العنوان:	مخاطر التقنيات الحديثة وبرمجيات إدارة الوثائق على خصوصية الأفراد والهيئات
المصدر:	Cybrarians Journal
الناشر:	البوابة العربية للمكتبات والمعلومات
المؤلف الرئيسي:	مقلد، أشرف عمر وهبة
المجلد/العدد:	ع50
محكمة:	نعم
التاريخ الميلادي:	2018
الشهر:	يونيو
الصفحات:	1 - 52
رقم MD:	961699
نوع المحتوى:	بحوث ومقالات
اللغة:	Arabic
قواعد المعلومات:	HumanIndex
مواضيع:	الخصوصية، أمن المعلومات، أمن المعلومات الحاسوبية، أمن نظم المعلومات، الجريمة المعلوماتية، إدارة الوثائق، المستودعات الرقمية
رابط:	http://search.mandumah.com/Record/961699

Cybrarians Journal

Issue 50, June 2018 العدد 50، يونيو 2018

Dangers of Modern technologies & Documents management programs on individuals' and Corporates' Privacy

Ashraf Maklad
School Librarian, Ministry of Education, Egypt
Ph.D. Candidate, Department of Libraries and information, Documents and Archives Branch
Faculty of Art, Alexandria University, Egypt
ashrafomar78@yahoo.com

Abstract:

Modern technologies and records management programs provide communications and records management fields with many critical services which help accelerating human and administrative communications vanishing both time and place restrictions. But these technologies became a kind of threat to individuals' and corporates' privacies because of its ability to hack privacy, and stealing information and/ or private or secret data using any type of unauthorized or illegal methods.

So, it became a must to be careful when dealing with modern technologies; specially programs and applications of cell phones and computers which connected to internet; NOT giving it any access permissions for private or secret data and/ or information except what corporates' privacy policy's allow to be public or by private access permission. So, individuals should reduce their personal use for these technologies and applications and should NOT save their personal information, data, photos, and documents in cell phones' memories or computers' web based depositories for saving their privacy and protect it from any type of hacking or unauthorized use.

مخاطر التقنيات الحديثة وبرمجيات إدارة الوثائق على خصوصية الأفراد والهيئات

أشرف مقلد
أخصائي أول وثائق ومكتبات بالتربية والتعليم
باحث دكتوراه بقسم المكتبات والمعلومات (تخصص الوثائق والأرشيف)
كلية الآداب – جامعة الإسكندرية، مصر
ashrafomar78@yahoo.com

المستخلص

توفر التقنيات الحديثة وبرمجيات إدارة الوثائق العديد من الخدمات المهمة في مجالي التواصل البشري، وإدارة الوثائق في آن واحد والتي تساعد على سرعة التواصل البشري والإداري دون الالتفات للحواجز الزمنية والمكانية .ولكن هذه التقنيات مثلت خطرا على خصوصية كلا من الأفراد والهيئات أو الكيانات الاعتبارية في الوقت ذاته وذلك من خلال قدرتها على انتهاك الخصوصية والحصول على معلومات و /أو بيانات خاصة أو سرية أو غير مصرح بها بأشكال وطرق مختلفة .

ويجب الحذر عند التعامل مع البرمجيات الحديثة خصوصا تلك البرمجيات أو التطبيقات المستخدمة في الهواتف والحاسبات المتصلة بشبكة الانترنت وعدم منحها أية أذون ولوج للمعلومات أو البيانات الخاصة والسرية إلا بالقدر الذي تسمح له سياسة الخصوصة لدى الجهة الإدارية أو الكيان الاعتباري .كما يجب على مستوى الأفراد الاقتصاد قدر الإمكان في استخدام مثل هذه التطبيقات أو البرمجيات وفي احتفاظهم بمعلومات أو بيانات أو صور أو وثائق خاصة بهم على الهواتف والحاسبات المتصلة بالويب وذلك للاحتفاظ بخصوصيتهم وحمايتهم من أي عمليات اختراق أو استغلال أو انتهاك للخصوصية.

المقدمة المنهجية:

أهمية الدراسة:

تكتسب هذه الدراسة أهميتها من معالجتها لموضوع غاية في الأهمية ولصيق الصلة بحياة أغلب البشر في الوقت الحالي ألا وهو خصوصية الأفراد والهيئات وما تمثله التكنولوجيا الحديثة وتطبيقات الانترنت بالحاسبات والهواتف المحمولة وبرمجيات إدارة الوثائق من مخاطر على هذه الخصوصية، وما قد يترتب على انتهاك خصوصية الأفراد أو الهيئات من نتائج سلبية قد تضر آحاد الناس وربما يصل ضررها لدول بأكملها.

مشكلة الدراسة:

تتلخص مشكلة هذه الدراسة في ظهور العديد من المخاطر التي قد تسببها التقنيات الحديثة وبرمجيات إدارة الوثائق على خصوصية كلا من الأفراد والهيئات، سواء نتجت هذه المخاطر عن سوء استخدام الأفراد لها أو كوسائل من الغير للسيطرة على الأفراد أو الهيئات من خلال الوصول لمعلومات سرية/ غير مصرح بها أو بيانات خاصة.

أسباب اختيار الموضوع:

وقع اختيار الباحث على هذا الموضوع للدراسة لما شهدته الأعوام الأخيرة من تكرار لحوادث انتهاك الخصوصية للأفراد والهيئات في العديد من مناطق ودول العالم – ومنها مصر والمنطقة العربية – وما تشهده هذه النوعية من التقنيات من تطورات كبيرة ما زالت تزداد وتتسارع كل يوم.

منهج الدراسة:

تتبع الدراسة المنهج الوصفي التحليلي من خلال رصد أهم المخاطر التي تمثلها التقنيات الحديثة وبرمجيات إدارة الوثائق على خصوصية الأفراد والهيئات وجمعها وتحليلها وتفسيرها والخروج بنتائج تساعد في

معالجة مشكلة الدراسة بالشكل المفيد الذي يساعد على حماية خصوصية الأفراد والهيئات عند التعامل مع التقنيات الحديثة.

أهداف الدراسة:

تتلخص أهداف الدراسة في بضع نقاط هي:

1) رصد التقنيات التي تمثل خطرا أو أكثر على خصوصية الأفراد والهيئات.
2) استعراض أهم المخاطر التي تمثلها التقنيات الحديثة على خصوصية الأفراد والهيئات.
3) دراسة الطرق والوسائل المختلفة لانتهاك خصوصية الأفراد والهيئات باستخدام التقنيات الحديثة وبرمجيات إدارة الوثائق.
4) تقديم التوصيات التي تساعد على تجنب التعرض لمخاطر التقنيات الحديثة انتهاك خصوصية الأفراد والهيئات.

الدراسات السابقة والمثيلة:

اهتم العديد من الباحثين والأكاديميين بقضية الخصوصية وبمناظير عدة منها المنظور القانوني والتشريعي، والمنظور الاجتماعي، والمنظور الإنساني. وقد أجريت الدراسات حول أهمية احترام الخصوصية والمخاطر المحتملة عليها خصوصا مع التطور التكنولوجي الكبير الحادث في العقدين الآخيرين. ومن هذا المنظور الأخير ظهرت الحاجة لإجراء الدراسات العلمية حول مخاطر التكنولوجيا الحديثة على خصوصية

الأفراد والهيئات خاصة في مجال إدارة الوثائق التي تحوي بطبيعتها الكثير من البيانات الشخصية والخاصة بالأفراد والهيئات والتي تحتاج لمراقبة وضبط وسيطرة أكبر تساعد على المحافظة على خصوصية كلا من الأفراد والهيئات؛ ومن الدراسات التي أجريت حول هذه النقاط المتعلقة بالخصوصية:

1. **يونس عرب (2006) . المخاطر التي تتهدد الخصوصية وخصوصية المعلومات في العصر الرقمي .ـ المركز الوطني للتوثيق: قاعدة المعطيات حول التنمية الاقتصادية والاجتماعية.** متاح في https://goo.gl/WRfBH1

يتناول هذا المقال تأثير التقنية الحديثة وتكنولوجيا المعلومات على الخصوصية. ويبدأ بإلقاء الضوء على خطورة التكنولوجيا الحديثة على الحياة الخاصة وخصوصية المجتمع والأفراد وحتى الأفكار، ثم شرع المقال في وصف قدرة التكنولوجيا الحديثة في جمع وتخزين المعلومات والبيانات بأشكال وصور متعددة سواء في شكل مكتوب أو مسموع أو مرئي وقدرتها على الوصول والنفاذ لأخص خصوصيات الأفراد من خلال المراقبة الدائمة والمستمرة لأنشطة الأفراد سواء على الانترنت أو في الحياة اليومية العامة والخاصة.

وركز المقال على خطورة نقل البيانات على شبكة الانترنت على الخصوصية حتى على مستوى الأمن القومي فبحسب المقال " في مجال نقل البيانات تتبدى المخاطر المهددة للخصوصية في عدم قدرة شبكات الاتصال على توفير الأمان المطلق أو الكامل لسرية ما ينقل عبرها من بيانات و إمكانية استخدام الشبكات في الحصول بصورة غير مشروعة ، عن بعد على المعلومات"

ثم استعرض المقال مخاطر الخصوصية في بيئة الإنترنت والتجارة الإلكترونية وذلك بسبب القدرة الفائقة للانترنت على جمع البيانات والمعلومات عن الأشخاص ورصد أنشطتهم على الانترنت ومتابعة تحركاتهم ووقفاتهم على الشبكة العنكبوتية ومعالجة هذه البيانات والمعلومات وإ عادة استخدامها أو إفشائها أو تناقلها بين

قطاعات معنية والتنبؤ بتحركات أصحابها خصوصا مع التنامي المتسارع لحركة التجارة الالكترونية على مستوى العالم.

وفي النهاية نبه المقال إلى خطورة تقنيات فك الارتباط أو الكوكيز Cookies على خصوصية مستخدمي الانترنت فهي قادرة على النفاذ إلى نظم التشغيل في الحاسبات والاستيلاء على معلومات أصحابها بشكل يشكل تهديدا خطيرا للخصوصية. بالإضافة لخطورة محركات البحث واستخدامها لقواعد بياناتها التي تضم معلومات خاصة جدا عن كل مستخدميها مثل المواقع وأرقام الهواتف والبريد الالكتروني .... الخ وإمكانية متاجرتها بقواعد بياناتها تلك ضد خصوصية مستخدميها سواء بعلمهم أو بغير علمهم. كما عرج على خطورة وسائل الدفع الالكترونية ومساسمها بخصوصية الأفراد وخطورتها على معاملاتهم المالية. وما تمثله وسائل الاتصال اللاسلكية من خطورة على الخصوية المعلوماتيه والمادية لمستخدمي الانترنت من خلال قدرتها على تتبع المستخدمين ورصد تحركاتهم بشكل كامل.

2. **Mendel, Toby et al. (2012). Global survey on Internet Privacy and Freedom of Expression. - UNESCO Series on Internet Freedom. - Paris (France): UNESCO− . PDF. Available at;** http://unesdoc.unesco.org/images/0021/002182/218273e.pdf

صدرت هذه الدراسة المسحية عن منظمة الأمم المتحدة للتربية والعلوم والثقافة (اليونسكو) عام 2012 وناقشت كيف تسبب الانترنت في تغيير طبيعة التهديدات التي تتعرض لها الخصوصية، والتهديدات الرئيسة

للخصوصية في العصر الرقمي. كما استعرضت الأشكال الجديدة للمعلومات الشخصية والقدرات الجديدة للحكومات والأشخاص في تحليل تلك المعلومات، وفرص الاستخدام التجاري للبيانات الشخصية.

وقد قدمت الدراسة نظرة عالمية عامة لأهم التحديات التي تواجه حماية الخصوصية على الانترنت وفرص مواجهة هذه التحديات. وعرضت أهم مبادرات حماية الخصوصية وإخفاء الهوية عبر الإنترنت، وأدوار ومسؤوليات مقدمي الخدمات والوسطاء، والتحديات الخاصة التي تطرحها التطبيقات المختلفة مثل، منصات الاتصالات ونماذج الأعمال، والحوسبة السحابية، ومحركات البحث، وشبكات التواصل الاجتماعي، والمخاطر المبنية على استخدام الهواتف المحمولة والذكية واستخدام الانترنت عبر الأجهزة المحمولة، والمعرفات الفريدة للمواطنين ومبادرات الحكومة الالكترونية. كما ناقشت الدراسة التهديدات التي تفرضها آليات مختلفة للمراقبة وجمع البيانات مثل، تعريف المستخدم على الانترنت – المعرفات الفريدة وملفات تعريف الارتباط وأشكال أخرى لتحديد هوية المستخدم – وقيام برامج الإعلانات المتسللة وبرامج التجسس والبرامج الضارة بإجراء عمليات مراقبة وتسجيل للبيانات السرية، وتفتيش الحزم العميقة (DPI)، وتقنية الموقع الجغرافي، وبرامج معالجة البيانات والتعرف على الوجه.

كما استعرضت الدراسة البيئة القانونية واللائحية العالمية لحماية الخصوصية وحرية التعبير وقامت باجراء مسح لحالة البيئة القانونية واللائحية لحماية الخصوصية في عدد من الدول هي: الصين، والهند، ومصر، وفرنسا، والأرجنتين، والمكسيك، والولايات المتحدة الأمريكية، ونيجيريا، وجنوب أفريقيا.

وخلصت الدراسة لوجود تقاطعات بين الخصوصية وحرية التعبير تتمثل في تأثير ضعف حماية الخصوصية على حرية التعبير. والتوترات بين حرية التعبير والخصوصية فيما يتعلق بالمصلحة العامة، والتناقض بين الخصوصية حماية البيانات. ونطاق حماية الخصوصية فيما يتعلق بالاختصاص القضائي في الاطلاع على أو نشر معلومات شخصية.

وفي الأخير أوصت الدراسة بضرورة اتخاذ بعض التدابير لحماية الخصوصية على مستوى العالم وأن يتم توحيد هذه التدابير على مستوى العالم والعمل على نفاذها داخل الدول تنقسم لتدابير دستورية، وقانونية مدنية

وجنائية وتنظيمية، وتوحيد سيادات الشركات والكيانات فيما يخص الخصوصية واحترام وحماية البيانات الشخصية، وزيادة الوعي لدى الأفراد حولالخصوصية وحماية بياناتهم واحترام بيانات الغير.

