

وزارة تكنولوجيا الاتصال والاقتصاد الرقمي - تونس

**تقديم مقترح أكساس ناو (Access Now) إلى وزارة تكنولوجيا الاتصال والاقتصاد الرقمي عرض
النظر في مشروع قانون مجلة الاتصالات الإلكترونية 14 أوت/ أغسطس 2018**

مقدم في 23 أكتوبر 2018

تم الإعداد من قبل:
ديما سمارو - باحثة قانونية

تمت الموافقة من قبل:
وفاء بن حسين - مديرة مكتب أكساس ناو

تتألف أكساس ناو (Access Now)، من ثلاث مجموعات: فريق صنع السياسات وتحليل القوانين، فريق الضغط والمناصرة والفريق التقني يعملون في جميع مناطق العالم، من أجل تعزيز حقوق الإنسان الرقمية وحمايتها، ولغايات تحقيق شبكة إنترنت مفتوحة ومجانية للجميع وذلك باستخدام خبرتها القانونية الفريدة في تطوير وتعزيز الحقوق والحريات المكفولة بموجب القوانين والمعاهدات الدولية. أنشئت في عام 2009، وتنشط في خمس قارات، تهدف أكساس ناو إلى ضمان التطوير التدريجي والتنفيذ الفعال لحقوق الإنسان الرقمية الدولية؛ ضمان حرية التعبير عن الرأي والفكر؛ الخصوصية وحماية المعطيات الشخصية؛ حياد الإنترنت؛ الأمن الرقمي وإدارة الأعمال وحقوق الإنسان.

14 Rue Salah Eddine Al Ayoubi, Mutuelle ville, 1082 Tunis, Tunisia
Numéro de téléphone : +216 71 840 335 - Site web : <https://www.accessnow.org>
Mail : dima@accessnow.org, wafa@accessnow.org

تقديم مقترح أكسس ناو (Access Now) إلى وزارة تكنولوجيا الاتصال والاقتصاد الرقمي عرض النظر في مشروع قانون مجلة الاتصالات الإلكترونية 14 أوت/ أغسطس 2018

1. في 13 سبتمبر 2018، أعلنت وزارة تكنولوجيا الاتصال والاقتصاد الرقمي بتونس عن فتح باب الاستشارة العامة الثالثة بشأن مراجعة وتقديم مقترحات وتعليقات لغايات تصحيح أو تحسين أو حتى إضافة عناصر فيما يخص مشروع قانون مجلة الاتصالات الإلكترونية، وذلك في موعد أقصاه في 30 أكتوبر 2018، الساعة 12:00 صباحاً.
2. وفي هذا السياق، ترحب أكسس ناو (Access Now) بالفرصة المتاحة لتقديم هذا التقرير إلى وزارة تكنولوجيا الاتصال والاقتصاد الرقمي في تونس بهدف مساعدتها في مراجعة مشروع قانون مجلة الاتصالات الإلكترونية في 14 أوت 2018.

مُلخَص عن المقترح

3. وفي هذا المقترح، قدمت أكسس ناو ردوداً وتعليقات بديلة و/ أو مَحسنة على بعض المسائل المدرجة في مشروع قانون مجلة الاتصالات الإلكترونية. كما تم طرح بعض الأسئلة بخصوص بعض المفاهيم والمصطلحات و/ أو بخصوص بعض المسائل التي يشوبها الغموض والتي لم يتم إدراجها بشكل كلي أو بشكل واضح في النص القانوني في مشروع القانون، وذلك من خلال تحليل النص القانوني بالاستناد إلى مراجع قانونية محلية مثل المرسوم رقم 115 لعام 2011 (المرسوم رقم 115/2011) بشأن الصحافة والطباعة والنشر والرسوم رقم 116 لعام 2011 (المرسوم رقم 116/2011) بشأن حرية الاتصال السمعي البصري وإنشاء هيئة عليا للاتصال السمعي البصري، المؤرخان بتاريخ 2 نوفمبر 2011. إضافة إلى مراجع قانونية دولية كالاتفاقيات والمعاهدات الدولية مثل الاتفاقية رقم 108 لمجلس أوروبا المتعلقة بحماية الأشخاص تجاه المعالجة الآلية للمعطيات الشخصية، وبروتوكولها الإضافي رقم 181 الخاص بسلطات المراقبة و انسياب وتدفق المعطيات عبر الحدود، إضافة إلى الإعلان العالمي لحقوق الإنسان لعام 1948.
4. اشتملت المقترحات المقدمة من قبل أكسس ناو على تحسينات، إضافة عناصر، تصحيح وفي بعض الأحوال تغيير أو إزالة نص قانوني نظراً لكونه متعسفاً وغير مرن. كما اشتملت المقترحات على تصحيحات متعلقة بحماية المعطيات الشخصية وإشراك هيئة حماية المعطيات الشخصية في هذه المسألة، إضافة إلى تصحيحات تتعلق بالمجال التقني، ومقترحات تتعلق بتوضيح أو تصحيح بعض المفاهيم والمصطلحات لغايات إزالة الغموض منها وتجنباً للوقوع في الخطأ. إضافة إلى ذلك، قمنا بإدراج ما يتعلق بأهمية تحقيق التوافق ما بين الضرورة والتناسب والشرعية في بعض المسائل المختلفة الواردة في مشروع القانون، وذلك لكونه من المبادئ الراسخة والمنصوص عليها صراحةً في القانون الدولي. كما تتطلع أكسس ناو (Access Now) من خلال المقترحات المقدمة من جانبها، إلى التأكيد على أهمية ضمان إشراك مختلف أطراف المجتمع المدني والخبراء المختصين في الأنشطة التي قامت أو تعتزم وزارة تكنولوجيا الاتصال والاقتصاد الرقمي القيام بها وذلك على صعيد الحريات الأساسية أو حتى في المسائل التقنية، وذلك لغايات ضمان الوصول إلى أفضل النتائج الممكنة سواء فيما يتعلق بتقوية ومثانة النصوص القانونية من جهة، وتوافق مشروع القانون مع المعاهدات والاتفاقيات الدولية من جهة أخرى.

