سلسلة أوراق

الحق في المعرفة

خصوصية البيانات الرقمية

سارة الشريف

سلسلة أوراق الحق في المعرفة تصدر عن مركز دعم لتقنية المعلومات

مركز دعم لتقنية المعلومات

2 ش حسين المعمار متفرع من محمود بسيوني – ميدان طلعت حرب – وسط البلد – القاهرة

sitcegypt.org | info@sitcegypt.org | 02 257 56 417

خصوصية البيانات الرقمية

البيانات الرقمية، هي المعاملات التي تتم عن طريق الآلة، أو وسيط إلكتروني بداية من ماكينة الصراف الآلي، ووصولاً إلى جهاز الحاسب الآلي. ومع التطور التكنولوجي السريع صارت معظم معاملاتنا في الحياة اليومية تتم بشكل رقمي، فبطاقات الهوية (الرقم القومي) هي بيانات رقمية مسجلة لدى المؤسسات الحكومية، يتم من خلالها الاستدلال على هوياتنا الشخصية، فمثلاً حجز المطاعم عن طريق الإنترنت، أو الترتيب لسفر، أو حجز تذاكر الطيران، أو دفع الفواتير المنزلية، أو التسجيل في اللجان الانتخابية والتصويت الإلكتروني، هي في الأصل معاملات رقمية وإلكترونية تتم عن طريق كتابة مجموعة من بياناتنا الشخصية على صفحات أو تطبيقات تلك المواقع بطريقة تمكنها من الاستدلال علينا لتقديم الخدمة المطلوبة، لكن الأمر لا يتوقف عند هذا الحد، فالسؤال الذي يطرح نفسه باستمرار هو: إلى أين تذهب بياناتنا ومعلوماتنا الشخصية بعد كتآبتها وبعد تقديم الخدمة وانقضائها؟ فهل يمكن استخدامها فيما بعد بشكل قد يسبب لنا ضرراً ما؟ أو هل تحتفظ المواقع والتطبيقات ببياناتنا الشخصية؟ وإذا كان الأمر كذلك، فأين تذهب تلك البيانات وكيف يتم استخدامها فيما بعد؟ أيضاً، هل الخطوات التي نتبعها عند إدخال البيانات الشخصية تكون مؤمنة بشكل كافٍ يضمن عدم تعرضها للسرقة وبالتالي تعرضنا للنصب والاحتيال؟ وما هو الإطار القانوني الذي يؤمن الخصوصية لبيانتنا الرقمية ويحميها في مصر؟.

تحاول هذه الورقة الإجابة على الأسئلة السآبقة، فتبدأ باستعراض بعض المفاهيم الخاصة للآليات الشائع استخدامها في عملية جمع البيانات الرقمية، ثم تتناول بعض الطرق الفعالة لحماية خصوصية الأفراد المستخدمين للشبكة العنكبوتية، مع عرض أمثلة لسياسة الخصوصية المتبعة في بعض المواقع والتطبيقات، وكذلك بعض النماذج الدولية في هذا المجال.

خصوصية البيانات الرقمية

آلية جمع البيانات الرقمية

تبدأ عملية تجميع البيانات الخاصة بالمستخدم عند اللحظة التي يقوم بتصفح أحد المواقع الالكترونية بواسطة بعض العناصر التي تحتوي عليها صفحة الإنترنت مثل **بروتوكول الإنترنت**[1] (Internet Protocol) أو ما يعرف اختصارا بإسم (IP address)، وهو بروتوكول أو مرسوم بكيفية تبادل المعلومات بين طرفين على شبكة الإنترنت بحيث لا يتشآبه أي عنوان للبروتوكول مع غيره على الإطلاق، فيما يشبه بصمة اليد ولكن بشكل رقمي، وعن طريق تتبع عنوان البروتوكول يتم الوصول إلى البيانات الشخصية للمستخدمين والتعرف أيضاً على موقع الجهاز الذي يقوم بعملية التصفح على الإنترنت، فمثلاً إذا كان عنوان (IP) للمستخدم (001.002.003.004) فإن رقم (001) يشير إلى بلد الجهاز المستخدم، ورقم (002) يشير إلى الجهة المنظمة للإنترنت داخل البلد، و(003) إلى شركة الإنترنت المشترك معها المستخدم، و(004) إلى رقم المشترك لدى شركة الإنترنت، وبالتالي عند إرسال مجموعة من البيانات أو استقبالها على شبكة الإنترنت يتم تقسيم تلك الرسالة إلى مجموعة من القطع الصغيرة والتي تعرف بإسم "حزم"، يحتوي كل منها على عنوان المرسل والمستقبل.

