مخاطر تهدد الحق في الخصوصية عبر التقانات الإلكترونية الرقمية

د. مصطفى موسى (*)

(*) أستاذ القانون العام في كلية القانون الكويتية العالمية

مقدمة

يبدأ البحث العلمي بظاهرة اجتماعية تشير إلى وجود مشكلة تحتاج إلى حل، ويعتبر تحديد المشكلة من أهم المراحل التي يمر بها البحث، لأنها بمثابة العلة التي ينبغي تشخيصها بدقة حتى يمكن اقتراح الحل، بعد الوقوف على بيئتها بحيث إذا كان التشخيص خاطئاً كان الحل غير مجد، وكانت كل خطوات البحث لا جدوى علمية أو اجتماعية من ورائها.

ويقصد بالجدوى العلمية مدى إسهام البحث في زيادة مخزون المعرفة في مجال موضوع المؤتمر وهو «التحديات المستجدة للحق في الخصوصية».

ويقصد بالجدوى الاجتماعية مدى إسهام البحث في حل مشكلة تؤرق بال المجتمع. ويقصد بالمشكلة في هذا البحث موضوع يحيط به الغموض ويطلب حلاً، ويكون البحث العلمي هو الوسيلة التي يمكن من خلالها اقتراح الحلول واستخلاص النتائج والتوصيات.

من هذا المنطلق يمكن تحديد المشكلة التي نحن بصددها وهي موضوع البحث، بعنوان «مخاطر تهدد الحق في الخصوصية عبر التقانات الإلكترونية الرقمية» في مجتمع المعلومات، والمجتمع الافتراضي وشبكاته سواء كانت إنترنت أو إنترانت أو إكسترانت أو تواصلاً اجتماعياً.

ينطلق البحث من مسلمة واضحة مؤداها أن هناك تحديات مستجدة تهدد حقوق الإنسان، نظراً لظهور إجرام بأساليب جديدة يستخدم التقانات الإلكترونية الرقمية مما ترتب عليه ظهور جرائم في مجتمع المعلومات والمجتمع الافتراضي عبر شبكاتها منها على سبيل المثال: البرامج الإلكترونية المتطفلة الضارة وهي: الفيروسات الإلكترونية، والديدان الإلكترونية وحصان طروادة الإلكتروني، والبريد الإلكتروني غير المرغوب فيه، والحصول على كلمات العبور بأسلوب غير مشروع وإثارة مشكلات فنية وأمنية عبر البريد الإلكتروني، واستخدام البريد الإلكتروني للآخرين في تناول وسائط تتنافي مع القيم والأخلاق والآداب.

نتبع في هذا البحث الدراسة الوصفية المرنة والمنهج التحليلي لمعرفة المخاطر التي تهدد الحق في الخصوصية عبر التقانات الإلكترونية من خلال الوثائق العالمية والدستورية والمبادئ التي قررتها المحكمة الدستورية وتقارير شركات الأمن المتخصصة مثل MCAFEE .

يهدف البحث إلى الإجابة على عدة أسئلة منها: ما هي الحقوق المتصلة بالحق في الخصوصية في عصر التقانات الإلكترونية الرقمية؟ وما هي تلك الحقوق في الوثائق الدولية والدستورية للدول؟ وما هي المبادئ التي أرستها المحكمة الدستورية العليا في هذا الشأن؟ وما هي اجتهادات تأصيل حقوق الإنسان في عصر التقانات الإلكترونية الرقمية ؟ ما هي بيئة المخاطر التي هددت وتهدد الحق في الخصوصية في عصر التقانات الإلكترونية الرقمية؟ وما هي المخاطر التي هددت وتهدد الحق في الخصوصية عبر التقانات الإلكترونية الرقمية؟

ينقسم البحث إلى مبحثين :

المبحث الأول – حقوق الإنسان في عصر التقانات الإلكترونية الرقمية.

المبحث الثاني – مخاطر التقانات الإلكترونية الرقمية على الحق في الخصوصية.

المبحث الأول

حقوق الإنسان في عصر التقانات الإلكترونية الرقمية

نتناول في هذا المبحث الحقوق المتصلة بالحق في الخصوصية في الإعلان العالمي لحقوق الإنسان وبعض الدساتير العربية والولايات المتحدة الأمريكية والمبادئ التي أرستها المحكمة الدستورية العليا في مصر في هذا الشأن ثم اجتهادات تأصيل حقوق الإنسان في عصر التقانات الإلكترونية الرقمية.

الحقوق المتصلة بالحق في الخصوصية:

أصدرت الأمم المتحدة الإعلان العالمي لحقوق الإنسان في 10 كانون الأول/ ديسمبر 1948 للإنسان قبل عصر التقانات الإلكترونية الرقمية وذكرت بعبارات واضحة الحقوق التي يتمتع بها كل فرد بالتساوي مع غيره، باعتباره صاحب هذه الحقوق وعليه معرفتها والدعوة لها والدفاع عنها من أجل كل إنسان وذكرت ديباجة الإعلان العالمي لحقوق الإنسان أن «.... تناسي حقوق الإنسان وازدراءها قد أفضيا إلى أعمال همجية آذت الضمير الإنساني. وكان غاية ما يرنو إليه عامة البشر انبثاق عالم يتمتع فيه الفرد بحرية القول والعقيدة ويتحرر من الفزع والفاقة ... على أن يتولى القانون حماية حقوق الإنسان لكي لاً يضطر المرء آخر الأمر إلى التمرد على الاستبداد والظلم ...» .

لم ينص الإعلان العالمي على الحق في الخصوصية بعبارة صريحة ومباشرة ولكن نص في المادة (3) على أن «لكل فرد الحق في الحياة والحرية وسلامة شخصيته».

وأشارت الجمعية العامة في قرارها 167 / 68 إلى أن القانون الدولي لحقوق الإنسان يوفر الإطار العالمي الذي يجب أن يقيم على ضوئه أي تدخل في حقوق الخصوصية الفردية. وتنص المادة 12 من الإعلان العالمي لحقوق الإنسان على أنه « لا يُعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته، أو لحملات

على شرفه وسمعته، ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات». ووفقاً للمادة 17 من العهد الدولي الخاص بالحقوق المدنية والسياسية، «لا يجوز تعريض أي شخص، على نحو تعسفي أو غير قانوني، لتدخل في خصوصياته أو شؤون أسرته أو بيئته أو مراسلاته، ولأي حملات غير قانونية تمس شرفه أو سمعته». وتشير هذه المادة علاوة على ذلك إلى أن «من حق كل شخص أن يحميه القانون من مثل هذا التدخل أو المساس»[1].

ولقد تضمنت دساتير الدول حقوق إنسانية مماثلة كحق جميع الأشخاص في أن تحترم حياتهم الخاصة وحياتهم العائلية وسكنهم ومراسلاتهم أو الحق في الاعتراف بكرامتهم أو سلامتهم الشخصية أو سمعتهم واحترامها. وبعبارة أخرى، هناك اعتراف عالمي بالأهمية الأساسية والصلة الوطيدة للحق في الخصوصية والحاجة إلى ضمان حماية هذا الحق في القانون والممارسة وعدم جواز المساس بها إلا بأمر قضائي مسبب أو في حالة التلبس بالجرم المشهود.

تطبيقاً لذلك نصت دساتير مصر والكويت والبحرين والإمارات العربية المتحدة وسلطنة عمان وقطر وتونس والولايات المتحدة الأمريكية على ما يلي:

أولاً- حرمة الأشخاص والحياة الخاصة والمراسلات والتنقل في دستور مصر الصادر 2014:

1- حرمة الأشخاص:

نصت المادة (54) من الباب الثالث – الحقوق والحريات والواجبات العامة – على أن «الحرية الشخصية حق طبيعي، وهي مصونة لا تمس، وفيما عدا حالة التلبس، لا يجوز القبض على أحد، أو تفتيشه، أو حبسه، أو تقييد حريته بأي قيد إلا بأمر قضائي مسبب يستلزم التحقيق».

(1) تقرير مفوضية الأمم المتحدة السامية لحقوق الإنسان، المقدم إلى مجلس حقوق الإنسان في دورته السابعة والعشرين وإلى الجمعية العامة في دورتها التاسعة والستين والمعنون « الحق في الخصوصية في العصر الرقمي ، 30/6/2014، ص6، راجع في ذلك الأمم المتحدة، الجمعية العامة، مجلس حقوق الإنسان الموقع الإلكتروني www.ahchr.org آخر زيارة للموقع (15/9/2014).

ويجب أن يبلغ فوراً كل من تقيد حريته بأسباب ذلك، ويحاط بحقوقه كتابة، ويمكن من الاتصال بذويه وبمحاميه فوراً، وأن يتقدم إلى سلطة التحقيق خلال أربع وعشرين ساعة من وقت تقييد حريته. ولا يبدأ التحقيق معه إلا في حضور محاميه، فإن لم يكن له محام، ندب له محام، مع توفير المساعدة اللازمة لذوي الإعاقة، وفقاً للإجراءات المقررة في القانون. ولكل من تقيد حريته، ولغيره، حق التظلم أمام القضاء من ذلك الإجراء والفصل فيه خلال أسبوع من ذلك الإجراء، وإلا وجب الإفراج عنه فوراً.

