حماية البيانات الشخصية والحق في الخصوصية

د. منى الاشقر جبور

تمهيد

" اذا لم يكن لديك شيء تخفيه، فليس لديك شيء تخافه"، شعار استخدمته الحكومة البريطانية، في سياق تبرير، زرعها كاميرات الرقابة،في المدن والقرى، فهل هذه المقولة صحيحة؟

تكون هذه المقولة صحيحة، فيما لو كان لدينا استعداد، لكشف ميولنا، ورغباتنا، ومحيطنا العائلي، واسماء اصدقائنا، ومحتوى مخابراتنا، واماكن تواجدنا، ونوعية مشترياتنا، وقيمة رصيدنا المالي، ومدخراتنا، وموقع منزلنا، ومحتويات غرف نومنا، لأي كان، وفي كل الاحوال والاوقات.

وقبل الموافقة على هذه المقولة، لا بد من تحديد ردة فعل أي شخص، ليس لديه شيء يخفيه، على غريب يقترب منه في الشارع، ويسأله عن رقم هاتفه، أو عنوان بيته، أو عن مقاس ثيابه، أو وزنه، أو حتى نوع سيارته.

وماذا لو سئل هذا الشخص، عن اسمه، واسم عائلته، ووالديه؟

أو ماذا لو سئل، عن الامكنة التي زارها خلال اليوم، أونوع الحساسية الذي يعاني منها، أو عن سوابقه المرضية، وحالته العصبية، وفئة دمه، وانتمائه السياسي، ومعتقداته الدينية؟

بعيدا عن القانون، ومن منظور اجتماعي بحت، يعتبر هذا النوع من الاسئلة، من الامور الممجوجة، وغير المقبولة، واعتداء فاضح على الخصوصية، في المجتمعات الغربية، كما في المجتمعات الشرقية، على حد سواء، والا لما نعت الناس السائلين بالفضول السلبي، وقلة الذوق، وغيرها من التعابير التي تطلق على من يقوم بهذه التصرفات. ولما ذهبت بعض ردات الفعل، الى التساؤل، عما اذا كان طارح الاسئلة، يعمل تحريا.

اذا كان صحيحا، ان من لا يخفي شيئا، لا يخشى من انفضاح اي تفصيل خاص، فالصحيح أيضا، أن لكل شخص حياته الخاصة، التي لا يريد عرض تفاصيلها أمام العالم، كما لا يريد لهذا العالم، ان يتدخل في شؤونه. والصحيح أيضا، أنه وبالرغم من انتماء الفرد الى مجتمع، فان للفرد حياة خاصة، وشخصية مميزة. ولذا، لحظت حرمة لمحيط الشخص، حيث تنتشر دلائل خصوصيته، كالبيت والمراسلات، ووضعت قواعد حماية، لا يجوز اختراقها، الا بموجب نص قانوني، وفي حال اعتداء هذا الشخص، على حقوق الآخرين، ومخالفته للقوانين المحددة، والمرعية الاجراء.

والصحيح أكثر، أن هذه المقولة، نوع من محاولة القضاء على الحق في الخصوصية، من خلال الايحاء، بان من يخشى على حماية بياناته الشخصية، لا بد وانه يخفي أمرا مخالفا للقانون، أو أمرا سيئا.

فما هي البيانات الشخصية ؟ وما هو الحق في الخصوصية ؟ وكيف يمكن الاعتداء على هذا الحق في غياب حماية البيانات الشخصية؟ وما هي الصلة بين حماية البيانات الشخصية، والحق في الخصوصية، والامن السيبراني؟ وما هو الاطار القانوني الذي يتم التعامل على أساسه، مع المخاطر التي يتعرض لها هذا الحق؟

هذا ما سنحاول الاجابة عليه، من خلال دراستنا هذه.

البيانات الشخصية أو البيانات ذات الطابع الشخصي

ان التعريف أو التحديد، أمر أساسي في الامن القانوني، الذي يستند فيما يستند، الى وضوح المفاهيم، وحدود التطبيق ومجالاته، لأي قاعدة قانونية. من هنا، لا بد من التوقف، وكما فعلت جميع النصوص التي أقرت، حول العالم، عند تعريف البيانات الشخصية.

فقد عرفت القواعد الارشادية، التي وضعتها منظمة التعاون الاقتصادي والتنمية، البيانات الشخصية، بانها "... كل معلومة عائدة لشخص طبيعي محدد او قابل للتحديد"[1]. وعليه، فهي تلك البيانات، التي تنقل معلومات، يمكن ربطها بشخص معين، لتحديد هويته.

الا ان هذا التعريف، يثير بعض الاشكالات، اذ استثنى بيانات، يمكنها هي الأخرى، ان تساعد على تحديد هوية الشخص، او تعقبه وملاحقته، عبر سماحها بتحديد هذه الهوية، بشكل غير مباشر، وان لم تكن مرتبطة بهويته الشخصية. وترد في هذا السياق، البيانات، التي لا تعود الى الشخص الطبيعي، وانما الى وسيلة يستعملها: كرقم تسجيل السيارة، ورقم الهاتف الثابت والنقال، أو المعلومة المرتبطة، بأي وسيلة أخرى يحملها معه. ويسمح هذا الاستثناء، بالتعدي على خصوصية الاشخاص، دون رادع، نظرا لعدم امكانية تطبيق النص، الذي يستبعدها، بطريقة غير مباشرة.

ونشير في هذا المجال، الى التشريع الفرنسي الذي صدر في العام 1978 ، وقد نص على حماية المعلومات الاسمية، حاصرا بذلك، نطاق تطبيقه بشكل دقيق، في كل معلومة تشير الى هوية الشخص، من دون اي التباس. الا ان هذا القانون، جرى تعديله في العام 2004[2] ، ليصبح نطاق تطبيقه أكثر اتساعا، بحيث اعتمدت عبارة "المعلومات ذات الطابع الشخصي، " بما يمهد لحماية بيانات غير اسمية[3]، فاتحا بذلك المجال امام حماية أوسع، ولكن أمام التباسات أكبر.

وبالفعل، فقد اعترضت لجنة المعلوماتية والحريات في فرنسا، على الاجتهاد[4]، الذي اعتبر في قرارين متتاليين، صادرين عن محكمة الاستئناف في باريس، ان العنوان الخاص برقم التعريف الالكتروني للجهاز IP[5] ، ليس من البيانات الشخصية، كونه يسمح بتحديد هوية جهاز، لا هوية الشخص الذي يستعمل الجهاز. وفي هذا، بحسب رأي اللجنة، خطر يفتح الباب للتعديات على الخصوصية، من خلال جمع هذه البيانات، من دون الحصول على ترخيص مسبق بذلك، كما هو مقرر لجمع البيانات الشخصية.

وكان مشروع القانون، الذي اعدته وزارة الاقتصاد والتجارة [6] اللبنانية، قد استخدم مصطلح " البيانات ذات الطابع الشخصي، لدى تعريف البيانات الشخصية، وجاء النص على الشكل التالي: "يقصد **بالبيانات ذات الطابع الشخصي**، جميع انواع المعلومات المتعلقة بشخص طبيعي، والتي تمكن من التعريف به، مباشرة أو غير مباشرة، بما في ذلك عن طريق مقارنة

---

[1] - lignes directives de l'OCDE . …"toute information relative a une personne physique identifiee ou identifiable'.
[2] - loi 801 intitulee « loi pour la confiance dans l'économie numerique » du 21 juin 2004
[3] - la loi du 6 janvier 1978 "informatique et libertés" visait les informations nominatives. La loi du 6 août 2004 remplace le terme "information nominative" par celui de "donnée à caractère personnelle".

[4] - CA Paris, 27 Avril 2007 :" *"L'adresse IP ne permet pas d'identifier le ou les personnes, qui ont utilisé cet ordinateur puisque seule l'autorité légitime pour poursuivre l'enquête (police ou gendarmerie) peut obtenir du fournisseur l'accès d'identité de l'utilisateur."*. Et CA Paris, 15 Mai 2007 : » *"Que cette série de chiffre en effet ne constitue en rien une donnée indirectement nominative relative à la personne dans la mesure où elle ne se rapporte qu'à une machine, et non à l'individu qui utilise l'ordinateur pour se livrer à la contrefaçon"*.
[5] - L'adresse IP est le numéro qui permet d'identifier chaque ordinateur sur le réseau Internet. Elle se décompose dans version 4 en une série de 4 nombres allant de 0 à 255.
[6] ECOMLEB

المعلومات المتعددة المصادر او التقاطع بينها". ويبدو واضحا ان هذا التعريف، المأخوذ عن قانون 2004 الفرنسي، هو ذو نطاق تطبيقي واسع.

ويتناسب هذا التعريف، مع قانون كانت الغاية الاساسية منه، تعزيز الثقة في التجارة الالكترونية، كما يدل عليه عنوانه. فتوفير مساحة اكبر للحماية، يعني معدلا اعلى من الثقة. بالاضافة الى ذلك، يستجيب هذا التعريف، لحاجة مركزية: بناء الثقة والامان في الفضاء السيبراني، من جهة اولى، و مواكبة التطورات المتسارعة، في مجال تقنيات المعلومات، من جهة أخرى، حيث لم يعد ممكنا، توقع المدى الذي تبلغه قدرات تكنولوجيا معالجة المعلومات، ولا نتائج الجمع بين تقنيات مختلفة ومتنوعة، سواء على حرمة الحياة الشخصية، أوعلى أمن الدول، التي تجمع وتعالج وتتبادل، البيانات الشخصية.

البيانات الشخصية والحق في الخصوصية

يعتبر هذا الحق من الحقوق الشخصية، المحمية في اطار الحريات العامة. وهكذا، تنبع أهمية حماية البيانات الشخصية، من ارتباطها الأكيد، بالكشف عن خصوصية الشخص المعني بها، عبر اتاحتها، امكانية تحديد هويته، ونوعية نشاطه، وحركته، ومكان تواجده، واهتماماته، وحالته الاجتماعية والصحية، وميوله السياسية والجنسية والثقافية، ووضعه المالي والوظيفي، وغير ذلك مما يمكن ان يحدد هويته، أو طيفه.

ويبدو واضحا، من التعريفات العديدة، التي اعتمدت، في القوانين التي تنظم معالجة البيانات الشخصية، أو تبادلها، او نشرها، أن الهم الأساس من حمايتها، هو الحفاظ على حق الشخص في الخصوصية. ويعود الاهتمام بالمحافظة على الحق في الخصوصية، في مواجهة المعالجات الآلية، إلى بدايات استخدام تكنولوجيا المعلومات والاتصالات، وإنشاء قواعد البيانات الشخصية[7].