عنصر أخر يتم عن طريقه جمع البيانات الرقمية للمستخدمين على شبكة الإنترنت وهو "**ملفات تعريف الارتباط**" أو **الكوكيز (cookies)**، ويقصد به الملفات النصية الصغيرة التي ترسلها شبكات الاتصال الخاصة بالمواقع الذي نقوم بزيارتها وتسمح للموقع بالتعرف على بياناتنا وبيانات الجهاز الرقمية، وعادة ما يتم ضبط تلك الملفات ضبطاً تلقائياً بحيث تقوم بجمع تلك البيانات دون الحصول على موافقة المستخدم، وبرغم أن تلك الملفات هي التي تسمح لنفس الموقع بالتعرف عليك في الزيارة التالية له، حيث يقوم بتسجيل اسم الدخول أو تفضيلاتك لتسهيل عملية إعادة التسجيل، إلا أنه من ناحية أخرى، فإن الاحتفاظ بتلك المعلومات والبيانات قد تعرض الحسآبات للسرقة وتمثل انتهاكا للخصوصية في حالة ما إذا كان المستخدم لا يرغب في احتفاظ الموقع ببياناته الرقمية ولو بشكل مؤقت، ولتفادى تلك المشكلة قامت بعض الشركات بتطوير مواقعها الالكترونية بحيث تسمح للمستخدمين بالموافقة أو الرفض على احتفاظ الموقع ببياناتهم أو تخزين ملفات الكوكيز على الجهاز المستخدم. ولملفات الكوكيز نوعان: الأول "**ملفات مؤقتة**" وهي التي يتم تخزينها بشكل مؤقت بذاكرة الجهاز، ويتم التخلص منها بعد إغلاق الصفحة، والغرض منها هو التعرف على المستخدم عند انتقاله من صفحة إلى أخرى. والثاني "**ملفات دائمة**" وهي التي تُحفظ بشكل دائم على الجهاز المستخدم أثناء التصفح، وللتخلص منها يجب أن يقوم المستخدم بإزالتها بنفسه.

ثالث تلك العناصر التي تحتويها صفحة الإنترنت وتعمل على جمع المعلومات بشكل تلقائي، هي ما يعرف بإسم "الويب باجز"[2] (Web Bugs)، وهي عناصر غير مرئية تتضمنها صفحات البريد الإلكتروني والمواقع الإلكترونية. وتعمل على إرسال المعلومات الخاصة بحركة المستخدم على الموقع الإلكتروني كَنَسخ أو تحميل الصفحات، كما تُمكن من التعرف على توقيت إطّلاع المستخدم على بريده الإلكتروني، وما إذا كان قد قام بإرسال البريد لآخرين. أيضاً يتم استخدام تلك العناصر في تحليل صفحات الإنترنت، وقد تتواجد في ملفات الصور وتحمل أسماء متعددة تختلف طبقاً لمكان وجودها، وهي عادةً عناصر غير ضارة ولا تعد من الفيروسات؛ إلا أن خطورتها تكمن في نوع المعلومات التي تقوم بجمعها، ويمكن توفير بعض الحماية للبيانات الشخصية من تطفل عناصر (Web Bugs) عن طريق إغلاق ملفات الكوكيز من متصفح الإنترنت.

