موجز عن تأثير قانون المعاملات الإلكترونية على الإنترنت في ليبيا

قانون رقم 6 لسنة 2022

موجز عن تأثير قانون المعاملات الإلكترونية على الإنترنت في ليبيا

قانون رقم 6 لسنة 2022

الفهرس

المقدمة 1

التحليل 1
التأثير على الخصائص الهامة لIWN 2

رؤى رئيسية 5

ملخص 5

خاتمة 6

توصيات للإصلاح 7
تعزيز حماية الخصوصية 7
تعزيز سرية البيانات 7
تعزيز الحوكمة التعاونية 7
ضمان الوصول غير المقيد 7

دعوة لإجراء تقييم شامل لتأثير الإنترنت 8

المساهمين 8

ليبيا القانون رقم 2022/6 التحليل باستخدام IIAT 9
الخصائص الحرجة لـ IWN 9
عوامل تمكين الإنترنت OGST 10

المقدمة

يقيّم موجز تأثير الإنترنت قانون المعاملات الإلكترونية الليبي رقم 6 لسنة 2022 (الطبعة العربية) باستخدام مجموعة أدوات تقييم تأثير الإنترنت (IIAT). وهو عبارة عن منهجية طورتها جمعية الإنترنت لتقييم القوانين والسياسات في ضوء الخصائص المهمة لطريقة الإنترنت للتواصل (IWN) وعوامل تمكين الإنترنت المفتوحة والمتصلة عالميًا والآمنة والجديرة بالثقة (OGST). وبينما يسعى القانون إلى تعزيز الأمن السيبراني وتنظيم المعاملات الرقمية، فإنه يثير مخاوف بشأن تأثيره على الخصوصية وسرية البيانات والحوكمة اللامركزية والوصول غير المقيد. يوضح هذا التحليل كيف يمكن لأحكام القانون أن تقوّض الخصائص الأساسية للإنترنت وتحد من دورها كمنصة شاملة وتمكينية. ويدعو الموجز إلى إجراء إصلاحات مستهدفة لمواءمة القانون مع مبادئ الإنترنت العالمية مع ضمان الأمن وإمكانية الوصول لجميع الليبيين.

التحليل

يقدم قانون المعاملات الإلكترونية الليبي رقم 6 لسنة 2022 تدابير تهدف إلى تنظيم المعاملات الرقمية وتعزيز الأمن السيبراني. ومع ذلك، يكشف التحليل باستخدام مجموعة أدوات تقييم تأثير الإنترنت (IIAT) عن تأثيرها الكبير على الخصائص المهمة لطريقة الإنترنت في التواصل (IWN) وعوامل تمكين الإنترنت المفتوحة والمتصلة عالميًا والآمنة والجديرة بالثقة (OGST). وفي حين يهدف القانون إلى تعزيز الأمن والتحديث الرقمي، فإنه يشكل مخاطر على الخصوصية، وسرية البيانات، والحوكمة التعاونية، والوصول غير المقيد، وبالتالي يهدد المبادئ الأساسية للإنترنت ودورها كأداة للتمكين والابتكار.

التأثير على الخصائص الهامة لIWN

واحدة من الخصائص الهامة لـ IWN، بنية تحتية يمكن الوصول إليها ببروتوكول مشترك، ويدعمها القانون جزئيا. ويؤدي تعزيز الخدمات العامة الإلكترونية إلى تعزيز إمكانية الوصول من خلال تشجيع رقمنة الوظائف الحكومية. ومع ذلك، يفرض القانون تدابير تقييدية على التشفير، مثل اشتراط الحصول على تصاريح لأدوات التشفير (المادتان 9 و39). تقوض هذه القيود إمكانية الوصول إلى أدوات الاتصال الآمنة، مما يؤثر بشكل غير متناسب على المستخدمين الذين يعتمدون على الإنترنت في التفاعلات الحساسة. ونتيجة لذلك، فبينما تتحسن البنية الأساسية العامة، تتضاءل ثقة المستخدم في التفاعلات الآمنة عبر الإنترنت.