وينظم القانون أحكام الحبس الاحتياطي، ومدته، وأسبابه، وحالات استحقاق التعويض الذي تلتزم الدولة بأدائه عن الحبس الاحتياطي، أو عن تنفيذ عقوبة صدر حكم بات بإلغاء الحكم المنفذة بموجبه. وفي جميع الأحوال لا يجوز محاكمة المتهم في الجرائم التي يجوز الحبس فيها إلا بحضور محام موكل أو منتدب» .

2- حرمة الحياة الخاصة في المراسلات:

نصت المادة (57) من الدستور في نفس الباب على أن « للحياة الخاصة حرمة، وهي مصونة لا تمس. وللمراسلات البريدية، والبرقية، والإلكترونية والمحادثات الهاتفية، وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة ولا تجوز مصادرتها، أو الإطلاع عليها، أو رقابتها إلا بأمر قضائي مسبب، ولمدة محددة، وفي الأحوال التي بينها القانون.

كما تلتزم الدولة بحماية حق المواطنين في استخدام وسائل الاتصال العامة بكافة أشكالها، ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها، بشكل تعسفي، وينظم القانون ذلك».

3- حرمة المسكن:

نصت المادة (58) من الدستور في نفس الباب على أن «للمنزل حرمة وفيما عدا حالات الخطر أو الاستغاثة لا يجوز دخولها، ولا تفتيشها، ولا مراقبتها أو التنصت عليها إلا بأمر قضائي مسبب، يحدد المكان، والتوقيت، والغرض منها وذلك كله في

الأحوال المبينة في القانون، وبالكيفية التي ينص عليها، ويجب تنبيه من في المنازل عند دخولها أو تفتيشها، وإطلاعهم على الأمر الصادر في هذا الشأن».

4- حرمة التنقل:

نصت المادة (62) ... من الدستور في نفس الباب على أن: «حرية التنقل والإقامة، والهجرة مكفولة. ولا يجوز إبعاد أي مواطن عن إقليم الدولة، ولا منعه من العودة إليه. ولا يكون منعه من مغادرة إقليم الدولة، أو فرض الإقامة الجبرية عليه، أو حظر الإقامة في جهة معينة عليه، إلا بأمر قضائي مسبب ولمدة محددة، وفي الأحوال المبينة في القانون».

ثانياً- حرمة الأشخاص والمساكن والمراسلات في دساتير بعض الدول العربية:

1- حرمة الأشخاص:

- دستور دولة الكويت: (الصادر في 11 نوفمبر 1962):

نص في المادة (31) في الباب الثالث المعنون « الحقوق والواجبات العامة» على أنه «لا يجوز القبض على إنسان أو حبسه أو تفتيشه أو تحديد إقامته أو تقييد حريته في الإقامة أو التنقل إلا وفق أحكام القانون ....».

- دستور مملكة البحرين: (الصادر في 14 نوفمبر 2002):

نصت المادة (19) من الدستور بفقراتها الأربع على ما يسمى بالحرية الشخصية حيث كفالتها وفقاً للقانون، فقد نصت الفقرة (أ) على أن الحرية الشخصية مكفولة وفقاً للقانون ونصت الفقرة (ب) على أنه: « .... لا يجوز القبض على إنسان أو توقيفه أو حبسه أو تفتيشه أو تحديد إقامته أو تقييد حريته في الإقامة أو التنقل إلا وفق أحكام القانون وبرقابة القضاء ....».

- دستور دولة الإمارات العربية المتحدة : (الصادر في 2 ديسمبر 1971).

نصت المادة (26) فقرة أولى من الدستور الصادر في الثاني من ديسمبر 1971 على أن الحرية الشخصية مكفولة لجميع المواطنين، ولا يجوز القبض على أحد أو تفتيشه أو حجزه أو حبسه إلا وفق أحكام القانون .

– دستور دولة قطر: (الصادر تعديله في 29 ابريل 2003):

أخذ دستورها الصادر تعديله في 29 أبريل 2003 بما أخذت به الدساتير السابقة من النص على كفالة الحرية الشخصية وذلك في نص مستقل، حيث نصت الفقرة الأولى من المادة (63) من الباب الثالث المعنون: «الحقوق والواجبات العامة» على أن: «الحرية الشخصية مكفولة ولا يجوز القبض على إنسان أو حبسه أو تفتيشه أو تحديد إقامته أو تقييد حريته في الإقامة أو التنقل إلا وفق أحكام القانون ....».

– دستور سلطنة عمان: (الصادر في نوفمبر1996):

نصت المادة (18) على أن: «الحرية الشخصية مكفولة وفقاً للقانون ولا يجوز القبض على إنسان أو تفتيشه أو حجزه أو حبسه أو تحديد إقامته أو تقييد حريته في الإقامة أو التنقل إلا وفق أحكام القانون.

ويقترب هذا النص ودستور مملكة البحرين والإمارات العربية المتحدة ودولة الكويت .

– مشروع دستور تونس: (1 يونيو 2013):

نصت المادة (23) من الباب الثاني: الحقوق والحريات «تحمي الدولة الحياة الخاصة، وحرمة المسكن، وسرية المراسلات، والاتصالات، والمعطيات الشخصية .

لكل مواطن الحرية في اختيار مقر إقامته وفي التنقل داخل الوطن وله الحق في مغادرته. لا يمكن المساس بهذه الحقوق والحريات إلا في حالات يضبطها القانون وبقرار قضائي».

2– حرمة المسكن:

– دستور دولة الكويت:

نصت المادة (38) على أن «للمساكن حرمة، فلا يجوز دخولها بغير إذن أهلها، إلا في الأحوال التي يعينها القانون وبالكيفية المنصوص عليها فيه» .

– دستور مملكة البحرين:

نصت المادة (25) على «حرمة المساكن وعدم جواز دخولها أو تفتيشها بغير إذن أهلها إلا استثناء في حالات الضرورة القصوى التي يعينها القانون وبالكيفية المنصوص عليها فيه». ويؤخذ من هذا النص أن المشرع الدستوري قد وجه المشرع القانوني للالتزام بالتشدد في إجراءات وضمانات إصدار الإذن الذي بمقتضاه يمكن دخول المسكن أو تفتيشه.

– دستور دولة الإمارات العربية المتحدة:

نصت المادة (36) على أن «للمساكن حرمة، فلا يجوز دخولها بغير إذن أهلها، إلا وفق أحكام القانون وفي الأحوال المحددة».

– دستور دولة قطر:

نصت المادة (37) على أنه «لخصوصية الإنسان حرمتها، ولا يجوز تعرض أي شخص، لأي تدخل في خصوصياته أو شئون أسرته أو مسكنه أو مراسلاته أو أية تدخلات تمس شرفه أو سمعته إلا وفقاً لأحكام القانون وبالكيفية المنصوص عليها فيه».

– دستور سلطنة عمان:

نصت المادة (27) على أن للمساكن حرمة فلا يجوز دخولها بغير إذن أهلها إلا في الأحوال التي يعينها القانون المنصوص عليه فيها .

2– حرمة المراسلات:

– دستور دولة الكويت :

نصت المادة (39) على أن «حرية المراسلة البريدية والبرقية والهاتفية مصونة، وسريتها مكفولة، فلا يجوز مراقبة الرسائل، أو إفشاء سريتها إلا في الأحوال المبينة في القانون وبالإجراءات المنصوص عليها فيه» .

– دستور مملكة البحرين:

كفل في المادة (26) حرية المراسلة البريدية، والهاتفية والإلكترونية، وأنها مصونة وسريتها مكفولة فلا يجوز مراقبة المراسلات أو إفشاء سريتها إلا في الضرورات التي يبينها القانون، ووفقاً للإجراءات والضمانات المنصوص عليها فيه.

– دستور دولة الإمارات العربية المتحدة:

نصت المادة (31) على حرية المراسلات البريدية والبرقية وغيرها من وسائل الاتصال وأن حرية تلك المراسلات وسريتها مكفولتان وفقاً للقانون.

– دستور دولة قطر:

نصت المادة (37) على خصوصية وحرمة المراسلات[1].

– دستور سلطنة عُمان :

نص الدستور في المادة (30) على حرية المراسلات البريدية والبرقيات والمخاطبات الهاتفية وغيرها من وسائل الاتصال.

ثالثاً– دستور الولايات المتحدة الأمريكية:

نص على الحرمات الثلاثة: الأشخاص والمساكن والمراسلات في مادة واحدة ورد في التعديل الرابع الذي نص على: «حق الناس في أن يكونوا آمنين في شخوصهم ومنازلهم وأوراقهم وممتلكاتهم ضد التفتيش والضبط غير القانوني. ويجب ألا ينتهك أي من ذلك، ولن يتم إصدار إذن ضبط وتفتيش إلا على أساس سبب معقول ومدعوم بقسم وإفادة موصوف فيها بدقة المكان المقصود تفتيشه والأفراد والأشياء المراد ضبطها[2].

(1) لم ينص على حرمة المراسلات في الدستور قبل تعديلاته الصادر في 29/4/2003.

(2) عمر محمد بن يونس، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي، (المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسيب وصولاً إلى الدليل الإلكتروني في التحقيقات الجنائية)، موسوعة التشريعات العربية، الطبعة الأولى 2004 ، 2005 ، ص55، وانظر النص باللغة العربية في هامش نفس الصفحة.