توصيات و/ أو مقترحات و/ أو تعليقات لغايات تصحيح أو تحسين و/أو إضافة عناصر فيما يخص مشروع قانون مجلة الاتصالات الإلكترونية في 14 أوت 2018

فيما يتعلق بالباب الأول من المجلة و الذي يتعلق بالثقة الرقمية وحماية الفضاء الرقمي الوطني فإن التعليقات والإقتراحات التي نود إدارجها وأخذها بعين الاعتبار كالآتي:

أولاً:

الفصل (146) نصّ على خدمات الثقة الرقمية على اعتبارها من الخدمات الإلكترونية، وفي هذا السياق فإن النقطة التي نقترح تعديلها كالآتي:

نقترح الإنتباه إلى التعريف المدرج بخصوص "الخدمات". إذ أن مشروع القانون لم يفسّر ماهية الخدمات واكتفى بذكر ستة خدمات (6) على سبيل الحصر. فبالرغم من أن مشروع القانون قد عرّف خدمات الثقة الإلكترونية في باب المصطلحات بأنها "خدمة إلكترونية تقدم مجاناً أو بمقابل والتي تتمثل في الإحداث والتدقيق في الإماءات الإلكترونية والأختام الإلكترونية وأختام التوقيت الإلكترونية وخدمات التراسل الإلكتروني المضمون الوصول والشهادات المتصلة بهذه الخدمات، الإحداث والتدقيق في شهادات المصادقة للمواقع الإلكترونية و الأرشيف الإلكتروني." إلا أنّ البروتوكولات التقنية¹ وتطبيقات البرمجيات المحددة الأخرى مثل الخوارزميات (اللوغاريتم) لم يتم الإشارة إليها بأنها مشمولة في خدمات الثقة الرقمية.

الأمر الذي سيساهم في تحديد نطاق الخدمات التي يشملها مشروع القانون. فعلى سبيل المثال، في حال تم تضمين البروتوكولات في مشروع القانون، فإن كتابة المواصفات في القانون يمكن أن يعرقل - بشكل خطير - الابتكار، الأمن والنظام البيئي المفتوح والتعاوني لتعريف البروتوكول وتطبيقه.

ثانياً:

الفصل (185) نصّ على "يخضع كل شخص طبيعي أو معنوي يرغب في تعاطي نشاط مزود خدمات ثقة رقمية، بالإضافة إلى أحكام هذا القانون، إلى كراس شروط تتم المصادقة عليه بقرار من الوزير المكلف بالاتصالات الإلكترونية." وفي هذا السياق فإننا نقترح مايلي:

1. نقترح ابتداءً أهمية الإشارة إلى القاعدة العامّة والتي تقضي بأن إنشاء أي خدمات، تطبيقات ووسائط جديدة وغيرها لا تحتاج إلى ترخيص أو تفويض مُسبق². ومع ذلك، يمكن أن يكون الترخيص أو التفويض المسبق معقولاً وفقاً لطبيعة التطبيق أو الخدمة (ففي حالة أن التطبيق أو الخدمة يتعاملان مع مع أمور تتعلق بالمصلحة العامة كالصحة على سبيل المثال) لكن كاستثناء فقط.
2. كما نقترح أن تتم الإشارة إلى جملة الشروط التي يترتب عليها منح الموافقة لتعاطي نشاط مزود خدمات ثقة رقمية، إذ أن معرفة الشروط مهمة لغاية تحقيق الشفافية من ناحية إنشاء التطبيقات الاجتماعية والاتصالات وغيرها وللتأكد من أن هذه الشروط لا تؤد في نهاية المطاف إلى تعقيد الإجراءات المطلوبة للحصول على الموافقة.

