مجلة كامبريدج للبحوث العلمية: مجلة علمية محكمة
تصدر عن مركز كامبريدج للبحوث والمؤتمرات–العدد الحادي الاربعون – كانون الثاني ٢٠٢٥– رجب ١٤٤٦
ISSN–2536–0027

مخاطر المساس بالمعلومات الشخصية في العالم الافتراضي

الباحث محمد رحيم عودة الغالي
Alghalymhmd٩٠٨@gmail.com
المشرف ا.د هلا العريس
Hala.ariss@gmail.com
الجامعة الاسلامية في لبنان.كلية الحقوق

المُلخص
مع ازدياد استخدام شبكة الإنترنت وانتشارها بين جميع شرائح المجتمع، تحول بعض الأفراد المنحرفين إلى استغلالها لأغراض سلبية، حيث يستخدمون مهاراتهم في تكنولوجيا المعلومات والاتصالات لاختراق خصوصية الآخرين دون الحاجة إلى التحرك من مكانهم. وهذا الأمر دفع الدول إلى تكثيف جهودها في مكافحة الجرائم المرتبطة بهذا النوع من الاعتداءات، التي أصبحت تتخطى الحدود الوطنية وتستخدم وسائل تكنولوجية متطورة للإضرار بمجتمعات عدة. وبواسطة التكنولوجيا الحديثة في مجال الاتصالات، تعمل الدول على تعزيز التعاون الدولي لمكافحة هذه الجرائم ومنع انتشارها في العالم الرقمي. يتضمن ذلك اتخاذ تدابير فعالة للحد من هذه الظواهر والقضاء عليها، بالإضافة إلى معاقبة الجناة. سيتم مناقشة الجهود الدولية والإقليمية ودورها في وضع توجيهات تهدف لحماية البيانات ومكافحة الجرائم المتعلقة بتكنولوجيا المعلومات وانتهاك خصوصية الأفراد.

Abstract
With the increasing use of the Internet and its spread among all segments of society, some deviant individuals have turned to exploiting it for negative purposes, as they use their skills in information and communication technology to violate the privacy of others without having to move from their place. This has prompted countries to intensify their efforts in combating crimes related to this type of attacks, which have become transnational and use advanced technological means to harm several societies. Through modern technology in the field of communications, countries are working to enhance international cooperation to combat these crimes and prevent their spread in the digital world. This includes taking effective measures to reduce and eliminate these phenomena, in addition to punishing the perpetrators. International and regional efforts and their role in developing guidelines aimed at protecting data and combating crimes related to information technology and violating individuals' privacy will be discussed.

مجلة كامبريدج للبحوث العلمية: مجلة علمية محكمة
تصدر عن مركز كامبريدج للبحوث والمؤتمرات–العدد الحادي الاربعون – كانون الثاني ٢٠٢٥– رجب ١٤٤٦
ISSN-2536-0027

المقدمة

إن المتأمل في الثورة المعلوماتية الحاصلة، يرى فوائدها الكثيرة في مختلف المجالات، كما يرى في الوقت نفسه المخاطر التي تنجر عنها، والتي تمس الحياة الاجتماعية والخلقية والثقافية والدينية، وقد أصبحت المعلومات واحدة من أكثر أنواع المنتجات قيمة ومن الضروري توفير طريقة جديدة بشكل أساسي لنقل المعلومات، باستثناء إمكانية مخاطر المعلومات. لا يوجد حاليًا طريقة مقبولة عمومًا تحدد بشكل موثوق المخاطر المحددة لتكنولوجيا المعلومات. ويرجع ذلك إلى حقيقة أنه لا توجد كمية كافية من البيانات الإحصائية التي تسمح بالحصول على مزيد من المعلومات المحددة حول المخاطر الشائعة. يؤدي الدور الهام أيضًا حقيقة أنه من الصعب تحديد حجم مصدر معلومات معين بطريقة شاملة، لأن الشركة المصنعة أو مالك أي مؤسسة يمكنها الاتصال بتكلفة ناقلات المعلومات بدقة مطلقة، ولكن من الصعب التعبير عن قيمة المعلومات المتعلقة بها. وهذا هو السبب في أن أفضل طريقة في الوقت الحالي لتحديد تكلفة مخاطر تكنولوجيا المعلومات هي التقييم النوعي، وذلك بفضل تحديد عوامل الخطر المختلفة وتحديد مجالات تأثيرها ونتائجها على المؤسسة بأكملها.

حاول الإنسان عبر العلم، السيطرة على الطبيعة المحيطة به، ولكن تطور العلوم بمختلف مشاربها، وما يترتب على ذلك من تقدم تكنولوجي هائل، دفع إلى التساؤل عن كيفية السيطرة على العلم نفسه، ولاسيما أن بعض المحللين[١] يرددون مقولة مفادها أن العالم دخل منذ فترة وجيزة في نوع من" الحداثة المتأملة ". وذلك من أجل تمييزها عن تلك الحداثة المرافقة سابقا للثورة الصناعية الكبرى التي يتم وصفها بانها عمياء لما تتضمنه من مخاطر بالنسبة للبيئة، لما ينذر به ذلك من كوارث ترتسم في أفق الإنسانية، وإن لفظ technology في معناه الحرفي يعنى علم التقنية هذا وقد عرفها ديبو – انطلاقا من نظرته للتكنولوجيا على حساب إنها وسيلة التطوير والصناعة والتنمية المترتبة على هذا التطوير في نفس الوقت بانها علم التقنيات أو البحث التطبيقي. من هذا التعبير يكون المقصود من الأخطار التكنولوجية من الناحية للغوية هي كل خطر ينتج عن الأبحاث الصناعية المطبقة.[٢]

ثانيا: أهمية البحث:

يعد البحث في مخاطر المساس بالمعلومات الشخصية في العالم الافتراضي أمرًا حيويًا لحماية الخصوصية والأمن الرقمي. من خلال فهم التهديدات وكيفية مواجهتها، يمكننا بناء عالم رقمي أكثر أمانًا وازدهارًا. أصبحت المعلومات الشخصية كنوزًا ثمينة تسعى العديد من الجهات للحصول عليها واستغلالها لأغراض مختلفة، قد تكون مشروعة أو غير مشروعة. لذا، فإن البحث في هذا المجال يكتسب أهمية بالغة

ثالثا: مشكلة البحث وتساؤلاته:

تتمثل الإشكالية؛ حول مخاطر المساس بالمعلومات الشخصية في العالم الافتراضي؟

ويتفرع عن هذه الإشكالية عدة تساؤلات فرعية يجاب عليها خلال الدراسة لعل أهمها؛

١- ما المقصود بمخاطر المساس بالمعلومات الشخصية ؟
٢- ما المقصود بضمانات حماية المعلومات الشخصية من المخاطر في العالم الافتراضي ؟
٣- ما هي آلية حماية البيانات الشخصية في العالم الافتراضي؟

رابعا: نطاق البحث:

يتحدد نطاق الموضوع محل البحث في المخاطر المساس بالمعلومات الشخصية في العالم الافتراضي في العراق، هذا ما يحدوا بنا إلى استبعاد المخاطر المتعلقة بالبيانات الأخرى كالبيانات التجارية أو المعلومات

مجلة كامبريدج للبحوث العلمية: مجلة علمية محكمة
تصدر عن مركز كامبريدج للبحوث والمؤتمرات–العدد الحادي الاربعون – كانون الثاني ٢٠٢٥– رجب ١٤٤٦
ISSN-2536-0027

العامة أو البيانات غير الشخصية، كذلك بيان ضمانات حماية المعلومات الشخصية من المخاطر في العالم الافتراضي.

خامسا: منهج البحث:

عمد الباحث إلى اتباع المنهج الوصفي لبيان وتحديد المفاهيم القانونية فصلا عن المنهج التحليلي للنصوص المتعلقة بموضوع البحث. من ثم يكون منهج البحث وصفي تحليلي.

سادسا: أهداف البحث:

يهدف البحث في هذا الموضوع حول تبيان مفهوم مفهوم المخاطر في العالم الافتراضي وتحديد مدى تأثيره على البيانات الشخصية، كذلك ضمانات حماية المعلومات الشخصية من المخاطر في العالم الافتراضي.

سابعا: خطة البحث:

المطلب الأول: مفهوم المخاطر في العالم الافتراضي.

المطلب الثاني: ضمانات حماية المعلومات الشخصية من المخاطر في العالم الافتراضي.

المطلب الأول

مفهوم المخاطر وصورها في العالم الافتراضي

تمهيد

مما لا شك فيه أن الإنسان معرض لعدد كبير من المخاطر غير المتوقعة والتي تختلف في طبيعتها، وتتفاوت في خطورتها، كما أن كل شخص في هذه الحياة إلا ويسعى إلى جعل نفسه وماله في أمان واطمئنان. وهكذا سعى الإنسان منذ القدم إلى مجابهة هذه المخاطر بوسائل متعددة، بدأت بالادخار الفردي وبالتضامن العائلي أو العشائري وانتهت بابتداع عقد التأمين.

الفرع الأول

ماهية المخاطر التكنولوجية

يقصد بالخطر الإشراف على الهلاك، وهناك اتفاق عام على أن الإنسان معرض إلى أخطار متعددة وذلك لان الأخطار شيء مواكب وملازم للحياة البشرية وهي جزء لا يتجزأ من عمل الأفراد والمنشآت، ولا سيما أن انتشار التأمين في مختلف نواحي الحياة أدى إلى تطور مفهوم الخطر المشمول بالتغطية، بشكل يجعل هذا المفهوم من الصعب حصره أو اختزاله في تعريف معين، فمنذ نشأة الإنسان تعرض لمخاطر متعددة، وحاول دائما دراسة تلك المخاطر والبحث عن انسب الوسائل لمنعها وتقليل الخسائر الناجمة عنها، وكل يوم يكتشف مخاطر جديدة، كما يكتشف وسائل الوقاية منها أو منع مخاطر كانت موجودة من قبل.

