ورقة سياسات قوانين الجرائم السيبرانية في المنطقة العربية: حماية للفضاء الرقمي أم قمع للحريات؟

accessnow

accessnow.org

تدافع أكساس ناو (https://www.accessnow.org) عن الحقوق الرقمية للأشخاص المعرضين للخطر حول العالم. نحن نكافح من أجل حقوق الإنسان في العصر الرقمي من خلال الجمع بين الدعم التقني المباشر والمشاركة الشاملة في مجال السياسات العامة والمناصرة الدولية وتقديم المنح للقواعد الشعبية وعقد المؤتمرات مثل الرايتسكون.

الفهرس

هذا التقرير هو أحد إصدارات منظمة أكساس ناو وقد كتبه أيمن الزغدودي. يود المؤلف أن يشكر بشكل خاص مروة فطافطة ووجد وقسّام المنجة ولوران جيودانو وأمينة خان وفريق مناصرة أكساس ناو على مساهماتهم.

للمزيد من المعلومات، يرجى التواصل مع:

د. أيمن الزغدودي | مستشار السياسات في منطقة الشرق الأوسط وشمال إفريقيا |
aymen@accessnow.org

مروة فطافطة | مديرة السياسات والمناصرة في منطقة الشرق الأوسط وشمال إفريقيا |
marwa@accessnow.org

تدافع أكساس ناو (https://www.accessnow.org) عن الحقوق الرقمية للأشخاص المعرضين للخطر حول العالم. نحن نكافح من أجل حقوق الإنسان في العصر الرقمي من خلال الجمع بين الدعم التقني المباشر والمشاركة الشاملة في مجال السياسات العامة والمناصرة الدولية وتقديم المنح للقواعد الشعبية وعقد المؤتمرات مثل الرايتسكون.

ملخص تنفيذي

من خلال ورقة السياسات هذه تبسط أكساس ناو موقفها إزاء قوانين الجرائم السيبرانية في المنطقة العربية بهدف مواءمتها مع المعايير الدولية المتعلقة بالحقوق الرقمية.

تأتي هذه الورقة إثر مجموعة من التحليلات القانونية والبيانات الصحفية بخصوص قوانين الجرائم السيبرانية الصادرة في المنطقة والتي أظهرت تشابهاً كبيراً على مستوى التهديدات التشريعية التي يمكن أن تطال الحق في حرية التعبير والحق في الخصوصية.[1] وفي هذا الخصوص، رأينا أنه من المهم تسليط الضوء على الضوابط التي يجب مراعاتها عند صياغة قوانين الجرائم السيبرانية بهدف حماية الفضاء السيبراني دون أي انتهاك للحقوق الرقمية.

وترى أكساس ناو أن استعمال قوانين الجرائم السيبرانية لانتهاك حقوق الإنسان من شأنه، لا فقط، أن يهدد سلامة الأفراد، بل أيضاً أن يضعف الأمن السيبراني للدول. علاوة على ذلك، فإن المواد

---

[1] على سبيل الذكر:

مشروع قانون الجرائم الإلكترونية الأردني يقوّض الحقوق الرقمية بشدة، للاطلاع:
https://www.accessnow.org/press-release/%d8%a7%d9%84%d8%ac%d8%b1%d8%a7%d8%a6%d9%85-%d8%a7%d9%84%d8%a5/%d9%84%d9%83%d8%aa%d8%b1%d9%88%d9%86%d9%8a%d8%a9-%d8%a7%d9%84%d8%a3%d8%b1%d8%af%d9%86

المرسوم عدد 54، ضربة جديدة لحرية التعبير في تونس، للاطلاع:
https://www.accessnow.org/%d8%b6%d8%b1%d8%a8%d8%a9-%d8%ac%d8%af%d9%8a%d8%af%d8%a9-%d9%84%d8%ad%d8%b1%d9%8a%d8%a9-%d8%a7%d9%84%d8%aa%d8%b9%d8%a8%d9%8a%d8%b1-%d9%81%d9%8a-%d8%aa%d9%88%d9%86%d8%b3/

قانون الجرائم الإلكترونية في ليبيا: تهديد لحرية التعبير وتقنين للرقابة الشاملة والحجب، للاطلاع:
https://www.accessnow.org/press-release/%d9%82%d8%a7%d9%86%d9%88%d9%86-%d8%a7%d9%84%d8%ac%d8%b1%d8%a7%d8%a6%d9%85-%d8%a7%d9%84%d8%a5%d9%84%d9%83%d8%aa%d8%b1%d9%88%d9%86%d9%8a%d8%a9-%d9%84%d9%8a%d8%a7%a8%d9%8a%d8%a7/

موافقة البرلمان المصري على قانون مكافحة جرائم تقنية المعلومات، خطوة جديدة لتقنين حجب المواقع الإلكترونية والمراقبة الشاملة على مصر، للاطلاع:
https://www.accessnow.org/%d9%85%d9%88%d8%a7%d9%81%d9%82%d8%a9-%d8%a7%d9%84%d8%a8%d8%b1%d9%84%d9%85%d8%a7%d9%86-%d8%a7%d9%84%d9%85%d8%b5%d8%b1%d9%8a-%d8%b9%d9%84%d9%89-%d9%82%d8%a7%d9%86%d9%88%d9%86-%d9%85%d9%83%d8%a7%d9%81/

القانونية التي تستهدف الحقوق الرقمية غالباً ما تكون غير فعالة في تحقيق الغايات المرجوة من هذه القوانين، إذ أن القذف أو الذم أو نشر الأخبار الزائفة كلها مضامين تحتاج إلى مقاربة شاملة لمعالجتها، ولا يمكن بالتالي للمقاربة الردعية من خلال قوانين العقوبات أو قوانين الصحافة أن تحمي كرامة الأفراد وأمن المجتمعات دون اللجوء إلى تدابير إيجابية كالتربية الإعلامية والرقمية وتعزيز استقلالية وسائل الإعلام.

كما يمكن أن تعيق هذه التشريعات الجهود الدولية في التعاون الثنائي أو متعدد الأطراف لضمان الأمن السيبراني، حيث أن احتواء هذه القوانين على جرائم تتعلق بالمحتوى الرقمي يمكن أن يشكّل مدخلاً للطعن في مدى احترامها للاتفاقيات الدولية المتعلقة بحقوق الإنسان. وبالتالي، قد تواجه مطالب التعاون رفضاً من الدول التي تحترم التزاماتها الدولية في حماية حقوق الإنسان.

المقدمة

في سياق قيام دول المنطقة في السنوات الأخيرة بسنّ تشريعات جديدة متعلّقة بمكافحة الجرائم السيبرانية، سواء لأول مرة كما في تونس، أو بتنقيح تشريعات قائمة كما في الإمارات العربية المتحدة، أو باستبدالها مثلما هو الحال في سوريا والأردن، رأت أكساس ناو من الضروري إعداد ورقة سياسات بخصوص هذه التشريعات التي غالباً ما يساء استعمالها وتُحرف وجهتها الحقيقية من قوانين تهدف لحماية أنظمة المعلومات والاتصالات والفضاء السيبراني إلى آليات تشريعية جديدة لانتهاك حق الأفراد في حرية التعبير والحق الخصوصية.

كما تأتي هذه الورقة في سياق يتسّم بتوجه الدول العربية نحو إرساء استراتيجية عربية موحّدة للتعامل مع شركات التواصل الاجتماعي الدولية، والتي تتضمّن إلزام المنصات الإلكترونية بتعيين ممثلها القانوني داخل الدولة وضرورة تنفيذ الأحكام القضائية بخصوص حذف المحتوى أو كشف هوية المستخدمين. وفي حالة عدم الامتثال لهذه الالتزامات، تقع هذه المنصات عُرضة إما لغرامات مالية تُحتسب كنسبة من أرباحها أو للتقليص من سرعة الوصول إليها (Throttling).[2]

أما على الصعيد الدولي، قامت الجمعية العامة للأمم المتحدة بإحداث لجنة خاصة لإعداد مشروع اتفاقية دولية بخصوص مكافحة استعمال تكنولوجيات المعلومات والاتصال للأغراض الإجرامية.[3]

---

[2] وفقاً للمقترحات التي قدمها اتحاد إذاعات الدول العربية إلى مجلس وزراء الإعلام العرب، تنقسم التوصيات إلى:

- توصيات متعلقة بكيفية التعامل مع المنصات الرقمية العالمية،
- توصيات متعلقة بالإجراءات التحفيزية والإصلاحية،
- توصيات متعلقة بتعزيز إنتاج المحتوى الرقمي العربي،
- توصيات بخصوص تطوير منصات المشاهدة حسب الطلب والبث التدفقي العربي،
- توصيات بخصوص حماية البيانات والأمن السيبراني،
- توصيات بخصوص تطوير الموارد البشرية.

لمزيد من التفاصيل، يراجع:

https://petra.gov.jo/Include/InnerPage.jsp?ID=249316&lang=ar&name=news

أيضاً بالخصوص: مجلة الإذاعات العربية، عدد 4 لسنة 2022، الصفحات 22 وما بعد.