3. **Ajayi, E. F. G. (August 2016) Challenges to enforcement of cyber-crimes laws and policy. Academic Journals ; Journal of Internet and Information Systems. Vol. 6(1). pp. 1-12. Available at**;
https://www.academicjournals.org/journal/JIIS/article-full-text-pdf/930ADF960210

يناقش هذا المقال أنواع الجرائم الالكترونية المختلفة ويقارن بين الجريمة الحاسوبية والجريمة السيبرانية ويوضح الفارق بين كلا الجريمتين ويركز على أن الجريمة السيبرانية هي معنى عام لكل أنواع الجرائم الالكترونية المرتبطة بالاتصالات والانترنت والتي يستخدم فيها الحاسوب وأجهزة الاتصالات الأخرى للاستيلاء على المعلومات أو تدمير البرمجيات.

في البداية ذكر المقال دوافع الجريمة السيبرانية وبعض التشريعات والإجراءات التي تم وضعها في مناطق مختلفة حول العالم ومن قبل هيئات وكيانات عدة بهدف مواجهة الجريمة السيبرانية وتحديدها. ثم ذكر المقال الصعوبات التي تواجه المختصين في تحديد هوية المجرمين السيبرانيين الذين عادة ما يتخفون خلف أسماء مستعارة ويستخدمون برمجيات متقدمة لإخفاء هوياتهم الحقيقية، والتعمية على أماكن تواجدهم.

وركز المقال على أهم التحديات التي تواجه انفاذ قوانين مواجهة الجرائم السيبرانية وأهمها، تحديد هوية المجرمين السيبرانيين، والتحديات التشريعية التي تتمثل في: تنازع الاختصاص القضائي أو عدم تحديده في قضايا الجرائم السيبرانية سواء اذا كان اختصاصا ولائيا يخص ولاية المحكمة على الدعوى الجنائية أو اختصاصا جغرافيا بجواز نظر الدعوى في ولاية أو اقليم أو دولة بعينها. وهناك التحدي المتعلق بعمليات تسليم المجرمين السيبرانيين حيث أن كثير من الدول ترفض تسليم المجرمين السيبرانيين الفاريين إليها من دول أخرى

أو الذين ارتكبوا جرائم اليكترونية في ولايات قضائية أخرى وهم مقيمين بأرضها في حين لا يوجد في القانون الدولي ما يلزم الدول على ذلك.

كما ركز المقال على التحديات المتعلقة بصعوبة توفير الأدلة الدامغة ضد مرتكبي الجرائم الالكترونية نظرا لعدم وجود تقارير فعالة و ندرة في البيانات، وارتفاع التكلفة والوقت والجهود المبذولة في التحقيق والملاحقة القضائية، وعدم وجود تشريعات كافية وعدم فعالية التشريعات الموجودة، وتفتقار القانون الدولي لآليات التنفيذ وتطبيقه ليلائم الظروف المحلية لكل دولة، وسوء التدريب وضعف الأجر ونقص الحماية لوكالات إنفاذ القانون، وندرة الخبراء في ملاحقة الجرائم السيبرانية.

وفي النهاية أوصى المقال بضرورة وضع قانون عالمي موحد لمكافحة الجريمة السيبرانية على أن يكون قابلا للتطبيق على نطاق دولي بولاية قضائية واحدة بحيث يمكن احتجاز المجرمين السيبرانيين من أي مكان في العالم ومحاكمتهم بغض النظر عن المكان الذي ارتكبوا فيه جرائمهم.

حدود الدراسة:

الحدود الموضوعية:

تتناول الدراسة مخاطر التقنيات الحديثة وبرمجيات إدارة الوثائق على خصوصية الأفراد والهيئات.

الحدود المكانية:

تغطى الدراسة مخاطر انتهاك الخصوصية من خلال التقنيات الحديثة في أي مكان في العالم.

الحدود الزمنية:

تغطى الدراسة الفترة من بداية الاعتماد على الحاسب الآلي وتكنولوجيا الاتصالات الحديثة والانترنت في إدارة حياة الأفراد وتيسير عمل الهيئات وإدارة الوثائق حتى نهاية 2016.

مصطلحات الدراسة:

فيما يلي قائمة بأهم المصلطحات الوادرة في الدراسة:

1 – **سياسة الخصوصية** Privacy Policy هي وثيقة مادية أو رقمية تتضمن مجموعة البنود والشروط التي توضح كيفية تعامل الجهة أو المنظمة أو الموقع الالكتروني مع البيانات والمعلومات التي يجمعها عن العملاء أو الزبائن أو أعضاء الجهة أو رواد وزوار الموقع الالكتروني، ومستوى الولوج المطلوب لبياناتهم، وطريقة تصرف الجهة في هذه المعلومات سواء بالنشر أو الإتاحة أو حتى البيع.

2 – **أمن المعلومات:** العلم الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها أو الاعتداء عليها وذلك من خلال توفير الأدوات والوسائل اللازمة لحماية المعلومات من المخاطر الداخلية أو الخارجية. أو هو المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين بالاطلاع عليها وذلك لضمان أصالة هذه الاتصالات وصحتها وسلامتها.

3 – **أمن المعلومات الحاسوبية:** حماية البيانات على الكمبيوتر من الإطلاع غير المصرح به ومن تعديلها أو تدميرها.

4 – **أمن نظم المعلومات :** حماية نظام الحاسب الآلي من الاستخدام أو الولوج غير المصرح به، أو التعديل على النظام أو الحرمان من الخدمة من قبل من لايحق لهم ذلك.

5 – **الجريمة المعلوماتية:** هي مجموعة من الأفعال المرتبطة بالاستخدام غير الشرعي للمعلومات وقد تكون هذه الأفعال جديرة بالعقاب.

6 – **كود الاستجابة السريع:** QR- Code هو نوع من أنواع الباركود أو رموز تخزين البيانات والمعلومات القابلة للاسترجاع عن طريق المسح الضوئي باستخدام أجهزة الحواسب الآلية والهواتف الذكية فتتم قراءتها وإظهار المعلومات المخزنة على الرمز.

7 – **التوسيم** هو المصطلح العربي المستخدم للمرادف الانجليزي Tagging ويعني ربط المحتوى على موقع أو صفحة ويب بكلمات دلالية مميزة تدل على محتوى موضوعي أو أسماء مستخدمين محددين. أو هو وضع وصف بالكلمات لموقع معين أو محتوى معين على شبكة الانترنت.

8 – **المستودعات الرقمية** digital dipositories إحدى أهم الوسائل التكنولوجية الحديثة التي يتم بها تخزين الوثائق الرقمية بهدف إدارتها سواء بالتبادل أو النشر أو البيع أو الحماية .... الخ.

9 – **ويكيليكس** WikiLeaks : منظمة دولية غير ربحية أسسها الصحفي والمبرمج الأسترالي جوليان أسانج Julian Assange تنشر تقارير خاصة وسرية تخص وسائل الإعلام والمنظمات المدنية والعسكرية والسياسية الرسمية وغير الرسمية من مصادر صحفية وتسريبات أخبارية مجهولة. بدأ موقعها على الإنترنت سنة 2006 تحت مسمى منظمة سن شاين الصحفية.

10 –**القرصنة الالكترونية** 1 Hacking: تعرف القرصنة الالكترونية بأنها التسلل غير المسموح به إلى أجهزة الحاسب الآلي أو شبكات الاتصال ويشار عادة إلى الشخص الذي يمارس القرصنة باسم القرصان Hacker

[1] https://www.techopedia.com/definition/26361/hacking

تمهيد:

ترتبط البيانات الخاصة بالأفراد بالخصوصية وأحياناً بالسرية، وهو ما ينسحب غالبا على الوثائق بجميع أشكالها وصورها سواء أكانت في شكل تقليدي مثل السجلات والدفاتر الورقية والوثائق المفردة أم كانت في شكل غير تقليدي مثل الميكروفيلم والوثائق الرقمية والمحولة رقمياً. ومنذ المحاولات الأولى لوضع قواعد لاتاحة البيانات وحرية تداول المعلومات وهناك إشكالية يتم تداولها بشكل دائم ألا وهي مشكلة حدود العلاقة بين حرية إتاحة المعلومات وتداولها وبين الخصوصية وسرية البيانات الشخصية. وقد كانت الوثائق ودور الأرشيف دائما محط أنظار المتسللين والسارقين ومحبي الاطلاع على بيانات أو أسرار الغير سواء أكان أحد الجانبين أو كلاهما أفراداً أو هيئات وكيانات اعتبارية.

ومع التطور التكنولوجي ودخول التقنيات الحديثة مجال إدارة الوثائق زاد الجدل حول هذه النقاط وأصبحت بيانات الأفراد والمؤسسات في مهب ريح التكنولوجيا الحديثة التي أصبحت تمثل شبحا مرعبا لكل

الكيانات والهيئات العاملة بالأرشيف والحاضنة له، ولكل الأفراد الذين لهم وثائق تحوي بيانات سرية أو شخصية عنهم. وأصبحت مؤسسات إدارة الوثائق وحفظها هدفاً للجريمة المعلوماتية مثلها مثل بقية المؤسسات والهيئات، كما أصبحت البيانات الشخصية للأفراد هدفاً آخر لهذه الجريمة، حيث بات من السهل للغاية التسلل إلى البيانات الشخصية للأفراد من خلال البرمجيات الحديثة وتطبيقات الهواتف المحمولة التي تطلب أحياناً من الأشخاص أنفسهم أذون للسماح لها للولوج إلى هواتفهم وحساباتهم الشخصية وبياناتهم الخاصة بل والولوج إلى حياتهم الخاصة نفسها من خلال كاميرات وميكروفونات الحواسب المكتبية والمحمولة والهواتف الذكية، وأصبح الكثيرون يعطون أذوناً بذلك للبرامج الحديثة وتطبيقات الحاسب الآلي والهواتف المحمولة دون دراية بالخطر المحدق بهم من خلال هذه التقنيات الحديثة الذي لا يقتصر على التسلل إلى معلوماتهم وبياناتهم الخاصة فقط بل تستطيع هذه التطبيقات في كثير من الأحيان السيطرة على حساباتهم الالكترونية المختلفة وأحيانا على مكونات هواتفهم المحمولة وحاسباتهم الخاصة نفسها.

كما تكاثرت أمثلة المراقبة الرقمية العلنية والسرية حول العالم، وظهرت المراقبة الحكومية الجماعية كعادة خطيرة وليست مجرد إجراءات احترازية أو تدبيرات استثنائية في حالات الضرورة، حيث تفيد التقارير بأن هناك العديد من الحكومات هددت بحظر شركات خدمات الاتصالات والمعدات اللاسلكية ما لم تحصل على إمكانية الوصول المباشر إلى حركة الاتصالات، وتنصتت بعضها على كابلات الألياف البصرية لأغراض المراقبة، وأن هذه الحكومات طلبت من الشركات أن تكشف بانتظام عن معلومات الزبائن والموظفين. وعلاوة على ذلك، تفيد التقارير بأن بعض هذه الحكومات استخدمت مراقبة شبكات الاتصالات لاستهداف أعضاء المعارضة السياسية و/أو المنشقين السياسيين. كما تفيد بعض التقارير بأن السلطات في بعض الدول تسجل بشكل روتيني جميع المكالمات الهاتفية وتحتفظ بها لتحليلها، بينما أُبلِغ عن رصد حكومات مضيقة للاتصالات أثناء الأحداث العالمية[1].

[1] الأمم المتحدة – مجلس حقوق الإنسان (2014). (الحق في الخصوصية الرقمية) تقرير مفوضية الأمم المتحدة السامية لحقوق الإنسان. ص3.

وسوف تعمل هذ هالدراسة على عرض أهم المخاطر التي تمثلها التقنيات الحديثة وبرمجيات إدارة الوثائق على خصوصية كلٍ من الأفراد والهيئات أو الكيانات الاعتبارية، وما الاحتياطات الواجب اتخاذها لتفادي هذه المخاطر أو التقليل من التعرض لها قدر الإمكان.

تعريف الخصوصية:

ما الخصوصية؟ وماذا يقصد بها تحديداً بالنسبة للأفراد وبالنسبة للهيئات؟ هذا السؤال يطرح نفسه عند الحديث عن حماية بيانات الأشخاص والهيئات داخل الوثائق. وينبري المدافعون عن حرية تداول المعلومات في الدفاع عن موقفهم ضد الخصوصية ويعتبرونها قيداً على تداول المعلومات وحاجباً للشفافية ومجرد ذريعة لحجب معلومات معينة عن فئة أو أكثر أو لاستحواذ فرد أو هيئة على هذه المعلومات بشكل حصري. بينما يدافع أصحاب الرأي الآخر عن موقفهم بوجوب حجب معلومات أو بيانات معينة وضمان سريتها بأن لكل فرد الحق في خصوصيته وعدم إفشاء معلومات أو بيانات خاصة به إلا بإذنه ورغبته ، والأمر نفسه بالنسبة للكيانات الاعتبارية التي يحق لها الاحتفاظ ببيانات و/ أو معلومات خاصة عنها أو عن العاملين بها وعدم أحقية أي شخص في الإطلاع عليها بدون إذن أو ترخيص.

والحقيقة أنه لا يوجد تعريف علمي محدد وجامع للخصوصية، فالخصوصية تعني العديد من الأشياء للعديد من الأشخاص وتعني أمورا مختلفة في سياقات مختلفة[1]، خصوصاً إذا ما اتسع الأمر ليشمل كلا من خصوصية الأفراد، وخصوصية الهيئات، ويرجع السبب في عدم تحديد تعريف واضح للخصوصية أو الحياة الخاصة إلى تنوع العادات والتقاليد واختلافها بين المجتمعات وإلى تطور تلك المفاهيم الاجتماعية والسياية والاقتصادية والدينية والثقافية، وتبدل مفهوم الحياة الخاصة نفسه وتطوره باستمرار [2]، وإلى البون الواضح بين القوانين ونظم التقاضي من ناحية وبين التطور التكنولوجي والقدرة على الوصول إلى المعلومات والبيانات بطرق غير مشروعة من ناحية أخرى. ولكن يمكن الرجوع لبعض المصادر لاستخراج بعض التعريفات المحددة أو على الأقل التي تحاول تحديد معنى علمي لخصوصية الأفراد والهيئات ، فعلى الرغم من أن الدراسات العلمية التي تتعمق في دراسة الخصوصية المعلوماتية وحقوق الإنسان قليلة للغاية لكن يمكن القول أن هذه الدراسات بدأت

[1] Berman, Jerry & Mulligan, Deirdre (January, 1998).Privacy in the Digital Age: Work in Progress. – Nova law review, vol.23, P549-582.

2 سوزان عدنان الأستاذ (2013). انتهاك حرمة الحياة الخاصة عبر الانترنت: دراسة مقارنة._ مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، مج29، ع3. ص ص 421-455.

