطات الضبط أن تختار الوسائل والإجراءات المناسبة أو الملائمة التي تكفي لمواجهة الإخلال بالنظام العام. فيتم التدخل لمراقبة ملاءمة القرارات للظروف التي صدر فيها، ومدى لزومها لصيانة النظام العام فى الظروف التي لابست إصدارها . وبالتالي لا يجوز لسلطات الضبط الإداري أن تلجأ إلى وسائل قاسية لمواجهة ظروف غير خطيرة)[٢].

وتطبيقا لمبدأ التناسب فى تدبير حجب وسائل التواصل الاجتماعي، فإنه يتعين على الهيئات المختصة أن يكون قرارها بحجب الموقع متوافقا مع طبيعة الإخلال وكذلك لا يجوز استغلال حجب وسائل التواصل الاجتماعي فى إطار مهمة الضبط الإداري ، لتحقيق أغراض فى مجالات أخرى.

ويرى الباحث أن تمتع الدولة بسلطة تقييد الحرية فقط عندما يكون ذلك ضروريا وبالقدر المتطلب الحماية حقوق الآخرين والمصالح العامة هو الأقرب للصواب؛ لأنه الأقرب للواقع، ويمكن لسلطات الضبط الإداري العمل به حاليا فى

(١) الطعن رقم ١٠١٧١ س ٥٤ ق. جلسة ٢٦ فبراير ٢٠١٢. مجموعة أحكام الإدارية العليا س ٥٦. ص ٨٧٧

(٢) عبد الرؤف هاشم بسيوني. نظرية الضبط الإداري فى النظم الوضعية المعاصرة والشريعة الإسلامية. دار الفكر الجامعي . مرجع سابق . ص ١٩٦.

إجراءات الحظر الإلكتروني لوسائل التواصل الاجتماعي؛ لأنه من الصعب تقييد الحرية أو فسح المجال بشكل مطلق.[١].

رابعا - موقف التشريع المصري والكويتي بما يخص الحظر الإلكتروني:

١-التشريع المصري: نصت المادة (٧) من القانون (١٧٥) لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات على أن: لجهة التحقيق المختصة متى قامت أدلة على قيام موقع يبث داخل الدولة أو خارجها، بوضع أي عبارات أو أرقام أو صور أو أفلام أو أي مواد دعائية أو ما فى حكمها، بما يعد جريمة من الجرائم المنصوص عليها فى هذا القانون، ويشكل تهديدا للأمن القومي أو يعرض أمن البلاد أو اقتصادها القومي للخطر، أن تأمر بحجب الموقع أو المواقع محل البث ، كلما أمكن تحقيق ذلك فنيا. وعلى جهة التحقيق عرض أمر الحجب على المحكمة المختصة، منعقده فى غرفة المشورة خلال أربع وعشرين ساعة مشفوعا بمذكرة برأيها. وأصدرت المحكمة قرارها فى الأمر مسببا إما بالقبول وإما بالرفض، فى مدة لا تجاوز اثنتين وسبعين ساعة من وقت عرضه عليها. ويجوز فى حالة الاستعجال لوجود خطر حال، أو ضرر وشيك الوقوع، أن تقوم جهات التحري والضبط المختصة بإبلاغ الجهاز؛ ليقوم بإخطار مقدم الخدمة على الفور بالحجب المؤقت للموقع أو المحتوى أو المواقع أو الروابط المذكورة فى الفقرة الأولى من هذه المادة وفقا لأحكامها. ويلتزم مقدم الخدمة بتنفيذ مضمون الإخطار فور وروده إليه. وعلى جهة التحري والضبط التي قامت بالإبلاغ بعد تحرير محضرا تثبت فيه ما تم من إجراءات وفق أحكام الفقرة السابقة يعرض على جهات التحقيق خلال ثماني وأربعين ساعة من تاريخ الإبلاغ الذي وجهته للجهاز، وتتبع فى هذا المحضر ذات الإجراءات المبينة بالفقرة الثانية من هذي المادة، وتصدر المحكمة المختصة قرارها فى هذه الحالة إما بتأييد ما تم من إجراءات حجب، أو بوقفها. فإذا لم يعرض المحضر المشار إليه فى الفقرة السابقة فى الموعد المحدد، يعد الحجب الذي ته كأن لم يكن. ولمحكمة الموضوع أثناء نظر الدعوى، أو بناء على طلب جهة التحقيق أو الجهاز أو ذوي الشأن أن تأمر بإنهاء القرار الصادر بالحجب ، أو تعديل نطاقه . وفي جميع الأحوال، يسقط القرار الصادر بالحجب بصدور أمر بألا وجه لإقامة الدعوى الجنائية، أو بصدور حكم نهائي فيها بالبراءة» .

(١) د. وليد محمد الشناوي. التطورات الحديثة للرقابة القضائية على التناسب فى القانون الإداري – دراسة تأصيلية تحليلية مقارنة. دار الفكر والقانون. المنصورة. ٢٠١٧. ص ٢١٠.

٢-التشريع الكويتي: إن القانون الكويتي الجديد رقم ٦٣ لسنة ٢٠١٥ فى شأن مكافحة جرائم تقنية المعلومات يتضمن قيوداً واسعة المدى على الحظر الإلكتروني فقد نصت المادة الثالثة[١] على أن «يعاقب بالحبس مدة لا تجاوز ثلاث سنوات وبغرامة لا تقل عن ثلاثة آلاف دينار ولا تجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين كل من:

١-ارتكب دخولا غير مشروع الى موقع أو نظام معلوماتي مباشرة أو عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات بقصد الحصول على بيانات أو معلومات حكومية سرية بحكم القانون.

فإذا ترتب على ذلك الدخول إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو نشرها أو تعديلها، تكون العقوبة الحبس مدة لا تجاوز عشر سنوات والغرامة التي لا تقل عن خمسة آلاف دينار ولا تجاوز عشرين ألف دينار أو بإحدى هاتين العقوبتين.

ويسرى هذا الحكم على البيانات والمعلومات المتعلقة بحسابات عملاء المنشآت المصرفية.

٢- زور أو أتلف مستندا أو سجلا أو توقيعا إلكترونيا أو نظام معالجة إلكترونية للبيانات أو نظاما إلكترونيا مؤتمتا أو موقعا أو نظام حاسب آلي أو نظاما إلكترونيا بطريق الاصطناع أو التغيير أو التحوير أو بأي طريقة أخرى، وذلك باستخدام وسيلة من وسائل تقنية المعلومات.

فإذا وقع التزوير على مستند رسمي أو بنكي أو بيانات حكومية أو بنكية إلكترونية تكون العقوبة الحبس مدة لا تجاوز سبع سنوات وبغرامة لا تقل عن خمسة آلاف دينار ولا تجاوز ثلاثين ألف دينار أو بإحدى هاتين العقوبتين ويعاقب بذات العقوبة بحسب الأحوال، كل من استعمل أيا مما ذكر مع علمه بتزويره أو فقده لقوته القانونية.

٣-غيّر أو أتلف عمدا مستندا إلكترونيا يتعلق بالفحوصات الطبية أو التشخيص الطبي أو العلاج الطبي أو الرعاية الطبية أو سهل للغير فعل ذلك أو مكنه منه، وذلك باستعمال الشبكة المعلوماتية أو باستخدام وسيلة من وسائل تقنية المعلومات.

(١) راجع فى ذلك قانون رقم ٦٣ لسنة ٢٠١٥ فى شأن مكافحة جرائم تقنية المعلومات نشر هذا القانون فى عدد الجريدة الرسمية رقم ١٢٤٤ تاريخ ١٢ يوليو (تموز) ٢٠١٥م. ص. ٤ أ.

٤-استعمل الشبكة المعلوماتية أو استخدام وسيلة من وسائل تقنية المعلومات فى تهديد أو ابتزاز شخص طبيعي أو اعتباري لحمله على القيام بفعل أو الامتناع عنه فإذا كان التهديد بارتكاب جناية أو بما يعد مساسا بكرامة الأشخاص أو خادشا للشرف والاعتبار أو السمعة كانت العقوبة الحبس مدة لا تجاوز خمس سنوات والغرامة التي لا تقل عن خمسة آلاف دينار ولا تجاوز عشرين ألف دينار أو بإحدى هاتين العقوبتين.

٥-توصل عن طريق الشبكة المعلوماتية أو باستخدام وسيلة من وسائل تقنية المعلومات الى الاستيلاء لنفسه أو لغيره على مال أو منفعة أو مستند أو توقيع على مستند، وذلك باستعمال طريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة متى كان ذلك من شأنه خداع المجني عليه.

المطلب الثالث

الصعوبات التي تواجه سلطات الضبط الإداري فى مجال وسائل التواصل الاجتماعي

هناك عدة معوقات تواجه سلطات الضبط الإداري أثناء ممارسة اختصاصهم فى الكشف والاستدلال عن الجرائم الإلكترونية، سنذكر البعض منها:

أولا : تكمن صعوبة كشف الجريمة الواقعة فى بيئة الإنترنت فى الطبيعة الخاصة لمثل تلك الجرائم و ما تتسم به من خصائص تميزها عن غيرها من الجرائم التقليدية ، وترجع تلك الصعوبة فى كشف جرائم الإنترنت إلى عاملين اثنين وهما : يتمثل العامل الأول فى خفاء تلك الجرائم ، أما العامل الثاني فيتمثل فى إحجام المجني عليهم عن الإبلاغ عن تلك الجرائم وبخاصة فى قطاع المال والأعمال.

أ : سهولة إخفاء الجريمة :جرائم الإنترنت فى أغلب الأحوال تكون خفيه مستترة ، وقد لا يشعر المجني عليهم بها ولا يلحظون وقوعها ، حيث إنه تتوافر لدى مرتكبي هذه الفئة من الجرائم خبرات ومعارف ومهارات فائقة بكيفية إخفاء وحجب الأفعال المكونة للجريمة [١]

(١) ونتيجة لصعوبة كشف جرائم الإنترنت . فقد بات اخفاء جرائم الإنترنت مصطلحا يستخدم فى دراسات علم الإجرام الأمريكية هو ، الطبيعة غير الأولية لمخرجات الحاسوب المطبوعة " Second - hand Nature of Computer Printouts . انظر : دكتور هشام محمد فريد رستم . الجوانب الإجرائية للجرائم المعلوماتية . أصول التحقيق الجنائي الفني والية التدريب التخصصي للمحققين بحث منشور بمجلة الأمن والقانون. تصدر عن كلية شرطة دبي . السنة السابعة العدد الثاني . ربيع الأول ١٤٢٠ د يوليو ١٩٦٩ م .ص ١٧

ب : الإحجام عن الإبلاغ فى جرائم الإنترنت :

يعد إحجام الجهات والمؤسسات بل والأشخاص التي تتضرر من الجرائم المتعلقة بشبكة الإنترنت عن إبلاغ الجهات الأمنية المختصة بنبأ وقوع إحدى هذه الجرائم هو أحد صعوبات ومعوقات التحقيق[١] .