الخصائص الأساسية لشبكة الإنترنت العالمية (IWN) تُحدد السمات التأسيسية المطلوبة لإنترنت قوي وشامل. بموجب القانون رقم 4، تبرز عدة تحديات في الحفاظ على هذه الخصائص.

أولاً، يدعم القانون جزئيًا بنية تحتية قابلة للوصول مع بروتوكول مشترك، من خلال توحيد جمع وتوثيق المعلومات بين الجهات المختلفة. هذا الجهد يُساهم في إنشاء نظام متكامل يمكنه دعم تبادل البيانات. ومع ذلك، فإن نموذج الإدارة المركزية يُقيد الوصول الأوسع، حيث يُسمح فقط للجهات المصرح لها بالتفاعل مع النظام، مما يجعله أقل شمولية وأقل توافقًا مع البروتوكولات العالمية التي تُركز على الوصول المفتوح.كما يؤثر القانون سلباً على البنية المفتوحة للبنات البناء القابلة للتشغيل البيني وقابلة لإعادة الاستخدام من الإنترنت. ومن خلال تقييد الوصول إلى مواقع الويب والبيانات الرقمية دون موافقة المالك (المادة 5)، يعيق القانون التبادل السلس للمعلومات، وهو أمر ضروري لطبيعة الإنترنت المفتوحة والقابلة للتشغيل البيني. وفي حين تهدف هذه الأحكام إلى تعزيز حماية

البيانات، فإن التنفيذ الصارم بشكل مفرط يهدد بخلق حواجز أمام تبادل المعلومات والابتكار، وتقويض البنية المفتوحة التي تجعل الإنترنت منصة قوية للتعاون والنمو.

خاصية رئيسية أخرى تواجه تحديات كبيرة بموجب القانون وهي الإدارة اللامركزية وأنظمة التوجيه الموزعة الفردية. إن صلاحيات المراقبة المركزية الممنوحة في المادة 7 تضع سيطرة كبيرة في أيدي السلطات، مما يعطل نموذج الإدارة اللامركزية المتأصل للإنترنت. تخلق مثل هذه المركزية اختناقات محتملة، مما يقلل التنوع في إدارة المحتوى ويحد من استقلالية التوجيه. وهذا التحول من الحكم اللامركزي لا يؤدي إلى خنق الابتكار فحسب، بل يزيد أيضا من خطر سوء الاستخدام والتجاوز، مما يؤدي إلى المزيد من تآكل ثقة المستخدم.

القانون يتجاهل أهمية المعرفات العالمية المشتركة مثل عناوين IP وأسماء النطاقات، مما يسمح لخاصية الإنترنت هذه بالبقاء غير متأثرة إلى حد كبير. ومع ذلك، فإن الحفاظ على هذه الخاصية الحيوية لا يخفف من المخاوف الأوسع الناجمة عن أحكام القانون الأخرى. وفي المقابل، دور الإنترنت كشبكة ذات أغراض عامة محايدة تكنولوجياً يتعرض للخطر بشكل كبير. يفرض القانون قيودًا واسعة النطاق على المحتوى بناءً على معايير محددة بشكل غامض، مثل حظر المقامرة والمخدرات والمحتوى المرتبط بالبغاء (المواد 8 و31 و33). تتجاوز هذه القيود الأنشطة القانونية وتعوق قدرة الإنترنت على التكيف وسهولة الاستخدام كمنصة للمحتوى والخدمات المتنوعة.