والخصوصية تعني، بشكل أساسي، المحافظة على السرية، ومنع التدخل، في ما يعتبر حميمية الشخص، وأسراره، عبر منع انتشار البيانات، أو المعلومات التي تكشفها، أو تعرضها للانكشاف. وعليه، هنالك اعتداء على الخصوصية، سواء تعلق الامر، بكشف سر دفين، وايصاله الى الآخرين، أم بمراقبة ورصد تحركات، لم يقترنا بكشف أسرار، أو بنشر معلومات حساسة. فالضرر واقع في الحالتين: اذ ينتج عن كشف المعلومات، في الحالة الاولى، وعن كون الشخص، وضع تحت المراقبة، في الحالة الثانية.

وتتمثل الجوانب القانونية، للاعتداء على الخصوصية، عبر استخدام البيانات الشخصية، بطريقة غير قانونية، في عدد من الجرائم، والاعمال غير القانونية، التي يمارسها الافراد، أو الجهات الحكومية، ومنها: انتحال هوية الشخص، وانتحال الصفة، والابتزاز، واختراق انظمة المعلومات، والوصول الى الاسرار المهنية والتجارية، اضافة الى الرصد غير المشروع لحركة الاشخاص والاموال، من قبل الاجهزة الحكومية، وتكوين ملفات معلومات، دون سبب قانوني، والتمييز العنصري أو العقائدي أو الديني.

من هنا، يعتبر الاقرار بحماية البيانات الشخصية، اقرارا بحق المواطن أو الفرد، في الحفاظ على خصوصيته، من جهة أولى، كما يعني اقرارا بحق الدولة، في الاطلاع على هذه البيانات، ومعالجتها، ضمن أطر قانونية وتنظيمية محددة وواضحة، بما يسمح للسلطات المختصة، بمنع وقوع اعمال مخلة بالامن والنظام، او بملاحقة ومعاقبة مرتكبيها، من جهة ثانية.

---

[7]- النص الأساسي حول الخصوصية وحماية المعلومات هو: "guidelines on Protection of Privacy and Transborder Flowa of Personal Data"، في العام 1980. OECD.
European Directive on Data Prtotection (95/46/EC)
وفي نفس الاتجاه The Council of Europe's Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data. 1981.

ولذلك، برز اهتمام عام، بالحفاظ على البيانات الشخصية، كخطوة ضرورية للحفاظ على الحق في الخصوصية[8]، استدعت ومنذ بداية السبعينات، اتخاذ قرارين من قبل المجلس الاوروبي، حول حماية الحياة الخاصة للاشخاص الطبيعيين، من نتائج معالجتها في اطار انشاء قواعد بيانات، في القطاعين العام والخاص، وذلك في العامين 1973 و1974.

الامن القومي وحماية البيانات الشخصية

ان مسألة التعامل مع البيانات الشخصية، ليست مستجدة، وما الاهمية التي تعطى لها، في الوقت الحاضر، الا نتيجة الابعاد الجديدة غير المسبوقة، التي اكتسبتها مع توظيف طاقات تكنولوجيا المعلومات والاتصالات، سواء على مستوى المعالجة والنشر، أوعلى مستوى التدفق عبر الحدود، اضافة الى عدد الاشخاص المعنيين، وحجم المعلومات.

فالكميات الهائلة من البيانات الشخصية، التي تتدفق عبر الانترنت، وفي الفضاء السيبيري، تترافق مع تقنيات جد متطورة، ومنهجيات معالجة، يمكنها أن تشكل تهديدا مباشرا، ليس فقط للاشخاص الذين تساعد في كشف هوياتهم، وانما ايضا للدول، ولمصالحها الحيوية، وأمنها. ويتمثل هذا التهديد، في الاعتداءات التي يمكن ان تقع على الاشخاص، الطبيعيين والمعنويين، في القطاعين العام والخاص، وعلى البيانات والمعلومات؛ سواء من خلال سرقتها، أو تعديلها دون وجه حق، أو تشويهها، وفي الاعتداءات على انظمة المعلومات، ومنع عملها، وعلى الحريات والحقوق التي يتمتع بها الافراد، في المجتمعات الديمقراطية، كالحق في الخصوصية، والحق في التعبير.

وتصبح هذه التهديدات، أشد خطورة، ويتعاظم الخوف من الاعتداء على البيانات الشخصية، (بما يمثله من تعرض للحريات والحقوق الفردية)، عندما يتعلق الامربالتزام الدول، مكافحة بعض الأعمال والجرائم، ذات الارتدادات الكارثية: كالارهاب مثلا، حيث تستعمل البيانات الشخصية، بشكل منهجي، من قبل الحكومات المختلفة، سواء في انشطتها الوطنية الداخلية، او في علاقاتها مع الدول الاخرى، من خلال اتفاقيات[9]، أو من خلال أنظمة أمن، وبرامج متخصصة[10].

في هذا السياق، تثير حماية البيانات الشخصية، عددا من الاشكاليات، نتيجة التقائها أو تناقضها، مع عدد من الحقوق والحريات الاخرى، مثل: الحق في الوصول الى المعلومة، حق الدولة في الرقابة على القيود الخاصة بالمواطنين، وحقها في ضبط هذه القيود، وغيرها. وتبدو الحاجة ملحة، الى رسم حدود واضحة ،لا يمكن للدولة ان تتجاوزها، تحت شعار الحفاظ على الامن القومي، منعا للاعتداء على الحريات والحقوق. ولعل الحالة التي يمكن اثارتها هنا، هي التشريعات[11] التي وضعت في العديد من الدول، بعد اعتداءات الحادي عشر من أيلول، تحت عنوان مكافحة الارهاب. فقد جرى في الولايات المتحدة الاميركية مثلا، اقرار صلاحيات واسعة للحكومة، واعطيت هامشا اوسع للتحقيق والملاحقة، واستبعدت المسؤولية عن أشخاص القانون الخاص، في حال افشائهم معلومات للحكومة. وكان البرلمان الاوروبي، قد اعرب عن قلقه، ازاء الاثر الذي يمكن لاجراءات تستهدف الامن، ان تتركه على الحقوق والحريات، وفي مقدمها، الحق في الخصوصية[12].

---

[8]- مؤتمر استوكهولم 1967 – مؤتمر طهران 1968 باشراف الامم المتحدة.

[9] - les accords entre l'union européenne et les états unis.
* le traite de prum, signe le 27 Mai 2005

[10] - les systèmes d'échanges d'informations crées a l'échelle de l'Union Européenne : le système d'information Schengen (SIS), le système d'information douanier, et le système d'information d'Europol et celui d'Eurojust.

[11] - le Patriot act aux états unis.
- plan d'action contre le terrorisme adopte par le parlement européen et modifie le 25 Mars 2004 suite aux attentats de Madrid puis suite aux attentats de Londres du 7 juillet 2005
- recommandation relative a l'élaboration de « profiles terroristes » adoptée par le conseil européen en 2002
- directive du 15 Mars 2006 qui a prévu la conservation des données téléphoniques par les operateurs.

[12] - [12] - Résolution du 14 janvier 2009 sur la situation des droits fondamentaux dans l'Union européenne (2004-2008).
le Parlement européen « *se préoccupe du fait que la coopération internationale dans la lutte contre le terrorisme a souvent abouti à une baisse du niveau de protection des droits de l'Homme et des libertés fondamentales,*

تآكل الحق في الخصوصية وتهديد الحريات العامة

تحتل أخبار انتهاك الحق في الخصوصية، والحريات المدنية، وحرية التعبير على الانترنت، الصفحات الاولى، في وسائل الاعلام. فمن ويكيليكس[13] ، الى تامبورا[14] في بريطانيا، الى سنودين[15] وبريسم[16] في الولايات المتحدة الاميركية، الى برامج الاستخبارات في كندا[17] ، الى تشديد الرقابة على الانترنت في فنزويلا[18] ، وسورم 2، وسورم 3، والسجل الواحد في روسيا[19]، واتخاذ اجراءات تضمن تحديد هوية الاشخاص[20]، وحجب مواقع التواصل الاجتماعي، والجدار العظيم في الصين[21]، تأكيد على اهمية البيانات الشخصية، وضرورة حمايتها، لمنع استغلالها في الاساءة الى حقوق الافراد، وفي الوصول الى مستخدمي وسائل الاتصالات، دون وجه حق.

وكانت تصريحات سنودين، وكشف عمليات تجسس الولايات المتحدة الاميركية، على الديبلوماسيين، والسياسيين، والمواطنين، كما الاجانب، قد أثارت موجة من الاستياء، حول العالم، أدت فيما أدت ، الى قيام الرئيسة البرازيلية، بالدعوة لعقد قمة دولية حول مستقبل الانترنت، تناقش فيها، بشكل أساسي، حقوق الدول المختلفة في سياسة ادارة الانترنت، وحماية الحقوق، لاسيما الحق في الخصوصية، وحماية البيانات الشخصية[22].

---

notamment du droit fondamental au respect de la vie privée, à la protection des données à caractère personnel et à la non-discrimination

[13] - https://wikileaks.org/

[14] - **Tempora**, is a clandestine security electronic surveillance program tested in 2008,[2] established in 2011 and operated by the British Government Communications Headquarters (GCHQ). Tempora uses intercepts on the fibre-optic cables that make up the backbone of the internet to gain access to large amounts of internet users' personal data. http://en.wikipedia.org/wiki/Tempora

[15] - http://edition.cnn.com/2013/09/11/us/edward-snowden-fast-facts/

- En juin 2013, l'informaticien de la National Security Agency (NSA) américaine, Edward Snowden, révélait l'existence de programmes de surveillance. Le plus connu, nommé PRISM, permet au gouvernement américain d'accéder directement aux serveurs de neuf compagnies : Microsoft, Yahoo, Google, Facebook, PalTalk, YouTube, Skype, AOL, Apple. La NSA aurait ainsi, en mars 2013, récupéré 97 milliards d'informations. http://www.la-croix.com/Actualite/Monde/Pourquoi-il-faut-reformer-Internet-2014-04-23-1140281

[16] - special source operation system legally immunized private companies that cooperate voluntarily with U.S. intelligence collection.

[17] - Attention fliers: Canada's electronic spy agency is following you - new Snowden leaks.http://rt.com/news/canada-snowden-spying-nsa-airport-442/

[18] - Venezuelan Government Expands Internet Censorship- http://mashable.com/2014/02/20/venezuela-social-media/

[19] - In Ex-Soviet States, Russian Spy Tech Still Watches You- By Andrei Soldatov and Irina Borogan- 12.21.12- 6:30 AM
http://www.wired.com/dangerroom/2012/12/russias-hand/all/

[20] - China orders real name register for online video uploads.
http://www.reuters.com/article/2014/01/21/us-china-internet-idUSBREA0K04T20140121

[21] - King, Gary, Jennifer Pan, and Margaret Roberts. 2014. Reverse Engineering Chinese Censorship through Randomized Experimentation and Participant Observation. Copy at
http://j.mp/16Nvzgehttp://gking.harvard.edu/publications/randomized-experimental-study-censorship-china

[22] - - Pourquoi il faut réformer Internet
http://www.la-croix.com/Actualite/Monde/Pourquoi-il-faut-reformer-Internet-2014-04-23-1140281

فمع دفق المعلومات، وتصاعد استخدامنا للهواتف الخليوية، وغيرها الكثير من الاجهزة المتصلة بالانترنت، وتضخم امكانات الاتصال، يتحول كل فرد منا، الى لاقط عند أجهزة الاستخبارات الدولية[23]، اذ تتطور سبل الرقابة، ووسائل جمع المعلومات، وأساليب رصدها، والتنقيب عنها، ومعالجتها، واستثمارها، وتحليلها.

