EUROMED JUSTICE

A programme funded by the European Union

مشروع يوروميد للعدالة

التحليل القانوني وتحليل الفجوة
الجريمة الإلكترونية

CrimEx

مجموعة خبراء يوروميد للعدالة في المسائل الجنائية

الجزائر، مصر، إسرائيل، الأردن، لبنان، المغرب، فلسطين، تونس

خبير يوروميد القضائي: السيد دانيال سوتر، المملكة المتحدة

مدير عام/رائد

FIIAPP COOPERACIÓN ESPAÑOLA

EIPA

CILC Center for International Legal Cooperation

JCI Justice Coopération Internationale

المؤلفون

كتب هذا التحليل القانوني والفجوات السيد دانيال سوتر (مدير آي جست إنترناشيونال، المملكة المتحدة)، بالتعاون مع: السيد دافيد مايور فيرناندیث (إسبانيا) والسيد جيل فرانسن (هولندا) والأستاذ الدكتور محمد عليوه بدر (مصر - المملكة المتحدة).

المحرر والمنسق

Virgil Ivan-Cucu، خبير قضائي في يوروميد، أستاذ محاضر في المعهد الأوروبي للإدارة العامة، اللوكسمبورج.

إصدارات لغوية

الإصدار الأصلي: الإنجليزية

أنجزت هذه المخطوطة في مارس 2018.زت هذه المخطوطة في يونيو 2018.

إخلاء طرف

المعلومات الواردة في تحليلات الثغرات القانونية وكُتيب ودليل الأدلة الرقمية، تستند إلى الأبحاث والمعلومات التي قدمها كبار الخبراء المعينون وممثلو دول الجنوب الشريكة في إطار العمل المنجز في إطار مشروع يوروميد للعدالة ، باستثناء لبنان. وفقاً للقانون اللبناني، لم يُساهم أي من القضاة والممثلين اللبنانين في العمل بأي وسيلة أو طريقة. لا يمكن اعتبار الكونسورتيوم الذي ينفذ المشروع مسؤولاً عن دقته أو واقعيته أو شموليته، كما لا يمكن اعتباره مسؤولاً عن أي أخطاء أو سهو يرد في هذه الوثيقة.

حقوق النشر

يصرح بالنسخ والترجمة لأغراض غير تجارية مصرح بها، شريطة ذكر المصدر، وفقًا لما يلي: «مشروع يوروميد للعدالة هو مشروع للاتحاد الأوروبي يعزز التعاون القضائي الدولي في المنطقة الأورومتوسطية». يرجى أيضًا إبلاغ يوروميد للعدالة وإرسال نسخة إلى العنوان التالي:

info@euromed-justice.eu

www.euromed-justice.eu

صفحة المحتويات

اختصارات 5

قاموس المصطلحات 6

مقدمة 11
الجرائم السيبرانية في دول الجنوب الشريكة 11
التهديدات السيبرانية 12
الأبعاد الدولية للجريمة السيبرانية 13

المنهجية 14
التحليل القانوني 14
تحليل الفجوة 15

السياق 16
المناهج الدولية 16
الأمم المتحدة 16
مجلس أوروبا 17
الاتحاد الأفريقي 18
جامعة الدول العربية ومجلس التعاون الخليجي 18
مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية (HIPCAR) 19
المركز الدولي للأطفال المفقودين والمستغلين (ICMEC) 19

التحليل القانوني وتحليل الفجوة 21
الجزائر 21
الجرائم 21
إجراءات 37
التعاون الدولي 48
مصر 57
الجرائم 57
إجراءات 73
التعاون الدولي 87
إسرائيل 96
الجرائم 96

إجراءات 106
التعاون الدولي 112
الأردن 116
الجرائم 116
إجراءات 129
التعاون الدولي 141
لبنان 151
الجرائم 151
إجراءات 168
التعاون الدولي 181
المغرب 190
الجرائم 190
إجراءات 207
التعاون الدولي 220
فلسطين 230
الجرائم 230
الإجراء 247
التعاون الدولي 253
تونس 259
الجرائم 259
إجراءات 278
التعاون الدولي 290

خلاصة 300

المرفق (أ) 301

اختصارات

AU	*الاتحاد الأفريقي*
AUC	*اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية*
BC	*اتفاقية بودابست بشأن الجريمة السيبرانية التابعة لمجلس أوروبا*
BSI	*معلومات المشترك الأساسية*
CA	*السلطة المركزية*
CERT	*فريق الاستعداد للحدث السيبراني*
CITO	*الاتفاقية العربية لمكافحة جرائم تقنية المعلومات*
CTED	*المديرية التنفيذية للجنة مكافحة الإرهاب التابعة للأمم المتحدة*
DDoS	*الحرمان من الخدمات الموزعة*
CSPs	*مزودو خدمة الاتصالات*
HIPCAR	*مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية*
IAP	*الرابطة الدولية للمدعين العامين*
ICMEC	*المركز الدولي للأطفال المفقودين والمستغلين*
ICT	*تكنولوجيا المعلومات والاتصالات*
INTERPOL	*منظمة الشرطة الجنائية الدولية*
ITU	*الاتحاد الدولي للاتصالات*
LoRs	*طلبات الإنابة القضائية*
LMA	*المساعدة القانونية المتبادلة*
MMS	*خدمة الرسائل المتعددة الوسائط*
MOU	*مذكرة تفاهم*
PA	*السلطة الفلسطينية*
SMS	*خدمة الرسائل القصيرة*
SPC	*بلد جنوبي شريك*
TRIPS	*الاتفاق المتعلق بجوانب حقوق الملكية الفكرية المتصلة بالتجارة*
UNTOC	*اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية*
URL	*عناوين الموارد الموحّدة*
UNODC	*مكتب الأمم المتحدة المعني بالمخدرات والجريمة*

قاموس المصطلحات

معلومات المشترك الأساسية (BSI)

يتم احتواء معلومات المشترك الأساسية في شكل بيانات حاسوبية أو أي شكل آخر، مثل السجلات الورقية وتتضمن معلومات تصف الشخص (على سبيل المثال، اسم وعنوان المشترك/صاحب الحساب)، وقد تتضمن بيانات عن استخدام الشخص لخدمة عبر الإنترنت في تاريخ ووقت محددين (على سبيل المثال، أوقات تسجيل الدخول إلى الحساب ومدة استخدام المشترك لهذه الخدمة المحددة، وما إلى ذلك). ويهدف "المشترك" إلى إدراج مجموعة كبيرة من عملاء مزودي الخدمة، من الأشخاص الذين لديهم اشتراكات مدفوعة وأولئك الذين يدفعون حسب الاستخدام وأولئك الذين يتلقون خدمات مجانية. كما يشمل المعلومات المتعلقة بالأشخاص الذين يحق لهم استخدام حساب المشترك.[1]

شبكات الحواسيب

شبكة من أجهزة الحاسوب المصابة ببرامج ضارة (فيروسات حاسوبية). وقد يتم تنشيط هذه الشبكة من أجهزة الحاسوب المعرضة للخطر ("الزومبي") لأداء إجراءات محددة، مثل مهاجمة أنظمة المعلومات (الهجمات الإلكترونية). ويمكن التحكم في هذه "الزومبي" - غالبًا دون علم مستخدمي أجهزة الحاسوب المعرضة للخطر - عن طريق حاسوب آخر. ويُعرف هذا الحاسوب "المسيطر" أيضًا باسم "مركز القيادة والتحكم"[2]

مزود خدمة الاتصالات (CSP)

يقوم مزود خدمة الاتصالات بنقل المعلومات إلكترونيًا، ويشمل الشركات في مجال الاتصالات (الأرضية واللاسلكية) والإنترنت والكابل والأقمار الصناعية وخدمات وسائل التواصل الاجتماعية.

نظام الحاسوب

أي جهاز أو مجموعة من الأجهزة المترابطة أو ذات الصلة، أو واحد أو أكثر من هذه الأجهزة يقوم بمعالجة البيانات تلقائيًا وفقًا لبرنامج ما[3]

1. التقرير التوضيحي لاتفاقية بودابست، الفقرة 177
2. ملاحظات توجيهية T-CY - فاتح مارس 2017 ص 6
3. المادة 1 أ. اتفاقية بودابست

العملة المشفرة

أصل رقمي مُصمم للعمل كوسيط لصرف العملات باستخدام التشفير لتأمين المعاملات والتحكم في إنشاء وحدات إضافية من العملة[4]

التنمر السيبراني أو التحرش السيبراني

التنمر أو التحرش باستخدام أشكال إلكترونية للاتصال والذي أصبح شائعًا بشكل متزايد، وخاصة بين المراهقين

الإنترنت المظلم

يشكل الإنترنت المظلم جزءًا صغيرًا من الشبكة العميقة، وهو جزء من الشبكة العنكبوتية العالمية غير المفهرسة بواسطة محركات البحث.[5]

الحرمان من الخدمات الموزعة

هجمات لقطع الخدمة (DOS) هي محاولات لجعل نظام الحاسوب غير متاح للمستخدمين من خلال مجموعة متنوعة من الوسائل. وقد تشمل تشبع أجهزة الحاسوب أو الشبكات المستهدفة بطلبات الاتصال الخارجية، وبالتالي عرقلة الخدمة للمستخدمين الشرعيين. هجمات لقطع الخدمة الموزعة (DDOS) هي هجمات لقطع الخدمة يتم تنفيذها بواسطة العديد من أجهزة الحاسوب في نفس الوقت. ويوجد حاليًا عدد من الطرق الشائعة التي يمكن بها تنفيذ الهجمات لقطع الخدمة (DOS) والهجمات لقطع الخدمة الموزعة (DDOS). وهي تشمل، على سبيل المثال، إرسال استعلامات تالفة إلى نظام الحاسوب؛ بما يتجاوز حد السعة للمستخدمين؛ وإرسال المزيد من رسائل البريد الإلكتروني إلى خوادم البريد الإلكتروني أكثر مما يمكن للنظام تلقيها ومعالجتها[6]

ازدواجية التجريم

تقتضي أن تكون الأفعال المحددة المزعومة تمثل جريمة في الدولة المتلقية للطلب والدولة المطالبة. ولا ينبغي أن تكون عناصر الجرائم المماثلة هي نفسها، ولكن يجب أن يكون معروفًا بالقدر الكافي أن السلوك إجرامي في كلتا الدولتين.

التشفير

هي عملية تشفير لرسالة أو معلومات بطريقة لا يمكن إلا للأطراف المصرح لها الوصول إليها (انظر أيضًا التشفير المطلق أدناه)

4. آندي غرينبرغ (20 أبريل 2011) العملة المشفرة
5. آندي غرينبرغ (19 نوفمبر 2014) معجم القرصنة: ما هي الشبكة المظلمة؟
6. ملاحظات توجيهية T-CY - فاتح مارس 2017 ص 18

التشفير المطلق

التشفير المطلق (E2EE) عبارة عن نظام اتصالات حيث يمكن للمستخدمين المتصلين فقط قراءة الرسائل. وتم تصميم التشفير المطلق E2EE للتغلب على أي محاولات للمراقبة أو العبث لأنه لا يمكن لأطراف ثالثة فك تشفير البيانات التي يتم توصيلها أو تخزينها في الخوادم. فعلى سبيل المثال، لا تستطيع الشركات، مثل WhatsApp، التي تستخدم التشفير المطلق، تسليم نصوص رسائل عملائها إلى جهات إنفاذ القانون.

القرصنة

انتهاك الدفاعات الأمنية للتمكن من الوصول غير القانوني إلى نظام حاسوب.

المناضل المقرصن

مقرصن يستخدم أجهزة الحاسوب وشبكات الحاسوب بطريقة تخريبية للترويج لأجندة سياسية أو تغيير اجتماعي.

IP عنوان

عنوان بروتوكول الإنترنت (عنوان IP) هو تسمية رقمية مخصصة لكل جهاز (مثل الحاسوب والطابعة) مشارك في شبكة الحاسوب التي تستخدم بروتوكول الإنترنت للاتصال. ويخدم عنوان IP وظيفتين أساسيتين: تحديد واجهة المضيف أو الشبكة ومعالجة الموقع.

Keylogger برامج

التسجيل بضغط المفاتيح، الذي يُشار إليه غالبًا باسم التسجيل بلوحة المفاتيح أو الالتقاط بلوحة المفاتيح، هو إجراء تسجيل (تسجيل الدخول) بالضغط على المفاتيح الموجودة في لوحة المفاتيح، بشكلٍ سري عادةً، بحيث يكون الشخص الذي يستخدم لوحة المفاتيح غير مدرك لمراقبة أفعاله.[7]

البرمجيات الخبيثة

توجد العديد من أشكال البرمجيات الخبيثة الحالية، والتي عرفتها منظمة التعاون الاقتصادي والتنمية بأنها "مصطلح عام لبرنامج يتم إدخاله في نظام معلومات للتسبب في ضرر لهذا النظام أو غيره من الأنظمة أو لإفساده واستخدامه في غرض بخلاف ذلك المقصود من قبل أصحابه."[8] وتشمل الأشكال المعروفة عادةً الفيروسات المتنقلة والفيروسات وأحصنة طروادة. تستطيع الأشكال الحالية من البرمجيات الخبيثة سرقة البيانات من خلال نسخها وإرسالها إلى عنوان آخر؛ كما يمكنهما التلاعب بالبيانات؛ ويمكنها عرقلة تشغيل أنظمة

7. "Keylogger" قواميس أكسفورد
8. http://www.oecd.org/internet/ieconomy/40724457.pdf

الحاسوب، بما في ذلك الأنظمة التي تتحكم في البنى التحتية الحيوية؛ وتستطيع فيروسات الفدية (رانسوم وير) حذف البيانات أو منعها أو عرقلة الوصول إليها؛ ويمكن للبرمجيات الخبيثة المصممة خصيصًا أن تستهدف أنظمة حاسوب محددة[9]

بيانات التعريف

هي البيانات التي توفر معلومات عن جانب أو أكثر من جوانب البيانات، مثل:

1. وسائل إنشاء البيانات
2. الغرض من البيانات
3. وقت الإنشاء وتاريخه
4. مُنشئ البيانات أو معدها
5. موقع إنشاء البيانات على شبكة الحاسوب
6. المعايير المستخدمة (مثل المعايير الهندسية أو التقنية الموحدة والأساليب والعمليات والممارسات)

التصيد الاحتيالي

محاولة الحصول على معلومات حساسة مثل أسماء المستخدمين وكلمات المرور وتفاصيل بطاقة الائتمان (والأموال بشكلٍ غير مباشر) لأغراض خبيثة في معظم الأحيان، عن طريق التنكر ككيان جدير بالثقة في الاتصالات الإلكترونية[10]

فيروسات الفدية (رانسوم وير)

نوع من البرمجيات الخبيثة التي تحجب الوصول إلى بيانات الضحية أو تهدد بنشرها أو حذفها حتى يتم دفع فدية

المعاملة بالمثل

يقصد بمبدأ المعاملة بالمثل، والذي يُعرف أيضًا في هذا السياق باسم التبادلية، اعتراف الدولة التي تتلقى الطلب بنفس عمليات التحقيق والمحاكمة التي يمكن للدولة الطالبة استخدامها محليًا.

الرسائل الإباحية القصيرة

إرسال الرسائل أو الصور الجنسية الصريحة أو تلقيها أو إعادة توجيهها

9. ملاحظات توجيهية T-CY - فاتح مارس 2017 ص 22
10. *Ramzan, Zulfikar (2010) Phishing attacks and countermeasures - In Stamp, Mark & Stavroulakis, Peter Handbook of Information and Communication Security Springer.*

البريد العشوائي

بريد إلكتروني مجمع غير مرغوب فيه، حيث يتم إرسال رسالة إلى عدد كبير من عناوين البريد الإلكتروني، حيث لا صلة لهوية المستلم الشخصية بالأمر لأن الرسالة تستهدف العديد من المستلمين الآخرين دون تمييز[11]

التصيُّد الاحتيالي الموجَّه

محاولات تصيد تستهدف أفراد أو كيانات مؤسسية محددة - وتعتبر هذه التقنية إلى حد بعيد الأكثر نجاحًا على الإنترنت اليوم، حيث تمثل 91% من الهجمات[12]

تور (الشبكة الخفية)

برنامج مجاني لتمكين الاتصال المجهول - والاسم مشتق من اختصار لاسم مشروع البرنامج الأصلي وهو "The Onion Router (التوجيه البصلي)"[13]

بيانات الحركة

المعلومات التي تتضمن السجلات التي تحدد هوية من قام المشترك بالتواصل معه ومواقع الويب التي زارها المشترك ومعلومات مماثلة عن نشاط المستخدم عبر الإنترنت

محدد موقع الموارد المُوحّد

يعد محدد موقع الموارد المُوحّد أحد أنواع معرفات الموارد الموحدة؛ ويطلق المصطلح العام على جميع أنواع الأسماء والعناوين التي تشير إلى الأشياء الموجودة على شبكة الويب العالمية.

11. ملاحظات توجيهية 1 - T-CY مارس 2017 ص 24
12. Debbie Stephenson (27 July 2014) Spear Phishing: Who's Getting Caught?
13. مشروع تور: الأسئلة الشائعة www.torproject.org

مقدمة

الجرائم السيبرانية أو الجرائم ذات الصلة بالحاسوب، هي الجرائم التي تنطوي على وجود حاسوب وشبكة اتصال.[14] قد يُستخدم الحاسوب في ارتكاب جريمة، أو قد يكون هو المستهدَف.[15] وتتألف الشبكة من أكثر من نظامي حاسوب[16] ويمكن أن تكون شبكة محلية أو شبكة منطقة أوسع.

تُعد الجرائم السيبرانية ظاهرة عالمية نظرًا لزيادة عدد أجهزة تكنولوجيا المعلومات والاتصالات المتصلة بالإنترنت. ففي عام 2016، أشارت التقديرات إلى أن تكلفة الجرائم السيبرانية قد تصل إلى 2.1 تريليون دولار على مستوى العالم بحلول عام 2019.[17] كما تشير التقديرات إلى أن أكثر من 80 في المائة من أفعال الجريمة السيبرانية تتخذ شكلاً ما من أشكال الجريمة المنظمة، لاسيما مع إنشاء الأسواق السوداء للجرائم السيبرانية والفيروسات الحاسوبية وإدارة شبكات الحواسيب وجمع البيانات الشخصية والمالية وبيع البيانات و "التربح" من المعلومات المالية.[18] أظهر هجوم واناكراي الإلكتروني بفيروسات الفدية (رانسوم وير) الذي وقع يوم 12 مايو 2017 الأثر العالمي للجرائم السيبرانية - التي قدرت بأنها أثرت على 200.000 جهاز حاسوب في 150 دولة.

ترجع الزيادة الحادة في الإجرام السيبراني بشكلٍ رئيسي إلى أن شبكة الإنترنت توفر فرصًا كبيرة للمجرمين المنظمين لتجميع أرباح هائلة من خلال مخططات احتيالية. ولا شك أن الطريقة التقليدية لإنفاذ القوانين والمتمثلة في القبض على المشتبه فيه والحصول على اعترافه وتوجيه التهمة إليه ومثوله أمام المحكمة باتت قديمة. فيما يتعلق بالجرائم السيبرانية، ربما يكون المشتبه فيه خارج نطاق الاختصاص القضائي، لذلك يجب النظر في مرحلة مبكرة في مقبولية الأدلة التي يتم الحصول عليها من خلال أساليب التحقيق الخاصة[19] والجرائم محل الاتهام والمساعدة القانونية المتبادلة وتسليم المجرمين وتقارير الخبراء. وتجري هذه التحقيقات في الوقت المناسب، لكنها معقدة ومكلفة. ويستغل مرتكبو الجرائم السيبرانية عدم تكيف القانون الجنائي مع بيئة الإنترنت، ويكون المسؤولون عن إنفاذ القوانين غير مجهزين بالأدوات اللازمة للتحقيق بشكلٍ صحيح. والغرض من هذا البحث هو مراجعة سياق الجرائم السيبرانية في دول الجنوب الشريكة وتحديد الفجوات التشريعية وتقديم توصيات لتعزيز أطرها القانونية وإجراءات التحقيق والتعاون الدولي.

الجرائم السيبرانية في دول الجنوب الشريكة

حددت مراجعة للجرائم السيبرانية في منطقة الشرق الأوسط وشمال إفريقيا عام 2012[20] خمسة تحديات أساسية وهي:

1. **المسؤولية:** لا توجد لوكالة حكومية وحدها السبق في صياغة أو تحديث قوانين الجرائم السيبرانية.
2. **التشريعات:** إما غير موجودة أو صيغت من غير إتقان دون النظر إلى العنصر الدولي والحاجة لأدوات تحقيق محددة
3. **القدرات التقنية:** ليس لدى مسؤولي إنفاذ القوانين فهمًا كافيًا لضمان سلامة الأدلة المتعلقة بالحاسوب
4. **الهيكل التنظيمي:** لا توجد وكالة محددة مكرسة لإنفاذ أحكام الجرائم السيبرانية ووضع استراتيجيات للتقدم التكنولوجي.
5. **التعليم:** يوجد عدد قليل من الحملات العامة لزيادة الوعي حول انتشار الجرائم السيبرانية أو التدريب لإنفاذ القوانين لضمان إدراك الجمهور للاتجاهات والتهديدات الحالية

14. R. Moore (2005) Cyber crime: Investigating High-Technology Computer Crime
15. Warren G. Kruse, Jay G. Heiser (2002) Computer forensics: incident response essentials
16. بمعنى جهاز حاسوب كامل عامل. ويشمل نظام الحاسوب أحد الحواسيب إلى جانب أي برمجيات وأجهزة طرفية ضرورية لعمل الحاسوب http://www.webopedia.com/TERM/C/computer_system.html
17. https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion
18. المرجع السابق
19. تشير المادة 20 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية إلى تقنيات التحقيق الخاصة، بما فيها «المراقبة الإلكترونية أو غيرها من أشكال المراقبة والعمليات السرية".
20. Mohamed N. El-Guindy (2012) Cybercrime Challenges in the Middle East

استجابت بعض دول الجنوب الشريكة لهذه التحديات كالآتي:

1. يوجد في إسرائيل فريق التأهب الوطني لمواجهة الأحداث السيبرانية - وهو جزء من الهيئة الوطنية للدفاع السيبراني، وقد انضم إلى اتفاقية بودابست ولديه قانون خاص بالأنظمة السيبرانية (قانون الحواسيب 1995).
2. أنشأت النيابة العامة الفلسطينية وحدة متخصصة في فبراير 2017، ولدى الشرطة الفلسطينية إدارة تتبع للجرائم السيبرانية والإلكترونية.
3. يوجد في مصر مباحث مكافحة جرائم الحاسبات وشبكات المعلومات لمواجهة التهديدات السيبرانية
4. حدَّث الأردن مؤخرًا التشريعات المختصة بقانون الجرائم الإلكترونية رقم 27 لسنة 2015
5. يوجد في الجزائر وكالة حكومية وهي الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال المنشأة بموجب المرسوم الرئاسي رقم 15-261 الصادر بتاريخ 08-10-2015 (في اليوم الرسمي 53 من العام 2015)، والهيئة مسؤولة عن جملة أمور منها اقتراح استراتيجية وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال والمساهمة في تحديث المعايير القانونية في هذا المجال.

التهديدات السيبرانية

حدد تقرير بخصوص تهديدات الجرائم السيبرانية في منطقة الشرق الأوسط وشمال أفريقيا صادر عام 2014 أن معظم الهجمات السيبرانية التي تستهدف البنية التحتية لتكنولوجيا المعلومات والاتصالات كانت هجمات الحرمان من الخدمات الموزعة (DDoS) أو تشويش على المواقع الإلكترونية.[21] كما يسلط التقرير الضوء على قابلية التعرض للهجمات السيبرانية بسبب الافتقار إلى التنظيم والأطر القانونية المناسبة.[22] إضافة إلى ذلك، يُنظر إلى قارة إفريقيا غالبًا باعتبارها ملاذًا آمنًا لمرتكبي الجرائم السيبرانية.[23]

تزداد التحديات أهمية إذا علمنا أن 55% من الأسر التي شملتها الدراسة في التقرير المتعلق بوسائل التواصل الاجتماعي العربية لديها 2-5 أجهزة مزودة بالإنترنت (بخلاف أجهزة الحاسوب والحواسيب المحمولة) و 25% أخرى لديها من 6 إلى 10 أجهزة متصلة بالإنترنت.[24]

بلغ عدد مستخدمي الإنترنت في الدول العربية 161 مليون مستخدم في عام 2016[25] ولا سيما منذ تزايد استخدام شعوب الربيع العربي لمنصات وسائل التواصل الاجتماعي بشكلٍ ملحوظ. حيث يوجد لدى فيسبوك 156 مليون مستخدم وهو ما يمثل زيادة قدرها 40 مليون مستخدم مقارنةً بالعام الماضي.[26] وازداد عدد مستخدمي فيسبوك في مصر بأكثر من 14 مليون مستخدم والجزائر 9.3 مليون والمغرب 5.5 مليون.[27] كذلك يستخدم تويتر عدد كبير، حيث يصدر من مصر 152 مليون تغريدة شهريًا والجزائر 71 مليون تغريدة.[28] ويترتب على هذا الاستخدام الكبير لوسائل التواصل الاجتماعي[29] سرقة الهوية والتنمر السيبراني وتداول المواد الجنسية والتطرف.[30] وقد استُخدمت وسائل التواصل الاجتماعي بشكلٍ كبير كقناة لجمع الأموال للإرهابيين وتجنيدهم ونشكر أفكارهم واستخدام المعلومات مفتوحة المصدر [31]لشن الهجمات.

21. Mohamed N. El-Guindy (2014) Middle East Security Threat Report
22. المرجع السابق.
23. Eric Tamarkin, (20 January 2015) The AU's Cybercrime Response. A Positive Start, but Substantial Challenges Ahead, Policy Brief 73
24. تقرير وسائل التواصل الاجتماعي العربية 2017 www.arabsocialmediareport.com
25. http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx
26. المرجع السابق، ص. 33
27. المرجع السابق، ص. 37
28. المرجع السابق، ص. 48
29. https://www.internetmatters.org/issues/
30. http://www.independent.co.uk/news/world/middle-east/what-makes-people-join-isis-expert-says-foreign-fighters-are-almost-never-recruited-at-mosque-a6748251.html
31. http://www.bbc.co.uk/news/world-middle-east-18532839

الأبعاد الدولية للجريمة السيبرانية

للتحقيق بشكلٍ فعال في الجرائم السيبرانية ومحاكمة مرتكبيها، يلزم وجود تعاون وثيق بين الدول. ويمكن للنظام الحالي للمساعدة القانونية المتبادلة (MLA) أن يكون معقدًا وبيروقراطيًا، مما يؤدي إلى التأخير في الحصول على الأدلة. ولا يتجاوب ذلك مع الطبيعة السريعة للجريمة السيبرانية، فالإنترنت لا يعرف الحدود. وإضافة إلى ذلك، تم إنشاء المسائل الخاصة بالولاية القضائية[32] من خلال الحوسبة السحابية، والتي تتطلب وجود دراسة متأنية حيث يتم إرسال طلبات المساعدة القانونية المتبادلة الرسمية للتنفيذ.[33] ومن المهم للغاية تحديد الإجراءات للاستجابة السريعة لحوادث الطوارئ والحفاظ على الأدلة، وكذلك طلبات التعاون الدولي.[34]

32. انظر: tropeR emoctuO ٦١٠٢ enuJ ٢ ,eugaH ehT ,tsujoruE «ecapsrebyC ot syeK» ranimeS cigetartS

33. بشأن مسألة مذكرة التفتيش لحساب بريد إلكتروني معين خاضع لسيطرة وتصرف شركة مايكروسوفت في القضية رقم ٥٨٩٢-٤١، قررت محكمة الاستئناف الأمريكية (الدائرة الثانية) عدم صحة مسألة المذكرة لمحتوى البريد الإلكتروني في الولايات المتحدة نظرًا لتخزين البيانات في الخارج وعلى وزارة العدل التواصل مع الحكومة الأيرلندية بموجب اتفاقية المساعدة القانونية المتبادلة القائمة للوصول لتلك البيانات. وهناك استئناف مقدم على القرار الآن أمام المحكمة العليا الأمريكية.

34. فهم الجريمة السيبرانية: الظواهر والتحديات والاستجابة القانونية (الاتحاد الدولي للاتصالات) صفحة ٣

المنهجية

إن التحديات القانونية والتقنية والمؤسسية التي تفرضها الجريمة السيبرانية مسألة عالمية ولا يمكن التعامل معها إلا باستراتيجية متماسكة، مع مراعاة دور مختلف أصحاب المصلحة والمبادرات القائمة،[35] في إطار التعاون الدولي.[36] وسيركز هذا البحث على الإطار التشريعي والتعاون الدولي، بما يتفق مع المعايير الدولية،[37] للتصدي للجريمة السيبرانية في دول الجنوب الشريكة.

يقدم هذا البحث التحليل القانوني وتحليل الفجوة للجريمة السيبرانية في دول الجنوب الشريكة، بناءً على:

1. الإجابات على استبيان الجريمة السيبرانية المرسلة إلى كل دولة من دول الجنوب الشريكة
2. عروض دول الجنوب الشريكة في جلسات CrimEx المنعقدة في ماسترخت بتاريخ 8 مايو 2017
3. البحوث التي أجراها المستشارين العلميين في كل دولة من دول الجنوب الشريكة
4. البحوث التي أجريت عبر الموارد عبر الإنترنت[38]

التحليل القانوني

استعرض هذا البحث التشريعات في كل دولة من دول الجنوب الشريكة والتصديق على الاتفاقيات الدولية[39] والإقليمية ذات الصلة بالجرائم السيبرانية وستركز على ثلاثة مجالات:

1. **الجرائم:** لتحقيق أغراض هذا البحث، سيتم النظر في الجرائم التالية:

a. الأعمال التي تمس بسرية البيانات أو النظم الحاسوبية وسلامتها وتوافرها

- النفاذ بطريقة غير مشروعة إلى نظام حاسوبي
- النفاذ غير المشروع إلى بيانات الحواسيب أو اعتراض هذه البيانات أو حيازتها
- التدخل غير المشروع في النظم أو البيانات الحاسوبية
- إنتاج أو توزيع أو حيازة أدوات لإساءة استعمال الحواسيب
- انتهاك تدابير حماية الخصوصية أو حماية البيانات

b. الأفعال المتصلة بالحاسوب والمرتكَبة للحصول على مكسب شخصي أو مالي أو لإحداث ضرر

- الاحتيال أو التزوير بواسطة الحواسيب
- جرائم الهوية المرتكبة بواسطة الحواسيب
- جرائم حقوق المؤلف أو العلامات التجارية المرتكبة بواسطة الحواسيب
- الأعمال المرتكبة بواسطة الحواسيب والتي تتسبب في ضرر شخصي
- إغواء أو مراودة الأطفال بواسطة الحواسيب

35. انظر المبادرات الدولية أدناه
36. جدول أعمال الأمن السيبراني العالمي الذي وضعه الاتحاد الدولي للاتصالات / فريق خبراء رفيعي المستوى، التقرير الاستراتيجي العالمي، 2008، صفحة 14، متاح على: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.
37. قرار الجمعية العامة للأمم المتحدة: إرساء ثقافة عالمية تكفل أمن الفضاء الإلكتروني وتقييم الجهود الوطنية الرامية إلى حماية الهياكل الأساسية الحيوية للمعلومات، A/RES/64/211.
38. ويشمل ذلك بوابة الموارد الإلكترونية والقوانين المتعلقة بالجريمة (شيرلوك) التي أنشأتها الأمم المتحدة وغيرها من الموارد والنصوص المتاحة على الإنترنت - انظر قائمة المراجع
39. اتفاقية مجلس أوروبا لمكافحة الجرائم السيبرانية (بودابست) واتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية والاتفاقية العربية لمكافحة جرائم تقنية المعلومات

c. الجرائم المتصلة بالمحتوى الحاسوبي

- الأعمال المرتكبة بواسطة الحواسيب والتي تتضمن خطاب الكراهية
- إنتاج أو توزيع أو حيازة المواد الإباحية المتعلقة بالأطفال بواسطة الحواسيب
- أعمال دعم الجرائم الإرهابية بواسطة الحواسيب

2. **الإجراء:** تحتاج وكالات إنفاذ القوانين إلى الصلاحيات المناسبة للتحقيق في الجرائم السيبرانية. ويمكن أن تكون هذه التحقيقات معقدة ومتطورة بسبب استخدام الجناة تقنيات لإخفاء هويتهم. وتعني هذه التحديات ضرورة أن تكون الأدوات اللازمة للمحققين مختلفة عن الأدوات المستخدمة للتحقيق في جرائم حيازة وعنف أكثر تقليدية. وسيتم مراجعة الإجراءات التشريعية الحالية للتحقيق في الجرائم الإلكترونية.
3. **التعاون الدولي:** يمكن أن تشمل الجرائم السيبرانية ولايات قضائية عديدة، ويمكن أن يكون مرتكبو الجرائم والضحايا في ولايات مختلفة وتوجد الأدلة لدى مزودي خدمة الاتصالات في الخارج. وستتم مراجعة عمليات تمكين حفظ المحتوى والكشف عن بيانات الحركة واعتراض الوقت الفعلي للتحقيقات عبر الحدود بالاستعانة بالمساعدة القانونية المتبادلة.

تحليل الفجوة

عند تحديد الثغرات من التحليل القانوني، ستتم مراجعة ذلك إلى جانب اتفاقية بودابست لمكافحة الجرائم السيبرانية والاتفاقية العربية لمكافحة جرائم تقنية المعلومات واتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية وغيرها من السوابق مثل المبادئ التوجيهية للسياسة النموذجية والنصوص التشريعية لمواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية (HIPCAR) والمراجعة الدولية والتشريع النموذجي لإباحية الأطفال (الطبعة الثامنة 2016) الصادر عن المركز الدولي للأطفال المفقودين والمستغلين (ICMEC)

إن حقيقة وجود أحكام في القوانين الجنائية وقوانين العقوبات فيما يتعلق بالجرائم الموضوعية، مثل الاحتيال، لا يعني أنه يمكن تطبيقها على الأفعال المرتكبة عبر الإنترنت كذلك. وحدد تحليل القوانين الوطنية الحالية الفجوات وقدم توصيات للتشريعات القائمة في قسم **الجرائم**

أُدرجت التوصيات الخاصة بتمكين التحقيقات والملاحقات والمحاكمات المحلية بفعالية وكفاءة في قسم **الإجراءات**.

لتعزيز التحقيقات عبر الحدود، تم تقديم توصيات في قسم **التعاون الدولي**. وتم تقديم هذه التوصيات لدعم المساعدة القانونية المتبادلة بين دول الجنوب الشريكة وبين الدول الأعضاء في الاتحاد الأوروبي.

هذه مجرد توصيات مقترحة ويتعين على دول الجنوب الشريكة أن تحدد الجدوى بناءً على الموارد والأولويات. وتتطور الجريمة السيبرانية باستمرار وتزداد التهديدات، حيث أصبح المجتمع يعتمد بشكل كبير على استخدام تكنولوجيا المعلومات في جميع جوانب الحياة اليومية. ويكمن التحدي في سرعة الإصلاح التشريعي لمواجهة هذه المخاطر المتزايدة وتزويد وكالات إنفاذ القوانين بالأدوات اللازمة للتحقيق وتمكين الملاحقات القضائية الناجحة.

السياق

المناهج الدولية

تعمل عدد من المنظمات الدولية باستمرار لتحليل آخر التطورات في الجريمة السيبرانية:

الأمم المتحدة

في ثلاثة قرارات صادرة منذ فترة وجيزة (2322 (2016) و 2331 (2016) و 2341 (2017))، دعا مجلس الأمن الدول الأعضاء إلى جمع الأدلة والمحافظة عليها حتى تتم التحقيقات والملاحقات القضائية لمحاسبة الأشخاص المسؤولين عن الهجمات الإرهابية. وأشار القرار 2322 (2016) بالتحديد إلى الزيادة الكبيرة في طلبات التعاون في جمع البيانات والأدلة الرقمية من الإنترنت، وشدد على أهمية النظر في إعادة تقييم الطرق وأفضل الممارسات، حسب الاقتضاء، على وجه الخصوص، فيما يتعلق بتقنيات التحقيق والأدلة الإلكترونية.

لمواجهة هذه التحديات، أطلقت المديرية التنفيذية للجنة مكافحة الإرهاب التابعة للأمم المتحدة ومكتب الأمم المتحدة المعني بالمخدرات والجريمة والرابطة الدولية للمدعين العامين في فبراير من عام 2018 مبادرة عالمية لتعزيز قدرة السلطات المركزية والمدعين العامين والمحققين في الحفاظ على الأدلة الإلكترونية والحصول عليها في التحقيقات المتعلقة بمكافحة الإرهاب والجريمة المنظمة ذات الصلة عبر الحدود.

يدور المشروع المقترح حول مجموعة منظمة من الأنشطة المصممة خصيصًا والمركزة لتعزيز كفاءة المساعدة القانونية المتبادلة بما يشمل الأدلة الإلكترونية وتعزيز قدرة السلطات المختصة على التفاعل في ممارسة المساعدة القانونية المتبادلة والتواصل مع مزودي خدمة الاتصالات لتحقيق هذا الغرض. ويتمثل الغرض العام والهدف من المشروع في **تعزيز** قدرة السلطات المركزية والمدعين العامين وموظفي إنفاذ القوانين بخصوص أحدث الإجراءات لطلب الأدلة الإلكترونية في قضايا مكافحة الإرهاب والجريمة المنظمة. والأهداف المحددة هي:

1. الاستفادة القصوى من الموارد المتاحة للمساعدة القانونية المتبادلة بما يشمل الأدلة الإلكترونية من خلال ضمان: تحديد أولويات طلبات المساعدة القانونية المتبادلة فقط عندما لا يمكن الحصول على المعلومات والأدلة من خلال وسائل التعاون غير الرسمية؛ المعرفة الجلية لأنواع المساعدة المخصصة؛ توافر الإرشادات المنظمة حول طلب وجمع الأدلة الإلكترونية؛ توافر المعلومات المفيدة حول نقاط الاتصال الخاصة بمزودي خدمة الاتصالات كذلك، لإتاحة اتصالات وتنسيق أسرع وجاهزيتها للاستخدام.
2. تعزيز التعاون والتواصل بين السلطات المركزية والمدعين العامين والمحققين من مختلف الولايات القضائية، بما في ذلك مع مزودي خدمة الاتصالات.

تشمل الأنشطة المقترحة لمدة ثلاث سنوات: 1) إنشاء قاعدة بيانات للسلطة الوطنية المركزية للقضايا المتعلقة بالإرهاب؛ 2) تنظيم اجتماعين (2) لفريق خبراء حول طلب الأدلة الإلكترونية وجمعها؛ 3) تجميع نقاط الاتصال الخاصة بكل بلد والأطر القانونية والمتطلبات العملية للتعاون بشأن المساعدة القانونية المتبادلة غير الرسمية (من الشرطة إلى الشرطة والمدعي العام إلى المدعي العام) والرسمية؛ 4) إنشاء شبكة عالمية متخصصة وقاعدة بيانات للمدعين العامين المتخصصين في مكافحة الإرهاب؛ 5) التواصل مع مزودي خدمة الاتصالات وجمع نقاط الاتصال والقواعد الداخلية للتعاون مع وكالات إنفاذ القوانين وإنشاء قاعدة بيانات بهذه المعلومات؛ 6) تنظيم سبع (7) ورش عمل إقليمية على التوالي حول آسيا الوسطى وجنوب آسيا وجنوب شرق آسيا والشرق الأوسط وشمال إفريقيا وأفريقيا جنوب الصحراء وأمريكا اللاتينية و 7) شرح منهج تدريبي للتعلّم الإلكتروني للمؤسسات الوطنية للتدريب على العدالة الجنائية والتعامل مع

طلب الأدلة الإلكترونية وجمعها، بما في ذلك من مزودي خدمة الاتصالات. ولاستكمال هذه المبادرة - تتعاون شرطة يوروميد ويوروميد للعدالة والمديرية التنفيذية للجنة مكافحة الإرهاب في صياغة موجه للأدلة الرقمية الخاص بدول الجنوب الشريكة (والتركيز على المساعدة القانونية المتبادلة مع مزودي خدمة الاتصالات في الولايات المتحدة) للتحقيقات والملاحقات في مكافحة الإرهاب.

مجلس أوروبا

في عام 1996، كونت اللجنة الأوروبية لمشاكل الإجرام لجنة من الخبراء[40] بين عامي 1997 و 2000 والتي صاغت اتفاقية لمكافحة الجرائم السيبرانية. والتي أصبحت معروفة باسم اتفاقية بودابست لمكافحة الجرائم السيبرانية[41] وهي أول معاهدة دولية بشأن الجرائم المرتكبة عن طريق شبكة الإنترنت وغيرها من شبكات الحاسوب، وهي الأولى من نوعها من حيث أنها تتناول على وجه الخصوص انتهاكات حقوق التأليف والغش المرتبط بالحاسوب والمواد الإباحية عن الأطفال وانتهاكات أمن الشبكة. كما تشتمل على سلسلة من الصلاحيات والإجراءات، من قبيل التفتيش عن الشبكات الحاسوبية واعتراضها.[42] ويتجلى الهدف الرئيسي من إبرامها، والوارد في ديباجتها، في السعي قدمًا وراء سياسة جنائية موحدة تهدف إلى حماية المجتمع من الجرائم السيبرانية، لا سيما عن طريق اعتماد تشريعات مناسبة وتعزيز التعاون الدولي. واعتبارًا من مايو 2017، صدّقت 55 دولة على الاتفاقية، بينما وقعت أربع دول أخرى على الاتفاقية ولكنها لم تصدق عليها.[43] وتدعم الاتفاقية منظمات دولية مثل الإنتربول.[44] وعلى الرغم من ذلك، تم التشكيك في تأثير اتفاقية بودابست،[45] لتصديق ثماني دول فقط عليها من خارج مجلس أوروبا[46] ونظرًا للقيود المفروضة على تطبيقها في بيئة الجريمة السيبرانية المتغيرة، مثل اعتراض الاتصالات الصوتية عبر بروتوكول الإنترنت (VoIP) ومسائل الولاية القضائية مع السحابة[47] ومقبولية الأدلة الرقمية[48] وإجراءات التعامل مع الاستخدام الناشئ لتكنولوجيا التشفير ووسائل الاتصال المجهول. ولم يتم تعديل الاتفاقية، وكانت الإضافة الوحيدة عليها هي البروتوكول الإضافي الأول.[49]

أحد الجوانب الأساسية في اتفاقية بودابست هو توفير شبكة على مدار الساعة[50] لتمكين التحقيق الفعال والحفاظ على الأدلة.[51] وأظهرت دراستان في عام 2008[52] و2009[53] أن الدول التي صدقت على الاتفاقية لا تزال تنشئ نقاط اتصال، على الرغم من أن هذا شرط إلزامي. وقد يمثل تحديًا لبعض الدول توفير نقطة اتصال واحدة (SPOC) في جميع الأوقات في حين أن الاستثمار في التحقيقات في الجرائم السيبرانية ضئيلاً. ورغم أنه بسبب سرعة الإجرام السيبراني، فإن نقطة اتصال واحدة عنصر أساسي لإطار دولي فعال.

40. التقرير التفسيري حول اتفاقية مكافحة الجرائم السيبرانية (185)، رقم 10
41. النص الكامل للاتفاقية 185 (اتفاقية مكافحة الجرائم السيبرانية) والبروتوكول الإضافي الأول وقائمة التوقيعات والتصديقات، انظر: www.coe.int
42. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
43. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=Sv9dObc4 - يُرجى ملاحظة أن القائمة غير محدّثة حيث قامة المغرب بالتصديق عليها في العام 2012
44. أبرز الإنتربول أهمية اتفاقية مكافحة الجرائم السيبرانية في قرار المؤتمر الدولي السادس المعني بالجريمة السيبرانية، القاهرة: "يُوصى باعتبار اتفاقية مجلس أوروبا لمكافحة الجرائم السيبرانية على أنها توفر الحد الأدنى من المعايير القانونية والإجرائية الدولية لمكافحة الجرائم السيبرانية. ويجب تشجيع الدول على التفكير في الانضمام إليها. وتوزع الاتفاقية على جميع البلدان الأعضاء في الإنتربول باللغات الرسمية الأربع"، وهي متاحة على الموقع التالي:
www.interpol.com/Public/TechnologyCrime/Conferences/6thIntConf/Resolution.asp
45. لمزيدٍ من المعلومات عن الإنجازات وأوجه القصور، انظر: جيرك، اتفاقية السنوات العشر بشأن الجرائم السيبرانية ومراجعة قانون الحاسوب الدولي، 2011، الصفحة 142 وما يليها.
46. المغرب (2012)، أستراليا (2013)، كندا (2015)، تشيلي (2017)، إسرائيل (2016)، اليابان (2012)، سريلانكا (2015) والولايات المتحدة (2007)
47. انظر: Strategic Seminar «Keys to Cyberspace» Eurojust, The Hague, 2 June 2016 Outcome Report
48. Lange/Nimsger (2004) Electronic Evidence and Discovery and Whitcomb, An Historical Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, No. 1.
49. البروتوكول الإضافي لاتفاقية مكافحة الجرائم السيبرانية والمتعلق بتجريم الأفعال ذات طابع العنصرية وكره الأجانب المرتكبة عن طريق أنظمة الحاسوب، سلسلة المعاهدات الأوروبية رقم 189، وهي متاحة على الموقع:https://www.coe.int/en/web/conventions/full-list/-/conventions/webContent/en_GB/7836079اشترك 29 دولة ووقع عليها 13 دولة، وسان مارينو هي آخر تلك الدولة الموقعة في 19 مايو 2017
-https://www.coe.int/en/web/cybercrime/-/signature-san-marino-of-the-protocol-on-xenophobia-and-racism
50. المادة 35
51. انظر التقرير التفسيري لاتفاقية مكافحة الجرائم السيبرانية، رقم 298.
52. Verdelho (2008) The effectiveness of international cooperation against cybercrime
53. The Functioning of 24/7 points of contact for cybercrime, 2009

الاتحاد الأفريقي

تقرر خلال المؤتمر الاستثنائي لوزراء الاتحاد الأفريقي المسؤولين عن تكنولوجيا الاتصالات والمعلومات المنعقد في جوهانسبرغ في عام 2009، أن تقوم مفوضية الاتحاد الأفريقي - بالاشتراك مع اللجنة الاقتصادية لأفريقيا التابعة للأمم المتحدة - بوضع إطار قانوني للبلدان الأفريقية الذي يتناول المعاملات الإلكترونية والأمن السيبراني وحماية البيانات.[54]

قدم الاتحاد الأفريقي مسودة اتفاقية الاتحاد الأفريقي بشأن إنشاء إطار قانوني موثوق للأمن السيبراني في أفريقيا في عام 2011.[55] في يوليو 2014، اعتمد الاتحاد الأفريقي اتفاقية الأمن السيبراني وحماية البيانات الشخصية (AUC). بحلول منتصف عام 2016، كان لدى 12 دولة فقط من أصل 54 دولة أفريقية أحكام قانون موضوعي أو إجرائي أساسية بشأن الجرائم السيبرانية والأدلة الإلكترونية. وكان كثيرون آخرون بصدد صياغة التشريعات، مع اتخاذ اتفاقيتي الاتحاد الأفريقي وبودابست كإرشادات.

يظهر تحليل مقارن لاتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية أنها تجرم بعض السلوكيات المنصوص عليها في اتفاقية بودابست وليس جميعها. وتفتقر معظم الجرائم بموجب اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية إلى توافر ركن القصد الجنائي المناسب، ويمكن أن تجرم السلوك الشرعي لسلطات إنفاذ القوانين وغيرها من السلوكيات التي ينبغي أن تكون قانونية بموجب أفضل الممارسات الدولية.[56] وعلاوةً على ذلك، لا تنص اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية على توفير مجموعة كاملة من الصلاحيات الإجرائية للتحقيق في الجرائم السيبرانية ومقاضاة مرتكبيها وتأمين الأدلة الإلكترونية في التحقيقات المحلية - فعلى سبيل المثال، لم ترد أوامر التقديم، التي تعتبر ضرورية للحصول على بيانات من مزودي خدمة الاتصالات.[57] وعلاوةً على ذلك، لا اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية أساسًا قانونيًا للتعاون الدولي في مجال الجرائم السيبرانية والأدلة الإلكترونية.[58]

جامعة الدول العربية ومجلس التعاون الخليجي

تم اعتماد الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في ديسمبر 2010 ودخلت حيز التنفيذ في فبراير 2014. وصدّق على الاتفاقية حتى الآن، الجزائر والأردن والإمارات العربية المتحدة والسودان والعراق والسلطة الفلسطينية وقطر والكويت ومصر. ويتمثل الالتزام الرئيسي للاتفاقية في تنفيذ التشريعات المحلية للتجريم والسلطات الإجرائية للتحقيق في الجرائم السيبرانية.

كما هو موضح أعلاه، تفتقر اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية - الاتفاقية العربية لمكافحة جرائم تقنية المعلومات إلى ركن القصد الجنائي لبعض الجرائم. فعلى سبيل المثال، لا تشير المواد 6 و 8[59] و 9[60] إلى عبارة «بدون حق».[61] وعلاوةً على ذلك، تجرم المادة 6 «الوصول غير المشروع»، لكنها لا تقدم تعريفًا للوصول غير المشروع. ولا تشمل الاتفاقية العربية لمكافحة جرائم تقنية المعلومات إلى حد كبير جريمة التدخل في النظم،[62] الذي يهدف إلى تجريم الإعاقة المتعمدة للاستخدام القانوني لأنظمة الحاسوب، بما فيها مرافق الاتصالات عن طريق استخدام بيانات الحاسوب أو التأثير عليها.

54. لمزيدٍ من المعلومات، انظر: African Union, Oliver Tambo Declaration, Johannesburg 2009، وهو متاح على: www.uneca.org/aisi/docs/AU/The%20Oliver%20Tambo%20Declaration.pdf
55. مسودة الاتفاقية متاحة للتنزيل على الموقع: www.itu.int/ITUD/projects/ITU_EC_ACP/hipssa/events/2011/WDOcs/CA_5/Draft%20Convention%20on%20Cyberlegislation%20in%20Africa%20Draft0.pdf
56. تحليل مقارن لاتفاقية مالابو للاتحاد الأفريقي واتفاقية بودابست لمكافحة الجرائم السيبرانية، 20 نوفمبر 2016
57. المرجع السابق
58. المرجع السابق
59. الجرائم المرتكبة ضد سلامة البيانات - المماثلة للمادة 4 من اتفاقية بودابست بشأن التشويش على البيانات
60. جرائم إساءة استخدام وسائل تكنولوجيا المعلومات - المماثلة للمادة 6 من اتفاقية بودابست بشأن إساءة استخدام الأجهزة
61. تشير المادة 2 من اتفاقية بودابست إلى الوصول «بدون حق» أو الوصول غير المصرح به - ويعني ذلك أن الجرائم ستكون ذات مسؤولية مقيدة ويمكن أن تعني أن أي شخص أو وكالة مسؤولة عن إنفاذ القوانين أو غيرهم يباشر الوصول إلى البيانات دون موافقة يكون مرتكبًا لجريمة.
62. انظر المادة 5 من اتفاقية بودابست

فيما يتعلق بالتعاون الدولي، تقدم[63] الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المادة 34 على أن تكون الأساس للمساعدة القانونية المتبادلة والمادة 31[64] لتسليم المجرمين إذا لم يكن هناك معاهدة ثنائية سارية. تُعد ازدواجية التجريم شرط أساسي لتوفير أي مساعدة قانونية متبادلة بموجب المادة 32 (5). ويتعارض ذلك مع الأعراف الدولية حيث يكون لازدواجية التجريم تعريف أوسع للمساعدة القانونية المتبادلة[65] وحيث لا يكون ذلك مطلوبًا بموجب اتفاقية بودابست[66] لصلاحيات أقل تدخلية لضمان المحافظة على أدلة الجريمة السيبرانية.

تتضمن الأحكام الدولية الهامة الأخرى الإفصاح عن المعلومات بموجب المادة 33[67] عن طريق إنفاذ القوانين لطرف آخر في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات والتي يمكن استخدامها بشكلٍ استباقي من قبل الدولة المتلقية والحفاظ على سرية أي طلب من طلبات المساعدة القانونية المتبادلة.[68] كما يوجد حكم بموجب المادة 43 بشأن «...هيئة متخصصة مكرسة للعمل على مدار الساعة لضمان تقديم مساعدة فورية لأغراض التحقيق أو الإجراءات المتعلقة بجرائم تكنولوجيا المعلومات أو جمع الأدلة في شكلٍ إلكتروني بشأن جريمة محددة.»[69]

لا تتضمن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات شرطًا مخصصًا لجمع بيانات أو محتوى حركة المرور في الوقت الفعلي عبر المساعدة القانونية المتبادلة.[70] قد يعوق ذلك التحقيقات الدولية في المواقف التي يكون فيها جمع عناوين IP أو المحتوى في الوقت الفعلي ضروريًا للكشف عن موقع المجرمين لمنع الجرائم الإلكترونية. يمكن سد هذه الفجوة بسهولة من خلال اعتماد المادة 34 من اتفاقية بودابست.

مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية (HIPCAR)

أدى تعزيز القدرة التنافسية في منطقة البحر الكاريبي من خلال مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية إلى سن تشريعات نموذجية لمكافحة الجرائم الإلكترونية في 15 دولة كاريبية في مجموعة دول إفريقيا ومنطقة البحر الكاريبي والمحيط الهادئ.[71] ويدير المشروع الاتحاد الدولي للاتصالات ولجنة توجيه عالمية تضم ممثلين عن المفوضية الأوروبية. وصيغت النصوص التشريعية النموذجية بعد إجراء تحليل قانوني للتشريعات الوطنية وأفضل الممارسات الدولية المقدمة من الأمم المتحدة ومنظمة التعاون الاقتصادي والتنمية والاتحاد الأوروبي وأُخذت تشريعات من المملكة المتحدة وأستراليا ومالطا والبرازيل كمعايير مرجعية. ونظرًا لصياغة هذه النصوص التشريعية النموذجية مع مراعاة الاحتياجات المحددة للدول الجزرية الصغيرة، فهي تُعد إطارًا توجيهيًا مفيدًا لتلك الدول التي ليس لديها تشريعات أو لديها تشريعات محدودة لمكافحة الجرائم السيبرانية.

المركز الدولي للأطفال المفقودين والمستغلين (ICMEC)

أخذ التشريع النموذجي للمركز الدولي للأطفال المفقودين والمستغلين (ICMEC) والمراجعة الدولية، الطبعة الثامنة 2016[72]، بعين الاعتبار مجموعة أساسية من المعايير في تقديم تحليل قانوني لتأكيد ما يلي:

1. إذا كان هناك تشريع وطني يولي اهتمامًا خاصًا للمواد الإباحية التي يظهر فيها أطفال؛

63. بما يتوافق مع المادة 23 من اتفاقية بودابست
64. بما يتوافق مع المادة 24 من اتفاقية بودابست
65. انظر المادة 18 (9) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة
66. على سبيل المثال، المادة 29.3 المتعلقة بالحفاظ على بيانات الحاسوب المخزنة
67. بما يتوافق مع المادة 26 من اتفاقية بودابست
68. المادة 34 (7) والمادة 36 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - بما يتفق مع المادة 28 من اتفاقية بودابست
69. ليس واضحًا بالنسبة إلى دول الجنوب الشريكة التي صادقت على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات (الأردن وفلسطين ومصر) ما إذا كانت قد أنشأت هذه الهيئة المتخصصة من عدمه
70. المادتان 33 و 34 من اتفاقية بودابست
71. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/HIPCAR%20Model%20Law%20Cybercrimes.pdf
72. https://www.icmec.org/wp-content/uploads/2016/02/Child-Pornography-Model-Law-8th-Ed-Final-linked.pdf

2. إذا كان التشريع الوطني يقدم تعريفًا للمواد الإباحية التي يظهر فيها أطفال؛
3. إذا كان التشريع الوطني يجرم الجرائم المتصلة بالحاسوب؛
4. إذا كان التشريع الوطني يجرم حيازة المعلومات المرتبطة بالمواد الإباحية التي يظهر فيها أطفال، بغض النظر عن وجود نية للتوزيع من عدمه؛
5. إذا كان التشريع الوطني يشترط إبلاغ مزودي خدمة الاتصالات وكالات إنفاذ القوانين أو غيرها من الوكالات المكلفة بما يتعلق بالمواد الإباحية التي يظهر فيها أطفال.

التحليل القانوني وتحليل الفجوة

يتم تقديم تحليل قانوني في هذا القسم للقوانين الوطنية الحالية وتحليل الفجوات مع توصيات لكل دولة من دول الجنوب الشريكة.[73]

الجزائر

صادقت الجزائر على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات (CITO).

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 2 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست - الوصول غير المشروع[74] يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لتجريم الوصول إلى النظام الكلي أو أي جزء من نظام الحاسوب، إذا ارتكب عمدًا، دون أي حق. قد يشترط طرف ما ارتكاب الجريمة عن طريق انتهاك إجراءات أمنية بقصد الحصول على بيانات الحاسوب أو نية أخرى غير نزيهة، أو فيما يتعلق بنظام كمبيوتر متصل بنظام كمبيوتر آخر. **القسم 4 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الوصول غير القانوني** 1. يعاقب بالسجن لمدة لا تتجاوز [المدة] أو غرامة لا تتجاوز [المبلغ] أو بالعقوبتين معاً أي شخص يدان بجريمة الوصول إلى نظام حاسوب كله أو جزء منه عن قصد ودون عذر مبرر قانونًا أو بتجاوز لسبب قانوني. 2. قد تقرر أي دولة عدم تجريم الوصول غير المصرح به بشرط توفر سبل انتصاف فعالة أخرى. علاوة على ذلك، قد يشترط بلد ما ارتكاب الجريمة عن طريق انتهاك الإجراءات الأمنية أو بقصد الحصول على بيانات الحاسوب أو بنية أخرى غير نزيهة.	**قانون العقوبات – 05-09-2009**[75] **المادة 394 مكرر** كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.	**التحليل القانوني** يتضمن الحكم الوطني إشارة إلى «عن طريق الاحتيال"، وهذا يشير إلى أن الجاني قد وصل إلى البيانات بطريقة غير شريفة؛ في حين تشير اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست إلى «بدون حق" وذلك للدلالة على الوصول غير المصرح به. تشير اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست إلى «نية غير شريفة"، لكن هذا المصطلح يشير إلى ذهنية إجرامية وليس إلى العمل على الوصول بشكل غير شرعي. في الوقت الحالي، يمكن ارتكاب هذه الجريمة على المستوى الوطني فقط في حالة كان لدى مرتكب الجريمة غرضًا غير شريف من الوصول. من غير الواضح إن كان تعريف " احتيالي « يستلزم وجود عمل صريح محدد أو إذا كان أي وصول غير قانوني يعتبر احتياليًا. ولهذا السبب يجب تعريف «الاحتيال". تم تعريف مصطلح «نظام الحاسوب" في المادة 2 من القانون رقم 04-09 الصادر بتاريخ 05-08-2009 والتي تنص على قواعد خاصة تتعلق بمنع ومكافحة المخالفات المرتبطة بتكنولوجيا المعلومات والاتصالات. يشير نص الجريمة أيضًا إلى «نظام معالجة البيانات المؤتمتة" دون وجود تعريف له. ومن غير الواضح ما إذا كان هذا يتعلق كذلك «بنظام الحاسوب" من عدمه تشير اتفاقية الجامعة العربية لمكافحة جرائم تكنولوجيا المعلومات إلى «الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به." دون تحديد ماهية هذه الأفعال، يستحسن لذلك استخدام تعريفات اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست ومواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية.

73. لإلقاء نظرة عامة على التشريعات المتعلقة بالجرائم السيبرانية في الدول الأعضاء وامتثالها لأفضل الممارسات المحددة في اتفاقية مكافحة الجرائم السيبرانية، انظر ملفات التعريف القطرية المقدمة على الموقع الإلكتروني لمجلس أوروبا، وهي متاحة على: www.coe.int/cybercrime/
74. المادة 6 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، والمادة 29 (1) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية
75. https://www.unodc.org/res/cld/document/code-penal-2009_html/Penal_Code_Algeria_2009.pdf

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
القسم 5 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الآثار غير القانونية 1. أي يشخص يظل مسجلاً في نظام حاسوب أو جزء من نظام حاسوب أو يواصل استخدام نظام حاسوب عن قصد ودون عذر أو مبرر قانوني، أو يتجاوز عذرًا أو مبررًا قانونيًا يعاقب عند إدانته بالسجن لمدة لا تتجاوز [المدة]، أو غرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً. 2. قد تقرر أي دولة عدم تجريم الآثار غير المصرح بها فقط، شرط أن تتوفر سبل انتصاف فعالة أخرى. بدلاً من ذلك، قد يشترط البلد ارتكاب الجرم عن طريق انتهاك الإجراءات الأمنية أو بقصد الحصول على بيانات الحاسوب أو بنية أخرى غير نزيهة.		**تحليل الفجوة** **التوصيات:** يمكن أن يدرج التشريع الوطني البرامج ضمن تعريف البيانات لأن بعض البيانات تشمل البرامج والبعض الآخر لا تشملها. علاوةً على ذلك، كي تتماشى التشريعات مع المعايير الدولية، ينبغي أن يشير التشريع إلى الوصول "بدون حق" بدلاً من عن طريق الغش
المادة 3 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[76] **الاعتراض غير القانوني** يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وتدابير أخرى لتجريم اعتراض عمليات نقل البيانات الحاسوبية غير العامة من نظام حاسوب وإليه وداخله، بما في ذلك الانبعاثات الكهرومغناطيسية من نظام الحاسوب الذي يحمل مثل هذه البيانات، وذلك عند ارتكاب هذا العمل عمدًا بوسائط تقنية، ويعتبر جريمة جنائية بموجب القانون الداخلي. قد يشترط الطرف أن تكون الجريمة قد ارتكبت بنية غير نزيهة، أو أن تتم ضد نظام حاسوب متصل بنظام حاسوب آخر. **القسم 6 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الاعتراض غير القانوني** 1. الشخص الذي يتعمد اعتراض الوسائل التقنية دون عذر أو مبرر قانوني أو يتجاوز عذرًا أو مبررًا قانونيًا: • أي نقل غير عام إلى نظام الحاسوب أو منه أو داخله؛ أو	**جرّم القانون رقم 1804 بتاريخ 10 مايو 2018 الذي ينص على قواعد عامة للاتصالات البريدية والإلكترونية، انتهاك سرية الاتصالات التي تُنقَل بوسائل إلكترونية. تنص المادة 164 من هذا القانون على ما يلي: "كل من ينتهك خصوصية الاتصالات التي تُنقَل بالبريد أو وسائل الاتصال الإلكترونية، أو يكشف محتواها أو ينشرها أو يستخدمها دون إذن من المُرسِل أو المُستَقبِل أو يكشف وجودها يعاقب بالسجن من سنة إلى خمس سنوات وبغرامة من 500 ألف إلى مليون دينار.**	**التحليل القانوني** تعتبر هذه الجريمة أساسية لملاحقة عمليات النقل غير العامة لبيانات الحاسوب إلى نظام حاسوبي أو منه أو داخله، والتي قد يتم اعتراضها بشكل غير قانوني للحصول على معلومات حول موقع الشخص (على سبيل المثال استهداف ذلك الشخص).[77] **تحليل الفجوة** **التوصيات:** استخدم لغة اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست في المادة 3، والقسم 6 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية باعتبارهما دليلًا؛ اللغة المستخدمة في المادة 7 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات مناسبة، وإن لم يكن هناك تعريف لـ "بيانات تكنولوجيا المعلومات"

76. المادة 29 (2) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية
77. http://www.coe.int/en/web/cybercrime/guidance-notes

الجرائم		
أفضل الممارسات الدولية	**التشريع الوطني**	**ملاحظات**
• الانبعاثات الكهرومغناطيسية من نظام الحاسوب يعتبر جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً. 2. قد يشترط البلد ارتكاب الجرم بنية غير شريفة، أو ضد نظام حاسوب متصل بنظام حاسوب آخر أو عن طريق التحايل على إجراءات الحماية المطبقة لمنع الوصول إلى محتوى الإرسال غير العام. **المادة 7 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست** **الاعتراض غير المشروع** الاعتراض غير القانوني المتعمد لحركة البيانات بأي وسيلة تقنية، وتعطيل نقل أو استقبال بيانات تكنولوجيا المعلومات.		
المادة 4 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[78] **التشويش على البيانات** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لكي تجرم قوانينها الوطنية محو بيانات الحاسوب أو إتلافها أو تغييرها أو حذفها دون حق، وذلك عند ارتكابها عمدًا. 2. يجوز لأي طرف الاحتفاظ بالحق في المطالبة بأن السلوك الموصوف في الفقرة 1 يؤدي إلى ضرر جسيم. **القسم 7 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية- التشويش غير القانوني على البيانات** الشخص الذي يقوم بأي من الأفعال التالية عمدا ودون عذر أو مبرر قانوني أو يتجاوز عذرًا أو مبررًا قانونيًا: • إلحاق الضرر ببيانات الحاسوب أو إتلافها؛ أو • حذف بيانات الحاسوب؛ أو • تغيير بيانات الحاسوب؛ أو • جعل بيانات الحاسوب بلا معنى أو عديمة الفائدة أو غير فعالة؛ أو • تعويق أو تقطيع أو تشويش الاستخدام القانوني لبيانات الحاسوب؛ أو • تعويق أو تقطيع أو التشويش على أي شخص في استخدامه القانوني لبيانات الحاسوب؛ أو	**قانون العقوبات – 05-09-2009**[79] **المادة 394 ج** أي شخص يقوم بما يلي عن قصد وعن طريق الغش: 1. تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق نظام حاسوبي يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم. 2. حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.	**التحليل القانوني** استخدام، "عن طريق الغش"، غير متسق (في الواقع بالتعارض مع) المادة 4.1 من اتفاقية بودابست "... عندما يرتكب عن قصد، إتلاف أو حذف أو إفساد أو تغيير أو إلغاء بيانات الحاسوب دون حق" (أو القسم 7 من مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية) الذي لا يتطلب إثبات وجود غش. يعني ذلك أن السلوك الذي يشكل جريمة تدخل في البيانات وفقًا للمادة 4.1 من اتفاقية بودابست (أو القسم 7 من مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية) لن يتم تجريمه بموجب المادة 394ج. لا تتضمن المادة 394ج عنصر محو بيانات الحاسوب **تحليل الفجوة** **التوصيات:** استخدم المادة 4 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست أو القسم 7 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية باعتبارهما دليلًا للتشريعات الوطنية

78. المادة 29 (1) (هـ - و) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية
79. https://www.unodc.org/res/cld/document/code-penal-2009_html/Penal_Code_Algeria_2009.pdf

الجرائم		
أفضل الممارسات الدولية	**التشريع الوطني**	**ملاحظات**
• منع الوصول إلى بيانات الحاسوب لأي شخص مصرح له بالوصول إليها؛ يعتبر جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً. **المادة 8 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست** **جريمة ضد سلامة البيانات** 1. تعمد محو أو حذف أو منع أو تعديل أو إخفاء بيانات تكنولوجيا المعلومات بشكل غير قانوني. 2. قد يطلب أحد الأطراف أن يتسبب الفعل بأضرار جسيمة من أجل تجريم الأفعال المذكورة في الفقرة 1.		
المادة 5 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[80] **التشويش على النظام** يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لكي تُجرّم في قانونها الداخلي أعمال الإعاقة الخطيرة التي ترتكب عمدًا ودون وجه حق من أجل إعاقة عمل نظام حاسوب من خلال إدخال بيانات حاسوب أو نقلها أو محوها أو حذفها أو إتلافها أو تغييرها أو منعها. **القسم 9 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - التشويش غير القانوني على النظام** 1. الشخص الذي يقوم عن قصد، ودون عذر أو مبرر قانوني، أو بتجاوز عذر أو مبرر قانوني: • إعاقة عمل نظام الحاسوب أو التشويش عليه؛ أو • إعاقة شخص يستخدم أو يشغل بشكل قانوني نظام الحاسوب أو التشويش عليه؛ يعتبر جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً.	**لا يوجد معادل**	**التحليل القانوني** تجريم هذه الأعمال من شأنه أن يمنع البرامج الضارة التي تتداخل مع عمل جهاز الحاسوب - على سبيل المثال ديدان الحاسوب - مجموعة فرعية من البرامج الضارة (مثل فيروسات الحاسوب). إنها برامج حاسوب ذاتية النسخ المتماثل تضر بالشبكة من خلال بدء عمليات نقل البيانات المتعددة. يمكن أن تؤثر على أنظمة الحاسوب عن طريق إعاقة التشغيل السلس لنظام الحاسوب، أو استخدام موارد النظام لتكرار نفسها عبر الإنترنت أو توليد حركة مرور في الشبكة يمكن أن تغلق بعض الخدمات (مثل المواقع الإلكترونية). **تحليل الفجوة** **التوصيات:** استخدم لغة اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست في المادة 5 أو القسم 9 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية باعتبارهما دليلًا للتشريعات الوطنية. ضع في اعتبارك أيضًا ما إذا كان منع ومكافحة الهجمات ضد البنية التحتية الحيوية يحتاج إلى جريمة منفصلة أو مشددة (القسم 9 (2) من بروتوكول مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية)، على سبيل المثال، قد يتم إعاقة عمل نظام الحاسوب لأغراض إرهابية (يمكن أن تؤدي إعاقة النظام الذي يخزن سجلات البورصة إلى أن تكون البيانات غير دقيقة، أو أن تعيق عمل البنية التحتية الحيوية).[81]

80. لا يوجد ما يعادل المادة 29 (1) (د) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات
81. http://www.coe.int/en/web/cybercrime/guidance-notes

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
2. يعاقب أي شخص الذي يتعمد دون عذر أو مبرر قانوني، أو بتجاوز عذر قانوني أو مبرر، إعاقة نظام حاسوب مخصص حصريًا لاستخدام عمليات البنية التحتية الحيوية أو التشويش عليه، أو في الحالات التي لا يكون فيها هذا النظام مخصصًا للاستخدام الحصري في عمليات البنية التحتية الحيوية، ولكنه يستخدم في عمليات البنية التحتية الحيوية وتؤثر هذه الإعاقة على استخدام عمليات البنية التحتية الحيوية، بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً.		
المادة 6 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[82] **سوء استخدام الأجهزة** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لتجريم الأفعال الإجرامية بموجب قوانينه الداخلي، عندما تُرتكب عمداً ودون حق: a. إنتاج أو بيع أو الشراء بغرض الاستخدام أو الاستيراد أو التوزيع أو توفير ما يلي بأية طريقة: – أي جهاز، بما في ذلك برنامج الحاسوب، تم تصميمه أو تكييفه بشكل أساسي بغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من 2 إلى 5؛ – كلمة مرور الحاسوب أو رمز الوصول أو البيانات المماثلة التي يمكن من خلالها الوصول إلى نظام الحاسوب كله أو جزء منه، بقصد استخدامه لغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من 2 إلى 5؛ و b. حيازة عنصر مشار إليه في الفقرتين أ.1 أو 2 أعلاه، بقصد استخدامه لغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من 2 إلى 5. يجوز لأي طرف أن يشترط بموجب القانون امتلاك عدد من هذه العناصر قبل إسناد المسؤولية الجنائية.	**لا يوجد معادل**	**التحليل القانوني** كما ذكر أعلاه للوصول غير المشروع، لا توجد إشارة إلى "بدون حق" ستمكّن تجريم هذه الأفعال من ملاحقة إنتاج وبيع والشراء من أجل الاستخدام واستيراد وتوزيع رموز الوصول والبيانات المحوسبة الأخرى المستخدمة في ارتكاب جرائم الإنترنت. - على سبيل المثال، يمكن الوصول إلى أنظمة الحاسوب لتسهيل أي هجوم إرهابي بالتدخل في شبكة الطاقة الكهربائية للبلد. يجب أن تأخذ أي جريمة في الاعتبار تلك الأجهزة التي لها استخدام شرعي وكذلك للاستخدام الجنائي ("الاستخدام المزدوج")– ينبغي أن يشمل ذلك اللغة المستخدمة في اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست "المكيف بشكل أساسي" **تحليل الفجوة** التوصيات: استخدم لغة اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست في المادة 6 أو القسم 10 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية باعتبارهما دليلًا للتشريعات الوطنية. يرجى ملاحظة أن مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية توفر خيار إدراج الأجهزة في جدول إذا كان ذلك مناسبًا - قد يكون هذا تقييدًا ويتطلب تحديثًا يتوافق مع التقدم التكنولوجي. يجب أن يوفر القانون الوطني عذرًا معقولًا حتى تتمكن أجهزة إنفاذ القانون من استخدام الأجهزة لتقنيات التحقيق الخاصة - راجع اللغة في المادة 6.2. اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست أو القسم 10 (2) من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية باعتبارهما دليلًا.	

82. المادة 9 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات والمادة 29 (1) (ح) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
2. لا يجوز تفسير هذه المادة على أنها تفرض مسؤولية جنائية عندما لا يكون الغرض من الإنتاج أو البيع أو الشراء بغرض الاستخدام أو الاستيراد أو التوزيع أو التوفير أو حيازة المشار إليه في الفقرة 1 من هذه المادة ارتكاب جريمة منصوص عليها وفقًا للشروط المواد من 2 إلى 5 من هذه الاتفاقية، مثل الاختبارات المسموح بها أو حماية نظام الحاسوب. 3. يجوز لكل طرف أن يحتفظ بالحق في عدم تطبيق الفقرة 1 من هذه المادة، شريطة أن لا يتعلق التحفظ ببيع أو توزيع أو توفير المواد المشار إليها في الفقرة 1 أ من هذه المادة بطريقة أخرى **القسم 10 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الأجهزة غير القانونية** 1. يرتكب الشخص جريمة إذا: a. أنتج أو باع أو اشترى بغرض الاستخدام أو استورد أو صدّر أو وزع أو وفّر بأي طريقة، عن قصد ودون عذر أو مبرر قانوني أو بتجاوز عذر أو مبرر قانوني: – جهاز بما في ذلك برنامج حاسوب، تم تصميمه أو تكييفه بغرض ارتكاب جريمة محددة بموجب أحكام أخرى من الجزء الثاني من هذا القانون؛ أو – كلمة مرور الحاسوب أو رمز الوصول أو البيانات المماثلة التي يمكن من خلالها الوصول إلى نظام الحاسوب كله أو جزء منه؛ – بقصد استخدامه من قبل أي شخص لغرض ارتكاب جريمة محددة بموجب أحكام أخرى من الجزء الثاني من هذا القانون؛ أو b. كان في حوزته غرض مشار إليه في الفقرة الفرعية "1" أو "2"، وكان القصد هو استخدامه من قبل أي شخص لارتكاب جريمة محددة بموجب أحكام أخرى من الجزء الثاني من هذا القانون، فإنه يعاقب عند إدانته بارتكاب هذه الجريمة بالسجن لمدة لا تزيد عن [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً.		

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
2. لا يجوز تفسير هذا الحكم على أنه يفرض مسؤولية جنائية عندما لا يكون الغرض من الإنتاج أو البيع أو الشراء للاستخدام أو الاستيراد أو التوزيع أو التوفير أو الحيازة المشار إليها في الفقرة 1 هو ارتكاب جريمة منصوص عليها وفقًا لأحكام أخرى من الجزء الثاني من هذا القانون، كأن تكون الأغراض مثل الاختبار أو الحماية المعتمدين لنظام الحاسوب. 3. قد يقرر بلد ما عدم تجريم الأجهزة غير القانونية أو قصر التجريم على الأجهزة المدرجة في الجدول.		
المادة 7 من مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست **أعمال التزوير المرتبطة بالحاسوب** يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم إدخال بيانات الحاسوب أو تغييرها أو حذفها أو محوها، عند ارتكاب ذلك عن قصد وبدون حق، مما يؤدي إلى بيانات غير موثوقة بهدف أن يتم التعامل معها أو التصرف فيها لأغراض قانونية كما لو كانت أصلية، بصرف النظر عما إذا كانت البيانات قابلة للقراءة ومقروءة مباشرة أم لا. قد يطلب طرف ما وجود نية الاحتيال، أو نية غير شريفة مماثلة، قبل إسناد المسؤولية الجنائية. **القسم 11 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - أعمال التزوير المتعلقة بالحاسوب** 1. كل شخص يقوم عن قصد ودون عذر أو مبرر قانوني أو بتجاوز عذر قانوني أو مبرر، بإدخال أو تبديل أو حذف أو منع بيانات الحاسوب، مما ينتج عنه بيانات غير موثوقة بقصد التعامل معها أو التصرف فيها لأغراض قانونية كما لو كانت صحيحة، بصرف النظر عما إذا كانت البيانات قابلة للقراءة مباشرة أم لا، يعاقب عند الإدانة بهذه الأعمال بالسجن لمدة لا تزيد عن [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً. 2. تكون العقوبة إذا ارتكبت الجريمة المذكورة أعلاه عن طريق إرسال رسائل بريد إلكتروني متعددة من أنظمة الحاسوب أو من خلالها هي السجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً.	**لا يوجد معادل**	**التحليل القانوني** ينصح بدمج المادة 7 من اتفاقية بازل، المادة 11 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية أو القسم 29 (2)(ب) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية، من أجل الحماية من المخالفات التي قد تشمل التصيد الاحتيالي والتصيد الاحتيالي بالرمح على سبيل المثال، قد يتم إدخال بيانات الحاسوب(مثل البيانات المستخدمة في جوازات السفر الإلكترونية) أو تغييرها أو حذفها أو إلغاؤها، مما يؤدي إلى تصديق البيانات غير الموثوقة أو التعامل معها لأغراض قانونية كما لو كانت صحيحة.[83] ينص القسم 11 (2) من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية أيضًا على إرسال رسائل بريد إلكتروني متعددة باعتبارها جريمة مشددة. لا تشير اللغة في المادة 10 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات إلى أي نية غير شريفة وتشترط التسبب في ضرر - اللغة المستخدمة في اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست و مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية هي الأفضل لأنها لا تشترط حدوث ضرر. تشترط اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست ومواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية فقط أن "البيانات الزائفة" "تعتبر" حقيقية **تحليل الفجوة** **التوصيات:** استخدم لغة اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست في المادة 7، القسم 11 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية أو المادة 29 (2) (ب) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية دليلًا للتشريعات الوطنية	

83. http://www.coe.int/en/web/cybercrime/guidance-notes

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 10 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست **جريمة التزوير** يعني استخدام تقنية المعلومات تغيير حقيقة البيانات بطريقة تسبب الضرر بغرض استخدامها كبيانات حقيقية. **المادة 29 (2)(ب) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية** تعمد إدخال بيانات الحاسوب أو تغييرها أو حذفها أو منعها، مما يؤدي إلى بيانات غير موثوقة بقصد التعامل معها أو التصرف فيها لأغراض قانونية كما لو كانت أصلية، بصرف النظر عما إذا كانت البيانات قابلة للقراءة أو واضحة بشكل مباشر أم لا. يجوز للطرف أن يشترط النية للاحتيال، أو نية غير شريفة مماثلة، قبل إسناد المسؤولية الجنائية		
المادة 8 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[84] **الاحتيال المرتبط بالحاسوب** يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وتدابير أخرى لتجريم الأفعال التالية بموجب قوانينه الداخلية، عند ارتكابها عمداً ودون حق، بما يسبب فقدان الممتلكات لشخص آخر عن طريق: أي إدخال أو تغيير أو حذف أو إلغاءلبيانات الحاسوب، أي تدخل في عمل نظام الحاسوب، مع نية احتيال أو نية غير شريفة من أجل الحصول، دون حق، على منفعة اقتصادية لنفسه أو لشخص آخر. **القسم 12 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الاحتيال المرتبط بالحاسوب** الشخص الذي يتسبب في فقدان الممتلكات لشخص آخر، عن قصد، ودون عذر أو مبرر قانوني أو بتجاوز عذر أو مبرر قانوني، وذلك عن طريق: • أي إدخال أو تغيير أو حذف أو إلغاء لبيانات الحاسوب؛ • أي تدخل في عمل نظام الحاسوب، بقصد احتيالي أو غير شريف للحصول، دون حق، على منفعة اقتصادية لنفسه أو لشخص آخر، وتكون عقوبة هذه الأعمال السجن لمدة لا تتجاوز [المدة]، أو غرامة لا تتجاوز [المبلغ]، أو العقوبتين معاً.	**قانون العقوبات - 05-09-2009** **المادة 394** كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها.	**التحليل القانوني** في حين أن عبارة "عن طريق الغش" الواردة في المادة 394 من التشريع الوطني تمنح درجة معينة من الحماية، حيث قد يؤدي عدم ارتكاب هذا السلوك دون إذن إلى عدم اليقين. تم تعريف مصطلح "معطيات الحاسوب" في المادة 2 من القانون رقم 04-09 الصادر بتاريخ 05-08-2009 والتي تنص على قواعد خاصة تتعلق بمنع ومكافحة المخالفات المرتبطة بتكنولوجيا المعلومات والاتصالات لا يوجد تعريف "لنظام المعالجة الآلية" وقد يخلق هذا حالة من عدم اليقين. اللغة في المادة 11 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات و المادة 29 (2) (د) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية غامضة مع عدم وجود إشارة إلى أي نية غير شريفة وتتطلب وقوع شكل من أشكال "الضرر" (الاتفاقية العربية لمكافحة جرائم تقنية المعلومات) أو حصول "منفعة" (اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية) دون تحديد ماهيته **تحليل الفجوة** **التوصيات:** توفير تعريف "لنظام المعالجة الآلية" وبما في ذلك "بدون ترخيص" - الصياغة في اتفاقية بودابست أو مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية لهذه المخالفة دليل جيد للتشريع الوطني

84. المادة 11 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات والمادة 29 (2) (د) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 9 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[85] **الجرائم ذات الصلة بالمحتوى (مثل المواد الإباحية التي يظهر فيها أطفال)** **القسم 13 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية- المواد الإباحية للأطفال**	**قانون العقوبات - 2009-09-05** **المادة 333 مكرر 1** تفرض عقوبة جنائية على كل من صور قاصرًا لم يكمل الثامنة عشرة (18) سنة بأي وسيلة كانت وهو يمارس أنشطة جنسية بصفة مبينة، حقيقية أو غير حقيقية، أو صور الأعضاء الجنسية للقاصر لأغراض جنسية أساسًا، أو قام بإنتاج أو توزيع أو نشر أو ترويج أو استيراد أو تصدير أو عرض أو بيع أو حيازة مواد إباحية متعلقة بالقصر.	**التحليل القانوني** تجريم هذه الأعمال يعتبر أساسيًا من أجل حماية الأطفال من الأذى، وذلك من خلال تجريم توزيع الصور غير اللائقة للأطفال ونقلها وتوفيرها وعرضها وحيازتها. **تحليل الفجوة** **التوصيات:** تؤكد مراجعة المركز الدولي للأطفال المفقودين والمستغلين العالمية أن التشريعات الوطنية تفي بمعاييرها الأساسية [86]
المادة 10 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[87] **انتهاك حقوق النشر** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وغيرها من التدابير لاعتبار انتهاك حقوق الطبع والنشر، جرائم جنائية بموجب قوانينه الداخلية، وفقًا للالتزامات التي تعهد بها بموجب قانون باريس الصادر في 24 يوليو 1971، مراجعة اتفاقية برن لحماية المصنفات الأدبية والفنية، والاتفاق المتعلق بجوانب حقوق الملكية الفكرية المتصلة بالتجارة ومعاهدة المنظمة العالمية للملكية الفكرية بشأن حق المؤلف، باستثناء أي حقوق معنوية ممنوحة بموجب هذه الاتفاقيات، عندما تُرتكب هذه الانتهاكات عمدا وعلى نطاق تجاري وعن طريق نظام الحاسوب. 2. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لاعتبار أي انتهاك للحقوق أدناه جرائم جنائية بموجب قوانينه الداخلية، وذلك عملاً بالالتزامات التي تعهد بها بموجب الاتفاقية الدولية لحماية فناني الأداء ومنتجي التسجيلات الصوتية وهيئات الإذاعة (اتفاقية روما) واتفاق جوانب حقوق الملكية الفكرية المتصلة بالتجارة ومعاهدة المنظمة العالمية للملكية الفكرية بشأن الأداء والتسجيل الصوتي، باستثناء أي حقوق معنوية ممنوحة بموجب هذه الاتفاقيات، حيثما ارتكبت هذه الانتهاكات عمدا وعلى نطاق تجاري وعن طريق نظام الحاسوب.	**الأمر رقم 03-05 الصادر بتاريخ 19-07-2003 المتعلق بحق المؤلف والحقوق المجاورة والأمر رقم 03-07 الصادر بتاريخ 19-07-2003 المتعلق ببراءات الاختراع.**	**التحليل القانوني** تستخدم هيئات تطبيق القانون على الصعيد الدولي جرائم حقوق النشر الرقمية باعتبارها سلوكًا إجراميًا إضافيًا للتحقيق في العديد من أشكال جرائم الإنترنت ومحاكمة مرتكبيها (بما في ذلك جرائم مثل التصيّد الاحتيالي والاحتيال الإلكتروني والتزوير الإلكتروني ومواقع الويب الاحتيالية وانتهاكات البيانات وسرقتها). تميل إحدى هذه الجرائم الأساسية في العديد من الحالات إلى أن تكون انتهاكًا لحقوق النشر الرقمية. هجوم Sony الإلكتروني[88] ليس إلا مثالًا حديث العهد تضافرت فيه المنظمات الإجرامية والقوى المرتبطة بجرائم الإنترنت وسرقة البيانات/التجسس على الشركات وانتهاك حقوق الطبع والنشر لتكمل عمل بعضها البعض. إن عدم وجود أي أحكام تتعلق بالملكية الفكرية يشكل إخفاقًا في حماية الابتكار في القرن الحادي والعشرين لدول الجنوب الشريكة والشركات والمواطنين. توجد حماية قانونية للأعمال الرقمية وقواعد البيانات وبرامج الحاسوب في الأمر رقم 03-05 الصادر بتاريخ 19-07-2003 المتعلق بحق المؤلف والحقوق المجاورة والأمر رقم 03-07 الصادر بتاريخ 19-07-2003 المتعلق ببراءات الاختراع.