ثانيا : نقص خبرة سلطات الضبط القضائي وجهات التحقيق :

يعد كذلك من الصعوبات المتعلقة بتحقيق جرائم الإنترنت هو عدم توافر الكفاءة اللازمة ، والخبرة الكافية ، والقدرات المؤهلة لمباشرة التحقيق فى هذا النوع من الجرائم لدى الأشخاص القائمين على أمر التصدي لها ومكافحتها سواء سلطات الضبط القضائي أو جهات التحقيق أو قضاء الحكم .

حيث يقتضي كشف جرائم الإنترنت والاهتداء إلى مرتكبيها وملاحقتهم قضائيا ، إضافة إلى أساسيات وأصول التحقيق الجنائي الفني المطبقة فى تحقيق الجرائم التقليدية ، استراتيجيات تحقيق وتدريب مهارات خاصة تسمح بتفهم أسس ومتطلبات مواجهة تقنيات الحوسبة الإلكترونية المتطورة وأساليب التلاعب المحاسبي المعقدة التي تستخدم فى ارتكاب هذه الجرائم عادة[٢].

ويمثل نقص الخبرات والمهارات الفنية[٣] اللازمة للتحقيق فى مثل هذا النوع من الجرائم صعوبة كبيرة بالنسبة لجهات التحقيق والمحاكمة .

ونظرا لنقص الخبرة لدى الأجهزة الأمنية والقضائية فقد لجأت هذه الجهات إلى استيعاب المتخصصين فى مجال الحاسوب والإنترنت ضمن كوادرها ، كما يجري تدريب رجال الشرطة والقانون على استخدامات الحاسوب ، ولكن رغم تلك الجهود فلن تكون تلك الأجهزة قادرة على مواكبة التطور السريع فى مجال الحاسوب وذلك لأسباب عدة منها :- [٤]

---

(١) د : هشام محمد فريد رستم . الجرائم المعلوماتية . مرجع سابق . ص٨٩ .

(٢) د . هشام رستم . المرجع السابق . ص٩٠ .

(٣) حيث يستخدم العاملون فى مجال الحاسوب والإنترنت مصطلحات علمية خاصة أصبحت تشكل الطابع المميز لمحادثتهم وأساليب التفاهم معهم . وليس هذا فحسب بل اختصر العاملون فى هذا المجال تلك المصطلحات والعبارات بالحروف اللاتينية الأولى لتكون لديهم لغة غريبة تعرف بلغة المختصرات (Acronyms) وهي لغة متطورة و متجددة كل هذا دفع معتادي الإجرام المعلوماتي أن يطلقوا على أنفسهم صفة النخبة وفي ذات الوقت يطلقون على رجالي إنفاذ القانون صفة الضعفاء أو القاصرين (Lamers) انظر : د. محمد الأمين البشري . التحقيق فى جرائم الحاسب الألي بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت . كلية الشريعة والقانون . جامعة الإمارات العربية المتحدة . خلال الفترة ١-٣ مايو ٢٠٠٠ . ط ٣ ، ٢٠٠٤ م . ص ١٠٧ .

(٤) د محمد الأمين البشري . التحقيق فى جرائم الحاسب الألي بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت . كلية الشريعة والقانون . جامعة الإمارات العربية المتحدة . خلال الفترة ١-٣ مايو ٢٠٠٠ . ط ٣ ، ٢٠٠٤ م . ص ٢٦٦.

١-أن الميزانيات المالية المرصودة لتدريب الكادر البشري لدى أجهزة الأمن والقضاء تكون ضعيفة وكذلك لا تفي هذه الميزانيات لاستقطاب النخبة المميزة فى مجال الحاسوب والتي تستقطبهم عادة شركات ومؤسسات القطاع الخاص .

٢-حداثة تجربة الأجهزة الأمنية والقضائية مع جرائم الحاسوب و الإنترنت و قلة عدد الجرائم المستكشفة منها لضعف الخبرة الفنية والإجرائية لدى الأجهزة الأمنية والقضائية فى الضبط والتحقيق فى تلك الأنماط الإجرامية المستجدة ، إلا أنه مع انتشار الحاسوب وتوغله فى الحياة العامة والخاصة ولدى الحكومة والقطاع الخاص ، وما يستتبعه من أفعال مخالفة ، وليست مجرمة نظرا لعدم وضوح الرؤية فى شأن نصوص التجريم فان ذلك سوف يثري عمل سلطات الضبط والتحقيق مستقبلا (١).

ولذا فإنه يتوجب على الأجهزة الأمنية والقضائية أن تعمل على توفير الإمكانيات التقنية اللازمة للتحقيق فى جرائم الحاسوب والإنترنت وعليها أيضا العمل على استقطاب الكفاءات المهنية المتخصصة فى هذا المجال ، للاستعانة بها فى التحقيق فى جرائم الإنترنت ، وحتى تكتمل قدرات الأجهزة الأمنية فى هذا المجال فإنه يتم الاستعانة بالنخبة المتخصصة فى مجال الحاسوب والإنترنت وفي تكنولوجيا المعلومات وكل ما يتعلق بها ، فى جميع مراحل الدعوى الجنائية ، منذ كشف الجريمة المتعلقة بالحاسوب أو بالإنترنت والتحقيق مع المتهمين فيها وأيضا فى تقديم الأدلة الجنائية مما يؤدي إلى تحقيق العدالة .

* ولأجل ذلك فلابد من إيجاد أسلوب خاص لسير التحقيق فى مثل هذه الجرائم ، أسلوب يحتوي على الخبرة الفنية والكفاءة المهنية .

ومن كل ما سبق يتضح مدى ما يشكله نقص خبرة رجال الشرطة والادعاء والقضاء من عوائق وصعوبات تقف عائقا وحاجزا أمام تحقيق العدالة وردع الجناة فى الجرائم المتعلقة بالحاسوب والإنترنت ، وهذا يثير مدى أهمية التدريب الفني التخصصي

(١) فهذه الجرائم عند ارتكابها سيما عن طريق شبكة الإنترنت . تتسم بالعشوائية والسهولة . الأمر الذي أفسح المجال لبعض من لديهم الخبرة التقنية وإن كانت متواضعة ليدل بدلوه فى المساس بأمن المعلومات بالرغم من تعدد الدوافع الأمر الذي أدى إلى زيادة حجم الخسائر على أثر العبث بالمواقع الالكترونية على شبكة المعلومات حيث قدرت الخسائر فى تزوير بطاقات الائتمان عام ١٩٩٩ م . على سبيل المثال بمبلغ (٢٨٠) مليون دولار فى الولايات المتحدة الأمريكية على حين بلغت خسائر العالم من سرقة المعلومات فى ذات العالم مبلغ (١٠٠) مليون دولار . الأمر الذي يسبب ارتباك فى الحركة التجارية على الإنترنت ويمس أمن التعاملات المصرفية على الشبكة وبالتالي سيعمل على الحد من انتشار التجارة الالكترونية . انظر/ د : سامح أحمد بلتاجي . الجوانب الاجرائية للحماية الجنائية لشبكة الانترنت . رسالة دكتوراة . كلية الحقوق . جامعة الاسكندرية . ٢٠١٠ . صـ ٢٢٤ .

لجهات الشرطة والتحقيق والقضاء على استخدامات وتطبيقات الحاسوب والإنترنت وسبل مواجهة الجرائم الواقعة فى نطاق هذه التقنيات التكنولوجية المتطورة

ويكفي للتدليل على أهمية هذا التدريب واكتساب الخبرة فى مجال جرائم تقنية المعلومات أن رجل الضبط وكذلك المحقق لن يمكنهما القيام بعملهما فى الاستدلال أو التحقيق إلا عن طريق الإلمام بتقنية الحاسب الآلي .

وتجدر الإشارة هنا بأنه - تأكيدا لما سبق - فقد واكب المشرع المصري هذه التطورات وخوَّل لسلطة التحقيق حجب المواقع الالكترونية محل بث أية جرائم الكترونية ، فنصَّ فى مادته السابعة من القانون رقم ١٧٥ لسنة ٢٠١٨ على الآتي : « لجهة التحقيق المختصة متى قامت أدلة على قيام موقع يُبث من داخل الدولة أو خارجها ، بوضع أي عبارات أو أرقـام أو صـور أو أفلام أو أي مواد دعـائية أو ما فى حكمها ، بما يُعد جريمة من الجرائم المنصوص عليها فى هذا القانون ، ويشكل تهديدًا للأمن القومي أو يعرِّض أمن البلاد أو اقتصادها القومي للخطر ، أن تأمر بحجب الموقع أو المواقع محل البث ، كلما أمكن تحقيق ذلك فنيًا » .

ثالثا : صعوبات إقامة الدليل فى جرائم الإنترنت :

يعد من أهم الصعوبات التي تواجه المحقق الجنائي فى جرائم الإنترنت تلك الصعوبة المتعلقة بكيفية الحصول على الدليل الرقمي ، وأيضا صعوبة الحفاظ على هذا الدليل والذي يتميز بطبيعته الخاصة والخصائص التي تميزه عن غيره من الأدلة التقليدية فى الجرائم الأخرى. فالدليل فى جرائم الحاسوب والإنترنت هو عبارة عن معلومات قد تحاط بوسائل فنية لحمايتها وتلك الوسائل قد تكون عائقا أمام عمليات البحث و التنقيب والتحري[1] من قبل الجهة المختصة بذلك ، وفي هذا النطاق ليس من الضروري أن يكون الدليل عبارة عن أوراق أو غير ذلك من الأشياء الملموسة .