¹ ISOC (2015). Fiche sur les politiques publiques: Normes Internet ouvertes.

<https://www.internetsociety.org/fr/policybriefs/openstandards/>

² Komaitis, K. (2014). Permissionless Innovation: Why It Matters.

http://www.circleid.com/posts/20140424_permissionless_innovation_why_it_matters/

فيما يتعلق بالباب الثاني من المجلة و الذي يتعلق بحماية الفضاء الرقمي الوطني والقسم الأول المتعلق بالاستراتيجية الوطنية للسلامة الرقمية فإن التعليقات والإقتراحات التي نود إدارجها وأخذها بعين الاعتبار كالآتي:

أولاً:

الفصل (192) نصّ على الاستراتيجية الوطنية للسلامة الرقمية، وفي هذا السياق فإننا فإن النقطة التي نقترح تعديلها كالآتي:

نقترح تعديل النص بحيث يشتمل على "وجود التزام بالإبلاغ عن البيانات المخترقة والمنتهكة إلى هيئة حماية المعطيات الشخصية الوطنية"، بالإضافة إلى النص على "الالتزام قواعد داخلية لغايات تحقيق سلامة وأمن البيانات واستغلالها في إنجاز المهام الموكلة لها" لغايات التوافق مع الأحكام القانونية المتعلقة بحماية المعطيات الشخصية الواردة في القانون الأساسي عدد 63 لسنة 2004 المؤرخ في جويلية 2004 وبالإشارة إلى المعايير الدولية³ في يومنا هذا والتي تتعلق بذات السياق.

ثانياً:

الفصل (194): نصّ على المهام التي تتولى الوكالة الوطنية للسلامة الرقمية القيام بها، في هذا السياق نقترح مايلي:

1. فيما يتعلق بالنص الوارد بخصوص جمع المعطيات والبيانات التي أدرجها القانون في هذا الفصل "جمع المعطيات والبيانات والإحصائيات المتعلقة بالسلامة الرقمية لإحداث قاعدة بيانات استغلالها في إنجاز المهام" الموكلة لها، نقترح الإشارة إلى "مدى توافق عملية جمع المعطيات مع مبادئ حماية البيانات المنصوص عليها في مشروع القانون الأساسي المتعلق بحماية المعطيات الشخصية مثل الموافقة الصريحة لإتمام عملية جمع المعلومات"⁴.

كما نقترح الإشارة في هذا الفصل إلى ما يتعلق بالبيانات مجهولة المصدر التي حددها قانون حماية البيانات العامة بأنها "البيانات المقدمة بطريقة مجهولة بحيث تجعل الشخص موضوع البيانات غير قابل للتعريف أو أنه لم يعد قابلاً للتحديد"⁵.

2. مما يجدر ملاحظته أن النص لم يشير إلى أن البيانات "الشخصية" وإنما أشار إليها ب "البيانات" فقط - لذلك نقترح توضيح ذلك ليتوافق مع مصطلح المعطيات الشخصية⁶ المشار إليه في مشروع القانون حيث عرّفها بأنها "المعطيات المعترية كذلك طبقاً لمقتضيات القانون الأساسي المتعلق بحماية المعطيات الشخصية".

3. في حال كان المقصود بهذه البيانات بأنها بيانات "شخصية"، نقترح إضافة "يجب أن تكون هيئة حماية المعطيات الشخصية المختصة في الترخيص والإشراف على عملية جمع المعطيات"⁷، كما "يجب أن يتم تضمين جميع حقوق حماية البيانات الخاصة بالمستخدم مثل حق الإعلام، حق الوصول، المحو، الإعتراض وغيرها من الحقوق المتعلقة بحماية المعطيات الشخصية"⁸.

³ General Data Protection Regulation (GDPR), (May, 2018), Article 33. Notification of a personal data breach to the supervisory authority. <https://gdpr-info.eu/art-33-gdpr/>

⁴ قانون أساسي عدد 63 لسنة 2004 مؤرخ في جويلية 2004 يتعلق بحماية المعطيات الشخصية، الباب الثالث في جمع المعطيات الشخصية وحفظها والتشطيط عليها واعدامها.

⁵ اللانحة الأوروبية العامة لحماية البيانات (GDPR)، قراءة رقم 26. <https://gdpr-info.eu/recitals/no-26/>

⁶ قانون أساسي عدد 63 لسنة 2004 مؤرخ في جويلية 2004 يتعلق بحماية المعطيات الشخصية، الفصل 4.

⁷ مصدر سابق، الفصل 15 من القسم الثاني في المسؤول عن معالجة المعطيات الشخصية وواجباته.

⁸ مصدر سابق، القسم الثالث في حقوق المعنى بالأمر و الباب الثالث في جمع المعطيات الشخصية وحفظها والتشطيط عليها واعدامها.

