موجز عن تأثير قانون الجرائم الإلكترونية على الإنترنت في ليبيا قانون رقم 5 لسنة 2022

موجز عن تأثير قانون الاتصالات على الانترنت في ليبيا

قانون رقم 22 لسنة 2010

الفهرس

المقدمة	**1**
التحليل	**1**
التأثير على الخصائص الحرجة لـ IWN	1
التأثير على ممكنات إنترنت OGST	3
ملخص	**5**
خاتمة	**5**
توصيات للإصلاح	**5**
تعزيز حماية الخصوصية	5
تعزيز الحوكمة التعاونية	6
تبسيط عمليات الترخيص	6
ضمان الوصول غير المقيد	6
تعزيز الحياد التكنولوجي	6
دعوة لإجراء تقييم شامل لتأثير الإنترنت	**7**
المساهمين	**7**
ليبيا القانون رقم 2022/6 التحليل باستخدام IIAT	**8**
الخصائص الحرجة لـ IWN (طريقة الإنترنت للتواصل)	8
عوامل تمكين الإنترنت OGST (المفتوح والمتصل عالميًا والآمن والجدير بالثقة)	9

المقدمة

يتناول هذا الموجز تأثير قانون الجرائم الإلكترونية رقم 5 لسنة 2022 علي الإنترنت في ليبيا (الترجمة الانجليزية/ الطبعة العربية)، وتحليل آثارها على الخصائص الهامة وعوامل التمكين لإنترنت مفتوح ومتصل عالمياً وآمن وجدير بالثقة. ويستفيد التحليل من إطار مجموعة أدوات تقييم تأثير الإنترنت (IIAT) التابع لجمعية الإنترنت، والذي يساعد في تقييم القوانين والسياسات والقرارات الفنية من خلال تأثيرها على القيم الأساسية المتمثلة في إمكانية الوصول والموثوقية والمرونة. وبينما يهدف القانون إلى تعزيز الأمن السيبراني، فإن أحكامه الواسعة تثير مخاوف بشأن الخصوصية وحرية التعبير وإمكانية الوصول إلى الإنترنت. ويدعو التقرير إلى إجراء إصلاحات متوازنة للحفاظ على الأمن مع حماية الحقوق الرقمية للمستخدمين الليبيين.

يسعى قانون الجرائم الإلكترونية الليبي رقم 5 لعام 2022 إلى مكافحة التهديدات السيبرانية وتعزيز أمن البيانات ولكنه يثير مخاوف جدية بشأن الانتهاكات المحتملة للخصوصية وحرية التعبير والقيود المفروضة على أدوات التشفير. تشمل القضايا الرئيسية صلاحيات واسعة للمراقبة الحكومية والجرائم المحددة بشكل غامض والتي قد تسهل التجاوز في إنفاذ القيود على الإنترنت، مما قد يعاقب التعبير عبر الإنترنت.

صدر هذا القانون وسط جهود ليبيا لتعزيز الأمن السيبراني مع تزايد المشاركة الرقمية والتحديات السياسية. وبينما يهدف القانون إلى تأمين الفضاء الإلكتروني، فإنه يتضمن أحكامًا للمراقبة الحكومية ويحد من الوصول إلى أدوات الخصوصية مثل التشفير. ويرى المنتقدون أن مثل هذه الأحكام، في بيئة هشة سياسيا، يمكن أن تحد من حرية التعبير، والنشاط الرقمي، والاستخدام الآمن للمنصات

عبـر الإنترنـت. وقـد تؤثـر هـذه القيـود علـى الصحفييـن ومنظمـات المجتمـع المدنـي والناشـطين، ممـا يعيـق الجهـود الراميـة إلـى تعزيـز مساحة رقمية مفتوحة وآمنة.