أولًا: الخطر التكنولوجي في مفهومه الشائع

بالنظر للخطر التكنولوجي بالمعنى اللفظي السابق نجد أن هذا التعريف جعل من كل خطر صناعي خطر تكنولوجي. ولكن ليس بالضرورة أن يكون الخطر الصناعي خطر تكنولوجي، ولا جدال أن لفظ technology توحي في حد ذاتها بالحداثة وهذه الأخيرة هي أول ما يتصف به الخطر التكنولوجي في مفهومه الشائع. ودائما ما يرتبط بالمفهوم الشائع للخطر التكنولوجي أنه من طائفة الأخطار الكبيرة:-

وعلى حد هذا المفهوم الشائع يكون الخطر التكنولوجي. هو خطر صناعي حديث – فادح الآثار والنتائج[٣]، هذا وقد ذهب بعض الفقه إليه القول بأن "هذا الفهم واقعي أي حد ما: فهناك ظاهرتان ملحوظتان في الدول الصناعية – هي ضخامة وحدة الإنتاج والميل إلى التخصص" وهذا الأخير يؤدى بدوره إلى تكديس أخطار وقيم مابية هامة. هذا وإن كانت صفة الجدة أو الحداثة للخطر التكنولوجي تجعل من الأضرار الناشئة عنه

مجلة كامبريدج للبحوث العلمية: مجلة علمية محكمة
تصدر عن مركز كامبريدج للبحوث والمؤتمرات–العدد الحادي الاربعون – كانون الثاني ٢٠٢٥– رجب ١٤٤٦
ISSN-2536-0027

أضرارا لا يمكن التنبؤ بحدودها سلفا[٤]، بل وتتعدى أحيانا حدود الدولة التي يوجد بها مصدر الخطر فالمنتج الحديث مثلا يتميز في حد ذاته بسعة الانتشار وضخامة عدد المتعاملين معه.

وان المخاطر التكنولوجية قد تعد مخاطر فنية: وينتج هذا النوع من الخطر نتيجة إنتاج معدات أو آلات حديثة، وقد ينتج عنها مخاطر فنية لم تكن موجودة من قبل، فتقديم منتج يحوي على العديد من المخاطر قد تكون نتائجه موجبة أو سالبة، فقد يقدم مزايا ومنافع موجودة من قبل، كما قد يقدم أضرارا لم تكن موجود في الحسبان، ويكون الناتج النهائي خسارة وليس ربحا[٥]، إلا أن وصف الخطر التكنولوجي بأنه خطر حديث وجديد هو تعريف يخالف المفهوم القانوني وذلك حيث أنه من الاشتراطات اللازمة للخطر محل التأمين من الناحية القانونية أن يكون الخطر غير محقق الوقوع، إلا أن هذا التعريف انطوى على خلط بين الحدث في حد ذاته وبين موضوع الخطر وعلى حد القول فهناك أخطار معروفة تماما مثل خطر التلوث الذري أو البيئية والخطر الإشعاعي – وهذه أخطار حديثة ولاسيما إنها أخطار تكنولوجية – كما أن تعريف الخطر التكنولوجي بهذا المعنى من الناحية الفنية يهدر أحد الأسس الفنية التي يقوم عليها نظام التأمين وهو ضرورة تجانس الأخطار، فان مفهوم الخطر التكنولوجي بحسابه أنه الخطر الصناعي الجديد كبير الحجم. يترتب عليه تغطية لمجموعة كبيرة من الأخطار غير المتجانسة. وما يجب جذب الاهتمام إليه هنا هو وجوب التفرقة بين تأثير الظاهرة الطبيعية قبل تحققها وهو الخطر وبين تأثيرها بعد تحققها في صورة حادث وهي الخسارة الفعلية. وعلى ذلك يمكن تعريف كل من الحادث والخسارة كالآتي:[٦]

الحادث **Accident**: يعرف الحادث بأنه التحقق المادي لظاهرة من الظواهر الطبيعية أو العامة مما ينتج عنه خسارة فعلية.

الخسارة **Loss:**ويقصد بها فقد الحياة أو الإصابات البدنية، النقص في قيمة الممتلكات أو فناؤها، النقص في قيمة الدخل أو زواله، زيادة النفقات، والذي قد ينتج من تحقق حادث معين للأشخاص أو ممتلكاتهم. ويمكن تقسيم الخسارة إلى: خسارة كلية، خسارة جزئية.

١- الخسارة الكلية **Total Loss:**ويقصد بها الفقد أو الضياع أو الهلاك التام لما هو معرض للخطر. على سبيل المثال: وفاة رب الأسرة، غرق السفينة، احتراق أصل من الأصول بالكامل.

٢- الخسارة الجزئية **Partial Loss:**ويقصد بها الفقد أو الضياع أو الهلاك الجزئي لما هو معرض للخطر، على سبيل المثال/ جنوح سفينة مما أدى إلى وقوع بعض الخسائر المادية بها، حدوث حريق أدى إلى هلاك جزء من أصل من الأصول.[٧]

ويتضح أن هذا المفهوم للخطر التكنولوجي يحتاج إلى شيء من التدقيق حتى يمكن التعويل عليه من الناحية الفنية وصولا إلى مفهوم أدق للخطر محل الدراسة.[٨]

ثانيًا: مفهوم الخطر التكنولوجي من الناحية الفنية

لما كان الاتجاه السابق في تعريف الخطر التكنولوجي يفتقر للدقة ويستحيل الأخذ به من الناحية الفنية ظهر اتجاه أخر في تعريف الخطر التكنولوجي[٩]، فعرف البعض الأخطار التكنولوجية " بانها أضرار مالية تنشأ من تعهدات تعاقدية تعهد بها المستأمن لعميله- أي إنها الجزاءات أو التعويضات أو المصاريف الإضافية التي يمكن أن يتعرض لها المورد إذا ثبتت مسئوليته العقدية في مواجهة العميل". إلا أن هذا الاتجاه كسابقه لم يسلم من النقد فنرى مع البعض[١٠] أن هذه اللجنة السابق ذكرها لجأت إلى منهجا قانونيا جانبه الصواب حيث عرفت الخطر التكنولوجي باللجوء إلى مسألة فرعية عنه والمتعلق بتغطية هذا الخطر ولاسيما أن تعريف الخطر يلزم أن ينطلق بداية من مقوماته. كما أن اللجنة سالفة الذكر حصرت الخطر التكنولوجي في مفهوم ضيق للغاية وهو المعمول به في إطار صفقات توريد المجموعات الصناعية المتكاملة فقط. وإزاء هذا

مجلة كامبريدج للبحوث العلمية: مجلة علمية محكمة
تصدر عن مركز كامبريدج للبحوث والمؤتمرات–العدد الحادي الاربعون – كانون الثاني ٢٠٢٥– رجب ١٤٤٦
ISSN-2536-0027

النقد الذي وجه لهذا الفريق ذهب اتجاه ثالث إلى أن الخطر التكنولوجي هو "خطر التقدم الصناعي" وبالنظر إلى هذا التعريق يتضح أنه نتج عن التصدي لمشكلة تأمين المسئولية المدنية عن أضرار المنتجات الصناعية.[١١]

ومن ثم يكون الضرر الناتج عن خطورة في المنتج، لم يكن طبقا للمستوى العلمي والفني للصانع أو أي شخص أخر يتوقع أن هذا المنتج ينطوي على هذا الخطر، هو ضرر تقوم عنه مسئولية. ونرى مع هذا الاتجاه أنه هو الأنسب في تعريف الخطر التكنولوجي بأنه هو خطر التقدم لما فيه من سعة في المفهوم ولما رآه القضاء الفرنسي[١٢] من أن فكرة خطر التقدم هي مجالا خصبا للتعويض عن الأضرار التكنولوجية.

ونجد أن هذا المفهوم هي تعريف الخطر التكنولوجي سيكون منشأ لمجالا خصبا للتعويض عن أضرار عدة في مجالات مختلفة منها الصناعي والبيئي وأخطار نظم المعلومات وعليه يكون موضوع الخطر التكنولوجي هو كل وسيلة صناعية جديدة تعمل أو منتجات صناعية جديدة تطرح، كما أن الخطر التكنولوجي بمفهوميه الشائع والفني "هو خطر مسئولية تهدد النشاط الابتكاري وخطر المسئولية في هذا النطاق لم يمكن قصره فقط على المسئولية العقدية"، وإنما يمتد ليشمل أيضًا المسئولية التقصيرية كما سنوضح فيما بعد، من كل ذلك نخلص إلى تعريف الخطر التكنولوجي بأنه "كل خطر يهدد النشاط الابتكاري يستوجب المسألة المدنية يكون موضوعه وسيلة صناعية جديدة تعمل أو منتجات جديدة تطرح".[١٣]

نرى أنه استئناسا بفكرة الخطر الواردة في التعريف السابق. يمكننا وضع تعريف للخطر التكنولوجي بأنه " كل حالة تتضمن احتمالية حدوث نتائج غير مرغوب فيها أو خسارة، تهدد النشاط التقني، وتثير المسئولية المدنية عن وسيلة صناعية جديدة تعمل أو منتجات جديدة تطرح ". من ذلك التعريف نجد أن الخطر التكنولوجي يرتبط بشكل أساسي بعدة مخاطر هي في الأصل وثيقة الصلة بالنشاط التكنولوجي[١٤] وإن كانت أخطار مبدئية مرتبطة بتشغيل النشاط التكنولوجي ذاته وليست نتيجة مباشرة لتفعيله، حيث أن تبنى تكنولوجيا جديدة مبتكرة يهدف تحقيق السبق والريادة، وميزة تنافسية في السوق، يصاحبه في كثير من الأحيان مخاطر فشل التكنولوجيا الحديثة غير المجربة.[١٥]

ويمكن أن تؤدى إلى توقف تدفق عمليات المنظمة كما أن بعض أنواع التكنولوجيا، وخاصة في حقل البرمجيات سريعة التقادم على سبيل المثال. وتكون مكلفة في بدايتها. ويصعب على الشركات الرائدة استثمارها اقتصاديا نتيجة سرعة تقدمها التكنولوجي.

ونعرض لبعض هذه المخاطر مرتبطة الصلة بالنشاط التكنولوجي.