فيما يتعلق بالكتاب الرابع الذي يتعلق بالحقوق والحريات والباب الأول من مشروع القانون والذي يتعلق بالأحكام العامة فإن التعليقات والإقتراحات التي نود إدارجها وأخذها بعين الاعتبار كالآتي:

أولاً:

الفصل (216) فيما يتعلق بالحق في التمتع بالخدمات الإلكترونية لكل شخص وخاصة ما نص عليه المشروع " المساواة في الحصول على خدمات الاتصالات الإلكترونية"، في هذا السياق فإن النقطة التي نقترح تعديلها كالآتي:

نقترح تحديد معيار المساواة ما بين مفهوم الوصول المتساوي لخدمة الاتصالات الإلكترونية و مفهوم حياذ الإنترنت.

على سبيل المثال: هل الشبكة غير المحايدة تعني في النتيجة أنها الشبكة التي لا تسمح للمستخدمين في حق الوصول لخدمات الاتصالات الإلكترونية بشكل مساوٍ؟ إذ لا بدّ من تحديد مفهوم ومعيار المساواة التي قصدها المشرع وذلك لتجنب الوقوع في الخطأ واللبس.

ثانياً:

الفصل (217) فيما يتعلق بحريات التعبير عن الرأي التي يكفلها المشروع حيث نص على "حرية الرأي والفكر والتعبير والإعلام والنشر والاتصال على شبكة الإنترنت مضمونة ولا يمكن الحد منها إلا في الحالات والضمانات التي ينص عليها القانون."، في هذا السياق نقترح مايلي:

1. نقترح الإشارة إلى "الضرورة والتناسب" إلى جانب الشرعية⁹، إذ أنها لا تعتبر الشرط الوحيد في القانون وإنما لا بدّ أن يكون النص القانوني مرناً وقابل للتكيف مع الظروف التي تستدعي ذلك.

2. نقترح توضيح مفهوم حرية تلقي المعلومات ونقلها. من خلال توضيح أن الإنترنت إلى جانب كونه تقنية حديثة تسمح للأفراد بالإطلاع والحصول على المعلومات، إلا أنه يعتبر أيضاً منصّة لتلقي الاتصالات ونقلها، و مشاركة الخبرات والأفكار وغيرها. من المهم أيضاً التأكيد على أن الحق في حرية الرأي والتعبير على الإنترنت يشمل حرية اعتناق الآراء دون أي تدخّل، إلى جانب الحق في البحث عن المعلومات والأفكار وتلقيها ونقلها عبر أي وسيلة إعلام وبصرف النظر عن اذا ما كان هناك حدود معينة تحكم هذه القواعد والحقوق¹⁰.

فيما يتعلق بالباب الثاني (من الباب الرابع) والذي يتعلق بالحقوق والحريات عبر الشبكات الإلكترونية والفضاء الرقمي والقسم الأول منه والذي يتعلق بحقوق مستخدمي الخدمات الإلكترونية، فإن التعليقات والإقتراحات التي نود إدارجها وأخذها بعين الاعتبار كالآتي:

أولاً:

الفصل (222) والذي نصّ على "لا يجوز لمشغلي شبكات الاتصالات إلكترونية ولمزود الخدمات أن يوقف الخدمة لعدم

⁹ مؤلفون مختلفون (2014). الضرورة والتناسب. المبادئ الدولية لتطبيق حقوق الإنسان على مراقبة الاتصالات. (باللغة الفرنسية)

<https://necessaryandproportionate.org/fr/n%C3%A9cessaires-et-proportionn%C3%A9>

¹⁰ الإعلان العالمي لحقوق الإنسان (1948)، المادة (19). (باللغة الإنجليزية)

<http://www.un.org/ar/universal-declaration-human-rights/index.html>

خلاصه في فاتورة استهلاكها، إلا بعد أن ينبه بالدفع على مستعمل الخدمة كما يجب وفي أجل معقول وبكيفية تبقى أثرا كتابيا ويمكنه من أجل معقول للخلص"، في هذا السياق فإن النقطة التي نقترح تعديلها كالآتي:

نقترح تحديد المقصود بـ "الأجل المعقول". إذ أن غموض المصطلح "معقول" يفشل في توفير اليقين القانوني لمستخدمي خدمات الإنترنت. كما يترتب على هذا الغموض إمكانية حصول خلاف أو نزاع كون المدة المعقولة بالنسبة لمشغلي شبكات الاتصالات ومزودي الخدمات يمكن أن تختلف عن المدة المعقولة بالنسبة للمستخدمين أو المنتفعين من الخدمات.

على هذا الأساس، نوصي باستخدام عملية محددة بوضوح، ومحدودة الوقت، مع وجود طرق وآليات واضحة لجبر الضرر للمستخدمين.