وبالفعل، تحاول الاجهزة الحكومية المختلفة، التعامل مع البيانات الشخصية والمعلومات، من منطلق ضرورة الرقابة، والسيطرة. وقد تطورت هذه المحاولات، بشكل دراماتيكي، وازدادت حدة الرقابة على البيانات والاتصالات الشخصية، بعد احداث الحادي عشر من أيلول، في الولايات المتحدة الاميركية، حيث ارتبطت هذه الرقابة، بحجة مكافحة الارهاب، والحرب عليه. وتستخدم العديد من الدول، برامج رقابة متطورة، كما أسلفنا، كما تلجأ معظم شركات الاتصال الكبرى، الى تسليم البيانات والمعلومات، الى ادارات وطنية أمنية.

وتستفيد هذه الاخيرة، من مقارنة البيانات التي تسلم اليها، بما جمعت هي من بيانات ولوائح، ومن تعقب الافراد عبر تطبيقات تحديد المواقع، والوصول الى لوائح اصدقائهم، وافراد عائلتهم، وبيانات اتصالاتهم، على الهاتف الذكي، والبيانات الجغرافية الموجودة على الصور، التي يتبادلونها على مواقع التواصل الاجتماعي، عبر هواتفهم، وبريدهم الالكتروني. وكانت اجهزة الاستخبارات البريطانية، قد اشارت في مستندات سرية، الى ان القدرة على التجسس، موجودة في برامج الالعاب الاكثر انتشارا، لاسيما عندما تسمح بتحديد موقع الشخص، وعمره، وجنسه، وغير ذلك من بياناته الشخصية[24].

تجدر الاشارة، الى ما يمثله هذا الواقع، من تهديد جدي للحياة الخاصة، ومن خلالها للحريات المدنية، والحقوق الشخصية الاخرى، التي تعتبر أساسية في ارساء قواعد الديمقراطية، والحكومة الرشيدة[25].

وعليه، ان تحول الرقابة، الى رقابة شاملة Mass Surveillance، والتحكم بوسائل الاتصالات المختلفة، وجمع البيانات عنها، لتعقب الافراد والمؤسسات، تهدد الحريات، بدءا من حرية المعتقد، مرورا بحرية الرأي والتعبير،التي يقرها الدستور اللبناني،

---

[23] - we are “somehow becoming a sensor for the world intelligence community” - Philippe Langlois- founder of the Paris-based company Priority One Security, on agencies’ ability to harvest personal data from users of smartphones.
http://www.nytimes.com/2014/01/28/pageoneplus/quotation-of-the-day-for-tuesday-january-28-2014.html?_r=0

[24] - Lisa Vaas on January 29, 2014- Spy agencies are slurping personal data from leaky mobile apps- http://nakedsecurity.sophos.com/2014/01/29/spy-agencies-are-slurping-personal-data-from-leaky-mobile-apps/- consulted on 30/1/2014
- A secret British intelligence document, from 2012, said that spies can scrub smart phone apps to collect details, like a user’s “political alignment”, and sexual orientation.

[25] - “The right to privacy, the right to access to information and freedom of expression are closely linked. The public has the democratic right to take part in the public affairs and this right cannot be effectively exercised by solely relying on authorized information.” Ms. Pillay- UN High Commissioner for Human Rightshttp://www.un.org/apps/news/story.asp?NewsID=46780&Cr=privacy&Cr1=#.UwCw6ThWHZY

وصولا الى حرية ممارسة النشاط السياسي والاجتماعي، بما يهدد الاقتصاد ونموه[26]، اضافة الى تقويضه اسس النظام الديمقراطي[27]

وقد رأى القضاء الاميركي، ان هذه الرقابة الشاملة، تشكل تعديا صريحا على الحريات.

ففي قضية مرفوعة من الاتحاد الاميركي للحريات المدنية، ضد عدد من الاجهزة الامنية والاستخباراتية، ووزير الدفاع، على خلفية التنصت على المواطنين الاميركيين، وجمع بيانات اتصالاتهم وبياناتهم الشخصية، اعتبرت محكمة في نيويورك، ان هذا العمل، يخرج عن الصلاحيات المعطاة لهذه الهيئات، في اطار مهمتها لحفظ الامن القومي، ويخالف التعديلين الاول والثاني من الدستور، اللذين يقران حرية التعبير، وحق الشخص في عدم انتهاك حرمة مسكنه، دون وجه حق[28].

مصادر الخطر: ممارسات حكومية وممارسات خاصة

يبقى الحق في الخصوصية، وبالرغم من الاعتراف به، من قبل العديد من الدول، والشرع والقوانين[29]، عرضة للاعتداء، ليس فقط نتيجة النقص التشريعي والتنظيمي، والممارسات الحكومية ، وانما نتيجة للامكانات التقنية الهائلة، التي تتيحها تقنيات المعلومات والاتصالات، والتي لا يمكن توقع امكاناتها. ونذكر هنا على سبيل المثال: تقنيات الرصد، وجمع البيانات، والتتبع، والمعالجة، والتنقيب، والوصول بسرعة فائقة، الى عدد أكبر من الناس، في أماكن مختلفة من العالم. يضاف الى ذلك، استحالة معالجة النتائج السلبية للاعتداءات، في أحيان كثيرة، مع تعذر استعادة البيانات، التي تم الاستيلاء عليها، أو تعذر السحب، أو الالغاء الكامل للبيانات، أو الاخبار،التي تم نشرها، أو تشويهها، أو تزويرها والتلاعب بها. هذا من دون ان ننسى، الخطر الذي

---

[26] - The NSA overreach poses a serious threat to our economy- http://www.theguardian.com/commentisfree/2013/nov/20/jim-sensenbrenner-nsa-overreach-hurts-business

[26] UNGA- 16 May 2011 A/HRC/17/27- **Human Rights Council- Seventeenth session-** Agenda item 3 **- Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development** "The growing use and sophistication of digital surveillance has outstripped the ability of societies to legislate their proper use, leading to "ad hoc practices that are beyond the supervision of any independent authority," and that threaten to repress free expression"

[27] - UNGA- 16 May 2011 A/HRC/17/27- **Human Rights Council- Seventeenth session-** Agenda item 3 - **Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development** "The growing use and sophistication of digital surveillance has outstripped the ability of societies to legislate their proper use, leading to "ad hoc practices that are beyond the supervision of any independent authority," and that threaten to repress free expression"

[28] - - **United states district court southern district of New York. 13 Civ. 3994- June 11 2013-** https://www.aclu.org/files/assets/nsa_phone_spying_complaint.pdf

47- الحق في الخصوصية من الحقوق الاساسية، المعترف بها في عدد من البلاد حول العالم، وفي نصوص عالمية، مثل الدساتير الوطنية والاتفاقية. الاعلان العالمي لحقوق الانسان، شرعة الحقوق السياسية والمدنية، الاتفاقية الاوروبية لحماية حقوق الانسان والحريات، والاتفاقية الاميركية لحقوق الانسان.

The Universal Declaration of Human Rights, (Article 17) of the International Covenant on Civil and Political Rights, (Article 8) of the European Convention on Human Rights, (Article 11) of the American Convention on Human Rights.

Article 12 of the Universal Declaration of Human Rights states, "No one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interferences or attacks."

يمثله، اقتحام بعض قواعد المعلومات الشخصية، سواء منها تلك التي تحتفظ بها الشركات، أو تلك التي تحتفظ بها الجهات الرسمية[30].

فالبيانات الشخصية، قيمة اقتصادية، يسعى اليها المستثمرون بكل الوسائل، من اجل تعزيز فرص وصولهم، الى شرائح أكبر وأوسع من الزبائن، والى تنمية فرص استثماراتهم، عبر تحديد أطياف الاشخاص. لذا، يبدو واضحا الارتباط الوثيق، بين حماية البيانات الشخصية، وبين الخطوات الأساسية، التي تتخذ في اطار حماية النمو الاقتصادي، سواء التقليدي منه ، أم الرقمي.

والبيانات الشخصية، هي ما تستخدمه السلطة، بشكل دائم ومستمر، كي تتمكن من تحديد هوية شخص ما، سواء أكان مواطنا ام أجنبيا. فالحكومة تجمع البيانات الشخصية، بشكل متزايد، ليس فقط بسبب اعتمادها الكثيف والمتزايد على تكنولوجيا المعلومات والاتصالات، وفي اطار تاديتها لدورها في ادارة أمور المواطنين، وشؤونهم الحياتية، بل أيضا، بسبب رغبتها في حماية هؤلاء، وحماية سيادتها، واستقرارها الامني، والاجتماعي، والاقتصادي.

وعليه، تتشكل مصادر الخطر على الخصوصية، نتيجة الاستخدام غير القانوني، أو التعسفي للبيانات الشخصية، أي من دون اعتبار لحقوق اصحابها، لاسيما حقهم في الخصوصية، وذلك، في القطاعين العام والخاص، على السواء.

ويعلو منسوب الاخطار، مع بعض البيانات الشخصية، التي يمكن اعتبارها بيانات حساسة، وذلك، نظرا لما يمكن ان يتركه انكشافها، من اثر سلبي على كيفية التعامل مع المعني بها، سواء من قبل السلطات المختصة، او من قبل الآخرين. وتتمثل هذه البيانات، في كل ما يسمح بتحديد الآراء والمعتقدات، والوضع الاجتماعي، والعرق، والهوية البيولوجية، والميول السياسية والجنسية. من هنا، تكون القاعدة فيما يتعلق بهذه البيانات هي حظر معالجتها، والسماح بمعالجتها هو الاستثناء، وذلك في حالات محددة حصرا[31].

الامن القومي والحق في الخصوصية

حددت التوصية الاوروبية الصادرة في العام 2002[32] ،الامن القومي، بانه:"... أمن الدولة، والدفاع، والسلامة العامة،...". وعليه، فالامن القومي هو جميع الاجراءات القانونية، والادارية، والعسكرية والامنية، التي تهدف الى حماية بلد معين، ضد اي نوع من التهديدات والاخطار، التي يمكن ان تعرض سلامة مواطنيه او اراضيه، أوسيادته.