أولا: مخاطر العمليات **Operational Risks** [١٦]

كثيرا ما يرافق استخدام التكنولوجيا الجديدة في عمليات الإنتاج وفى بداية إدخالها لأول مرة في العملية الإنتاجية مخاطر تتعلق بتوقف العمليات نتيجة أخطاء في مواءمة التكنولوجيا الجديدة مع نظام الإنتاج القائم. وهذه التوقفات قد تكون ذات أثار كبيرة على سير العمليات.

كما أن إدخال التكنولوجيا الحديثة في عمليات الإنتاج يتطلب في البداية إعادة تنظيم العمل، وكذلك إعادة تدريب وتأهيل الأفراد، وهذا يقود إلى إبطاء أو أخطاء في بداية استخدام التكنولوجيا الحديثة في العملية الإنتاجية.

ثانيا: المخاطر التنظيمية **Organization Risks** [١٧]

في كثير من الحالات يفتقر أصحاب الشركات ومدراء الإدارة العليا إلى ثقافة تنظيمية واسعة، والتزام إداري ثابت. وهذا الافتقار إذا ما اقترن ببعض الأخطاء الأولية المرافقة لإحلال التكنولوجيا الحديثة في المنظمة يدفع أصحاب الشركات والمدراء الإدارة العليا إلى التخلي بسرعة عن برامج إحلال التكنولوجيا.

مجلة كامبريدج للبحوث العلمية: مجلة علمية محكمة
تصدر عن مركز كامبريدج للبحوث والمؤتمرات–العدد الحادي الاربعون – كانون الثاني ٢٠٢٥– رجب ١٤٤٦
ISSN-2536-0027

وهذا يرتب على الشركة خسائر مضاعفة منها توقف العمل مؤقتا حتى يتم إعادة النظام إلى وضعه قبل عملية الإحلال وخسائر ناتجة عن خسارة التكنولوجيا التي تم إدخالها. وإذا ما تمتع أصحاب الشركات ببعض الثقافة التنظيمية والالتزام الإداري فانهم في كثير من الحالات يدركون ذلك في منتصف الطريق، وبالتالي لن يتخلوا عن عملية الإحلال بخاصة بعد أن دفعوا تكاليفها كاملة، وكذلك لن يقوموا بإجراء تغييرات جوهرية رئيسية لتصحيح عمليات الشركة القديمة وغير الفعالة.

وفى كلا الحالتين لن يحصلوا على فوائد إحلال التكنولوجيا الحديثة ولو على المدى القصير[١٨]، لهذا يتوجب على مدراء الشركات أن يتمتعوا بمقدار من الثبات والالتزام الإداري والثقافة التنظيمية حتى يستطيعوا امتصاص المخاطر التنظيمية لإحلال التكنولوجيا، ولو على المدى القصير، ويثبتوا أمام التوقفات القصيرة في عملية الإنتاج. وهذا الثبات يساعدهم إلى حد بعيد على تسريع عملية دمج التكنولوجيا الحديثة وتأهيلها في العملية الإنتاجية.

ثالثا: أخطار بيئية وأخطار السوق **Environment Market Risks** [١٩]

ان المخاطر البيئية وكذلك أخطار السوق مرافقة لعملية إحلال التكنولوجيا في العملية الإنتاجية. وهذه المخاطر تزيد من حذر المستثمرين في الشركات الصناعية في زيادة الاستثمار في التكنولوجيا الحديثة، وتدفعهم إلى الإبطاء من عملية الإحلال وبخاصة عندما تكون كل من المخاطر البيئية ومخاطر السوق مؤكدة وعلى المدى الطويل. فمثلا عندما يكون أصحاب الشركات متأكدون ولحد بعيد أن تغيرات بيئية ترافق نوع من التكنولوجيا فانهم سوف يترددون في الاستثمار فيه، لان فوائد ذلك سوف تتوقف خلال فترة قصيرة.

على سبيل المثال فان أصحاب شركات صناعة السيارات الكهربائية مازالوا مترددين وغير متأكدين من المعايير البيئية والحكومية المعتمدة حول العوادم.

كما أن هناك احتمالية لخفض عوادم سيارات النفط، وكذلك هناك احتمالية لحصول تقدم كبير في تقنيات البطاريات التي سوف تستخدم في السيارات الكهربائية. فكل هذه العوامل البيئية تؤثر على عملية الإحلال التكنولوجي إلا إنها تثير أيضًا تساؤل حول مسئولية التعويض عنها.

الفرع الثاني

صور المخاطر المتعلقة بالمعلومات الشخصية في العالم الافتراضي

مع توسع استخدام شبكات الإنترنيت ودخول جميع فئات المجتمع إليها دفع المنحرفون منهم إلى استغلالها لأغراض دنيئة وتوظيف معلوماتهم ومهاراتهم في تقنية المعلومات وتكنولوجيا الاتصالات للاعتداء على حقوق الآخرين من دون أن يتجه احدهم عناء التحرك من مكانه؛ لذلك تكاثفت جهود الدول في مكافحة الجرائم والاعتداءات التي لم تعد تتمركز في دولة معينة أو مجتمع معين بل أصبحت عابرة للحدود وبوسائل تكنولوجية متطورة لتلحق الضرر بعدة دول ومجتمعات مستغلة التقنية الحديثة في الاتصالات ولتعزيز التعاون بين الدول من أجل مكافحة هذه الجرائم ومنعها من التفشي بين المجتمعات الديمقراطية في العالم الرقمي، واتخاذ التدابير اللازمة وفعالة للحد منها والقضاء عليها ولمعاقبة مرتكبيها وسوف نتعرض للجهود الدولية والإقليمية ودورها في وضع قواعد إرشادية تكفل حماية البيانات ومكافحة الجرائم المستحدثة في مجال التكنولوجيا والاعتداء على خصوصية الأشخاص.

بيد أنه لا يستطيع أحد أن ينكر أهمية الحاسوب بوصفه من المظاهر الفذة للتقدم العلمي التي وفرت على الإنسانية جهداً كبيراً، ولكن في الوقت نفسه لا يمكن التغاضي عن مثالبه ذات الخطورة الجمة، حتى قيل إن شفافية الإنسان وخصوصياته قد باتت عارية أمام ما تمخض عنه العلم من إعجاز في مجال الحاسوب.[٢٠]

مجلة كامبريدج للبحوث العلمية: مجلة علمية محكمة
تصدر عن مركز كامبريدج للبحوث والمؤتمرات–العدد الحادي الاربعون – كانون الثاني ٢٠٢٥– رجب ١٤٤٦
ISSN-2536-0027

ورغم المزايا العظيمة التي يقدمها الحاسوب لمجتمعنا المعاصر، والتي هي في تكاثر مستمر فإنها قد أوجدت إلى جانب ذلك العديد من الأخطار الجديدة وإمكانية التعرض إلى أضرار جسيمة جعل البعض يشك حتى في مصداقية جدواها أو فائدتها للبشرية مطالباً بوقف العمل بأنظمة الحاسوب أو تجميدها لفترة ما.[٢١]

ونتيجة لاستخدام الحاسوب في معظم إدارات الدول الحديثة سواء في السجل المدني أو في مجال الضرائب والجمارك أو أجهزة الشرطة والأمن، يتوقع أن تنشأ تعقيدات لم يسبق وجودها في العلاقة بين الدولة والمواطن .[٢٢]

فالمعلومات التي كانت من قبل منعزلة ومتفرقة ومن الصعب التوصل إليها نظراً لصعوبة الكشف عنها أصبحت سهلة المنال باستخدام الحواسيب، إذ ساعدت على تكامل الحقائق عن الأفراد وتوفرها، ومن بين النتائج المخيفة لسوء استخدام الحاسوب هو إمكانية التعرف على الأفراد وشفافية صورهم وسماتهم نتيجة للتوسع في جمع صور الأفراد، لذلك يجب الحرص على أن لا يساء استخدام مثل هذه المعلومات إذ ثبت أهمية بقاء المعلومات وضرورتها.[٢٣]

وتعد إساءة استخدام الحاسوب السبب الرئيسي لأكثر أخطار الحاسوب وأوسعها نطاقاً حيث تشمل الأفعال غير القانونية كافة سواء عدت جرائم أم لا.

ويعرف الفقه حالة إساءة استخدام الحاسوب بانها: جميع أنواع الأفعال التي تكون مرتبطة بوضوح بأجهزة الحاسوب والاتصالات المتعلقة بالبيانات التي تعرض ضحاياها إلى خسارة أو أضرار مالية أو شخصية أو التي يكون مرتكبوها قد حصلوا أو يمكن أن يحصلوا على كسب غير مشروع منها .[٢٤]

ان الكثير من المؤسسات الكبرى والشركات الحكومية الخاصة، تجمع عن الأفراد بيانات عديدة ومفصلة تتعلق بالوضع المادي، أو الصحي، أو التعليمي، أو العائلي، أو العادات الاجتماعية وغيرها من البيانات المهمة وتستخدم شبكات الاتصال في خزنها ومعالجتها وتحليلها والربط بينها واسترجاعها ومقارنتها ونقلها من خلال الحدود، مما يجعل فرصة الوصول للبيانات بشكل غير مأذون، أو مصرح به، وبطرق غير مشروعة بحيث يفتح مجالاً أوسع لإساءة استخدامها، أو توجيهها توجيهاً منحرفاً، أو خاطئاً، أو مراقبة الأفراد والتجسس على خصوصياتهم، وقد تصدر أحكام عليهم غيابية من واقع سجلات بياناتهم الشخصية المخزنة.

إنّ شيوعَ النقل الرقمي للبيانات خلق مشكلة أمنية وطنية، إذ سهل استراق السمع والتجسس الإلكتروني، ففي مجال نقل البيانات تتبدى المخاطر المهددة للخصوصية في عدم قدرة شبكات الاتصال على توفير الأمان في سرية ما ينقل من خلالها من بيانات وإمكانية استخدام الشبكات في الحصول بصورة غير مشروعة، وتشير أحدث التقارير عن الخصوصية أنه ما تزال حياة الأفراد وأسرارهم في بيئة النقل الرقمي معرضة للاعتداء في ظل التطور التكنولوجي المتسارع.