---

[1] INTERNET PROTOCOL http://tools.ietf.org/html/rfc760

[2] Nearly undetectable tracking device raises concern http://news.cnet.com/2100-1017-243077.html

خصوصية البيانات الرقمية

حماية البيانات الرقمية

عن طريق الأدوات الثلاث السآبقة يتم جمع عدد ضخم من بيانات المستخدمين وزائري المواقع الالكترونية ، والتي يمكن من خلال تحليلها وترتيبها توقع نمط المستخدم وتفاعله مع الإنترنت بحيث تمثل تلك المعلومات مكسباً اقتصادياً كبيراً لشركات الإعلان والتسويق. ولتلافي تسرب البيانات الشخصية عبر شبكة الإنترنت على غير رغبة المستخدم أو دون معرفته لتأثيراتها عن طريق العناصر الثلاث السآبقة، تقوم عادة المواقع الالكترونية عند التسجيل عليها بوضع نوعين من السياسات على موقعها: **سياسة للخصوصية** (Privacy Policy)، **وسياسة الاستخدام** (Usage Policy).

تشرح **سياسة الخصوصية** ماهية المعلومات الشخصية التي يتم جمعها وكيفية استخدام الموقع للبيانات المجمعة، ويتم توضيح كل أو بعض الطرق التي يتم بها جمع وتخزين بيانات المستخدم، أو حفظها بسرية ، أو استخدمها، أو الإفصاح عنها والتحكم بها، أو تداولها مع طرف ثالث. وتسمح بعض المواقع للمستخدمين بإمكانية تعزيز سياسة الخصوصية الخاصة بهم أو إمكانية عدم الموافقة على بعض بنودها، بينما تقوم **سياسة الاستخدام** بإعلام المستخدم عن قواعد استخدم الموقع وما هو مسموح به، وما تعتبره إدارة الموقع انتهاكاً يُلزم وقف حسآب المستخدم أو إلغائه.

من خلال هاتين الاتفاقيتان تتمكن التطبيقات والمواقع من استخدام بيانات الزوار الشخصية والاستفادة بها بشكل يبدو وكأن المستخدم يقوم بالدفع مقآبل الخدمة التي يحصل عليها عن طريق الإنترنت من بياناته الشخصية، فقد يُفاجئ مثلاً بإن الصور التي قام بتصويرها ونشرها على حسآبه قد تم استخدامها، ونشرها، وبيعها بواسطة الشركة المقدمة للخدمة، دون أن يحصل على أي عائد أدبي أو مادي. الأمر ذاته يتم مع ملفات الكوكيز، حيث تخيّر بعض المواقع المستخدمين بين الموافقة أو الرفض على تخزين ملفات الكوكيز على أجهزتهم الخاصة، ولأن معظم المستخدمين لا يقضون فترة كافية في قراءة سياسيات الخصوصية واتفاقية المستخدم لأسبآب بعضها يعود إلى المستخدم نفسه، وبعضها الأخر إلى الطريقة التي تتم بها كتآبة سياسات الخصوصية بشكل معقد وقانوني وغير سلس أو يتم تصميمها بشكل غير جذآب أو ملفت.