في الستينيات والسبعينيات من القرن العشرين، حيث كانت هذه الفترة هي بداية إنطلاق مثل هذا النوع من الدراسات التي مازالت في طور التحديث والتطوير حتى الآن[1]، ويمكن مناقشة هذه التعريفات في ما يلي:

يعرف البروفيسور الأمريكي وأستاذ القانون الدولي آلان ويستن Alan Westin مؤلف كتاب "الحرية والخصوصية Privacy and Freedom " 1967 خصوصية المعلومات أو الحق في الحياة الخاصة أو الحرمة الشخصية بأنها "حق الأفراد أو الجماعات أو المؤسسات في أن يقرروا بأنفسهم زمن وكيفية ومدى نقل المعلومات عن أنفسهم الى الآخرين [2]" في حين عرفها ميلر Miller مؤلف كتاب "الاعتداء على الحرية The Assault on Privacy " بأنها " قدرة الأفراد في التحكم بدورة المعلومات التي تتعلق بهم" في حين ترى منى الموسوي أن الخصوصية هي الحق لمنع إساءة استخدام الحكومة للبيانات التي يتم معالجتها آليا أو اليكترونيا أو تقييد استخدامها وفقاً للقانون[3].

ويعرف محمد الطاهر الخصوصية بأنها "قدرة الأشخاص في التحكم في سرية بياناتهم ومعلوماتهم الشخصية والتحكم في من يمكنه الوصول لهذه المعلومات سواء أكانوا أفراداً آخرين أو حكومات أو حواسيب [4]"
ومع تطور وسائل الاتصال تطور مفهوم الخصوصية على الانترنت ليعني كل عمليات جمع المعلومات الشخصية على الخط المباشر On Line واستخدامها مثل اسم الشخص أو عنوانه أو رقم هاتفه أو حالته العائلية أو ضمانه الاجتماعي أو غير ذلك من المعلومات الشخصية الأكثر عمقا مثل رقم الهوية والإحصاءات المالية والصحية[5].

---

[1] منى تركي الموسوي الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها._ منى تركي الموسوي، جان سيريل فضل الله._ جامعة بغداد: مجلة كلية بغداد للعلوم الاقتصادية الجامعة العدد الخاص بمؤتمر الكلية. ص6.

[2] Westin, Alan F. Privacy and freedom.- New York: Atheneum, 1967. P7.

[3] الموسوي._ المصدر السابق والصفحة.

[4] محمد الطاهر(2013). الحريات الرقمية: المفاهيم الأساسية._ ط1._ القاهرة: مؤسسة حرية الفكر والتعبير. ص6.

5 Strauss, Jared & Rogerson, Kenneth S. (2002).Policies for online privacy in the United States and the European Union.- Telematics and Informatics, vol. 19. PP. 173–192.

وقد عرف المجلس الدولي للأرشيف الخصوصية بأنها: الحق في ضمان عدم إفشاء المعلومات غير المصرح بها، الواردة في الوثائق الجارية/ الوثائق الأرشيفية والتي تتعلق بموضوعات شخصية أو خاصة. كما عرف حماية البيانات بأنها: الحماية القانونية لحقوق الأفراد الخاصة بجمع البيانات الشخصية ومعالجتها وتخزينها في شكل مقروء آلياً وإتاحة مثل هذه البيانات. بينما عرف رفع السرية بأنه: إزالة جميع القيود السرية المفروضة على المعلومات أو الوثائق1.

ورغم اختلاف التعريفات إلا أن خصوصية بيانات الأشخاص أو المعلومات المتداولة عنهم يبقى حق لصيق بكل شخص لايجب على الحكوم ات انتهاكه ويُجرَّم من يفعل ذلك من الأفراد. وقد حددت المعايير القانونية الدولية التي صدرت في القرن العشرين الخصوصية كحق من حقوق الإنسان التي يجب احترامها وصيانتها حيث تضمن الإعلان العالمي لحقوق الإنسان الصادر 1948، أول محاولة لحماية الخصوصية كحق إنساني متميز فنصت المادة 12 منه على ما يلي: "لا يجوز تعريض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أوالمنزل أو المراسلات ، ولا الهجمات على شرفه وسمعته فلكل فرد الحق في حماية القانون من مثل هذا التدخل أو الهجمات[2]"

ويمكن القول أن تطور التكنولوجيا الحديثة يزيد من الحاجة إلى تحديد وتطوير مفهوم الخصوصية بما يتلائم مع كل وضع جديد أو إمكانية تكنولوجية تستحدث في الكشف عن المعلومات أو اختراق خصوصية وحسابات الأفراد والهيئات أو حتى الحكومات نفسها ، فلكل فرد الحق في الخصوصية علي الإنترنت بما في ذلك الحق في حماية البيانات الشخصية التي تتعلق به، والحق في اتصال مجهول الهوية على شبكة الانترنت واستخدام التكنولوجيا المناسبة لضمان اتصال آمن وخاص ومجهول[3].

[1] المجلس الدولي للأرشيف (2012). مبادئ إتاحة الوثائق._ ترجمة: أماني محمد عبدالعزيز. ص5، 6.
[2] Mendel, Toby et al (2012). Global survey on internet privacy and freedom of expression. – UNESCO: France. - UNESCO Series on Internet Freedom. P10.
[3] الإعلان الإفريقي لحقوق وحريات الانترنت._ ص8. متاح في:

الخصوصية وأمن المعلومات:

قد يبدو مصطلح الخصوصية متداخل مع أمن المعلومات أو أنه جزء منه أو أن كلا الأمرين يمثلان الشئ نفسه، لكن في الحقيقة هناك بعض الاختلافات الجوهرية بين الخصوصية وأمن المعلومات وإن كانا مرتبطين معاً في عدة أمور. يمكن تعريف أمن المعلومات بأنه " العلم الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها أو الاعتداء عليها وذلك من خلال توفير الأدوات والوسائل اللازمة لحماية المعلومات من المخاطر الداخلية أو الخارجية ، أو هو المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين بالاطلاع عليها وذلك لضمان أصالة وصحة هذه الاتصالات "[1] أما إذا تعلق الأمر بأمن المعلومات الحاسوبية وأمن نظم المعلومات فإنه يعرف عادة بـ "حماية البيانات على الكمبيوتر من الإطلاع غير المصرح به ومن تعديلها أو تدميرها، وحماية نظام الحاسب الآلي نفسه من الاستخدام أو الولوج غير المصرح به، أو التعديل على النظام أو الحرمان من الخدمة من قبل من لايحق لهم ذلك "[2] أو هو نظام مصمم لحماية سرية بيانات نظام الكمبيوتر ونزاهتها وإتاحتها من ذوي النوايا الخبيثة[3]، وكذلك يتم تعريف أمن المعلومات بأنه ممارسة حماية المعلومات في جميع أشكالها ، سواء كانت مكتوبة أو منطوقة أو إلكترونية أو رسومية أو باستخدام طرق اتصال أخرى[4].

ويتضح من التعريفات السابقة أن الفارق بين أمن المعلومات وخصوصية البيانات الشخصية هو أن المعلومات معنى عام لكل ما تم حفظه لغرض الاطلاع المحدد وقد يكون معلومات تخص أي شخص أو كيان

---

http://africaninternetrights.org/wp-content/uploads/2016/08/African-Declaration-arabic-24-pages-plus-cover.pdf

[1]https://ar.wikipedia.org/wiki/%D8%A3%D9%85%D9%86_%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA

[2]Micki, Krause. Handbook of Information Security Management.- available at; https://www.cccure.org/Documents/HISM/ewtoc.html

3 https://www.techopedia.com/definition/10282/information-security-is

[4]Rhodes-Ousley, Mark (2013). Information Security: The Complete Reference.- Second Edition.- New york: McGraw-Hill. P817.

أو جهة وتشمل جميع المعاملات والأنشطة البشرية، وأن مصطلح أمن المعلومات يشار به إلى الوسائل والاحتياطات والبرمجيات التي تعمل على ضمان سلامة نظم حفظ المعلومات نفسها وعدم اختراقها أو تعطيلها او تدميرها أو السيطرة عليها بأي شكل ومن خلال أي فرد أو كيان؛ بينما تتمحور الخصوصية حول البيانات المتعلقة بشخص أو كيان واللصيقة الصلة به في حد ذاته وليست المعلومات حوله أو حول أنشطته. وقد تكون خصوصية وسرية البيانات الشخصية للأفراد جزء أو مكون من مكونات أمن المعلومات في نظم المعلومات وأمن الشبكات[1].

والحقيقة أن كلاً من الخصوصية وأمن المعلومات تتهددهم العديد من الأخطار منها التطورات التكنولوجية المتسارعة، والمشكلات الفنية المتزايدة، والضعف البشري، وضعف قدرة الهيئات والكيانات الاعتبارية على مواجهة ا لمتغيرات المتلاحقة، حيث تتبع التهديدات والمخاطر التي تواجه نظم المعلومات من الأفعال والتصرفات المقصودة وغير المقصودة علي السواء التي قد ترد من مصادر داخلية أو خارجية[2].

بين خصوصية الأفراد وخصوصية الهيئات والكيانات:

أول ما يتبادر إلى الذهن عند الحديث عن مفهوم الخصوصية هو خصوصية الأفراد. ولكن يجب التنبيه على أن الهيئات والكيانات الاعتبارية سواء الاجتماعية أو حتى الحكومية تشارك الأفراد في الخصوصية وينبغي صياغة بروتوكول أو قواعد أو سياسة تحدد هذه الخصوصية بشكل واضح[3]. فبينما يمكن فهم خصوصية الأفراد

---

[1] رجب عبدالحميد حسنين(سبتمبر 2012). أمن شبكات المعلومات الالكترونية: المخاطر والحلول._ Cybrarians Journal._ ع30._ 2015/8/20._ متاح في:
http://journal.cybrarians.info/index.php?option=com_content&view=article&id=629:networks&catid=257:studies&Itemid=0

[2] محمد محمد الهادي (يونيو 2006). توجهات أمن وشفافية المعلومات في ظل الحكومة الإلكترونية._ cybrarians journal ._. ع 9._ 2015/8/20._ متاح في:
http://www.journal.cybrarians.org/index.php?option=com_content&view=article&id=370:2009-07-15-09-59-43&catid=161:2009-05-20-10-01-08&Itemid=70

3 Westin, Alan F. (2003). Social and Political Dimensions of Privacy.- Journal of Social Issues, Vol. 59, No. 2. PP. 431-453.

أو ما يسمى الحياة الخاصة للأفراد على أنها البيانات اللصيقة الصلة بالشخص ذاته، يمكن فهم خصوصية الكيانات والهيئات من خلال مجموعة البيانات أو المعلومات التي يحجبها الكيان أو الهيئة عن الاطلاع العام ويحدد أدوار من يمكن لهم الإطلاع عليها وإلى أي مستوى يستطيع صاحب كل دور الوصول بدقة. ولا يمكن تأمين الأنظمة الحاسوبية وحمايتها بأدوات وبرمجيات فقط؛ فتطبيق أمن المعلومات بشكل كامل يتطلب بالإضافة إلى ذلك الاهتمام بالجانب البشري وكذلك سن السياسات والإجراءات الأمنية للتعامل مع المعلومات والمعدات والبرمجيات والمستخدمين بشكل منظم ومدروس[1].

سياسة الخصوصية:

سياسة الخصوصية yPrivacy Polic عبارة عن وثيقة تتضمن مجموعة البنود والشروط التي توضح كيفية تعامل الجهة أو المنظمة أو الموقع الالكتروني مع البيانات والمعلومات التي يجمعها عن العملاء أو الزبائن أو أعضاء الجهة أو رواد وزوار الموقع الالكتروني، ومستوى الولوج المطلوب لبياناتهم، وطريقة تصرف الجهة في هذه المعلومات سواء بالنشر أو الإتاحة أو حتى البيع[2]، حيث تعتبر سياسة الخصوصية تطبيقا لمبدأ الإشعار أو التوعية بإعطاء المستهلكين إشعارًا بممارسات المعلومات الخاصة بالهيئة أو الجهة قبل تجميع المعلومات الشخصية منهم[3].

وفي سياق تكنولوجيا المعلومات، يمكن تعريف سياسة الخصوصية بأنها وثيقة تطلع القراء على كيفية استخدام منتج أو مزود بالخدمة لمعلوماتهم الشخصية[4]، ومن المفترض أن يعلن أي كيان أو جهة تقوم بجمع

---

[1] خالد بن سليمان الغثبر، أمل ناصر الصبيح (مايو 2012). حال أمن المعلومات في المملكة العربية السعودية._ دراسات المعلومات، ع14._ ص195.

[2] http://whatis.techtarget.com/definition/privacy-policy/ Web services, SOA glossary/22-12-2916; 11:24pm.

[3] Landesberg, Martha K. & Mazzarella, Laura (July1999). Self-Regulation and Privacy Online: A Report to Congress.- U.S.A: Federal Trade Commission. P3.

[4] https://www.techopedia.com/definition/23679/privacy-policy

بيانات و/ أو معلومات عن الأفراد أو الهيئات أو تخول بالإطلاع عليها أو حتى تشارك في صنعها وانتاجها سواء بشكل تقليدي أو غير تقليدي عن سياسة الخصوصية لديها. وعادة ما يقترن استخدام مصطلح "سياسة الخصوصية" بتكنولوجيا المعلومات الرقمية لأن منتجات وتطبيقات ونظم تكنولوجيا المعلومات الرقمية تجمع المعلومات و/أو البيانات الشخصية من/ عن المستخدمين وتستخدمها بطرق مختلفة وبشكل موسع ودوري.

وتختلف سياسة الخصوصية من موقع الكتروني أو تطبيق لآخر في مستوى الولوج لبيانات المستخدمين الشخصية ومعلوماتهم السرية وفي مستويات نشرها أو تخزينها أو تصديرها لمواقع أو تطبيقات أخرى تابعة لتلك المواقع أو التطبيقات أو مرتبطة بها. ومن المفترض أن تقوم المواقع المختلفة بشرح وإيضاح سياسة الخصوصية لديها لمستخدميها بكل وضوح وشفافية حتى يتسنى لهم الوقوف على مستويات الأمان لدى مستخدمي هذه المواقع، مثال الوثيقة التي تثبتها شركة جوجل على موقعها الشهير، وتحدثها بشكل دائم، وتوضح بها ثلاثة أمور مهمة وهي[1]:

1 - المعلومات التي يجمعها الموقع عن مستخدميه، ولماذا يجمعها؟

2 - كيف يستخدم الموقع هذه المعلومات.

3 - الخيارات التي يقدمها الموقع لمستخدميه عن استخدامه لمعلوماتهم وبياناتهم الشخصية، بما في ذلك تحديث هذه المعلومات والبيانات.

وقد تقتصر سياسة الخصوصية لدى بعض المواقع أو التطبيقات على شرح عام وقد تمتد لشرح مفصل عن الأنشطة التي تستخدم فيها معلوماتهم وبياناتهم المتاحة على الانترنت وما قد تفعله بهذه المعلومات والبيانات خارج مستوى الموقع نفسه مثل تصديرها لمواقع ذات صلة أو أحقيتها في استخدام هذه المعلومات والبيانات في حالة ما تم إيقاف الموقع أو تعطيله أو تغيير نشاطة.