ثانياً:

الفصل (224) والذي نصّ على "تحت الهيئة الوطنية للاتصالات الإلكترونية مشغلي شبكات الاتصالات الإلكترونية ومزودي الخدمات على صياغة واعتماد مدونات قواعد سلوك تضمن حقوق مستعملي الخدمات"، في هذا السياق نقترح مايلي:

1. ابتداءً نقترح الإشارة إلى أنّ مدونة قواعد السلوك مختلفة عن شروط الخدمة¹¹، إذ يجب أن تكون حقوق مستعملي الخدمات قابلة للتنفيذ كما يجب أن تحدد بموجب القانون، وليس بموجب مدونة قواعد سلوك قام مشغلو شبكات الاتصالات ومزودي الخدمات بصياغتها.

أي يجب حماية حقوق المستخدمين بموجب القوانين التي تكون الخدمات ملزمة بالامتثال لها والتوافق معها، كما يجب مراقبة هذه القوانين وإنفاذها بطريقة شفافة وإخضاعها للمساءلة. وأخيراً، يجب ضمان وصول المستخدمين إلى سبل التعويض (الانتصاف والجبر).

2. أمّا بخصوص شروط الخدمة التي يتم وضعها من قبل مشغلي شبكات الاتصالات الإلكترونية ومزودي الخدمات، نقترح أن يتم الإشارة فيها إلى الخطوات الملموسة التي سيتم اتخاذها من أجل الامتثال لهذا القانون.

3. كما نقترح إدراج معايير لتقييم التطبيقات والخدمات في حالة عدم امتثال تطبيق دولي على سبيل المثال لشروط الخدمة، إضافة إلى الخطوات المترتبة على ذلك إذ أن هذا الأمر مرتبط بالإنفاذ والتطبيق ولا بدّ من الإشارة إليه لتجنب الوقوع في أي لبس.

ثالثاً:

الفصل (226) والذي نصّ في الجزئية الأخيرة منه على "يمنع الاعتراض أو التنصت أو التسجيل أو الاستنساخ لمراسلات عبر الشبكات العمومية للاتصالات الإلكترونية"، في هذا السياق نقترح مايلي:

1. إلى جانب الاعتراض، التنصت، التسجيل، استنساخ المراسلات فإننا نقترح إضافة "التدخّل" في إحدى هذه الأفعال¹²

¹¹ مدونة قواعد السلوك: هي الممارسات العامة غير الملزمة، يتم الاتفاق عليها بين القطاعات الصناعية لمعالجة مسألة ما. شروط الخدمات: هي شروط التي يتم تحديدها وفقاً لتقدير الخدمة التي يتم فرضها على المستخدمين، في كثير من الأحيان بطريقة غير شفافة.

¹² الإعلان العالمي لحقوق الإنسان (1948)، المادة (19).

<http://www.un.org/ar/universal-declaration-human-rights/index.html>

2. نقترح تعديل "عبر الشبكات العمومية للاتصالات الإلكترونية" لتشمل الشبكات الأخرى التي لا تعتمد بالضرورة على الإنترنت. إذ أن هذا الأمر لا يتعلق بشكل كلي بالاتصال عبر الإنترنت فقط، فمن الناحية التقنية، يستخدم بروتوكول نقل الصوت عبر الإنترنت (VoIP) أيضاً جزءاً من شبكة الهاتف، وهذا ينطبق أيضاً على التطبيقات الأخرى التي تعتمد على شبكة هاتف الميبل الأخير لإيصال الاتصالات.

رابعاً:

الفصل (225) والذي نصّ على "مع احترام مقتضيات الأمن والدفاع الوطني وصلاحيات السلطة القضائية، يتعين على مشغلي الشبكات العمومية للاتصالات الإلكترونية ومزودي الخدمات احترام سرية المراسلات عبر هذه الشبكات وحماية المعطيات الشخصية والحياة الخاصة لمستخدميها"، في هذا السياق فإن النقطة التي نقترح تعديلها كالآتي:

يشمل النص فيما يتعلق باحترام سرية المراسلات كل من مزودي خدمات الإنترنت ومشغلي الشبكات العمومية للاتصالات الإلكترونية، الأمر الذي يعني أن تطبيقات المراسلة مكلفة باحترام السرية إلا في حالات الأمن القومي والطلب القضائي.

استناداً لذلك، نقترح أن يمتد الإلتزام باحترام سرية المراسلات (في مقتضيات الأمن والدفاع الوطني) إلى ما هو "معقول"¹³. هذا يعني أن الحكومة يجب ألا تكون قادرة على تفويض استثناءات غير متناسبة أو غير ضرورية للسرية؛ (مثل كسر التشفير على سبيل المثال¹⁴).