[3] بخصوص الجدول الزمني المتعلق بهذه اللجنة، يراجع:

وقد جرت مناقشات هامّة بين الدول بخصوص محتوى ونطاق الاتفاقية الدولية التي لا ينبغي أن تحيد عن غاياتها الأساسية في تعزيز التعاون الدولي لمكافحة الجرائم السيبرانية دون أن يمتد الأمر لتهديد المكتسبات التي جاءت بها الصكوك الدولية المتعلقة بحقوق الإنسان.[4]

وتوصلت اللجنة المذكورة أعلاه في 8 أغسطس 2024، بعد عامين من المفاوضات، إلى اتفاق حول النسخة النهائية من مشروع الاتفاقية والتي سيتم عرضها على الجمعية العامة للأمم المتحدة للمصادقة عليها وسط مخاوف العديد من المنظمات التي تعنى بالحقوق الرقمية.[5]

من جهة أخرى، أدّى تطبيق قوانين الجرائم السيبرانية في المنطقة إلى خنق الفضاء العام وقمع الحريات، مما أدّى إلى ترهيب الأفراد من التعبير عن آرائهم بشأن قضايا تهم الشأن العام. ويأتي هذا الخوف نتيجة للعقوبات الصارمة السالبة للحرية، والتي وصلت في إحدى دول المنطقة، وهي المملكة العربية السعودية، إلى السجن 34 عاماً بسبب تغريدة ناقدة للسلطة السياسية.[6]

---

https://www.eff.org/ar/deeplinks/2023/04/un-cybercrime-treaty-timeline

[4] بخصوص التهديدات التي يمكن أن تترتب عن هذه الاتفاقية، يراجع المقال التالي:

Joan Barata, *New United Nations Cybercrime Convention Sets Unprecedented International Anti-Human Rights Standard*, Tech Policy Press, 4 September 2024. Available online at: https://www.techpolicy.press/new-united-nations-cybercrime-convention-sets-unprecedented-international-antihuman-rights-standard/

[5] لمزيد من التفاصيل، يراجع:

https://documents.un.org/doc/undoc/gen/v24/055/04/pdf/v2405504.pdf

[6] أكساس ناو ومنظمات أخرى، على السلطات السعودية الإفراج عن ناشطة حقوق المرأة سلمى الشهاب، 29 أغسطس 2022.
https://www.accessnow.org/press-release/%D8%B9%D9%84%D9%89-%D8%A7%D9%84%D8%B3%D9%84%D8%B7%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D8%B9%D9%88%D8%AF%D9%8A%D8%A9-%D8%A7%D9%84%D8%A5%D9%81%D8%B1%D8%A7%D8%AC-%D8%B9%D9%86-%D9%86%D8%A7%D8%B4%D8%B7%D8%A9/

سلمى الشهاب،[7] خليفة الربيع،[8] غازي الشواشي،[9] عدنان الروسان،[10] مهند حسن،[11] ياسين الرمضاني،[12] هبة أبو طه،[13] وسارة دريس،[14] جميعهم أشخاص تعرضوا لتتبعات القضائية أو الملاحقة الأمنية أو السجن على أساس قوانين الجرائم السيبرانية التي سنّتها أغلب الدول في المنطقة.[15] وتتمثّل السمة المشتركة لهذه الانتهاكات في معاقبة هؤلاء الأفراد بسبب ممارستهم لحقهم الشرعيّ في حرية التعبير وانتقاد السلطات السياسية أو المطالبة بالحقوق والحريات. إذ أنهم لم يقوموا بتدمير أنظمة المعلومات والاتصال أو قرصنة البيانات للإضرار بحقوق الأفراد أو المؤسسات.

---

[7] أنظر/ي:
https://www.hrw.org/ar/news/2022/08/19/saudi-arabia-woman-sentenced-34-years-tweets

[8] أنظر/ي:
https://www.hrw.org/ar/news/2019/07/09/331877

[9] أنظر/ي:
https://www.accessnow.org/%D8%B6%D8%B1%D8%A8%D8%A9-%D8%AC%D8%AF%D9%8A%D8%AF%D8%A9-%D9%84%D8%AD%D8%B1%D9%8A%D8%A9-%D8%A7%D9%84%D8%AA%D8%B9%D8%A8%D9%8A%D8%B1-%D9%81%D9%8A-%D8%AA%D9%88%D9%86%D8%B3/

[10] أنظر/ي:
https://www.gc4hr.org/ar/%d8%a3%d8%b7%d9%84%d9%82%d9%88%d8%a7-%d8%b3%d8%b1%d8%a7%d8%ad-%d8%b9%d8%af%d9%86%d8%a7%d9%86-%d8%a7%d9%84%d8%b1%d9%88%d8%b3%d8%a7%d9%86/

[11] أنظر/ي:
https://snhr.org/arabic/2023/08/18/%d8%a7%d9%84%d9%82%d8%a7%d9%86%d9%88%d9%86-%d8%b1%d9%82%d9%85-20-%d9%84%d8%b9%d8%a7%d9%85-2022-%d8%a7%d9%84%d8%b0%d9%8a-%d8%a3%d8%b5%d8%af%d8%b1%d9%87-%d8%a7%d9%84%d9%86%d8%b8%d8%a7%d9%85-%d8%a7%d9%84/

[12] أنظر/ي:
https://www.assabahnews.tn/ar/الاخبار/جهات-73207-وقفة-تضامنية-للمطالبة-باطلاق-سراح-الصحفي-ياسين-الرمضاني-ومح-امينه-تتحدث-لـ-الصباح-نيوز

[13] أنظر/ي:
https://www.amnesty.org/en/latest/news/2024/08/jordan-new-cybercrimes-law-stifling-freedom-of-expression-one-year-on/

[14] أنظر/ي:
https://www.fidh.org/ar/الكويت-قانون-الجرائم-الالكترونية

[15] أنظر/ي الجدول التوضيحي رقم 1.

ويطرح اللجوء المكثّف للسلطات إلى مثل هذه القوانين سؤالاً مشروعاً حول الغاية الأساسية من وراء وضع مثل هذه التشريعات. فهل الهدف هو التصدي للجرائم التي تستهدف أنظمة المعلومات والأمن السيبراني للأفراد والدول والمؤسسات الاقتصادية أو غيرها، أم هو التضييق على الحقوق والحريات السياسية والمدنية مثل الحق في الخصوصية أو حرية التعبير؟

يدعم هذا التساؤل وجود عدة جرائم ذات طابع سياسي لا نجد لها مثيلاً في اتفاقية بودابست المتعلقة بالجريمة الالكترونية، والتي يمكن اعتبارها النص القانوني الدولي المرجعي في هذا المجال، على الرغم من بعض الهنات بخصوص افتقارها لبعض ضمانات حقوق الإنسان. بل حتى الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الصادرة سنة 2010، لم تضم هي الأخرى أي جرائم بخصوص الإساءة إلى الحكومات أو القذف والذم أو نشر الأخبار المضللة.[16]

ويجدر التذكير هنا بأن المقرر الخاص بحماية وتعزيز الحق في حرية التعبير أكدّ على خضوع حرية التعبير في الفضاء الرقمي إلى نفس النظام القانوني المنطبق في الفضاء الحقيقي وبالتالي لا يوجد أي مبرر لإضافة جرائم متعلّقة بالمحتوى الرقمي (جرائم المحتوى) إلى قوانين الجرائم السيبرانية طالما أنها مجرَّمة بموجب قوانين وطنية أخرى مثل قانون العقوبات وقوانين الصحافة والنشر...إلخ.[17] كما نبّهت عدة منظمات دولية من مخاطر توسيع نطاق الجرائم السيبرانية ليشمل السماح بتتبع الأفراد بسبب ما يقومون بنشره أو إرساله عبر الإنترنت لما في ذلك من تهديد للحق في حرية التعبير المضمون بموجب المعاهدات الدولية.[18]

---

[16] للحصول على نظرة شاملة بخصوص أصناف الجرائم السيبرانية المنصوص عليها صلب اتفاقية بوادابست والاتفاقية العربية لمكافحة جرائم تقنية المعلومات ومختلف التشريعات الوطنية في المنطقة، يراجع الجدول التوضيحي أسفله.

حول الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، يراجع التحليل الذي أنجزته مؤسسة حرية الفكر والتعبير:

https://afteegypt.org/research/research-papers/2015/03/11/9770-afteegypt.html

[17] تجدر الإشارة هنا إلى أن تنصيص القوانين الوطنية في المنطقة العربية على جرائم التشهير يتعارض مع المعايير الدولية التي تقتضي نزع صفة الجرم عن التشهير والاقتصار على الدعاوى المدنية.

[18] أنظر مثلاً، مؤسسة الحدود الالكترونية، فك شفرة معاهدة الأمم المتحدة لمكافحة الجرائم الإلكترونية، 7 أبريل 2023.

https://www.eff.org/ar/deeplinks/2023/04/decoding-uncybercrime-treaty

منظمة المادة 19 وهيومن رايتس ووتش، تعليق بخصوص مشروع المعاهدة الدولية المتعلقة بالجرائم السيبرانية، 4 سبتمبر 2023.

وعلى هذا الصعيد، تعتبر أكساس ناو أن صياغة قوانين الجرائم السيبرانية يجب أن تهدف إلى حماية أنظمة المعلومات والاتصال دون أن تمتد لتجريم المحتوى الرقمي الذي يقوم بنشره الأفراد أو المؤسسات والمنظمات. كما يجب إضافة ضمانات إجرائية تتيح وجود رقابة من جهات قضائية أو من قبل هيئات مستقلة على السلطات الواسعة التي يتمتع بها الجهاز التنفيذي للتحقيق في الجرائم الإلكترونية وملاحقتها. كما تعيق مثل هذه التشريعات أي إمكانية للتعاون الدولي وإيجاد إطار قانوني دولي موّحد من شأنه دفع الدول نحو حماية أمثل للفضاء السيبراني دون الزيغ نحو استهداف الحقوق والحريات.

وبناءً عليه، تنقسم هذه الورقة إلى **أربعة** أجزاء:

- أولاً، تعريف الجرائم السيبرانية والتشفير
- ثانياً، المعايير الدولية المتعلقة بالحق في حرية التعبير والحق في الخصوصية
- ثالثاً، الإشكاليات القانونية المترتبة عن التشريعات المتعلقة بالجرائم السيبرانية في المنطقة العربية
- أخيراً، تقدّم أكساس ناو مجموعة من التوصيات بهدف تحسين نصوص التشريعات المتعلقة بالجرائم السيبرانية بالعودة إلى المعايير الدولية، والتي يمكن اعتمادها ليس في سياق المنطقة العربية فحسب، بل في سياقات أخرى أينما تقوم الحكومات باستعمال هذه التشريعات لانتهاك الحق في حرية التعبير والحق في الخصوصية.

https://www.article19.org/resources/un-oral-statement-at-6th-session-of-cybercrime-convention/

تعريف المصطلحات

الجرائم السيبرانية

إن التمييز بين الجرائم السيبرانية والجرائم غير السيبرانية يعتبر أمراً بالغ الأهمية، خاصة عند العودة إلى التشريعات المتعلقة بالجرائم السيبرانية في الدول العربية التي تتعمّد إضافة جرائم غير سيبرانية في جوهرها ضمن هذه القوانين. وهذا يترافق مع تشديد العقاب ومنح الأجهزة الأمنية سلطات واسعة للتحقيق، مثل اعتراض الاتصالات وحجز أنظمة المعلومات والأجهزة الإلكترونية، وغيرها من الصلاحيات التقنية التي من شأنها تهديد خصوصية الأفراد.

على الرغم من غياب توافق دولي حول تعريف الجرائم السيبرانية، إلا أننا نلاحظ بأن كل التعريفات ترتكز على استعمال أنظمة المعلومات والاتصال لارتكاب الجريمة كعنصر جوهري في التعريف.[19] وعلى هذا الأساس، ظهرت عدة تصنيفات[20] من أهمها التصنيف بين الجرائم السيبرانية الصرفة (Cyber-dependent crimes) والجرائم السيبرانية بالتبعية (Cyber-enabled crimes).