ويقصد بالمخاطر في العالم الافتراضي سلامة وصحة البيانات الشخصية تلك المخاطر التي تهدد البيانات ذاتها من الإتلاف أو العبث بها أو بطبيعة الحال إفشاء سريتها ومن ثم يفترض أن تتخذ المؤسسة المعنية بها حماية البيانات الشخصية تدابير لحماية تلك البيانات من المخاطر السابقة لعل أهمها ما يلي:

أولاً: ضرورة توفير مجموعة من الوسائل والإجراءات التي تحقق الحماية من الأحداث المستقبلية غير المرغوب فيها والتي تعتبر بمثابة تهديدات لنظام المعلومات الذي يحمي البيانات الشخصية ذاتها لأنها تؤدي إلى حدوث إخلال بالأمن Breach of security وفقدان التكامل والدقة داخل النظام.[٢٥]

مجلة كامبريدج للبحوث العلمية: مجلة علمية محكمة
تصدر عن مركز كامبريدج للبحوث والمؤتمرات–العدد الحادي الاربعون – كانون الثاني ٢٠٢٥– رجب ١٤٤٦
ISSN-2536-0027

ثانياً: وجود مجموعة من الإجراءات والأساليب التي تهدف إلى تحقيق الحماية للنظام من أي أحداث مستقبلية تهدد النظام وتؤدي إلى فقد المعلومات أو عدم دقتها، وبالأخص فقد سرية البيانات[٢٦]. ومن ثم يمكن إجمال مخاطر حماية سلامة البيانات وصحتها في التدابير الأتية :[٢٧]

١- مخاطر سرية البيانات Confidentiality: وتعني عدم إتاحة البيانات لمن ليس له تصريح للاطلاع عليها أو عدم حصول الأطراف غير المسموح لهم عليها.

٢- مخاطر تكامل البيانات Integrity: وتعني الحفاظ على البيانات من التغيير أو التدمير أو التحريف وذلك لضمان أن تكون دقيقة وصحيحة ومكتملة أثناء تخزينها وأثناء نقلها، وإن يتم تشغيلها بطريقة صحيحة.

٣- مخاطر الإتاحة Availability: أي إمكانية الوصول إلى البيانات وتوافرها واستخدامها عند طلبها في الوقت الملائم من قبل المستخدمين المصرح لهم وفي المكان المناسب.

٤- مخاطر إمكان المساءلة عن البيانات Accountability: أو إمكانية مراجعة البيانات ويشير ذلك إلى أن القيام بفحص معين يتضمن أن أفعال وعمليات وتصرفات منشأة معينة يمكن ردها إلى تلك المنشأة فقط دون أي لبس أو غموض.

٥- مخاطر توثيق البيانات: وتعني مخاطر عدم التحقق من سلامة هوية الشخص أو الجهة التي يتم التعامل معها، والتأكد أنه من طرف مصرح له بالدخول إلى موقع أو نظام معلومات المنشأة والاطلاع على ما به من معلومات.

ترتب على استخدام النظم الإلكترونية Computerized Systems نمو في جرائم الحاسبات Computer Crimes، ويقصد بجرائم الحاسبات Computer Crimes "استخدام النظم الإلكترونية بشكل مباشر من خلال القائمين على نظام المعلومات أو بشكل غير مباشر (عن بُعد) للقيام بأنشطة تتصف بعدم القانونية كالسرقة أو التخريب أو التلاعب مما قد يؤدي إلى تحقيق أضرار بالغة سواء بالنسبة لحائزي الحاسبات الإلكترونية الشخصية (PC) والتي تؤدي بطبيعة الحال إلى إفشاء سرية البيانات أو إتلافها.

وقد تتنوع مصادر التهديد بإفشاء سرية البيانات الشخصية إلى مصادر طبيعية[٢٨] وأخري بشرية خارجية والتي ترتبط بالقابلية للتعرض لمخاطر الإفشاء نتيجة لخلل في نظام أمن المعلومات من الضعف في نظام التشغيل ومكوناته[٢٩]، وقد تكون التهديدات بشرية خارجية والتي تنشأ من أفراد خارج المنشأة أهمها القرصنة عن طريق الإنترنت والتجسس لإفشاء سرية البيانات الشخصية.

بالإضافة إلى مخاطر إفشاء سرية البيانات الشخصية قد تتعرض البيانات إلى الآتي:

- إمكانية تحريف بيانات النظام وبالتالي يؤدي استخدامها إلى قرارات خاطئة.
- إمكانية إدخال فيروسات إلى نظام المعلومات تعمل على إتلاف وتدمير أو تخريب كل أو بعض البيانات الشخصية أو الملفات وبالتالي تفريغ المحتوى المعلوماتي للنظام.
- إمكانية إعاقة عمل نظام المعلومات من خلال إغراقه بطلبات تبادل البيانات مما يؤدي إلى إعاقة وصول المستخدمين الطبيعيين إلى النظام.

كما قد تكون التهديدات التي تمثل خطرا على سرية البيانات الشخصية من داخل المنشاة ذاتها كالموظفين في السجل المدني أو العيني وغيرها من المؤسسات التي تحتفظ ببيانات المواطنين الشخصية سواء كانوا من الموظفين السابقين الذين فقدوا وظائفهم أو الموظفين الحاليين مستخدمين لما لديهم من سلطات أو معلومات بهدف تحقيق مصالح شخصية خاصة بهم أو لأقاربهم وبصرف النظر عن دوافعهم، ويمثل الموظفون تهديداً حقيقياً لأن لديهم القدرة على الوصول إلى بيانات الأشخاص داخل المنشأة.

مجلة كامبريدج للبحوث العلمية: مجلة علمية محكمة
تصدر عن مركز كامبريدج للبحوث والمؤتمرات–العدد الحادي الاربعون – كانون الثاني ٢٠٢٥– رجب ١٤٤٦
ISSN-2536-0027

وأن حدوث أي من التهديدات والأخطار السابق ذكرها يمكن أن يؤدي إلى الأثار التالية :[٣٠]

- تحمل المنشأة تكاليف مباشرة لإصلاح الأضرار الناتجة عن حدوث هذه التهديدات والأخطار بالإضافة إلى خسائر مالية.
- توقف نظام المعلومات لبعض الوقت، مما يؤدي إلى احتمال فقد بعض الإيرادات متى كانت تعمل في مجال التجارة الإلكترونية.
- خسائر نتيجة إفشاء بعض البيانات الهامة للأشخاص، مما يمكنهم من التعرف على خطط التشغيل المزمع تنفيذها، أو المنتجات الجديدة ومواصفتها ومنافذ توزيعها.. إلخ، وغيرها من المعلومات الهامة كطبيعة العقود وشروطها.

يؤكد البعض على أن "عالم المعلومات الإلكترونية يتعرض لكثير من المخاطر والتهديدات ومنها التلاعب في البيانات بقصد تدميرها سواء بالحذف أو التغيير أو الدمج غير الصحيح لبعضها أو بخلطها ببيانات أخرى غير حقيقية أو تبويبها بشكل خاطئ تفقد معها مدلولها ومعناها".[٣١]

وقد يحدث هذا التلاعب في مراحل مختلفة من النظام مثل المدخلات أو التشغيل أو التخزين أو المخرجات، ويمكن أن يكون إفشاء البيانات جزئياً أو كلياً وفي الحالة الأخيرة قد يصعب تصحيح البيانات أو استعادتها مما يشكل خسارة كبيرة لنظام المعلومات وما ينتجه من مخرجات، وقد يهدف التلاعب في النظام إلى الاطلاع على بيانات سرية Disclosure Of Confidential Data مثل بيانات تخطيط الربحية أو بيانات الأفراد (الرواتب والترقيات والعلاوات).

ويمكن للمتلاعب في هذه الحالة ليس فقط الاطلاع على البيانات وإساءة استخدامها أو إفشائها بل أيضًا سرقة بعضها أو كلها[٣٢]، وبالتالي تكون هناك إمكانية لحدوث خسارة أو تدمير أو إفشاء للبيانات أو استخدام البيانات أو البرامج بطريقة تضر بطرف أخر أو إمكانية حدوث أضرار بالأجهزة أو النظام سواء كانت تلك الخسارة ناتجة من الداخل أو الخارج بغرض تحقيق مصلحة شخصية أو بغرض العبث.

والجدير بالذكر أن إحدى الدراسات[٣٣] في مجال أمن نظم المعلومات قد أوجدت نوعاً من عدم التمييز الواضح بين مخاطر أمن نظم المعلومات Security Threats وبين عدم كفاية الضوابط الرقابية لأمن تلك النظم Inadequacy of Security controls فقد اعتبرت تلك الدراسة ضعف أو عدم كفاية بعض الأدوات والضوابط الرقابية المتعلقة بأمن نظم المعلومات على إنها تهديدات أو مخاطر لأمن تلك النظم.

إنّ هذه المخاطر أثارت مسألة الأهمية الاستثنائية للحماية القانونية والتقنية للبيانات الشخصية على الصعيد الوطني والدولي ولازالت تثير. ومن العوامل الرئيسة التي أوجبت توفير حماية تشريعية وسن قوانين في هذا المجال ولاسيما وإن النصوص التقليدية لحماية شرف الإنسان وحياته الخاصة لا تغطي إلا جانبا من الحقوق الشخصية وبعيدة عن حمايته عن مخاطر جمع وتخزين والوصول إلى وسيلة نقل المعلومات في بيئة الوسائل التقنية الجديدة التي تستهدف الخصوصية. دفعت أغلب الدول لوضع تشريعات تضمن حماية البيانات وإمكانية الاحتفاظ بها من دون المساس بحقوق الغير وعدّها مسوّغاً لتدخل في خصوصياتهم، ولأجل المحافظة على الحقوق الشخصية وكذلك العامة سعت أغلب الدول إلى إيجاد توازن بين هذه الحقوق.