85. المادة 12 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات والمادة 29 (3) (أ-ج) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية
86. تقرير ICMEC العالمي، صفحة 18
87. لا يوجد ما يعادلها في اتفاقية الاتحاد الأفريقي ومواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية
88. https://en.wikipedia.org/wiki/Sony_Pictures_hack

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
3. يجوز لأي طرف أن يحتفظ بالحق في عدم فرض مسؤولية جنائية بموجب الفقرتين 1 و 2 من هذه المادة في ظروف محدودة، شريطة توفر سبل انتصاف فعالة أخرى، وأن لا ينتقص هذا التحفظ من التزامات الطرف الدولية المنصوص عليها في المواثيق الدولية المشار إليها في الفقرتين 1 و 2 من هذه المادة. **المادة 17 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - الجرائم المتعلقة بحق المؤلف والحقوق المرتبطة بها** انتهاك حقوق النشر كما هو محدد وفقًا لقانون الدولة الطرف، إذا كان الفعل قد ارتكب عمداً وليس لغرض الاستخدام الشخصي، وانتهاك الحقوق المرتبطة بحقوق الطبع والنشر ذات الصلة على النحو المحدد وفقًا لقانون الدولة الطرف، إذا كان الفعل ارتكب عمدا وليس لهدف الاستخدام الشخصي.		
المادة 11 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[89] **المساعدة والتحريض** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لتجريم الأفعال التالية بموجب قانونه الداخلي، وذلك عندما يتم التحريض على ارتكاب أي من الجرائم المقررة وفقا للمواد من 2 إلى 10 من هذه الاتفاقية أو المساعدة عليها عمدًا، مع نية أن ترتكب هذه الجريمة. 2. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وتدابير أخرى لتجريم محاولة ارتكاب أي من الأفعال الإجرامية المنصوص عليها في المواد من 3 إلى 5 و7 و8 و9.1. أ و ج من هذه الاتفاقية عمدًا. **المادة 19 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - محاولة ارتكاب الجرائم والاشتراك فيها** 1. الاشتراك في ارتكاب أية جريمة من الجرائم المنصوص عليها في هذا الفصل مع وجود نية ارتكاب الجريمة في قانون الدولة الطرف. 2. الشروع في ارتكاب الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية. 3. يجوز لأي دولة طرف الاحتفاظ بحقها في عدم تطبيق الفقرة الثانية من هذه المادة كليا أو جزئيا.	**القانون الجنائي** المادة 394	**التحليل القانوني** تعتبر مساعدة الآخرين وتحريضهم على ارتكاب جرائم أمرًا ضروريًا لمحاكمة أولئك الذين يكونون قد قدموا المساعدة أو شجعوا على ارتكاب جرائم الإنترنت. تعاقب المادة 394 من القانون الجنائي المشاركة والتواطؤ في ارتكاب جرائم ضد أنظمة معالجة المعطيات المحوسبة.

89. المادة 29 (2) (و) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 12 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[90] **مسؤولية الشركات** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وتدابير أخرى لضمان أن الأشخاص الاعتباريين يمكن اعتبارهم مسؤولين عن أي جريمة جنائية منشأة وفقًا لهذه الاتفاقية، إذا ارتكبها أي شخص طبيعي لصالحهم، سواء كان ذلك بصفته الفردية أو باعتباره جزءًا من جهاز الشخص الاعتباري، أو باعتباره شخصًا قياديًا ضمن تنظيم الشخص الاعتباري، بناءً على: a. سلطة تمثيل الشخص الاعتباري؛ b. سلطة اتخاذ القرارات نيابة عن الشخص الاعتباري؛ c. سلطة ممارسة السيطرة داخل الشخص الاعتباري. 2. بالإضافة إلى الحالات المنصوص عليها بالفعل في الفقرة 1 من هذه المادة، يتخذ كل طرف الإجراءات اللازمة لضمان أن يتحمل الشخص الاعتباري المسؤولية عندما يكون عدم الإشراف أو السيطرة من قبل أي شخص طبيعي مشار إليه في الفقرة 1 قد جعل من الممكن ارتكاب جريمة جنائية منصوص عليها بموجب هذه الاتفاقية لصالح ذلك الشخص الاعتباري من قبل شخص طبيعي يعمل تحت سلطته. 3. مع مراعاة المبادئ القانونية للطرف، قد تكون مسؤولية الشخص الاعتباري جنائية أو مدنية أو إدارية. 4. تكون هذه المسؤولية دون المساس بالمسؤولية الجنائية للأشخاص الطبيعيين الذين ارتكبوا الجريمة.	**القانون الجنائي** المادة 394	**التحليل القانوني** يُعد هذا الحكم عنصرًا أساسيًا بحيث يستطيع الأشخاص الاعتباريون (مثل الكيانات التجارية) التصرف نيابةً عن الأشخاص الطبيعيين الذين تقع عليهم مسؤولية جنائية. كما أن مسؤولية الشخص الاعتباري في ارتكاب جرائم ضد أنظمة معالجة المعطيات المحوسبة منصوص عليها في المادة 394 من القانون الجنائي.

90. المادة 20 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، والمادة 30 (2) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
البروتوكول الإضافي لاتفاقية الجريمة السيبرانية، المتعلق بتجريم أعمال العنصرية وكراهية الأجانب المرتكبة من خلال أنظمة الحاسوب **المادة 3[91] 1. نشر المواد التي تحض على العنصرية وكراهية الأجانب من خلال أنظمة الحاسوب** 1. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم السلوك التالي في قوانينه المحلية، عندما يرتكب عمدا وبدون حق: توزيع المواد العنصرية وكراهية الأجانب أو إتاحتها للجمهور من خلال نظام الحاسوب. 2. أ. يجوز للطرف أن يحتفظ بحقه في عدم إسناد المسؤولية الجنائية بالتصرف على النحو المحدد في الفقرة 1 من هذه المادة، عندما تحض المواد الموزعة، كما هو محدد في الفقرة 1 من المادة 2، وتشجع على التمييز غير المرتبط بالكراهية أو العنف، شريطة أن تتوفر سبل انتصاف فعالة أخرى. 3. بصرف النظر عن الفقرة 2 من هذه المادة، يجوز للطرف أن يحتفظ بالحق في عدم تطبيق الفقرة 1 على حالات التمييز، لأن هذه الفقرة لا يمكن أن تمثل سبل انتصاف فعالة على النحو المشار إليه الفقرة 2، وذلك بسبب مبادئ ثابتة في نظامه القانوني الوطني متعلقة بحرية التعبير.	**لا يوجد معادل**	**التحليل القانوني** لا تتضمن المادة 3 (1) (هـ) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية، التي تتضمن إنشاء وتنزيل مواد متعلقة بدافع العنصرية وكراهية الأجانب من نظام حاسوبي بدلاً من مجرد نشر أو إتاحة مثل هذه المواد، القصد أو عبارة "بدون حق" - وتُفضل صياغة اتفاقية بودابست. **تحليل الفجوة** **التوصيات:** استخدم لغة اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست في المادة 3 من البروتوكول الإضافي كدليل للتشريعات الوطنية
بروتوكول إضافي **المادة 4[92] - التهديد بدافع العنصرية وكراهية الأجانب** يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم السلوك التالي في قوانينه المحلية، عندما يرتكب عمدا وبدون حق: التهديد، من خلال نظام الحاسوب، بارتكاب جريمة جنائية خطيرة على النحو المحدد في قانونها الداخلي، (1) ضد أشخاص لسبب أنهم ينتمون إلى جماعة يميزها عرقها أو لونها أو نسبها أو أصلها القومي أو العرقي أو دينها، إذا تم استخدام أي من هذه العوامل ذريعةً، أو (2) ضد مجموعة من الأشخاص تتميز بأي من هذه الخصائص.	**لا يوجد معادل**	**تحليل الفجوة** **التوصيات:** استخدم لغة اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست في المادة 4 من البروتوكول الإضافي كدليل للتشريعات الوطنية

91. المادة 29 (3) (هـ) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية لا يوجد ما يعادلها في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات
92. المادة 29 (3) (و) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية لا يوجد ما يعادلها في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
بروتوكول إضافي **المادة 5[93] - الإهانة بدافع العنصرية وكراهية الأجانب** يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم السلوك التالي في قوانينه المحلية، عندما يرتكب عمدا وبدون حق: 1. إهانة الجمهور، من خلال نظام حاسوبي، (1) الأشخاص لكونهم ينتمون إلى مجموعة يميزها عرقها أو لونها أو نسبها أو أصلها القومي أو العرقي أو دينها، إذا تم استخدام أي من هذه العوامل ذريعةً؛ أو (2) مجموعة من الأشخاص تتميز بأي من هذه الخصائص. 2. أ. يجوز للطرف إما: a. أن يشترط أن يكون للجريمة المشار إليها في الفقرة 1 من هذه المادة أثر على الشخص أو مجموعة الأشخاص المشار إليهم في الفقرة 1 والذين يتعرضون للكراهية أو الاحتقار أو السخرية؛ أو b. أن يحتفظ بالحق في عدم تطبيق الفقرة 1 من هذه المادة بشكل كلي أو جزئي.	**لا يوجد معادل**	**تحليل الفجوة** **التوصيات:** استخدم لغة اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست في المادة 5 من البروتوكول الإضافي كدليل للتشريعات الوطنية
بروتوكول إضافي **المادة 6[94] - الإنكار أو التقليل إلى الحد الأدنى أو الموافقة أو التبرير للإبادة الجماعية أو الجرائم ضد الإنسانية** يعتمد كل طرف ما قد يلزم من إجراءات تشريعية لجعل الأفعال التالية يعتبر جرائم جنائية بموجب قوانينها الداخلية، عندما تُرتكب عمداً وبدون حق: 1. توزيع أو توفير عبر نظام الحاسوب بأية طريقة من الطرق للجمهور، مواد تنكر أو تقلل أو تقر أو تقلل بشكل كبير الأفعال التي تشكل إبادة جماعية أو جرائم ضد الإنسانية، على النحو المحدد في القانون الدولي والمعترف بها على هذا النحو في القرارات النهائية والملزمة للمحكمة العسكرية الدولية، المنشأة بموجب اتفاقية لندن المؤرخة في 8 أغسطس 1945، أو أي محكمة دولية أخرى تنشأ بموجب المواثيق الدولية ذات الصلة والتي يعترف هذا الطرف باختصاصها القضائي.	**لا يوجد معادل**	**تحليل الفجوة** **التوصيات:** استخدم لغة اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست في المادة 6 من البروتوكول الإضافي كدليل للتشريعات الوطنية

93. المادة 29 (3) (ز) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية لا يوجد ما يعادلها في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات
94. المادة 29 (3) (ح) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية لا يوجد ما يعادلها في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
2. يجوز للحزب إما a. أن يشترط أن يكون الإنكار أو التقليل إلى الحد الأدنى المشار إليه في الفقرة 1 من هذه المادة قد ارتكب بهدف التحريض على الكراهية أو التمييز أو العنف ضد أي فرد أو مجموعة من الأفراد على أساس العرق أو اللون أو النسب أو الأصل القومي أو العرقي أو الدين أو إذا استخدمت هذه العوامل ذريعة لذلك، أو b. أن يحتفظ بالحق في عدم تطبيق الفقرة 1 من هذه المادة بشكل كلي أو جزئي.		
جرائم إضافية للمراجعة		
الجرائم المتعلقة بالهوية **القسم 14 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية** يعاقب الشخص الذي يقوم عن قصد ودون عذر أو مبرر قانوني، أو يتجاوز عذرًا قانونيًا أو مبررًا باستخدام نظام حاسوب في أي مرحلة من مراحل الجريمة بنقل أو تملك أو استخدام وسيلة لتحديد الهوية شخص آخر بنية ارتكاب أي نشاط غير قانوني يشكل جريمة أو المساعدة أو التحريض عليها، عند إدانته بهذه الأعمال بالسجن لمدة لا تتجاوز [المدة] أو بغرامة لا يتجاوز [المبلغ]، أو بالعقوبتين معاً.		**التحليل القانوني** تغطي هذه الجريمة مرحلة التحضير لجريمة خيانة الأمانة المتعلقة بالهوية **تحليل الفجوة** **التوصيات:** يستحسن أن تدرج في التشريعات المحلية.
الكشف عن تفاصيل التحقيق **القسم 16 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية** موفر خدمة الإنترنت الذي يتلقى أمرًا يتعلق بتحقيق جنائي ينص صراحةً على الحفاظ على السرية أو على التزام شبيه ينص عليه القانون، ثم يقوم عن عمد ودون عذر أو مبرر قانوني أو بتجاوز لعذر قانوني مبرر، بالإفصاح عن: • حقيقة أنه قد تم إصدار أمر؛ أو • أي شيء تم تنفيذه بموجب الأمر؛ أو • أي بيانات تم جمعها أو تسجيلها بموجب الطلب؛ يعتبر جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً.	**القانون رقم 04-09 بتاريخ 14 شعبان 1430 الموافق 5 أغسطس 2009 الذي يضع قواعد محددة بشأن منع ومكافحة الانتهاكات المتعلقة بتكنولوجيا المعلومات والاتصالات** **المادة 10**	**التحليل القانوني** تنص المادة 10 من القانون 04-09 على إمكانية مقاضاة مزودي خدمة الاتصالات (كأشخاص اعتباريين) أو الأشخاص العاديين الذين يقوضون سرية العمليات إذا طلبت السلطات القضائية أو سلطات إنفاذ القوانين ذلك، لخرق سرية التحقيق.

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
عدم السماح بالمساعدة **القسم 17 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية** 1. أي شخص آخر غير المشتبه فيه فشل عمداً دون عذر أو مبرر قانوني أو بتجاوز عذر أو مبرر قانوني، بمساعدة شخص أو السماح بمساعدته، بناءً على أمر مثلما تحدد المواد 20 إلى 22[95] يرتكب جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً. 2. قد يقرر أي بلد عدم تجريم عدم السماح بالمساعدة شرط أن تتوفر سبل انتصاف فعالة أخرى.		**التحليل القانوني** تتعلق هذه الجريمة بالأشخاص الذين لديهم معرفة محددة بالأدلة ذات الصلة والذين يرفضون تقديم المساعدة. غالبًا ما يعتمد تطبيق القانون على هؤلاء الأشخاص لتأمين الأدلة في التحقيقات الإلكترونية. هنالك مخالفة مستقلة وهي عدم توفير كلمات مرور أو الوصول إلى الرموز للأجهزة المشفرة أو البيانات (مثل "مفتاح المعلومات المحمية") - ينص القسم 53 من قانون تنظيم سلطات التحقيق في المملكة المتحدة لعام 2000 (RIPA)) [96] على وجود جرم جنائي يتحمله الأشخاص الذين لا يمتثلون للمادة 49 من إخطار قانون تنظيم سلطات التحقيق والقاضية بالكشف عن "المفتاح" **تحليل الفجوة** **التوصيات:** يستحسن أن تدرج في التشريعات المحلية.
المطاردة السيبرانية **القسم 18 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية** الشخص الذي يقوم، دون عذر أو مبرر قانوني، أو يتجاوز عذرًا قانونيًا أو مبررًا، ببدء أي اتصال إلكتروني، بقصد إكراه شخص ما أو تخويفه أو مضايقته أو التسبب في ضائقة عاطفية كبيرة له، باستخدام نظام حاسوب لدعم السلوك المتكرر والعدائي والعنيف، يرتكب جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً.		**التحليل القانوني** هذه الجريمة تُجرم من يضايقون الأشخاص عبر الإنترنت - قد تنص بعض الولايات القضائية على جرائم تحرش غير مرتبطة بالحاسوب - لكن يوصى باعتماد هذه الجريمة لمتابعة لتلك الجرائم المرتكبة عبر الإنترنت. **تحليل الفجوة** **التوصيات:** يستحسن أن تدرج في التشريعات المحلية.
رعاية الأطفال على الإنترنت **القانون الجنائي الهولندي 248e** يعاقب الشخص الذي يقترح ترتيب لقاء، بوسائل عمل آلية أو باستخدام خدمة اتصال، مع شخص يعرف، أو ينبغي منطقيًا أن يعرف، أن هذا الشخص لم يصل بعد إلى سن السادسة عشرة، مع نية ارتكاب أفعال غير لائقة مع هذا الشخص أو لعمل صور عن عمل جنسي يشارك فيه هذا الشخص، بالسجن لمدة لا تقل عن سنتين أو بغرامة من الفئة الرابعة، إذا ارتكب أي عمل يقصد به تحقيق اللقاء. **قانون العقوبات الكندي** **القسم 172.1** 1. يرتكب جريمة كل شخص يتواصل عن طريق وسائل الاتصالات مع		**التحليل القانوني** لإثبات الجرم الهولندي، يلزم عقد لقاء لأغراض جنسية مع تقديم أدلة إثبات مأخوذة من تاريخ الدردشة عبر الإنترنت تفصح عن قصد جنسي؛ طلب عقد اللقاء مع الأدلة على أنه تم التخطيط لذلك (أي التاريخ والمكان). الغرض من القانون الكندي هو منع استدراج الكبار المفترسين للأطفال عبر الإنترنت. لا تتطلب هذه الجريمة حدوث جريمة جنسية. وهذا يعني أن المتهم لا يحتاج إلى الذهاب فعلاً لمقابلة الضحية شخصيًا. تكتمل الجريمة قبل اتخاذ أي إجراءات لارتكاب الجريمة الموضوعية. **تحليل الفجوة** **التوصيات:** يُنصح بإدراجها في التشريعات المحلية لتجريم هذا السلوك التحضيري قبل ارتكاب جريمة جنسية

95. أوامر البحث والاستيلاء والمساعدة والإنتاج
96. http://www.legislation.gov.uk/ukpga/2000/23/section/53

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
a. شخص يكون عمره أقل من 18 عامًا، أو يظن المتهم أن عمره أقل من ذلك، بغرض تسهيل ارتكاب جريمة مرتبطة بهذا الشخص، وذلك بموجب المادة الفرعية 153 (1)، المادة 155، 163.1، 170 أو 171 أو القسم الفرعي 212 (1) أو (2) أو (2.1) أو (4)؛ b. شخص يكون عمره أقل من 16 عامًا، أو يظن المتهم أن عمره أقل من ذلك، بغرض تسهيل ارتكاب جريمة مرتبطة بهذا الشخص، وذلك بموجب المواد 151 أو 152، أو الفقرة الفرعية 160(3) أو 173(2) أو الأقسام 271 أو 272 أو 273 أو 280؛ أو c. شخص يكون عمره أقل من 14 عامًا، أو يظن المتهم أن عمره أقل من ذلك، بغرض تسهيل ارتكاب جريمة مرتبطة بهذا الشخص بموجب المادة 281. عقاب 2. يعتبر كل شخص يرتكب جريمة بموجب الفقرة الفرعية (1) مذنبًا a. مذنبًا بارتكاب جريمة ويكون عرضة لعقوبة السجن لمدة تتراوح بين 10 سنوات كحد أقصى وسنة واحدة كحد أدنى؛ أو b. مذنبًا بارتكاب جريمة يعاقب عليها في ملخص الإدانة بالسجن لمدة تتراوح بين 18 شهرًا كحد أقصى و 90 يومًا كحد أدنى. افتراض إعادة تقدير العمر 3. الأدلة على أن الشخص المشار إليه في الفقرة (1) (أ) أو (ب) أو (ج) قُدِّم للمتهم وعمره أقل من ثمانية عشر عامًا أو ستة عشر عامًا أو أربعة عشر عامًا، حسب الحالة، في حالة عدم وجود أدلة تثبت عكس ذلك تثبت أن المتهم يعتقد أن الشخص كان أقل من تلك السن. لا دفاع 4. لا يقبل دفاع المتهم أمام التهم الموجهة بموجب الفقرة (1) (أ) أو (ب) أو (ج) بأنه كان يعتقد أن الشخص المشار إليه في تلك الفقرة لا يقل عمره عن ثمانية عشر عامًا أو ستة عشر عامًا أو أربعة عشر عامًا، حسب الحالة، إلا في حالة اتخذ المتهم خطوات معقولة للتأكد من عمر الشخص.		

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 19 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[97] **البحث عن بيانات الحاسوب وضبطها** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لتمكين سلطاته المختصة من البحث في أو الوصول إلى: a. نظام الحاسوب أو جزء منه وبيانات الحاسوب المخزنة فيه؛ و b. وسيلة تخزين بيانات الحاسوب، حيث يمكن تخزين بيانات الحاسوب في أراضيها. 2. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وغيرها من الإجراءات لضمان تستطيع سلطاته عند تفتيشها نظام حاسوب معينًا أو جزءًا منه أو الوصول إليه بطريقة مماثلة، وذلك وفقًا للفقرة 1. أ، ويكون لدها أسباب للاعتقاد بأن البيانات المطلوبة مخزنة في نظام حاسوب آخر أو أن جزءًا منها موجود في إقليمها، وهذه البيانات يمكن الوصول إليها قانونيًا من النظام الأولي أو متاحة لها، فإنها قادرة على توسيع نطاق البحث أو الوصول المشابه للنظام الآخر على وجه السرعة. 3. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لتمكين سلطاته المختصة من ضبط أو تأمين بيانات الحاسوب التي وصلت إليها وفقا للفقرتين 1 أو 2. تشمل هذه التدابير القدرة على: a. الاستيلاء على نظام حاسوب أو جزء منه أو وسيلة تخزين بيانات الحاسوب، والقيام بما يلزم لتأمينه؛ b. إنشاء نسخة من بيانات الحاسوب هذه والاحتفاظ بها؛ c. الحفاظ على سلامة بيانات الحاسوب المخزنة ذات الصلة؛ d. أن يجعل الوصول إلى بيانات الحاسوب في نظام الحاسوب الذي تم الوصول إليه غير ممكن أو أن يحذفها.	**القانون رقم 04-09 بتاريخ 14 شعبان 1430 الموافق 5 أغسطس 2009 الذي يضع قواعد محددة بشأن منع ومكافحة الانتهاكات المتعلقة بتكنولوجيا المعلومات والاتصالات**[98] **المادة 3** وفقًا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وهذا القانون والقواعد الخاضعة للأحكام القانونية التي تكفل سرية المراسلات والاتصالات، يجوز النص على المتطلبات التقنية لحماية النظام العام أو لأغراض التحقيقات أو المعلومات القضائية الجارية وذلك لتنفيذ عمليات مراقبة الاتصالات الإلكترونية وجمع وتسجيل محتوياتها في الوقت الفعلي، وكذلك **عمليات التفتيش والمصادرة في نظام الحاسوب.** **المادة 4** قد تُنفذ عمليات المراقبة المنصوص عليها في المادة 3 في حالة الآتي: منع الجرائم المصنفة على أنها أعمال إرهابية أو تخريبية والجرائم المرتكبة ضد أمن الدولة. عند وجود معلومات عن احتمال حدوث خلل في نظام الحاسوب الذي يمثل تهديدًا للنظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني؛ لأغراض التحقيقات والمعلومات القضائية حيثما يصعب تحقيق النتائج المتصلة بالتفتيش المستمر دون الاستعانة بالمراقبة الإلكترونية؛ في تنفيذ طلبات المساعدة القضائية الدولية، لا يجوز تنفيذ عمليات المراقبة المذكورة أعلاه إلا بتصريح خطي من السلطة القضائية المختصة.	**التحليل القانوني** سلطة المادة 3 هي التفتيش والمصادرة بدلاً من مجرد الوصول. في "التقرير التوضيحي لاتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست، يعني "البحث" التفتيش عن البيانات أو قراءتها أو فحصها أو مراجعتها. ويشمل ذلك مفهوم البحث عن البيانات والبحث عن (فحص) البيانات. لكلمة "الوصول" معنى محايد وتعكس بدقة أكثر مصطلحات الحاسوب.[99] تشير المادة 5 إلى " الوصول"، ولكن يجب الإشارة إلى ذلك باستمرار في المادة 3 - المادة 26 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات تشير إلى "الوصول" تشير المادتان 3 و5 أيضًا إلى «نظام الحاسوب" وتشير المادة 5 إلى "بيانات الحاسوب المخزنة" و"نظام تخزين في الحاسوب" - وبالتالي - يمكن مصادرة البيانات **المخزنة** فقط. تعرف المادة 2 من القانون 04-09 "نظام الحاسوب" و "بيانات الحاسوب" و "مقدمي الخدمات" و "بيانات الحركة" و "الاتصالات الإلكترونية" وفقًا للغة اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست والاتفاقية العربية لمكافحة جرائم تقنية المعلومات. **تحليل الفجوة** **التوصيات:** يجب أن يشير التشريع الوطني باستمرار إلى الوصول تقيد المادة 4 أحكام التفتيش والمصادرة على فئات معينة من الجرائم - وهذا يعني أن العديد من الجرائم السيبرانية التي لا تشكل جرائم ضد الأمن القومي أو الإرهاب، لن تتمتع بسلطات إجرائية ذات صلة للتفتيش والمصادرة (فقط في سياق المنع) تتخطى المادة 5 المادة 19 من اتفاقية بودابست والقسم 20 من مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية (HIPCAR) التي تجيز تمديد صلاحيات التفتيش في الأنظمة المتصلة بأي حاسوب في العالم بناءً على مبدأ المعاملة بالمثل - وسيتم أيضًا تقييد هذا الحكم على أساس أنه لن ينطبق إلا على فئة الجرائم المذكورة في المادة 4 يجب أن تكون سلطة الوصول والتفتيش أوسع من التصنيف المقيد الحالي للجرائم لتشمل الجرائم السيبرانية المذكورة في القانون 04-09. وتشير المادة 6 إلى ضمان النسخ ومحتوى البيانات الأصلي وسلامة أي دليل يتم مصادرته. وعلى الرغم من أنها لا تشير إلى جعل البيانات غير قابلة للوصول لمنع المزيد من الجرائم.

97. المادة 3 من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية
98. https://www.unodc.org/res/cld/document/dza/2009/loi_n_09-04_du_14_chaabane_1430_correspondant_au_5_aout_2009_portant_regles_particulieres_relatives_a_la_prevention_et_a_la_lutte_contre_les_infractions_liees_aux_technologies_de_linformation_et_de_la_communication_html/Loi_prevention_et_lutte_contre_les_infractions_liees_aux_technologies_de_linformation_et_de_la_communication.pdf
99. التقرير التوضيحي لاتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست، الفقرة 191

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
4. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لتمكين سلطاته المختصة من أن تأمر أي شخص لديه معرفة بعمل نظام الحاسوب أو التدابير المطبقة لحماية البيانات الموجودة فيه بتوفير ما يلزم من المعلومات التي تكفل تنفيذ الإجراءات المشار إليها في الفقرتين 1 و 2. 5. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و 15. **القسم 20 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - البحث والضبط** 1. إذا اقتنع [القاضي] بناء على [معلومات تحت القَسَم] [شهادة خطية] أن هناك أسبابًا معقولة [للاشتباه] [للاعتقاد] أنه قد يكون هناك في مكان ما شيء أو بيانات حاسوب: • قد تكون مادية كدليل في إثبات الجريمة؛ أو • قد اكتسبها شخص نتيجة لجريمة؛ [يجوز] [يأمر] يصدر [القاضي] تفويضًا لضابط [إنفاذ القانون] [الشرطة]، ويزوده بما قد يلزم من مساعدة، لدخول المكان للتفتيش عن الشيء أو بيانات الحاسوب ومصادرتها، وعمل ما يلزم، بما في ذلك التفتيش أو عمليات الوصول الشبيهة: – نظام الحاسوب أو جزء منه وبيانات الحاسوب المخزنة فيه؛ و – وسيلة تخزين بيانات الحاسوب، حيث يمكن تخزين بيانات الحاسوب في إقليم البلد. 2. إذا كان[قوة إنفاذ القانون] [الشرطة] الذي يجري عملية بحث على أساس القسم 20 (1) أسباب للاعتقاد بأن البيانات المطلوبة مخزنة في نظام حاسوب آخر أو جزء منه في إقليمها، وأن هذه البيانات يمكن الوصول إليها قانونيًا أو يمكن أن تكون متاحة من النظام الأولي، فيجب أن يكون قادرًا على توسيع نطاق البحث أو الوصول إلى النظام الآخر بطريقة مماثلة.	في الحالة المشار إليها في الفقرة (أ) من هذه المادة، يصدر التفويض إلى ضباط الشرطة القضائية بموجب السلطات المشار إليها في المادة 13 أدناه الممنوحة له من النائب العام لمحكمة الجزائر، لمدة ستة (6) أشهر قابلة للتجديد، على أساس تقرير يوضح طبيعة العملية التقنية المستخدمة والأهداف التي يشير إليها. بموجب العقوبات المنصوص عليها في القانون الجنائي فيما يتعلق بانتهاك خصوصية الآخرين، يجب توجيه الأجهزة التقنية المعدة للأغراض الموضحة في الفقرة (أ) من هذه المادة حصرًا إلى جمع وتسجيل البيانات المتعلقة بمنع الأعمال الإرهابية والهجمات المتعلقة بالنيل من أمن الدولة ومراقبتها. **المادة 5** يجوز للسلطات القضائية المختصة وضباط الشرطة القضائية الذين يعملون في إطار قانون الإجراءات الجنائية وفي الحالات المنصوص عليها في المادة 4 أعلاه، **لأغراض التفتيش، الوصول إلى** المسافة: **(أ) نظام حاسوب أو جزء منه وبيانات الحاسوب المخزنة فيه؛** **أو (ب) نظام تخزين في الحاسوب.** في الحالة المنصوص عليها في الفقرة (أ) من هذه المادة، إذا كان لدى السلطة التي تجري عملية التفتيش سببًا للاعتقاد بأن البيانات المطلوبة مخزنة في نظام حاسوبي آخر وأن هذه البيانات يمكن الوصول إليها من النظام الأصلي، **فقد تمدد عملية التفتيش على الفور للنظام المعني أو إلى جزء منه بناءً على إخطار مسبق من السلطة القضائية المختصة.** **إذا ثبت من قبل أن البيانات المطلوبة، التي يمكن الوصول إليها عن طريق النظام الأول، يتم تخزينها في نظام حاسوبي آخر موجود خارج الإقليم الوطني، فيجب الحصول عليها بمساعدة السلطات الأجنبية المختصة وفقًا لمبدأ المعاملة بالمثل في الاتفاقيات الدولية ذات الصلة.**	يجب النظر في إدراج صياغة المادة 19.3 د في اتفاقية بودابست لضمان عدم إمكانية الوصول إلى البيانات المصادرة لمنع أي استخدام آخر. تشير المادة 5 إلى "طلب" الفرد للمساعدة في المعلومات المتعلقة بتشغيل نظام الحاسوب أو حماية البيانات - وليس من الواضح ما تعنيه كلمة "طلب" وما هي الصلاحيات المتاحة إذا رفض هذا الفرد التعاون. تنص المادة 21 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية على التشريع لضمان تقديم المساعدة من قبل أولئك الذين لديهم معرفة متخصصة بموقع الأدلة ذات الصلة - يمكن استخدام هذا كدليل - انظر أيضًا القسم 17 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية، المتعلق بالجريمة في حال تم رفض المساعدة دون عذر قانوني يجب أن يتضمن التشريع الوطني نصًا يقضي "باستخراج نسخة من بيانات الحاسوب ومصادرة نظام الحاسوب أو جزء منه أو وسيلة تخزين بيانات الحاسوب، والقيام بما يلزم لتأمينه بطريقة مماثلة؛ "- انظر تعريف "المصادرة" في مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية (HIPCAR) القسم 3 (16) تعريف "طلب" والصلاحيات المتاحة لضمان تقديم مساعدة معقولة - أو استخدام القسم 21 من مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية (HIPCAR) كدليل مع الجرم الوارد في القسم 17

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
3. يتم تمكين ضابط [تطبيق القانون] [الشرطة] الذي يقوم بالبحث من مصادرة أو تأمين بيانات الحاسوب المماثلة التي يتم الوصول إليها وفقًا للفقرات 1 أو 2. **القسم 21 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - المساعدة** يجب على أي شخص لا يشتبه في ارتكابه جريمة ولكن لديه علم بسير عمل نظام الحاسوب أو التدابير المطبقة لحماية بيانات الحاسوب الواردة فيه والتي تخضع لعملية بحث بموجب المادة 20، أن يسمح وأن يساعد إذا لزم الأمر وطلب منه الشخص المسؤول أن يجري البحث عن طريق: • توفير المعلومات التي تمكن من اتخاذ التدابير المشار إليها في المادة 20؛ • الوصول إلى نظام حاسوب أو وسيط تخزين بيانات الحاسوب واستخدامه للبحث في أي بيانات حاسوب متاحة أو في النظام؛ • الحصول على ونسخ بيانات حاسوب هذه؛ • استخدام المعدات لعمل نسخ؛ و • الحصول على معلومات واضحة من نظام حاسوب بشكل مقبول في الإجراءات القانونية. **المادة 26 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - فحص المعلومات المخزنة** 1. تلتزم كل دولة طرف يتبني الإجراءات الضرورية لتمكين سلطاتها المختصة من التفتيش أو الوصول إلى: a. تقنية معلومات أو جزء منها والمعلومات المخزنة فيها أو المخزنة عليها. b. بيئة أو وسيط تخزين معلومات تقنية معلومات والذي قد تكون معلومات التقنية مخزنة فيه أو عليه. 2. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من التفتيش أو الوصول إلى تقنية معلومات معينة أو جزء منها بما يتوافق مع الفقرة (-1 أ) إذا كان هناك اعتقاد بأن المعلومات المطلوبة مخزنة في تقنية معلومات أخرى أو جزء منها في إقليمها وكانت هذه المعلومات قابلة للوصول قانونا أو متوفرة في التقنية الأولى فيجوز توسيع نطاقالتفتيش والوصول للتقنية الأخرى.	**يحق للسلطات المسؤولة عن التفتيش طلب أي شخص مطلع على تشغيل نظام الحاسوب المعني أو التدابير المطبقة لحماية بيانات الحاسوب الواردة فيه لمساعدتهم وتزويدهم بجميع المعلومات اللازمة لإنجاز مهمتهم.** **المادة 6** عندما تكتشف سلطة التفتيش البيانات المخزنة في نظام الحاسوب ذي الصلة بالتحقيق في الجريمة أو مرتكبها، ولا يكون إدخال النظام بأكمله ضروريًا، يتم نسخ البيانات المعنية وكذلك تلك اللازمة لفهمها على وسائط تخزين الحاسوب التي يمكن مصادرتها وضبطها وفقًا للشروط المنصوص عليها في قانون الإجراءات الجنائية. يجب على السلطة التي تجري التفتيش والمصادرة، على أي حال، أن تضمن سلامة البيانات في نظام الحاسوب المعني. ومع ذلك، فقد تستخدم الوسائل التقنية اللازمة لتنسيق أو إعادة تكوين مثل هذه البيانات لجعلها قابلة للاستخدام لأغراض التحقيق، بشرط ألا يؤدي إعادة التكوين أو تنسيق البيانات إلى تغيير المحتوى	

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 27 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - ضبط المعلومات المخزنة 1. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من ضبط وتأمين معلومات تقنية المعلومات التي يتم الوصول إليها حسب الفقرة 1 من المادة 26 من هذه الاتفاقية. a. هذه الإجراءات تشمل صلاحيات: b. ضبط وتأمين تقنية المعلومات أو جزء منها أو وسيط تخزين معلومات تقنية المعلومات. c. عمل نسخة معلومات تقنية المعلومات والاحتفاظ بها. d. الحفاظ على سلامة معلومات تقنية المعلومات المخزنة. 2. إزالة أو منع الوصول إلى تلك المعلومات في تقنية المعلومات التي يتم الوصول إليها. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى أي شخص لديه معرفة بوظيفة تقنية المعلومات أو الإجراءات المطبقة لحماية تقنية المعلومات من أجل تقديم المعلومات الضرورية لإتمام تلك الإجراءات المذكورة في الفقرتين 2 و 3 من المادة 26 من هذه الاتفاقية.		
المادة 16 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[100] **الحفظ المستعجل لبيانات الحاسوب المخزنة والكشف عنها** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وغيرها من الإجراءات لتمكين سلطاته المختصة من طلب الحفظ السريع لبيانات الحاسوب المحددة أو الحصول عليها بشكل مماثل، بما في ذلك بيانات الحركة التي تم تخزينها عن طريق نظام حاسوبي، ولا سيما عندما يكون هناك أسباب للاعتقاد بأن بيانات الحاسوب معرضة بشكل خاص للفقد أو التعديل. 2. عندما يقوم أحد الأطراف بتنفيذ الفقرة 1 أعلاه عن طريق أمر شخص بحفظ بيانات الحاسوب المخزنة المحددة وذلك بوضعها في حوزته أو تحت سيطرته، يعتمد هذا الطرف الإجراءات التشريعية وغيرها من الإجراءات التي قد تكون ضرورية لإلزام ذلك الشخص بالحفاظ على سلامة بيانات الحاسوب لفترة زمنية طويلة، حدها الأقصى تسعين يومًا، وذلك لتمكين السلطات المختصة من طلب الكشف عنها. يجوز للطرف أن ينص على تجديد هذا الأمر لاحقًا.	**لا يوجد معادل**	**التحليل القانوني** هذه القوة الإجرائية مهمة لضمان الحفاظ على البيانات المعرضة للحذف أو الفقد **تحليل الفجوة** **التوصيات:** تعد هذه القدرة المستعجلة للاحتفاظ بمعلومات المشترك الأساسية والبيانات الوصفية والمعاملات والمحتويات المخزنة ضرورية كجزء من تحقيقات جرائم الإنترنت، ولضمان أن تكون الأدلة متاحة للبحث والوصول والضبط والمراجعة. يمكن استخدام لغة المادة 16 من اتفاقية بازل أو القسم 23 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية أو المادة 23 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. سيتطلب ذلك أيضًا تعريف "معلومات المشترك أو معلومات المشترك الأساسية (BSI)"

100. لا يوجد ما يعادلها في اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
3. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لإلزام الحارس أو أي شخص آخر يحفظ بيانات الحاسوب بالحفاظ على سرية تنفيذ هذه الإجراءات للفترة الزمنية المنصوص عليها في قانونه الداخلي. 4. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و 15. **القسم 23 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الحفظ المستعجل** إذا اقتنع ضابط [تطبيق القانون] [الشرطة] بوجود أسباب معقولة للاعتقاد بأن بيانات الحاسوب المطلوبة لأغراض التحقيق الجنائي معرضة للضياع أو التعديل، يجوز لضابط [تطبيق القانون] [الشرطة]، عن طريق إشعار مكتوب مقدم إلى شخص يتحكم في بيانات الحاسوب، أن يطلب من هذا الشخص الحفاظ على البيانات المحددة في الإشعار لمدة تصل إلى سبعة (7) أيام على وفقًا لما هو محدد في الإشعار. يمكن تمديد الفترة إلى ما بعد سبعة (7) أيام إذا سمح [قاضي]، بناءً على طلب من طرف واحد، وذلك لمدة زمنية أخرى محددة. **المادة 23 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات- الحفظ المستعجل للبيانات المخزنة في تكنولوجيا المعلومات** 1. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأمر أو الحصول على الحفظ العاجل للمعلومات المخزنة بما في ذلك معلومات تتبع المستخدمين والتي خزنت على تقنية معلومات وخصوصا إذا كان هناك اعتقاد بأن تلك المعلومات عرضة للفقدان أو التعديل. 2. تلتزم كل دولة طرف بتبني الإجراءات الضرورية فيما يتعلق بالفقرة 1 بواسطة إصدار أمر إلى شخص من أجل حفظ معلومات تقنية المعلومات المخزنة والموجودة بحيازته أو سيطرته ومن أجل إلزامه بحفظ وصيانة سلامة تلك المعلومات لمدة أقصاها 90 يوما قابلة للتجديد، من أجل تمكين السلطات المختصة من البحث والتقصي 3. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لإلزام الشخص المسؤول عن حفظ تقنية معلومات للإبقاء على سرية الإجراءات طوال الفترة القانونية المنصوص عليها في القانون الداخلي.		تعريف معلومات المشترك في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات هو:[101] " أي معلومات لدى مزود الخدمة بخصوص المشتركين في الخدمة، باستثناء المعلومات التي يمكن من خلالها معرفة ما يلي: نوع خدمة الاتصال المستخدمة والأحكام الفنية المتعلقة بها وفترة الخدمة. هوية المشترك وعنوانه البريدي أو الجغرافي أو رقم الهاتف ومعلومات الدفع المتاحة بموجب اتفاقية الخدمة أي معلومات أخرى على موقع تركيب معدات الاتصالات بموجب اتفاقية الخدمة." ينبغي إيلاء اهتمام لأن يكون طول مدة الحفظ معقولًا في هذه الظروف، وأن يُسمَح بتطبيق التمديد في الظروف الملحة - تنص اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست والاتفاقية العربية لمكافحة جرائم تقنية المعلومات على 90 يومًا، فيما تنص اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية على 7 أيام. ووفقًا للتجربة فإن مدة 90 يومًا هي مدة قصيرة في التحقيقات عبر الإنترنت، ويجب أن تكون حوالي 180 يومًا يمكن تمديدها.

101. انظر المادة 2 (9) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 17 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[102] **الحفظ المستعجل والكشف الجزئي لبيانات الحركة** 1. فيما يتعلق ببيانات الحركة التي يتعين الحفاظ عليها بموجب المادة 16، يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى من أجل a. التأكد من أن مثل هذا الحفظ المستعجل لبيانات الحركة متاح بغض النظر عما إذا كان هناك واحد أو أكثر من مقدمي الخدمة قد شاركوا في نقل ذلك الاتصال؛ و b. ضمان الكشف السريع للسلطة المختصة لدى الدولة الطرف، أو للشخص المعين من قبل تلك السلطة، عن كمية كافية من بيانات الحركة لتمكينه من تحديد مقدمي الخدمات والمسار الذي تم من خلاله نقل الاتصال. 2. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و 15. **القسم 23 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الحفظ المستعجل** إذا اقتنع ضابط [تطبيق القانون] [الشرطة] بوجود أسباب معقولة للاعتقاد بأن بيانات الحاسوب المطلوبة لأغراض التحقيق الجنائي معرضة للضياع أو التعديل، يجوز لضابط [تطبيق القانون] [الشرطة]، عن طريق إشعار مكتوب مقدم إلى شخص يتحكم في بيانات الحاسوب، أن يطلب من هذا الشخص الحفاظ على البيانات المحددة في الإشعار لمدة تصل إلى سبعة (7) أيام على وفقًا لما هو محدد في الإشعار. يمكن تمديد الفترة إلى ما بعد سبعة (7) أيام إذا سمح [قاضي]، بناءً على طلب من طرف واحد، وذلك لمدة زمنية أخرى محددة.	**القانون رقم 04-09 بتاريخ 14 شعبان 1430 الموافق 5 أغسطس 2009 الذي يضع قواعد محددة بشأن منع ومكافحة الانتهاكات المتعلقة بتكنولوجيا المعلومات والاتصالات** **المادتان 2 و 10**	**التحليل القانوني** تعد هذه القوة الإجرائية مهمة بشكل خاص لضمان توفير مقدمي خدمات الإنترنت لعناوين بروتوكول إنترنت يمكنها تحديد موقع مرتكب الجريمة السيبرانية. **تحليل الفجوة** **التوصيات:** تفرض المادة 10 من القانون رقم 04-09 التزامًا على مزودي خدمة الاتصالات للحفاظ على بيانات الحركة خلال عام واحد. تعرف المادة 2 من القانون 04-09 "نظام الحاسوب" و "بيانات الحاسوب" و "مقدمي الخدمات" و "بيانات الحركة" و "الاتصالات الإلكترونية" وفقًا للغة اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست والاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

102. لا يوجد ما يعادلها في اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
القسم 24 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - جمع بيانات حركة الاتصالات إذا اقتنع ضابط [الشرطة] المعني [بتطبيق القانون] بناءً على أسباب معقولة بأن البيانات المخزنة في نظام الحاسوب ضرورية لأغراض التحقيق الجنائي، يجوز له أن يطلب، عبر إشعار خطي، من شخص له السيطرة على نظام الحاسوب كشف بيانات حركة مرور تتعلق باتصال محدد بشكل كافٍ لتحديد: • مزودو خدمة الإنترنت؛ و/ أو • المسار الذي تم من خلاله نقل الاتصال. **المادة 24 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - لتحفظ العاجل والكشف الجزئي لمعلومات تتبع المستخدمين** تلتزم كل دولة طرف بتبني الإجراءات الضرورية فيما يختص بمعلومات تتبع المستخدمين من أجل: 1. ضمان توفر الحفظ العاجل لمعلومات تتبع المستخدمين بغض النظر عن اشتراك واحد أو أكثر من مزودي الخدمة في بث تلك الاتصالات. 2. ضمان الكشف العاجل للسلطات المختصة لدى الدولة الطرف أو لشخص تعينه تلك السلطات لمقدار كاف من معلومات تتبع المستخدمين لتمكين الدولة الطرف من تحديد مزودي الخدمة ومسار بث الاتصالات.		
المادة 18 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[103] **أمر النسخ** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وتدابير أخرى لتمكين سلطاته المختصة من أن تأمر: a. شخصًا موجودًا في إقليمها بتقديم بيانات حاسوب محددة في حيازته أو تحت سيطرته، وتُخَزّن في نظام حاسوب أو بوسيلة تخزين بيانات الحاسوب؛ و b. مقدم خدمة يقدم خدماته في إقليم الدولة الطرف بتقديم معلومات المشترك المرتبطة بهذه الخدمات، والتي تكون في حيازة أو تحت سيطرة مقدم الخدمة.	**لا يوجد معادل**	**التحليل القانوني** هذا شرط أساسي لإجراء تحقيق فعال في جرائم الإنترنت وسيؤثر غيابه على الملاحقات القضائية والتعاون الدولي. **تحليل الفجوة** **التوصيات:** تعتبر قوة التحقيق هذه ضرورية لضمان توفير مزودي خدمة الاتصالات في الجزائر لمعلومات المشترك الأساسية وبيانات الحركة وبيانات المحتوى المخزنة. من المستحسن أن يكون هناك تعريف لمصطلح "معلومات المشترك أو معلومات المشترك الأساسية (BSI)" حيث يمكن إصدار أنواع مختلفة من الأدلة من جانب مزودي خدمة الاتصالات (أي معلومات المشترك الأساسية وحركة المرور والمحتوى). علاوةً على ذلك، سوف تتطلب هذه السلطة من الأفراد وغيرهم (مثل الكيانات المؤسسية والمؤسسات المالية وغيرها من المنظمات) ممن يحملون البيانات أن يقوموا بإصدارها بناء على طلب سلطات إنفاذ القانون.

103. لا يوجد ما يعادلها في اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
2. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و 15. 3. تعني "معلومات المشترك" أي معلومات محفوظة بشكل بيانات حاسوب أو أي شكل آخر ويحتفظ بها مزود الخدمة، وترتبط بالمشتركين في خدماته، بخلاف بيانات الحركة أو المحتوى، والتي يمكن إنشاؤها من خلال: a. نوع خدمة الاتصال المستخدمة والأحكام الفنية المتعلقة بها وفترة الخدمة؛ b. هوية المشترك أو العنوان البريدي أو الجغرافي، ورقم الهاتف وأرقام الاتصال الأخرى ومعلومات الفوترة والدفع المتاحة بناءً على اتفاقية الخدمة؛ c. أي معلومات أخرى متاحة على موقع تركيب معدات الاتصالات بناءً على اتفاقية الخدمة أو الترتيب. **القسم 22 من نظام اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - أمر النسخ** إذا كان [قاض] مقتنعًا بناءً على طلب قدمه [ضابط أنفاذ القانون] [الشرطة] بأن بيانات حاسوب محددة أو نسخة مطبوعة أو غيرها من المعلومات ضرورية لإجراء تحقيق جنائي أو لإجراءات جنائية، يجوز [للقاضي] أن يأمر بما يلي: • أن ينسخ شخص في إقليم [الدولة المشترعة] يتحكم في نظام الحاسوب نسخًا محددة من بيانات الحاسوب أو نسخة مطبوعة أو معلومات أخرى واضحة من تلك البيانات؛ أو • مزود خدمة الإنترنت في [الدولة المشترعة] لتقديم معلومات حول الأشخاص المشتركين في الخدمة أو الذين يستخدمونها بطريقة أخرى. **المادة 25 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - أمر تسليم المعلومات** تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى: 1. أي شخص في إقليمها لتسليم معلومات معينة في حيازة ذلك الشخص والمخزنة على تقنية معلومات أو وسيط تخزين معلومات. 2. أي مزود خدمة يقدم خدماته في إقليم الدولة الطرف لتسليم معلومات المشترك المتعلقة بتلك الخدمات في حوزة مزود الخدمة أو تحت سيطرته.		يمكن أن تكون المادة 18 من اتفاقية بودابست والقسم 22 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية بمثابة دليل مع التطبيق الثابت للتعريفات.

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 21 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[104] **اعتراض بيانات المحتوى** **المادة 29 من** الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - **اعتراض معلومات المحتوى**	**القانون رقم 04-09 بتاريخ 14 شعبان 1430 الموافق 5 أغسطس 2009 الذي يضع قواعد محددة بشأن منع ومكافحة الانتهاكات المتعلقة بتكنولوجيا المعلومات والاتصالات** **المادة 3** وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وهذا القانون والقواعد الخاضعة للأحكام القانونية التي تكفل سرية المراسلات والاتصالات، يجوز النص على المتطلبات التقنية لحماية النظام العام أو لأغراض التحقيقات أو المعلومات القضائية الجارية **وذلك لتنفيذ عمليات مراقبة الاتصالات الإلكترونية وجمع وتسجيل محتوياتها في الوقت الحقيقي**، وكذلك عمليات البحث والحجز في نظام الحاسوب.	**التحليل القانوني** تجيز المادة 3 جمع المحتوى في الوقت الفعلي. لا توجد ضمانات لمنع التطفل الناتج عن النظام أو لتقييم ما إذا كان استخدام هذه السلطة ضروريًا ومتناسبًا ومعقولاً من عدمه. **يجب أن يؤمر بهذا الإجراء وفقًا لأحكام قانون الإجراءات الجزائية بناء على إذن من وكيل الجمهورية أو قاضي التحقيق. يجب أن يتضمن هذا التفويض جميع العناصر التي تسمح بتعريف الاتصالات التي يتم اعتراضها، والجريمة التي تبرر اللجوء إلى هذا الإجراء، بالإضافة إلى مدة الإجراء (4 شهور قابلة للتجديد).** **لا يمكن لهذا الإجراء أن يؤثر على السرية المهنية.** **تنص المادة 10 من "القانون رقم 04-09 تاريخ 05/08/2009 بشأن القواعد الخاصة المتعلقة بمنع ومكافحة الجرائم المرتبطة بتكنولوجيا المعلومات والاتصالات على إلزام مزودي الخدمة بتقديم الدعم إلى السلطات المسؤولة عن التحقيقات القضائية من أجل جمع أو تسجيل بيانات المحتوى في الوقت الحقيقي للاتصالات وإذا لم يلتزموا بذلك، فيمكن محاكمتهم لعرقلة سير العدالة أو انتهاك سرية التحقيق.** **توسع المادتان 1 و 2 من "القانون رقم 04-09 تاريخ 05/08/2009 بشأن القواعد الخاصة المتعلقة بمنع ومكافحة الجرائم المرتبطة بتكنولوجيا المعلومات والاتصالات" هذا الإجراء ليشمل جميع الجرائم التي ترتكبها أو تسهل ارتكابها أنظمة الاتصالات الإلكترونية أو الحاسوبية.** **تحليل الفجوة** **التوصيات:** يقترح اتخاذ المعايير التالية كحد أدنى: 1. للتأكد باستمرار من أن المراقبة مبررة ولمنع التطفل الناتج عنها، طبّق الاختبارات التالية: a. **الضرورة**: يجب أن يكون وكيل الجمهورية أو قاضي التحقيق مقتنعًا بأن إجراء المراقبة المقترح ضروري بشكل مطلق لغرض التحقيق وذلك بإثبات أن جميع الوسائل الأخرى إما قد استنفذت أو أنها غير قابلة للتطبيق. b. **معقول**: يجب أن يكون وكيل الجمهورية أو قاضي التحقيق مقتنعًا بأن إجراءات المراقبة لغرض جمع المعلومات المستهدفة هي الأقل تطفلًا c. **التناسب:** يجب أن يقتنع وكيل الجمهورية أو قاضي التحقيق، عند انتهاك الخصوصية الشخصية، أن المراقبة متناسبة مع خطورة الجريمة - ويشمل ذلك الأخذ بعين الاعتبار التطفل المترافق معها وتقليص الضرر التي يمكن أن تقع على أطراف أخرى

104. لا يوجد ما يعادلها في اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية

إجراءات		
أفضل الممارسات الدولية	**التشريع الوطني**	**ملاحظات**
المادة 20 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[105] **جمع بيانات حركة الاتصالات في الوقت الحقيقي** 1. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتمكين سلطاته المختصة من: a. الجمع أو التسجيل من خلال تطبيق الوسائل التقنية على أراضي ذلك الطرف، و b. إلزام مزود الخدمة، في حدود قدرته التقنية الحالية: i. الجمع أو التسجيل من خلال تطبيق الوسائل التقنية على أراضي ذلك الطرف؛ أو ii. التعاون ومساعدة السلطات المختصة في الجمع أو التسجيل، بيانات حركة الاتصالات المرتبطة باتصالات محددة في أراضيها، والمرسلة عن طريق نظام حاسوب، وذلك في الوقت الحقيقي. 2. في الحالات التي لا يمكن فيها لأي طرف، بسبب المبادئ المستقرة في نظامه القانوني الداخلي، أن يعتمد التدابير المشار إليها في الفقرة 1.أ، يجوز له بدلا من ذلك اعتماد تدابير تشريعية وتدابير أخرى قد تكون ضرورية لضمان جمع أو تسجيل البيانات الحركية المرتبطة باتصالات محددة مرسلة في أراضيه، في الوقت الفعلي، من خلال تطبيق الوسائل التقنية على ذلك الإقليم. 3. يعتمد كل طرف التدابير التشريعية والتدابير الأخرى التي قد تكون ضرورية لإلزام مقدم الخدمة بالحفاظ على سرية تنفيذ أي سلطة منصوص عليها في هذه المادة وأي معلومات تتعلق بها. 4. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و 15. **القسم 25 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - جمع بيانات حركة الاتصالات**	**القانون رقم 04-09 بتاريخ 14 شعبان 1430 الموافق 5 أغسطس 2009 الذي يضع قواعد محددة بشأن منع ومكافحة الانتهاكات المتعلقة بتكنولوجيا المعلومات والاتصالات** **المادة 3** وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وهذا القانون والقواعد الخاضعة للأحكام القانونية التي تكفل سرية المراسلات والاتصالات، يجوز النص على المتطلبات التقنية لحماية النظام العام أو لأغراض التحقيقات أو المعلومات القضائية الجارية **وذلك لتنفيذ عمليات مراقبة الاتصالات الإلكترونية وجمع وتسجيل محتوياتها في الوقت الحقيقي**، وكذلك عمليات البحث والحجز في نظام الحاسوب.	**التحليل القانوني** **توجد سلطة محددة ومستقلة لجمع بيانات الحركة في الوقت الحقيقي مثل ما هو منصوص عليه في المرسوم الرئاسي 15-261 الصادر بتاريخ 08/10/2015، فيما يتعلق بتكوين وتنظيم وعمل الهيئة الوطنية للوقاية من جرائم تكنولوجيا الإعلام والاتصالات ومكافحتها. (الجريدة الرسمية رقم 53 بتاريخ 08/10/2015).** **تحليل الفجوة** **التوصيات:** يجب أن تكون هناك ضمانات لضمان قانونية الجمع وأنه ضروري ومعقول ومتناسب في هذه الظروف. يقترح اتخاذ المعايير التالية كحد أدنى: 1. **الضرورة**: يجب أن يكون وكيل الجمهورية أو قاضي التحقيق مقتنعًا بأن إجراء المراقبة المقترح ضروري بشكل مطلق لغرض التحقيق وذلك بإثبات أن جميع الوسائل الأخرى إما قد استنفذت أو أنها غير قابلة للتطبيق. 2. **معقول**: يجب أن يكون وكيل الجمهورية أو قاضي التحقيق مقتنعًا بأن إجراءات المراقبة لغرض جمع المعلومات المستهدفة هي الأقل تطفلًا 3. **التناسب:** يجب أن يقتنع وكيل الجمهورية أو قاضي التحقيق، عند انتهاك الخصوصية الشخصية، أن المراقبة متناسبة مع خطورة الجريمة - ويشمل ذلك الأخذ بعين الاعتبار التطفل المترافق معها وتقليص الضرر التي يمكن أن تقع على أطراف أخرى لا تشير المادة 28 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات إلى الوقت الفعلي - بل تشير إلى الجمع السريع فقط. تسمح المادة 31 (3) (هـ) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية بجمع البيانات في الوقت الحقيقي، لكن هنالك حاجة إلى ضمانات. لذلك، يجب استخدام المادة 20 من اتفاقية بودابست والقسم 25 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية باعتبارهما دليلاً

105. المادة 31 (3) (هـ) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية - تشير المادة 28 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات إلى الجمع المستعجل بدلاً من الجمع في الوقت الفعلي

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
1. إذا تأكد [قاض] بناء على [شهادة تحت القسم] [شهادة خطية] بأن هناك أسباباً معقولة لـ [الاشتباه] [الظن] بأن بيانات حركة الاتصالات المرتبطة ببلاغ محدد ضرورية بشكل معقول لأغراض [التحقيق] في تحقيق جنائي، [يجوز] [للقاضي] [يجب] أن يأمر شخصًا يتحكم بهذه البيانات بما يلي: • جمع أو تسجيل بيانات حركة الاتصالات المرتبطة باتصالات محددة خلال فترة محددة؛ أو • التصريح ومساعدة ضابط [الشرطة] [قوة تنفيذ القانون] محدد لجمع أو تسجيل تلك البيانات. 2. إذا تأكد [قاض] بناء على [شهادة تحت القسم] [شهادة خطية] بأن هناك أسباباً معقولة لـ [الاشتباه] [الظن] بأن بيانات حركة الاتصالات المرتبطة ببلاغ محدد ضرورية بشكل معقول لأغراض [التحقيق] في تحقيق جنائي، [يجوز] [للقاضي] [يجب] أن يسمح لـ [قوة تنفيذ القانون] [الشرطة] بجمع أو تسجيل بيانات حركة الاتصالات المرتبطة برسالة محددة خلال فترة محددة من خلال تطبيق الوسائل التقنية. 3. قد تقرر دولة عدم تنفيذ القسم 25.		
		واجب الكشف عن مفاتيح التشفير مع استخدام الإرهابيين والمجرمين المنظمين بشكل روتيني لتطبيقات الرسائل المشفرة[106] قد يعتبر الكشف عن مفاتيح التشفير قوة ملائمة لإطلاق مفاتيح كلمات المرور لفتح الأجهزة[107] **تحليل الفجوة** **التوصيات:** عدم القدرة على توضيح ما إذا كانت هناك أية صلاحيات في الجزائر - لكن هذه الصلاحيات ستتيح لوكالات إنفاذ القوانين إجبار أصحاب الأجهزة على فتحها
		التزامات الاحتفاظ بالبيانات[108] تسمح مثل هذه السلطة لوكالات إنفاذ القانون بـ 1. تتبع وتحديد مصدر الاتصال 2. تحديد وجهة الاتصال؛ 3. تحديد تاريخ ووقت ومدة الاتصال؛ و 4. تحديد نوع الاتصال الجزائر لديها هذا النوع من الالتزام[109]

106. Eleanor Saitta. “Can Encryption Save Us?” Nation 300, no. 24 (15 يونيو 2015): 16-18. Academic Search Premier, EBSCOhost (تمت زيارته في 29 فبراير 2016).

107. انظر مثلاً القسم 49 من القانون الإنجليزي (Regulation of Investigatory Powers Act 2000 (UK) - http://www.legislation.gov.uk/ukpga/2000/23/section/49

108. أصدر الاتحاد الأوروبي في عام 2006 توجيهه بشأن الاحتفاظ بالبيانات - اضطرت الدول الأعضاء في الاتحاد الأوروبي إلى تخزين بيانات الاتصالات الإلكترونية لمدة ستة أشهر على الأقل و 24 شهراً على الأكثر للتحقيق في الجرائم الخطيرة وكشفها ومقاضاة مرتكبيها. أبطلت محكمة العدل الأوروبية في عام 2014 توجيه الاحتفاظ بالبيانات، حيث قررت أنها قدمت ضمانات غير كافية ضد التدخلات في الخصوصية وحماية البيانات. في حالة عدم وجود توجيه صالح للاتحاد الأوروبي بشأن الاحتفاظ بالبيانات، فقد تواصل الدول الأعضاء تقديم خطة للاحتفاظ بالبيانات - للاطلاع على الخطط الوطنية، انظر: http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention

109. تقرير المراجعة العالمي ICMEC صفحة 18

التعاون الدولي		
أفضل الممارسات الدولية	**التشريع الوطني**	**ملاحظات**
المادة 22 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[110] **الاختصاص القضائي** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وغيرها من الإجراءات لإقامة ولاية قضائية على أي جرم منصوص عليه في المواد من 2 إلى 11 من هذه الاتفاقية، عندما تُرتكب الجريمة: a. في أراضيها؛ أو b. على متن سفينة ترفع علم تلك الدولة الطرف؛ أو c. على متن طائرة مسجلة بموجب قوانين ذلك الطرف؛ أو من قِبَل أحد رعاياها، إذا كانت الجريمة معاقبًا عليها بموجب القانون الجنائي حيث ارتكبت، أو إذا ارتكبت الجريمة خارج الولاية الإقليمية لأي دولة. 2. يجوز لكل طرف أن يحتفظ بالحق في عدم تطبيق أو تطبيق قواعد الاختصاص المنصوص عليها في الفقرات من 1 إلى 1 د من هذه المادة أو أي جزء منها فقط في حالات أو شروط محددة. 3. يعتمد كل طرف ما قد يلزم من إجراءات لإقامة ولاية قضائية على الجرائم المشار إليها في الفقرة 1 من المادة 24 من هذه الاتفاقية، في الحالات التي يكون فيها الجاني المفترض موجودا في إقليمه ولا يسلمه إلى بلد آخر بعد طلب التسليم على أساس جنسيته فقط. 4. لا تستبعد هذه الاتفاقية أي ولاية قضائية جنائية يمارسها أي طرف وفقًا لقانونه الداخلي. 5. عندما يطالب أكثر من طرف بالولاية القضائية على جريمة مفترضة تم النص عليها في هذه الاتفاقية، يتشاور الطرفان المعنيان، عند الضرورة من أجل تحديد الولاية القضائية الأنسب. **القسم 19من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الولاية القضائية** ينطبق هذا القانون على أي فعل أو تقصير: • في إقليم [الدولة المشترعة]؛ أو	**القانون رقم 04-09 بتاريخ 14 شعبان 1430 الموافق 5 أغسطس 2009 الذي يضع قواعد محددة بشأن منع ومكافحة الانتهاكات المتعلقة بتكنولوجيا المعلومات والاتصالات** **المادة 15**	**التحليل القانوني** بدون وجود نطاق محدد بوضوح للجرائم الإلكترونية، وهي دولية بطبيعتها سيبقى أي تشريع مقيدًا. **وفقًا للمادة 15 من القانون رقم 04-09، تتمتع المحاكم الجزائرية الآن بصلاحية مقاضاة الجرائم المتعلقة بتكنولوجيا المعلومات والاتصالات المرتكبة في الخارج عندما يكون مرتكب الجريمة شخصًا أجنبيًا، عند استهداف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني.** **تجيز المادة 588 من قانون الإجراءات الجنائية (بصيغته المعدلة بموجب المرسوم 15-02 الصادر بتاريخ 23-07-2015) للمحاكم الجزائرية بمحاكمة أي أجنبي يقوم بارتكاب جريمة (جناية أو جنحة) في الخارج ضد أمن الدولة أو المصالح الأساسية للدولة أو الضباط الدبلوماسيين والقنصليين الجزائريين أو ضد أي مواطن جزائري.** **تحليل الفجوة** **التوصيات:** إذا كان هناك تعارض بين السلطات القضائية، فيجب أن تؤخذ في الاعتبار المبادئ التوجيهية المتعلقة بتحديد الولاية القضائية المناسبة لمحاكمة جريمة ما - انظر المبادئ التوجيهية يوروجست لتقرير الولاية القضائية التي في الجرائم التي تجب ملاحقتها (المراجعة 2016)[111]

110. لا يوجد ما يعادلها في اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية
111. http://www.eurojust.europa.eu/Practitioners/operational/Documents/Operational-Guidelines-for-Deciding.pdf

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
• على سفينة أو طائرة مسجلة في [الدولة المشترعة]؛ أو • من قبل أحد مواطني [الدولة المشترعة] خارج الولاية القضائية لأي بلد؛ أو من قبل أحد مواطني [الدولة المشترعة] خارج إقليم [الدولة المشترعة]، إذا كان سلوك هذا الشخص يشكل أيضًا جريمة بموجب قانون البلد الذي ارتكبت فيه الجريمة. **المادة 30 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - الاختصاص** 1. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد اختصاصها على أي من الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية وذلك إذا ارتكبت الجريمة كلياً أو جزئياً أو تحققت: a. في إقليم الدولة الطرف b. على متن سفينة تحمل علم الدولة الطرف. c. على متن طائرة مسجلة تحت قوانين الدولة الطرف. d. من قبل أحد مواطني الدولة الطرف إذا كانت الجريمة يعاقب عليها حسب القانون الداخلي في مكان ارتكبها أو إذ ارتكبت خارج منطقة الاختصاص القضائي لأية دولة. e. إذا كانت الجريمة تمس أحد المصالح العليا للدولة. 2. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد الاختصاص الذي يغطي الجرائم المنصوص عليها في المادة 31، الفقرة 1 من هذه الاتفاقية في الحالات التي يكون فيها الجاني المزعوم حاضرا في إقليم تلك الدولة الطرف ولا يقوم بتسليمه إلى طرف آخر بناء على جنسيته بعد طلب التسليم. 3. إذا ادعت أكثر من دولة بالاختصاص القضائي لجريمة منصوص عليها في هذه الاتفاقية فيقدم طلب الدولة التي أخلت الجريمة بأمنها أو بمصالحها ثم الدولة التي وقعت الجريمة في إقليم ثم الدولة التي يكون الشخص المطلوب من رعاياها وإذا اتحدت الظروف فتقدم الدولة الأسبق في طلب التسليم. في حالة وجود ظروف مماثلة، تُعطى الأولوية لأول دولة تطلب التسليم.		

التعاون الدولي		
أفضل الممارسات الدولية	**التشريع الوطني**	**ملاحظات**
المادة 43 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات **الهيئات المتخصصة**[112] 1. تكفل كل دولة طرف، وفقا للمبادئ الأساسية لنظامها القانوني، وجود جهاز متخصص ومتفرغ على مدار الساعة لضمان توفير المساعدة الفورية لغايات التحقيق أو الإجراءات المتعلقة بجرائم تقنية المعلومات أو لجمع الأدلة بشكلها الإلكتروني في جريمة معينة ويجب أن تشمل مثل هذه المساعدة تسهيل أو تنفيذ a. توفير المشورة الفنية . ب- حفظ المعلومات استنادا للمادتين السابعة والثلاثين والثامنة والثلاثين .. 2. جمع الأدلة وإعطاء المعلومات القانونية وتحديد مكان المشبوهين . . أ- يجب أن يكون ذلك الجهاز في أي دولة طرف القدرة على الاتصالات مع الجهاز المماثل في دولة طرف أخرى بصورة عاجلة . ب- إذا لم يكن الجهاز المذكور المعين من قبل أي دولة طرف جزءاً من سلطات تلك الدولة الطرف المسؤولة عن المساعدة الثنائية الدولية فيجب على ذلك الجهاز ضمان القدرة على التنسيق مع تلك السلطات بصورة عاجلة .. 3. على كل دولة طرف ضمان توفر العنصر البشري الكفء من أجل تسهيل عمل الجهاز المذكور أعلاه .	**لا يوجد معادل**	**التحليل القانوني** هذه آلية أساسية لتحقيق قدرة فعالة على التحقيق في الجرائم الإلكترونية. **تحليل الفجوة** **التوصيات:** لا ينبغي أن يتطلب ذلك تشريعًا خاصًا لتنفيذه، وفيما يتعلق بالموارد يجب أن تُعطى الأولوية. يجب مشاركة تفاصيل الاتصال لنقطة الاتصال الوحيدة المعينة (SPOC) على المستوى الوطني ومع السلطات المركزية على المستوى الدولي والإنتربول. ينبغي أيضًا النظر في صياغة مذكرة تفاهم مع الوكالات الوطنية بحيث يكون لدى نقطة الاتصال الوحيدة المعينة سلطة القيام بالإجراءات المطلوبة كجزء من تحقيق دولي في جرائم الإنترنت وتطبيق القوانين والمعاهدات الوطنية. ستتضمن مذكرة التفاهم هذه الطلبات الواردة والصادرة وتضمن عملية فعالة وكفؤة.
المادة 25 من اتفاقية بودابست **المبادئ العامة المتعلقة بالمساعدة المتبادلة** 1. يقدم الطرفان المساعدة المتبادلة إلى أقصى حد ممكن لغرض إجراء التحقيقات أو الإجراءات المتعلقة بالجرائم الجنائية المتعلقة بأنظمة الحاسوب والبيانات، أو لجمع الأدلة المتعلقة بالجرائم الجنائية في شكل إلكتروني. 2. يعتمد كل طرف أيضًا الإجراءات التشريعية وغيرها من الإجراءات التي قد تكون ضرورية لتنفيذ الالتزامات المنصوص عليها في المواد من 27 إلى 35.	**القانون رقم 04-09 بتاريخ 14 شعبان 1430 الموافق 5 أغسطس 2009 الذي يضع قواعد محددة بشأن منع ومكافحة الانتهاكات المتعلقة بتكنولوجيا المعلومات والاتصالات** **المادة 16** في سياق التحقيقات أو التحقيقات القضائية في الكشف عن الجرائم التي تدخل في نطاق هذا القانون والبحث عن مرتكبيها، **يجوز للسلطات المختصة الاستعانة بالمساعدة القضائية الدولية للحصول على إثبات في شكل إلكتروني.**	**التحليل القانوني** صدقت الجزائر على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بموجبالمرسوم الرئاسي رقم 252-14 الصادر بتاريخ 2014-09-08 والمنشور في الجريدة الرسمية في العدد 57 عام 2014 تضمن المادة 32 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات أنه يمكن استخدامها كأداة لتسهيل المساعدة القانونية المتبادلة[113] وتنص على الحفظ المستعجل لبيانات الحاسوب المخزنة،[114] والحفظ المستعجل والكشف الجزئي لبيانات المرور،[115] والكشف عن البيانات المخزنة[116] وبيانات الحركة[117] **لدول الاتفاقية.**

112. المادة 35 من اتفاقية بودابست والمادة 25 (2) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية
113. لا يوجد حكم مماثل في اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية
114. المادة 29 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست والمادة 37 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات
115. المادة 30 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست والمادة 38 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات
116. المادة 31 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست والمادة 39 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات
117. المادة 33 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست والمادة 41 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

التعاون الدولي		
أفضل الممارسات الدولية	**التشريع الوطني**	**ملاحظات**
3. يجوز لكل طرف في الظروف العاجلة تقديم طلبات للمساعدة المتبادلة أو الاتصالات المتعلقة بها عن طريق وسائل الاتصال العاجلة، بما في ذلك الفاكس أو البريد الإلكتروني، إلى الحد الذي توفر فيه هذه الوسائل مستويات مناسبة من الأمن والمصادقة (بما في ذلك استخدام التشفير، عند الضرورة)، مع تأكيد رسمي لاحق، حيثما يطلب ذلك الطرف متلقي الطلب. يجب على الطرف متلقي الطلب قبول الطلب والرد عليه بأي وسيلة اتصال سريعة. 4. باستثناء ما هو منصوص عليه على وجه التحديد في المواد الواردة في هذا الفصل، تخضع المساعدة المتبادلة للشروط المنصوص عليها في قانون الطرف متلقي الطلب أو معاهدات المساعدة المتبادلة المطبقة، بما في ذلك الأسباب التي تُجيز للطرف متلقي الطلب أن يرفض التعاون. لا يجوز للطرف متلقي أن يبني حقه في رفض المساعدة المتبادلة المتعلقة بالجرائم المشار إليها في المواد من 2 إلى 11، فقط على أساس أن الطلب يتعلق بجريمة يعتبرها جريمة مالية. 5. عندما تسمح أحكام هذا الفصل للطرف متلقي الطلب بتقييد المساعدة المتبادلة بشرط ازدواجية التجريم، يعتبر هذا الشرط مستوفيًا، بصرف النظر عما إذا كانت قوانينه تضع الجريمة في نفس الفئة الجرمية، أو إذا أعطيت الجريمة نفس التسمية عند الطرف الطالب، وذلك إن كان السلوك الكامن وراء الجريمة التي طلبت المساعدة من أجلها جريمة جنائية بموجب قوانينه.	**في الحالات العاجلة، وعملاً بالاتفاقيات الدولية ومبدأ المعاملة بالمثل، تكون طلبات المساعدة القانونية المتبادلة المشار إليها في الفقرة الفرعية السابقة مقبولة إذا تم تقديمها عن طريق وسائل الاتصال السريعة، مثل الفاكس أو البريد السريع أو الوسائل الإلكترونية شريطة أن توفر هذه الوسائل شروط أمان ومصادقة كافية.** **المادة 17** **يجب الامتثال لطلبات المساعدة المتبادلة في تبادل المعلومات أو عند اتخاذ أي تدبير مؤقت وفقًا للاتفاقيات الدولية ذات الصلة والاتفاقات الثنائية ومبدأ المعاملة بالمثل.** **المادة 18** يُرفض تنفيذ طلب المساعدة إذا كان له تأثير على السيادة الوطنية أو النظام العام. قد يكون تلبية طلبات المساعدة المتبادلة مشروطًا بسرية المعلومات المقدمة أو بشرط عدم استخدامها لأغراض أخرى غير الأغراض المشار إليها في الطلب.	ينص القانون رقم 04-09 بتاريخ 14 شعبان على الطلبات العاجلة وإرسال الأدلة إلى الدولة التي تتلقى الطلب عن طريق البريد الإلكتروني - ولكنه عبارة عن آلية تتيح التعاون الدولي الفعال وتوفير أدوات التحقيق المحددة للجرائم السيبرانية (مثل أوامر التقديم والحفظ) ويكون مطلوبًا **تحليل الفجوة** **التوصيات:** يُطلب من القانون المحلي الحفاظ على بيانات الحاسوب المخزنة على وجه السرعة، والحفظ المستعجل والكشف الجزئي لبيانات الحركة وطلبات النسخ. يمكن استخدام اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست واتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية و الاتفاقية العربية لمكافحة جرائم تقنية المعلومات كسوابق من أجل المحافظة المستعجلة على بيانات الحاسوب المخزنة،[118] والحفظ المستعجل والكشف الجزئي لبيانات الحركة،[119] والكشف عن البيانات المخزنة[120] والجمع المستعجل لبيانات الحركة[121] - هناك حاجة أيضًا للنظر في إمكانية السماح باعتراض بيانات ومحتويات حركة المرور في الوقت الحقيقي[122]. علاوة على ذلك، يجب أن يكون هناك إطار للتعاون في تحقيقات جرائم الإنترنت التي تنص عليها اتفاقيات متعددة الأطراف مثل المادة 27 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست والمادة 32 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.[123] ينبغي النظر في السماح للسلطات المختصة بإعطاء الإذن لهيئات إنفاذ القانون المحلي بإجراء تحقيق في الدولة التي تأكد فيها الوصول إلى الجهاز. يعد الوصول إلى المعلومات هو المعيار الأساسي لبدء التحقيق في الحالات التي يتعذر فيها معرفة مكان تخزين البيانات (أي في التخزين السحابي). يمكن أن يشمل ذلك «اعترافًا متبادلًا» بأوامر المحكمة الصادرة تجاه مقدمي خدمات الاتصالات في دولة معينة، والتي يمكن تقديمها إلى فروع مقدمي خدمة العملاء الموجودين في دول أخرى، اعتمادًا على مكان تخزين البيانات.