وتمثل البيانات الشخصية المتدفقة عبر الإنترنت للشركات عائد اقتصادي كبير، ومتراكم. إذ يمكن استخدامها في تطوير العديد من خطط الدعاية والتسويق التي تتبناها الشركات، فالتطور الكبير في أدوات جمع المعلومات وتحليلها، مكن الشركات من جمع المعلومات الخاصة بنمط حياة المستخدمين عن طريق تتبع نمط سلوكهم الاستهلاكي أو المواقع الإلكترونية المفضلة لديهم، ليتم بعدها بناء قواعد بيانات عريضة للمستخدمين وربطها باهتماماتهم وبتفصيلاتهم، ومن ثم تلعب هذه البيانات دوراً اقتصادياً كبيراً في عمليات التسويق والإعلانات، واختيار جمهور مستهدف بالدعاية، ومعرفة النمط الاستهلاكي لكل فرد، وتصنيف المستخدمين حسب شرائحهم العمرية أو الاجتماعية أو الاقتصادية. الأمر الذي يمكن استغلاله في عمليات بيع قواعد البيانات المصنفة تلك إلى شركات أخرى لتحقيق عائد مادي. وفي تقرير لمركز معلومات الخصوصية[3] (EPIC) فإن "القائمون على جمع معلومات المستخدمين يعتزمون تصنيف أية معلومة وجمعها إليكترونيا" فمثلا شركة Medical Marketing Service تقوم ببيع قوائم الأفراد الذين يعانون من عدة أمراض وتكون مرتبطة بإشارات مرجعية مع المعلومات المتعلقة بالعمر والمستوى التعليمي وحجم الأسرة ونوع الجنس والدخل وأسلوب الحياة والوضع الاجتماعي ووجود أو عدم وجود أطفال لدى المرضى، وتشمل قائمة الأمراض مرض السكري وسرطان الثدي وأمراض القلب، بينما

[3] ورد التصريح في دراسة استقصائية عالمية حول خصوصية الإنترنت وحرية التعبير، صادرة عن اليونسكو متاحة على الرابط التالي
http://unesdoc.unesco.org/images/0021/002182/218273a.pdf

تبيع شركات أخرى قواعد بيانات تحتوى على معلومات تتعلق بعادات حياة الأفراد وكتبهم المفضلة وصولاً لمعتقداتهم الدينية[4].

وفي حالة عدم رغبة المستخدم في تبادل بياناته الشخصية أو جمعها أو بيعها لشركات تسويق أو إعلانات بمبالغ ضخمة فإن هذه العمليات تمثل انتهاكاً لخصوصية بياناته الشخصية. خطورة أخرى يمكن أن تتعرض لها البيانات الشخصية للمستخدمين أثناء عملية تبادل المعلومات وجمعها وهي عدم تأمين مسارات نقل تلك البيانات بشكل كافي، مما يعرضها للسرقة، بشكل يهدد الأمان الاجتماعي والمالي لأصحآب المعلومات، ويعرضهم للخطر عن طريق الوصول لأرقام حسآباتهم الائتمانية أو كلمات المرور التي قد تحتفظ بها المواقع لمدد غير محددة.

أمثلة لسياسة الخصوصية في بعض المواقع والتطبيقات

تنص سياسة الخصوصية في العديد من المواقع والتطبيقات على بعض الشروط التي تمثل انتهاكا لخصوصية المستخدم، والتي قد لا يلتفت إليها عند إنشائه حسآب على الموقع أو تحميله لتطبيقات بعض تلك المواقع. وقد استجآبت بعض الشركات المنتجة للتطبيقات لمطالبات المستخدمين التي أثيرت حول مستويات الخصوصية التي توفرها، وعملت على تحسين شروط خصوصيتها، ورهن نشر ومشاركة بيانات المستخدم مع آخرين بموافقته أو رفضه. موقع وتطبيق لمشاركة الصور والفيديوهات القصيرة على الإنترنت **إنستجرام** [5] (Instegram) على سبيل المثال، ، كانت سياسة خصوصية الموقع والتطبيق تنص على حق الموقع في استعمال أو حذف أو تعديل أو عرض صور المستخدمين بشكل علني، إلا أنه وبعد تذمر العديد من المستخدمين قامت الشركة بالاعتذار عن هذا الشرط وحذفه حسب تصريحات للمدير التنفيذي للشركة[6].