المطلب الثاني

ضمانات حماية المعلومات الشخصية من المخاطر في العالم الافتراضي

تمهيد

يعد ضمان سرية البيانات قاعدة عامة أقرتها أغلب القواعد الدولية المتعلقة بحماية البيانات، فقد أكدت أغلبها على وجوب اتخاذ كافة الإجراءات الضرورية واللازمة لضمان سرية البيانات الشخصية من مقدمي

مجلة كامبريدج للبحوث العلمية: مجلة علمية محكمة
تصدر عن مركز كامبريدج للبحوث والمؤتمرات–العدد الحادي الاربعون – كانون الثاني ٢٠٢٥– رجب ١٤٤٦
ISSN-2536-0027

الخدمات، والالتزام بعدم نشر تلك المعطيات لأي غرض كان إلا بموافقة مسبقة من الشخص التي جمعت عنه البيانات، ولا يجوز له إفشاء، أو تحويل، أو إعلان، أو نشر تلك البيانات لأي غرض مهما كان إلا بموافقة مسبقة من الشخص الذي جمعت عنه البيانات ولا يجوز له إفشاء، أو تحويل، أو إعلان، أو نشر تلك البيانات لأي غرض مهما كان إلا بموافقة مسبقة من الشخص الذي جمعت عنه البيانات، ولعل الهدف من إقرار هذه القاعدة هو رغبة المشرع في إيجاد نوع من الثقة والأمان في التعاملات الإلكترونية، فشعور الشخص بالأمان والاطمئنان تجاه أن بياناته الشخصية التي تجمع عنه وأنها سوف تكون بمأمن من الآخرين ومن دون أي ريب فأنه سوف يقدم على إجراء معاملاته إلكترونياً بكل ثقة واطمئنان.

الفرع الأول

ضمانات الاحتفاظ والاطلاع على المعلومات الشخصية دون المساس

ان عدم وجود حماية للبيانات الشخصية قبل معالجتها سوف يؤدي إلى تقاعس صاحب البيانات عن الإدلاء بها وسيؤثر ذلك سلبيا في ازدهار وتطور التعاملات الإلكترونية خاصة أن البيانات غير مؤمنة بدرجة كافية يمكن اختراقها وسرقتها والاستفادة منها على وجه قد يسبب ضررا بالغاً لهذا الشخص خاصة إذا تعلقت هذه البيانات بحياته الخاصة أو الشخصية[١](٣٤)، وعلى سبيل المثال حرص المشرع العماني في مشروع القانون على إلزام مقدم الخدمات الإلكتروني أن يؤمن حماية فاعلة لهذه المعطيات بل ويحظر صاحب الشأن نفسه بإجراءاتها ليس هذا فحسب وأنّما يجب عليه أن يزود صاحب البيانات بنظام الدخول إلى إجراءات الحماية وبطريقة سهلة وبسيطة فالمادة (٤٥)[٢](٣٥)، ويجب على أي شخص يسيطر على البيانات الشخصية بحكم عمله في المعاملات، أن يعلم الشخص الذي جمعت عنه البيانات قبل معالجتها بواسطة إشعار خاص وإجراءات يتبعها لحراسة البيانات الشخصية، ويجب أن تتضمن هذه الإجراءات تحديد هوية المسؤول عن المعالجة وطبيعة البيانات والغرض من معالجتها وطرق ومواقع المعالجة وكل المعلومات الضرورية لضمان معالجة مأمونة للبيانات والرجوع إليها بشكل منظم ومتى يشاء.

ومن الضمانات التي أكدت عليها أغلب التشريعات حق العميل أو الشخص في الاعتراض على معالجة بياناته الشخصية الخاصة به ولا يجبر على قبول الوثائق الإلكترونية المتضمنة هذه البيانات ويحق له رفضها صراحة وكذلك ضمن المشرع للشخص حقه في عدم جواز القيام بمعالجة البيانات الشخصية متى ما كانت هذه المعالجة قد تسببت بضرر للأشخاص الذين جمعت عنهم البيانات، أو تنال من حقوقهم، أو من حرياتهم، والسبب في ذلك أن الهدف من تجميع البيانات ومعالجتها تمكين صاحبها من إجراء معاملاته إلكترونيا وليس الإضرار به والنيل من حرياته.

وعند تحويل تلك البيانات يجب توفير الحماية اللازمة والمناسبة لها وبصفة خاصة طبيعة المعلومات ومصدرها والدولة المرسلة لها والأغراض المراد معالجة البيانات لها فضلاً عن القانون الواجب التطبيق في الدولة المعنية والالتزامات الدولية لتلك الدولة وأي نظام أو سلوك أو قواعد ذات صلة مطبقة فيها، والإجراءات الأمنية المتخذة لحماية تلك البيانات في تلك الدولة مع الأخذ بالنظر إلى طبيعة البيانات الشخصية ومصدر المعلومات المضمنة في البيانات والإقليم الذي ينتهي إليه تحويل البيانات والأغراض المراد معالجة البيانات من أجلها ومدتها مع مراعاة القانون المطبق في الإقليم المعني ومدى التزام هذا الإقليم دولياً.

إن أغلب الدول التي سعت وبذلت جهود كبيرة في تقنين الحق في الخصوصية في إطار المعلوماتية والعالم الافتراضي وعدم العبث به، أو سوء استخدامه، وإعطاء الفرد الضمانات القانونية اللازمة وإن بدت هذه الضمانات هزيلة، ولا تكاد ترقى إلى المستوى الكافي لحماية البيانات الشخصية وحماية حياة الأشخاص

مجلة كامبريدج للبحوث العلمية: مجلة علمية محكمة
تصدر عن مركز كامبريدج للبحوث والمؤتمرات–العدد الحادي الاربعون – كانون الثاني ٢٠٢٥– رجب ١٤٤٦
ISSN-2536-0027

وحقوقهم لكنها سعت إلى إعادة التوازن بين السلطات ومعرفة الأشخاص الذين يشكلون موضوعا للحماية وما هي الحقوق المعترف لهم بها؟

ومن الضمانات التي اتفقت عليها أغلب الدول المتقدمة مثل فرنسا وأمريكا وأغلب دول الاتحاد الأوربي وهي كما يأتي :)[٣٦](١

أولًا: إعطاء الضمانة بالمحافظة على الحق بالسرية والنسيان

يجب الحفاظ على كل ما هو سري جدير بالحماية؛ لكيلا يتعرض صاحب هذه المعلومات لأضرار قد لا يمكن تصور مداها، فبنوك المعطيات الخاصة والعامة حوت عدداً كبيراً من المعلومات المتعلقة بالصحة الجسدية والعلاقات العائلية وبعض الخصوصيات الشخصية وإقاماتهم في الخارج وكذلك ملائمتهم المالية والملاحقات التي تحصل بحقهم من قبل الشرطة بوساطة المعلوماتية عندها تصبح المعلومات غير قابلة للشطب وتجمع في مركز واحد مما يسمح لمستعملها أن يحدد أي فرد كان بصورة دقيقة خاصة إذا ما أعطي لكل فرد رقم خاص به ومن ثم يتم التأكد من صحة المعلومات وفي حالة عدم وجود أية رقابة توجب إمكانية لتصحيح أو شطب المعلومات غير الصحيحة. وتكون هذه المعلومات عرضة للاستعمال غير المراقب للسرقة وعدم التكتم عليها بالشكل الذي تسمح به التقنية. لذلك نجد في القطاع العام تعمد السلطات إلى إخضاع الموظفين المكلفين بالكومبيوتر إلى سرية الوظيفة ويعمد القطاع الخاص في بعض المؤسسات الخاصة إلى إخضاع مستخدميها للسرية المهنية، لان مخاطر نشر هذه المعلومات أصبح كبيرا جدا ولا يمكن معالجته ما لم تكن السرية المهنية محمية بأحكام قانونية ولا يوجد أي أثر للسّرية ولحق النسيان في عصر العالم الافتراضي .)[٣٧](١

ثانيًا: إعطاء الضمانة للفرد تجاه السلطات العامة

بعد أن يُعْطي كلُّ مواطن رقماً خاصاً به، يتحول كل مواطن إلى رقم تجاه السلطات العامة، بحيث يمكن مخاطبته بطريقة أسهل مما لو كان شخصا حقيقيا، لكن هذا الأمر يدعو إلى القلق والتخوف من أن يقدم أي شخص على استعمال هذه المعلومات الموجودة في بنك المعلومات بطريقة غير سليمة لذلك قامت أغلب الدول وخاصة الصناعية منها باعتماد قوانين لحماية حياة الإنسان الخاصة ودول أخرى لا تزال في مرحلة وضع مشاريع لقوانين تكفل حماية البيانات وتضمن تطبيق هذه القواعد حسب المبادئ الدولية، وقد أعطيت الإدارات العامة بعض الامتيازات فيحق للمحقق العدلي مثلا القيام بجمع معلومات حتى لو كانت ممنوعة وتتعلق بالحياة الخاصة لكنها تصب في مصلحة الفرد، أو المصلحة العامة مع الاحتفاظ بحق الشخص في السرية، وهنا يثار تساؤل كيف تضمن عدم استخدام هذه المعلومات من سلطات أخرى غير السلطات القضائية التي قامت بالجمع؟ لذلك يجب اللجوء إلى معايير معينة لتسويغ الامتيازات التي تمنح لسلطات من دون غيرها وحسب المصلحة.