118. المادة 29 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست، القسم 23 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية والمادة 37 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات
119. المادة 30 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست، القسمان 23 و 24 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية والمادة 38 الاتفاقية العربية لمكافحة جرائم تقنية المعلومات
120. المادة 31 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست والمادة 39 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات
121. المادة 41 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات
122. المادتان 33 و 34 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست، والقسمان 25 و 26 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية
123. لا توجد أحكام مكافئة بشأن إجراءات المساعدة القانونية المتبادلة في اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 34 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - الإجراءات المتعلقة بطلبات التعاون والمساعدة المتبادلة 1. تطبق بنود الفقرات (2-9) من هذه المادة في حالة عدم وجود معاهدة أو اتفاقية مساعدة متبادلة وتعاون على أساس التشريع النافذ بين الدولة الطرف الطالبة والمطلوب منها، أما في حال وجودها فلا تطبق الفقرات المشار إليها إلا إذا اتفقت الأطراف المعنية على تطبيقها كاملة أو بشكل جزئي 2. a. أ- على كل دولة طرف تحديد سلطة مركزية تكون مسؤولة عن إرسال وإجابة طلبات المساعدة المتبادلة وتنفيذ هذه الطلبات وإيصالها إلى السلطات المعنية لتنفيذها. b. على السلطات المركزية أن تتصل ببعضها مباشرة. c. على كل دولة طرف- وقت التوقيع إو إيداع أدوات التصديق أو القبول أو الموافقة- أن تتصل بالأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس العدل العرب وتنقل إليهما أسماء وعناوين السلطات المحددة خصيصا لغايات هذه الفقرة. d. تقوم الأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس وزراء العدل العرب بإنشاء وتحديث سجل للسلطات المركزية والمعينة من قبل الدول الأطراف . وعلى كل دولة طرف أن تتأكد من أن التفاصيل الموجودة في السجل صحيحة دائما . 3. يتم تنفيذ مطالب المساعدة المتبادلة في هذه المادة حسب الإجراءات المحددة من قبل الدولة الطرف الطالبة لها باستثناء حالة عدم التوافق مع قانون الدولة الطرف المطلوب منها المساعدة 4. يجوز للدولة الطرف المطلوب منها المساعدة أن تؤجل الإجراءات المتخذة بشأن الطلب إذا كانت هذه الإجراءات تؤثر على التحقيقات الجنائية التي تجري من قبل سلطاتها . 5. قبل رفض أو تأجيل المساعدة يجب على الدولة الطرف المطلوب منها المساعدة بعد استشارة الدولة الطرف الطالبة لها أن تقرر فيما إذ سيتم تلبية الطلب جزئيا أو يكون خاضعا للشروط التي قد ترها ضرورية .		

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
6. تلتزم الدولة الطرف المطلوب منها المساعدة ان تعلم الدولة الطرف الطالبة لها بنتيجة تنفيذ الطلب، وإذا تم رفضأو تأجيل الطلب يجب إعطاء أسباب هذا الرفض أو التأجيل، ويجب على الدولة الطرف المطلوب منها المساعدة أن تعلم الدولة الطرف الطالبة لها بالأسباب التي تمنع تنفيذ الطلب بشكل نهائي أو الأسباب التي تؤخره بشكل كبير . 7. يجوز للدولة الطرف الطالبة للمساعدة أن تطلب من الطرف المطلوب منها المساعدة الإبقاء على سرية حقيقة ومضمونأي طلب يندرج في هذا الفصل ما عدا القدر لكافي لتنفيذ الطلب، وإذالم تستطع الدولة الطرف المطلوب منها المساعدة الالتزام بهذا الطلب للسرية يجب عليها إعلام الدولة الطرف الطالبة والتي ستقرر مدى إمكانية تنفيذ الطلب . 8. a. في الحالات العاجلة يجوز إرسال طلبات المساعدة المتبادلة مباشرة إلى السلطات القضائية في الدولة الطرف المطلوب منها المساعدة من نظيرتها في الدولة الطرف الطالبة لها، وفي مثل هذه الحالات يجب إرسال نسخة الوقت من السلطة المركزية في الدولة الطرف الطالبة إلى نظيرتها في الدولة الطرف المطلوب منها. b. يجوز عمل الاتصالات وتقديم الطلبات حسب هذه الفقرة بواسطة الإنتربول. c. حيثما يتم تقديم طلب حسب الفقرة (أ) ولم تكن السلطة مختصة بالتعامل مع الطلب فيجب عليها إحالة الطلب إلى السلطة المختصة وإعلام الدولة الطرف الطالبة للمساعدة مباشرة بذلك . d. إن الاتصالات والطلبات التي تتم حسب هذه الفقرة والتي لا تشمل الإجراء القسري يمكن بثها مباشرة من قبل السلطات المختصة في الدولة الطرف الطالبة للمساعدة إلى نظيرتها في الدولة الطرف المطلوب منها المساعدة. e. يجوز لكل دولة طرف، وقت التوقيع أو التصديق أو القبول أو الإقرار أو الإنضمام إبلاغ الأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس وزراء العدل العرب بأن الطلبات حسب هذه الفقرة يجب توجيهها إلى السلطة المركزية لغايات الفعالية .		

التعاون الدولي		
أفضل الممارسات الدولية	**التشريع الوطني**	**ملاحظات**
المادة 26 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[124] **المعلومات التلقائية** 1. يجوز للطرف، في حدود قانونه الداخلي ودون طلب مسبق، أن يحيل إلى الطرف الآخر المعلومات التي تم الحصول عليها في إطار تحقيقاته، عندما يرى أن الكشف عن هذه المعلومات قد يساعد الطرف المتلقي في بدء أو التحقيقات أو الإجراءات المتعلقة بالجرائم الجنائية المنصوص عليها في هذه الاتفاقية، أو قد تؤدي إلى طلب تعاون من جانب هذا الطرف بموجب هذا الفصل. 2. قبل تقديم هذه المعلومات، يجوز للطرف المقدم أن يطلب الحفاظ على سريتها أو استخدامها فقط وفقًا للشروط. إذا لم يستطع الطرف المتلقي الامتثال لهذا الطلب، فيجب عليه إخطار الطرف المقدم الذي يحدد بعد ذلك ما إذا كان ينبغي تقديم المعلومات. إذا قبل الطرف المتلقي المعلومات وفقًا لهذه الشروط فعليه أن يلتزم بها. **المادة 33 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - المعلومات العرضية المتلقاة** 1. يجوز لأي دولة طرف- ضمن حدود قانونها الداخلي- وبدون طلب مسبق أن تعطي لدولة أخرى معلومات حصلت عليها من خلال تحقيقاتها إذا اعتبرت أن كشف مثل هذه المعلومات يمكن أن تساعد الدولة الطرف المرسلة إليها في إجراء الشروع أو القيام بتحقيقات في الجرائم المنصوص عليها في هذه الاتفاقية أو قد تؤدي إلى طلب للتعاون من قبل تلك الدولة الطرف. 2. قبل إعطاء مثل هذه المعلومات يجوز للدولة الطرف المزودة أن تطلب الحفاظ على سرية المعلومات، وإذا لم تستطع الدولة الطرف المستقبلة الالتزام بهذا الطلب يجب عليها إبلاغ الدولة الطرف المزودة بذلك والتي تقرر بدورها مدى إمكانية التزويد بالمعلومات. وإذا قبلت الدولة الطرف المستقبلة المعلومات مشروطة بالسرية فيجب أن تبقى المعلومات بين الطرفين.	**لا يوجد معادل**	**التحليل القانوني** يعد هذا إجراءً هامًا لمساعدة دولة أخرى في منع الجريمة السيبرانية أو التحقيق فيها. تنص المادة 18 (4) - (5) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة على تبادل المعلومات الاستخباراتية تلقائيًا في الأمور التي تفي بتعريف جريمة خطيرة[125]، ذات طابع عبر وطني[126] وأن جماعة إجرامية منظمة ضالعة في ارتكاب الجرم[127]. ودون استيفاء هذا التعريف، يجب إرسال طلب رسمي عبر قنوات المساعدة القانونية المتبادلة المعتادة. وبسبب الطبيعة السريعة للجريمة السيبرانية، فإن المشاركة وسيلة فعالة للتعاون مع الدول الأخرى، ويؤدي غيابها إلى منع التعاون الدولي الفعال. ويمكن أن يكون هناك مشاركة غير رسمية في انتظار المساعدة القانونية المتبادلة من خلال الاستعانة بقاضي اتصال[128] ولكن لا يوجد أساس تشريعي محلي للمشاركة التلقائية مع دولة أخرى للاستخدام السري لجميع المسائل المتعلقة بالجرائم السيبرانية. **تحليل الفجوة** **التوصيات:** استخدام المادة 18 (4)-(5) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية أساسًا لمشاركة المعلومات (مع ضمانات مقدمة حول الاستخدام في الأدلة أو الكشف عن المعلومات الحساسة لطرف ثالث (بما في ذلك دولة أخرى)).[129] خلاف ذلك، يتعين النظر في التشريعات القائمة على المادة 33 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات أو المادة 26 من اتفاقية بودابست.

124. لا يوجد حكم مماثل في اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية
125. يقصد بتعبير «جريمة خطيرة» في المادة 2 (ب) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة أي سلوك يمثل جرما يعاقب عليه بالحرمان التام من الحرية لمدة لا تقل عن أربع سنوات أو بعقوبة أشد"
126. المادة 3 (1) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية
127. تُعرّف المادة 2 (أ) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية "الجماعة الإجرامية المنظمة" بأنها جماعة ذات هيكل تنظيمي، مؤلفة من ثلاثة أشخاص أو أكثر، موجودة منذ فترة من الزمن وتعمل بصورة متضافرة بهدف ارتكاب واحدة أو أكثر من الجرائم الخطيرة أو الأفعال المجرمة وفقًا لهذه الاتفاقية، من أجل الحصول، بشكل مباشر أو غير مباشر، على منفعة مالية أو منفعة مادية أخرى"
128. تقدم استبيانات المساعدة القانونية المتبادلة الجزائرية نموذجًا بين قضاة الاتصال في فرنسا والجزائر
129. انظر المادة 33 (2) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

التعاون الدولي		
أفضل الممارسات الدولية	**التشريع الوطني**	**ملاحظات**
المادة 32 من اتفاقية بودابست **الوصول عبر الحدود إلى بيانات الحاسوب المخزنة بموافقة أو عندما تكون متاحة للجمهور** يجوز للطرف، دون إذن من طرف آخر: 1. الوصول إلى بيانات الحاسوب المخزنة (مفتوحة المصدر) المتاحة للجمهور، بغض النظر عن مكان وجود البيانات جغرافيا؛ أو 2. الوصول إلى بيانات الحاسوب المخزنة الموجودة لدى طرف آخر أو استلامها، من خلال نظام حاسوب في إقليمها، إذا حصل الطرف على موافقة مشروعة وطوعية من الشخص الذي لديه السلطة القانونية للكشف عن البيانات للطرف من خلال نظام الحاسوب هذا. **القسم 27 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - البرامج الشرعية** 1. إذا كان [القاضي] [قاضي التحقيق] مقتنعًا بناءً على [معلومات مقدمة تحت القَسَم] [شهادة خطية] أنه في سياق تحقيق متعلق بجريمة مدرجة في الفقرة 7 أدناه، توجد أسباب معقولة للاعتقاد بأنه لا يمكن جمع الأدلة الأساسية عن طريق تطبيق أحكام أخرى مدرجة في الجزء الرابع ولكنها ضرورية لأغراض التحقيق الجنائي، فإن [القاضي] [القاضي] [أن] يأذن لضابط [إنفاذ القانون] [الشرطة] بناءً على طلب باستخدام برنامج شرعي عن بعد في مهمة محددة ضرورية للتحقيق وتثبيته في نظام الحاسوب المشتبه به من أجل جمع الأدلة ذات الصلة. يجب أن يحتوي الطلب على المعلومات التالية: • المشتبه في ارتكابه الجريمة، إذا كان ذلك ممكنا مع الاسم والعنوان؛ و • وصف نظام الحاسوب المستهدف؛ و • وصف الوسيلة المقصود ومدى ومدة الاستخدام؛ و • أسباب ضرورة الاستخدام.	**لا يوجد معادل**	**التحليل القانوني** تمكن هذه السلطة الإجرائية الدولة من تأمين المحتوى المخزن في دولة أخرى في ظروف محدودة. إن المادة 32.ب من اتفاقية بودابست والمادة 40 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات هما استثناء من مبدأ الإقليمية وتسمحان بوصول منفرد عبر الحدود دون الحاجة إلى مساعدة قانونية متبادلة عندما تكون هناك موافقة أو تكون المعلومات متاحة للجمهور. من أمثلة استخدام هذه القوة الإجرائية بموجب المادة 32 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست: قد يتم تخزين البريد الإلكتروني لشخص ما في بلد آخر بواسطة مزود خدمة، أو قد يقوم شخص ما بتخزين البيانات عن قصد في بلد آخر. يجوز لهؤلاء الأشخاص استرداد البيانات بشرط أن يكون لديهم السلطة القانونية التي تخولهم ذلك، ويجوز لهم الكشف طوعًا عن البيانات لموظفي إنفاذ القانون أو السماح لهؤلاء المسؤولين بالوصول إلى البيانات[130] يمكن اعتقال إرهابي مشتبه به بشكل قانوني عندما يكون بريده الإلكتروني، الذي قد يحوي دليلًا على ارتكاب جريمة، مفتوحًا على الجهاز اللوحي أو الهاتف الذكي أو أي جهاز آخر. إذا وافق المشتبه طوعًا على وصول الشرطة إلى الحساب وإذا كانت الشرطة متأكدة من وجود بيانات صندوق البريد في ولاية أخرى، يجوز للشرطة الوصول إلى البيانات بموجب المادة 32. ب. **تحليل الفجوة** **التوصيات:** تم تضمين هذه السلطة التي تؤمن الأدلة من طرف واحد في التشريعات مع ضمانات الحصول على الموافقة بشكل قانوني من المستخدم.[131] يمكن استخدام لغة المادة 32 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست والمادة 40 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. تم انتقاد المادة 32.ب بشدة، ويمكن اعتبار أن موافقة الدولة حيث تُخزَّن بيانات الحاسوب قد تم الحصول عليها بالإضافة إلى المستخدم. ينص القسم 27 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية على البرامج الشرعية وهذا قد يسمح بالوصول إلى جهاز حاسوب في دولة أخرى. هناك عدد من القيود التي تشترط عدم إمكانية الحصول على الأدلة بوسائل أخرى، وتتطلب أمرًا قضائيًا، ويمكن أن تُطبَّق على جرائم معينة فقط ضمن مدة مقيدة (3 أشهر). يجب أيضًا إيلاء الاعتبار لموافقة الدولة الأخرى التي قد يتطفل عليها البرنامج الشرعي.

130. التقرير التفسيري للفقرة 294 في اتفاقية بودابست
131. يجب الانتباه لمواقف مثل عدم وجود المستخدم (في حالة الوفاة) وإذا كان يمكن الحصول على موافقة في دولة أخرى

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
2. من الضروري التأكد في مثل هذا التحقيق من أن التعديلات التي يتم إدخالها على نظام الحاسوب الخاص بالمشتبه به مقصورة على تلك الضرورية للتحقيق وأن أي تغييرات يمكن التراجع عنها إذا أمكن بعد نهاية التحقيق. أثناء التحقيق، من الضروري تسجيل الدخول • الوسيلة الفنية المستخدمة ووقت وتاريخ التطبيق؛ و • تحديد نظام الحاسوب وتفاصيل التعديلات التي أجريت في التحقيق؛ • أي معلومات تم الحصول عليها. يجب حماية المعلومات التي يتم الحصول عليها عن طريق استخدام هذا البرنامج من أي تعديل أو حذف غير مصرح به أو وصول غير مصرح به. 3. تقتصر مدة الترخيص في القسم 27 (1) على [3 أشهر]. يتم إيقاف الإجراء المتخذ على الفور إذا لم تعد شروط الترخيص مستوفاة. 4. يتضمن ترخيص تثبيت البرنامج الوصول عن بُعد إلى نظام الحاسوب المشتبه به. 5. إذا كانت عملية التثبيت تتطلب الوصول الفعلي إلى مكان ما، يجب استيفاء متطلبات القسم 20. 6. يجوز لضابط [تطبيق القانون] [الشرطة] أن يطلب من المحكمة أن تأمر مقدم خدمة بالمساعدة في عملية التسليم إذا لزم الأمر، وذلك بموجب أمر المحكمة الممنوح في (1) الطلب المذكور أعلاه. 7. [قائمة الجرائم]. 8. قد تقرر دولة عدم تنفيذ القسم 27. **المادة 40 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - الوصول إلى معلومات تقنية المعلومات عبر الحدود** يجوز لأي دولة طرف، وبدون الحصول على تفويض من دولة طرف أخرى: 1. أن تصل إلى معلومات تقنية المعلومات المتوفرة للعامة (مصدر مفتوح) بغض النظر عن الموقع الجغرافي للمعلومات. 2. أن تصل أو تستقبل- من خلال تقنية المعلومات في إقليمها- معلومات تقنية المعلومات الموجودة لدى الدولة الطرف الأخرى وذلك إذا كانت حاصلة على الموافقة الطوعية والقانونية من الشخص الذي يملك السلطة القانونية لكشف المعلومات إلى تلك الدولة الطرف بواسطة تقنية المعلومات المذكورة.		

مصر

صدقت مصر على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في 14 أغسطس 2018، وأصدرت القانون 175/2018 المتعلق بمكافحة جرائم تقنية المعلومات. ينظم قانون مكافحة الجرائم الإلكترونية النشاطات التي على الإنترنت، ويهدف وفقًا لبيان رسمي إلى لإكمال قانون الصحافة والإعلام الجديد الذي يجرّم، بين أمور أخرى، نشاطات الإنترنت غير المرخص بها وانتهاكات المحتوى، مثل الأخبار الكاذبة. يسعى فريق يورميد للعدالة لأن تكون المعلومات محدّثة وصحيحة؛ غير أنه لم يكن ممكنًا إجراء تحليل لأحكام 2018 القانونية الجديدة في هذه المرحلة بسبب القيود التي يفرضها وقت المشروع الحالي وموارده؛ بعض التعديلات التي نص القانون على العمل بها موجودة في كتيب أدلة يوروميد الرقمية.

الجرائم

أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 2 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست - الوصول غير المشروع[132] يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لتجريم الوصول إلى النظام الكلي أو أي جزء من نظام الحاسوب، إذا ارتكب عمدًا، دون أي حق. قد يشترط طرف ما ارتكاب الجريمة عن طريق انتهاك إجراءات أمنية بقصد الحصول على بيانات الحاسوب أو نية أخرى غير نزيهة، أو فيما يتعلق بنظام كمبيوتر متصل بنظام كمبيوتر آخر. **القسم 4 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الوصول غير القانوني** يعاقب بالسجن لمدة لا تتجاوز [المدة] أو غرامة لا تتجاوز [المبلغ] أو بالعقوبتين معاً أي شخص يدان بجريمة الوصول إلى نظام حاسوب كله أو جزء منه عن قصد ودون عذر مبرر قانونًا أو بتجاوز لسبب قانوني. قد تقرر أي دولة عدم تجريم الوصول غير المصرح به بشرط توفر سبل انتصاف فعالة أخرى. علاوة على ذلك، قد يشترط بلد ما ارتكاب الجريمة عن طريق انتهاك الإجراءات الأمنية أو بقصد الحصول على بيانات الحاسوب أو بنية أخرى غير نزيهة.	**لا يوجد معادل**	**التحليل القانوني** تشير الاتفاقية العربية لمكافحة جرائم تقنية المعلومات إلى «الوصول غير المشروع أو التواجد أو الاتصال بـ" دون تحديد معنى هذه الأفعال. تشير اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست إلى «بغير حق" في المادة 2 على أساس أن الوصول غير مصرح به. أكد التقرير التفسيري لاتفاقية بودابست اشتقاق عبارة "بدون حق" مثل، "التصرف الذي تم دون سلطة (سواء كانت تشريعية أو تنفيذية أو إدارية أو قضائية أو تعاقدية أو توافقية) أو تصرفًا لا يشمله، بأي حال، الدفوع القانونية أو الأعذار أو المبررات أو المبادئ ذات الصلة بموجب القانون المحلي"[133] تقدم أقسام التعليق في التشريع النموذجي[134] لاتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية، شرحًا لشرط "بدون عذر أو مبرر قانوني" على النحو التالي، "تمكن ملاحقة الوصول إلى نظام الحاسوب وفقًا للمادة 4 فقط، وفي حالة حدوث ذلك "دون عذر أو مبرر قانوني". ويتطلب ذلك أن يتصرف الجاني دون سلطة (سواء كانت تشريعية أو تنفيذية أو إدارية أو قضائية أو تعاقدية أو توافقية) وأن الدفوع القانونية أو الأعذار أو المبررات أو المبادئ ذات الصلة لا تبرر تصرفه. إن الوصول إلى نظام يسمح بالوصول المجاني والمفتوح للجمهور أو الوصول إلى نظام بإذن من المالك أو غيره من أصحاب الحقوق لا يعتبر بالتالي جريمة. لا يرتكب مسؤولو الشبكات وشركات الأمان الذين يختبرون حماية أنظمة الحاسوب من أجل تحديد الثغرات المحتملة في التدابير الأمنية عملاً إجرامياً".

132. المادة 6 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، والمادة 29 (1) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية
133. الفقرة 38، الصفحة 8 من التقرير التوضيحي لاتفاقية الجريمة الإلكترونية - رقم 185 https://rm.coe.int/16800cce5b
134. صفحة 30 قسم الشرح في اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية، النموذج التشريعي

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
القسم 5 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الآثار غير القانونية أي شخص يظل مسجلاً في نظام حاسوب أو جزء من نظام حاسوب أو يواصل استخدام نظام حاسوب عن قصد ودون عذر أو مبرر قانوني، أو يتجاوز عذرًا أو مبررًا قانونيًا يعاقب عند إدانته بالسجن لمدة لا تتجاوز [المدة]، أو غرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً. قد تقرر أي دولة عدم تجريم الآثار غير المصرح بها فقط، شرط أن تتوفر سبل انتصاف فعالة أخرى. بدلاً من ذلك، قد يشترط البلد ارتكاب الجرم عن طريق انتهاك الإجراءات الأمنية أو بقصد الحصول على بيانات الحاسوب أو بنية أخرى غير نزيهة.		تشير المادة 6 من الاتفاقية إلى "الوصول غير المشروع أو الوجود أو الاتصال بـ" دون تحديد ما تعنيه هذه الأفعال، لذلك يفضل استخدام اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست واتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية. **تحليل الفجوة** **التوصيات:** يمكن أن يتضمن التشريع الوطني الصياغة ذات الصلة من المادة 2 في اتفاقية بودابست / القسمان 4 و5 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية لتشمل تعاريف نظام الحاسوب وإدراج البرامج ضمن تعريف البيانات لأن بعض البيانات تشمل البرامج والبعض الآخر لا تشملها. علاوة على ذلك، ولكي تتماشى التشريعات مع المعايير الدولية، ينبغي أن يشير التشريع إلى الوصول "بغير حق" بدلاً من عن طريق الاحتيال. يجب أيضًا الأخذ بعين الاعتبار النص على جريمة منفصلة تشكلها الآثار الباقية في نظام الحاسوب وفقًا للمادة 5 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية.
المادة 3 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[135] **اعتراض غير قانوني** يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وتدابير أخرى لتجريم اعتراض عمليات نقل البيانات الحاسوبية غير العامة من نظام حاسوب وإليه وداخله، بما في ذلك الانبعاثات الكهرومغناطيسية من نظام الحاسوب الذي يحمل مثل هذه البيانات، وذلك عند ارتكاب هذا العمل عمدًا بوسائط تقنية، ويعتبر جريمة جنائية بموجب القانون الداخلي. قد يشترط الطرف أن تكون الجريمة قد ارتكبت بنية غير نزيهة، أو أن تتم ضد نظام حاسوب متصل بنظام حاسوب آخر. **القسم 6 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - اعتراض غير قانوني** 1. الشخص الذي يتعمد اعتراض الوسائل التقنية دون عذر أو مبرر قانوني أو يتجاوز عذرًا أو مبررًا قانونيًا: • أي نقل غير عام إلى نظام الحاسوب أو منه أو داخله؛ أو • الانبعاثات الكهرومغناطيسية من نظام الحاسوب	**القانون الجنائي رقم 58/1937** **المادة 309 مكرر** **قانون الاتصالات رقم 10 لسنة 2003** **المادة 73**	**التحليل القانوني** يُعتبر تجريم هذا الفعل ضروريًا لمقاضاة عمليات نقل بيانات الحاسوب من وإلى وداخل نظام الحاسوب الذي قد يتم اعتراضه بشكل غير قانوني للحصول على معلومات (مثل wikileaks أو PanamaPapers). المادة 309 مكرر من القانون الجنائي ليست خاصة بالتكنولوجيا السيبرانية. يمكن استخدام المادة 309 مكرر، إلى جانب المادة 73 ب من قانون الاتصالات رقم 10 لسنة 2003 من جانب النيابة العامة والمحاكم الاقتصادية لاعتراض الحاسوب غير القانوني. **تحليل الفجوة** **التوصيات:** استخدم لغة اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست في المادة 3، والقسم 6 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية باعتبارهما دليلًا؛ اللغة المستخدمة في المادة 7 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات مناسبة، وإن لم يكن هناك تعريف لـ "بيانات تكنولوجيا المعلومات"

135. المادة 29 (2) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية

الجرائم		
أفضل الممارسات الدولية	**التشريع الوطني**	**ملاحظات**
يعتبر جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً. 2. قد يشترط البلد ارتكاب الجرم بنية غير شريفة، أو ضد نظام حاسوب متصل بنظام حاسوب آخر أو عن طريق التحايل على إجراءات الحماية المطبقة لمنع الوصول إلى محتوى الإرسال غير العام. **المادة 7 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست** **اعتراض غير قانوني** الاعتراض غير القانوني المتعمد لحركة البيانات بأي وسيلة تقنية، وتعطيل نقل أو استقبال بيانات تكنولوجيا المعلومات.		
المادة 4 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[136] **التشويش على البيانات** يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لكي تجرم قوانينها الوطنية محو بيانات الحاسوب أو إتلافها أو تغييرها أو حذفها دون حق، وذلك عند ارتكابها عمدًا. 2أ يجوز لأي طرف أن يحتفظ بالحق في المطالبة بأن يؤدي السلوك الموصوف في الفقرة 1 إلى ضرر جسيم. **القسم 7 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية- التشويش غير القانوني على البيانات** الشخص الذي يقوم بأي من الأفعال التالية عمدا ودون عذر أو مبرر قانوني أو يتجاوز عذرًا أو مبررًا قانونيًا: • محو أو إتلاف بيانات الحاسوب؛ أو • حذف بيانات الحاسوب؛ أو • تغيير بيانات الحاسوب؛ أو • جعل بيانات الحاسوب بلا معنى لها أو غير ذات فائدة أو غير فعالة؛ أو • يعوق أو يقاطع أو يشوش على الاستخدام القانوني لبيانات الحاسوب؛ أو • يعوق أو يقاطع أو يشوش على أي شخص في استخدامه القانوني لبيانات الحاسوب؛ أو • يمنع الوصول إلى بيانات الحاسوب لأي شخص مصرح له بالوصول إليها؛	**لا يوجد معادل**	**التحليل القانوني** على النحو الوارد أعلاه، وفيما يتعلق بالوصول غير المشروع، لا توجد إشارة في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات إلى "بغير حق" ولا تشمل حذف بيانات الحاسوب التي تعد عنصرا من عناصر التصيد الاحتيالي للحصول على وصول غير قانوني عن طريق تثبيت مسجل أساسي للحصول على معلومات حساسة.[137] **تحليل الفجوة** **التوصيات:** يمكن تصحيح نقص بعض العناصر الرئيسة المتعلقة بهذه الجريمة في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات باستخدام لغة المادة 4 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست أو القسم 7 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية.

136. المادة 29 (1) (هـ - و) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية
137. http://www.coe.int/en/web/cybercrime/guidance-notes

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
يعتبر جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً. **المادة 8 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست** **جريمة ضد سلامة البيانات** 1. تعمد محو أو حذف أو منع أو تعديل أو إخفاء بيانات تكنولوجيا المعلومات بشكل غير قانوني. 2. قد يطلب أحد الأطراف أن يتسبب الفعل بأضرار جسيمة من أجل تجريم الأفعال المذكورة في الفقرة 1.		
المادة 5 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[138] **التشويش على النظام** يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لتمكين سلطاته المختصة من تجريم الأفعال التالية عند ارتكابها عمداً، بموجب قانونه الداخلي، أية عرقلة خطيرة دون حق لعمل نظام الحاسوب عن طريق إدخال أو نقل أو إتلاف أو حذف أو محو أو تغيير أو كتم بيانات الحاسوب. **القسم 9 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - التشويش غير القانوني على النظام** 1. الشخص الذي يقوم عن قصد، ودون عذر أو مبرر قانوني، أو بتجاوز عذر أو مبرر قانوني: • أعاقة عمل نظام الحاسوب أو التشويش عليه؛ أو • إعاقة شخص يستخدم أو يشغل بشكل قانوني نظام الحاسوب أو التشويش عليه؛ يعتبر جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً.	**لا يوجد معادل**	**التحليل القانوني** تجريم هذه الأعمال من شأنه أن يمنع البرامج الضارة التي تتداخل مع عمل جهاز الحاسوب - على سبيل المثال ديدان الحاسوب - مجموعة فرعية من البرامج الضارة (مثل فيروسات الحاسوب). إنها برامج حاسوب ذاتية النسخ المتماثل تضر بالشبكة من خلال بدء عمليات نقل البيانات المتعددة. يمكن أن تؤثر على أنظمة الحاسوب عن طريق إعاقة التشغيل السلس لنظام الحاسوب، أو استخدام موارد النظام لتكرار نفسها عبر الإنترنت أو توليد حركة مرور في الشبكة يمكن أن تغلق بعض الخدمات (مثل المواقع الإلكترونية). **تحليل الفجوة** **التوصيات:** استخدم لغة اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست في المادة 5 أو القسم 9 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية باعتبارهما دليلًا للتشريعات الوطنية. ضع في اعتبارك أيضًا ما إذا كان منع ومكافحة الهجمات ضد البنية التحتية الحيوية يحتاج إلى جريمة منفصلة أو مشددة (القسم 9 (2) من بروتوكول مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية)، على سبيل المثال، قد يتم إعاقة عمل نظام الحاسوب لأغراض إرهابية (يمكن أن تؤدي إعاقة النظام الذي يخزن سجلات البورصة إلى أن تكون البيانات غير دقيقة، أو أن تعيق عمل البنية التحتية الحيوية).[139]

138. لا يوجد ما يعادل المادة 29 (1) (د) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات
139. http://www.coe.int/en/web/cybercrime/guidanotes

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
2. يعاقب أي شخص الذي يتعمد دون عذر أو مبرر قانوني، أو بتجاوز عذر قانوني أو مبرر، إعاقة نظام حاسوب مخصص حصريًا لاستخدام عمليات البنية التحتية الحيوية أو التشويش عليه، أو في الحالات التي لا يكون فيها هذا النظام مخصصًا للاستخدام الحصري في عمليات البنية التحتية الحيوية، ولكنه يستخدم في عمليات البنية التحتية الحيوية وتؤثر هذه الإعاقة على استخدام عمليات البنية التحتية الحيوية، بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً.		
المادة 6 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[140] **سوء استخدام الأجهزة** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لتجريم الأفعال الإجرامية بموجب قوانينه الداخلي، عندما تُرتكب عمداً ودون حق: a. أ. إنتاج أو بيع أو الشراء بغرض الاستخدام أو الاستيراد أو التوزيع أو توفير ما يلي بأية طريقة: – أي جهاز، بما في ذلك برنامج الحاسوب، تم تصميمه أو تكييفه بشكل أساسي بغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من 2 إلى 5؛ – كلمة مرور الحاسوب أو رمز الوصول أو البيانات المماثلة التي يمكن من خلالها الوصول إلى نظام الحاسوب كله أو جزء منه، بقصد استخدامه لغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من 2 إلى 5؛ و – حيازة عنصر مشار إليه في الفقرتين أ.1 أو 2 أعلاه، بقصد استخدامه لغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من 2 إلى 5. يجوز لأي طرف أن يشترط بموجب القانون امتلاك عدد من هذه العناصر قبل إسناد المسؤولية الجنائية.	**لا يوجد معادل**	**التحليل القانوني** كما ذكر أعلاه للوصول غير المشروع، لا توجد إشارة إلى "بدون حق" ستمكّن تجريم هذه الأفعال من ملاحقة إنتاج وبيع والشراء من أجل الاستخدام واستيراد وتوزيع رموز الوصول والبيانات المحوسبة الأخرى المستخدمة في ارتكاب جرائم الإنترنت. فمثلًا يمكن الوصول إلى أنظمة الحاسوب لتسهيل أي هجوم إرهابي بالتدخل في شبكة الطاقة الكهربائية للبلد. يجب أن تأخذ أي جريمة في الاعتبار تلك الأجهزة التي لها استخدام شرعي وكذلك للاستخدام الجنائي ("الاستخدام المزدوج") – ينبغي أن يشمل ذلك اللغة المستخدمة في اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست "المكيف بشكل أساسي" **تحليل الفجوة** **التوصيات:** استخدام صياغة اتفاقية بودابست في المادة 6 أو القسم 10 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية باعتبارهما دليلاً للتشريعات الوطنية. يرجى ملاحظة أن مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية توفر خيار إدراج الأجهزة في جدول إذا كان ذلك مناسبًا - قد يكون هذا تقييدًا ويتطلب تحديثًا يتوافق مع التقدم التكنولوجي. يجب أن يوفر القانون الوطني عذرًا معقولًا حتى تتمكن أجهزة إنفاذ القانون من استخدام الأجهزة لتقنيات التحقيق الخاصة - راجع اللغة في المادة 6.2. اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست أو القسم 10 (2) من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية باعتبارهما دليلاً.

140. المادة 9 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات والمادة 29 (1) (ح) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
2. لا يجوز تفسير هذه المادة على أنها تفرض مسؤولية جنائية عندما لا يكون الغرض من الإنتاج أو البيع أو الشراء بغرض الاستخدام أو الاستيراد أو التوزيع أو التوفير أو حيازة المشار إليه في الفقرة 1 من هذه المادة ارتكاب جريمة منصوص عليها وفقًا للشروط المواد من 2 إلى 5 من هذه الاتفاقية، مثل الاختبارات المسموح بها أو حماية نظام الحاسوب. 3. يجوز لكل طرف أن يحتفظ بالحق في عدم تطبيق الفقرة 1 من هذه المادة، شريطة أن لا يتعلق التحفظ ببيع أو توزيع أو توفير المواد المشار إليها في الفقرة 1 أ من هذه المادة بطريقة أخرى **القسم 10 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الأجهزة غير القانونية** 1. يرتكب الشخص جريمة إذا: a. أنتج أو باع أو اشترى بغرض الاستخدام أو استورد أو صدّر أو وزع أو وفّر بأي طريقة، عن قصد ودون عذر أو مبرر قانوني أو بتجاوز عذر أو مبرر قانوني: 1. جهاز بما في ذلك برنامج حاسوب، تم تصميمه أو تكييفه بغرض ارتكاب جريمة محددة بموجب أحكام أخرى من الجزء الثاني من هذا القانون؛ أو b. كلمة مرور الحاسوب أو رمز الوصول أو البيانات المماثلة التي يمكن من خلالها الوصول إلى نظام الحاسوب كله أو جزء منه بقصد استخدامه من قبل أي شخص لغرض ارتكاب جريمة محددة بموجب أحكام أخرى من الجزء الثاني من هذا القانون؛ أو ب. كان في حوزته غرض مشار إليه في الفقرة الفرعية «1» أو «2»، وكان القصد هو استخدامه من قبل أي شخص لارتكاب جريمة محددة بموجب أحكام أخرى من الجزء الثاني من هذا القانون، فإنه يعاقب عند إدانته بارتكاب هذه الجريمة بالسجن لمدة لا تزيد عن [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً.		

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
2. لا يجوز تفسير هذا الحكم على أنه يفرض مسؤولية جنائية عندما لا يكون الغرض من الإنتاج أو البيع أو الشراء للاستخدام أو الاستيراد أو التوزيع أو التوفير أو الحيازة المشار إليها في الفقرة 1 هو ارتكاب جريمة منصوص عليها وفقًا لأحكام أخرى من الجزء الثاني من هذا القانون، كأن تكون الأغراض مثل الاختبار أو الحماية المعتمدين لنظام الحاسوب. 3. قد يقرر بلد ما عدم تجريم الأجهزة غير القانونية أو قصر التجريم على الأجهزة المدرجة في الجدول.		
المادة 7 من اتفاقية بودابست **أعمال التزوير المرتبطة بالحاسوب** يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم إدخال بيانات الحاسوب أو تغييرها أو حذفها أو محوها، عند ارتكاب ذلك عن قصد وبدون حق، مما يؤدي إلى بيانات غير موثوقة بهدف أن يتم التعامل معها أو التصرف فيها لأغراض قانونية كما لو كانت أصلية، بصرف النظر عما إذا كانت البيانات قابلة للقراءة ومقروءة مباشرة أم لا. قد يطلب طرف ما وجود نية الاحتيال، أو نية غير شريفة مماثلة، قبل إسناد المسؤولية الجنائية. **القسم 11 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - أعمال التزوير المتعلقة بالحاسوب** 1. كل شخص يقوم عن قصد ودون عذر أو مبرر قانوني أو بتجاوز عذر قانوني أو مبرر، بإدخال أو تبديل أو حذف أو منع بيانات الحاسوب، مما ينتج عنه بيانات غير موثوقة بقصد التعامل معها أو التصرف فيها لأغراض قانونية كما لو كانت صحيحة، بصرف النظر عما إذا كانت البيانات قابلة للقراءة مباشرة أم لا، يعاقب عند الإدانة بهذه الأعمال بالسجن لمدة لا تزيد عن [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً. 2. تكون العقوبة إذا ارتكبت الجريمة المذكورة أعلاه عن طريق إرسال رسائل بريد إلكتروني متعددة من أنظمة الحاسوب أو من خلالها هي السجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً.	**القانون رقم 10/2003** **المادة 73** يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر وبغرامة لا تقل عن خمسة آلاف جنيه ولا تجاوز خمسين ألف جنيه أو بإحدى هاتين العقوبتين، كل من قام أثناء تأدية وظيفته في مجال الاتصالات أو بسببها بأحد الأفعال الآتية: إذاعة أو نشر أو تسجيل لمضمون رسالة اتصالات أو لجزء منها دون أن يكون له سند قانوني في ذلك. إخفاء أو تغيير أو إعاقة أو تحوير أية رسالة اتصالات أو لجزء منها تكون قد وصلت إليه. الامتناع عمدًا عن إرسال رسالة اتصالات بعد تكليفه بإرسالها. إفشاء أية معلومات خاصة بمستخدمي شبكات الاتصال أو عما يجرونه أو ما يتلقونه من اتصالات وذلك دون وجه حق.	**التحليل القانوني** المادة 73 لها نطاق ضيق إذا ما قورنت بأفضل الممارسات الدولية، حيث إنها لا تجرّم سوى أعمال التزوير ذات الصلة بالحاسوب بالنسبة للأفراد الذين يرتكبون هذه الجريمة أثناء العمل في مجال الاتصالات. ينصح بدمج المادة 7 من اتفاقية بازل، المادة 11 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية أو القسم 29 (2)(ب) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية، من أجل الحماية من المخالفات التي قد تشمل التصيد الاحتيالي والتصيد الاحتيالي بالرمح على سبيل المثال، قد يتم إدخال بيانات الحاسوب(مثل البيانات المستخدمة في جوازات السفر الإلكترونية) أو تغييرها أو حذفها أو إلغاؤها، مما يؤدي إلى تصديق البيانات غير الموثوقة أو التعامل معها لأغراض قانونية كما لو كانت صحيحة.[141] ينص القسم 11 (2) من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية أيضًا على إرسال رسائل بريد إلكتروني متعددة باعتبارها جريمة مشددة. لا تشير اللغة في المادة 10 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات إلى أي نية غير شريفة وتشترط التسبب في ضرر - اللغة المستخدمة في اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست ومواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية هي الأفضل لأنها لا تشترط حدوث ضرر. تشترط اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست ومواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية فقط أن "البيانات الزائفة" "تعتبر" حقيقية

141. http://www.coe.int/en/web/cybercrime/guidance-notes

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 10 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست **جريمة التزوير** يعني استخدام تقنية المعلومات تغيير حقيقة البيانات بطريقة تسبب الضرر بغرض استخدامها كبيانات حقيقية. **المادة 29 (2)(ب) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية** تعمد إدخال بيانات الحاسوب أو تغييرها أو حذفها أو منعها، مما يؤدي إلى بيانات غير موثوقة بقصد التعامل معها أو التصرف فيها لأغراض قانونية كما لو كانت أصلية، بصرف النظر عما إذا كانت البيانات قابلة للقراءة أو واضحة بشكل مباشر أم لا. يجوز للطرف أن يشترط النية للاحتيال، أو نية غير شريفة مماثلة، قبل إسناد المسؤولية الجنائية		**تحليل الفجوة** **التوصيات:** استخدم لغة اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست في المادة 7، القسم 11 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية أو 29 المادة (2) (ب) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية دليلًا للتشريعات الوطنية
المادة 8 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[142] **الاحتيال المرتبط بالحاسوب** يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وتدابير أخرى لتجريم الأفعال التالية بموجب قوانينه الداخلية، عند ارتكابها عمداً ودون حق، بما يسبب فقدان الممتلكات لشخص آخر عن طريق: أي إدخال أو تغيير أو حذف أو إلغاء لبيانات الحاسوب، أي تدخل في عمل نظام الحاسوب، مع نية احتيال أو نية غير شريفة من أجل الحصول، دون حق، على منفعة اقتصادية لنفسه أو لشخص آخر. **القسم 12 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الاحتيال المرتبط بالحاسوب** الشخص الذي يتسبب في فقدان الممتلكات لشخص آخر، عن قصد، ودون عذر أو مبرر قانوني أو بتجاوز عذر أو مبرر قانوني، وذلك عن طريق: • أي إدخال أو تغيير أو حذف أو إلغاء لبيانات الحاسوب؛ • أي تدخل في عمل نظام الحاسوب، بقصد احتيالي أو غير شريف للحصول، دون حق، على منفعة اقتصادية لنفسه أو لشخص آخر، وتكون عقوبة هذه الأعمال السجن لمدة لا تتجاوز [المدة]، أو غرامة لا تتجاوز [المبلغ]، أو العقوبتين معاً.	**لا يوجد معادل**	**التحليل القانوني** اللغة في المادة 11 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات و المادة 29 (2) (د) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية غامضة مع عدم وجود إشارة إلى أي نية غير شريفة وتتطلب وقوع شكل من أشكال «الضرر" (الاتفاقية العربية لمكافحة جرائم تقنية المعلومات) أو حصول «منفعة» (اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية) دون تحديد ماهيته **تحليل الفجوة** **التوصيات:** تقديم تعريفات لعبارات «البيانات" و"نظام المعالجة الآلي"، بما في ذلك "بدون إذن" - تعتبر الصياغة الموجودة في اتفاقية بودابست أو مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية لهذه الجريمة دليلاً جيدًا للتشريع الوطني

142. المادة 11 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات والمادة 29 (2) (د) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 9[143] **الجرائم ذات الصلة بالمحتوى (مثل المواد الإباحية للأطفال)** 1. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم السلوك التالي في قوانينه المحلية، عندما يرتكب عمدا وبدون حق: a. إنتاج مواد إباحية للأطفال بغرض توزيعها من خلال نظام حاسوب؛ b. عرض أو إتاحة مواد إباحية للأطفال من خلال نظام الحاسوب؛ c. توزيع أو نقل المواد الإباحية للأطفال من خلال نظام الحاسوب؛ d. شراء مواد إباحية للأطفال من خلال نظام حاسوب بقصد الاستخدام الشخصي أو لإعطائها لشخص آخر؛ e. امتلاك مواد إباحية للأطفال في نظام حاسوب أو على وسائط تخزين بيانات الحاسوب. 2. لأغراض الفقرة 1 أعلاه، يجب أن يشمل مصطلح «استغلال الأطفال في المواد الإباحية» أية مواد إباحية تصور بصريًا: a. قاصر مشترك في سلوك جنسي صريح؛ b. شخص يبدو أنه قاصر يشارك في سلوك جنسي صريح؛ c. صور واقعية تمثل قاصرًا مشاركًا في سلوك جنسي صريح. 3. لأغراض الفقرة 2 أعلاه، يشمل مصطلح «القاصر» جميع الأشخاص الذين تقل أعمارهم عن 18 عامًا. ومع ذلك، يجوز لأي طرف أن يطلب حدًا أدنى للسن، لا يقل عن 16 عامًا. 4. يجوز لكل طرف أن يحتفظ بالحق في عدم تطبيق الفقرات الفرعية 1، د. و ه، و 2، الفقرتين الفرعيتين ب. و ج كليًا أو جزئيًا. **القسم 3 (4) من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - تعريف المواد الإباحية التي يظهر فيها أطفال** 1. المواد الإباحية التي يظهر فيها أطفال تعني المواد الإباحية التي تصور أو تعرض أو	**قانون الطفل المعدل بالقانون 126 لسنة 2008** **المادة 116 مكرر (ب)** كل من استورد أو أصدر أو أنتج أو أعد أو عرض أو طبع أو روج أو حاز أو بث أي أعمال إباحية يشارك فيها أطفال أو تتعلق بالاستغلال الجنسي للطفل... ومع عدم الإخلال بأي عقوبة أشد ينص عليها في قانون آخر، يعاقب بذات العقوبة كل من: استخدم الحاسب الآلي أو الإنترنت أو الرسوم المتحركة لإعداد أو لحفظ أو لمعالجة أو لعرض أو لطباعة أو لنشر أو لترويج أنشطة أو أعمال إباحية تتعلق بتحريض الأطفال أو استغلالهم في الدعارة والأعمال الإباحية أو التشهير بهم أو بيعهم استخدم الحاسب الآلي أو الإنترنت أو الرسوم المتحركة لتحريض الأطفال علي الانحراف أو لتسخيرهم في ارتكاب جريمة أو علي القيام بأنشطة أو أعمال غير مشروعة أو منافية للآداب، ولو لم تقع الجريمة فعلاً	**التحليل القانوني** لا تشمل هذه الجريمة حيازة المواد أو عرضها أو توفيرها أو إتاحة شرائها لشخص آخر. لا يوجد تعريف لمصطلحات "المواد الإباحية" أو"الحاسوب" - لا يتضح إذا كان هذا يشمل أيضًا نظام الحاسوب أو وسائط التخزين على الحاسوب؟ قد يعني هذا أنه إذا تم تخزين المواد الإباحية التي يظهر فيها أطفال على ذاكرة USB (أو أي وسائط تخزين أخرى)، فلا توجد أي مخالفة. **تحليل الفجوة** **التوصيات:** الصياغة في المادة 9.2 من اتفاقية بودابست أو القسم 3 (4) من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية هو دليل لتعريف المواد الإباحية التي يظهر فيها أطفال المادة 9.1 د و هـ من اتفاقية بودابست أو القسم 13 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية دليل على جرائم سعي الشخص للحصول على مواد إباحية عن الأطفال لنفسه أو لغيره وتخزينها على نظام الحاسوب أو وسائط التخزين على الحاسوب.

143. المادة 29 (3) (أ-د) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية

الجرائم		
أفضل الممارسات الدولية	**التشريع الوطني**	**ملاحظات**
تظهر: a. طفلاً وهو يمارس سلوكًا جنسيًا واضحًا؛ b. شخصًا يبدو كطفل وهو يمارس سلوكًا جنسيًا واضحًا؛ c. صور واقعية تمثل طفلاً وهو يمارس سلوكًا جنسيًا واضحًا؛ d. ويشمل ذلك، على سبيل المثال لا الحصر، أي مواد إباحية صوتية أو مرئية أو نصية. **القسم 13 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية- المواد الإباحية للأطفال** 1. الشخص الذي يقوم عن قصد ودون عذر أو مبرر قانوني ب: a. إنتاج مواد إباحية للأطفال بغرض توزيعها من خلال نظام حاسوب؛ b. تقدم أو توفر مواد إباحية للأطفال من خلال نظام حاسوب؛ c. توزيع أو نقل المواد الإباحية عن الأطفال من خلال نظام حاسوب؛ d. شراء و/أو الحصول على مواد إباحية للأطفال من خلال نظام حاسوب لاستخدامه الشخصي أو لإعطائها لشخص آخر؛ e. حيازة مواد إباحية للأطفال في نظام حاسوب أو على وسائط تخزين بيانات الحاسوب؛ أو f. الوصول عمدًا، من خلال تكنولوجيا المعلومات والاتصالات، إلى المواد الإباحية عن الأطفال،، g. يعتبر جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً. 2. يمكن الدفاع أمام تهمة بجريمة منصوص عليها في الفقرة (1) (ب) إلى (1) (و) إذا أثبت الشخص أن المواد الإباحية عن الأطفال كانت بغرض إنفاذ القانون بحسن نية. 3. لا يجوز لدولة ما أن تجرم السلوك الموصوف في القسم 13 (1) (د) - (و).		
المادة 10 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[144] **انتهاك حقوق النشر**	**قانون حماية حقوق الملكية الفكرية رقم 82 لسنة 2002** **المادة 181**	**التحليل القانوني** هذا الحق محمي بشكل كاف من خلال التشريعات الوطنية

144. لا يوجد معادل للمادة 17 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 11 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[145] **المساعدة والتحريض** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لتجريم الأفعال التالية بموجب قانونه الداخلي، وذلك عندما يتم التحريض على ارتكاب أي من الجرائم المقررة وفقا للمواد من 2 إلى 10 من هذه الاتفاقية أو المساعدة عليها عمدًا، مع نية أن ترتكب هذه الجريمة. 2. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وتدابير أخرى لتجريم محاولة ارتكاب أي من الأفعال الإجرامية المنصوص عليها في المواد من 3 إلى 5 و 7 و 8 و 9.1. أ و ج من هذه الاتفاقية عمدًا. **المادة 19 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - محاولة ارتكاب الجرائم والاشتراك فيها** 1. الاشتراك في ارتكاب أية جريمة من الجرائم المنصوص عليها في هذا الفصل مع وجود نية ارتكاب الجريمة في قانون الدولة الطرف. 2. الشروع في ارتكاب الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية. 3. يجوز لأي دولة طرف الاحتفاظ بحقها في عدم تطبيق الفقرة الثانية من هذه المادة كليا أو جزئيا.	**القانون الجنائي رقم 58/1937** **المادتان 40 و 41**	**التحليل القانوني** تعتبر مساعدة الآخرين وتحريضهم على ارتكاب جرائم أمرًا ضروريًا لمحاكمة أولئك الذين يكونون قد قدموا المساعدة أو شجعوا على ارتكاب جرائم الإنترنت. المادتان 40 و41 من القانون الجنائي تمثلان القواعد العامة للمساعدة على ارتكاب الجرائم أو التحريض عليها أو الشروع في ارتكابها. ويمكن تطبيق هذه الأحكام على القوانين الموضوعية الأخرى. **تحليل الفجوة** **التوصيات:** في حين يتضمن القانون الجنائي بالفعل المساعدة على ارتكاب الجرائم أو التحريض عليها أو الشروع في ارتكابها، يُوصى بعمل المادة 11 من اتفاقية بودابست والمادة 19 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات كدليل لإدراجها في قانون مكافحة الجرائم السيبرانية المحلي، حتى لا يوجد مجال للشك بأن المساعدة على ارتكاب الجرائم أو التحريض عليها أو الشروع في ارتكابها مجرّمة.
المادة 12 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[146] **مسؤولية الشركات** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وتدابير أخرى لضمان أن الأشخاص الاعتباريين يمكن اعتبارهم مسؤولين عن أي جريمة جنائية منشأة وفقًا لهذه الاتفاقية، إذا ارتكبها أي شخص طبيعي لصالحهم، سواء كان ذلك بصفته الفردية أو باعتباره جزءًا من جهاز الشخص الاعتباري، أو باعتباره شخصًا قياديًا ضمن تنظيم الشخص الاعتباري، بناءً على: a. سلطة تمثيل الشخص الاعتباري؛ b. سلطة اتخاذ القرارات نيابة عن الشخص الاعتباري؛ c. سلطة ممارسة السيطرة داخل الشخص الاعتباري.	**لا يوجد معادل**	**التحليل القانوني** هذا الحكم هو عنصر أساسي بحيث يستطيع الأشخاص الاعتباريون (مثلًا الكيانات التجارية) التصرف نيابة عن الأشخاص الطبيعيين الذين تقع عليهم مسؤولية جنائية **تحليل الفجوة** **التوصيات:** استخدم لغة اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست في المادة 12 باعتبارها دليلًا للتشريعات الوطنية

145. المادة 29 (2) (و) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية
146. المادة 20 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، والمادة 30 (2) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
2. بالإضافة إلى الحالات المنصوص عليها بالفعل في الفقرة 1 من هذه المادة، يتخذ كل طرف الإجراءات اللازمة لضمان أن يتحمل الشخص الاعتباري المسؤولية عندما يكون عدم الإشراف أو السيطرة من قبل أي شخص طبيعي مشار إليه في الفقرة 1 قد جعل من الممكن ارتكاب جريمة جنائية منصوص عليها بموجب هذه الاتفاقية لصالح ذلك الشخص الاعتباري من قبل شخص طبيعي يعمل تحت سلطته. 3. مع مراعاة المبادئ القانونية للطرف، قد تكون مسؤولية الشخص الاعتباري جنائية أو مدنية أو إدارية. 4. تكون هذه المسؤولية دون المساس بالمسؤولية الجنائية للأشخاص الطبيعيين الذين ارتكبوا الجريمة.		
البروتوكول الإضافي لاتفاقية الجريمة السيبرانية، المتعلق بتجريم أعمال العنصرية وكراهية الأجانب المرتكبة من خلال أنظمة الحاسوب **المادة 3[147] - نشر المواد التي تحض على العنصرية وكراهية الأجانب من خلال أنظمة الحاسوب** يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم السلوك التالي في قوانينه المحلية، عندما يرتكب عمداً وبدون حق: توزيع المواد العنصرية وكراهية الأجانب أو إتاحتها للجمهور من خلال نظام الحاسوب. 2أ يجوز للطرف أن يحتفظ بالحق في عدم إسناد المسؤولية الجنائية بالتصرف على النحو المحدد في الفقرة 1 من هذه المادة، عندما تحض المواد الموزعة، كما هو محدد في الفقرة 1 من المادة 2، وتشجع على التمييز غير المرتبط بالكراهية أو العنف، شريطة أن تتوفر سبل انتصاف فعالة أخرى. 3 بصرف النظر عن الفقرة 2 من هذه المادة، يجوز للطرف أن يحتفظ بالحق في عدم تطبيق الفقرة 1 على حالات التمييز، لأن هذه الفقرة لا يمكن أن تمثل سبل انتصاف فعالة على النحو المشار إليه الفقرة 2، وذلك بسبب مبادئ ثابتة في نظامه القانوني الوطني متعلقة بحرية التعبير.	**القانون الجنائي رقم** 58/1937 **المادة** 161 **مكرر** يعاقب بالحبس وبغرامة لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسين ألف جنيه كل من قام بعمل أو بالامتناع عن عمل يكون من شأنه إحداث التمييز بين الأفراد أو ضد طائفة من طوائف الناس بسبب الجنس أو الأصل أو اللغة أو الدين أو العقيدة. وترتب على هذا التمييز إهدار لمبدأ تكافؤ الفرص أو العدالة الاجتماعية أو تكدير للسلم العام. وتكون عقوبة الحبس مدة لا تقل عن ثلاثة أشهر والغرامة التي لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين إذا ارتكبت الجريمة المشار إليها في الفقرة الأولى من هذه المادة من موظف عام أو مستخدم عمومي أو أي إنسان مكلف بخدمة عمومية. **القانون رقم** 10/2003 **المادة** 76 (2) مع عدم الإخلال بالحق في التعويض المناسب، يعاقب بالحبس وبغرامة لا تقل عن خمسمائة جنيه ولا تجاوز عشرين ألف جنيه أو بإحدى هاتين العقوبتين كل من: 1. استخدام أو ساعد على استخدام وسائل غير مشروعة لإجراء اتصالات. 2. تعمد إزعاج أو مضايقة غيره بإساءة استعمال أجهزة الاتصالات.	**التحليل القانوني** لا تشير المادتان 161 مكرر و76 (2) بالتحديد إلى استخدام النشر من خلال أنظمة الحاسوب، ولكن يمكن تطبيق هذه الجرائم من جانب النيابة العامة إذا تم نشر مواد متعلقة بدافع العنصرية وكراهية الأجانب. لا تتضمن المادة 3 (1) (هـ) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية، التي تتضمن إنشاء وتنزيل مواد متعلقة بدافع العنصرية وكراهية الأجانب من نظام حاسوبي بدلاً من مجرد نشر أو إتاحة مثل هذه المواد، القصد أو عبارة «بدون حق" - وتُفضل صياغة اتفاقية بودابست. **تحليل الفجوة** **التوصيات:** على الرغم من وجود أحكام عامة في المادتين 161 مكرر و 76 (2)، يوصى باستخدام لغة اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست في المادة 3 من البروتوكول الإضافي باعتبارها دليلًا للتشريعات الوطنية لتجريم مثل هذا السلوك الذي يتم من خلال نظام الحاسوب.

147. المادة 29 (3) (هـ) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية لا يوجد ما يعادلها في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
بروتوكول إضافي **المادة 4[148] - التهديد بدافع العنصرية وكراهية الأجانب** يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم السلوك التالي في قوانينه المحلية، عندما يرتكب عمداً وبدون حق: التهديد، من خلال نظام الحاسوب، بارتكاب جريمة جنائية خطيرة على النحو المحدد في قانونها الداخلي، (1) ضد أشخاص لسبب أنهم ينتمون إلى جماعة يميزها عرقها أو لونها أو نسبها أو أصلها القومي أو العرقي أو دينها، إذا تم استخدام أي من هذه العوامل ذريعةً، أو (2) ضد مجموعة من الأشخاص تتميز بأي من هذه الخصائص.	**القانون الجنائي رقم** 58/1937 **المادة** 161 **مكرر** **قانون الاتصالات** 10/2003 **المادة** 76 (2)	**التحليل القانوني** لا تشير المادتان 161 مكرر و 76 (2) بالتحديد إلى التهديدات المتعلقة بدافع العنصرية وكراهية الأجانب من خلال أنظمة الحاسوب، ولكن يمكن تطبيق هذه الجرائم من جانب النيابة العامة في مثل هذه الحالة **تحليل الفجوة** **التوصيات:** على الرغم من وجود أحكام عامة في المادتين 161 مكرر و 76 (2) ، يوصى باستخدام لغة اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست في المادة 4 من البروتوكول الإضافي باعتبارها دليلًا للتشريعات الوطنية لتجريم مثل هذا السلوك الذي يتم من خلال نظام الحاسوب.
بروتوكول إضافي **المادة 5[149] - الإهانة بدافع العنصرية وكراهية الأجانب** يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم السلوك التالي في قوانينه المحلية، عندما يرتكب عمداً وبدون حق: إهانة الجمهور، من خلال نظام حاسوبي، (1) الأشخاص لكونهم ينتمون إلى مجموعة يميزها عرقها أو لونها أو نسبها أو أصلها القومي أو العرقي أو دينها، إذا تم استخدام أي من هذه العوامل ذريعةً؛ أو (2) مجموعة من الأشخاص تتميز بأي من هذه الخصائص. يجوز للطرف 2A إما: أن يشترط أن يكون للجريمة المشار إليها في الفقرة 1 من هذه المادة أثر على الشخص أو مجموعة الأشخاص المشار إليهم في الفقرة 1 والذين يتعرضون للكراهية أو الاحتقار أو السخرية؛ أن يحتفظ بالحق في عدم تطبيق الفقرة 1 من هذه المادة بشكل كلي أو جزئي.	**القانون الجنائي رقم** 58/1937 **المادة** 161 **مكرر** **قانون الاتصالات** 10/2003 **المادة** 76 (2)	**التحليل القانوني** لا تشير المادتان 161 مكرر و 76 (2) بالتحديد إلى الإهانات المتعلقة بدافع العنصرية وكراهية الأجانب من خلال أنظمة الحاسوب، ولكن يمكن تطبيق هذه الجرائم من جانب النيابة العامة في مثل هذه الحالة **تحليل الفجوة** **التوصيات:** على الرغم من وجود أحكام عامة في المادتين 161 مكرر و 76 (2) ، يوصى باستخدام لغة اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست في المادة 5 من البروتوكول الإضافي باعتبارها دليلًا للتشريعات الوطنية لتجريم مثل هذا السلوك الذي يتم من خلال نظام الحاسوب.

148. المادة 29 (3) (و) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية لا يوجد ما يعادلها في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات
149. المادة 29 (3) (ز) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية لا يوجد ما يعادلها في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
بروتوكول إضافي **المادة 6[150] - الإنكار أو التقليل إلى الحد الأدنى أو الموافقة أو التبرير للإبادة الجماعية أو الجرائم ضد الإنسانية** 1. يلتزم كل طرف باتخاذ التدابير التشريعية لجعل الأفعال التالية جرائم جنائية بموجب قوانينها الداخلية، عندما تُرتكب عمدًا وبدون حق: توزيع أو توفير عبر نظام الحاسوب بأية طريقة من الطرق للجمهور، مواد تنكر أو تقلل أو تقر أو تقلل بشكل كبير الأفعال التي تعتبر إبادة جماعية أو جرائم ضد الإنسانية، على النحو المحدد في القانون الدولي والمعترف بها على هذا النحو في القرارات النهائية والملزمة للمحكمة العسكرية الدولية، المنشأة بموجب اتفاقية لندن المؤرخة في 8 أغسطس 1945، أو أي محكمة دولية أخرى تنشأ بموجب المواثيق الدولية ذات الصلة والتي يعترف هذا الطرف باختصاصها القضائي. 2. يجوز لأي طرف أن يشترط أن يكون الإنكار أو التقليل إلى الحد الأدنى المشار إليه في الفقرة 1 من هذه المادة قد ارتكب بهدف التحريض على الكراهية أو التمييز أو العنف ضد أي فرد أو مجموعة من الأفراد على أساس العرق أو اللون أو النسب أو الأصل القومي أو العرقي أو الدين أو إذا استخدمت هذه العوامل ذريعة لذلك، أو ب أن يحتفظ بالحق في عدم تطبيق الفقرة 1 من هذه المادة بشكل كلي أو جزئي.	**لا يوجد معادل**	**تحليل الفجوة** **التوصيات:** استخدم لغة اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست في المادة 6 من البروتوكول الإضافي كدليل للتشريعات الوطنية
جرائم إضافية للمراجعة		
الجرائم المتعلقة بالهوية - القسم 14 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية يعاقب الشخص الذي يقوم عن قصد ودون عذر أو مبرر قانوني، أو يتجاوز عذرًا قانونيًا أو مبررًا باستخدام نظام حاسوب في أي مرحلة من مراحل الجريمة بنقل أو تملك أو استخدام وسيلة لتحديد الهوية شخص آخر بنية ارتكاب أي نشاط غير قانوني يشكل جريمة أو المساعدة أو التحريض عليها، عند إدانته بهذه الأعمال بالسجن لمدة لا تتجاوز [المدة] أو بغرامة لا يتجاوز [المبلغ]، أو بالعقوبتين معاً.		**التحليل القانوني** تغطي هذه الجريمة مرحلة التحضير لجريمة خيانة الأمانة المتعلقة بالهوية **تحليل الفجوة** **التوصيات:** يستحسن أن تدرج في التشريعات المحلية.

150. المادة ٩٢ (٣) (ح) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية لا يوجد ما يعادلها في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
الكشف عن تفاصيل التحقيق **القسم 16 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية** موفر خدمة الإنترنت الذي يتلقى أمرًا يتعلق بتحقيق جنائي ينص صراحةً على الحفاظ على السرية أو على التزام شبيه ينص عليه القانون، ثم يقوم عن عمد ودون عذر أو مبرر قانوني أو بتجاوز لعذر قانوني مبرر، بالإفصاح عن: • حقيقة أنه قد تم إصدار أمر؛ أو • أي شيء تم تنفيذه بموجب الأمر؛ أو • أي بيانات تم جمعها أو تسجيلها بموجب الطلب؛ يعتبر جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً.	**القانون الجنائي** **المواد** 85 (2) و 189 و 190 و 193	**التحليل القانوني** يعاقب على الانتهاكات المتعلقة بالبيانات والكشف عن المعلومات الحساسة التي يمكن أن تؤثر على التحقيقات الجنائية بموجب مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية قد يجرم التشريع الوطني، على الرغم من عدم الإشارة إلى الانتهاكات المتعلقة بالبيانات بشكل صريح، - انتهاكات إجراءات التحقيق، والتي ينبغي أن تشمل الانتهاكات المتعلقة بالبيانات والمعلومات الحساسة.
عدم السماح بالمساعدة **القسم 17 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية** 1. أي شخص آخر غير المشتبه فيه فشل عمداً دون عذر أو مبرر قانوني أو بتجاوز عذر أو مبرر قانوني، بمساعدة شخص أو السماح بمساعدته، بناءً على أمر مثلما تحدد المواد 20 إلى 22[151] يرتكب جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً. 2. قد يقرر أي بلد عدم تجريم عدم السماح بالمساعدة شرط أن تتوفر سبل انتصاف فعالة أخرى.		**التحليل القانوني** تتعلق هذه الجريمة بالأشخاص الذين لديهم معرفة محددة بالأدلة ذات الصلة والذين يرفضون تقديم المساعدة. غالبًا ما يعتمد تطبيق القانون على هؤلاء الأشخاص لتأمين الأدلة في التحقيقات الإلكترونية. هنالك مخالفة مستقلة وهي عدم توفير كلمات مرور أو الوصول إلى الرموز للأجهزة المشفرة أو البيانات (مثل «مفتاح المعلومات المحمية") - ينص القسم 53 من قانون تنظيم سلطات التحقيق في المملكة المتحدة لعام 2000 (RIPA) [152] على وجود جرم جنائي يتحمله الأشخاص الذين لا يمتثلون للمادة 49 من إخطار قانون تنظيم سلطات التحقيق في المملكة المتحدة والقاضية بالكشف عن «المفتاح" **تحليل الفجوة** **التوصيات:** يستحسن أن تدرج في التشريعات المحلية.
المطاردة السيبرانية **القسم 18 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية** الشخص الذي يقوم، دون عذر أو مبرر قانوني، أو يتجاوز عذرًا قانونيًا أو مبررًا، ببدء أي اتصال إلكتروني، بقصد إكراه شخص ما أو تخويفه أو مضايقته أو التسبب في ضائقة عاطفية كبيرة له، باستخدام نظام حاسوب لدعم السلوك المتكرر والعدائي والعنيف، يرتكب جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً.		**التحليل القانوني** هذه الجريمة تُجرم من يضايقون الأشخاص عبر الإنترنت - قد تنص بعض الولايات القضائية على جرائم تحرش غير مرتبطة بالحاسوب - لكن يوصى باعتماد هذه الجريمة لمتابعة لتلك الجرائم المرتكبة عبر الإنترنت. **تحليل الفجوة** **التوصيات:** يستحسن أن تدرج في التشريعات المحلية.

151. أوامر البحث والاستيلاء والمساعدة والإنتاج
152. http://www.legislation.gov.uk/ukpga/2000/23/section/53

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
رعاية الأطفال على الإنترنت **القانون الجنائي الهولندي 248e** يعاقب الشخص الذي يقترح ترتيب لقاء، بوسائل عمل آلية أو باستخدام خدمة اتصال، مع شخص يعرف، أو ينبغي منطقيًا أن يعرف، أن هذا الشخص لم يصل بعد إلى سن السادسة عشرة، مع نية ارتكاب أفعال غير لائقة مع هذا الشخص أو لعمل صور عن عمل جنسي يشارك فيه هذا الشخص، بالسجن لمدة لا تقل عن سنتين أو بغرامة من الفئة الرابعة، إذا ارتكب أي عمل يقصد به تحقيق اللقاء. **قانون العقوبات الكندي** **القسم** 172.1 1. يرتكب جريمة كل شخص يتواصل عن طريق وسائل الاتصالات مع a. شخص يكون عمره أقل من 18 عامًا، أو يظن المتهم أن عمره أقل من ذلك، بغرض تسهيل ارتكاب جريمة مرتبطة بهذا الشخص، وذلك بموجب المادة الفرعية 153 (1)، المادة 155، 163.1، 170 أو 171 أو القسم الفرعي 212 (1) أو (2) أو (2.1) أو (4)؛ b. شخص يكون عمره أقل من 16 عامًا، أو يظن المتهم أن عمره أقل من ذلك، بغرض تسهيل ارتكاب جريمة مرتبطة بهذا الشخص، وذلك بموجب المواد 151 أو 152، أو الفقرة الفرعية 160(3) أو 173(2) أو الأقسام 271 أو 272 أو 273 أو 280؛ أو c. شخص يكون عمره أقل من 14 عامًا، أو يظن المتهم أن عمره أقل من ذلك، بغرض تسهيل ارتكاب جريمة مرتبطة بهذا الشخص بموجب المادة 281. عقاب 2. يعتبر كل شخص يرتكب جريمة بموجب الفقرة الفرعية (1) مذنبًا a. مذنبًا بارتكاب جريمة ويكون عرضة لعقوبة السجن لمدة تتراوح بين 10 سنوات كحد أقصى وسنة واحدة كحد أدنى؛ أو b. مذنبًا بارتكاب جريمة يعاقب عليها في ملخص الإدانة بالسجن لمدة تتراوح بين 18 شهرًا كحد أقصى و 90 يومًا كحد أدنى. افتراض إعادة تقدير العمر		**التحليل القانوني** لإثبات الجرم الهولندي، يلزم عقد لقاء لأغراض جنسية مع تقديم أدلة إثبات مأخوذة من تاريخ الدردشة عبر الإنترنت تفصح عن قصد جنسي؛ طلب عقد اللقاء مع الأدلة على أنه تم التخطيط لذلك (أي التاريخ والمكان). الغرض من القانون الكندي هو منع استدراج الكبار المفترسين للأطفال عبر الإنترنت. لا تتطلب هذه الجريمة حدوث جريمة جنسية. وهذا يعني أن المتهم لا يحتاج إلى الذهاب فعلاً لمقابلة الضحية شخصيًا. تكتمل الجريمة قبل اتخاذ أي إجراءات لارتكاب الجريمة الموضوعية. **تحليل الفجوة** **التوصيات:** يُنصح بإدراجها في التشريعات المحلية لتجريم هذا السلوك التحضيري قبل ارتكاب جريمة جنسية

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
3. الأدلة على أن الشخص المشار إليه في الفقرة (1) (أ) أو (ب) أو (ج) قُدِّم للمتهم وعمره أقل من ثمانية عشر عامًا أو ستة عشر عامًا أو أربعة عشر عامًا، حسب الحالة، في حالة عدم وجود أدلة تثبت عكس ذلك تثبت أن المتهم يعتقد أن الشخص كان أقل من تلك السن. 4. لا يقبل دفاع المتهم أمام التهم الموجهة بموجب الفقرة (1) (أ) أو (ب) أو (ج) بأنه كان يعتقد أن الشخص المشار إليه في تلك الفقرة لا يقل عمره عن ثمانية عشر عامًا أو ستة عشر عامًا أو أربعة عشر عامًا، حسب الحالة، إلا في حالة اتخذ المتهم خطوات معقولة للتأكد من عمر الشخص.		

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 19 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[153] **البحث عن بيانات الحاسوب وضبطها** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لتمكين سلطاته المختصة من البحث في أو الوصول إلى: a. نظام الحاسوب أو جزء منه وبيانات الحاسوب المخزنة فيه؛ و b. وسيلة تخزين بيانات الحاسوب، حيث يمكن تخزين بيانات الحاسوب في أراضيها. 2. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وغيرها من الإجراءات لضمان تمكن سلطاته عند تفتيشها نظام حاسوب معينًا أو جزءًا منه أو الوصول إليه بطريقة مماثلة، وذلك وفقًا للفقرة 1-أ،		**التحليل القانوني** لا تشير الأحكام الواردة في قانون الإجراءات الجنائية وقانون الاتصالات إلى الحواسيب أو أنظمة الحاسوب أو وسائط التخزين على الحاسوب الأخرى وهي أكثر قابلية للتطبيق على الاعتراض (انظر أدناه) هذه صلاحية تحقيق أساسية ويجب أن تشير إلى «الحصول على حق الوصول" وليس "التفتيش." في "التقرير التوضيحي لاتفاقية بودابست بشأن الجريمة السيبرانية، يعني "البحث" التفتيش عن البيانات أو قراءتها أو فحصها أو مراجعتها. ويشمل ذلك مفهوم البحث عن البيانات والبحث عن (فحص) البيانات. لكلمة "الوصول" معنى محايد وتعكس بدقة أكثر مصطلحات الحاسوب.[154] **تحليل الفجوة** **التوصيات:** يمكن أن يقتبس التشريع الوطني اللغة المناسبة من اتفاقية بودابست بشأن الجريمة السيبرانية واتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية وذلك لتضمين تعريفات لنظام الحاسوب[155] وبيانات الحاسوب[156] والإحالة دائمًا إلى الوصول يجب أن يكون هناك تعريف «للحجز" لضمان النزاهة ولتحديد الإجراءات - القسم 3 (16) من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية

153. المادة 3 من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية
154. التقرير التوضيحي لاتفاقية بودابست بشأن الجريمة السيبرانية، الفقرة 191
155. انظر المادة 1.أ. من اتفاقية بودابست: «يعني نظام الحاسوب أي جهاز أو مجموعة من الأجهزة المترابطة أو ذات الصلة، أو واحدًا أو أكثر من هذه الأجهزة يقوم بمعالجة البيانات تلقائيًا أو تسجيلها وفقا لأحد البرامج" **أو** القسم 3 (5) من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية: «جهاز أو مجموعة من الأجهزة المترابطة أو ذات الصلة، بما في ذلك الإنترنت، يقوم واحد منها أو أكثر بمعالجة تلقائية للبيانات أو بأداء أي وظيفة أخرى وفقًا لأحد البرامج".
156. انظر المادة 1.ب. من اتفاقية بودابست: «أي تمثيل للوقائع أو المعلومات أو المفاهيم في نموذج مناسب للمعالجة في نظام حاسوب، بما في ذلك البرامج المناسبة لأن يقوم نظام حاسوب بأداء وظيفة ما"، **أو** القسم 3 (6) من مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية: تتضمن بيانات الحاسوب أي تمثيل للوقائع أو المعلومات أو المفاهيم (سواء أكانت نصوصًا أو أصواتًا أو صورًا) أو رموز آلة مقروءة أو تعليمات، في نموذج مناسب للمعالجة في نظام الحاسوب، بما في ذلك البرامج المناسبة لأن يقوم نظام الحاسوب بأداء وظيفة ما".

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
ويكون لديها أسباب للاعتقاد بأن البيانات المطلوبة مخزنة في نظام حاسوب آخر أو أن جزءًا منها موجود في إقليمها، وهذه البيانات يمكن الوصول إليها قانونيًا من النظام الأولي أو متاحة لها، فإنها قادرة على توسيع نطاق التفتيش أو الوصول المشابه للنظام الآخر على وجه السرعة. 3. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وغيرها من الإجراءات لتمكين سلطاته المختصة من مصادرة أو تأمين بيانات الحاسوب التي تم الوصول إليها وفقًا للفقرات 1 أو 2. تشمل هذه التدابير القدرة على: a. الاستيلاء على نظام حاسوب أو جزء منه أو وسيلة تخزين بيانات الحاسوب، والقيام بما يلزم لتأمينه؛ b. إنشاء نسخة من بيانات الحاسوب هذه والاحتفاظ بها؛ c. الحفاظ على سلامة بيانات الحاسوب المخزنة ذات الصلة؛ d. أن يجعل الوصول غير ممكن إلى البيانات في نظام الحاسوب الذي تم الوصول إليه أو أن يحذفها من نظام الحاسوب 4. الذي تم الوصول إليه.يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لتمكين سلطاته المختصة من أن تأمر أي شخص لديه معرفة بعمل نظام الحاسوب أو التدابير المطبقة لحماية البيانات الموجودة فيه 5. بتوفير ما يلزم من المعلومات التي تكفل تنفيذ الإجراءات المشار إليها في الفقرتين 1 و2. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و 15. **القسم 20 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - البحث والضبط** 1. إذا اقتنع [القاضي] بناء على [معلومات تحت القَسَم] [شهادة خطية] أن هناك أسبابًا معقولة [للاشتباه] [للاعتقاد] أنه قد يكون هناك في مكان ما شيء أو بيانات حاسوب: • قد تكون مادية كدليل في إثبات الجريمة؛ أو • قد اكتسبها شخص نتيجة لجريمة؛		”يشمل الحجز: • تشغيل أي نظام حاسوب في الموقع ووسائط تخزين بيانات الحاسوب؛ • إنشاء نسخة من بيانات الحاسوب والاحتفاظ بها، بما في ذلك عن طريق استخدام معدات في الموقع؛ • الحفاظ على سلامة بيانات الحاسوب المخزنة ذات الصلة؛ • أن يجعل الوصول غير ممكن إلى بيانات الحاسوب في نظام الحاسوب الذي تم الوصول إليه أو أن يحذفها؛ • أخذ نسخة مطبوعة من بيانات غير ممكن؛ أو • الاستيلاء على نظام حاسوب أو جزء منه أو وسيلة تخزين بيانات الحاسوب، والقيام بما يلزم لتأمينه». تنص المادة 21 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية على التشريع لضمان تقديم المساعدة من قبل أولئك الذين لديهم معرفة متخصصة بموقع الأدلة ذات الصلة - يمكن استخدام هذا كدليل - انظر أيضًا القسم 17 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية، المتعلق بالجريمة في حال تم رفض المساعدة دون عذر قانوني

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
[يجوز] [يأمر] يصدر [القاضي] تفويضًا لضابط [إنفاذ القانون] [الشرطة]، ويزوده بما قد يلزم من مساعدة، لدخول المكان للبحث عن الشيء أو بيانات الحاسوب وضبطها، وعمل ما يلزم بما في ذلك البحث أو عمليات الوصول الشبيهة: a. نظام الحاسوب أو جزء منه وبيانات الحاسوب المخزنة فيه؛ و b. وسيلة تخزين بيانات الحاسوب، حيث يمكن تخزين بيانات الحاسوب في إقليم البلد. 2. إذا كان[قوة إنفاذ القانون] [الشرطة] الذي يجري عملية بحث على أساس القسم 20 (1) أسباب للاعتقاد بأن البيانات المطلوبة مخزنة في نظام حاسوب آخر أو جزء منه في إقليمها، وأن هذه البيانات يمكن الوصول إليها قانونيًا أو يمكن أن تكون متاحة من النظام الأولي، فيجب أن يكون قادرًا على توسيع نطاق البحث أو الوصول إلى النظام الآخر بطريقة مماثلة. 3. يتم تمكين ضابط [تطبيق القانون] [الشرطة] الذي يقوم بالبحث من مصادرة أو تأمين بيانات الحاسوب المماثلة التي يتم الوصول إليها وفقًا للفقرات 1 أو 2. **القسم 21 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - المساعدة** يجب على أي شخص لا يشتبه في ارتكابه جريمة ولكن لديه علم بسير عمل نظام الحاسوب أو التدابير المطبقة لحماية بيانات الحاسوب الواردة فيه والتي تخضع لعملية بحث بموجب المادة 20، أن يسمح وأن يساعد إذا لزم الأمر وطلب منه الشخص المسؤول أن يجري البحث عن طريق: • توفير المعلومات التي تمكن من اتخاذ التدابير المشار إليها في المادة 20؛ • الوصول إلى نظام حاسوب أو وسيط تخزين بيانات الحاسوب واستخدامه للبحث في أي بيانات حاسوب متاحة أو في النظام؛ • الحصول على ونسخ بيانات حاسوب هذه؛ • استخدام المعدات لعمل نسخ؛ و • الحصول على معلومات واضحة من نظام حاسوب بشكل مقبول في الإجراءات القانونية.		