تويتبيك (Twitpic) أيضاً، وهو موقع لمشاركة الصور عبر موقع التدونيات القصيرة "تويتر"، تنص سياسة خصوصيته على حقه في استخدام الصور [7]وبيعها إلى طرف ثالث، وفي عام 2011، قام بتوقيع عقد شراكة مع إحدى شبكات الأخبار المتخصصة في تغطية أخبار المشاهير لتتمكن من استخدام الصور الموجودة على الموقع، بينما ينص موقع **تويتر**(Twitter) في سياسة خصوصيته على حقه في الاحتفاظ بصور المستخدم المحذوفة لمدة 5 أسآبيع على الأكثر. أيضاً، برنامج المحادثة الشهير **سكايب** (Skype) نص في صفحة السؤال والجوآب الخاصة به على أحقية المستخدم في إلغاء حسآبه من على الموقع أو التطبيق، ولكن هذا لا يمنع الشركة من الاحتفاظ بنسخة من بياناته الشخصية المحذوفة. الأمر ذاته يتكرر في موقع التدوين **وورد برس** (WordPress). أما موقع التواصل الاجتماعى **الفيسبوك** (Facebook) فقد تعرض للعديد من الانتقادات بسبب سياسات خصوصيته التي تسمح بانتهاك خصوصية البيانات الشخصية لمستخدميه واستغلالها في الترويج للإعلانات، عن طريق بيعها لشركات إعلان، تقوم باستهداف المستخدمين طبقاً لبياناتهم الشخصية المختلفة. كذلك عند التسجيل لدى موقع وتطبيق **ياهو** (yahoo) فإن سياسة خصوصيته تنص على حقه في تغيير سياسة

[4] Hearing on Data Mining: Current Applications and Future Possibilities
http://epic.org/privacy/profiling/datamining3.25.03.html
[5] Instagram responds to outrage, tweaks privacy policy to limit photo use in ads
http://www.nbcnews.com/technology/instagram-responds-outrage-tweaks-privacy-policy-limit-photo-use-ads-1C7660196
[6] Thank you, and we're listening http://blog.instagram.com/post/38252135408/thank-you-and-were-listening
[7] Terms & Conditions: Twitpic holds your photos hostage http://www.digitaltrends.com/social-media/terms-conditions-avoid-twitpic/

الخصوصية دون إعلام مسبق للمشتركين. وكذلك تطبيق **الواتس آب** [8](whatsapp) الذي تعرض للعديد من الانتقادات خاصة بعد أن قامت عدد من المنظمات المهتمة بحماية البيانات والخصوصية بالكشف في تقرير يفيد بقيامه بالنفاذ إلى كل الأرقام المسجلة على هاتف المستخدم دون سؤاله.

ولعل صفقة شراء الفيسبوك لتطبيق الواتس آب يطرح العديد من التساؤلات حول خصوصية بيانات مستخدمي الواتس آب الرقمية استناداً على تاريخ الفيسبوك مع سياسات الخصوصية الرخوة، والمتلاعب بها، والقلق بعد أن أصبح مستخدمو الواتس آب على وشك أن يتحولوا إلى أحد منتجات الفيسبوك أرادوا ذلك أو لم يريدوا[9]، ورغم تأكيدات كل من الشركتين على أن هذه الصفقة لن تغير شيئا من سياسة الخصوصية التي يتبعها الواتس آب وأنه سيعمل بشكل مستقل عن الفيسبوك وسيبقى خالياً من الإعلانات كما اعتاد مستخدموه، حيث تبنى الواتس آب منذ نشأته سياسة متشددة تجاه الإعلانات، إلا أن التساؤل حول إلى أي مدى سيصمد تطبيق الواتس آب أمام آلة الدعاية التي أصبح عليها الفيسبوك، فهل يدرك 450 مليون مستخدم لتطبيق الواتس آب، والمرشحين للزيادة بشكل يومي بمقدار مليون مستخدم أنهم على وشك مشاركة محادثتهم مع الفيسبوك عبر الإنترنت، فحتى وإن لم يهتم البعض بهذه الإشكالية، فبالنسبة للمستخدم الذي يلجأ لاستخدام الواتس آب لعدم رغبته في معرفة الآخرين لكل شيء عنه سيمثل هذا الأمر إزعاجاً له.