وبالانتقال إلى العوامل التمكينية لإنترنت OGST، فإن القانون له آثار عميقة على الخصوصية. تسمح المادتان 7 و39 بمراقبة واسعة النطاق

وتفـرض قيـودًا علـى التشـفير، ممـا يسـمح للسـلطات بالوصـول علـى نطـاق واسـع إلـى الاتصـالات والبيانـات الشـخصية. تنتهـك هـذه الإجراءات حقـوق الخصوصيـة، ممـا يمنـع المسـتخدمين مـن الانخـراط فـي أنشـطة آمنـة وحساسـة عبـر الإنترنـت. وبـدون ضمانـات كافيـة أو رقابـة قضائيـة، يُضعف القانون الثقة في الإنترنت كوسيلة آمنة ومأمونة للاتصال.

وبالمثـل، يقـوض القانـون سـرية البيانـات، حجـر الزاويـة فـي التفـاعلات الآمنـة عبـر الإنترنـت. إن حقـوق المراقبـة الواسـعة إلـى جانـب ضوابـط التشـفير، تهـدد قـدرة المسـتخدمين علـى حمايـة المعلومـات الحساسـة، سـواء كانـت شـخصية أو مهنيـة. وهـذا التـآكل فـي السـرية لا يشـجع علـى المشـاركة فـي المنصـات الإلكترونيـة، وخاصـة بيـن الفئـات الضعيفـة مثـل الصحفييـن والناشـطين ومنظمـات المجتمـع المدنـي، الذيـن يعتمدون على قنوات آمنة في عملهم.

القانـون يقيـد أيضـا الحوكمـة التعاونيـة، وهـي السـمة المميـزة لطبيعـة الإنترنـت اللامركزيـة والشـاملة. ومـن خلال مركزيـة المراقبـة والإنفـاذ تحـت سـلطة واحـدة (المـادة 7) يسـتبعد القانـون مشـاركة أصحـاب المصلحـة المتعدديـن مـن العمليـات التنظيميـة. وتعتمـد الحوكمـة التعاونيـة علـى مسـاهمات مـن مختلـف أصحـاب المصلحـة، بمـا فـي ذلـك المجتمـع المدنـي والقطـاع الخـاص والخبـراء الفنييـن، لضمـان الشـفافية والشـمولية والابتـكار. ويـؤدي الافتقـار إلـى مثـل هـذه المـدخلات إلـى إضعـاف نمـوذج الحوكمـة، ممـا يقلـل مـن فـرص صنـع السياسات التكيفية والتطلعية.

وأخيـراً، يشـكل القانـون تحديـات كبيـرة أمـام الوصـول غيـر المقيـد إلـى الإنترنـت. يسـمح تجـاوز الولايـة القضائيـة (المـادة 3) بتطبيـق القانـون علـى الإجـراءات التـي تنشـأ خـارج ليبيـا، ممـا قـد يعـزل المسـتخدمين الليبييـن عـن المـوارد العالميـة. بالإضافـة إلـى ذلـك، فـإن الحظـر الانتقائي

للمحتوى (المادتان 8 و31) يحد من قدرة المستخدمين على الوصول إلى المعلومات والخدمات المتنوعة، مما يقلل من دور الإنترنت كأداة للتعليم والتبادل الثقافي والفرص الاقتصادية.

في الختام، فإن قانون المعاملات الإلكترونية الليبي رقم 6 لسنة 2022، رغم سعيه لمعالجة الأمن السيبراني والتحديث الرقمي، يؤثر سلبًا على الخصائص والعوامل التمكينية الحيوية للإنترنت. إن أحكامها المتعلقة بالمراقبة والتشفير والحوكمة والوصول إلى المحتوى تقوض الخصوصية وسرية البيانات والحوكمة التعاونية والوصول غير المقيد. وتهدد هذه التأثيرات المبادئ الأساسية للإنترنت وقدرتها على العمل كمنصة شاملة وتمكينية لمستقبل ليبيا الرقمي.