وأيضا من الصعوبات التي تواجه أجهزة التحقيق أثناء القيام بالتحقيق فى جرائم الحاسوب والإنترنت والمتعلقة بالدليل الرقمي المطلوب التوصل إليه وإقامته تلك الصعوبة الخاصة بكمية المعلومات والبيانات الضخمة التي يجب فحصها ودراستها وتحليلها ، لكي يستخلص منها دليل إثبات نسبة الجريمة إلى المتهمين فيها .

(١) عميد / محمد عبد اللطيف فرج ، مشكلات ملاحقة وتحقيق الجرائم المعلوماتية ، مجلة مركز البحوث بأكاديمية الشرطة ، القاهرة ، العدد العاشر ، سنة ٢٠٠٠ م ، ص ١٤٤ .

ولمواجهة صعوبة ضخامة كم البيانات والمعلومات المتعين على جهة التحقيق فحصها وتحليلها لاستخلاص الأدلة على ارتكاب جريمة الإنترنت منها ، فإن مواجهة تلك الصعوبة بما يعمل على تقليص حدتها وتيسير مواجهتها عن طريق وسيلتين ، هما :[١]

الوسيلة الأولى : الاستعانة بالخبرة الفنية لتحديد ما يجب دون سواه البحث عنه للاطلاع عليه أو ضبطه

الوسيلة الثانية : الاستعانة بما تتيحه نظم المعالجة الآلية للبيانات من أساليب للتدقيق والفحص المنظم أو المنهجي ونظم ووسائل الاختيار والمراجعة ، بالإضافة إلى أساليب الفحص بوجه خاص على الحالة أو الواقعة .

ويرى الباحث أنه نظراً لعدم وجود إطار قانوني إجرائي ينظم إجراءات الضبط والتحقيق فى جرائم تقنية المعلومات ، ويزداد الأمر صعوبة بسبب القصور التشريعي وندرة التطبيقات القضائية ، حيث إن الجريمة المعلوماتية كغيرها من الجرائم تقوم على ذات الأركان والعناصر وتمر الدعوى الجنائية فيها بنفس المراحل الخاصة بسائر الجرائم ، كما أن ارتكابها يقتضى التفكير فى الجريمة والتحضير لها (الشروع) ،ثم تنفذيها ومحاولة التخلص من آثارها ، ولذلك تثور هنا مسألة استخلاص الدليل الذي تثبت به الجريمة المعلوماتية ، وإذا كان الاعتراف وشهادة الشهود والقرائن والآثار الناجمة عن النشاط الإجرامي لها دور فى إثبات هذا النوع من الجرائم المعلوماتية وكشف الحقائق فيها ، وهي أمور تعين المحقق على استجواب المتهمين وسؤال الشهود ، إلا أن ذلك يبدو قصوراً فى ملاحقة مرتكبي الجريمة المعلوماتية.

رابعًا - النقص التشريعي:

يؤثر النقص التشريعي على عمل سلطات الضبط الإداري، وعندما لا تجد السلطات قانونا يتعلق بالجرائم الإلكترونية من أجل الاستناد عليه، فهذا يؤثر ويقف عائقا أمام واجباتهم تجاه جرائم وسائل التواصل الاجتماعي أو الجرائم الإلكترونية بشكل عام، فعدم وجود قانون ينظم تلك الجرائم يؤثر على الاستدلال سواء المعاينة، التفتيش، الحظر الإلكتروني، أو المراقبة الإلكترونية.

(١) د، هشام محمد فريد رستم . الجوانب الإجرائية للجرائم المعلوماتية . مرجع سابق .ص٢٤ .

وعندما لا يجد القاضي أو رجل الإدارة نصا تشريعا يحكم واقعة معينة، فإن الحل يكون بالرجوع إلى مصادر القانون الأخرى، والقصور التشريعي قد يؤدي إلى التداخل بين القوانين الأخرى من ناحية الاختصاص.

ومن أجل كل هذا وغيره، وفي سبيل وضع معالجات لكل المشاكل المتعلقة بالجرائم الإلكترونية، اتجه المشرع فى العديد من الدول إلى استحداث قسم جديد للجرائم الإلكترونية على غرار الأقسام التقليدية كقسم جرائم الأموال، وإضافة نصوص جديدة إليه لتمثل الجرائم الإلكترونية كافة أو تجميع ما يتعلق بالجريمة المعلوماتية فى تشريع مستقل يوضح الطبيعة الخاصة للجريمة المعلوماتية، وقد أخذت الولايات المتحدة وبريطانيا بهذا الاتجاه.

ويرى الباحث أنه يمكن لأي دولة معرض نظامها العام للتهديد من الجرائم الإلكترونية ومن أجل السرعة وإدراك الخطر الذي يهدد نظامها العام، أن تستحدث قسما للجرائم الإلكترونية ومن ثم إضافة نصوص جديدة؛ لأن استحداث القسم أسرع من إضافة النصوص القانونية ، فتعديل النصوص التقليدية أو إضافة نصوص جديدة بعد النصوص التقليدية لا يعالج التهديدات الكبيرة التقنية المتطورة، فينبغي إصدار قوانين خاصة تتعلق بتلك الجرائم.

المبحث الثاني

الضمانات التشريعية والإدارية لحماية حق الخصوصية فى مجال وسائل التواصل الاجتماعي

يحظى الحق فى الخصوصية بالحماية فى جميع الشرائع، ويعد موضوع الحق فى الخصوصية من أهم الموضوعات فى الوقت الحاضر؛ وذلك لارتباطه بكرامة الإنسان التي تعد شيئا جوهريا له علاقة بحياته الخاصة التي منحها له الله - سبحانه وتعالى - ثم تبنت هذا الحق الأحكام الوضعية، كالمواثيق الدولية والقوانين الوطنية. فالخصوصية تتعلق بشكل مباشر بحرمة الحياة الخاصة للإنسان، كتوجهاته السياسية ومعتقداته الدينية وتعاملاته البنكية وجنسيته.

وقد أثر التقدم التقني المتسارع فى العقود الأخيرة على حياة الإنسان وحرياته الخاصة، مما أدى إلى تغيير الحياة الاجتماعية، جراء التطفل على الحياة الخاصة للأفراد وانتهاكها.

ولحماية الخصوصية الإلكترونية فإن الأمر يتطلب حماية تقنية وحماية قانونية، وكذلك حماية إدارة وتنظيمية، وهذه الحماية تكون من خلال استراتيجية أمن المعلومات الوطنية لدى كل مؤسسة، وقد سارت مشكلة الحماية الشخصية ولا سيما فى مجال الحياة الخاصة، لمواجهة الأخطار الإلكترونية فى مختلف القوانين؛ لأن الدول لم تسلك مسلكا موحدا لحماية الحق فى الخصوصية لمواجهة أخطار الجرائم الإلكترونية.

وإن انتشار وسائل التواصل الاجتماعي أدى إلى حدوث تغيرات اجتماعية خطيرة بات من اللازم وضع ضمانات لحماية هذي الحياة الخاصة بعد أن أصبحت محاصرة بالتطور الهائل الذي تشهده استخدامات وسائل التواصل الاجتماعي، وهذا التطور أصبح يهدد النظام العام، ويجب أن تكون هناك موازنة بين حق الفرد فى الخصوصية وحق سلطات الضبط الإداري فى اتخاذ الإجراءات واتخاذ العقاب، أي على سلطات الضبط أن لا تتجاوز الحدود التي قدها القانون. .

وسيقسم الباحث هذا المبحث إلى مطلبين،

المطلب الأول: ماهية حماية حق الخصوصية فى وسائل التواصل الاجتماعي.

المطلب الثاني: حماية حق الخصوصية فى وسائل التواصل الاجتماعي فى النظم المقارنة.

المطلب الأول

ماهية حماية حق الخصوصية فى وسائل التواصل الاجتماعي

يعد الحق فى الحياة الخاصة منذ القدم حقا مشروعا يمنع التعدي عليه وحظي بالحماية الدينية والقانونية فى كل الدول والتشريعات، ومع التطور الإلكتروني فى مجال الاتصال والإعلام عبر الشبكة العنكبوتية واتساع التواصل الاجتماعي اللامحدود واللامشروط؛ أصبح الحق فى الخصوصية معرضا للانتهاك، وبات من السهل الاطلاع على أسرار الأفراد والهيئات والمؤسسات والتلاعب بها، الأمر الذي دفع إلى ضرورة إيجاد آليات قانونية تحمي هذا الحق وتضبطه فى إطار دولي وداخلي وطني يحقق سعة الشعور بالأمان والطمأنينة فى مجتمع أضحى فيه استعمال الوسائل الإلكترونية أمرا ضروريا لا غني عنه.

وقد عرفت مسألة حماية الحق فى الخصوصية الإلكترونية تطورا ملحوظا فى التشريعات المقارنة، وسنوضح ذلك فى هذا المبحث، وسنوضح أيضا أنواع الخصوصية التي تنتهك فى الشبكات الإلكترونية، وكذلك سنتناول تعريف الحق فى الخصوصية بشكلها التقليدي والحق فى الخصوصية بوسائل التواصل الاجتماعي.

أولا: تعريف الحق فى الخصوصية:

ينعقد شبه إجماع بين الفقه والتشريع على عدم إيجاد تعريف جامع مانع للحق فى الخصوصية ، وهذا يترجم من خلال تعد التعريفات لهذا المفهوم ، ولعل هذه الصعوبة فى توحيد المفهوم ترجع إلى طبيعة الحق التي تكتسب صفة المرونة.

عرف المشرع المصري البيانات الشخصية الحساسة فى قانون حماية البيانات الشخصية رقم (١٥١) لسنة ٢٠٢٠، فى المادة رقم (١) من هذا القانون بأنها: «البيانات التي تفصح عن الصحة النفسية أو العقلية أو البدنية أو الجينية، أو بيانات القياسات الحيوية البيومترية» أو البيانات المالية أو المعتقدات الدينية أو الآراء السياسية أو الحالة الأمنية، وفي جميع الأحوال تع بيانات الأطفال من البيانات الشخصية الحساسة».

وكذلك عرف المشرع المصري البيانات الشخصية فى قانون حماية البيانات الشخصية رقم (١٥١) لسنة ٢٠٢٠، وورد تعريف البيانات الشخصية فى المادة (١) من

هذا القانون بأنها: أي بيانات متعلقة بشخص طبيعي محدد، أو يمكن تحديده بشكل مباشر أو غير مباشر عن طريق الربط بين هذه البيانات وأي بيانات أخرى كالاسم، أو الصوت، أو الصورة، أو رقم تعريفي، أو محدد للهوية عبر الإنترنت، أو أي بيانات حدد الهوية النفسية، أو الصحية، أو الاقتصادية، أو الثقافية، أو الاجتماعية[١].