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 26 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - فحص المعلومات المخزنة 1. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين سلطاتها المختصة من التفتيش أو الوصول إلى: a. تقنية معلومات أو جزء منها والمعلومات المخزنة فيها أو المخزنة عليها. b. بيئة أو وسيط تخزين معلومات تقنية معلومات والذي قد تكون معلومات التقنية مخزنة فيه أو عليه. 2. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من التفتيش أو الوصول إلى تقنية معلومات معينة أو جزء منها بما يتوافق مع الفقرة (1- أ) إذا كان هناك اعتقاد بأن المعلومات المطلوبة مخزنة في تقنية معلومات أخرى أو جزء منها في إقليمها وكانت هذه المعلومات قابلة للوصول قانونا أو متوفرة في التقنية الأولى فيجوز توسيع نطاق التفتيش والوصول للتقنية الأخرى. **المادة 27 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - ضبط المعلومات المخزنة** 1. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من ضبط وتأمين معلومات تقنية المعلومات التي يتم الوصول إليها حسب الفقرة 1 من المادة 26 من هذه الاتفاقية. a. هذه الإجراءات تشمل صلاحيات: b. ضبط وتأمين تقنية المعلومات أو جزء منها أو وسيط تخزين معلومات تقنية المعلومات. c. عمل نسخة معلومات تقنية المعلومات والاحتفاظ بها. d. الحفاظ على سلامة معلومات تقنية المعلومات المخزنة. 2. إزالة أو منع الوصول إلى تلك المعلومات في تقنية المعلومات التي يتم الوصول إليها. تلتزم كل طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى أي شخص لديه معرفة بوظيفة تقنية المعلومات أو الإجراءات المطبقة لحماية تقنية المعلومات من أجل تقديم المعلومات الضرورية لإتمام تلك الإجراءات المذكورة في الفقرتين 2 و 3 من المادة 26 من هذه الاتفاقية.		

إجراءات		
أفضل الممارسات الدولية	**التشريع الوطني**	**ملاحظات**
المادة 16 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[157] **الحفظ المستعجل لبيانات الحاسوب المخزنة والكشف عنها** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وغيرها من الإجراءات لتمكين سلطاته المختصة من طلب الحفظ السريع لبيانات الحاسوب المحددة أو الحصول عليها بشكل مماثل، بما في ذلك حركة البيانات التي تم تخزينها عن طريق نظام حاسوبي، ولا سيما عندما يكون هناك أسباب للاعتقاد بأن بيانات الحاسوب معرضة بشكل خاص للفقد أو التعديل. 2. عندما يقوم أحد الأطراف بتنفيذ الفقرة 1 أعلاه عن طريق أمر شخص بحفظ بيانات الحاسوب المخزنة المحددة وذلك بوضعها في حوزته أو تحت سيطرته، يعتمد هذا الطرف الإجراءات التشريعية وغيرها من الإجراءات التي قد تكون ضرورية لإلزام ذلك الشخص بالحفاظ على سلامة بيانات الحاسوب لفترة زمنية طويلة، حدها الأقصى تسعين يومًا، وذلك لتمكين السلطات المختصة من طلب الكشف عنها. يجوز للطرف أن ينص على تجديد هذا الأمر لاحقًا. 3. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لإلزام الحارس أو أي شخص آخر يحفظ بيانات الحاسوب بالحفاظ على سرية تنفيذ هذه الإجراءات للفترة الزمنية المنصوص عليها في قانونه الداخلي. 4. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و 15.	**لا يوجد معادل**	**التحليل القانوني** هذه القوة الإجرائية مهمة لضمان الحفاظ على البيانات المعرضة للحذف أو الفقد **تحليل الفجوة** **التوصيات:** تعد هذه القدرة المستعجلة للاحتفاظ بمعلومات المشترك الأساسية والبيانات الوصفية والمعاملات والمحتويات المخزنة ضرورية كجزء من تحقيقات جرائم الإنترنت، ولضمان أن تكون الأدلة متاحة للبحث والوصول والضبط والمراجعة. يمكن استخدام لغة المادة 16 من اتفاقية بودابست أو القسم 23 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية أو المادة 23 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. سيتطلب ذلك أيضًا تعريفات «بيانات الحاسوب»، و[158] "معلومات المشترك أو معلومات المشترك الأساسية"، و "حركة البيانات" و[159] "مزود خدمة الاتصالات"[160] يجب ملاحظة أن اتفاقية بودابست واتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية لا تقدمان تعريفًا لمعلومات المشترك الأساسية؛ غير أن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات تقدم تعريفًا لمعلومات المشترك:[161] " أي معلومات لدى مزود الخدمة بخصوص المشتركين في الخدمة، باستثناء المعلومات التي يمكن من خلالها معرفة ما يلي: نوع خدمة الاتصال المستخدمة والأحكام الفنية المتعلقة بها وفترة الخدمة. هوية المشترك وعنوانه البريدي أو الجغرافي أو رقم الهاتف ومعلومات الدفع المتاحة بموجب اتفاقية الخدمة أي معلومات أخرى على موقع تركيب معدات الاتصالات بموجب اتفاقية الخدمة." ينبغي إيلاء اهتمام لأن يكون طول مدة الحفظ معقولًا في هذه الظروف، وأن يُسمَح بتطبيق التمديد في الظروف الملحة - تنص اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست والاتفاقية العربية لمكافحة جرائم تقنية المعلومات على 90 يومًا، فيما تنص اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية على 7 أيام. ووفقًا للتجربة فإن مدة 90 يومًا هي مدة قصيرة في التحقيقات عبر الإنترنت ، ويجب أن تكون حوالي 180 يومًا يمكن تمديدها.

157. لا يوجد ما يعادلها في اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية

158. انظر المادة 1.ب. اتفاقية بودابست **أو** القسم 3 (6) من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية

159. انظر المادة 1.د من اتفاقية بودابست: "أي بيانات حاسوب تتعلق باتصال عن طريق نظام حاسوب، يتم إنشاؤها بواسطة نظام حاسوب يشكل جزءًا من سلسلة الاتصال، وتعرض مصدر الاتصال أو وجهته أو مساره أو الوقت أو التاريخ أو حجمه أو مدته أو نوع الخدمة الأساسية"، **أو** القسم 3 (18) من مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية: "حركة البيانات تعني أي بيانات حاسوب تتعلق باتصال عن طريق نظام حاسوب، يتم إنشاؤها بواسطة نظام حاسوب يشكل جزءًا من سلسلة الاتصال، وتعرض مصدر الاتصال أو وجهته أو مساره أو الوقت أو التاريخ أو الحجم أو المدة أو نوع الخدمة الأساسية".

160. انظر المادة 1.ج من اتفاقية بودابست: "1 أي كيان عام أو خاص يوفر للمستخدمين قدرة الاتصال عن طريق نظام الحاسوب، و 2 أي كيان آخر يعالج أو يخزن بيانات الحاسوب نيابة عن خدمة الاتصال هذه أو مستخدمي هذه الخدمة».

161. انظر المادة 2 (9) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
القسم 23 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الحفظ المستعجل إذا اقتنع ضابط [تطبيق القانون] [الشرطة] بوجود أسباب معقولة للاعتقاد بأن بيانات الحاسوب المطلوبة لأغراض التحقيق الجنائي معرضة للضياع أو التعديل، يجوز لضابط [تطبيق القانون] [الشرطة]، عن طريق إشعار مكتوب مقدم إلى شخص يتحكم في بيانات الحاسوب، أن يطلب من هذا الشخص الحفاظ على البيانات المحددة في الإشعار لمدة تصل إلى سبعة (7) أيام على وفقًا لما هو محدد في الإشعار. يمكن تمديد الفترة إلى ما بعد سبعة (7) أيام إذا سمح [قاضي]، بناءً على طلب من طرف واحد، وذلك لمدة زمنية أخرى محددة. **المادة 23 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات- الحفظ المستعجل للبيانات المخزنة في تكنولوجيا المعلومات** 1. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأمر أو الحصول علىالحفظ العاجل للمعلومات المخزنة بما في ذلك معلومات تتبع المستخدمين والتي خزنت على تقنية معلومات وخصوصا إذا كان هناك اعتقاد بأن تلك المعلومات عرضة للفقدان أو التعديل. 2. تلتزم كل دولة طرف بتبني الإجراءات الضرورية فيما يتعلق بالفقرة 1 بواسطة إصدار أمر إلى شخص من أجل حفظ معلومات تقنية المعلومات المخزنة والموجودة بحيازته أو سيطرته ومن أجل إلزامه بحفظ وصيانة سلامة تلك المعلومات لمدة أقصاها 90 يوما قابلة للتجديد، من أجل تمكين السلطات المختصة من البحث والتقصي 3. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لإلزام الشخص المسؤول عن حفظ تقنية معلومات للإبقاء على سرية الإجراءات طوال الفترة القانونية المنصوص عليها في القانون الداخلي.		

إجراءات		
أفضل الممارسات الدولية	**التشريع الوطني**	**ملاحظات**
المادة 17 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[162] **الحفظ المستعجل والكشف الجزئي لبيانات المرور** 1. فيما يتعلق بحركة البيانات التي يتعين الحفاظ عليها بموجب المادة 16، يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى من أجل: a. التأكد من أن مثل هذا الحفظ المستعجل لحركة البيانات متاح بغض النظر عما إذا كان هناك واحد أو أكثر من مقدمي الخدمة قد شاركوا في نقل ذلك الاتصال؛ و b. ضمان الكشف السريع للسلطة المختصة لدى الدولة الطرف، أو للشخص المعين من قبل تلك السلطة، عن كمية كافية من حركة البيانات لتمكينه من تحديد مقدمي الخدمات والمسار الذي تم من خلاله نقل الاتصال. 2. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و 15. **القسم 23 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الحفظ المستعجل** إذا اقتنع ضابط [تطبيق القانون] [الشرطة] بوجود أسباب معقولة للاعتقاد بأن بيانات الحاسوب المطلوبة لأغراض التحقيق الجنائي معرضة للضياع أو التعديل، يجوز لضابط [تطبيق القانون] [الشرطة]، عن طريق إشعار مكتوب مقدم إلى شخص يتحكم في بيانات الحاسوب، أن يطلب من هذا الشخص الحفاظ على البيانات المحددة في الإشعار لمدة تصل إلى سبعة (7) أيام على وفقًا لما هو محدد في الإشعار. يمكن تمديد الفترة إلى ما بعد سبعة (7) أيام إذا سمح [قاضي]، بناءً على طلب من طرف واحد، وذلك لمدة زمنية أخرى محددة.	**لا يوجد معادل**	**التحليل القانوني** تعد هذه القوة الإجرائية مهمة بشكل خاص لضمان توفير مقدمي خدمات الإنترنت لعناوين بروتوكول إنترنت يمكنها تحديد موقع مرتكب الجريمة السيبرانية. **تحليل الفجوة** **التوصيات:** يجب تضمين هذه القوة المستعجلة جنبًا إلى جنب مع الكشف عن حركة البيانات في التشريعات لتمكين التحقيقات الفعالة في جرائم الإنترنت. يمكن استخدام لغة المادة 17 من اتفاقية بودابست، القسمين 23 و 24 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية أو المادة 24 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. سيتطلب ذلك أيضًا تعريفات لـ «حركة البيانات" و "مزود خدمة الاتصالات"[163]

162. لا يوجد ما يعادلها في اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية
163. انظر التعريفات أعلاه

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
القسم 24 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - جمع بيانات حركة الاتصالات إذا اقتنع ضابط [تطبيق القانون] [الشرطة] بناءً على أسباب معقولة بأن البيانات المخزنة في نظام الحاسوب ضرورية لأغراض التحقيق الجنائي، يجوز له أن يطلب، عبر إشعار خطي، من شخص له السيطرة على نظام الحاسوب كشف بيانات حركة مرور تتعلق باتصال محدد بشكل كافٍ لتحديد: • مزودو خدمة الإنترنت؛ و/ أو • المسار الذي تم من خلاله نقل الاتصال. **المادة 24 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - لتحفظ العاجل والكشف الجزئي لمعلومات تتبع المستخدمين** تلتزم كل دولة طرف بتبني الإجراءات الضرورية فيما يختص بمعلومات تتبع المستخدمين من أجل: 1. ضمان توفر الحفظ العاجل لمعلومات تتبع المستخدمين بغض النظر عن اشتراك واحد أو أكثر من مزودي الخدمة في بث تلك الاتصالات. 2. ضمان الكشف العاجل للسلطات المختصة لدى الدولة الطرف أو لشخص تعينه تلك السلطات لمقدار كاف من معلومات تتبع المستخدمين لتمكين الدولة الطرف من تحديد مزودي الخدمة ومسار بث الاتصالات.		
المادة 18 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[164] **أمر النسخ** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وتدابير أخرى لتمكين سلطاته المختصة من أن تأمر:	**قانون الإجراءات الجنائية رقم** 150/1950 **المواد** 95 **و** 206 **و** 206 **مكرر** **القانون رقم** 10/2003 **المادتان** 19 **و** 64	**التحليل القانوني** هذا شرط أساسي لإجراء تحقيق فعال في جرائم الإنترنت وسيؤثر غيابه على الملاحقات القضائية والتعاون الدولي. لا تشير الأحكام الواردة في قانون الإجراءات الجنائية وقانون الاتصالات إلى الحواسيب أو أنظمة الحاسوب أو وسائط التخزين على الحاسوب الأخرى وهي أكثر قابلية للتطبيق على الاعتراض (انظر أدناه). **تحليل الفجوة** **التوصيات:** تعتبر هذه السلطة الأساسية ضرورية لضمان توفير مزودي خدمة الاتصالات في مصر لمعلومات المشترك الأساسية وحركة البيانات وبيانات المحتوى المخزنة. سيتطلب ذلك أيضًا تعريفات لـ «بيانات الحاسوب" و "معلومات المشترك أو معلومات المشترك الأساسية" و "حركة البيانات" و "مزود خدمة الاتصالات".[165]

164. لا يوجد ما يعادلها في اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية
165. انظر التعريفات أعلاه

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
a. شخصًا موجودًا في إقليمها بتقديم بيانات حاسوب محددة في حيازته أو تحت سيطرته، وتُخَزّن في نظام حاسوب أو بوسيلة تخزين بيانات الحاسوب؛ و b. مقدم خدمة يقدم خدماته في إقليم الدولة الطرف بتقديم معلومات المشترك المرتبطة بهذه الخدمات، والتي تكون في حيازة أو تحت سيطرة مقدم الخدمة. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و 15. -3 لأغراض هذه المادة، يعني مصطلح "معلومات المشترك" أي معلومات محفوظة بشكل بيانات حاسوب أو أي شكل آخر ويحتفظ بها مزود الخدمة، وترتبط بالمشتركين في خدماته، بخلاف حركة البيانات أو المحتوى، والتي يمكن إنشاؤها من خلال: نوع خدمة الاتصال المستخدمة والأحكام الفنية المتعلقة بها وفترة الخدمة؛ هوية المشترك أو العنوان البريدي أو الجغرافي، ورقم الهاتف وأرقام الاتصال الأخرى ومعلومات الفوترة والدفع المتاحة بناءً على اتفاقية الخدمة؛ أي معلومات أخرى متاحة على موقع تركيب معدات الاتصالات بناءً على اتفاقية الخدمة أو الترتيب. **القسم 22 من نظام اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - أمر النسخ** إذا كان [قاض] مقتنعًا بناءً على طلب قدمه [ضابط إنفاذ القانون] [الشرطة] بأن بيانات حاسوب محددة أو نسخة مطبوعة أو غيرها من المعلومات ضرورية لإجراء تحقيق جنائي أو لإجراءات جنائية، يجوز [للقاضي] أن يأمر بما يلي: • أن ينسخ شخص في إقليم [الدولة المشترعة] يتحكم في نظام الحاسوب نسخًا محددة من بيانات الحاسوب أو نسخة مطبوعة أو معلومات أخرى واضحة من تلك البيانات؛ أو • مزود خدمة الإنترنت في [الدولة المشترعة] لتقديم معلومات حول الأشخاص المشتركين في الخدمة أو الذين يستخدمونها بطريقة أخرى.		المادة 25 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات هي نموذج يمكن استخدامه ويستخدم تعريفات مختلفة بما في ذلك «تكنولوجيا المعلومات"، و[166] "مزود الخدمة" و[167] "البيانات"؛[168] غير أنه من المستحسن أن تكون هناك تعريفات لـ «معلومات المشترك أو معلومات المشترك الأساسية" أو "حركة البيانات" لأنها ستكون أنواع مختلفة من الأدلة التي يمكن توليدها في دول الجنوب الشريكة. علاوة على ذلك، سوف تتطلب هذه السلطة من الأفراد وغيرهم (مثل الكيانات المؤسسية والمؤسسات المالية وغيرها من المنظمات) ممن يحملون البيانات أن يقوموا بتوليدها بناء على طلب سلطات إنفاذ القانون. يمكن أن تكون المادة 18 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست والمادة 22 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية بمثابة دليل مع التطبيق الثابت للتعريفات

166. المادة 2 (1) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات: "أية وسيلة مادية أو معنوية أو مجموعة وسائل مترابطة أو غير مترابطة تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها وفقا للأوامر والتعليمات المخزونة بها. ويشمل ذلك جميع المدخلات والمخرجات المرتبطة بها سلكيا أو لا سلكيا في نظام أو شبكة".

167. المادة 2 (2) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات: «أي شخص طبيعي أو معنوي عام أو خاص يزود المشتركين بالخدمات للتواصل بواسطة تقنية المعلومات، أو يقوم بمعالجة أو تخزين المعلومات نيابة عن خدمة الاتصالات أو مستخدميها».

168. المادة 2 (3) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات: «كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة تقنية المعلومات، كالأرقام والحروف والرموز وما إلى ذلك».

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 25 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - أمر تسليم المعلومات تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى: 1. أي شخص في إقليمها لتسليم معلومات معينة في حيازة ذلك الشخص والمخزنة على تقنية معلومات أو وسيط تخزين معلومات. 2. أي مزود خدمة يقدم خدماته في إقليم الدولة الطرف لتسليم معلومات المشترك المتعلقة بتلك الخدمات في حوزة مزود الخدمة أو تحت سيطرته.		
المادة 21 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[169] **اعتراض بيانات المحتوى** 1. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وغيرها من الإجراءات، فيما يتعلق بمجموعة من الجرائم الخطيرة التي يحددها القانون المحلي، لتمكين سلطاته المختصة من: a. الجمع أو التسجيل من خلال تطبيق الوسائل التقنية على أراضي ذلك الطرف، و b. إلزام مزود الخدمة، في حدود قدرته التقنية الحالية: i. الجمع أو التسجيل من خلال تطبيق الوسائل التقنية على أراضي ذلك الطرف؛ أو ii. التعاون ومساعدة السلطات المختصة في جمع أو تسجيل بيانات المحتوى في الوقت الحقيقي، لاتصالات محددة تتم في أراضيها وترسل عن طريق نظام حاسوبي. 2. في الحالات التي لا يمكن فيها لأي طرف، بسبب المبادئ المستقرة في نظامه القانوني الداخلي، أن يعتمد التدابير المشار إليها في الفقرة 1.أ، يجوز له بدلا من ذلك اعتماد تدابير تشريعية وتدابير أخرى قد تكون ضرورية لضمان جمع أو تسجيل البيانات المرورية المرتبطة باتصالات محددة مرسلة في أراضيه، في الوقت الحقيقي، من خلال تطبيق الوسائل التقنية على ذلك الإقليم.	**قانون الإجراءات الجنائية** **المواد 95 و 206 و 206 مكرر** **المادة 95** «لقاضي التحقيق أن يأمر بضبط جميع الخطابات والرسائل والجرائد والمطبوعات والطرود لدى مكاتب البريد وجميع البرقيات لدى مكاتب البرق وأن يأمر بمراقبة المحادثات السلكية واللاسلكية أو إجراء تسجيلات لأحاديث جرت في مكان خاص متى كان لذلك فائدة في ظهور الحقيقة في جناية أو جنحة معاقب عليها بالحبس لمدة تزيد على ثلاثة أشهر. وفي جميع الأحوال يجب أن يكون الضبط أو الاطلاع أو المراقبة أو التسجيل بناء على أمر معلّل ولمدة لا تزيد على ثلاثين يوما قابلة للتجديد لمدة أو لمدد أخرى مماثلة» **قانون الاتصالات** 10/2003 **المادة 19** تلتزم جميع الجهات والشركات العاملة في مجال الاتصالات بموافاة الجهاز القومي لتنظيم الاتصالات بما يطلبه من تقارير أو إحصاءات أو معلومات تتصل بنشاطه عدا ما يتعلق منها بالأمن القومي.	**التحليل القانوني** لقاضي التحقيق/أو النائب العام أن يأمر (عبر أمر قضائي صادر عن قاضٍ) بتسجيل محادثات سلكية ولاسلكية في ظروف معينة عَملاً بالمواد 95 و 206 و 206 مكرر. لا يشير قانون الإجراءات الجنائية إلى المحادثات التي تتم عبر الإنترنت أو أجهزة الحاسوب، ولم يتم البت في القضية من قبل محكمة النقض المصرية. يتم إرسال طلبات المساعدة القانونية المتبادلة إلى مكتب التعاون الدولي في النيابة العامة. يتم إرسال الطلب إذا وافق عليه النائب العام إلى إدارة المعلومات والوثائق بوزارة الداخلية المصرية التي تقوم بتنفيذ الاعتراض من خلال ضباط الشرطة المدربين. يقوم هؤلاء الضباط بإعداد تقرير حول النتيجة «دون إعطاء أي تفاصيل حول خطوات وتقنيات الاعتراض". يجب على ضباط الشرطة الذين يقومون بعمليات اعتراض «رسائل البريد الإلكتروني وعناوين بروتوكول الإنترنت وحسابات شبكات التواصل الاجتماعي» القيام بذلك دون انتهاك خصوصية الأفراد الآخرين. يتم كتابة أسس كل عمل اعتراض في قانون الإجراءات الجنائية مع الشروط اللازمة لإصدار مثل هذا القرار من قاضي التحقيق. **تحليل الفجوة** **التوصيات:** يجب اتخاذ تدابير محددة لإلزام مزودي خدمات الاتصالات في مصر بالتعاون لجمع المحتوى في الوقت الفعلي؛ ويجب إدراج ضمانات لضمان أن جمعها قانوني وضروري ومعقول ومتناسب مع الحالة. يجب مراعاة مراجعة المادة 29 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات والمادة 21 من اتفاقية بودابيست والقسم 26 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية وإدراج اللغة في التشريعات الوطنية

169. لا يوجد ما يعادلها في اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
3. يعتمد كل طرف التدابير التشريعية والتدابير الأخرى التي قد تكون ضرورية لإلزام مقدم الخدمة بالحفاظ على سرية تنفيذ أي سلطة منصوص عليها في هذه المادة وأي معلومات تتعلق بها. 4. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و 15. **القسم 26 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - اعتراض بيانات المحتوى** 1. إذا تأكد [قاضٍ] بناء على [شهادة تحت القسم] [شهادة خطية] بأن هناك أسباباً معقولة لـ [الاشتباه] [الظن] بأن محتوى البلاغات الإلكترونية هو مطلوب بشكل معقول لأغراض [التحقيق] في تحقيق جنائي، [يجوز] [للقاضي] [يجب] أن: • يطلب من مزود خدمة الإنترنت الذي تتوفر خدمته في [بلد المشرع] جمع أو تسجيل أو السماح أو مساعدة السلطات المختصة في جمع أو تسجيل بيانات المحتوى المرتبطة بالاتصالات المحددة التي يتم إرسالها عن طريق نظام حاسوب، وذلك من خلال استخدام وسائل تقنية؛ أو • السماح لموظف [قوة تنفيذ القانون] [الشرطة] بجمع أو تسجيل تلك البيانات من خلال تطبيق الوسائل التقنية. 2. قد تقرر دولة عدم تنفيذ القسم 26. **المادة 29 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات- اعتراض معلومات المحتوى** 1. تلتزم كل دولة طرف باعتماد الإجراءات التشريعية اللازمة المتعلقة بسلسلة من الجرائم المنصوص عليها في القانون المحلي، وذلك لتمكين السلطات المختصة من: a. تسجيل أو جمع المعلومات من خلال الوسائل التقنية في أراضي هذه الدولة الطرف، أو b. التعاون مع السلطات المختصة ومساعدتها على تسريع جمع وتسجيل معلومات المحتوى الخاصة بالاتصالات ذات الصلة في إقليمها والتي يتم نقلها عن طريق تكنولوجيا المعلومات.	**المادة 64** "يلتزم مشغلو ومقدمو خدمات الاتصالات والتابعون لهم وكذلك مستخدمو هذه الخدمات بعدم استخدام أية أجهزة لتشفير خدمات الاتصالات إلا بعد الحصول على موافقة من كل من الجهاز القومي لتنظيم الاتصالات والقوات المسلحة وأجهزة الأمن القومي، ولا يسري ذلك على أجهزة التشفير الخاصة بالبث الإذاعي والتليفزيوني. ومع مراعاة حرمة الحياة الخاصة للمواطنين التي يحميها القانون يلتزم كل مشغل أو مقدم خدمة أن يوفر على نفقته داخل شبكة الاتصالات المرخص له بها كافة الإمكانيات الفنية من معدات ونظم وبرامج واتصالات داخل شبكة الاتصالات والتي تتيح للقوات المسلحة وأجهزة الأمن القومي ممارسة اختصاصها في حدود القانون. على أن يتزامن تقديم الخدمة مع توفير الإمكانيات الفنية المطلوبة. كما يلتزم مقدمو ومشغلو خدمات الاتصالات ووكلائهم المنوط بهم تسويق تلك الخدمات بالحصول على معلومات وبيانات دقيقة عن مستخدميها من المواطنين ومن الجهات المختلفة بالدولة".	

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
2. إذا تعذر على الدولة الطرف، بسبب النظام القانوني المحلي، اعتماد الإجراءات المبينة في الفقرة 1 (أ)، يجوز لها اعتماد إجراءات أخرى بالشكل الضروري لضمان تسريع جمع وتسجيل معلومات المحتوى المقابلة الاتصالات ذات الصلة في أراضيها باستخدام الوسائل التقنية في ذلك الإقليم. 3. تلتزم كل دولة طرف باعتماد الإجراءات اللازمة لمطالبة مقدم الخدمة بالحفاظ على سرية أي معلومات عند ممارسة السلطة المنصوص عليها في هذه المادة.		
المادة 20 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[170] **جمع بيانات حركة الاتصالات في الوقت الحقيقي** 1. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتمكين سلطاته المختصة من: a. الجمع أو التسجيل من خلال تطبيق الوسائل التقنية على أراضي ذلك الطرف، و b. إلزام مزود الخدمة، في حدود قدرته التقنية الحالية: i. الجمع أو التسجيل من خلال تطبيق الوسائل التقنية على أراضي ذلك الطرف؛ أو ii. التعاون ومساعدة السلطات المختصة في الجمع أو التسجيل، بيانات حركة الاتصالات المرتبطة باتصالات محددة في أراضيها، والمرسلة عن طريق نظام حاسوب، وذلك في الوقت الحقيقي. 2. في الحالات التي لا يمكن فيها لأي طرف، بسبب المبادئ المستقرة في نظامه القانوني الداخلي، أن يعتمد التدابير المشار إليها في الفقرة 1.أ، يجوز له بدلا من ذلك اعتماد تدابير تشريعية وتدابير أخرى قد تكون ضرورية لضمان جمع أو تسجيل البيانات المرورية المرتبطة باتصالات محددة مرسلة في أراضيه، في الوقت الفعلي، من خلال تطبيق الوسائل التقنية على ذلك الإقليم.	**قانون الإجراءات الجنائية** **المواد** 95 و 206 و 206 **مكرر** **قانون الاتصالات** 10/2003 **المادتان** 19 و 64	**التحليل القانوني** على النحو الوارد أعلاه، بالنسبة لاعتراض بيانات المحتوى، يمكن الاستعانة بقانون الإجراءات الجنائية وقانون الاتصالات لجمع حركة البيانات في الوقت الفعلي. ومع ذلك، قد يكون هناك حد أدنى لجمع حركة البيانات في الوقت الفعلي. قد تكون هناك حالات لا يضع فيها مقدم الطلب حدًا قانونيًا أعلى لتأمين المحتوى، ولكن يمكن وجود حد أدنى لتأمين حركة البيانات. لهذا السبب، يجب أن يكون هناك تمييز بين جمع المحتوى المخزن وحركة البيانات في الوقت الحقيقي. يجب أن تكون هناك ضمانات ومتطلبات/إجراءات لإلزام مزودي خدمة الاتصالات على التعاون في جمع أو تسجيل بيانات المحتوى في الوقت الفعلي لاتصالات محددة تتم في مصر **تحليل الفجوة** **التوصيات:** ينبغي توفير صلاحية محددة لجمع حركة البيانات في الوقت الفعلي، وينبغي إدراج حكم لإلزام مزودي خدمة الاتصالات في مصر على التعاون لجمع حركة البيانات في الوقت الفعلي؛ ويجب إدراج ضمانات لضمان أن جمعها قانوني وضروري ومعقول ومتناسب مع الحالة. يمكن اعتماد اللغة من المادة 28 الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لكنها لا تشير إلى الجمع المستعجل في الوقت الحقيقي. تسمح المادة 31 (3) (ه) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية بجمع البيانات في الوقت الحقيقي، لكن هنالك حاجة إلى ضمانات. لذلك، يجب استخدام المادة 20 من اتفاقية بودابست والقسم 25 من مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية باعتبارهما دليلاً للتشريعات الوطنية

170. المادة 31 (3) (هـ) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية - تشير المادة 28 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات إلى الجمع المستعجل بدلاً من الجمع في الوقت الفعلي

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
3. يعتمد كل طرف التدابير التشريعية والتدابير الأخرى التي قد تكون ضرورية لإلزام مقدم الخدمة بالحفاظ على سرية تنفيذ أي سلطة منصوص عليها في هذه المادة وأي معلومات تتعلق بها. 4. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و 15. **القسم 25 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - جمع بيانات حركة الاتصالات** 1. إذا تأكد [قاض] بناء على [شهادة تحت القسم] [شهادة خطية] بأن هناك أسباباً معقولة لـ [الاشتباه] [الظن] بأن بيانات حركة الاتصالات المرتبطة ببلاغ محدد ضرورية بشكل معقول لأغراض [التحقيق] في تحقيق جنائي، [يجوز] [للقاضي] [يجب] أن يأمر شخصًا يتحكم بهذه البيانات بما يلي: • جمع أو تسجيل بيانات حركة الاتصالات المرتبطة باتصالات محددة خلال فترة محددة؛ أو • التصريح ومساعدة ضابط [الشرطة] [قوة تنفيذ القانون] محدد لجمع أو تسجيل تلك البيانات. 2. إذا تأكد [قاض] بناء على [شهادة تحت القسم] [شهادة خطية] بأن هناك أسباباً معقولة لـ [الاشتباه] [الظن] بأن بيانات حركة الاتصالات المرتبطة ببلاغ محدد ضرورية بشكل معقول لأغراض [التحقيق] في تحقيق جنائي، [يجوز] [للقاضي] [يجب] أن يسمح لـ [قوة تنفيذ القانون] [الشرطة] بجمع أو تسجيل بيانات حركة الاتصالات المرتبطة برسالة محددة خلال فترة محددة من خلال تطبيق الوسائل التقنية. 3. قد تقرر دولة عدم تنفيذ القسم 25.		

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
	قانون الاتصالات رقم 10 لسنة 2003 **المادة 64** "يلتزم مشغلو ومقدمو خدمات الاتصالات والتابعون لهم وكذلك مستخدمو هذه الخدمات بعدم استخدام أية أجهزة لتشفير خدمات الاتصالات إلا بعد الحصول على موافقة من كل من الجهاز القومي لتنظيم الاتصالات والقوات المسلحة وأجهزة الأمن القومي، ولا يسري ذلك على أجهزة التشفير الخاصة بالبث الإذاعي والتليفزيوني. ومع مراعاة حرمة الحياة الخاصة للمواطنين التي يحميها القانون يلتزم كل مشغل أو مقدم خدمة أن يوفر على نفقته داخل شبكة الاتصالات المرخص له بها كافة الإمكانيات الفنية من معدات ونظم وبرامج واتصالات داخل شبكة الاتصالات والتي تتيح للقوات المسلحة وأجهزة الأمن القومي ممارسة اختصاصها في حدود القانون. على أن يتزامن تقديم الخدمة مع توفير الإمكانيات الفنية المطلوبة. كما يلتزم مقدمو ومشغلو خدمات الاتصالات ووكلائهم المنوط بهم تسويق تلك الخدمات بالحصول على معلومات وبيانات دقيقة عن مستخدميها من المواطنين ومن الجهات المختلفة بالدولة".	**التحليل القانوني** تمنع هذه المادة استخدام الأجهزة المشفرة - مثل أجهزة مقفلة برقم تعريف شخصي. تتيح المادة أيضًا توفير برنامج للوصول إلى الخدمات المشفرة. ليس من الواضح ما إذا كان هناك أي حكم خاص بالإنفاذ من عدمه. **تحليل الفجوة** **التوصيات:** يمكن اعتبار ذلك من الصلاحيات الكبيرة للغاية وغير قابلة للتنفيذ في ضوء عدد الأجهزة المشفرة وتطبيقات الرسائل - كما أن الصلاحية القابلة للتطبيق لتحرير مفاتيح كلمات المرور لإلغاء قفل الأجهزة على أساس كل حالة على حدة من أحكام القانون البريطاني[171]
		التزامات الاحتفاظ بالبيانات[172] 1. تسمح مثل هذه السلطة لوكالات إنفاذ القانون بـ 2. تتبع وتحديد مصدر الاتصال 3. تحديد وجهة الاتصال؛ 4. تحديد تاريخ ووقت ومدة الاتصال؛ و 5. تحديد نوع الاتصال مصر ليس لديها هذا النوع من الالتزام[173]

171. انظر مثلاً القسم 49 من القانون الانجليزي (Regulation of Investigatory Powers Act 2000 (UK - http://www.legislation.gov.uk/ukpga/2000/23/section/49

172. أصدر الاتحاد الأوروبي في عام 2006 توجيهه بشأن الاحتفاظ بالبيانات - اضطرت الدول الأعضاء في الاتحاد الأوروبي إلى تخزين بيانات الاتصالات الإلكترونية لمدة ستة أشهر على الأقل و 24 شهراً على الأكثر للتحقيق في الجرائم الخطيرة وكشفها ومقاضاة مرتكبيها. أبطلت محكمة العدل الأوروبية في عام 2014 توجيه الاحتفاظ بالبيانات، حيث قررت أنها قدمت ضمانات غير كافية ضد التدخلات في الخصوصية وحماية البيانات. في حالة عدم وجود توجيه صالح للاتحاد الأوروبي بشأن الاحتفاظ بالبيانات، فقد تواصل الدول الأعضاء تقديم خطة للاحتفاظ بالبيانات - للاطلاع على الخطط الوطنية، انظر: http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention

173. تقرير ICMEC العالمي ، الصفحة 25

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 22 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[174] **الاختصاص القضائي** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وغيرها من الإجراءات لإقامة ولاية قضائية على أي جرم منصوص عليه في المواد من 2 إلى 11 من هذه الاتفاقية، عندما تُرتكب الجريمة: a. في أراضيها؛ أو b. على متن سفينة ترفع علم تلك الدولة الطرف؛ أو c. على متن طائرة مسجلة بموجب قوانين ذلك الطرف؛ أو d. من قِبَل أحد رعاياها، إذا كانت الجريمة معاقبًا عليها بموجب القانون الجنائي حيث ارتكبت، أو إذا ارتكبت الجريمة خارج الولاية الإقليمية لأي دولة. 2. يجوز لكل طرف أن يحتفظ بالحق في عدم تطبيق أو تطبيق قواعد الاختصاص المنصوص عليها في الفقرات من 1 إلى 1 د من هذه المادة أو أي جزء منها فقط في حالات أو شروط محددة. 3. يعتمد كل طرف ما قد يلزم من إجراءات لإقامة ولاية قضائية على الجرائم المشار إليها في الفقرة 1 من المادة 24 من هذه الاتفاقية، في الحالات التي يكون فيها الجاني المفترض موجودا في إقليمه ولا يسلمه إلى بلد آخر بعد طلب التسليم على أساس جنسيته فقط. 4. لا تستبعد هذه الاتفاقية أي ولاية قضائية جنائية يمارسها أي طرف وفقًا لقانونه الداخلي. 5. عندما يطالب أكثر من طرف بالولاية القضائية على جريمة مفترضة تم النص عليها في هذه الاتفاقية، يتشاور الطرفان المعنيان، عند الضرورة من أجل تحديد الولاية القضائية الأنسب. **القسم 19من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الولاية القضائية** ينطبق هذا القانون على أي فعل أو تقصير: • في إقليم [الدولة المشترعة]؛ أو • على سفينة أو طائرة مسجلة في [الدولة المشترعة]؛ أو	**لا يوجد معادل**	**التحليل القانوني** بدون وجود نطاق محدد بوضوح للجرائم الإلكترونية ، وهي دولية بطبيعتها سيبقى أي تشريع مقيدًا. **تحليل الفجوة** **التوصيات:** يضمن التشريع الوطني أن يتم تعريف الاختصاص باستخدام لغة المادة 22 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست، القسم 19 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية أو المادة 30 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. إذا كان هناك تعارض بين السلطات القضائية، فيجب أن تؤخذ في الاعتبار المبادئ التوجيهية المتعلقة بتحديد الولاية القضائية المناسبة لمحاكمة جريمة ما - انظر المبادئ التوجيهية يوروجست لتقرير الولاية القضائية التي في الجرائم التي تجب ملاحقتها (المراجعة 2016)[175]

174. لا يوجد ما يعادلها في اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية
175. http://www.eurojust.europa.eu/Practitioners/operational/Documents/Operational-Guidelines-for-Deciding.pdf

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
• من قبل أحد مواطني [الدولة المشترعة] خارج الولاية القضائية لأي بلد؛ أو من قبل أحد مواطني [الدولة المشترعة] خارج إقليم [الدولة المشترعة]، إذا كان سلوك هذا الشخص يشكل أيضًا جريمة بموجب قانون البلد الذي ارتكبت فيه الجريمة. **المادة 30 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - الاختصاص** 1. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد اختصاصها على أي من الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية وذلك إذا ارتكبت الجريمة كلياً أو جزئياً أو تحققت: a. في إقليم الدولة الطرف b. على متن سفينة تحمل علم الدولة الطرف. c. على متن طائرة مسجلة تحت قوانين الدولة الطرف. d. من قبل أحد مواطني الدولة الطرف إذا كانت الجريمة يعاقب عليها حسب القانون الداخلي في مكان ارتكبها أو إذ ارتكبت خارج منطقة الاختصاص القضائي لأية دولة. e. إذا كانت الجريمة تمس أحد المصالح العليا للدولة. 2. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد الاختصاص الذي يغطي الجرائم المنصوص عليها في الفقرة 1 من المادة 31 من هذه الاتفاقية في الحالات التي يكون فيها الجاني المزعوم حاضرا في إقليم تلك الدولة الطرف ولا يقوم بتسليمه إلى طرف آخر بناء على جنسيته بعد طلب التسليم. 3. إذا ادعت أكثر من دولة بالاختصاص القضائي لجريمة منصوص عليها في هذه الاتفاقية فيقدم طلب الدولة التي أخلت الجريمة بأمنها أو بمصالحها ثم الدولة التي وقعت الجريمة في إقليم ثم الدولة التي يكون الشخص المطلوب من رعاياها وإذا اتحدت الظروف فتقدم الدولة الأسبق في طلب التسليم. في حالة وجود ظروف مماثلة، تُعطى الأولوية لأول دولة تطلب التسليم.		

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 43 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست **الهيئات المتخصصة**[176] 1. تضمن كل دولة طرف، وفقا للمبادئ الأساسية لنظامها القانوني، وجود هيئة متخصصة مكرسة على مدار 24 ساعة في اليوم لضمان تقديم المساعدة العاجلة لأغراض التحقيق أو الإجراءات المتعلقة بجرائم تكنولوجيا المعلومات أو جمع الأدلة بشكل إلكتروني بشأن جريمة محددة. تتضمن هذه المساعدة تسهيل أو تنفيذ: 2. تقديم المشورة الفنية. 3. حماية المعلومات على أساس المادتين 37 و 38. 4. جمع الأدلة وتقديم المعلومات القانونية وتحديد مكان المشتبه بهم. • يجب أن تكون هذه الهيئة في جميع الدول الأطراف قادرة على التواصل الفوري مع الهيئة المقابلة في أي دولة طرف أخرى • إذا كانت الهيئة المذكورة، المعينة من قبل دولة طرف، ليست جزءًا من السلطات المسؤولة عن المساعدة الثنائية الدولية في تلك الدولة، يجب أن تضمن تلك الهيئة قدرتها على التنسيق الفوري مع تلك السلطات. • تضمن كل دولة طرف توافر موارد بشرية قادرة على تيسير عمل الهيئة المذكورة أعلاه.	**لا يوجد معادل**	**التحليل القانوني** هذه آلية أساسية لتحقيق قدرة فعالة على التحقيق في الجرائم الإلكترونية. إن مباحث مكافحة جرائم الحاسبات وشبكات المعلومات، المنشأة بقرار وزير الداخلية رقم 13507 لسنة 2002 (كجزء من الإدارة العامة للمعلومات والتوثيق)، لديها القدرة على اعتراض رسائل البريد الإلكتروني وعناوين بروتوكول الإنترنت وحسابات شبكات التواصل الاجتماعي (دون انتهاك خصوصية الأفراد الآخرين). صممت هذه الشبكة للاستجابة الفورية على مدار الساعة للطلبات الدولية للتحفظ على البيانات **وجمع** الأدلة **وغيرها** من المساعدات للتحقيق في الجرائم السيبرانية (أي تحديد مكان أحد المشتبه بهم) **تحليل الفجوة** **التوصيات:** لا ينبغي أن يتطلب ذلك تشريعًا خاصًا لتنفيذه، وفيما يتعلق بالموارد يجب أن تُعطى الأولوية. وقد يتطلب ذلك فقط توسيع صلاحيات مباحث مكافحة جرائم الحاسبات وشبكات المعلومات المنشأة بالفعل، وذلك بتعيين نقطة اتصال واحدة (SPOC) على مدار الساعة. ويجب مشاركة معلومات الاتصال لنقطة الاتصال الواحدة المعينة على المستوى الوطني ومع السلطات المركزية على المستوى الدولي والإنتربول. ينبغي أيضًا النظر في صياغة مذكرة تفاهم مع الوكالات الوطنية بحيث يكون لدى نقطة الاتصال الوحيدة المعينة سلطة القيام بالإجراءات المطلوبة كجزء من تحقيق دولي في جرائم الإنترنت وتطبيق القوانين والمعاهدات الوطنية. ستتضمن مذكرة التفاهم هذه الطلبات الواردة والصادرة وتضمن عملية فعالة وكفؤة.
المادة 25 من اتفاقية بودابيست **المبادئ العامة المتعلقة بالمساعدة المتبادلة** 1. يقدم الطرفان المساعدة المتبادلة إلى أقصى حد ممكن لغرض إجراء التحقيقات أو الإجراءات المتعلقة بالجرائم الجنائية المتعلقة بأنظمة الحاسوب والبيانات، أو لجمع الأدلة المتعلقة بالجرائم الجنائية في شكل إلكتروني. 2. يعتمد كل طرف أيضًا الإجراءات التشريعية وغيرها من الإجراءات التي قد تكون ضرورية لتنفيذ الالتزامات المنصوص عليها في المواد من 27 إلى 35.		**التحليل القانوني** تضمن المادة 32 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات أنه يمكن استخدامها كأداة لتسهيل المساعدة القانونية المتبادلة[177] وتنص على الحفظ المستعجل لبيانات الحاسوب المخزنة،[178] والحفظ المستعجل والكشف الجزئي لبيانات المرور،[179] والكشف عن البيانات المخزنة[180] وحركة البيانات[181] **لدول الاتفاقية.** **تحليل الفجوة** **التوصيات:** يُنصح بتشريع السلطات الإجرائية المنصوص عليها في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على المستوى الوطني، وبذلك يمكن استخدامها للتحقيقات المحلية وتؤسس لصلاحيات متبادلة لاستخدام الدول التي ليست طرفًا في الاتفاقية

176. المادة 35 من اتفاقية بودابست والمادة 25 (2) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية
177. لا يوجد حكم مماثل في اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية
178. المادة 29 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست والمادة 37 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات
179. المادة 30 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست والمادة 38 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات
180. المادة 31 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست والمادة 39 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات
181. المادة 33 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست والمادة 41 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
3. يجوز لكل طرف في الظروف العاجلة تقديم طلبات للمساعدة المتبادلة أو الاتصالات المتعلقة بها عن طريق وسائل الاتصال العاجلة، بما في ذلك الفاكس أو البريد الإلكتروني، إلى الحد الذي توفر فيه هذه الوسائل مستويات مناسبة من الأمن والمصادقة (بما في ذلك استخدام التشفير، عند الضرورة)، مع تأكيد رسمي لاحق، حيثما يطلب ذلك الطرف متلقي الطلب. يجب على الطرف متلقي الطلب قبول الطلب والرد عليه بأي وسيلة اتصال سريعة. 4. باستثناء ما هو منصوص عليه على وجه التحديد في المواد الواردة في هذا الفصل، تخضع المساعدة المتبادلة للشروط المنصوص عليها في قانون الطرف متلقي الطلب أو معاهدات المساعدة المتبادلة المطبقة، بما في ذلك الأسباب التي تُجيز للطرف متلقي الطلب أن يرفض التعاون. لا يجوز للطرف متلقي أن يبني حقه في رفض المساعدة المتبادلة المتعلقة بالجرائم المشار إليها في المواد من 2 إلى 11، فقط على أساس أن الطلب يتعلق بجريمة يعتبرها جريمة مالية. 5. عندما تسمح أحكام هذا الفصل للطرف متلقي الطلب بتقييد المساعدة المتبادلة بشرط ازدواجية التجريم، يعتبر هذا الشرط مستوفيًا، بصرف النظر عما إذا كانت قوانينه تضع الجريمة في نفس الفئة الجرمية، أو إذا أعطيت الجريمة نفس التسمية عند الطرف الطالب، وذلك إن كان السلوك الكامن وراء الجريمة التي طلبت المساعدة من أجلها جريمة جنائية بموجب قوانينه. **المادة 34 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - الإجراءات المتعلقة بطلبات التعاون والمساعدة المتبادلة** 1. تطبق أحكام الفقرات 2-9 من هذه المادة في حالة عدم وجود معاهدة أو اتفاقية تعاون ومساعدة متبادلة وفقًا للتشريعات المعمول بها بين الدول الأطراف التي تطلب المساعدة وتلك التي تُطلَب منها المساعدة. في حال وجوده جود معاهدة أو اتفاقية فلا تطبق الفقرات المشار إليها إلا إذا اتفقت الأطراف المعنية على تطبيقها كاملة أو بشكل جزئي .		لا تنص الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على اعتراض المحتوى وحركة البيانات في الوقت الحقيقي؛ يجب اعتبار ما نصت عليه اتفاقية بودابست و اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية سوابق في هذا الاتجاه.[182] ومع ذلك، يمكن تطبيق مبدأ المعاملة بالمثل على هذه الأحكام التي تطبق المواد 95 و 206 و 206 مكرر من قانون الإجراءات الجنائية والمادتين 19 و 64 من قانون الاتصالات. ينبغي النظر في السماح للسلطات المختصة بإعطاء الإذن لهيئات إنفاذ القانون المحلي بإجراء تحقيق في الدولة التي تأكد فيها الوصول إلى الجهاز. يعد الوصول إلى المعلومات هو المعيار الأساسي لبدء التحقيق في الحالات التي يتعذر فيها معرفة مكان تخزين البيانات (أي في التخزين السحابي). يمكن أن يشمل ذلك "اعترافًا متبادلًا" بأوامر المحكمة الصادرة تجاه مقدمي خدمات الاتصالات في دولة معينة، والتي يمكن تقديمها إلى فروع مقدمي خدمة العملاء الموجودين في دول أخرى، اعتمادًا على مكان تخزين البيانات.

182. المادتان 33 و 34 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست، والقسمان 25 و 26 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
2. على كل دولة طرف تحديد سلطة مركزية تكون مسؤولة عن إرسال وإجابة طلبات المساعدة المتبادلة وتنفيذ هذه الطلبات وإيصالها إلى السلطات المعنية لتنفيذها. على السلطات المركزية أن تتصل ببعضها مباشرة. على كل دولة طرف- وقت التوقيع أو إيداع أدوات التصديق أو القبول أو الموافقة- أن تتصل بالأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس العدل العرب وتنقل إليهما أسماء وعناوين السلطات المحددة خصيصا لغايات هذه الفقرة. تقوم الأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس وزراء العدل العرب بإنشاء وتحديث سجل للسلطات المركزية والمعينة من قبل الدول الأطراف. وعلى كل دولة طرف أن تتأكد من أن التفاصيل الموجودة في السجل صحيحة دائما 3. يتم تنفيذ طلبات المساعدة المتبادلة في هذه المادة وفقًا للإجراءات التي تحددها الدولة الطرف الطالبة، إلا في حالة عدم الامتثال لقانون الدولة الطرف متلقية طلب المساعدة. 4. يجوز للدولة الطرف المطلوب منها المساعدة أن تؤجل الإجراءات المتخذة بشأن الطلب إذا كانت هذه الإجراءات تؤثر على التحقيقات الجنائية التي تجري من قبل سلطاتها. 5. قبل رفض أو تأجيل المساعدة يجب على الدولة الطرف المطلوب منها المساعدة بعد استشارة الدولة الطرف الطالبة لها أن تقرر فيما إذ سيتم تلبية الطلب جزئيا أو يكون خاضعا للشروط التي قد ترها ضرورية. 6. تلتزم الدولة الطرف المطلوب منها المساعدة أن تُعلم الدولة الطرف الطالبة لها بنتيجة تنفيذ الطلب. وإذا تم رفض أو تأجيل الطلب يجب إعطاء أسباب هذا الرفض أو التأجيل. ويجب على الدولة الطرف المطلوب منها المساعدة أن تعلم الدولة الطرف الطالبة لها بالأسباب التي تمنع تنفيذ الطلب بشكل نهائي أو الأسباب التي تؤخره بشكل كبير.		

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
7. يجوز للدولة الطرف الطالبة للمساعدة أن تطلب من الطرف المطلوب منها المساعدة الإبقاء على سرية حقيقة ومضمون أي طلب يندرج في هذا الفصل ما عدا القدر لكافي لتنفيذ الطلب. وإذا لم تستطع الدولة الطرف المطلوب منها المساعدة الالتزام بهذا الطلب للسرية يجب عليها إعلام الدولة الطرف الطالبة والتي ستقرر مدى إمكانية تنفيذ الطلب. 8. • في الحالات العاجلة يجوز إرسال طلبات المساعدة المتبادلة مباشرة إلى السلطات القضائية في الدولة الطرف المطلوب منها المساعدة من نظيرتها في الدولة الطرف الطالبة لها. وفي مثل هذه الحالات يجب إرسال نسخة الوقت من السلطة المركزية في الدولة الطرف الطالبة إلى نظيرتها في الدولة الطرف المطلوب منها. • يجوز عمل الاتصالات وتقديم الطلبات حسب هذه الفقرة بواسطة الإنتربول. • حيثما يتم تقديم طلب حسب الفقرة أ ولم تكن السلطة مختصة بالتعامل مع الطلب فيجب عليها إحالة الطلب إلى السلطة المختصة وإعلام الدولة الطرف الطالبة للمساعدة مباشرة بذلك. • إن الاتصالات والطلبات التي تتم حسب هذه الفقرة والتي لا تشمل الإجراء القسري يمكن بثها مباشرة من قبل السلطات المختصة في الدولة الطرف الطالبة للمساعدة إلى نظيرتها في الدولة الطرف المطلوب منها المساعدة. • يجوز لكل دولة طرف، وقت التوقيع أو التصديق أو القبول أو الإقرار أو الانضمام إبلاغ الأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس وزراء العدل العرب بأن الطلبات حسب هذه الفقرة يجب توجيهها إلى السلطة المركزية لغايات الفعالية.		

التعاون الدولي		
أفضل الممارسات الدولية	**التشريع الوطني**	**ملاحظات**
المادة 26 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[183] **المعلومات التلقائية** 1. يجوز للطرف، في حدود قانونه الداخلي ودون طلب مسبق، أن يحيل إلى الطرف الآخر المعلومات التي تم الحصول عليها في إطار تحقيقاته، عندما يرى أن الكشف عن هذه المعلومات قد يساعد الطرف المتلقي في بدء أو التحقيقات أو الإجراءات المتعلقة بالجرائم الجنائية المنصوص عليها في هذه الاتفاقية، أو قد تؤدي إلى طلب تعاون من جانب هذا الطرف بموجب هذا الفصل. 2. قبل تقديم هذه المعلومات، يجوز للطرف المقدم أن يطلب الحفاظ على سريتها أو استخدامها فقط وفقًا للشروط. إذا لم يستطع الطرف المتلقي الامتثال لهذا الطلب، فيجب عليه إخطار الطرف المقدم الذي يحدد بعد ذلك ما إذا كان ينبغي تقديم المعلومات. إذا قبل الطرف المتلقي المعلومات وفقًا لهذه الشروط فعليه أن يلتزم بها. **المادة 33 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - المعلومات العرضية المتلقاة** 1. يجوز لأي دولة طرف- ضمن حدود قانونها الداخلي- وبدون طلب مسبق أن تعطي لدولة أخرى معلومات حصلت عليها من خلال تحقيقاتها إذا اعتبرت أن كشف مثل هذه المعلومات يمكن أن تساعد الدولة الطرف المرسلة إليها في إجراء الشروع أو القيام بتحقيقات في الجرائم المنصوص عليها في هذه الاتفاقية أو قد تؤدي إلى طلب للتعاون من قبل تلك الدولة الطرف. 2. قبل إعطاء مثل هذه المعلومات يجوز للدولة الطرف المزودة أن تطلب الحفاظ على سرية المعلومات، وإذا لم تستطع الدولة الطرف المستقبلة الالتزام بهذا الطلب يجب عليها إبلاغ الدولة الطرف المزودة بذلك والتي تقرر بدورها مدى إمكانية التزويد بالمعلومات. وإذا قبلت الدولة الطرف المستقبلة المعلومات مشروطة بالسرية فيجب أن تبقى المعلومات بين الطرفين.	**لا يوجد معادل**	**التحليل القانوني** يعد هذا إجراءً هامًا لتمكين الدولة من الاحتفاظ بمعلومات من شأنها أن تساعد دولة أخرى على منع جريمة الإنترنت أو التحقيق فيها. وعلى الرغم من أن ذلك متاحًا بين الدول التي صدقت على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الوارد ذكرهم في المادة 33 من الاتفاقية، فليس لمصر أي أساس قانوني محلي يجبره بمشاركة هذه المعلومات مع الدول غير الموقعة على الاتفاقية ما لم يتم إرسال طلب رسمي عبر قنوات المساعدة القانونية المتبادلة المعتادة. تنص المادة 18 (4) - (5) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة على تبادل المعلومات الاستخباراتية تلقائيًا في الأمور التي تفي بتعريف جريمة خطيرة[184]، ذات طابع عبر وطني[185] وأن جماعة إجرامية منظمة ضالعة في ارتكاب الجرم[186]. دون استيفاء هذا التعريف، يجب إرسال طلب رسمي عبر قنوات المساعدة القانونية المتبادلة المعتادة إلى الدول التي ليست عضوًا في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. وبسبب الطبيعة السريعة الحركة للجريمة السيبرانية، فإن المشاركة التلقائية هي وسيلة فعالة للتعاون مع الدول الأخرى، وغياب هذه المشاركة يمنع التعاون الدولي الفعال مع الدول غير العضو في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. **تحليل الفجوة** **التوصيات:** استخدمت اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة المادة 18 (4) - (5) أساسًا لمشاركة المعلومات التي تدخل ضمن مجال هذه الاتفاقية بشكل تلقائي (مع ضمانات مقدمة حول الاستخدام في الأدلة أو الكشف عن المعلومات الحساسة لطرف ثالث (بما في ذلك دولة أخرى).[187] النظر في التشريعات القائمة على المادة 33 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات أو المادة 26 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست.

183. المادة 33 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - لا يوجد حكم مماثل في اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية
184. يقصد بتعبير «جريمة خطيرة» في المادة 2 (ب) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة أي سلوك يمثل جرما يعاقب عليه بالحرمان التام من الحرية لمدة لا تقل عن أربع سنوات أو بعقوبة أشد"
185. المادة 3 (1) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية
186. تُعرّف المادة 2 (أ) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة «الجماعة الإجرامية المنظمة» بأنها جماعة ذات هيكل تنظيمي، مؤلفة من ثلاثة أشخاص أو أكثر، موجودة لفترة من الزمن وتعمل بصورة متضافرة بهدف ارتكاب واحدة أو أكثر من الجرائم الخطيرة أو الأفعال المجرمة وفقا لهذه الاتفاقية، من أجل الحصول، بشكل مباشر أو غير مباشر، على منفعة مالية أو منفعة مادية أخرى"
187. انظر المادة 33 (2) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 32 من اتفاقية بودابيست **الوصول عبر الحدود إلى بيانات الحاسوب المخزنة بموافقة أو عندما تكون متاحة للجمهور** يجوز للطرف، دون إذن من طرف آخر: الوصول إلى بيانات الحاسوب المخزنة (مفتوحة المصدر) المتاحة للجمهور، بغض النظر عن مكان وجود البيانات جغرافيا؛ أو الوصول إلى بيانات الحاسوب المخزنة الموجودة لدى طرف آخر أو استلامها، من خلال نظام حاسوب في إقليمها، إذا حصل الطرف على موافقة مشروعة وطوعية من الشخص الذي لديه السلطة القانونية للكشف عن البيانات للطرف من خلال نظام الحاسوب هذا. **القسم 27 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - البرامج الشرعية** 1. إذا كان [القاضي] [قاضي التحقيق] مقتنعًا بناءً على [معلومات مقدمة تحت القَسَم] [شهادة خطية] أنه في سياق تحقيق متعلق بجريمة مدرجة في الفقرة 7 أدناه، توجد أسباب معقولة للاعتقاد بأنه لا يمكن جمع الأدلة الأساسية عن طريق تطبيق أحكام أخرى مدرجة في الجزء الرابع ولكنها ضرورية لأغراض التحقيق الجنائي، فإن [القاضي] [القاضي] [أن] يأذن لضابط [إنفاذ القانون] [الشرطة] بناءً على طلب باستخدام برنامج شرعي عن بعد في مهمة محددة ضرورية للتحقيق وتثبيته في نظام الحاسوب المشتبه به من أجل جمع الأدلة ذات الصلة. يجب أن يحتوي الطلب على المعلومات التالية: • المشتبه في ارتكابه الجريمة، إذا كان ذلك ممكنا مع الاسم والعنوان؛ و • وصف نظام الحاسوب المستهدف؛ و • وصف الوسيلة المقصود ومدى ومدة الاستخدام؛ و • أسباب ضرورة الاستخدام.	**لا يوجد معادل**	**التحليل القانوني** تمكن هذه السلطة الإجرائية الدولة من تأمين المحتوى المخزن في دولة أخرى في ظروف محدودة. المادة 32 ب. إن اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست والمادة 40 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات هما استثناء من مبدأ الإقليمية وتسمحان بوصول منفرد عبر الحدود دون الحاجة إلى مساعدة قانونية متبادلة عندما تكون هناك موافقة أو تكون المعلومات متاحة للجمهور. أمثلة على استخدام هذه السلطة الإجرائية بموجب المادة 32 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست تتضمن: قد يتم تخزين البريد الإلكتروني لشخص ما في بلد آخر بواسطة مزود خدمة، أو قد يقوم شخص ما بتخزين البيانات عن قصد في بلد آخر. يجوز لهؤلاء الأشخاص استرداد البيانات بشرط أن يكون لديهم السلطة القانونية التي تخولهم ذلك، ويجوز لهم الكشف طوعًا عن البيانات لموظفي إنفاذ القانون أو السماح لهؤلاء المسؤولين بالوصول إلى البيانات[188] يمكن اعتقال إرهابي مشتبه به بشكل قانوني عندما يكون بريده الإلكتروني، الذي قد يحوي دليلًا على ارتكاب جريمة، مفتوحًا على الجهاز اللوحي أو الهاتف الذكي أو أي جهاز آخر. إذا وافق المشتبه طوعًا على وصول الشرطة إلى الحساب وإذا كانت الشرطة متأكدة من وجود بيانات صندوق البريد في ولاية أخرى، يجوز للشرطة الوصول إلى البيانات بموجب المادة 32. ب. **تحليل الفجوة** **التوصيات:** تم تضمين هذه السلطة التي تؤمن الأدلة من طرف واحد في التشريعات مع ضمانات الحصول على الموافقة بشكل قانوني من المستخدم.[189] يمكن استخدام لغة المادة 32 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست والمادة 40 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. تم انتقاد المادة 32 (ب) بشدة، ويمكن اعتبار أن موافقة الدولة التي تُخزَّن لديها بيانات الحاسوب قد تم الحصول عليها بالإضافة إلى المستخدم. ينص القسم 27 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية على البرامج الشرعية وهذا قد يسمح بالوصول إلى جهاز حاسوب في دولة أخرى. هناك عدد من القيود التي تشترط عدم إمكانية الحصول على الأدلة بوسائل أخرى، وتتطلب أمرًا قضائيًا، ويمكن أن تُطبَّق على جرائم معينة فقط ضمن مدة مقيدة (3 أشهر). يجب أيضًا إيلاء الاعتبار لموافقة الدولة الأخرى التي قد يتطفل عليها البرنامج الشرعي.

188. الفقرة 294، الصفحة 53 من التقرير الإيضاحي في اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست
189. يجب الانتباه لمواقف مثل عدم وجود المستخدم (في حالة الوفاة) وإذا كان يمكن الحصول على موافقة في دولة أخرى

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
2. من الضروري التأكد في مثل هذا التحقيق من أن التعديلات التي يتم إدخالها على نظام الحاسوب الخاص بالمشتبه به مقصورة على تلك الضرورية للتحقيق وأن أي تغييرات يمكن التراجع عنها إذا أمكن بعد نهاية التحقيق. أثناء التحقيق، من الضروري تسجيل الدخول • الوسيلة الفنية المستخدمة ووقت وتاريخ التطبيق؛ و • تحديد نظام الحاسوب وتفاصيل التعديلات التي تمت خلال التحقيق؛ • أي معلومات تم الحصول عليها. يجب حماية المعلومات التي يتم الحصول عليها عن طريق استخدام هذا البرنامج من أي تعديل أو حذف غير مصرح به أو وصول غير مصرح به. 3. تقتصر مدة الترخيص في القسم 27 (1) على [3 أشهر]. يتم إيقاف الإجراء المتخذ على الفور إذا لم تعد شروط الترخيص مستوفاة. 4. يتضمن ترخيص تثبيت البرنامج الوصول عن بُعد إلى نظام الحاسوب المشتبه به. 5. إذا كانت عملية التثبيت تتطلب الوصول الفعلي إلى مكان ما، يجب استيفاء متطلبات القسم 20. 6. يجوز لضابط [تطبيق القانون] [الشرطة] أن يطلب من المحكمة أن تأمر مقدم خدمة بالمساعدة في عملية التسليم إذا لزم الأمر، وذلك بموجب أمر المحكمة الممنوح في (1) الطلب المذكور أعلاه. 7. [قائمة الجرائم]. 8. قد تقرر دولة عدم تنفيذ القسم 27. **المادة 40 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - الوصول إلى معلومات تقنية المعلومات عبر الحدود** يجوز لأي دولة طرف، وبدون الحصول على تفويض من دولة طرف أخرى: 1. أن تصل إلى معلومات تقنية المعلومات المتوفرة للعامة (مصدر مفتوح) بغض النظر عن الموقع الجغرافي للمعلومات. 2. أن تصل أو تستقبل- من خلال تقنية المعلومات في إقليمها- معلومات تقنية المعلومات الموجودة لدى الدولة الطرف الأخرى وذلك إذا كانت حاصلة على الموافقة الطوعية والقانونية من الشخص الذي يملك السلطة القانونية لكشف المعلومات إلى تلك الدولة الطرف بواسطة تقنية المعلومات المذكورة.		

إسرائيل

أودعت إسرائيل صك انضمامها إلى اتفاقية بودابست يوم 9 مايو 2016.

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 2 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست - الوصول غير المشروع يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لتجريم الوصول إلى النظام الكلي أو أي جزء من نظام الحاسوب، إذا ارتكب عمدًا، دون أي حق. قد يشترط طرف ما ارتكاب الجريمة عن طريق انتهاك إجراءات أمنية بقصد الحصول على بيانات الحاسوب أو نية أخرى غير نزيهة، أو فيما يتعلق بنظام حاسوب متصل بنظام حاسوب آخر.	**قانون أجهزة الحاسوب** 1995 **القسم 4** يُعاقب بالحبس مدة ثلاث سنوات كل من اخترق بطريقة غير قانونية مواد الحاسوب الموجودة في جهاز حاسوب؛ لهذا الغرض، يُقصد بعبارة «اختراق مواد الحاسوب» - الاختراق عن طريق الاتصال أو الربط بجهاز حاسوب، أو عن طريق تشغيله، ولكن باستثناء اختراق مواد الحاسوب التي تشكل التنصت بموجب قانون التنصت، 5729 - 1979. **القسم 5** يُعاقب بالحبس مدة خمس سنوات كل من يقوم بعمل محظور بموجب القسم 4، لغايات ارتكاب جريمة بموجب أي قانون، باستثناء هذا القانون.	**التحليل القانوني** تشير اتفاقية بودابست إلى عبارة «بدون حق" يشير القسم 4 من التشريع الوطني إلى اختراق «مواد الحاسوب" "بطريقة غير قانونية" وتجرّم فقط الوصول إلى أي مادة من "مواد الحاسوب" وليس قفلها، ويشكل نشاط الحصول على المعلومات جريمة، مثل جريمة انتهاك الخصوصية أو الحصول على مادة أو سرقة عن طريق الاحتيال أو الخداع لا يتطلب القانون الإسرائيلي سوى القصد لارتكاب جريمة خطيرة (أي الظروف المشددة). ويعد الاختراق غير القانوني المخالف للقسم 4 بمثابة جريمة قائمة بذاتها. ويتفق ذلك مع اتفاقية بودابست، والتي لا تتطلب إثبات أن الوصول غير القانوني كان لغايات ارتكاب جريمة أخرى.
المادة 3 من اتفاقية بودابيست - اعتراض غير قانوني	**قانون التنصت على المكالمات الهاتفية** **القسم 2**	**التحليل القانوني** ينص القسم 2 من قانون التنصت على المكالمات الهاتفية على هذه الجريمة الجنائية، وتعتبر جريمة الاعتراض غير القانوني جريمة أساسية لملاحقة عمليات النقل غير العامة لبيانات الحاسوب إلى نظام حاسوبي أو منه أو داخله، والتي قد يتم اعتراضها بشكل غير قانوني للحصول على معلومات حول موقع الشخص (على سبيل المثال استهداف ذلك الشخص).[190]

190. http://www.coe.int/en/web/cybercrime/guidance-notes

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 4 من اتفاقية بودابست - التشويش على البيانات	**قانون أجهزة الحاسوب 1995** **القسمان 2 و 6** 2. يعاقب بالسجن لمدة ثلاث سنوات كل شخص يقوم بأحد الأفعال التالية: (1) ... (2) يحذف مواد الحاسوب أو يغيرها أو يعطلها بأي طريقة أخرى أو يتداخل مع استخدامها. 6. (أ) الشخص الذي يقوم بتكوين برنامج ما بطريقة تمكنه من التسبب في تلف أو خلل بحاسوب أو مواد حاسوب غير محددة، للتسبب بشكل غير قانوني في تلف أو خلل بحاسوب أو مواد حاسوب، سواء كانت محددة أو غير محددة، (ب) يعاقب بالحبس مدة خمس سنوات كل شخص ينقل برنامجًا إلى برنامج آخر، أو يتسلل إلى حاسوب آخر، وهو برنامج قادر على التسبب في تلف أو خلل كما هو مذكور في القسم الفرعي (أ)، للتسبب بشكل غير قانوني في حدوث التلف أو الخلل السابق ذكرهما.	**التحليل القانوني** تشير اتفاقية بودابست إلى عبارة «بدون حق» والتشريع الوطني إلى "بشكل غير قانوني" على أساس أن الوصول غير مصرح به. وتشير الجريمة الوطنية في القسم 2 (2) إلى حذف عبارة "مواد الحاسوب" وليس هناك أي شرط لإظهار الحذف الذي تسبب في الخلل أو التلف.[191] تشمل الجريمة الواردة في القسم 6 إنشاء شبكات الحواسيب التي تؤدي إلى إحداث تلف أو حذف أو تدهور أو تغيير أو منع إذا كان هناك أي حذف أو «منع لبيانات" كما هو محدد في المادة 4 من اتفاقية بوادبست، فإن الجريمة الواردة في القسم 2 تكون ذات صلة.
المادة 5 من اتفاقية بودابست - التشويش على النظام	**قانون أجهزة الحاسوب 1995** **القسم 2** يعاقب بالسجن لمدة ثلاث سنوات كل شخص يقوم بأحد الأفعال التالية: (1) يعطل التشغيل السليم لجهاز الحاسوب أو يتداخل مع استخدامه؛	**التحليل القانوني** يشير قانون الحواسيب إلى عبارة تعطيل «تشغيل الحاسوب" في القسم 2 (1) **تحليل الفجوة** **التوصيات:** ضع في اعتبارك ما إذا كان منع ومكافحة الهجمات ضد البنية التحتية الحيوية يحتاج إلى جريمة منفصلة أو مشددة على سبيل المثال، قد يتم إعاقة عمل نظام الحاسوب لأغراض إرهابية (يمكن أن تؤدي إعاقة النظام الذي يخزن سجلات البورصة إلى أن تكون البيانات غير دقيقة، أو أن تعيق عمل البنية التحتية الحيوية).[192]

191. فيما يخص قضية إسرائيل ضد ريفاييلي أوديد، اتُهم السيد ريفاييلي بالتطفل الحاسوبي من حاسوب خارجي على الحاسوب الخاص بصاحب عمله السابق وقام بحذف أي أدلة. وقضت المحكمة أن التفسير الصحيح والمعقول للمادة 2 (2) من قانون الحاسوب هو أن أي حذف و/أو تحويل لمواد الحاسوب يكون محظورًا بموجب قانون الحاسوب ولا يُطلب إثبات أن الحذف تسبب في أي تلف أو خلل.

192. http://www.coe.int/en/web/cybercrime/guidance-notes

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 6 من اتفاقية بودابست - **سوء استخدام الأجهزة**	**قانون أجهزة الحاسوب 1995** **القسم 6** 1. *الشخص الذي يقوم بتكوين برنامج ما بطريقة تمكنه من التسبب في تلف أو خلل بحاسوب أو مواد حاسوب غير محددة، للتسبب بشكل غير قانوني في تلف أو خلل بحاسوب أو مواد حاسوب، سواء كانت محددة أو غير محدد،...* 2. *الشخص الذي ينقل برنامجًا إلى برنامج آخر، أو يتسلل إلى حاسوب آخر، وهو برنامج قادر على التسبب في تلف أو خلل كما هو مذكور في القسم الفرعي (أ)، للتسبب بشكل غير قانوني في حدوث التلف أو الخلل السابق ذكرهما...*	**التحليل القانوني** تجرم المادة 6 إنتاج ونقل برنامج حاسوبي للتسلل أو التسبب في تلف أو خلل. يشمل النقل في القسم 6 (ب) بيع هذه البرامج (على سبيل المثال فيروسات أحصنة طروادة) في القسم 6 (ب) و (ج). قدمت إسرائيل حجزًا بشأن إعادة الحصول لاستخدام واستيراد وحيازة توزيع رموز الوصول وغيرها من البيانات المحوسبة المستخدمة في ارتكاب الجرائم السيبرانية عندما وقعت على اتفاقية بودابست. يجب أن تأخذ أي جريمة بعين الاعتبار تلك الأجهزة التي لها استخدام شرعي وكذلك استخدام جنائي («الاستخدام المزدوج") - التشريع واضح أن أي برنامج يستخدم "للتسبب بشكل غير قانوني في تلف أو خلل بجهاز حاسوب أو مواد حاسوب" بحيث تضم الاستخدام المزدوج بشكل كاف. تم استخدام «التسلل" في القسم 6 (ب) وفي حين أن هذا قد يعني الوصول غير القانوني، يجب توضيح ذلك تنص المادة 2-6 من اتفاقية بودابست على أنه لا توجد حاجة لتفسير هذه المادة على أنها تفرض مسؤولية جنائية عندما تكون الإجراءات قد نُفذت بخلاف الإجراءات المتبعة عند ارتكاب جريمة، مثل عمليات تفتيش الحماية المرخص بها أو الشرطة. وبموجب القانون الإسرائيلي، فإن الشرط اللازم لتكوين جريمة هو أن الإجراء قد تم تنفيذه بطريقة غير قانونية، وبالتالي فمن الواضح أن سلطات الإنفاذ التي تتصرف قانونًا لن يتم تجريمها، وبالتالي لا تتطلب إعفاء **تحليل الفجوة** **التوصيات**: يتعين إدراج تعريف «التسلل" في قانون الحواسيب، بحيث يتضح معناه
المادة 7 من اتفاقية بودابست - **أعمال التزوير المرتبطة بالحاسوب** يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم إدخال بيانات الحاسوب أو تغييرها أو حذفها أو محوها، عند ارتكاب ذلك عن قصد وبدون حق، مما يؤدي إلى بيانات غير موثوقة بهدف أن يتم التعامل معها أو التصرف فيها لأغراض قانونية كما لو كانت أصلية، بصرف النظر عما إذا كانت البيانات قابلة للقراءة ومقروءة مباشرة أم لا. قد يطلب طرف ما وجود نية الاحتيال، أو نية غير شريفة مماثلة، قبل إسناد المسؤولية الجنائية.	**قانون أجهزة الحاسوب 1995** **القسم 3** 1. *يعاقب بالحبس مدة ثلاث سنوات كل شخص يقوم بأحد الأفعال التالية:* a. نقل معلومات كاذبة إلى شخص آخر أو تخزينها في جهاز حاسوب أو تنفيذ إجراء فيما يتعلق بالمعلومات بحيث يؤدي إلى إصدار معلومات خاطئة أو مخرجات خاطئة؛ b. إعداد البرنامج أو نقله إلى شخص آخر أو تخزينه في جهاز حاسوب، بحيث يؤدي إلى إصدار معلومات خاطئة أو مخرجات خاطئة، أو تشغيل جهاز حاسوب أثناء استخدام البرنامج كما هو مذكور. 2. *في هذا القسم، يُقصد بـ"المعلومات الخاطئة" و"المخرجات الخاطئة" - المعلومات أو المخرجات التي يمكن أن تضللها، وفقًا لأهداف استخدامها.*	**التحليل القانوني** تغطي المادة 7 البيانات التي تعادل وثيقة عامة أو خاصة. «المدخلات" غير المصرح بها من البيانات الصحيحة أو غير الصحيحة تؤدي إلى وجود موقف يتوافق مع إعداد وثيقة مزورة. التعديلات اللاحقة (التعديلات والاختلافات والتغييرات الجزئية) والحذف (إزالة البيانات من وسائط البيانات) والمنع (استبقاء وإخفاء البيانات) تتوافق بشكل عام مع تزوير وثيقة أصلية. تحيط الجريمة الواردة في القسم 3 بالتزوير المتعلق بالحاسوب الذي يؤدي إلى «معلومات خاطئة" أو "مخرجات خاطئة". إرسال وثيقة مزورة أو تغيير البيانات (مثل البيانات المستخدمة في التصيد الاحتيالي) سيكون كافيًا لوجود إدانة. تتطلب جريمة التزوير الواردة في المادة 7 من اتفاقية بودابست القصد بحيث يتم اعتبار البيانات غير الموثوقة أصلية. القسم 3 لا يشترط وجود القصد - وأدرج القصد في المادة 7 من اتفاقية بودابست حسب تقدير الأطراف وليس شرطًا محددًا. يمكن استخدام القسم 6، إعادة إنتاج ونقل برنامج حاسوبي للتسلل أو التسبب في تلف أو خلل، لأولئك الذين يكتبون أو يرسلون برنامجًا مزورًا، ولكن يتطلب إثباتًا بحدوث خلل أو تلف

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 8 من اتفاقية بودابست - **أعمال الاحتيال المرتبطة بالحاسوب** يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال الجنائية بموجب قوانينه الداخلية، عند ارتكابها عمدًا ودون حق، بما يسبب فقدان الممتلكات لشخص آخر عن طريق: أي مدخلات أو تغيير أو حذف أو إلغاء لبيانات الحاسوب، وأي تدخل في عمل نظام الحاسوب، بقصد احتيالي أو قصد غير شريف من أجل الحصول، دون حق، على منفعة اقتصادية لنفسه أو لشخص آخر. **القسم 12 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الاحتيال المرتبط بالحاسوب** الشخص الذي يتسبب في فقدان الممتلكات لشخص آخر، عن قصد، ودون عذر أو مبرر قانوني أو بتجاوز عذر أو مبرر قانوني، وذلك عن طريق: • أي إدخال أو تغيير أو حذف أو إلغاء لبيانات الحاسوب؛ • أي تدخل في عمل نظام الحاسوب، بقصد احتيالي أو قصد غير شريف للحصول، دون حق، على منفعة اقتصادية لنفسه أو لشخص آخر، وتكون عقوبة هذه الأعمال الحبس لمدة لا تتجاوز [المدة]، أو غرامة لا تتجاوز [المبلغ]، أو العقوبتين كليهما	**قانون أجهزة الحاسوب 1995** **القسم 3**	**التحليل القانوني** الهدف من المادة 8 من اتفاقية بودابست هو تجريم أي تلاعب لا لزوم له في سياق معالجة البيانات بقصد التأثير على النقل غير المشروع للممتلكات. يجب أن ترتكب الجريمة الواردة في المادة 8 من اتفاقية بودابست «بدون حق"، ويتم الحصول على منفعة اقتصادية نتيجة لذلك. وهذا لمنع تجريم الممارسات التجارية المشتركة المشروعة. على سبيل المثال، الأنشطة المنفذة بموجب عقد ساري بين الأشخاص المتضررين بوجه حق (مثل تعطيل موقع ويب كما هو مخول وفقًا لشروط العقد).[193] يجب أن ترتكب الجريمة الواردة في المادة 8 من اتفاقية بودابست «عمدًا". ويشير عنصر القصد العام إلى التلاعب في الحاسوب أو التداخل الذي يؤدي إلى فقد ممتلكات لشخص آخر. كما تتطلب الجريمة القصد غير الاحتيالي أو قصد غير شريف محدد للحصول على منفعة اقتصادية أو غيرها من المنافع لنفسه أو لشخص آخر. وبالتالي، على سبيل المثال، لا يُقصد بالممارسات التجارية المتعلقة بالمنافسة في السوق والتي قد تسبب ضررًا اقتصاديًا لأحد الأشخاص ويستفيد منه شخصًا آخر، ولكنها لا تُنفَّذ بقصد احتيالي أو قصد غير شريف، أن تُدرج في الجرم المنصوص عليه في هذه المادة. على سبيل المثال، ليس القصد تجريم استخدام برامج جمع المعلومات للمقارنة بين المتاجر على الإنترنت (" الروبوتات")، حتى لو لم يكن مصرحًا به من قِبل موقع تمت زيارته بواسطة "الروبوت".[194] القسم 3 لا يتطلب توافر التشويه الكاذب أو القصد غير الشريف. ويمكن استخدام القسم 6 لأولئك الذين يكتبون أو يرسلون برنامجًا، ولكن يتطلب إثبات حدوث خلل أو تلف **تحليل الفجوة** **التوصيات:** تُدرج جريمة الاحتيال المرتبط بالحاسوب في قانون الحواسيب لسنة 1995 لضمان ارتكاب أي من هذه الجرائم «بدون حق" وعمدًا - باستخدام المادة 8 من اتفاقية بودابست أو القسم 12 من مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية.
المادة 9 من اتفاقية بودابست - **الجرائم ذات الصلة بالمحتوى (مثل المواد الإباحية للأطفال)**	**قانون العقوبات** **القسم 214**	**التحليل القانوني** يتعلق القسم 214 من قانون العقوبات بالمنشورات الفاحشة مصطلح "المواد المخلة بالآداب العامة التي تشمل صورة قاصر" هو المصطلح الإسرائيلي "للمواد الإباحية التي يظهر فيها أطفال". - القسم 214 (ب)
المادة 10 من اتفاقية بودابست - **انتهاك حقوق النشر**	**الاتفاق الخاص بجوانب حقوق الملكية الفكرية المتصلة بالتجارة (TRIPS)**	بصفتها طرفًا في الاتفاق الخاص بجوانب حقوق الملكية الفكرية المتصلة بالتجارة، أكدت إسرائيل على أن المسؤولية الجنائية لديها تتفق مع التزاماتها

193. الفقرة 89، الصفحة 15 من التقرير الإيضاحي في اتفاقية بودابست بشأن الجريمة السيبرانية
194. الفقرة 90، الصفحة 15 من التقرير الإيضاحي في اتفاقية بودابست بشأن الجريمة السيبرانية

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 11 من اتفاقية بودابست **المساعدة والتحريض** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لتجريم الأفعال التالية بموجب قانونه الداخلي، وذلك عندما يتم التحريض على ارتكاب أي من الجرائم المقررة وفقا للمواد من 2 إلى 10 من هذه الاتفاقية أو المساعدة عليها عمدًا، مع نية أن ترتكب هذه الجريمة. 2. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وتدابير أخرى لتجريم محاولة ارتكاب أي من الأفعال الإجرامية المنصوص عليها في المواد من 3 إلى 5 و 7 و 8 و 9.1. أ و ج من هذه الاتفاقية عمدًا.	**قانون العقوبات** **القسم** 25 **القسم** 31 **القسم** 32	**التحليل القانوني** تعتبر مساعدة الآخرين وتحريضهم على ارتكاب جرائم أمرًا ضروريًا لمحاكمة أولئك الذين يكونون قد قدموا المساعدة أو شجعوا على ارتكاب جرائم الإنترنت. يتضمن القسمان 31 و 32 من قانون العقوبات المساعدة على ارتكاب الجرائم أو التحريض عليها. إضافة إلى ذلك، يحدد القسم 25 من قانون العقوبات محاولة ارتكاب جريمة
المادة 12 من اتفاقية بودابست - **مسؤولية الشركات** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وتدابير أخرى لضمان أن الأشخاص الاعتباريين يمكن اعتبارهم مسؤولين عن أي جريمة جنائية منشأة وفقًا لهذه الاتفاقية، إذا ارتكبها أي شخص طبيعي لصالحهم، سواء كان ذلك بصفته الفردية أو باعتباره جزءًا من جهاز الشخص الاعتباري، أو باعتباره شخصًا قياديًا ضمن تنظيم الشخص الاعتباري، بناءً على: • سلطة تمثيل الشخص الاعتباري؛ • سلطة اتخاذ القرارات نيابة عن الشخص الاعتباري؛ • سلطة ممارسة السيطرة داخل الشخص الاعتباري. 2. بالإضافة إلى الحالات المنصوص عليها بالفعل في الفقرة 1 من هذه المادة، يتخذ كل طرف الإجراءات اللازمة لضمان أن يتحمل الشخص الاعتباري المسؤولية عندما يكون عدم الإشراف أو السيطرة من قبل أي شخص طبيعي مشار إليه في الفقرة 1 قد جعل من الممكن ارتكاب جريمة جنائية منصوص عليها بموجب هذه الاتفاقية لصالح ذلك الشخص الاعتباري من قبل شخص طبيعي يعمل تحت سلطته. 3. مع مراعاة المبادئ القانونية للطرف، قد تكون مسؤولية الشخص الاعتباري جنائية أو مدنية أو إدارية. 4. تكون هذه المسؤولية دون المساس بالمسؤولية الجنائية للأشخاص الطبيعيين الذين ارتكبوا الجريمة.	**قانون العقوبات** **القسم** 23	**التحليل القانوني** يشير القسم 23 من قانون العقوبات إلى المسؤولية الجنائية للشركة، وكذلك المسؤولية المدنية المحتملة (الإخلال بالتزام قانوني أو الإهمال).