يدعـو التغييـر المقتـرح إلـى إصلاح القانـون لضمـان عـدم انتهـاك تدابيـر الأمـن السـيبراني للحقـوق الرقميـة والقيـم الأساسـية للانترنـت. وتشـمل التوصيـات المحـددة توضيـح المصطلحـات فـي القانـون، وقصـر المراقبـة علـى الحـالات الخاضعـة للرقابـة القضائيـة، وتقليـل القيـود المفروضـة علـى أدوات التشـفير التـي تتيـح خصوصيـة المسـتخدم. والهـدف هـو إنشـاء قانـون فعـال للجرائـم الإلكترونيـة يحمـي المواطنين مـن التهديدات السـيبرانية دون المسـاس بخصوصيتهـم أو حريتهـم فـي التعبيـر، وبالتالـي تعزيز بيئة رقمية آمنة ومفتوحة.

التحليل

1. 1. إمكانية الوصول والمخاوف المتعلقة بالخصوصية

تؤثـر أذونـات المراقبـة الشـاملة التـي يفرضهـا القانـون (المـادة 7) والقيـود المفروضـة علـى التشـفير (المادتـان 9 و39) بشـكل كبيـر علـى إمكانيـة الوصـول والخصوصيـة مـن خلال الحـد مـن تحكـم المسـتخدم فـي أدوات الاتصـال الآمنـة. تتعـارض هـذه القيـود مـع تمكيـن خصوصيـة وممتلـكات IWN لـ الإدارة اللامركزيـة، مركزيـة سـلطة المراقبـة تحـت إشـراف الهيئـة الوطنيـة لأمـن وسلامـة المعلومـات. وهـذا مـن شـأنه أن يثبـط حريـة التعبيـر، ويحـد مـن المشـاركة عبـر الإنترنـت، ويقلـل مـن شـمولية الإنترنت باعتبارها مساحة للحوار المفتوح.

2. 2. التأثير على البنية المفتوحة وإمكانية الوصول غير المقيدة

أحـكام حجـب المواقـع الإلكترونيـة بنـاءً علـى أسـس "أخلاقيـة" محـددة

بشكل غامض (المادتان 8 و31) إمكانية الوصول غير المقيدة و العمارة المفتوحة. تعمل هذه القيود على تقييد وصول المستخدمين إلى موارد المعلومات المختلفة، مما قد يؤدي إلى مستودعات المعلومات. وهذا يضر بغرض الإنترنت كشبكة قابلة للتشغيل المتبادل لمحتوى ووجهات نظر متنوعة، مما يؤثر على قدرة المستخدمين على التعامل مع مجموعة واسعة من الموارد العالمية. ومع ذلك، تتوافق هذه المواد مع القوانين واللوائح المحلية المعمول بها، بالإضافة إلى السياق الثقافي.

3. 3. التهديد للتنمية التعاونية والإدارة

تركيز سلطة المراقبة دون تحديات الرقابة من جانب أصحاب المصلحة المتعددين التنمية التعاونية والحوكمة من خلال إسناد الرقابة التنظيمية إلى سلطة واحدة. وهذا يقلل من فرص المساءلة المشتركة ومشاركة المجتمع في إدارة الإنترنت، مما يحد من قدرة الإنترنت على التكيف. ومن خلال تقييد المدخلات التعاونية، يمكن للقانون أن يخنق الابتكار والمرونة، مما يؤثر على ملكية IWN التوجيه الموزع.

4. 4. تقييد سرية البيانات وسلامتها

قيود التشفير دون التنازل عن الرقابة الكافية سرية البيانات و سلامة المعلومات. تعمل هذه القيود على تقييد التبادل الآمن للبيانات، مما يؤثر على ثقة المستخدم وسلامته عبر الإنترنت. يتناقض عنصر التحكم هذا مع خاصية IWN الخاصة بـ البنية التحتية التي يمكن الوصول إليهاحيث يفقد المستخدمون الوسائل الموثوقة لحماية المعلومات الحساسة، الأمر الذي قد يعيق المشاركة عبر الإنترنت، خاصة بين الناشطين والصحفيين.