خامساً:

الفصل (228) والذي نصّ على "يتعين على الهيئة الوطنية لحماية المعطيات الشخصية الحصول على رأي الهيئة الوطنية للاتصالات الإلكترونية المسبق في كل قرار متعلق بمبادلات عبر الشبكات العمومية للاتصالات الإلكترونية من شأنها المساس بحماية المعطيات الشخصية لمستخدمي الخدمات وحياته الخاصة"، في هذا السياق فإن النقطة التي نقترح تعديلها كالآتي:

لابد من الإشارة إلى أنّ الهيئة الوطنية لحماية البيانات الشخصية وبصفتها هيئة مَنحت الاختصاص بموجب القانون الأساسي عدد 63 لسنة 2004 مؤرخ في جويلية 2004 المتعلق بحماية المعطيات الشخصية، وكونها المختصة بالنظر في القضايا المتعلقة بالمعطيات الشخصية. إلا أنّ النص القانوني في هذا الفصل أعطى الهيئة الوطنية للاتصالات الإلكترونية صلاحية إبداء الرأي في كل قرار يتعلق بمبادلات عبر الشبكات العمومية للاتصالات الإلكترونية والتي من شأنها المساس بحماية المعطيات الشخصية وذلك على عكس القاعدة الأصلية والأساسية التي تعطي للهيئة الوطنية لحماية المعطيات الشخصية صلاحية¹⁵ إبداء رأيها في القضايا التي تمس بالمعطيات الشخصية. بناءً على ذلك نقترح تعديل النص القانوني ليصبح كالآتي: "يتعين على الهيئة الوطنية للاتصالات الإلكترونية الحصول على رأي الهيئة الوطنية لحماية المعطيات الشخصية المسبق في كل قرار متعلق بمبادلات عبر الشبكات العمومية للاتصالات الإلكترونية من شأنها المساس بحماية المعطيات الشخصية لمستخدمي الخدمات

¹³ IEEE (2018) Statement on strong encryption

<https://globalpolicy.ieee.org/new-ieee-position-statement-supports-strong-encryption-for-confidentiality-and-data-integrity/>, Access Now (2018) Crypto Colloquium Outcomes Report <https://www.accessnow.org/cms/assets/uploads/2018/02/Encryption-in-the-United-States-Crypto-Colloquium-Outcomes-Report.pdf>

¹⁴ Amie Stepanovich and Michael Karanicolas (2018) Why an encryption backdoor for just the "good guys" won't work. <https://www.justsecurity.org/53316/criminalize-security-criminals-secure/>

¹⁵ مصدر سابق، الباب السادس في الهيئة الوطنية لحماية المعطيات الشخصية، الفصل 76.

و حياته الخاصة" إذ أن رأي الهيئة الوطنية لحماية المعطيات الشخصية ملزماً وليس العكس.

سادساً:

الفصل (235) والذي نصّ على "يتحمل ناشرو المحتويات على الإنترنت وعلى الشبكات الإلكترونية المسؤولية المدنية أو الجزائية طبق الأحكام التشريعية الجاري بها العمل" إضافةً إلى الفصل (236) والذي نصّ على "يتحمل مشغلو المنصات الرقمية المسؤولية المدنية و الجزائية عن المحتويات التي ينشرونها وعن الخدمات التي يوفرنها طبق الأحكام التشريعية الجاري بها العمل" في هذا السياق نقترح مايلي:

1. فيما يتعلق بالفصل (235) فإن ما يتم نشره من قبل مستخدمي الشبكات الإلكترونية يتم توجيهه إلى محتوى ناتج عن طريق مستخدم، الأمر الذي يعني على سبيل المثال أن التغريدات على "تويتر" سيترتب عليها تحمل المسؤولية الجنائية أو المدنية.

إذ لم يتم في هذا الفصل تحديد طبيعة القواعد والاستثناءات لكل من المسؤولية المدنية والجنائية. إذ أن هذا الأمر من شأنه أن يحفز اتخاذ شروط الخدمة التي يضعها كل من مشغلي الشبكات ومزودي الخدمات كمنصة للحد من الحريات الأساسية كحق التعبير عن الرأي. فقد جاء النص شاملاً لجميع المحتويات التي يتم نشرها وما يترتب عليها من تبعات كتحمل المسؤولية الجنائية والمدنية.

2. فيما يتعلق بالفصل (236) نظراً لعدم وضوح النص السابق، إذ يتضح أن نص هذه المادة يتعارض مع نص المادة الواردة أعلاه (235) نظراً لإمكانية وقوع إشكالية في التفريق بين الجهة التي ستتحمل المسؤولية، إذ لا بد من وضع محددات واستثناءات لكل من المسؤولية الجنائية والمدنية في كلا الفصلين.

3. يمكن للغة المقترحة في كل من الفصلين (235) و (236)، أن تخلق عبئاً (غير متناسب) على الخدمات التي تعتمد على شبكة الإنترنت كما أنها قد تشكل حافزاً للخدمات لمراقبة المحتوى و/ أو إزالته، الأمر الذي سيؤثر سلباً على كل من الحق في الخصوصية وحرية التعبير والحق في الوصول إلى المعلومات¹⁶.

4. إن المنصات الرقمية القائمة على الخوف من تحمل المسؤوليات والعقوبات، ستشكل في الواقع حافزاً اقتصادياً لإزالة العديد من المحتويات الأخرى بشكل تدريجي. واستناداً لما تقدم، فلا بد من وجود عملية قانونية قائمة على أساس سيادة القانون، إلى جانب وجود ضوابط وتوازنات مناسبة للحد من هذه المخاطر¹⁷.