[1] https://static.googleusercontent.com/media/www.google.com/en//intl/en/policies/privacy/google_privacy_policy_en.pdf/22-6-2-17;01:50Am.

وإذا كانت كل المواقع والتطبيقات مجبرة على أخذ موافقة مستخدميها على ما تجمعه من معلومات عنهم وما تستخدمه من بياناتهم الشخصية قبل استخدامها فإن هذه المواقع والتطبيقات تجبر المستخدمين على عدم الولوج إليها إلا بعد الموافقة على سياسة الخصوصية الخاصة بها أولا وهو ما يفعله معظم المستخدمين دون قراءة وثيقة سياسة الخصوصية تلك ولا التدقيق بها ويقومون بالموافقة بشكل روتيني بدون الاكتراث لخطورة هذا الأمر على خصوصيتهم المعلوماتية بل وعلى حياتهم الخاصة نفسها.

مفاهيم الخصوصية:

يمكن تقسيم الخصوصية إلى عدد من المفاهيم المنفصلة لكنها ترتبط معا في الوقت ذاته وهي[1]:

1. خصوصية المعلومات Information Privacy وهي القواعد التي تحكم إدارة البيانات والمعلومات الخاصة كمعلومات بطاقات الهوية، والمعلومات المالية، والسجلات الطبية، والسجلات الحكومية، وهي المحل الذي يتصل عادة بمفهوم حماية البيانات Data Protection .
2. الخصوصية الجسدية أو المادية [2] Bodily Privacy: والتي تتعلق بالحماية الجسدية للأفراد ضد أية إجراءات ماسة بالنواحي المادية لأجسادهم كفحوص الجينات GENETIC TESTS ، وفحص المخدرات DRUG TESTING.
3. خصوصية الاتصالات Telecommunication Privacy والتي تغطي سرية وخصوصية المكالمات الهاتفية ، وبرمجيات الاتصال الصوتي والمرئي ، والمراسلات البريدية الورقية ، والبريد الالكتروني وغيرها من الاتصالات.

[1] عايض المري. الخصوصية وحماية البيانات._ متاح في:
http://www.dralmarri.com/show.asp?field=res_a&id=199.-20/8/2015

2 الموسوي. مصدر سابق._ ص4.

4. الخصوصية الاقليمية (نسبة إلى الاقليم المكاني) والتي تتعلق بالقواعد المنظمة للدخول إلى المنازل وبيئة العمل أو الأماكن العامة والتي تتضمن التفتيش والرقابة الالكترونية والتوثق من بطاقات الهوية.

الجريمة المعلوماتية:

يعرف البعض الجريمة المعلوماتية بأنها "الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي " وأنها "أية جريمة ضد المال مرتبطة بالمعالجة الآلية للمعلومات"[1] في حين يعرفها آخرون بأنها "الاعتداءات التي ترتكب باستخدام المعلومات بغرض تحقيق ربح" وتعرف كذلك بأنها "مجموعة الجرائم المتصلة بعلم المعالجة المنطقية للمعلومات" أو هي "مجموعة من الأفعال المرتبطة بالمعلوماتية يمكن أن تكون جديرة بالعقاب[2]"

والجريمة المعلوماتية لصيقة الصلة بانتهاك الخصوصية على الإنترنت وعبر وسائل الاتصال الحديثة حيث أن كل جريمة معلوماتية هي بالضرورة تعدي على خصوصية فرد أو هيئة. وعلى الرغم من أن الجريمة المعلوماتية الالكترونية ظاهرة حديثة نسبيا إلا أنها احتلت مركز الاهتمام الدولي لأن العالم ببساطة يحيا عصر المعلومات[3].

وتتنوع أشكال الجرائم المعلوماتية باختلاف وسائلها ودوافعها؛ فمنها جرائم تحدث ضد أجهزة الكمبيوتر ونظم المعلومات ووسائل الاتصال ومنها جرائم الإضرار بالبيانات والمعلومات الخاصة أو العامة، وجرائم الإعتداء على الأشخاص سواء بالسب أو التشهير أو الابتزاز، وجرائم نشر الفيروسات والبرامج الضارة، وجرائم

[1] أمينة حمشاشي. ماهية الجريمة المعلوماتية (2009). دراسات وابحاث، مج1، ع1._ ص ص 450_458.

[2] محمد على سالم، حسون عبيد هجيج (2007). الجريمة المعلوماتية._ مجلة جامعة بابل للعلوم الانسانية._ مج15، ع2._ ص ص87-100.

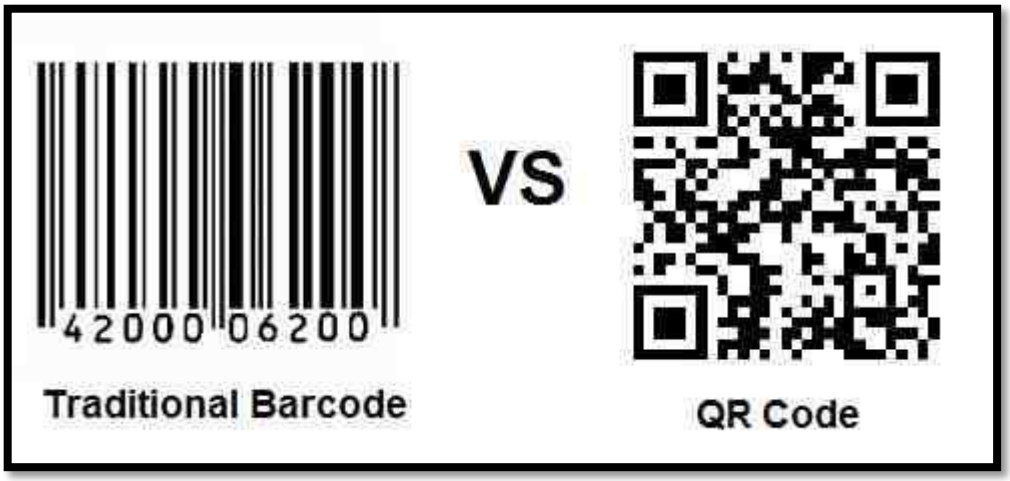
[3] Ajayi, E. F. G. (August 2016). Challenges to enforcement of cyber-crimes laws and policy.-Academic Journals; Journal of Internet and Information Systems. Vol.6 (1). PP. 1-12.

الإعتداء على الأموال، وجرائم الإستغلال الجنسي للأطفال عبر الانترنت. ومن ناحية الدوافع فيعتبر تحقيق ربح مالي دافعا أساسيا وراء ارتكاب الجرائم الالكترونية، بالإضافة لدوافع أخرى مثل الرضا أو المتعة عند بعض المتسللين نتيجة حصولهم على معلومات خاصة، وهناك طريقة أخرى للتحفيز للمجرمين الإلكترونيين تمثل تحديًا أو احتجاجًا على أنظمة الكمبيوتر التي تمثل المظهر الخارجي لتسجيل عدم الاتفاق أو الرفض ضد المالكين أو المشغلين، وهذا النموذج أو الدافع هو أيضًا في الغالب يهدف إلى تحقيق الربح من الأنشطة الإجرامية السيبرانية أو الشعور بالانتصار عن طريق اختراق أنظمة معلوماتية محظورة أو مؤمنة [1]، ويضاف لكل ما سبق الدوافع السياسية والأمنية التي تحرك أجهزة رسمية لارتكاب مثل هذه الجرائم.

مخاطر التقنيات الحديثة على الخصوصية:

1. مخاطر كود الاستجابة السريع: QR- Code

يمثل كود أو رمز الاستجابة السريع (QR Code) Quick Response code أحد أهم أنواع رموز تخزين المعلومات القابلة للاسترجاع حالياً، وهو واحد من أكثر أنواع رموز الباركود تطوراً وانتشاراً وحداثة **(شكل رقم 1)**



[1] Ajayi. P3.

شكل 1 كود الاستجابة السريع مقارنة بالشكل التقليدي للباركود

ويتميز هذا الشكل أو الطور من أطوار الرموز المشفرة أو رموز الباركود بأنه لايحتاج لأجهزة أو معدات خاصة لقراءته والتعامل معه كما هو الحال في الشكل التقليدي للباركود (الشكل الشريطي) المعروف والمتداول الذي يحتاج إلى قارئ باركود خاص، أو تكنولوجيا FIDR [1]، حيث يمكن قراءة رمز الاستجابة السريع بواسطة الحاسب الآلي عن طريق إدخال صورة الرمز لأي موقع ويب من المواقع المتخصصة في قراءة رموز الاستجابة فتتم قراءته وإظهار النتيجة فوراً عبر الانترنت، كما يمكن مسح هذا الكود ضوئيا باستخدام كاميرا الهاتف الذكي ومعالجته بأحد تطبيقات قراءة الباركود أو التقاط صورة له بالهاتف المحمول وادخال الصورة لأي موقع ويب أو أي تطبيق عبر الموبايل انترنت فتتم قراءتها وإظهار المعلومات المخزنة على الرمز مباشرة من خلال الهاتف مع إتاحة رابط لكل كود استجابة يُمَكّن من إظهار معلومات عنه بعد ذلك (شكل رقم2)

شكل 2 إتاحة رابط الكتروني لكود الاستجابة السريع

وقد تم تصميم رمز الاستجابة السريع في الأساس كتطوير للرمز الشريطي التقليدي (باركود) الذي تم اختراعه في اليابان في ستينيات القرن العشرين للمساعدة في بيع السلع اليابانية التي ازدادت وانتشرت بسرعة بعد النهضة الاقتصادية اليابانية الحديثة وأصبح من الصعب على البائعين التعرف على سعر السلعة يدويا قتم

[1] RFID هو اختصار لجملة Radio Frequency Identification وتعني كشف الهوية باستخدام ترددات الراديو وهي تقنية تمكن من التعرف على بيانات ومعلومات أي شئ مثبته به عبر ترددات راديوية ترسلها كبسوله خاصة تثبت في هذا الشئ (سلعة أو كتاب مثلاً)، وتتميز هذه التقنية بقدرتها على قراءة أكثر من كبسولة وإظهار المعلومات الخاصة بها في وقت واحد، كما تستطيع توزيع السلع على أماكنها المخصصة لها عبر معدات خاصة دون الحاجة للتدخل البشري.

اختراع الباركود لمساعدة البائعين على معرفة وصف وسعر السلعة بشكل سهل وسريع، ولكن رمزالباركود لم يكن يسمح بتخزين أكثر من 20 حرف فقط فقام فريق من قسم Denso Wave التابع لشركة دينسو اليابانية عام 1994 بتطوير رمز ثنائي الأبعاد جديد هو كود الاستجابة السريع ليتم استخدامه في مصانع السيارات في تعقب قطع غيار المركبات أثناء عملية التصنيع مما جعل عمليات التصنيع أكثر كفاءة وفعالة ودقة، وهذا الأمر دفع بقية المصانع والشركات لاستخدام كود الاستجابة السريع ثم انتشر بعد ذلك على جميع المنتجات الغذائية والدوائية وغيرها[1].

ويتميز كود الاستجابة السريع بسهولة القراءة بشكل سريع ونسبة التخزين العالية حيث يتكون الرمز من وحدات سوداء مرتبة على شكل مربع على خلفية بيضاء ، ويحتوي معلومات مشفرة من أي نوع من البيانات (على سبيل المثال الأرقام، والحروف والأرقام، والبيانات الثنائية المتكونة من أرقام ورحوف، أو حتى رموز كانجي اليابانية[2]) كما يتميز بفك محتوياته بسرعة عالية جداً إذ أنه يحمل بداخله بيانات مشفرة للمنتج أو السلعة التي يرفق حيث يمكن لأي شخص الاطلاع على بيانات الرمز فقط من خلال تصويره وادخاله إلى موقع أو أو برنامج لفك شيفرة هذا الكود أو الرمز أو مسحه مباشرة من خلال أحد تطبيقات قراءة كود الاستجابة السريع المتوافرة حاليا على المتاجر الالكترونية للهواتف المحمولة حيث من الممكن أن تحمل الشيفرة الموجودة داخل المربع بيانات عديدة مثل: رابط لموقع ما على الانترنت يحتوي أي نوع من البيانات مثل الفيديو أو الصوت أو النصوص المختلفة ... الخ ، أو رقم هاتف، أو حتى بيانات شخصية مثل الاسم والبريد الالكتروني وحتى موقع الشركة وبيانات حول الشركة، أو تضمينه رسالة نصية تصل لأكثر من 160 حرف[3].

وقد تطور رمز الاستجابة السريع ونتج منه عدة نسخ أو إصدارات مطورة حتى زادت فيها قدرته على استيعاب المعلومات بأشكالها المختلفة، وتختلف القدرة الاستيعابية للرمز في الإصدار الواحد حسب نوع البيانات المخزنة ومستوى تصحيح الخطأ في الكلمات المشفرة حيث يوجد 4 مستويات لتصحيح الخطأ والمستوى الأعلى

[1] http://www.qrcode.com/en/history/
[2] https://en.wikipedia.org/wiki/QR_code
[3] http://ardroid.com/2011/11/03/what-is-qr-code /

يكون ذو قيمة تخزينية أقل وهذه المستويات هي: المستوي (L) حيث يمكن استعادة 7% من الكلمات المشفرة ، والمستوي (M)يمكن استعادة 15% من الكلمات المشفرة، والمستوى (Q) حيث يمكن استعادة 25% من الكلمات المشفرة ، والمستوى (H) حيث يمكن استعادة 30% من الكلمات المشفرة. ويستطيع الإصدار 40 مع مستوى تصحيح الخطأ (L) كحد أقصى تخزين 7089 حرف رقمي، أو 4,296 حرف هجائي رقمي، أو 2,953 عددا ثنائيا (Binary / byte)، أو 1,817 حرف كانجي اليابانية[1].

ويمكن الاستفادة من تكنولوجيا رمز الاستجابة السريع في مجال إدارة الوثائق لقدرته على تخزين المعلومات والبيانات وتخزين صور الوثائق بداخله. ولكن ظهرت بعض المخاطر التي نتجت عن إدارة الوثائق من خلال تكنولوجيا رمز الاستجابة السريعة ، ومن هذه المخاطر ظهور بعض رموز الاستجابة الضارة التي تحمل برمجيات خبيثة (فيروسات) والتي يمكن تصميمها بسهولة وتجعل محتويات كمبيوتر أو هاتف المستخدم في خطر بسبب انتهاكها لخصوصيته واستيلائها على معلوماته أو بياناته الخاصة مثل كلمات المرور وأسماء المستخدم التي يستخدمها للولوج للمواقع الالكترونية أو للبريد الالكتروني الخاص به أو خداعه والاستيلاء على معلوماته المالية عن طريق الاحتيال عليه باستخدام رموز استجابة سريعة تبدو شرعية لكنها محملة ببرمجيات ضارة ترسل معلومات المستخدم لمواقع المجرمين الالكترونيين [2]. ويمكن إضافة البرمجيات الضارة والخبيثة إلى رموز الاستجابة السريعة الشرعية كجزء من محتوياتها ثم بثها عبر الانترنت أو في إعلانات ترويجية لاصطياد ضحايا يتم الاستيلاء على بياناتهم الخاصة واستعمالها في أنشطة غير مشروعة[3].