فتطبيق الواتس آب الذى يمكن تحميله بشكل مجاني من معظم متاجر الإنترنت لكن الخدمة نفسها غير مجانية، فمن أجل أن يبقى خاليا من الإعلانات يقوم بتحصيل 99 سنت في العام بعد السنة المجانية الأولى، أما الآن وبعد أن أصبحت الخدمة تنتمي للفيسبوك فإن المستخدمين لن يقوموا فقط بدفع مقابلها من أموالهم ولكن من معلوماتهم الشخصية أيضا، فالفيسبوك الآن يمكنه النفاذ إلى كل بيانات مستخدمي الواتس آب (كأرقام الهاتف، العناوين، معلومات الدفع) وهى البيانات التي لم يكن لديه القدرة على الوصول إليها ما لم يقم المستخدمين أنفسهم بربطها بحساباتهم على الفيسبوك.

خبرات دولية وأممية في حماية الخصوصية الرقمية

استدعت الحاجة، والتطور التكنولوجي، ودخول الحوسبة والإنترنت في معظم مجالات الحياة إلى إقرار مجموعة من التوجيهات والقوانين والتشريعات التي تخص حماية البيانات الرقمية للمستخدمين حتى بالنسبة للدول التي لا تنص دساتيرها بشكل مباشر على الالتزام بحماية الخصوصية بشكل عام لما له من تبعات وتأثيرات على الجانب الاقتصادي للدول، ففي عام 1995 قام الاتحاد الأوروبي بإصدار "التوجيه الأوروبي لحماية البيانات"[10] وعَرف هذا التوجيه البيانات الشخصية على "إنها أي معلومات خاصة بشخص طبيعي غير محدد أو لا يمكن تحديده"، ويستهدف التوجيه شركات الاتصالات العمومية والدولية بحيث ينص على فرض التزامات خاصة بحماية البيانات على الشركات المتحكمة فيها، وأن يتم النفاذ إلى البيانات الشخصية بتفويض شخصي للأغراض المصرح بها قانوناً، وبناءً على هذا التوجيه، قامت العديد من المنظمات التي تعمل مع الاتحاد الأوروبي بشكل تجارى بصياغة

[8] Dutch and Canadian DPAs challenge WhatsApp's compliance with their privacy laws http://www.privacylaws.com/Publications/enews/International-E-news/Dates/2013/1/Dutch-and-Canadian-DPAs-challenge-WhatsApp/

[9] Why Facebook's WhatsApp Deal Is Bad For Users http://readwrite.com/2014/02/20/facebook-whatsapp-acquisition-users

[10] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

سياسات تتماشى مع هذا التوجيه. وفي نفس العام قامت لجنة التجارة الفيدرالية الأمريكية (Federal Trade Commission) بنشر "مبادئ المعلومات العادلة"، وهي وثيقة غير إلزامية، ويجري العمل بها باعتبارها دليل أو توجيه للقلق المتنامي حول صياغة سياسات الخصوصية .

خريطة للأماكن التي تسري فيها قوانين حماية البيانات أو تلك التي تكون فيها هذه الحماية في الطور التشريعي

جدول يوضح الدول والأطر الإقليمية التي تسري فيها قوانين حماية البيانات الرقمية

الدولة	القانون
الولايات المتحدة	FCRA, GLB, CAN-SPAM, DO-NOT-CALL and State Harbor principles Privacy Protection Act of 2003 قانون حماية الخصوصية لعام 2003
كندا	PIPEOA and provincial privacy laws قوانين الخصوصية الخاصة بالمقاطعات
الأرجنتين	Personal Data Protection Law, Confidentiality Of Information Law قانون حماية البيانات الشخصية قانون المعلومات السرية
شيلي	Law For The Protection Of Private Life قانون حماية الحياة الخاصة
الاتحاد الأوروبي **المنطقة الاقتصادية الأوروبية**	Data Protection Directive And Privacy And Electronic Communications Directive as Implemented by 27 different member state data protection laws التوجيه الخاص بحماية البيانات والخصوصية والاتصالات الإلكترونية

