دروس مقتبسة من القانون العام لحماية المعطيات الشخصية للاتحاد الأوروبي

accessnow

جانفي 2018

أكساس ناو تدعم وتدافع عن الحقوق الرقمية للمستخدمين المعرضين للخطر حول العالم.
فمن خلال الجمع بين الدعم الفني المباشر،و الالتزام بسياسة شاملة ، والدعوة الى ذلك على صعيد عالمي، و اللجوء الى المنح الشعبية، وعقد الاجتماعات كتلك التي تقوم بها رايتس كون، يكون كفاحنا من أجل حقوق الإنسان في العصر الرقمي

هذه الورقة من مطبوعات أكسس ناو

لمزيد من المعلومات الرجاء زيارة موقع :

https://www.accessnow.org

أو الاتصال ب :

Estelle Masse | Senior Policy Analyst | **estelle@accesnow.org**

المحتويات

المقدمة

تقدم أكسس ناو هذا الدليل بعنوان " إنشاء إطار المعطيات الشخصية: دليل للمشرعين - حول ما يجب فعله واجتنابه- دروس مقتبسة من القانون العام للاتحاد الأوروبي الخاص بحماية البيانات" للمساهمة في الخطاب العالمي حول حماية البيانات. وتعكس الورقة بشكل خاص مقاربة الاتحاد الأوروبي حول هذه المسألة و مستوى حماية البيانات الشخصية في جميع أنحاء العالم.

إن القانون العام للاتحاد الأوروبي الخاص بحماية البيانات يشكل إطارا إيجابيا لحماية المستخدمين وسوف يساعد المستخدمين على استعادة السيطرة على معلوماتهم الشخصية. و رغم أن القانون يجري حاليا تنفيذه ، فإنه بالفعل أصبح مصدر الهام للحكومات في جميع أنحاء العالم لرفع مستوى التشريعات المتعلقة بحماية البيانات أو تطويرها ،حيث تتيح هذه التشريعات فرصا هائلة. تمة دروس هامة يمكن استخلاصها من المفاوضات التي تجري حول القانون العام لحماية البيانات ،كثير منها إيجابي والبعض سلبي.[1] من خلال تجربتنا فقد قمنا بإنشاء قائمة بما يجب فعله و اجتنابه نرى أن يتم أخذها بعين الاعتبار من طرف المشرعين عند وضع في إطار قانوني لحماية المعطيات الشخصية.

الخلفية

هل سبق لك أن قمت بأداء الضرائب أو إجراء مكالمة هاتفية؟ هل تملك هاتف ذكي؟ هل سبق لك استخدام الإنترنت؟ هل لديك حساب في وسائل الاعلام الاجتماعية أو قمت بارتداء جهاز تعقب اللياقة البدنية؟ إذا كان الجواب هو نعم على أي من هذه الأسئلة، فهذا يعني أن كنت قد تتقاسم معلومات شخصية ، سواء عبر الإنترنت أو خارجها، مع كيانات من القطاع الخاص أو العام، بما في ذلك بعض الجهات التي لم تسمع عنها قط. أن تقاسم البيانات هو ممارسة عادية أصبحت تنتشر على نحو متزايد في كل مكان بحكم استعمال المجتمع للإنترنت. فتقاسم البيانات لا يعود بالفائدة على المستخدمين فحسب، بل غالبا ما يكون ضروريا أيضا للقيام بالواجبات الإدارية أو التعامل مع المجتمع اليوم. ولكن هذا لا يخلو من المخاطر. ان معلوماتك الشخصية تكشف الكثير عنك، وعن أفكارك، و حياتك، ولهذا السبب يجن أن تكون محمية.

إن الحق في حماية البيانات الشخصية يرتبط ارتباطا وثيقا بالحق في الخصوصية الا أنه يتميز عنه.

أكثر من 160 دولة تشير إلى الحق في الخصوصية في دساتيرها، ولكن معنى "الخصوصية" يختلف من بلد لآخر بحكم التاريخ، والثقافة، أو التأثيرات الفلسفية.[2] وهذا ما يفسر سبب اختلاف طريقة حماية الخصوصية تختلف من بلد إلى آخر حتى لو كان العديد من التقاليد القانونية تحصر حماية الخصوصية على الحق في احترام الحياة الخاصة والأسرية، والبيت والمراسلات.

أما حماية المعطيات الشخصية ، فهي من ناحية أخرى, لا تعتبر دائما حقا في حد ذاتها. إن الدول 28 أعضاء الاتحاد الأوروبي تعتبر استثناء مي هذا المجال، لأنها اعترفت بحماية البيانات باعتبارها حقا أساسيا في ميثاق الاتحاد الأوروبي 2001.[3]

ومع ذلك، فإن حماية البيانات الشخصية ذات أهمية قصوى في مجتمعنا الرقمي المتغير. وكثيرا ما يعترف بهذه الحماية من خلال أطر ملزمة على الصعيد الوطني، والإقليمي، والدولي، وفي العديد من الأماكن التي لم يتم فيها

[1] Access Now, General Data Protection Regulation – what tidings do ye bring? https://www.accessnow.org/general-data-protection-regulation-what-tidings-do-ye-bring/
[2] https://www.constituteproject.org/search?lang=en&key=privacy
[3] http://www.europarl.europa.eu/charter/pdf/text_en.pdf

تدوين مجلة لحماية البيانات بعد نجد ان المشرعين هم بصدد القيام بذلك. ونعتقد أنه ينبغي أن يحدث هذا بأسرع وقت ممكن.

إن حماية البيانات الشخصية أو معلومات التعريف الشخصية تعني إنشاء قواعد واضحة على كل كيان يعالج المعلومات الخاصة بك أن يتبعها. هذا ليس مفهوما جديدا حيث أن قوانين حماية البيانات متوفرة في العديد من البلدان حول العالم منذ أكثر من 40 عاما، ولكن هذه القوانين أصبحت ذات أهمية متزايدة حيث أن تقاسم البيانات بين الناس في ازدياد وجمع الشركات للبيانات واستخدامها يرتفع بسرعة فائقة. فقد تم إقرار أول قانون لحماية البيانات في سنة 1970 من قبل. ولاية هيس الاتحادية الألمانية[4] .وبعد سنوات قليلة وضعت الولايات المتحدة " الاستعمالات النزيهة للمعلومات" التي أثرت في القوانين الحديثة لحماية البيانات على الرغم من أن الولايات المتحدة لم تقم بمتابعة أي قانون مقنن لإطار حماية البيانات على المستوى الفدرالي،واكتفت بدلا من ذلك باعتماد قوانين خاصة بكل قطاع.[5] ثم جاءت أول قوانين على مستوى البلاد لحماية البيانات الشخصية، في السويد وألمانيا وفرنسا، قبل أن تعتمد منظمات دولية مثل مجلس أوروبا الأطر الدولية. أما اتفاقية مجلس أوروبا لحماية الأفراد فيما يتعلق بالمعالجة الاتوماتيكية للبيانات الشخصية - المعروف أيضا باسم الاتفاقية 108 فقد تمت المصادقة عليها سنة 1980 وأصبح باب التوقيع عليها مفتوحا في عام 1981 [6] . وفي عام 1980 وضعت منظمة التعاون والتنمية في الميدان الاقتصادي مبادئها التوجيهية المتعلقة بالخصوصية[7] ومنذ اعتمادها، صادقت جميع البلدان الأعضاء مجلس أوروبا ال 47 على الاتفاقية رقم 108 و صادقت عليها جزر الموريس والسنغال، وأوروغواي، ومؤخرا تونس في سنة2017 [8] . وقد لعبت الاتفاقية 108 دورا محوريا في اعتماد أول قانون لحماية البيانات في أوروبا سنة 1995 على نطاق واسع.[9] واليوم، اعتمدت مئات البلدان في جميع أنحاء العالم قوانين حماية البيانات العامة أو القطاعية.[10]

وبالإضافة إلى الأطر القائمة، هناك بلدان تنظر حاليا في تشريعات حماية البيانات من بينها: تونس والهند واليابان وكوريا الجنوبية والبرازيل والأرجنتين[11] وبالنسبة لبعض هذه البلدان، سيكون هذا أول قانون لها لحماية البيانات. وقد عملت أكساس ناو في مجال التشريع لحماية البيانات في جميع أنحاء العالم منذ عام 2009، ولا سيما فيما يخص عملية الإصلاح التي قام بها الاتحاد الأوروبي. بخصوص القانون العام لحماية البيانات.[12] إن الاتحاد الأوروبي والدول الاعضاء فيه لها خبرة جيدة في مجال حماية البيانات وغالبا ما تعتبر معيارا في هذا المجال، مما يبرز كون عديد من البلدان تهتم بتطبيق القانون العام لحماية البيانات في مناطق نفوذها. فهناك دروس مهمة تقتبس من مفاوضات القانون العام لحماية المعطيات الشخصية يمكن الاستفادة منها كثيرها إيجابي وبعضها سلبي. من خلال تجربتنا، أنشأنا قائمة للمشرعين في جميع أنحاء العالم في ما يجب فعله و تركه.

[4] Hessische Datenschutzgesetz,Original version dated from 7 October 1970. (GVBl. I S. 625).
[5] See EPIC, the code of fair information practices. https://epic.org/privacy/consumer/code_fair_info.html
[6] Council of Europe, Convention for the protection of individuals with regard to automatic processing of personal data, 1981. http://www.coe.int/web/conventions/full-list/-/conventions/treaty/108
[7] Privacy International, Data Protection. https://www.privacyinternational.org/node/44
[8] تونس تصدق على الاتفاقية108 وتؤكد الالتزام بحماية البيانات الشخصية أكسس ناو:
https://www.accessnow.org/tunisia-ratifies-convention-108-affirms-commitment-protection-personal-data
[9] Peter Hustinx, EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation, 2015. https://edps.europa.eu/sites/edp/files/publication/14-09-15_article_eui_en.pdf
[10] See Privacy International, Data Protection. https://www.privacyinternational.org/node/44
[11] السلطة الوطنية التونسية لحماية البيانات الشخصية مسرؤع قانون حماية البيانات الشخصية 2017.
http://www.inpdp.nat.tn/Projet_PDP_2017.pdf
[12] الاتحاد الأوروبي، اللائحة رقم 2016/679 / بخصوص حماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية وحرية تنقل هذه البيانات وإلغاء التوجيه 95/46 / (اللائحة العامة لحماية البيانات) 12
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

ما يجب فعله

تجد أسفله 10 توصيات لواضعي السياسات يجب اتباعها عند تطوير قانون حماية المعطيات الشخصية. وهذه الخطوات العشرة ضرورية سواء بمفردها أوبمجموعها لضمان مفاوضات مفتوحة واعتماد إطار يركز على المستخدم.