تعتبر الجرائم السيبرانية بطبيعتها جرائم مُستحدثة ظهرت نتيجة للتطور التكنولوجي الذي عرفه العالم في العقود الأخيرة والتي لا يمكن ارتكابها إلا عبر أنظمة المعلومات والاتصال، مثل تعطيل أنظمة المعلومات والاتصال أو النفاذ غير المشروع إليها. في المقابل، هناك جرائم سيبرانية بالتبعية، التي

---

[19] يراجع في هذا الإطار:

Kirsty Phillips, Julia C. Davidson,Ruby R. Farr,Christine Burkhardt,Stefano Caneppele and Mary P. Aiken, Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies, available online: https://www.mdpi.com/2673-6756/2/2/28

Rick Sarre, Laurie Yiu-Chung Lau & Lennon Y.C. Chang (2018) Responding to cybercrime: current trends, Police Practice and Research, available online: https://doi.org/10.1080/15614263.2018.1507888

[20] يراجع في هذا الإطار:

Kirsty Phillips, Julia C. Davidson,Ruby R. Farr,Christine Burkhardt,Stefano Caneppele and Mary P. Aiken, Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies, available online: https://www.mdpi.com/2673-6756/2/2/28

أصبح بالإمكان ارتكابها داخل الفضاء السيبراني إلى جانب الفضاء الحقيقي. ويشمل هذا التصنيف عدة جرائم مثل نشر المحتوى الذي يتضمن اعتداءات جنسية على القُصّر أو الاعتداء على المُلكيّة الفكرية أو الاحتيال والابتزاز الرقميين، وغيرها من الجرائم التي يمكن أن تمارس خارج الفضاء السيبراني.

وعند العودة إلى التشريعات الموجودة في المنطقة العربية، نلاحظ أن المواد المتعلقة بالجرائم السيبرانية بالتبعية أكثر من المواد المتعلقة بالجرائم السيبرانية الصرفة. كما يوجد توجه مفرط نحو تجريم طائفة واسعة من المضامين وفقاً لعبارات فضفاضة، مثل تعطيل العمل بالدستور أو المساس برموز الدولة أو الترويج لمظاهرات دون ترخيص أو نشر الأخبار الزائفة والإساءة إلى الأفراد. وقد وصل الأمر في بعض الدول العربية إلى أن عدد جرائم المحتوى تجاوز الجرائم السيبرانية الصرفة، مثل الاختراق السيبراني وتدمير أنظمة الاتصال، وهي الجرائم التي كانت السبب الأصلي لتوجه الدول نحو سن مثل هذه التشريعات.[21]

كما لاحظنا أيضاً ضُعفاً في الضمانات القانونية حتى بالنسبة للجرائم السيبرانية الصرفة، حيث تكتفي أغلب الدول العربية إما بتجريم النفاذ غير المشروع لأنظمة المعلومات والاتصال أو تشترط في أحسن الأحوال نية العمد، في حين أن عليها أن تشترط أيضاً أن يكون النفاذ غير المشروع لأنظمة المعلومات والاتصال بدون وجه حق.

ومن شأن هذا الشرط الأخير (النفاذ بغير حق) أن يحمي عدة ممارسات مشروعة يتعمد أصحابها النفاذ غير المشروع من أجل غايات سامية ونبيلة، مثل الأعمال التي تقوم بها الصحافة الاستقصائية للكشف عن انتهاكات حقوق الإنسان ومكامن الفساد أو أنشطة الباحثين في مجال السلامة المعلوماتية الذين يمكن أن تساهم أنشطتهم في كشف الثغرات التي تشكو منها بعض أنظمة المعلومات والاتصال وتطوير أدائها.

---

[21] **ليبيا**: جرائم المحتوى 18/ الجرائم السيبرانية الصرفة 12.

الإمارات العربية المتحدة: جرائم المحتوى 30/ الجرائم السيبرانية الصرفة 19.

التشفير

وفقاً لما ورد في تقرير المقرر الخاص المعني بتعزيز وحماية الحق في حرية التعبير، يمكن تعريف التشفير بأنه "عملية رياضية لتحويل الرسائل أو المعلومات أو البيانات إلى شكل لا يمكن أن يقرأه إلا المتلقي المستهدف" وبالتالي، يُمكّن التشفير من ضمان سرية وسلامة المحتوى من أي اعتراض أو مراقبة من طرف الغير.[22]

ويسمح الحق في التشفير للأفراد بممارسة الحق في حرية التعبير بفضل حيز الخصوصية الذي يوفره، مما يتيح الحصول على المعلومات والآراء وتبادلها خاصة في سياقات الأنظمة السلطوية. كما يُمكن الأفراد من إخفاء هويتهم لتجنب الملاحقات القضائية والاعتداءات الجسدية بسبب آرائهم وأفكارهم.

وفي هذا السياق، تجدر الإشارة إلى أن القوانين في معظم الدول العربية، مثل الأردن وتونس وليبيا والإمارات العربية المتحدة وسوريا، وضعت شروطاً للحصول على ترخيص لاستعمال خدمات التشفير أو منعت استيراد هذه الخدمات دون ترخيص مسبق من طرف الدولة، فارضة عقوبات سالبة للحرية في حال خرق هذه المواد.

وقبل التطرق إلى الإشكالات القانونية التي يمكن أن تترتب عن هذه القوانين في مجال الحق في حرية التعبير والحق في الخصوصية سنقوم بعرض أهم المعايير الدولية المتعلقة بهذين الحقّين.

المعايير الدولية ذات الصلة

ساهم التطور التكنولوجي في تمكين الأفراد من ممارسة حقوقهم والتواصل فيما بينهم للدفاع عن القضايا التي تهم المصلحة العامة، مما ساعد على تعزيز المشاركة الواسعة في النقاشات العامة والحصول على المعلومات الضرورية لتقييم السياسات التي تتبناها الدول في شتى المجالات.

---

[22] تقرير المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير حول استخدام التشفير وإخفاء الهوية في الاتصالات الرقمية، 22 مايو 2015، **A/HRC/29/32**، الفقرة 7.

ومع اتساع نطاق العمل المدني والسياسي بفضل الفضاء الرقمي، سارعت الدول العربية بسن عدة قوانين من بينها التشريعات السيبرانية بهدف تطويق هذه الأنشطة، بصورة تبدو في أحيان عديدة متعارضة مع التزاماتها الدولية في حماية حقوق الإنسان. ومن أكثر الحقوق تضرراً جراء هذه السياسات والتشريعات هما الحق في حرية التعبير والحق في الخصوصية.

الحق في حرية التعبير

إن الحق في حرية الرأي والتعبير محمي بموجب المادة **19** من العهد الدولي الخاص بالحقوق المدنية والسياسية الذي صادقت عليه أغلب دول المنطقة باستثناء المملكة العربية السعودية والإمارات العربية المتحدة وسلطنة عُمان.[23]

ويتحتم على الدول، وفقا للمادة **19**، أن تضمن لجميع الأفراد حرية البحث عن المعلومات أو الأفكار مهما كان نوعها أو طريقة تلقيها أو نقلها، وذلك دون اعتبار للحدود وعبر أي نوع من الوسائط التي يختارها الشخص المعني. وأكدت اللجنة المعنية بحقوق الإنسان التابعة للأمم المتحدة أن نطاق الحق يمتد إلى التعبير عن الآراء والأفكار التي قد يعتبرها الآخرون مهينة للغاية.[24]

على الرغم من أن الحق في حرية التعبير حق أساسي، إلا أنه ليس مطلقاً. إذ يمكن للدول أن تقوم بتقييده وفقاً لأحكام الفقرة الثالثة من المادة **19** من العهد الدولي الخاص بالحقوق المدنية والسياسية، شريطة أن يتوافق القيد مع متطلبات الاختبار الثلاثي في قانون حقوق الإنسان الدولي المتمثل في:

1. **التنصيص على القيد** ضمن قانون وصياغته بصورة واضحة ودقيقة تسمح للأفراد بتنظيم سلوكهم وتوقّع العقاب الذي يمكن أن تيفرض عليهم عند مخالفة النص القانوني. وفي

---

[23] يمكن الاطلاع على قائمة الدول الموقعة على العهد الدولي الخاص بالحقوق المدنية والسياسية عبر الرابط التالي:
https://tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/Treaty.aspx?Treaty=CCPR&Lang=en

[24] أنظر/ي: التعليق العام رقم **34** لسنة **2011**، متوفر عبر الرابط التالي:
http://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsrdB0H1l5979OVGGB%2BWPAXiks7ivEzdmLQdosDnCG8FaOQ8NtR0qo4QbSwsZswN%2B9bC7%2FEzsK6tod9c78bXmcQ6AhdwlYYbPRQT9A3SJawC8

هذا الإطار، أكد المقرر الخاص سنة **2016** على أن استخدام المصطلحات الفضفاضة في النصوص القانونية يتعارض مع شرط الدقة بما أنها "تسمح للمسؤولين بسلطة تقديرية مفرطة لتحديد معناها"[25]

2. **تحقيق إحدى الغايات المشروعة** بموجب قانون حقوق الإنسان الدولي وهي احترام حقوق الآخرين أو سمعتهم، أو حماية الأمن القومي أو النظام العام، أو الصحة العامة أو الآداب العامة.

3. **شرط الضرورة والتناسب** في مجتمع ديمقراطي ويكون ذلك عبر اختيار العقاب أو الإجراء الضروري لتحقيق الغاية ولكن الأقل تقييداً وتدخلاً في الحرية.

في ضوء ما سبق، فإن أي تقييد تقرّه الدولة على الحق في حرية التعبير ينبغي أن يكون ملائماً لمقتضيات الاختبار الثلاثي. من جهة ثانية، أكد مجلس الأمم المتحدة لحقوق الإنسان بأن "نفس الحقوق التي يتمتع بها الأشخاص خارج الإنترنت يجب أن تكون محمية أيضًا عبر الإنترنت، ولا سيما حرية التعبير، التي تنطبق دونما اعتبار للحدود وبأي وسيط من وسائط الإعلام يختاره الفرد"[26]

كما أوصى أصحاب الولايات الأربع لحماية الحق في حرية التعبير الدول بأن "تمتنع عن اعتماد قوانين غير ضرورية و / أو غير متناسبة تجرم أو تفرض عقوبات على التعبير على الإنترنت أشد من تلك المرادفة

---

[25] تقرير المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير حول التحديات المعاصرة التي تعترض حرية الرأي والتعبير، 6 سبتمبر 2016، **A/71/373**، الفقرة 13.

[26] قرار مجلس حقوق الإنسان رقم **20/8** بتاريخ 16 يوليو 2012 المتعلق بتعزيز وحماية حقوق الإنسان على الإنترنت والتمتع بها، **A/HRC/RES/20/8**، الفقرة الأولى.

