مشروع الحقوق الرقمية

الخصوصية وحماية البيانات الرقمية في اليمن

الواقع والمأمول

https://dg.samrl.org | أكتوبر - 2022

سام
للحقوق والحريات

مشروع الحقوق الرقمية

نافذة حقوقية غير ربحية تابعة لمنظمة سام، بدعم من منظمة إنترنيوز، تهدف إلى التعريف بالحقوق الرقمية، ورصد الانتهاكات الرقمية بحق مستخدمي الفضاء الرقمي، حيث تعمل على مناصرة الحقوق الرقمية لليمنيين، بهدف الوصول إلى فضاء رقمي آمن وعادل وحر. تتيح النافذة تقديم البلاغات عن الانتهاكات الرقمية، كما تساهم في توثيقها وتشكيل قاعدة بيانات عنها. وتعمل على إصدار دراسات وأبحاث حول النشاط الرقمي، والحقوق الرقمية والأمان الرقمي، بالإضافة إلى تخطيط وإدارة حملات المناصرة المحلية والدولية.

https://dg.samrl.org

مقدمة

مع التطور التكنولوجي واتساع نطاق ثورة الإنترنت، برزت حالة من القلق المبرر بشأن الخصوصية والبيانات الشخصية الرقمية، ذلك أن إمكانية تخزين البيانات ومشاركتها عبر الشبكة العنكبوتية، يجعلها عرضة للانتهاك والتلاعب، وإساءة الاستخدام.

ومن الوارد أن تتعرض بيانات مستخدمي الإنترنت للخطر، في ظل وجود نقاط ضعف تعتري الشبكة العنكبوتية، فضلا عن انتشار التقنيات والبرمجيات الذكية، التي تُسهِّل من اختراق الخصوصية، وتجعل من تواجد الأفراد في الفضاء الافتراضي بمثابة مغامرة محفوفة بالمخاطر.

تتعدد أشكال انتهاك الخصوصية في اليمن، فمن الرقابة والتجسس، مرورا بقرصنة المواقع واختراق حسابات منصات التواصل الاجتماعي، إلى هجمات البرمجيات الضارة، والحصول على بيانات المواطنين ونشرها دون رغبتهم، على نحو يمثل خرقا خطيرا لخصوصيتهم الرقمية.

إلى ذلك، فإن "المخاطر الكبيرة التي نواجهها يوميًا عبر الإنترنت ترتبط ارتباطًا وثيقًا بالنموذج الاقتصادي الرأسمالي (اقتصاد المراقبة الرقمية) الذي نعيش فيه. وفي قلب هذا الشكل الجديد من نموذج الأعمال الذي يعتمد على الحصول على كميات كبيرة جدًا من البيانات الشخصية ودمجها واستغلالها لتوجيه الإعلانات، والتلاعب بسلوك المستهلك، يتم رشوة المستخدمين وحثهم على إتاحة بياناتهم بأقل تكلفة ممكنة للمسوقين". وفقا لـ يونايتد، الشبكة الأوروبية المناهضة للتمييز.

إن عدم وجود قانون يمني لحماية البيانات الرقمية، يمثل أحد أسباب/عوامل تفشي الجرائم الإلكترونية، وعليه، فإن سن مثل هكذا قانون يعد الخطوة الأولى نحو تنظيم المشهد الرقمي المضطرب، وما يحدث فيه من انتهاكات تمس الحقوق الرقمية، بما فيها الحق في الخصوصية.

إطار مفاهيمي

الخصوصية الرقمية

تشير خصوصية الإنترنت إلى مجموعة واسعة من التقنيات والبروتوكولات والمفاهيم المتعلقة بمنح المستخدمين الفرديين أو الأطراف الأخرى مزيدًا من حماية الخصوصية في استخدامهم للإنترنت العالمي. وتتخذ خصوصية الإنترنت أشكالًا عديدة ، بما في ذلك بيانات الخصوصية الإلزامية على مواقع الويب، وضوابط مشاركة البيانات، ومبادرات شفافية البيانات والمزيد. Tech Opedia

بحسب ميكرو أناليتكس Micro Analytics (وهي شركة معنية بالتحليلات والخصوصية الرقمية والأمن عبر الإنترنت) يمكن تقسيم الخصوصية الرقمية إلى ثلاث فئات رئيسية، (وجميعها تؤدي إلى نفس المسار؛ وهو تأمين المعلومات الخاصة من الوصول غير المصرح به)، كالتالي:

خصوصية الاتصالات

ويعني أن على الأفراد أن يتواصلوا رقميًا مع بقاء اتصالاتهم ومراسلاتهم آمنة وسرية، بحيث يمكن الوصول إليها فقط من قبل المستلم المقصود. وتتعلق خصوصية الاتصالات بحماية الاتصالات من الرسائل والمكالمات إلى الاجتماعات عبر الإنترنت.