ثالثًا: إعطاء الضمانة للفرد تجاه السلطات الخاصة

قد يصبح الفرد تجاه السلطات الخاصة التي تملك المعلومات السرية المتعلقة به لعبه فقد تقوم بإرسال بياناته من مؤسسة إلى أخرى بدون أي عائق وبسرعة قصوى فمثلا، ماذا يحــل بالعامل الذي يطلب عملاً ويقوم بتسجيل اسمه في منشئ بنك المعلومات المستعملة من التنظيمات النقابية؟

رابعا: الحماية من عدم التوازن القائم بين السلطات

إن استعمال المعلوماتية في القطاع العام قد يخلق خللاً في مبدأ التوازن بين السلطات مما يجعل مبدأ انفصال السلطات المضمون في الدستور يتزعزع، فعندما تقدم السلطات الإدارية العامة على جمع المعلومات المتعلقة بالمواطنين يعطيها إمكانيات وقدرات هائلة جديدة يتم معها إعادة التوازن بين السلطات وذلك حماية

مجلة كامبريدج للبحوث العلمية: مجلة علمية محكمة
تصدر عن مركز كامبريدج للبحوث والمؤتمرات–العدد الحادي الاربعون – كانون الثاني ٢٠٢٥– رجب ١٤٤٦
ISSN-2536-0027

للديمقراطية نفسها، فالتقنية بحد ذاتها تصبح بمثابة السلطة مما يستوجب وضع لجان للمراقبة وإعطاء المواطن حقه في الكشف على الفيش مع الاحتفاظ بحق السلطة التشريعية. فالشركات العملاقة الخاصة بالوسائل التقنية المتطورة تتسلط على القدرات الاقتصادية التي تدخل في الأسواق لأنها تزود العقول الإلكترونية ببرامج مسبقة في هذا المجال تشكل مخاطر، وتسلط إلكتروني على أجهزة الدولة بشكل كبير جدا؛ لذلك لابد من إيجاد توازن، وحث السلطات على إتباع الوسائل الحديثة للحد من الاختراقات الإلكترونية من الشركات المقدمة للخدمات؛ لأنها تقدم الخدمة للجميع وبطرق مشروعة وغير مشروعة.

وإذا كان الحصول على المعلومات هو الغاية النهائية من استخدام شبكات الإنترنيت سواء كان بإرسالها أم نقلها لهذه المعلومات ليحصل عليها المتلقي كمعلومات نهائية، أو إدخالها في نظام معالجة أخر، وهذا يجعلنا نتساءل ما العلاقة بين الحرية والمسؤولية؟ أي حق الفرد في ممارسة حريته من جهة ومسؤوليته تجاه ما وضعه المجتمع الدولي في إطار فكرة النظام العام من جهة أخرى، وبما أن فكرة النظام العام نسبية، فإن تضارب الحريات يبلغ أشده في نطاق شبكة الإنترنيت، خاصة مع سمو مبدأ حرية انسياب المعلومات لخدمة كل مواطن والذي يرد عليه بعض القيود فيما يتعلق بمضمون وطبيعة المعلومات وبثها وكذلك استغلال قضاء الدولة وسلطتها في الرقابة على بث المعلومات .[١](٣٨)

وبما أن شبكة الإنترنيت أصبحت من أهم وسائل الإعلام المقروءة والأكثر تطوراً في عالم المتغيرات فإن حرية الإعلام يجب أن تتوازن على وفق واجباته من دون المساس بحريات الآخرين إلا بالقدر الذي تنظمه المبادئ التي تنظم حق النشر للخبر ونقده لضمان آمن للمجتمع والفرد والتزاماً بالوثائق التشريعية الدولية منها والداخلية المتعلقة بحقوق الإنسان وحرياته، كما أشرنا سابقاً أن البيانات الشخصية المتصلة بالحياة الخاصة للفرد غالباً ما يقدمها الشخص بنفسه أو قد تتوصل الهيئات إليها بوسيلة أو بأخرى فأن تهديد الحرية الشخصية يثور إذا ما أفشيت هذه المعلومات من دون موافقته، أو نشرت بشكل مغاير عن السابق، أو حورت بشكل مغاير، ولأهمية الخصوصية والحق في المعلومات تحتاج إلى توفير معيار منضبط يوازن بين احترام الحق في الخصوصية وخصوصية المعلومات تحديدا وبين الحق في المعلومات والوصول إليها ولكننا في ظل النقص التشريعي لهذين الحقين نجد أن كلا الحقين يهدران في مجتمع تتزايد فيه مخاطر انتهاك الخصوصية ولا تحمى فيه البيانات الشخصية من الاختراق وإساءة الاستخدام.

وفي هذا المجال يثار لدينا تساؤل مهم هل ثمة تعارض بين خصوصية المعلومات والحق في المعلومات؟ وأين يبدأ نطاق كل حق منها؟ وأين ينتهي؟ أثمة أثر مقيد للخصوصية في حق الإعلام وارتباطه بالحق في الرأي والتعبير أم إنها حقوق تتكامل في ظل معيار متوازن يدرك أثره ونطاق كل حق ومدى فعاليته؟

وقد أوضحنا سابقاً أن الخصوصية لا تعني حماية البيانات الشخصية؛ لأنّ الخصوصية على إطلاقها تنطوي على خصوصية البيانات وخصوصية الاتصالات في مواجهة أنشطة الرقابة والتجسس وخصوصية المكان وحرمته في مواجهة الاعتداء المادي وهي مسائل حرمة المسكن وحرمة الشخص من التفتيش غير القانوني وخصوصية المراسلات ومن ضمنها مراسلات مادية وأخرى إلكترونية وغيرها من أوجه الحماية ذات الطبيعة المادية أو المعنوية، أما حماية البيانات فهي جزء من الخصوصية وتتعلق بمواجهة الاعتداءات على البيانات الشخصية وتنظم الحق في البيانات الشخصية وسيطرة صاحبها عليها.

الفرع الثاني

ضمانات تدخل الدولة في البيانات الشخصية

هناك تساؤل مهم يطرح متى يجوز لسلطات الدولة أن تطلب الكشف عن إفشاء أسرار خاصة متعلقة ببعض الأفراد؟ أو الجماعات؟ وما هي الشروط التي تحد من سلطات الدولة في التدخل في خصوصيات مواطنيها؛

مجلة كامبريدج للبحوث العلمية: مجلة علمية محكمة
تصدر عن مركز كامبريدج للبحوث والمؤتمرات–العدد الحادي الاربعون – كانون الثاني ٢٠٢٥– رجب ١٤٤٦
ISSN-2536-0027

وهل هناك حالات تمكن الدولة من التدخل في خصوصيات الأفراد وتحت ذرائع مختلفة؟ على سبيل المثال لموازنة حق الخصوصية والأمن لأن الحريات الدستورية في أي دولة عصرية لابد أن تتعرض للخطر في فترات الحروب، أو أخطار واضطرابات من شأنها أن تحدث نتائج خطيرة وجوهرية تؤثر في مستقبل الوطن والأفراد، وفي هذه الحالة يجوز لسلطات الدولة أن تقوم بإجراءات قد تحد، أو تنظم حريات الأفراد وقد تضع بعض القيود على خصوصياتهم بشرط إلا تتعارض مع المبادئ الأساسية المنصوص عليها في الدستور.

لذلك نجد أن حق الخصوصية ليس مطلقا، كما أشرنا سابقا وترد عليه قيود واستثناءات ومصالح متنافسة معترف بها في مجال حماية المعلومات الشخصية في العالم الافتراضي، وفي الواقع العملي أن أغلب الدساتير الوطنية والقرارات القضائية والصكوك الدولية المتعلقة بحقوق الإنسان تسلم بوجود قيود واستثناءات محتملة لعدم التقييد، أو ورود حدود ومبدأ إمكانية ورود استثناءات أقرته أغلب الدول، وهذا المبدأ ينطوي على سلطة تقرير، وفرض قيود إذا كانت ضرورية لحماية الأمن القومي، أو النظام العام، أو الصحة العامة، أو الأخلاق العامة، أو لحماية حقوق الآخرين وهذه القيود مسموح بها لضمان العيش في بيئة آمنة)[٣٩] تكفل حماية حقوق الآخرين وحرياتهم وكذلك الحاجة إلى تطبيق القانون بصورة فعالة والتعاون القضائي في مكافحة الجرائم على الصعيد الدولي بمـــا في ذلك التهديدات التي يشكلها الإرهاب الدولي والجريمة المنظمة وتفسر معالجة البيانات الشخصية على وفق مبادئ حقوق الإنسان، وتكون الأهداف المحققة للمصلحة العامة مسوّغاً للتدخل في الحياة الخاصة إذا كانت الأهداف. أ) متفقة مع القانون، أي وجود أساس قانوني في القانون المحلي وهذا يتطلب إمكانية الوصول إلى المعلومات وإمكانية التنبؤ الأساس القانوني، وإمكانية التنبؤ هذه تستلزم الدقة الكافية لصياغة القاعدة بغية تمكن أي فرد من تنظيم سلوكه. ب) ضرورية في مجتمع ديمقراطي لتحقيق أهداف مشروعة. ج) أن يكون متناسباً مع الهدف المتوخى.

ومع إمكانية اطلاع الحكومات على قواعد البيانات الخاصة والعامة وقدرة الحكومات على شراء معلومات عن الأفراد لاستخدامها في مجال إنفاذ قواعد البيانات خاصة، وكثيرا ما يجري تجميع قواعد البيانات هذه بصورة طوعية ويجري تقاسمها طوعياً مع السلطات الحكومية، وبما أن الحكومات قادرة على شراء المعلومات متى ما رغبت، وقد أصبح من الضروري وضع، أو تحديد ضمانات تكفل عدم انتهاك خصوصية الشخص وبخلافه لا قيمة للشخصية، لذا الاحتفاظ بالبيانات وإمكانية الاطلاع على قواعد البيانات تضمنها الكفالة المسبقة للاطلاع، وقد أكدت اتفاقية مجلس أوربا رقم ١٠٨ لعام ١٩٨١ المتعلقة بحماية الأفراد فيما يتصل بالمعالجة الآلية للبيانات الشخصية، على مبادئ أساسية تتعلق بحماية طائفة معينة من البيانات وهي البيانات الحساسة المتعلقة بالأصل العرقي والآراء السياسية والمعتقدات الدينية والإيديولوجية وبيانات الحياة الصحية والجنسية، أو المتصلة بالأدلة الجنائية، وتقر الاتفاقية مبدأ حرية انتقال البيانات بين أطراف الاتفاقية التي تقدم حماية كافية للخصوصية وقد تمحورت هذه المبادئ حول ما يأتي:

١. وجوب مراعاة صحة ودقة البيانات التي يجري جمعها، وإن تكون كاملة ومستمدة بطرق مشروعة.
٢. تحديد المدة الزمنية لحفظ البيانات والأغراض المعالجة بشأنها.
٣. عدم إفشاء أو استعمال البيانات في غير الأغراض المخصصة لها.
٤. حق الشخص المعني في التعرف على البيانات المسجلة المتعلقة به وتصحيحها وتعديلها ومحوها إذا كانت غير صحيحة.
٥. توفير الحماية الأمنية الكافية والتي تلائم وتضمن عدم الوصول للبيانات أو استخدامها بشكل غير مشروع.