رابعاً- المبادئ التي قررتها المحكمة الدستورية العليا في مصر بشأن الحقوق المتصلة بالحق في الخصوصية:

أرست المحكمة الدستورية العليا في مصر عدة مبادئ بشان حرمة الحياة الخاصة، وحرمة المسكن على النحو التالي:

حرمة الحياة الخاصة:

الحياة الخاصة لكل فرد تشمل مناطق لا يجوز النفاذ إليها أو اقتحامها أو محاولة التلصص عليها أو اختلاس بعض جوانبها. وفي هذا المفهوم قالت المحكمة الدستورية العليا المصرية: «... ثمة مناطق من الحياة الخاصة لكل فرد تمثل أغواراً لا يجوز النفاذ إليها، وينبغي - دوماً ولاعتبار مشروع- ألا يقتحمها أحد ضماناً لسريتها، وصوناً لحرمتها، ودفعاً لمحاولة التلصص عليها، أو اختلاس بعض جوانبها، وبوجه خاص من خلال الوسائل العلمية الحديثة التي بلغ تطورها حداً مذهلاً، وكان لتنامي قدراتها على الاختراق أثراً بعيداً على الناس جميعهم وبياناتهم الشخصية التي غدا الإطلاع عليها وتجميعها نهباً لأعينها ولأذانها، وكثيراً ما ألحق النفاذ إليها الحرج أو الضرر بأصحابها، وهذه المناطق من خواص الحياة ودخائلها، تصون مصلحتين قد تبدوان منفصلتين، إلا أنها تتكاملان، ذلك أنهما تتعلقان بوجه عام بنطاق المسائل الشخصية التي ينبغي كتمانها، وكذلك نطاق استقلال كل فرد ببعض قراراته الهامة التي تكون- بالنظر إلى خصائصها وآثارها - أكثر اتصالاً بمصيره وتأثيراً في أوضاع الحياة التي اختار أنماطها، وتبلور هذه المناطق جميعها - التي يلوذ الفرد بها، مطمئناً لحرمتها ليهجع إليها بعيداً عن أشكال الرقابة وأدواتها - الحق في أن تكون للحياة الخاصة تخومها بما يرعى الروابط الحميمة في نطاقها، ولئن كانت بعض الوثائق الدستورية لا تقدر هذا الحق بنص صريح فيها، إلا أن البعض يعتبره من أشمل الحقوق وأوسعها، وهو كذلك أعمقها اتصالاً بالقيم التي تدعو إليها الأمم المتحضرة»[1].

(1) مجموعة المبادئ التي قررتها المحكمة العليا والمحكمة الدستورية العليا في أربعين عاماً 1969-2009 المحكمة الدستورية العليا، جمهورية مصر العربية، ص384، وانظر إشارتها للقضية رقم 23 لسنة 16 قضائية «دستورية» بجلسة 18/3/1995، ج6، دستورية، ص567 .

حرمة المسكن:

أرست المحكمة الدستورية مبدأ عدم جواز انتهاك حرمة المسكن بدخوله أو تفتيشه ما لم يصدر أمر قضائي مسبب، ولو توافرت حالة التلبس بالجريمة التي تخول القبض على الشخص وتفتيشه .

نصت الفقرة الأولى من المادة (41) في الباب الثالث– الحريات والحقوق والواجبات العامة من الدستور المصري الصادر 1971 على أن: «الحرية الشخصية حق طبيعي، وهي مصونة لا تمس»، وفيما عدا حالة التلبس لا يجوز القبض على أحد أو تفتيشه أو حبسه أو تقييد حريته بأي قيد، أو منعه من التنقل إلا بأمر تستلزمه ضرورة التحقيق، وصيانة أمن المجتمع، ويصدر هذا الأمر من القاضي المختص أو النيابة العامة، وذلك وفقاً لأحكام القانون، ثم نصت المادة (44) من الدستور على أن « للمساكن حرمة فلا يجوز دخولها أو تفتيشها إلا بأمر قضائي مسبب وفقاً لأحكام القانون» .

ونصت المادة (34) من الباب الثاني – الحقوق والحريات– الفصل الأول – الحقوق الشخصية من الدستور المصري الصادر 2012(1) أن: «الحرية الشخصية حق طبيعي وهي مصونة لا تمس»، ونصت المادة (39) من نفس الدستور: «للمنازل حرمة، وفيما عدا حالات الخطر والاستغاثة، لا يجوز دخولها، ولا تفتيشها، ولا مراقبتها، إلا في الأحوال المبينة في القانون وبأمر قضائي مسبب يحدد المكان والتوقيت والغرض، ويجب تنبيه من في المنازل قبل دخولها أو تفتيشها».

ونصت الفقرة الأولى من المادة (54) من الباب الثالث– الحقوق والحريات والواجبات العامة من الدستور المصري الصادر 2014 أن: «الحرية الشخصية حق طبيعي، وهي مصونة لا تمس، وفيما عدا حالة التلبس، لا يجوز القبض على أحد وتفتيشه، أو حبسه، أو تقييد حريته بأي قيد إلا بأمر قضائي مسبب يستلزمه التحقيق...».

(1) عطل العمل به في 2013/7/3 راجع في ذلك للمؤلف: الإجراءات التشريعية والقضائية والإدارية لمرحلة العدالة الانتقالية، مجلة كلية الحقوق – جامعة الإسكندرية، العدد (3) لسنة 2014 .

ونصت المادة (58) من نفس الدستور أن: «للمنازل حرمة، وفيما عدا حالات الخطر، أو الاستغاثة لا يجوز دخولها، ولا تفتيشها، ولا مراقبتها أو التنصت عليها إلا بأمر قضائي مسبب، يحدد المكان، والتوقيت، والغرض منه، وذلك كله في الأحوال المبينة في القانون، وبالكيفية التي ينص عليها ويجب تنبيه من في المنازل عند دخولها أو تفتيشها، وإطلاعهم على الأمر الصادر في هذا الشأن» .

ميزت – النصوص (44) من دستور مصر 1971، و(39) من دستور مصر 2012 والمادة (58) من دستور مصر 2014 – تلك النصوص بين دخول المساكن، وبين تفتيشها إلا أنه جميعها في ضمانات واحدة متى كانا يمثلان انتهاكاً لحرمة المساكن، وبين تفتيشها إلا أنه جمعها في ضمانات واحدة متى كانا يمثلان انتهاكاً لحرمة المساكن التي قدستها الدساتير .

ويبين من المقابلة بين تلك المواد أن المشرع الدستوري قد فرق في الحكم بين تفتيش الأشخاص، وتفتيش المساكن فيما يتعلق بضرورة أن يتم التفتيش في الحالتين بأمر قضائي ممن له سلطة التحقيق، أو من القاضي المختص كضمانة أساسية لحصول التفتيش تحت إشراف مسبق من القضاء. فقد استثنت المادة (41) من الدستور المصري 1971 والمادة (54) من دستور 2014 من هذه الضمانة حالة التلبس بالجريمة، بالنسبة للقبض على الشخص، وتفتيشه فضلاً عن عدم اشتراطها تسبيب أمر القاضي المختص أو النيابة العامة بالتفتيش، في حين أن المادة (44) من الدستور لم تستثن حالة التلبس من ضرورة صدور أمر قضائي مسبب ممن له سلطة التحقيق، أو من القاضي المختص بتفتيش المسكن، سواء قام به الآمر بنفسه، أم إذن لمأمور الضبط القضائي بإجرائه، فجاء نص المادة (44) من الدستور المشار إليه عاماً مطلقاً لم يرد عليه ما يخصصه أو يقيده، مما مؤداه : أن النص الدستوري يستلزم في جميع أحوال تفتيش المساكن صدور الأمر القضائي المسبب وذلك صوناً لحرمة المسكن التي تنبثق من الحرية الشخصية التي تتعلق بكيان الفرد وحياته الخاصة ومسكنه الذي يأوي إليه، وهو موضع سره وسكينته، ولذلك حرص الدستور – في الظروف التي صدر فيها – على التأكيد على عدم انتهاك حرمة المسكن سواء بدخوله أو بتفتيشه ما لم يصدر أمر قضائي مسبب دون أن يستثنى من ذلك حالة التلبس بالجريمة التي لا

تجيز – وفقاً للمادة (41) من دستور 1961 والمادة (54) من دستور 2014 سوى القبض على الشخص وتفتيشه أينما وجد[1].

ولحرص دستور 2014 وصوناً لحرمة المسكن نصت المادة (58) على أن يكون الأمر القضائي المسبب، يحدد المكان، والتوقيت والغرض منه وذلك كله في الأحوال المبينة في القانون وبالكيفية التي ينص عليها، ويجب تنبيه من في المنازل عند دخولها أو تفتيشها، أو إطلاعهم على الأمر الصادر في هذا الشأن.

اجتهادات تأصيل حقوق الإنسان في عصر التقانات الإلكترونية الرقمية :

أشارت الوثائق الصادرة عن دورتي القمة العالمية لمجتمع المعلومات التي نظمتها الأمم المتحدة في كل من جنيف عام 2003 م، وتونس عام 2005 م، إلى قضية حقوق الإنسان في عصر التقانات الإلكترونية الرقمية ومجتمع المعلومات والمجتمع الافتراضي وشبكات التواصل الاجتماعي.