جنوب أفريقيا	Electronic Communications And Transactions Act قانون الاتصالات والمعاملات الإلكترونية
سويسرا	Federal Act On Data Protection القانون الفيدرالي لحماية البيانات
روسيا	Federal law of July 27 2006 on personal data القانون الفيدرالي للبيانات الشخصية الصادر في 27 يوليو لعام 2006
دبي– المركز المالي الدولي	Data Protection Law 2007 قانون حماية البيانات لعام 2007
كوريا الجنوبية	Act on Promotion of Information and Communications Network Utilization and Data Protection قانون تعزيز المعلومات واستخدام شبكات الاتصالات وحماية البيانات
اليابان	Personal Information Protection Act (PIPA) قانون حماية البيانات الشخصية
تايوان	Computer Processed Data Protection Law قانون حماية البيانات الإلكترونية
هونج كونج	Personal Data Privacy Ordinance قانون خصوصية البيانات الشخصية
أستراليا	Amended Privacy Act, Spam Act القانون المعدل للخصوصية والبريد المزعج "السخام"
نيوزلندا	Privacy Act قانون الخصوصية

تعد **فرنسا** واحدة من الدول التي تمتلك تاريخ طويل في تطبيق سياسات الخصوصية وحماية البيانات الرقمية. ففي عام 1995، أقرت المحكمة الدستورية الفرنسية الحق في الخصوصية معترف به ضمنياً بدستورها، وتلتزم فرنسا بتطبيق قوانين الاتحاد الأوروبي الخاصة بحماية البيانات والاحتفاظ بها، حيث قامت بتأسيس "اللجنة الوطنية للمعلومات والحريات"[11] (CNIL)كهيئة إدارية رقابية مستقلة تعمل على إعلام ونصح وتعليم المستخدمين بحقهم التشريعي في حماية بياناتهم الرقمية، كما تتيح سهولة التواصل معها لكل مستخدم وجد صعوبة في ممارسة حقه في حماية بياناته الشخصية، كما تقوم بفحص وتوقيع العقوبات – بحكم القانون– على الأنظمة التكنولوجية التي لا توفر ضمانات كفاية، أو لا تعمل على حماية بيانات المستخدمين الرقمية. أيضاً، ينص قانون "تكنولوجيا المعلومات وملفات البيانات والحريات المدنية"[12] الفرنسي في بعض مواده على ضرورة إلتزام شركات الاتصالات مقدمة خدمات الإنترنت بحفظ بيانات حركة المرور بين المواقع للمستخدمين لعام واحد فقط، كما أقر مجلس الوزراء الفرنسي في 2011، قراراً بحق مستخدمي خدمات الاتصالات في معرفة الغرض من أي ملف لتعريف

[11] Constitution and Composition http://www.cnil.fr/english/the-cnil/constitution-and-composition/

[12] قانون رقم 78-17 بتاريخ 6 يناير 1978 والذى تم تعديله والإضافة عليه بموجب القوانين فى 2004 و2209 و2011 AMENDED BY THE FOLLOWING LAWS:ACT OF 6 AUGUST 2004 RELATIVE TO THE PROTECTION OF INDIVIDUALS WITH REGARD TO THEPROCESSING OF PERSONAL DATAACT OF 13 MAY 2009 RELATIVE TO THE SIMPLIFICATION AND CLARIFICATION OF LAW AND LIGHTER PROCEDURES
http://www.cnil.fr/fileadmin/documents/en/Act78-17VA.pdf

الارتباط cookies، والوسائل المتاحة بحيث يعطى موافقة صريحة على قبول إضافتها لصفحة الموقع والتعرف على بياناته، ويحمى قانون "سرية المراسلات المرسلة من خلال الاتصالات الالكترونية" خصوصية بيانات المستخدمين وحمايتها من الاعتراض أو الحجب أو الفحص أو الحذف إلا بموجب قرار من رئيس الوزراء.