أما المشرع الكويتي بالرغم من أن المشرّع فى معظم الدول ومنها الكويت يعترف بالحق فى الحياة الخاصة إلا أنه لم يضع له تعريفاً، ومن ثم يصبح الأمر متروكاً لاجتهاد القضاء والفقه.

إن الفكرة الأساسية لحياة الإنسان الخاصة: «أن يكون لكل إنسان الحق فى أن يترك وشأنه» والتي يعبر عنها بالحق فى الخصوصية. ولا يفهم من ذلك بأن الحق فى الخصوصية هو ذاته الحق فى الحرية، فنطاق الأخير أوسع من الأول ؛ لأن الحق فى الخصوصية لا يثار إلا بصدد جانب من الحق فى الحرية يتصف بممارسته بمنأى عن الآخرين أما الجوانب الأخرى من الحق فى الحرية والتي يحتك فيها الشخص بالآخرين، مثل حرية التعبير عن الرأي، وحرية الاجتماع، فينفكُ فيها الرابط بين الحقين، ومن ثم يكون منع الغير من التعدي على الشخص فى مثل هذه الصور تطبيقاً لحقه فى الحرية وليس حقه فى الخصوصية. ومن جهة أخرى هناك مجال للحق فى الخصوصية لا علاقة له بالحق فى الحرية، فالسجين له الحق فى الخصوصية على الرغم من تقييد حريته.»[٢].

ثانيا - الحق فى الخصوصية عند الفقه:

عرف بعض الفقه الحق فى الخصوصية بأنها: «المحافظة على السرية ومنع التدخل فيما يعتبر حميمة الشخص وأسراره عبر حماية بعض البيانات الشخصية، بشكل يمنع انتشار المعلومات التي تكشف الحياة الخاصة أو تعرضها للانكشاف، وعليه هنالك اعتداء على الخصوصية سواء تعلق الأمر بكشف سر دفين وإيصاله إلى الآخرين، أم بمراقبة ورصد تحركات لم يقترنا بكشف أسرار أو بنشر معلومات حساسة، فالضرر واقع فى الحالتين: إذ ينتج عن كشف المعلومات فى الحالة الأولى، وعن كون الشخص وضع تحت المراقبة فى الحالة الثانية»[٣]

(١) الجريدة الرسمية، العدد ٢٨ (هـ) فى ١٥ يوليه سنة ٢٠٢٠.

(٢) محمود عبدالرحمن محمد: نطاق الحق فى الحياة الخاصة، دار النهضة العربية، القاهرة، ١٩٩٤ ص١٢٢.

(٣) منى الأشقر جبور، محمد جبور، البيانات الشخصية والقوانين العربية الهم الأمني وحقوق الأفراد، المركز العربي للبحوث القانونية والقضائية، بيروت، ط١، ٢٠١٨، ص ٢٢.

والذي يميل إليه الباحث فى هذا الصدد أن حق الخصوصية هو: «حق الإنسان فى أن تحترم الحياة الخاصة به، وأن تحفظ أسراره التي يجب ألا يطلع عليها الآخرون بغير إذنه، يتمثل فى حماية حرمة المسكن وحرمة الاتصالات والمراسلات الخاصة بالإنسان»[١].

ثالثا- حق الخصوصية فى وسائل التواصل الاجتماعي:

اتجه غالبية الفقه إلى ربط ولادة مفهوم الحق فى الخصوصية الإلكترونية بمخاطر هذه الشبكات الإلكترونية على النظام العام، ويمكن أن تعرف الخصوصية فى وسائل التواصل الاجتماعي بأنها: «حق الفرد المستخدم فى أن يقر بنفسه متى وكيف وإلى أي مدى ممكن أن تصل المعلومات الخاصة به إلى الآخرين من المستخدمين أو القائمين عليها»، وبذلك يتضح أن لكل فرد الحق من الحماية من التدخل فى شؤونه، وله الحق أيضا فى الاختيار الحر للآلية التي يعبر بها عن نفسه ورغباته وتصرفاته للآخرين على وسائل التواصل الاجتماعي[٢].

ويمكن أن تعرف أيضا بأنها: «وصف حماية البيانات الشخصية للفرد، والتي يتم نشرها وتداولها من خلال وسائط رقمية، وتتمثل البيانات الشخصية فى البريد الإلكتروني والحسابات البنكية، والصور الشخصية، ومعلومات عن العمل والمسكن، وكل البيانات التي فى تفاعلنا على الإنترنت أثناء استخدامنا للحاسب الآلي أو التليفون المحمول أو أي من وسائل الاتصال الرقمي بالشبكة العنكبوتية»[٣].

ويرى الباحث أنه من الصعب إيجاد تعريف شامل كامل فى مجال الحق فى الخصوصية عموما، إذ من الصعب إيجاد اختلاف بين المصالح العامة لسلطات الضبط وبين الحق فى الخصوصية، وفي اعتقادنا أن سبب هذي الصعوبة يرجع إلى التقدم التقني فى هذا العصر وتأثيره على اختراق حقوق الأفراد فى الخصوصية وفي الحرية الفردية، فالحواجز المانعة من انتهاك الخصوصية باتت ضئيلة جدا، بل إن مفهوم الحق فى الخصوصية فى تصورنا صار له اليوم مفهوم مختلف جدا فى ظل وجود أنظمة الفيس بوك والتويتر ونحوها؛ إذ الجميع صار يتباهى بإشراك الآخرين

(١) طارق عفيفي صادق أحمد، الجرائم الإلكترونية - جرائم الهاتف المحمول، المركز القومي للإصدارات القانونية، القاهرة، ط١، ٢٠١٥، ص ١٥٠.

(٢) محمود عبد الرحمن محمد، نطاق الحق فى الحياة الخاصة - دراسة مقارنة بالقانون الوضعي (الأمريكي - الفرنسي المصري) والشريعة الإسلامية، دار النهضة العربية، ٢٠١٠، ص ٧٧.

(٣) انتهاك الخصوصية الرقمية فى الصحافة المهنية والحياة الشخصية، مركز هردو لدعم التعبير الرقمي، القاهرة، ٢٠١٧، ص ٥.

بأدق تفاصيل حياته اليومية مما كانت إلى وقت قريب من أشد الخصوصيات ، وعلى هذا النحو فالخصوصية فى وسائل التواصل الاجتماعي وفي أبسط معانيها ترتبط بسرية الحياة الخاصة لمستخدمي تلك الوسائل، سواء كانت وقائع أو معلومات فى الحاسب الآلي الشخصي أو الهاتف الذكي، أو تم تخزينها فى إحدى وسائل التواصل الاجتماعي التي يشترك فيها المستخدم والتي قد يتم اختراقها مثل الفيس بوك) أو البريد الإلكتروني، حيث إن سرقتها أو الاعتداء عليها بعد انتهاكا للخصوصية ، كذلك اعتراض الرسائل البريدية المرسلة بغرض الاطلاع عليها أو معرفة محتوياتها، ومن ثم إنشاء الأسرار التي قد تحتويها تلك الرسائل، ومن قبيل ذلك الأسرار السياسية والاجتماعية والصحية وغيرها من الانتهاك والاختراق، وكل هذا يضر ويؤثر على النظام العام.

كما أن حماية الخصوصية فى وسائل التواصل الاجتماعي تنحصر فى حق الشخص أن يتحكم بالمعلومات التي تخصه، وهو يعد من أهم المفاهيم التي تستدعيها كافة النظم والقوانين الهادفة إلى حماية الخصوصية الإلكترونية، وعليه يمكن القول : إن حماية الخصوصية الإلكترونية هي حماية البيانات الخاصة بالأفراد الذين يستخدمون تلك الوسائل عبر الشبكة العنكبوتية).[1]

ثانياً: صور حق الخصوصية فى وسائل التواصل الاجتماعي :

إن صور الانتهاك الإلكتروني لخصوصية الأفراد كثيرة ومتنوعة، مما يستدعي معه تنوع الحماية تبعا لتنوع صور الحق فى الحياة الخاصة، ومن أهم أنواع حماية الخصوصية التي تتعلق بالنظام العام - على سبيل المثال لا الحصر - ما يلي:

١- حماية خصوصية المراسلات والمحادثات:

تتمثل حماية المراسلات والمحادثات فى حق الأفراد فى سرية وخصوصية المراسلات الهاتفية والبريدية ووسائل التواصل الاجتماعي، فالمراسلات والمحادثات وحمايتها مكفولة بموجب النظم والقوانين، فلا يجوز مراقبتها أو إفشاء سريتها.

(١) تومي فضيلة . أيديولوجيا الشبكات الاجتماعية وخصوصية المستخدم بين الانتهاك والاختراق. مجلة العلوم الإنسانية والاجتماعية، العدد ٣٠، ٢٠١٧، ص ٤٤.

وتعد المراسلات مجالا مهما لإيداع أسرار الأفراد سواء تعلقت بالمرسل أو المرسل إليه أو بالغير من خلال حماية الرسائل المكتوبة والمحادثات باختلاف أنواعها، واليوم أصبحنا نتحدث عن رسائل ومحادثات إلكترونية أصبح الولوج إليها أمرا سهلا.

وحرصا من موقع فيس بوك على سرية وخصوصية الاتصالات فقد وافق على إضافة وصلة فى خانة رسائل البريد الإلكتروني غير المرغوب فيها، تتيح للمستخدمين رفض استقبال هذه الرسائل، وعلى أنه لن يضيف صورا مأخوذة من بيانات المستخدمين إلى هذه الرسائل.[١]

وعلى الرغم من أهمية حماية الخصوصية على وسائل التواصل الاجتماعي فإن هناك بعض الوسائل التي لا تعير لهذا الموضوع أدنى اهتمام، حيث يقول خبراء الخصوصية: إن بعض وسائل التواصل الاجتماعي تجعل من الصعب على المتعاملين معها حماية خصوصياتهم عن طريق ضبط برمجياتها على أن تكون الخصوصية مفتوحة، حيث تنص سياسة الخصوصية فى العديد من المواقع والتطبيقات على بعض الشروط التي تم انتهاكا لخصوصية المستخدم، والتي قد لا يلتفت إليها عند إنشائه حسابا على الموقع أو تحميله لتطبيقات بعض تلك المواقع، وقد استجابت بعض الشركات المنتجة التطبيقات لمطالبات المستخدمين التي أثيرت حول مستويات الخصوصية التي توفرها، وعملت على تحسين شروط خصوصيتها، وكان من بين هذه التحسينات عدم نشر ومشاركة بيانات المستخدم مع آخرين إلا بموافقته، ويتيح موقع فيس بوك ومواقع التواصل الاجتماعي الأخرى للمستخدمين تعديل ضبط البرمجيات، ومع ذلك فإن الضبط المعتاد يدفع المستخدمين دائما إلى المزيد من الانفتاح[٢].