ومجتمع المعلومات: هو المجتمع الذي يحسن استخدام إمكانيات تكنولوجيا المعلومات والاتصالات المتطورة لتحسين نوعية حياته من أجل الإنماء والتطور والتقدم في أمان وسلام مع احترام حقوق الآخر والمحافظة على النظام العام : الأمن العام والسكينة العامة، والصحة العامة، والآداب العامة والبيئة[2].

أما المجتمع الافتراضي: فهو مجموعة من الناس يشتركون في تفاعل اجتماعي، وبعض الروابط المشتركة بينهم ويعيشون في مكان ولبعض الوقت مستخدمين التقانات الإلكترونية الرقمية في اتصالاتهم[3] والتي ترتب عليها ظهور شبكات التواصل الاجتماعي التي تعتبر تجسيد للمدى الكبير الذي وصلت إليه شبكة الإنترنت وخدماتها وأدواتها وتقاناتها في العمل كقنوات للتواصل والتفاعل وتبادل

(1) مجموعة المبادئ التي قررتها المحكمة العليا والمحكمة الدستورية العليا في أربعين عاماً 1969–2009 مرجع سبق ذكره ، ص386–385 وانظر إشارته إلى القضية رقم 5 لسنة 4 قضائية «دستورية» بجلسة 2/6/1984 ج(3) « دستورية « ص67 .

(2) للمؤلف: التحري في جرائم مجتمع المعلومات والمجتمع الافتراضي، دار النهضة العربية، مصر 1432–2011، ص23

(3) انطلق موقع «ماي سبيس» عام 2003، وموقع فيس بوك فبراير 2004، وموقع «يوتيوب» فبراير 2005، المدونات فبراير عام 2004 .

للمعلومات بين مستخدميها اجتماعياً، وتعبر عن سلسلة مواقع على الإنترنت يشترك فيها الملايين من الأشخاص ويستخدمونها كقنوات تواصل وتفاعل اجتماعي فيما بينهم، بحيث بات الموقع أشبه بشبكة توفر روابط وقنوات تواصل بلا حصر بين مستخدميها، وخلال السنوات الأخيرة أصبحت هذه الشبكات واحدة من أسرع استخدامات الإنترنت انتشاراً .

وقد أصبحت مواقع مثل: «ماي سبيس» www.myspace.com«فيس بوك» www.facebook.com، «هاي فايف» www.hi5.com «وفريند ستر» www.frinendster.com، «أوركت» www.orkut.com، «بلوجر» www.blogger.com «يوتيوب» www.yotube.com،«ويكبيديا» www.wikibedia.com، تمثل هذا الاتجاه في شبكات الإنترنت ذات التوجه الاجتماعي، أو ما يسمى بظاهرة «التشبيك الاجتماعي، ومن أول نظرة تبدو هذه المواقع وكأنها مجرد مدونات أثرياء، ولكن الأدوات التي تجعلها أبسط تتيح إمكانية استخدامها لإرسال نصوص فوتوغرافية وموسيقى وعروض مصورة (مقاطع فيديو) أعدت في المنزل، وقد حولت هذه الأدوات شبكات الاتصال الاجتماعي إلى ظاهرة على الإنترنت. فهذه المواقع ليست مجرد مواقع إلكترونية عادية بل هي مجتمعات [1] ديناميكية عبر الإنترنت تتشكل فيها مجموعات حيوية وممتدة قائمة على التفاعل .

وبهذه المواقع تحولت شبكة الإنترنت من شبكة من المواقع الإلكترونية التي تسمح للمؤسسات بعرض المعلومات إلى منصة معلوماتية في ذاتها سواء كان الشخص يبحث عن التطوير أو المشاطرة أو التواصل الاجتماعي. تقوم الشبكة الإلكترونية الجديدة في شكل أساسي على المشاركة وليست تلقى المعلومات بصورة سلبية، ولم تعد الشبكة الإلكترونية تقتصر على البحث الجامد أو القراءة أو الإنصات أو المشاهدة من دون أية مساهمة من الفرد، إنها تقوم على العلاقات الندية: المشاطرة والتواصل الاجتماعي والتعاون، والأهم من ذلك كله الابتكار ضمن متحدات لا تربط بينها صلات قوية [2].

(1) الشرق الأوسط، مواقع التشبيك الاجتماعي الإلكتروني يجتذب الملايين 24/10/2006 ، ص10 .

(2) القبس، «ويكينو ميكس» بقلم دون تابسكوت وانطواني وِيليامز (منشورات بنغوانه 8 مايو 2008 ص65 ، وهو عرض لكتاب بعنوان wikinomics وفيه يتبنى المؤلفان علماً جديداً من التعاون يسميانه «ويكينو مكس» (كلمة تجمع بين ، «ويكي» وهو برنامج إلكتروني يسمح للأشخاص الذين يزورون المواقع الإلكترونية بتعديل صفحاتها و«أيكونو ميكس أي اقتصادي» .

يضفي جيل الشباب الجديد على أماكن تواجدهم أخلاقيات جديدة قوامها الانفتاح والمشاركة والتفاعل، ويرتكز هذا الجيل على بناء الشبكات الاجتماعية[1] عبر تلك المواقع وأصبحت جزءاً من النسيج الاجتماعي[2].

يوجد العديد من الاجتهادات التي تحاول تأصيل وتحديد حقوق الإنسان في عصر التقانات الإلكترونية الرقمية في نصوص واضحة وبتقصي هذا الموضوع عبر الإنترنت نجد الكثير من البحوث والتقارير التي تتحدث عن حقوق الإنسان الرقمي وبعضها يركز على الموضوعات ذات العلاقة بالإنترنت وتداول المعلومات داخلها وأحياناً خارجها، وبعض آخر يركز على الموضوعات ذات الصلة بقدرة الإنسان على الاتصال والتواصل مع البيئة المحيطة به عموماً من خلال خطوط وشبكات الاتصالات، ومن هذه الوثائق:

– تلك التي تحمل عنوان «الديمقراطية الرقمية» والمنشورة على موقع مركز الديمقراطية الرقمية على الإنترنت، وتورد عشرة حقوق للإنسان في عصر التقانات الإلكترونية الرقمية وهي:

1. حق الاتصال المفتوح بالإنترنت.
2. الحق في اتصالات غير مقيدة .

---

(1) تتنوع شبكات التواصل الاجتماعي عبر شبكة الإنترنت إلى ثلاثة أنواع :
النوع الأول – يطلق عليه شبكات إعادة شمل الأصدقاء Reuniting وهي المواقع التي تقوم بإعادة العلاقات بين الأشخاص الذين كانون يعرفون بعضهم من قبل ، ولكن مع مرور الزمن لم تعد هذه الصلة موجودة. عندما يقوم مستخدم الإنترنت بالدخول على أحد هذه المواقع فيطلب منه أن يدخل معلومات عنه Profile مثل الاسم وتاريخ الميلاد والمدرسة والجامعة التي تلقى تعليمه بها وأية معلومات أخرى تفيد الآخرين في التعرف عليه ، ومن أشهر هذه النوعية من الشبكات الاجتماعي موقع الفيس بوك Facebook.
النوع الثاني– هو أصدقاء الأصدقاء Friend of a friend وهي مصممة لكي يقوم المستخدمون بالتعرف على أصدقاء جدد لم يعرفونهم من قبل ، ولكن لديهم أصدقاء مشتركين. نظرية هذه المواقع أن هناك احتمالا كبيراً أن يكون صديق صديقك هو صديق جديد لك.
النوع الثالث– هو شبكات الاهتمامات المشتركة، وهي مخصصة للمشتركين الذين لديهم اهتمامات مشتركة ولا يعرفون بعضهم البعض من قبل ولا تربطهم صداقة، فإذا كنت تهتم بتبادل الصور على سبيل المثال فسوف تجد الشبكة الاجتماعية Flickr هو الموقع المناسب لك، أما إذا كنت مهتماً بعلاقات العمل والتجارة فإن الشبكة الاجتماعية Linkedin هي الأنسب لك . راجع في ذلك :عمر سامي : مفاهيم أساسية: الشبكات الاجتماعية ، الأهرام ، مصر ، العدد 44745 ، 9/6/2009 ص20.

(2) محمد أبو زيد ، «فيس بوك» وكالة أنباء دولية .. أنت ، الشرق الأوسط 9/9/2007 ، ص9 .

3. الحق في شبكات مجتمعية قوية.
4. الحق في حصته بالتليفزيون الرقمي.
5. الحق في الخصوصية عبر الإنترنت.
6. الحق في الترددات اللاسلكية الشائعة، مثل واي فاي.
7. الحق في أجهزة ومعدات خالية من القيود.
8. الحق في برمجيات متحررة من القيود.
9. الحق في مواقع عامة على الويب.
10. الحق في خدمة رقمية عامة.