5. 5. المخاطر على الموثوقية والمرونة والمساءلة

عقوبات صارمة (على سبيل المثال، الوصول غير المصرح به في المادتين 11 و15) شبكة الدعم الموثوقية والنزاهة ولكن قد يضر المساءلة بسبب عدم الشفافية الكافية وبينما تهدف هذه الإجراءات العقابية إلى تأمين الشبكة، فإنها تخاطر بعدم الاتساق في التنفيذ، مما قد يؤدي إلى فرض قيود لا يمكن التنبؤ بها ويؤثر على المرونة. ومن شأن إضافة الشفافية إلى إجراءات الإنفاذ والضمانات الإجرائية أن يحسن المساءلة، ويعزز التنظيم المتوازن والموثوق في مجال الإنترنت.

ملخص

تنبع أقوى تأثيرات قانون الجرائم الإلكترونية الليبي رقم 5 لعام 2022 من قيوده على التشفير ومركزية المراقبة والقيود الواسعة على المحتوى. تخاطر هذه الأحكام بانتهاك خصوصية المستخدم، وحرية التعبير، والوصول إلى مجموعة متنوعة من المعلومات، مما قد يخنق المشاركة الرقمية. ويتم تشجيع صناع السياسات على مراجعة القانون بتعريفات أكثر وضوحا، وتنفيذ الرقابة القضائية على المراقبة، والحد من قيود التشفير. سيؤدي هذا إلى إنشاء إطار عمل يحافظ على الأمان مع دعم إنترنت مفتوح ويمكن الوصول إليه.

خاتمة

في حين يهدف قانون الجرائم الإلكترونية في ليبيا إلى تعزيز الأمن السيبراني، فإنه يفرض تدابير تقييدية يمكن أن تقوض الخصوصية وحرية التعبير وشمولية الإنترنت. وللتخفيف من هذه المخاطر، يوصى بإجراء مراجعة شاملة للقانون، مع التركيز على ضمانات الخصوصية، وحدود المراقبة، وحماية استخدام أدوات التشفير. ومن

أن يـؤدي التقييـم الكامـل لتأثيـر الإنترنـت إلـى زيـادة توضيـح الآثـار المحتملـة للقانـون، ودعـم الإصلاحـات المتوازنـة التـي تحمـي مـن التهديدات السيبرانية مع الحفاظ على شبكة إنترنت مفتوحة ومرنة.

التوصيات الخاصة بالإصلاح

للتعامـل مـع المخاطـر التـي يفرضهـا قانـون الجرائـم الإلكترونيـة رقـم 5 لسـنة 2022 فـي ليبيـا ومواءمتـه مـع مبـادئ الإنترنـت المفتوحـة والمتصلة عالميًا والآمنة والجديرة بالثقة، يوصى بالإصلاحات التالية:

1. توضيح وتضييق التعريفات:

تحسيـن المصطلحـات الغامضـة مثـل "النظـام العـام" و"الآداب العامـة" و"الإخلال بالسـلم الاجتماعـي" (المـادة 4، 7) لضمـان عدم فتحها للتفسير الواسـع أو الذاتـي. تحديـد الجرائـم بوضـوح لتجنـب إسـاءة الاسـتخدام أو التجاوز.

2. حماية الخصوصية والحد من صلاحيات المراقبة:

تقييـد صلاحيـات المراقبـة (المـادة 7) علـى حـالات محـددة ومبـررة قانونًـا. تقديـم إشـراف قضائـي إلزامـي لجميـع أنشـطة المراقبـة لضمـان الضوابـط والتوازنات.

3. تمكين التشفير دون ترخيص مفرط:

إزالــة أو تخفيــف متطلــب ترخيــص أدوات التشــفير (المادتــان 9 و39). التشـفير هـو أداة بالغـة الأهميـة لخصوصيـة المسـتخدم وأمـن البيانـات ويجب أن يكون متاحًا بحرية للأفراد والشركات.

4. تقليص القيود المفروضة على المحتوى:

الحـد مـن السـلطة الواسـعة لحظـر أو تقييـد المحتـوى (المـواد 8 و31

و33) فـي حـالات الانتهـاكات القانونيـة الواضحـة، مـع آليـات الاسـتئناف والرقابة المستقلة.