ويرى الباحث أن كثيرا من الفقهاء يركزون على الخصوصية المتعلقة بمراسلات ومحادثات الأفراد فقط، فكذلك تعد خصوصية المراسلات والمحادثات البريدية أو الهاتفية للدولة لها أهمية كبيرة، فإذا تم إفشاء تلك المراسلات - ولربما تكون سرية - أو انتهاك خصوصيتها فإن ذلك يشكل خطرا على الأمن القومي للدولة ونظامها العام.

(١) محمد بن عيد القحطاني. حماية الخصوصية الشخصية لمستخدمي مواقع التواصل الاجتماعي. رسالة ماجستير. كلية العدالة الجنائية. جامعة نايف العربية للعلوم الأمنية. ٢٠١٠. ص ١٠٩.

(٢) علاء حسين الحمامي. سعد عبد العزيز العاني. تكنولوجيا أمنية المعلومات وأنظمة الحماية. دار وائل للنشر والتوزيع. عمان. ط١. ٢٠٠٧. ص ٣٧.

٢ - حماية الخصوصية المكانية:

تتعلق الخصوصية المكانية بحرمة المسكن، وتعد حرمة المسكن من العناصر الأساسية للحق فى حرمة الحياة الخاصة فى التشريعات المختلفة، وقد كفلته أغلب الدساتير.

ويجب وضع القواعد المنظمة للتفتيش والرقابة الإلكترونية، والتأكد من بطاقات الهوية سواء كان الفرد فى محل العمل أو فى الأماكن العامة. ونظرا لأهمية حماية الخصوصية المكانية ، فقد طلبت هيئة حماية البيانات فى ألمانيا - عام ٢٠١٠ - من موقع فيس بوك تعديل التطبيق الخاص بتحديد عناوين الأصدقاء Friend Finder، ووافق الموقع على إبلاغ المستخدمين بأنه إذا قاموا بتحميل عناوينهم على التطبيق الخاص بتحديد عناوين الأصدقاء ، فإن الموقع سوف يحتفظ بالمعلومات الخاصة بتلك العناوين، وقد يستخدمها فى دعوة أصحابها إلى الانضمام إلى فيسبوك[١].

٣ - حماية خصوصية الحياة المهنية وأسرارها:

بمعنى حماية الأسرار المهنية وعدم الإخلال بواجب كتمان وحفظ الأسرار المهنية ،ويعد الإخلال بواجب كتمان وحفظ الأسرار المهنية جريمة تعترض مرتكبها للعقاب؛ لأنها تخل بالنظام العام للدولة، كما اتجهت التشريعات المقارنة لذلك[٢].

ويراد بإفشاء الأسرار المهنية الكشف عن واقعة لها صفة السرية صادرة ممن علم بها بمقتضى مهنته مع توافر القصد.

٤ - حماية خصوصية الصورة:

يعد موضوع الحق فى حماية خصوصية الصورة من الموضوعات الحديثة والمهمة فى الوقت الحالي؛ بسبب ما أسفرت عنه المتغيرات التقنية الحالية، فقد أظهرت أهميتها مع انتشار الوسائل والتقنيات التي غيرت من المفهوم التقليدي للصورة الذي كان سائدا قبل دخول العصر الإلكتروني).[٣]

---

(١) محمد بن عيد القحطاني، مرجع سابق ،ص ١٠٥.

(٢) مبدر الويس ،أثر التطور التكنولوجي على الحريات العامة، منشأة المعارف بالاسكندرية، ص ١٠٢.

(٣) بوزيدي سليم، الاعتداء على الحق فى الصورة فى ظل التطورات التكنولوجية الحديثة، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة، بجاية، ٢٠١٩، ص ٧.

والحق فى حرمة الصورة هو انعكاس لشخصية الإنسان، فهي تعكس أحاسيسه ورغباته، ويتحقق هذا الحق من خلال سلطة الشخص فى منع غيره من أن يرسمه أو يصوره إذا لم يكن هو نفسه راغبا فى ذلك، إضافة إلى إمكانية الاعتراض عن نشر صورة من طرف وسائل الإعلام باختلاف وسائطها، وتجدر الإشارة إلى أن الفقه فى عدد من الدول يرى أن انتهاكات الحق فى الصورة تتحقق حتى وإن كان من قام بالتقاطها حسن النية وليس سيئ النية.

وعلى سبيل المثال ، فقد جرم المشرع الجنائي العراقي نشر صورة الشخص بإحدى طرق العلانية إذا كان من شأن نشرها الإساءة إلى صاحب الصورة ؛ إذ نصت الفقرة الأولى من المادة رقم (٤٣٨) من قانون العقوبات العراقي على أنه : يعاقب بالحبس مدة لا تزيد على سنة وبغرامة لا تزيد عن مائة دينار أو بإحدى هاتين العقوبتين: ١من نشر بإحدى طرق العلانية أخبارا أو صورا أو تعليقات تتصل بأسرار الحياة الخاصة أو العائلية للأفراد ولو كانت صحيحة إذا كان من شأن نشرها الإساءة إليهم .

ونصت المادة (٢٦) من قانون حماية حق المؤلف الأردني على أنه: « لا يجوز نشر صورة الشخص دون إذنه »، وقد ذهب القضاء الفرنسي إلى عدم جواز أخذ الصورة أو نشرها بدون إذن صاحبها [١].

٥ - حماية الخصوصية الصحية:

تدخل الحالة الصحية ضمن الخصوصيات التي يجب أن لا تنتهك، وتعد الحالة الصحية للفرد والأدوية والعلاجات التي يخضع لها عنصرا مهما من عناصر الحق فى الحياة الخاصة، فهي من أمور شخصية التي لا يرغب بإفشائها للغير، وهنا يبرز دور الطبيب فى إطار عدم إفشائه السر المهني فى وسائل التواصل الاجتماعي أو غيرها.

ويرى الباحث أنه من الممكن أن نضيف عناصر وأنواعا أخرى مكونة للخصوصية على اعتبار التغيرات الزمنية والتطور التقني الحالي الذي أسهم بخلق عناصر جديدة.

ويرى الباحث أن أنواع حماية الخصوصية فى وسائل التواصل الاجتماعي التي ذكرت تؤثر وتخل بالنظام العام فى المجتمع إذا انتهكت، فعلى سلطات الضبط الإداري فى الدولة أن تأخذ على عاتقها حماية خصوصية الأفراد وعدم انتهاكها من قبل

(١) مصطفى أحمد عبد الجواد الحجازي، الحياة الخاصة ومسؤولية الصحفي، دار الفكر العربي، القاهرة، ٢٠٠٠، ص ٨٧.

الآخرين، وعلى سلطات الضبط أن تكيف نفسها وتواكب التطورات التقنية من أجل الحد من الخطورة القائمة على انتهاك الخصوصية.

ثالثا: أثر التطور التقني على حق الخصوصية فى وسائل التواصل الاجتماعي :

أدى التطور التقني الحاصل وانتشار الحواسيب والنمو العالمي فى الاتصالات الرقمية إلى توسيع نطاق الخصوصية، وإلى ظهور الآثار الإيجابية والآثار السلبية التي أثرت على الخصوصية، وسنتكلم عن الآثار الإيجابية والآثار السلبية على النحو التالي :

١- الآثار الإيجابية للتطور التقني على الخصوصية:

إن التطور التقني للشبكة العنكبوتية بشكل عام ولوسائل التواصل الاجتماعي بشكل خاص أثر بالشكل الإيجابي على الخصوصية الرقمية للأفراد ، حيث سهل حياتهم اليومية ، وساعدهم على مواكبة عصر السرعة، إذ أصبح الفرد يقوم بعد من الأعمال فى وقت وجيز وجه قليل، كما ارتبط هذا التطور بخصوصية الأفراد بتحركاتهم ومتابعة أخبارهم وتوجهاتهم وتعاملاتهم المالية ، الشيء الذي مكن من تقريب الشعوب واختصار المسافات فيما بينهم.

كما أن استعمال المجال الإلكتروني أو الرقمي فى جمع البيانات الشخصية المتصلة بحياة الأفراد ومعالجتها، وسع استعمال هذه الوسائل فى معالجة البيانات وتخزينها وجمعها لأغراض متعددة خاصة فيما يتعلق بجمع وتخزين المعلومات إلى مدة غير محدودة سواء من طرف الدول أو من طرف الأفراد.

وكذلك ترتب على تطور وسائل الاتصال الحديثة، ومنها الهاتف المحمول ووسائل التواصل الاجتماعي، وكذلك الاتصال عبر الأقمار الصناعية، ما يعرف اليوم بالانسياب الدولي للمعلومات، وهي وسائل الاتصال الحديثة والتي أصبحت تؤدي خدمات كبيرة للأفراد، ولا غنى للمجتمعات عنها، وتبرز آثارها الإيجابية على الحق فى حرمة الحياة الخاصة[١].

(١) عبد الفتاح بيومي حجازي، الحكومة الإلكترونية بين الواقع والطموح، دار الفكر الجامعي، الإسكندرية ٢٠٠٨، ص ٨٣.

وكذلك من الآثار الإيجابية ظهور ما يعرف ببنوك المعلومات التي تنظم عمل الدول والأفراد والتي تحتوي على المعلومات الشخصية والبيانات لمستخدمي الشبكات الإلكترونية أو العنكبوتية[١].

وبفضل الكفاءة العالية فى وسائل تقنية المعلومات الحديثة والقدرة الفائقة لها فى عملية تحليل واسترجاع المعلومات؛ اتجهت جميع الدول إلى إنشاء قواعد البيانات لتنظيم عملها.