تميل هذه الحقوق العشر إلى قضايا تتعلق بالإنترنت وتداول المعلومات وهو وضع يختلف إلى حد مع الطريقة التي عالجت بها وثائق أخرى هذه الحقوق وتنتمي للمسار نفسه، حيث عالجت قضايا حرية التعبير والحريات العامة بأسلوب أكثر وضوحاً ومباشرة، كما اعتبرت أن الاستفادة من تقانات المعلومات في التعليم والتعلم المستمر يعد حقاً من حقوق الإنسان، ومن أبرز الوثائق الأخرى في هذا الصدد وثيقة حقوق الإنسان في مجتمع المعلومات التي ناقشت القمة العالمية للمعلومات وكتبتها ديبورا هيورلي، وحددت حقوق الإنسان الرقمية في (7) حقوق وهي:

1. الحق في الخصوصية، والأمن.
2. الحق في حرية التنقل.
3. الحق في حرية التجمع.
4. الحق في الحصول والوصول إلى التكنولوجيا.
5. الحق في حرية التعبير والوصول للمعلومات.
6. حق الملكية الفكرية.
7. الحق في التعليم.

وهناك كذلك وثيقة حقوق الإنسان في مجتمع المعلومات الصادرة في سبتمبر 2005 عن اجتماعات المجلس الأوروبي التي انعقدت بستراسبورج بفرنسا وتحدثت عن سبعة حقوق لم تختلف كثيراً عن الواردة بوثيقة القمة العالمية لمجتمع المعلومات وهي:

1. الحق في حرية التجمع.
2. الحق في انتخابات حرة.
3. الحق في حماية الملكية الفكرية.
4. الحق في حرية التجريب المجاني لأدوات التكنولوجيا وأنه لا عقوبة بلا قانون.
5. الحق في التعليم وأهمية تشجيع الوصول لتكنولوجيا المعلومات التي يتعين أن تستخدم بلا تمييز.
6. الحق في احترام الحياة الخاصة.
7. الحق في حرية التعبير والاتصال[1].

(1) جمال محمد غيطاس، حقوق الإنسان في العصر الرقمي، ومجتمع المعلومات، الجزء (2) صفحة لغة العصر، الأهرام، 27/7/2006، ص16.

المبحث الثاني

مخاطر التقانات الإلكترونية

الرقمية التي تهدد الحق في الخصوصية

نتناول تعريف المخاطر والتقانات ومكونات بيئة التقانات الإلكترونية الرقمية وشبكات المعلومات والخصوصية، والمخاطر التي تهدد الحق في الخصوصية.

تعريفات :

يقصد بالمخاطر مواضع الأخطار أي المهالك[1]. ويقصد بالتقانات الطرق التي يستخدمها الناس في اختراعاتهم واكتشافاتهم لتلبية حاجاتهم وإشباع رغباتهم ويسميها البعض التكنولوجيا، فالتقنية تعني استخدام الأدوات، والآلات والمواد والأساليب ومصادر الطاقة لكي تجعل العمل ميسوراً وأكثر إنتاجية[2]. ولذلك تغيرت الثقافات مثل ثقافة العمل والتعليم والتصويت والأمن. فعلى سبيل المثال غيرت التقنية ثقافة العمل فأصبح العمل من المنزل عبر أجهزة الاتصال الحديثة حقيقة وأصبح الموظفون يعملون في منازلهم وحتى في المنزل لا يعد الموظفين مضطرين للبقاء وراء المكتب، فيفضل نظام واي فاي للاتصال الذي يمكنك من الدخول إلى شبكة الشركة على جهاز الكمبيوتر المحمول، والعمل من أي مكان في المنزل. وهناك – أيضاً – برنامج جديد وكاميرا فيديو جديدة. تمكن رؤساء العمل من مراقبة موظفيهم أينما كانوا[3].

كما ميزت التقنية ثقافة التعليم، فأصبح التعليم عبر أجهزة الاتصال دون التوجه إلى المؤسسات التعليمية وهو ما يطلق عليه التعلم عن بُعد .

---

(1) المعجم الوجيز، مجمع اللغة العربية، جمهورية مصر العربية، طبعة خاصة بوزارة التربية التعليم، 1414هـ، 1993م، ص202 .

(2) الموسوعة العربية العالمية، 1416هـ1996–م، الجزء السابع تحت حرف (ت)، ص68–67 .

(3) القبس، ثورة في نظام العمل، الكويت 16/9/2003، ص28 .

وأيضاً ثقافة التصويت في العملية السياسية، فأصبح التصويت يتم عبر برامج خاصة في تقنية الاتصال وشبكات الإنترنت .

وعلى ذلك تنوعت التقانات ونتج عنها في مجال الاتصال شبكات مجتمع المعلومات والمجتمع الافتراضي بعد ظهور شبكة الإنترنت وما تقدمه من خدمات .

مكونات بيئة التقانات الإلكترونية الرقمية وشبكات المعلومات[1] :

تعني التقنية – كما سبق وأن أوضحنا – استخدام الأدوات والمواد والأساليب ومصادر الطاقة لكي تجعل العمل ميسوراً وأكثر إنتاجية، وهي تشمل الأجهزة والبرامج التي تنظمها نظم لكي يعملان بفاعلية وكفاية. فالأجهزة Hardware مصطلح يعبر عن المكونات الأساسية المادية للحاسب، ونظم مكونات الحاسب وتشمل : المدخلات، والتشغيل، والتخزين، والمخرجات .

وتنقسم مكونات الحاسب الآلي الرقمي إلى أجهزة Hardware ونظم برامج Software .

أما البرامج Software : فهي مصطلح يعبر عن مجموعة منظمة من التعليمات للحاسب الآلي الرقمي تمكن من التحكم فيه واستخدامه لإنتاج معلومات وعمل مفيدة.

وشبكات المعلومات ثلاث أنواع[2]: هي شبكة الإنترنت والإنترانت والإكسترانت يستخدمها الأشخاص (طبيعيون أو اعتباريون) من خلال الخدمات التي تقدمها بصفتها أداة اتصال في تبادل المعلومات .

الإنترنت Internet :

هي مجموعة متصلة من الحاسبات الآلية الرقمية يطلق عليها اصطلاح الحاسبات المضيفة. وتستخدم في جميع المجالات والتخصصات فهي تستخدم في مجالات الثقافة والتربية والتعليم والاتصال والإعلام والأمن ومكافحة الجريمة وغيرها من مناحي الحياة الإنسانية.

(1) لمزيد من التفصيلات راجع: للمؤلف: التحري في جرائم مجتمع المعلومات والمجتمع الافتراضي، دار النهضة العربية، مصر – القاهرة، الطبعة الأولى ، 1432هـ– 2011 ، ص50–102 .

(2) للمؤلف، المرجع السابق، ص103–158 .

الإنترانت Intranet:

هي عبارة عن شبكة حاسوب آلي رقمي (كمبيوتر) خاصة بأية مؤسسة (مصارف مثلاً) تستخدم القواعد التي بنى عليه الإنترنت. تمكن الانترانت الأشخاص العاملين في أية مؤسسة من الاتصال بعضهم ببعض. والوصول إلى المعلومات بطريقة أسرع وأفضل وأكثر كفاءة وأقل تكلفة من الأساليب التقليدية المعتادة. فمن خلال الإنترانت يمكن إنجاز الاجتماعات وتحضير الرسائل والمذكرات وإرسال البريد وإنجاز الاجتماعات.

الإكسترانت Extranet:

هي عبارة عن شبكات حاسوب آلي رقمي (كمبيوتر) خاصة بعدة مؤسسات (مجموعة المصارف والبنوك) تستخدم القواعد التي بنى عليه الإنترنت. تمكن الإكسترانت الأشخاص العاملين والمتعاملين مع تلك المؤسسات من الاتصال والوصول إلى المعلومات. وتعتبر الإكسترانت نسخة مصغرة من الإنترنت تعمل داخل عدة مؤسسات ولا يمكن لأحد الوصول إليها إلا من يعمل ويتعامل مع المؤسسة ولديه كلمة السر للدخول إليها.

المقصود بالخصوصية:

يختلف تعريف الخصوصية من بيئة إلى أخرى ولكن الصفة المشتركة في التعريفات أن الخصوصية إحدى حقوق الإنسان ولكنها تعتمد في الأساس على البيئة التي ينشأ فيها هذا الإنسان، ويمكن تقسيم الخصوصية إلى عدة مفاهيم ترتبط ببعضها وهي[1]:

- خصوصية الاتصالات والتي تغطي سرية خصوصية المراسلات الهاتفية والبريد الإلكتروني وغيرها من الاتصالات.

(1) أسامة عبدالله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة العربية، 1994.

– الخصوصية المتعلقة بالقواعد المنظمة للدخول إلى المنازل وبيئة العمل أو الأماكن العامة والتي تتضمن التفتيش والرقابة الإلكترونية .

– الخصوصية المتعلقة بالقواعد التي تحكم جميع إدارات البيانات الخاصة كمعلومات بطاقات الهوية والمعلومات المالية.

– الخصوصية الجسدية وهي تلك المتعلقة بالحماية الجسدية للأفراد ضد أي إجراءات ماسة كفحص المخدرات في الإنسان.

عرف روجر كلارك[1] الخصوصية بأنها « قدرة الأشخاص على المحافظة على مساحتهم الشخصية في مأمن من التدخل من قبل منشآت أو أشخاص آخرين». ثم قام بتحديد أبعاد الخصوصية وهي:

خصوصية البيانات الشخصية: وتعين عدم توفر البيانات الخاصة عن الأشخاص تلقائياً لغيرهم من الأفراد أو المنظمات. وهذا ما يعرف «بخصوصية المعلومات أو خصوصية البيانات». وعرفها روجر كلارك «بأنها رغبة الشخص بالتحكم، أو على الأقل التأثير بشكل كبير في كيفية التعامل مع بياناته الشخصية».