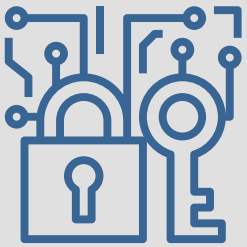
خصوصية المعلومات

مشاركة المعلومات دون تسريبها إلى أفراد غير مرغوب فيهم، وهي العلاقة بين كيفية جمع البيانات ونشرها فيما بين الكيانات. تهدف خصوصية المعلومات إلى حماية البيانات المشتركة عبر الإنترنت من الوصول الضار.

الخصوصية الفردية

تتعلق الخصوصية الفردية بضمان بقاء المعلومات الفردية خاصة. قد يشمل ذلك معلومات صحية أو مالية أو حتى معلومات عن الموقع.

حماية البيانات



مجموعة العمليات والإجراءات التي تحمي البيانات من التلف أو الانكشاف أو الفقدان. وتتضمن حماية البيانات إمكانية الوصول إلى البيانات للأغراض المصرح بها فقط، وأن تكون متوافقة مع المتطلبات القانونية أو التنظيمية المعمول بها، كما يجب أن تكون البيانات المحمية متاحة عند الحاجة ويمكن استخدامها للغرض المقصود منها. SNIA

وغالبًا ما يتم استخدام مصطلحي حماية البيانات وخصوصية البيانات بالتبادل، ولكن هناك فرق مهم بين الاثنين.

بحسب ميكرو أناليتكس Micro Analytics (وهي شركة معنية بالتحليلات والخصوصية الرقمية والأمن عبر الإنترنت) يمكن تقسيم الخصوصية الرقمية إلى ثلاث فئات رئيسية، (وجميعها تؤدي إلى نفس المسار؛ وهو تأمين المعلومات الخاصة من الوصول غير المصرح به)، كالتالي:

الوضع التشريعي

تعد اليمن واحدة من البلدان التي تفتقر إلى قانون الخصوصية وحماية البيانات، لكن، ومع ذلك، فهناك نصوص قانونية تطرقت لموضوع الخصوصية وحماية البيانات، حيث تنص المواد (15-18) من قانون الاتصالات اليمني على الآتي:

15 - حق الجمهور في الإستعمال الحر للإتصالات وضمان سريتها أمر مكفول طبقاً للدستور والقانون.

16 - يجوز للوزير في حالة الطوارئ أو الحالات الأخرى المحددة في القانون وبعد صدور إذن من الجهة القضائية المختصة أن يقوم برقابة المحادثات والرسائل عبر دوائر الإتصالات وإبلاغ مضمونها إلى الجهة المخولة قانونا بطلب إجراء هذه الرقابة.

17 - أية رقابة على الإتصالات يجب أن تكون بأمر صادر مباشرة عن الوزير أو ممن يفوضه بذلك.

18 - لا تجوز بأي حال رقابة المحادثات والرسائل إلا بإذن خطي مسبق من السلطة القضائية وذلك وفقاً لأحكام قانون الإجراءات الجزائية وبواسطة الوزير.

إضافة إلى ذلك، فإن مشروع قانون رقم (13) لسنة 2012م بشأن حق الحصول على المعلومات (لم يُنفذ) أورد نصوصا قانونية عن حماية المعلومات، وحماية الخصوصية، (من المادة 44 إلى المادة 57).

السياسات التنظيمية

تحدد السياسة التنظيمية مجموعة الإجراءات التي تتخذها السلطات لحماية تكنولوجيا المعلومات وأنظمة الكمبيوتر، وإدارة المخاطر عبر الإنترنت. وقد تضمنت السياسات العامة لأمن المعلومات في الجهات الحكومية (الصادرة بقرار حكومة صنعاء رقم 59 لسنة 2020) على إجراءات بشأن سياسة خصوصية البيانات واستخدامها، كالتالي:

سياسة خصوصية البيانات

يجب على الموظفين عدم الإفصاح لأي شخص عن أي معلومات، أو طبيعة وموقع أنظمة المعلومات ولا عن أنظمة الرقابة المستخدمة، كما يجب مراعاة الخصوصية عند التعامل مع البيانات الشخصية.

سياسة تطوير وصيانة الأنظمة والتطبيقات

يجب أن يكون هناك ضمان لأي تطبيق أو اختبار لأنظمة المعلومات، ويجب أن تصان الوثائق وقوائم الأنظمة والتطبيقات بشكل سليم، مع الحفاظ على سلامتها. وعند تطوير/اقتناء أي نظم معلومات جديدة يجب أن تختبر.