1 ضمان مفاوضات شفافة وشاملة لجميع الاطراف

يتعين على الحكومات وصانعي القرار ضمان إجراء مفاوضات مفتوحة، شفافة، وشاملة بشأن أطر حماية البيانات. وهذا يعني إجراء مشاورات عامة واجتماعات و موائد مستديرة للخبراء، بنشر النصوص التفاوضية، والسماح لجميع الأطراف المهتمة بالتعليق بتوفير أجال نهائية معقولة، وتقديم التغذية الراجعة على التعليقات الواردة. وفي جميع المراحل، يجب ضمان المشاركة الفعالة من جانب أطياف المجتمع المدني، وأن يتم تنظيم اجتماعات صانعي القرار مع ذوي الاختصاص والمنظمات غير الحكومية وجمعيات الدفاع عن المستهلكين حيث تكون هذه الاجتماعات علنية و التسجيل فيها في متناول الجميع. وينبغي أن يرافق هذه العملية أقصى قدر من الشفافية فيما يخص الضغط. وينبغي إيلاء الاهتمام الواجب بأراء أفراد المجتمع المدني، لمعالجة الاختلال الحتمي في عدد الأصوات مقارنة بأهل الاختصاص.

تجارب مفاوضات القانون العام لحماية المعطيات الشخصية

وأجريت مفاوضات القانون العام لحماية المعطيات الشخصية وفقا للعملية التشريعية للاتحاد الأوروبي وهذه العملية شفافة إلى حد ما وكفلت عموما نشر مشاريع المقترحات، والآراء والتقارير والتعديلات، والآراء القانونية لجميع مؤسسات الاتحاد الأوروبي حول كل مسالة تشريعية تتم مناقشتها. بيد أنه يمكن إدخال بعض التحسينات على هذه العملية التشريعية. أولا، ينبغي أن تكون هناك مساءلة أكبر في مرحلة الصياغة الأولى من التشريعات. من خلال مطلب قانون حرية المعلومات على سبيل المثال تمكنت أكسس ناو من الحصول على بريد إلكتروني يكشف كيف أن وزارة الشؤون الداخلية في المفوضية الأوروبية كانت تعمل جنبا إلى جنب مع الإدارة الأمريكية خلال المراحل الأولى من جهود إصلاح الخصوصية[13] وبالإضافة إلى ذلك، فإن المرحلة الثلاثية من المفاوضات بين جميع مؤسسات الاتحاد الأوروبي غير شفافة. وقد انضمت أكسس ناو الى الجهود بقيادة الحقوق الرقمية الأوروبية "إدري" في الدعوة إلى إصلاح العملية منذ سنوات.[14] وبسبب انعدام الشفافية خلال تلك المرحلة،لا يتم إعلام الجمهور بأهم النقاط في المفاوضات؛ أي عندما يجتمع المشرعون للاتفاق على نص يشمل حلا توفيقيا نهائيا سيصبح ملزما بعد ختمه من طرف مؤسسات الاتحاد الأوروبي.

كما يجب على أصحاب المصلحة الخارجيين الذين يسعون للتأثير على المفاوضات أن يلتزموا بمبادئ الشفافية والمساءلة. فلقد تعرضت مفاوضات القانون العام لحماية البيانات إلى جهود ضغط لم يسبق لها مثيل، حيث كان ممثلو الصناعة يهدفون إلى إضعاف المعايير القائمة لحماية البيانات، ومنع المقترحات من تعزيز حقوق المستخدمين. وأصبح تأثير بعض الصناعات والشركات الأجنبية واضحا عندما قام المشرعون بنسخ ولصق مقترحات التعديل من مقترحات الضغط,[15] في تلك الحالة، استطاعت مجموعات الدعوة أن تساعد الجمهور على مقارنة اللغة التي تقترحها جماعات الضغط بالنص الذي يقترحه المشرعون[16] . هذه العملية مكنت العموم من التعليق على معنى هذه المقترحات وساعدت على مكافحة النفوذ عن طريق سرية التعاملات الخلفية. ان اقتراح التعديلات ليس بالضرورة نشاطا مشبوها، ولكن يجب أن يتم بطريقة شفافة. يجب أن يعرف الناس من أين تأتي هذه المقترحات و على جماعات الضغط أن توضح دائما الجهات التي تنتمي إليها في مقترحاتها و أن تجعلها متاحة للجمهور.

[13] Access Now, Big brother's little helper inside the European Commission https://www.accessnow.org/big-brothers-little-helper-inside-the-european-commission/
[14] Access Now, EU "trilogues" consultation: A foot in the door for transparency https://www.accessnow.org/eu-trialogues-consultation-foot-door-transparency/
[15] Access Now, Privacy under siege: Unprecedented lobby efforts against the Regulation are revealed https://www.accessnow.org/privacy-under-siege-unprecedented-lobby-efforts-against-the-regulation-are/
[16] LobbyPlag initiative http://lobbyplag.eu/compare/overview

2 تعريف قائمة مبادئ لحماية البيانات تكون ملزمة وتضمينها في الإطار القانوني

ويجب أن يتضمن أي إطار يهدف إلى حماية المعلومات الشخصية تعريفا واضحا للبيانات الشخصية والحساسة. وينبغي أن يتوافق مستوى الحماية مع حساسية كل فئة من فئات البيانات. وينبغي أن يتم تعريف البيانات الحساسة بشكل يجعلها تشمل البيانات الوراثية و البيومترية، فضلا عن محتوى الاتصالات والبيانات الشرحية، حيث أن هذه المعلومات تكشف عن سمات شخصية حساسة بشكل خاص. وهذا يعني أن إطار حماية البيانات يمكن أن يتضمن أيضا اجراءات محددة لحماية البيانات المتبادلة أثناء الاتصالات وما يتصل بها من أحكام الخصوصية لضمان سرية الاتصالات.

وإلى جانب التعاريف الواضحة، فإن المبادئ الثمانية التالية هي في صميم أطر حماية البيانات.[17] تضع هذه المبادئ المترابطة التدابير اللازمة لأي إطار حماية بيانات يسعى إلى إيجاد حماية فعالة لحقوق المستخدمين. يتطلب التدوين الفعال لهذه المبادئ تطوير مجموعة من حقوق المستخدمين، و وضع الأساس القانوني لمعالجة البيانات، وتدابير أمن البيانات، وآليات الرقابة، والتزامات الكيانات التي تعالج البيانات، والتدابير التي تمكن من نقل البيانات إلى بلدان أخرى.

1. **الإنصاف والشرعية:** يجب أن تتم معالجة البيانات الشخصية بشكل عادل وقانوني مما يعني أنه ينبغي معالجة المعلومات وفق أساس قانوني واضح من أجل غرض مشروع، وبصورة عادلة وطريقة شفافة حتى يتمكن المستخدمون من التعرف بشكل كاف عن كيفية جمع البيانات الخاصة بهم، المستخدمة، أو المخزنة، وعن الجهة التي تقوم بذلك.

2. **تحديد الغرض:** لا يتم جمع البيانات الشخصية و معالجتها إلا لغرض محدد ومشروع. و يجب أن يكون هذا الغرض محددا وصريحا ولا يتجاوز مدة زمنية محدودة. ولا يجوز معالجة البيانات بأي طريقة لا تتفق مع هذا الغرض.

3. **تقليص البيانات:** يجب أن تقتصر البيانات الشخصية التي تم جمعها واستخدامها على ما يكفي لغرض محدد ومعين ، وتكون مناسبة لهذا الغرض ، وأن لا يكون هناك افراط في ذلك.

4. **الدقة:** يجب أن تكون البيانات الشخصية دقيقة، وأن يتم تحيينها عند الضرورة. للمستخدمين الحق في حذف ،إصلاح وتصحيح، المعلومات الشخصية الخاصة بهم.

5. **تحديد مدة الاحتفاظ بالبيانات:** لا يجوز الاحتفاظ بالمعطيات الشخصية لمدة أطول مما هو ضروري.

6. **حقوق المستخدمين:** تتم معالجة البيانات الشخصية وفقا لحقوق المستخدمين مثل الحق في النفاذ الى المعلومة أو الحق في حذفها (انظر النقطة 4).

7. **النزاهة والسرية:** يجب أن تتم معالجة البيانات الشخصية بطريقة تضمن أحدث ما توصلت إليه أمن البيانات، بما في ذلك الحماية ضد المعالجة غير المصرح بها أو غير المشروعة وضد أي فقدان ، تدمير أو ضرر عرضي قد يلحق بها ، وذلك باستخدام التدابير التقنية أو التنظيمية المناسبة.

8. **التلاؤم:** لا يجوز نقل البيانات الشخصية إلى بلد ثالث أو إقليم ثالث، ما لم يكن ذلك البلد أو الإقليم يضمن مستوى كاف من الحماية.

لحقوق وحريات المستخدمين فيما يتعلق بمعالجة البيانات الشخصية. يجب أن تنص أطر حماية البيانات على آليات تمكن من التدفق الحر للبيانات بين البلدان و تحافظ في نفس الوقت على مستوى عال من حماية البيانات.

تجارب مفاوضات القانون العام لحماية المعطيات الشخصية

ان المصدر الاساسي للمبادئ الثمانية لحماية البيانات هو المعايير الدولية، ولا سيما الاتفاقية 108 والمبادئ التوجيهية لمنظمة التعاون والتنمية في الميدان الاقتصادي[18] . ان مبادئ حماية البيانات هذه تعتبر "معايير دنيا" لحماية الحقوق الأساسية للبلدان التي صادقت على الأطر الدولية لحماية البيانات. هذه المبادئ ينبغي أن تكون أساس أي إطار لحماية البيانات و هي متواجدة في قوانين حماية البيانات في جميع أنحاء العالم، من توجيه الاتحاد الأوروبي لحماية البيانات عام 1995 البيانات، ومعظم قوانين حماية البيانات المعمول بها في أمريكا اللاتينية.

[17] UK Information Commissioner's Office, Data Protection Principles
https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/

[18] منظمة التعاون والتنمية في الميدان الاقتصادي . سبتمبر 1980. المبادئ التوجيهية التي تحكم حماية الخصوصية والتدفقات عبر الحدود للبيانات الشخصية
https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/OECD_Privacy_Guidelines_1980.pdf

3 تحديد الأساس القانوني الذي يسمح بمعالجة البيانات

ويجب أن يحدد أي قانون لحماية البيانات بوضوح الأساس القانوني الذي يمكن بموجبه معالجة البيانات الشخصية للمستخدمين. على أي كيان، عام أو خاص،يسعى إلى معالجة البيانات الشخصية أن يلتزم على الأقل بالأسس القانونية المنصوص عليها في القانون. وتشمل هذه عادة تنفيذ بنود العقد، والامتثال لواجب قانوني، وموافقة المستخدم.

يتم تعريف الموافقة على أنها مطلب فعال ومستنير وصريح من المستخدم. يجب أن تعطى بحرية من طرف المستخدم الذي يجب أن تكون لديه القدرة على سحب الموافقة في أي وقت. وهذا يعني، على سبيل المثال، فإن الصناديق التي تم مسبقا إدراج علامة عليها لن تعتبر موافقة صحيحة. وبالإضافة إلى ذلك، لا يمكن للشركات أن تمنع وصول المستخدم إلى خدمة بسبب رفضه لمشاركة بيانات تزيد على ما هو ضروري لاستعمال وظائفها. وإلا فإن الموافقة لن تمنح بدون مقابل.