خصوصية الاتصالات الشخصية: وهي قدرة الأشخاص على الاتصال فيما بينهم دون مراقبة روتينية من قبل أشخاص آخرين أو منظمات وهو ما يعرف «باعتراض الخصوصية».

خصوصية السلوك الشخصي: ويعرف بوسائل الخصوصية للشخص للتعبير بشأن الأنشطة السياسية والممارسة الدينية سواء في الحياة الخاصة أو الأماكن العامة.

خصوصية الشخص: المعنية بسلامة الفرد في جسده، مثل قضايا التطعيم أو نقل الدم دون الحصول على موافقة الشخص، أو الإجبار على تقديم عينات من سوائل جسده أو أنسجته.

---

(1) استشاري وخبير في خصوصية البيانات والأعمال الإلكترونية، راجع في ذلك: منى تركي الموسوى، وجان سيريل فضل الله : الخصوصية المعلوماتية وأهميتها ومخاطر التقانات الحديثة عليها، مجلة كلية بغداد للعلوم الاقتصادية، العدد الخاص بمؤتمر الكلية، 2013 ، ص203، وانظر إشارتهما إلى Roger Clarke، « personalia page 2008 ».

المخاطر التي تهدد الحق في الخصوصية:

نتناول مواضع مخاطر التقانات الإلكترونية الرقمية التي تهدد الحق في الخصوصية ومن أبرزها مخاطر البرامج الإلكترونية المتطفلة الضارة ومخترقي الأجهزة، ومخاطر أجهزة التقانات الإلكترونية الرقمية وشبكات المعلومات والتواصل الاجتماعي.

مخاطر البرامج الإلكترونية المتطفلة الضارة[1]:

يطلق المختصون الكترونياً على البرامج الإلكترونية المتطفلة الضارة «الشفرة الخبيثة» وهو « برنامج يوضع عن قصد في نظام لتحقيق هدف غير مرخص به ».

توجد أربعة أنواع رئيسية للبرامج الإلكترونية المتطفلة الضارة:

1. الفيروسات الإلكترونية.
2. حصان طروادة الإلكتروني.
3. الدودة الإلكترونية.
4. البريد الإلكتروني غير المرغوب فيه «سبام» Spam.

1- الفيروس الإلكتروني:

هو برنامج مصمم عمداً ليقترن ببرنامج آخر بحيث يعمل الفيروس عندما يعمل ذلك البرنامج، ومن ثم يعيد إنتاج نفسه باقترانه ببرامج أخرى، وقد يغير الفيروس نفسه عند إعادة الإنتاج فيظهر كنسخة معدلة من النسخة التي قبلها.

ففيروس الحاسب الآلي الرقمي هو برنامج يصمم لإحداث إرباك وخراب في برمجيات الحاسوب، كما أن باستطاعته أن يتكاثر ويعيد إنتاج نفسه باستعمال وحدات وتجهيزات وبرامج الحاسوب بدون علم صاحب جهاز الحاسوب أو مستعمل شبكة الحاسوب ويزداد تأثيرها يوماً بعد يوم[2].

---

(1) لمزيد من المعرفة راجع للمؤلف: السيرة الذاتية للفيروسات الإلكترونية، دار الكتب القانونية، مصر – القاهرة، الطبعة الأولى، 1429هـ 2008–م .

(2) حسني مرتضى، «التطور التاريخي للفيروسات الكمبيوترية ومسألة حماية البيانات» مجلة الكمبيوتر والاتصالات والإلكترونيات ، المجلد 17 ، العدد (9) ، نوفمبر 2000 ، ص53 .

وللوقاية منه توضع تقانات «جدران النار» لمنع أو تقييد الدخول الخارجي إلى الحاسب الآلي الرقمي الخاص أو إلى الشبكة.

2- حصان طروادة الإلكتروني:

هو برنامج مصمم لإظهار غير ما يخفى، فهو خادع يخفى ظاهره غرضاً غير مشروع يضمره، إذ يظهر كبرنامج عادي يؤدي بعض المهام المفيدة لمستخدمه، بينما يكون موجوداً بطريقة خفية داخله بعض الأوامر أو التعليمات التي تؤدي عند تشغيلها مهاماً ضارة غير متوقعة تمثل أغراضه التي يضمرها[1].

الدودة الإلكترونية:

هي برنامج صمم خصيصاً لنشر نفسه من حاسب آلي رقمي إلى حاسب آخر على الشبكة وليس لديه اهتمام بنشر نفسه في أكثر من ملف رقمي على نفس الجهاز بل إن إتمامه هو إصابة أكبر عدد من الحاسبات الرقمية. فالدودة الإلكترونية تتكون لتتكاثر وتنطلق لتنشر أكثر، فهدفها استنساخ نفسها أي تتكاثر وتزرع نفسها داخل الذاكرة النشطة، وتبدأ بمراقبة أي مسح بهدف العثور على مواطن الضعف فيها، ثم نقل نفسها إلى الحاسبات الآلية الرقمية الأخرى .

وعلى ذلك «فالدودة Worm» عبارة عن برنامج ينقل نفسه من حاسب إلى حاسب آخر عبر الشبكة، ويزرع نفسه كملف مستقل على أقراص الحاسب المستهدف[2]. وإحدى الديدان التي استحقت النشر في الصحف (واليت) بدأها طالب في جامعة كورنيل Cornell University، انتقلت طولاً وعرضاً في البلاد من خلال شبكة البريد الإلكتروني، مما نتج عنه إغلاق الآلاف من الحاسبات. وقد تم تصميم برنامج الدودة في الشبكة وتكاثرت دون تحكم في تكاثرها، مما أثقل ذاكرة الحاسبات التي أصيبت بها حتى عجزت كلية عن العمل.

---

(1) مهندس جبر مراد، الفيروسات التي تغزو جهازك متعددة الأنواع ، الرأي العام ، الكويت ، 9/ 11/ 2001 ، ص11.

(2) كابرون: الحاسبات والاتصالات والإنترنت، ترجمة د.م سرور على إبراهيم سرور ، (دار المريخ ، الرياض) المملكة العربية السعودية ، 1424هـ - 2003م ، ص698.

4- البريد الإلكتروني غير المرغوب فيه «Spam»- البريد العشوائي:

هي رسائل إلكترونية دعائية ترسل عبر البريد الإلكتروني (E-mail)[1] ومن أكثر سلبياته إزعاجاً، هو وصول بريد الكتروني غير مرغوب فيه إلى بريد المستخدم، وهو ما يشبه في إزعاجه الفاكس غير المرغوب فيه والذي لا فائدة منه سوى القضاء على رزمة أوراق الفاكس، كما يشبه في بعض جوانبه المعاكسات الهاتفية. ويسمى هذا النوع من الإرساليات «Spam» ويمكن تعريبه (البريد الإقحامي) أو (البريد التطفلي) .

لكن النقطة التي يتفوق فيها البريد الإلكتروني على ما سواه من الإزعاجات هو التكلفة المنعدمة تقريباً على مرسليه، أما التكلفة الحقيقة فتقع على كاهل المرسل إليه. حيث يستطيع المرسل كتابة تحتوي ثلثاً هذه الرسائل على معلومات غير صحيحة بشكل أو بآخر، وأن 44% منها احتوت على عناوين زائفة للرد لإخفاء هوية مرسل الرسالة، أو استخدمت موضوعاً مضللاً لخداع مستقبل الرسالة حتى يفتحها .

ويرجح أن 66% من إجمالي رسائل البريد الإلكتروني العشوائية المفحوصة قد انتهكت القوانين الاتحادية عن طريق نوع من الخداع في ممارسات الأعمال[2].

مخاطر مخترقي الأجهزة «Hackers» [3]:

بسبب انتشار برامج القرصنة ووجودها في الكثير من المواقع، أصبح من الممكن اختراق أي جهاز حاسوب وبدون عناء فور إنزال أحد برامج القرصنة. والمقصود بالقرصنة هو سرقة المعلومات من برامج وبيانات بصورة غير شرعية وهي

(1) ظهر منذ 1998 مع تصاعد نشاط التجارة الإلكترونية، عبر شبكة الإنترنت ، حيث بدأت الشركات في محاولة جذب مزيد من المشترين لمنتجاتها عن طريق شبكة الإنترنت بإستحدام البريد الإلكتروني (E-mail) في الدعاية لمنتجاتها وازدادت الرسائل الإلكترونية يوماً بعد يوم حتى أصبحت تشكل عبئاً (بل كابوسا) على كل من يستخدم هذه الخدمة التي لا يمكن الاستغناء عنها ، لأنها تصل إلى المستخدم دون أن يطلبها ، وتستغرق منه وقتاً طويلاً لكي يقوم بقراءة عنوانها على الأقل لكي يتعرف على محتواها ، ثم يقوم بإلغاء الرسالة ، وإذا افترضنا أن هذه العملية تستغرق 10 دقائق فقط يومياً من مستخدمي شبكة الإنترنت الذين تجاوز عددهم 600 مليون شخص فيمكن أن تعرف حجم الخسائر التي تسببها هذه الرسائل بمجتمع شبكة الإنترنت .