---

[30]- منى الاشقر جبور ومحمود جبور- القانون والانترنت: تحدي التكيف والضبط- المنشورات الحقوقية- صادر- بيروت- 2008

[31] - ECOMLEB- art. 20 « Il est interdit de collecter et de traiter des données à caractère personnel qui révèlent, directement ou indirectement, les opinions philosophiques ou politiques, l'appartenance syndicale ou confessionnelle, l'état de santé, l'identité génétique ou la vie sexuelle de la personne concernée.
Toutefois, il est fait exception à cette interdiction de principe dans les cas suivants :
1°- Lorsque la personne concernée a rendu publiques lesdites données ou qu'elle consent expressément à leur traitement, à moins qu'une interdiction légale ne s'y oppose ;
2°- Lorsque le recueil et le traitement des données sont nécessaires à l'établissement d'un diagnostic médical ou à l'administration de soins par un membre d'une profession de santé ;
3°- Lorsque le recueil et le traitement des données sont nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice ;
4°- Lorsque des groupements sans but lucratif, à caractère philosophique, politique, syndical ou confessionnel tiennent, à leur usage exclusif, des registres de leurs membres ou correspondants non communicables à des tiers ;
5°- Lorsque des traitements justifiés par un intérêt public bénéficient des autorisations prévues à l'article 30 ci-après.

[32] - la directive européenne 2002/58/CE, remplacée par la directive 2006/24/CE.
La sécurité nationale est "… la sûreté de l'état, la défense, et la sécurité publique…"

واعتبر المسؤول السابق عن الامن الوطني الاميركي، مايكل ماكونال، ان الانترنت، قد رفعت مستوى الاخطار التي يتعرض لها النظام، بشكل غير مسبوق[33]. وفي ذلك اشارة واضحة، الى التهديدات الجديدة، التي تستهدف الامن القومي، والتي يمكن ان تتخذ اشكالا غير متوقعة، وتطاول مجالات اساسية وحيوية. يضاف الى ذلك، اتساع مفهوم الامن القومي، في العصر الحالي، ليشمل السلامة المادية للشخص او الوطن، الى جانب الامن الاقتصادي، والامن الاجتماعي، والامن الانساني. وما الدليل على ذلك، سوى التنسيق المتزايد، بين ادارات الامن والاقتصاد[34]، اضافة الى الترابط الذي يراه قادة العالم، بين أمن الفضاء السيبيري، والاقتصاد، والامن القومي. فقد أعلن الرئيسي الاميركي، باراك اوباما، أن امن الفضاء السيبيري، يأتي في مقدمة اهتماماته، معتبرا التهديد الآتي من الفضاء السيبيري، من أخطر المسائل، التي تطرح على المستوى الاقتصادي، كما على مستوى الامن القومي، ما دفعه الى تعيين مسؤول عن أمن الفضاء السيبيري، يكون على اتصال وتنسيق دائمين معه، ويكون عضوا في الامن القومي، وفي المجلس الاقتصادي الوطني[35]. ولم تتأخر الادارة الاميركية، عن استحداث قيادة عسكرية جديدة، تتولى أمن الفضاء السيبيري[36]. وكان رئيس الوزراء الانكليزي، غوردن براون، قد اعلن هو ايضا، عن انشاء وحدة خاصة، لمكافحة الجريمة السيبيرانية[37].

الا ان الرئيس الاميركي، حرص في المقابل، على تأكيد التزام ادارته، بحرية الانترنت، وبحرية الاتصالات، معتبرا ان من واجبها، حماية الحريات المدنية، والحق في الخصوصية، والمحافظة عليها.

في السياق عينه، أثار القانون حول "الامن في الفضاء السيبيري"، في الولايات المتحدة الاميركية، عددا من الاحتجاجات، نظرا للصلاحيات الواسعة، وغير المسبوقة، التي يمنحها للحكومة على الانترنت[38]. ورأى العديد من الخبراء، ان القانون، يشكل منعطفا خطيرا وجديا، نحو سحب صلاحيات وسلطات من القطاع الخاص، الذي يشرف على استثمار الخدمات المرتبطة بالبنية التحتية، عبر تحويل أمن هذه البنية[39]، الى السلطات الفدرالية، ما يخضع جزءا كبيرا، من صلاحيات الشركات المعنية بالاستثمار فيها، الى الحكومة الفدرالية.

ويظهر القانون، نوعا من نظام الطوارىء، الذي يعطي الرئيس الاميركي، صلاحية قطع الاتصال عبر الانترنت، وفصل البنية التحتية عنها، على أساس اعتبارات تتعلق بالامن الوطني. الا ان القانون، لا يحدد بدقة، الظروف والشروط الواضحة، التي تمنح الرئيس القدرة على التدخل، في اداء خدمات تديرها شركات خاصة، وترتكز الى رؤوس اموال خاصة.

---

[33] - McConnell said the Internet has "introduced a level of vulnerability that is unprecedented." Cybersecurity starts at home and in the office.
http://www.google.com:80/hostednews/ap/article/ALeqM5gkZ5sKNT86kqT9TWeDlogVPoASyQD9B469980

[34] - l'institution militaire en France loge, le poste de Haut représentant charge de l'intelligence économique (HRIE), responsable de la coordination des réponses gouvernementales en ce domaine, a savoir le secrétariat général de la défense nationale (SGDN).

[35] - Loppsi en France et Cyber-securite aux USA http://www.natchers.com/actualite-2009/8239/loppsi-en-france-et-cyber-securite-aux-usa

[36] - les USA se dotent d'un commandement militaire pour le cyberspace. …porte parole du pentagone : « les risques lies a la cybersecurite figurent parmi les defis economiques et de securite nationale les plus serieux du XXIe siecle ». http://www.elwatan.com/Les-USA-se-dotent-d-un

[37] - le cyberspace anglais desormais protégé par d'anciens pirates informtiques. http://techno.branchez-vous.com/actualite/2009/06/le_cyberspace_anglais_desormais

[38] - There's a new bill working its way through Congress that is cause for some alarm: the Cybersecurity Act of 2009 (PDF summary here), The bill as it exists now risks giving the federal government unprecedented power over the Internet

[39] - الطاقة والاتصالات، والصحة، و المصارف

فيما يتعلق بالخصوصية، يبدو واضحا، اتساع دائرة الصلاحية في الوصول الى البيانات، الى حد تجاوز، بعض النصوص القانونية القائمة[40]، والتي تعني حماية البيانات الشخصية. ويعطي القانون، لوزير التجارة الاميركي، حقا بالوصول الى جميع البيانات الخاصة بالبنية التحتية الحساسة critical، دون مراعاة لاي نص قانوني، او نظام، او قاعدة، او سياسة تمنع هذا الوصول.

وبالتالي، يتجه القانون، الى منح السلطة، حق الوصول الى "جميع البيانات ذات الصلة"، العائدة الى القطاع الخاص، خارج اطار "حالة الطوارىء، دون اعتبار، لضرورة حماية الحق في الخصوصية، أو للقواعد القانونية، والاصول القضائية الواجب احترامها، في الظروف العادية.

الامن العابر للحدود: البيانات الشخصية للمسافرين

تستدعي مكافحة الجرائم العابرة للحدود، كتبييض الاموال، والارهاب، والاتجار غير المشروع بالمخدرات ، اهتماما خاصا ، من قبل الحكومات المختلفة، بالبيانات التي تنتقل عبر الانترنت، ووسائل الاتصال الاخرى. فالبيانات الشخصية، تجمع بكميات كبيرة من المسافرين، ومن الوافدين الى اي بلد، وتنظم في لوائح وقواعد معلومات، ويتم تبادلها، في محاولة لرصدالتحركات المشبوهة. ويشكل هذا الموضوع، عقبة أساسية، أمام امكانية الحفاظ على الحق في الخصوصية، اذ انه يفقد صاحب البيانات امكانية السيطرة عليها.
وتفرض القوانين الأميركية، في هذا المجال، على شركات الطيران، التي تقدم خدمات النقل، من والى أراضيها، أو عبر المرور بها، أن تقدم بيانات شخصية، حول الركاب الذين تنقلهم، الى وزارة الداخلية الاميركية [41] . ويستهدف هذا الاجراء، المساهمة في تأمين سلامة الطيران، بشكل عام، من جهة اولى، والحفاظ على أمن الولايات المتحدة، بشكل خاص، من جهة ثانية. وتتوزع هذه البيانات على فئتين:

1- البيانات الخاصة باسم المسافر وسجله[42]، والتي تمثل المعلومات، التي تقدم خلال عملية الحجز لدى الشركة، عن تفاصيل الرحلة، مثل: اسم المسافر، وتاريخ الرحلة، ونقطة الانطلاق والوصول، ورقم المقعد، وعدد الحقائب، اضافة الى تفاصيل خاصة بالحجز، مثل: اسم وكالة السفر التي أجرت الحجز، وتفاصيل ايفاء قيمة التذكرة، وافادته من برامج خاصة بالزبائن، أو غيرها.

2- البيانات الأكثر تحديدا[43]، وتتناول: المعلومات التي تؤخذ من جواز السفر، والتي تجمع خلال عملية التسجيل، والتي تقدم الى السلطات المختصة بمراقبة الحدود، قبل الوصول، وذلك، للتأكد من أن المسافر، لا ينتمي الى لائحة الاشخاص، الذين يمثلون خطرا على سلامة الطيران.

وكانت الولايات المتحدة الاميركية، قد وقعت في هذا الاطار، اتفاقا مع الاتحاد الاوروبي، في 16 تشرين الاول (أوكتوبر) 2004، يفرض على هذا الاخير، أن يتأكد من التزام الناقلين الجويين، بتقديم هذه المعلومات[44]، كما هو مطلوب، الى وزارة الداخلية الاميركية. ويتيح الاتفاق المذكور، امكانية الحصول على هذه المعلومات، بالطريقة الالكترونية، وبشكل مسبق، لقيام الرحلات أو وصولها، ما يعني اتاحة امكانية، توقع المخاطر وتجنبها، بفاعلية أكبر.

في المقابل، يمكن للاتحاد الاوروبي، وبحسب هذا الاتفاق، أن يطلب من الولايات المتحدة الاميركية، نقل معطيات اليه، حول المسافرين من الولايات المتحدة الاميركية الى أوروبا، في حال اعتماده لسياسة مشابهة، لتلك التي تعتمدها حاليا. ويأتي ذلك،

---

[40] - The Electronic Communications Privacy Act, the Privacy Protection Act, The financial privacy regulations.
[41] - US Department of Homeland Security.
[42] - Passenger Name Record (PNR).
[43] - (Advanced Passenger Information (API)).
[44] - décision de la Commission 2004/535/EC: http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_235/l_23520040706en00110022.pdf

في اطار المحادثات التي يقودها الاتحاد الاوروبي، في المنظمة العالمية للطيران المدني، من أجل تحديد معايير عالمية، حول استخدامات المعطيات الخاصة بالمسافرين، بهدف الحماية على المعابر، وفي النقل الجوي.