وقع التأكيد على نفس المبدأ صلب الإعلان المشترك الصادر عن المقرر الخاص للأمم المتحدة حول حرية الرأي والتعبير وممثل منظمة الأمن والتعاون في أوروبا حول الإعلام والمقرر الخاص لمنظمة الدول الأمريكية حول حرية التعبير والمقرر الخاص للجنة الأفريقية لحقوق الإنسان والشعوب حول حرية التعبير والوصول إلى المعلومات حول "حرية التعبير والإنترنت"، **2011**.

خارج الإنترنت"[27] وبناءً عليه، يعتبر تجريم المحتوى في التشريعات السيبرانية وفرض عقوبات أشد من تلك المنصوص عليها في قوانين العقوبات أو الصحافة والنشر مخالفاً للمعايير الدولية.

الحق في الخصوصية

جاء الحق في الخصوصية صلب المادة **17** من العهد الدولي الخاص بالحقوق المدنية والسياسية إذ تنص على أن "لا يجوز تعريض أي شخص، على نحو تعسفي أو غير قانوني، لتدخل في خصوصياته أو شؤون أسرته أو بيته أو مراسلاته، ولا لأي حملات غير قانونية تمس شرفه أو سمعته. من حق كل شخص أن يحميه القانون من مثل هذا التدخل أو المساس"[28]

يمثّل الحق في الخصوصية ضمانة أساسية لبقية الحقوق في العصر الرقمي، بما أن المساس به من شأنه أن يثير الرعب والخوف لدى الأفراد وبالتالي منعهم من ممارسة حقوقهم بكل حرية وأمان. وفي هذا الصدد، أكدت المحكمة العليا في الهند على أن "الخصوصية أسمى تعبير عن حرمة الفرد. وهي قيمة دستورية تمتد عبر طائفة واسعة من الحقوق الأساسية، وتحمي للفرد حيزاً من الاختيار وتقرير المصير"[29]

وفي خضم تواتر عمليات التنصت والتجسس على المدافعين/ات عن حقوق الإنسان والصحفيين/ات والمعارضين/ات وغيرهم/ن من الذين يصدعون بآرائهم بكل حرية، شدّدت المفوضية السامية لحقوق الإنسان في تقريرها حول الحق في الخصوصية في العصر الرقمي على أهمية قيام الدول

---

[27] إعلان مشترك حول "استقلال وتنوع وسائل الإعلام في العصر الرقمي" صادر عن المقرر الخاص للأمم المتحدة حول حرية الرأي والتعبير وممثل منظمة الأمن والتعاون في أوروبا حول الإعلام والمقرر الخاص لمنظمة الدول الأمريكية حول حرية التعبير والمقرر الخاص للجنة الأفريقية لحقوق الإنسان والشعوب حول حرية التعبير والوصول إلى المعلومات، **2018**.

[28] يمكن الاطلاع على التعليق العام رقم **16** بخصوص الحق في حرمة الحياة الخاصة الصادر عن اللجنة المعنية بالحقوق المدنية والسياسية عبر الرابط التالي:

http://hrlibrary.umn.edu/arabic/hrc-gc16.html

[29] وقع ذكر هذا القرار في تقرير المقرر الخاص المعني بالحق في الخصوصية الذي قدمه خلال الدورة **37** لمجلس حقوق الإنسان.

https://www.ohchr.org/ar/documents/reports/report-special-rapporteur-right-privacy-0

بتوفير جميع الضمانات اللازمة لمنع أي انتهاك. ومن أهم هذه الضمانات إنشاء هياكل رقابية مستقلة لرصد عمليات الرقابة التي تمارسها الدول أو أطراف أخرى.[30]

وفي نفس السياق، أكدت المحكمة الأوروبية في عدة قرارات على ضرورة استجابة إجراء الرقابة على الاتصالات التي يجريها الأفراد إلى شروط الشرعية والمشروعية والتناسب.[31] كما تقوم المحكمة بالتثبت من مدى احترام الإطار القانوني الوطني للضوابط التالية:

1. الأسباب التي تبيح إجراء الرقابة واعتراض الاتصالات،
2. الظروف التي يمكن خلالها اعتراض الاتصالات التي يجريها الأفراد،
3. الإجراءات المعتمدة للحصول على ترخيص الاعتراض،
4. الإجراءات المتبعة لاختيار وفحص واستعمال المضامين التي وقع اعتراضها،
5. الاحتياطات التي ينبغي مراعاتها عند تسليم المحتوى التي وقع اعتراضه لأطراف أخرى،
6. القيود المتعلقة بمدة الاعتراض وتأمين نتائج الاعتراض وإتلافها،
7. الإجراءات المتعلقة بمراقبة هذا الإجراء من طرف هيكل مستقل وصلاحياته الردعية في صورة مخالفة الضمانات المذكورة أعلاه،
8. إجراءات الرقابة البعدية والضمانات التي تمكّن من ترتيب الجزاء المناسب.[32]

---

[30] تقرير مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، 30 يونيو 2014، **A/HRC/27/37**.
https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F27%2F37&Language=E&DeviceType=Desktop

[31] يراجع في هذا السياق الدليل الصادر عن المحكمة الأوروبية لحقوق الإنسان بخصوص تطبيقات الفصل **الثامن** من الاتفاقية الأوروبية لحقوق الإنسان:
https://www.echr.coe.int/documents/d/echr/guide_art_8_eng

[32] يمكن الاطلاع على القرار عبر الرابط التالي:
https://hudoc.echr.coe.int/eng#{%22languageisocode%22:[%22FRE%22],%22appno%22:[%2258170/13%22,%2262322/14%22,%2224960/15%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22],%22itemid%22:[%22001-210280%22

من جهته، شدّد المقرر الخاص المعني بتعزيز وحماية الحق في حرية التعبير على أهمية التشفير في ممارسة فعالة وحقيقية لحرية التعبير عن الآراء والمعلومات ونشرها واستقائها. كما تعرّض إلى أهمية استخدام الشبكات الافتراضية الخاصة أو شبكة "تور" (Tor) بالإضافة إلى التشفير لتمكين الأفراد من الوصول إلى المعلومات في الدول التي تفرض قيوداً تمييزية على المحتوى.[33] وأوصى بأن تضمن الدول حق الأفراد في التعبير عن آرائهم دون إجبارهم على كشف هويتهم وتجنب اشتراط استعمال الهوية الحقيقية عند إنشاء الحسابات. واعتبر أن الحظر الشامل يتعارض مع مبدأ الضرورة والتناسب في مجتمع ديمقراطي.

نستنتج مما سبق الارتباط الوثيق بين الحق في حرية التعبير والحق في الخصوصية، وأن أي قيد على هذين الحقّين ينبغي أن يتماشى مع الاختبار الثلاثي، وهو ما تفتقر إليه غالبية المواد القانونية التي تتضمّنها التشريعات السيبرانية في المنطقة العربية.

الإشكاليات القانونية المترتبة عن التشريعات المتعلقة بالجرائم السيبرانية في المنطقة العربية

تترتب عن التشريعات المتعلقة بالجرائم السيبرانية عدة آثار وخيمة على تمتع الأفراد بحقوقهم، إذ أن العقوبات السالبة للحرية والسلطات الواسعة للدول في اعتراض الاتصالات وحجز الأجهزة تنفّرهم من المشاركة في الحياة العامة والتصريح بمواقفهم.[34]

---

[33] تقرير المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير حول استخدام التشفير وإخفاء الهوية في الاتصالات الرقمية، 22 مايو 2015، **A/HRC/29/32**.

[34] لمزيد من التفاصيل حول الانتهاكات المتصلة بالحق في حرية التعبير، أنظر/ي:
الشبكة العربية السورية لحقوق الإنسان، القانون رقم **20** لسنة **2022** الذي أصدره النظام السوري كرس قمع حرية الرأي والتعبير وتسبب في عشرات حالات الاعتقال التعسفي:
https://snhr.org/arabic/2023/08/18/%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%B1%D9%82%D9%85-20-%D9%84%D8%B9%D8%A7%D9%85-2022-%D8%A7%D9%84%D8%B0%D9%8A-%D8%A3%D8%B5%D8%AF%D8%B1%D9%87-%D8%A7%D9%84%D9%86%D8%B8%D8%A7%D9%85-%D8%A7%D9%84/#:~:text=%D8%B0%D9%83%D8%B1%20%D8%A7%D9%84%D8%AA%D9%82%D8%B1%D9%8A%D8%B1%20%D8%A3%D9%86%20%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86%202

وعلى الصعيد الدولي، تعيق هذه التشريعات التعاون الدولي من أجل التصدي للجرائم السيبرانية نظراً لأنها تحتوي على مواد عديدة مخالفة للقانون الدولي لحقوق الإنسان الأمر الذي يدفع في بعض الأحيان بعض الدول إلى رفض تقديم المساعدة التقنية أو إرسال الأدلة الرقمية أو تسليم المطلوبين للقضاء بسبب استناد طلبات الدول العربية إلى تشريعات متعارضة مع الصكوك الدولية المتعلقة بحقوق الإنسان.

ا. عدم احترام الاختبار الثلاثي المتعلق بضوابط الحق في حرية التعبير

في البداية، نذكّر بموقفنا الرافض لإدماج جرائم المحتوى ضمن القوانين المتعلقة بالجرائم السيبرانية. من جهة أخرى، سنقوم في هذا الجزء بإبراز أوجه تعارض القوانين العربية المتعلقة بالجرائم السيبرانية مع مقتضيات الفقرة الثالثة من المادة **19** من العهد الدولي للحقوق المدنية والسياسية والتي تنص على أنه بإمكان الدول تقييد الحق في حرية التعبير شريطة احترام شروط الشرعية والمشروعية والضرورة والتناسب في مجتمع ديمقراطي.