وهناك آثار إيجابية كثيرة رفعت من قيمة خصوصية الأفراد الإلكترونية، وساعدت فى التعرف على الأخر وخصوصيته فى نطاق إيجابي، لكن البعض يستغل هذي التقنية وهذا التطور فى وسائل التواصل الاجتماعي أو غيرها بالجانب السلبي مشكلا مساسا بالخصوصية فى الوسيط الإلكتروني.

٢ - الآثار السلبية للتطور التقنية على الخصوصية:

على الرغم من أهمية وسائل التواصل الاجتماعي والتقنيات الرقمية بشكل عام، وما لها من آثار إيجابية سبق بيانها، فإن هناك مخاطر وآثارا سلبية كثيرة تؤثر على النظام العام واجه الحق فى الخصوصية بالنظر لإمكانية انتهاكها عبر هذه الوسائل.

ومع تزايد استعمال وسائل التواصل الاجتماعي والشبكة العنكبوتية، أصبحت المعلومات والبيانات ذات قيمة عالية، وهذا يؤدي إلى تزايد الحديث عن مخاطر تخزين البيانات وجمعها، ومخاطر تقنية المعلومات سيما فى مجال الخصوصية والحريات العامة.[٢]

وان تزايد استعمال وسائل التواصل الاجتماعي يزيد عمليات مراقبة الأفراد وتهديدهم وملاحقتهم والتعدي على خصوصياتهم؛ من خلال الوصول إلى البيانات الشخصية بصورة غير مشروعة، ويزيد من فرص إساءة استخدام تلك الوسائل؛ لأن المعلومات أو البيانات أصبحت متوفرة وبشكل أسهل من ذي قبل[٣].

فحينما يستعمل الفرد وسائل التواصل الاجتماعي فهو يتوقع نوعا من التخفي والتستر لكل معلوماته، إنما فى الحقيقة يمكن أن تكون حياته محمية أكثر فى الواقع؛

(١) عودة يوسف سلمان، الجرائم المائة بحرمة الحياة الخاصة التي تقع عبر وسائل تقنية المعلومات، مرجع سابق، ص ٨.
(٢) مارية بوجداين، مريم آل سيدي الغازي، الحق فى الحياة الخاصة إلى الحق الخصوصية الرقمية، مرجع سابق، صـ٧٠.
(٣) عودة يوسف سلمان، الجرائم المائة بحرمة الحياة الخاصة التي تقع عبر وسائل تقنية المعلومات، مرجع سابق، ص ٨٠.

نظرا للتحديات التي يطرحها العالم الافتراضي، فمثلا: فى وسائل التواصل نقدم معلوماتنا لجهات خارجية وداخلية ليس لها مكان معروف فى إطار عولمة المعلومات والاتصالات التي يعرفها هذا الوسيط)[١].

وكذلك هناك شركات اتصالات وشركات تقنية المعلومات لديها علاقة وثيقة مع بعض الدول وتعتمد عليها تلك الدول فى الحصول على تراخيص تتيح لها الوصول إلى بيانات المستخدمين، وبالتالي انتهاك خصوصيتهم الرقمية.[٢]

وهناك بعض وسائل التواصل الاجتماعي تقوم باستغلال بيانات المستخدم وتعدها موردا ماليا مهما، إذ تقوم هذه المواقع بالحصول على مبالغ مالية من المعلنين مقابل تقديم البيانات لهم، كونها تعد قاعدة بيانات تكشف وتعطي انطباعا عن اهتمام وميول المستخدم التي أبدى بها لهذا الموقع، وتسمى هذه العملية (بالتسويق الإلكتروني.[٣]

وقد أورد المشرع المصري نصا عن التسويق الإلكتروني فى المادة (٤٣) من قانون حماية البيانات الشخصية رقم (١٥١) لسنة ٢٠٢٠ على أنه: «يعاقب بغرامة لا تقل عن مائتي ألف جنيه ولا تجاوز مليوني جنيه، كل من خالف أحكام التسويق المنصوص عليها فى المادتين (١٧، ١٨) من هذا القانون».

والمادة (١٧) التي أشارت إليها المادة (٤٣) على أنه: «يحظر إجراء أي اتصال إلكتروني بغرض التسويق المباشر للشخص المعني بالبيانات إلا بتوافر الشروط الآتية: ١- الحصول على موافقة من الشخص المعني بالبيانات ٢- أن يتضمن الاتصال هوية منشئه ومرسله ٣- أن يكون للمرسل عنوان صحيح وكاف للوصول إليه ٤- الإشارة إلى أن الاتصال الإلكتروني مرسل لأغراض التسويق المباشر ٥- وضع آليات واضحة وميسرة لتمكين الشخص المعني بالبيانات من رفض الاتصال الإلكتروني أو العدول عن موافقته على إرسالها».

---

(١) بارق منتظر عبد الوهاب لامي. جريمة انتهاك الخصوصية عبر الوسائل الإلكترونية فى التشريع الأردني. رسالة ماجستير. كلية الحقوق. جامعة الشرق الأوسط. الأردن. ٢٠١٧. ص ١٠ - ٥٠.

(٢) رزق سلمودي. ليندا ربايعة. هديل الرزي. عصام براهمة. الموقف المعاصر لقواعد القانون الدولي من الحق فى الخصوصية فى العصر الرقمي. مجلة الجامعة العربية الأمريكية للبحوث. مجلد ٣. العدد ٢. ٢٠١٧. ص ٨.

(٣) وقد عرف قانون حماية البيانات الشخصية المصري المرقم (١٥١) لسنة ٢٠٢٠ التسويق الإلكتروني فى المادة (١) بأنه: «إرسال أي رسالة أو بيان أو محتوى إعلاني أو تسويقي بأي وسيلة تقنية أيا كانت طبيعتها أو صورتها تستهدف بشكل مباشر أو غير مباشر ترويج سلع أو خدمات أو التماسات أو طلبات تجارية أو سياسية أو اجتماعية أو خيرية موجهة إلى أشخاص بعينهم».

والمادة (١٨) التي أشارت إليها المادة (٤٣) على أنه: «يلتزم المرسل لأي اتصال إلكتروني بغرض التسويق المباشر بالالتزامات الآتية: ١- الغرض التسويقي المحدد ٢- عدم الإفصاح عن بيانات الاتصال للشخص المعني بالبيانات ٣- الاحتفاظ بسجلات إلكترونية مثبت بها موافقة الشخص المعني بالبيانات وتعديلاتها، أو عدم اعتراضه على استمراره ، بشأن تلقي الاتصال الإلكتروني التسويقي وذلك لمدة ثلاث سنوات من تاريخ آخر إرسال. وتحدد اللائحة التنفيذية لهذا القانون القواعد والشروط والضوابط المتعلقة بالتسويق الإلكتروني المباشر».

وكذلك هناك بعض الدول تدعو سلطات الضبط الإداري بأن تتجسس أو تطلع على البيانات الشخصية للأفراد وأسرارهم لا سيما وأن بعض الدول بدأت العمل بما يعرف بالحكومات الإلكترونية.

ويري بعض الفقهاء أن من حق الدولة أن تتدخل وتطلع على البيانات الشخصية للأفراد لحماية الأمن القومي ولا يعتبر ذلك انتهاكا للحقوق والحريات ولا يعد اعتداء على الحق فى الخصوصية؛ لأن الغرض منه تتبع الخارجين على القانون ولتستطيع أجهزة الدولة من ضبط الجناة قبل وقوع أي تهديد، وهناك الكثير من دول العالم كفرنسا وألمانيا وأمريكا تقوم بعملية تسجيل المحادثات الهاتفية والرسائل الإلكترونية الداخلية والخارجية ولا يعد ذلك انتهاكا لحق الخصوصية، ويمكن أن تسترجع هذه التسجيلات فى أي وقت حال وقوع جريمة ما[1].

ويري الباحث أن النظام العام والمصلحة العامة للدولة فوق كل اعتبار، وعلى الدول أن تشرع القوانين التي تبيح للدولة أن تتدخل بقدر معين، وكذلك أن يكون هذا القانون يحمي حرية الأفراد وخصوصياتهم، وأن يكون هذا القانون ملائما للتطور التقني الحاصل، وبعض الدول شرعت قانونا يتلاءم مع هذا التطور، وبعض الدول إلى الآن لم تواكب التطور التقني.

(١) شريف يوسف خاطر. حماية الحق فى الخصوصية المعلوماتية دراسة تحليلية لحق الاطلاع على البيانات الشخصية ، دراسة مقارنة .. دار الفكر والقانون. المنصورة. ٢٠١٥. ص ٢٣.

المطلب الثاني

حماية حق الخصوصية فى وسائل التواصل الاجتماعي فى النظم المقارنة

تعد الخصوصية حقا من الحقوق الدستورية الأساسية اللازمة للشخص الطبيعي بصفته الإنسانية كأصل عام، والتي كفلتها الشريعة الإسلامية لكونها أساس بنيان كل مجتمع سليم.

لذا تحرص الدول - خاصة الديمقراطية منها - على حماية هذا الحق وتعده حقا مستقلا قائما بذاته، ولا تكتفي بحماية نظامها العام أو بسن القوانين لحمايته؛ بل تسعى إلى ترسيخه فى الأذهان؛ وذلك لغرس القيم النبيلة التي تلعب دورا كبيرا وفعالا فى منع المتطفلين من التدخل فى خصوصيات الآخرين وكشف أسرارهم. لذا حظي هذا الحق باهتمام كبير سواء من جانب الهيئات والمنظمات الدولية أو من جانب الدساتير والنظم القانونية.

وهناك دول نصت دساتيرها على حماية الحياة الخاصة فى مواجهة أخطار الجرائم الإلكترونية التي تهدد النظام العام وكفلت حماية البيانات الشخصية، وهناك دول وضعت تشريعات خاصة لحماية الحياة الخاصة فى مواجهة الجرائم الإلكترونية، وسنبين ما نصت عليه التشريعات لحماية البيانات لأهم الدول الغربية والعربية.