ومن أخطر أنواع البرامج الضارة في هذا المجال تلك البرمجيات التي تمكن صاحبها من التحكم في الأجهزة الالكترونية عن بعد مثل كاميرا الهاتف المحمول أو ميكروفونه أو التسلل لقائمة جهات الإتصال وبياناتها والاتصال بهم والتنصت على الضحية بشكل كامل، كما تستطيع هذه البرامج استخدام الهاتف الذكي

[1] https://en.wikipedia.org/wiki/QR_code
[2] Borrett, Lloyd. Beware of malicious QR codes.- available at; http://www.abc.net.au/technology/articles/2011/06/08/3238443.htm
3 https://www.pcworld.idg.com.au/mediareleases/12655/avg-aunz-cautions-beware-of-malicious-qr-codes /

للضحية في تحديد مكانه وخريطة تنقلاته عبر برنامج تحديد المواقع العالمي GPS مما قد يسبب خطراً على حياة الضحية نفسها[1].

ويمكن الخلاص إلى أن الخطر الرئيس في استعمال رمز أو كود الاستجابة السريعة في إدارة الوثائق هو قابلية هذا الرمز/ الكود لتحمل الفيروسات والبرمجيات الضارة التي تخترق أنظمة حفظ الوثائق والاستيلاء على بيانات الوثائق، وصورها، والبيانات الخاصة للأفراد أو الشركات المنظمة لهذه النظم والمديرة لها، وبالطبع يمكن من خلال اختراق نظم حفظ الوثائق الإطلاع على البيانات الخاصة التي تحويها هذه الوثائق سواء أكانت هذه البيانات تخص أفراد/ هيئات.

2. مخاطر التوسيم: Tagging

التوسيم هو المصطلح العربي المستخدم للمرادف الانجليزي Tagging، ووسم الشئ يسمه يعني كواه فأثر فيه بعلامه ومنه ما جاء في القرآن "**سَنَسِمُهُ عَلَى الْخُرْطُومِ** [2]" واشتقت منه كلمة وسام أي العلامة أو الإشارة تعلق على الصدر كمكافأة وللتمييز عن الغير ، ومنه الوَسَامَة التي تميز شخص ما في الحسن [3].

والوسم بالإنجليزية Tag :هو كلمة مفتاحية أو عبارة تصنف بها معلومة معينة (صورة، خريطة، تدوينة، مقطع فيديو، إلى آخره) هذه الوسوم يتم إدراجها بغرض وصف المادة أو المعلومة ولتسهيل البحث والتصنيف [4].

والتوسيم هو إحدى الآليات التكنولوجية البديلة للتكشيف على شبكة الانترنت أو يمكن القول أن التوسيم هو أحد الأشكال غير التقليدية لتكشيف المعلومات والكلمات.

---

[1] https://ar.wikipedia.org/wiki/%D8%B1%D9%85%D8%B2_%D8%A7%D8%B3%D8%AA%D8%AC%D8%A7%D8%A8%D8%A9_%D8%B3%D8%B1%D9%8A%D8%B9%D8%A9

2 سورة القلم 16.

3 المعجم الوسيط_ مادة؛ وسم.

[4] https://ar.wikipedia.org/wiki/%D9%88%D8%B3%D9%85_(%D8%AA%D8%B5%D9%86%D9%8A%D9%81(

ويمكن تعريف التوسيم بأنه ربط المحتوى على موقع أو صفحة ويب بكلمات دلالية مميزة تدل على محتوى موضوعي أو أسماء مستخدمين محددين. أو هو وضع وصف بالكلمات لموقع معين أو محتوى معين على شبكة الانترنت[1].

وترجع بدايات مفهوم مشاركة المواقع على شبكة الانترنت إلى حدود عام 1996 ولكن ظهور المواقع المتخصصة التي توفر خدمة التوسيم كان عام 2003 عندما انطلقت بعض المواقع التي تقدم خدمة تخزين عناوين مواقع الإنترنت مع إضافة وسوم لوصف محتوى الموقع المخزن مما يجعلها متاحة لأي فرد من أي مكان وباستخدام أي جهاز. وتقوم خدمة التوسيم على مشاركة مجتمع المستفيدين في المصادر المفضلة لدى كل منهم. وكان في مقدمة هذه المواقع موقع خدمة المفضلة الاجتماعية del.icio.us الذي ظهر في عام 2003 وهو أول موقع يقدم تطبيقات وصف المحتوى، ومن خلاله يمكن للمشتركين في الموقع حفظ أي موقع أو صفحة على الإنترنت ووضع الكلمات المفتاحية التي تصف الموقع، وبحفظ هذا الموقع في Delicious يصبِح لدى كل عضو في هذه الخدمات قائمة من الروابط لمواقع ولمحتويات مفضلة لديه، محفوظة ومفهرسة عن طريق عملية التوسيم Tagging ويمكن للعضو أن يجعل قائمته مُشاعة بين كل الأعضاء المسجلين في نفس الخدمة، ويحق له أيضاً قصرها على نفسه فقط، دون أن يطلع عليها أحد [2]. ثم استمرت هذه الخدمة في الانتشار بعد ذلك وظهرت مواقع كثيرة توفر نفس الخدمة وتتوسع فيها وظهرت نسخة نظام التشغيل ويندوز فيستا Vista لتكون أول نسخة ويندوز تعتمد نظام التوسيم لتخزين المواقع التي يزورها المستخدمون للرجوع لها أو لمحتوياتها بعد ذلك، ثم انتشرت الخدمة في الإصدارات التالية من الويندوز كما انتشرت بين متصفحات الانترنت المختلفة.

وتكمن أهمية التوسيم في إدارة الوثائق On Line في إنه يمثل طريقة للتكشيف المباشر بالكلمات الدلالية على المحتوى الالكتروني فيمكن من خلال البحث بالكلمات المستخدمة في التوسيم إظهار كل الكلمات المطابقة أو ذات الصلة على نطاق معين. وبتطبيق ذلك على إدارة الوثائق فيمكن من خلال توسيم الصور التي تعتبر

[1] arab-librarians.blogspot.com/2006/03/blog-post_02.html
[2] https://ar.wikipedia.org/wiki/%D9%85%D9%81%D8%B6%D9%84%D8%A9_%D8%A7%D8%AC%D8%AA%D9%85%D8%A7%D8%B9%D9%8A%D8%A9

وثائق أو توسيم صور الوثائق نفسها على شبكة الانترنت بكلمات مفتاحية معينة ليتم استرجاع هذه الصور أو استرجاع محتوى الوثائق مرة أخرى بالاستعانة بتلك الكلمات المفتاحية المستخدمة في توسيم هذه الوثائق. ويعتبر موقع فليكر flicker من أشهر المواقع التي تقدم خدمة التوسيم على الصور لاستخدامها في البحث عن الصور بعد ذلك[1].

وتتمثل الخطورة في استعمال التوسيم كأداه لتكشيف الوثائق بالكلمات الدلالية في أن التوسيم عبر الويب يجعل الوثائق/الصور نفسها متاحة بشكل واسع على شبكة الانترنت وحتى مع وجود احتياطات الأمن والخصوصية في بعض المواقع فإنه بإمكان قراصنة الويب الولوج للمواقع المختصة في تقديم هذه الخدمة واختراقها والاستيلاء على خزائن الصور بها وانتهاك خصوصية أصحاب الصور/ الوثائق.

كما ينطوي التوسيم على خطورة أخرى على خصوصية الأفراد والهيئات وتظهر بشكل أكبر في مواقع التواصل الاجتماعي ألا وهي التوسيم من الغير لموقع أو حساب شخص أو جهة على صورة ونشرها على مواقع التواصل الاجتماعي (خصوصا الفيس بوك وتويتر) مما يتيح نشر هذه الصور لدي جميع أصدقاء ومتابعي هذا الشخص أو الجهة وكأنه موافق عليها أو مشتركاً فيها مما يعد انتهاك واضح لخصوصيته ونشر أشياء مصحوبه باسمه قد لايكون موافقا عليها أو متوافقا معها ، ومما يعد انتهاكاً أكبر للخصوصية على مواقع التواصل الاجتماعي أن هذه الخاصية تستخدم أيضاً في نشر الفيديوهات التي قد تكون غير لائقة أو ربما تكون إباحية ويستخدمها بعض ذوي النفوس المريضة على مواقع التواصل الاجتماعي للإساءة للآخرين والتعدي على خصوصيتهم مما يسبب حرجاً شديداً لأصحاب الحسابلت التي يتم توسيمها بعمل إشارة Tag أو Mention لها على مثل هذه المواد بغير علم أو استئذان وقد لا يستطيع الشخص دفع مثل هذه التهم عنه لدى أصدقائه أو متابعيه.

كما أن من مخاطر التوسيم في مواقع التواصل الاجتماعي استخدام القراصنة لبعض الحيل للاستيلاء على البيانات الشخصية وقوائم الأصدقاء لبعض مستخدمي مواقع التواصل الاجتماعي من خلال وسمهم أو وسم

[1] https://www.flickr.com/

أصدقاء لهم في لينكات وهمية لفيروسات أو برمجيات ضارة تحمل عناوين مشوقة وجذابة حسب رغبة المستخدم مثل أخبار فضائح المشهوين والأفلام الإباحية وبثها في لينكات موسومة بأسماء حساباتهم على مواقع التواصل الاجتماعي وما إن يضغط أي شخص على الرابط (اللينك) حتى يتم اختراق حسابه وسرقة بياناته الخاصة مثل بريده الالكتروني وكلمة مرور حسابـه على موقع التواصل وقائمة الأصدقاء، وقد تكون بعض الفيروسات أكثر خطورة من ذلك إذ تقوم بعضها بإعادة إرسال نفسها تلقائياً بعد عمل وسم أو إشارة Tag بنفس اللينكات الوهمية لجميع قوائم أصدقاء الضحايا مما يدخل عدد كبير من مستخدمي مواقع التواصل الاجتماعي في هذه الحلقة من انتهاك الخصوصية أو الاستيلاء على البيانات الشخصية.

ونظراً لسرعة التواصل عبر مواقع التواصل الاجتماعي وإقبال الجميع عليها فقد قامت معظم الهيئات والكيانات الاعتبارية بإنشاء حسابات خاصة بها على هذه المواقع، وبالطبع فإن مؤسسات حفظ الوثائق وإدارتها من ضمن هذه الكيانات التي تتعرض لخطورة الهجوم عليها من خلال فيروسات التوسيم على مواقع التواصل الاجتماعي وتهديد مستودعاتها الرقمية اذا كانت مرتبطة بالموقع أو تهديد مواقع ادارتها للوثائق عبر الانترنت.

3. مخاطر إدارة الوثائق من خلال المستودعات الرقمية و/أو نظم إدارة البريد الالكتروني:

تمثل المستودعات الرقمية digital dipositories إحدى أهم الوسائل التكنولوجية الحديثة لإدارة الوثائق. وتنقسم إدارة الوثائق في البيئة الرقمية إلى عدة أقسام وأنواع حسب الأساس المستخدم في تقسيم إدارة الوثائق. فإذا ما اعتمد التقسيم على شكل أو طبيعة الوثائق نفسها فهناك إدارة الوثائق الورقية بـلستخدام أدوات ووسائل الكترونية، وإدارة الوثائق الرقمية ذات الأصل الورقي أو المحولة رقميا Digitalized، وإدارة الوثائق المنشأة في بيئة رقمية Non Paper material. ومن حيث طريقة الإدارة نفسها هناك إدارة الوثائق بالاعتماد على برامج أرشفة الكترونية في غير بيئة الويب، وإدارة الوثائق من خلال بيئة الويب سواء من خلال برامج أرشفة متصلة بالويب أو من خلال مواقع الويب مباشرة.

ولإنشاء مستودعات رقمية يجب الاعتماد على برامج إدارة الكترونية/ رقمية للوثائق أو ما يعرف ببرامج الأرشفة الالكترونية. وهذه البرامج تضم نوعين رئيسين؛ نوع تتم من خلاله إدارة الوثائق في معزل عن بيئة الويب ونوع آخر تتم من خلاله إدارة الوثائق بالاعتماد أو بالاستعانة بالانترنت أو الويب.

وتعتبر برامج الأرشفة الالكترونية غير المعتمدة على بيئة الويب أكثر أمناً على خصوصية الأفراد والمؤسسات من تلك البرامج المتصلة بالنت أو المعتمدة على الويب. ويرجع ذلك لأن البرامج التي لا تعتمد على الويب تعمل غالباً من خلال شبكات حاسب محلية Local Networks متصلة بجهاز خادم Server يعمل على إدارة البرنامج من خلال أسماء مستخدمين وكلمات مرور تحدد من لهم حق الولوج إلى النظام أوالبرنامج ومن ثَم إلى مستودعات الحفظ الرقمي. كما تعمل هذه البرامج عادة على تقسيم أدوار المستخدمين User's Rules وتحديد الصلاحيات بينهم سواء بشكل أفقي أو هرمي، وكل هذا يحدث في معزل عن بيئة الانترنت وتنحصر الخطورة في مثل هذه البرامج في عمليات اختراق النظام الكامل الذي يسمح باخترق برنامج الأرشفة الالكتروني والحصول على اسم/ أسماء المستخدمين، وكلمة/كلمات المرور وهو ما يؤدي إلى اختراق مستودعات الحفظ الرقمي بالسيرفر (الخادم) والحصول على أي بيانات خاصة بالأفراد داخل الهيئة أو الكيان الذي يخدمه البرنامج وبيانات الهيئات أو الكيانات ذات الصلة، وهي بلاشك خطورة كبيرة ولكنها تحتاج مجهود كبير من المخترقين سواء بالتسلل من الخارج أو التسريب من الداخل لأسماء المستخدمين وكلمات المرور.