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
البروتوكول الإضافي لاتفاقية الجريمة السيبرانية، المتعلق بتجريم أعمال العنصرية وكراهية الأجانب المرتكبة من خلال أنظمة الحاسوب **المادة 3 - نشر المواد التي تحض على العنصرية وكراهية الأجانب من خلال أنظمة الحاسوب** يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم السلوك التالي في قوانينه المحلية، عندما يرتكب عمدا وبدون حق: 1. توزيع المواد العنصرية وكراهية الأجانب أو إتاحتها للجمهور من خلال نظام الحاسوب. 2. يجوز لأي طرف أن يحتفظ بالحق في عدم إسناد المسؤولية الجنائية للسلوك على النحو المحدد في يجوز للطرف أن يحتفظ بالحق في عدم إسناد المسؤولية الجنائية بالتصرف على النحو المحدد في الفقرة 1 من هذه المادة، عندما تحض المواد الموزعة، كما هو محدد في الفقرة 1 من المادة 2، وتشجع على التمييز غير المرتبط بالكراهية أو العنف، شريطة أن تتوفر سبل انتصاف فعالة أخرى. 3. بصرف النظر عن الفقرة 2 من هذه المادة، يجوز للطرف أن يحتفظ بالحق في عدم تطبيق الفقرة 1 على حالات التمييز، لأن هذه الفقرة لا يمكن أن تمثل سبل انتصاف فعالة على النحو المشار إليه الفقرة 2، وذلك بسبب مبادئ ثابتة في نظامه القانوني الوطني متعلقة بحرية التعبير.	**لا يوجد معادل**	**التحليل القانوني** لا توجد أي جريمة مماثلة في القانون الإسرائيلي - يُرجى ملاحظة أن إسرائيل لم توقع على البروتوكول الإضافي وليس هناك شرط لتنفيذ هذه المادة **تحليل الفجوة** **التوصيات**: استخدم لغة اتفاقية بودابست في المادة 3 من البروتوكول الإضافي كدليل للتشريعات الوطنية إذا لزم الأمر
بروتوكول إضافي **المادة 4 - التهديد بدافع العنصرية وكراهية الأجانب** يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم السلوك التالي في قوانينه المحلية، عندما يرتكب عمدا وبدون حق: التهديد، من خلال نظام الحاسوب، بارتكاب جريمة جنائية خطيرة على النحو المحدد في قانونها الداخلي، (1) ضد أشخاص لسبب أنهم ينتمون إلى جماعة يميزها عرقها أو لونها أو نسبها أو أصلها القومي أو العرقي أو دينها، إذا تم استخدام أي من هذه العوامل ذريعةً، أو (2) ضد مجموعة من الأشخاص تتميز بأي من هذه الخصائص.	**قانون العقوبات** **القسم** 144 (ب) **القسم** 192	**التحليل القانوني** تُحظر التهديدات بوجه عام بموجب القسم 192 من قانون العقوبات، وهذا يشمل التهديدات بدافع العنصرية وغير العنصرية. ويشكل القسم 144 و (ب) من قانون العقوبات (جريمة الكراهية) ظروفًا مشددة، مما يضاعف العقوبة القصوى المحددة للجريمة لتصل إلى الحبس لمدة ست سنوات.

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
بروتوكول إضافي **المادة 5 - الإهانة بدافع العنصرية وكراهية الأجانب** يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم السلوك التالي في قوانينه المحلية، عندما يرتكب عمداً وبدون حق: 1. إهانة الجمهور، من خلال نظام حاسوبي، (1) الأشخاص لكونهم ينتمون إلى مجموعة يميزها عرقها أو لونها أو نسبها أو أصلها القومي أو العرقي أو دينها، إذا تم استخدام أي من هذه العوامل ذريعةً؛ أو (2) مجموعة من الأشخاص تتميز بأي من هذه الخصائص. 2. يجوز للطرف إما: • أن يشترط أن يكون للجريمة المشار إليها في الفقرة 1 من هذه المادة أثر على أن الشخص أو مجموعة الأشخاص المشار إليهم في الفقرة 1 والذين يتعرضون للكراهية أو الاحتقار أو السخرية؛ أو • أن يحتفظ بالحق في عدم تطبيق الفقرة 1 من هذه المادة بشكل كلي أو جزئي.	**لا يوجد معادل**	**التحليل القانوني** لا توجد أي جريمة في القانون الإسرائيلي - يُرجى ملاحظة أن إسرائيل لم توقع على البروتوكول الإضافي وليس هناك شرط لتنفيذ هذه المادة **تحليل الفجوة** **التوصيات:** استخدم لغة المادة 5 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست، البروتوكول الإضافي باعتبارها دليلًا للتشريعات الوطنية إذا لزم الأمر.
بروتوكول إضافي **المادة 6 - إنكار والتقليل والموافقة وتبرير الإبادة الجماعية أو جرائم ضد الإنسانية** يعتمد كل طرف ما قد يلزم من إجراءات تشريعية لجعل الأفعال التالية يعتبر جرائم جنائية بموجب قوانينها الداخلية، عندما تُرتكب عمداً وبدون حق: 1. توزيع أو توفير عبر نظام الحاسوب بأية طريقة من الطرق للجمهور، مواد تنكر أو تقلل أو تقر أو تقلل بشكل كبير الأفعال التي تشكل إبادة جماعية أو جرائم ضد الإنسانية، على النحو المحدد في القانون الدولي والمعترف بها على هذا النحو في القرارات النهائية والملزمة للمحكمة العسكرية الدولية، المنشأة بموجب اتفاقية لندن المؤرخة في 8 أغسطس 1945، أو أي محكمة دولية أخرى تنشأ بموجب المواثيق الدولية ذات الصلة والتي يعترف هذا الطرف باختصاصها القضائي. يجوز للطرف كذلك	**لا يوجد معادل**	**التحليل القانوني** لا يشتمل القانون الإسرائيلي على حظر إنكار الإبادة الجماعية أو تبريرها (طالما أنه لا يعتبر تحريضًا على العنف) - يُرجى ملاحظة أن إسرائيل لم توقع على البروتوكول الإضافي وليس هناك شرط لتنفيذ هذه المادة **تحليل الفجوة** **التوصيات:** استخدم لغة المادة 6 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست، البروتوكول الإضافي باعتبارها دليلًا للتشريعات الوطنية إذا لزم الأمر.

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
2. أن يشترط أن يكون الإنكار أو التقليل إلى الحد الأدنى المشار إليه في الفقرة 1 من هذه المادة قد ارتكب بهدف التحريض على الكراهية أو التمييز أو العنف ضد أي فرد أو مجموعة من الأفراد على أساس العرق أو اللون أو النسب أو الأصل القومي أو العرقي أو الدين أو إذا استخدمت هذه العوامل ذريعة لذلك، أو أن يحتفظ بالحق في عدم تطبيق الفقرة 1 من هذه المادة بشكل كلي أو جزئي.		
جرائم إضافية للمراجعة		
الجرائم المتعلقة بالهوية **القسم 14 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية** يعاقب الشخص الذي يقوم عن قصد ودون عذر أو مبرر قانوني، أو يتجاوز عذرًا قانونيًا أو مبررًا باستخدام نظام حاسوب في أي مرحلة من مراحل الجريمة بنقل أو تملك أو استخدام وسيلة لتحديد الهوية شخص آخر بنية ارتكاب أي نشاط غير قانوني يشكل جريمة أو المساعدة أو التحريض عليها، عند إدانته بهذه الأعمال بالسجن لمدة لا تتجاوز [المدة] أو بغرامة لا يتجاوز [المبلغ]، أو بالعقوبتين كليهما.	**قانون العقوبات** **القسم** 441 **قانون الحواسيب** **القسم** 3	**التحليل القانوني** تغطي هذه الجريمة مرحلة التحضير لجريمة خيانة الأمانة المتعلقة بالهوية. قد تشكل هذه الأفعال جريمة انتحال شخصية (القسم 441 بموجب قانون العقوبات) ومعلومات خاطئة (القسم 3 بموجب قانون الحواسيب)
الكشف عن تفاصيل التحقيق **القسم 16 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية** موفر خدمة الإنترنت الذي يتلقى أمرًا يتعلق بتحقيق جنائي ينص صراحةً على الحفاظ على السرية أو على التزام شبيه ينص عليه القانون، ثم يقوم عن عمد ودون عذر أو مبرر قانوني أو بتجاوز لعذر قانوني مبرر، بالإفصاح عن: • حقيقة أنه قد تم إصدار أمر؛ أو • أي شيء تم تنفيذه بموجب الأمر؛ أو • أي بيانات تم جمعها أو تسجيلها بموجب الطلب؛ يعتبر جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين كليهما.	**الإجراءات الجنائية (صلاحيات الإنفاذ - بيانات الاتصالات)** 5768 - 2007 **القسمان** 5 **و** 11 (أ) **قانون العقوبات** **القسم** 287	**التحليل القانوني** يعاقب على جريمة اختراق البيانات والكشف عن المعلومات الحساسة التي يمكن أن تؤثر على سير التحقيقات الجنائية. ينص القسم 5 إلى جانب القسم 11 (أ) بموجب الإجراءات الجنائية (صلاحيات الإنفاذ - بيانات الاتصالات)، 5768 - 2007 على المسؤولية الجنائية لمزود خدمة الإنترنت الذي يكتشف أنه قد صدر أمرًا ويتصرف بانتهاك لتعليمات الأمر بموجب قانون بيانات الاتصالات. فيما يتعلق بالأوامر الأخرى، يتضمن القانون الإسرائيلي جريمة انتهاك التعليمات القانونية (القسم 287 بموجب قانون العقوبات).

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
عدم السماح بالمساعدة **القسم 17 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية** 1. أي شخص آخر غير المشتبه فيه فشل عمداً دون عذر أو مبرر قانوني أو بتجاوز عذر أو مبرر قانوني، بمساعدة شخص أو السماح بمساعدته، بناءً على أمر مثلما تحدد المواد 20 إلى 22[195] يرتكب جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة] ، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين كليهما. 2. قد يقرر أي بلد عدم تجريم عدم السماح بالمساعدة شرط أن تتوفر سبل انتصاف فعالة أخرى.	**قانون العقوبات** **تحقير نظام المحكمة**	**التحليل القانوني** تتعلق هذه الجريمة بالأشخاص الذين لديهم معرفة محددة بالأدلة ذات الصلة والذين يرفضون تقديم المساعدة. غالبًا ما يعتمد تطبيق القانون على هؤلاء الأشخاص لتأمين الأدلة في التحقيقات الإلكترونية. هنالك مخالفة مستقلة وهي عدم توفير كلمات مرور أو الوصول إلى الرموز للأجهزة المشفرة أو البيانات (مثل «مفتاح المعلومات المحمية") - ينص القسم 53 من قانون تنظيم سلطات التحقيق في المملكة المتحدة لعام 2000 (RIPA) [196] على وجود جرم جنائي يتحمله الأشخاص الذين لا يمتثلون للمادة 49 من إخطار قانون تنظيم سلطات التحقيق في المملكة المتحدة والقاضية بالكشف عن «المفتاح" يُعد انتهاك التعليمات القانونية بمثابة جريمة بموجب قانون العقوبات الإسرائيلي أو وفقًا لمرسوم ازدراء المحكمة الإسرائيلية. يتضمن ذلك عدم الامتثال لتعليمات توفير كلمة مرور أو رمز سري.
المطاردة السيبرانية **القسم 18 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية** الشخص الذي يقوم، دون عذر أو مبرر قانوني، أو يتجاوز عذرًا قانونيًا أو مبررًا، ببدء أي اتصال إلكتروني، بقصد إكراه شخص ما أو تخويفه أو مضايقته أو التسبب في ضائقة عاطفية كبيرة له، باستخدام نظام حاسوب لدعم السلوك المتكرر والعدائي والعنيف، يرتكب جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين كليهما.	**قانون الاتصالات (بيزك والبث)** **القسم 30**	**التحليل القانوني** إن جريمة مخالفة القسم 30 من قانون الاتصالات تجرم من يضايقون الأشخاص عبر الإنترنت.
رعاية الأطفال على الإنترنت **القانون الجنائي الهولندي 248e** يعاقب الشخص الذي يقترح ترتيب لقاء، بوسائل عمل آلية أو باستخدام خدمة اتصال، مع شخص يعرف، أو ينبغي منطقيًا أن يعرف، أن هذا الشخص لم يصل بعد إلى سن السادسة عشرة، مع نية ارتكاب أفعال غير لائقة مع هذا الشخص أو لعمل صور عن عمل جنسي يشارك فيه هذا الشخص، بالسجن لمدة لا تقل عن سنتين أو بغرامة من الفئة الرابعة، إذا ارتكب أي عمل يقصد به تحقيق اللقاء. **قانون العقوبات الكندي** **القسم 172.1** 1. يرتكب جريمة كل شخص يتواصل عن طريق وسائل الاتصالات مع		**التحليل القانوني** لإثبات الجرم الهولندي، يلزم عقد لقاء لأغراض جنسية مع تقديم أدلة إثبات مأخوذة من تاريخ الدردشة عبر الإنترنت تفصح عن قصد جنسي؛ طلب عقد اللقاء مع الأدلة على أنه تم التخطيط لذلك (أي التاريخ والمكان). الغرض من القانون الكندي هو منع استدراج الكبار المفترسين للأطفال عبر الإنترنت. لا تتطلب هذه الجريمة حدوث جريمة جنسية. وهذا يعني أن المتهم لا يحتاج إلى الذهاب فعلاً لمقابلة الضحية شخصيًا. تكتمل الجريمة قبل اتخاذ أي إجراءات لارتكاب الجريمة الموضوعية. **تحليل الفجوة** **التوصيات:** يُنصح بإدراجها في التشريعات المحلية لتجريم هذا السلوك التحضيري قبل ارتكاب جريمة جنسية

195. أوامر البحث والاستيلاء والمساعدة والإنتاج
196. http://www.legislation.gov.uk/ukpga/2000/23/section/53

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
شخص يكون عمره أقل من 18 عامًا، أو يظن المتهم أن عمره أقل من 18 عامًا، بغرض تسهيل ارتكاب جريمة مرتبطة بهذا الشخص، وذلك بموجب المادة الفرعية 153 (1) ، المادة 155، 163.1 ، 170 أو 171 أو القسم الفرعي 212 (1) أو (2) أو (2.1) أو (4)؛ a. شخص يكون عمره أقل من 16 عامًا، أو يظن المتهم أن عمره أقل من 16 عامًا، بغرض تسهيل ارتكاب جريمة مرتبطة بهذا الشخص، وذلك بموجب المواد 151 أو 152، أو الفقرة الفرعية 160(3) أو 173 (2) أو الأقسام 271 أو 272 أو 273 أو 280؛ أو b. شخص يكون عمره أقل من 14 عامًا، أو يظن المتهم أن عمره أقل من 14 عامًا، بغرض تسهيل ارتكاب جريمة مرتبطة بهذا الشخص بموجب المادة 281. عقاب 2. يعتبر كل شخص يرتكب جريمة بموجب الفقرة الفرعية (1) مذنبًا a. مذنبًا بارتكاب جريمة ويكون عرضة لعقوبة السجن لمدة تتراوح بين 10 سنوات كحد أقصى وسنة واحدة كحد أدنى؛ أو b. مذنبًا بارتكاب جريمة يعاقب عليها في ملخص الإدانة بالسجن لمدة تتراوح بين 18 شهرًا كحد أقصى و 90 يومًا كحد أدنى. افتراض إعادة تقدير العمر 3. الأدلة على أن الشخص المشار إليه في الفقرة (1) (أ) أو (ب) أو (ج) قُدِّم للمتهم وعمره أقل من ثمانية عشر عامًا أو ستة عشر عامًا أو أربعة عشر عامًا، حسب الحالة، في حالة عدم وجود أدلة تثبت عكس ذلك تثبت أن المتهم يعتقد أن الشخص كان أقل من تلك السن. لا دفاع 4. لا يقبل دفاع المتهم أمام التهم الموجهة بموجب الفقرة (1) (أ) أو (ب) أو (ج) بأنه كان يعتقد أن الشخص المشار إليه في تلك الفقرة لا يقل عمره عن ثمانية عشر عامًا أو ستة عشر عامًا أو أربعة عشر عامًا، حسب الحالة، إلا في حالة اتخذ المتهم خطوات معقولة للتأكد من عمر الشخص.		

إجراءات		
أفضل الممارسات الدولية	**التشريع الوطني**	**ملاحظات**
المادة 19 من اتفاقية بودابست - **البحث عن بيانات الحاسوب وضبطها** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لتمكين سلطاته المختصة من التفتيش أو عمليات الوصول الشبيهة: a. نظام الحاسوب أو جزء منه وبيانات الحاسوب المخزنة فيه؛ و b. وسيلة تخزين بيانات الحاسوب، حيث يمكن تخزين بيانات الحاسوب في أراضيها. 2. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وغيرها من الإجراءات لضمان تستطيع سلطاته عند تفتيشها نظام حاسوب معينًا أو جزءًا منه أو الوصول إليه بطريقة مماثلة، وذلك وفقًا للفقرة 1. أ، ويكون لدها أسباب للاعتقاد بأن البيانات المطلوبة مخزنة في نظام حاسوب آخر أو أن جزءًا منها موجود في إقليمها، وهذه البيانات يمكن الوصول إليها قانونيًا من النظام الأولي أو متاحة لها، فإنها قادرة على توسيع نطاق البحث أو الوصول المشابه للنظام الآخر على وجه السرعة. 3. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لتمكين سلطاته المختصة من ضبط أو تأمين بيانات الكمبيوتر التي وصلت إليها وفقا للفقرتين 1 أو 2. تشمل هذه التدابير القدرة على: a. الاستيلاء على نظام حاسوب أو جزء منه أو وسيلة تخزين بيانات الحاسوب، والقيام بما يلزم لتأمينه؛ b. إنشاء نسخة من بيانات الحاسوب هذه والاحتفاظ بها؛ c. الحفاظ على سلامة بيانات الحاسوب المخزنة ذات الصلة؛ d. أن يجعل الوصول غير ممكن إلى البيانات في نظام الحاسوب الذي تم الوصول إليه أو أن يحذفها من نظام الحاسوب الذي تم الوصول إليه. 4. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لتمكين سلطاته المختصة من أن تأمر أي شخص لديه معرفة بعمل نظام الحاسوب أو التدابير المطبقة لحماية البيانات الموجودة فيه بتوفير ما يلزم من المعلومات التي تكفل تنفيذ الإجراءات المشار إليها في الفقرتين 1 و2. 5. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و 15.	**مرسوم الإجراءات الجنائية (الاعتقال والتفتيش) [النسخة الجديدة]، 5729 - 1969 القسم 23 أ** **اختراق مواد الحاسوب** **القسم 32** **صلاحيات مصادرة الأشياء**	**التحليل القانوني** يتيح القسم 23 أ «باختراق مواد الحاسوب - بالمعنى المقصود الوارد في القسم 4 من قانون الحواسيب -5755 1995" يعرّف القسم 1 من قانون الحواسيب «اختراق مواد الحاسوب". ينص القسم 32 على أنه يجوز لرجال الشرطة مصادرة « الشيء" الذي يتضمن "مواد الحاسوب" على الرغم من أن القسم 32 يشير إلى مسؤول مدرب، فإنه لا يشير إلى نسخ محتوى البيانات الأصلي أو الحفاظ عليه أو ضمان سلامة أي دليل تم مصادرته أو جعل البيانات غير قابلة للوصول لمنع المزيد من الجرائم. ومع ذلك، تقوم الشرطة الإسرائيلية بالنسخ والحفظ كمسألة روتينية، ويتم الاحتفاظ بالمعلومات.

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 16 من اتفاقية بودابست **الحفظ المستعجل لبيانات الحاسوب المخزنة والكشف عنها** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وغيرها من الإجراءات لتمكين سلطاته المختصة من طلب الحفظ السريع لبيانات الحاسوب المحددة أو الحصول عليها بشكل مماثل، بما في ذلك بيانات المرور التي تم تخزينها عن طريق نظام حاسوبي، ولا سيما عندما يكون هناك أسباب للاعتقاد بأن بيانات الحاسوب معرضة بشكل خاص للفقد أو التعديل. 2. عندما يقوم أحد الأطراف بتنفيذ الفقرة 1 أعلاه عن طريق أمر شخص بحفظ بيانات الحاسوب المخزنة المحددة وذلك بوضعها في حوزته أو تحت سيطرته، يعتمد هذا الطرف الإجراءات التشريعية وغيرها من الإجراءات التي قد تكون ضرورية لإلزام ذلك الشخص بالحفاظ على سلامة بيانات الحاسوب لفترة زمنية طويلة، حدها الأقصى تسعين يومًا، وذلك لتمكين السلطات المختصة من طلب الكشف عنها. يجوز للطرف أن ينص على تجديد هذا الأمر لاحقًا. 3. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لإلزام الحارس أو أي شخص آخر يحفظ بيانات الحاسوب بالحفاظ على سرية تنفيذ هذه الإجراءات للفترة الزمنية المنصوص عليها في قانونه الداخلي. 4. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و 15.	**قانون أصول المحاكمات الجزائية (بيانات الاتصال) (2007)** **المادتان 3 و 4** **قانون أصول المحاكمات الجزائية (الاعتقال والبحث) (1969)** **المادة 43**	**التحليل القانوني** هذه القوة الإجرائية مهمة لضمان الحفاظ على البيانات المعرضة للحذف أو الفقد **تنص المادتان 3 و4 من قانون الإجراءات الجنائية (بيانات الاتصالات) (2007) على الحفاظ على بيانات الاتصال.** **تنص المادة 43 من قانون الإجراءات الجنائية (الاعتقال والتفتيش) (1969) على الحفاظ على أي بيانات حاسوب أخرى.**
المادة 17 من اتفاقية بودابست **الحفظ المستعجل والكشف الجزئي لبيانات المرور** 1. فيما يتعلق ببيانات المرور التي يتعين الحفاظ عليها بموجب المادة 16، يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى من أجل: • التأكد من أن مثل هذا الحفظ المستعجل لبيانات المرور متاح بغض النظر عما إذا كان هناك واحد أو أكثر من مقدمي الخدمة قد شاركوا في نقل ذلك الاتصال؛ و • ضمان الكشف السريع للسلطة المختصة لدى الدولة الطرف، أو للشخص المعين من قبل تلك السلطة، عن كمية كافية من بيانات المرور لتمكينه من تحديد مقدمي الخدمات والمسار الذي تم من خلاله نقل الاتصال. 2. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و 15.	**قانون الاتصالات** **المادة 13 (ب) (2)** **قانون الإجراءات الجنائية (بيانات الاتصالات)** (2007)	**التحليل القانوني** تعد هذه القوة الإجرائية مهمة بشكل خاص لضمان توفير مقدمي خدمات الإنترنت لعناوين بروتوكول إنترنت يمكنها تحديد موقع مرتكب الجريمة السيبرانية. **تتيح المادة 13 (ب) (2) من قانون الاتصالات (1982)، إلى جانب المبادئ التوجيهية المحددة للشرطة الإسرائيلية، بالإفصاح الجزئي عن بيانات المرور مع الإشراف القضائي عملاً بالمادتين 3 و 4 من قانون الإجراءات الجنائية (بيانات الاتصالات) (2007).**

إجراءات		
أفضل الممارسات الدولية	**التشريع الوطني**	**ملاحظات**
المادة 18 من اتفاقية بودابست **أمر النسخ** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وتدابير أخرى لتمكين سلطاته المختصة من أن تأمر: a. شخصًا موجودًا في إقليمها بتقديم بيانات حاسوب محددة في حيازته أو تحت سيطرته، وتُخَزّن في نظام حاسوب أو بوسيلة تخزين بيانات الحاسوب؛ و b. مقدم خدمة يقدم خدماته في إقليم الدولة الطرف بتقديم معلومات المشترك المرتبطة بهذه الخدمات، والتي تكون في حيازة أو تحت سيطرة مقدم الخدمة. 2. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و 15. 3. تعني «معلومات المشترك» أي معلومات محفوظة بشكل بيانات حاسوب أو أي شكل آخر ويحتفظ بها مزود الخدمة، وترتبط بالمشتركين في خدماته، بخلاف بيانات المرور أو المحتوى، والتي يمكن إنشاؤها من خلال: a. نوع خدمة الاتصال المستخدمة والأحكام الفنية المتعلقة بها وفترة الخدمة؛ b. هوية المشترك أو العنوان البريدي أو الجغرافي، ورقم الهاتف وأرقام الاتصال الأخرى ومعلومات الفوترة والدفع المتاحة بناءً على اتفاقية الخدمة؛ c. أي معلومات أخرى متاحة على موقع تركيب معدات الاتصالات بناءً على اتفاقية الخدمة أو الترتيب.	**الإجراءات الجنائية (إنفاذ القوى - بيانات الاتصالات) 5768 - 2007** **المادتان 3 و 4** **قانون أصول المحاكمات الجزائية (الاعتقال والبحث) (1969)** **المادة 43**	**التحليل القانوني** **تنص المادتان 3 و 4 من الإجراءات الجنائية (صلاحيات الإنفاذ - بيانات الاتصالات) 5768 - 2007 على الحفاظ على بيانات الاتصال.** **تنص المادة 43 من قانون الإجراءات الجنائية (الاعتقال والتفتيش) (1969) على الحفاظ على أي بيانات حاسوب أخرى.**
	قانون التنصت على المكالمات الهاتفية 1979	**التحليل القانوني**[197] يتيح قانون التنصت على المكالمات الهاتفية لسنة 1979 بمراقبة أو تسجيل أو نسخ محادثات الآخرين دون موافقة أي من المشاركين عملاً بحماية الخصوصية. تم تعديل قانون التنصت على المكالمات الهاتفية لعام 1979 في عام 1995 للحفاظ على التوازن بين المصالح والحقوق، مع الحق في الخصوصية من خلال التنصت على المكالمات الهاتفية الذي يأذن به القضاء. يحدد قانون حماية الخصوصية لسنة 1981 القيود القانونية وغير القانونية على الخصوصية. وتشمل: التقييد المعقول للخصوصية من قبل سلطة الأمن أثناء أدائها لمهامها (أي تحقيقات الشرطة). يعطى الحق في الخصوصية الأولوية ولا يتم قبول الأدلة التي تم الحصول عليها بطريقة غير مشروعة إلا في حالات استثنائية للحفاظ على سيادة القانون.[198]

197. بطاقات يوروميد 2014 الصفحات 84-82
198. محكمة العدل العليا 3815/90 غيلات ضد وزير الأمن الداخلي وآخرين؛ 3816 بيفيت وآخرون ضد وزير الأمن الداخلي وآخرين

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 21 من اتفاقية بودابست - **اعتراض بيانات المحتوى** 1. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وغيرها من الإجراءات، فيما يتعلق بمجموعة من الجرائم الخطيرة التي يحددها القانون المحلي، لتمكين سلطاته المختصة من: a. الجمع أو التسجيل من خلال تطبيق الوسائل التقنية على أراضي ذلك الطرف، و إلزام مزود الخدمة، في حدود قدرته التقنية الحالية: i. الجمع أو التسجيل من خلال تطبيق الوسائل التقنية على أراضي ذلك الطرف؛ أو ii. التعاون ومساعدة السلطات المختصة في الجمع أو التسجيل، بيانات المحتوى المرتبطة باتصالات محددة في أراضيها، والمرسلة عن طريق نظام حاسوب وذلك في الوقت الفعلي. 2. في الحالات التي لا يمكن فيها لأي طرف، بسبب المبادئ المستقرة في نظامه القانوني الداخلي، أن يعتمد التدابير المشار إليها في الفقرة 1.أ، يجوز له بدلا من ذلك اعتماد تدابير تشريعية وتدابير أخرى قد تكون ضرورية لضمان جمع أو تسجيل البيانات المرورية المرتبطة باتصالات محددة مرسلة في أراضيه، في الوقت الحقيقي، من خلال تطبيق الوسائل التقنية على ذلك الإقليم. 3. يعتمد كل طرف التدابير التشريعية والتدابير الأخرى التي قد تكون ضرورية لإلزام مقدم الخدمة بالحفاظ على سرية تنفيذ أي سلطة منصوص عليها في هذه المادة وأي معلومات تتعلق بها. 4. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و 15.		تُعرَّف المحادثة في القانون بأنها الكلام، والمحادثة الهاتفية، ومحادثات الهاتف المحمول، وعلى موجات الراديو، وعبر الفاكس والتلكس، والطابعة عن بعد، **والاتصال بين أجهزة الحاسوب.** يجوز استخدام هذا الإجراء عند الضرورة لاكتشاف جريمة مصنفة كجناية أو التحقيق فيها أو منع ارتكابها (جرائم يعاقب عليها بالسجن لمدة لا تقل عن 3 سنوات)، أو لاكتشاف المجرمين الذين ارتكبوا مثل هذه الجرائم أو القبض عليهم، أو لأجل تحقيق هدف مصادرة الممتلكات المرتبطة بهذه الجرائم. يتيح قانون المساعدة القانونية بين الدول لسنة 1998 للدولة مقدمة الطلب بأن تطلب الاعتراض إذا كان ضروريًا ومرتبطًا بمسألة جنائية في الدولة مقدمة الطلب، فيما يتعلق بأحد الأمور التالية: 1. جريمة يعاقب عليها بموجب قوانين الدولة مقدمة الطلب بالحبس لمدة تزيد عن 3 سنوات. 2. جريمة كان من شأنها أن توفر أسسًا للسماح بالتنصت على المكالمات الهاتفية لو ارتكبت في إسرائيل. 3. لأغراض المصادرة رئيس المحكمة الجزئية أو نائبه المفوض هو الجهة المخوّلة بالسماح بالتنصت على المكالمات الهاتفية من خلال مذكرة قضائية. يجب كما ذُكر سابقًا أن يُقدَّم طلب للحصول على أمر قضائي من قبل ضابط شرطة برتبة قائد (Nitzav Mishneh) وما فوق. يجب تقديم الطلب باستخدام نموذج قياسي، ويحدد على سبيل المثال الأساس الوقائي الذي يستند إليه الطلب، وأسباب الطلب، وتفاصيل الإجراء المطلوب. يسمع الطلب من طرف واحد. يمنح الإذن بعد أن تنظر الهيئة المختصة في خطورة انتهاك الخصوصية، ويجوز استخدام هذا الإجراء عند الضرورة لاكتشاف جريمة مصنفة كجناية أو التحقيق فيها أو منع ارتكابها (جرائم يعاقب عليها بالسجن لمدة لا تقل عن 3 سنوات)، أو لاكتشاف المجرمين الذين ارتكبوا مثل هذه الجرائم أو القبض عليهم، أو لأجل تحقيق هدف مصادرة الممتلكات المرتبطة بهذه الجرائم. يجب أن يحدد التصريح هوية الشخص أو هوية الخط أو تركيبه أو مكانه أو نوع المحادثات وأساليب التنصت. يجب أن تكون مدة الترخيص لمدة تصل إلى ثلاثة أشهر ويمكن تمديدها من وقت لآخر. يقوم مفوض الشرطة مرة واحدة في الشهر بتقديم تقرير عن التصاريح الصادرة. يخول مفوض الشرطة بإصدار تصريح عاجل لمدة 48 ساعة عندما لا يكون هناك وقت للحصول على تصريح، ويكون التصريح ضروريًا لمنع جناية واكتشاف مرتكبها. يقوم المفوض بتقديم تقرير إلى النائب العام فور إصدار الإذن ويكون للأخير سلطة سحبه.

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
		بموجب القانون، قد يتم تلقي طلبات المساعدة القانونية في المسائل الجنائية من قبل مديرية المحاكم أو مدير إدارة الشؤون الدولية في مكتب النائب العام أو المفتش العام للشرطة الإسرائيلية أو رئيس شعبة الاستخبارات. من الناحية العملية، تُرسل الطلبات إلى الإدارة القضائية التي ترسلها إلى وحدة المساعدة القانونية التابعة للشرطة الإسرائيلية التي تشرف على تنفيذ الطلبات من السلطات المختصة. وتتشاور وحدة المساعدة القانونية في بعض الحالات مع إدارة الشؤون الدولية بشأن تنفيذ الطلب. في حين يمكن اتخاذ القرارات المتعلقة بتنفيذ الطلبات من قبل وزارة الشؤون الخارجية في مكتب النائب العام ووحدة المساعدة القانونية، فإن وزير العدل فقط هو المخول برفض طلب مقدم. يجب أن يحدد طلب المساعدة القانونية نوع الإجراءات التي تُطلب من أجلها المساعدة، والحقائق التي تشكل أساس الاشتباه في ارتكاب الجريمة وعلاقته بالمساعدة المطلوبة. ويجب النظر في طلبات المساعدة من هذا النوع إلى جملة أمور، من بينها إن كان الطلب متوافقًا مع متطلبات القانون الإسرائيلي وذلك فيما يتعلق بإصدار أمر التنصت على المكالمات الهاتفية، على النحو المنصوص عليه أعلاه تقوم الشرطة بتنفيذ الإجراءات المطلوبة في إطار الطلب.
المادة 20 من اتفاقية بودابست - **جمع بيانات حركة الاتصالات في الوقت الحقيقي** 1. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتمكين سلطاته المختصة من: a. الجمع أو التسجيل من خلال تطبيق الوسائل التقنية على أراضي ذلك الطرف، و b. إلزام مزود الخدمة، في حدود قدرته التقنية الحالية: i. الجمع أو التسجيل من خلال تطبيق الوسائل التقنية على أراضي ذلك الطرف؛ أو ii. التعاون ومساعدة السلطات المختصة في الجمع أو التسجيل، بيانات حركة الاتصالات المرتبطة باتصالات محددة في أراضيها، والمرسلة عن طريق نظام حاسوب، وذلك في الوقت الحقيقي.	**الإجراءات الجنائية (إنفاذ القوى - بيانات الاتصالات) 5768 - 2007** **المادة 3 (ز)** **قانون الاتصالات (1982)** **المادة 13 (ب) (2)**	**التحليل القانوني** **تتيح المادة 3 (ز) من الإجراءات الجنائية (صلاحيات الإنفاذ - بيانات الاتصالات) 5768 - 2007 والمادة 13 (ب) (2) من قانون الاتصالات الإسرائيلي (1982) بجمع بيانات حركة المرور في الوقت الفعلي.**

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
2. في الحالات التي لا يمكن فيها لأي طرف، بسبب المبادئ المستقرة في نظامه القانوني الداخلي، أن يعتمد التدابير المشار إليها في الفقرة 1.أ، يجوز له بدلا من ذلك اعتماد تدابير تشريعية وتدابير أخرى قد تكون ضرورية لضمان جمع أو تسجيل البيانات المرورية المرتبطة باتصالات محددة مرسلة في أراضيه، في الوقت الفعلي، من خلال تطبيق الوسائل التقنية على ذلك الإقليم. 3. يعتمد كل طرف التدابير التشريعية والتدابير الأخرى التي قد تكون ضرورية لإلزام مقدم الخدمة بالحفاظ على سرية تنفيذ أي سلطة منصوص عليها في هذه المادة وأي معلومات تتعلق بها. 4. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و 15.		
واجب الكشف عن مفاتيح التشفير		**التحليل القانوني** مع استخدام الإرهابيين والمجرمين المنظمين بشكل روتيني لتطبيقات الرسائل المشفرة[199] قد يعتبر الكشف عن مفاتيح التشفير قوة ملائمة لإطلاق مفاتيح كلمات المرور لفتح الأجهزة[200] **تحليل الفجوة** **التوصيات:** لا توجد صلاحيات لفك تشفير في إسرائيل - يُوصى بتطبيق هذا الحكم للسماح لوكالات إنفاذ القوانين بإجبار أصحاب الأجهزة على توفير رموز التعريف الشخصي وكلمات المرور لإلغاء قفل الأجهزة
التزامات الاحتفاظ بالبيانات[201]		**التحليل القانوني** تسمح مثل هذه السلطة لوكالات إنفاذ القانون ب 1. تتبع وتحديد مصدر الاتصال 2. تحديد وجهة الاتصال؛ 3. تحديد تاريخ ووقت ومدة الاتصال؛ و 4. تحديد نوع الاتصال لا تتضمن قوانين حماية البيانات والخصوصية الإسرائيلية قيودًا محددة فيما يتعلق بالفترة التي يجب فيها الاحتفاظ بتلك السجلات. ومع ذلك، توجد متطلبات محددة فيما يتعلق بأنواع محددة من البيانات، مثل البيانات الطبية (خاصة في المستشفيات) والبيانات الائتمانية، والتي تقضي بالاحتفاظ بالبيانات ذات الصلة لفترات بحد أدنى محددة. كما أنه كجزء من مسودة المبادئ التوجيهية التي نشرتها سلطة القانون والمعلومات والتكنولوجيا الإسرائيلية (ILITA) فيما يتعلق بأرقام التعريف، فسرت السلطة مصطلح "موافقة" الفرد على أنه يعني موافقة الفرد على الاحتفاظ بالسجلات ما دام الأمر يقتضي ذلك (وليس لفترة أطول من ذلك). ولم يتم فرض أي قيود صريحة على الفترة التي يجوز (أو يجب) للمنظمة الاحتفاظ فيها بالسجلات.

199. Eleanor Saitta. "Can Encryption Save Us?" Nation 300, no. 24 (51 يونيو 5102): 61
18. Academic Search Premier, EBSCOhost (تمت زيارته في 29 فبراير 2016).
200. انظر مثلاً القسم 49 من القانون الإنجليزي (Regulation of Investigatory Powers Act 2000 (UK) - http://www.legislation.gov.uk/ukpga/2000/23/section/49
201. **انظر أعلاه** بشأن التوجيه الصادر عن الاتحاد الأوروبي بشأن الاحتفاظ بالبيانات لسنة 2006 ومخططات الدول الأعضاء بالاتحاد الأوروبي، انظر: http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention

التعاون الدولي		
أفضل الممارسات الدولية	**التشريع الوطني**	**ملاحظات**
المادة 22 من اتفاقية بودابست - **الاختصاص القضائي** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وغيرها من الإجراءات لإقامة ولاية قضائية على أي جرم منصوص عليه في المواد من 2 إلى 11 من هذه الاتفاقية، عندما تُرتكب الجريمة: a. في أراضيها؛ أو على متن سفينة ترفع علم تلك الدولة الطرف؛ أو على متن طائرة مسجلة بموجب قوانين ذلك الطرف؛ أو من قِبَل أحد رعاياها، إذا كانت الجريمة معاقبًا عليها بموجب القانون الجنائي حيث ارتكبت، أو إذا ارتكبت الجريمة خارج الولاية الإقليمية لأي دولة. 2. يجوز لكل طرف أن يحتفظ بالحق في عدم تطبيق أو تطبيق قواعد الاختصاص المنصوص عليها في الفقرات من 1 إلى 1 د من هذه المادة أو أي جزء منها فقط في حالات أو شروط محددة. 3. يعتمد كل طرف ما قد يلزم من إجراءات لإقامة ولاية قضائية على الجرائم المشار إليها في الفقرة 1 من المادة 24 من هذه الاتفاقية، في الحالات التي يكون فيها الجاني المفترض موجودا في إقليمه ولا يسلمه إلى بلد آخر بعد طلب التسليم على أساس جنسيته فقط. 4. لا تستبعد هذه الاتفاقية أي ولاية قضائية جنائية يمارسها أي طرف وفقًا لقانونه الداخلي. 5. عندما يطالب أكثر من طرف بالولاية القضائية على جريمة مفترضة تم النص عليها في هذه الاتفاقية، يتشاور الطرفان المعنيان، عند الضرورة من أجل تحديد الولاية القضائية الأنسب.	**قانون العقوبات لسنة 1977** **المادة 7 (أ)(1)** **المادة 7 (ج)** **المادة 15 (أ)**	**التحليل القانوني** يؤكد التشريع الوطني على تعريف الاختصاص القضائي باستخدام صياغة المادة 22 من اتفاقية بودابست (رهنًا بتحفظ إسرائيل على الفقرة 1.د.) إذا كان هناك تعارض بين السلطات القضائية، فيجب أن تؤخذ في الاعتبار المبادئ التوجيهية المتعلقة بتحديد الولاية القضائية المناسبة لمحاكمة جريمة ما - انظر المبادئ التوجيهية يوروجست لتقرير الولاية القضائية التي في الجرائم التي تجب ملاحقتها (المراجعة 2016)[202]
المادة 35 من اتفاقية بودابست **شبكة تعمل على مدار اليوم والساعة** 1. يعين كل طرف جهة اتصال متاحة على مدار الساعة لضمان تقديم مساعدة فورية لغرض سير التحقيقات أو الإجراءات بخصوص الجرائم الجنائية المتعلقة بأنظمة الحاسوب والبيانات، أو لجمع الأدلة في شكل إلكتروني لجريمة جنائية. يجب أن تشمل هذه المساعدة تيسير التدابير التالية، أو تنفيذها مباشرة إذا سمح القانون الداخلي بذلك:	**في المكان**	**التحليل القانوني** تُعد هذه آلية أساسية للقدرة الدولية الفعالة في مجال التحقيق في الجرائم السيبرانية وهي مطلب إلزامي للتصديق على اتفاقية بودابست يعمل المركز الوطني السيبراني في لاهف 433 وفقًا لما تقتضيه اتفاقية بودابست كجزء من شبكة على مدار الساعة

202. http://www.eurojust.europa.eu/Practitioners/operational/Documents/Operational-Guidelines-for-Deciding.pdf

التعاون الدولي		
أفضل الممارسات الدولية	**التشريع الوطني**	**ملاحظات**
• تقديم المشورة الفنية؛ الحفاظ على البيانات وفقا للمادتين 29 و 30؛ جمع الأدلة وتوفير المعلومات القانونية وتحديد مكان المشتبه به. 2. • يجب أن تتوفر لجهة الاتصال الخاصة بأحد الأطراف القدرة على إجراء الاتصالات مع • نقطة اتصال الطرف الآخر على وجه السرعة. • إذا كانت نقطة الاتصال التي حددها أحد الأطراف ليست جزءًا من سلطة ذلك الطرف أو • السلطات المسؤولة عن المساعدة المتبادلة أو تسليم المجرمين الدوليين، يجب أن تضمن نقطة الاتصال قدرتها على التنسيق مع هذه السلطة أو السلطات على وجه السرعة. 3. يجب على كل طرف التأكد من توفر الأفراد المدربين والمجهزين من أجل تسهيل تشغيل الشبكة.		
المادة 25 من اتفاقية بودابست - المبادئ العامة المتعلقة بالمساعدة المتبادلة 1. يقدم الطرفان المساعدة المتبادلة إلى أقصى حد ممكن لغرض إجراء التحقيقات أو الإجراءات المتعلقة بالجرائم الجنائية المتعلقة بأنظمة الحاسوب والبيانات، أو لجمع الأدلة المتعلقة بالجرائم الجنائية في شكل إلكتروني. 2. يعتمد كل طرف أيضًا الإجراءات التشريعية وغيرها من الإجراءات التي قد تكون ضرورية لتنفيذ الالتزامات المنصوص عليها في المواد من 27 إلى 35. 3. يجوز لكل طرف في الظروف العاجلة تقديم طلبات للمساعدة المتبادلة أو الاتصالات المتعلقة بها عن طريق وسائل الاتصال العاجلة، بما في ذلك الفاكس أو البريد الإلكتروني، إلى الحد الذي توفر فيه هذه الوسائل مستويات مناسبة من الأمن والمصادقة (بما في ذلك استخدام التشفير، عند الضرورة)، مع تأكيد رسمي لاحق، حيثما يطلب ذلك الطرف متلقي الطلب. يجب على الطرف متلقي الطلب قبول الطلب والرد عليه بأي وسيلة اتصال سريعة.	**قانون المساعدة القانونية الدولية، 5758-1998** **الأقسام 2-11** **القسم 5 (أ) (4)** **القسم 8 (ب)**	**التحليل القانوني** تضمن المادة 25 من اتفاقية بودابست إمكانية استخدامها كأداة لتسهيل المساعدة القانونية المتبادلة لإسرائيل. ينص القسم 8 (ب) من قانون المساعدة القانونية الدولية 5758-1998 على عدم تنفيذ طلب أي دولة أجنبية الحصول على مساعدة قانونية إلا إذا كان الفعل مسموحًا به بموجب القانون الإسرائيلي. **وفقًا للقسم 5 (أ) (4) من قانون المساعدة القانونية الدولية 5758-1998، يجوز لوزير العدل الإسرائيلي رفض طلب المساعدة القانونية المتبادلة إذا كان الطلب يستند إلى جريمة مالية. ومع ذلك، فإن الجرائم الواردة في الأقسام من 2 إلى 11 من الاتفاقية مستثناة من مصطلح "جريمة مالية"، كما هي محددة في القسم 1 من قانون المساعدة القانونية الدولية 5758-1998** ينبغي النظر في السماح للسلطات المختصة بإعطاء الإذن لهيئات إنفاذ القانون المحلي بإجراء تحقيق في الدولة التي تأكد فيها الوصول إلى الجهاز. يعد الوصول إلى المعلومات هو المعيار الأساسي لبدء التحقيق في الحالات التي يتعذر فيها معرفة مكان تخزين البيانات (أي في التخزين السحابي). يمكن أن يشمل ذلك "اعترافًا متبادلًا" بأوامر المحكمة الصادرة تجاه مقدمي خدمات الاتصالات في دولة معينة، والتي يمكن تقديمها إلى فروع مقدمي خدمة العملاء الموجودين في دول أخرى، اعتمادًا على مكان تخزين البيانات.

التعاون الدولي		
أفضل الممارسات الدولية	**التشريع الوطني**	**ملاحظات**
4. باستثناء ما هو منصوص عليه على وجه التحديد في المواد الواردة في هذا الفصل، تخضع المساعدة المتبادلة للشروط المنصوص عليها في قانون الطرف متلقي الطلب أو معاهدات المساعدة المتبادلة المطبقة، بما في ذلك الأسباب التي تُجيز للطرف متلقي الطلب أن يرفض التعاون. لا يجوز للطرف متلقي أن يبني حقه في رفض المساعدة المتبادلة المتعلقة بالجرائم المشار إليها في المواد من 2 إلى 11، فقط على أساس أن الطلب يتعلق بجريمة يعتبرها جريمة مالية. 5. عندما تسمح أحكام هذا الفصل للطرف متلقي الطلب بتقييد المساعدة المتبادلة بشرط ازدواجية التجريم، يعتبر هذا الشرط مستوفًيا، بصرف النظر عما إذا كانت قوانينه تضع الجريمة في نفس الفئة الجرمية، أو إذا أعطيت الجريمة نفس التسمية عند الطرف الطالب، وذلك إن كان السلوك الكامن وراء الجريمة التي طلبت المساعدة من أجلها جريمة جنائية بموجب قوانينه.		
المادة 26 من اتفاقية بودابست - **المعلومات التلقائية** 1. يجوز للطرف، في حدود قانونه الداخلي ودون طلب مسبق، أن يحيل إلى الطرف الآخر المعلومات التي تم الحصول عليها في إطار تحقيقاته، عندما يرى أن الكشف عن هذه المعلومات قد يساعد الطرف المتلقي في بدء أو التحقيقات أو الإجراءات المتعلقة بالجرائم الجنائية المنصوص عليها في هذه الاتفاقية، أو قد تؤدي إلى طلب تعاون من جانب هذا الطرف بموجب هذا الفصل. 2. قبل تقديم هذه المعلومات، يجوز للطرف المقدم أن يطلب الحفاظ على سريتها أو استخدامها فقط وفقًا للشروط. إذا لم يستطع الطرف المتلقي الامتثال لهذا الطلب، فيجب عليه إخطار الطرف المقدم الذي يحدد بعد ذلك ما إذا كان ينبغي تقديم المعلومات. إذا قبل الطرف المتلقي المعلومات	**لا يوجد معادل**	**التحليل القانوني** يُعد هذا إجراءً هامًا لتمكين الدولة من الاحتفاظ بمعلومات من شأنها مساعدة دولة أخرى في منع الجريمة السيبرانية أو التحقيق فيها. يمكن لإسرائيل مشاركة هذه المعلومات إذا كان ذلك مناسبًا.

التعاون الدولي		
أفضل الممارسات الدولية	**التشريع الوطني**	**ملاحظات**
المادة 32 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست يجوز للطرف، دون إذن من طرف آخر: الوصول إلى بيانات الحاسوب المخزنة (مفتوحة المصدر) المتاحة للجمهور، بغض النظر عن مكان وجود البيانات جغرافيا؛ أو الوصول إلى بيانات الحاسوب المخزنة الموجودة لدى طرف آخر أو استلامها، من خلال نظام حاسوب في إقليمها، إذا حصل الطرف على موافقة مشروعة وطوعية من الشخص الذي لديه السلطة القانونية للكشف عن البيانات للطرف من خلال نظام الحاسوب هذا.	**لا يوجد معادل**	**التحليل القانوني** تمكن هذه السلطة الإجرائية الدولة من تأمين المحتوى المخزن في دولة أخرى في ظروف محدودة. المادة 32 ب. إن اتفاقية بودابست استثناء من مبدأ الإقليمية وتسمح بوصول منفرد عبر الحدود دون الحاجة إلى مساعدة قانونية متبادلة عندما تكون هناك موافقة أو تكون المعلومات متاحة للجمهور. أمثلة على استخدام هذه السلطة الإجرائية بموجب المادة 32 من اتفاقية بودابست تتضمن: قد يتم تخزين البريد الإلكتروني لشخص ما في بلد آخر بواسطة مزود خدمة، أو قد يقوم شخص ما بتخزين البيانات عن قصد في بلد آخر. يجوز لهؤلاء الأشخاص استرداد البيانات بشرط أن يكون لديهم السلطة القانونية التي تخولهم ذلك، ويجوز لهم الكشف طوعًا عن البيانات لموظفي إنفاذ القانون أو السماح لهؤلاء المسؤولين بالوصول إلى البيانات[203] يمكن اعتقال إرهابي مشتبه به بشكل قانوني عندما يكون بريده الإلكتروني، الذي قد يحوي دليلًا على ارتكاب جريمة، مفتوحًا على الجهاز اللوحي أو الهاتف الذكي أو أي جهاز آخر. إذا وافق المشتبه طوعًا على أن تصل الشرطة إلى الحساب وكانت الشرطة واثقة من أن بيانات صندوق البريد موجودة في ولاية أخرى، يجوز للشرطة الوصول إلى البيانات بموجب المادة 32. ب. إذا كانت المعلومات مفتوحة المصدر (مثل فيسبوك)، فلا يوجد أي حظر يتعلق بالجمع - يكون أي شخص مصرح له بالوصول إلى تلك الصفحات، بما في ذلك ضابط الشرطة. كما تطلب الشرطة الإسرائيلية بشكل روتيني الموافقة على تأمين بيانات الحاسوب المخزنة في ولاية قضائية أخرى.

203. الفقرة 294، الصفحة 53 من التقرير التفسيري في اتفاقية بودابست

الأردن

صدق الأردن على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات وأصدر مؤخرًا قانون الجرائم الإلكترونية رقم 27 لسنة 2015.

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 2 من اتفاقية بودابست **الوصول غير القانوني** يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لتجريم الوصول إلى النظام الكلي أو أي جزء من نظام الحاسوب، إذا ارتكب عمدًا، دون أي حق. قد يشترط طرف ما ارتكاب الجريمة عن طريق انتهاك إجراءات أمنية بقصد الحصول على بيانات الحاسوب أو نية أخرى غير نزيهة، أو فيما يتعلق بنظام حاسوب متصل بنظام حاسوب آخر.	**قانون الجرائم الإلكترونية رقم 27 لعام 2015** **المادة 3** كل من دخل قصدًا إلى الشبكة المعلوماتية بأي وسيلة دون تصريح أو بما يخالف أو يجاوز التصريح. **المادة 12 (أ)** كل من دخل قصدًا دون تصريح أو بما يخالف أو يجاوز التصريح إلى الإنترنت أو نظام معلومات بأي وسيلة كانت بهدف الاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني	**التحليل القانوني** يُشار إلى الوصول غير القانوني إلى «الشبكة المعلوماتية" والتي تم تعريفها في المادة 2 بأنها "ارتباط بين أكثر من نظام معلومات لإتاحة البيانات والمعلومات والوصول إليها. » يتم تعريف «نظام المعلومات" في المادة 2 بأنه "مجموعة البرامج والأدوات المعدة لإنشاء البيانات أو المعلومات إلكترونيًا، أو إرسالها أو تسلمها أو معالجتها أو تخزينها أو إدارتها أو عرضها بالوسائل الإلكترونية." تعتبر الجريمة الواردة في المادة 12 (أ) نموذجًا مشددًا للوصول غير القانوني إلى أجهزة الحاسوب المتعلقة بالبنية التحتية الحيوية. **تحليل الفجوة** **التوصيات:** ترجمة التشريع غير واضحة - لكن يبدو أن تعريف الشبكة المعلوماتية مماثل لتعريف نظام الحاسوب[204] في اتفاقية بودابست لأنه ينطوي على معالجة البيانات. وإذا كان الأمر كذلك، فإن هذه المادة تتفق مع المعايير الدولية.
المادة 3 من اتفاقية بودابست **اعتراض غير قانوني**	**قانون الجرائم الإلكترونية رقم 27 لعام 2015** **المادة 5** كل من قام قصدًا بالتقاط أو باعتراض أو بالتنصت أو أعاق ما هو مرسل عن طريق الشبكة المعلوماتية أو أي نظام معلومات	**التحليل القانوني** يُعتبر تجريم هذا الفعل ضروريًا لمقاضاة عمليات نقل بيانات الحاسوب من وإلى وداخل نظام الحاسوب الذي قد يتم اعتراضه بشكل غير قانوني للحصول على معلومات (مثل wikileaks أو PanamaPapers). تتفق الجريمة بصيغتها الحالية مع أفضل الممارسات الدولية
المادة 4 من اتفاقية بودابست **التشويش على البيانات** يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لكي تجرم قوانينها الوطنية محو بيانات الحاسوب أو إتلافها أو تغييرها أو حذفها دون حق، وذلك عند ارتكابها عمدًا. 2 يجوز لأي طرف أن يحتفظ بالحق في المطالبة بأن يؤدي السلوك الموصوف في الفقرة 1 إلى ضرر جسيم.	**قانون الجرائم الإلكترونية رقم 27 لعام 2015** **المادة 3 (ب) و (ج)** (ب) إذا كان الدخول المنصوص عليه في الفقرة (أ) من هذه المادة لإلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو توقيف أو تعطيل عمل الشبكة المعلوماتية	**التحليل القانوني** تشير المادة 3 (ب) إلى الجريمة الواردة في المادة 3 (أ) والدخول إلى الشبكة المعلوماتية دون تصريح بقصد التدخل في البيانات. لا تشير المادة 3 (ج) المتعلقة بالموقع الإلكتروني إلى تداخل البيانات «دون تصريح" تشير اتفاقية بودابست إلى «بدون حق" في المادة 4 على أساس أن الوصول غير مصرح به. أكد التقرير التفسيري لاتفاقية بودابست اشتقاق عبارة "بدون حق" مثل "التصرف

204. انظر المادة 1.أ. من اتفاقية بودابست: «يعني نظام الحاسوب أي جهاز أو مجموعة من الأجهزة المترابطة أو ذات الصلة، أو واحدًا أو أكثر من هذه الأجهزة يقوم بمعالجة البيانات تلقائيًا أو تسجيلها وفقا لأحد البرامج" **أو** القسم 3 (5) من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية: «جهاز أو مجموعة من الأجهزة المترابطة أو ذات الصلة، بما في ذلك الإنترنت، يقوم واحد منها أو أكثر بمعالجة تلقائية للبيانات أو بأداء أي وظيفة أخرى وفقًا لأحد البرامج".

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
	(ج) كل من دخل قصدًا إلى موقع إلكتروني لتغييره أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفته أو انتحال شخصية مالكه **المادة 12 (ج)** إذا كان الدخول المشار إليه في الفقرة (أ) من هذه المادة بهدف إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو تعديلها أو تغييرها أو نقلها أو نسخها أو إفشائها	الذي تم دون سلطة (سواء كانت تشريعية أو تنفيذية أو إدارية أو قضائية أو تعاقدية أو توافقية) أو تصرفًا لا يشمله، بأي حال، الدفوع القانونية أو الأعذار أو المبررات أو المبادئ ذات الصلة بموجب القانون المحلي."[205] لا يتضمن التشريع الوطني إلغاء بيانات الحاسوب التي تعد عنصرًا من عناصر التصيد الاحتيالي التي تستخدم غالبًا لتأمين الوصول غير القانوني عن طريق تثبيت برنامج Keylogger للحصول على معلومات حساسة.[206] تتعلق المادة 12 (ج) بجريمة مشددة لتداخل البيانات التي تؤثر على البنية التحتية الحيوية (تشير الفقرة 12 (أ) إلى عبارة دون تصريح). **تحليل الفجوة** **التوصيات:** يجب أن يضيف التشريع الوطني فعل «الإلغاء" يجب إدراج عبارة «بدون تصريح» في المادة 3 (ج) بما يتوافق مع المادة 3 (ب). وفي الوقت الحاضر، تمت صياغة القانون باعتباره مسؤولية صارمة تجاه الجريمة، لذلك يمكن إدانة أي متهم بأي تعديل للموقع الإلكتروني. وستكون الشرطة القضائية محمية بموجب المادة 13 (ب) - ولكن لن يتم حماية الآخرين الذين قد يساعدون في التحقيقات أو الذين يغيرون البيانات بشكل قانوني في المواقع الإلكترونية.
المادة 5 من اتفاقية بودابست **التشويش على النظام**	**قانون الجرائم الإلكترونية رقم 27 لعام 2015** **المادة 4** من يدخل أو يستخدم عن قصد البرامج عبر الإنترنت أو عن طريق استخدام نظام معلومات لإلغاء البيانات أو المعلومات أو حذفها أو الإضافة إليها أو إتلافها أو كشفها أو محوها أو كتمها أو تعديلها أو تبديلها أو نقلها أو نسخها أو اعتراضها أو يمكّن الآخرين من الاطلاع عليها من أجل تعطيل عمل نظام المعلومات أو التدخل فيه أو إغلاقه أو منعه من العمل، أو يصل إلى موقع ويب أو يغيره أو يلغيه أو يدمره أو يعدل محتوياته أو ينتحل شخصية المالك دون إذن أو في تجاوز للسلطة الممنوحة له	**التحليل القانوني** تنص المادة 4 على جريمة تداخل النظام. وفي حين أن تداخل البيانات والوصول غير القانوني يمثلان جريمة مشددة بسبب التأثير على البنية التحتية الحيوية، لا يوجد ما يعادل تداخل النظام. **تحليل الفجوة** **التوصيات:** يجب مراعاة جريمة أخرى تتمثل في منع ومكافحة الهجمات ضد البنية التحتية الحيوية التي تعيق عمل نظام الحاسوب - على سبيل المثال، قد يؤدي إعاقة النظام الذي يخزن سجلات البورصة إلى جعلها غير دقيقة.[207] يُشار إلى «المواقع الإلكترونية" أو "نظام المعلومات"، مع مراعاة الإشارة إلى "أنظمة الحاسوب" أو "شبكات الحاسوب" و"البيانات" - وهذا سيكون متوافقًا مع اتفاقية بودابست والاتفاقية العربية لمكافحة جرائم تقنية المعلومات. يجب أن يتضمن التشريع الوطني إشارات إلى «أنظمة الحاسوب" و"شبكات الحاسوب" و "البيانات"

205. الفقرة 38، الصفحة 8 من التقرير التوضيحي لاتفاقية الجريمة الإلكترونية - رقم 185 https://rm.coe.int/16800cce5b
206. http://www.coe.int/en/web/cybercrime/guidance-notes
207. http://www.coe.int/en/web/cybercrime/guidance-notes

الجرائم		
أفضل الممارسات الدولية	**التشريع الوطني**	**ملاحظات**
المادة 6 من اتفاقية بودابست **سوء استخدام الأجهزة** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لتجريم الأفعال الإجرامية بموجب قوانينه الداخلية، عندما تُرتكب عمدًا ودون حق: a. إنتاج أو بيع أو الشراء بغرض الاستخدام أو الاستيراد أو التوزيع أو توفير ما يلي بأية طريقة: i. أي جهاز، بما في ذلك برنامج الحاسوب، تم تصميمه أو تكييفه بشكل أساسي بغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من 2 إلى 5؛ ii. كلمة مرور الحاسوب أو رمز الوصول أو البيانات المماثلة التي يمكن من خلالها الوصول إلى نظام الحاسوب كله أو جزء منه، بقصد استخدامه لغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من 2 إلى 5؛ و iii. حيازة عنصر مشار إليه في الفقرتين أ.1 أو 2 أعلاه، بقصد استخدامه لغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من 2 إلى 5. يجوز لأي طرف أن يشترط بموجب القانون امتلاك عدد من هذه العناصر قبل إسناد المسؤولية الجنائية. 2. لا يجوز تفسير هذه المادة على أنها تفرض مسؤولية جنائية عندما لا يكون الغرض من الإنتاج أو البيع أو الشراء بغرض الاستخدام أو الاستيراد أو التوزيع أو التوفير أو حيازة المشار إليه في الفقرة 1 من هذه المادة ارتكاب جريمة منصوص عليها وفقًا للشروط المواد من 2 إلى 5 من هذه الاتفاقية، مثل الاختبارات المسموح بها أو حماية نظام الحاسوب. 3. يجوز لكل طرف أن يحتفظ بالحق في عدم تطبيق الفقرة 1 من هذه المادة، شريطة أن لا يتعلق التحفظ ببيع أو توزيع أو توفير المواد المشار إليها في الفقرة 1 أ من هذه المادة بطريقة أخرى	**لا يوجد معادل**	**التحليل القانوني** ستمكّن تجريم هذه الأفعال من ملاحقة إنتاج وبيع والشراء من أجل الاستخدام واستيراد وتوزيع رموز الوصول والبيانات المحوسبة الأخرى المستخدمة في ارتكاب جرائم الإنترنت. هذه هي العناصر الموجودة في كثير من الأحيان في ملاحقة البرمجيات الخبيثة. يجب أن تأخذ أي جريمة في الاعتبار تلك الأجهزة التي لها استخدام شرعي وكذلك للاستخدام الجنائي («الاستخدام المزدوج") – ينبغي أن يشمل ذلك اللغة المستخدمة في اتفاقية بودابست "المكيف بشكل أساسي" **تحليل الفجوة** **التوصيات:** يجب أن يتضمن التشريع الوطني الجريمة باستخدام الصياغة ذات الصلة من اتفاقية بودابست أو الاتفاقية العربية لمكافحة جرائم تقنية المعلومات أو مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية لضمان تكيف أي وصول دون تصريح وأي أجهزة «أساسًا" لارتكاب الجريمة يرجى ملاحظة أن مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية توفر خيار إدراج الأجهزة في جدول إذا كان ذلك مناسبًا - قد يكون هذا تقييدًا ويتطلب تحديثًا يتوافق مع التقدم التكنولوجي. يجب أن يوفر القانون الوطني عذرًا معقولاً حتى تتمكن وكالات إنفاذ القوانين من استخدام الأجهزة لتقنيات التحقيق الخاصة - الصياغة في المادة 6.2. ويمكن استخدام اتفاقية بودابست أو القسم 10 (2) من مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية باعتبارهما دليلاً.

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
القسم 10 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الأجهزة غير القانونية 1. يرتكب الشخص جريمة إذا: a. أنتج أو باع أو اشترى بغرض الاستخدام أو استورد أو صدّر أو وزع أو وفّر بأي طريقة، عن قصد ودون عذر أو مبرر قانوني أو بتجاوز عذر أو مبرر قانوني: i. جهاز بما في ذلك برنامج حاسوب، تم تصميمه أو تكييفه بغرض ارتكاب جريمة محددة بموجب أحكام أخرى من الجزء الثاني من هذا القانون؛ أو ii. كلمة مرور الحاسوب أو رمز الوصول أو البيانات المماثلة التي يمكن من خلالها الوصول إلى نظام الحاسوب كله أو جزء منه؛ بقصد استخدامه من قبل أي شخص لغرض ارتكاب جريمة محددة بموجب أحكام أخرى من الجزء الثاني من هذا القانون؛ أو كان في حوزته غرض مشار إليه في الفقرة الفرعية «1» أو «2»، وكان القصد هو استخدامه من قبل أي شخص لارتكاب جريمة محددة بموجب أحكام أخرى من الجزء الثاني من هذا القانون، فإنه يعاقب عند إدانته بارتكاب هذه الجريمة بالسجن لمدة لا تزيد عن [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين كليهما. 2. لا يجوز تفسير هذا الحكم على أنه يفرض مسؤولية جنائية عندما لا يكون الغرض من الإنتاج أو البيع أو الشراء للاستخدام أو الاستيراد أو التوزيع أو التوفير أو الحيازة المشار إليها في الفقرة 1 هو ارتكاب جريمة منصوص عليها وفقًا لأحكام أخرى من الجزء الثاني من هذا القانون، كأن تكون الأغراض مثل الاختبار أو الحماية المعتمدين لنظام الحاسوب. 3. قد يقرر بلد ما عدم تجريم الأجهزة غير القانونية أو قصر التجريم على الأجهزة المدرجة في الجدول.		

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 7 من اتفاقية بودابست **أعمال التزوير المرتبطة بالحاسوب** يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم إدخال بيانات الحاسوب أو تغييرها أو حذفها أو محوها، عند ارتكاب ذلك عن قصد وبدون حق، مما يؤدي إلى بيانات غير موثوقة بهدف أن يتم التعامل معها أو التصرف فيها لأغراض قانونية كما لو كانت أصلية، بصرف النظر عما إذا كانت البيانات قابلة للقراءة ومقروءة مباشرة أم لا. قد يطلب طرف ما وجود نية الاحتيال، أو نية غير شريفة مماثلة، قبل إسناد المسؤولية الجنائية. **المادة 10 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست** **جريمة التزوير** يعني استخدام تقنية المعلومات تغيير حقيقة البيانات بطريقة تسبب الضرر بغرض استخدامها كبيانات حقيقية. **القسم 11 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - أعمال التزوير المتعلقة بالحاسوب** 1. كل شخص يقوم عن قصد ودون عذر أو مبرر قانوني أو بتجاوز عذر قانوني أو مبرر، بإدخال أو تبديل أو حذف أو منع بيانات الحاسوب، مما ينتج عنه بيانات غير موثوقة بقصد التعامل معها أو التصرف فيها لأغراض قانونية كما لو كانت صحيحة، بصرف النظر عما إذا كانت البيانات قابلة للقراءة مباشرة أم لا، يعاقب عند الإدانة بهذه الأعمال بالسجن لمدة لا تزيد عن [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً. 2. تكون العقوبة إذا ارتكبت الجريمة المذكورة أعلاه عن طريق إرسال رسائل بريد إلكتروني متعددة من أنظمة الحاسوب أو من خلالها هي السجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً.	**قانون الجرائم الإلكترونية رقم 27 لعام 2015** **المادة 4** من يدخل أو يستخدم عن قصد البرامج عبر الإنترنت أو عن طريق استخدام نظام معلومات لإلغاء البيانات أو المعلومات أو حذفها أو الإضافة إليها أو إتلافها أو كشفها أو محوها أو كتمها أو تعديلها أو تبديلها أو نقلها أو نسخها أو اعتراضها أو يمكّن الآخرين من الاطلاع عليها من أجل تعطيل عمل نظام المعلومات أو التدخل فيه أو إغلاقه أو منعه من العمل، أو يصل إلى موقع ويب أو يغيره أو يلغيه أو يدمره أو يعدل محتوياته أو ينتحل شخصية المالك دون إذن أو في تجاوز للسلطة الممنوحة له	**التحليل القانوني** تشير هذه الجريمة فقط إلى انتحال شخصية المالك ولا تتضمن أي إشارة إلى القصد غير الشريف وهي أكثر صلة بجريمة تداخل النظام. يُنصح بتضمين المادة 7 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست أو القسم 11 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية من أجل الحماية من المخالفات التي قد تشمل التصيد الاحتيالي والتصيد الاحتيالي بالرمح على سبيل المثال، قد يتم إدخال بيانات الحاسوب (مثل البيانات المستخدمة في جوازات السفر الإلكترونية) أو تغييرها أو حذفها أو إلغاؤها، مما يؤدي إلى تصديق البيانات غير الموثوقة أو التعامل معها لأغراض قانونية كما لو كانت صحيحة.[208] ينص القسم 11 (2) من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية أيضًا على إرسال رسائل بريد إلكتروني متعددة باعتبارها جريمة مشددة. لا تشير اللغة في المادة 10 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات إلى أي نية غير شريفة وتشترط التسبب في ضرر - اللغة المستخدمة في اتفاقية بودابست ومواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية هي الأفضل لأنها لا تشترط حدوث ضرر. تشترط اتفاقية ومواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية فقط أن "البيانات الزائفة" "تعتبر" حقيقية **تحليل الفجوة** **التوصيات:** استخدام صياغة اتفاقية بودابست في المادة 7 أو القسم 11 من مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية باعتبارهما دليلاً للتشريعات الوطنية

208. http://www.coe.int/en/web/cybercrime/guidance-notes

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 8 من اتفاقية بودابست **أعمال الاحتيال المرتبطة بالحاسوب** يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وتدابير أخرى لتجريم الأفعال التالية بموجب قوانينه الداخلية، عند ارتكابها عمداً ودون حق، بما يسبب فقدان الممتلكات لشخص آخر عن طريق: أي مدخلات أو تغيير أو حذف أو إلغاء لبيانات الحاسوب، وأي تدخل في عمل نظام الحاسوب، بقصد احتيالي أو قصد غير شريف من أجل الحصول، دون حق، على منفعة اقتصادية لنفسه أو لشخص آخر. **القسم 12 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الاحتيال المرتبط بالحاسوب** الشخص الذي يتسبب في فقدان الممتلكات لشخص آخر، عن قصد، ودون عذر أو مبرر قانوني أو بتجاوز عذر أو مبرر قانوني، وذلك عن طريق: • أي إدخال أو تغيير أو حذف أو إلغاء لبيانات الحاسوب؛ • أي تدخل في عمل نظام الحاسوب، بقصد احتيالي أو غير شريف للحصول، دون حق، على منفعة اقتصادية لنفسه أو لشخص آخر، وتكون عقوبة هذه الأعمال السجن لمدة لا تتجاوز [المدة]، أو غرامة لا تتجاوز [المبلغ]، أو العقوبتين معاً.	**قانون الجرائم الإلكترونية رقم 27 لعام 2015** **المادة 6** كل من حصل قصدًا دون تصريح عن طريق الشبكة المعلوماتية أو أي نظم معلومات على بيانات أو معلومات تتعلق ببطاقات الائتمان أو بالبيانات أو بالمعلومات التي تستخدم في تنفيذ المعاملات المالية أو المصرفية الإلكترونية **المادة 7** كل من ارتكب أحد الأفعال المنصوص عليها في المواد 3 أو 4 أو 5 أو 6 من هذا القانون فيما يتعلق بنظام معلومات أو موقع إلكتروني أو شبكة معلومات بشأن تحويل الأموال أو تقديم خدمات الدفع أو المقاصة أو التسوية أو أي من الخدمات المصرفية التي تقدمها البنوك والشركات المالية	**التحليل القانوني** لا تتعلق هذه الجريمة سوى بالحصول على بيانات بطاقة الائتمان أو المعاملات المصرفية المالية واستخدامها دون تصريح. لن تغطي جميع أنواع التصيد الاحتيالي أو أنواع الاحتيال السيبراني الأخرى، مثل سرقة الهوية. يتطلب الاحتيال توافر التشويه الكاذب أو القصد غير الشريف - لا يعتمد على البيانات التي يتم الحصول عليها أو استخدامها. يرتبط الاحتيال بالحاسوب بمرتكب الجريمة الذي يقصد الحصول على منفعة اقتصادية لنفسه أو لشخص آخر. وليس من الضروري دائمًا إثبات تلك الخسارة أو توضيحها. **تحليل الفجوة** **التوصيات:** تُدرج جريمة الاحتيال مع القصد غير شريفة لتحيط بجميع أنواع النشاط الاحتيالي ذات الصلة بالحاسوب - استخدام القسم 12 من مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية أو المادة 8 من اتفاقية بودابست
المادة 9 **الجرائم ذات الصلة بالمحتوى (مثل المواد الإباحية للأطفال)** 1. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم السلوك التالي في قوانينه المحلية، عندما يرتكب عمدا وبدون حق: a. إنتاج مواد إباحية للأطفال بغرض توزيعها من خلال نظام حاسوب؛ عرض أو إتاحة مواد إباحية للأطفال من خلال نظام الحاسوب؛ توزيع أو نقل المواد الإباحية للأطفال من خلال نظام الحاسوب؛ شراء مواد إباحية للأطفال من خلال نظام حاسوب بقصد الاستخدام الشخصي أو لإعطائها لشخص آخر؛ امتلاك مواد إباحية للأطفال في نظام حاسوب أو على وسائط تخزين بيانات الحاسوب.	**قانون الجرائم الإلكترونية رقم 27 لعام 2015** **المادة 9** يُعاقب كل من أرسل أو نشر عن طريق نظام معلومات أو الشبكة المعلوماتية قصدًا كل ما هو مسموع أو مقروء أو مرئي يتضمن أعمالاً إباحية أو تتعلق بالاستغلال الجنسي لمن لم يكملا الثامنة عشرة من العمر. كل من قام قصدًا باستخدام نظام معلومات أو الشبكة المعلوماتية في إنشاء أو إعداد أو حفظ أو معالجة أو عرض أو طباعة أو نشر أو ترويج أنشطة أو أعمال إباحية لغايات التأثير على من لم يكمل الثامنة عشرة من العمر أو من هو معوق نفسيًا أو عقليًا، أو توجيهه أو تحريضه على ارتكاب جريمة.	**التحليل القانوني** تجريم هذه الأعمال يعتبر أساسيًا من أجل حماية الأطفال من الأذى، وذلك من خلال تجريم توزيع الصور غير اللائقة للأطفال ونقلها وتوفيرها وعرضها وحيازتها. يركز التشريع الوطني على توزيع أو استخدام «نظام معلومات أو الشبكة المعلوماتية «لإنشاء المواد الإباحية. لا تشمل هذه الجريمة حيازة المواد أو عرضها أو توفيرها أو إتاحة شرائها لشخص آخر. لا توجد تعريفات لعبارات «أعمال إباحية" أو "إنشاء» أو «إعداد» أو «حفظ» أو «عرض» أو «طباعة» أو «نشر» أو «ترويج أنشطة أو أعمال إباحية» ترتبط الفقرة ج على وجه التحديد بالاستغلال الجنسي للأطفال - ولكنها لا تقتصر على توفير صور غير لائقة للأطفال أو حيازتها **تحليل الفجوة** **التوصيات:** يفضل استخدام صياغة المادة 9 من اتفاقية بودابست أو القسم 13 من مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية لحماية الأطفال ومقاضاة الجناة

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
2. لأغراض الفقرة 1 أعلاه، يجب أن يشمل مصطلح «استغلال الأطفال في المواد الإباحية» أية مواد إباحية تصور بصريًا: a. قاصر مشترك في سلوك جنسي صريح؛ شخص يبدو أنه قاصر يشارك في سلوك جنسي صريح؛ صور واقعية تمثل قاصرًا مشاركًا في سلوك جنسي صريح. 3. لأغراض الفقرة 2 أعلاه، يشمل مصطلح «القاصر» جميع الأشخاص الذين تقل أعمارهم عن 18 عامًا. ومع ذلك، يجوز لأي طرف أن يطلب حدًا أدنى للسن، لا يقل عن 16 عامًا. 4. يجوز لكل طرف أن يحتفظ بالحق في عدم تطبيق الفقرات الفرعية 1 ، د. و ه، و 2، الفقرتين الفرعيتين ب و ج كليًا أو جزئيًا. **القسم 13 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية- المواد الإباحية للأطفال** 1. الشخص الذي يقوم عن قصد ودون عذر أو مبرر قانوني بـ: • إنتاج مواد إباحية للأطفال بغرض توزيعها من خلال نظام حاسوب؛ • تقدم أو توفر مواد إباحية للأطفال من خلال نظام حاسوب؛ • توزيع أو نقل المواد الإباحية عن الأطفال من خلال نظام حاسوب؛ • شراء و/أو الحصول على مواد إباحية للأطفال من خلال نظام حاسوب لاستخدامه الشخصي أو لإعطائها لشخص آخر؛ • حيازة مواد إباحية للأطفال في نظام حاسوب أو على وسائط تخزين بيانات الحاسوب؛ أو • الوصول عمدًا، من خلال تكنولوجيا المعلومات والاتصالات، إلى المواد الإباحية عن الأطفال، ، 2. يعتبر جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً. يمكن الدفاع أمام تهمة بجريمة منصوص عليها في الفقرة (1) (ب) إلى (1) (و) إذا أثبت الشخص أن المواد الإباحية عن الأطفال كانت بغرض إنفاذ القانون بحسن نية. 3. لا يجوز لدولة ما أن تجرم السلوك الموصوف في القسم 13 (1) (د) - (و).	كل من قام قصدًا باستخدام نظام معلومات أو الشبكة المعلوماتية لغايات استغلال من لم يكمل الثامنة عشرة من العمر أو من هو معوق نفسيًا أو عقليًا، في الدعارة أو الأعمال الإباحية	