رؤى رئيسية

يؤثر قانون المعاملات الإلكترونية الليبي رقم 6 لسنة 2022 بشكل كبير على الخصائص الأساسية للإنترنت وممكناتها. وفي حين تهدف إلى تعزيز الأمن السيبراني، فإن أحكامها المتعلقة بالتشفير والمراقبة المركزية وقيود المحتوى تقوض الانفتاح والخصوصية والحوكمة التعاونية. إن تبني الإصلاحات للحد من المراقبة، وضمان إمكانية الوصول إلى التشفير، وتضييق قيود المحتوى أمر ضروري لمواءمة القانون مع مبادئ حوكمة الإنترنت العالمية. ستعمل هذه التغييرات على تعزيز شبكة إنترنت آمنة ومفتوحة تمكن المستخدمين وتدعم التحول الرقمي في ليبيا.

ملخص

يسعى قانون المعاملات الإلكترونية الليبي رقم 6 لسنة 2022 إلى تنظيم المعاملات الرقمية وتعزيز الأمن السيبراني في مجتمع رقمي

متزايـد. وفـي حيـن أن القانـون يعـزز رقمنـة الخدمـات ويعـزز بعـض التدابيـر الأمنيـة، فإنـه يفـرض قيـودًا كبيـرة علـى الخصوصيـة، وسـرية البيانـات، والحوكمـة التعاونيـة، والوصـول غيـر المقيـد إلـى المـوارد عبـر الإنترنـت. إن أحـكام مثـل سـلطة المراقبـة المركزيـة، والقيـود الواسـعة النطـاق علـى المحتـوى، وضوابـط التشـفير، تعمـل علـى تقويـض المبـادئ الأساسـية للإنترنـت، وتهـدد انفتاحهـا وشـموليتها وقدرتهـا علـى التكيـف. ورغـم أن هـذه التدابيـر تهـدف إلـى معالجـة تهديـدات الأمـن السـيبراني، فإنهـا تخاطـر بخنـق الابتـكار، وعـزل المسـتخدمين الليبييـن عـن الإنترنـت العالمي، وتقويض الثقة في منصات الإنترنت.

يسـلط تحليـل مجموعـة أدوات تقييـم تأثيـر الإنترنـت (IIAT) الضـوء علـى أن القانـون يتعـارض مـع الخصائـص المهمـة لطريقـة الإنترنـت للتواصـل (IWN) وعوامـل تمكيـن الإنترنـت المفتوحـة والمتصلـة عالميًـا والآمنـة والجديـرة بالثقـة (OGST). ومـن خلال إعطـاء الأولويـة للسـيطرة المركزيـة والمراقبـة الواسـعة علـى الحكـم اللامركـزي وحقـوق المسـتخدمين، فـإن القانـون يعيـق التحـول الرقمـي فـي ليبيـا وإمكانـات الإنترنـت كأداة تمكينية للتنمية الاجتماعية والاقتصادية.

خاتمة

تفـرض الأحـكام الحاليـة لقانـون المعـاملات الإلكترونيـة الليبـي رقـم 6 لسـنة 2022 مخاطـر كبيـرة علـى المبـادئ الأساسـية للإنترنـت وحقـوق المسـتخدم. وفـي حيـن أن معالجـة المخـاوف المتعلقـة بالأمن السـيبراني أمـر بالـغ الأهميـة، فـإن التدابيـر التقييديـة التـي يفرضهـا القانـون تهـدد انفتـاح الإنترنـت ومصداقيتـه، وتمنـع المشـاركة عبـر الإنترنـت وتحـد مـن الوصـول إلـى المـوارد العالميـة. وبـدون ضمانـات كافيـة للخصوصيـة والشـفافية والحوكمـة التعاونيـة، فـإن القانـون قـد يعيـق قـدرة ليبيـا علـى الاستفادة من الإنترنت لتحقيق النمو الشامل والابتكار.

توصيات للإصلاح

1. تعزيز حماية الخصوصية:

- قصر صلاحيات المراقبة على حالات محددة مع رقابة قضائية صارمة وآليات شفافية.
- السماح بالاستخدام غير المقيد لأدوات التشفير لتمكين الاتصال الآمن للأفراد والمؤسسات.