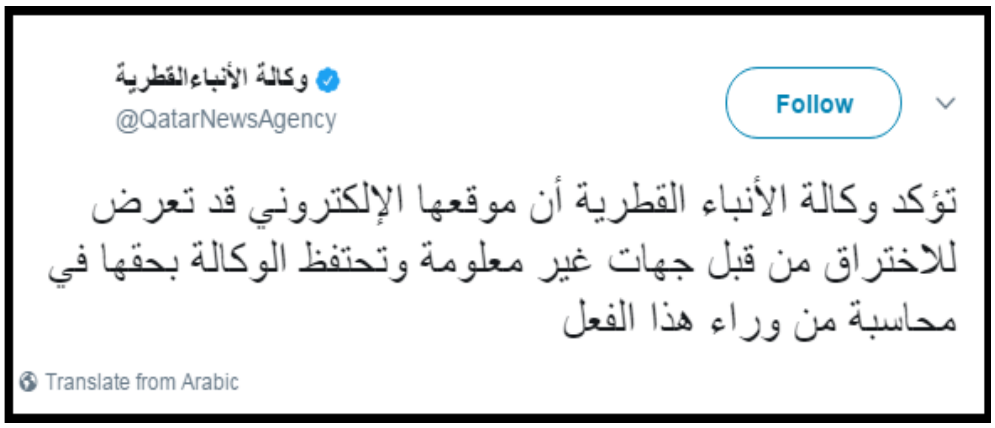
وتمثل البرامج المتصلة بالانترنت أو التي تعمل في بيئة الويب خطورة أكبر على خصوصية بيانات / معلومات الأفراد والهيئات وذلك لأنها عرضة أكبر للأختراق مباشرة من خلال الانترنت أو بيئة الويب التي تحتوي على العديد من أساليب الاختراق أو السرقة أو انتهاك الخصوصية ، ولأن تقييم مواقع الأرشيف على الانترنت يوضح أنها ذات مخاطر حقيقة وعالية لذا فهي تحتاج برامج ذات موثوقية عالية توفر الحفظ المستدام

الآمن للوثائق والملفات بصيغها المختلفة [1]، فقد يتم اختراق البرنامج من خلال الحصول على اسم المستخدم وكلمة المرور عبر برامج خاصة لسرقتهم، وهذه البرامج منتشرة على الانترنت، أو من خلال اختراق مواقع الشركات المنتجة لبرامج إدارة الوثائق والتي تكون أحياناً متصلة بها من خلال الانترنت لتحديث هذه البرامج وتقديم خدمات التحديث والصيانة عبر الخط المباشر On Line وهو ما يجعل كل البرامج المنتجة من هذه الشركات عرضة للاختراق وسرقة المعلومات و/أو البيانات الشخصية والسرية الخاصة بعملاء هذه الشركات سواء أكانوا شركات أو أفراد.

كما تتعرض نظم إدارة البريد الالكتروني للكثير من الأخطار التي تهدد خصوصية الأفراد والهيئات ، ويعد الاختراق المباشر لحسابات البريد الالكتروني من أ كبر المخاطر التي قد تمكن القراصنة من الاختراق الكامل لمستودعات حفظ الوثائق المرتبطة بنظم الحفظ المعتمدة على البريد الالكتروني. ومن أشهر حالات الاختراق التي حدثت في هذا الصدد التسريبات المعروفة باسم ويكيليكس WikiLeaks حيث تمكن مؤسسها الاسترالي "*جون أسانج*" من اختراق أنظمة وحسابات بريد الكتروني للعديد من الهيئات الدولية مثل وزارة الدفاع الأمريكية (البنتاجون) نفسها والولوج لمستودعاتها الرقمية وتسريب ملايين النسخ من الوثائق الأصلية أو صور الوثائق ونشرها على موقع ويكيلكس الذي يحاكم *أسانج* حتى الآن بسبب تأسيسه له ومازال مطلوباً في دول عدة ويلوذ باللجوء السياسي للحماية من مصير السجن مدى الحياة عقابا على هذه التسريبات ، وقد فجر هذا الموقع يوم الجمعة 19 يونيو 2015 مفاجأة مدوية بتسرية لأكثر من نصف مليون نسخة وثيقة وبرقية الكترونية تخص السعودية ونشرها على الموقع[2]. وما حدث يوم الثلاثاء 23 مايو 2017 من نشر تصريحات نسبت لأمير دولة قطر على موقع وكالة الأنباء القطرية الرسمية "قنا" ثم زعم الوكالة على حسابها على موقع تويتر أن موقعها قد تم اختراقه وأنها لم تنشر هذه التصريحات، وذلك كما يتضح بالصورة التالية:

[1] Lawrence, Gregory W. et al. (2000). Risk Management of Digital Information: A File Format Investigation.- Washington, D.C.: Council on Library and Information Resources. P.15.

[2] https://wikileaks.org/saudi-cables/press-ar



وكذلك اختراق بريد سفير دولة الإمارات في واشنطن بداية يونيو 2017 وتسريب مراسلات تعود حتى عام 2014، وغير ذلك من أمثلة اختراق مستوعات حفظ الوثائق الخاصة والعامة التي لا يتوقع أن تنتهي أو يتم القضاء عليها قريبا أو بشكل نهائي.

كما تعتبر القرصنة على القراصنة من المخاطر التي تهدد خصوصية الأفراد والهيئات على عدة مستويات. ومن ذلك قرصنة بعض محترفي الاختراق الالكتروني على شركة هاكينج تيم Hacking Team الإيطالية المتخصصة في تزويد الحكومات ببرمجيات التجسس المختلفة سواء على الأفراد أو على الشركات والهيئات الاعتبارية المختلفة [1]، وعلى الرغم من تأكيد الشركة على التزامها بعدم تزويد أي حكومة أو دولة ببرمجياتها إلا تلك الحكومات التي تحترم حقوق الإنسان ولا توجد عليها عقوبات من جهات دولية عدة منها الأمم المتحدة والاتحاد الأوروبي وحلف شمال الأطلنطي[2]، إلا أن الدور الذي تقوم به الشركة يثير حولها العديد من الشكوك، ومازالت العديد من المنظمات والهيئات الحقوقية توجه للشركة أصابع الاتهام حول تعاونها في هذا الصدد مع حكومات مارقة أو غير شرعية، أو لا تحترم حقوق المواطنين وذلك خارج إطار القانون.

وقد تمكن موقع التسريبات الأشهر في العالم ويكيلكس من الاستيلاء حسب زعم القائمين عليه على أكثر من مليون وثيقة مسربة من موقع شركة هاكينج تيم Hacking Team تخص حكومات وهيئات تعاملت معها

[1] https://en.wikipedia.org/wiki/Hacking_Team
[2] http://www.hackingteam.it/index.php/about-us

الشركة وبيانات ومعلومات استطاعت هذه الحكومات الوصول إليها باستخدام برامج الشركة [1]، ويعد هذا نموذجا للقرصنة على القراصنة وهو ما يمثل خطورة على خصوصية الشركة المنتجة لبرمجيات التجسس هاكنج تيم، وعلى الحكومات/ الهيئات التي استعملت هذه البرمجيات، وعلى الأفراد أو الهيئات التي استخدمت هذه البرامج للتجسس عليهم.

4. مخاطر إدارة الوثائق في نظم الحياة الثانية: Second Life

الحياة الثانية أو **Second Life** هي لعبة قامت بتصميمها شركة ليندن لاب Linden Lab ومقرها سان فرانسيسكو عام 2003 [2]. وهذه اللعبة تقوم على تكوين عالم افتراضي متكامل من شخصيات وهيئات ومباني وأراضي وجامعات ومؤسسات صحفية وإعلامية .....الخ. وقد انتشرت الفكرة حتى خرجت من إطار اللعبة وانضمت إليها كيانات حقيقة أنشأت لها كيانات افتراضية في عالم الحياة الثانية، وقد كان من بين هذه الكيانات وكالة رويترز، وبي بي سي، والكثير من الشركات الكبرى، وبعض الأندية الرياضية الشهيرة؛ حتى أن دولة السويد افتتحت سفارة افتراضية بالحياة الثانية[3]. وقد أنشئت جامعات دولية كبرى فروع لها في عالم الحياة الثانية ومنها جامعات عربية مثل جامعة الملك عبدالعزيز، كما قامت جامعة ستانفورد بإنشاء مقر افتراضي لها في الحياة الثانية، وأنشأت كذلك أرشيف خاص بها هناك[4].

ومع تحول الحياة الثانية من مجرد لعبة إلى عالم وواقع افتراضي متكامل بدأ الاتجاه نحو إدارة الوثائق والأرشيف من خلال هذا الواقع الافتراضي الذي أصبح يتطور يوماً بعد يوم ويوفر إمكانيات كبيرة لإدارة الوثائق من خلاله. ولكن تبقى المخاطر قائمة لإدارة الوثائق في الحياة الثانية مثلها تماماً مثل تلك المخاطر التي تهدد إدارة الوثائق والأرشيف في المستودعات الرقمية المتصلة بالانترنت حيث أن الحياة الثانية تمثل نوع من هذه

---

[1] https://wikileaks.org/hackingteam/emails/
[2] secondlife.com
[3] https://ar.wikipedia.org/wiki/%D8%B3%D9%8A%D9%83%D9%86%D8%AF_%D9%84%D8%A7%D9%8A%D9%81
[4] https://library.stanford.edu/spc/more-about-us/projects-and-initiatives/virtual-archives-second-life

المستودعات التي تعمل على إدارة الوثائق مباشرة من خلال بيئة الويب، وما قيل عن مخاطر تتهدد المستودعات الرقمية للوثائق ينطبق تماماً على إدارة الوثائق من خلال الحياة الثانية أو العالم الافتراضي حيث أنه عرضه للقرصنة والاختراق بشكل كامل.

5. المخاطر المبنية على إنشاء الوثائق في البيئة الرقمية:

يعتبر إنشاء الوثائق في البيئة الرقمية إحدى تجليات عصر الانترنت والحكومة الالكترونية الذي أصبح منتشراً في العالم الآن. ويقصد بالوثائق المنشأة في البيئة الرقمية Born-digital archival material تلك الوثائق التي ليس لها أصل ورقي وإنما أنشئت واستعملت مباشرة عبر الحاسب الآلي وشبكة الانترنت، ومن أمثلة هذا النوع من الوثائق و/أو المواد الأرشيفية؛ المراسلات البريدية عبر البريد الالكتروني ومواقع الهيئات والكيانات ذات الصفة القانونية، والرسائل النصية الهاتفية....وغيرها.

وقد خصصت بعض الهيئات والجهات المتخصصة والبحثية برامج لدراسة الأخطار التي تهدد هذا النوع من الوثائق والمواد الأرشيفية واقتراح الخطط والبرامج لحمايتها من هذا الأخطار. وقد عمدت جامعة ستانفورد لإطلاق مشروع أطلق عليه برنامج الوثائق المولودة رقمياً The Born-Digital Program يتبع مكتبة جامعة استانفورد SUL حيث يهدف لحماية الوثائق المنشأة في البيئة الرقمية والعمل على الولوج إليها بشكل دائم وآمن[1]. ويمكن حصر الأخطار التي تواجه الوثائق المنشأة رقمياً في الآتي:

أ. التقادم الذي يصيب البرامج التي توفر إمكانية قراءة هذه الوثائق أو المواد الأرشيفية والولوج إليها.

ب. إمكانية تدمير هذه الوثائق أو المستودعات الرقمية المتضمنة لها ومحوها من الوجود بشكل كامل، في حالة عدم وجود نظير مادي لها.

ج. الولوج غير المصرح لهذه الوثائق من قبل القراصنة.

[1] https://library.stanford.edu/spc/more-about-us/born-digital-program

د. التلاعب في شكل وطبيعة هذه الوثائق من خلال البرامج الحديثة مما يغير من بياناتها أو يشكك في صحتها.

هـ. عدم اكتسابها الحجية القانونية الكاملة في بعض الدول نتيجة تخلف البنية التشريعية عن البنية التكنولوجية.

6. المخاطر المبنية على استعمال البطاقات الائتمانية/ الفيزا كارت ATM

تعتبر البطاقات الائتمانية/ الفيزا كارت أحدث شكل من أشكال التعامل المالي وأكثرها انتشاراً في العالم الآن فهي تحل محل النقود الورقية ويمكن الشراء والدفع عن طريقها في الأسواق والمحلات وعبر الانترنت. وبطاقات الائتمان هي نوع من أنواع الوثائق المالية المعترف بها عالمياً وتحمل بيانات مهمة لحاملها وعن حاملها.

وهناك العديد من المخاطر التي تواجه استعمال بطاقات الائتمان بسبب طمع اللصوص في الاستيلاء على بياناتها الخاصة مما يعني الاستيلاء عملياً عليها واستعمالها في دفع ثمن سلع يتم شرائها عبر الانترنت، أو في تحويل مبالغ من حساب صاحبها لحساباتهم الخاصة. وتتعدد أساليب الاستيلاء على الأموال من خلال بطاقات الائتمان، حيث تتراوح هذه الأساليب بين الاستيلاء المادي على البطاقة نفسها، أو تزويرها وتزييفها، أو الاستيلاء على بياناتها الخاصة واستعمالها في سحب النقود أو أداء ديون بها، وهذه البيانات هي رقم البطاقة المسلسل وبياناتها داخل البنك وهذه البيانات تكون مسجلة على الشريط الممغنط على جسم البطاقة، بينما يعتبر الرقم السري الذي يدخله العميل بمثابة التوقيع الالكتروني لصاحب البطاقة، أو بمثابة مفتاح بطاقة الائتمان نفسها، وهوما اعتبره جانب من الفقه القانوني المصري ارتكاباً لجريمة السرقة باستعمال مفتاح مُصنَّع، وتعتبر البطاقة المزورة ورقمها السري من قبيل المفتاح المصنع، وهو ما يؤكد ذلك أن المُشرِّع لم يحدد المقصود بالمفتاح[1].

[1] عبد الجبار الحنيص (2010). الاستخدام غير المشروع لبطاقات الائتمان الممغنطة من وجهة نظر القانون الجزائي._ مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، مج26، ع1._ ص86.

وهناك أساليب متعددة للحصول على بيانات البطاقات الائتمانية بشكل غير مشروع، يمكن تخيصها في الآتي[1]:

- **أسلوب الخداع:** وتستخدم في هذا الأسلوب أشكال مختلفة من الخدع التي تستخدم للحصول على البيانات الخاصة ببطاقة الائتمان. ويعد أشهر هذه الأشكال إنشاء مواقع الكترونية وهمية للشركات والمؤسسات التجارية الكبرى عن طريق سرقة بيانات مواقع هذه الشركات من على الانترنت، ومن ثم اصطياد زبائن هذه الشركات وسرقة بيانات بطاقاتهم الائتمانية.

- **تخليق أرقام البطاقات:** ويسمى هذا الأسلوب Card cash وتستخدم فيه برامج متطورة تستعمل معادلات رياضية معقدة لتخليق أرقام بطاقات ائتمانية تبع بنك معين وسرقة حسابات هذه البطاقات.