ا.ا استعمال عبارات فضفاضة لتجريم المحتوى الرقمي

وفقاً للجنة الأمم المتحدة المعنية بحقوق الإنسان، يجب على الدول أن تنص على القيود الواردة على الحق في حرية التعبير ضمن قانون. وأكدت على أن تقع صياغته "بدقة كافية لكي يتسنى للفرد ضبط سلوكه وفقاً لها" كما شددت على أنه "لا يجوز أن يمنح القانون الأشخاص المسؤولين عن تنفيذه

0,%D9%88%D8%A5%D9%86%D9%85%D8%A7%20%D8%B9%D8%A8%D8%B1%20%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86%20%D8%A7%D9%84%D8%AC%D8%AF%D9%8A%D8%AF%20%D9%81%D9%87%D9%88

أكساس ناو، الحق في حرية التعبير بتونس: إطار قانوني يشجع على السكوت:

https://www.accessnow.org/foe-report-ar

مركز الخليج لحقوق الإنسان، خارطة قوانين مكافحة الجرائم الالكترونية وانتهاكات الحقوق الرقمية في منطقة الخليج والدول المجاورة:

https://www.gc4hr.org/ar/%d8%ae%d8%a7%d8%b1%d8%b7%d8%a9-%d9%82%d9%88%d8%a7%d9%86%d9%8a%d9%86-%d9%85%d9%83%d8%a7%d9%81%d8%ad%d8%a9-%d8%a7%d9%84%d8%ac%d8%b1%d8%a7%d8%a6%d9%85-%d8%a7%d9%84%d8%a5%d9%84%d9%83%d8%aa%d8%b1%d9%88/

سلطة تقديرية مطلقة في تقييد حرية التعبير. ويجب أن ينص القانون على توجيهات كافية للمكلفين بتنفيذه لتمكينهم من التحقق على النحو المناسب من أنواع التعبير التي تخضع للتقييد وتلك التي لا تخضع لهذا التقييد"[35]

بالرجوع إلى القوانين المتعلقة بالجرائم السيبرانية في الدول العربية نلاحظ أنها تحتوي على عبارات فضفاضة وغير دقيقة يمكن استعمالها من قبل الأجهزة الأمنية والمحاكم لتقييد الحق في حرية التعبير بصورة غير مشروعة. على سبيل المثال، جرّمت المادة **28** من القانون السوري والمادة **22** من القانون الإماراتي والمادة **24** من القانون السوداني كل من ينشر أخبار كاذبة من شأنها **النيل من هيبة الدولة**.

كما نصت المادة **6** من القانون السعودي والمادة **19** من القانون السوداني والمادتان **15 و17g** من القانون العُماني والمادة **26** من القانون المصري والمادة **26** من القانون السوري والمادتان **33** و**34** من القانون الإماراتي على تجريم نشر كل ما من شأنه **المساس بالآداب العامة**.

كذلك نجد تجريماً للمحتوى الذي **يمس بقيم الإسلام** في كل من المادة **19** من القانون العُماني والمادة **21** من القانون الموريتاني والمادة **22** من القانون السوداني والمادة **31** من القانون السوري والمادة **6** من القانون السعودي والمادة **17** من القانون الأردني.

ومن بين الجرائم الغريبة، نجد **جريمة اغتيال الشخصية عبر منصات التواصل الاجتماعي** التي جاءت بها المادة **16** من القانون الأردني أو **جريمة الإغواء لارتكاب الفجور** ضمن المادة **15** من القانون العُماني و**جريمة تحسين المعاصي** الواردة بالمادة **37** من القانون الإماراتي.

أخيراً، نَصّ القانون الجزائري المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في المادة **2** أن الجرائم السيبرانية هي جرائم المساس بأنظمة

---

[35] أنظر/ي: التعليق العام رقم **34** لسنة **2011**، الفقرة 25، متوفر عبر الرابط التالي:
http://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6OkG1d%2FPPRiCAqhKb7yhsrdB0H1l5979OVGGB%2BWPAXiks7ivEzdmLQdosDnCG8FaOQ8NtR0qo4QbSwsZswN%2B9bC7%2FEzsK6tod9c78bXmcQ6AhdwlYYbPRQT9A3SJawC8

المعالجة الآلية للمعطيات المحددة في قانون العقوبات و**أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظوم معلوماتية أو نظام للاتصالات الإلكترونية**. تتمثل خطورة هذا التوجه التشريعي في تحويل كل الجرائم التي يمكن أن ترتكب في الفضاء السيبراني إلى جرائم سيبرانية وتغدو بالتالي خاضعة إلى الإجراءات التحقيقية الواسعة من مراقبة للاتصالات العمومية إلى تفتيش المنظومات المعلوماتية وحجز المعطيات المعلوماتية وغيرها من السلطات التي كان من الأسلم حصرها في الجرائم السيبرانية بالصرفة.

تتميز كل الجرائم المذكورة بطابعها المطاطي وقابليتها لعدة تأويلات وهو أمر خطير جداً على مبدأ الأمان القانوني للأفراد الذين لن يتمكنوا من توقّع الآثار التي يمكن أن تترتب عن المضامين الرقمية التي يقومون بنشرها وبالتالي يصبحون عرضة للتتبعات والملاحقات الأمنية والقضائية.

١.٢ تقييد حرية التعبير لحماية غايات غير مشروعة

وفقاً للفقرة الثالثة من المادة **19** من العهد الدولي الخاص بالحقوق المدنية والسياسية، يجوز للدول وضع ضوابط للحق في حرية التعبير بهدف احترام حقوق الآخرين أو سمعتهم، أو حماية الأمن القومي أو النظام العام، أو الصحة العامة أو الآداب العامة. وبالعودة إلى مختلف التشريعات في المنطقة، نلاحظ وجود عدة جرائم محتوى لا تتلاءم مع شرط المشروعية، مما يجعلها مخالفة لأحكام المادة **19** المذكورة.

من ناحية أولى، وضعت الدول العربية عدة جرائم تهدف لمنع انتقاد المسؤولين وأجهزة الدولة، مثل المواد **25** من القانون الإماراتي و**28** من القانون السوري و**24** من القانون السوداني و**24** من القانون التونسي. نذكّر في هذا السياق بأن أشكال التعبير المهينة للشخصيات السياسية لا تكفي لتبرير فرض عقوبات وفقاً للتعليق العام رقم **34** لسنة **2011 الصادر عن** اللجنة المعنية بحقوق الإنسان. كما أعربت اللجنة عن "قلقها إزاء القوانين التي تتعلق بمسائل، مثل العيب في الذات الملكية وإهانة الموظف العمومي وعدم احترام السلطات وعدم احترام العلم والرموز، والتشهير برئيس الدولة وحماية شرف الموظفين العموميين"

من ناحية أخرى، تضمّنت التشريعات التي تناولتها هذه الورقة عدة جرائم محتوى بهدف الحفاظ على الآداب العامة، وقيم الأسرة، ومبادئ الإسلام وهيبة الدولة. وتتأسس هذه الجرائم على عبارات فضفاضة وقابلة للتأويلات المتضاربة، مما يسمح لأجهزة الدولة بفرض ذوقها التسلّطي على الآراء والعادات المختلفة عنها. وفي هذا الصدد، أكدت اللجنة المعنية بحقوق الإنسان أن "مفهوم الأخلاق مستمد من تقاليد اجتماعية وفلسفية ودينية عديدة؛ وعليه، يجب أن تستند القيود المفروضة بغرض حماية الأخلاق إلى مبادئ غير مستمدة حصراً من تقليد واحد. ويجب أن تفهم هذه القيود في ضوء عالمية حقوق الإنسان ومبدأ عدم التمييز"[36]

١.٣ سن عقوبات غير ضرورية ومتناسبة في مجتمع ديمقراطي

ترى أكساس ناو أن جلّ جرائم المحتوى غير ضرورية علاوة على عدم تناسب العقوبات مع الأفعال موضوع التجريم.

من ناحية أولى، نذكّر بأنه من واجب الدول، طبقاً لأحكام المادة **19**، أن تضمن لجميع الأفراد حرية البحث عن المعلومات أو الأفكار مهما كان نوعها أو تلقيها أو نقلها، وذلك دون اعتبار للحدود وعبر أي نوع من الوسائط التي يختارها الشخص المعني. وفي هذا الإطار، أكد المقرر الخاص المعني بتعزيز وحماية الحق في حرية التعبير على أن حرية التعبير في الفضاء الرقمي تخضع إلى نفس النظام القانوني المنطبق في الفضاء الحقيقي.

من هذا المنطلق، يصبح من غير الضروري إضافة جرائم القذف والسب والإساءة ونشر الأخبار المضللة إلى قوانين الجرائم السيبرانية طالما أنها مجرمة بموجب قوانين أخرى. على سبيل المثال، تجرم المادة **24** من مرسوم الجرائم السيبرانية في تونس الثلب والشتم على الرغم من التنصيص عليها في المادتين **55** و**57** من المرسوم عدد 115 المتعلق بحرية الصحافة والطباعة والنشر والمادة **245**

---

[36] أنظر/ي: التعليق العام رقم **34** لسنة **2011**، الفقرة 25، متوفر عبر الرابط التالي:
http://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6OkG1d%2FPPRiCAqhKb7yhsrdB0H1l5979OVGGB%2BWPAXiks7ivEzdmLQdosDnCG8FaOQ8NtR0qo4QbSwsZswN%2B9bC7%2FEzsK6tod9c78bXmcQ6AhdwlYYbPRQT9A3SJawC8

من المجلة الجزائية.[37] ونلاحظ نفس الأمر في سلطنة عُمان حيث تجرم المادة **16** من قانون الجرائم السيبرانية القذف والسب على الرغم من التنصيص عليها في المواد **366** وما بعد من قانون الجزاء.

والأخطر من كل هذا هو التشديد في العقاب عندما تُرتكب نفس الجريمة عبر أنظمة المعلومات والاتصال. ففي تونس، يعاقب الثلب بموجب المرسوم **115** بخطية قدرها 700 دولار، في حين يصبح العقاب بموجب المرسوم المتعلق بالجرائم السيبرانية خمس سنوات سجن ويمكن أن يصل إلى 10 سنوات في حال إذا وُجِّه الثلب إلى موظف عمومي. أما في سلطنة عُمان، فعقوبة السب حسب المادة **367** من قانون الجزاء هي السجن من 10 أيام إلى ستة أشهر، في حين أن المادة **16** من قانون الجرائم السيبرانية تضمّنت عقوبة أدناها سنة وأقصاها ثلاث سنوات.

نستنتج بالتالي أن إضافة جرائم المحتوى ضمن التشريعات المتعلقة بالجرائم السيبرانية تظل غير ضرورية نظراً لوجود قوانين أخرى قابلة للتطبيق. كما أن وضع عقوبات متفاوتة بالنسبة لنفس المضامين يتعارض مع مبدأ المساواة الذي يقتضي تطبيق نفس القواعد القانونية على الوضعيات المتشابهة.

من ناحية ثانية، أكدت اللجنة المعنية بحقوق الإنسان التابعة للأمم المتحدة على أن نطاق الحق يمتد إلى التعبير عن الآراء والأفكار التي قد يعتبرها الآخرون مهينة للغاية.[38] ولذلك فإن تجريم المضامين التي يُمكن أن توصف بالمسيئة تعد مخالفة لما دعت إليه اللجنة المذكورة لا سيما عندما يتعلق الأمر بالانتقادات الموجهة لكبار المسؤولين في الدولة.