في عام 1998 قامت **إنجلترا**، بتوحيد واستبدال قوانين حماية البيانات كقانون "حماية البيانات" الصادر في 1984 وقانون "الوصول إلى الملفات الشخصية" 1987 سعياً إلي تنفيذ "توجيه حماية البيانات الأوروبية" خاصة فيما يتعلق بالبيانات الإلكترونية والاتصالات والتسويق، حيث جاء قانون "تنظيم الخصوصية والاتصالات الإلكترونية " عام 2003 ليغير من أساس الموافقة على شروط التسويق الإلكتروني، ليصبح من حق المستخدم الموافقة أو الإنسحاب من تلقي عروض التسويق وقتما يشاء.

بينما في **الهند** التي لا يحتوى دستورها على نص صريح للخصوصية، فقد شَرّعَت العديد من القوانين التي تحمي خصوصية البيانات الرقمية، ففي عام 2000، أصدرت قانون "تكنولوجيا المعلومات" [13]الذي أقر بدفع تعويضات وتوقيع عقوبة جنائية في حالة الكشف غير المشروع عن البيانات أو إساءة استخدامها.

وبالنسبة **لمصر** فرغم أن الدساتير المصرية المتعاقبة تنص على حق الخصوصية وحق حمايتها واحترام حرمتها، فإنه لا يوجد في القانون المصري ما ينص على حماية الخصوصية الرقمية للمستخدمين على الإنترنت الأمر الذي يمثل فراغ يسمح بحدوث العديد من الانتهاكات لبيانات المستخدمين الرقمية في غياب رقابة تشريعية أو قوانين تحمى خصوصية المستخدمين، ومثال على ذلك فإن عدد قليل جداً من المواقع الإلكترونية للوزارات المصرية هي التي تلتزم بنشر بيان لسياسة الخصوصية بخصوص البيانات الرقمية المجمعة للزائر عبر زيارته للموقع عن طريق بروتوكول الإنترنت وملفات الارتباط مثل: وزارة الثقافة [14]و وزارة الكهرباء[15] بينما لا تلتزم معظم الوزارات بكتابة أو نشر بيان للخصوصية، ومنها موقع وزارة المالية المصرية[16] ، لذلك تظهر هنا الحاجة الملحة لوجود تشريع قانوني يضبط أداء المواقع الالكترونية وطريقة جمعها للبيانات الرقمية للمستخدمين وكيفية استخدامها ومدة الاحتفاظ بحركة الزوار بين المواقع المختلفة بالإضافة إلى خلق وعى مجتمعي تجاه خطورة تدفق البيانات الشخصية للمستخدمين دون تأمينها مما يعرض سلامتهم الشخصية وأمنهم الاجتماعي والمالي للخطر، وضمان حماية المستخدمين من التعرض لإساءة استخدام أو تعرض بياناتهم التي تجمعها الهيئات العاملة داخل مصر للسرقة، والتي تبدأ من سرقة الهوية وكلمات المرور وأرقام البطاقات الائتمانية على الإنترنت، عبر ضمان توفير إلزام قانوني لتلك الهيئات بحماية بيانات المستخدمين.

[13] India's new Data Protection Legislation http://www2.law.ed.ac.uk/ahrc/script-ed/vol8-2/ananthapur.asp

[14] سياسة الخصوصية http://www.moc.gov.eg/index.php?option=com_content&view=article&id=321&Itemid=367&lang=ar

[15] سياسة الخصوصية http://www.moee.gov.eg/test_new/policy.aspx

[16] وزارة المالية http://www.mof.gov.eg/Arabic/Pages/Home.aspx