استخدام البيانات

لا يسمح باستخدام البيانات الحقيقية قيد الاستخدام عند اختبار الأنظمة قبل وضع ضوابط خاصة لضبط أمن هذه البيانات والمعلومات وسلامتها، ويجب التأكد من تطبيق التحديثات، وتقييم المخاطر الأمنية للأنظمة.

سياسة الخصوصية لدى مقدمي الخدمات الرقمية

تحدد سياسة الخصوصية، الآلية التي يتم من خلالها جمع واستخدام معلومات المستخدم، ومشاركتها وظروف الإفصاح عنها لأطراف ثالثة. وبالنظر إلى سياسة الخصوصية لدى مقدمي الخدمات الرقمية في اليمن، يتبين لنا مدى القصور الذي يعتريها، حيث أنها في الغالب، مقتضبة، وغير محددة بوضوح، فضلا عن أن بعض المزودين لا يمتلك سياسة خصوصية مكتوبة، كـ (اليمنية العمانية المتحدة للاتصالات YOU) وشركة تيليمن، وشركة واي للاتصالات، وشركة عدن نت.

وينبغي ملاحظة أن سياسة الخصوصية لا تحدد الطريقة التي تتعامل شركات الاتصالات اليمنية بموجبها مع بيانات المشتركين، في خدمات الاتصال والانترنت، بقدر ما تحدد آلية جمع المعلومات من مرتادي المواقع الإلكترونية لهذه الشركات، كما أن سياسة الخصوصية هذه يغلب عليها إغفال الجانب المتعلق بحقوق المستخدم، كـ (الحق في الاعتراض، والحق في المحو).

علاوة على ذلك، فإن غالبية المواقع الإلكترونية اليمنية (حكومية، إخبارية، تجارية... إلخ) لا تمتلك سياسة خصوصية، وإن وجدت، فهي مجرد كلام منسوخ في معظمه، وهو ما يعني أنها تجمع معلومات عن متصفحيها بطريقة غامضة وغير شفافة.

المعلومات التي تُجمع

المعلومات الشخصية والمعلومات التقنية، والمعلومات المستخدمة لأغراض الإعلانات، إضافة إلى معلومات الملف الشخصي على الشبكات الاجتماعية.

استخدام المعلومات

لأغراض تحليل استخدام الخدمات وإدارتها وتطويرها، وتوفير الدعم الفني، والترويج، والاستجابة للطلبات.

الإفصاح عن المعلومات

قد يتم مشاركة معلومات المستخدم مع أطراف ثالثة وفقًا للظروف التالية: مطلوب من قبل سلطات إنفاذ القانون، لحماية حقوق وممتلكات وسلامة العملاء أو غيرهم، لأغراض الترويج أو المسابقة أو الاستطلاع.

نقل وتخزين المعلومات

قد يتم نقل المعلومات وتخزينها في وجهة خارج إطار الشركة ومكاتبها، ويمكن نقلها إلى الشركات التابعة للشركة الأم إضافة إلى الشركاء المحليين والدوليين.

مظاهر انتهاك الخصوصية

احتلت اليمن المرتبة الثانية ضمن أعلى 10 دول ومناطق من حيث نسبة المستخدمين الذين هاجمتهم البرامج الضارة للأجهزة المحمولة، عند درجة خطورة 17,97، من أصل 26 درجة، بحسب تقرير كاسبر سكاي 2022. وكان برنامج التجسس Tro-jan-Spy.AndroidOS.Agent.aas هو التهديد الذي غالبًا ما يواجهه المستخدمون في البلد.

تتعدد أشكال انتهاك الخصوصية في اليمن، فمن الرقابة والتجسس، مرورا بقرصنة المواقع واختراق حسابات منصات التواصل الاجتماعي، إلى هجمات البرمجيات الضارة، والحصول على بيانات المواطنين ونشرها دون رغبتهم، على نحو يمثل خرقا خطيرا لخصوصيتهم الرقمية.

الرقابة والتجسس

أورد تقرير صدر في أكتوبر 2015 عن سيتزن لاب (وهو مختبر معني بدراسة ضوابط المعلومات التي تؤثر على انفتاح وأمن الإنترنت) أن المراقبة الإلكترونية الخارجية والمحلية منتشرة على نطاق واسع في اليمن، من قبل النزاع المسلح الحالي وخلاله أيضا، ويضيف التقرير: قبل النزاع، كان لليمن سجل حافل في تصفية المحتوى السياسي، من مجموعة متنوعة من الفئات، بما في ذلك أدوات إخفاء الهوية.