تجارب مفاوضات القانون العام لحماية المعطيات الشخصية

ويتيح القانون العام لحماية البيانات ستة قواعد لمعالجة البيانات الشخصية من لحظة إبرام العقد إلى الموافقة[19] وتم تعزيز وتوضيح تعريف الموافقة خلال المفاوضات مقارنة بالتعريف المنصوص عليه في التوجيه 95/46. السابق،. يشير القانون العام لحماية البيانات إلى أن الموافقة يجب أن "عملا إيجابيا واضحا ينشئ بحرية، ويحتوي على إشارة محددة، ومستنيرة، ولا لبس فيها للمستخدم". ومع ذلك، فإن القانون العام لحماية المعطيات الشخصية يجيز أيضا معالجة بيانات لما يسمى أغراض "المصلحة المشروعة" التي يحددها الكيان المستعمل للمعلومات. هذا الحكم يحد كثيرا من سيطرة المستخدمين على معلوماتهم الشخصية لأنهم في كثير من الأحيان لا علم لهم بعملية جمع للبيانات أو معالجتها عندما تعتمد الكيانات على المصلحة المشروعة (انظر المزيد عن المصلحة المشروعة في النقطة الثانية من قسم "ما يجب تركه").

4 إدراج قائمة بحقوق المستخدمين الملزمة في القانون

ان حماية بيانات المستخدمين وضمان تحكمهم في معطياتهم الشخصية يتطلب إيجاد مجموعة من الحقوق التي يجب الالتزام بممارستها:

ومفهومة من الكيانات التي تعالج بياناتهم الشخصية، سواء كانت هذه الكيانات قد جمعت هذه المعلومات مباشرة أو تلقتها من خلال أطراف ثالثة. كل المعلومات المقدمة للمستخدم يجب توفيرها بطريقة موجزة، واضحة، و يمكن النفاذ إليها بسهولة، باستخدام لغة واضحة وغير معقدة. يجب أن تتضمن هذه المعلومات تفاصيل حول البيانات التي يتم معالجتها، والغرض من هذه المعالجة، و مدة التخزين، إن وجدت. كما يجب على الكيانات توفير معلومات عن تفاصيل الاتصال بهم وعنوان بريد إلكتروني للسماح للمستخدمين للاتصال بهم في حالة وجود أي إشكال.

6. الحق في الاستفسار: يمكن المستخدمين من الحصول على معلومات عن الأساس المنطقي وراء المعالجة التلقائية للبيانات الشخصية، ونتائج تلك المعالجة. وهذا الحق ضروري لتحقيق المساءلة والشفافية عند استخدام الخوارزميات لأخذ القرارات التي تؤثر على حياة المستخدمين.

7. الحق في الاستفسار: يمكن المستخدمين من الحصول على معلومات عن الأساس المنطقي وراء المعالجة التلقائية للبيانات الشخصية، ونتائج تلك المعالجة. وهذا الحق ضروري لتحقيق المساءلة والشفافية عند استخدام الخوارزميات لأخذ القرارات التي تؤثر على حياة المستخدمين.

1. الحق في النفاذ الى البيانات: يمكن المستخدمين من الحصول على تأكيد من الخدمات والشركات حول ما إذا كانت عملية جمع البيانات الشخصية المتعلقة بهم قد تمت وهل هي في طور المعالجة. إذا كان هذا هو الحال، يجب على المستخدمين النفاذ إلى البيانات، و التعرف على الغرض من المعالجة و على هوية من يعالجها، الى غير ذلك.

2. الحق في الاعتراض: يمكن المستخدم من القول "لا" بخصوص معالجة المعلومات الشخصية الخاصة به، في حالة موافقته على معالجة البيانات وعدم توقيع العقد. ينطبق هذا الحق في الاعتراض على الآليات الاتوماتيكية لصنع القرار، بما في ذلك التنميط، حيث أن المستخدم له الحق في عدم التعرض لاستخدام هذه التقنيات.

3. الحق في المحو: يسمح للمستخدمين بطلب حذف جميع البيانات الشخصية المتعلقة بهم عند مغادرتهم الخدمة أو التطبيق.

4. الحق في التصحيح: يسمح للمستخدمين طلب تعديل معلومات غير دقيقة عنهم.

5. يضمن الحق في المعلومة: أي أن يتلقى المستخدمون معلومات واضحة

[19] انظر الفصل 6. الاتحاد الأوروبي، اللائحة 2016/679 / بشأن حماية الأشخاص الطبيعيين فيما يتعلق بمعالجةز البيانات الشخصية وحرية تنقل هذه البيانات وإلغاء التوجيه 95/46 / إيك (اللائحة العامة لحماية البيانات)
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

وعلى الرغم من أن هذه القائمة ليست شاملة، فإن هذه الحقوق يجب أن ينص عليها القانون، ولا تترك لتقدير الكيانات التي تستخدم البيانات. يجب أن يكون المستخدمون قادرين على ممارسة أي من هذه الحقوق مجانا.

تجربة من القانون العام لحماية المعطيات الشخصية

ويتيح القانون العام لحماية البيانات للمستخدمين جميع الحقوق المذكورة مجانا.ان الأحكام التي تكرس تلك الحقوق يحدد واجبات مفصلة على الكيانات التي تقوم بمعالجة البيانات تنفيذها، تنص على حماية هذه الحقوق وحمايتها واحترامها.[20] ويشكل القانون العام لحماية البيانات خطوة هامة في ضمان تمكن المستخدمني من ممارسة حقهم في حماية البيانات بكل حرية. ومع ذلك، لضمان أن تكون جميع التدابير فعالة، ينبغي أن يكون هناك مزيد من بذل جهود لزيادة الوعي حول وجود القانون ومضمونه. يجب على الحكومات، والسلطات العامة، والشركات، والمنظمات غير الحكومية أن تعمل معا لتحقيق هذا الهدف وأخيرا، فإن ممارسة بعض الحقوق مثل الحق في قابلية التنقل والحق في الاستفسار لها أهمية خاصة في عصر البيانات الكبيرة والذكاء الاصطناعي. غير أن الإعمال الكامل لهذه الحقوق لن يتحقق دون التعاون من الكيانات الخاصة التي تقوم بتطوير الخوارزميات والمنتجات والخدمات. ويجب علينا أن نضمن أن المهندسين سيقومون بإنشاء الاليات اللازمة لتمكينهم من التنفيذ والاستمتاع بهذه الحقوق. فعلى سبيل المثال، أن الحق في قابلية التنقل لي له أي معنى إذا لم تكن المنصات غير قابلة للتشغيل المتبادل.[21] كذلك، فإن الحق في الاستفسار لا يمكن أن يكون متوفرا إلا إذا كان موظفو الشركات الذين يعتمدون على الخوارزميات يفهمون جيدا كيفية أداء وظائفها، وإذا كانوا يعرفون لماذا يجري استخدام هذه الخوارزمية ،و ما هي البيانات المستخدمة في الخوارزمية،و البيانات التي تم إنشاؤها بواسطة الخوارزمية، والمتغيرات التي تستخدمها الخوارزمية لاتخاذ قرار ما.و نظرا لأن لغة القانون العام لحماية البيانات محدودة في هذا المجال ، فإن العديد من الأكاديميين يتساءلون حتى عن مشروعية الوجود القانوني و قابلية تنفيذ هذا الحق[22] . ويبدو واضحا أن القانون العام لحماية البيانات كان يعتزم خلق مثل هذا السبيل للمستخدمين ولكن سيكون من الضروري الحصول على مزيد من التوجيه من سلطات حماية البيانات وأصحاب المصلحة بشأن كيفية تفسير النص عمليا. باختصار،فان إيجاد مثل هذه الحقوق هو شيء إيجابي ولكن يجب أيضا وضع شروط لممارسة هذه الحقوق.

5 تحديد نطاق واضح للتطبيق

ان تطبيق الحقوق والمبادئ المنصوص عليها في قانون حماية البيانات و التي تضمن حماية المستخدمين يجب أن تتم في جميع الأوقات. هذا يعني، على سبيل المثال، أنه إذا كانت المؤسسة تقدم خدمة عامة أو خاصة تنطوي على معالجة البيانات التي تستهدف المستخدمين في الاتحاد الأوروبي، فإن حقوق المستخدمين المدرجة بموجب قانون الاتحاد الأوروبي تكون ملزمة.

وفي العصر الرقمي، قد يكون من الصعب على المشرعين ضمان حماية كافية للبيانات الشخصية وحقوق المستخدمين دون تطبيق مبدأ تجاوز الحدود الإقليمية. لكي نتمكن من فهم فوائد توسيع نطاق الولاية القضائية لحماية المعطيات الشخصية، نحن بحاجة إلى النظر في المسألة لا من منظور "المؤسسة" (أين يقع الكيان؟) ولكن من وجهة نظر المستخدم (أين يوجد المستخدم وأي مكان هو؟). إن الهدف من قوانين حقوق الإنسان، مثل أطر حماية البيانات، هو أولا وقبل كل شيء حماية الأفراد في جميع الأوقات. ولذلك فمن المنطقي لضمان ذلك أن يتم احترام حقوق المستخدمين بغض النظر عن مكان وجود الكيانات التي تستخدم بيانات الأشخاص.

[20] انظر الفصل 3. الاتحاد الأوروبي، اللائحة 2016/679 / بشأن حماية الأشخاص الطبيعة
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
[21] الفصل 29 فرقة العمل المعنية بحماية البيانات، مبادئ توجيهية بشأن قابلية نقل البيانات
http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf
[22] ساندرا واشتر، برنت ميتلستادت ولوتشيانو فلوريدي، جامعة أوكسفورد، معهد أكسفورد للإنترنت. لماذا لا يوجد الحق في شرح صنع القرار الآلي في اللائحة العامة لحماية البيانات
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903469

كما أن تطبيق هذا النطاق الإقليمي ينطوي أيضا على إمكانية رفع مستوى الحماية للمستخدمين على الصعيد العالمي إذا بدأت الشركات والسلطات في تنفيذ تدابير حماية البيانات والخصوصية في ممارساتها اليومية في جميع أنحاء العالم. وفيما يتعلق بالمنافسة، يمكن لهذه التدابير القضائية أن تتجنب سباقا من الأسفل من حيث الحماية، حيث تقرر بعض الصناعات نقل شركاتها إلى خارج البلد لتجنب تطبيق تدابير حماية المستعملين.

ومن المهم أن نلاحظ مع ذلك أن توسيع نطاق اختصاص التشريع لا يخلو من المخاطر وينبغي أن ينظر فيه المشرعون بعناية. وقد ينشأ تضارب في القوانين، ويمكن لبعض الدول أن تسعى إلى توسيع نطاق التدابير التي تضر بالحقوق من خارج حدودها باستخدام نفس المبرر. وعلاوة على ذلك، لا يعرف كل كيان كيفية معالجة البيانات في جميع أنحاء العالم فكل قانون خاص بكل بلد. وكثيرا ما يكون من غير الواضح من عليه مسؤولية إبلاغ الشركات والأفراد بالتزاماتهم وحقوقهم. يجب القيام بحملات توعية لضمان أن الكيانات في جميع أنحاء العالم تعرف التزاماتها. ولكي تعمل قوانين حماية البيانات بشكل صحيح، تحتاج السلطات العامة إلى التوكيل والموارد اللازمة لتنفيذ التكوين العام. ان المجتمع المدني يمكن وينبغي أن يكون له دور حيوي في هذه العملية، ولا سيما لتمكين الناس من تفعيل حقوقهم.