أخيراً، أقرّت جل التشريعات العربية المتعلقة بالجرائم السيبرانية عقوبات سالبة للحرية في جرائم القذف كالمادة **16** من القانون العماني أو **24** من القانون التونسي أو **15** من القانون الأردني أو **25** من

---

[37] لمزيد من التفاصيل حول الإطار القانوني التونسي المتعلق بحرية التعبير، يراجع:
https://www.accessnow.org/foe-report-ar

[38] أنظر/ي: التعليق العام رقم **34** لسنة **2011**، متوفر عبر الرابط التالي:
http://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsrdB0H1l5979OVGGB%2BWPAXiks7ivEzdmLQdosDnCG8FaQQ8NtR0qo4QbSwsZswN%2B9bC7%2FEzsK6tod9c78bXmcQ6AhdwlYYbPRQT9A3SJawC8

القانون السوداني. يتعارض هذا التّوجه التشريعي مع دعوات المنظمات الدولية واللجنة المعنية بحقوق الإنسان إلى نزع صفة الجرم عن التشهير، وألا تكون عقوبة السجن على الإطلاق هي العقوبة المناسبة.[39]

٢. غياب الضمانات المرتبطة بالحق في الخصوصية

لا شك أن التطور التكنولوجي ساهم في دعم الحقوق والحريات وتعزيز الفضاء المدني وتطوير آليات عمل عدة جهات، سواء كانت حكومات أو مؤسسات اقتصادية وأكاديمية أو منظمات دولية أو جمعيات محلية. لكن في المقابل، برزت تهديدات رقمية جديدة متعلقة خصوصاً بالرقابة واعتراض الاتصالات، ومنع العديد من الدول استعمال أدوات التشفير.

٢.١ ضعف الضمانات المتعلقة بالرقابة على الاتصالات

نبّه المقرر الخاص بتعزيز وحماية الحق في حرية التعبير من مخاطر الرقابة على بقية الحقوق والحريات خاصة وأن عدة دول تستغلها لتكميم أفواه المعارضين/ات أو معاقبة المنتقدين/ات أو معاقبة معدي/ات التقارير المستقلة.[40] وبالنظر لأثرها على الحق في الخصوصية وحرية التعبير، يجب أن تخضع عمليات التنصت والرقابة إلى إجراءات مشددة نظراً لكونها تؤدي إلى التطفل على خصوصية الأفراد وانتهاك حُرمة حياتهم/ن الخاصة. وينبغي أن تخضع لإشراف جهة قضائية مستقلة، وأن تقتصر على الكشف عن جرائم خطيرة وأن لا توجد تدابير أخرى أقل شدة من شأنها تحقيق نفس الغاية. كما ينبغي تحديد الفترة الزمنية التي سيقع فيها التنصت وإعلام الشخص المعني بالأمر إثر انتهاء التحقيقات بأنه كان عرضة لهذا الإجراء وحقّه في التقاضي في صورة وجود ضرر حصل له جراء هذه العملية.[41]

---

[39] يمكن الحصول على أكثر تفاصيل في دراسة لمنظمة المادة 19 حول تعريف القذف:
https://www.article19.org/data/files/medialibrary/38641/Defamation-Principles-(online)-.pdf

[40] تقرير المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير حول الحكومات وقطاع المراقبة الخاص، 28 مايو 2019، **A/HRC/41/35**. الفقرة 21.

[41] للاطلاع على المبادئ القانونية المتعلقة بالرقابة على الاتصالات، أنظر/ي:

وخلافاً لهذه المبادئ والإجراءات، تُقنّن التشريعات العربية المتعلقة بالجرائم السيبرانية اعتراض الاتصالات بين الأفراد ومراقبتها عبر منح الأجهزة الأمنية سلطات واسعة للرقابة بهدف إجراء التحقيقات في هذه الجرائم. فقد وقع التنصيص على هذا الإجراء مثلاً في المواد **10** من القانون التونسي و**4** من القانون الجزائري و**46** من القانون الموريتاني و**7** من القانون الليبي و**36** من القانون الفلسطيني.

وبالتمعّن في المواد المذكورة، نستنتج افتقارها للضّمانات الضرورية للحفاظ على التوازن بين الحق في الخصوصية والأهداف المشروعة التي تجيز عمليات التنصت.

أما في الجزائر فقد تضمّن القانون في مادته **4** عدة ضمانات كالإذن القضائي وأن يقع استنفاذ كل التدابير الأقل تدخلاً في خصوصية الأفراد، إلا أنه لم يتم التنصيص على ضرورة إعلام المعني بالأمر بعد انتهاء التحقيقات خاصة إذا لم يثبت ضده أي سلوك إجرامي.

٢.٢ منع التشفير وإخفاء الهوية

يشكّل التشفير أداة فعالة لتأمين سريّة محتوى الاتصالات والبيانات المحفوظة في الأجهزة التي يمكن أن تكون هدفاً لدى أطراف أخرى تسعى الاطلاع عليها لغايات غير مشروعة. واعتبر المقرر الخاص المعني بتعزيز وحماية الحق في حرية التعبير أن للتشفير وإخفاء الهوية أهمية بالغة في سياقات الأنظمة السلطوية بما أنهما يوفران "للأفراد والجماعات حيزاً من الخصوصية على الإنترنت يمكنهم من اعتناق الآراء وممارسة حرية التعبير دون تدخلات أو هجمات تعسفية أو غير

EFF and ARTICLE 19, International principles on the application of human rights law to communications surveillance, available online: https://www.ohchr.org/sites/default/files/Documents/Issues/Privacy/ElectronicFrontierFoundation.pdf

يراجع أيضا: تقرير المقرر الخاص المعني بتعزيز حماية حقوق الإنسان والحريات الأساسية في سياق مكافحة الإرهاب، 23 سبتمبر 2014، **A/69/397**، الفقرة 66.

قانونية"[42] كما يسمح التشفير وإخفاء الهوية للأفراد باستقاء المعلومات والأفكار عبر الإنترنت في الدول التي تمارس حجباً ممنهجاً على تدفق المعلومات كما هو الحال في معظم الدول العربية.

لكن عند مراجعة التشريعات المتعلقة بالجرائم السيبرانية في المنطقة، نلاحظ قيام العديد من الدول العربية (مثل المواد **22** من القانون المصري و**16** من القانون الإماراتي و**9** من القانون البحريني والمادة **12** من القانون الأردني) بتجريم استعمال التشفير كلما وقع استعماله لارتكاب الجرائم المنصوص عليها. أما ليبيا فقد منعت بمقتضى المادة **9** من قانونها بصورة مطلقة حيازة أدوات التشفير، إلا إذا تم الحصول على ترخيص يسند من طرف الهيئة الوطنية لأمن وسلامة المعلومات.

ورغم أن معاقبة من يستخدم التشفير عمداً ودون وجه حق بهدف التدخل في أنظمة المعلومات وتدميرها وإتلاف البيانات أمر مقبول، إلا أن المواد المذكورة تتجاوز هذه الغاية المشروعة لتشمل كل جرائم المحتوى مثل الدعوة إلى التظاهر، أو المساس بهيبة النظام وقيم الأسرة والدعوة إلى الفجور وتحسين المعاصي. وهذه كلها مضامين محمية، في الأصل، بموجب الحق في حرية التعبير.

لذلك ترى أكساس ناو أن أي قيود عامة على التشفير وإخفاء الهوية هي غير شرعية، وفي حال وجود تحقيقات جنائية تتعلق بأفراد معينين ينبغي أن تكون خاضعة للاختبار الثلاثي، أي يجب أن ينص عليها قانون واضح ودقيق، وأن تكون الغاية منها حماية مصلحة مشروعة، وأن تتلاءم خاصة مع شرطي الضرورة والتناسب، علاوة على وجود إذن قضائي يسمح بهذا التدخل.

٢.٣ إلزام مزودي خدمات الاتصال بالاحتفاظ ببيانات المستخدمين بصورة مسبقة وشاملة

يحظى الحق في الخصوصية، والتبعات المترتبة عليه بخصوص حماية البيانات الشخصية في العصر الرقمي، بحماية واسعة على مستوى القانون الدولي لحقوق الإنسان لما له من ارتباط وثيق بحماية الذات الإنسانية وبقية الحقوق والحريات.

[42] تقرير المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير حول استخدام التشفير وإخفاء الهوية في الاتصالات الرقمية، A/HRC/29/32، 22 مايو 2015، الفقرة 16.

ومن بين أكثر المواد التي من شأنها المساس بحماية البيانات الشخصية نجد تلك المتعلقة بإلزام مزودي خدمات الاتصال بالاحتفاظ بصورة مسبقة بالبيانات المتعلقة بحركة الاتصالات لجميع المستخدمين بقطع النظر عن وجود إذن قضائي في إطار تحقيقات جنائية تجاه أفراد محددين (مثل المواد **11** من القانون الجزائري، **72** من القانون اللبناني، **31** من القانون الفلسطيني، **6** من القانون التونسي، و **2** من القانون المصري).

من المعترف به عموماً أن تحليل هذا النوع من البيانات يُمكّن من استخلاص استنتاجات دقيقة حول العادات اليومية للأفراد وأماكن إقامتهم وتحركاتهم وعلاقاتهم الاجتماعية وغيرها من المعلومات التي يمكن استخلاصها من بيانات الاتصالات. لذلك يمثّل التخزين المسبق والعام لهذه البيانات مساساً بالحق في الخصوصية وانتهاكاً لحماية البيانات الشخصية وتدخلاً غير ضروري ولا متناسب في هذا الحق. فالطبيعة الشمولية والعشوائية لهذا الالتزام المفروض على مقدمي خدمات الاتصال تهدد بشكل واضح الحق في الخصوصية وحرية التعبير، خاصة للأشخاص الذين يرغبون في إخفاء هويتهم عندما يعبرون عن آرائهم أو ميولاتهم السياسية والفكرية والجندرية.[43]

لهذا السبب بالذات أصدرت محكمة العدل الأوروبية عدة قرارات اعتبرت فيها أن إلزام مقدمي خدمات الاتصال بتخزين بيانات الحركة لجميع المستخدمين بصورة مسبقة وآلية دون وجود أي شبهات ارتكاب جريمة معينة يشكل مساساً بالحق في حماية البيانات الشخصية والحياة الخاصة. وكانت الدعاوى تتعلق إما بمصادقة البرلمان الأوروبي ومجلس الاتحاد الأوروبي على التوجيه رقم EC/2006/24 سنة 2006، بخصوص تخزين مقدمي خدمات الاتصال لبيانات الاتصالات بهدف مزيد إحكام التصدي للجرائم الخطيرة في الاتحاد الأوروبي، أو بخصوص قوانين ولوائح صادرة عن بعض الدول الأوروبية بخصوص

---

[43] يراجع الدليل الذي أعدته منظمة الأمن والتعاون الأوروبي حول ضمان احترام حقوق الإنسان عند مباشرة التحقيقات في الجرائم السيبرانية (باللغة الانجليزية):

Organization for Security and Co-operation in Europe, Ensuring Human Rights Compliance in Cybercrime Investigations, 13 October 2023. Available online: https://www.osce.org/secretariat/554901

تقرير المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير حول استخدام التشفير وإخفاء الهوية في الاتصالات الرقمية، 22 مايو 2015، A/HRC/29/32، الفقرة 16.