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 10 من اتفاقية بودابست **انتهاك حقوق النشر** **المادة 17 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - الجرائم المتعلقة بحق المؤلف والحقوق المرتبطة بها**	1. الكتب والكتيبات وغيرها من المواد المكتوبة. 2. الأعمال الموجودة في المحاضرات والخطب والوعظ. 3. الأعمال المسرحية والمسرحيات الموسيقية والموسيقى والتمثيل المسرحي. 4. الأعمال الموسيقية، سواء كانت مرقمة أم لا، أو مصحوبة بكلمات أم لا. 5. الأعمال السينمائية والسمعية البصرية. 6. الرسم والنحت والنقش والهندسة المعمارية والفنون التطبيقية والزخرفية. 7. الرسوم التوضيحية والخرائط والتصاميم والرسومات والصور النمطية المتعلقة بالجغرافيا وخرائط سطح الأرض. 8. البرمجيات سواء بلغة المصدر أو لغة الجهاز، ج - يجب أن تتضمن الحماية عنوان العمل فقط إذا كان العنوان عبارة عن مصطلح مستمر للإشارة إلى موضوع العمل.	**التحليل القانوني** يضمن هذا الحكم حماية الابتكار في القرن الحادي والعشرين لدى دول الجنوب الشريكة والشركات والمواطنين. إضافة إلى ذلك، فإنه يحمي مجموعة الأعمال الأدبية أو الفنية مثل الموسوعات والمختارات والبيانات التي تم جمعها، إما في شكل مقروء آليًا أو بأي شكل آخر، ومن حيث اختيار محتوياتها أو ترتيبها، الأعمال التي تشكل أعمالاً فنية إبداعية. والمجموعات التي تحتوي على مقتطفات مختارة من الشعر أو النثر أو الموسيقى أو غيرها ممن ترد في هذه المجموعات ومصدر المقتطفات ومؤلفيها دون المساس بحقوق المؤلفين فيما يتعلق بكل عمل يشكل جزءًا من هذه المجموعات
المادة 11 من اتفاقية بودابست **المساعدة والتحريض** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لتجريم الأفعال التالية بموجب قانونه الداخلي، وذلك عندما يتم التحريض على ارتكاب أي من الجرائم المقررة وفقا للمواد من 2 إلى 10 من هذه الاتفاقية أو المساعدة عليها عمدًا، مع نية أن ترتكب هذه الجريمة. 2. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وتدابير أخرى لتجريم محاولة ارتكاب أي من الأفعال الإجرامية المنصوص عليها في المواد من 3 إلى 5 و 7 و 8 و 9.1. أ و ج من هذه الاتفاقية عمدًا. **المادة 19 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - محاولة ارتكاب الجرائم والاشتراك فيها** 1. الاشتراك في ارتكاب أية جريمة من الجرائم المنصوص عليها في هذا الفصل مع وجود نية ارتكاب الجريمة في قانون الدولة الطرف. 2. الشروع في ارتكاب الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية. 3. يجوز لأي دولة طرف الاحتفاظ بحقها في عدم تطبيق الفقرة الثانية من هذه المادة كليا أو جزئيا.	**قانون الجرائم الإلكترونية رقم 27 لعام 2015** **المادة 14** كل من قام قصدًا بالاشتراك أو التدخل أو التحريض على ارتكاب أي من الجرائم المنصوص عليها في هذا القانون بالعقوبة المحددة فيه لمرتكبيها	**التحليل القانوني** تعتبر مساعدة الآخرين وتحريضهم على ارتكاب جرائم أمرًا ضروريًا لمحاكمة أولئك الذين يكونون قد قدموا المساعدة أو شجعوا على ارتكاب جرائم الإنترنت. كما تشمل المادة 19 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات عبارة المحاولة وهي ليست مدرجة في المادة 14 **تحليل الفجوة** **التوصيات:** استخدام المادة 19 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات (حيث لا توجد إشارة إلى عبارة المحاولة في القانون الأردني) كدليل للتشريع الوطني

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 12 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[209] **مسؤولية الشركات**	**قانون المسطرة الجنائية**	**التحليل القانوني** هذا الحكم هو عنصر أساسي بحيث يستطيع الأشخاص الاعتباريون (مثلًا الكيانات التجارية) التصرف نيابة عن الأشخاص الطبيعيين الذين تقع عليهم مسؤولية جنائية
البروتوكول الإضافي لاتفاقية الجريمة السيبرانية، المتعلق بتجريم أعمال العنصرية وكراهية الأجانب المرتكبة من خلال أنظمة الحاسوب **المادة 3 - نشر المواد التي تحض على العنصرية وكراهية الأجانب من خلال أنظمة الحاسوب** يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم السلوك التالي في قوانينه المحلية، عندما يرتكب عمدا وبدون حق: 1. توزيع المواد العنصرية وكراهية الأجانب أو إتاحتها للجمهور من خلال نظام الحاسوب. 2. يجوز للطرف أ2 أن يحتفظ بالحق في عدم إسناد المسؤولية الجنائية بالتصرف على النحو المحدد في الفقرة 1 من هذه المادة، عندما تحض المواد الموزعة، كما هو محدد في الفقرة 1 من المادة 2، وتشجع على التمييز غير المرتبط بالكراهية أو العنف، شريطة أن تتوفر سبل انتصاف فعالة أخرى. 3. بصرف النظر عن الفقرة 2 من هذه المادة، يجوز للطرف أن يحتفظ بالحق في عدم تطبيق الفقرة 1 على حالات التمييز، لأن هذه الفقرة لا يمكن أن تمثل سبل انتصاف فعالة على النحو المشار إليه الفقرة 2، وذلك بسبب مبادئ ثابتة في نظامه القانوني الوطني متعلقة بحرية التعبير.	**قانون العقوبات**	**تحليل الفجوة** **التوصيات:** استخدم لغة المادة 3 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست، البروتوكول الإضافي باعتبارها دليلًا للتشريعات الوطنية حيث يتم تحديد أي فجوات محتملة
بروتوكول إضافي **المادة 4**[210] **- التهديد بدافع العنصرية وكراهية الأجانب** يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم السلوك التالي في قوانينه المحلية، عندما يرتكب عمدا وبدون حق: التهديد، من خلال نظام الحاسوب، بارتكاب جريمة جنائية خطيرة على النحو المحدد في قانونها الداخلي، (1) ضد أشخاص لسبب أنهم ينتمون إلى جماعة يميزها عرقها أو لونها أو نسبها أو أصلها القومي أو العرقي أو دينها، إذا تم استخدام أي من هذه العوامل ذريعةً، أو (2) ضد مجموعة من الأشخاص تتميز بأي من هذه الخصائص.	**المادة 278** يُعاقب بالحبس مدة لا تزيد على ثلاثة أشهر أو بغرامة لا تزيد على عشرين دينارًا كل من: 1. نشر شيئًا مطبوعًا أو مخطوطًا أو صورة أو رسمًا أو رمزًا من شأنه أن يؤدي إلى إهانة الشعور الديني لأشخاص آخرين أو إلى إهانة معتقدهم الديني؛ 2. تفوه في مكان عام وعلى مسمع من شخص آخر بكلمة أو بصوت من شأنه أن يؤدي إلى إهانة الشعور أو المعتقد الديني لذلك الشخص الآخر.	**التحليل القانوني** ترتبط المادة 278 بالمادة 15 من قانون الجرائم الإلكترونية رقم 27 لسنة 2015 التي تنص على أن كل من ارتكب أي جريمة معاقب عليها بموجب أي تشريع نافذ باستخدام الشبكة المعلوماتية أو أي نظام معلومات أو موقع إلكتروني أو اشترك أو تدخل أو حرض على ارتكابها، يعاقب بالعقوبة المنصوص عليها في ذلك التشريع **تحليل الفجوة** **التوصيات:** تشير المادة 278 إلى إهانة المعتقد الديني فحسب وليس إلى الجريمة الأوسع نطاقًا التي تنطوي على تهديدات بدافع كراهية الأجانب أو العنصرية. وعلاوةً على ذلك، لا توجد إشارة إلى ركن القصد الجنائي لعبارات «عن قصد» أو «بدون حق» - أو إلى السلوك التهديدي. استخدم لغة اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست في المادة 4 من البروتوكول الإضافي كدليل للتشريعات الوطنية

209. المادة 20 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات
210. لا يوجد ما يعادلها في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
بروتوكول إضافي **المادة 5[211] - الإهانة بدافع العنصرية وكراهية الأجانب** يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم السلوك التالي في قوانينه المحلية، عندما يرتكب عمدا وبدون حق: إهانة الجمهور، من خلال نظام حاسوبي، (1) الأشخاص لكونهم ينتمون إلى مجموعة يميزها عرقها أو لونها أو نسبها أو أصلها القومي أو العرقي أو دينها، إذا تم استخدام أي من هذه العوامل ذريعةً؛ أو (2) مجموعة من الأشخاص تتميز بأي من هذه الخصائص. يجوز للطرف أ2 إما: أن يشترط أن يكون للجريمة المشار إليها في الفقرة 1 من هذه المادة أثر على أن الشخص أو مجموعة الأشخاص المشار إليهم في الفقرة 1 والذين يتعرضون للكراهية أو الاحتقار أو السخرية؛ أو أن يحتفظ بالحق في عدم تطبيق الفقرة 1 من هذه المادة بشكل كلي أو جزئي.	**قانون العقوبات**	**التحليل القانوني** ترتبط المادة ذات الصلة بالمادة 15 من قانون الجرائم الإلكترونية رقم 27 لسنة 2015 التي تنص على أن كل من ارتكب أي جريمة معاقب عليها بموجب أي تشريع نافذ باستخدام الشبكة المعلوماتية أو أي نظام معلومات أو موقع إلكتروني أو اشترك أو تدخل أو حرض على ارتكابها، يعاقب بالعقوبة المنصوص عليها في ذلك التشريع **تحليل الفجوة** **التوصيات:** استخدم لغة المادة 5 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست، البروتوكول الإضافي باعتبارها دليلًا للتشريعات الوطنية حيث يتم تحديد أي فجوات محتملة
بروتوكول إضافي **المادة 6[212] - إنكار الإبادة الجماعية أو التقليل منها أو الموافقة عليها أو تبريرها** **جرائم ضد الإنسانية** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية لجعل الأفعال التالية يعتبر جرائم جنائية بموجب قوانينها الداخلية، عندما تُرتكب عمداً وبدون حق: a. توزيع أو توفير عبر نظام الحاسوب بأية طريقة من الطرق للجمهور، مواد تنكر أو تقلل أو تقر أو تقلل بشكل كبير الأفعال التي تشكل إبادة جماعية أو جرائم ضد الإنسانية، على النحو المحدد في القانون الدولي والمعترف بها على هذا النحو في القرارات النهائية والملزمة للمحكمة العسكرية الدولية، المنشأة بموجب اتفاقية لندن المؤرخة في 8 أغسطس 1945، أو أي محكمة دولية أخرى تنشأ بموجب المواثيق الدولية ذات الصلة والتي يعترف هذا الطرف باختصاصها القضائي.	**قانون العقوبات**	**التحليل القانوني** ترتبط المادة ذات الصلة بالمادة 15 من قانون الجرائم الإلكترونية رقم 27 لسنة 2015 التي تنص على أن كل من ارتكب أي جريمة معاقب عليها بموجب أي تشريع نافذ باستخدام الشبكة المعلوماتية أو أي نظام معلومات أو موقع إلكتروني أو اشترك أو تدخل أو حرض على ارتكابها، يعاقب بالعقوبة المنصوص عليها في ذلك التشريع **تحليل الفجوة** **التوصيات:** استخدم لغة المادة 6 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست، البروتوكول الإضافي باعتبارها دليلًا للتشريعات الوطنية حيث يتم تحديد أي فجوات محتملة

211. لا يوجد ما يعادلها في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات
212. لا يوجد ما يعادلها في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

الجرائم		
أفضل الممارسات الدولية	**التشريع الوطني**	**ملاحظات**
2. 2A يجوز للطرف إما a. أن يشترط أن يكون الإنكار أو التقليل إلى الحد الأدنى المشار إليه في الفقرة 1 من هذه المادة قد ارتكب بهدف التحريض على الكراهية أو التمييز أو العنف ضد أي فرد أو مجموعة من الأفراد على أساس العرق أو اللون أو النسب أو الأصل القومي أو العرقي أو الدين أو إذا استخدمت هذه العوامل ذريعة لذلك، أو b. أن يحتفظ بالحق في عدم تطبيق الفقرة 1 من هذه المادة بشكل كلي أو جزئي.		
جرائم إضافية للمراجعة		
الجرائم المتعلقة بالهوية **القسم 14 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية** يعاقب الشخص الذي يقوم عن قصد ودون عذر أو مبرر قانوني، أو يتجاوز عذرًا قانونيًا أو مبررًا باستخدام نظام حاسوب في أي مرحلة من مراحل الجريمة بنقل أو تملك أو استخدام وسيلة لتحديد الهوية شخص آخر بنية ارتكاب أي نشاط غير قانوني يشكل جريمة أو المساعدة أو التحريض عليها، عند إدانته بهذه الأعمال بالسجن لمدة لا تتجاوز [المدة] أو بغرامة لا يتجاوز [المبلغ]، أو بالعقوبتين معاً.	**قانون الجرائم الالكترونية** **رقم 27 لسنة 2015** **المادة 15** كل من ارتكب أي جريمة معاقب عليها بموجب أي تشريع نافذ باستخدام الشبكة المعلوماتية أو أي نظام معلومات أو موقع إلكتروني أو اشترك أو تدخل أو حرض على ارتكابها، يُعاقب بالعقوبة المنصوص عليها في ذلك التشريع.	**التحليل القانوني** في حين أن المادة 15 تجرم أي جريمة جوهرية تستخدم شبكة معلوماتية أو نظام معلومات أو موقع إلكتروني - لا توجد إشارة إلى أي جريمة في القانون الأردني تغطي مرحلة التحضير لجريمة خيانة الأمانة المتعلقة بالهوية. **تحليل الفجوة** **التوصيات:** يستحسن أن تدرج في التشريعات المحلية.
الكشف عن تفاصيل التحقيق **القسم 16 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية** موفر خدمة الإنترنت الذي يتلقى أمرًا يتعلق بتحقيق جنائي ينص صراحةً على الحفاظ على السرية أو على التزام شبيه ينص عليه القانون، ثم يقوم عن عمد ودون عذر أو مبرر قانوني أو بتجاوز لعذر قانوني مبرر، بالإفصاح عن: • حقيقة أنه قد تم إصدار أمر؛ أو • أي شيء تم تنفيذه بموجب الأمر؛ أو • أي بيانات تم جمعها أو تسجيلها بموجب الطلب؛ يعتبر جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً.		**التحليل القانوني** يعاقب على اختراق البيانات والكشف عن المعلومات الحساسة التي يمكن أن تؤثر على التحقيقات الجنائية **تحليل الفجوة** **التوصيات:** يستحسن أن تدرج في التشريعات المحلية.

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
عدم السماح بالمساعدة **القسم 17 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية** 1. أي شخص آخر غير المشتبه فيه فشل عمداً دون عذر أو مبرر قانوني أو بتجاوز عذر أو مبرر قانوني، بمساعدة شخص أو السماح بمساعدته، بناءً على أمر مثلما تحدد المواد 20 إلى 22[213] يرتكب جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة] ، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً. 2. قد يقرر أي بلد عدم تجريم عدم السماح بالمساعدة شرط أن تتوفر سبل انتصاف فعالة أخرى.		**التحليل القانوني** تتعلق هذه الجريمة بالأشخاص الذين لديهم معرفة محددة بالأدلة ذات الصلة والذين يرفضون تقديم المساعدة. غالبًا ما يعتمد تطبيق القانون على هؤلاء الأشخاص لتأمين الأدلة في التحقيقات الإلكترونية. هنالك مخالفة مستقلة وهي عدم توفير كلمات مرور أو الوصول إلى الرموز للأجهزة المشفرة أو البيانات (مثل «مفتاح المعلومات المحمية") - ينص القسم 53 من قانون تنظيم سلطات التحقيق في المملكة المتحدة لعام 2000 (RIPA)[214] على وجود جرم جنائي يتحمله الأشخاص الذين لا يمتثلون للمادة 49 من إخطار قانون تنظيم سلطات التحقيق في المملكة المتحدة والقاضية بالكشف عن «المفتاح" **تحليل الفجوة** **التوصيات:** يستحسن أن تدرج في التشريعات المحلية.
المطاردة السيبرانية **القسم 18 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية** الشخص الذي يقوم، دون عذر أو مبرر قانوني، أو يتجاوز عذرًا قانونيًا أو مبررًا، ببدء أي اتصال إلكتروني، بقصد إكراه شخص ما أو تخويفه أو مضايقته أو التسبب في ضائقة عاطفية كبيرة له، باستخدام نظام حاسوب لدعم السلوك المتكرر والعدائي والعنيف، يرتكب جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً.		**التحليل القانوني** هذه الجريمة تُجرم من يضايقون الأشخاص عبر الإنترنت - قد تنص بعض الولايات القضائية على جرائم تحرش غير مرتبطة بالحاسوب - لكن يوصى باعتماد هذه الجريمة لمتابعة لتلك الجرائم المرتكبة عبر الإنترنت. **تحليل الفجوة** **التوصيات:** يستحسن أن تدرج في التشريعات المحلية.
رعاية الأطفال على الإنترنت **القانون الجنائي الهولندي** 248e يعاقب الشخص الذي يقترح ترتيب لقاء، بوسائل عمل آلية أو باستخدام خدمة اتصال، مع شخص يعرف، أو ينبغي منطقيًا أن يعرف، أن هذا الشخص لم يصل بعد إلى سن السادسة عشرة، مع نية ارتكاب أفعال غير لائقة مع هذا الشخص أو لعمل صور عن عمل جنسي يشارك فيه هذا الشخص، بالسجن لمدة لا تقل عن سنتين أو بغرامة من الفئة الرابعة، إذا ارتكب أي عمل يقصد به تحقيق اللقاء. **قانون العقوبات الكندي** **القسم** 172.1 1. يرتكب جريمة كل شخص يتواصل عن طريق وسائل الاتصالات مع		**التحليل القانوني** لإثبات الجرم الهولندي، يلزم عقد لقاء لأغراض جنسية مع تقديم أدلة داعمة لتاريخ الدردشة عبر الإنترنت بقصد جنسي؛ طلب عقد لقاء مع دليل عن التخطيط لذلك (أي التاريخ والمكان). الغرض من القانون الكندي هو منع استدراج الكبار المفترسين للأطفال عبر الإنترنت. لا تتطلب هذه الجريمة حدوث جريمة جنسية. وهذا يعني أن المتهم لا يحتاج إلى الذهاب فعلاً لمقابلة الضحية شخصيًا. تكتمل الجريمة قبل اتخاذ أي إجراءات لارتكاب الجريمة الموضوعية. **تحليل الفجوة** **التوصيات:** يُنصح بإدراجها في التشريعات المحلية لتجريم هذا السلوك التحضيري قبل ارتكاب جريمة جنسية

213. أوامر البحث والاستيلاء والمساعدة والإنتاج
214. http://www.legislation.gov.uk/ukpga/2000/23/section/53

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
a. شخص يكون عمره أقل من 18 عامًا، أو يظن المتهم أن عمره أقل من 18 عامًا، بغرض تسهيل ارتكاب جريمة مرتبطة بهذا الشخص، وذلك بموجب المادة الفرعية 153 (1)، المادة 155، 163.1، 170 أو 171 أو القسم الفرعي 212 (1) أو (2) أو (2.1) أو (4)؛ b. شخص يكون عمره أقل من 16 عامًا، أو يظن المتهم أن عمره أقل من 16 عامًا، بغرض تسهيل ارتكاب جريمة مرتبطة بهذا الشخص، وذلك بموجب المواد 151 أو 152، أو الفقرة الفرعية 160(3) أو 173(2) أو الأقسام 271 أو 272 أو 273 أو 280؛ أو c. شخص يكون عمره أقل من 14 عامًا، أو يظن المتهم أن عمره أقل من 14 عامًا، بغرض تسهيل ارتكاب جريمة مرتبطة بهذا الشخص بموجب المادة 281. عقاب 2. يعتبر كل شخص يرتكب جريمة بموجب الفقرة الفرعية (1) مذنبًا a. مذنبًا بارتكاب جريمة ويكون عرضة لعقوبة السجن لمدة تتراوح بين 10 سنوات كحد أقصى وسنة واحدة كحد أدنى؛ أو مذنبًا بارتكاب جريمة يعاقب عليها في ملخص الإدانة بالسجن لمدة تتراوح بين 18 شهرًا كحد أقصى و 90 يومًا كحد أدنى. b. افتراض إعادة تقدير العمر 3. الأدلة على أن الشخص المشار إليه في الفقرة (1) (أ) أو (ب) أو (ج) قُدِّم للمتهم وعمره أقل من ثمانية عشر عامًا أو ستة عشر عامًا أو أربعة عشر عامًا، حسب الحالة، في حالة عدم وجود أدلة تثبت عكس ذلك تثبت أن المتهم يعتقد أن الشخص كان أقل من تلك السن. لا دفاع 4. لا يقبل دفاع المتهم أمام التهم الموجهة بموجب الفقرة (1) (أ) أو (ب) أو (ج) بأنه كان يعتقد أن الشخص المشار إليه في تلك الفقرة لا يقل عمره عن ثمانية عشر عامًا أو ستة عشر عامًا أو أربعة عشر عامًا، حسب الحالة، إلا في حالة اتخذ المتهم خطوات معقولة للتأكد من عمر الشخص.		

إجراءات		
أفضل الممارسات الدولية	**التشريع الوطني**	**ملاحظات**
المادة 19 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[215] **التفتيش وضبط** **بيانات الكمبيوتر المخزنة** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لتمكين سلطاته المختصة من البحث في أو الوصول إلى: a. نظام الحاسوب أو جزء منه وبيانات الحاسوب المخزنة فيه؛ و b. وسيلة تخزين بيانات الحاسوب، حيث يمكن تخزين بيانات الحاسوب في أراضيها. 2. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وغيرها من الإجراءات لضمان تستطيع سلطاته عند تفتيشها نظام حاسوب معينًا أو جزءًا منه أو الوصول إليه بطريقة مماثلة، وذلك وفقًا للفقرة 1. أ، ويكون لدها أسباب للاعتقاد بأن البيانات المطلوبة مخزنة في نظام حاسوب آخر أو أن جزءًا منها موجود في إقليمها، وهذه البيانات يمكن الوصول إليها قانونيًا من النظام الأولي أو متاحة لها، فإنها قادرة على توسيع نطاق البحث أو الوصول المشابه للنظام الآخر على وجه السرعة. 3. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وغيرها من الإجراءات لتمكين سلطاته المختصة من مصادرة أو تأمين بيانات الحاسوب التي تم الوصول إليها وفقًا للفقرات 1 أو 2. تشمل هذه التدابير القدرة على: a. حجز على نظام حاسوب أو جزء منه أو وسيلة تخزين بيانات الحاسوب، والقيام بما يلزم لتأمينه؛ إنشاء نسخة من بيانات الحاسوب هذه والاحتفاظ بها؛ الحفاظ على سلامة بيانات الحاسوب المخزنة ذات الصلة؛ أن يجعل الوصول إلى بيانات الحاسوب في نظام الحاسوب الذي تم الوصول إليه غير ممكن أو أن يحذفها.	**قانون الجرائم الإلكترونية رقم 27 لعام 2015** **المادة 13** مع مراعاة الشروط والأحكام المقررة في التشريعات النافذة ومراعاة حقوق المشتكى عليه الشخصية، يجوز لموظفي الضابطة العدلية، بعد الحصول على إذن من المدعي العام المختص أو من المحكمة المختصة، الدخول إلى أي مكان تشير الدلائل إلى استخدامه لارتكاب أي من الجرائم المنصوص عليها في هذا القانون، كما يجوز لهم تفتيش الأجهزة والأدوات والبرامج وأنظمة التشغيل والشبكة المعلوماتية والوسائل التي تشير الدلائل في استخدامها لارتكاب أي من الجرائم المنصوص عليها في القانون، كما يجوز لهم تفتيش الأجهزة والأدوات والبرامج والأنظمة والوسائل التي تشير الدلائل في استخدامها لارتكاب أي من تلك الجرائم، وفي جميع الأحوال على الموظف الذي قام بالتفتيش أن ينظم محضرا بذلك ويقدمه إلى المدعي العام المختص.	**التحليل القانوني** هذه هي صلاحية التحقيق الأكثر أهمية ويجب أن تشير إلى الحصول على حق الوصول وليس التفتيش. في «التقرير التوضيحي لاتفاقية بودابست، يعني «البحث" التفتيش عن البيانات أو قراءتها أو فحصها أو مراجعتها. ويشمل ذلك مفهوم البحث عن البيانات والبحث عن (فحص) البيانات. لكلمة "الوصول" معنى محايد وتعكس بدقة أكثر المصطلحات الحاسوبية؛ يتم استخدامها كذلك في المادتين 26 و 27 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.[216] **تحليل الفجوة** **التوصيات**: يجب أن يكون هناك إشارة محددة إلى المصادرة على النحو المنصوص عليه في المادة 27 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. ويُنصح بوجود تعريف لكلمة «مصادرة" لضمان النزاهة ولتحديد الإجراءات - انظر القسم 3 (16) من مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية "يشمل الحجز: • تشغيل أي نظام حاسوب في الموقع ووسائط تخزين بيانات الحاسوب؛ • إنشاء نسخة من بيانات الحاسوب والاحتفاظ بها، بما في ذلك عن طريق استخدام معدات في الموقع؛ • الحفاظ على سلامة بيانات الحاسوب المخزنة ذات الصلة؛ • أن يجعل الوصول غير ممكن إلى بيانات الحاسوب في نظام الحاسوب الذي تم الوصول إليه أو أن يحذفها؛ • أخذ نسخة مطبوعة من بيانات غير ممكن؛ أو • حجز نظام حاسوب أو جزء منه أو وسيلة تخزين بيانات الحاسوب، والقيام بما يلزم لتأمينه» تنص المادة 21 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية على التشريع لضمان تقديم المساعدة من قبل أولئك الذين لديهم معرفة متخصصة بموقع الأدلة ذات الصلة - يمكن استخدام هذا كدليل - انظر أيضًا القسم 17 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية، المتعلق بالجريمة في حال تم رفض المساعدة دون عذر قانوني

215. المادتين 26 و 27 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات
216. الفقرة 191، الصفحة 33 التقرير التوضيحي لاتفاقية بودابست

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
4. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لتمكين سلطاته المختصة من أن تأمر أي شخص لديه معرفة بعمل نظام الحاسوب أو التدابير المطبقة لحماية البيانات الموجودة فيه بتوفير ما يلزم من المعلومات بما يكفل تنفيذ الإجراءات المشار إليها في الفقرتين 1 و 2. 5. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و 15. **القسم 20 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - البحث والضبط** 1. إذا اقتنع [القاضي] بناء على [معلومات تحت القسَم] [شهادة خطية] أن هناك أسبابًا معقولة [للاشتباه] [للاعتقاد] أنه قد يكون هناك في مكان ما شيء أو بيانات حاسوب: • قد تكون مادية كدليل في إثبات الجريمة؛ أو • قد اكتسبها شخص نتيجة لجريمة؛ [يجوز] [يأمر] يصدر [القاضي] تفويضًا لضابط [إنفاذ القانون] [الشرطة]، ويزوده بما قد يلزم من مساعدة، لدخول المكان للبحث عن الشيء أو بيانات الحاسوب وضبطها، وعمل ما يلزم بما في ذلك البحث أو عمليات الوصول الشبيهة: – نظام الحاسوب أو جزء منه وبيانات الحاسوب المخزنة فيه؛ و – وسيلة تخزين بيانات الحاسوب، حيث يمكن تخزين بيانات الحاسوب في إقليم البلد. 2. إذا كان[قوة إنفاذ القانون] [الشرطة] الذي يجري عملية بحث على أساس القسم 20 (1) أسباب للاعتقاد بأن البيانات المطلوبة مخزنة في نظام حاسوب آخر أو جزء منه في إقليمها، وأن هذه البيانات يمكن الوصول إليها قانونيًا أو يمكن أن تكون متاحة من النظام الأولي، فيجب أن يكون قادرًا على توسيع نطاق البحث أو الوصول إلى النظام الآخر بطريقة مماثلة. 3. يتم تمكين ضابط [تطبيق القانون] [الشرطة] الذي يقوم بالبحث من مصادرة أو تأمين بيانات الحاسوب المماثلة التي يتم الوصول إليها وفقًا للفقرات 1 أو 2.		

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
القسم 21 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - المساعدة يجب على أي شخص لا يشتبه في ارتكابه جريمة ولكن لديه علم بسير عمل نظام الحاسوب أو التدابير المطبقة لحماية بيانات الحاسوب الواردة فيه والتي تخضع لعملية بحث بموجب المادة 20، أن يسمح وأن يساعد إذا لزم الأمر وطلب منه الشخص المسؤول أن يجري البحث عن طريق: • توفير المعلومات التي تمكن من اتخاذ التدابير المشار إليها في المادة 20؛ • الوصول إلى نظام حاسوب أو وسيط تخزين بيانات الحاسوب واستخدامه للبحث في أي بيانات حاسوب متاحة أو في النظام؛ • الحصول على ونسخ بيانات حاسوب هذه؛ • استخدام المعدات لعمل نسخ؛ و • الحصول على معلومات واضحة من نظام حاسوب بشكل مقبول في الإجراءات القانونية. **المادة 26 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - فحص المعلومات المخزنة** 1. تلتزم كل دولة طرف يتبني الإجراءات الضرورية لتمكين سلطاتها المختصة من التفتيش أو الوصول إلى: a. تقنية معلومات أو جزء منها والمعلومات المخزنة فيها أو المخزنة عليها. b. بيئة أو وسيط تخزين معلومات تقنية معلومات والذي قد تكون معلومات التقنية مخزنة فيه أو عليه. 2. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من التفتيش أو الوصول إلى تقنية معلومات معينة أو جزء منها بما يتوافق مع الفقرة (-1 أ) إذا كان هناك اعتقاد بأن المعلومات المطلوبة مخزنة في تقنية معلومات أخرى أو جزء منها في إقليمها وكانت هذه المعلومات قابلة للوصول قانونا أو متوفرة في التقنية الأولى فيجوز توسيع نطاق التفتيش والوصول للتقنية الأخرى.		

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 27 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - حجز المعلومات المخزنة 1. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من حجز وتأمين معلومات تقنية المعلومات التي يتم الوصول إليها حسب الفقرة 1 من المادة 26 من هذه الاتفاقية. هذه الإجراءات تشمل صلاحيات: a. حجز وتأمين تقنية المعلومات أو جزء منها أو وسيط تخزين معلومات تقنية المعلومات. عمل نسخة معلومات تقنية المعلومات والاحتفاظ بها. الحفاظ على سلامة معلومات تقنية المعلومات المخزنة. إزالة أو منع الوصول إلى تلك المعلومات في تقنية المعلومات التي يتم الوصول إليها. 2. تلتزم كل طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى أي شخص لديه معرفة بوظيفة تقنية المعلومات أو الإجراءات المطبقة لحماية تقنية المعلومات من أجل تقديم المعلومات الضرورية لإتمام تلك الإجراءات المذكورة في الفقرتين 2 و3 من المادة السادسة والعشرين من هذه الاتفاقية.		
المادة 16 من اتفاقية بودابست **الحفظ المستعجل لبيانات الحاسوب المخزنة والكشف عنها** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وغيرها من الإجراءات لتمكين سلطاته المختصة من طلب الحفظ السريع لبيانات الحاسوب المحددة أو الحصول عليها بشكل مماثل، بما في ذلك بيانات المرور التي تم تخزينها عن طريق نظام حاسوبي، ولا سيما عندما يكون هناك أسباب للاعتقاد بأن بيانات الحاسوب معرضة بشكل خاص للفقد أو التعديل.	**لا يوجد معادل**	**التحليل القانوني** هذه السلطة الإجرائية مهمة لضمان الحفاظ على البيانات المعرضة للحذف أو الفقد. **تحليل الفجوة** **التوصيات:** تعد هذه القدرة المستعجلة للاحتفاظ بمعلومات المشترك الأساسية والبيانات الوصفية والمعاملات والمحتويات المخزنة ضرورية كجزء من تحقيقات جرائم الإنترنت، ولضمان أن تكون الأدلة متاحة للبحث والوصول والضبط والمراجعة. يمكن استخدام لغة المادة 16 من اتفاقية بودابست أو القسم 23 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية أو المادة 23 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. سيتطلب ذلك أيضًا تعريفات «بيانات الحاسوب»،[217] و"معلومات المشترك أو معلومات المشترك الأساسية"، و "حركة البيانات"[218] و"مزود خدمة الاتصالات"[219]

217. انظر المادة 1.ب. اتفاقية بودابست **أو** القسم 3 (6) من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية
218. انظر المادة 1.د من اتفاقية بودابست: "أي بيانات حاسوب تتعلق باتصال عن طريق نظام حاسوب، يتم إنشاؤها بواسطة نظام حاسوب يشكل جزءًا من سلسلة الاتصال، وتعرض مصدر الاتصال أو وجهته أو مساره أو الوقت أو التاريخ أو حجمه أو مدته أو نوع الخدمة الأساسية"، **أو** القسم 3 (18) من مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية: "حركة البيانات تعني أي بيانات حاسوب تتعلق باتصال عن طريق نظام حاسوب، يتم إنشاؤها بواسطة نظام حاسوب يشكل جزءًا من سلسلة الاتصال، وتعرض مصدر الاتصال أو وجهته أو مساره أو الوقت أو التاريخ أو الحجم أو المدة أو نوع الخدمة الأساسية".
219. انظر المادة 1.ج من اتفاقية بودابست: "1 أي كيان عام أو خاص يوفر للمستخدمين قدرة الاتصال عن طريق نظام الحاسوب، و 2 أي كيان آخر يعالج أو يخزن بيانات الحاسوب نيابة عن خدمة الاتصال هذه أو مستخدمي هذه الخدمة».

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
2. عندما يقوم أحد الأطراف بتنفيذ الفقرة 1 أعلاه عن طريق أمر شخص بحفظ بيانات الحاسوب المخزنة المحددة وذلك بوضعها في حوزته أو تحت سيطرته، يعتمد هذا الطرف الإجراءات التشريعية وغيرها من الإجراءات التي قد تكون ضرورية لإلزام ذلك الشخص بالحفاظ على سلامة بيانات الحاسوب لفترة زمنية طويلة، حدها الأقصى تسعين يومًا، وذلك لتمكين السلطات المختصة من طلب الكشف عنها. يجوز للطرف أن ينص على تجديد هذا الأمر لاحقًا. 3. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لإلزام الحارس أو أي شخص آخر يحفظ بيانات الحاسوب بالحفاظ على سرية تنفيذ هذه الإجراءات للفترة الزمنية المنصوص عليها في قانونه الداخلي. 4. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و 15. **القسم 23 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الحفظ المستعجل** إذا اقتنع ضابط [تطبيق القانون] [الشرطة] بوجود أسباب معقولة للاعتقاد بأن بيانات الحاسوب المطلوبة لأغراض التحقيق الجنائي معرضة للضياع أو التعديل، يجوز لضابط [تطبيق القانون] [الشرطة]، عن طريق إشعار مكتوب مقدم إلى شخص يتحكم في بيانات الكمبيوتر، أن يطلب من هذا الشخص الحفاظ على البيانات المحددة في الإشعار لمدة تصل إلى سبعة (7) أيام على وفقًا لما هو محدد في الإشعار. يمكن تمديد الفترة إلى ما بعد سبعة (7) أيام إذا سمح [قاضي]، بناءً على طلب من طرف واحد، وذلك لمدة زمنية أخرى محددة. **المادة 23 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات- الحفظ المستعجل للبيانات المخزنة في تكنولوجيا المعلومات** 1. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأمر أو الحصول على الحفظ العاجل للمعلومات المخزنة بما في ذلك معلومات تتبع المستخدمين والتي خزنت على تقنية معلومات وخصوصا إذا كان هناك اعتقاد بأن تلك المعلومات عرضة للفقدان أو التعديل.		يجب ملاحظة أن اتفاقية بودابست واتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية لا تقدمان تعريفًا لمعلومات المشترك الأساسية؛ غير أن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات تقدم تعريفًا لمعلومات المشترك:[220] "أي معلومات لدى مزود الخدمة بخصوص المشتركين في الخدمة، باستثناء المعلومات التي يمكن من خلالها معرفة ما يلي: • نوع خدمة الاتصال المستخدمة والأحكام الفنية المتعلقة بها وفترة الخدمة. • هوية المشترك وعنوانه البريدي أو الجغرافي أو رقم الهاتف ومعلومات الدفع المتاحة بموجب اتفاقية الخدمة • أي معلومات أخرى على موقع تركيب معدات الاتصالات بموجب اتفاقية الخدمة". ينبغي إيلاء اهتمام لأن يكون طول مدة الحفظ معقولًا في هذه الظروف، وأن يُسمَح بتطبيق التمديد في الظروف الملحة - تنص اتفاقية بودابست والاتفاقية العربية لمكافحة جرائم تقنية المعلومات على 90 يومًا، فيما تنص اتفاقية بودابست ومواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية على 7 أيام. ووفقًا للتجربة فإن مدة 90 يومًا هي مدة قصيرة في التحقيقات عبر الإنترنت، ويجب أن تكون حوالي 180 يومًا يمكن تمديدها.

220. انظر المادة 2 (9) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
2. تلتزم كل دولة طرف بتبني الإجراءات الضرورية فيما يتعلق بالفقرة 1 بواسطة إصدار أمر إلى شخص من أجل حفظ معلومات تقنية المعلومات المخزنة والموجودة بحيازته أو سيطرته ومن أجل إلزامه بحفظ وصيانة سلامة تلك المعلومات لمدة أقصاها 90 يوما قابلة للتجديد، من أجل تمكين السلطات المختصة من البحث والتقصي تلتزم كل دولة طرف بتبني الإجراءات الضرورية لإلزام الشخص المسؤول عن حفظ تقنية معلومات للإبقاء على سرية الإجراءات طوال الفترة القانونية المنصوص عليها في القانون الداخلي.		
المادة 17 من اتفاقية بودابست **الحفظ المستعجل والكشف الجزئي لحركة البيانات** 1. فيما يتعلق بحركة البيانات التي يتعين الحفاظ عليها بموجب المادة 16، يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى من أجل: a. التأكد من أن مثل هذا الحفظ المستعجل لحركة البيانات متاح بغض النظر عما إذا كان هناك واحد أو أكثر من مقدمي الخدمة قد شاركوا في نقل ذلك الاتصال؛ و b. ضمان الكشف السريع للسلطة المختصة لدى الدولة الطرف، أو للشخص المعين من قبل تلك السلطة، عن كمية كافية من حركة البيانات لتمكينه من تحديد مقدمي الخدمات والمسار الذي تم من خلاله نقل الاتصال. 2. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و 15. **القسم 23 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الحفظ المستعجل** إذا اقتنع ضابط [تطبيق القانون] [الشرطة] بوجود أسباب معقولة للاعتقاد بأن بيانات الحاسوب المطلوبة لأغراض التحقيق الجنائي معرضة للضياع أو التعديل، يجوز لضابط [تطبيق القانون] [الشرطة]، عن طريق إشعار مكتوب مقدم إلى شخص يتحكم في بيانات الكمبيوتر، أن يطلب من هذا الشخص الحفاظ على البيانات المحددة في الإشعار لمدة تصل إلى سبعة (7) أيام على وفقًا لما هو محدد في الإشعار. يمكن تمديد الفترة إلى ما بعد سبعة (7) أيام إذا سمح [قاضي]، بناءً على طلب من طرف واحد، وذلك لمدة زمنية أخرى محددة.	**لا يوجد معادل**	**التحليل القانوني** تعد هذه القوة الإجرائية مهمة بشكل خاص لضمان توفير مقدمي خدمات الإنترنت لعناوين بروتوكول إنترنت يمكنها تحديد موقع مرتكب الجريمة السيبرانية. يؤكد الاستبيان أنه يمكن حفظ البيانات عند استلام أحد طلبات الإنابة القضائية **تحليل الفجوة** **التوصيات:** يجب تضمين هذه القوة المستعجلة جنبًا إلى جنب مع الكشف عن حركة البيانات في التشريعات لتمكين التحقيقات الفعالة في جرائم الإنترنت. يمكن استخدام لغة المادة 17 من اتفاقية بازل، القسمين 23 و 24 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية أو المادة 24 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. سيتطلب ذلك أيضًا تعريفات لـ «حركة البيانات" و "مزود خدمة الاتصالات"[221]

221. انظر التعريفات أعلاه

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
القسم 24 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - جمع بيانات حركة الاتصالات إذا اقتنع ضابط [تطبيق القانون] [الشرطة] بناءً على أسباب معقولة بأن البيانات المخزنة في نظام الحاسوب ضرورية لأغراض التحقيق الجنائي، يجوز له أن يطلب، عبر إشعار خطي، من شخص له السيطرة على نظام الحاسوب كشف بيانات حركة مرور تتعلق باتصال محدد بشكل كافٍ لتحديد: مزودو خدمة الإنترنت؛ و/ أو المسار الذي تم من خلاله نقل الاتصال. **المادة 24 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - لتحفظ العاجل والكشف الجزئي لمعلومات تتبع المستخدمين** تلتزم كل دولة طرف بتبني الإجراءات الضرورية فيما يختص بمعلومات تتبع المستخدمين من أجل: 1. ضمان توفر الحفظ العاجل لمعلومات تتبع المستخدمين بغض النظر عن اشتراك واحد أو أكثر من مزودي الخدمة في بث تلك الاتصالات. 2. ضمان الكشف العاجل للسلطات المختصة لدى الدولة الطرف أو لشخص تعينه تلك السلطات لمقدار كاف من معلومات تتبع المستخدمين لتمكين الدولة الطرف من تحديد مزودي الخدمة ومسار بث الاتصالات.		

إجراءات		
أفضل الممارسات الدولية	**التشريع الوطني**	**ملاحظات**
المادة 18 من اتفاقية بودابست[222] **أمر النسخ** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وتدابير أخرى لتمكين سلطاته المختصة من أن تأمر: a. شخصًا موجودًا في إقليمها بتقديم بيانات حاسوب محددة في حيازته أو تحت سيطرته، وتُخَزّن في نظام حاسوب أو بوسيلة تخزين بيانات الحاسوب؛ و مقدم خدمة يقدم خدماته في إقليم الدولة الطرف بتقديم معلومات المشترك المرتبطة بهذه الخدمات، والتي تكون في حيازة أو تحت سيطرة مقدم الخدمة. 2. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و 15. 3. تعني «معلومات المشترك» أي معلومات محفوظة بشكل بيانات حاسوب أو أي شكل آخر ويحتفظ بها مزود الخدمة، وترتبط بالمشتركين في خدماته، بخلاف بيانات الحركة أو المحتوى، والتي يمكن إنشاؤها من خلال: a. نوع خدمة الاتصال المستخدمة والأحكام الفنية المتعلقة بها وفترة الخدمة؛ هوية المشترك أو العنوان البريدي أو الجغرافي، ورقم الهاتف وأرقام الاتصال الأخرى ومعلومات الفوترة والدفع المتاحة بناءً على اتفاقية الخدمة؛ أي معلومات أخرى متاحة على موقع تركيب معدات الاتصالات بناءً على اتفاقية الخدمة أو الترتيب. **القسم 22 من نظام اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - أمر النسخ** إذا كان [قاض] مقتنعًا بناءً على طلب قدمه [ضابط إنفاذ القانون] [الشرطة] بأن بيانات حاسوب محددة أو نسخة مطبوعة أو غيرها من المعلومات ضرورية لإجراء تحقيق جنائي أو لإجراءات جنائية، يجوز [للقاضي] أن يأمر بما يلي:	**لا يوجد معادل**	**التحليل القانوني** هذا شرط أساسي لإجراء تحقيق فعال في جرائم الإنترنت وسيؤثر غيابه على الملاحقات القضائية والتعاون الدولي. **تحليل الفجوة** **التوصيات:** تعتبر هذه السلطة الأساسية ضرورية لضمان توفير مزودي خدمة الاتصالات في مصر لمعلومات المشترك الأساسية وحركة البيانات وبيانات المحتوى المخزنة. سيتطلب ذلك أيضًا تعريفات لـ «بيانات الحاسوب" و "معلومات المشترك أو معلومات المشترك الأساسية" و "حركة البيانات" و "مزود خدمة الاتصالات".[223] المادة 25 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات هي نموذج يمكن استخدامه ويستخدم تعريفات مختلفة بما في ذلك «تكنولوجيا المعلومات"،[224] و"مزود الخدمة"[225] و"البيانات"؛[226] غير أنه من المستحسن أن تكون هناك تعريفات لـ «معلومات المشترك أو معلومات المشترك الأساسية" أو "حركة البيانات" لأنها ستكون أنواع مختلفة من الأدلة التي يمكن توليدها في دول الجنوب الشريكة. علاوةً على ذلك، سوف تتطلب هذه السلطة من الأفراد وغيرهم (مثل الكيانات المؤسسية والمؤسسات المالية وغيرها من المنظمات) ممن يحملون البيانات أن يقوموا بإصدارها بناء على طلب سلطات إنفاذ القانون. يمكن أن تكون المادة 18 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست والمادة 22 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية بمثابة دليل مع التطبيق الثابت للتعريفات

222. المادة 25 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات
223. انظر التعريفات أعلاه
224. المادة 2 (1) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات: "أية وسيلة مادية أو معنوية أو مجموعة وسائل مترابطة أو غير مترابطة تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها وفقا للأوامر والتعليمات المخزونة بها. ويشمل ذلك جميع المدخلات والمخرجات المرتبطة بها سلكيا أو لا سلكيا في نظام أو شبكة".
225. المادة 2 (2) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات: "أي شخص طبيعي أو معنوي عام أو خاص يزود المشتركين بالخدمات للتواصل بواسطة تقنية المعلومات، أو يقوم بمعالجة أو تخزين المعلومات نيابة عن خدمة الاتصالات أو مستخدميها".
226. المادة 2 (3) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات: "كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة تقنية المعلومات، كالأرقام والحروف والرموز وما إلى ذلك".

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
• أن ينسخ شخص في إقليم [الدولة المشترعة] يتحكم في نظام الحاسوب نسخًا محددة من بيانات الحاسوب أو نسخة مطبوعة أو معلومات أخرى واضحة من تلك البيانات؛ أو • مزود خدمة الإنترنت في [الدولة المشترعة] لتقديم معلومات حول الأشخاص المشتركين في الخدمة أو الذين يستخدمونها بطريقة أخرى. **المادة 25 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - أمر تسليم المعلومات** تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى: 1. أي شخص في إقليمها لتسليم معلومات معينة في حيازة ذلك الشخص والمخزنة على تقنية معلومات أو وسيط تخزين معلومات. 2. أي مزود خدمة يقدم خدماته في إقليم الدولة الطرف لتسليم معلومات المشترك المتعلقة بتلك الخدمات في حوزة مزود الخدمة أو تحت سيطرته.		
المادة 21 من اتفاقية بودابست[227] **اعتراض بيانات المحتوى** 1. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وغيرها من الإجراءات، فيما يتعلق بمجموعة من الجرائم الخطيرة التي يحددها القانون المحلي، لتمكين سلطاته المختصة من: a. الجمع أو التسجيل من خلال تطبيق الوسائل التقنية على أراضي ذلك الطرف، و إلزام مزود الخدمة، في حدود قدرته التقنية الحالية: i. الجمع أو التسجيل من خلال تطبيق الوسائل التقنية على أراضي ذلك الطرف؛ أو ii. التعاون ومساعدة السلطات المختصة في جمع أو تسجيل بيانات المحتوى في الوقت الحقيقي، لاتصالات محددة تتم في أراضيها وترسل عن طريق نظام حاسوبي.	**قانون الجرائم الإلكترونية رقم 27 لعام 2015** **المادة 13** مع مراعاة الشروط والأحكام المقررة في التشريعات النافذة ومراعاة حقوق المشتكى عليه الشخصية، يجوز لموظفي الضابطة العدلية، بعد الحصول على إذن من المدعي العام المختص أو من المحكمة المختصة، الدخول إلى أي مكان تشير الدلائل إلى استخدامه لارتكاب أي من الجرائم المنصوص عليها في هذا القانون، كما يجوز لهم تفتيش الأجهزة والأدوات والبرامج وأنظمة التشغيل والشبكة المعلوماتية والوسائل التي تشير الدلائل في استخدامها لارتكاب أي من الجرائم المنصوص عليها في القانون، كما يجوز لهم تفتيش الأجهزة والأدوات والبرامج والأنظمة والوسائل التي تشير الدلائل في استخدامها لارتكاب أي من تلك الجرائم، وفي جميع الأحوال على الموظف الذي قام بالتفتيش أن ينظم محضرا بذلك ويقدمه إلى المدعي العام المختص.	**التحليل القانوني** تسمح هذه المادة للشرطة القضائية باعتراض الاتصالات بإذن من المدعي العام **تحليل الفجوة** **التوصيات:** ينبغي اتخاذ تدابير لإلزام مقدمي الخدمات في الأردن بالتعاون مع جمع المحتويات في الوقت الحقيقي لجميع الجرائم؛ وينبغي إدراج الضمانات لضمان أن تكون عمليات الاعتراض والجمع قانونية وضرورية ومعقولة ومتناسبة مع الحالة. يجب مراعاة مراجعة المادة 29 من CITO والمادة 21 من اتفاقية بودابست والقسم 26 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية وإدراج اللغة في التشريعات الوطنية

٢٢٧. المادة ٩٢ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
2. في الحالات التي لا يمكن فيها لأي طرف، بسبب المبادئ المستقرة في نظامه القانوني الداخلي، أن يعتمد التدابير المشار إليها في الفقرة 1.أ، يجوز له بدلا من ذلك اعتماد تدابير تشريعية وتدابير أخرى قد تكون ضرورية لضمان جمع أو تسجيل البيانات المرورية المرتبطة باتصالات محددة مرسلة في أراضيه، في الوقت الحقيقي، من خلال تطبيق الوسائل التقنية على ذلك الإقليم. 3. يعتمد كل طرف التدابير التشريعية والتدابير الأخرى التي قد تكون ضرورية لإلزام مقدم الخدمة بالحفاظ على سرية تنفيذ أي سلطة منصوص عليها في هذه المادة وأي معلومات تتعلق بها. 4. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و 15. **القسم 26 مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - اعتراض بيانات المحتوى** 1. إذا تأكد [قاض] بناء على [شهادة تحت القسم] [شهادة خطية] بأن هناك أسباباً معقولة لـ [الاشتباه] [الظن] بأن محتوى البلاغات الإلكترونية هو مطلوب بشكل معقول لأغراض [التحقيق] في تحقيق جنائي، [يجوز] [للقاضي] [يجب] أن: • يطلب من مزود خدمة الإنترنت الذي تتوفر خدمته في [بلد المشرع] جمع أو تسجيل أو السماح أو مساعدة السلطات المختصة في جمع أو تسجيل بيانات المحتوى المرتبطة بالاتصالات المحددة التي يتم إرسالها عن طريق نظام حاسوب، وذلك من خلال استخدام وسائل تقنية؛ أو • السماح لموظف [قوة تنفيذ القانون] [الشرطة] بجمع أو تسجيل تلك البيانات من خلال تطبيق الوسائل التقنية. 2. قد تقرر دولة عدم تنفيذ القسم 26.	مع مراعاة الفقرة (أ) من هذه المادة ومراعاة حقوق الآخرين ذوي النية الحسنة، وباستثناء المرخص لهم وفق أحكام قانون الاتصالات ممن لم يشتركوا بأي جريمة منصوص عليها في هذا القانون، يجوز لموظفي الضابطة العدلية ضبط الأجهزة والأدوات والبرامج وأنظمة التشغيل والوسائل المستخدمة لارتكاب أي من الجرائم المنصوص عليها أو يشملها هذا القانون والأموال المتحصلة منها والتحفظ على المعلومات والبيانات المتعلقة بارتكاب أي منها. للمحكمة المختصة الحكم بمصادرة الأجهزة والأدوات وتوقيف أو تعطيل عمل أي نظام معلومات أو موقع إلكتروني مستخدم في ارتكاب أي من الجرائم المنصوص عليها أو يشملها هذا القانون ومصادرة الأموال المتحصلة من تلك الجرائم والحكم بإزالة المخالفة على نفقة الفاعل.	

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 29 الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - اعتراض معلومات المحتوى 1. تلتزم كل دولة طرف باعتماد الإجراءات التشريعية اللازمة المتعلقة بسلسلة من الجرائم المنصوص عليها في القانون المحلي، وذلك لتمكين السلطات المختصة من: a. تسجيل أو جمع المعلومات من خلال الوسائل التقنية في أراضي هذه الدولة الطرف، أو التعاون مع السلطات المختصة ومساعدتها على تسريع جمع وتسجيل معلومات المحتوى الخاصة بالاتصالات ذات الصلة في إقليمها والتي يتم نقلها عن طريق تكنولوجيا المعلومات. 2. إذا تعذر على الدولة الطرف، بسبب النظام القانوني المحلي، اعتماد الإجراءات المبينة في الفقرة 1 (أ)، يجوز لها اعتماد إجراءات أخرى بالشكل الضروري لضمان تسريع جمع وتسجيل معلومات المحتوى المقابلة الاتصالات ذات الصلة في أراضيها باستخدام الوسائل التقنية في ذلك الإقليم. 3. تلتزم كل دولة طرف باعتماد الإجراءات اللازمة لمطالبة مقدم الخدمة بالحفاظ على سرية أي معلومات عند ممارسة السلطة المنصوص عليها في هذه المادة.		
المادة 20 من اتفاقية بودابست[228] **جمع بيانات حركة الاتصالات في الوقت الحقيقي** 1. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتمكين سلطاته المختصة من: a. الجمع أو التسجيل من خلال تطبيق الوسائل التقنية على أراضي ذلك الطرف، و إلزام مزود الخدمة، في حدود قدرته التقنية الحالية: i. الجمع أو التسجيل من خلال تطبيق الوسائل التقنية على أراضي ذلك الطرف؛ أو ii. يتعاون ويساعد السلطات المختصة في جمع أو تسجيل حركة البيانات في الوقت الفعلي، مع الاتصالات المعينة في إقليمها والتي تبث بواسطة نظام حاسوبي.	**لا يوجد معادل** **التحليل القانوني** لا توجد سلطة إجرائية لجمع بيانات الحركة في الوقت الحقيقي. يمكن أن يكون هناك حد أدنى لجمع بيانات الحركة في الوقت الحقيقي، وتعد هذه الحركة أداة تحقيق أساسية. قد تكون هناك حالات لا يضع فيها مقدم الطلب حدًا قانونيًا أعلى لتأمين المحتوى، ولكن يمكن وجود حد أدنى لتأمين حركة البيانات. لهذا السبب، يجب أن يكون هناك تمييز بين جمع المحتوى المخزن وبيانات الحركة في الوقت الحقيقي. يجب أن تكون هناك ضمانات ومتطلبات/إجراءات لإلزام مزودي خدمة الاتصالات على التعاون في جمع أو تسجيل بيانات المحتوى في الوقت الفعلي لاتصالات محددة تتم في الأردن	

228. تشير المادة 28 من اتفاقية الاتفاقية العربية لمكافحة جرائم تقنية المعلومات إلى الجمع المستعجل بدلًا من الجمع في الوقت الحقيقي

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
2. في الحالات التي لا يمكن فيها لأي طرف، بسبب المبادئ المستقرة في نظامه القانوني الداخلي، أن يعتمد التدابير المشار إليها في الفقرة 1.أ، يجوز له بدلا من ذلك اعتماد تدابير تشريعية وتدابير أخرى قد تكون ضرورية لضمان جمع أو تسجيل البيانات المرورية المرتبطة باتصالات محددة مرسلة في أراضيه، في الوقت الفعلي، من خلال تطبيق الوسائل التقنية على ذلك الإقليم. 3. يعتمد كل طرف التدابير التشريعية والتدابير الأخرى التي قد تكون ضرورية لإلزام مقدم الخدمة بالحفاظ على سرية تنفيذ أي سلطة منصوص عليها في هذه المادة وأي معلومات تتعلق بها. 4. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و 15. **القسم 25 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - جمع بيانات حركة الاتصالات** 1. إذا تأكد [قاض] بناء على [شهادة تحت القسم] [شهادة خطية] بأن هناك أسباباً معقولة لـ [الاشتباه] [الظن] بأن بيانات حركة الاتصالات المرتبطة ببلاغ محدد ضرورية بشكل معقول لأغراض [التحقيق] في تحقيق جنائي، [يجوز] [للقاضي] [يجب] أن يأمر شخصًا يتحكم بهذه البيانات بما يلي: • جمع أو تسجيل بيانات حركة الاتصالات المرتبطة باتصالات محددة خلال فترة محددة؛ أو • التصريح ومساعدة ضابط [الشرطة] [قوة تنفيذ القانون] محدد لجمع أو تسجيل تلك البيانات. 2. إذا تأكد [قاض] بناء على [شهادة تحت القسم] [شهادة خطية] بأن هناك أسباباً معقولة لـ [الاشتباه] [الظن] بأن بيانات حركة الاتصالات المرتبطة ببلاغ محدد ضرورية بشكل معقول لأغراض [التحقيق] في تحقيق جنائي، [يجوز] [للقاضي] [يجب] أن يسمح لـ [قوة تنفيذ القانون] [الشرطة] بجمع أو تسجيل بيانات حركة الاتصالات المرتبطة برسالة محددة خلال فترة محددة من خلال تطبيق الوسائل التقنية. 3. قد تقرر دولة عدم تنفيذ القسم 25.		**تحليل الفجوة** **التوصيات:** ينبغي توفير صلاحية محددة لجمع حركة البيانات في الوقت الفعلي، وينبغي إدراج حكم لإلزام مزودي خدمة الاتصالات في الأردن على التعاون لجمع حركة البيانات في الوقت الفعلي؛ ويجب إدراج ضمانات لضمان أن جمعها قانوني وضروري ومعقول ومتناسب مع الحالة. يمكن اعتماد اللغة من المادة 28 الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لكنها لا تشير إلى الجمع المستعجل في الوقت الحقيقي. يجب استخدام المادة 20 من اتفاقية بودابست والمادة 25 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية باعتبارهما دليلًا للتشريعات الوطنية

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
		واجب الكشف عن مفاتيح التشفير مع استخدام الإرهابيين والمجرمين المنظمين بشكل روتيني لتطبيقات الرسائل المشفرة[229] قد يعتبر الكشف عن مفاتيح التشفير قوة ملائمة لإطلاق مفاتيح كلمات المرور لفتح الأجهزة[230] **تحليل الفجوة** **التوصيات:** يتعذر توضيح ما إذا كانت هناك مثل هذه الصلاحيات في الأردن - سيسمح ذلك لوكالات إنفاذ القوانين بإجبار أصحاب الأجهزة على فتحها
		التزامات الاحتفاظ بالبيانات[231] تسمح مثل هذه السلطة لوكالات إنفاذ القانون ب 1. تتبع وتحديد مصدر الاتصال 2. تحديد وجهة الاتصال؛ 3. تحديد تاريخ ووقت ومدة الاتصال؛ و 4. تحديد نوع الاتصال 5. الأردن ليس لديه هذا النوع من الالتزام[232]

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 22 من اتفاقية بودابست **الاختصاص القضائي** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وغيرها من الإجراءات لإقامة ولاية قضائية على أي جرم منصوص عليه في المواد من 2 إلى 11 من هذه الاتفاقية، عندما تُرتكب الجريمة: a. في أراضيها؛ أو على متن سفينة ترفع علم تلك الدولة الطرف؛ أو على متن طائرة مسجلة بموجب قوانين ذلك الطرف؛ أو من قِبَل أحد رعاياها، إذا كانت الجريمة معاقبًا عليها بموجب القانون الجنائي حيث ارتكبت، أو إذا ارتكبت الجريمة خارج الولاية الإقليمية لأي دولة.	**لا يوجد معادل**	**التحليل القانوني** بدون وجود نطاق محدد بوضوح للجرائم الإلكترونية ، وهي دولية بطبيعتها سيبقى أي تشريع مقيدًا. **تحليل الفجوة** **التوصيات:** يضمن التشريع الوطني أن يتم تعريف الاختصاص باستخدام لغة المادة 22 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست، القسم 19 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية أو المادة 30 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. إذا كان هناك تعارض بين السلطات القضائية، فيجب أن تؤخذ في الاعتبار المبادئ التوجيهية المتعلقة بتحديد الولاية القضائية المناسبة لمحاكمة جريمة ما - انظر المبادئ التوجيهية Eurojust لتقرير الولاية القضائية التي في الجرائم التي تجب ملاحقتها (المراجعة 2016)[233]

229. Eleanor Saitta. “Can Encryption Save Us?” Nation 300, no. 24 (15 يونيو 2015): 16
81. Academic Search Premier, EBSCOhost ((تمت زيارته في 92 فبراير 6102.
230. انظر مثلاً القسم 49 من القانون الإنجليزي (Regulation of Investigatory Powers Act 2000 (UK) - http://www.legislation.gov.uk/ukpga/2000/23/section/49
231. في عام 2006، بموجب توجيه الاحتفاظ بالبيانات - اضطرت الدول الأعضاء في الاتحاد الأوروبي إلى تخزين بيانات الاتصالات الإلكترونية لمدة 6 أشهر على الأكثر للتحقيق في الجرائم الخطيرة وكشفها ومقاضاة مرتكبيها. أبطلت محكمة العدل الأوروبية في عام 2014 توجيه الاحتفاظ بالبيانات، حيث قررت أنها قدمت ضمانات غير كافية ضد التدخلات في الخصوصية وحماية البيانات. للاطلاع على المخططات الوطنية، انظر:
http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention
232. تقرير ICMEC العالمي، صفحة 29
233. http://www.eurojust.europa.eu/Practitioners/operational/Documents/Operational-Guidelines-for-Deciding.pdf

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
2. يجوز لكل طرف أن يحتفظ بالحق في عدم تطبيق أو تطبيق قواعد الاختصاص المنصوص عليها في الفقرات من 1 إلى 1 د من هذه المادة أو أي جزء منها فقط في حالات أو شروط محددة. 3. يعتمد كل طرف ما قد يلزم من إجراءات لإقامة ولاية قضائية على الجرائم المشار إليها في الفقرة 1 من المادة 24 من هذه الاتفاقية، في الحالات التي يكون فيها الجاني المفترض موجودا في إقليمه ولا يسلمه إلى بلد آخر بعد طلب التسليم على أساس جنسيته فقط. 4. لا تستبعد هذه الاتفاقية أي ولاية قضائية جنائية يمارسها أي طرف وفقًا لقانونه الداخلي. 5. عندما يطالب أكثر من طرف بالولاية القضائية على جريمة مفترضة تم النص عليها في هذه الاتفاقية، يتشاور الطرفان المعنيان، عند الضرورة من أجل تحديد الولاية القضائية الأنسب. **القسم 19من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الولاية القضائية** ينطبق هذا القانون على أي فعل أو تقصير: • في إقليم [الدولة المشترعة]؛ أو • على سفينة أو طائرة مسجلة في [الدولة المشترعة]؛ أو • من قبل أحد مواطني [الدولة المشترعة] خارج الولاية القضائية لأي بلد؛ أو من قبل أحد مواطني [الدولة المشترعة] خارج إقليم [الدولة المشترعة]، إذا كان سلوك هذا الشخص يشكل أيضًا جريمة بموجب قانون البلد الذي ارتكبت فيه الجريمة. **المادة 30 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - الاختصاص** 1. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد اختصاصها على أي من الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية وذلك إذا ارتكبت الجريمة كلياً أو جزئياً أو تحققت:		

التعاون الدولي		
أفضل الممارسات الدولية	**التشريع الوطني**	**ملاحظات**
a. في إقليم الدولة الطرف على متن سفينة تحمل علم الدولة الطرف. على متن طائرة مسجلة تحت قوانين الدولة الطرف. من قبل أحد مواطني الدولة الطرف إذا كانت الجريمة يعاقب عليها حسب القانون الداخلي في مكان ارتكبها أو إذ ارتكبت خارج منطقة الاختصاص القضائي لأية دولة. 2. إذا كانت الجريمة تمس أحد المصالح العليا للدولة. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد الاختصاص الذي يغطي الجرائم المنصوص عليها في الفقرة 1 من المادة 31 من هذه الاتفاقية في الحالات التي يكون فيها الجاني المزعوم حاضرا في إقليم تلك الدولة الطرف ولا يقوم بتسليمه إلى طرف آخر بناء على جنسيته بعد طلب التسليم. 3. إذا ادعت أكثر من دولة بالاختصاص القضائي لجريمة منصوص عليها في هذه الاتفاقية فيقدم طلب الدولة التي أخلت الجريمة بأمنها أو بمصالحها ثم الدولة التي وقعت الجريمة في إقليم ثم الدولة التي يكون الشخص المطلوب من رعاياها وإذا اتحدت الظروف فتقدم الدولة الأسبق في طلب التسليم. في حالة وجود ظروف مماثلة، تُعطى الأولوية لأول دولة تطلب التسليم.		
المادة 43 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست **الهيئات المتخصصة**[234] 1. تضمن كل دولة طرف، وفقا للمبادئ الأساسية لنظامها القانوني، وجود هيئة متخصصة مكرسة على مدار 24 ساعة في اليوم لضمان تقديم المساعدة العاجلة لأغراض التحقيق أو الإجراءات المتعلقة بجرائم تكنولوجيا المعلومات أو جمع الأدلة بشكل إلكتروني بشأن جريمة محددة. تتضمن هذه المساعدة تسهيل أو تنفيذ: a. تقديم المشورة الفنية. b. حماية المعلومات على أساس المادتين 37 و 38. c. جمع الأدلة وتقديم المعلومات القانونية وتحديد مكان المشتبه بهم.	**لا يوجد معادل**	**التحليل القانوني** **هذه آلية أساسية لتحقيق قدرة فعالة على التحقيق في الجرائم الإلكترونية.** **تحليل الفجوة** **التوصيات:** لا ينبغي أن يتطلب ذلك تشريعًا خاصًا لتنفيذه، وفيما يتعلق بالموارد يجب أن تُعطى الأولوية. يجب مشاركة تفاصيل الاتصال لنقطة الاتصال الوحيدة المعينة (SPOC) على المستوى الوطني ومع السلطات المركزية على المستوى الدولي والإنتربول. ينبغي أيضًا النظر في صياغة مذكرة تفاهم مع الوكالات الوطنية بحيث يكون لدى نقطة الاتصال الوحيدة المعينة سلطة القيام بالإجراءات المطلوبة كجزء من تحقيق دولي في جرائم الإنترنت وتطبيق القوانين والمعاهدات الوطنية. ستتضمن مذكرة التفاهم هذه الطلبات الواردة والصادرة وتضمن عملية فعالة وكفؤة.

234. المادة ٥٣ من اتفاقية بودابست

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
2. a. يجب أن تكون هذه الهيئة في جميع الدول الأطراف قادرة على التواصل الفوري مع الهيئة المقابلة في أي دولة طرف أخرى b. إذا كانت الهيئة المذكورة، المعينة من قبل دولة طرف، ليست جزءًا من السلطات المسؤولة عن المساعدة الثنائية الدولية في تلك الدولة، يجب أن تضمن تلك الهيئة قدرتها على التنسيق الفوري مع تلك السلطات. 3. تضمن كل دولة طرف توافر موارد بشرية قادرة على تيسير عمل الهيئة المذكورة أعلاه.		
المادة 25 من اتفاقية بودابست **المبادئ العامة المتعلقة بالمساعدة المتبادلة** 1. يقدم الطرفان المساعدة المتبادلة إلى أقصى حد ممكن لغرض إجراء التحقيقات أو الإجراءات المتعلقة بالجرائم الجنائية المتعلقة بأنظمة الحاسوب والبيانات، أو لجمع الأدلة المتعلقة بالجرائم الجنائية في شكل إلكتروني. 2. يعتمد كل طرف أيضًا الإجراءات التشريعية وغيرها من الإجراءات التي قد تكون ضرورية لتنفيذ الالتزامات المنصوص عليها في المواد من 27 إلى 35. 3. يجوز لكل طرف في الظروف العاجلة تقديم طلبات للمساعدة المتبادلة أو الاتصالات المتعلقة بها عن طريق وسائل الاتصال العاجلة، بما في ذلك الفاكس أو البريد الإلكتروني، إلى الحد الذي توفر فيه هذه الوسائل مستويات مناسبة من الأمن والمصادقة (بما في ذلك استخدام التشفير، عند الضرورة)، مع تأكيد رسمي لاحق، حيثما يطلب ذلك الطرف متلقي الطلب. يجب على الطرف متلقي الطلب قبول الطلب والرد عليه بأي وسيلة اتصال سريعة.		**التحليل القانوني** تضمن المادة 32 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات أنه يمكن استخدامها كأداة لتسهيل المساعدة القانونية المتبادلة وتنص على الحفظ المستعجل لبيانات الحاسوب المخزنة،[235] والحفظ المستعجل والكشف الجزئي لبيانات المرور،[236] والكشف عن البيانات المخزنة[237] وحركة البيانات[238] **لدول الاتفاقية.** **تحليل الفجوة** **التوصيات:** يُنصح بتشريع السلطات الإجرائية المنصوص عليها في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على المستوى الوطني، وبذلك يمكن استخدامها للتحقيقات المحلية وتؤسس لصلاحيات متبادلة لاستخدام الدول التي ليست طرفًا في الاتفاقية لا تنص الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على اعتراض المحتوى وحركة البيانات في الوقت الحقيقي؛ يجب اعتبار ما نصت عليه اتفاقية بودابست و اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية سوابق في هذا الاتجاه.[239] ينبغي النظر في السماح للسلطات المختصة بإعطاء الإذن لهيئات إنفاذ القانون المحلي بإجراء تحقيق في الدولة التي تأكد فيها الوصول إلى الجهاز. يعد الوصول إلى المعلومات هو المعيار الأساسي لبدء التحقيق في الحالات التي يتعذر فيها معرفة مكان تخزين البيانات (أي في التخزين السحابي). يمكن أن يشمل ذلك "اعترافًا متبادلًا" بأوامر المحكمة الصادرة تجاه مقدمي خدمات الاتصالات في دولة معينة، والتي يمكن تقديمها إلى فروع مقدمي خدمة العملاء الموجودين في دول أخرى، اعتمادًا على مكان تخزين البيانات.

235. المادة 29 من اتفاقية بودابست والمادة 37 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات
236. المادة 30 من اتفاقية بودابست والمادة 38 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات
237. المادة 31 من اتفاقية بودابست والمادة 39 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات
238. المادة 33 من اتفاقية بودابست والمادة 41 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات
239. المادتان 33 و 34 من اتفاقية بودابست، والقسمان 25 و 26 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
4. باستثناء ما هو منصوص عليه على وجه التحديد في المواد الواردة في هذا الفصل، تخضع المساعدة المتبادلة للشروط المنصوص عليها في قانون الطرف متلقي الطلب أو معاهدات المساعدة المتبادلة المطبقة، بما في ذلك الأسباب التي تُجيز للطرف متلقي الطلب أن يرفض التعاون. لا يجوز للطرف متلقي أن يبني حقه في رفض المساعدة المتبادلة المتعلقة بالجرائم المشار إليها في المواد من 2 إلى 11، فقط على أساس أن الطلب يتعلق بجريمة يعتبرها جريمة مالية. 5. عندما تسمح أحكام هذا الفصل للطرف متلقي الطلب بتقييد المساعدة المتبادلة بشرط ازدواجية التجريم، يعتبر هذا الشرط مستوفًيا، بصرف النظر عما إذا كانت قوانينه تضع الجريمة في نفس الفئة الجرمية، أو إذا أعطيت الجريمة نفس التسمية عند الطرف الطالب، وذلك إن كان السلوك الكامن وراء الجريمة التي طلبت المساعدة من أجلها جريمة جنائية بموجب قوانينه. **المادة 34 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - الإجراءات المتعلقة بطلبات التعاون والمساعدة المتبادلة** 1. تطبق أحكام الفقرات 2-9 من هذه المادة في حالة عدم وجود معاهدة أو اتفاقية تعاون ومساعدة متبادلة وفقًا للتشريعات المعمول بها بين الدول الأطراف التي تطلب المساعدة وتلك التي تُطلَب منها المساعدة. في حال وجوده جود معاهدة أو اتفاقية فلا تطبق الفقرات المشار إليها إلا إذا اتفقت الأطراف المعنية على تطبيقها كاملة أو بشكل جزئي . 2. a. على كل دولة طرف تحديد سلطة مركزية تكون مسؤولة عن إرسال وإجابة طلبات المساعدة المتبادلة وتنفيذ هذه الطلبات وإيصالها إلى السلطات المعنية لتنفيذها. على السلطات المركزية أن تتصل ببعضها مباشرة. على كل دولة طرف- وقت التوقيع أو إيداع أدوات التصديق أو القبول أو الموافقة- أن تتصل بالأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس العدل العرب وتنقل إليهما أسماء وعناوين السلطات المحددة خصيصا لغايات هذه الفقرة.		

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
3. تقوم الأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس وزراء العدل العرب بإنشاء وتحديث سجل للسلطات المركزية والمعينة من قبل الدول الأطراف. وعلى كل دولة طرف أن تتأكد من أن التفاصيل الموجودة في السجل صحيحة دائما 4. يتم تنفيذ طلبات المساعدة المتبادلة في هذه المادة وفقًا للإجراءات التي تحددها الدولة الطرف الطالبة، إلا في حالة عدم الامتثال لقانون الدولة الطرف متلقية طلب المساعدة. 5. يجوز للدولة الطرف المطلوب منها المساعدة أن تؤجل الإجراءات المتخذة بشأن الطلب إذا كانت هذه الإجراءات تؤثر على التحقيقات الجنائية التي تجري من قبل سلطاتها. 6. قبل رفض أو تأجيل المساعدة يجب على الدولة الطرف المطلوب منها المساعدة بعد استشارة الدولة الطرف الطالبة لها أن تقرر فيما إذ سيتم تلبية الطلب جزئيا أو يكون خاضعا للشروط التي قد ترها ضرورية. 7. تلتزم الدولة الطرف المطلوب منها المساعدة أن تُعلِم الدولة الطرف الطالبة لها بنتيجة تنفيذ الطلب. وإذا تم رفض أو تأجيل الطلب يجب إعطاء أسباب هذا الرفض أو التأجيل. ويجب على الدولة الطرف المطلوب منها المساعدة أن تعلم الدولة الطرف الطالبة لها بالأسباب التي تمنع تنفيذ الطلب بشكل نهائي أو الأسباب التي تؤخره بشكل كبير. 8. يجوز للدولة الطرف الطالبة للمساعدة أن تطلب من الطرف المطلوب منها المساعدة الإبقاء على سرية حقيقة ومضمون أي طلب يندرج في هذا الفصل ما عدا القدر لكافي لتنفيذ الطلب. وإذا لم تستطع الدولة الطرف المطلوب منها المساعدة الالتزام بهذا الطلب للسرية يجب عليها إعلام الدولة الطرف الطالبة والتي ستقرر مدى إمكانية تنفيذ الطلب. في الحالات العاجلة يجوز إرسال طلبات المساعدة المتبادلة مباشرة إلى السلطات القضائية في الدولة الطرف المطلوب منها المساعدة من نظيرتها في الدولة الطرف الطالبة لها. وفي مثل هذه الحالات يجب إرسال نسخة الوقت من السلطة المركزية في الدولة الطرف الطالبة إلى نظيرتها في الدولة الطرف المطلوب منها.		

التعاون الدولي		
أفضل الممارسات الدولية	**التشريع الوطني**	**ملاحظات**
يجوز عمل الاتصالات وتقديم الطلبات حسب هذه الفقرة بواسطة الإنتربول. حيثما يتم تقديم طلب حسب الفقرة أ ولم تكن السلطة مختصة بالتعامل مع الطلب فيجب عليها إحالة الطلب إلى السلطة المختصة وإعلام الدولة الطرف الطالبة للمساعدة مباشرة بذلك. إن الاتصالات والطلبات التي تتم حسب هذه الفقرة والتي لا تشمل الإجراء القسري يمكن بثها مباشرة من قبل السلطات المختصة في الدولة الطرف الطالبة للمساعدة إلى نظيرتها في الدولة الطرف المطلوب منها المساعدة. يجوز لكل دولة طرف، وقت التوقيع أو التصديق أو القبول أو الإقرار أو الانضمام إبلاغ الأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس وزراء العدل العرب بأن الطلبات حسب هذه الفقرة يجب توجيهها إلى السلطة المركزية لغايات الفعالية.		
المادة 26 من اتفاقية بودابست[240] **المعلومات التلقائية** 1. يجوز للطرف، في حدود قانونه الداخلي ودون طلب مسبق، أن يحيل إلى الطرف الآخر المعلومات التي تم الحصول عليها في إطار تحقيقاته، عندما يرى أن الكشف عن هذه المعلومات قد يساعد الطرف المتلقي في بدء أو التحقيقات أو الإجراءات المتعلقة بالجرائم الجنائية المنصوص عليها في هذه الاتفاقية، أو قد تؤدي إلى طلب تعاون من جانب هذا الطرف بموجب هذا الفصل. 2. قبل تقديم هذه المعلومات، يجوز للطرف المقدم أن يطلب الحفاظ على سريتها أو استخدامها فقط وفقًا للشروط. إذا لم يستطع الطرف المتلقي الامتثال لهذا الطلب، فيجب عليه إخطار الطرف المقدم الذي يحدد بعد ذلك ما إذا كان ينبغي تقديم المعلومات. إذا قبل الطرف المتلقي المعلومات وفقًا لهذه الشروط فعليه أن يلتزم بها.	**لا يوجد معادل**	**التحليل القانوني** يعد هذا إجراءً هامًا لتمكين الدولة من الاحتفاظ بمعلومات من شأنها أن تساعد دولة أخرى على منع جريمة الإنترنت أو التحقيق فيها. وعلى الرغم من أن ذلك متاحًا بين الدول التي صدقت على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الوارد ذكرهم في المادة 33 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، فليس للأردن أي أساس قانوني محلي يجبره بمشاركة هذه المعلومات مع الدول غير الموقعة على الاتفاقية ما لم يتم إرسال طلب رسمي عبر قنوات المساعدة القانونية المتبادلة المعتادة. تنص المادة 18 (4) - (5) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة على تبادل المعلومات الاستخباراتية تلقائيًا في الأمور التي تفي بتعريف جريمة خطيرة[241]، ذات طابع عبر وطني[242] وأن جماعة إجرامية منظمة ضالعة في ارتكاب الجرم[243]. دون استيفاء هذا التعريف، يجب إرسال طلب رسمي عبر قنوات المساعدة القانونية المتبادلة المعتادة إلى الدول التي ليست عضوًا في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. وبسبب الطبيعة السريعة الحركة للجريمة السيبرانية، فإن المشاركة التلقائية هي وسيلة فعالة للتعاون مع الدول الأخرى، وغياب هذه المشاركة يمنع التعاون الدولي الفعال مع الدول غير العضو في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

240. المادة 33 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

241. يقصد بتعبير «جريمة خطيرة» في المادة 2 (ب) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة أي سلوك يمثل جرما يعاقب عليه بالحرمان التام من الحرية لمدة لا تقل عن أربع سنوات أو بعقوبة أشد"

242. المادة 3 (1) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية

243. تُعرّف المادة 2 (أ) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة «الجماعة الإجرامية المنظمة» بأنها جماعة ذات هيكل تنظيمي، مؤلفة من ثلاثة أشخاص أو أكثر، موجودة لفترة من الزمن وتعمل بصورة متضافرة بهدف ارتكاب واحدة أو أكثر من الجرائم الخطيرة أو الأفعال المجرمة وفقا لهذه الاتفاقية، من أجل الحصول، بشكل مباشر أو غير مباشر، على منفعة مالية أو منفعة مادية أخرى"

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 33 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - المعلومات العرضية المتلقاة 1. يجوز لأي دولة طرف- ضمن حدود قانونها الداخلي- وبدون طلب مسبق أن تعطي لدولة أخرى معلومات حصلت عليها من خلال تحقيقاتها إذا اعتبرت أن كشف مثل هذه المعلومات يمكن أن تساعد الدولة الطرف المرسلة إليها في إجراء الشروع أو القيام بتحقيقات في الجرائم المنصوص عليها في هذه الاتفاقية أو قد تؤدي إلى طلب للتعاون من قبل تلك الدولة الطرف. 2. قبل إعطاء مثل هذه المعلومات يجوز للدولة الطرف المزودة أن تطلب الحفاظ على سرية المعلومات، وإذا لم تستطع الدولة الطرف المستقبلة الالتزام بهذا الطلب يجب عليها إبلاغ الدولة الطرف المزودة بذلك والتي تقرر بدورها مدى إمكانية التزويد بالمعلومات. وإذا قبلت الدولة الطرف المستقبلة المعلومات مشروطة بالسرية فيجب أن تبقى المعلومات بين الطرفين.		**تحليل الفجوة** **التوصيات:** استخدمت اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة المادة 18 (4) - (5) أساسًا لمشاركة المعلومات التي تدخل ضمن مجال هذه الاتفاقية بشكل تلقائي (مع ضمانات مقدمة حول الاستخدام في الأدلة أو الكشف عن المعلومات الحساسة لطرف ثالث (بما في ذلك دولة أخرى).[244] النظر في التشريعات القائمة على المادة 33 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات أو المادة 26 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست.
المادة 32 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست 1. يجوز للطرف، دون إذن من طرف آخر: a. الوصول إلى بيانات الحاسوب المخزنة (مفتوحة المصدر) المتاحة للجمهور، بغض النظر عن مكان وجود البيانات جغرافيا؛ أو الوصول إلى بيانات الكمبيوتر المخزنة الموجودة لدى طرف آخر أو استلامها، من خلال نظام حاسوب في إقليمها، إذا حصل الطرف على موافقة مشروعة وطوعية من الشخص الذي لديه السلطة القانونية للكشف عن البيانات للطرف من خلال نظام الحاسوب هذا.	**لا يوجد معادل**	**التحليل القانوني** تمكن هذه السلطة الإجرائية الدولة من تأمين المحتوى المخزن في دولة أخرى في ظروف محدودة. المادة 32 ب. إن اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست والمادة 40 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات هما استثناء من مبدأ الإقليمية وتسمحان بوصول منفرد عبر الحدود دون الحاجة إلى مساعدة قانونية متبادلة عندما تكون هناك موافقة أو تكون المعلومات متاحة للجمهور. أمثلة على استخدام هذه السلطة الإجرائية بموجب المادة 32 من اتفاقية بودابست تتضمن: قد يتم تخزين البريد الإلكتروني لشخص ما في بلد آخر بواسطة مزود خدمة، أو قد يقوم شخص ما بتخزين البيانات عن قصد في بلد آخر. يجوز لهؤلاء الأشخاص استرداد البيانات بشرط أن يكون لديهم السلطة القانونية التي تخولهم ذلك، ويجوز لهم الكشف طوعًا عن البيانات لموظفي إنفاذ القانون أو السماح لهؤلاء المسؤولين بالوصول إلى البيانات[245] يمكن اعتقال إرهابي مشتبه به بشكل قانوني عندما يكون بريده الإلكتروني، الذي قد يحوي دليلًا على ارتكاب جريمة، مفتوحًا على الجهاز اللوحي أو الهاتف الذكي أو أي جهاز آخر. إذا وافق المشتبه طوعًا على وصول الشرطة إلى الحساب وإذا كانت الشرطة متأكدة من وجود بيانات صندوق البريد في ولاية أخرى، يجوز للشرطة الوصول إلى البيانات بموجب المادة 32. ب.