وتوسيع نطاق الاختصاص ليس حلا أحاديا يناسب الجميع وينبغي وضع معايير محددة في قوانين حماية البيانات للحد من النسخ السيئة أو العواقب الضارة. فعلى سبيل المثال، يجب على المشرعين أن يشيروا بوضوح إلى السيناريوهات التي ينطبق عليها القانون خارج حدودهم، والى الجهات الفاعلة على وجه التحديد، وآليات التنفيذ التي سيتم تطبيقها، و غليها تزويد المستخدمين والشركات والسلطات بسبل واضحة لحل المشاكل.
وأخيرا، فإن الالتزامات المنصوص عليها في قانون حماية البيانات تنطبق بوضوح على كل من القطاعين الخاص والعام. وتقوم السلطات العامة بجمع معلومات الأفراد بشكل متزايد، والحصول على قواعد بيانات القطاع الخاص، أو بناء قواعد بيانات كبيرة للبيانات الشخصية. تخضع هذه المعالجة لالتزامات واضحة لحماية المعلومات الشخصية للأفراد، بالطريقة نفسها التي تخضع للمعالجة من قبل الكيانات الخاصة.

تجارب مفاوضات القانون العام لحماية المعطيات الشخصية

ويوسع نطاق القانون العام لحماية البيانات النطاق الإقليمي للقانون مقارنة بتوجيه حماية البيانات لعام 1995. وينطبق القانون العام لحماية البيانات على أي من الشركات والسلطات المنشأة في الاتحاد الأوروبي ولكن أيضا على الكيانات المنشأة خارج الاتحاد الأوروبي إذا كانت تشمل معالجة المعلومات الشخصية المتعلقة بتقديم السلع أو الخدمات الى المستخدمين الذين هم في الاتحاد الأوروبي، أو مراقبة سلوكهم.[23] هذا التغيير المهم في مجال تطبيق القانون يعكس تطور التشريع الأوروبي. ولعدة سنوات، تمت مقاضاة محاكم في الاتحاد الأوروبي لشركات التكنولوجيا الكبيرة التي رفضت الامتثال لقوانين حماية البيانات المحلية ، استنادا إلى مسائل الاختصاص. فقد أكدت جوجل وفيسبوك بشكل متكرربأنهما لا تشملها قوانين حماية البيانات في إسبانيا أوبلجيكا ، على سبيل المثال، ، لأنهما لم تنشأ رسميا في هذه البلدان. اتخذتا هذا الموقف على الرغم من أن الشركات كانت تعمل على تعدين واستغلال المعلومات الشخصية للمستخدمين في هذين البلدين[24] [25] وبتوسيع نطاق التطبيق الإقليمي، سعى القانون العام لحماية البيانات إلى الاستجابة لهذه الثغرات في حماية المستخدمين وتحقيق اليقين القانوني للمستخدمين. بيد أن هذا التغيير لا يخلو من تحديات لأنه ليس من الواضح كيف ستكون سلطات حماية البيانات في الاتحاد الأوروبي قادرة على تنفيذ إجراءات الإنفاذ تجاه الكيانات التي تقع خارج الاتحاد الأوروبي وبالتالي كيف ستحمي الحقوق بكل كفاءة.

[23] انظر الفصل 3. الاتحاد الأوروبي، اللائحة 2016/679 / بشأن حماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية وحرية تنقل هذه البيانات وإلغاء التوجيه 95/46 / إيك (اللائحة العامة لحماية البيانات)
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
[24] محكمة العدل، الاتحاد الأوروبي، الحكم في قضية ىي غوغل إسبانيا ضد ماريو كوستيجا غونزاليس، 13 مايو 2014
http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d5eb572d024de-249578524881c67efe5ec.e34KaxiLc3eQc40LaxqMbN4PaN0Te0?text=&docid=152065&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=574499
[25] رويترز، فيسبوك يفوز بقضية الخصوصية ضد البلجيكية هيئة حماية البيانات، يونيو 2016.
https://www.reuters.com/article/us-facebook-belgium-idUSKCN0ZF1VV

6 إنشاء آليات ملزمة وشفافة لنقل البيانات بشكل آمن إلى بلدان ثالثة

تم تصميم أطر حماية البيانات لضمان التدفق الحر للبيانات من خلال إنشاء آليات مناسبة لنقل البيانات والضمانات الفعالة لحقوق المستخدمين. ويجب وضع هذه الآليات تحت رقابة صارمة وشفافة وتشمل سبل انتصاف فعالة لضمان حقوق المستخدمين في السفر مع البيانات.

تجربة من القانون العام لحماية المعطيات الشخصية

وفي إطار القانون العام لحماية المعطيات الشخصية، لا يمكن نقل البيانات عبر الحدود خارج المنطقة الاقتصادية الأوروبية إلا إذا تم نقلها إلى بلد منح وضع كفاية أو عندما تكون هناك آلية قانونية لنقل البيانات[26] . ويتيح القانون العام لحماية البيانات المزيد من آليات النقل من التوجيه لعام 1995 من خلال مدونات قواعد السلوك وخطط إصدار الشهادات. ويوفر هذا النهج للشركات مرونة أكبر. وستكون الرقابة الفعالة وإنفاذ هذه الآليات حاسمة لضمان حماية حقوق المستخدمين أثناء النقل وبعده.

وفيما يتعلق بالكفاية، تتمتع المفوضية الأوروبية بسلطة تحديد ما إذا كان بلد ثالث يكفل مستوى كاف من الحماية بسبب قانونه الداخلي أو بسبب الالتزامات الدولية التي أقرها، مما يسمح بتصدير البيانات إلى تلك الولاية القضائية. يمكن لأي بلد التقدم بطلب للحصول على قرار الكفاية التي ستطلق عملية مراجعة أجريت وفقا لتقدير اللجنة الأوروبية. وفي الوقت الحالي، منح الاتحاد الأوروبي كفاية للبلدان التالية[27]: الأرجنتني وهندوراس وكندا وسويسرا وجزر فارو غويرنسي ودولة إسرائيل وجزيرة ماين وجيرزي ونيوزيلندا والولايات المتحدة الأمريكية و جمهورية أوروغواي الشرقية . إن الالتزام باتفاقية المجلس الأوروبي عدد 108 له أهمية خاصة في هذا الصدد، وهو أحد العناصر التي تؤخذ في الاعتبار عند تقييم منح الكفاية.

في سنة 2016 ، فقدت الولايات المتحدة الترتيب المسمى "الملاذ الآمن" الذي استند إليه تحديد مدى كفايتها بسبب عدم الامتثال لقانون حقوق الإنسان الأساسية للاتحاد الأوروبي.[28] ولا تزال صحة عدة عناصر من ترتيبها الجديد (درع الخصوصية التابع للاتحاد الأوروبي والولايات المتحدة) قيد التدقيق[29] وقد طلبت بلدان أخرى مثل أستراليا قرارا بشأن الكفاية ولكنها أخفقت حتى الآن في تلبية الاحتياجات اللازمة[30] وأخيرا، تجري حاليا مفاوضات مع اليابان بشأن المراجعة والكفاية الجديدة.[31]

[26] نأظر الفصل 5. الاتحاد الأوروبي، اللائحة رقم 2016/679 / بشأن حماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية وحرية تنقل هذه البيانات وإلغاء التوجيه 95/46 / إيك (اللائحة العامة لحماية البيانات)
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
[27] Eمفوضية الاتحاد الأوروبي، قرارات اللجنة بشأن كفاية حماية البيانات الشخصية في بلدان ثالثة s
http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm
[28] أكسيس ناو، سجيو تعلن أن مرفأ الآمن غير صالح
/https://www.accessnow.org/cjeu-declares-safe-harbour-invalid
[29] Access Now, Comments to EU Commission on Privacy Shield review https://www.accessnow.org/cms/assets/uploads/2017/07/AN-PSReviewResponse-1.pdf
[30] المفوضية الأوروبية، دغ العدل، دراسة مقارنة حول المناهج المختلفة للتحديات الخصوصية الجديدة، لا سيما في ضوء التطورات التكنولوجية
http://ec.europa.eu/justice/data-protection/document/studies/files/new_privacy_challenges/final_report_country_report_b2_australia.pdf
[31] المفوضية الأوروبية، البيان المشترك الذي أدلى به نائب الرئيس أندروس أنسيب والمفوض فيرا جورافا بشأن الحوار حول حماية البيانات وتدفقات البيانات مع اليابان، آذار / مارس2017
http://europa.eu/rapid/press-release_STATEMENT-17-690_en.htm

7 حماية أمن ونزاهة البيانات

لتجربة فوائد الاقتصاد الرقمي، يحتاج المستخدمون إلى أن يكونوا قادرين على الثقة في الخدمات التي يستخدمونها عبر الإنترنت. أي معطيات شخصية يتم مشاركتها تولد خطرا. ولذلك، من المهم على نحو متزايد ضمان أن يتم النظر في حماية الخصوصية والبيانات من قبل المهندسين في مرحلة تصميم المنتج والخدمات، وأنها وضعت على أعلى معايير الحماية افتراضيا; هذا هو مفهوم حماية البيانات حسب التصميم وبشكل افتراضي. وينبغي أن ينص القانون على هذه المفاهيم التي تقتضي من الكيانات أن تعتمدها.

تجربة من مفاوضات القانون العام لحماية المعطيات الشخصية

ويقيس القانون العام لحماية المعطيات الشخصية مبادئ حماية البيانات حسب التصميم، وبصورة افتراضية توفر عددا كبيرا من الفوائد، مثل المساهمة في أمن البيانات وسلامتها[32] . تتخذ السڑكات نهجا إيجابيا لحماية حقوق المستخدمين، مع الخصوصية وحماية البيانات حسب التصميم وبشكل افتراضي، من خلال تضمين مبادئ حماية الخصوصية في كل من التكنولوجيا والسياسات التنظيمية. تصبح الخصوصية وحماية البيانات جزءا من إطار الثقافة والمساءلة، بدلا من كونها عنصر "بسيط" للامتثال. وهذا يتطلب التفكير في الخصوصية وحماية البيانات من بداية عملية تطوير منتج أو خدمة.[33] يمكن لهذا النهج أن يساعد السڑكات على توفير تكاليف تطوير المنتجات أو الخدمات. ونظرا لأن فرق المهندسين والتنمية سوف تنظر في الخصوصية وحماية البيانات في بداية مرحلة التطوير، سيكون هناك تعديلات أقل يجب إجراؤها عندما يستعرض فريق قانوني المنتج النهائي. كما أنه يقلل من خطر مقاضاة الشركة بسبب انتهاكات الخصوصية أو يعاني من ضرر السمعة بسبب تسرب البيانات، حيث أنها ستكون قادرة على إثبات التزامها بحقوق المستخدمين. باختصار، يمكن أن يساعد الانتقال من فهم الخصوصية وحماية البيانات كمسألة امتثال لتضمين الخصوصية وأمن البيانات حسب التصميم وبشكل افتراضي الشركات على زيادة الثقة في خدماتها.