- **الاختراق غير المشروع Illegal access لمنظومة خطوط الاتصالات العالمية:** وفي هذا الأسلوب يقوم القراصنة باختراق الحسابات الحقيقية الخاصة بالمتاجر والشركات على شبكة الانترنت وسرقة بيانات البطاقات الائتمانية لزبائن هذه المتاجر والشركات.

- **أسلوب تفجير الموقع المستهدف:** ويستهدف مستخدمو هذا الأسلوب في السرقة الحواسب المركزية للبنوك والمؤسسات المالية وذلك من خلال بث آلاف أو عشرات الآلاف من الرسائل الالكترونية للموقع المستهدف في نفس الوقت مما يشكل حملاً ثقيلاً على الموقع ومع تزايد الضغط قد ينفجر الموقع نتيجة تحميله سعة تخزينية أكبر من قدرته مما يتسبب في انفجار الموقع وتشتت المعلومات به، فيستطيع المخترقون الحصول على خزائن بيانات البطاقات الائتمانية بالموقع.

---

[1] سليمان أحمد فضل (بدون تاريخ). الجرائم المتعلقة باستخدام بطاقات الائتمان عبر شبكة الانترنت._ مركز الإعلام الأمني._ ص4.

- **السرقة المباشرة لبيانات بطاقات الائتمان:** يعمد بعض اللصوص في المتاجر والمطاعم، وغيرها إلى استخدام ماكينات دفع اليكتروني تحتفظ ببيانات البطاقة الائتمانية والرقم السري الذي أدخله العميل ومن خلال هذه البيانات يتم استخدام البطاقة للدفع أو تحويل الأموال عبر الانترنت، أو يقومون بتخليق بطاقات مادية واستخدامها في صرف الأموال من حساب العميل.

7. مخاطر التكنولوجيا على الأرشيف الشفوى Oral Archive

يعد الأرشيف الشفوي من أكثر مباحث الأرشيف حرجاً وغموضاً وصعوبة في التقنين. فالأرشيف الشفوي يضم عدة أنواع من المواد الأرشيفية قد يصعب تقنينها معاً في معيار واحد. ومازال الجدل قائماً بين الأرشيفيين حول الأرشيف الشفوي، وحول أنواع المواد الشفوية التي يمكن أن تدخل ضمن هذا الأرشيف وكيفية حفظها أو إدارتها حيث تتعدد الآراء حول ما يمكن أن يعد مصدراً شفوياً، وما لا يدخل في عداد تلك المصادر. فالبعض لا يوافق على عد كل ما يتم إعداده دون نظام محكم دقيق يلتزم بمعايير وقواعد وقوانين الشاهد والدليل المتعارف عليه كمصدر شفوي، في الوقت الذي يشعر فيه آخرون بالرضا نحو أي شكل من أشكال المواد الشفوية مثل بعض المواد الصحفية ومجموعات روايات الأدب الشعبي وغيرها. كذلك يُدْخِل بعضهم في المصادر الشفوية التسجيلات المعاصرة للاجتماعات واللقاءات والخطب وغيرها، وهذا القبول الواسع لأنواع المواد الشفوية يضع صعوبات بالغة أمام الأرشيف ليقرر ما يصلح منها أن يكون مصدراً أرشيفياً وما لا يصلح[1].

وفى ظل المدّ التكنولوجى الذى طغى على الحياة التقليدية، ينبغى أن ينتبه الأرشيفيون بدورهم إلى قيمة المعلومات التى يقدّمها التاريخ الشفهى لسدّ الثغرات التى يتركها ـ عادة ـ التاريخ الرسمى، فإذا كان من أهداف الوظيفة الأرشيفية حفظ الوثائق لإتاحتها لأنها ذاكرة الأمة؛ فينبغي أن يخرج الأرشيفيون خارج دوائر الوثائق

[1] ناهد حمدي أحمد. المصادر الشفوية والأرشيف._ متاح في: https://goo.gl/DEXRva

المكتوبة أو المنتجة الكترونيا ويشاركوا فى إنتاج وإدارة وثائق تمثّل جزءًا أصيلاً من عملهم الأكاديمى والمهنى وهي الوثائق المعتمدة على الأرشيف الشفهي[1].

ويعتبر الاعتداء على الأرشيف الشفوي من أخطر صور الاعتداء على الخصوصية سواء للأفراد أو الهيئات، حيث عادة ما يحوي الأرشيف الشفوي مخاطبات أو محادثات شخصية بين أفراد أو بين ممثلي هيئات تتضمن بيانات سرية أو خاصة لايجب الاطلاع عليها إلا بإذن صاحبها.

وتعتبر برامج التجسس على الاتصالات، والمحادثات الهاتفية من أكبر المخاطر على الأرشيف الشفوي سواء للأفراد أو الهيئات. خصوصا تلك البرامج التي تقتنيها بعض الحكومات للتجسس على المواطنين أو المعارضين أو التجسس على الكيانات الاعتبارية بشكل غير قانوني أو شرعي. وقد ظهرت في مصر في السنوات الأخيرة نماذج للاستخدام السئ لمثل هذه البرامج من خلال التنصت على هواتف بعض الشخصيات العامة ونشر محادثاتهم الهاتفية على الجمهور وفي برامج تليفزيونية مما يعد انتهاك صارح لخصوصية هؤلاء الأفراد خصوصا وأن هذا الأمر حدث بدون إذن قضائي ولم يعاقَب مرتكبوه على انتهاكهم لخصوصية أشخاص آخرين دون وجه حق وبلا سند قانوني أو إذن قضائي، رغم أن المادة 309 مكرر من قانون العقوبات عاقبت بالحبس ومصادرة الأجهزة والأدوات المستخدمة ومحو التسجيلات المتحصلة من الجريمة كل من ارتكب إحدى صور الاعتداء على حرمة الحياة الخاصة للمواطنين التي قسمها هذا النص إلى نوعين:

1 –استراق السمع أو التسجيل أو النقل عن طريق أي جهاز لمحادثات جرت في مكان خاص أو عن طريق التليفون.

2 –التقاط صورة لشخص في مكان خاص.

كما نصت المادة 309 مكرر (أ) على الآتي:

"يعاقب بالحبس كل من أذاع أو سهل إذاعة أو استعمل ولو في غير علانية تسجيلا أو مستندا متحصلا عليه بإحدى الطرق المبينة بالمادة السابقة أو كان بغير رضاء صاحب الشأن.

[1] أمنية عامر (يونيو2005). التاريخ الشفهي: تاريخ يغفله التاريخ._ cybrarian journal، ع5._ 2015/8/19._ متاح في: http://www.journal.cybrarians.org/index.php?option=com_content&view=article&id=556:2011-09-21-06-32-42&catid=245:2011-09-21-06-27-06&Itemid=69

ويعاقب بالسجن مدة لا تزيد على خمس سنوات كل من هدد بإفشاء أمر من الأمور التي تم التحصل عليها بإحدى الطرق المشار إليها لحمل شخص على القيام بعمل أو الامتناع عنه.

ويعاقب بالسجن الموظف العام الذي يرتكب أحد الأفعال المبينة في هذه المادة اعتمادا على سلطة وظيفته، ويحكم في جميع الأحوال بمصادرة الأجهزة وغيرها مما يكون قد استخدم في الجريمة أو تحصل عنها، كما يحكم بمحو التسجيلات المتحصلة عن الجريمة أو إعدامها[1]". وهذه المفارقة بين النص القانوني والأداء الرسمي للدولة المصري جعل سمعة مصر عالمياً تتأثر بكونها تاريخياً دولة لاتهتم كثيراً بحماية خصوصية الأفراد بها على الرغم من وجود العديد من النصوص الدستورية والقوانين التي تؤكد على حماية الدولة لخصوصية المواطنين في كل المراسلات والاتصالات الخاصة[2].

وتلجأ الحكومات عادة لشركات متخصصة في مجال الـ IT لشراء مثل هذه البرمجيات التي تتيح لها التنصت على الهواتف والمحادثات عبر الانترنت، خصوصا وأن الهواتف المحمولة الآن أصبحت تمتلك تقنيات متقدمة جدا لجمع المعلومات فهي قادرة على رصد وتخزين كل بريد الكتروني يجريه مالكها أو مستخدمها وكل أغنية يستمع لها بالإضافة إلى كل مكالمة يجريها أو رسالة نصية يرسلها أو يستقبلها، غير أنها قادرة على رصد وتحديد الموقع الجغرافي له وتتبعه وإرسال ذلك عبر شبكة الانترنت[3].

ومن أشهر هذه الشركات شركة Fin Fisher [4]، والتي تزود الحكومات ببرامج تجسس على الأفراد تستطيع الولوج منها إلى هواتف الأفراد الشخصية ونسخ قوائم الأصدقاء وإرسال التطبيقات الضارة منها إلى الهواتف الأخرى، كما تستطيع هذه البرامج اختراق الحواسيب الشخصية وفتح الكاميرا والميكروفون والتسجيل لصاحبها دون أن يشعر، وكذلك الحصول على ملفات وصور من حاسبه الشخصي دون معرفته.

---

[1] مؤسسة حرية الفكر والتعبير (2011). حرية تداول المعلومات: دراسة قانونية مقارنة._ ط 1._ مؤسسة حرية الفكر والتعبير: القاهرة._ ص47، 48.

[2] Mendel. P.81.

[3] Richard M., Marsh Jr. (2009). Legislation for Effective Self-Regulation: A New Approach to Protecting Personal Privacy on the Internet, Michigan Telecommunications and Technology Law Review, Volume15, Issue 2. PP. 542-563; Available at: http://repository.law.umich.edu/mttlr/vol15/iss2/8

[4] https://www.finfisher.com/FinFisher/index.html

وتسعى الحكومات من خلال الرقابة على الانترنت وانتهاك خصوصية الأفراد إلى السيطرة على المجتمعات التي أصبحت مفتوحة ولايمكن السيطرة عليها، وحتى الدول الديمقراطية التي لديها قوانين تحمي خصوصية الأفراد تتعلل أحياناً بحجج مثل الإرهاب ومكافحة الجرائم الالكترونية لانتهاك خصوصية الأفراد والحصول على بياناتهم السرية[1].

وسائل مكافحة السطو الرقمي على البيانات الشخصية:

يهيمن حاليًا اتجاهين رئيسين على النقاش حول كيفية حماية الخصوصية الشخصية على الإنترنت، المعسكر الأول يدعو إلى حماية الخصوصية على شبكة الإنترنت عن طريق التدخل الحكومي باللوائح والقوانين ووضع تشريع يضع حدودًا صارمة على كيفية قيام الشركات بجمع البيانات عبر الإنترنت، وأنواع المعلومات الشخصية التي يمكنها جمعها، وكيفية استخدامها، ويؤكد أنصار هذا النهج على أن التنظيم الحكومي القوي ضروري لحماية مستخدمي الإنترنت غير المتشككين من سلوك الشركات على الإنترنت. بينما ويقاوم أصحاب المعسكر الآخر تدخل الحكومة في اقتصاد الإنترنت الهش وسريع الحركة، ويرون أن التنظيم الذاتي للسوق والصناعة سيحقق نتائج أفضل من القواعد واللوائخ الحكومية، ويؤكد أصحاب هذا الرأي أن شركات الإنترنت لديها بالفعل حافز في السوق لحماية خصوصية المستخدم لتجنب فقدان الزبائن، وبالتالي فإن التدخل الحكومي في هذه الحالة غير ضروري ويمكن أن يؤدي إلى نتائج عكسية[2].

تنقسم وسائل مكافحة السطو على البيانات الشخصية إلى عدة أقسام أو محاور قد تعمل منفردة كل على حدة أو تعمل معاً في تناغم وتكامل. وهذه المحاور أو الأقسام هي:

1. الاحتياطات الشخصية للفرد أو المؤسسة للمحافظة على سرية البيانات الشخصية.

[1] محمد الطاهر.مصدر سابق ._ ص6.

[2] Hirsch, Dennis D. (2011). The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?.- *Seattle University Law Review.*- Vol. 34. PP. 439-480.

استخدام اسم/أسماء مستخدمين، و كلمات مرور قوية يصعب التنبه بها ولا يمكن الوصول لها أو توقعها بسهولة، على أن يتم تغييرها كل فترة. كما تعمد بعض الجهات لتغيير كلمات المرور بشكل دائم وهو أمر مستحب يساعد في حماية النظام من التسلل. كما تستخدم بعض الهيئات أسلوب أدوار المستخدمين لتحديد صلاحيات كل فرد داخل الهيئة في الولوج للنظام بها. علاوة على ذلك يمنع تسجيل بيانات الولوج للنظام أو البيانات الشخصية أو السرية غير المتصلة بالنظام مباشرة على الحاسب الآلي للشخص أو الهيئة حتى لا تعطي الفرصة لأحد بالاطلاع عليها ومعرفتها ولو من قبيل المصادفة.

2. الإجراءات المتخذة لعدم الوقوع كفريسة للبرمجيات الخبيثة.

تتجه الهيئات الاعتبارية والأشخاص ذوي الأهمية لاستخدام برامج مكافحة الفيروسات، والجدران النارية، واستخدام برامج الكترونية أصلية وحديثة. ورغم التكلفة المالية التي تمثلها مثل هذه الاحتياطات لكنها توفر على مستخدميها الكثير في حماية خصوصيتهم، وبياناتهم الشخصية. كما تعمل البرمجيات الأصلية على منع تسلل الفيروسات والبرمجات الضارة إلى النظام وتنبه لها أولاً بأول وتستطيع البرامج الأصلية لمكافحة الفيروسات التخلص من أي برامج ضارة أو غريبة على النظام ولم يتم السماح لها من ذي صفة بالولوج إلى النظام وأجهزة الحاسب به.

3. الإجراءات الوقائية لمنع تسلل القراصنة إلى البيانات الشخصية.

لعدم تسلل القراصنة إلى البيانات الشخصية للأفراد والهيئات والكيانات الاعتبارية يعمد البعض لاتخاذ بعض الإجراءات الوقائية منها عدم الدخول على مواقع الكترونية غير موثوقة وعدم قبول أي دعوات الكترونية غير معلومة المصدر ومؤمنة بشكل كامل. وكذلك عدم الدخول على مواقع الدعاية أو الألعاب، وعدم فتح رسائل البريد الالكتروني العشوائية/المؤذية Spam خصوصاً إذا كانت تحمل مرفقات Attachments، أو روابط لمواقع الكترونية.

وسوف يقدم البحث مجموعة من التوصيات في هذا الصدد في نهاية البحث تنبه للاحتياطات الواجب اتخاذها من قبل الأفراد و/أو الهيئات والكيانات الاعتبارية لحماية خصوصيتهم وبياناتهم السرية.