وقد جاءت الضمانات، التي تلتزم بها الولاياتت المتحدة الاميركية، لتأمين مستوى حماية مقبول في الاتحاد الاوروبي، على الشكل التالي:

- حصر البيانات التي تنقل الى الولايات المتحدة الاميركية، ضمن 34 فئة، وهي أقل من تلك التي تجمع وتحفظ من قبل الولايات المتحدة الاميركية، عادة.
- حظر نقل البيانات التي تعتبر حساسة، والخاصة بالدين أو الصحة. وفي حال نقلها، يجري تنقيتها والغاؤها فيما بعد.
- حصر استعمال هذه البيانات ، بأهداف مكافحة الارهاب، والجرائم الكبرى.
- محو هذه البيانات، بعد فترة زمنية، حددت بثلاث سنوات وثلاثة أشهر، ما عدا حالات مراجعتها، في اطار تحقيقات خاصة، أو مراجعتها يدويا.
- الزام الولايات المتحدة الاميركية، اعلام المسافرين، بهدف جمع هذه المعطيات ومعالجتها، وبهوية المسؤول عن المعالجة.
- اقرار حق أصحاب البيانات، في النفاذ اليها، لمراجعتها، وتصحيحها.
- اقرار صلاحية السلطات المختصة في الاتحاد الاوروبي، مساعدة الافراد، لتقديم شكوى أمام السلطات الاميركية.
- منع فرز المعلومات، من قبل السلطات الاميركية، الا وفقا لكل حالة على حدة، ولاهداف متفق عليها.
- حظر نقل البيانات ، الى جهات اميركية أو هيئات أخرى، وطنية أو أجنبية، الا بعد ابلاغ سلطة مختصة، يعينها الاتحاد الاوروبي.
- وضع تقرير سنوي، من قبل الهيئات المختصة، على المستوى الاوروبي، حول مدى احترام الولايات المتحدة الاميركية، لالتزاماتها.

ويمكن للهيئات المكلفة حماية البيانات الشخصية، ممارسة صلاحيتها، في وقف انتقال البيانات، الى وزارة الداخلية الاميركية، بهدف حماية الاشخاص، من معالجة هذه البيانات، بطريقة مخالفة لما جاء في الاتفاق، مع الاتحاد الاوروبي.

وفي العام 2012، وقع الاتحاد الاوروبي والولايات المتحدة الاميركية، اتفاقا آخرا، حول نقل بيانات المسافرين، يقضي بما يلي:

- مشاركة ملفات بيانات المسافرين، والتحليلات الخاصة بها، مع الهيئات القضائية في الاتحاد الاوروبي، لمكافحة الجرائم العابرة للحدود، والارهاب، وتفعيل الملاحقات
- التزام الولايات المتحدة، استخدام هذه البيانات، في مكافحة الارهاب، والجرائم الخطيرة، مثل: تهريب المخدرات، والرقيق، والجرائم التي تصل عقوبتها الدنيا، الى ثلاث سنوات حبس.
- تحديد مدة الاحتفاظ بهذه البيانات، بعشر سنوات، على ان يبقى الرجوع اليها ممكنا، لمدة 15 سنة، لقضايا تتعلق بمكافحة الارهاب، وعلى ان تتم معالجة البيانات، بطريقة تمنع التعرف على اصحابها، بعد مرور 6 أشهر من تلقي السلطات الاميركية لها، ونقلها الى قاعدة معلومات غير موضوعة في الخدمة، بعد مرور 5 سنوات، وحيث لا يمكن للمسؤولين الاميركيين الوصول اليها، الا ضمن شروط معينة.

- تعيين مسؤول عن حماية البيانات الشخصية، في وزارة الداخلية الاميركية، يقدم تقارير حول الموضوع الى الكونغرس، ويتابع قضايا الحماية مع الهيئات المسؤولة، في الاتحاد الاوروبي، كما يتابع القضايا، التي يتقدم بها مواطنون، اعتبروا ان الولايات المتحدة، لا تلتزم احترام خصوصيتهم.
- اتاحة الامكانية أمام المواطنين الاوروبيين، للاعتراض على حفظ البيانات، وتقديم الشكاوى الادارية والقضائية، وتصحيح البيانات، والمطالبة بمحوها.
- التزام الناقل، اعلام المسافرين، باهداف وكيفية استخدام بياناتهم، وآليات ممارسة حقوقهم.
- منع تحديد ا طياف المسافرين، على أساس معالجة آلية، ومنع الملاحقة على هذا الاساس.
- استخدام محدد للبيانات الحساسة، مع التزام تطبيقات، تمنع معالجة البيانات الحساسة.
- وضع آليات ادارية، واصول تقنية، تضمن أمن البيانات ، ضد التلف، والمحو، والتلاعب وغير ذلك من الأخطار. ويفترض في هذا المجال تشفير البيانات.

وسائل الحماية: الاطار التشريعي

تتكون وسائل حماية البيانات الشخصية، بالاضافة الى التوعية، من اجراءات تقنية وقانونية. لكننا سنحصر بحثنا، في الوسائل، التشريعية والتنظيمية، نظرا لدورها الأساسي، حتى في تقرير الحماية التقنية نفسها، عندما تفرضها، وتنظم المحاسبة عن عدم الالتزام بها.

ويتناول التشريع في مسألة حماية البيانات الشخصية، مجالات: الحريات والحقوق الأساسية، الامن والعدالة، التقنيات والاجراءات المطلوب الالتزام بها، لضمان الحماية. ويرتبط تنظيم الفئة الاولى من الحماية ، بالاستخدامات الخاصة، وبالممارسات التجارية، بينما يرتبط تنظيم الفئات الاخرى، بتنظيم علاقات الافراد مع الدولة، وعلاقات ادارات الحكومة فيما بينها، لاسيما منها الهيئات المتخصصة، في ملاحقة الممارسات والاعمال، المخالفة للقوانين، والمخلة بالامن. وهذا يعني، وجود قواعد منشئة أو مقرة للحقوق والموجبات، والحريات، وكيفية الحفاظ عليها، في مواجهة معالجة البيانات الشخصية، بطريقة تعرض هذه الحقوق للخطر. كما يعني أيضا، وجود قواعد أخرى خاصة، تلحظ الحالات والاستثناءات، التي تبرر معالجتها، وتبادلها ونقلها، خارج قواعد الحماية المعمول بها.

ويطرح هذا الامر، ضرورة رفع التحدي، الخاص بايجاد التوازن بين الحماية، وحقوق وحريات اخرى، منها ما يتعلق بالافراد الآخرين في المجتمع، وحرياتهم، مثل: حرية التعبير، وحرية تبادل البيانات، والحق في الوصول الى المعلومات، ومنها ما يتعلق بحقوق المؤسسات التجارية، في ادراة هذه البيانات وجمعها، والافادة منها في نشاطها الاعتيادي، ومنها الآخر، ما يتصل بواجبات الدولة في حماية السلامة العامة، والامن القومي، والتي لطالما ارتبطت، بجمع المعلومات، وتبادلها، والوصول اليها.

على المستوى الدولي

ينطلق التشريع لحماية البيانات الشخصية، على المستوى الدولي، مما يمكن اعتباره، اطارا تشريعيا عالميا للحريات الشخصية، وهو شرعة حقوق الانسان الصادرة عن الامم المتحدة 1948 ، التي اقرت في المادة 12 " حق الشخص بعدم التعرض

الاعتباطي لخصوصيته، وحقه في حفظ كرامته، وحقوقه الفردية". ويندرج في هذا السياق، الاهتمام في انحاء العالم، بالحفاظ على البيانات الشخصية، كخطوة ضرورية، للحفاظ على الحق في الخصوصية[45].

وكانت منظمة التعاون الاقتصادي والتنمية قد أصدرت، دليلا حول حماية الخصوصية، وتوصية للدول الاعضاء، لالالتزام به. وقد لعب هذا الدليل، دورا أساسيا، في التوجهات التشريعية للدول الاوروبية، وتضمن عددا من المبادىء، هي: محدودية عمليات جمع البيانات Collection-limitation، نوعية البيانات Data quality ، وتحديد الهدف Purpose-specification ، وحصر الاستخدام بالهدف المحدد Use-limitation ، و تأمين وسائل حماية وامن المعلومات Security-Safeguards ، العلانية Openness ، والحق في المشاركة والمساءلة Individual Participation and Accountability. ويطبق هذا الدليل، على البيانات الخاصة بالاشخاص الطبيعيين، المعالجة آليا، أو يدويا، في القطاعين العام والخاص. كما تبنت الامم المتحدة عام 1990، من خلال هيئتها العامة ، دليلا لتنظيم المعالجة الآلية للبيانات الشخصية، تضمن مبادىء الدليل، الذي اصدرته منظمة التعاون الاقتصادي والتنمية. ويمثل هذا الدليل، توصية للدول الاعضاء، بضرورة تبني تشريعات، تنظم معالجة البيانات الشخصية.

[45]- مؤتمر استوكهولم 1967 – مؤتمر طهران 1968 باشراف الامم المتحدة.

على المستوى الاوروبي

وفي سنة 1978 ، صدر قانون فرنسي حول حماية البيانات الشخصية، تحول الى أداة عمل، في اتفاقية المجلس الاوروبي الصادرة عام 1981 . بعد ذلك، صدر الارشاد الاوروبي في العام 1995، أي بعد صدور توجيهات منظمة التعاون الاقتصادي والتطوير، عام 1980، وذلك، بهدف منع التناقض وعدم الانسجام، بين القوانين الاوروبية الخاصة بحمايات البيانات الشخصية، يؤثر سلبا على التجارة الالكترونية والخدمات، بين دول الاتحاد. وبالفعل، فقد ارسى هذا الارشاد، مبادىء عامة، وقواعد واضحة، يمكن الركون اليها، والاسترشاد بها، لاسيما وانه قد جاء خاليا من أي تفاصيل اجرائية، يمكن ان تعرقل عملية التطبيق، ومؤسسا لانشاء سلطات وطنية للرقابة. وكان الهم الاساس في هذا الارشاد، الحفاظ على الحريات الشخصية، واحترام حقوق الانسان، ضمن البيئة الجديدة. وبالفعل، فقد شكل ارشاد العام 1995 ، نواة الحركة التشريعية الاوروبية، الهادفة الى حماية البيانات الشخصية. وقد أدخل هذا الارشاد، مصطلحات جديدة، كالبيانات الشخصية، ومعالجة البيانات الشحصية، ومراقب المعالجة، والمعالج، والشخص الثالث، والمتلقي، وأصحاب البيانات. واقتصر تطبيق هذا الارشاد، على معالجة البيانات الشخصية، التي تجري ضمن الاتحاد الاوروبي، والتي تخضع لقوانينه، مستثنيا، عمليات المعالجة الخاصة بالسلامة العامة، والدفاع، وأمن الدولة، ونشاطات الحكومة، في المجال الجزائي.