8 تطوير آليات منع انتهاك البيانات والإبلاغ عنها

وحيث أنه ينبغي أن تشجع أطر حماية البيانات التدابير التي تعزز أمن وسلامة البيانات، إلا أن خروقات البيانات لا تزال قائمة. ولذلك، يجب وضع تدابير لمعالجة هذه المشاكل وإشعار المستخدمين لها.وقد اكتسبت خروقات البيانات اهتماما واسع النطاق حيث أصبحت الشركات من جميع الأحجام تعتمد بشكل متزايد على الحوسبة السحابية والخدمات عبر الإنترنت.مع البيانات الشخصية والحساسة المخزنة على الأجهزة المحلية وعلى خوادم سحابة، أصبح خرق شبكة وأمن المعلومات جذابا لأولئك الذين يسعون إلى فضح أو استغلال المعلومات الخاصة أو طلب فدية.وقد وجدت خروقات البيانات ما دام يتم الاحتفاظ بسجلات الأفراد الخاصة وتخزينها. قبل العصر الرقمي، كان يمكن أن يكون خرق البيانات أمرا بسيطا مثل عرض ملف الفرد دون إذن، أو العثور على وثائق لم يتم التخلص منها بشكل صحيح.[34] لكن مع رقمنة السجلات وتزايد البيانات الشخصية ، فإن حجم البيانات تجاوز الإختراقات، مما يعرض المعلومات الشخصية للمستخدمين لخطر أكبر.

[32] انظر افصل 25. الاتحاد الأوروبي، اللائحة 2016/679 / بشأن حماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية وحرية تنقل هذه البيانات وإلغاء التوجيه 95/46 / إيك (اللائحة العامة لحماية البيانات)
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

[33] لمزيد من المعلومات حول الخصوصية من تصميم انظر آن كافوكيان، الخصوصية من خلال التصميم، 7 المبادئ التأسيسية
https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

[34] نيت لورد، تاريخ خروقات البيانات، يوليو
https://digitalguardian.com/blog/history-data-breaches

ولمنع هذه المخاطر والتخفيف من حدتها، ينبغي بالتالي وضع آليات لإخطار انتهاك المعلومات ومنع حدوث مثل هذه الانتهاكات، سواء في إطار حماية البيانات أو في تشريعات تكميلية. وقد أدت الحوادث البارزة في فقدان البيانات الشخصية أو السرقة في جميع أنحاء العالم إلى إجراء نقاش واسع النطاق بشأن مستوى الأمن المقدم إلى المعلومات الشخصية التي تمت مشاركتها ومعالجتها وتخزينها ونقلها إلكترونيا. وفي هذا السياق، يمثل اكتساب ثقة المستخدمين والحفاظ على أمان بياناتهم وحمايتها تحديا رئيسيا للمنظمات. وقد سجل مركز تبادل حقوق الخصوصية للمنظمات غير الحكومية 7,619 مخالفة للبيانات تم نشرها منذ عام2005 في الولايات المتحدة وحدها[35] . وهذا يعني أن ما لا يقل عن 926,686,928 سجلا خاصا قد تم اختراقها في الولايات المتحدة منذ ذلك الحين. وتقول آي بي إم وبونيمون إنستيتيوت أنه في عام 2017 ، بلغ متوسط التكلفة العالمية لخرق البيانات 3.62 مليون دولار[36] . وفي حني أن هذه التكلفة قد انخفضت بشكل طفيف مقارنة بالعام الماضي، فإن الدراسة تبني أن الشركات تواجه انتهاكات أكبر. وتقدر دراسات أخرى أن متوسط تكلفة خرق البيانات سيتجاوز 150 مليون دولار بحلول عام 2020، مع توقع أن تبلغ التكلفة السنوية العالمية 2.1 تريليون دولار.[37] وهذا يعني أن منع وتخفيف خروقات البيانات ليست جيدة فقط للمستخدمين، ولكن أيضا جيدة للشركات من أجل توفير التكاليف.

تجربة من مفاوضات القانون العام لحماية المعطيات الشخصية

وقد أدخلت متطلبات إخطار انتهاك البيانات في الاتحاد الأوروبي لقطاع الاتصالات الإلكترونية في عام 2002.[38] التي تم تطويرها منذ ذلك الحين حتى يتم تنسيق هذه التدابير في إطار القانون العام لحماية البيانات لتسهيل الامتثال للمنظمات.

وتتطلب التدابير المعتمدة في إطار القانون العام لحماية البيانات أن تقوم المنظمة بالإبلاغ عن خرق بيانات "دون تاخير غير مبرر"، وأن يكون ذلك ممكنا في غضون 72 ساعة بعد علمها بالحادث[39] .وإذا كان من الواضح أن الهدف من التدبير هو ضمان الإبلاغ عن انتهاكات البيانات في أسرع وقت ممكن، فإن التعبير عن ذلك لا يزال غامضا.ثم يصف القانون العام لحماية البيانات الخطوات التي يجب أن تتبعها أي منظمة تواجه خرقا وتنص على إمكانية إبلاغ المستخدمين. وهذه الإخطارات إيجابية من منظور المساءلة والشفافية، وهي أيضا حاسمة لضمان أن يمكن للمستخدمين اتخاذ الإجراءات المناسبة لتأمين معلوماتهم والسعي إلى الانتصاف إذا لزم الأمر.ومع ذلك، فإن القانون العام لحماية البيانات يترك للمنظمات إمكانية تحديد ما إذا كان ينبغي إخطار المستخدمين بالخرق استنادا إلى تقييمهم المخاطر الخاصة بحقوق المستخدمين وحرياتهم. يجب أن يكون الإشعار للمستخدمين شرطا لأي خرق للبيانات الشخصية، والذي يتضمن ليس فقط معلومات المشترك، ولكن البيانات الشخصية الأخرى مثل الصور.يجب أن يكون الإخطار في الوقت المناسب، سهل الفهم، وشامل، ويجب الإشارة إلى خيارات المعالجة بوضوح وبطريقة يمكن النفاذ إليها بسهولة من خلال ترك الكثير من السلطة التقديرية للمنظمات، فإن هذا الحكم يفشل في تمكين المستخدمين من السيطرة على معلوماتهم. فالمنظمات التي تعاني من خرق المعطيات الشخصية لها مصلحة اقتصادية واضحة في التقليل من المخاطر المرتبطة بالانتهاك وعدم إخطار المستخدمين، مما قد يؤدي إلى انتهاكات غير محمية لمعالجة البيانات.ونحن نشجع المشرعين في جميع أنحاء العالم لتجنب تلك العيوب وتطوير آليات لا لبس فيها لمنع خرق البيانات والإخطار.

[35] Privacy Rights Clearinghouse, Data Breaches. https://www.privacyrights.org/data-breaches

[36] معهد بونيمون ل عب، 2017 تكلفة دراسة خرق البيانات: نظرة عامة عالمية
https://www.ibm.com/security/data-breach

[37] The Experian, Data Breach Industry Forecast, 2015.
https://www.experian.com/assets/data-breach/white-papers/2015-industry-forecast-experian.pdf

[38] لاتحاد الأوروبي، التوجيه 2002/58 / إيك للبرلمان الأوروبي والمجلس المؤرخ 12 جويلية 2002 بشأن تجهيز البيانات الشخصية وحماية الخصوصية في قطاع الاتصالات الإلكترونية (التوجيه المتعلق بالخصوصية والاتصالات الإلكترونية)
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML

[39] أنظر المادتي 33 و 34. الاتحاد الأوروبي، اللائحة رقم 2016/679 / يو بشأن حماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية وحرية تنقل هذه البيانات وإلغاء التوجيه 95/46 / إيك (حماية البيانات العامة اللائحة)
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

9 إنشاء سلطة مستقلة وإنشاء آليات قوية لإنفاذ القانون

لا يمكن لإطار حماية البيانات أن يكون كاملا من دون آلية قوية (تشمل إنشاء سلطة إشرافية مستقلة) سلطة أو هيئة لحماية المعطيات الشخصية. وحتى أفضل قانون لحماية البيانات في العالم لن يكون لديه أي معنى إذا لم تكن لديه سلطة تتمتع بالصلاحيات والموارد لرصد التنفيذ وإجراء التحقيقات ومعاقبة الكيانات في حالة حدوث انتهاكات (متكررة أو مهملة أو متعمدة) لحماية المعطيات الشخصية.

و يجب إيجاد غرامات عقابية، لكن يجب أن تفرض سلطات حماية البيانات غرامات محدودة على الشركات، ولا سيما المؤسسات الصغيرة والمتوسطة الحجم التي لا تشارك في معالجة بيانات هامة، ولا تملك الوسائل اللازمة لفهم التزاماتها باحترام قانون حماية البيانات ، و كانت قد ارتكبت أخطاء جراء الجهل لا جراء الخداع. كما تبذل الحكومة جهودا للتوعية من أجل تجنب الحالات التي تكون فيها الشركات جاهلة بوجود قوانين حماية البيانات وأهميتها. وتقترح تونس، التي تناقش حاليا أول قانون لحماية البيانات على الإطلاق، نهجا تدريجيا مبتكرا للجزاءات يشمل غرامات أعلى في حالات العود[40] . ونتيجة لذلك، فإن الشركة التي تبث أنها ارتكبت انتهاكات لحماية البيانات التي سبق أن أقرت بها ستحصل على غرامة أعلى بكثير.

بيد أن الجزاءات والغرامات لا تمثل إلا جزءا صغيرا من عمل اتفاقات العمل. إن دور سلطات حماية البيانات هو بالطبع إنفاذ قوانين حماية البيانات والرقابة ولكن أيضا لمساعدة المنظمات في واجباتها المتعلقة بالامتثال.

ويعني ذلك أن تتعاون الشركات والسلطات العامة والمنظمات غير الحكومية مع سلطات حماية البيانات لفهم واجبات كل طرف والتزاماته. وينبغي ألا تتردد المنظمات في إقامة اتصال مع إدارة الشؤون السياسية التابعة لها التي يمكن أن توفر لها الموارد والمواد اللازمة للمساعدة في تنفيذ القانون.

وأخيرا، تتمتع إدارة الشؤون السياسية بالصلاحيات اللازمة لبدء تحقيقات مستقلة في المنظمات والاستماع إلى القضايا التي يقدمها إليها أفراد أو منظمات غير حكومية. ومن هذا المنطلق، تعمل إدارة الشؤون السياسية كحارس لحقوق المستخدمين ويمكن أن تساعد في حماية الحقوق الأساسية. غير أن هذه السلطات لا تزال غير معروفة إلى حد كبير من قبل المستخدمين في جميع أنحاء العالم. وللمزيد من المساعدة في حماية حقوق المستخدمين، ينبغي تمكين المنظمات غير الحكومية لتمثيل المستخدمين وتقديم القضايا بشكل مستقل أمام إدارة الشؤون السياسية والمحاكم. كما ينبغي للحكومات أن تواصل تعزيز عمل اتفاقات العمل الوطنية، وأن تفسر دورها، وتزودها بميزانية كافية لضمان أن تكون اتفاقات سياسات التنمية قادرة على الوفاء بواجباتها.