أولا - التشريع الفرنسي: تعد فرنسا من الدول الرائدة فى ميدان حماية حقوق وحريات المواطنين فى مواجهة مخاطر وتطور تقنية المعلومات[1]، حيث أصدرت بتاريخ ١٩٧٨/١/٦ قانون المعلوماتية والحريات)، والذي تم تعديله عدة مرات وتتميمه بعدة مراسيم خلال الأعوام ١٩٨٨ و ١٩٩٢، وفي عام ١٩٧٨ أنشأ هذا القانون سلطة إدارية مستقلة هي (اللجنة الوطنية للمعلوماتية والحريات).

أما حماية حق الخصوصية فى التشريعات العربية فقد شرعت كل دولة ما رأته مناسبا من قوانين لحماية حق الخصوصية، ومن أجل عدم الإخلال بالنظام العام بما تفرضه عليها الظروف المحيطة بمجتمعها وشعوبها.

(١) عصام عبد الفتاح مطر. التجارة الإلكترونية فى التشريعات العربية والأجنبية. دار الجامعة. الإسكندرية.٢٠١٥. ص ٢٠١.

كما أن التطورات التقنية السريعة فى مجال وسائل التواصل الاجتماعي والشبكة العنكبوتية كان لها تأثير فى تعديل وتغيير كثير من الدول لقوانينها الوطنية التي رأت فيها عدم تحقيقها لأغراض العقوبة والتحري من قبل سلطات الضبط الإداري أمام الانتشار السريع للجريمة الإلكترونية، وهناك بعض الدول إلى الآن لم تواكب التطورات التقنية الحاصلة، وسنتناول هذا الحق فى بعض التشريعات العربية المقارنة.

وقد سعت مصر فى العديد من تشريعاتها إلى تنظيم الحق فى الخصوصية، وذلك عبر العديد من المواد القانونية، ولعل أبرزها ما ورد فى الدستور المصري لسنة ٢٠٠٤، وما ورد فى قانون مكافحة جرائم تقنية المعلومات رقم (١٧٥) لسنة ٢٠١٨، وما ورد من نصوص قانونية فى قانون حماية البيانات الشخصية رقم (١٥١) لسنة ٢٠٢٠.

فقد نص الدستور المصري فى المادة (٥٧) منه: الحياة الخاصة حرمة، وهي مصونة لا تمس وللمراسلات البريدية، والبرقية، والإلكترونية، والمحادثات الهاتفية، وغيرها من وسائل الاتصال محرمة، وسها مكفولة، ولا تجوز مصادرتها، أو الاطلاع عليها، أو رقابتها إلا بأمر قضائي مسبب، ولمدة محددة، وفي الأحوال التي بينها القانون. كما تلتزم الدولة بحماية حق المواطنين فى استخدام وسائل الاتصال العامة بكافة أشكالها، ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها، بشكل تعسفي، وينظم القانون ذلك «.

ونصت المادة (٩٩) من الدستور على أنه: «كل اعتداء على الحرية الشخصية أو حرمة الحياة الخاصة للمواطنين، وغيرها من الحقوق والحريات العامة التي يكفلها الدستور والقانون، جريمة لا تسقط الدعوى الجنائية ولا المدنية الناشئة عنها بالتقادم، وللمضرور إقامة الدعوى الجنائية بالطريق المباشر. وتكفل الدولة تعويضا عادلا لمن وقع عليه الاعتداء، وللمجلس القومي لحقوق الإنسان إبلاغ النيابة العامة عن أي انتهاك لهذه الحقوق، وله أن يتدل فى الدعوى المدنية منضما إلى المضرور بناء على طلبه، وذلك كله على الوجه المبين بالقانون «[١].

وقد عالج المشرع المصري عملية إفشاء البيانات الشخصية فى عدة مواد قانونية فى قانون حماية البيانات الشخصية رقم (١٠١) لسنة ٢٠٢٠، وسنذكر بعض هذه المواد.

(١) الجريدة الرسمية، العدد ٣ مكرر (أ) بتاريخ ١٨ يناير ٢٠٠٤.

نصت المادة (٢) من هذا القانون على أنه: «لا يجوز جمع البيانات الشخصية أو معالجتها أو الإفصاح عنها أو إفشاؤها بأي وسيلة من الوسائل إلا بموافقة صريحة من الشخص المعني بالبيانات، أو فى الأحوال المصرح بها قانونا»، ونصت الفقرة الأولى فى المادة (٣٦) من هذا القانون بأنه: يعاقب بغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مليون جنيه كل حائز أو متحكم أو معالج جمع أو عالج أو أفشي أو أتاح أو تداول بيانات شخصية معالجة إلكترونيا بأي وسيلة من الوسائل فى غير الأحوال المصرح بها قانونا أو بدون موافقة الشخص المعني بالبيانات»، وكذلك نصت المادة (٤١) من هذا القانون على أنه: يعاقب بالحبس مدة لا تقل عن ثلاثة شهور وبغرامة لا تقل عن خمسمائة ألف جنيه ولا تجاوز خمسة ملايين جنيه، أو بإحدى هاتين العقوبتين، كل حائز أو متحكم أو معالج جمع أو أتاح أو تداول أو عالج أو أفشي أو خن أو نقل أو حفظ بيانات شخصية حساسة بدون موافقة الشخص المعني بالبيانات أو فى غير الأحوال المصرح بها قانونا».

أما قانون مكافحة جرائم تقنية المعلومات لسنة ٢٠١٨ فقد نصت المادة (٢٠) منه على أنه: يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من اعتدى على أي من المبادئ أو القيم الأسرة فى المجتمع المصري أو انتهك حرمة الحياة الخاصة، أو أرسل بكثافة العديد من الرسائل الإلكترونية لشخص معين دون موافقته، أو من بيانات شخصية إلى نظام أو موقع إلكتروني لترويج السلع أو الخدمات دون موافقته، أو نشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات معلومات أو أخبارا أو صورا وما فى حكمها، تنتهك خصوصية أي شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحة أو غير صحيحة[١].

تجدر الإشارة إلى أن القضاء المصري قد تعرض إلى قانونية المراقبة على المجال الإلكتروني فى مصر، حيث كشف حكم محكمة القضاء الإداري الصادر عام ٢٠١١ فى قضية قطع الاتصالات خلال أحداث ثورة ٢٥ يناير، أن هناك محاولات للمراقبة بدأت وفقا لأقل التقديرات عام ٢٠٠٨ عندما قامت وزارات الداخلية والاتصالات والإعلام بمشاركة شركات الهاتف المحمول بإجراء بعض تجارب المراقبة، كانت إحداها فى ٦ أبريل عام ٢٠٠٨، والأخرى فى ١٠ أكتوبر ٢٠١٠، وقد استهدفت التجربتان قطع

(١) الجريدة الرسمية، العدد ٣٢ مكرر (ج) فى ١٤ أغسطس سنة ٢٠١٨.

الاتصالات عن مصر وكيفية حجب بعض المواقع الإلكترونية، وأسلوب منع الدخول على الشبكة العنكبوتية لمدينة أو لمحافظة أو لعدة محافظات، ووضع خطة لسرعة الحصول على بيانات مستخدمي الشبكة عقب استخدامها خلال فترة لا تقل عن ثلاثة أشهر.

أيضا أصدرت المحكمة ذاتها حكما فى عام ٢٠١٠ بصدد مراقبة خدمة رسائل المحمول المجمع (BULK SMS)، حيث قضت بوقف تنفيذ قرار الجهاز القومي لتنظيم الاتصالات بإخضاع خدمة الرسائل النصية القصيرة المجمعة للرقابة المسبقة أو اللاحقة، وبحظر تعليق مباشرة الشركات المرخص لها لنشاطها المتعلق بتقديم تلك الخدمة على وجوب الحصول على موافقات مسبقة قبل تقديم الخدمة تقوم على رقابة محتوى الرسائل) محل الترخيص من أية جهات.[١]

اما فى الدستور الكويتي الصادر عام ١٩٦٢، أعيد العمل به عام ١٩٩٢ نص فى المادة (٣٩) علي الحق فى احترام الخصوصية حرية المراسلة البريدية والبرقية والهاتفية مصونة، وسيرتها مكفولة، فلا يجوز مراقبة الرسائل أو إفشاء سريتها إلا فى الأحوال المبينة فى القانون وبالإجراءات المنصوص عليها فيه.

(١) حكم المحكمة الإدارية العليا، الدائرة الأولى عليا، الطعون أرقام ٢٠٠٣٠ و ٢٠٩٥٩، جلسة رقم ٥٧ بتاريخ ٢٠١١/٤/١٦.

الخاتمة

نخلص من هذا البحث بمجموعة من التوصيات نجملها فى الآتي :

١-يقترح الباحث على المشرع المصري والكويتي إعادة النظر فى التشريعات على النحو الذي ينسجم ويتوافق مع متطلبات التطور التقني وبالأخص فيما يتعلق بالجرائم الالكترونية بمختلف أنواعها .

٢-يوصي الباحث المشرع بضرورة سن قانون جديد ينظم سلطة الضبط الإداري فى مجال الجرائم الالكترونية فى جميع جوانبها وأبعادها .

٣-نوصي الجهات الأمنية بتأسيس موقع الكتروني يسمح للأفراد بالتبليغ الالكتروني عن أي أفعال تمثل تهديدا للنظام العام ، سواء كانت هذه الافعال تقليدية أم الكترونية .

٤-يوصي الباحث بضرورة تأهيل سلطات الضبط الإداري من خلال تزويدهم بالأجهزة الحديثة وجعلها مواكبة للتطورات التقنية وتدريبهم فى مجال التعامل مع الأدلة الالكترونية وتحديث وسائل المراقبة لمواجهة القصور الممكن حدوثه فى إثبات الجريمة الالكترونية .

٥-زيادة الاهتمام بالتخيط الاستراتيجي على المستوى الوطني فى حملات التوعية لمواجهة الاستخدام السلبي لوسائل التواصل الاجتماعي .

٦-ضرورة توفير كوادر شرطية مختصة ومدربة وعلى دراية عالية بوسائل تقنية المعلومات لتكون قادرة على التحري عن هذا النوع من الجرائم . وضرورة تأهيل قضاة مختصين للنظر فى مثل هذه القضايا ، فضلا عن الاهتمام بالجانب الوقائي لمكافحة الجريمة المعلوماتية وذلك من خلال المتابعة المستمرة لآخر ما يتوصل له خبراء أمن المعلومات من الوسائل الفنية الكفيلة بحماية أم الانسان من اعتداء علي عرضه الكترونيا .