تبع هذا الارشاد، ارشادات وقرارات لاحقة، احتفظت بالمبادىء العامة، واضافت ما يتماشى مع مستجدات المعالجة الالكترونية، ونقل البيانات، لاسيما فيما يتعلق باساليب المعالجة، وطرق النقل.

ونورد في هذا المجال، اتفاق الملاذ الآمن، الموقع بين الاتحاد الاوروبي، والولايات المتحدة الاميركية، والذي يوجب على كل شركة، راغبة في تلقي بيانات شخصية من احدى دول الاتحاد الاوروبي، ان تلتزم مستوى حماية ملائما للارشاد رقم EC/46/95. كذلك، الارشاد الصادر، عام 2002، والمعدل في العام 2008، حول الخصوصية الالكترونية، والاطار التنظيمي لعمل المجلس للعام 2008، تاريخ 27 نوفمبر، حول حماية البيانات الشخصية، في مجال العمل التعاون القضائي، والامني. وينظم هذا الاطار، بعض الحقوق، مثل: اعلام صاحب البيانات، والوصول الى البيانات المحفوظة لدى الاجهزة الامنية المعنية بالملاحقة والتحقيق، والتعويض في حال كانت المعالجة مخالفة للقانون، والقيود الموضوعة على معالجة البيانات الشخصية. وينحصر مدى تطبيقه ، على البيانات الخاصة بالشؤون الامنية والعسكرية، التي يتم تبادلها بين دول الاتحاد، دون تلك التي تتم معالجتها، على المستوى الوطني.

تمايز في اتجاهات التنظيم

لكن الانسجام الذي تحقق على المستوى الاوروبي، وبعض المستوى الدولي، لا يمنع وجود اختلافات وتمايز، ناتجة احيانا عن اختلاف الانظمة القانونية. ويبدو هذا الاختلاف واضحا، على مستوى بعض المسائل الخاصة بحماية البيانات، مثل: نوعية الاشخاص المعنيين بالحماية (الشخص الطبيعي والشخص المعنوي)، ونوعية المعالجة المقصودة (الآلية أو اليدوية)، والجهات المراقبة، وأصول نقل وتبادل البيانات، والاعمال الجرمية.
فاهتمام الدول، بالحفاظ على هذه الحقوق والحريات، يختلف باختلاف ثقافتها القانونية. ففي فرنسا، حيث تسود القواعد الصارمة لحماية الحريات الشخصية، تتولى هيئة خاصة، الرقابة على أمن المعلومات الشخصية، بينما لا توجد في الولايات المتحدة الأميركية، سلطة مشابهة لها[46]. لا بل ان اللجوء الى القضاء، لحماية هذا الحق، يصبح دون جدوى، متى اختلفت القواعد القانونية، والاسس التي يتم على أساسها، التعامل مع البيانات الشخصية. ففي الولايات المتحدة الاميركية، تعتبر هذه

[46] -CNIL en France.
Aux USA il ya Federal Trade Commission qui suit les dossiers internet et poursuit quelques sites web qui n'ont pas respecte sur leur site les déclarations sur la protection des données personnelles.

البيانات، بيانات تجارية، ذات قيمة خاضعة لحاجات السوق، بينما تعتبر هذه البيانات في اوروبا، كجزء من خصائص الميزات الشخصية[47]، ما يجعل تعامل القضاء مع شروط استثمارها، ومعالجتها، يختلف بشكل أكيد.

وتتوزع اتجاهات التنظيم، على المستوى العالمي، بشكل أساسي، بين تلك التي تنضوي تحت لواء الولايات المتحدة الأميركية، وتلك التي تنضوي تحت لواء الاتحاد الأوروبي، وتلك التي تنضوي تحت لواء الأنظمة القمعية[48]. إلا إن الجميع، يخضع بشكل أو بآخر، للشروط الخاصة التي تمليها تقنيات الانترنت، والشركات القائمة على تطويرها، مع الإشارة إلى خضوع الشركات التجارية هي الأخرى، إلى الاعتبارات التجارية والاقتصادية التي ترتبط بها، والتي أخضعتها إلى رغبات الأنظمة السياسية وسياستها الخاصة[49]، في مجال الرقابة على الانترنت، والحد من النفاذ إلى المعلومات، واستخدام البيانات الشخصية.

ويطاول هذا الاختلاف، الجهات التي تساهم في التنظيم، وصولا الى آلياته ومضمونه. ففي أوروبا، تخضع عملية تطوير المقاييس، المعتمدة في تكنولوجيا لمعلومات والاتصالات، إلى جهات رسمية، بينما يسيطر القطاع الخاص على هذه العملية، في الولايات المتحدة الاميركية. كذلك، يعكس كل من التشريعين، الأوروبي والأميركي، قيما ثقافية مختلفة عن: السلطة العامة، والسوق، ومجالات التشريع والتنظيم.

ويبدو هذا الاختلاف الثقافي واضحا[50]، على مستوى المضمون، كما على مستوى المقاربة، لاسيما في مسألة معالجة البيانات الشخصية، وحماية حق الأفراد في الحفاظ على الخصوصية[51]، حيث يبرز الاختلاف، بدءا من الدستور، اذ تتقدم حرية التعبير على الحق في الخصوصية، بحسب الدستور الاميركي، بينما تتقدم الخصوصية على هذا الحق، في دول الاتحاد الاوروبي، وحيث يتولى الأفراد أنفسهم والشركات التجارية، في الولايات المتحدة الأميركية، مسؤولية تقرير سياسة الحماية الشخصية على الانترنت، الى حد كبير. ويعتمد في هذا المجال، مبدأ الانضباط الذاتي. ويجد هذا الامر مبرراته، في وجود اطار تشريعي للحماية، يشمل منع المنافسة غير المشروعة، ومنع الاحتكار، وحماية المستهلك، ومنع الغش.

في المقابل، تتولى الدولة، الجزء الاكبر والاشمل من هذه المهمة، في أوروبا، باعتبارها أحدى واجبات السلطة، في حماية المواطنين، دون اسقاط مبدأ المشاركة في الضبط، والذي يعني مساهمة القطاعات المعنية، التجارية منها والمدنية[52]. وتعمل هيئات الاتحاد الاوروبي، على توجيه الدول الاعضاء، الى اصدار تشريعات، تتلاءم مع القواعد المقررة في التوصيات الصادرة عن منظماته: كمجلس اوروبا، واللجنة الاوروبية، والاتحاد الأوروبي. كما يبرز الاتجاه الاوروبي بوضوح، نحو التنظيم التشريعي الشامل، عبر قوانين البرلمان الأوروبي.

---

[47] - l'oubli numérique, future droit constitutionnel? Selon Alex Türk, le président de la commission nationale de l'informatique et des libertés (CNIL) et président du G29 : « Pour les américains, les données personnelles sont des données commerciales qui ont une valeur marchande. En Europe, nous pensons que ce sont des attributs de la personnalité ».
http://eulogos.blogactiv.eu/2009/11/23/1%2%80%99oubli-numerique-futur-droit-con

[48]- وتأتي في هذه الفئة على سبيل المثال: الصين وبعض البلاد العربية.

[49]- موافقة googleو microsoftو yahoo على الالتزام بمنع الوصول الى بعض المواقع، بناء على رغبة الحكومة الصينية، وبما ينسجم مع النظام السياسي المعتمد من قبل هذه الاخيرة.

[50] - "While the United States and the European Union share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacyfrom that taken by the European Union", Safe Harbor Principles.

[18]- من التفسيرات التي يمكن ان تساق في هذا المجال، هو ميل الانظمة التي تعتمد النظام العرفي الى التركيز بنسبة أكبر على العلاقة، بين القانون والاقتصاد والمجتمع، بينما تميل الثانية، الى التركيز اكثر، على العلاقة، بين القانون والسياسة والمجتمع.

[52] Law put to the test by information technologies. Interviews with French parliamentary Deputy Christian Paul, and Olivier Debouzy. www.france.diplomatie.gouv.fr -on the amerrican side, the individuals active on the web intend to regulate their activities themselves. On the French side, the concept of co-regulation is being promoted by the combined forces of business, users and the authorities.

التعاون الدولي: اتفاق الملاذ الآمن

أبرز الاختلاف في التنظيم، خطورته على حماية البيانات الشخصية، ما أدى إلى تهديد الاتحاد الأوروبي، بحظر انتقال البيانات الشخصية، الى البلاد التي لا تؤمن معايير حماية ، موازية لتلك المعمول بها، في التوصيات الصادرة عنه[53]، وذلك انسجاما مع المبادىء التي تقرها هذه الأخيرة، فكان تشاور بين وزارة التجارة الاميركية، و اللجنة الاوروبية، لايجاد آلية تسهل عملية الانتقال هذه، أدت الى وضع اتفاق الملاذ الآمن: "safe Harbor Agreement".

يضم الاتفاق عددا من المبادىء، التي لا بد من الالتزام بها، من قبل الشركات الأميركية، الراغبة في الافادة، من استمرار دفق البيانات الشخصية اليها. وتتناول هذه المبادىء، ضرورة الالتزام بعدد من الاصول، التي تلحظ اطارا تشريعيا معقولا، يمكن ان يمنع الاعتداء على خصوصية الافراد. ومن هذه المبادىء:

- موجب الاعلام: اذ يفترض بالشركات، توفير المعلومات، التي توضح أهداف جمع، ومعالجة بياناتهم الشخصية، وطريقة التصرف بها، لاسيما عندما يتعلق الامر، بنقلها الى جهة ثالثة. وفي الحالة الأخيرة، يجب اطلاع الافراد، على طبيعة الجهة الثالثة، التي يمكن أن تحصل على هذه المعلومات، مع اشارتها الى الخيارات المتاحة، للحد من استخدام هذه البيانات، ومن كشفها. يضاف الى ذلك، اعطاؤهم المعلومات، حول كيفية الاتصال بالشركة، لنقل أي سؤال، أو شكوى.

- حق القبول أو الرفض: اعطاء الافراد، الحق في قبول أو رفض، كشف، أو نقل بياناتهم الشخصية، الى جهة ثالثة، أو استخدامها، في الهدف لا يتناسب مع الهدف الذي جمعت لاجله، والذي تم على أساسه القبول.

- نقل البيانات الى جهة ثالثة: في هذه الحال، تلتزم الشركات، موجب الاعلام الواضح، كما تلتزم تأمين الخيارات. بالاضافة الى ذلك، يتوجب عليها، أن تتأكد من أن التزام الجهة الثالثة، اتفاق الملاذ الآمن، أو التوصية الاوروبية لحماية البيانات الشخصية، أو أي سياسة حماية أخرى، جدي. كما يمكن، أن تتفق الشركة، مع الجهة الثالثة، على احترام مستوى الحماية المطلوب.