مجلة كامبريدج للبحوث العلمية: مجلة علمية محكمة
تصدر عن مركز كامبريدج للبحوث والمؤتمرات–العدد الحادي الاربعون – كانون الثاني ٢٠٢٥– رجب ١٤٤٦
ISSN-2536-0027

٦. تحديد الأشخاص والجهات المرخص لهم بالوصول والاطلاع على البيانات وإخضاعهم لقيد الالتزام بالسر المهني.
٧. ان تكون السياسة العامة للتطوير والتطبيق والحفظ معلنة ومتاحة للجميع خاصة البيانات ذات الطبيعة الشخصية.
٨. مسألة الأشخاص وكذلك الجهات المرخص لهم الوصول والاطلاع على البيانات ومعاقبتها وتحمل الأشخاص، أو الجهات المسؤولية عن الأضرار الناجمة عن إساءة استخدام البيانات.

الخاتمة

تلقت هذه المخاطر اهتماما متزايدا بضرورة حماية البيانات الشخصية قانونيا وتقنيا على الصعيدين الوطني والدولي، وهذا الاهتمام مستمر وغير متوقف. أحد الدوافع الرئيسية وراء تطوير تشريعات وقوانين في هذا المجال يعود إلى أن الإجراءات التقليدية لحماية خصوصية الأفراد وحياتهم الشخصية لا تكفي لتغطية كل جوانب الحقوق الشخصية، خاصة في ظل التحديات المتعلقة بجمع البيانات، تخزينها، والوصول إليها من خلال وسائل النقل الإلكترونية الحديثة التي تستهدف الخصوصية. هذه الضغوطات دعت العديد من الدول إلى إقرار تشريعات تضمن حماية بيانات الأفراد واحترام حقوقهم، واعتبرت هذه الخطوة مبررة للتدخل في خصوصياتهم. ومن أجل الحفاظ على الحقوق الشخصية بما في ذلك الحقوق العامة، سعت الدول إلى تحقيق توازن ملائم بين هذه الحقوق. وخلصت هذه الدراسة الي بعض النتائج والتوصيات نعرضها في الاتي؛

النتائج

أولا: الخطر التكنولوجي هو كل حالة تتضمن احتمالية حدوث نتائج غير مرغوب فيها أو خسارة، تهدد النشاط التقني، وتثير المسئولية المدنية عن وسيلة صناعية جديدة تعمل أو منتجات جديدة تطرح.

ثانيا: حالة إساءة استخدام الحاسوب هي جميع أنواع الأفعال التي تكون مرتبطة بوضوح بأجهزة الحاسوب والاتصالات المتعلقة بالبيانات التي تعرض ضحاياها إلى خسارة أو أضرار مالية أو شخصية أو التي يكون مرتكبوها قد حصلوا أو يمكن أن يحصلوا على كسب غير مشروع منها.

ثالثا: شيوعَ النقل الرقمي للبيانات خلق مشكلة أمنية وطنية، إذ سهل استراق السمع والتجسس الإلكتروني، ففي مجال نقل البيانات تتبدى المخاطر المهددة للخصوصية في عدم قدرة شبكات الاتصال على توفير الأمان في سرية ما ينقل من خلالها من بيانات.

رابعا: شبكة الإنترنيت أصبحت من أهم وسائل الإعلام المقروءة والأكثر تطوراً في عالم المتغيرات فإن حرية الإعلام يجب أن تتوازن على وفق واجباته من دون المساس بحريات الآخرين إلا بالقدر الذي تنظمه المبادئ التي تنظم حق النشر للخبر ونقده لضمان آمن للمجتمع والفرد

التوصيات

أولاً: ضرورة توفير مجموعة من الوسائل والإجراءات التي تحقق الحماية من الأحداث المستقبلية غير المرغوب فيها والتي تعتبر بمثابة تهديدات لنظام المعلومات الذي يحمي البيانات الشخصية ذاتها لأنها تؤدي إلى حدوث إخلال بالأمن وفقدان التكامل والدقة داخل النظام.

ثانياً: ضرورة وجود مجموعة من الإجراءات والأساليب التي تهدف إلى تحقيق الحماية للنظام من أي أحداث مستقبلية تهدد النظام وتؤدي إلى فقد المعلومات أو عدم دقتها، وبالأخص فقد سرية البيانات. ومن ثم يمكن إجمال مخاطر حماية سلامة البيانات وصحتها.

ثالثا: يجب الحفاظ على كل ما هو سري جدير بالحماية؛ لكيلا يتعرض صاحب هذه المعلومات لأضرار قد لا يمكن تصور مداها، فبنوك المعطيات الخاصة والعامة حوت عدداً كبيراً من المعلومات المتعلقة بالصحة

ISSN-2536-0027

الجسدية والعلاقات العائلية وبعض الخصوصيات الشخصية وإقاماتهم في الخارج وكذلك ملائمتهم المالية والملاحقات التي تحصل بحقهم من قبل الشرطة بوساطة المعلوماتية عندها تصبح المعلومات غير قابلة للشطب وتجمع في مركز واحد.

قائمة المراجع:

أولا: المراجع القانونية

١- أحمد عبد السلام أبو موسى: أهمية مخاطر نظم المعلومات المحاسبية الإلكترونية – دراسة تطبيقية على المنشآت السعودية المحلية العلمية، التجارة والتمويل، مصر، كلية التجارة – جامعة طنطا، ٢٠٠٤.

٢- سعيد سعد عبد السلام: مشكلة تعويض أضرار البيئة التكنولوجية، مصر، دار النهضة العربية، ٢٠٠٨.

٣- السيد عبد المقصود دبيان وآخرون: نظم المعلومات المحاسبية وتكنولوجيا المعلومات، مصر، الدار الجامعية، ٢٠٠٤.

٤- عبد الله سلامة: الخطر والتأمين، الطبعة السابعة، مصر، مكتبة دار النهضة العربية، ١٩٨٦.

٥- عبد الوهاب نصر، شحاتة السيد: مراجعة الحسابات في بيئة الخصخصة وأسواق المال والتجارة الإلكترونية، الإسكندرية، الدار الجامعية –٢٠٠٤.

٦- محمد شكري سرور: التأمين ضد الأخطار التكنولوجية، مصر، دار الفكر العربية، ١٩٨٧.

٧- محمد عبد المحسن المقاطع: حماية الحياة الخاصة للأفراد وضماناتها في مواجهة استخدام الحاسوب الآلي، ذات السلاسل للطباعة والنشر، ١٩٩٢.

٨- نعيم مغبغب: مخاطر المعلوماتية والإنترنت، الطبعة الثانية، لبنان، منشورات الحلبي الحقوقية، ٢٠٠٨.

ثانيا: المجلات والمنشورات والمقالات

١- حسين بن سعيد الغامزي: الحماية القانونية للخصوصية المعلوماتية، بحث مقدم لمؤتمر آمن المعلومات والخصوصية في ظل قانون الإنترنيت، القاهرة، ٢٠٠٨.

٢- فضيلة محمد فتوح: توحيد النظم في بنوك المعلومات وإمساك الدفاتر الاجتماعية والسرية، المجلة الدولية للعلوم الاجتماعية، ع١١، س ٣، ١٩٧٣.

٣- كاسر نصر المنصور: إدارة المخاطر واستراتيجية التأمين في ظل تكنولوجيا المعلومات، المؤتمر العلمي الدولي السابع، إدارة المخاطر واقتصاد المعرفة، الأردن، ٢٠٠٧.

٤- كاسر نصر المنصور: أسس تنظيم العلاقة بين الصيغ التكنولوجية والصيغ التنظيمية، مجلة التعاون الصناعي في الخليج العربي، العدد ٨٣، السنة الحادية والعشرون، يناير ٢٠٠١.

٥- كاسر نصر المنصور، وآخرون، تكثيف استخدام التكنولوجيا المعلومات في الصناعة العربية وصولا إلى مستويات التصنيع العالمية، المؤتمر العلمي السنوي الثاني، جامعة الزيتونة الأردنية، عمان، ٢٠٠٢.

٦- محمد رشدي: الإنترنيت والجوانب القانونية لنظم المعلومات، بحث مقدم، مؤتمر الإعلام والقانون، كلية القانون، جامعة حلوان، ١٩٩٩.

٧- محمد فتحي الشاذلي: المعلوماتية وأثارها على البيئة الإنسانية، مجلة السياسة الدولية، ع٧٧، ١٩٨٤.

ISSN–2536–0027

٨- ممدوح خليل بحر: الحماية القانونية لبرامج الكمبيوتر وأثرها في الأمن القومي العربي، بغداد: مجلة الأمن العام، ع ١، س ١٢، ١٩٩٢.

ثالثا: المواقع الإلكترونية

١- الموقع الإلكتروني لمقال منشور تحت عنوان " تقييم وإدارة المخاطر". المنتدى العربي لإدارة الموارد البشرية، بتاريخ ٢٠٠٨/١٢/١٠.. WWW.hrdiscussion.com

رابعا: المراجع الأجنبية

Calheriene Crump, data, retention: privacy and Accountability online, Stanford law review, vol.٥٦ (٢٠٠٣ – ٢٠٠٤) pp. ١٩١ – ٢٢٠.

Information Technical Committee، "Technical Pronouncements on Information Technology"، IFAC Handbook، July، ٢٠٠٠ P.٤. (WWW.IFAC.Com).

JEAN BAPTISTE, FARESSOZ. L'apocalypse joyeuse. Seuil, Paris, ٢٠١٢, p ١٢.

R Y A N S.D BARDALAI، "Evaluating Security Threats in Mainframe and Client / Server Environments"، The CPA Journal. Vo١. ٣٠، ١٩٩٧، ١٣٧-١٤٢. (WWW.nysscpa /cpa Journal/١٩٩٧).