2. تعزيز سرية البيانات:

- إزالة متطلبات تصاريح التشفير لتمكين المستخدمين من حماية الاتصالات الحساسة دون عوائق بيروقراطية.
- فرض عقوبات على انتهاكات البيانات غير المصرح بها مع ضمان الضمانات ضد سوء استخدام صلاحيات المراقبة.

3. تعزيز الحوكمة التعاونية:

- تحقيق اللامركزية في سلطة المراقبة وإنشاء أطر حوكمة لأصحاب المصلحة المتعددين والتي تشمل المجتمع المدني والخبراء الفنيين والقطاع الخاص.
- تشجيع صنع السياسات الشاملة التي تعطي الأولوية للشفافية وتعزز الابتكار.

4. ضمان الوصول غير المقيد:

- تضييق نطاق قيود المحتوى من خلال تحديد الأنشطة المحظورة بوضوح لتجنب تجاوزها.
- إزالة الأحكام التي تطبق القانون خارج الحدود الإقليمية لحماية الوصول إلى الموارد العالمية.

دعوة لإجراء تقييم شامل لتأثير الإنترنت

لتقييم الآثار الكاملة للقانون وتوجيه الإصلاحات، يوصى بإجراء تقييم شامل لتأثير الإنترنت. وينبغي لهذا التقييم أن يُبنى على:

- دراسة كيفية توافق القانون مع المعايير العالمية لإدارة الإنترنت وحقوق الإنسان.
- تحديد المخاطر المحددة التي تهدد وظائف الإنترنت وثقة المستخدم والابتكار.
- إشراك مجموعة واسعة من أصحاب المصلحة، بما في ذلك الوكالات الحكومية والمجتمع المدني والخبراء الفنيين والمنظمات الدولية، لضمان توصيات متوازنة وشاملة.

ومن خلال إجراء مثل هذا التقييم وتنفيذ الإصلاحات المقترحة، تستطيع ليبيا إنشاء إطار قانوني يعالج تهديدات الأمن السيبراني مع الحفاظ على انفتاح الإنترنت وأمنه وقدرته على دفع التقدم الاقتصادي والاجتماعي.

المساهمين:

تمت قيادة هذا التحليل من قبل أمجدبدر الشويهدي ممول من قبل مبادرة أنير بالتعاون مع جمعية الإنترنت ليبيا ومع عدد من أصحاب المصلحة من المؤسسات الحكومية والمجتمع المدني والأكاديميين والناشطين ومستخدمي الإنترنت.

ليبيا القانون رقم 6/2022 التحليل باستخدام IIAT

الخصائص الحرجة لـ IWN (طريقة الإنترنت للتواصل)

الخصائص الحرجة لـ IWN	تأثير؟	وإذا كان التأثير لماذا؟
بنية تحتية يمكن الوصول إليها باستخدام بروتوكول مشترك	مختلط	يشجع القانون على رقمنة الخدمات العامة، وتعزيز إمكانية الوصول إليها للمستخدمين. ومع ذلك، فإن القيود المفروضة على التشفير (المادتان 9 و39) وصلاحيات المراقبة الواسعة (المادة 7) تقوض إمكانية الوصول عن طريق تقليل الثقة في التفاعلات الآمنة عبر الإنترنت.
بنية مفتوحة لبنات البناء القابلة للتشغيل البيني والقابلة لإعادة الاستخدام	سلبي	القيود المفروضة على الوصول إلى مواقع الويب والبيانات دون موافقة المالك (المادة 5) تدعم حماية البيانات ولكنها قد تحد من إمكانية التشغيل البيني، حيث أن الضوابط الصارمة للغاية تعيق التبادل المفتوح للمعلومات الضرورية لوظائف الإنترنت.
الإدارة اللامركزية ونظام التوجيه الموزع الفردي	سلبي	سلطات المراقبة والتنفيذ المركزية (المادتان 7 و 8) تقوض الإدارة اللامركزية. يمكن أن تؤدي هذه المركزية إلى اختناقات، وتقليل استقلالية التوجيه، وخنق تنوع المحتوى.
المعرفات العالمية المشتركة	حيادي	لا يؤثر القانون بشكل مباشر على المعرفات العالمية مثل عناوين IP وأسماء النطاقات، مما يسمح باستمرارية نظام المعرفات العالمية.
شبكة محايدة تكنولوجياً ذات أغراض عامة	سلبي	الأحكام التي تحظر المحتوى مثل المقامرة والمخدرات (المواد 8 و31 و33) تقيد طبيعة الأغراض العامة للشبكة، مما قد يحد من المحتوى والخدمات المشروعة بناءً على معايير فضفاضة وغامضة.