- حق الوصول الى البيانات والتعديل: اعطاء الافراد، حق الوصول الى البيانات الشخصية، التي تجمع عنهم، لتصحيحها، وتعديلها، أو الغائها، حين لا تكون صحيحة. ويمكن السماح للجهة التي تجمع البيانات، بعدم اعطاء هذا الحق للمعنيين بالبيانات، في حال كان هذا الوصول، ذي كلفة مرتفعة، لا تتناسب وحجم المخاطر التي يتعرض لها الفرد، أو في حال كان وصوله، الى هذه البيانات، يتعرض لحق الآخرين في الخصوصية.

- أمن المعلومات: تلتزم الشركات، موجب حماية البيانات. ويفترض بها، اتخاذ الاجراءات الكفيلة، بمنع تعريضها للضياع، أو اساءة الاستعمال، أو الانكشاف، أو التشويه، أو التلاعب بها.

- صحة البيانات Data integrity: يجب أن تتناسب البيانات الشخصية، مع الاهداف التي ستستخدم لاجلها. ويفترض بالشركة، اتخاذ الخطوات المعقولة، لضمان مصداقية البيانات، وصحتها.

- آليات الاعتراض والتطبيق: تلتزم الشركات، ايجاد آلية، تسمح بالنظر في شكاوى الافراد، وحل النزاعات، وتقرير التعويضات حيث يجب، وبمقتضى القواعد القانونية. الى جانب ذلك، يجب توفير اصول خاصة، لمراقبة مدى التزام الشركات، وتنفيذها للخطوات المطلوبة، كشرط لقبول انضمامها، وفرض عقوبات شديدة، على مخالفة هذه الالتزامات، كالشطب من لائحة الشركات، التي تستفيد من الاتفاق.

---

[53] - The "safe Harbor Agreement" formula., was suggested by US Ambassador Aaron. Safe Harbor Privacy Principles issued by the U.S. Department of Commerce on July 21, 2000

بحسب هذا الاقتراح، يمكن للشركات الأميركية التي تتعاطى معالجة المعلومات الشخصية، أن تلتزم القواعد المعمول بها في الاتحاد الأوروبي حول حماية المعلومات الشخصية.

هذا، ويعود قرار الانضمام الى الاتفاق، الى الشركات نفسها، التي يفترض بها، أن تعلن التزامها بتطبيق شروطه، وتحترم هذا الالتزام. ويتم ذلك، بتوجيه رسالة بهذا المعنى، الى وزارة التجارة الاميركية، كل عام. وتتضمن الرسالة الاعلان، والحق في الوصول الى البيانات، والحق في قبول أو رفض السماح باستخدام البيانات، وآليات الاعتراض والتطبيق[54]. ويفترض بالشركة، التي ترغب في الافادة من هذا الاتفاق، أن تعلن عن انضمامها اليه، وذلك في سياسة الحماية، التي تنشرها على موقعها.

ويشترط لقبول انضمام هذه الشركات الى الاتفاق، أن يكون لديها سياسة حماية، خاصة بالبيانات الشخصية، سواء عبر انضمامها الى أحد برامج الحماية، الملحق بالاتفاق، أو عبر تطويرها لبرنامج خاص بها، يتناسب ومندرجات التوصية الاوروبية.

وسائل الحماية في العالم العربي: غياب شبه كامل

يسجل في الدول العربية، نقص واضح، في الاطار التشريعي والتنظيمي، لحماية البيانات الشخصية، والحياة الخاصة. واذا كان البعض، يعتبر ان الدستور، اطار ملائم لهذه الحماية، استنادا الى المبادىء والقواعد، التي تقر حماية الحريات الفردية، فان دساتير خمس دول عربية فقط، تقر هذا الحق صراحة، وهي: مصر، وقطر، وموريتانيا، وليبيا والجزائر. فقد أقر الدستور المصري، في المادة 45 حماية الحياة الخاصة للمواطنين، والدستور القطري (2003) حرمة خصوصية الانسان، والدستور الجزائري، عدم انتهاك حرمة حياة المواطن الخاصة، في المادة 39، ونص الدستور الليبي، في المادة 16 منه، على أن: للحياة الخاصة حرمة، ويحظر التدخل فيها، الا اذا شكلت مساسا بالنظام والآداب العامة، أو اضرارا بالآخرين، واذا اشتكى أحد أطرافها. ونص الدستور الموريتاني، في المادة 13، انه على الدولة، أن تضمن شرف المواطن، وحياته الخاصة.

الى ذلك، يمكن اضافة بعض الدساتير، التي نصت على ما يمكن اعتباره، حماية لمكون من مكونات الخصوصية: حرية الاتصالات وسريتها. وقد أوردت ذلك، دساتير اليمن في المادة 52، وسلطنة عمان في المادة 30، والصومال في المادة 22.

وليس الحال بأفضل، على مستوى القوانين الوضعية العربية. فبالرغم من الجهود والمبادرات، الرامية الى تعزيز الانخراط في مجتمع المعلومات، وانشاء الحكومات الالكترونية، وتنمية التجارة الالكترونية، عبر اقرار عدد من التشريعات، الا انه ليس هنالك نصوص صريحة وشاملة، لحماية البيانات الشخصية في الوطن العربي، سوى قانون حماية البيانات الشخصية، الصادر في الامارات العربية المتحدة، في العام 2007، وهو قانون خاص بالمركز المالي، صادر باللغة الانجليزية، ومنسجم الى حد بعيد، مع الارشاد الاوروبي للعام 1995. وقانون رقم 63، للعام 2004، في تونس، والذي تضمن بعض النصوص الخاصة بحماية البيانات الشخصية، في اطار التجارة الالكترونية. أما القوانين العربية الاخرى، التي يمكن ذكرها، فهي: القانون المغربي رقم 2008-09، يضاف الى ذلك، بعض المواد التي وردت عرضا في بعض القوانين، دون اي تفصيل، او آلية حماية، تضمن تنفيذا فاعلا لها، لاسيما لدى تعارض هذا الحق وهذه الحماية، مع المصلحة العامة وحقوق الغير، كقانون الاحصاءات العامة المؤقت لسنة 2008، الصادر في الاردن، وفيه مواد خاصة بسرية البيانات الاحصائية، ومنع افشائها [55]، وقانون الاتصالات، رقم 18 الصادر في سوريا عام 2010[56]، الذي يؤكد على مبدأ احترام الخصوصية. وفي هذا التجاهل لآليات الحماية والتنفيذ، وحدود الممارسة، خطر أكيد، مع تصاعد وتيرة معالجة البيانات الشخصية، وازدياد حجمها، وامكانات معالجتها، واستخدامها، والربط بينها، والتنقيب عنها، بدون معرفة اصحابها وموافقتهم. هذا، ويسجل وجود عدد من مشاريع القوانين، الخاصة بالمعاملات الاكترونية، في كل من الكويت، ولبنان، وسوريا.

تجدر الاشارة هنا، الى ان جميع الدول العربية، اعضاء في الامم المتحدة، وملتزمة الاعلان العالمي لحقوق الانسان، لاسيما المادة 12 منه، التي تقرعدم جواز التدخل التعسفي، في حياة الافراد الخاصة، أو مراسلاتهم، وحقهم في حماية قانونية، تضمن ذلك. الا أن آليات التطبيق والتنفيذ، ليست متوافرة لضمان حماية البيانات الشخصية والخصوصية، في غياب قواعد تفصيلية،

---

[54] - includes elements such as notice, choice, access, and enforcement.

[55] - المواد 11و12و51و16و17

[56] - المادة 50 من القانون

وتطبيقية، لحالات معالجة البيانات، وحفظها، والوصول اليها، وحقوق الاشخاص في المراقبة، والاعتراض، والتصويب، والمحو، وغير ذلك.

ومما لا شك فيه، ان هذا الفراغ التشريعي، سيتسبب في تخبط في مواجهة المسائل القانونية الناتجة عن انتشار معالجة البيانات الشخصية، على جميع المستويات، الحكومية والتجارية، الداخلية والخارجية، اضافة الى استمرار جمع وتدفق البيانات عبر الحدود، دون علم اصحابها، واستثمارها واستخدامها، بشكل مناف لحقوق اصحابها.

يضاف الى ما تقدم، غياب الوعي، لدى العديد من المشرعين العرب، لأهمية حماية البيانات الشخصية، ودورها في تعزيز الانخراط السليم في مجتمع المعلومات، والنمو الاقتصادي والاجتماعي، كذلك عدم ادراك خطورة الامر، والقدرة، لدى غالبية مستخدمي وسائل المعلومات والاتصالات الحديثة، على حماية انفسهم، في مواجهة الاخطار والاعتداءات، التي تمارس من خلال عمليات معالجة بياناتهم، وتبادلها، ونقلها واستثمارها. ويزيد الامر سوءا، انسداد مجالات المراجعة والاعتراض، أمام القلة التي تدرك خطورة الامر، في حال تعرض خصوصيتها للانتهاك، من خلال جمع ومعالجة بياناتها الشخصية.

التاسيس على الاطار الدولي

نظرا للبعد العالمي، والعابر للحدود، لحماية البيانات الشخصية، لا بد من الالتفات، الى الاطر التي يمكن البناء عليها، والانطلاق منها. لاسيما وان لهذه الحماية ، ولحماية الخصوصية التي تعنيها، دور حاسم، في تشجيع التجارة والخدمات الالكترونية، وفي تحقيق الانسجام، مع توجهات المنظمات والهيئات الدولية، مثل: منظمة التعاون الاقتصادي والتنمية والاتحاد الاوروبي، والامم المتحدة.

من هنا، يمكن الانطلاق على المستوى الوطني، من الارشادات التي وضعتها منظمة الاقتصاد والتنمية، حول حماية الحياة الخاصة، وحركة انتقال هذه البيانات عبر الحدود. ويثير الموضوع الاخير، مسألتين هما: الشفافية والمسؤولية. ويقوم مبدأ الشفافية، بحسب الارشادات، على تأمين الوسائل الكفيلة بتحديد وجود البيانات الشخصية، وطبيعتها، واهداف معالجتها، ووجهة استخدامها، كما وبتحديد هوية الحائز على هذه البيانات، والمكان الذي يمارس فيه نشاطه. أما المسؤولية، فتعني: ان يحترم الشخص الذي يحتفظ بالمعلومات، القواعد والاجراءات، التي تضمن تطبيق الارشادات.

وتأسيسا على الانسجام الذي تحقق على المستوى الاوروبي، فيما يتعلق بحماية البيانات الشخصية، وطرق نقلها عبر الحدود، وانطلاقا من الانسجام بين بعض الانظمة القانونية العربية ذات المنشأ الاوروبي، يمكن الافادة من التجربة الاوروبية، في هذا المجال، كنقطة انطلاق، الى تحقيق الحماية والانسجام على المستوى العربي، بالرغم من غياب اطار مؤسساتي عربي جامع، على غرار الاتحاد الاوروبي. كذلك يمكن الافادة، من التفسيرات والجوانب العملية، لكيفية تطبيق الارشاد الاوروبي، والقوانين الاوروبية، والتي أبرزتها القرارات القضائية، الصادرة في مجال حماية البيانات الشخصية، وذلك في اطار تطبيق القوانين الاوروبية، الخاصة بهذا الموضوع.