RUSSELL, Roberts and Taylor, Bernard W., (١٩٩٥), Production and Operations Management, Englewood Cliffs N.J.,p.٢٩٨..

RUSSELL, Roberts and Taylor, Bernard W., (١٩٩٥), Production and Operations Management, Englewood Cliffs N.J.,p.٢٩٩..

TURBAN, E., Mclean &. Wetherbe J.,J., Information Technology for Management, John Wiley, Inc. New York,١٩٩٦m p.٦.

---

[1] JEAN BAPTISTE, FARESSOZ. L'apocalypse joyeuse. Seuil, Paris, ٢٠١٢,p ١٢.

[2] د. محمد شكري سرور، التأمين ضد الأخطار التكنولوجية، مصر، دار الفكر العربية، ١٩٨٧، ص١٤ وما بعدها.

[3] د. محمد شكري سرور، التأمين ضد الأخطار التكنولوجية، المرجع السابق، ص١٤ ومابعدها.

[4] د. سعيد سعد عبد السلام، مشكلة تعويض أضرار البيئة التكنولوجية، مصر، دار النهضة العربية، ٢٠٠٨، ص ٢٤.

[5] مقال منشور تحت عنوان " تقييم وإدارة المخاطر". المنتدى العربي لإدارة الموارد البشرية، بتاريخ ٢٠٠٨/١٢/١٠. WWW.hrdiscussion.com

[6] في هذا المعنى: عبد الله سلامة، الخطر والتأمين، الطبعة السابعة، مصر، مكتبة دار النهضة العربية، ١٩٨٦، ص ١٧ وما بعدها.

[7] كاسر نصر المنصور، إدارة المخاطر واستراتيجية التأمين في ظل تكنولوجيا المعلومات، المؤتمر العلمي الدولي السابع، إدارة المخاطر واقتصاد المعرفة، الأردن، ٢٠٠٧، ص ٢٠٠.

[8] د. محمد شكري سرور، التأمين ضد الأخطار التكنولوجية، المرجع السابق، ص١٧.

مجلة كامبريدج للبحوث العلمية: مجلة علمية محكمة
تصدر عن مركز كامبريدج للبحوث والمؤتمرات–العدد الحادي الاربعون – كانون الثاني ٢٠٢٥– رجب ١٤٤٦
ISSN–2536–0027

[٩٥] انظر تقرير لجنة روزا الفرنسية، عام ١٩٦٩، المشكلة من ممثلين عن شركات التأمين والشركات الصناعية والخاصة لدراسة المجموعات الصناعية المتكاملة لمزيد من التفاصيل د. سعيد سعد عبد السلام، مشكلة تعويض أضرار البيئة التكنولوجية، المرجع السابق، ص ٢٥.

[١٠٥] د. محمد شكري سرور، التأمين ضد الأخطار التكنولوجية، المرجع السابق، ص٢٣.

[١١٥] د. سعيد سعد عبد السلام، مشكلة تعويض أضرار البيئة التكنولوجية، المرجع السابق، ص٢٦ وما بعدها.

[١٢٥] د. سعيد سعد عبد السلام، مشكلة تعويض أضرار البيئة التكنولوجية، المرجع السابق، ص٢٧.

[١٣٥] المرجع نفسه، ص٢٧.

[١٤٥] كاسر نصر المنصور، وآخرون، تكثيف استخدام التكنولوجيا المعلومات في الصناعة العربية وصولا إلى مستويات التصنيع العالمية، المؤتمر العلمي السنوي الثاني، جامعة الزيتونة الأردنية، عمان، ٢٠٠٢، ص٢٣٦.

[١٥٥] - RUSSELL, Roberts and Taylor, Bernard W., (١٩٩٥), Production and Operations Management, Englewood Cliffs N.J.,p.٢٩٨..

[١٦٥] - RUSSELL, Roberts and Taylor, Bernard W., (١٩٩٥), Production and Operations Management, Englewood Cliffs N.J.,p.٢٩٩..

[١٧٥] كاسر نصر المنصور، أسس تنظيم العلاقة بين الصيغ التكنولوجية والصيغ التنظيمية، مجلة التعاون الصناعي في الخليج العربي، العدد ٨٣، السنة الحادية والعشرون، يناير ٢٠٠١، ص ٢٨.

[١٨٥] كاسر نصر المنصور، إدارة المخاطر واستراتيجية التأمين في ظل تكنولوجيا المعلومات، المرجع السابق، ص١٩.

[١٩٥] - TURBAN, E., Mclean &. Wetherbe J.,J., Information Technology for Management, John Wiley, Inc. New York,١٩٩٦m p.٦.

[٢٠٥] د. ممدوح خليل بحر، الحماية القانونية لبرامج الكمبيوتر وأثرها في الأمن القومي العربي، بغداد: مجلة الأمن العام، ع ١، س ١٢، ١٩٩٢، ص ١٢١.

[٢١٥] لقد لخص " آرثر ميلر " المتاعب المتولدة من الحاسوب إذ يرى (أن الكمبيوتر بشراهته التي لا تشبع في جمعه للمعلومات، وما هو معروف عنه من دقة وعدم نسيان أي شيء يوضع فيه، قد تنقلب معه الحياة راساً على عقب فيخضع الأفراد لنظام رقابي مشدد يتحول معه المجتمع إلى عالم شفاف ترقد فيه عارية بيوت الناس ومعاملاتهم المالية لأي مشاهد). مشار إليه لدى د. ممدوح خليل بحر، الحماية القانونية لبرامج الكمبيوتر وأثرها في الأمن القومي العربي، المرجع السابق، ص ١٦.

[٢٢٥] د. محمد فتحي الشاذلي، المعلوماتية وأثارها على البيئة الإنسانية، مجلة السياسة الدولية، ع٧٧، ١٩٨٤، ص ١٠٤.

[٢٣٥] د. فضيلة محمد فتوح، توحيد النظم في بنوك المعلومات وإمساك الدفاتر الاجتماعية والسرية، المجلة الدولية للعلوم الاجتماعية، ع١١، س ٣، ١٩٧٣، ص ١٧٩ – ١٨٠.

[٢٤٥] Charles R. wagner، the CPA and computer fraud، New-yourk، P..

[٢٥٥] Information Technical Committee، "Technical Pronouncements on Information Technology"، IFAC Handbook، July، ٢٠٠٠ P.٤. (WWW.IFAC.Com).

[٢٦٥] عبد الوهاب نصر، شحاتة السيد، مراجعة الحسابات في بيئة الخصخصة وأسواق المال والتجارة الإلكترونية، الإسكندرية، الدار الجامعية –٢٠٠٤، ص٢٧٧.

[٢٧٥] للمزيد أنظر:

Information Technology Committee، op.cit، p p٥.٦.

مجلة كامبريدج للبحوث العلمية: مجلة علمية محكمة
تصدر عن مركز كامبريدج للبحوث والمؤتمرات–العدد الحادي الاربعون – كانون الثاني ٢٠٢٥– رجب ١٤٤٦
ISSN–2536–0027

[٢٨] السيد عبد المقصود دبيان، وآخرون، نظم المعلومات المحاسبية وتكنولوجيا المعلومات، مصر، الدار الجامعية، ٢٠٠٤، ص٥٥١-٥٥٢.

[٢٩] السيد عبد المقصود دبيان، وآخرون، نظم المعلومات المحاسبية وتكنولوجيا المعلومات، المرجع السابق، ص٥٥١-٥٥٢ وما بعدها.

[٣٠] السيد عبد المقصود دبيان، وآخرون، نظم المعلومات المحاسبية وتكنولوجيا المعلومات، ص٥٥٥ وما بعدها.

[٣١] د. أحمد عبد السلام أبو موسى، أهمية مخاطر نظم المعلومات المحاسبية الإلكترونية – دراسة تطبيقية على المنشآت السعودية المحلية العلمية، التجارة والتمويل، مصر، كلية التجارة – جامعة طنطا، ٢٠٠٤، ص٤.

[٣٢] د. أحمد عبد السلام أبو موسى، أهمية مخاطر نظم المعلومات المحاسبية الإلكترونية – دراسة تطبيقية على المنشآت السعودية المحلية العلمية، المرجع السابق، ص٤ وما بعدها.

[٣٣] للمزيد يمكن الرجوع إلى:

R Y A N S.D BARDALAI، "Evaluating Security Threats in Mainframe and Client / Server Environments"، The CPA Journal. Vo١. ٣٠، ١٩٩٧، ١٣٧-١٤٢. (WWW.nysscpa /cpa Journal/١٩٩٧).

[٣٤] د. حسين بن سعيد الغامزي، الحماية القانونية للخصوصية المعلوماتية، بحث مقدم لمؤتمر آمن المعلومات والخصوصية في ظل قانون الإنترنيت، القاهرة، ٢٠٠٨، ص ٩ – ١٣.

[٣٥] المادة (٤٥) من مشروع قانون المعاملات الإلكتروني العماني، الحماية القانونية للخصوصية المعلومات، ٢٠٠٨، ص ١٢.

[٣٦] د. نعيم مغبغب، مخاطر المعلوماتية والإنترنت، الطبعة الثانية، لبنان، منشورات الحلبي الحقوقية، ٢٠٠٨، ص ٢٣٢ – ٢٣٩.

[٣٧] د. محمد عبد المحسن المقاطع، حماية الحياة الخاصة للأفراد وضماناتها في مواجهة استخدام الحاسوب الآلي، ذات السلاسل للطباعة والنشر، ١٩٩٢، ص ١٣٢.

[٣٨] محمد رشدي، الإنترنيت والجوانب القانونية لنظم المعلومات، بحث مقدم، مؤتمر الإعلام والقانون، كلية القانون، جامعة حلوان، ١٩٩٩، ص ٣٥.

[٣٩] (١) Calheriene Crump , data , retention: privacy and Accountability online , Stanford law review , vol.٥٦ (٢٠٠٣ – ٢٠٠٤) pp. ١٩١ – ٢٢٠.