نفس الموضوع. وقامت محكمة العدل الأوروبية بتقييم مدى انسجام التوجيه والقوانين المذكورة مع المادتين 7 و8 من الميثاق الأوروبي لحقوق الإنسان لتتوصل لكونه مخالفاً للميثاق بسبب عدم احترام شرطي الضرورة والتناسب.[44]

[44] بخصوص قرارات محكمة العدل الأوروبية، يراجع:

القرار المؤرخ في 8 أبريل 2014، متوفر عبر الرابط التالي:

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293

القرار المؤرخ في 21 ديسمبر 2016، متوفر عبر الرابط التالي:

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62015CJ0203

القرار المؤرخ في 6 أكتوبر 2020، متوفر عبر الرابط التالي:

https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:62017CJ0623

جدول توضيحي بخصوص أغلب الجرائم السيبرانية في المنطقة العربية بالمقارنة مع اتفاقية بودابست والاتفاقية العربية لمكافحة جرائم تقنية المعلومات[45]

الجريمة	اتفاقية بودابست	الاتفاقية العربية	تونس	مصر	قطر	الكويت	الاتفاقية العربية	العربية السعودية	البحرين	عمان	الأردن	الجزائر 46	المغرب 47	ليبيا	موريتانيا	السودان	سوريا	العراق	لبنان 48	فلسطين	اليمن
النفاذ غير المشروع	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	X	√	√	X
الاعتراض غير	√	√	√	√	√	√	X	√	√	√	√	√	√	√	√	√	√	X	X	√	X

[45] اعتمدنا في إعداد هذا الجدول بصورة أساسية على الجرائم التي نصت عليها القوانين المتصلة بالجرائم السيبرانية.
بالنسبة للدول التي قامت بتعديل قانونها الجنائي وإضافة جرائم متعلقة بأنظمة المعلومات والاتصال، قمنا بالاعتماد على هذه الجرائم فقط دون غيرها من الجرائم التي يمكن أن تُستعمل فيها أنظمة المعلومات والاتصال مثل القذف والسب في الفضاء السيبراني.
بالنسبة للدول التي اعتمدت تعريفا واسعا للجرائم السيبرانية من خلال اعتبار أن كل جريمة ارتكبت بواسطة أنظمة المعلومات والاتصال، اعتمدنا على قانونها الجنائي لإثراء هذا الجدول.

[46] وقع تضمين الجرائم السيبرانية صلب قانون العقوبات الجزائري بموجب القانون رقم **15-04** المؤرخ في 10 نوفمبر 2004. في سنة 2009، أصدرت الجزائر القانون رقم **04-09** المؤرخ في 5 أغسطس 2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. ويتعلق هذا القانون بالجانب الإجرائي فقط حيث ظلت الجرائم منظمة بموجب قانون العقوبات. عرف قانون 2009 الجريمة السيبرانية بكونها جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية. من هذا المنطلق، تصبح كل الجرائم القابلة للارتكاب بواسطة أنظمة المعلومات الاتصال جرائم سيبرانية.

[47] على الرغم من عدم وجود قانون للجرائم السيبرانية لكن توجد عدة قوانين تضم عددا من الجرائم التي يمكن أن ترتكب بواسطة أنظمة المعلومات الاتصال مثل القانون الجنائي وقانون مكافحة الإرهاب وقانون المسطرة الجنائية والقانون المتعلق بتعزيز الحماية الجنائية للطفل والمرأة.

[48] قمنا بالاعتماد على القانون رقم **81** المؤرخ في 10 أكتوبر 2018 المتعلق بالمعاملات الالكترونية والبيانات ذات الطابع الشخصي لاستخراج الجرائم السيبرانية.

المشروع																				
التدخل في البيانات	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	X
التدخل في نظام المعلومات والاتصال	√	X	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	X
إساءة استخدام الأجهزة	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	X
التزوير السيبراني	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	X
الاحتيال السيبراني	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	X	√	X
الجرائم ذات الصلة بمواد إباحية عن الأطفال	√	√	√	√	X	√	√	√	√	√	√	√	√	√	√	√	√	√	√	X
الجرائم المتعلقة بانتهاكات حقوق النشر والتأليف	√	√	√	X	√	√	√	√	√	√	√	√	√	√	√	√	√	X	√	X
الجرائم المتعلقة بالمواد الإباحية للراشدين/ات أو نشر المحتوى المخل بالحياء	X	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	X	√	X
المقامرة	X	√	X	X	√	X	√	X	√	X	√	X	√	√	X	X	X	X	√	X
الاعتداء على الحياة الخاصة	X	√	√	√	√	√	√	X	√	√	√	X	√	√	√	√	√	X	√	X

الجرائم المتعلقة بالإرهاب	X	√	X	X	X	√	X	√	√	√	X	√	X	√	√	√	√	X	X	√	X	X
الجرائم المتعلقة بغسيل الأموال أو ترويج المخدرات أو الاتجار بالأشخاص أو الاتجار غير المشروع بالأسلحة	X	√	X	X	√	√	X	√	X	√	√	√	X	√	√	√	X	X	X	√	X	X
الاستخدام غير المشروع لأدوات الدفع الالكترونية	X	√	X	X	√	X	X	√	X	√	√	√	X	X	√	√	√	√	X	√	X	X
جرائم متعلقة باستخدام أدوات التشفير	X	X	X	X	X	X	X	√	X	X	√	X	√	X	√	X	X	√	X	X	X	X
الدعوة إلى قلب نظام الحكم أو تعطيل أحكام الدستور والقوانين	X	X	X	X	√	X	X	X	X	√	X	X	X	X	√	√	X	X	X	X	X	X
نشر معلومات للإضرار بمصالح الدولة أو السخرية من رموزها أو المساس بدولة أجنبية	X	X	X	X	√	√	√	√	X	√	X	√	X	√	√	√	√	√	X	X	X	X
الترويج لإثارة الفتنة والإضرار	X	X	X	X	√	√	X	√	X	√	√	X	X	√	√	X	X	X	X	X	X	X

بالوحدة الوطنية																			
التحريض على مأموري الضبط القضائي أو بصورة عامة الموظفين العموميين	X	X	X	X	X	√	X	X	X	√	X	X	X	X	√	√	X	X	√	X	X
الدعوة والترويج لمظاهرات دون ترخيص	X	X	X	X	X	X	X	X	X	X	X	X	X	X	√	X	X	X	X	X	X
ازدراء الأديان	X	X	X	X	√	√	√	√	X	√	√	√	X	√	√	√	X	X	X	X	X
ترويج منتجات مظللة أو دون ترخيص	X	X	X	X	X	X	X	√	X	X	X	X	X	X	√	X	X	X	X	X	X
القذف والسب	X	√	X	X	√	√	X	√	X	√	√	√	X	√	√	√	√	√	√	X	X
نشر الأخبار الزائفة	X	X	X	X	√	√	X	√	X	√	√	X	X	X	√	√	√	X	√	X	X
قبول عطايا أو منافع لنشر أو فبركة أخبار زائفة أو مسيئة	X	X	X	X	X	X	X	√	X	X	√	X	X	X	X	X	X	√	X	X	X
التسول الإلكتروني	X	X	X	X	X	X	X	X	X	√	√	X	X	X	√	X	X	X	X	X	X

على ضوء المعايير الدولية المتعلقة بالحق في حرية التعبير والخصوصية واستناداً إلى التشريعات المتعلقة بالجرائم السيبرانية في المنطقة العربية والتطبيقات المتصلة بها، وضعت أكساس ناو ثماني توصيات لصناع القوانين والسياسات بهدف ضمان حقوق الإنسان في العصر الرقمي. مع التنويه بأن هذه التوصيات تمثل الحد الأدنى عند سن تشريعات متعلقة بالجرائم السيبرانية يأمل واضعوها أن تكون متماشية مع المعايير الدولية.

ما يجب على الدول فعله عند صياغة تشريعات متعلقة بالجرائم السيبرانية

- **ضرورة التنصيص الصريح على احترام الاتفاقيات الدولية المتعلقة بحقوق الإنسان**

لئن تعتبر الدول ملزمة باحترام الاتفاقيات الدولية المتعلقة بحقوق الإنسان بمجرد المصادقة عليها، إلا أن التنصيص على هذا الأمر ضمن التشريعات المتعلقة بالجرائم السيبرانية ضروري ومفيد عند التطبيق من طرف السلطات العمومية وخاصة المحاكم التي ينبغي عليها تأويل هذه التشريعات في ضوء الالتزامات الدولية في مجال حقوق الإنسان.

- **اشتراط نية العمد دون وجه حق كرُكن من أركان جرائم النفاذ إلى أنظمة المعلومات والاتصال**

يعتبر شرط نية العمد دون وجه حق شرطاً ضرورياً لتجنب تجريم ومعاقبة ممارسات مشروعة يكفلها قانون حقوق الإنسان الدولي مثل العمل الصحفي الاستقصائي أو الأنشطة التي يقوم بها الباحثون في مجال السلامة المعلوماتية. ذلك لأنهم لا يسعون من خلال أنشطتهم إلى تحقيق أي ضرر، بل

على العكس من ذلك، يمكن أن تساعد أنشطتهم في كشف التجاوزات والثغرات الأمنية في أنظمة المعلومات والاتصال.

- **يجب وضع ضوابط دقيقة بخصوص الرقابة على الاتصالات**

تشكّل عمليات التنصت واعتراض الاتصالات من أشد الوسائل تدخلاً في الحق في الخصوصية ولها تبعات مباشرة على التمتع الفعلي بالحق في حرية التعبير. وبموجب مبدأ الضرورة والتناسب ، يجب ألا يتم اللجوء لمثل هذه الأعمال إلا في صورة غياب سبل أخرى للكشف عن الجرائم. إذ ينبغي على الدول أن تختار الإجراء الأقل تدخلاً في الحرية والكفيل بضمان المصلحة الجديرة بالحماية.