5. تعزيز الحوكمة التعاونية:

إنشـاء هيئـة متعـددة الأطـراف تضم الحكومـة والقطـاع الخـاص والمجتمع المدنـي والخبـراء الفنييـن للإشـراف علـى تنفيـذ القانـون. وهـذا مـن شـأنه أن يضمن الشفافية والمساءلة.

6. دعم حرية التعبير:

إزالـة أو مراجعـة الأحـكام التـي قـد تنتهـك حريـة التعبيـر (علـى سـبيل المثـال، القيـود المفروضـة علـى المحتـوى "التحيـزي"" المحـدد بشـكل غامـض). التوافـق مـع معاييـر حقـوق الإنسـان الدوليـة لضمـان حمايـة التعبير عبر الإنترنت.

7. تعزيز الضمانات الإجرائية:

إدخـال الشـفافية فـي آليـات التنفيـذ، وضمـان إبلاغ الأفـراد بالإجـراءات المتخذة ضدهم وحصولهم على عمليات استئناف عادلة.

8. المراجعة والتحديث المنتظمان:

إدراج بنـد للمراجعـة الدوريـة للقانـون لضمـان تطـوره مـع التقـدم التكنولوجي واستمراره في احترام حقوق المستخدم.

الدعوة إلى إجراء تقييم كامل لتأثير الإنترنت

يعـد إجـراء تقييـم كامـل لتأثيـر الإنترنـت أمـرًا ضروريًـا لتقييـم المخاطـر المحتملـة والعواقـب غيـر المقصـودة لقانـون الجرائـم الإلكترونيـة الليبـي رقم 5 لعام 2022 بشكل شامل. يجب أن يتضمن هذا التقييم:

- تحليل توافق القانون مع الخصائص الأساسية لشبكة الإنترنت (IWN) وممكنات الإنترنت المفتوحة والآمنة والجديرة بالثقة.
- تحديد كيف يمكن أن تؤثر الأحكام المحددة على إمكانية الوصول والخصوصية وحرية التعبير والاتصال بالإنترنت العالمي.
- تقديم توصيات قائمة على الأدلة للتخفيف من المخاطر ومواءمة القانون مع أفضل الممارسات الدولية للحقوق الرقمية والأمن السيبراني.

يجب أن يتضمن التقييم مدخلات من مجموعة متنوعة من أصحاب المصلحة، بما في ذلك الخبراء الفنيون ومنظمات المجتمع المدني وصناع السياسات والقطاع الخاص. من خلال القيام بهذه العملية، يمكن لليبيا ضمان أن يكون إطار الأمن السيبراني الخاص بها قويًا ومحترمًا للحقوق وملائمًا لتعزيز بيئة رقمية شاملة.

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 5/2022 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	نعم	**تأثير:** المواد التي تقيد التشفير (المادتان 9 و39) وتتطلب تصاريح تحد من الوصول المفتوح إلى وسائل الاتصال الآمنة. يمكن أن يعيق عنصر التحكم هذا إمكانية التشغيل البيني وقد يؤثر بشكل غير متناسب على وصول المستخدم إلى الموارد الآمنة عبر الإنترنت. **سبب:** يمكن لضوابط التشفير والتراخيص الصارمة أن تحد من إمكانية الوصول الآمن إلى البنية التحتية، مما يشكل تحديًا لقدرة المستخدمين على المشاركة في أنشطة آمنة عبر الإنترنت.
بنية مفتوحة لبنات البناء القابلة للتشغيل البيني والقابلة لإعادة الاستخدام	نعم	**تأثير:** القيود المفروضة على الوصول إلى موقع الويب والبيانات الرقمية (المادة 5) دون موافقة المالك تدعم حماية البيانات ولكنها قد تقيد أيضًا مشاركة المعلومات المفتوحة في حالة التنفيذ الصارم للغاية. **سبب:** قد يؤدي تقييد الوصول بناءً على موافقة المالك إلى تقويض إمكانية التشغيل البيني لمحتوى الويب، مما يقيد مشاركة المعلومات المهمة لوظائف الإنترنت المفتوحة.