(2) الأهرام : «35% من رسائل البريد الإلكتروني غير حقيقية « ، 2003/6/29 ، مصر- القاهرة ، مؤسسة الأهرام، ص25 .

(3) (آخر زيادة للموقع 2014/10/14) www.Ao-ACADEMY.org/Docs .

مخزنة في دائرة الحاسوب، أو نسخ برامج معلوماتية بصورة غير قانونية وتتم هذه العملية إما بالحصول على كلمة السر أو بوساطة التقاط موجات الكهرومغناطيسية بحاسوب خاص ويمكن إجراء عملية القرصنة بواسطة رشوة العاملين في المنظمات المنافسة. أما عن الهدف في عمليات القرصنة فهو سرقة الأسرار أو المعلومات التجارية أو التسويقية أو التعرف على حسابات المنظمات أو أحياناً بهدف التلاعب بقيود المصارف أو المؤسسات المالية بهدف سرقة الأموال أو يكون الهدف الكشف عن أسرار صناعية (تصاميم منتجات) بهدف إعادة تصنيعها دون إجازة قانونية أو لأهداف سياسية وعسكرية من أجل الحصول على الملفات والخطط السرية العسكرية أو الحكومية. والأمثلة على حالات القرصنة عديدة، فقد قامت الشركات الصينية بنقل أسرار تكنولوجيا صناعية من الولايات المتحدة وكندا مستخدمة الحاسوب ومن ثم القيام بإنتاج سلع على ضوء ذلك وتصديرها لهاتين الدولتين لتباع في أسواقها بثلث الأسعار الأصلية، ونفس الشيء قامت به شركة متسوبيشي لبناء السفن والصناعات التقليدية حيث استخدمت سماسرة للقيام بعملية التجسس الصناعي .

مخاطر أجهزة التقانات الإلكترونية الرقمية وشبكات المعلومات والتواصل الاجتماعي[1]:

مكنت التقانات الإلكترونية الرقمية من تخزين واسترجاع وتحليل كميات هائلة من البيانات الشخصية التي يتم تجميعها من قبل المؤسسات والدوائر والوكالات الحكومية ومن قبل الشركات الخاصة، ويعود الفضل في هذا إلى مقدرة الحاسبات الإلكترونية الرقمية الرخيصة، وأكثر من هذا فإنه يمكن مقارنة المعلومات المخزونة في ملف بمعلومات في قاعدة بيانات أخرى، ويمكن نقلها عبر البلد في فمتو ثانية وبتكاليف منخفضة نسبياً، إن هذا بوضوح يكشف إلى أي مدى يمكن أن يكون تهديد الخصوصية.

وتتزايد مخاطر التقانات الإلكترونية الرقمية الحديثة على حماية الخصوصية، كتقانات رقابة (كاميرات الفيديو) وبطاقات الهوية الإلكترونية، وقواعد البيانات

(1) (آخر زيادة للموقع 2014/10/14) www.Ao-ACADEMY.org/Docs .

الشخصية، ووسائل اعتراض ورقابة البريد والاتصالات، ورقابة بيئة العمل وغيرها، وإذا كانت الجهود الدولية والاتجاه نحو الحماية التشريعية للحياة الخاصة عموماً، وحمايتها من مخاطر استخدام الحواسب وشبكاتها على نحو خاص، مثل المسلك الصائب في مواجهة الأثر السلبي للتقنية على الحياة الخاصة فإن هذا المسلك قد رافقه اتجاه متشائم لاستخدام التقنية في معالجة البيانات الشخصية. فالتوسع الهائل لاستخدام الحاسبات الإلكترونية قد أثار المخاوف من إمكانات انتهاك الحياة الخاصة المتعلقة بجميع جوانب حياة الفرد الشخصية كالوضع الصحي، والأنشطة الاجتماعية والمالية والسلوك والآراء السياسية وغيرها عن طريق جمعها وتخزينها لفترة غير محددة، كما يمكن الرجوع إليها جميعاً بمنتهى السرعة والسهولة، ومع الزيادة في تدفق المعلومات التي تحدثها الحواسيب الإلكترونية الرقمية، تضعف قدرة الفرد على التحكم في تدفق المعلومات عنه. إن هذه النظرة كما يظهر لنا، نظرة متشائمة من شيوع استخدام الحاسبات الإلكترونية الرقمية أثرها على تهديد الخصوصية، وهي وإن كانت نظرة تبدو مبالغاً فيها، إلا أنها تعكس حجم التخوف من الاستخدام غير المشروع للتقانات وتحديداً الحواسيب الإلكترونية الرقمية وشبكاتها، في كل ما من شأنه تهديد الحق في الحياة الخاصة، ويمكننا فيما يلي إجمال المعالم الرئيسة لمخاطر الحاسبات الإلكترونية الرقمية وشبكاتها على الحق في الحياة الخاصة بما يأتي :

1- تجمع الكثير من المؤسسات الكبرى والشركات الحكومية الخاصة عن الأفراد بيانات عديدة ومفصلة تتعلق بالوضع المادي أو الصحي أو التعليمي أو العائلي أو العادات الاجتماعية أو العمل .. الخ، وتستخدم الحاسبات الإلكترونية الرقمية وشبكاتها في تخزينها ومعالجتها وتحليلها والربط بينها واسترجاعها ومقارنتها ونقلها، وهو ما يجعل فرص الوصول إلى هذه البيانات على نحو غير مأذون به أو بطريق التحايل أكثر من ذي قبل، ويفتح مجالاً أوسع لإساءة استخدامها أو توجيهها توجيهاً منحرفاً أو خاطئاً أو مراقبة الأفراد وتعرية خصوصياتهم أو الحكم عليهم حكماً خفياً من واقع سجلات البيانات الشخصية المخزنة .. على سبيل المثال فإن حكومة الولايات المتحدة وفق دراسات 1990 جمعت

(4) بليون سجل مختلف حول الأمريكيين، بمعدل (17) بند لكل رجل وامرأة وطفل، ومصلحة الضريبة (IRS) في الولايات المتحدة تمتلك سجلات الضرائب لحوالي (100) مليون أمريكي على حواسيبها، وتمتلك الوكالة الفيدرالية – عدا البنتاجون– ثلاث شبكات اتصالات منفصلة تغطي كل الولايات المتحدة الأمريكية لنقل وتبادل المعلومات .

2– شيوع النقل الرقمي للبيانات سهل استراق السمع والتجسس الإلكتروني. ففي مجال نقل البيانات تتبدى المخاطر المهددة للخصوصية في عدم قدرة شبكات الاتصال على توفير الأمان المطلق أو الكامل لسرية ما ينقل عبرها من بيانات وإمكانية استخدام الشبكات في الحصول بصورة غير مشروعة، عن بعد على المعلومات. في الأعوام من 1993 وحتى 2000 نشط البيت الأبيض الأمريكي والهيئات المتخصصة التي أنشأت لهذا الغرض في توجيه جهات التقنية إلى العمل الجاد على خلق تقنيات أمان كافية للحفاظ على السرية والخصوصية وعلى الرغم من التقدم الكبير على هذا الصعيد إلا أن تقارير الخصوصية تشير إلى أنه ما تزال حياة الأفراد وأسرارهم في بيئة النقل الرقمي معرضة للاعتداء في ظل عدم تكامل حلقات الحماية القانونية والتنظيمية والتقنية .

وأصبح من الواضح أن حماية الخصوصية يتعين أن تمتد إلى الكمبيوترات الخاصة بسبب إطلاق الحواسيب الشخصية وأن يتم إحداث توازن ما بين الحق في الخصوصية أو الحق في الحياة الخاصة وبين الحق في الوصول إلى المعلومات هذا التغير في الواقع التقني انعكس على حقل الحماية القانونية في الخصوصية بأبعادها التنظيمية والمدنية والجزائية وبدأت تكثر الأحاديث بشأن دعاوى الاستخدام غير المشروع للمعلومات وللوثائق الشخصية، وظهرت أحداث شهيرة في حقل الاعتداء على البيانات الخاصة من بينها على سبيل المثال الحادثة التي حصلت في جنوب أفريقيا حيث أمكن للمعتدين الوصول إلى الأشرطة التي خزنت عليها المعلومات الخاصة بمصابي أمراض الإيدز وفحوصاتهم، وقد تم تسريب هذه المعلومات الخاصة والسرية إلى جهات عديدة. ومن الحوادث الشهيرة الأخرى حادثة حصلت عام 1989 عندما تمكن أحد كبار موظفي أحد البنوك السويسرية بمساعدة سلطات

الضرائب الفرنسية بأن سرب إليها شريطاً يحتوى على أرصدة الزبائن، وقد تكرر مثل هذا الحادث في ألمانيا أيضاً. وقد أظهرت القضايا التي حصلت ما بين عام –96 97 في الحقل المصرفي أن الوصول إلى البيانات الشخصية ارتبط في الغالب بأنشطة الابتزاز التي غالباً ما تتعلق بالتحايل على الضريبة من قبل زبائن البنوك. وفي عام 1986 اتهمت شركة IBM، وهي شركة أمريكية تعمل في مجال الحواسيب والبرامج، بأن نظام الأمن الذي تنتجه المسمى RACF يستخدم للرقابة على الموظفين داخل المنشآت، وفي عام 1994 أيضاً وفي ألمانياً أثير جدل واسع حول حق دائرة التأمينات الصحية بنقل البيانات إلى شركات خارجية، وشبيه بهذا الجدل مدى أحقية شركات تزويد الإنترنت والهواتف الكشف عن معلومات الزبائن لجهات أخرى .