ويسجل في هذا المجال، اللجوء العملي، لمعظم المشرعين الذين وضعوا قوانين، كما اولئك الذين اعدوا مشاريع قوانين في هذا المجال، الى النصوص الاوروبية، وغيرها مما هو مطبق في هذا المجال. ونذكر هنا، اقتراح القانون اللبناني، حول تنظيم المعاملات الالكترونية، الذي التزم مبادىء التوصية الاوروبية، حول حماية البيانات الشخصية، وأخذ عن تشريعات غربية، واهمها، التشريع الفرنسي في هذا المجال، والصادر عام 2004. فقد خصص هذا الاقتراح، المؤلف من 175 مادة، 30 مادة منه، ، في الباب الخامس، تحت عنوان " حماية المعلومات ذات الطابع الشخصي"، لحماية المعلومات ذات الطابع الشخصي. وقد توزعت على خمسة فصول، أبرزت عناوينها الاحكام العامة، وعمليات جمع ومعالجة المعلومات، والاجراءات الخاصة بتنفيذ هذه الاخيرة، وحق الوصول والتصحيح، والاحكام الجزائية التي تطال مخالفة الاحكام الخاصة، بحماية المعلومات.

مجالات التشريع: ضبط المعالجة والتبادل والنقل والتخزين في السحاب

تفترض حماية البيانات الشخصية، احاطة شاملة، بكل الآليات التقنية، ووسائل المعالجة، والتصرف بالبيانات، بحيث لا تترك ثغرات، يمكن النفاذ منها للالتفاف على الهدف الذي وضعت من اجله. وعليه، لا بد لأي اطار تشريعي أو تنظيمي، أو ارشاد، وعلى غرار أي نص قانوني آخر، أو ارشاد أو اتفاقية، ان يلحظ الآتي:

- الاسباب الموجبة، التي تلحظ فلسفة النص، وأهدافه.

- التعريفات الضرورية لوضوح النص، ومجال تطبيقه. وعليه، لا بد هنا من تحديد: البيانات الشخصية، وعمليات المعالجة، والانظمة أو الآليات التي يتم العمل بموجبها، اضافة الى الهيئات، والاشخاص المسؤولين والمعنيين.

- تحديد الجهات التي يمكنها جمع البيانات الشخصية، دون اذن مسبق، على ان تحدد أهداف هذا الاستثناء بوضوح، وعلى أن ينسجم هذا الاستثناء، مع مقتضيات السلامة العامة، والامن القومي، وطبيعة بعض النشاطات المهنية الخاصة.

- تحديد الشروط، التي يمكن على أساسها، الحصول على اذن بمعالجة البيانات الشخصية، ونقلها، وتبادلها، توضح فيها، نوعية البيانات التي يمكن معالجتها، أو نقلها، او تبادلها، كموافقة صاحب البيانات، والمصلحة المبررة والمشروعة من جمعها.

- تحديد البيانات المستثناة، والاسباب المانعة لمعالجتها، اضافة الى الحالات التي يمكن فيها تجاوز هذا الاستثناء، شرط الانسجام مع فلسفة النص واهدافه؛ أي الحفاظ على حرمة الحياة الشخصية، والحريات الفردية والعامة، والحقوق الاساسية للانسان، والنصوص القانونيةوالاحكام، والمصلحة العامة، او المصلحة الخاصة للشخص المعني، وحرية التعبير.

- اقرار حقوق اصحاب البيانات في الوصول اليها، والتدقيق فيها، وطلب تصحيحها او محوها، او منع النفاذ اليها. يضاف الى ذلك، حق الاعتراض على المعالجة، متى توافرت لدى الشخص اسباب مشروعة، أو متى كان هدف المعالجة، أعمالا تجارية وترويجية.

- انشاء هيئات رقابية، ذات صلاحيات ملاحقة وردع، تسهر على التطبيق، وحسن سير آليات التنفيذ، بحيث تضمن جميع حقوق الشخص، صاحب البيانات، من جهة أولى، لاسيما لناحية حقوقه في مراقبة التصرف ببياناته، وأوجه استخدامها، ودقتها، ومصداقيتها، والاهداف التي تستخدم لاجلها. وتدخل في هذا الاطار، الشكاوى، والمراجعات والاعتراضات. اما من الجهة الثانية، فلا بد من تنظيم حقوق الجهات المعنية بمعالجة هذه البيانات، سواء أكانت مؤسسات عامة، أم خاصة، أم أشخاصا طبيعيين يستثمرون هذه البيانات، ويديرونها في اطار نشاطهم العلمي، أو التجاري.

- تحديد مسؤوليات الجهات المراقبة، وموجباتها، لاسيما لجهة الالتزام بسرية البيانات، والحفاظ على سلامتها وعدم انكشافها، أو تسربها، وتلفها، والتلاعب بها.

- اقرار الحق في التعويض عن المخالفات المرتكبة، ووضع اصول مراجعات قضائية وادارية ملائمة، تعزز ممارسة الشخص لحقه في الحفاظ على بياناته الشخصية، ومن خلالها على حريته الشخصية، وحياته الخاصة.

- تأمين حماية البيانات الشخصية المنقولة عبر الحدود، الى بلد أجنبي، بموجب اتفاقات واضحة، تحترم المبادىء العامة للنص الخاص بالحماية، وفلسفته، على ان تلحظ آليات موافقة وتصريح، لا تعيق تدفق البيانات لاهداف تخدم تطور التجارة الالكترونية، والمصلحة العامة، والاقتصاد، والامن.

- ارساء أخلاقيات خاصة، تجارية و مهنية، و ادارية، بالتعامل في مجال معالجة البيانات الشخصية،ونقلها، والتصرف بها، تعزز دور الاطارين التشريعي والتنظيمي.

- وضع آليات مواجهة للتحديات الجديدة، التي تفرضها الحوسبة السحابية، لاسيما على المستويات التالية: تشجيع التزام الشركات بقواعد الحماية والامن، تحديد مسؤولية المتعاقدين مع موفري الخدمة الاساسيين، نوعية الخدمة، طبيعة المسؤوليات، مستويات الحماية، نقل البيانات الى بلاد، يمكن ان تكون على عداء مع بلد المصدر.

الخطوات العملية المطلوبة

- اقرار توصية، أو ارشاد على المستوى العربي، من خلال جامعة الدول العربية، تتضمن المبادىء العامة لحماية البيانات الشخصية، وتنسجم مع الاتجاه الدولي في هذا المجال، لجهة الأهداف والفلسفة، لحماية البيانات العابرة للحدود.

- اقرار الاطر التشريعية والتنظيمية الملائمة، على المستوى الوطني.

- انشاء الهيئات الرقابية المناسبة، لاسيما منها، الهيئة الوطنية للمعلوماتية والحريات.

- وضع اطر تشريعية وتنظيمية، لتبادل البيانات الخاصة بمجالات الامن، مع الدول الاخرى.

- انشاء هيئات تنسيق وتعاون وطنية، تتولى متابعة التنفيذ على المستوى العربي، والدولي، لاسيما في حالات انتقال بيانات، تخص مواطني أكثر من دولة.

- تعزيز الوعي في المجتمع، بكل قطاعاته المدنية، والمهنية، والحكومية، بأهمية حماية البيانات الشخصية، ودورها في حماية الفرد والمجتمع.

- التعاون على ايجاد آليات حماية، تسمح للمواطن بممارسة حقه في الاطلاع على البيانات، وطلب تصحيحها، لدى الدول الاخرى التي تتولى معالجتها،، وملاحقة المؤسسات أو الهيئات، التي تمتنع عن تطبيق القوانين الخاصة بالحماية، على غرار ما هو معمول به في مجال ملاحقة المجرمين، ومكافحة الارهاب، والجرائم العابرة للحدود، بكل أشكالها.

خلاصة

بناء على ما تقدم، تعتبر حماية البيانات الشخصية، وحماية الخصوصية، من خلالها، حاجة ملحة، لاسيما وان للاعتداء عليها، جوانب قانونية، نتيجة عدد من الجرائم السيبرانية، ومنها: انتحال هوية الشخص، انتحال الصفة، اختراق انظمة المعلومات، الوصول الى الاسرار المهنية والتجارية، الرصد غير المشروع لحركة الاشخاص والاموال، التمييز العنصري، أو العقائدي، أو الديني.

كذلك، يعتبر الحفاظ على البيانات الشخصية، كوسيلة للحفاظ على الحق في الخصوصية، في أساسيات تعزيز الثقة، في الفضاء السيبراني، والافادة من طاقات تقنيات المعلومات والاتصالات، على المستويات: الاجتماعية، والاقتصادية، والثقافية. فالتحديات الحالية، التي تطرحها وسائل معالجة البيانات وجمعها، واستخدامها، واستثمارها، لا بد وان تكون ذات انعكاسات سلبية، على استخدام الانترنت، ومروحة التقنيات المتصلة بها، سواء تجاريا، او اجتماعيا، او حكوميا. لذا، لا بد من ايجاد الاطر التشريعية والتنظيمية، التي تمكن المستخدمين، من فهم حقيقة ما يجري، من ممارسات تطاول بياناتهم الشخصية، والمعلومات التي يضعونها على الانترنت. كما لا بد من تمكينهم، من ممارسة حقوقهم، في ادارتها، بالشكل الذي يطمئنهم، الى امكانية الحفاظ على خصوصيتهم، وعلى حقوقهم الفكرية، والصناعية والادبية.

ولا بد لهذا للاطار القانوني، ان يتضمن قانونا خاصا، لحماية البيانات الشخصية، وانشاء هيئة خاصة للمعلوماتية والحريات، تشكل مرجعا لحماية المواطنين وحقوقهم، من كل استثمار غير شرعي في بياناتهم الشخصية، كما ومن كل اعتداء على خصوصيتهم، نتيجة عمليات جمع البيانات، والتنقيب عنها، وتحليلها، واستثمارها، واي عملية اخرى تطاولها، خارج القواعد القانونية، المرعية الاجراء.

يضاف الى ذلك، ضرورة الانتباه، الى أهمية توعية المواطنين، كما المعنيين بمعالجة البيانات الشخصية، في الادارات العامة والخاصة، على المخاطر التي تنطوي عليها هذه العملية، كما عملية انكشافها، وتسربها.

ويمكن البناء في هذا المجال، كما أسلفنا، على التجارب الدولية، أو الاقليمية الناجحة، وعلى التوصيات والاتفاقيات الموجودة، سواء منها، تلك التي تعنى بحماية البيانات الشخصية، أو تلك الخاصة ببيانات الاتصالات.