244. انظر المادة 33 (2) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات
245. الفقرة 294، الصفحة 53 من التقرير الإيضاحي في اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
القسم 27 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية 1. إذا كان [القاضي] [قاضي التحقيق] مقتنعًا بناءً على [معلومات مقدمة تحت القَسَم] [شهادة خطية] أنه في سياق تحقيق متعلق بجريمة مدرجة في الفقرة 7 أدناه، توجد أسباب معقولة للاعتقاد بأنه لا يمكن جمع الأدلة الأساسية عن طريق تطبيق أحكام أخرى مدرجة في الجزء الرابع ولكنها ضرورية لأغراض التحقيق الجنائي، فإن [القاضي] [القاضي] [أن] يأذن لضابط [إنفاذ القانون] [الشرطة] بناءً على طلب باستخدام برنامج شرعي عن بعد في مهمة محددة ضرورية للتحقيق وتثبيته في نظام الحاسوب المشتبه به من أجل جمع الأدلة ذات الصلة. يجب أن يحتوي الطلب على المعلومات التالية: • المشتبه في ارتكابه الجريمة، إذا كان ذلك ممكنا مع الاسم والعنوان؛ و • وصف نظام الحاسوب المستهدف؛ و • وصف الوسيلة المقصود ومدى ومدة الاستخدام؛ و • أسباب ضرورة الاستخدام. 2. من الضروري التأكد في مثل هذا التحقيق من أن التعديلات التي يتم إدخالها على نظام الحاسوب الخاص بالمشتبه به مقصورة على تلك الضرورية للتحقيق وأن أي تغييرات يمكن التراجع عنها إذا أمكن بعد نهاية التحقيق. أثناء التحقيق، من الضروري تسجيل الدخول • الوسيلة الفنية المستخدمة ووقت وتاريخ التطبيق؛ و • تحديد نظام الحاسوب وتفاصيل التعديلات التي تمت خلال التحقيق؛ • أي معلومات تم الحصول عليها. يجب حماية المعلومات التي يتم الحصول عليها عن طريق استخدام هذا البرنامج من أي تعديل أو حذف غير مصرح به أو وصول غير مصرح به.		**تحليل الفجوة** **التوصيات:** تم تضمين هذه السلطة التي تؤمن الأدلة من طرف واحد في التشريعات مع ضمانات الحصول على الموافقة بشكل قانوني من المستخدم.[246] يمكن استخدام لغة المادة 32 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست والمادة 40 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. تم انتقاد المادة 32.ب بشدة، ويمكن اعتبار أن موافقة الدولة حيث تُخزَّن بيانات الكمبيوتر قد تم الحصول عليها بالإضافة إلى المستخدم. ينص القسم 27 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية على البرامج الشرعية وهذا قد يسمح بالوصول إلى جهاز حاسوب في دولة أخرى. هناك عدد من القيود التي تشترط عدم إمكانية الحصول على الأدلة بوسائل أخرى، وتتطلب أمرًا قضائيًا، ويمكن أن تُطبَّق على جرائم معينة فقط ضمن مدة مقيدة (3 أشهر). يجب أيضًا إيلاء الاعتبار لموافقة الدولة الأخرى التي قد يتطفل عليها البرنامج الشرعي.

246. يجب الانتباه لمواقف مثل عدم وجود المستخدم (في حالة الوفاة) وإذا كان يمكن الحصول على موافقة في دولة أخرى

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
3. تقتصر مدة الترخيص في القسم 27 (1) على [3 أشهر]. يتم إيقاف الإجراء المتخذ على الفور إذا لم تعد شروط الترخيص مستوفاة. 4. يتضمن ترخيص تثبيت البرنامج الوصول عن بُعد إلى نظام الحاسوب المشتبه به. 5. إذا كانت عملية التثبيت تتطلب الوصول الفعلي إلى مكان ما، يجب استيفاء متطلبات القسم 20. 6. يجوز لضابط [تطبيق القانون] [الشرطة] أن يطلب من المحكمة أن تأمر مقدم خدمة بالمساعدة في عملية التسليم إذا لزم الأمر، وذلك بموجب أمر المحكمة الممنوح في (1) الطلب المذكور أعلاه. 7. قائمة الجرائم]. 8. قد تقرر دولة عدم تنفيذ القسم 27. **المادة 40 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - الوصول إلى معلومات تقنية المعلومات عبر الحدود** يجوز لأي دولة طرف، وبدون الحصول على تفويض من دولة طرف أخرى: 1. أن تصل إلى معلومات تقنية المعلومات المتوفرة للعامة (مصدر مفتوح) بغض النظر عن الموقع الجغرافي للمعلومات. 2. أن تصل أو تستقبل- من خلال تقنية المعلومات في إقليمها- معلومات تقنية المعلومات الموجودة لدى الدولة الطرف الأخرى وذلك إذا كانت حاصلة على الموافقة الطوعية والقانونية من الشخص الذي يملك السلطة القانونية لكشف المعلومات إلى تلك الدولة الطرف بواسطة تقنية المعلومات المذكورة.		

لبنان

أقرّ لبنان في 10 أكتوبر 2018 القانون رقم 18 المتعلق بالمعاملات الإلكترونية والبيانات ذات الطابع الشخصي، وقد أصبح القانون ساريًا في يناير 2019. يعمل فريق يورميد للعدالة على أن تكون المعلومات محدّثة وصحيحة؛ غير أنه ورغم أننا بذلنا أقصى جهدنا، وبسبب القيود التي يفرضها وقت المشروع الحالي وموارده، فإن تحليل أحكام 2018 القانونية الجديدة سيكون ممكنًا في المرحلة التالية.

الجرائم

أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 2 من اتفاقية بودابست - الوصول غير المشروع يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لتجريم الوصول إلى النظام الكلي أو أي جزء من نظام الكمبيوتر، إذا ارتكب عمدًا، دون أي حق. قد يشترط طرف ما ارتكاب الجريمة عن طريق انتهاك إجراءات أمنية بقصد الحصول على بيانات الكمبيوتر أو نية أخرى غير نزيهة، أو فيما يتعلق بنظام كمبيوتر متصل بنظام كمبيوتر آخر. **المادة 6 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - جريمة الدخول غير المشروع** 1. الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به. 2. تشدد العقوبة إذا ترتب على هذا الدخول أو البقاء أو الاتصال أو الاستمرار بهذا الاتصال: • محو أو تعديل أو تشويه أو نسخ أو نقل أو محو للبيانات المحفوظة وللأجهزة والأنظمة الالكترونية وشبكات الاتصال وإلحاق الضرر بالمستخدمين والمستفيدين. الحصول على معلومات حكومية سرية. **القسم 4 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الوصول غير القانوني** 1. يعاقب بالسجن لمدة لا تتجاوز [المدة] أو غرامة لا تتجاوز [المبلغ] أو بالعقوبتين معاً أي شخص يدان بجريمة الوصول إلى نظام حاسوب كله أو جزء منه عن قصد ودون عذر مبرر قانونًا أو بتجاوز لسبب قانوني.	**لا يوجد معادل**	**التحليل القانوني** تشير الاتفاقية العربية لمكافحة جرائم تقنية المعلومات إلى «الوصول غير المشروع أو التواجد أو الاتصال بـ" دون تحديد معنى هذه الأفعال. تشير اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست إلى «بغير حق" في المادة 2 على أساس أن الوصول غير مصرح به. أكد التقرير التفسيري لاتفاقية بودابست اشتقاق عبارة "بدون حق" مثل، "التصرف الذي تم دون سلطة (سواء كانت تشريعية أو تنفيذية أو إدارية أو قضائية أو تعاقدية أو توافقية) أو تصرفًا لا يشمله، بأي حال، الدفوع القانونية أو الأعذار أو المبررات أو المبادئ ذات الصلة بموجب القانون المحلي." تقدم أقسام التعليق في التشريع النموذجي[247] لاتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية، شرحًا لشرط "بدون عذر أو مبرر قانوني" على النحو التالي، «تمكن ملاحقة الوصول إلى نظام الحاسوب وفقًا للمادة 4 فقط، وفي حالة حدوث ذلك «دون عذر أو مبرر قانوني». ويتطلب ذلك أن يتصرف الجاني دون سلطة (سواء كانت تشريعية أو تنفيذية أو إدارية أو قضائية أو تعاقدية أو توافقية) وأن الدفوع القانونية أو الأعذار أو المبررات أو المبادئ ذات الصلة لا تبرر تصرفه. إن الوصول إلى نظام يسمح بالوصول المجاني والمفتوح للجمهور أو الوصول إلى نظام بإذن من المالك أو غيره من أصحاب الحقوق لا يعتبر بالتالي جريمة. لا يرتكب مسؤولو الشبكات وشركات الأمان الذين يختبرون حماية أنظمة الحاسوب من أجل تحديد الثغرات المحتملة في التدابير الأمنية عملاً إجرامياً". تشير اتفاقية الجامعة العربية لمكافحة جرائم تكنولوجيا المعلومات إلى «الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به." دون تحديد ماهية هذه الأفعال، يستحسن لذلك استخدام تعريفات اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست ومواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية.

247. صفحة 30 قسم الشرح في اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية، النموذج التشريعي

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
2. قد تقرر أي دولة عدم تجريم الوصول غير المصرح به بشرط توفر سبل انتصاف فعالة أخرى. علاوة على ذلك، قد يشترط بلد ما ارتكاب الجريمة عن طريق انتهاك الإجراءات الأمنية أو بقصد الحصول على بيانات الحاسوب أو بنية أخرى غير نزيهة. **القسم 5 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الآثار غير القانونية** 1. أي يشخص يظل مسجلاً في نظام حاسوب أو جزء من نظام حاسوب أو يواصل استخدام نظام حاسوب عن قصد ودون عذر أو مبرر قانوني، أو يتجاوز عذرًا أو مبررًا قانونيًا يعاقب عند إدانته بالسجن لمدة لا تتجاوز [المدة]، أو غرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً. 2. قد تقرر أي دولة عدم تجريم الآثار غير المصرح بها فقط، شرط أن تتوفر سبل انتصاف فعالة أخرى. بدلاً من ذلك، قد يشترط البلد ارتكاب الجرم عن طريق انتهاك الإجراءات الأمنية أو بقصد الحصول على بيانات الحاسوب أو بنية أخرى غير نزيهة.		**تحليل الفجوة** **التوصيات:** يمكن أن يتضمن التشريع الوطني الصياغة ذات الصلة من المادة 2 في اتفاقية بودابست / القسمان 4 و5 من مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية لتشمل تعاريف نظام الحاسوب[248] وإدراج البرامج ضمن تعريف البيانات لأن بعض البيانات تشمل البرامج والبعض الآخر لا تشملها. علاوة على ذلك، ولكي تتماشى التشريعات مع المعايير الدولية، ينبغي أن يشير التشريع إلى الوصول «بغير حق" بدلاً من عن طريق الاحتيال. يجب أيضًا الأخذ بعين الاعتبار النص على جريمة منفصلة تشكلها الآثار الباقية في نظام الحاسوب وفقًا للمادة 5 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية.
المادة 3 من اتفاقية بودابست **الاعتراض غير القانوني** يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وتدابير أخرى لتجريم اعتراض عمليات نقل البيانات الحاسوبية غير العامة من نظام حاسوب وإليه وداخله، بما في ذلك الانبعاثات الكهرومغناطيسية من نظام الحاسوب الذي يحمل مثل هذه البيانات، وذلك عند ارتكاب هذا العمل عمدًا بوسائط تقنية، ويعتبر جريمة جنائية بموجب القانون الداخلي. قد يشترط الطرف أن تكون الجريمة قد ارتكبت بنية غير نزيهة، أو أن تتم ضد نظام حاسوب متصل بنظام حاسوب آخر.	**لا يوجد معادل**	**التحليل القانوني** يُعتبر تجريم هذا الفعل ضروريًا لمقاضاة عمليات نقل بيانات الحاسوب من وإلى وداخل نظام الحاسوب الذي قد يتم اعتراضه بشكل غير قانوني للحصول على معلومات (مثل wikileaks أو PanamaPapers). **تحليل الفجوة** **التوصيات:** استخدم صياغة اتفاقية بودابست في المادة 3 والقسم 6 من مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية باعتبارهما دليلاً للتشريعات الوطنية - الصياغة المستخدمة في المادة 7 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات مناسبة، وإن لم يكن هناك تعريف لـ «بيانات تكنولوجيا المعلومات"

248. انظر المادة 1.أ. من اتفاقية بودابست: «يعني نظام الحاسوب أي جهاز أو مجموعة من الأجهزة المترابطة أو ذات الصلة، أو واحدًا أو أكثر من هذه الأجهزة يقوم بمعالجة البيانات تلقائيًا أو تسجيلها وفقا لأحد البرامج" **أو** القسم 3 (5) من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية: «جهاز أو مجموعة من الأجهزة المترابطة أو ذات الصلة، بما في ذلك الإنترنت، يقوم واحد منها أو أكثر بمعالجة تلقائية للبيانات أو بأداء أي وظيفة أخرى وفقًا لأحد البرامج".

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
القسم 6 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الاعتراض غير القانوني 1. الشخص الذي يتعمد اعتراض الوسائل التقنية دون عذر أو مبرر قانوني أو يتجاوز عذرًا أو مبررًا قانونيًا: • أي نقل غير عام إلى نظام الحاسوب أو منه أو داخله؛ أو • الانبعاثات الكهرومغناطيسية من نظام الحاسوب يعتبر جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً. 2. قد يشترط البلد ارتكاب الجرم بنية غير شريفة، أو ضد نظام حاسوب متصل بنظام حاسوب آخر أو عن طريق التحايل على إجراءات الحماية المطبقة لمنع الوصول إلى محتوى الإرسال غير العام. **المادة 7 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست** **الاعتراض غير القانوني** الاعتراض غير القانوني المتعمد لحركة البيانات بأي وسيلة تقنية، وتعطيل نقل أو استقبال بيانات تكنولوجيا المعلومات.		
المادة 4 من اتفاقية بودابست **التشويش على البيانات** يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لكي تجرم قوانينها الوطنية محو بيانات الحاسوب أو إتلافها أو تغييرها أو حذفها دون حق، وذلك عند ارتكابها عمدًا. يجوز لأي طرف الاحتفاظ بالحق في المطالبة بأن السلوك الموصوف في الفقرة 1 يؤدي إلى ضرر جسيم. **القسم 7 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية- التشويش غير القانوني على البيانات** الشخص الذي يقوم بأي من الأفعال التالية عمدا ودون عذر أو مبرر قانوني أو يتجاوز عذرًا أو مبررًا قانونيًا: • محو أو إتلاف بيانات الحاسوب؛ أو • محو أو إتلاف بيانات الحاسوب؛ أو	**لا يوجد معادل**	**التحليل القانوني** على النحو الوارد أعلاه، وفيما يتعلق بالوصول غير المشروع، لا توجد إشارة في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات إلى «بغير حق" ولا تشمل حذف بيانات الحاسوب التي تعد عنصرا من عناصر التصيد الاحتيالي للحصول على وصول غير قانوني عن طريق تثبيت مسجل أساسي للحصول على معلومات حساسة.[249] **تحليل الفجوة** **التوصيات:** يمكن تصحيح نقص بعض العناصر الرئيسة المتعلقة بهذه الجريمة في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات باستخدام لغة المادة 4 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست أو القسم 7 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية.

249. http://www.coe.int/en/web/cybercrime/guidance-notes

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
• xتغيير بيانات الحاسوب؛ أو • جعل بيانات الحاسوب بلا معنى لها أو غير ذات فائدة أو غير فعالة؛ أو • يعوق أو يقاطع أو يشوش على الاستخدام القانوني لبيانات الحاسوب؛ أو • يعوق أو يقاطع أو يشوش على أي شخص في استخدامه القانوني لبيانات الحاسوب؛ أو • يمنع الوصول إلى بيانات الكمبيوتر لأي شخص مصرح له بالوصول إليها؛ يعتبر جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً. **المادة 8 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست** **الجريمة ضد سلامة البيانات** 1. تعمد محو أو حذف أو منع أو تعديل أو إخفاء بيانات تكنولوجيا المعلومات بشكل غير قانوني. 2. قد يطلب أحد الأطراف أن يتسبب الفعل بأضرار جسيمة من أجل تجريم الأفعال المذكورة في الفقرة 1.		
المادة 5 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[250] **التشويش على النظام** يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لكي تُجرّم في قانونها الداخلي أعمال الإعاقة الخطيرة التي ترتكب عمدًا ودون وجه حق من أجل إعاقة عمل نظام حاسوب من خلال إدخال بيانات حاسوب أو نقلها أو محوها أو حذفها أو إتلافها أو تغييرها أو منعها. **القسم 9 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - التشويش غير القانوني على النظام** 1. الشخص الذي يقوم عن قصد، ودون عذر أو مبرر قانوني، أو بتجاوز عذر أو مبرر قانوني: • أعاقة عمل نظام الحاسوب أو التشويش عليه؛ أو • إعاقة شخص يستخدم أو يشغل بشكل قانوني نظام الحاسوب أو التشويش عليه؛	**لا يوجد معادل**	**التحليل القانوني** تجريم هذه الأعمال من شأنه أن يمنع البرامج الضارة التي تتداخل مع عمل جهاز الحاسوب - على سبيل المثال ديدان الكمبيوتر - مجموعة فرعية من البرامج الضارة (مثل فيروسات الكمبيوتر). إنها برامج حاسوب ذاتية النسخ المتماثل تضر بالشبكة من خلال بدء عمليات نقل البيانات المتعددة. يمكن أن تؤثر على أنظمة الحاسوب عن طريق إعاقة التشغيل السلس لنظام الحاسوب، أو استخدام موارد النظام لتكرار نفسها عبر الإنترنت أو توليد حركة مرور في الشبكة يمكن أن تغلق بعض الخدمات (مثل المواقع الإلكترونية). **تحليل الفجوة** **التوصيات:** استخدم لغة اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست في المادة 5 أو القسم 9 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية باعتبارهما دليلًا للتشريعات الوطنية. ضع في اعتبارك أيضًا ما إذا كان منع ومكافحة الهجمات ضد البنية التحتية الحيوية يحتاج إلى جريمة منفصلة أو مشددة (القسم 9 (2) من بروتوكول مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية)، على سبيل المثال، قد يتم إعاقة عمل نظام الكمبيوتر لأغراض إرهابية (يمكن أن تؤدي إعاقة النظام الذي يخزن سجلات البورصة إلى أن تكون البيانات غير دقيقة، أو أن تعيق عمل البنية التحتية الحيوية).[251]

250. لا يوجد ما يعادلها في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات
251. http://www.coe.int/en/web/cybercrime/guidance-notes

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
2. يعتبر جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً. يعاقب أي شخص الذي يتعمد دون عذر أو مبرر قانوني، أو بتجاوز عذر قانوني أو مبرر، إعاقة نظام حاسوب مخصص حصريًا لاستخدام عمليات البنية التحتية الحيوية أو التشويش عليه، أو في الحالات التي لا يكون فيها هذا النظام مخصصًا للاستخدام الحصري في عمليات البنية التحتية الحيوية، ولكنه يستخدم في عمليات البنية التحتية الحيوية وتؤثر هذه الإعاقة على استخدام عمليات البنية التحتية الحيوية، بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً.		
المادة 6 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[252] **سوء استخدام الأجهزة** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لتجريم الأفعال الإجرامية بموجب قوانينه الداخلي، عندما تُرتكب عمداً ودون حق: a. إنتاج أو بيع أو الشراء بغرض الاستخدام أو الاستيراد أو التوزيع أو توفير ما يلي بأية طريقة: i. أي جهاز، بما في ذلك برنامج الحاسوب، تم تصميمه أو تكييفه بشكل أساسي بغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من 2 إلى 5؛ ii. كلمة مرور الحاسوب أو رمز الوصول أو البيانات المماثلة التي يمكن من خلالها الوصول إلى نظام الحاسوب كله أو جزء منه، بقصد استخدامه لغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من 2 إلى 5؛ و	**لا يوجد معادل**	**التحليل القانوني** كما ذكر أعلاه للوصول غير المشروع، لا توجد إشارة إلى «بدون حق" ستمكّن تجريم هذه الأفعال من ملاحقة إنتاج وبيع والشراء من أجل الاستخدام واستيراد وتوزيع رموز الوصول والبيانات المحوسبة الأخرى المستخدمة في ارتكاب جرائم الإنترنت. فمثلًا يمكن الوصول إلى أنظمة الحاسوب لتسهيل أي هجوم إرهابي بالتدخل في شبكة الطاقة الكهربائية للبلد. يجب أن تأخذ أي جريمة في الاعتبار تلك الأجهزة التي لها استخدام شرعي وكذلك للاستخدام الجنائي («الاستخدام المزدوج") – ينبغي أن يشمل ذلك اللغة المستخدمة في اتفاقية بودابست «المكيف بشكل أساسي" **تحليل الفجوة** **التوصيات:** استخدام صياغة اتفاقية بودابست في المادة 6 أو القسم 10 من مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية باعتبارهما دليلاً للتشريعات الوطنية. يرجى ملاحظة أن مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية توفر خيار إدراج الأجهزة في جدول إذا كان ذلك مناسبًا - قد يكون هذا تقييدًا ويتطلب تحديثًا يتوافق مع التقدم التكنولوجي. يجب أن يوفر القانون الوطني عذرًا معقولًا حتى تتمكن أجهزة إنفاذ القانون من استخدام الأجهزة لتقنيات التحقيق الخاصة - راجع اللغة في المادة 6.2. اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست أو القسم 10 (2) من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية باعتبارهما دليلًا.

252. المادة 9 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
2. حيازة أي بند مذكور في الفقرتين أ. 1 أو 2 أعلاه، بقصد استخدامه لغايات ارتكاب أي من الجرائم المذكورة في المادة 2 إلى المادة 5. يجوز لأي طرف أن يشترط بموجب القانون امتلاك عدد من هذه العناصر قبل إسناد المسؤولية الجنائية. لا يجوز تفسير هذه المادة على أنها تفرض مسؤولية جنائية عندما لا يكون الغرض من الإنتاج أو البيع أو الشراء بغرض الاستخدام أو الاستيراد أو التوزيع أو التوفير أو حيازة المشار إليه في الفقرة 1 من هذه المادة ارتكاب جريمة منصوص عليها وفقًا للشروط المواد من 2 إلى 5 من هذه الاتفاقية، مثل الاختبارات المسموح بها أو حماية نظام الكمبيوتر. 3. يجوز لكل طرف أن يحتفظ بالحق في عدم تطبيق الفقرة 1 من هذه المادة، شريطة أن لا يتعلق التحفظ ببيع أو توزيع أو توفير المواد المشار إليها في الفقرة 1 أ من هذه المادة بطريقة أخرى **القسم 10 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الأجهزة غير القانونية** 1. يرتكب الشخص جريمة إذا: a. أنتج أو باع أو اشترى بغرض الاستخدام أو استورد أو صدّر أو وزع أو وفّر بأي طريقة، عن قصد ودون عذر أو مبرر قانوني أو بتجاوز عذر أو مبرر قانوني: i. جهاز بما في ذلك برنامج حاسوب، تم تصميمه أو تكييفه بغرض ارتكاب جريمة محددة بموجب أحكام أخرى من الجزء الثاني من هذا القانون؛ أو ii. كلمة مرور الحاسوب أو رمز الوصول أو البيانات المماثلة التي يمكن من خلالها الوصول إلى نظام الحاسوب كله أو جزء منه بقصد استخدامه من قبل أي شخص لغرض ارتكاب جريمة محددة بموجب أحكام أخرى من الجزء الثاني من هذا القانون؛ أو		

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
كان في حوزته غرض مشار إليه في الفقرة الفرعية «1» أو «2»، وكان القصد هو استخدامه من قبل أي شخص لارتكاب جريمة محددة بموجب أحكام أخرى من الجزء الثاني من هذا القانون، فإنه يعاقب عند إدانته بارتكاب هذه الجريمة بالسجن لمدة لا تزيد عن [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً. 2. لا يجوز تفسير هذا الحكم على أنه يفرض مسؤولية جنائية عندما لا يكون الغرض من الإنتاج أو البيع أو الشراء للاستخدام أو الاستيراد أو التوزيع أو التوفير أو الحيازة المشار إليها في الفقرة 1 هو ارتكاب جريمة منصوص عليها وفقًا لأحكام أخرى من الجزء الثاني من هذا القانون، كأن تكون الأغراض مثل الاختبار أو الحماية المعتمدين لنظام الكمبيوتر. 3. قد يقرر بلد ما عدم تجريم الأجهزة غير القانونية أو قصر التجريم على الأجهزة المدرجة في الجدول.		
المادة 7 من اتفاقية بودابست **أعمال التزوير المرتبطة بالحاسوب** يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم إدخال بيانات الحاسوب أو تغييرها أو حذفها أو محوها، عند ارتكاب ذلك عن قصد وبدون حق، مما يؤدي إلى بيانات غير موثوقة بهدف أن يتم التعامل معها أو التصرف فيها لأغراض قانونية كما لو كانت أصلية، بصرف النظر عما إذا كانت البيانات قابلة للقراءة ومقروءة مباشرة أم لا. قد يطلب طرف ما وجود نية الاحتيال، أو نية غير شريفة مماثلة، قبل إسناد المسؤولية الجنائية. **المادة 10 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست** **جريمة التزوير** يعني استخدام تقنية المعلومات تغيير حقيقة البيانات بطريقة تسبب الضرر بغرض استخدامها كبيانات حقيقية.	**لا يوجد معادل**	**التحليل القانوني** تتم مقاضاة مرتكب أي جريمة تزوير كجريمة جوهرية فقط - الغرض من المادة 7 من اتفاقية بودابست هو سد الفجوات الموجودة في القانون الجنائي المتعلق بالتزوير التقليدي، الأمر الذي يتطلب قراءة مرئية للبيانات، أو الإعلانات المتضمنة في مستند والتي لا تنطبق على البيانات المخزنة إلكترونيًا. ويتضمن التزوير المرتبط بالحاسوب إنشاء البيانات المخزنة أو تغييرها بشكل غير مصرح به للحصول على قيمة ثبوتية مختلفة في سياق المعاملات القانونية، التي تعتمد على صحة المعلومات الواردة في البيانات، وتخضع للخداع. وتكمن المصلحة القانونية المحمية في أمان وموثوقية البيانات الإلكترونية التي قد يكون لها عواقب على العلاقات القانونية.[253] يُنصح بتضمين المادة 7 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست أو القسم 11 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية من أجل الحماية من المخالفات التي قد تشمل التصيد الاحتيالي والتصيد الاحتيالي بالرمح على سبيل المثال، قد يتم إدخال بيانات الحاسوب(مثل البيانات المستخدمة في جوازات السفر الإلكترونية) أو تغييرها أو حذفها أو إلغاؤها، مما يؤدي إلى تصديق البيانات غير الموثوقة أو التعامل معها لأغراض قانونية كما لو كانت صحيحة.[254]

253. الفقرة ١٨، الصفحة ٤١ التقرير التوضيحي لاتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية
254. http://www.coe.int/en/web/cybercrime/guidance-notes

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
القسم 11 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - أعمال التزوير المتعلقة بالحاسوب 1. كل شخص يقوم عن قصد ودون عذر أو مبرر قانوني أو بتجاوز عذر قانوني أو مبرر، بإدخال أو تبديل أو حذف أو منع بيانات الحاسوب، مما ينتج عنه بيانات غير موثوقة بقصد التعامل معها أو التصرف فيها لأغراض قانونية كما لو كانت صحيحة، بصرف النظر عما إذا كانت البيانات قابلة للقراءة مباشرة أم لا، يعاقب عند الإدانة بهذه الأعمال بالسجن لمدة لا تزيد عن [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً. 2. تكون العقوبة إذا ارتكبت الجريمة المذكورة أعلاه عن طريق إرسال رسائل بريد إلكتروني متعددة من أنظمة الحاسوب أو من خلالها هي السجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً.		ينص القسم 11 (2) من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية أيضًا على إرسال رسائل بريد إلكتروني متعددة باعتبارها جريمة مشددة. لا تشير اللغة في المادة 10 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات إلى أي نية غير شريفة وتشترط التسبب في ضرر - اللغة المستخدمة في اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست و مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية هي الأفضل لأنها لا تشترط حدوث ضرر. تشترط اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست ومواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية فقط أن "البيانات الزائفة" "تعتبر" حقيقية **تحليل الفجوة** **التوصيات:** استخدام صياغة اتفاقية بودابست في المادة 7 أو القسم 11 من مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية باعتبارهما دليلاً للتشريعات الوطنية
المادة 8 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[255] **الاحتيال المرتبط بالحاسوب** يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وتدابير أخرى لتجريم الأفعال التالية بموجب قوانينه الداخلية، عند ارتكابها عمداً ودون حق، بما يسبب فقدان الممتلكات لشخص آخر عن طريق: أي إدخال أو تغيير أو حذف أو إلغاء لبيانات الحاسوب، أي تدخل في عمل نظام الحاسوب، مع نية احتيال أو نية غير شريفة من أجل الحصول، دون حق، على منفعة اقتصادية لنفسه أو لشخص آخر. **القسم 12 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الاحتيال المرتبط بالحاسوب** الشخص الذي يتسبب في فقدان الممتلكات لشخص آخر، عن قصد، ودون عذر أو مبرر قانوني أو بتجاوز عذر أو مبرر قانوني، وذلك عن طريق: • أي إدخال أو تغيير أو حذف أو إلغاء لبيانات الحاسوب؛ • أي تدخل في عمل نظام الحاسوب،	**لا يوجد معادل**	**التحليل القانوني** تتم مقاضاة مرتكب أي جريمة احتيال كجريمة موضوعية. يتكون الاحتيال المرتبط بالحاسوب بشكل أساسي من عمليات التلاعب في المدخلات، حيث يتم إدخال البيانات غير الصحيحة في الحاسوب، أو عن طريق التلاعب بالبرنامج والتداخلات الأخرى أثناء معالجة البيانات. الهدف من المادة 8 من اتفاقية بودابست هو تجريم أي تلاعب لا لزوم له في سياق معالجة البيانات بقصد التأثير على النقل غير المشروع للممتلكات.[256] الصياغة في المادة 11 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات غامضة مع عدم وجود إشارة إلى أي نية غير شريفة وتتطلب وقوع شكل من أشكال «الضرر" (الاتفاقية العربية لمكافحة جرائم تقنية المعلومات) دون تعريف ماهيته **تحليل الفجوة** **التوصيات:** اللغة المتعلقة بهذه الجريمة في اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست أو اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية لهذه الجريمة هي دليل جيد للتشريع الوطني

255. المادة 11 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات
256. الفقرة 86، الصفحتان 14 و15 من التقرير التفسيري لاتفاقية بودابست

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
بقصد احتيالي أو غير شريف للحصول، دون حق، على منفعة اقتصادية لنفسه أو لشخص آخر، وتكون عقوبة هذه الأعمال السجن لمدة لا تتجاوز [المدة] ، أو غرامة لا تتجاوز [المبلغ]، أو العقوبتين معاً.		
المادة 9 من اتفاقية بودابست **الجرائم ذات الصلة بالمحتوى (مثل المواد الإباحية للأطفال)** 1. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم السلوك التالي في قوانينه المحلية، عندما يرتكب عمدا وبدون حق: a. إنتاج مواد إباحية للأطفال بغرض توزيعها من خلال نظام حاسوب؛ عرض أو إتاحة مواد إباحية للأطفال من خلال نظام الحاسوب؛ توزيع أو نقل المواد الإباحية للأطفال من خلال نظام الحاسوب؛ شراء مواد إباحية للأطفال من خلال نظام حاسوب بقصد الاستخدام الشخصي أو لإعطائها لشخص آخر؛ امتلاك مواد إباحية للأطفال في نظام حاسوب أو على وسائط تخزين بيانات الحاسوب. 2. لأغراض الفقرة 1 أعلاه، يجب أن يشمل مصطلح «استغلال الأطفال في المواد الإباحية» أية مواد إباحية تصور بصريًا: a. قاصر مشترك في سلوك جنسي صريح؛ شخص يبدو أنه قاصر يشارك في سلوك جنسي صريح؛ صور واقعية تمثل قاصرًا مشاركًا في سلوك جنسي صريح. 3. لأغراض الفقرة 2 أعلاه، يشمل مصطلح «القاصر» جميع الأشخاص الذين تقل أعمارهم عن 18 عامًا. ومع ذلك، يجوز لأي طرف أن يطلب حدًا أدنى للسن، لا يقل عن 16 عامًا. 4. يجوز لكل طرف أن يحتفظ بالحق في عدم تطبيق الفقرات الفرعية 1 ، د. و هـ ، و2، الفقرتين الفرعيتين ب. و ج كليًا أو جزئيًا. **القسم 13 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية- المواد الإباحية للأطفال** 1. الشخص الذي يقوم عن قصد ودون عذر أو مبرر قانوني ب:	**لا يوجد معادل**	**التحليل القانوني** تجريم هذه الأعمال يعتبر أساسيًا من أجل حماية الأطفال من الأذى، وذلك من خلال تجريم توزيع الصور غير اللائقة للأطفال ونقلها وتوفيرها وعرضها وحيازتها. **تحليل الفجوة** **التوصيات:** إن صياغة المادة 9 من اتفاقية بودابست أو القسم 13 من مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية عبارة عن دليل للتشريعات الوطنية لحماية الأطفال ومقاضاة الجناة

الجرائم		
أفضل الممارسات الدولية	**التشريع الوطني**	**ملاحظات**
• إنتاج مواد إباحية للأطفال بغرض توزيعها من خلال نظام حاسوب؛ • تقدم أو توفر مواد إباحية للأطفال من خلال نظام حاسوب؛ • توزيع أو نقل المواد الإباحية عن الأطفال من خلال نظام حاسوب؛ • شراء و/أو الحصول على مواد إباحية للأطفال من خلال نظام حاسوب لاستخدامه الشخصي أو لإعطائها لشخص آخر؛ • حيازة مواد إباحية للأطفال في نظام حاسوب أو على وسائط تخزين بيانات الحاسوب؛ أو • الوصول عمدًا، من خلال تكنولوجيا المعلومات والاتصالات، إلى المواد الإباحية عن الأطفال، ، يعتبر جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً. 2. يمكن الدفاع أمام تهمة بجريمة منصوص عليها في الفقرة (1) (ب) إلى (1) (و) إذا أثبت الشخص أن المواد الإباحية عن الأطفال كانت بغرض إنفاذ القانون بحسن نية. 3. لا يجوز لدولة ما أن تجرم السلوك الموصوف في القسم 13 (1) (د) - (و).		
المادة 10 من اتفاقية بودابست **انتهاك حقوق النشر** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وغيرها من التدابير لاعتبار انتهاك حقوق الطبع والنشر، جرائم جنائية بموجب قوانينه الداخلية، وفقًا للالتزامات التي تعهد بها بموجب قانون باريس الصادر في 24 يوليو 1971، مراجعة اتفاقية برن لحماية المصنفات الأدبية والفنية، والاتفاق المتعلق بجوانب حقوق الملكية الفكرية المتصلة بالتجارة ومعاهدة المنظمة العالمية للملكية الفكرية بشأن حق المؤلف، باستثناء أي حقوق معنوية ممنوحة بموجب هذه الاتفاقيات، عندما تُرتكب هذه الانتهاكات عمدا وعلى نطاق تجاري وعن طريق نظام الحاسوب.	**لا يوجد معادل**	**التحليل القانوني** تستخدم هيئات تطبيق القانون على الصعيد الدولي جرائم حقوق النشر الرقمية باعتبارها سلوكًا إجراميًا إضافيًا للتحقيق في العديد من أشكال جرائم الإنترنت ومحاكمة مرتكبيها (بما في ذلك جرائم مثل التصيّد الاحتيالي والاحتيال الإلكتروني والتزوير الإلكتروني ومواقع الويب الاحتيالية وانتهاكات البيانات وسرقتها). تميل إحدى هذه الجرائم الأساسية في العديد من الحالات إلى أن تكون انتهاكًا لحقوق النشر الرقمية. إن الهجوم السيبراني على سوني[257] ليس إلا مثالًا حديث العهد تضافرت فيه المنظمات الإجرامية والقوى المرتبطة بجرائم الإنترنت وسرقة البيانات / التجسس على الشركات وانتهاك حقوق الطبع والنشر لتكمل عمل بعضها البعض. إن عدم وجود أي أحكام تتعلق بالملكية الفكرية يشكل إخفاقًا في حماية الابتكار في القرن الحادي والعشرين لدول الجنوب الشريكة والشركات والمواطنين. قد تكون هذه الحقوق محمية في تشريعات أخرى لم تتم مراجعتها كجزء من هذا التحليل **تحليل الفجوة** **التوصيات:** يجب التأكد من وجود حماية ضد انتهاك حقوق النشر التي تتوافق مع الالتزامات الدولية.	

257. https://en.wikipedia.org/wiki/Sony_Pictures_hack

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
2. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لاعتبار أي انتهاك للحقوق أدناه جرائم جنائية بموجب قوانينه الداخلية، وذلك عملاً بالالتزامات التي تعهد بها بموجب الاتفاقية الدولية لحماية فناني الأداء ومنتجي التسجيلات الصوتية وهيئات الإذاعة (اتفاقية روما) واتفاق جوانب حقوق الملكية الفكرية المتصلة بالتجارة ومعاهدة المنظمة العالمية للملكية الفكرية بشأن الأداء والتسجيل الصوتي، باستثناء أي حقوق معنوية ممنوحة بموجب هذه الاتفاقيات، حيثما ارتكبت هذه الانتهاكات عمدا وعلى نطاق تجاري وعن طريق نظام الحاسوب. 3. يجوز لأي طرف أن يحتفظ بالحق في عدم فرض مسؤولية جنائية بموجب الفقرتين 1 و 2 من هذه المادة في ظروف محدودة، شريطة توفر سبل انتصاف فعالة أخرى، وأن لا ينتقص هذا التحفظ من التزامات الطرف الدولية المنصوص عليها في المواثيق الدولية المشار إليها في الفقرتين 1 و 2 من هذه المادة. **المادة 17 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - الجرائم المتعلقة بحق المؤلف والحقوق المرتبطة بها** انتهاك حقوق النشر كما هو محدد وفقًا لقانون الدولة الطرف، إذا كان الفعل قد ارتكب عمداً وليس لغرض الاستخدام الشخصي، وانتهاك الحقوق المرتبطة بحقوق الطبع والنشر ذات الصلة على النحو المحدد وفقًا لقانون الدولة الطرف، إذا كان الفعل ارتكب عمدا وليس لهدف الاستخدام الشخصي.		
المادة 11 من اتفاقية بودابست **المساعدة والتحريض** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لتجريم الأفعال التالية بموجب قانونه الداخلي، وذلك عندما يتم التحريض على ارتكاب أي من الجرائم المقررة وفقا للمواد من 2 إلى 10 من هذه الاتفاقية أو المساعدة عليها عمدًا، مع نية أن ترتكب هذه الجريمة. 2. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وتدابير أخرى لتجريم محاولة ارتكاب أي من الأفعال الإجرامية المنصوص عليها في المواد من 3 إلى 5 و7 و8 و9.1. أ و ج من هذه الاتفاقية عمدًا.	**لا يوجد معادل**	**التحليل القانوني** تعتبر مساعدة الآخرين وتحريضهم على ارتكاب جرائم أمرًا ضروريًا لمحاكمة أولئك الذين يكونون قد قدموا المساعدة أو شجعوا على ارتكاب جرائم الإنترنت. تنص المادة 19 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على الشروع أيضًا **تحليل الفجوة** **التوصيات:** استخدم المادة 11 من اتفاقية بودابست والمادة 19 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات باعتبارهما دليلاً للتشريعات الوطنية

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 19 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - محاولة ارتكاب الجرائم والاشتراك فيها 1. الاشتراك في ارتكاب أية جريمة من الجرائم المنصوص عليها في هذا الفصل مع وجود نية ارتكاب الجريمة في قانون الدولة الطرف. 2. الشروع في ارتكاب الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية. 3. يجوز لأي دولة طرف الاحتفاظ بحقها في عدم تطبيق الفقرة الثانية من هذه المادة كليا أو جزئيا.		
المادة 12 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[258] **مسؤولية الشركات** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وتدابير أخرى لضمان أن الأشخاص الاعتباريين يمكن اعتبارهم مسؤولين عن أي جريمة جنائية منشأة وفقًا لهذه الاتفاقية، إذا ارتكبها أي شخص طبيعي لصالحهم، سواء كان ذلك بصفته الفردية أو باعتباره جزءًا من جهاز الشخص الاعتباري، أو باعتباره شخصًا قياديًا ضمن تنظيم الشخص الاعتباري، بناءً على: a. سلطة تمثيل الشخص الاعتباري؛ سلطة اتخاذ القرارات نيابة عن الشخص الاعتباري؛ سلطة ممارسة السيطرة داخل الشخص الاعتباري. 2. بالإضافة إلى الحالات المنصوص عليها بالفعل في الفقرة 1 من هذه المادة، يتخذ كل طرف الإجراءات اللازمة لضمان أن يتحمل الشخص الاعتباري المسؤولية عندما يكون عدم الإشراف أو السيطرة من قبل أي شخص طبيعي مشار إليه في الفقرة 1 قد جعل من الممكن ارتكاب جريمة جنائية منصوص عليها بموجب هذه الاتفاقية لصالح ذلك الشخص الاعتباري من قبل شخص طبيعي يعمل تحت سلطته. 3. مع مراعاة المبادئ القانونية للطرف، قد تكون مسؤولية الشخص الاعتباري جنائية أو مدنية أو إدارية. 4. تكون هذه المسؤولية دون المساس بالمسؤولية الجنائية للأشخاص الطبيعيين الذين ارتكبوا الجريمة.	**لا يوجد معادل**	**التحليل القانوني** هذا الحكم هو عنصر أساسي بحيث يستطيع الأشخاص الاعتباريون (مثلًا الكيانات التجارية) التصرف نيابة عن الأشخاص الطبيعيين الذين تقع عليهم مسؤولية جنائية **تحليل الفجوة** **التوصيات:** استخدم لغة اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست في المادة 12 باعتبارها دليلًا للتشريعات الوطنية

258. المادة ١٠ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
البروتوكول الإضافي لاتفاقية الجريمة السيبرانية، المتعلق بتجريم أعمال العنصرية وكراهية الأجانب المرتكبة من خلال أنظمة الحاسوب **المادة 3[259] - نشر المواد التي تحض على العنصرية وكراهية الأجانب من خلال أنظمة الحاسوب** 1. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال الجنائية بموجب قوانينه الداخلية، عند ارتكابها عمدًا ودون حق، كسلوك جنائي: توزيع المواد بدافع العنصرية وكراهية الأجانب أو إتاحتها للجمهور من خلال نظام الحاسوب. 2. يجوز لأي طرف أن يحتفظ بالحق في عدم إسناد المسؤولية الجنائية للسلوك على النحو المحدد في يجوز للطرف أن يحتفظ بالحق في عدم إسناد المسؤولية الجنائية بالتصرف على النحو المحدد في الفقرة 1 من هذه المادة، عندما تحض المواد الموزعة، كما هو محدد في الفقرة 1 من المادة 2، وتشجع على التمييز غير المرتبط بالكراهية أو العنف، شريطة أن تتوفر سبل انتصاف فعالة أخرى. 3. بصرف النظر عن الفقرة 2 من هذه المادة، يجوز للطرف أن يحتفظ بالحق في عدم تطبيق الفقرة 1 على حالات التمييز، لأن هذه الفقرة لا يمكن أن تمثل سبل انتصاف فعالة على النحو المشار إليه الفقرة 2، وذلك بسبب مبادئ ثابتة في نظامه القانوني الوطني متعلقة بحرية التعبير.	**لا يوجد معادل**	**تحليل الفجوة** **التوصيات:** استخدم لغة اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست في المادة 3 من البروتوكول الإضافي كدليل للتشريعات الوطنية
بروتوكول إضافي **المادة 4[260] - التهديد بدافع العنصرية وكراهية الأجانب** يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم السلوك التالي في قوانينه المحلية، عندما يرتكب عمدا وبدون حق: التهديد، من خلال نظام الحاسوب، بارتكاب جريمة جنائية خطيرة على النحو المحدد في قانونها الداخلي، (1) ضد أشخاص لسبب أنهم ينتمون إلى جماعة يميزها عرقها أو لونها أو نسبها أو أصلها القومي أو العرقي أو دينها، إذا تم استخدام أي من هذه العوامل ذريعةً، أو (2) ضد مجموعة من الأشخاص تتميز بأي من هذه الخصائص.	**لا يوجد معادل**	**تحليل الفجوة** **التوصيات:** استخدم لغة اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست في المادة 4 من البروتوكول الإضافي كدليل للتشريعات الوطنية

259. لا يوجد ما يعادلها في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات
260. لا يوجد ما يعادلها في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
بروتوكول إضافي **المادة 5[261] - الإهانة بدافع العنصرية وكراهية الأجانب** يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم السلوك التالي في قوانينه المحلية، عندما يرتكب عمدا وبدون حق: إهانة الجمهور، من خلال نظام حاسوبي، (1) الأشخاص لكونهم ينتمون إلى مجموعة يميزها عرقها أو لونها أو نسبها أو أصلها القومي أو العرقي أو دينها، إذا تم استخدام أي من هذه العوامل ذريعةً؛ أو (2) مجموعة من الأشخاص تتميز بأي من هذه الخصائص. يجوز للطرف إما: أن يشترط أن يكون للجريمة المشار إليها في الفقرة 1 من هذه المادة أثر على أن الشخص أو مجموعة الأشخاص المشار إليهم في الفقرة 1 والذين يتعرضون للكراهية أو الاحتقار أو السخرية؛ أو أن يحتفظ بالحق في عدم تطبيق الفقرة 1 من هذه المادة بشكل كلي أو جزئي.	**لا يوجد معادل**	**تحليل الفجوة** **التوصيات:** استخدم لغة اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست في المادة 5 من البروتوكول الإضافي كدليل للتشريعات الوطنية

261. لا يوجد ما يعادلها في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
بروتوكول إضافي **المادة 6[262] - الإنكار أو التقليل إلى الحد الأدنى أو الموافقة أو التبرير للإبادة الجماعية أو الجرائم ضد الإنسانية** يعتمد كل طرف ما قد يلزم من إجراءات تشريعية لجعل الأفعال التالية يعتبر جرائم جنائية بموجب قوانينها الداخلية، عندما تُرتكب عمداً وبدون حق: توزيع أو توفير عبر نظام الحاسوب بأية طريقة من الطرق للجمهور، مواد تنكر أو تقلل أو تقر أو تقلل بشكل كبير الأفعال التي تشكل إبادة جماعية أو جرائم ضد الإنسانية، على النحو المحدد في القانون الدولي والمعترف بها على هذا النحو في القرارات النهائية والملزمة للمحكمة العسكرية الدولية، المنشأة بموجب اتفاقية لندن المؤرخة في 8 أغسطس 1945، أو أي محكمة دولية أخرى تنشأ بموجب المواثيق الدولية ذات الصلة والتي يعترف هذا الطرف باختصاصها القضائي. يجوز للطرف كذلك أ- أن يشترط أن يكون الإنكار أو التقليل إلى الحد الأدنى المشار إليه في الفقرة 1 من هذه المادة قد ارتكب بهدف التحريض على الكراهية أو التمييز أو العنف ضد أي فرد أو مجموعة من الأفراد على أساس العرق أو اللون أو النسب أو الأصل القومي أو العرقي أو الدين أو إذا استخدمت هذه العوامل ذريعة لذلك، أو أن يحتفظ بالحق في عدم تطبيق الفقرة 1 من هذه المادة بشكل كلي أو جزئي.	**لا يوجد معادل**	**تحليل الفجوة** **التوصيات:** استخدم لغة اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست في المادة 6 من البروتوكول الإضافي كدليل للتشريعات الوطنية
جرائم إضافية للمراجعة		
الجرائم المتعلقة بالهوية **القسم 14 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية** يعاقب الشخص الذي يقوم عن قصد ودون عذر أو مبرر قانوني، أو يتجاوز عذرًا قانونيًا أو مبررًا باستخدام نظام حاسوب في أي مرحلة من مراحل الجريمة بنقل أو تملك أو استخدام وسيلة لتحديد الهوية شخص آخر بنية ارتكاب أي نشاط غير قانوني يشكل جريمة أو المساعدة أو التحريض عليها، عند إدانته بهذه الأعمال بالسجن لمدة لا تتجاوز [المدة] أو بغرامة لا يتجاوز [المبلغ]، أو بالعقوبتين معاً.		**التحليل القانوني** تغطي هذه الجريمة مرحلة التحضير لجريمة خيانة الأمانة المتعلقة بالهوية **تحليل الفجوة** **التوصيات:** يستحسن أن تدرج في التشريعات المحلية.

262. لا يوجد ما يعادلها في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
الكشف عن تفاصيل التحقيق **القسم 16 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية** موفر خدمة الإنترنت الذي يتلقى أمرًا يتعلق بتحقيق جنائي ينص صراحةً على الحفاظ على السرية أو على التزام شبيه ينص عليه القانون، ثم يقوم عن عمد ودون عذر أو مبرر قانوني أو بتجاوز لعذر قانوني مبرر، بالإفصاح عن: • حقيقة أنه قد تم إصدار أمر؛ أو • أي شيء تم تنفيذه بموجب الأمر؛ أو • أي بيانات تم جمعها أو تسجيلها بموجب الطلب؛ يعتبر جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً.		**التحليل القانوني** يعاقب على اختراق البيانات والكشف عن المعلومات الحساسة التي يمكن أن تؤثر على التحقيقات الجنائية **تحليل الفجوة** **التوصيات:** يستحسن أن تدرج في التشريعات المحلية.
عدم السماح بالمساعدة **القسم 17 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية** 1. أي شخص آخر غير المشتبه فيه فشل عمداً دون عذر أو مبرر قانوني أو بتجاوز عذر أو مبرر قانوني، بمساعدة شخص أو السماح بمساعدته، بناءً على أمر مثلما تحدد المواد 20 إلى 22[263] يرتكب جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة] ، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً. 2. قد يقرر أي بلد عدم تجريم عدم السماح بالمساعدة شرط أن تتوفر سبل انتصاف فعالة أخرى.		**التحليل القانوني** تتعلق هذه الجريمة بالأشخاص الذين لديهم معرفة محددة بالأدلة ذات الصلة والذين يرفضون تقديم المساعدة. غالبًا ما يعتمد تطبيق القانون على هؤلاء الأشخاص لتأمين الأدلة في التحقيقات الإلكترونية. هنالك مخالفة مستقلة وهي عدم توفير كلمات مرور أو الوصول إلى الرموز للأجهزة المشفرة أو البيانات (مثل «مفتاح المعلومات المحمية") - ينص القسم 53 من قانون تنظيم سلطات التحقيق في المملكة المتحدة لعام 2000 (RIPA) [264] على وجود جرم جنائي يتحمله الأشخاص الذين لا يمتثلون للمادة 49 من إخطار RIPA والقاضية بالكشف عن «المفتاح" **تحليل الفجوة** **التوصيات:** يستحسن أن تدرج في التشريعات المحلية.
المطاردة السيبرانية **القسم 18 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية** الشخص الذي يقوم، دون عذر أو مبرر قانوني، أو يتجاوز عذرًا قانونيًا أو مبررًا، ببدء أي اتصال إلكتروني، بقصد إكراه شخص ما أو تخويفه أو مضايقته أو التسبب في ضائقة عاطفية كبيرة له، باستخدام نظام حاسوب لدعم السلوك المتكرر والعدائي والعنيف، يرتكب جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً.		**التحليل القانوني** هذه الجريمة تُجرم من يضايقون الأشخاص عبر الإنترنت - قد تنص بعض الولايات القضائية على جرائم تحرش غير مرتبطة بالحاسوب - لكن يوصى باعتماد هذه الجريمة لمتابعة لتلك الجرائم المرتكبة عبر الإنترنت. **تحليل الفجوة** **التوصيات:** يستحسن أن تدرج في التشريعات المحلية.

263. أوامر البحث والاستيلاء والمساعدة والإنتاج
264. http://www.legislation.gov.uk/ukpga/2000/23/section/53

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
استدراج الأطفال على الإنترنت **القانون الجنائي الهولندي** 248e يعاقب الشخص الذي يقترح ترتيب لقاء، بوسائل عمل آلية أو باستخدام خدمة اتصال، مع شخص يعرف، أو ينبغي منطقيًا أن يعرف، أن هذا الشخص لم يصل بعد إلى سن السادسة عشرة، مع نية ارتكاب أفعال غير لائقة مع هذا الشخص أو لعمل صور عن عمل جنسي يشارك فيه هذا الشخص، بالسجن لمدة لا تقل عن سنتين أو بغرامة من الفئة الرابعة، إذا ارتكب أي عمل يقصد به تحقيق اللقاء. **قانون العقوبات الكندي** **القسم** 172.1 1. يرتكب جريمة كل شخص يتواصل عن طريق وسائل الاتصالات مع شخص يكون عمره أقل من 18 عامًا، أو يظن المتهم أن عمره أقل من 18 عامًا، بغرض تسهيل ارتكاب جريمة مرتبطة بهذا الشخص، وذلك بموجب المادة الفرعية 153 (1) ، المادة 155، 163.1 ، 170 أو 171 أو القسم الفرعي 212 (1) أو (2) أو (2.1) أو (4)؛ شخص يكون عمره أقل من 16 عامًا، أو يظن المتهم أن عمره أقل من 16 عامًا، بغرض تسهيل ارتكاب جريمة مرتبطة بهذا الشخص، وذلك بموجب المواد 151 أو 152، أو الفقرة الفرعية 160(3) أو 173(2) أو الأقسام 271 أو 272 أو 273 أو 280؛ أو شخص يكون عمره أقل من 14 عامًا، أو يظن المتهم أن عمره أقل من 14 عامًا، بغرض تسهيل ارتكاب جريمة مرتبطة بهذا الشخص بموجب المادة 281. عقاب يعتبر كل شخص يرتكب جريمة بموجب الفقرة الفرعية (1) مذنبًا بارتكاب جريمة ويكون عرضة لعقوبة السجن لمدة تتراوح بين 10 سنوات كحد أقصى وسنة واحدة كحد أدنى؛ أو مذنبًا بارتكاب جريمة يعاقب عليها في ملخص الإدانة بالسجن لمدة تتراوح بين 18 شهرًا كحد أقصى و 90 يومًا كحد أدنى. افتراض إعادة تقدير العمر		**التحليل القانوني** لإثبات الجرم الهولندي، يلزم عقد لقاء لأغراض جنسية مع تقديم أدلة إثبات مأخوذة من تاريخ الدردشة عبر الإنترنت تفصح عن قصد جنسي؛ طلب عقد اللقاء مع الأدلة على أنه تم التخطيط لذلك (أي التاريخ والمكان). الغرض من القانون الكندي هو منع استدراج الكبار المفترسين للأطفال عبر الإنترنت. لا تتطلب هذه الجريمة حدوث جريمة جنسية. وهذا يعني أن المتهم لا يحتاج إلى الذهاب فعلاً لمقابلة الضحية شخصيًا. تكتمل الجريمة قبل اتخاذ أي إجراءات لارتكاب الجريمة الموضوعية. **تحليل الفجوة** **التوصيات:** يُنصح بإدراجها في التشريعات المحلية لتجريم هذا السلوك التحضيري قبل ارتكاب جريمة جنسية

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
2. الأدلة على أن الشخص المشار إليه في الفقرة (1) (أ) أو (ب) أو (ج) قُدِّم للمتهم وعمره أقل من ثمانية عشر عامًا أو ستة عشر عامًا أو أربعة عشر عامًا، حسب الحالة، في حالة عدم وجود أدلة تثبت عكس ذلك تثبت أن المتهم يعتقد أن الشخص كان أقل من تلك السن. لا دفاع 3. لا يقبل دفاع المتهم أمام التهم الموجهة بموجب الفقرة (1) (أ) أو (ب) أو (ج) بأنه كان يعتقد أن الشخص المشار إليه في تلك الفقرة لا يقل عمره عن ثمانية عشر عامًا أو ستة عشر عامًا أو أربعة عشر عامًا، حسب الحالة، إلا في حالة اتخذ المتهم خطوات معقولة للتأكد من عمر الشخص.		

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 19 من اتفاقية بودابست **التفتيش والضبط** **بيانات الكمبيوتر المخزنة** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لتمكين سلطاته المختصة من البحث في أو الوصول إلى: a. نظام الحاسوب أو جزء منه وبيانات الحاسوب المخزنة فيه؛ و b. وسيلة تخزين بيانات الحاسوب، حيث يمكن تخزين بيانات الحاسوب في أراضيها. 2. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وغيرها من الإجراءات لضمان تستطيع سلطاته عند تفتيشها نظام حاسوب معينًا أو جزءًا منه أو الوصول إليه بطريقة مماثلة، وذلك وفقًا للفقرة 1. أ، ويكون لدها أسباب للاعتقاد بأن البيانات المطلوبة مخزنة في نظام حاسوب آخر أو أن جزءًا منها موجود في إقليمها، وهذه البيانات يمكن الوصول إليها قانونيًا من النظام الأولي أو متاحة لها، فإنها قادرة على توسيع نطاق البحث أو الوصول المشابه للنظام الآخر على وجه السرعة.	**لا يوجد معادل**	**التحليل القانوني** هذه هي قوة التحقيق الأكثر أهمية ويجب أن تشير إلى الحصول على حق الوصول وليس البحث. في «التقرير التوضيحي لاتفاقية بودابست، يعني «البحث" التفتيش عن البيانات أو قراءتها أو فحصها أو مراجعتها. ويشمل ذلك مفهوم البحث عن البيانات والبحث عن (فحص) البيانات. لكلمة "الوصول" معنى محايد وتعكس بدقة أكثر المصطلحات الحاسوبية؛ يتم استخدامها كذلك في المادتين 26 و 27 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.[265] **تحليل الفجوة** **التوصيات:** يمكن أن يقتبس التشريع الوطني الصياغة المناسبة من اتفاقية بودابست ومواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية وذلك لإدراج تعريفات لنظام الحاسوب[266] وبيانات الحاسوب[267] يجب أن يكون هناك تعريف «للحجز" لضمان النزاهة ولتحديد الإجراءات - القسم 3 (16) من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية

265. الفقرة 191، الصفحة 33 التقرير التوضيحي لاتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية
266. انظر المادة 1.أ. من اتفاقية بودابست: «يعني نظام الحاسوب أي جهاز أو مجموعة من الأجهزة المترابطة أو ذات الصلة، أو واحدًا أو أكثر من هذه الأجهزة يقوم بمعالجة البيانات تلقائيًا أو تسجيلها وفقا لأحد البرامج" **أو** القسم 3 (5) من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية: «جهاز أو مجموعة من الأجهزة المترابطة أو ذات الصلة، بما في ذلك الإنترنت، يقوم واحد منها أو أكثر بمعالجة تلقائية للبيانات أو بأداء أي وظيفة أخرى وفقًا لأحد البرامج".
267. انظر المادة 1.ب. من اتفاقية بودابست: «أي تمثيل للوقائع أو المعلومات أو المفاهيم في نموذج مناسب للمعالجة في نظام حاسوب، بما في ذلك البرامج المناسبة لأن يقوم نظام حاسوب بأداء وظيفة ما"، **أو** القسم 3 (6) من مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية: تتضمن بيانات الحاسوب أي تمثيل للوقائع أو المعلومات أو المفاهيم (سواء أكانت نصوصًا أو أصواتًا أو صورًا) أو رموز آلة مقروءة أو تعليمات، في نموذج مناسب للمعالجة في نظام الحاسوب، بما في ذلك البرامج المناسبة لأن يقوم نظام الحاسوب بأداء وظيفة ما".

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
3. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وغيرها من الإجراءات لتمكين سلطاته المختصة من مصادرة أو تأمين بيانات الحاسوب التي تم الوصول إليها وفقًا للفقرات 1 أو 2. تشمل هذه التدابير القدرة على: a. الاستيلاء على نظام حاسوب أو جزء منه أو وسيلة تخزين بيانات الحاسوب، والقيام بما يلزم لتأمينه؛ إنشاء نسخة من بيانات الحاسوب هذه والاحتفاظ بها؛ الحفاظ على سلامة بيانات الحاسوب المخزنة ذات الصلة؛ أن يجعل الوصول إلى بيانات الحاسوب في نظام الحاسوب الذي تم الوصول إليه غير ممكن أو أن يحذفها. 4. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لتمكين سلطاته المختصة من أن تأمر أي شخص لديه معرفة بعمل نظام الحاسوب أو التدابير المطبقة لحماية البيانات الموجودة فيه بتوفير ما يلزم من المعلومات بما يكفل تنفيذ الإجراءات المشار إليها في الفقرتين 1 و 2. 5. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و 15. **القسم 20 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - البحث والضبط** 1. إذا اقتنع [القاضي] بناء على [معلومات تحت القَسَم] [شهادة خطية] أن هناك أسبابًا معقولة [للاشتباه] [للاعتقاد] أنه قد يكون هناك في مكان ما شيء أو بيانات حاسوب: • قد تكون مادية كدليل في إثبات الجريمة؛ أو • قد اكتسبها شخص نتيجة لجريمة؛ [يجوز] [يأمر] يصدر [القاضي] تفويضًا لضابط [إنفاذ القانون] [الشرطة]، ويزوده بما قد يلزم من مساعدة، لدخول المكان للبحث عن الشيء أو بيانات الحاسوب وضبطها، وعمل ما يلزم بما في ذلك البحث أو عمليات الوصول الشبيهة: – نظام الحاسوب أو جزء منه وبيانات الحاسوب المخزنة فيه؛ و		”يشمل الحجز: • تشغيل أي نظام حاسوب في الموقع ووسائط تخزين بيانات الحاسوب؛ • إنشاء نسخة من بيانات الحاسوب والاحتفاظ بها، بما في ذلك عن طريق استخدام معدات في الموقع؛ • الحفاظ على سلامة بيانات الحاسوب المخزنة ذات الصلة؛ • أن يجعل الوصول غير ممكن إلى بيانات الحاسوب في نظام الحاسوب الذي تم الوصول إليه أو أن يحذفها؛ • أخذ نسخة مطبوعة من بيانات غير ممكن؛ أو حجز نظام حاسوب أو جزء منه أو وسيلة تخزين بيانات الحاسوب، والقيام بما يلزم لتأمينه» تنص المادة 21 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية على التشريع لضمان تقديم المساعدة من قبل أولئك الذين لديهم معرفة متخصصة بموقع الأدلة ذات الصلة - يمكن استخدام هذا كدليل - انظر أيضًا القسم 17 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية، المتعلق بالجريمة في حال تم رفض المساعدة دون عذر قانوني

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
– وسيلة تخزين بيانات الحاسوب، حيث يمكن تخزين بيانات الحاسوب في إقليم البلد. 2. إذا كان[قوة إنفاذ القانون] [الشرطة] الذي يجري عملية بحث على أساس القسم 20 (1) أسباب للاعتقاد بأن البيانات المطلوبة مخزنة في نظام حاسوب آخر أو جزء منه في إقليمها، وأن هذه البيانات يمكن الوصول إليها قانونيًا أو يمكن أن تكون متاحة من النظام الأولي، فيجب أن يكون قادرًا على توسيع نطاق البحث أو الوصول إلى النظام الآخر بطريقة مماثلة. 3. يتم تمكين ضابط [تطبيق القانون] [الشرطة] الذي يقوم بالبحث من مصادرة أو تأمين بيانات الحاسوب المماثلة التي يتم الوصول إليها وفقًا للفقرات 1 أو 2. **القسم 21 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - المساعدة** يجب على أي شخص لا يشتبه في ارتكابه جريمة ولكن لديه علم بسير عمل نظام الحاسوب أو التدابير المطبقة لحماية بيانات الحاسوب الواردة فيه والتي تخضع لعملية بحث بموجب المادة 20، أن يسمح وأن يساعد إذا لزم الأمر وطلب منه الشخص المسؤول أن يجري البحث عن طريق: • توفير المعلومات التي تمكن من اتخاذ التدابير المشار إليها في المادة 20؛ • الوصول إلى نظام حاسوب أو وسيط تخزين بيانات الحاسوب واستخدامه للبحث في أي بيانات حاسوب متاحة أو في النظام؛ • الحصول على ونسخ بيانات حاسوب هذه؛ • استخدام المعدات لعمل نسخ؛ و • الحصول على معلومات واضحة من نظام حاسوب بشكل مقبول في الإجراءات القانونية. **المادة 26 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - فحص المعلومات المخزنة** 1. تلتزم كل دولة طرف يتبنى الإجراءات الضرورية لتمكين سلطاتها المختصة من التفتيش أو الوصول إلى:		

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
تقنية معلومات أو جزء منها والمعلومات المخزنة فيها أو المخزنة عليها. بيئة أو وسيط تخزين معلومات تقنية معلومات والذي قد تكون معلومات التقنية مخزنة فيه أو عليه. 2. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من التفتيش أو الوصول إلى تقنية معلومات معينة أو جزء منها بما يتوافق مع الفقرة (-1 أ) إذا كان هناك اعتقاد بأن المعلومات المطلوبة مخزنة في تقنية معلومات أخرى أو جزء منها في إقليمها وكانت هذه المعلومات قابلة للوصول قانونا أو متوفرة في التقنية الأولى فيجوز توسيع نطاق التفتيش والوصول للتقنية الأخرى. **المادة 27 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - ضبط المعلومات المخزنة** 1. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من ضبط وتأمين معلومات تقنية المعلومات التي يتم الوصول إليها حسب الفقرة 1 من المادة 26 من هذه الاتفاقية. هذه الإجراءات تشمل صلاحيات: • ضبط وتأمين تقنية المعلومات أو جزء منها أو وسيط تخزين معلومات تقنية المعلومات.عمل نسخة معلومات تقنية المعلومات والاحتفاظ بها. الحفاظ على سلامة معلومات تقنية المعلومات المخزنة. إزالة أو منع الوصول إلى تلك المعلومات في تقنية المعلومات التي يتم الوصول إليها. 2. تلتزم كل طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى أي شخص لديه معرفة بوظيفة تقنية المعلومات أو الإجراءات المطبقة لحماية تقنية المعلومات من أجل تقديم المعلومات الضرورية لإتمام تلك الإجراءات المذكورة في الفقرتين 2 و3 من المادة السادسة والعشرين من هذه الاتفاقية.		

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 16 من اتفاقية بودابست **الحفظ المستعجل لبيانات الحاسوب المخزنة والكشف عنها** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وغيرها من الإجراءات لتمكين سلطاته المختصة من طلب الحفظ السريع لبيانات الحاسوب المحددة أو الحصول عليها بشكل مماثل، بما في ذلك حركة البيانات التي تم تخزينها عن طريق نظام حاسوبي، ولا سيما عندما يكون هناك أسباب للاعتقاد بأن بيانات الحاسوب معرضة بشكل خاص للفقد أو التعديل. 2. عندما يقوم أحد الأطراف بتنفيذ الفقرة 1 أعلاه عن طريق أمر شخص بحفظ بيانات الحاسوب المخزنة المحددة وذلك بوضعها في حوزته أو تحت سيطرته، يعتمد هذا الطرف الإجراءات التشريعية وغيرها من الإجراءات التي قد تكون ضرورية لإلزام ذلك الشخص بالحفاظ على سلامة بيانات الحاسوب لفترة زمنية طويلة، حدها الأقصى تسعين يومًا، وذلك لتمكين السلطات المختصة من طلب الكشف عنها. يجوز للطرف أن ينص على تجديد هذا الأمر لاحقًا. 3. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لإلزام الحارس أو أي شخص آخر يحفظ بيانات الحاسوب بالحفاظ على سرية تنفيذ هذه الإجراءات للفترة الزمنية المنصوص عليها في قانونه الداخلي. 4. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و 15.	**لا يوجد معادل**	**التحليل القانوني** هذه السلطة الإجرائية مهمة لضمان الحفاظ على البيانات المعرضة للحذف أو الفقد. على الرغم من عدم توفير أي حكم للحفظ عليه - يؤكد الاستبيان أن أي طلب للحفظ يجب إرساله إلى مكتب المدعي العام بالقرب من محكمة النقض. **تحليل الفجوة** **التوصيات:** تعد هذه القدرة المستعجلة للاحتفاظ بمعلومات المشترك الأساسية والبيانات الوصفية والمعاملات والمحتويات المخزنة ضرورية كجزء من تحقيقات جرائم الإنترنت، ولضمان أن تكون الأدلة متاحة للبحث والوصول والضبط والمراجعة. يمكن استخدام لغة المادة 16 من اتفاقية بودابست أو القسم 23 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية أو المادة 23 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. سيتطلب ذلك أيضًا تعريفات «بيانات الحاسوب"، و[268] "معلومات المشترك أو معلومات المشترك الأساسية"، و "حركة البيانات" و[269] "مزود خدمة الاتصالات"[270] يجب ملاحظة أن اتفاقية بودابست واتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية لا تقدمان تعريفًا لمعلومات المشترك الأساسية؛ غير أن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات تقدم تعريفًا لمعلومات المشترك:[271] • " أي معلومات لدى مزود الخدمة بخصوص المشتركين في الخدمة، باستثناء المعلومات التي يمكن من خلالها معرفة ما يلي: • نوع خدمة الاتصال المستخدمة والأحكام الفنية المتعلقة بها وفترة الخدمة. • هوية المشترك وعنوانه البريدي أو الجغرافي أو رقم الهاتف ومعلومات الدفع المتاحة بموجب اتفاقية الخدمة • أي معلومات أخرى عن موقع تركيب معدات الاتصال بناءً على اتفاق الخدمة.» ينبغي إيلاء اهتمام لأن يكون طول مدة الحفظ معقولًا في هذه الظروف، وأن يُسمَح بتطبيق التمديد في الظروف الملحة - تنص اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست والاتفاقية العربية لمكافحة جرائم تقنية المعلومات على 90 يومًا، فيما تنص اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية على 7 أيام. ووفقًا للتجربة فإن مدة 90 يومًا هي مدة قصيرة في التحقيقات عبر الإنترنت ، ويجب أن تكون حوالي 180 يومًا يمكن تمديدها.

268. انظر المادة 1.ب. اتفاقية بودابست أو القسم 3 (6) من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية

269. انظر المادة 1.د من اتفاقية بودابست: «أي بيانات حاسوب تتعلق باتصال عن طريق نظام حاسوب، يتم إنشاؤها بواسطة نظام حاسوب يشكل جزءًا من سلسلة الاتصال، وتعرض مصدر الاتصال أو وجهته أو مساره أو الوقت أو التاريخ أو حجمه أو مدته أو نوع الخدمة الأساسية، أو القسم 3 (18) من مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية: «حركة البيانات تعني أي بيانات حاسوب تتعلق باتصال عن طريق نظام حاسوب، يتم إنشاؤها بواسطة نظام حاسوب يشكل جزءًا من سلسلة الاتصال، وتعرض مصدر الاتصال أو وجهته أو مساره أو الوقت أو التاريخ أو الحجم أو المدة أو نوع الخدمة الأساسية».

270. انظر المادة 1.ج. من اتفاقية بودابست: "1 أي كيان عام أو خاص يوفر للمستخدمين قدرة الاتصال عن طريق نظام الحاسوب، و 2 أي كيان آخر يعالج أو يخزن بيانات الحاسوب نيابة عن خدمة الاتصال هذه أو مستخدمي هذه الخدمة».

271. انظر المادة 2 (9) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
القسم 23 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية ـ الحفظ المستعجل إذا اقتنع ضابط [تطبيق القانون] [الشرطة] بوجود أسباب معقولة للاعتقاد بأن بيانات الحاسوب المطلوبة لأغراض التحقيق الجنائي معرضة للضياع أو التعديل، يجوز لضابط [تطبيق القانون] [الشرطة]، عن طريق إشعار مكتوب مقدم إلى شخص يتحكم في بيانات الكمبيوتر، أن يطلب من هذا الشخص الحفاظ على البيانات المحددة في الإشعار لمدة تصل إلى سبعة (7) أيام على وفقًا لما هو محدد في الإشعار. يمكن تمديد الفترة إلى ما بعد سبعة (7) أيام إذا سمح [قاضي]، بناءً على طلب من طرف واحد، وذلك لمدة زمنية أخرى محددة. **المادة 23 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات- الحفظ المستعجل للبيانات المخزنة في تكنولوجيا المعلومات** 1. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأمر أو الحصول على الحفظ العاجل للمعلومات المخزنة بما في ذلك معلومات تتبع المستخدمين والتي خزنت على تقنية معلومات وخصوصا إذا كان هناك اعتقاد بأن تلك المعلومات عرضة للفقدان أو التعديل. 2. تلتزم كل دولة طرف بتبني الإجراءات الضرورية فيما يتعلق بالفقرة 1 بواسطة إصدار أمر إلى شخص من أجل حفظ معلومات تقنية المعلومات المخزنة والموجودة بحيازته أو سيطرته ومن أجل إلزامه بحفظ وصيانة سلامة تلك المعلومات لمدة أقصاها 90 يوما قابلة للتجديد، من أجل تمكين السلطات المختصة من البحث والتقصي 3. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لإلزام الشخص المسؤول عن حفظ تقنية معلومات للإبقاء على سرية الإجراءات طوال الفترة القانونية المنصوص عليها في القانون الداخلي. **المادة 17 من اتفاقية بودابست** **الحفظ المستعجل والكشف الجزئي لبيانات المرور** 1. فيما يتعلق ببيانات المرور التي يتعين الحفاظ عليها بموجب المادة 16، يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى من أجل:		

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
a. التأكد من أن مثل هذا الحفظ المستعجل لبيانات المرور متاح بغض النظر عما إذا كان هناك واحد أو أكثر من مقدمي الخدمة قد شاركوا في نقل ذلك الاتصال؛ و ضمان الكشف السريع للسلطة المختصة لدى الدولة الطرف، أو للشخص المعين من قبل تلك السلطة، عن كمية كافية من بيانات المرور لتمكينه من تحديد مقدمي الخدمات والمسار الذي تم من خلاله نقل الاتصال. 2. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و 15. **القسم 23 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الحفظ المستعجل** إذا اقتنع ضابط [تطبيق القانون] [الشرطة] بوجود أسباب معقولة للاعتقاد بأن بيانات الحاسوب المطلوبة لأغراض التحقيق الجنائي معرضة للضياع أو التعديل، يجوز لضابط [تطبيق القانون] [الشرطة]، عن طريق إشعار مكتوب مقدم إلى شخص يتحكم في بيانات الكمبيوتر، أن يطلب من هذا الشخص الحفاظ على البيانات المحددة في الإشعار لمدة تصل إلى سبعة (7) أيام على وفقًا لما هو محدد في الإشعار. يمكن تمديد الفترة إلى ما بعد سبعة (7) أيام إذا سمح [قاضي]، بناءً على طلب من طرف واحد، وذلك لمدة زمنية أخرى محددة. **القسم 24 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - جمع بيانات حركة الاتصالات** إذا اقتنع ضابط [تطبيق القانون] [الشرطة] بناءً على أسباب معقولة بأن البيانات المخزنة في نظام الحاسوب ضرورية لأغراض التحقيق الجنائي، يجوز له أن يطلب، عبر إشعار خطي، من شخص له السيطرة على نظام الحاسوب كشف بيانات حركة مرور تتعلق باتصال محدد بشكل كافٍ لتحديد: • مزودو خدمة الإنترنت؛ و/ أو • المسار الذي تم من خلاله نقل الاتصال.	**لا يوجد معادل**	**التحليل القانوني** تعد هذه القوة الإجرائية مهمة بشكل خاص لضمان توفير مقدمي خدمات الإنترنت لعناوين بروتوكول إنترنت يمكنها تحديد موقع مرتكب الجريمة السيبرانية. **تحليل الفجوة** **التوصيات:** يجب تضمين هذه القوة المستعجلة جنبًا إلى جنب مع الكشف عن بيانات المرور في التشريعات لتمكين التحقيقات الفعالة في جرائم الإنترنت. يمكن استخدام لغة المادة 17 من اتفاقية بازل، القسمين 23 و 24 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية أو المادة 24 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. سيتطلب ذلك أيضًا تعريفات لـ «حركة البيانات" و "مزود خدمة الاتصالات"[272]

272. انظر التعريفات أعلاه

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 24 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - لتحفظ العاجل والكشف الجزئي لمعلومات تتبع المستخدمين تلتزم كل دولة طرف بتبني الإجراءات الضرورية فيما يختص بمعلومات تتبع المستخدمين من أجل: 1. ضمان توفر الحفظ العاجل لمعلومات تتبع المستخدمين بغض النظر عن اشتراك واحد أو أكثر من مزودي الخدمة في بث تلك الاتصالات. 2. ضمان الكشف العاجل للسلطات المختصة لدى الدولة الطرف أو لشخص تعينه تلك السلطات لمقدار كاف من معلومات تتبع المستخدمين لتمكين الدولة الطرف من تحديد مزودي الخدمة ومسار بث الاتصالات.		
المادة 18 من اتفاقية بودابست **أمر النسخ** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وتدابير أخرى لتمكين سلطاته المختصة من أن تأمر: • شخصًا موجودًا في إقليمها بتقديم بيانات حاسوب محددة في حيازته أو تحت سيطرته، وتُخَزّن في نظام حاسوب أو بوسيلة تخزين بيانات الحاسوب؛ و مقدم خدمة يقدم خدماته في إقليم الدولة الطرف بتقديم معلومات المشترك المرتبطة بهذه الخدمات، والتي تكون في حيازة أو تحت سيطرة مقدم الخدمة. 2. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و 15. 3. تعني «معلومات المشترك» أي معلومات محفوظة بشكل بيانات حاسوب أو أي شكل آخر ويحتفظ بها مزود الخدمة، وترتبط بالمشتركين في خدماته، بخلاف بيانات المرور أو المحتوى، والتي يمكن إنشاؤها من خلال:	**لا يوجد معادل**	**التحليل القانوني** هذا شرط أساسي لإجراء تحقيق فعال في جرائم الإنترنت وسيؤثر غيابه على الملاحقات القضائية والتعاون الدولي. **تحليل الفجوة** **التوصيات:** تعتبر هذه القوة الأساسية ضرورية لضمان توفير مزودي خدمة الاتصالات في لبنان لمعلومات المشترك الأساسية وبيانات المرور وبيانات المحتوى المخزنة. سيتطلب ذلك أيضًا تعريفات «بيانات الحاسوب»، و "معلومات المشترك أو معلومات المشترك الأساسية"، و "حركة البيانات" و "مزود خدمة الاتصالات"[273] المادة 25 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات هي نموذج يمكن استخدامه ويستخدم تعريفات مختلفة بما في ذلك «تكنولوجيا المعلومات"، و[274] "مزود الخدمة" و[275] "البيانات"؛[276] غير أنه من المستحسن أن تكون هناك تعريفات لـ «معلومات المشترك أو معلومات المشترك الأساسية" أو "حركة البيانات" لأنها ستكون أنواع مختلفة من الأدلة التي يمكن توليدها في دول الجنوب الشريكة. علاوة على ذلك، سوف تتطلب هذه السلطة من الأفراد وغيرهم (مثل الكيانات المؤسسية والمؤسسات المالية وغيرها من المنظمات) ممن يحملون البيانات أن يقوموا بتوليدها بناء على طلب سلطات إنفاذ القانون. يمكن أن تكون المادة 18 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست والمادة 22 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية بمثابة دليل مع التطبيق الثابت للتعريفات

273. انظر التعريفات أعلاه

274. المادة 2 (1) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات: "أية وسيلة مادية أو معنوية أو مجموعة وسائل مترابطة أو غير مترابطة تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها وفقا للأوامر والتعليمات المخزونة بها. ويشمل ذلك جميع المدخلات والمخرجات المرتبطة بها سلكيا أو لا سلكيا في نظام أو شبكة".

275. المادة 2 (2) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات: «أي شخص طبيعي أو معنوي عام أو خاص يزود المشتركين بالخدمات للتواصل بواسطة تقنية المعلومات، أو يقوم بمعالجة أو تخزين المعلومات نيابة عن خدمة الاتصالات أو مستخدميها».

276. المادة 2 (3) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات: «كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة تقنية المعلومات، كالأرقام والحروف والرموز وما إلى ذلك».