إن هذه المخاطر أثارت وتثير مسألة الأهمية الاستثنائية للحماية القانونية – إلى جانب الحماية التقنية– للبيانات الشخصية، ومن العوامل الرئيسه، في الدفع نحو وجوب توفير حماية تشريعية وسن قوانين في هذا الحقل، إنه وقبل اختراع الكمبيوتر فإن حماية هؤلاء الأشخاص كانت تتم بواسطة النصوص الجنائية التي تحمي الأسرار التقليدية (كحماية الملفات الطبية أو الأسرار المهنية بين المحامي والموكل) وعلى الرغم من ذلك فإن هذه النصوص التقليدية لحماية شرف الإنسان وحياته الخاصة لا تغطي إلا جانباً من الحقوق الشخصية وبعيدة عن حمايته من مخاطر جمع وتخزين والوصول إلى ومقارنة واختيار وسيلة نقل المعلومات في بيئة التقانات الإلكترونية الرقمية.

هذه المخاطر الجديدة التي تستهدف الخصوصية دفعت العديد من الدول لوضع تشريعات ابتداء من السبعينات من القرن العشرين تتضمن قواعد إدارية ومدنية وجنائية من أجل حماية الخصوصية وتوصف بأنها تشريعات السرية وليس فقط مجرد تشريعات تحمي من أفعال مادية تطال الشرف والحياة الخاصة. كما أن هذه المخاطر، وما يتفرع عنها من مخاطر أخرى كتلك الناتجة عن معالجة البيانات في شبكات الحواسيب المربوطة ببعضها البعض والتي تتيح تبادل المعلومات بين المراكز المتباعدة والمختلفة من حيث أغراض تخزين البيانات بها كانت محل اهتمام دولي وإقليمي ووطني أفرز قواعد ومبادئ تتفق وحجم هذه المخاطر، كوجوب مراعاة الدقة

في جمع البيانات وكفالة صحتها وسلامتها واتخاذ تدابير أمنية لمعالجتها وتخزينها ونقلها، وإقرار مبدأ حق المشاركة الفردية في تعديل وتصحيح طلب إلغاء البيانات، ووجوب تحديد الغرض من حجمها ومدة استخدامها، وإقرار مبدأ مسؤولية القائمين على وظائف شبكات المعلومات والتواصل الاجتماعي لأي تجاوز أو مخالفة للمبادئ الموضوعية والشكلية في جمع ومعالجة وتخزين ونقل البيانات الشخصية.

الخاتمـة

نصل إلى ختام هذا البحث الذي يدور حول «مخاطر تهدد الحق في الخصوصية عبر التقانات الإلكترونية الرقمية» .

عرضنا في المبحث الأول – حقوق الإنسان في عصر التقانات الإلكترونية الرقمية. حيث درسنا الحقوق المتصلة بالحق في الخصوصية في هذا العصر من خلال الإعلان العالمي لحقوق الإنسان وتطبيقات ذلك في بعض الدساتير العربية والولايات المتحدة الأمريكية، ثم عرضنا لاجتهادات تأصيل حقوق الإنسان في عصر التقانات الإلكترونية الرقمية ومجتمع المعلومات والمجتمع الافتراضي.

وخصصنا المبحث الثاني– لدراسة مخاطر التقانات الإلكترونية الرقمية التي تهدد الحق في الخصوصية من خلال تعريف المخاطر والتقانات ومكونات بيئة الخصوصية في عصر التقانات الإلكترونية الرقمية وشبكات المعلومات التي تهدد الخصوصية .

ووجدنا أن مواضع مخاطر التقانات الإلكترونية الرقمية التي تهدد الحق في الخصوصية تتركز في البرامج الإلكترونية المتطفلة الضارة وتشمل : الفيروسات الإلكترونية وحصان طروادة الإلكتروني والدودة الإلكترونية والبريد الإلكتروني غير المرغوب فيه. كما تتركز في أجهزة التقانات الإلكترونية الرقمية وشبكات المعلومات والتواصل الاجتماعي.

النتائج والتوصيات:

من النتائج السابقة نوصي بما يلي:

1. الإسراع بإصدار قانون يحمى سرية الخصوصية وتجريم الجرائم المعلوماتية من منطلق أنه لا جريمة ولا عقوبة إلا بنص.
2. اهتمام وسائل الإعلام المرئية والمسموعة والمقروءة بتنمية وعي وإدراك مستخدمي التقانات الإلكترونية الرقمية بحماية خصوصيتهم لأنهم خط الدفاع الأول.
3. عقد ندوات ودورات ومؤتمرات بصفة دورية حول هذا الموضوع لمناقشة أبعاده وتأثيره على المجتمع الوطني والإقليمي والدولي سواء المعلوماتي أو الافتراضي وشبكاته .

المراجع

أولاً- المراجع العربية :

- أسامة عبدالله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة العربية، 1994 .
- المعجم الوجيز، مجمع اللغة العربية، جمهورية مصر العربية، طبعة خاصة بوزارة التربية والتعليم، 1414هـ، 1993 .
- القبس، ثورة في نظام العمل، الكويت، 16/9/2003 .
- الموسوعة العربية العالمية، 1416هـ1996-م الجزء (7) .
- تقرير مفوضية الأمم المتحدة السامية لحقوق الإنسان المقدم إلى مجلس حقوق الإنسان في دورته السابعة والعشرين وإلى الجمعية العامة في دورتها التاسعة والستين والمعنون » الحق في الخصوصية في العصر الرقمي، 30/6/2014.
- مهندس جبر مراد، الفيروسات التي تغزو جهازك متعددة الأنواع، الرأي العام الكويتي، 9/11/2001 .
- حسني مرتضى، التطور التاريخي للفيروسات الكمبيوترية، ومسألة حماية البيانات، مجلة الكمبيوتر والاتصالات والإلكترونيات، المجلد (17) العدد (9)، نوفمبر 2000 .
- جمال محمد غيطاس، حقوق الإنسان في العصر الرقمي ومجتمع المعلومات، الجزء الثاني، صفحة لغة العصر، الأهرام، 25/7/2006 م .
- عمر سامي، مفاهيم أساسية الشبكات الاجتماعية، الأهرام، مصر – القاهرة، العدد 44745، 9/6/2009.
- عمر محمد بن يونس، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي، موسوعة التشريعات العربية، الطبعة الأولى، 2004-2005 .
- مجموعة المبادئ التي قررتها المحكمة العليا والمحكمة الدستورية العليا في أربعين عاماً 1969-2009م .

– محمد أبو زيد، «فيس بوك – وكالة أنباء دولية « أنت»، جريدة الشرق الأوسط 2007/9/9 .

– مصطفى محمد موسى،

- السيرة الذاتية للفيروسات الإلكترونية – دار الكتب القانونية– مصر– القاهرة، الطبعة الأولى، 1424هـ، 2008 .
- التحري في جرائم مجتمع المعلومات والمجتمع الافتراضي، دار النهضة مصر 1422هـ – 2011م .

– منى تركي الموسوي وجان سيريل فضل الله، الخصوصية المعلوماتية وأهميتها ومخاطر التقانات الحديثة عليها، مجلة كلية بغداد للعلوم الاقتصادية العدد الخاص بمؤتمر الكلية، 2013 م .

ثانيا– الدساتير:

– دساتير مصر : 1971 ، 2012 ، 2014 .

– دستور دولة الكويت 11 نوفمبر 1962 .

– دستور دولة الإمارات العربية المتحدة الصادر في 2 ديسمبر 1971 .

– دستور دولة قطر الصادر في 29 ابريل 2003 .

– دستور سلطنة عمان الصادر في نوفمبر 1996 .

– مشروع دستور تونس 1 يونيو 2013 .

– دستور الولايات المتحدة الأمريكية .

ثالثاً– مواقع إلكترونية :

– www.Ao-ACADEMY.org/Docs

– www.ohchr.org

الموضوع	الصفحة
المقدمة	
المبحث الأول – حقوق الإنسان في عصر التقانات الإلكترونية الرقمية	
الحقوق المتصلة بالحق في الخصوصية	
اجتهادات تأصيل حقوق الإنسان في عصر التقانات الإلكترونية الرقمية	
المبحث الثاني– مخاطر التقانات الإلكترونية الرقمية التي تهدد الحق في الخصوصية	
تعريفات	
مكونات بيئة التقانات الإلكترونية الرقمية وشبكات المعلومات	
المخاطر التي تهدد الخصوصية	
مخاطر البرامج الإلكترونية المتطفلة الضارة	
مخاطر مخترقي الأجهزة (الهاكرز)	
مخاطر أجهزة التقانات الإلكترونية الرقمية وشبكات المعلومات والتواصل الاجتماعي	
الخاتمة	
النتائج والتوصيات	
المراجع	
أولاً: المراجع العربية	
ثانياً: الدساتير	
ثالثاً : مواقع إلكترونية	