تجربة من مفاوضات القانون العام لحماية المعطيات الشخصية

ان لدى الاتحاد الأوروبي والدول الأعضاء فيه قوانين لحماية البيانات منذ ما يقرب من 30 عاما. وعلى الرغم من ذلك، كانت العديد من الشركات تتجاهلها بسبب عدم وجود سلطات إنفاذ لسلطات حماية البيانات ومستوى منخفض نسبيا من الغرامات (تصل إلى150.000 €)[41] . لعدة سنوات في أوروبا، كثيرا ما نصح المستشارون القانونيون الشركات بعدم الامتثال لقانون حماية البيانات في الاتحاد الأوروبي، حيث أن خطر الغرامة كان أقل من المبلغ الذي يتعين عليهم دفعه .[42] وقد تم تناول هذا التجاهل الصارخ للحقوق الأساسية في إطار القانون العام لحماية البيانات عن طريق رفع مستوى الغرامة إلى حد أقصى قدره 4٪ من معدل دوران الشركة في جميع أنحاء العالم[43] . كما تم توضيح الصلاحيات التنفيذية وأداء اتفاقات العمل الوطنية وتنسيقها. وسيتم الآن جمع هذه الاتفاقات داخل مجلس حماية البيانات الأوروبي الذي يسمح لها بإجراء تحقيقات مشتركة في مختلف بلدان الاتحاد الأوروبي على سبيل المثال.

[40] السلطة الوطنية التونسية لحماية البيانات الشخصية. المادة 211 مسرّوع قانون بشأن حماية البيانات الشخصية، 2017 ،
http://www.inpdp.nat.tn/Projet_PDP_2017.pdf

[41] الإتحاد الأوربي. والتوجيه 95/46 / إيك الصادر عن البرلمان الأوروبي والمجلس المؤرخ 24 تسرين الأول / أكتوبر 1995 بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية وحرية تنقل هذه البيانات
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046

[42] انظر مناقشة الفريق في الكمبيوتر والخصوصية وحماية البيانات، بروكسل،
https://www.youtube.com/watch?v=sikwHfoiylg

[43] انظر الفصلي 7 و 8. الاتحاد الأوروبي، اللائحة رقم 2016/679 / يو بشأن حماية الأشخاص الطبيعيي فيما يتعلق بمعالجة البيانات الشخصية وحرية تنقل هذه البيانات وإلغاء التوجيه 95/46 / إيك (حماية البيانات العامة اللائحة)
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

10 مواصلة حماية البيانات والخصوصية

ويعد وجود قانون شامل معلما بارزا، ولكنه لا يعني أن الحكومات يجب أن تكتفي هنا بحماية البيانات الشخصية والخصوصية. ومن المحتمل أن تظهر تحديات جديدة للخصوصية وحماية البيانات خلال مراحل التنفيذ حتى لو كانت الحكومات تهدف إلى جعل القوانين "واقية من المستقبل".وهذا يعني أنه من المرجح أن تكون عملية المراجعة ضرورية، وهي فرصة عظيمة لتحديث القانون ومعالجة أي مشاكل محتملة مع الامتثال وتوفير مزيد من الوضوح واليقين القانوني عند الحاجة.

ومن المهم أيضا أن نفهم قانون حماية البيانات كحد أدنى وليس سقفا في حماية حقوق المستخدمين. وهذا يعني أن المنظمات يجب أن تمتثل للقانون، كحد أدنى، ولكن ينبغي أيضا تشجيعها على تجاوز واتخاذ المزيد من الإجراءات لحماية خصوصية الناس. وبالمثل، يمكن أن تؤخذ في الاعتبار نهج مختلف لحماية البيانات وخصوصيتها، تبعا لهيكل وشكل حكومة بلد ما. على سبيل المثال، في الولايات المتحدة، يجب على الحكومة الاتحادية ألا تمنع الحكومات المحلية والدول من توفير الحماية للمستخدم، بالإضافة إلى التدابير المحدودة المقدمة على المستوى الاتحادي، والامتناع عن استخدام سلطتها لاستباق القوانين الإقليمية والمحلية[44] ، في حالة الاتحاد الأوروبي، تتجنب الدول الأعضاء وضع قواعد إضافية لأن ذلك من شأنه أن يؤدي إلى تفتيت مستوى الحماية المنسق للمستعملين المتفق عليه في القانون العام لحماية المعطيات الشخصية.

تجربة من مفاوضات القانون العام لحماية المعطيات الشخصية

منذ عام 1995 ، تبنت الدول الأعضاء في الاتحاد الأوروبي قوانين محلية مختلفة لحماية البيانات استنادا إلى المعيار الذي وضعه توجيه الاتحاد الأوروبي لحماية البيانات. وقد اكتمل قانون الاتحاد الأوروبي في الوقت الذي كان فيه 1٪ فقط من السكان على الإنترنت، وكان في حاجة ماسة إلى التحديث عندما اقترحت مفوضية الاتحاد الأوروبي لائحة حماية البيانات العامة للاتحاد الأوروبي في عام 2012.[45] استغرق الأمر حوالي خمس سنوات من المفاوضات من أجل موافقة المشرعين على التدابير الجديدة في القانون التي ستصبح قابلة للتطبيق مباشرة اعتبارا من أيار / مايو 2018 (على خلاف التوجيه الذي يلزم نقله إلى القانون الوطني، فإن اللائحة قابلة للتنفيذ مباشرة). وسوف يتم تعويض جميع القوانين الوطنية المتعلقة بحماية البيانات البالغ عددها ٢٨ بقانون وحيد ينص على حقوق وقواعد منسقة في جميع أنحاء الاتحاد الأوروبي. ان هذا النظام يعمل بموجب النظام القانوني للاتحاد الأوروبي، لكنه قد لا يكون السيناريو المثالي في مناطق أو بلدان أخرى. ويمكن أن يكون من الصعب الاتفاق على القوانين التي تتجاوز الحدود الوطنية وقد لا تكون بالضرورة أفضل وسيلة لحماية المستخدمين. وبالتالي لا يوجد نموذج مثالي للقانون ولكن جميع قوانين حماية البيانات تأخذ بعين الاعتبار جميع النقاط الواردة في هذه المقالة.

[44] EPIC, Privacy preemption watch. https://epic.org/privacy/preemption/
[45] المفوضية الأوروبية، إصلاح قواعد حماية البيانات في الاتحاد الأوروبي، 2012
http://ec.europa.eu/justice/data-protection/reform/index_en.htm

ما يجب اجتنابه

أدناه سوف تجد خمس توصيات لصانعي السياسة التي يجب اتباعها عند وضع قانون حماية البيانات. وننصح بالحذر بشأن العناصر الخمسة التالية التي يمكن أن تقلل من فوائد القانون المقترح أو تضر بحقوق الأفراد إذا ما تم تجاهلها.

1 لا تسعى إلى حماية البيانات و تقييد خصوصيات الأمن القومي

الحكومات ليس لديها التزام فقط ولكن أيضا مصلحة أمنية في ضمان حماية البيانات الشخصية، وعلى وجه الخصوص عندما تكون المعلومات تحتفظ بها الوكالات الحكومية.ففي سنة 2015 ، ونتيجة لحوادث الأمن السيبراني في الولايات المتحدة، تم سرقة 21.5 مليون سجل الموظفين الاتحاديين وأفراد الأسرة المخزنة في مكتب إدارة شؤون الموظفين[46] . ومع تزايد هذه الأنواع من الحوادث والهجمات على الصعيد العالمي، يجب على البلدان أن تتخذ تدابير لحماية معلومات الأفراد بشكل أفضل.

وعلى الرغم من ذلك، غالبا ما تسعى الحكومات إلى فرض قيود على حماية البيانات وحقوق الخصوصية لاستخدامها الشخصي للبيانات الشخصية من خلال طلب استثناءات واسعة النطاق. ويجب أن تقتصر هذه الاستثناءات على تدابير واضحة ومحددة ومتناسبة تشمل الإشراف القضائي وآليات الانتصاف التي يمكن النفاذ إليها.وينبغي على التشريعات ألا تعطي الحكومات والهيئات العامة القدرة على حماية نفسها من واجب حماية حق المستخدمين في حماية البيانات. ولدى البلدان مصلحة أمنية في حماية البيانات الشخصية التي تحتفظ بها الوكالات الحكومية.

تجربة من مفاوضات القانون العام لحماية البيانات

ويعرض هذا التقرير قائمة بالأسباب التي يمكن للدول الأعضاء أن تعتمد عليها لتقييد حقوق وحريات المستخدمين المحميين بموجب القانون، مثل الأمن القومي أو الدفاع[47] . ومع أنه من الشائع إيجاد أحكام تسمح للدول بتقييد الحقوق في كل قطعة من الاتحاد الأوروبي والتشريعات الوطنية، فإن لغة هذه الأحكام غالبا ما تكون غامضة بشكل مقصود ويمكن أن تغطي طائفة واسعة من أنشطة الدولة. وعلى سبيل المثال، يسمح القانون العام لحماية البيانات بالقيود المفروضة على الحقوق من أجل "أهداف مهمة أخرى ذات أهمية عامة للاتحاد أو لدولة عضو". ونظرا لأثر هذه القيود على حقوق المستخدمين وحرياتهم ، ينبغي أن تكون محددة بوضوح وايضا محددة في القانون، وان تخضع لمعايير الشفافية والرقابة الصارمة، وأن تكون تدابير ضرورية ومتناسبة في مجتمع ديمقراطي.

2 لا تسمح بمعالجة البيانات الشخصية استنادا إلى المصلحة المشروعة للشركات دون قيود صارمة

وكثيرا ما تجادل الشركات بأنه ينبغي أن يكون لها الحق في جمع ومعالجة بيانات المستخدمين، عندما تكون هذه "مصلحتها المشروعة"، دون الحاجة إلى إخطار المستخدمين. وما لم تعرَّف هذه الاستثناءات بأنها استثناءات (ليست الحالة في إطار القانون العام لحماية البيانات أو توجيه عام 1995) وتعرف تحديدا ضيقا (وهو ما يتحقق على نحو أفضل في القانون العام لحماية البيانات)، فلا ينبغي السماح بذلك. وإلا، فإن هذا يتناقض جوهريا مع هدف حماية البيانات، وهو وضع المستخدمين في السيطرة على معلوماتهم. ويجب منع هذه المحاولات للحد من حقوق المستخدمين.