قائمة المراجع

١. أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات - دراسة مقارنة، دار النهضة العربية، القاهرة، ط ٣، ١٩٩٤.

٢. أيمن عبد الله فكري، جرائم نظم المعلومات - دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، ٢٠٠٧.

٣. بارق منتظر عبد الوهاب لامي، جريمة انتهاك الخصوصية عبر الوسائل الإلكترونية فى التشريع الأردني، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، الأردن، ٢٠١٧،

٤. بوزيدي سليم، الاعتداء على الحق فى الصورة فى ظل التطورات التكنولوجية الحديثة، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة، بجاية، ٢٠١٩.

٥. بن قارة مصطفى عائشة، الحق فى الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية القانونية، المجلة العربية للعلوم ونشر الأبحاث، المجلد الثاني، العدد ٥، ٢٠١٦.

٦. حسن علي شاهين، التحريات الأمنية فى مجال الضبط الإداري ، دار النهضة العربية، القاهرة، ٢٠١٥.

٧. راشد محمد الشحي، الرقابة القضائية على قرارات الضبط الإداري فى الحكومة الإلكترونية، أطروحة دكتوراه، كلية الحقوق، جامعة القاهرة، ٢٠١١.

٨. رامي الجالي، التنظيم القانوني لحرية الصحافة الإلكترونية، دار الجامعة الجديدة، الإسكندرية، ٢٠١٩.

٩. زينة عبد الله محمد مصطفى، الرقابة الإلكترونية وحرية الرأي والتعبير - دراسة مقارنة بين مصر وايران، مقال منشور عبر موقع المركز العربي لأبحاث الفضاء الإلكتروني على الرابط التالي: http://accronline.com/article detail.aspx?id=258

١٠. سامي حسن نجم الحمداني، حسين طلال مال الله العزاوي، دور الضبط الإدارية الإلكتروني فى مكافحة الشائعات المخلة بالأمن العام، كلية الحقوق والعلوم السياسية ، جامعة كركوك ،٢٠١٩.

١١. سامح أحمد بلتاجي ،الجوانب الاجرائية للحماية الجنائية لشبكة الانترنت ، رسالة دكتوراة ، كلية الحقوق ، جامعة الاسكندرية ، ٢٠١٠

١٢. سوزان عدنان ، انتهاك حرمة الحياة الخاصة عبر الإنترنت، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد ٢٩، العدد الثالث، ٢٠١٣،

٣١. صفاء أوتاني، الوضع تحت المراقبة الإلكترونية (السوار الإلكتروني فى السياسة العقابية الفرنسية، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد ٤٥، العدد ١، ٢٠٠٩،

١٤. طارق عفيفي صادق أحمد، الجرائم الإلكترونية - جرائم الهاتف المحمول، المركز القومي للإصدارات القانونية، القاهرة، ط١، ٢٠١٥.

١٥. عبد الفتاح بيومي حجازي: الحكومة الإلكترونية بين الواقع والطموح، دار الفكر الجامعي، الإسكندرية، ط١، ٢٠٠٨.

١٦. عبد الهادي درار، نظام المراقبة الإلكترونية فى ظل تطورات النظم الإجرائية الجزائية بموجب الأمر (١٥ - ٢٠)مجلة الدراسات والبحوث القانونية، العدد ٣.

١٧. عبد الرؤف هاشم بسيوني، نظرية الضبط الإداري فى النظم الوضعية المعاصرة والشريعة الإسلامية، دار الفكر الجامعي، الإسكندرية، ط١، ٢٠٠٧ .

٨١. عزيز ملحم برير، الشبكات والإنترنت، جامعة نايف العربية للعلوم الأمنية ،٢٠٠٨ .

١٩. عصام عبد الفتاح مطر، التجارة الإلكترونية فى التشريعات العربية والأجنبية، دار الجامعة الجديدة، الإسكندرية،٢٠١٥.

٢٠. عمر سالم، المراقبة الإلكترونية طريقة حديثة لتنفيذ العقوبة السالبة للحرية خارج السجن، دار النهضة العربية، القاهرة ، ط ٢.

٢١. محمد عزت عبد العظيم، الجرائم المعلوماتية الماسة بالحياة الخاصة، دار النهضة العربية، مصر، ٢٠١٦.

٢٢. محمد علي سويلم ، مكافحة الجرائم الإلكترونية - دراسة مقارنة بالدراسات العربية والأجنبية، دار المطبوعات الجامعية ، الاسكندرية ، ط١ ، ٢٠١٩ .

٢٣. محمد بن عيد القحطاني، حماية الخصوصية الشخصية لمستخدمي مواقع التواصل الاجتماعي، رسالة ماجستير، كلية العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، ٢٠١٠.

٢٤. محمود عبد الرحمن محمد، نطاق الحق فى الحياة الخاصة - دراسة مقارنة بالقانون الوضعي (الأمريكي – الفرنسي المصري) والشريعة الإسلامية، دار النهضة العربية، ٢٠١٠.

٢٥. مصطفى محمد موّسى، المراقبة الإلكترونية عبر شبكة الإنترنت بين المراقبة الأمنية التقليدية والإلكترونية، دار الكتب والوثائق المصرية، القاهرة، ٢٠٠٣.

٢٦. مصطفى جمال حنفي زينو، دور الضبط الإداري فى مجال الجرائم الإلكترونية المخلة بالأمن العام، رسالة ماجستير ، كلية الحقوق ، جامعة الأزهر ، غزة ، ٢٠١٧.

٢٧. وليد محمد الشناوي، التطورات الحديثة للرقابة القضائية على التناسب فى القانون الإداري – دراسة تأصيلية تحليلية مقارنة، دار الفكر والقانون، المنصورة، ٢٠١٧.

٢٨. نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت فى مرحلة جمع الاستدلالات ، دار الفكر الجامعي، الإسكندرية، ٢٠١٢.

٢٩. هشام محمد فريد رستم ، الجوانب الإجرائية للجرائم المعلوماتية ، أصول التحقيق الجنائي الفني والية التدريب التخصصي للمحققين بحث منشور بمجلة الأمن والقانون، تصدر عن كلية شرطة دبي ، السنة السابعة العدد الثاني ، ربيع الأول ١٤٢٠

ملخص المبحث :

إذا كانت خصوصية الأفراد لها أهمية كبيرة جعلتها تحظي باهتمام الفقه والقضاء منذ قديم الأزل، فإن هذه الأهمية تزداد عندما يتعلق الأمر بالأضرار التي يسببها التطور الهائل فى مجال الاتصالات والتواصل هذا ويكتسب البحث فى هذا المجال أهميته لأنه يعتبر الحق فى الخصوصية وحماية البيانات الشخصية من أهم الحقوق الدستورية اللصيقة بالإنسان، بيد أن التقدم التكنولوجي فى الاتصالات الالكترونية أضحى أهم الأسباب التي تمثل مساسا بهذا الحق.

ولقد انغمس الأفراد وبشدة فى استخدام التقنيات الحديثة بما تشمله من وسائل اتصال، وتكنولوجيا للمعلومات، فضلا عن بروز الدور الجديد لوسائل التواصل الاجتماعي بكافة أنواعها، حتى أصبحت جزءا مهما فى حياتنا، اخترقت خصوصياتنا، وزاحمت علاقتنا الاجتماعية.

وتطورت خصوصية الإنسان عن المعنى التقليدي المألوف نتيجة التطور العلمي الهائل فى مجال التكنولوجيا، فبظهور الحواسيب أصبحت هناك خصوصية بالبيانات المخزنة عليها، كما أضحت هناك خصوصية للبيانات الشخصية عبر شبكة الانترنت.

ولقد خلفت ثورة المعلومات والاتصالات أثراً عميقاً فى مختلف المجالات، ولم تعد وسائل الحماية التقليدية صالحة لمواجهة التعدي على حقوق ملكية البيانات والمعلومات ، لاسيما مع التزايد المستمر لآليات الحصول على المعلومة عبر شبكة الإنترنت، وسهولة الحصول عليها عبر مواقع التواصل، والمدونات والمنتديات والمواقع الإلكترونية الحكومية وغير الحكومية، المفتوحة وذات الاشتراك .

فأنواع حماية الخصوصية فى وسائل التواصل الاجتماعي التي ذكرت تؤثر وتخل بالنظام العام فى المجتمع إذا انتهكت، فعلى سلطات الضبط الإداري فى الدولة أن تأخذ على عاتقها حماية خصوصية الأفراد وعدم انتهاكها من قبل الآخرين، وعلى سلطات الضبط أن تكيف نفسها وتواكب التطورات التقنية من أجل الحد من الخطورة القائمة على انتهاك الخصوصية.

الكلمات المفتاحية : ضبط إداري ، جرائم الكترونية ، مواقع التواصل الاجتماعي ، المراقبة الالكترونية ، الخصوصية المعلوماتية.

Administrative Control Measures to Combat Social Media crimes

Dr. Fawzi Muhammad Saqr

PhD in Public Law - Ain Shams University

Abstract

If the privacy of individuals has a great importance that has made it the attention of jurisprudence and the judiciary since ancient times, this importance increases when it comes to the damage caused by the tremendous development in the field of communication and communication. Research in this area is important because it considers the right to privacy and the protection of personal data to be among the most important constitutional rights attached to humans, but technological progress in electronic communications has become the most important reason that represents an infringement of this right.

Individuals have immersed themselves heavily in the use of modern technologies, including the means of communication and information technology, as well as the emergence of the new role of social media of all kinds, until it became an important part of our lives, penetrated our privacy and crowded our social relationship.

Human privacy has evolved from the traditional, familiar meaning as a result of the tremendous scientific development in the field of technology. With the emergence of computers, there is privacy in the data stored on them, and there is privacy for personal data over the Internet.

I have left information and communication revolution, a profound impact in various fields, and no longer the means of protection of traditional valid to counter infringement data and information ownership rights, especially with the ever-increasing mechanisms of access to information over the Internet, and get it

through networking sites, blogs, forums, websites, governmental and non Governmental, open, and subscription-based.

The types of privacy protection in the social media mentioned above affect and disturb the public order in society if they are violated. The administrative control authorities in the state must take upon themselves to protect the privacy of individuals and not violate it by others, and the control authorities must adapt themselves and keep pace with technological developments in order to reduce The risk of breaching privacy.

key words: Administrative control, electronic crimes, social networking sites, electronic surveillance, information privacy.