الخصوصية الرقمية والمشكلات التشريعية في مصر:

لا يوجد تشريع خاص مُلزِم عالمياً للتعامل في مسائل الخصوصية وحماية سرية البيانات الخاصة يغطي جميع بلدان العالم. وقد طبّقت 89 دولة قوانين حماية الخصوصية والبيانات، وكثير منها ينظِّم التدفق الدولي للبيانات كآلية لحماية خصوصية الأفراد وإنفاذ السياسات الوطنية [1]. وتتسم التشريعات المصرية عموماً والتشريعات المتعلقة بالتكنولوجيا الحديثة خصوصاً بالتقادم الشديد وعدم صلاحيتها أو على الأقل عدم مجاراتها لمستجدات البيئة الرقمية التي تتغير وتتطور كل يوم. ويجب العمل على إعادة بناء البيئة والبنية التشريعية المصرية لتوائم التطور التكنولوجي لضمان حقوق الأفراد في خصوصيتهم وسرية بياناتهم عبر الانترنت، ولمكافحة جرائم الانترنت بالشكل الذي يناسب تطورها وتسارعها وتغير أشكالها يوما بعد يوم.

وينبغي مراعاة أن أي قانون يصدر للتعامل مع جرائم الانترنت يجب ألا يكون الهدف منه تقييد حرية الأفراد على الشبكة العالمية ولكن الحرص على حماية خصوصية الأفراد والهيئات من الاختراق أو التعدي عليها، وأن يعاقب مرتكبوا هذه الجرائم بمثل العقوبات المترتبة عن انتهاك خصوصية الأفراد والهيئات في الواقع المادي والاستيلاء على مايضر بهذه الخصوصية أو التلاعب بها.

كما ينبغي تطوير البنية التشريعية المصرية بحيث يتم الاعتراف بالوثائق التي تنتج في البيئة الرقمية والتعامل بها في الجهات الرسمية لتسهيل إتاحة وإدارة الوثائق من ناحية، ولتسهيل تعامل المواطنين مع الجهات

[1] الاتحاد الدولي للاتصالات (2013). حماية البيانات والخصوصية في الحوسبة السحابية؛ جزء من تقرير "اتجاهات الإصلاح في الاتصالات لعام 2013._ موقع مجلة الاتحاد الدولي للاتصالات swen UIT. _2015/8/21_ متاح في: https://itunews.itu.int/Ar/Note.aspx?Note=3726

الجكومية من ناحية أخرى، وذلك بعد أخذ الاحتياطات والضمانات اللازمة لضمان صحة هذه الوثائق وخلوها من التلاعب بالتزييف أو التزوير.

النتائج والتوصيات:

أولاً: النتائج: يمكن الخروج من هذه الدراسةبالنتائج التالية:

1. تمثل البرمجيات الضارة (الفيروسات) الخطر الأكبر على خصوصية الأفراد والهيئات في عالم إدارة الوثائق عبر الانترنت. وأكثر الجرائم انتشاراً وتأثيراً في عالم الشبكات[1].
2. قد يكون الأفراد أنفسهم السبب الرئيس في انتهاك خصوصيتهم عبر وقوعهم فريسة أو ضحية للفيروسات والبرمجيات الضارة نتيجة فضولهم وحب استطلاعهم أو عدم خبرتهم أو ميولهم الإباحية.
3. تمثل تصرفات بعض الحكومات غير المسؤولة خطراً على خصوصية مواطنيها والكيانات الاعتبارية بها بل خطرا على أمنها القومي نفسه عن طريق استعانتها بشركات دولية للتنصت على الأفراد والهيئات والكيانات الاعتبارية بها.
4. مع تطور التكنولوجيا تتطور تلقائياً فرص انتهاك خصوصية الأفراد وربما بشكل أكبر وأسرع نمواً.
5. مازالت البنية التشريعية والفنية في مصر والعالم العربي عموماً متأخرة عن التطور التكنولوجي في إدارة الوثائق وحماية خصوصية الأفراد على حد سواء.
6. مع التطور التكنولوجي أصبح انتهاك الخصوصية ممكن على مستويات متعددة قد تصل إلى اختراق المخترقين والقرصنة على القراصنة أنفسهم مما يؤدي لانتهاكات واسعة النطاق كماً وكيفاً.

[1] عزيزة عبدالرحمن العتيبي (2010). أثر استخدام تكنولوجيا المعلومات على أداء الموارد البشرية: دراسة ميدانية على الأكاديمية الدولية الاسترالية._ الأكاديمية العربية البريطانية للتعليم العالي._ ص39.

7. مازالت برامج الحماية من القرصنة ومن اختراق الخصوصية عاجزة عن السيطرة بشكل كامل على أعمال انتهاك الخصوصية المختلفة.

8. مع دخول تطبيقات الهواتف الذكية لمجال إدارة المواد الوثائقية عبر الانترنت أصبح الأفراد معرضون لانتهاك خصوصيتهم على أكبر مستوى، حيث قد يصل الاختراق الى سرقة بيانات الشخص وبيانات أصدقائه وحتى فتح كاميرا هاتفه المحمول وتسجيل مكالماته.

ثانياً: التوصيات:

1. التوصية للأفراد بعدم التعامل مع أي برمجيات أو لينكات غير موثوقة تصل لهم عبر مواقع التواصل الاجتماعي أو البريد الالكتروني.

2. التوصية لدى الهيئات والكيانات الاعتبارية باستعمال برمجيات أصلية وموثوقة في إدارة وثائقها والاستعانة ببرامج أصلية لمكافحة للفيروسات.

3. التوصية بتجنب استخدام بطاقات الصرف الآلي للشراء عبر الانترنت إلا في أضيق الحدود ومن خلال مواقع معروفة وموثوقة ومؤمَّنة.

4. التوصية بالابتعاد عن استخدام تطبيقات الهاتف الذكي للدخول لمواقع غير موثوقة قد تكون أداة للسيطرة على الهاتف واختراق خصوصية صاحبه وخصوصية أصدقائه.

5. تجنب الحكومات استخدام برامج التجسس الدولية والتوصية بتجريم أي مسؤول يعمل على انتهاك خصوصية المواطنين والكيانات الاعتبارية.

6. التوصية لدى الأفراد والهيئات باستخدام كلمات مرور للمواقع والبريد الالكتروني مختلفة أي عدم تكرار كلمة المرور ذاتها في أكثر من موقع، واختيار كلمات مرور قوية وتغييرها كل فترة، وعدم تدوينها في أي وسيط ورقي أو على الهاتف أو الكمبيوتر[1].

7. التوصية لدى الحكومات، والهيئات والكيانات الاعتبارية بتوعية الموظفين بمخاطر الانترنت والنظم الحديثة في إدارة الوثائق وكيف مواجهتها وتجنب الوقع فريسة للبرمجيات الضارة، وتدريبهم على التعامل مع هذه المواقف بشكل محترف.

8. التوصية بعد ترك أجهزة الاتصال الشخصية متصلة بالانترنت بشكل دائم وفصلها فور الانتهاء من الأعمال على الويب.

9. التوصية بتعمية [2] كاميرا اللاب توب في حالة عدم استخدامها حتى لاينفذ من خلالها المخترقون وربما يصوروا الشخص في وضع يمثل تهديدا له.

الخاتمة:

في ختلم هذه الدراسة يمكن القول بأن البرامج والأنظمة الحديثة لإدارة الوثائق مثلت نقله مهمة في عالم الأرشيف، وسهلت إدارة الوثائق وإتاحتها بشكل أفضل والاستفادة منها على نطاق أوسع. كما ساعدت هذه البرامج والنظم على المحافظة على الأصول المادية للوثائق غير المنشأة في البيئة الرقمية، وسهلت التعامل مع نسخ منها دون اتلاف أو ضياع الأصل. كما ساعدت على إنشاء الوثائق في بيئة رقمية وإدارتها رقمياً بالكامل مما سهل حياة الناس بشكل كبير.

[1] http://privacyanddatasecurity.blogspot.com/

[2] **من الممكن وضع شريط لاصق على الكاميرا لاغلاقها مادياً.**

وينبغي التأكيد على أن التكنولوجيا دائما تحمل معها حلولاً ومخاطر في ذات الوقت؛ لذا وجب التنبيه لهذه المخاطر والتحذير منها، والعمل على مكافحتها بشكل دائم. كما يجب اتخاذ الاحتياطات اللازمة لحماية الوثائق في البيئة الرقمية من الاختراق أو التدمير أو السرقة ولحماية خصوصية الأفراد والهيئات من القراصنة والمتسللين.

قائمة المصادر والمراجع:

أولا: المصادر العربية:

1) **الاتحاد الدولي للاتصالات (2013). حماية البيانات والخصوصية في الحوسبة السحابية؛ جزء من تقرير "اتجاهات الإصلاح في الاتصالات لعام 2013._ موقع مجلة الاتحاد الدولي للاتصالات.**

2) **الأمم المتحدة – مجلس حقوق الإنسان (2014). (الحق في الخصوصية الرقمية) تقرير مفوضية الأمم المتحدة السامية لحقوق الإنسان.**

3) أمنية عامر. التاريخ الشفهي (يونيو2005): تاريخ يغفله التاريخ._ cybrarian journal._ ع5.

4) أمينة حمشاشي (2009). ماهية الجريمة المعلوماتية._ دراسات وابحاث، مج 1، ع 1، ص ص 450_458.

5) رجب عبد الحميد حسنين (سبتمبر2012). أمن شبكات المعلومات الالكترونية: المخاطر والحلول._ Cybrarians Journal._ ع30.

6) خالد بن سليمان الغثبر، أمل ناصر الصبيح (مايو 2012). حال أمن المعلومات في المملكة العربية السعودية._ دراسات المعلومات، ع14.

7) سوزان عدنان الأستاذ (2013). انتهاك حرمة الحياة الخاصة عبر الانترنت: دراسة مقارنة._ مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، مج29، ع3._ ص ص 421-455.

8) سليمان أحمد فضل. الجرائم المتعلقة باستخدام بطاقات الائتمان عبر شبكة الانترنت._ مركز الإعلام الأمني.

9) عايض المري. الخصوصية وحماية البيانات. متاح في: https://goo.gl/NjGqc6

10) عبد الجبار الحنيص (2010). الاستخدام غير المشروع لبطاقات الائتمان الممغنطة من وجهة نظر القانون الجزائي._ مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، مج26، ع1.

11) عزيزة عبدالرحمن العتيبي (2010). أثر استخدام تكنولوجيا المعلومات على أداء الموارد البشرية: دراسة ميدانية على الأكاديمية الدولية الاسترالية._ الأكاديمية العربية البريطانية للتعليم العالي.

12) المجلس الدولي للأرشيف (2012). مبادئ إتاحة الوثائق._ ترجمة: أماني محمد عبدالعزيز.

13) مجمع اللغة العربية (2004). المعجم الوسيط._ ط4._ القاهرة: مكتبة الشروق الدولية.

14) محمد الطاهر (2013). الحريات الرقمية: المفاهيم الأساسية._ ط 1._ القاهرة: مؤسسة حرية الفكر والتعبير.

15) محمد على سالم، حسون عبيد هجيج (2007). الجريمة المعلوماتية._ مجلة جامعة بابل للعلوم الانسانية._ مج15، ع2.

16) محمد محمد الهادي (يونيو 2006). توجهات أمن وشفافية المعلومات في ظل الحكومة الإلكترونية._ ._ Cybrarians journalع 9

17) منى تركي الموسوي (2013). الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها._ منى تركي الموسوي، جان سيريل فضل الله._ جامعة بغداد: مجلة كلية بغداد للعلوم الاقتصادية الجامعة العدد الخاص بمؤتمر الكلية.

18) مؤسسة حرية الفكر والتعبير (2011). حرية تداول المعلومات: دراسة قانونية مقارنة._ ط 1._ مؤسسة حرية الفكر والتعبير: القاهرة.

19) ناهد حمدي أحمد. المصادر الشفوية والأرشيف. متاح في: https://goo.gl/DEXRva

ثانيا: المصادر الأجنبية:

1) Ajayi, E. F. G. (August 2016). Challenges to enforcement of cyber-crimes laws and policy.-Academic Journals; Journal of Internet and Information Systems. Vol. 6(1), PP. -12

2) Berman, Jerry & Mulligan, Deirdre (1998). Privacy in the Digital Age: Work in Progress. – Nova law review, vol.23. P549-582. January.

3) Hirsch, Dennis D. (2011). The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?.- Seattle University Law Review.- Vol.3. PP. 439-480.

4) Landesberg, Martha K. & Mazzarella, Laura. (July1999). Self-Regulation and Privacy Online: A Report to Congress.- U.S.A: Federal Trade Commission.

5) Lawrence, Gregory W. et al. (2000). Risk Management of Digital Information: A File Format Investigation.- Washington, D.C.: Council on Library and Information Resources

6) Mendel, Toby et al. (2012). Global survey on internet privacy and freedom of expression. – UNESCO: France. - UNESCO Series on Internet Freedom.

7) Micki, Krause. Handbook of Information Security Management.

8) Rhodes-Ousley, Mark (2013). Information Security: The Complete Reference.- Second Edition.- New york: McGraw-Hill.

9) Richard M., Marsh Jr. (2009). Legislation for Effective Self-Regulation: A New Approach to Protecting Personal Privacy on the Internet, Michigan Telecommunications and Technology Law Review, Volume15, Issue 2. PP. 542-563.

10) Strauss, Jared & Rogerson, Kenneth S. (2002). Policies for online privacy in the United States and the European Union.- Telematics and Informatics, vol. 19. PP. 173–192.

11) Westin, Alan F. (1967). Privacy and freedom. - New York: Atheneum.

12) Westin, Alan F. (2003). Social and Political Dimensions of Privacy.- Journal of Social Issues, Vol. 59, No. 2, pp. 431-453.

المواقع الالكترونية:

1) http://www.abc.net.au/technology/articles/2011/06/08/3238443.htm

2) arab-librarians.blogspot.com/2006/03/blog-post_02.html

3) http://ardroid.com/2011/11/03/what-is-qr-code /

4) http://journal.cybrarians.info/

5) http://privacyanddatasecurity.blogspot.com/

6) http://www.dralmarri.com/

7) http://www.hackingteam.it/

8) https://itunews.itu.int/Ar/

9) https://library.stanford.edu/

10) https://www.pcworld.idg.com.au/mediareleases/12655/avg-aunz-cautions-beware-of-malicious-qr-codes/

11) http://www.qrcode.com/en/history/

12) *https://static.googleusercontent.com/media/www.google.com/en//intl/en/policies/privacy/google_privacy_policy_en.pdf*

13) https://wikileaks.org/

14) https://www.cccure.org/

15) https://www.finfisher.com/

16) https://www.flickr.com/

17) secondlife.com

18) www.abahe.co.uk