[46] اتريشيا زنجرل، ميغان كاسيلا، الملايني المزيد من الأمريكيني ضرب من قبل موظفي الحكومة الإختراق البيانات، رويترز، 2015 .46
https://www.reuters.com/article/us-cybersecurity-usa/millions-more-americans-hit-by-government-personnel-data-hack-idUSKCN0PJ2M420150709

[47] انظر المادة 23. الاتحاد الأوروبي، اللائحة رقم 2016/679 / يو بشأن حماية الأشخاص الطبيعيني فيما يتعلق بمعالجة البيانات الشخصية وحرية تنقل هذه البيانات وإلغاء التوجيه 95/46 / إيك (اللائحة العامة لحماية البيانات)

تجربة من مفاوضات القانون العام لحماية البيانات

إن المصلحة المشروعة للمنظمات هي أحد الأسس القانونية التي يمكن استخدامها لمعالجة البيانات الشخصية في إطار القانون العام لحماية البيانات[48] . ويتمثل جوهر حماية البيانات في مراقبة المستخدمني , وتوقعاتهم بشأن استخدام بياناتهم. ويتنافى حكم المصلحة المشروعة مع هذه المبادئ. و بموجب "المصلحة المشروعة"، يؤذن للمنظمة بجمع واستخدام المعلومات الشخصية دون الاضطرار إلى إبلاغ المستخدمين المعنيين. إذا كنت لا تعرف أن الكيان يحمل بيانات عنك، كيف يمكنك ممارسة حقك في النفاذ إلى البيانات أو حقك في الاعتراض؟

وكان هذا الحكم من أكثر المسائل التي جرت مناقشتها خلال المفاوضات بشأن القانون العام لحماية البيانات. وقد كانت الشركات تدافع عن حكم واسع وغامض التعريف للمصلحة المشروعة، و المجتمع المدني كان يحاول إزالته أو الحد بشكل كبير من نطاقه. حاول المشرعون الحد من تأثير الحكم في الأشهر الأخيرة من المفاوضات من خلال تضمين الشرط مطالبة الشركات بتحقيق التوازن بين مصلحتها المشروعة والحقوق الأساسية. في حين أن النية جديرة بالثناء، فإن الشركات إجراء هذا التقييم وفقا لتقديرهم الخاص ويمكن عدم إشعار المستخدمين بذلك. والنتيجة النهائية لا ترضي أحدا لأن الشركات أرادت مزيدا من المرونة مما هو منصوص عليه في النص وما يقابلها من حجج، وأرادت المنظمات غير الحكومية فرض قيود واضحة. ونحن نفهم الحاجة إلى تزويد الشركات بالتدابير التي تسمح لها بإجراء الأعمال التجارية، ومع ذلك، فإن التدابير التي تمنع المستخدمين من التحكم في معلوماتهم الشخصية سوف يتم استثناءها لأنها تتعارض مع روح وهدف قانون حماية البيانات. وكان هذا الحكم من أكثر المسائل التي جرت مناقشتها خلال المفاوضات بشأن القانون العام لحماية البيانات. وكانت الشركات تدافع عن حكم واسع وغامض التعريف للمصلحة المشروعة، ويحاول المجتمع المدني إزالته أو الحد بشكل كبير من نطاقه. حاول المشرعون الحد من تأثير الحكم في الأشهر الأخيرة من المفاوضات من خلال تضمين الشرط مطالبة الشركات بتحقيق التوازن بين مصلحتها المشروعة والحقوق الأساسية. في حين أن النية جديرة بالثناء،فإن الشركات ستقوم باجراء هذا التقييم ويمكن أن يبقى المستخدمون في الظلام (يمكن أن يتم عدم إعلام المستخدمين بهذا الشأن).والنتيجة النهائية غير مرضية لأحد لأن الشركات أرادت مزيدا من المرونة مما هو منصوص عليه في النص وما يقابلها من حجج، و المنظمات غير الحكومية أرادت فرض قيود واضحة. ونحن نفهم الحاجة إلى تزويد الشركات بالتدابير التي تسمح لها بإجراء الأعمال التجارية، ومع ذلك، فإن التدابير التي تمنع المستخدمين من التحكم في معلوماتهم الشخصية يجب أن تستثنى لأنها تتعارض مع روح وهدف حماية المعطيات الشخصية.

3 لا تنشئ "الحق في النسيان"

ويظهر "الحق في النسيان" أو "الحق في إلغاء القائمة" من قانون حماية البيانات في الاتحاد الأوروبي بما في ذلك حكم "غوغل اسبانيا"[49] . ويتيح هذا الحق للمستخدمين في ظروف معينة أن يطلبوا من محركات البحث إلغاء عناوين الويب من النتائج عندما يتم البحث باستخدام أسمائهم. ولا ينبغي الخلط بين هذا الحق وبين الحق في المحو الذي يسمح للأفراد بحذف جميع البيانات الشخصية المتعلقة بهم عندما يغادرون الخدمة أو التطبيق. الحق في المحو أمر ضروري لضمان سيطرة المستخدم على المعلومات الشخصية. كما يجب عدم الخلط بينه وبين أي تدبير من إجراءات الإبطال نظرا لأن الحق في النسيان الذي تم تطويره بموجب الفقه القانوني في الاتحاد الأوروبي لا يتطلب أو يطلب أي محتوى عبر الإنترنت يتم إزالته من الويب أو من فهارس محرك البحث.

والطريقة التي تفسر بها عدة حكومات على الصعيد الدولي، بطريق الخطأ أو غير ذلك، الحق في الشطب أو السعي إلى توسيع نطاقها للحد من حرية التعبير أو المعلومات تشكل تهديدا كبيرا لحقوق الإنسان. وقد أبدت المحاكم والمشرعين في جميع أنحاء العالم اهتماما كبيرا بوضع تدابير لإرساء "الحق

[48] انظر المادة 6. 1 (و). الاتحاد الأوروبي، اللائحة رقم 2016/679 / يو بشأن حماية الأشخاص الطبيعيني فيما يتعلق بتجهني البيانات الشخصية وحرية تنقل هذه البيانات وإلغاء الأمر التوجيهي 95/46 / إيك (اللائحة العامة لحماية البيانات n)
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

[49] محكمة العدل في الاتحاد الأوروبي، الحكم في قضية غوغل إسبانيا بيى ضد ماريو كوستيجا غونزاليس، 13 مايو 2014
http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d5eb572d024de-249578524881c67efe5ec.e34KaxiLc3eQc40LaxqMbN4PaN0Te0?text=&docid=152065&pageIn-dex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=574499

في النسيان" الذي ينحرف كثيرا عن النهج الذي وضعته محاكم الاتحاد الأوروبي، وتفويض إزالة المحتوى[50] [51] [52] أي ما يسمى "الحق في النسيان" التدبير الذي من شأنه أن يؤدي إلى حذف المحتوى عبر الإنترنت هو سوء تفسير جسيم للحق. ولا يجوز تحت أي ظرف من الظروف تطبيق الحق في إلغاء القائمة للتمكين من إزالة المحتوى. وبالمثل، لا يجوز لسلطات حماية البيانات أن تطلب حذف المعلومات على الإنترنت دون إشراف قاض يمكنه ضمان احترام جميع الحقوق الأساسية، بما في ذلك الحق في حرية التعبير وحرية النفاذ إلى المعلومات.

اكساس ناو تعارض أي تطوير من قبيل "الحق في النسيان". ومع ذلك، فإن حق إلغاء قائمة مماثلة لتلك القائمة في الاتحاد الأوروبي كان من المقرر أن ينظر فيها المشرعون، وقد حددت أكسس ناو سلسلة من الضمانات القانونية التي يجب أن يضعها المشرعون لمواصلة تخفيف مخاطر الإيذاء وانتهاك حقوق الإنسان.[53]

تجربة من مفاوضات القانون العام لحماية البيانات

وأضيف الحق في أن ينسى إلى الحق في الشطب في إطار القانون العام لحماية البيانات.[54] إن الحق في أن ينسى يقنن الاجتهاد القضائي لمحكمة العدل الأوروبية في قضية "غوغل إسبانيا" [55] . وقد وضعت المحكمة مجموعة من المعايير لمحركات البحث للنظر فيها عندما تتلقى طلبا للشطب. يجب على محركات البحث أن تمنح طلب رفع الأسماء من القائمة فقط إذا كانت المعلومات الشخصية المضمنة في عنوان الويب المعين "غير ملائمة أو لم تعد ذات صلة أو مفرطة"، و لا يتم ذلك الا إذا كانت المعلومات لا تتعلق بشخصية عامة أو ليست من المصلحة العامة. ومع ذلك، لا يجوز إزالة المعلومات أو الروابط من فهرس البحث. ويجب أن تظل متاحة عند إجراء المستخدمين لعمليات البحث باستخدام مصطلحات أخرى غير اسم الفرد الذي يقدم طلب رفع الأسماء من القائمة. والأهم من ذلك، يوضح القانون العام لحماية البيانات أيضا أن المعلومات لا يجوز شطبها إذا كان ذلك ضروريا لممارسة الحق في حرية التعبير والمعلومات.

وعلى الرغم من هذه الضمانات، فإن المزيد من التوجيه من الاتحاد الأوروبي والدول الأعضاء ضروري لضمان عدم امتثال او تجاوز محركات البحث للقانون والحكم. وقد أدى عدم اليقين فيما يتعلق بالنطاق الجغرافي لتطبيق الحق في النسيان، على سبيل المثال، إلى إجراءات قانونية جديدة[56] . وينبغي لمحركات البحث، من جانبها، أن تكون أكثر شفافية بشأن المعايير التي تستخدمها داخليا لمعالجة هذه الطلبات.

وأخيرا، في إطار التنفيذ الحالي للحق في رفع الأسماء في الاتحاد الأوروبي، فإن إمكانية الحصول على العلاج محدودة. وشكل اللجوء الوحيد للمستخدم هو الفرصة للطعن في قرار محرك البحث لرفض طلب إلغاء القائمة. وينبغي أن يكون هناك مزيد من الوضوح بشأن سبل الانتصاف القائمة، وينبغي توسيع نطاقها.

[50] Access Now, O direito ao esquecimento no Brasil: quais os riscos para os direitos humanos? https://www.accessnow.org/o-direito-ao-esquecimento-no-brasil-quais-os-riscos-para-os-direitos-humanos/
[51] Access Now, Documento de posición: El "derecho al olvido" y su impacto en la protección de los Derechos Humanos https://www.accessnow.org/documento-de-posicion-el-derecho-al-olvido-y-su-impacto-en-la-proteccion-de-los-derechos-humanos/
[52] Access Now, In India, the "right to be forgotten" is in the hands of the Delhi High Court https://www.accessnow.org/india-right-forgotten-hands-delhi-high-court/
[53] أكسس ناو فهم الحق في أن تنسى عالميا، سبتمبر 2016
https://www.accessnow.org/cms/assets/uploads/2016/09/Access-Not-paper-the-Right-to-be-forgotten.pdf
[54] انظر الفصل 17. الاتحاد الأوروبي، اللائحة 2016/679 / بشأن حماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية وحرية تنقل هذه البيانات وإلغاء التوجيه 95/46 / إيك (اللائحة العامة لحماية البيانات) n)
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
[55] أكسس ناو أسئلة وأجوبة على الحق في أن تنسى، 2014
https://www.accessnow.org/cms/assets/uploads/archive/docs/GoogleSpainFAQRtbF.pdf
[56] أكسس ناو سنة فقط حتى يصبح القانون العام لحماية البيانات فاعلا: هل أوروبا جاهزة؟
/https://www.accessnow.org/year-gdpr-becomes-applicable-europe-ready

4 لا تفوض الشركات لجمع البيانات الحساسة دون موافقة

ونظرا لأهمية البيانات الحساسة، يجب توفير مستوى من الحماية أعلى من ذلك الذي يشمل بقية البيانات الشخصية لضمان مستوى كاف من الرقابة للأفراد. ولذلك، لا يؤذن بجمع ومعالجة البيانات الشخصية الحساسة إلا إذا أعطى الأفراد موافقتهم الصريحة والمستنيرة ولهم الحق في سحب تلك الموافقة في وقت لاحق.