وفي هذا السياق، أعرب المقرر المعني بالحق في الخصوصية عن قلقه إزاء "القوانين الحديثة المتعلقة بالمراقبة التي تسمح على نحو متزايد بإنشاء البيانات الشخصية والوصول إليها وتحليلها دون إذن وإشراف كافيين."[49]

ورغم أن الدول يحق لها اللجوء إلى اعتراض الاتصالات في صور محددة ومبررة بدوافع حقيقية وجدية، إلا أنه لا يمكن اللجوء إلى هذه التدابير إلا في حالات استثنائية وبعد استنفاذ الإجراءات الأخرى التي من شأنها كشف الحقيقة.

كذلك ينبغي أن تخضع عمليات الرقابة والتنصت إلى ضمانات أساسية ابتداء باشتراط الإذن القضائي المسبق الصادر عن سلطة قضائية مستقلة، وتحديد الأسباب التي بررت اللجوء إلى هذه الإجراء والمدة. كما ينبغي إعلام الشخص الذي تعرّض إلى هذا الإجراء إثر انتهاء الأبحاث مهما كانت نتائجها.[50]

---

[49] تقرير المقرر الخاص المعني بالحق في الخصوصية الذي وقع تقديمه خلال الدورة 34 لمجلس حقوق الإنسان.
https://www.ohchr.org/ar/documents/reports/report-special-rapporteur-right-privacy-note-secretariat

[50] للاطلاع على الضمانات المتصلة بالرقابة على الاتصالات، يراجع:
EFF and ARTICLE 19, International principles on the application of human rights law to communications surveillance, available online:
https://www.ohchr.org/sites/default/files/Documents/Issues/Privacy/ElectronicFrontierFoundation.pdf

- **احترام التعددية والشفافية عند صياغة قوانين الجرائم السيبرانية**

من الضروري أن يتم إشراك أصحاب المصلحة، وخاصة منظمات المجتمع المدني وخبراء حقوق الإنسان، عند صياغة التشريعات وتجنب المصادقة عليها بصورة فوقية. فتنظيم مشاورات واسعة من طرف السلطة التنفيذية أو التشريعية من شأنه أن يساعد في تحسين جودة التشريعات وتجنب التضارب بين النصوص القانونية والتعرف على الممارسات الفضلى في الأنظمة المقارنة.

- **يجب تخصيص باب ضمن قوانين الجرائم السيبرانية حول التربية الرقمية والإعلامية**

تمثّل التربية الرقمية والإعلامية وسيلة هامة لحماية الفضاء السيبراني من خلال تعزيز قدرات الأفراد على مستوى فهم طرق إنتاج المعلومات وآليات عمل المنصات الإلكترونية، بالإضافة إلى تعزيز المبادئ العالمية لحقوق الإنسان. كما تُمكن الأفراد من اكتساب المهارات الأساسية اللازمة حول كيفية استعمال أنظمة المعلومات والاتصال وحماية البيانات الشخصية.

وفي هذا السياق، أكد أصحاب الولايات لحماية الحق في حرية التعبير على أهمية الاعتماد على مقاربة شاملة ومستدامة لمواجهة الأضرار المحتملة الناتجة عن المحتوى الرقمي. وتعتمد هذه المقاربة على تبني تدابير إيجابية كالتربية على وسائل الإعلام ودعم منصات التحقق من الأخبار والمؤسسات الصحفية، بهدف تعزيز قدرة المجتمع على التعامل مع مختلف التحديات التكنولوجية الحديثة.[51]

[51] الإعلان المشترك الصادر عن المقرر الخاص للأمم المتحدة حول حرية الرأي والتعبير وممثل منظمة الأمن والتعاون في أوروبا حول الإعلام والمقرر الخاص لمنظمة الدول الأمريكية حول حرية التعبير والمقرر الخاص للجنة الأفريقية لحقوق الإنسان والشعوب حول حرية التعبير والوصول إلى المعلومات حول "حرية التعبير والإنترنت"، 2011.

تعتبر التربية الرقمية والإعلامية إجراءً مهماً من شأنه أن يعزز ملكة النقد لدى الأفراد وخاصة الناشئة. في هذا الإطار، وقع التأكيد، دولياً، على أهمية إدراج التربية على وسائل الإعلام ضمن المناهج التعليمية في المدارس والجامعات.[52]

إن التربية الرقمية والإعلامية تمثل حلاً مستداماً من خلال تحصين أفراد المجتمع وتزويدهم بالأدوات الضرورية لفهم المحتوى الرقمي وطرق إنتاجه. وهذا يجعلهم بمثابة جهاز مناعة مجتمعي قادر على التصدي للأخبار المضللة وغيرها من المضامين التي تمس بحقوق الإنسان.

ما يجب على الدول تركه عند صياغة تشريعات متعلقة بالجرائم السيبرانية

- **عدم إدراج جرائم المحتوى ضمن القوانين السيبرانية**

تخضع حرية التعبير في الفضاء الرقمي إلى نفس النظام القانوني المنطبق في الفضاء الواقعي. لذلك، ينبغي عدم إدراج جرائم المحتوى ضمن التشريعات السيبرانية والاقتصار على الجرائم السيبرانية بالصرفة أي التي تستهدف سلامة أنظمة المعلومات والاتصال.

- **عدم إلزام مزودي خدمات الاتصال بالمراقبة المسبقة للمحتوى أو تخزين البيانات بصورة شاملة ومسبقة**

يجب أن لا يقع إلزام مقدمي خدمات الاتصال بمراقبة المحتوى بصورة مسبقة لتفادي الرقابة القمعية على المضامين، بل يجب أن تكون الرقابة بعدية وبواسطة إذن قضائي من المحكمة المختصة واحترام الإجراءات المتعلقة بحقوق الدفاع ومبدأ المواجهة.

[52] إعلان مشترك حول "حرية التعبير والأخبار الزائفة، التضليل الإعلامي والدعاية" صادر عن المقرر الخاص للأمم المتحدة حول حرية الرأي والتعبير وممثل منظمة الأمن والتعاون في أوروبا حول الإعلام والمقرر الخاص لمنظمة الدول الأمريكية حول حرية التعبير والمقرر الخاص للجنة الأفريقية لحقوق الإنسان والشعوب حول حرية التعبير والوصول إلى المعلومات، 2017.

كما ينبغي عدم إلزام مقدمي خدمات الاتصال بتخزين بيانات الاتصال بصورة شاملة ومسبقة نظراً لتعارض هذا الالتزام مع المعايير الدولية المتعلقة بحماية البيانات الشخصية وأن يقع الاقتصار فقط على تقنين مسألة حفظ البيانات المتعلقة بحركة الاتصال في صورة وجود إذن قضائي صادر عن محاكم مستقلة في إطار تحقيقات جنائية متعلقة بأفراد محددين وأن يكون الإذن محدداً من ناحية زمنية مع ضرورة إعلام المعنيين به بعد انتهاء التحقيقات مهما كان مآلها.

- **عدم تجريم استعمال برمجيات التشفير وإخفاء الهوية**

للتشفير وإخفاء الهوية أهمية بالغة لممارسة حقوق الإنسان في العصر الرقمي دون خوف. لذلك ينبغي أن لا يقع تجريم استعمال أو توريد أو تداول أدوات التشفير وأن لا تقوم الدولة باتخاذ أي تدابير من شأنها إضعاف هذه الأدوات، لأن أي قيود شاملة على استعمال التشفير من طرف إلى طرف للاتصالات الآمنة أو أي إجراء يضعف هذه التكنولوجيا الآمنة للجميع سيكون متعارضاً بشكل أساسي مع المعايير الدولية لحقوق الإنسان، بما في ذلك الضرورة والتناسب.

ملحق بخصوص الإطار القانوني المتعلق بالجرائم السيبرانية في المنطقة العربية

الدول التي أصدرت تشريعات متعلقة بالجرائم السيبرانية (15)	الدول التي أدمجت الجرائم السيبرانية في قانون العقوبات (2)	الدول التي تفتقر لمواد قانونية متعلقة بالجرائم السيبرانية (2)
المملكة العربية السعودية (2007) المرسوم الملكي رقم م/17 لسنة 2007 المتعلق بنظام مكافحة جرائم المعلوماتية	**المغرب (2003)** القانون رقم 07.03 يتمم مجموعة القانون الجنائي في ما يتعلق بالجرائم المتعلقة بنظم المعالجة الآلية للمعطيات	**اليمن**
سلطنة عُمان (2011) مرسوم سلطاني رقم 12 / 2011 بإصدار قانون مكافحة جرائم تقنية المعلومات	**الجزائر (2004)** القانون رقم 04-15 الذي نقح قانون العقوبات لإضافة جرائم سيبرانية. قانون رقم 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها (يتعلق بالجانب الإجرائي فقط)	**العراق**
البحرين (2014) قانون رقم (60) لسنة 2014 بشأن جرائم تقنية المعلومات		
قطر (2014) قانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية		
الكويت (2015) قانون رقم 63 لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات		
موريتانيا (2016) القانون رقم 2016 - 007 المتعلق بالجريمة السيبرانية		
السودان (2018) قانون مكافحة الجرائم المعلوماتية		
فلسطين (2018) قرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية		
مصر (2018) قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018		

الدول التي أصدرت تشريعات متعلقة بالجرائم السيبرانية (15)	الدول التي أدمجت الجرائم السيبرانية في قانون العقوبات (2)	الدول التي تفتقر لمواد قانونية متعلقة بالجرائم السيبرانية (2)
المملكة العربية السعودية (2007) المرسوم الملكي رقم م/17 لسنة 2007 المتعلق بنظام مكافحة جرائم المعلوماتية	**المغرب (2003)** القانون رقم 07.03 يتمم مجموعة القانون الجنائي في ما يتعلق بالجرائم المتعلقة بنظم المعالجة الآلية للمعطيات	**اليمن**
لبنان (2018) قانون رقم 81 بخصوص المعاملات الالكترونية والبيانات ذات الطابع الشخصي		
الإمارات العربية المتحدة (2021) مرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية		
ليبيا (2022) قانون رقم 5 لسنة 2022 م بشأن مكافحة الجرائم الإلكترونية		
سوريا (2022) قانون الجرائم المعلوماتية رقم 20 لعام 2022		
تونس (2022) مرسوم عدد 54 لسنة 2022 مؤرخ في 13 سبتمبر 2022 يتعلق بمكافحة الجرائم المتصلة بأنظمة المعلومات والاتصال		
الأردن (2023) القانون رقم 17 لسنة 2023 المتعلق بالجرائم الالكترونية		