عوامل تمكين الإنترنت TSGO (المفتوح والمتصل عالميًا والآمن والجدير بالثقة)

تمكين الإنترنت OGST	تأثير؟	وإذا كان التأثير لماذا؟
وصول سهل وغير مقيد	نعم	**الاختصاص الواسع (المادة 3) والحجب الانتقائي للمواقع يحد من الوصول إلى الموارد العالمية ويعزل المستخدمين الليبيين عن المحتوى المتنوع.**
الاستخدام غير المقيد ونشر تقنيات الإنترنت	نعم	**ضوابط التشفير وأذونات المراقبة (المواد 9 و39 و7) تحد من قدرة المستخدمين على الاستفادة من تقنيات تعزيز الخصوصية، وتقييد الاستخدام الآمن والمبتكر للإنترنت.**
التنمية التعاونية والإدارة والحوكمة	نعم	**إن مركزية سلطة المراقبة (المادة 7) تقلل من تعاون أصحاب المصلحة المتعددين وتعرقل الحوكمة الشاملة، وهي السمات المميزة لإدارة الإنترنت.**
إمكانية الوصول غير المقيدة	سلبي	**الاختصاص الواسع (المادة 3) والحجب الانتقائي للمواقع يحد من الوصول إلى الموارد العالمية ويعزل المستخدمين الليبيين عن المحتوى المتنوع.**
القدرة المتاحة	سلبي	ضوابط التشفير وأذونات المراقبة (المواد 9 و39 و7) تحد من قدرة المستخدمين على الاستفادة من تقنيات تعزيز الخصوصية، وتقييد الاستخدام الآمن والمبتكر للإنترنت.
سرية البيانات من معلومات وأجهزة وتطبيقات	سلبي	إن مركزية سلطة المراقبة (المادة 7) تقلل من تعاون أصحاب المصلحة المتعددين وتعرقل الحوكمة الشاملة، وهي السمات المميزة لإدارة الإنترنت.

تمكين الإنترنت OGST	تأثير؟	وإذا كان التأثير لماذا؟
سلامة المعلومات والتطبيقات والخدمات	سلبي	**قيود المحتوى (المادتان 8 و31) وضوابط الوصول التي تفرضها السلطات تحد من إمكانية الوصول، مما يقلل من قدرة المستخدمين على الوصول إلى الموارد المتنوعة عبر الإنترنت ومشاركتها.**
الموثوقية والمرونة والتوافر	محايدة إلى سلبية	**وفي حين أن القانون لا يقيد بشكل مباشر قدرة الشبكة، فإن الضوابط التقييدية للمحتوى والتشفير يمكن أن تمنع الاستثمار في البنية التحتية، مما يؤثر بشكل غير مباشر على القدرة على المدى الطويل.**
المساءلة	سلبي	**حقوق المراقبة الشاملة (المادة 7) وقيود التشفير (المادتان 9 و39) تهدد سرية البيانات، وتثبط الأنشطة الآمنة والحساسة عبر الإنترنت.**
خصوصية	مختلط	معاقبة الوصول غير المصرح به (المادتان 10 و11) تدعم سلامة البيانات. ومع ذلك، فإن صلاحيات المراقبة الواسعة يمكن أن تقوض الثقة في صحة المعلومات وسلامتها.