وتشمل البيانات الحساسة مجموعة واسعة من المعلومات الشخصية مثل الأصل الإثني أو العرقي أو الرأي السياسي أو المعتقدات الدينية أو غيرها من المعتقدات المشابهة أو العضوية أو تفاصيل الصحة البدنية أو العقلية مثل البيانات الجينية أو البيومترية والمعلومات عن الحياة الشخصية والحياة الجنسية أو الجرائم المدنية. وتعني الطبيعة الخاصة لهذه المعلومات وأهميتها أن المستخدمين ينبغي أن يكونوا دائما قادرين على التحكم في من يحصل على هذه المعلومات واستخدامها.ونتيجة لذلك، ينبغي ألا يؤذن بمعالجة المعلومات الحساسة إلا إذا أعطى المستخدمون الموافقة الحرة والصريحة بحرية. ولحماية جوهر الحقوق الأساسية للمستخدمين في الخصوصية وحماية البيانات، لا يسمح بأي استثناء من هذه القواعد.

تجربة من مفاوضات القانون العام لحماية البيانات

يتطلب القانون العام لحماية البيانات من المنظمات الحصول على موافقة صريحة من المستخدم لجمع البيانات الحساسة كأساس عام. وفي حين أن هذا الأمر إيجابي للغاية، فإن القانون يجيز أيضا جمع واستخدام البيانات الحساسة دون موافقة المستخدمين على بعض الأهداف المحددة، بما في ذلك "أغراض البحث العلمي أو التاريخي أو الأغراض الإحصائية" [57] . هذا الاستثناء الواسع يحرم المستخدمي من السيطرة على معلوماتهم الأكثر حميمية، بل هو أكثر إشكالية في سياق نمو صناعة الصحة الإلكترونية، على نطاق واسع، تحليل البيانات الكبيرة للآراء السياسية، وأكثر من ذلك. وإن لم يكن ذلك محدودا، فانه يمكن للشركات أن تحصل على ملايين الأجزاء من المعلومات الحساسة على مدى السنوات القليلة القادمة، في البداية لإجراء البحوث وجمع الإحصاءات حول منتجاتها. ومن الناحية العملية، سيكون من المعقد إجراء رقابة على كيفية استخدام المنظمات لهذه البيانات، نظرا لأن المستخدمين لن يتم اشعارهم بذلك. يجب أن يكون المستخدمون قادرين على التحكم بالمنظمة التي لديها حق النفاذ إلى سجلاتهم الصحية أو التصويت. ويجب تجنب هذا النوع من الثغرات، أو على الأقل على وجه التحديد من خلال تقييد استخدام هذه البيانات لأغراض البحث، ويجب إجراء البحوث الإحصائية من أجل المصلحة العامة تحت رقابة صارمة.

5 لا تستخدم آليات التنظيم الذاتي والتنظيم المشترك

لسنوات عديدة، الشركات والكيانات التي تجمع البيانات كانت تدعو إلى تنظيم الخصوصية وحماية البيانات ليس من خلال أطر ملزمة ولكن من خلال آليات التنظيم الذاتي أو المشاركة التي توفر قدرا أكبر من المرونة. وعلى الرغم من المحاولات العديدة، لا توجد أمثلة لنظم غير ملزمة ناجحة لحماية البيانات الشخصية أو الخصوصية التي كانت إيجابية بالنسبة لحقوق المستخدمين أو، في الواقع، الأعمال ككل.

وبما أن المزيد من البيانات يجري تقاسمها عبر الإنترنت وخارجها، فقد حان الوقت لوضع أطر إلزامية لحماية البيانات والخصوصية في جميع أنحاء العالم لمنع أو إنهاء هذه السلوكيات وإعادة المستخدمين إلى السيطرة على معلوماتهم. وهذا سيمكن أيضا من تطوير الابتكار الصديق للخصوصية الذي يقتصر حاليا على عدد قليل من الشركات التي اتخذت نهج المشاركة طويلة الأجل لحماية مستخدميها بدلا من استناد نموذج أعمالهم في تحقيق الدخل من المعلومات الخاصة للمستخدمين.

[57] انظر الفصل 2-9 (ي). الاتحاد الأوروبي، اللائحة رقم 2016/679 / بشأن حماية الأشخاص الطبيعيين فيما يتعلق بتجهيز البيانات الشخصية وحرية تنقل هذه البيانات وإلغاء الأمر التوجيهي 95/46 / إيك (اللائحة العامة لحماية البيانات)
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

ويمكن أن تكون نماذج الأعمال المبنية على الخصوصية ميزة تنافسية. وفي البلدان التي ليس لديها قوانين شاملة لحماية البيانات، يمكن للشركات أن تبتكر من خلال ممارساتها الداخلية وضع ضمانات ومبادئ توجيهية لتحسين ثقة الناس في الاقتصاد الرقمي. وعلى الرغم من أن التنظيم الذاتي غير كاف بوصفه آلية إنفاذ وغير مستدامة لحماية حقوق الأفراد، يمكن أن يكون من المفيد في ظروف معينة أن تعتمد الشركات والأفراد إطارا تطوعيا في تلك البلدان. لا يمكن الاعتماد عليها، سواء من وجهة نظر الأفراد أو الشركات، وذلك بسبب خطر "ركوب مجاني" من قبل الجهات الفاعلة السيئة التي من شأنها تقويض الخصوصية والثقة والابتكار والاستيلاء على منتجات جديدة.

تجربة من مفاوضات القانون العام لحماية البيانات

ويملك الاتحاد الأوروبي خبرة طويلة في محاولات فاشلة التنظيم الذاتي أو التنظيم المشترك في مجال حرية التعبير[58] . وفي مجال الخصوصية وحماية البيانات، كان الاتحاد الأوروبي رائدا في تطوير مستوى رفيع من حماية للمستخدمين. ويعتبر القانون العام لحماية البيانات مثالا آخر على هذا النجاح. وفي حين انه أبعد ما يكون عن الكمال، فهو أداة رئيسية لحماية الحقوق الأساسية في الاتحاد الأوروبي، ويعكس سنوات من الخبرة المكتسبة من تنفيذ القوانين والفقه السابقة التي وضعتها المحاكم. كما يخلق القانون العام لحماية البيانات التزامات واضحة وقوية للمنظمات، ولكنه يقدم أيضا العديد من أدوات المساءلة لتعزيز حقوق حماية البيانات، مثل مبادئ حماية البيانات حسب التصميم والفرض الافتراضي والأحكام الجديدة لإصدار شهادات الشركات وخطط قواعد السلوك على مستوى الصناعة. وتهدف هذه الأدوات إلى وضع رؤية لحماية البيانات تتجاوز مجرد الامتثال للقانون وتشجيع الابتكار في هذا المجال.

[58] دري، حقوق الإنسان والخصخصة أ
https://edri.org/wp-content/uploads/2014/02/EDRi_HumanRights_and_PrivLaw_web.pdf

استنتاج

اكساس ناو تدعم بكل إخلاص تطوير الأطر المحلية والإقليمية والدولية لحماية المعطيات الشخصية. علماً وأن هذه الأطر يجب أن تكون مرتكزة على المستخدم وأن تركز على صون الحقوق وتعزيزها، وأن تقدم في الوقت ذاته قواعد واضحة يمكن التنبؤ بها لكي تتوافق الكيانات العامة والخاصة معها. وأخيرا، وليس آخرا، لا يمكننا أن نسلط الضوء بما فيه الكفاية على أهمية آليات إنفاذ شاملة وقوية تشرف عليها سلطة مستقلة للتأكد من أن الحماية المقترحة تعمل بكامل طاقتها.

كانت المحافظة على حماية البيانات على الصعيد العالمي مجالا طويلا من التركيز لاكساس ناو، وهي لا تزال واحدة من أعلى أولوياتنا. ومن بين القضايا الأخرى، يشارك فريقنا بنشاط في تنفيذ القانون العام لحماية البيانات ، وإصلاح تشريعات حماية البيانات في الأرجنتين، والمفاوضات في الهند وتونس من أجل وضع أول قانون لحماية البيانات.

CREATING A DATA PROTECTION FRAMEWORK:
A DO'S AND DON'TS GUIDE FOR LAWMAKERS

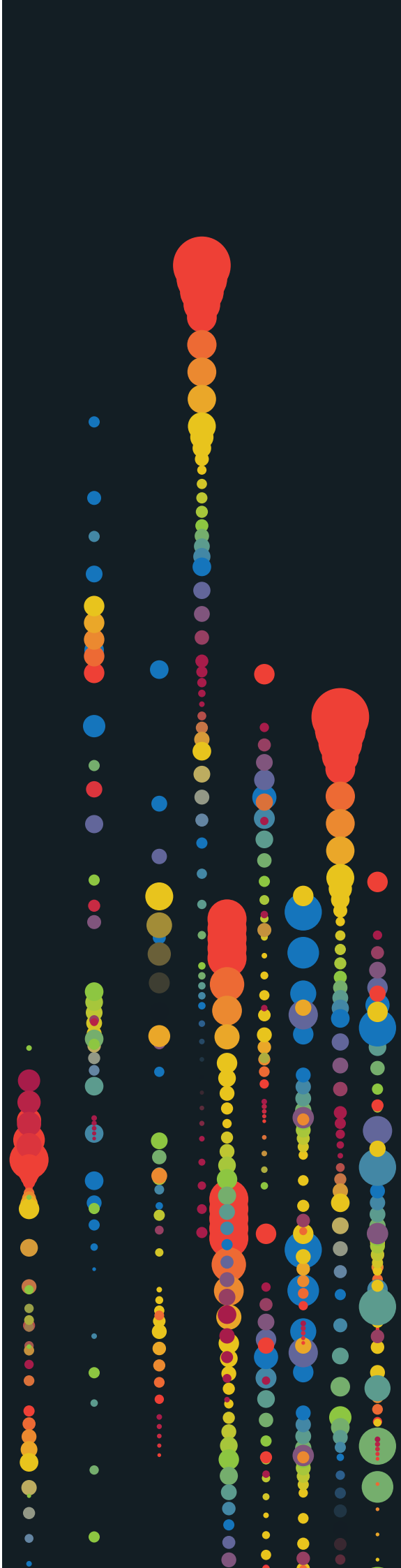
هذه الورقة من مطبوعات أكسس ناو

لمزيد من المعلومات الرجاء زيارة موقع :

https://www.accessnow.org

أو الاتصال ب :

Estelle Masse | Senior Policy Analyst | **estelle@accesnow.org**



accessnow

أكساس ناو تدعم وتدافع عن الحقوق الرقمية للمستخدمين المعرضين للخطر حول العالم. فمن خلال الجمع بين الدعم الفني المباشر،و الالتزام بسياسة شاملة ، والدعوة الى ذلك على صعيد عالمي، و اللجوء الى المنح الشعبية، وعقد الاجتماعات كتلك التي تقوم بها رايتس كون، يكون كفاحنا من أجل حقوق الإنسان في العصر الرقمي

https://www.accessnow.org