الخصائص الحرجة لـ IWN	تأثير؟	وإذا كان التأثير لماذا؟
		تأثير: الأحكام التي تسمح بالمراقبة والحجب (المادتان 7 و8) تعمل على مركزية السيطرة على المحتوى، مما قد يتعارض مع الطبيعة اللامركزية للإنترنت.
الإدارة اللامركزية ونظام التوجيه الموزع الفردي	نعم	سبب: يمكن أن تؤدي المراقبة المركزية من قبل السلطات إلى إنشاء نقاط اختناق في إدارة الشبكة، مما قد يؤثر على استقلالية التوجيه وخنق تنوع المحتوى. التبرير: بما يتماشى مع القوانين واللوائح المحلية المعمول بها، وكذلك السياق الثقافي.
المعرفات العالمية المشتركة	لا	**تأثير:** لا يؤثر القانون بشكل مباشر على المعرفات العالمية مثل عناوين IP أو أسماء النطاقات، مما يحافظ على هذه الخاصية المهمة دون أن تتأثر إلى حد كبير. **سبب:** لا توجد أحكام في القانون تقيد استخدام عناوين IP أو أنظمة النطاق، مما يسمح باستمرارية نظام المعرفات العالمي هذا.
شبكة محايدة تكنولوجياً ذات أغراض عامة	نعم	تأثير: نطاق المحتوى المحظور، لا سيما فيما يتعلق بالمقامرة والمخدرات والدعارة (المواد 8 و31 و33)، يمكن أن يحد من طبيعة الإنترنت ذات الأغراض العامة عن طريق حظر المحتوى القانوني بناءً على معايير واسعة. سبب: قد تؤدي هذه الأحكام إلى تقييد قدرة الشبكة على التكيف، مما يحد من نطاق المحتوى والخدمات المسموح بها عبر الإنترنت. التبرير: بما يتماشى مع القوانين واللوائح المحلية المعمول بها، وكذلك السياق الثقافي.

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

تمكين الإنترنت OGST	تأثير؟	وإذا كان التأثير لماذا؟
وصول سهل وغير مقيد	نعم	**تأثير:** إن تطبيق القانون على نطاق واسع، حتى بالنسبة للأعمال التي تنشأ خارج ليبيا (المادة 3)، يمكن أن يقيد الوصول إلى المحتوى والموارد الدولية. **سبب:** من خلال السماح بالولاية القضائية على الإجراءات في الخارج، قد يعزل القانون المستخدمين الليبيين عن المحتوى المتاح عالميًا، مما يؤثر على وصولهم إلى المعلومات والخدمات، وقد يؤثر على أولئك الذين مارسوا حقوقهم المكتسبة خارج ليبيا وتمت محاسبتهم بموجب هذا القانون.
الاستخدام غير المقيد ونشر تقنيات الإنترنت	نعم	**تأثير:** الضوابط على التشفير (المادتان 9 و39) وأذونات المراقبة (المادة 7) تحد من الاستخدام المجاني لتقنيات الإنترنت الأساسية. **سبب:** يمكن أن تمنع هذه القيود المستخدمين من الوصول بحرية إلى أدوات الخصوصية والأمان، مما يعيق قدرتهم على استخدام الإنترنت كمنصة آمنة وتمكينية.
التنمية التعاونية والإدارة والحوكمة	نعم	**تأثير:** إن مركزية سلطة المراقبة (المادة 7) والتنفيذ من خلال هيئة واحدة تحد من نموذج الإدارة التعاونية النموذجي للإنترنت. **سبب:** يقيد الهيكل المركزي مدخلات أصحاب المصلحة المتعددين، مما يقلل من فرص مناهج الحوكمة التعاونية والشاملة ويحتمل أن يؤدي إلى خنق الابتكار.