تقرير فريق الخبراء التابع لمجلس الأمن الدولي (يناير 2021) قال إن اللجنة تحقق في مزاعم بشأن استخدام الحوثيين لأدوات الاتصالات لمراقبة البيانات والرسائل والنصوص وحركة المرور الصوتية والمرئية التي تشمل خصومهم، لكن تيليمن في صنعاء أوضحت للجنة أن "القوانين اليمنية تلزم مزودي خدمة الإنترنت بتصفية محتوى معين يتعارض مع الشريعة والعقائد الإسلامية وأنهم يستخدمونها لغرض حماية الأطفال من أي محتوى غير لائق ولا يوجد استخدام غير قانوني.

قرصنة المواقع الإلكترونية

ساهمت حقيقة أن اليمن دولة تفتقر إلى الخبرة نسبيًا عندما يتعلق الأمر بالعمليات التقنية المتعلقة بالإنترنت في خلق بيئة خصبة لاختراق مواقع الويب ورسائل البريد الإلكتروني وحسابات وسائل التواصل الاجتماعي. وفقا لـ منظمة المراقبة العالمية لمجتمع المعلومات (مصدر سابق).

الحصول على البيانات الشخصية بطريقة غير قانونية

يُعتبرُ تطبيق "كاشف الأرقام اليمنية" وسياساته وخدمته انتهاكًا صارخًا لكل خصوصيات المستخدم وبياناته المختلفة، وفقًا لـ: عدنان عثمان، مطور ويب وباحث أمن رقمي، الذي تحدث لـ"خيوط" (بتاريخ أبريل 2022) قائلًا: إن "(كاشف الأرقام اليمني) لا يكتفي بسجل أسماء المستخدم فقط، بل يخزن بالإضافة إلى ذلك، إيميلاتهم وعناوين حساباتهم الأخرى المرتبطة بسجل الأسماء."

ويؤكد عثمان أنّ التهديد الأسوأ هو مشاركة سجلات الأسماء لدى أطراف ثالثة، باستخدام محرك بحث بيانات التطبيق، بالقول: "إن هذه الثغرة المسكوت عنها هي في الواقع تخلف وستخلف نتائج مأساوية مختلفة، بما فيها عنف وخلافات ومشاكل أسرية مأهولة؛ لأن الكثير من المستخدمين يثقون بهذه النتائج بشكل كلي، دون أي شكوك".

اختراق حسابات منصات التواصل الاجتماعي

في تقرير نشره الموقع بوست (بتاريخ نوفمبر 2018) كشف فريق التحرير عن تعرض حسابات صحفيين في موقع "تويتر" للقرصنة من قبل جهات تبين أنها تعمل من العاصمة صنعاء، ومارست التهكير لعدة حسابات في تويتر أغلبها لصحفيين يمنيين معروفين، عن طريق استدراجهم بحيل إلكترونية، تعكس في مجملها وجود شبكة تتعلق مهمتها بالقرصنة والاستحواذ على تلك الحسابات لمصالح القائمين على تلك العمليات.

هجمات البرمجيات الضارة

خلال المؤتمر الوطني الأول للأمن السيبراني المنعقد في صنعاء خلال يونيو 2021 أشار رئيس قسم أمن المعلومات بشركة يمن موبايل، المهندس علي الوصابي، إلى أن شركات الإتصالات تحجب مئات الآف من الرسائل التي تُرسل من بعض الهواتف المصابة ببرمجيات ضارة، لافتا إلى أن هذه البرمجيات تعمل في الخفاء وترسل رسائل أو تتصل دون علم المستخدم، وفي حال نجحت في المرور فإنها لاحقا تستوجب الدفع للمزودين الخارجيين مقابل هذه الرسائل.

لا يتسع المجال، للحديث باستفاضة عن ما ورد في هذا القسم، وسنتناول المواضيع بشيء من التفصيل في تقارير قادمة، لتكتمل الصورة القاتمة للمشهد الرقمي في اليمن.

ما الحل؟

يعد إصدار "قانون الخصوصية وحمايــة البيانات"، الخطوة الأولى نحو تنظيم المشــهد الرقمــي المضطرب، وما يحــدث فيه من انتهاكات تمس الحقوق الرقمية، بما فيها الحق في الخصوصية.