5. بالإضافة إلى ذلك، لا ينبغي أن تكون المنصة الرقمية مسؤولة جنائياً عن المحتوى الذي تم تحميله من قبل طرف أو جهة ثالثة. فعندما تكون المنصات الرقمية مسؤولة عن أنشطة مستخدميها على الإنترنت، فإن هذا الأمر يعد شكلاً من أشكال الرقابة والتي بدورها تؤثر سلباً على الابتكار وحرية التعبير عبر منصات التواصل الاجتماعي. كما أن المنصات القائمة على الخوف الدائم من التعرض للمسائلة الجنائية من شأنها أن تؤثر على النمو الاقتصادي خاصة فيما يتعلق بالمنصات القائمة على إدارة الأعمال. بالإضافة لذلك، فإن أغلب الحكومات في مختلف دول العالم والإجماع العام حول موضوع "الانترنت الجيد" عملوا بجهد من أجل احترام حقوق الإنسان وخاصة الحق المتمثل بأنه لا يجب أن تكون هناك أية مسؤولية جنائية مفروضة على المنصات الرقمية استناداً لمحتواها.

¹⁶ الحقوق الرقمية الأوروبية (2014) حقوق الإنسان وخصخصة إنفاذ القانون.

https://edri.org/wp-content/uploads/2014/02/EDRi_HumanRights_and_PrivLaw_web.pdf

¹⁷ مصدر سابق.

فيما يتعلق بالباب الثالث و الذي يتعلق بحوكمة الإنترنت والقسم الثاني منه والذي يتعلق بمنتهى الإنترنت، فإن التعليق/ الاقتراح الذي نود إدراجه وأخذُه بعين الاعتبار كالاتي:

الفصل (246) والذي نصّ على "يضم منتهى الإنترنت ثلاثين شخصية ذات مهارات وخبرة في مجال الانتقال الرقمي يوزعون كالتالي:- عشر شخصيات من القطاع العام، عشرون شخصية من القطاع الخاص والأكاديمي والجمعياتي. يتم انتخاب أعضاء منتهى الإنترنت من القطاع الخاص من قبل مستخدمي الإنترنت عن طريق التصويت الإلكتروني عن بعد، يتم تعيين الأعضاء من القطاع العام من قبل الوزير المكلف بالاتصالات الإلكترونية. يتم انتخاب رئيس المنتهى من بين أعضائه بالأغلبية. ويصادق منتهى الإنترنت على نظامه الداخلي بالأغلبية. وتحدد شروط وإجراءات تعيين الأعضاء ورئيس المنتهى وبيان الموارد المادية والبشرية الموضوعة على ذمته بمقتضى أمر حكومي" في هذا السياق فإن النقطة التي نقترح تعديلها كالاتي:

يجب ابتداءً أن يتم التأكد من أن كل فئة من فئات أصحاب المصلحة التي يضمها منتهى الإنترنت متساوية في التمثيل النسبي، بحيث لا ينتهي الأمر مع 18 شركة من القطاع الخاص، ومنظمة غير حكومية أو جمعية واحدة وأكاديمية واحدة و 10 شخصيات من القطاع العام. لذلك نقترح أن يتم تعديل عدد الشخصيات في المنتهى، بحيث يكون عدد الشخصيات وأصحاب المصلحة في كل من القطاع العام و القطاع الخاص والأكاديمي والجمعياتي متساوٍ في التمثيل. (على سبيل المثال: 6 من القطاع العام، 6 من القطاع الخاص، 6 من القطاع الأكاديمي، و 6 من القطاع الجمعياتي = 24 شخصية موزعة بالتساوي)

فيما يتعلق بالباب الثالث و الذي يتعلق بالأعمال الإلكترونية والقسم الثاني منه والذي يتعلق بالتبادل الإلكتروني بين الهياكل العمومية وبينها وبين المتعاملين معها والفرع الثالث المتعلق بتبادل المعطيات والوثائق، فإن التعليقات والإقتراحات التي نود إدراجها وأخذها بعين الاعتبار كالاتي:

أولاً:

الفصل (276) والذي نصّ على " إذا حدث طارئ من شأنه أن يمسّ سلامة أنظمة المعلومات والاتصال المؤمّنة لتبادل المعطيات أو محتواها، فعلى الهيكل العمومي المعني أن يتخذ الإجراءات الكفيلة ببدء ذلك الخطر وأن يبادر بإيقاف عملية التبادل مؤقتاً. ويتولى الهيكل العمومي المعني إعلام طالب الخدمة بذلك التوقف بإحدى وسائل الاتصال المتاحة له" في هذا السياق نقترح مايلي:

1. فيما يتعلق بالالتزام بالإخطار في حالة وقوع انتهاك (إخطار بالانتهاك) فيجب ألا يكون الإخطار حكرًا على الهيكل العمومي، إذ يجب بالتوافق مع مشروع قانون حماية المعطيات الشخصية أن تكلف الهيئة¹⁸ بذلك وأن تتخذ الإجراءات المترتبة على انتهاك المعلومات كونها الجهة صاحبة الاختصاص. إذ قد يتعارض هذا الأمر في نهاية المطاف مع مشروع قانون حماية المعطيات الشخصية.
2. لا بدّ من الإشارة إلى المدة الزمنية المتعلقة بالإخطار، أي تحديد الأجل الزمني للإخطار¹⁹ حتى لا يتم المسّ بسلامة المعطيات أو محتواها إذ لم تتناسب المدة الزمنية مع الغاية التي وضعت من أجلها وهي حماية المعطيات والتأكد من سلامتها²⁰.

ثانياً:

¹⁸ مصدر سابق، القسم الثاني. في المسؤول عن معالجة المعطيات الشخصية وواجباته، الفصل 21.

¹⁹ مصدر سابق، القسم الثاني. في المسؤول عن معالجة المعطيات الشخصية وواجباته، الفصل 21.

²⁰ مصدر سابق، القسم الثاني. في المسؤول عن معالجة المعطيات الشخصية وواجباته، الفصل 21.

الفصل (277) والذي نصّ على "ويؤمن الهيكل العمومي المحدث لهذا الفضاء سرية وسلامة المعطيات المخزنة به عن طريق اتخاذ التدابير الكفيلة بمنع النفاذ غير المشروع إليه" في هذا السياق فإن النقطة التي نقترح تعديلها كالآتي:

تستخدم مصطلحات السرية بشكل أكثر شيوعاً في القطاع المصرفي، من أجل الوضوح واليقين القانوني، إلا أننا ننصح هنا باستخدام اللغات التي تشير إلى حقوق الإنسان والمعايير الفنية. نقترح استخدام: "الخصوصية والأمن وسلامة البيانات والبنية التحتية"

فيما يتعلق بالباب الثاني والذي يتعلق بالعقوبات الجزائية ، فإن التعليقات والإقتراحات التي نود إدراجها وأخذها بعين الاعتبار كالآتي:

أولاً:

الفصل (290) والذي نصّ على " يعاقب بخطية من ألف إلى خمسة آلاف دينار كل من قام عن غير عمد بإتلاف أو إفساد خطوط أو أجهزة الاتصالات الإلكترونية بأية طريقة كانت" و "كل من تسبب عمداً في تعطيل الاتصالات بقطع خطوط الربط أو إفساد أو إتلاف التجهيزات بأية طريقة كانت" في هذا السياق نقترح مايلي:

1. إن تجريم الأفعال والحوادث غير المقصودة وفرض العقوبات على الأفعال التي وقعت دون وجود نية للإخلال بالقانون أو الإقدام على فعل غير مشروع يعتبر أمراً تعسفياً، الأمر الذي سيؤثر على قوة ومثانة النص القانوني. على هذا الأساس نقترح أن يتم الإشارة فقط إلى تجريم الأفعال التي تقع بقصد، وإزالة النص القانوني المتعلق بتجريم الأفعال غير المقصودة.

2. أما فيما يتعلق بتعطيل الاتصالات من خلال إفساد أو إتلاف المعدات، فإن النص القانوني لم يوضح المقصود ب"المعدات"، وما إذا كان هذا النص ينطبق على المعدات التي في أيدي ومتناول المستخدمين أيضاً. إذ يمكن أن يكون هذا النص القانوني رادعاً للوصول إلى شبكة الإنترنت إذا كانت الأجهزة والمعدات المذكورة في مشروع القانون تشمل الهواتف المحمولة أو أجهزة الكمبيوتر المعدة والمخصصة للاستخدام الخاص.

ثانياً:

الفصل (292) والذي نصّ على "يعاقب بالسجن لمدة تتراوح بين شهر واحد وستة أشهر و بخطية من ألف إلى عشرة آلاف دينار أو بإحدى هاتين العقوبتين، كل من صنع للسوق الداخلية أو استورد أو حاز لأجل البيع أو التوزيع مجاناً أو بمقابل أو عرض للبيع أو باع الأجهزة الراديوية و ربطها بشبكة عمومية للاتصالات الإلكترونية دون الحصول على المصادقة من طرف الهيئة المختصة" في هذا السياق فإن النقطة التي نقترح تعديلها كالآتي:

نقترح إضافة استثناء إلى هذه القاعدة فيما يتعلق بالأبحاث الأكاديمية و/أو الأمنية²¹ المستخدمة في ذات الغرض.

²¹ Various authors (2016) Digital Rights Organizations Express Concerns Over Election Reform in Argentina

<https://www.accessnow.org/organizaciones-latinoamericanas-de-derechos-digitales-expresan-preocupacion-por-la-reforma-electoral-argentina/>.