تمكين الإنترنت OGST	تأثير؟	وإذا كان التأثير لماذا؟
إمكانية الوصول غير المقيدة	نعم	**تأثير:** القيود المفروضة على محتوى معين (المادتان 8 و31) والتحكم في الوصول من قبل السلطات تمثل تحديًا لإمكانية الوصول إلى الإنترنت. **سبب:** يؤدي الحجب الانتقائي لمواقع الويب إلى الحد من قدرة المستخدمين على الوصول إلى الموارد المختلفة عبر الإنترنت، مما قد يمنع تنوع المعلومات ويحد من إمكانية الوصول. **التبرير:** بما يتماشى مع القوانين واللوائح المحلية المعمول بها، وكذلك السياق الثقافي.
القدرة المتاحة	نعم	تأثير: على الرغم من أن القانون لا يقيد سعة الشبكة، إلا أن السيطرة المفرطة على المحتوى والتشفير يمكن أن تحد بشكل غير مباشر من توفر الإنترنت. سبب: يمكن أن تؤدي القيود الشديدة إلى إعاقة الاستثمار في البنية التحتية وخدمات الإنترنت، مما قد يؤثر على سعة الشبكة على المدى الطويل.
سرية البيانات من معلومات وأجهزة وتطبيقات	نعم	تأثير: حقوق المراقبة الشاملة (المادة 7) وضوابط التشفير (المادتان 9 و39) تهدد سرية المستخدم. سبب: تضع هذه الأحكام قيودًا على خصوصية المستخدم وسريته، مما قد يثني الأشخاص عن استخدام الإنترنت لإجراء اتصالات أو معاملات حساسة.

تمكين الإنترنت OGST	تأثير؟	وإذا كان التأثير لماذا؟
سلامة المعلومات والتطبيقات والخدمات	نعم	**تأثير:** الأحكام التي تعاقب الوصول غير المصرح به (المادتان 11، 10) تحمي سلامة المعلومات، ولكن المراقبة والقيود يمكن أن تهدد صحة البيانات. **سبب:** تساعد العقوبات الصارمة المفروضة على الوصول غير المصرح به إلى النظام في الحفاظ على سلامة البيانات، ولكن صلاحيات المراقبة المفرطة في التوسع يمكن أن تؤدي إلى تقويض الثقة في سلامة المعلومات.
الموثوقية والمرونة والتوافر	نعم	**تأثير:** تدابير القانون ضد التهديدات السيبرانية (على سبيل المثال، عقوبات التلاعب بالبيانات في المادتين 11، 15) تدعم موثوقية الإنترنت، ولكن صلاحيات المراقبة يمكن أن تشكل مخاطر على المرونة. **سبب:** على الرغم من أن هذه التدابير تحمي موثوقية الشبكة، إلا أنها يمكن أن تضر بالمرونة إذا أساءت السلطات استخدام سيطرتها على محتوى الإنترنت والوصول إليه.
المساءلة	نعم	**تأثير:** الرقابة القضائية على بعض أنشطة المراقبة (المادة 7) تعزز مستوى معين من المساءلة، على الرغم من أن القيود الأوسع على التشفير قد تحد من الرقابة على استخدام البيانات. **سبب:** على الرغم من أن الأوامر القضائية تضيف طبقة من المساءلة، إلا أن سلطة القانون الواسعة للمراقبة والتحكم في التشفير قد تقلل من الشفافية والرقابة.

تمكين الإنترنت OGST	تأثير؟	وإذا كان التأثير لماذا؟
		تأثير: المادتان 7 و 39، اللتان تجيزان المراقبة وتتطلبان تصاريح التشفير، تنتهكان خصوصية المستخدم من خلال منح وصول واسع النطاق إلى الاتصالات والبيانات الشخصية.
خصوصية	نعم	سبب: تعمل عناصر التحكم هذه على إضعاف حماية الخصوصية، حيث قد يتعرض المستخدمون للمراقبة والقيود على أدوات تحسين الخصوصية، مما يقلل من ثقتهم في التفاعلات الآمنة عبر الإنترنت.