الخطة الاستراتيجية الوطنية للأمن السيبراني، التي تمخضت عن المؤتمر الوطنــي الأول للأمن الســيبراني، المنعقد في صنعاء خلال الفترة (7-9 يونيو) 2021، اشــتملت علــى محور (إقرار قوانين الحمايــة الإلكترونية الفــردي)، لوضــع قوانين حمايــة البيانات والخصوصية، وحماية الأطفال على الإنترنت، بالإضافة إلى وضع قوانين الملكية الفكرية الإلكترونية، وإقرار تصور للتوقيع الرقمي. هذه الخطة بما تضمنته من موجهات سيكون من الجيد تنفيذها إذا ما تم إعادة مناقشتها وتعديلها بالتشارك والتوافق مع وزارة الاتصالات في عدن، والأطراف الأخرى ذات الصلة.

وفي هذا الســياق، تقترح مؤسســة أكســس ناو (وهي منظمة دوليــة تعمل علــى الدفاع عن الحقــوق الرقمية لمســتخدمي الإنترنــت) 10 توصيات ينبغي لواضعي السياســات مراعاتها عند تطوير قانون البيانات، كالآتي:

1 ضمان إجراء مفاوضات شفافة وشاملة

2 تحديــد وإدراج قائمــة بمبادئ حمايــة المعطيات الشــخصية الملزمة حسب القانون

3 تحديد الأساس القانوني الذي يسمح بمعالجة البيانات

4 إدراج قائمة بحقوق المستخدمين الملزمة في القانون

5 تحديد نطاق واضح للتطبيق
6 إنشـــاء آليات ملزمة وشـــفافة لنقل البيانات بشـــكل آمن إلى بلدان ثالثة
7 حماية أمن البيانات وسلامة البيانات
8 تطوير آليات منع خرق البيانات والإبلاغ.
9 إنشاء سلطة مستقلة وآليات قوية للإنقاذ
10 مواصلة حماية حماية البيانات والخصوصية

ويمكن لشـــركات الاتصالات الاسترشـــاد بـ اللائحة العامة لحماية البيانـــات GDPR الصادرة عن الاتحاد الأوروبـــي (بتاريخ أبريل 2016) بشأن حماية الأشـــخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية وحرية نقل هذه البيانات.
حيث تضع اللائحة مبادئ ينبغي مراعاتها:
لا يجـــوز جمـــع البيانات الشـــخصية إلا لأغراض محددة ومشـــروعة وواضحة.
يجب أن تكون معالجة البيانات الشخصية قانونية وعادلة وتتسم بالشفافية.
يجـــب أن تكون البيانات الشـــخصية التي تتم معالجتها مناســـبة وذات صلة وليست واسعة.
يجب أن تكـــون البيانات الشـــخصية التي تتـــم معالجتها دقيقة ومحدثة إذا لزم الأمر.
لا يجوز الاحتفاظ بالبيانات الشـــخصية طالما كانت مطلوبة لغرض المعالجة فحسب.
عند معالجة البيانات الشخصية، يجب التأكد من حمايتها جيدا من خلال اتخاذ الإجراءات الأمنية المناسبة.

وعندما يتعلق الأمر بأعمال المراقبة، يحتاج المجتمع المدني إلى إجراء المزيد من البحوث المنهجية لتحديد كيفية إجراء المراقبة، ويمكن للباحثين في اليمن، ربما بالتعاون مع الجهات المانحة والمعاهد الدولية، العمل معًا في تتبع وتحديد حالات المراقبة الرقمية واقتراح الحلول، وستكون هناك حاجة إلى مجموعات المناصرة لتنسيق أعمالها، وإجراء مناقشات مع مختلف أصحاب المصلحة، واقتراح سياسات للحد من إساءة استخدام السلطة، سواء من قبل الحكومة أو أي طرف آخر. ولكي يتم ذلك ، سيكون من الضروري المشاركة بشكل أكبر مع الجهات الفاعلة الدولية والإقليمية في هذا المجال وحشد الموارد لإطلاق حملات ومشاريع منهجية وطويلة الأجل يمكن أن تضع قضية حقوق الإنسان على الإنترنت في المقدمة. منظمة المراقبة العالمية لمجتمع المعلومات - مصدر سابق.

بالنظر إلى ما يعانيه مستخدمي الإنترنت من انتهاكات وتجاوزات تمس حقوقهم الرقمية، فإن من الضروري إنشاء هيئة تعنى بحقوق المستخدمين، بحيث تكون المعبر عنهم أمام السلطات، والممثل لهم في أية فعالية أو نشاط إقليمي/ دولي ذي صلة.

الخصوصية وحماية البيانات الرقمية في اليمن

الواقع والمأمول

مشروع الحقوق الرقمية

| SamDigitalRight
| violations@samrl.org
| Digital.Rights.Yemen
| https://dg.samrl.org