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
نوع خدمة الاتصال المستخدمة والأحكام الفنية المتعلقة بها وفترة الخدمة؛ هوية المشترك أو العنوان البريدي أو الجغرافي، ورقم الهاتف وأرقام الاتصال الأخرى ومعلومات الفوترة والدفع المتاحة بناءً على اتفاقية الخدمة؛ أي معلومات أخرى متاحة على موقع تركيب معدات الاتصالات بناءً على اتفاقية الخدمة أو الترتيب. **القسم 22 من نظام اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - أمر النسخ** إذا كان [قاض] مقتنعًا بناءً على طلب قدمه [ضابط أنفاذ القانون] [الشرطة] بأن بيانات حاسوب محددة أو نسخة مطبوعة أو غيرها من المعلومات ضرورية لإجراء تحقيق جنائي أو لإجراءات جنائية، يجوز [للقاضي] أن يأمر بما يلي: • أن ينسخ شخص في إقليم [الدولة المشترعة] يتحكم في نظام الحاسوب نسخًا محددة من بيانات الحاسوب أو نسخة مطبوعة أو معلومات أخرى واضحة من تلك البيانات؛ أو • مزود خدمة الإنترنت في [الدولة المشترعة] لتقديم معلومات حول الأشخاص المشتركين في الخدمة أو الذين يستخدمونها بطريقة أخرى. **المادة 25 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - أمر تسليم المعلومات** تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى: 1. أي شخص في إقليمها لتسليم معلومات معينة في حيازة ذلك الشخص والمخزنة على تقنية معلومات أو وسيط تخزين معلومات. 2. أي مزود خدمة يقدم خدماته في إقليم الدولة الطرف لتسليم معلومات المشترك المتعلقة بتلك الخدمات في حوزة مزود الخدمة أو تحت سيطرته.		

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 21 من اتفاقية بودابست **اعتراض بيانات المحتوى** 1. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وغيرها من الإجراءات، فيما يتعلق بمجموعة من الجرائم الخطيرة التي يحددها القانون المحلي، لتمكين سلطاته المختصة من: a. الجمع أو التسجيل من خلال تطبيق الوسائل التقنية على أراضي ذلك الطرف، و إلزام مزود الخدمة، في حدود قدرته التقنية الحالية: i. الجمع أو التسجيل من خلال تطبيق الوسائل التقنية على أراضي ذلك الطرف؛ أو ii. التعاون ومساعدة السلطات المختصة في جمع أو تسجيل بيانات المحتوى في الوقت الحقيقي، لاتصالات محددة تتم في أراضيها وترسل عن طريق نظام حاسوبي. 2. في الحالات التي لا يمكن فيها لأي طرف، بسبب المبادئ المستقرة في نظامه القانوني الداخلي، أن يعتمد التدابير المشار إليها في الفقرة 1.أ، يجوز له بدلا من ذلك اعتماد تدابير تشريعية وتدابير أخرى قد تكون ضرورية لضمان جمع أو تسجيل البيانات المرورية المرتبطة باتصالات محددة مرسلة في أراضيه، في الوقت الحقيقي، من خلال تطبيق الوسائل التقنية على ذلك الإقليم. 3. يعتمد كل طرف التدابير التشريعية والتدابير الأخرى التي قد تكون ضرورية لإلزام مقدم الخدمة بالحفاظ على سرية تنفيذ أي سلطة منصوص عليها في هذه المادة وأي معلومات تتعلق بها. 4. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و 15.	**القانون 140/99 ، المعدل بموجب القانون 158/99.** **المواد 2 و 3 و 9**	**التحليل القانوني** القانون رقم 140 لسنة 1999 المعدل بالقانون رقم 158 لسنة 1999. يسمح باعتراض جميع وسائل الاتصال والاستماع إليها ومراقبتها - بما في ذلك رسائل البريد الإلكتروني لا يُسمح بالاعتراض إلا باتخاذ قرار قضائي أو إداري على النحو المنصوص عليه في المادتين 2 و3 من القانون رقم 140 لسنة 1999 وذلك لمدة أقصاها شهران قابلة للتمديد. تسمح المادة 2 باعتراض الاتصالات في الحالات العاجلة جدًا إذا كانت متعلقة بجرائم يعاقب عليها بالسجن لمدة لا تقل عن سنة. تسمح المادة 9 لوزير الدفاع ووزير الداخلية باعتراض الاتصالات بعد موافقة رئيس الوزراء وذلك من أجل جمع المعلومات عن جرائم الإرهاب والجريمة المنظمة. تعتبر هذه السلطة ضرورية للتشريعات الوطنية - ويجب أن تكون هناك ضمانات ومتطلبات/إجراءات لإلزام مزودي خدمة الاتصالات على التعاون في جمع أو تسجيل بيانات المحتوى في الوقت الفعلي لاتصالات محددة تتم في لبنان. **تحليل الفجوة** **التوصيات:** يجب اتخاذ تدابير لإلزام مزودي خدمة الاتصالات في لبنان (لما هو أبعد من رسائل البريد الإلكتروني مثل تطبيقات المراسلة) بالتعاون لجمع المحتوى في الوقت الفعلي؛ ويجب إدراج ضمانات لضمان أن جمعها قانوني وضروري ومعقول ومتناسب مع الحالة. يجب مراعاة مراجعة المادة 29 من CITO والمادة 21 من اتفاقية بودابست والقسم 26 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية وإدراج اللغة في التشريعات الوطنية

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
القسم 26 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - اعتراض بيانات المحتوى 1. إذا تأكد [قاضٍ] بناء على [شهادة تحت القسم] [شهادة خطية] بأن هناك أسباباً معقولة لـ [الاشتباه] [الظن] بأن محتوى البلاغات الإلكترونية هو مطلوب بشكل معقول لأغراض [التحقيق] في تحقيق جنائي، [يجوز] [للقاضي] [يجب] أن: • يطلب من مزود خدمة الإنترنت الذي تتوفر خدمته في [بلد المشرع] جمع أو تسجيل أو السماح أو مساعدة السلطات المختصة في جمع أو تسجيل بيانات المحتوى المرتبطة بالاتصالات المحددة التي يتم إرسالها عن طريق نظام حاسوب، وذلك من خلال استخدام وسائل تقنية؛ أو • السماح لموظف [قوة تنفيذ القانون] [الشرطة] بجمع أو تسجيل تلك البيانات من خلال تطبيق الوسائل التقنية. 2. قد تقرر دولة عدم تنفيذ القسم 26. **المادة 29 CITO - اعتراض معلومات المحتوى** 1. تلتزم كل دولة طرف باعتماد الإجراءات التشريعية اللازمة المتعلقة بسلسلة من الجرائم المنصوص عليها في القانون المحلي، وذلك لتمكين السلطات المختصة من: a. تسجيل أو جمع المعلومات من خلال الوسائل التقنية في أراضي هذه الدولة الطرف، أو 2. التعاون مع السلطات المختصة ومساعدتها على تسريع جمع وتسجيل معلومات المحتوى الخاصة بالاتصالات ذات الصلة في إقليمها والتي يتم نقلها عن طريق تكنولوجيا المعلومات. 3. إذا تعذر على الدولة الطرف، بسبب النظام القانوني المحلي، اعتماد الإجراءات المبينة في الفقرة 1 (أ)، يجوز لها اعتماد إجراءات أخرى بالشكل الضروري لضمان تسريع جمع وتسجيل معلومات المحتوى المقابلة الاتصالات ذات الصلة في أراضيها باستخدام الوسائل التقنية في ذلك الإقليم. تلتزم كل دولة طرف باعتماد الإجراءات اللازمة لمطالبة مقدم الخدمة بالحفاظ على سرية أي معلومات عند ممارسة السلطة المنصوص عليها في هذه المادة.		

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 20 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[277] **جمع بيانات حركة الاتصالات في الوقت الحقيقي** 1. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتمكين سلطاته المختصة من: a. الجمع أو التسجيل من خلال تطبيق الوسائل التقنية على أراضي ذلك الطرف، و إلزام مزود الخدمة، في حدود قدرته التقنية الحالية: يجمع أو يسجل بواسطة الوسائل الفنية على إقليم تلك الدولة الطرف؛ أو يتعاون ويساعد السلطات المختصة في جمع أو تسجيل بيانات المرور في الوقت الفعلي، مع الاتصالات المعينة في إقليمها والتي تبث بواسطة نظام حاسوبي. 2. في الحالات التي لا يمكن فيها لأي طرف، بسبب المبادئ المستقرة في نظامه القانوني الداخلي، أن يعتمد التدابير المشار إليها في الفقرة 1.أ، يجوز له بدلا من ذلك اعتماد تدابير تشريعية وتدابير أخرى قد تكون ضرورية لضمان جمع أو تسجيل البيانات المرورية المرتبطة باتصالات محددة مرسلة في أراضيه، في الوقت الفعلي، من خلال تطبيق الوسائل التقنية على ذلك الإقليم. 3. يعتمد كل طرف التدابير التشريعية والتدابير الأخرى التي قد تكون ضرورية لإلزام مقدم الخدمة بالحفاظ على سرية تنفيذ أي سلطة منصوص عليها في هذه المادة وأي معلومات تتعلق بها. 4. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و 15. **القسم 25 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - جمع بيانات حركة الاتصالات** 1. إذا تأكد [قاض] بناء على [شهادة تحت القسم] [شهادة خطية] بأن هناك أسباباً معقولة لـ [الاشتباه] [الظن] بأن بيانات حركة الاتصالات المرتبطة ببلاغ محدد ضرورية بشكل معقول لأغراض [التحقيق] في تحقيق جنائي، [يجوز] [للقاضي] [يجب] أن يأمر شخصًا يتحكم بهذه البيانات بما يلي:	**لا يوجد معادل**	**التحليل القانوني** لا توجد سلطة إجرائية لجمع بيانات حركة المرور في الوقت الحقيقي. يمكن أن يكون هناك حد أدنى لجمع بيانات حركة المرور في الوقت الحقيقي، وتعد هذه الحركة أداة تحقيق أساسية. قد تكون هناك حالات لا يضع فيها مقدم الطلب حدًا قانونيًا أعلى لتأمين المحتوى، ولكن يمكن وجود حد أدنى لتأمين حركة المرور. لهذا السبب، يجب أن يكون هناك تمييز بين جمع المحتوى المخزن وبيانات المرور في الوقت الحقيقي. يجب أن تكون هناك ضمانات ومتطلبات/إجراءات لإلزام مزودي خدمة الاتصالات على التعاون في جمع أو تسجيل بيانات المحتوى في الوقت الفعلي لاتصالات محددة تتم في لبنان **تحليل الفجوة** **التوصيات:** ينبغي توفير صلاحية محددة لجمع بيانات المرور في الوقت الفعلي، وينبغي إدراج حكم لإلزام مزودي خدمة الاتصالات في لبنان على التعاون لجمع بيانات المرور في الوقت الفعلي؛ ويجب إدراج ضمانات لضمان أن جمعها قانوني وضروري ومعقول ومتناسب مع الحالة. يمكن اعتماد اللغة من المادة 28 الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لكنها لا تشير إلى الجمع المستعجل في الوقت الحقيقي. يجب استخدام المادة 20 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست والمادة 25 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية باعتبارهما دليلًا للتشريعات الوطنية

277. تشير المادة 28 من اتفاقية الاتفاقية العربية لمكافحة جرائم تقنية المعلومات إلى الجمع المستعجل بدلًا من الجمع في الوقت الحقيقي

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
• جمع أو تسجيل بيانات حركة الاتصالات المرتبطة باتصالات محددة خلال فترة محددة؛ أو • التصريح ومساعدة ضابط [الشرطة] [قوة تنفيذ القانون] محدد لجمع أو تسجيل تلك البيانات. 2. إذا تأكد [قاض] بناء على [شهادة تحت القسم] [شهادة خطية] بأن هناك أسباباً معقولة لـ [الاشتباه] [الظن] بأن بيانات حركة الاتصالات المرتبطة ببلاغ محدد ضرورية بشكل معقول لأغراض [التحقيق] في تحقيق جنائي، [يجوز] [للقاضي] [يجب] أن يسمح لـ [قوة تنفيذ القانون] [الشرطة] بجمع أو تسجيل بيانات حركة الاتصالات المرتبطة برسالة محددة خلال فترة محددة من خلال تطبيق الوسائل التقنية. 3. قد تقرر دولة عدم تنفيذ القسم 25.		
		واجب الكشف عن مفاتيح التشفير مع استخدام الإرهابيين والمجرمين المنظمين بشكل روتيني لتطبيقات الرسائل المشفرة[278] قد يعتبر الكشف عن مفاتيح التشفير قوة ملائمة لإطلاق مفاتيح كلمات المرور لفتح الأجهزة[279] **تحليل الفجوة** **التوصيات:** عدم القدرة على توضيح ما إذا كانت هناك أية صلاحيات في لبنان - لكن هذه الصلاحيات ستتيح لوكالات إنفاذ القوانين إجبار أصحاب الأجهزة على فتحها
		التزامات الاحتفاظ بالبيانات[280] تسمح مثل هذه السلطة لوكالات إنفاذ القانون ب 1. تتبع وتحديد مصدر الاتصال 2. تحديد وجهة الاتصال؛ 3. تحديد تاريخ ووقت ومدة الاتصال؛ و 4. تحديد نوع الاتصال لبنان لديها هذا النوع من الالتزام[281]

278. Eleanor Saitta. "Can Encryption Save Us?" Nation 300، رقم 24 (51 يونيو 5102): 16-
18. Academic Search Premier, EBSCOhost (تمت زيارته في 29 فبراير 2016).
279. انظر مثلاً القسم 49 من القانون الإنجليزي (Regulation of Investigatory Powers Act 2000 (UK) -
http://www.legislation.gov.uk/ukpga/2000/23/section/49
280. أصدر الاتحاد الأوروبي في عام 2006 توجيهه بشأن الاحتفاظ بالبيانات - اضطرت الدول الأعضاء في الاتحاد الأوروبي إلى تخزين بيانات الاتصالات الإلكترونية لمدة ستة أشهر على الأقل و 24 شهراً على الأكثر للتحقيق في الجرائم الخطيرة وكشفها ومقاضاة مرتكبيها. أبطلت محكمة العدل الأوروبية في عام 2014 توجيه الاحتفاظ بالبيانات، حيث قررت أنها قدمت ضمانات غير كافية ضد التدخلات في الخصوصية وحماية البيانات. في حالة عدم وجود توجيه صالح للاتحاد الأوروبي بشأن الاحتفاظ بالبيانات، فقد تواصل الدول الأعضاء تقديم خطة للاحتفاظ بالبيانات - للاطلاع على الخطط الوطنية، انظر: http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention
281. تقرير ICMEC العالمي، صفحة 30

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 22 من اتفاقية بودابست **الاختصاص القضائي** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وغيرها من الإجراءات لإقامة ولاية قضائية على أي جرم منصوص عليه في المواد من 2 إلى 11 من هذه الاتفاقية، عندما تُرتكب الجريمة: a. في أراضيها؛ أو على متن سفينة ترفع علم تلك الدولة الطرف؛ أو على متن طائرة مسجلة بموجب قوانين ذلك الطرف؛ أو من قِبَل أحد رعاياها، إذا كانت الجريمة معاقبًا عليها بموجب القانون الجنائي حيث ارتكبت، أو إذا ارتكبت الجريمة خارج الولاية الإقليمية لأي دولة. 2. يجوز لكل طرف أن يحتفظ بالحق في عدم تطبيق أو تطبيق قواعد الاختصاص المنصوص عليها في الفقرات من 1 إلى 1 د من هذه المادة أو أي جزء منها فقط في حالات أو شروط محددة. 3. يعتمد كل طرف ما قد يلزم من إجراءات لإقامة ولاية قضائية على الجرائم المشار إليها في الفقرة 1 من المادة 24 من هذه الاتفاقية، في الحالات التي يكون فيها الجاني المفترض موجودا في إقليمه ولا يسلمه إلى بلد آخر بعد طلب التسليم على أساس جنسيته فقط. 4. لا تستبعد هذه الاتفاقية أي ولاية قضائية جنائية يمارسها أي طرف وفقًا لقانونه الداخلي. 5. عندما يطالب أكثر من طرف بالولاية القضائية على جريمة مفترضة تم النص عليها في هذه الاتفاقية، يتشاور الطرفان المعنيان، عند الضرورة من أجل تحديد الولاية القضائية الأنسب. **القسم 19من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الولاية القضائية** ينطبق هذا القانون على أي فعل أو تقصير: • في إقليم [الدولة المشترعة]؛ أو • على سفينة أو طائرة مسجلة في [الدولة المشترعة]؛ أو • من قبل أحد مواطني [البلد المشترع] خارج الولاية القضائية لأي بلد؛	**لا يوجد معادل**	**التحليل القانوني** بدون وجود نطاق محدد بوضوح للجرائم الإلكترونية ، وهي دولية بطبيعتها سيبقى أي تشريع مقيدًا. **تحليل الفجوة** **التوصيات:** يضمن التشريع الوطني أن يتم تعريف الاختصاص باستخدام لغة المادة 22 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست، القسم 19 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية أو المادة 30 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. إذا كان هناك تعارض بين السلطات القضائية، فيجب أن تؤخذ في الاعتبار المبادئ التوجيهية المتعلقة بتحديد الولاية القضائية المناسبة لمحاكمة جريمة ما - انظر المبادئ التوجيهية Eurojust لتقرير الولاية القضائية التي في الجرائم التي تجب ملاحقتها (المراجعة 2016)[282]

282. http://www.eurojust.europa.eu/Practitioners/operational/Documents/Operational-Guidelines-for-Deciding.pdf

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
من قبل أحد مواطني [البلد المشترع] خارج إقليم [البلد المشترع]، إذا كان سلوك هذا الشخص يشكل أيضًا جريمة بموجب قانون البلد الذي ارتكبت فيه الجريمة. **المادة 30 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - الاختصاص** 1. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد اختصاصها على أي من الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية وذلك إذا ارتكبت الجريمة كلياً أو جزئياً أو تحققت: a. في إقليم الدولة الطرف على متن سفينة تحمل علم الدولة الطرف. على متن طائرة مسجلة تحت قوانين الدولة الطرف. من قبل أحد مواطني الدولة الطرف إذا كانت الجريمة يعاقب عليها حسب القانون الداخلي في مكان ارتكبها أو إذ ارتكبت خارج منطقة الاختصاص القضائي لأية دولة. إذا كانت الجريمة تمس أحد المصالح العليا للدولة. 2. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد الاختصاص الذي يغطي الجرائم المنصوص عليها في المادة الحادية والثلاثين الفقرة 1 من هذه الاتفاقية في الحالات التي يكون فيها الجاني المزعوم حاضرا في إقليم تلك الدولة الطرف ولا يقوم بتسليمه إلى طرف آخر بناء على جنسيته بعد طلب التسليم. 3. إذا ادعت أكثر من دولة بالاختصاص القضائي لجريمة منصوص عليها في هذه الاتفاقية فيقدم طلب الدولة التي أخلت الجريمة بأمنها أو بمصالحها ثم الدولة التي وقعت الجريمة في إقليم ثم الدولة التي يكون الشخص المطلوب من رعاياها وإذا اتحدت الظروف فتقدم الدولة الأسبق في طلب التسليم. في حالة وجود ظروف مماثلة، تُعطى الأولوية لأول دولة تطلب التسليم.		

التعاون الدولي		
أفضل الممارسات الدولية	**التشريع الوطني**	**ملاحظات**
المادة 35 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[283] **شبكة تعمل على مدار اليوم والساعة** 1. يعين كل طرف جهة اتصال متاحة على مدار أربع وعشرين ساعة وطوال أيام الأسبوع، من أجل ضمان تقديم مساعدة فورية بغرض إجراء تحقيقات أو إجراءات تتعلق بالجرائم الجنائية المتعلقة بأنظمة الكمبيوتر والبيانات، أو لجمع أدلة عن الجرائم الجنائية في شكل إلكتروني. يجب أن تشمل هذه المساعدة تيسير الإجراءات التالية، أو تنفيذها مباشرة إذا سمح القانون الداخلي بذلك: a. تقديم المشورة الفنية؛ الحفاظ على البيانات وفقا للمادتين 29 و 30؛ جمع الأدلة وتوفير المعلومات القانونية وتحديد مكان المشتبه به. 2. يجب أن يكون لدى جهة الاتصال التابعة لكل طرف القدرة على إجراء الاتصالات مع جهة اتصال الطرف الآخر على وجه السرعة. إذا لم تكن نقطة الاتصال التي حددها أحد الأطراف جزءًا من سلطة أو سلطات ذلك الطرف المسؤولة عن المساعدة أو التسليم المتبادلين الدوليين، فيجب أن تضمن قدرتها على التنسيق مع هذه السلطة أو السلطات على وجه السرعة. 3. يجب على كل طرف التأكد من توفر الأفراد المدربين والمجهزين من أجل تسهيل تشغيل الشبكة.	**لا يوجد معادل**	**التحليل القانوني** هذه آلية أساسية لتحقيق قدرة فعالة على التحقيق في الجرائم الإلكترونية. **تحليل الفجوة** **التوصيات:** لا ينبغي أن يتطلب ذلك تشريعًا خاصًا لتنفيذه، وفيما يتعلق بالموارد يجب أن تُعطى الأولوية. يجب مشاركة تفاصيل الاتصال لنقطة الاتصال الوحيدة المعينة (SPOC) على المستوى الوطني ومع السلطات المركزية على المستوى الدولي والإنتربول. ينبغي أيضًا النظر في صياغة مذكرة تفاهم مع الوكالات الوطنية بحيث يكون لدى نقطة الاتصال الوحيدة المعينة سلطة القيام بالإجراءات المطلوبة كجزء من تحقيق دولي في جرائم الإنترنت وتطبيق القوانين والمعاهدات الوطنية. ستتضمن مذكرة التفاهم هذه الطلبات الواردة والصادرة وتضمن عملية فعالة وكفؤة.
المادة 25 من اتفاقية بودابست **المبادئ العامة المتعلقة بالمساعدة المتبادلة** 1. يقدم الطرفان المساعدة المتبادلة إلى أقصى حد ممكن لغرض إجراء التحقيقات أو الإجراءات المتعلقة بالجرائم الجنائية المتعلقة بأنظمة الحاسوب والبيانات، أو لجمع الأدلة المتعلقة بالجرائم الجنائية في شكل إلكتروني. 2. يعتمد كل طرف أيضًا الإجراءات التشريعية وغيرها من الإجراءات التي قد تكون ضرورية لتنفيذ الالتزامات المنصوص عليها في المواد من 27 إلى 35.	**لا يوجد معادل**	**التحليل القانوني** لبنان ليس طرفًا في اتفاقية بودابست أو الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. لبنان ليس طرفًا في أي اتفاقية دولية مخصصة للجرائم السيبرانية، وسيعيق ذلك التحقيقات الدولية لأن السلطات الإجرائية لن يكون لها أساس قانوني. بخلاف أي اتفاقية ثنائية - لبنان من الدول الموقعة على اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية[284] لذلك فإن المادة 18 من تلك الاتفاقية هي أساس المساعدة القانونية المتبادلة والتبادلية/مبدأ المعاملة بالمثل.[285]

283. المادة 43 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات
284. تم التصديق في 5 أكتوبر 2005
285. يمكن للمادة 18 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة أن تكون أساس قانون مكافحة غسل الأموال إذا كان تعريف الجريمة المنظمة عبر الوطنية مصدقًا عليه، ويمكن أن تكون اتفاقية الرياض بشأن التعاون القضائي أساسًا تشريعيًا للدول التي صادقت عليها

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
3. يجوز لكل طرف في الظروف العاجلة تقديم طلبات للمساعدة المتبادلة أو الاتصالات المتعلقة بها عن طريق وسائل الاتصال العاجلة، بما في ذلك الفاكس أو البريد الإلكتروني، إلى الحد الذي توفر فيه هذه الوسائل مستويات مناسبة من الأمن والمصادقة (بما في ذلك استخدام التشفير، عند الضرورة)، مع تأكيد رسمي لاحق، حيثما يطلب ذلك الطرف متلقي الطلب. يجب على الطرف متلقي الطلب قبول الطلب والرد عليه بأي وسيلة اتصال سريعة. 4. باستثناء ما هو منصوص عليه على وجه التحديد في المواد الواردة في هذا الفصل، تخضع المساعدة المتبادلة للشروط المنصوص عليها في قانون الطرف متلقي الطلب أو معاهدات المساعدة المتبادلة المطبقة، بما في ذلك الأسباب التي تُجيز للطرف متلقي الطلب أن يرفض التعاون. لا يجوز للطرف متلقي أن يبني حقه في رفض المساعدة المتبادلة المتعلقة بالجرائم المشار إليها في المواد من 2 إلى 11، فقط على أساس أن الطلب يتعلق بجريمة يعتبرها جريمة مالية. 5. عندما تسمح أحكام هذا الفصل للطرف متلقي الطلب بتقييد المساعدة المتبادلة بشرط ازدواجية التجريم، يعتبر هذا الشرط مستوفيًا، بصرف النظر عما إذا كانت قوانينه تضع الجريمة في نفس الفئة الجرمية، أو إذا أعطيت الجريمة نفس التسمية عند الطرف الطالب، وذلك إن كان السلوك الكامن وراء الجريمة التي طلبت المساعدة من أجلها جريمة جنائية بموجب قوانينه.		وهذا يعني أنه بدون التشريعات الوطنية لا يمكن تقديم طلبات للحفظ المستعجل لبيانات الحاسوب المخزنة والحفظ المستعجل والكشف الجزئي لبيانات المرور والكشف عن البيانات المخزنة وبيانات المرور، بمعنى وجود قيود على التعاون الدولي الذي يمكن أن يوفره لبنان للدول مقدمة الطلب. **تحليل الفجوة** **التوصيات:** يُطلب من القانون المحلي الحفاظ على بيانات الحاسوب المخزنة على وجه السرعة، والحفظ المستعجل والكشف الجزئي لبيانات المرور وطلبات النسخ. يمكن استخدام اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست واتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية و الاتفاقية العربية لمكافحة جرائم تقنية المعلومات كسوابق من أجل المحافظة المستعجلة على بيانات الحاسوب المخزنة،[286] والحفظ المستعجل والكشف الجزئي لبيانات المرور،[287] والكشف عن البيانات المخزنة[288] والجمع المستعجل لبيانات المرور[289] - هناك حاجة أيضًا للنظر في إمكانية السماح باعتراض بيانات ومحتويات حركة المرور في الوقت الحقيقي[290]. علاوة على ذلك، يجب أن يكون هناك إطار للتعاون في تحقيقات جرائم الإنترنت التي تنص عليها اتفاقيات متعددة الأطراف مثل المادة 27 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست والمادة 32 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.[291] ينبغي النظر في السماح للسلطات المختصة بإعطاء الإذن لهيئات إنفاذ القانون المحلي بإجراء تحقيق في الدولة التي تأكد فيها الوصول إلى الجهاز. يعد الوصول إلى المعلومات هو المعيار الأساسي لبدء التحقيق في الحالات التي يتعذر فيها معرفة مكان تخزين البيانات (أي في التخزين السحابي). يمكن أن يشمل ذلك "اعترافًا متبادلًا" بأوامر المحكمة الصادرة تجاه مقدمي خدمات الاتصالات في دولة معينة، والتي يمكن تقديمها إلى فروع مقدمي خدمة العملاء الموجودين في دول أخرى، اعتمادًا على مكان تخزين البيانات.

286. المادة 29 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست، القسم 23 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية والمادة 37 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

287. المادة 30 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست، القسمان 23 و 24 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية والمادة 38 الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

288. المادة 31 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست والمادة 39 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

289. المادة 41 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

290. المادتان 33 و 34 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست، والقسمان 25 و 26 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية

291. لا توجد أحكام مكافئة بشأن إجراءات المساعدة القانونية المتبادلة في اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 34 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - الإجراءات المتعلقة بطلبات التعاون والمساعدة المتبادلة 1. تطبق أحكام الفقرات 2-9 من هذه المادة في حالة عدم وجود معاهدة أو اتفاقية تعاون ومساعدة متبادلة وفقًا للتشريعات المعمول بها بين الدول الأطراف التي تطلب المساعدة وتلك التي تُطلَب منها المساعدة. في حال وجوده جود معاهدة أو اتفاقية فلا تطبق الفقرات المشار إليها إلا إذا اتفقت الأطراف المعنية على تطبيقها كاملة أو بشكل جزئي . 2. a. على كل دولة طرف تحديد سلطة مركزية تكون مسؤولة عن إرسال وإجابة طلبات المساعدة المتبادلة وتنفيذ هذه الطلبات وإيصالها إلى السلطات المعنية لتنفيذها. b. على السلطات المركزية أن تتصل ببعضها مباشرة. c. على كل دولة طرف- وقت التوقيع أو إيداع أدوات التصديق أو القبول أو الموافقة- أن تتصل بالأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس العدل العرب وتنقل إليهما أسماء وعناوين السلطات المحددة خصيصا لغايات هذه الفقرة. d. تقوم الأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس وزراء العدل العرب بإنشاء وتحديث سجل للسلطات المركزية والمعينة من قبل الدول الأطراف. وعلى كل دولة طرف أن تتأكد من أن التفاصيل الموجودة في السجل صحيحة دائما 3. يتم تنفيذ طلبات المساعدة المتبادلة في هذه المادة وفقًا للإجراءات التي تحددها الدولة الطرف الطالبة، إلا في حالة عدم الامتثال لقانون الدولة الطرف متلقية طلب المساعدة. 4. يجوز للدولة الطرف المطلوب منها المساعدة أن تؤجل الإجراءات المتخذة بشأن الطلب إذا كانت هذه الإجراءات تؤثر على التحقيقات الجنائية التي تجري من قبل سلطاتها. 5. قبل رفض أو تأجيل المساعدة يجب على الدولة الطرف المطلوب منها المساعدة بعد استشارة الدولة الطرف الطالبة لها أن تقرر فيما إذ سيتم تلبية الطلب جزئيا أو يكون خاضعا للشروط التي قد ترها ضرورية.		

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
6. تلتزم الدولة الطرف المطلوب منها المساعدة أن تُعلِم الدولة الطرف الطالبة لها بنتيجة تنفيذ الطلب. وإذا تم رفض أو تأجيل الطلب يجب إعطاء أسباب هذا الرفض أو التأجيل. ويجب على الدولة الطرف المطلوب منها المساعدة أن تعلم الدولة الطرف الطالبة لها بالأسباب التي تمنع تنفيذ الطلب بشكل نهائي أو الأسباب التي تؤخره بشكل كبير. 7. يجوز للدولة الطرف الطالبة للمساعدة أن تطلب من الطرف المطلوب منها المساعدة الإبقاء على سرية حقيقة ومضمون أي طلب يندرج في هذا الفصل ما عدا القدر لكافي لتنفيذ الطلب. وإذا لم تستطع الدولة الطرف المطلوب منها المساعدة الالتزام بهذا الطلب للسرية يجب عليها إعلام الدولة الطرف الطالبة والتي ستقرر مدى إمكانية تنفيذ الطلب. 8. a. في الحالات العاجلة يجوز إرسال طلبات المساعدة المتبادلة مباشرة إلى السلطات القضائية في الدولة الطرف المطلوب منها المساعدة من نظيرتها في الدولة الطرف الطالبة لها. وفي مثل هذه الحالات يجب إرسال نسخة الوقت من السلطة المركزية في الدولة الطرف الطالبة إلى نظيرتها في الدولة الطرف المطلوب منها. b. يجوز عمل الاتصالات وتقديم الطلبات حسب هذه الفقرة بواسطة الإنتربول. c. حيثما يتم تقديم طلب حسب الفقرة أ ولم تكن السلطة مختصة بالتعامل مع الطلب فيجب عليها إحالة الطلب إلى السلطة المختصة وإعلام الدولة الطرف الطالبة للمساعدة مباشرة بذلك. d. إن الاتصالات والطلبات التي تتم حسب هذه الفقرة والتي لا تشمل الإجراء القسري يمكن بثها مباشرة من قبل السلطات المختصة في الدولة الطرف الطالبة للمساعدة إلى نظيرتها في الدولة الطرف المطلوب منها المساعدة. e. يجوز لكل دولة طرف، وقت التوقيع أو التصديق أو القبول أو الإقرار أو الانضمام إبلاغ الأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس وزراء العدل العرب بأن الطلبات حسب هذه الفقرة يجب توجيهها إلى السلطة المركزية لغايات الفعالية.		

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 26 من اتفاقية بودابست **المعلومات التلقائية** 1. يجوز للطرف، في حدود قانونه الداخلي ودون طلب مسبق، أن يحيل إلى الطرف الآخر المعلومات التي تم الحصول عليها في إطار تحقيقاته، عندما يرى أن الكشف عن هذه المعلومات قد يساعد الطرف المتلقي في بدء أو التحقيقات أو الإجراءات المتعلقة بالجرائم الجنائية المنصوص عليها في هذه الاتفاقية، أو قد تؤدي إلى طلب تعاون من جانب هذا الطرف بموجب هذا الفصل. 2. قبل تقديم هذه المعلومات، يجوز للطرف المقدم أن يطلب الحفاظ على سريتها أو استخدامها فقط وفقًا للشروط. إذا لم يستطع الطرف المتلقي الامتثال لهذا الطلب، فيجب عليه إخطار الطرف المقدم الذي يحدد بعد ذلك ما إذا كان ينبغي تقديم المعلومات. إذا قبل الطرف المتلقي المعلومات وفقًا لهذه الشروط فعليه أن يلتزم بها. **المادة 33 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - المعلومات العرضية المتلقاة** 1. يجوز لأي دولة طرف- ضمن حدود قانونها الداخلي- وبدون طلب مسبق أن تعطي لدولة أخرى معلومات حصلت عليها من خلال تحقيقاتها إذا اعتبرت أن كشف مثل هذه المعلومات يمكن أن تساعد الدولة الطرف المرسلة إليها في إجراء الشروع أو القيام بتحقيقات في الجرائم المنصوص عليها في هذه الاتفاقية أو قد تؤدي إلى طلب للتعاون من قبل تلك الدولة الطرف. 2. قبل إعطاء مثل هذه المعلومات يجوز للدولة الطرف المزودة أن تطلب الحفاظ على سرية المعلومات، وإذا لم تستطع الدولة الطرف المستقبلة الالتزام بهذا الطلب يجب عليها إبلاغ الدولة الطرف المزودة بذلك والتي تقرر بدورها مدى إمكانية التزويد بالمعلومات. وإذا قبلت الدولة الطرف المستقبلة المعلومات مشروطة بالسرية فيجب أن تبقى المعلومات بين الطرفين.	**لا يوجد معادل**	**التحليل القانوني** يعد هذا إجراءً هامًا لتمكين الدولة من الاحتفاظ بمعلومات من شأنها أن تساعد دولة أخرى على منع جريمة الإنترنت أو التحقيق فيها. وعلى الرغم من أن ذلك متاحًا بين الدول التي صدقت على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الوارد ذكرهم في المادة 33 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، فليس للبنان أي أساس قانوني محلي يجبره بمشاركة هذه المعلومات مع الدول غير الموقعة على الاتفاقية ما لم يتم إرسال طلب رسمي عبر قنوات المساعدة القانونية المتبادلة المعتادة. تنص المادة 18 (4) - (5) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة على تبادل المعلومات الاستخباراتية تلقائيًا في الأمور التي تفي بتعريف جريمة خطيرة[292]، ذات طابع عبر وطني[293] وأن جماعة إجرامية منظمة ضالعة في ارتكاب الجرم[294]. دون استيفاء هذا التعريف، يجب إرسال طلب رسمي عبر قنوات المساعدة القانونية المتبادلة المعتادة إلى الدول التي ليست عضوًا في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. وبسبب الطبيعة السريعة الحركة للجريمة السيبرانية، فإن المشاركة التلقائية هي وسيلة فعالة للتعاون مع الدول الأخرى، وغياب هذه المشاركة يمنع التعاون الدولي الفعال مع الدول غير العضو في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. **تحليل الفجوة** **التوصيات:** استخدمت اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة المادة 18 (4) - (5) أساسًا لمشاركة المعلومات التي تدخل ضمن مجال هذه الاتفاقية بشكل تلقائي (مع ضمانات مقدمة حول الاستخدام في الأدلة أو الكشف عن المعلومات الحساسة لطرف ثالث (بما في ذلك دولة أخرى).[295] النظر في التشريعات القائمة على المادة 33 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات أو المادة 26 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست.

292. يقصد بتعبير "جريمة خطيرة" في المادة 2 (ب) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة أي سلوك يمثل جرما يعاقب عليه بالحرمان التام من الحرية لمدة لا تقل عن أربع سنوات أو بعقوبة أشد"

293. المادة 3 (1) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية

294. تُعرّف المادة 2 (أ) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة «الجماعة الإجرامية المنظمة» بأنها جماعة ذات هيكل تنظيمي، مؤلفة من ثلاثة أشخاص أو أكثر، موجودة لفترة من الزمن وتعمل بصورة متضافرة بهدف ارتكاب واحدة أو أكثر من الجرائم الخطيرة أو الأفعال المجرمة وفقا لهذه الاتفاقية، من أجل الحصول، بشكل مباشر أو غير مباشر، على منفعة مالية أو منفعة مادية أخرى"

295. انظر المادة 33 (2) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 32 من اتفاقية بودابست **الوصول عبر الحدود إلى بيانات الحاسوب المخزنة بموافقة أو عندما تكون متاحة للجمهور** يجوز للطرف، دون إذن من طرف آخر: • الوصول إلى بيانات الحاسوب المخزنة (مفتوحة المصدر) المتاحة للجمهور، بغض النظر عن مكان وجود البيانات جغرافيا؛ أو الوصول إلى بيانات الكمبيوتر المخزنة الموجودة لدى طرف آخر أو استلامها، من خلال نظام حاسوب في إقليمها، إذا حصل الطرف على موافقة مشروعة وطوعية من الشخص الذي لديه السلطة القانونية للكشف عن البيانات للطرف من خلال نظام الحاسوب هذا. **القسم 27 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - البرامج الشرعية** 1. إذا كان [القاضي] [قاضي التحقيق] مقتنعًا بناءً على [معلومات مقدمة تحت القَسَم] [شهادة خطية] أنه في سياق تحقيق متعلق بجريمة مدرجة في الفقرة 7 أدناه، توجد أسباب معقولة للاعتقاد بأنه لا يمكن جمع الأدلة الأساسية عن طريق تطبيق أحكام أخرى مدرجة في الجزء الرابع ولكنها ضرورية لأغراض التحقيق الجنائي، فإن [القاضي] [القاضي] [أن] يأذن لضابط [إنفاذ القانون] [الشرطة] بناءً على طلب باستخدام برنامج شرعي عن بعد في مهمة محددة ضرورية للتحقيق وتثبيته في نظام الحاسوب المشتبه به من أجل جمع الأدلة ذات الصلة. يجب أن يحتوي الطلب على المعلومات التالية: • المشتبه في ارتكابه الجريمة، إذا كان ذلك ممكنا مع الاسم والعنوان؛ و • وصف نظام الحاسوب المستهدف؛ و • وصف الوسيلة المقصودة ومدى ومدة الاستخدام؛ أسباب ضرورة الاستخدام.	**لا يوجد معادل**	**التحليل القانوني** تمكن هذه السلطة الإجرائية الدولة من تأمين المحتوى المخزن في دولة أخرى في ظروف محدودة. المادة 32 ب. إن اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست والمادة 40 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات هما استثناء من مبدأ الإقليمية وتسمحان بوصول منفرد عبر الحدود دون الحاجة إلى مساعدة قانونية متبادلة عندما تكون هناك موافقة أو تكون المعلومات متاحة للجمهور. أمثلة على استخدام هذه السلطة الإجرائية بموجب المادة 32 من اتفاقية بودابست تتضمن: قد يتم تخزين البريد الإلكتروني لشخص ما في بلد آخر بواسطة مزود خدمة، أو قد يقوم شخص ما بتخزين البيانات عن قصد في بلد آخر. يجوز لهؤلاء الأشخاص استرداد البيانات بشرط أن يكون لديهم السلطة القانونية التي تخولهم ذلك، ويجوز لهم الكشف طوعًا عن البيانات لموظفي إنفاذ القانون أو السماح لهؤلاء المسؤولين بالوصول إلى البيانات[296] يمكن اعتقال إرهابي مشتبه به بشكل قانوني عندما يكون بريده الإلكتروني، الذي قد يحوي دليلًا على ارتكاب جريمة، مفتوحًا على الجهاز اللوحي أو الهاتف الذكي أو أي جهاز آخر. إذا وافق المشتبه طوعًا على أن تصل الشرطة إلى الحساب وكانت الشرطة واثقة من أن بيانات صندوق البريد موجودة في ولاية أخرى، يجوز للشرطة الوصول إلى البيانات بموجب المادة 32. ب. **تحليل الفجوة** **التوصيات:** تم تضمين هذه السلطة التي تؤمن الأدلة من طرف واحد في التشريعات مع ضمانات الحصول على الموافقة بشكل قانوني من المستخدم.[297] يمكن استخدام لغة المادة 32 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست والمادة 40 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. تم انتقاد المادة 32.ب بشدة، ويمكن اعتبار أن موافقة الدولة حيث تُخزَّن بيانات الكمبيوتر قد تم الحصول عليها بالإضافة إلى المستخدم. ينص القسم 27 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية على البرامج الشرعية وهذا قد يسمح بالوصول إلى جهاز حاسوب في دولة أخرى. هناك عدد من القيود التي تشترط عدم إمكانية الحصول على الأدلة بوسائل أخرى، وتتطلب أمرًا قضائيًا، ويمكن أن تُطبَّق على جرائم معينة فقط ضمن مدة مقيدة (3 أشهر). يجب أيضًا إيلاء الاعتبار لموافقة الدولة الأخرى التي قد يتطفل عليها البرنامج الشرعي.

296. الفقرة 294، الصفحة 53 من التقرير التفسيري لاتفاقية بودابست
297. يجب الانتباه لمواقف مثل عدم وجود المستخدم (في حالة الوفاة) وإذا كان يمكن الحصول على موافقة في دولة أخرى

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
2. من الضروري التأكد في مثل هذا التحقيق من أن التعديلات التي يتم إدخالها على نظام الحاسوب الخاص بالمشتبه به مقصورة على تلك الضرورية للتحقيق وأن أي تغييرات يمكن التراجع عنها إذا أمكن بعد نهاية التحقيق. أثناء التحقيق، من الضروري تسجيل الدخول: - الوسيلة الفنية المستخدمة ووقت وتاريخ التطبيق؛ • تحديد نظام الحاسوب وتفاصيل التعديلات التي تمت خلال التحقيق؛ • أي معلومات تم الحصول عليها. يجب حماية المعلومات التي يتم الحصول عليها عن طريق استخدام هذا البرنامج من أي تعديل أو حذف غير مصرح به أو وصول غير مصرح به. 3. تقتصر مدة الترخيص في القسم 27 (1) على [3 أشهر]. يتم إيقاف الإجراء المتخذ على الفور إذا لم تعد شروط الترخيص مستوفاة. 4. يتضمن ترخيص تثبيت البرنامج الوصول عن بُعد إلى نظام الحاسوب المشتبه به. 5. إذا كانت عملية التثبيت تتطلب الوصول الفعلي إلى مكان ما، يجب استيفاء متطلبات القسم 20. 6. يجوز لضابط [تطبيق القانون] [الشرطة] أن يطلب من المحكمة أن تأمر مقدم خدمة بالمساعدة في عملية التسليم إذا لزم الأمر، وذلك بموجب أمر المحكمة الممنوح في (1) الطلب المذكور أعلاه. 7. [قائمة الجرائم]. 8. قد تقرر دولة عدم تنفيذ القسم 27. **المادة 40 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - الوصول إلى معلومات تقنية المعلومات عبر الحدود** يجوز لأي دولة طرف، وبدون الحصول على تفويض من دولة طرف أخرى: 1. أن تصل إلى معلومات تقنية المعلومات المتوفرة للعامة (مصدر مفتوح) بغض النظر عن الموقع الجغرافي للمعلومات. 2. أن تصل أو تستقبل- من خلال تقنية المعلومات في إقليمها- معلومات تقنية المعلومات الموجودة لدى الدولة الطرف الأخرى وذلك إذا كانت حاصلة على الموافقة الطوعية والقانونية من الشخص الذي يملك السلطة القانونية لكشف المعلومات إلى تلك الدولة الطرف بواسطة تقنية المعلومات المذكورة.		

المغرب[298]

صدقت ووقعت على اتفاقية بودابست في عام 2012

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 2 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست - الوصول غير المشروع[299] يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لتجريم الوصول إلى النظام الكلي أو أي جزء من نظام الكمبيوتر، إذا ارتكب عمدًا، دون أي حق. قد يشترط طرف ما ارتكاب الجريمة عن طريق انتهاك إجراءات أمنية بقصد الحصول على بيانات الكمبيوتر أو نية أخرى غير نزيهة، أو فيما يتعلق بنظام كمبيوتر متصل بنظام كمبيوتر آخر. **المادة 6 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - جريمة الدخول غير المشروع** 1. الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به. 2. تشدد العقوبة إذا ترتب على هذا الدخول أو البقاء أو الاتصال أو الاستمرار بهذا الاتصال: a. محو أو تعديل أو تشويه أو نسخ أو نقل أو محو للبيانات المحفوظة وللأجهزة والأنظمة الالكترونية وشبكات الاتصال وإلحاق الضرر بالمستخدمين والمستفيدين. الحصول على معلومات حكومية سرية. **القسم 4 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الوصول غير القانوني** 1. يعاقب بالسجن لمدة لا تتجاوز [المدة] أو غرامة لا تتجاوز [المبلغ] أو بالعقوبتين كليهما أي شخص يدان بجريمة الوصول إلى نظام حاسوب كله أو جزء منه عن قصد ودون عذر مبرر قانونًا أو بتجاوز لسبب قانوني.	**قانون العقوبات** **المادة 607-3** كل من دخل إلى مجموع أو بعض نظام للمعالجة الآلية للمعطيات عن طريق الاحتيال... ويعاقب بنفس العقوبة من بقي في نظام للمعالجة الآلية للمعطيات أو في جزء منه، كان قد دخله عن طريق الخطأ وهو غير مخول له حق دخوله. تضاعف العقوبة إذا نتج عن ذلك حذف أو تغيير المعطيات المدرجة في نظام للمعالجة الآلية للمعطيات أو اضطراب في سيره. **المادة 607-4** دون الإخلال بالمقتضيات الجنائية الأشد، يعاقب بالحبس من ستة أشهر إلى سنتين وبالغرامة من10,000 إلى 100,000 درهم كل من ارتكب الأفعال المشار إليها في المادة السابقة في حق مجموع أو بعض نظام للمعالجة الآلية للمعطيات يفترض أنه يتضمن معلومات تخص الأمن الداخلي أو الخارجي للدولة أو أسرارًا تهم الاقتصاد الوطني.	**التحليل القانوني** يتضمن الحكم الوطني إشارة إلى «عن طريق الاحتيال"، وهذا يشير إلى أن الجاني قد وصل إلى البيانات بطريقة غير شريفة؛ في حين تشير اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست إلى «بدون حق" وذلك للدلالة على الوصول غير المصرح به. تشير اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست إلى «نية غير شريفة"، لكن هذا المصطلح يشير إلى ذهنية إجرامية وليس إلى العمل على الوصول بشكل غير شرعي. في الوقت الحالي، يمكن ارتكاب هذه الجريمة على المستوى الوطني فقط في حالة كان لدى مرتكب الجريمة غرضًا غير شريف من الوصول. من غير الواضح إن كان تعريف " احتيالي « يستلزم وجود عمل صريح محدد أو إذا كان أي وصول غير قانوني يعتبر احتياليًا. ولهذا السبب يجب تعريف «الاحتيال". تشير اتفاقية الجامعة العربية لمكافحة جرائم تكنولوجيا المعلومات إلى «الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به." دون تحديد ماهية هذه الأفعال، يستحسن لذلك استخدام تعريفات اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست ومواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية. يشير نص الجريمة أيضًا إلى «نظام معالجة البيانات المؤتمتة" دون وجود تعريف له. من غير الواضح ما إذا كان هذا يتعلق بـ «نظام حاسوب" (يعني أي جهاز أو مجموعة من الأجهزة المترابطة أو ذات الصلة، يقوم واحد أو أكثر منها، وفقًا لبرنامج ما، بمعالجة تلقائية للبيانات - المادة 1 من اتفاقية بودابست) أو «البيانات المحوسبة" (أي تمثيل للوقائع أو المعلومات أو المفاهيم في شكل مناسب للمعالجة في نظام الكمبيوتر، بما في ذلك برنامج مناسب لكي يقوم نظام الحاسوب بأداء وظيفة ما - المادة 1 من اتفاقية بودابست) يمكن أن يكون الشكل المشدد للجريمة في المادة 607-4 أوسع ليشمل جميع المصالح الوطنية للدولة مثل الصحة.

298. سيقدم قريبًا مشروع قانون بشأن قانون الإجراءات الجنائية إلى البرلمان المغربي للتصديق عليه؛ يتضمن العناصر الواردة في هذا التقرير في شكل توصيات.
299. المادة 29 (1) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
2. قد تقرر أي دولة عدم تجريم الوصول غير المصرح به بشرط توفر سبل انتصاف فعالة أخرى. علاوة على ذلك، قد يشترط بلد ما ارتكاب الجريمة عن طريق انتهاك الإجراءات الأمنية أو بقصد الحصول على بيانات الحاسوب أو بنية أخرى غير نزيهة. **القسم 5 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الآثار غير القانونية** 1. أي يشخص يظل مسجلاً في نظام حاسوب أو جزء من نظام حاسوب أو يواصل استخدام نظام حاسوب عن قصد ودون عذر أو مبرر قانوني، أو يتجاوز عذرًا أو مبررًا قانونيًا يعاقب عند إدانته بالسجن لمدة لا تتجاوز [المدة]، أو غرامة لا تتجاوز [المبلغ]، أو بالعقوبتين كليهما. 2. قد تقرر أي دولة عدم تجريم الآثار غير المصرح بها فقط، شرط أن تتوفر سبل انتصاف فعالة أخرى. بدلاً من ذلك، قد يشترط البلد ارتكاب الجرم عن طريق انتهاك الإجراءات الأمنية أو بقصد الحصول على بيانات الحاسوب أو بنية أخرى غير نزيهة.		**تحليل الفجوة** **التوصيات:** يمكن أن يتضمن التشريع الوطني الصياغة ذات الصلة من اتفاقية بودابست ومواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية لتشمل تعاريف نظام الحاسوب[300] وإدراج البرامج ضمن تعريف البيانات لأن بعض البيانات تشمل البرامج والبعض الآخر لا تشملها. علاوةً على ذلك، ولكي تتماشى التشريعات مع اتفاقية بودابست ومواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية، ينبغي الإشارة إلى الوصول «بدون حق" بدلاً من عن طريق الغش. يمكن أن يكون الشكل المشدد للجريمة في المادة 607-4 أوسع لمراعاة الوصول غير القانوني إلى بيانات البنية التحتية الحيوية، بدلاً من تلك المتعلقة بالأمن القومي والاقتصاد فقط، انظر القسم 4 (2) من مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية
المادة 3 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[301] **اعتراض غير قانوني** يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وتدابير أخرى لتجريم اعتراض عمليات نقل البيانات الحاسوبية غير العامة من نظام حاسوب وإليه وداخله، بما في ذلك الانبعاثات الكهرومغناطيسية من نظام الحاسوب الذي يحمل مثل هذه البيانات، وذلك عند ارتكاب هذا العمل عمدًا بوسائط تقنية، ويعتبر جريمة جنائية بموجب القانون الداخلي. قد يشترط الطرف أن تكون الجريمة قد ارتكبت بنية غير نزيهة، أو أن تتم ضد نظام حاسوب متصل بنظام حاسوب آخر.	**لا يوجد معادل**	**التحليل القانوني** تعتبر هذه الجريمة أساسية لملاحقة عمليات النقل غير العامة لبيانات الحاسوب إلى نظام حاسوبي أو منه أو داخله، والتي قد يتم اعتراضها بشكل غير قانوني للحصول على معلومات حول موقع الشخص (على سبيل المثال استهداف ذلك الشخص).[302] غالبًا ما تستلزم سرقة الهوية استخدام برامج Keylogger أو أنواع البرمجيات الخبيثة الأخرى للاعتراض غير القانوني لعمليات نقل بيانات الحاسوب غير العامة إلى أو من أو في نظام حاسوب يحتوي على معلومات حساسة مثل معلومات الهوية. يُعتبر تجريم هذا الفعل ضروريًا لمقاضاة عمليات نقل بيانات الحاسوب من وإلى وداخل نظام الحاسوب الذي قد يتم اعتراضه بشكل غير قانوني للحصول على معلومات (مثل wikileaks أو PanamaPapers). الصياغة في المادة 7 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات (الاعتراض غير القانوني) لا يوجد بها تعريف لتعبير «بيانات تكنولوجيا المعلومات"

300. انظر المادة 1.أ. من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست: «أي جهاز أو مجموعة من الأجهزة المترابطة أو ذات الصلة، أو واحد أو أكثر من هذه الأجهزة يقوم بمعالجة البيانات تلقائيًا وفقًا لبرنامج ما" **أو** القسم 3 (5) من مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية: «جهاز أو مجموعة من الأجهزة المترابطة أو ذات الصلة، بما في ذلك الإنترنت، أو واحد أو أكثر من هذه الأجهزة يقوم بمعالجة تلقائية للبيانات أو بأداء أي وظيفة أخرى وفقًا لبرامج ما"

301. المادة 29 (2) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية

302. http://www.coe.int/en/web/cybercrime/guidance-notes

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 7 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست **اعتراض غير قانوني** الاعتراض غير القانوني المتعمد لحركة البيانات بأي وسيلة تقنية، وتعطيل نقل أو استقبال بيانات تكنولوجيا المعلومات. **القسم 6 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - اعتراض غير قانوني** 1. الشخص الذي يتعمد اعتراض الوسائل التقنية دون عذر أو مبرر قانوني أو يتجاوز عذرًا أو مبررًا قانونيًا: • أي نقل غير عام إلى نظام الحاسوب أو منه أو داخله؛ أو • الانبعاثات الكهرومغناطيسية من نظام الحاسوب يعتبر جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين كليهما. 2. قد يشترط البلد ارتكاب الجرم بنية غير شريفة، أو ضد نظام حاسوب متصل بنظام حاسوب آخر أو عن طريق التحايل على إجراءات الحماية المطبقة لمنع الوصول إلى محتوى الإرسال غير العام.		**تحليل الفجوة** **التوصيات:** يمكن استخدام المادة 7 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات مع تعريف «بيانات تكنولوجيا المعلومات" أو المادة 3 من اتفاقية بودابست أو القسم 6 من مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية كدليل للتشريعات الوطنية
المادة 4 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[303] **التشويش على البيانات** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لتمكين سلطاته المختصة من تجريم الأفعال الجنائية، بموجب قوانينه الداخلية، من محو بيانات الحاسوب أو إتلافها أو تغييرها أو حذفها دون حق، وذلك عند ارتكابها عمدًا. 2. يجوز لأي طرف أن يحتفظ بالحق في المطالبة بأن يؤدي السلوك الموصوف في الفقرة 1 إلى ضرر جسيم.	**قانون العقوبات** **المادة 607-6** كل من أدخل معطيات في نظام للمعالجة الآلية للمعطيات أو أتلفها أو حذفها منه أو غير المعطيات المدرجة فيه، أو غير طريقة معالجتها أو طريقة إرسالها عن طريق الاحتيال	**التحليل القانوني** الاستخدام «عن طريق الاحتيال" هو غير متناسقة (تتعارض في الواقع مع) المعيار 4.1 الذي نصت عليه اتفاقية بودابست «... عندما يقوم عن قصد بإتلاف بيانات الكمبيوتر أو حذفها أو محوها أو تغييرها أو العبث بها دون حق" والذي لا يشترط إثبات الاحتيال. يعني ذلك في الأساس أن السلوك الذي يشكل جريمة تدخل في البيانات وفقًا للمادة 4.1 من اتفاقية بودابست لن يتم تجريمه بموجب المادة 607-6 لا تشمل هذه المادة عنصر محو بيانات الحاسوب **تحليل الفجوة** **التوصيات:** استخدم المادة 4 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست أو القسم 7 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية باعتبارهما دليلًا للتشريعات الوطنية

303. المادة 29 (1) (هـ - و) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
القسم 7 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية- التشويش غير القانوني على البيانات الشخص الذي يقوم بأي من الأفعال التالية عمدا ودون عذر أو مبرر قانوني أو يتجاوز عذرًا أو مبررًا قانونيًا: • محو أو إتلاف بيانات الحاسوب؛ أو • يحذف بيانات الحاسوب؛ أو • تغيير بيانات الحاسوب؛ أو • جعل بيانات الحاسوب بلا معنى لها أو غير ذات فائدة أو غير فعالة؛ أو • يعوق أو يقاطع أو يشوش على الاستخدام القانوني لبيانات الحاسوب؛ أو • يعوق أو يقاطع أو يشوش على أي شخص في استخدامه القانوني لبيانات الحاسوب؛ أو • يمنع الوصول إلى بيانات الكمبيوتر لأي شخص مصرح له بالوصول إليها؛ يرتكب جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة] ، أو غرامة لا تتجاوز [المبلغ]، أو بالعقوبتين كليهما. **المادة 8 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست** **جريمة ضد سلامة البيانات** 1. تعمد محو أو حذف أو منع أو تعديل أو إخفاء بيانات تكنولوجيا المعلومات بشكل غير قانوني. 2. قد يطلب أحد الأطراف أن يتسبب الفعل بأضرار جسيمة من أجل تجريم الأفعال المذكورة في الفقرة 1.		
المادة 5 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[304] **التشويش على النظام** يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لتمكين سلطاته المختصة من تجريم الأفعال التالية عند ارتكابها عمداً، بموجب قانونه الداخلي، أية عرقلة خطيرة دون حق لعمل نظام الحاسوب عن طريق إدخال أو نقل أو إتلاف أو حذف أو محو أو تغيير أو كتم بيانات الحاسوب.	**قانون العقوبات** **المادة 5-607** كل من عرقل عمدًا سير نظام للمعالجة الآلية للمعطيات أو أحدث فيه خللاً.	**التحليل القانوني** تجريم هذه الأعمال من شأنه أن يمنع البرامج الضارة التي تتداخل مع عمل جهاز الحاسوب - على سبيل المثال ديدان الكمبيوتر - مجموعة فرعية من البرامج الضارة (مثل فيروسات الكمبيوتر). إنها برامج حاسوب ذاتية النسخ المتماثل تضر بالشبكة من خلال بدء عمليات نقل البيانات المتعددة. يمكن أن تؤثر على أنظمة الحاسوب عن طريق إعاقة التشغيل السلس لنظام الحاسوب، أو استخدام موارد النظام لتكرار نفسها عبر الإنترنت أو توليد حركة مرور في الشبكة يمكن أن تغلق بعض الخدمات (مثل المواقع الإلكترونية) لا تشير المادة 5-607 إلى حدوث «العرقلة أو الخلل عمدًا" بأنه تم "بدون وجه حق"

٣٠٤. لا يوجد ما يعادل المادة ٩٢ (١) (د) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
القسم 9 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - التشويش غير القانوني على النظام 1. الشخص الذي يقوم عن قصد، ودون عذر أو مبرر قانوني، أو بتجاوز عذر أو مبرر قانوني: • أعاقة عمل نظام الحاسوب أو التشويش عليه؛ أو • إعاقة شخص يستخدم أو يشغل بشكل قانوني نظام الحاسوب أو التشويش عليه؛ يعتبر جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين كليهما. 2. يعاقب أي شخص الذي يتعمد دون عذر أو مبرر قانوني، أو بتجاوز عذر قانوني أو مبرر، إعاقة نظام حاسوب مخصص حصريًا لاستخدام عمليات البنية التحتية الحيوية أو التشويش عليه، أو في الحالات التي لا يكون فيها هذا النظام مخصصًا للاستخدام الحصري في عمليات البنية التحتية الحيوية، ولكنه يستخدم في عمليات البنية التحتية الحيوية وتؤثر هذه الإعاقة على استخدام عمليات البنية التحتية الحيوية، بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين كليهما.		علاوةً على ذلك، لا تشير المادة 5-607 إلى أفعال العرقلة أو الخلل عمدًا من خلال «إدخال بيانات حاسوب أو نقلها أو محوها أو حذفها أو إتلافها أو تغييرها أو منعها" وستضمن الإشارة إلى هذه الأفعال أن الجريمة تصف ما تعنيه العرقلة أو الخلل عمدًا. **تحليل الفجوة** **التوصيات:** استخدم صياغة اتفاقية بودبست في المادة 5 بإضافة «العرقلة أو الخلل عمدًا" بدون وجه حق" وأفعال إدخال بيانات حاسوب أو نقلها أو محوها أو حذفها أو إتلافها أو تغييرها أو منعها" ضع في اعتبارك أيضًا ما إذا كان منع الهجمات ضد البنية التحتية الحيوية ومحاكمة مرتكبيها يحتاج إلى جريمة منفصلة أو مشددة، على سبيل المثال، قد يتم عرقلة عمل نظام الحاسوب لأغراض إرهابية (يمكن أن تؤدي عرقلة النظام الذي يخزن سجلات البورصة إلى أن تكون البيانات غير دقيقة، أو أن تعرقل عمل البنية التحتية الحيوية.[305] انظر السابقة في القسم 9 (2) من مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية.
المادة 6 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[306] **سوء استخدام الأجهزة** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لتجريم الأفعال الإجرامية بموجب قوانينه الداخلي، عندما تُرتكب عمداً ودون حق: a. إنتاج أو بيع أو الشراء بغرض الاستخدام أو الاستيراد أو التوزيع أو توفير ما يلي بأية طريقة: i. أي جهاز، بما في ذلك برنامج الحاسوب، تم تصميمه أو تكييفه بشكل أساسي بغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من 2 إلى 5؛	**القانون الجنائي** **المادة 10-607** يعاقب بالحبس من سنتين إلى خمس سنوات وبالغرامة من 50.000 إلى 2.000.000 درهم كل من صنع تجهيزات أو أدوات أو أعد برامج للمعلوماتيات أو أية معطيات أعدت أو اعتمدت خصيصًا لأجل ارتكاب الجرائم المعاقب عليها في هذا الباب أو تملكها أو حازها أو تخلى عنها للغير أو عرضها أو وضعها رهن إشارة الغير.	**التحليل القانوني** ستمكّن تجريم هذه الأفعال من ملاحقة إنتاج وبيع والشراء من أجل الاستخدام واستيراد وتوزيع رموز الوصول والبيانات المحوسبة الأخرى المستخدمة في ارتكاب جرائم الإنترنت. - على سبيل المثال، يمكن الوصول إلى أنظمة الحاسوب لتسهيل أي هجوم إرهابي بالتدخل في شبكة الطاقة الكهربائية للبلد. كما ذكر أعلاه للوصول غير المشروع، لا توجد إشارة إلى عبارة «بدون حق" أو قصد - يتوافق قصد ارتكاب الجريمة مع التعديلات المقترحة على الجرائم السابقة وأيضًا حيثما يكون القصد منصوص عليه بالفعل في المادة 5-607 لا تجرِّم المادة 10-607 على وجه التحديد أعمال «البيع أو الشراء بغرض الاستخدام أو الاستيراد أو التوزيع" - على الرغم من وجود أمر بالتصرف بطريقة أخرى.

305. seton-ecnadiug/emircrebyc/http://www.coe.int/en/web
306. المادة 9 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات والمادة 29 (1) (ح) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
ii. كلمة مرور الحاسوب أو رمز الوصول أو البيانات المماثلة التي يمكن من خلالها الوصول إلى نظام الحاسوب كله أو جزء منه، بقصد استخدامه لغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من 2 إلى 5؛ و حيازة عنصر مشار إليه في الفقرتين أ.1 أو 2 أعلاه، بقصد استخدامه لغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من 2 إلى 5. يجوز لأي طرف أن يشترط بموجب القانون امتلاك عدد من هذه العناصر قبل إسناد المسؤولية الجنائية. 2. لا يجوز تفسير هذه المادة على أنها تفرض مسؤولية جنائية عندما لا يكون الغرض من الإنتاج أو البيع أو الشراء بغرض الاستخدام أو الاستيراد أو التوزيع أو التوفير أو الحيازة المشار إليها في الفقرة 1 من هذه المادة بقصد استخدامها لغايات ارتكاب أي من الجرائم المذكورة في المادة 2 إلى المادة 5 من هذه الاتفاقية، مثل الاختبارات المسموح بها أو حماية نظام الحاسوب. 3. يجوز لكل طرف أن يحتفظ بالحق في عدم تطبيق الفقرة 1 من هذه المادة، شريطة ألاّ يتعلق التحفظ ببيع أو توزيع أو توفير المواد المشار إليها في الفقرة 1 أ (2) من هذه المادة بطريقة أخرى. **القسم 10 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الأجهزة غير القانونية** 1. يرتكب الشخص جريمة إذا: a. أنتج أو باع أو اشترى بغرض الاستخدام أو استورد أو صدّر أو وزع أو وفّر بأي طريقة، عن قصد ودون عذر أو مبرر قانوني أو بتجاوز عذر أو مبرر قانوني: i. جهاز، بما في ذلك برنامج حاسوب، تم تصميمه أو تكييفه بغرض ارتكاب جريمة محددة بموجب أحكام أخرى من الجزء الثاني من هذا القانون؛ أو		لا توجد إشارة إلى كلمة مرور الحاسوب أو رمز الوصول أو البيانات المماثلة التي يمكن من خلالها الوصول إلى نظام الحاسوب كله أو جزء منه، بقصد استخدامه لغرض ارتكاب أي جريمة من الجرائم السيبرانية. ومن شأن هذا الإدراج أن يضمن أن هذا السلوك الإجرامي محدد بوضوح. تنص المادة 2.6 من اتفاقية بودابست على عذر معقول إذا كان الفعل المتعمد لغرض «الاختبارات المسموح بها أو حماية نظام الحاسوب". وسيضمن ذلك ألا تكون وكالات إنفاذ القوانين مسؤولة عن هذه الجريمة (انظر أيضًا القسم 10 (2) من مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية) يرجى ملاحظة أن مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية توفر خيار إدراج الأجهزة في جدول إذا كان ذلك مناسبًا - قد يكون هذا تقييدًا ويتطلب تحديثًا يتوافق مع التقدم التكنولوجي. **تحليل الفجوة** **التوصيات:** استخدام صياغة مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية في القسم 10 أو صياغة اتفاقية بودابست في المادة 6 بإضافة عبارة «بدون حق" والقصد لارتكاب هذه الجريمة - كما يجب مراعاة تحديد استخدام كلمات المرور ورموز الوصول. يجب أن توفر المادة عذرًا معقولاً حتى تتمكن وكالات إنفاذ القوانين من استخدام الأجهزة لتقنيات التحقيق الخاصة - ويمكن استخدام الصياغة في المادة 2.6 كدليل.

الجرائم		
أفضل الممارسات الدولية	**التشريع الوطني**	**ملاحظات**
ii. كلمة مرور الحاسوب أو رمز الوصول أو البيانات المماثلة التي يمكن من خلالها الوصول إلى نظام الحاسوب كله أو جزء منه؛ بقصد استخدامه من قبل أي شخص لغرض ارتكاب جريمة محددة بموجب أحكام أخرى من الجزء الثاني من هذا القانون؛ أو كان في حوزته غرض مشار إليه في الفقرة الفرعية «1» أو «2»، وكان القصد هو استخدامه من قبل أي شخص لارتكاب جريمة محددة بموجب أحكام أخرى من الجزء الثاني من هذا القانون، فإنه يعاقب عند إدانته بارتكاب هذه الجريمة بالسجن لمدة لا تزيد عن [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً. 2. لا يجوز تفسير هذا الحكم على أنه يفرض مسؤولية جنائية عندما لا يكون الغرض من الإنتاج أو البيع أو الشراء للاستخدام أو الاستيراد أو التوزيع أو التوفير أو الحيازة المشار إليها في الفقرة 1 هو ارتكاب جريمة منصوص عليها وفقًا لأحكام أخرى من الجزء الثاني من هذا القانون، كأن تكون الأغراض مثل الاختبار أو الحماية المعتمدين لنظام الحاسوب. 3. قد يقرر بلد ما عدم تجريم الأجهزة غير القانونية أو قصر التجريم على الأجهزة المدرجة في الجدول.		
المادة 7 من اتفاقية بودابست **أعمال التزوير المرتبطة بالحاسوب** يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم إدخال بيانات الحاسوب أو تغييرها أو حذفها أو محوها، عند ارتكاب ذلك عن قصد وبدون حق، مما يؤدي إلى بيانات غير موثوقة بهدف أن يتم التعامل معها أو التصرف فيها لأغراض قانونية كما لو كانت أصلية، بصرف النظر عما إذا كانت البيانات قابلة للقراءة ومقروءة مباشرة أم لا. قد يطلب طرف ما وجود نية الاحتيال، أو نية غير شريفة مماثلة، قبل إسناد المسؤولية الجنائية.	**القانون الجنائي** **المادة 7-607** دون الإخلال بالمقتضيات الجنائية الأشد، يعاقب كل من زور أو زيف وثائق الحاسوب أيًا كان شكلها إذا كان من شأن التزوير أو التزييف إلحاق ضرر بالغير.	**التحليل القانوني** كما ذكر أعلاه للوصول غير المشروع، لا توجد إشارة إلى عبارة «بدون حق" أو قصد - يتوافق قصد ارتكاب الجريمة مع التعديلات المقترحة على الجرائم السابقة وأيضًا حيثما يكون القصد منصوص عليه بالفعل في المادة 5-607 لا يوجد تعريف لعبارة «وثائق الحاسوب" تتطلب المادة 7-607 وجود الضرر، في حين أن النهج المتبع في المادة 7 هو القصد دون تصريح إدخال معطيات الحاسوب أو تغييرها أو حذفها أو تبديلها بمعطيات مزيفة، بغرض التعامل معها كما لو كانت معطيات حقيقية. وليس هناك أي شرط يستلزم وقوع الضرر أو الخسارة على شخص آخر. وقد يقيد هذا الشرط الإضافي بموجب المادة 7-607 عدد الملاحقات القضائية الناجحة حيث قد تكون هناك حالات لا يوجد فيها أي ضرر ناتج عن قصد القيام بذلك. فعلى سبيل المثال، يتم توزيع عبارة مزورة بعنوان غير صحيح لمحدد موقع الموارد المُوحّد في عملية التصيُّد الاحتيالي الموجَّه، لكن المستخدم لا يتصرف بناءً عليها، ولا يتسبب في حدوث أي ضرر.

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
القسم 11 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - أعمال التزوير المتعلقة بالحاسوب 1. كل شخص يقوم عن قصد ودون عذر أو مبرر قانوني أو بتجاوز عذر قانوني أو مبرر، بإدخال أو تبديل أو حذف أو منع بيانات الحاسوب، مما ينتج عنه بيانات غير موثوقة بقصد التعامل معها أو التصرف فيها لأغراض قانونية كما لو كانت صحيحة، بصرف النظر عما إذا كانت البيانات قابلة للقراءة مباشرة أم لا، يعاقب عند الإدانة بهذه الأعمال بالسجن لمدة لا تزيد عن [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً. 2. تكون العقوبة إذا ارتكبت الجريمة المذكورة أعلاه عن طريق إرسال رسائل بريد إلكتروني متعددة من أنظمة الحاسوب أو من خلالها هي السجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً. **المادة 10 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات** **جريمة التزوير** يعني استخدام تقنية المعلومات تغيير حقيقة البيانات بطريقة تسبب الضرر بغرض استخدامها كبيانات حقيقية. **المادة 29 (2)(ب) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية** تعمد إدخال بيانات الحاسوب أو تغييرها أو حذفها أو منعها، مما يؤدي إلى بيانات غير موثوقة بقصد التعامل معها أو التصرف فيها لأغراض قانونية كما لو كانت أصلية، بصرف النظر عما إذا كانت البيانات قابلة للقراءة أو واضحة بشكل مباشر أم لا. يجوز للطرف أن يشترط النية للاحتيال، أو نية غير شريفة مماثلة، قبل إسناد المسؤولية الجنائية		**تحليل الفجوة** **التوصيات:** تم تقديم تعريف لعبارة «وثائق الحاسوب" والنظر في الاستعاضة عنها بعبارة "بيانات الحاسوب" على النحو المحدد في المادة 1 ب. من اتفاقية بودابست إدراج عبارة «بدون حق" والقصد لارتكاب الجريمة - ينبغي النظر فيما إذا كان هذا القصد غير شريف من عدمه. مراجعة ما إذا كان الضرر يجب أن يكون ركنًا من أركان الجريمة - من الأفضل عدم استخدام عبارة الضرر حتى يتم ارتكاب التزوير بمجرد إنشاء البيانات غير الموثوقة والنظر فيها. وقد يعني هذا أنه في حالة إرسال رابط مزور أو وثيقة مزورة كجزء من عملية تصيد احتيالي، تكون الجريمة مكتملة بمجرد نظر المستلم فيها (أي يفتح البريد الإلكتروني الذي يحتوي على الرابط أو يفتح الوثيقة المرفقة) - بدلاً من الاضطرار إلى إثبات وقوع أي ضرر على المستلم

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 8 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[307] **أعمال الاحتيال المرتبطة بالحاسوب** يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لتمكين سلطاته المختصة من تجريم الأفعال الجنائية بموجب قوانينه الداخلية، عند ارتكابها عمدًا ودون حق، التسبب في فقدان الممتلكات للغير عن طريق: أي إدخال أو تغيير أو حذف أو إلغاء لبيانات الحاسوب، أي تدخل في عمل نظام الحاسوب، مع نية احتيال أو نية غير شريفة من أجل الحصول، دون حق، على منفعة اقتصادية لنفسه أو لشخص آخر. **القسم 12 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الاحتيال المرتبط بالحاسوب** الشخص الذي يتسبب في فقدان الممتلكات لشخص آخر، عن قصد، ودون عذر أو مبرر قانوني أو بتجاوز عذر أو مبرر قانوني، وذلك عن طريق: • أي إدخال أو تغيير أو حذف أو إلغاء لبيانات الحاسوب؛ • أي تدخل في عمل نظام الحاسوب، بقصد احتيالي أو غير شريف للحصول، دون حق، على منفعة اقتصادية لنفسه أو لشخص آخر، وتكون عقوبة هذه الأعمال السجن لمدة لا تتجاوز [المدة] ، أو غرامة لا تتجاوز [المبلغ]، أو العقوبتين معاً.	**القانون الجنائي** **المادة 6-607** يعاقب بالحبس من سنة إلى ثلاث سنوات وبالغرامة من 10.000 إلى 200.000 درهم أو بإحدى هاتين العقوبتين فقط كل من أدخل معطيات في نظام للمعالجة الآلية للمعطيات أو أتلفها أو حذفها منه أو غير المعطيات المدرجة فيه، أو غير طريقة معالجتها أو طريقة إرسالها عن طريق الاحتيال **ظهير شريف رقم 1-09-15 صادر في 22 من صفر 1430 (18 فبراير 2009) بتنفيذ القانون رقم 08-09 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي** **المادة 54** يعاقب بالحبس من 3 أشهر إلى سنة وبغرامة من 20.000 درهم إلى 200.000 درهم، كل من قام بخرق أحكام (أ) و (ب) و (ج) من المادة 3 من هذا القانون بجمع معطيات ذات طابع شخصي بطريقة تدليسية أو غير نزيهة أو غير مشروعة، أو أنجز معالجة لأغراض أخرى غير تلك المصرح بها أو المرخص لها، أو أخضع المعطيات المذكورة لمعالجة لاحقة متعارضة مع الأغراض المصرح بها أو المرخص لها. **المادة 61** يعاقب بالحبس من ستة أشهر إلى سنة وبغرامة من 20.000 إلى 300.000 درهم أو بإحدى هاتين العقوبتين فقط، كل مسؤول عن معالجة وكل معالج من الباطن وكل شخص، بالنظر إلى مهامه مكلف بمعالجة معطيات ذات طابع شخصي، يتسبب أو يسهل، ولو بفعل الإهمال، الاستعمال التعسفي أو التدليسي للمعطيات المعالجة أو المستلمة، أو يوصلها لأغيار غير مؤهلين. زيادة على ذلك يمكن للمحكمة أن تقضي بحجز المعدات المستعملة في ارتكاب هذه المخالفة، وكذا بمسح كل المعطيات ذات الطابع الشخصي موضوع المعالجة التي أدت إلى ارتكاب المخالفة، أو جزء منها.	**التحليل القانوني** في حين أن عبارة «عن طريق الاحتيال" في هذا السياق تمنح درجة معينة من الحماية، فإن عدم وجود الفعل الإجرامي لارتكاب هذا السلوك دون تصريح مفقود وقد يؤدي ذلك إلى عدم اليقين. لا يوجد تعريف لعبارة «المعطيات" أو "نظام للمعالجة الآلية للمعطيات" وقد يؤدي ذلك إلى عدم اليقين. يمكن أن تجرِّم المادتان 54 و 61 نشر المعطيات ذات الطابع الشخصي. ولن تجرِّم هاتان المادتان اختراق المعطيات ذات الطابع الشخصي بفعل الإهمال، مثل سوء وضع المعطيات أو إرسالها عن غير قصد إلى مرسل إليه غير صحيح. وعلى الرغم من أن المادة 61 تشير إلى فعل الإهمال، فقد يتم الكشف عن المعطيات لغرض احتيالي لإثبات الجريمة. **تحليل الفجوة** **التوصيات:** توفير تعاريف لعبارات «المعطيات" و"نظام للمعالجة الآلية للمعطيات"، بما في ذلك "بدون حق" في المادة 6-607. اللغة المتعلقة بهذه الجريمة في اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست أو اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية لهذه الجريمة هي دليل جيد للتشريع الوطني

307. المادة 11 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات والمادة 29 (2) (د) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 9 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[308] **الجرائم ذات الصلة بالمحتوى (مثل المواد الإباحية للأطفال)** 1. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم السلوك التالي في قوانينه المحلية، عندما يرتكب عمدا وبدون حق: • إنتاج مواد إباحية للأطفال بغرض توزيعها من خلال نظام حاسوب؛ • عرض أو إتاحة مواد إباحية للأطفال من خلال نظام الحاسوب؛ • توزيع أو نقل المواد الإباحية للأطفال من خلال نظام الحاسوب؛ • شراء مواد إباحية للأطفال من خلال نظام حاسوب بقصد الاستخدام الشخصي أو لإعطائها لشخص آخر؛ • امتلاك مواد إباحية للأطفال في نظام حاسوب أو على وسائط تخزين بيانات الحاسوب. 2. لأغراض الفقرة 1 أعلاه، يجب أن يشمل مصطلح «استغلال الأطفال في المواد الإباحية» أية مواد إباحية تصور بصريًا: • قاصر مشترك في سلوك جنسي صريح؛ شخص يبدو أنه قاصر يشارك في سلوك جنسي صريح؛ • صور واقعية تمثل قاصرًا مشاركًا في سلوك جنسي صريح. 3. لأغراض الفقرة 2 أعلاه، يشمل مصطلح «القاصر» جميع الأشخاص الذين تقل أعمارهم عن 18 عامًا. ومع ذلك، يجوز لأي طرف أن يطلب حدًا أدنى للسن، لا يقل عن 16 عامًا. 4. يجوز لكل طرف أن يحتفظ بالحق في عدم تطبيق الفقرات الفرعية 1، (د) و (ه) ، و 2، الفقرتين الفرعيتين (ب) و (ج) كليًا أو جزئيًا. **القسم 13 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية- المواد الإباحية للأطفال** 1. الشخص الذي يقوم عن قصد ودون عذر أو مبرر قانوني بـ: • إنتاج مواد إباحية للأطفال بغرض توزيعها من خلال نظام حاسوب؛	**القانون الجنائي** **المادة 503 - 2** يعاقب كل من حرض أو شجع أو سهل استغلال أطفال تقل سنهم عن ثمان عشرة سنة في مواد إباحية، وذلك بإظهار أنشطة جنسية بأية وسيلة كانت سواء أثناء الممارسة الفعلية أو بالمحاكاة أو المشاهدة أو أي تصوير للأعضاء الجنسية للأطفال يتم لأغراض ذات طبيعة جنسية... تطبق نفس العقوبة على كل من قام بإنتاج أو توزيع أو نشر أو استيراد أو تصدير أو عرض أو بيع أو حيازة مواد إباحية من هذا النوع. يعاقب على هذه الأفعال حتى لو ارتكبت عناصرها خارج المملكة.	**التحليل القانوني** تجريم هذه الأعمال يعتبر أساسيًا من أجل حماية الأطفال من الأذى، وذلك من خلال تجريم توزيع الصور غير اللائقة للأطفال ونقلها وتوفيرها وعرضها وحيازتها. لا تشير المادة 503-2 على وجه التحديد إلى أي من أفعال «الإنتاج أو التوزيع أو النشر أو الاستيراد أو التصدير أو العرض أو البيع " التي تتم من خلال نظام الحاسوب أو الشبكة أو وسائط التخزين على الحاسوب. في حين تُوفر الحماية بواسطة مرجع خارج الحدود الإقليمية، فإن النص على استخدام نظام الحاسوب سيوفر خصوصية أي عنصر يتم ارتكابه سواء داخل المملكة أو خارجها. كما تشير المادة 1.9 إلى الأفعال التالية التي لم تُدرج في المادة 503-2 وهي «عرض أو توفير مواد إباحية يظهر فيها أطفال من خلال نظام حاسوب" أو شراء مواد إباحية يظهر فيها أطفال من خلال نظام حاسوب لاستخدامه الشخصي أو لإعطائها لشخص آخر"، **تحليل الفجوة** **التوصيات:** تم توسيع نطاق الأفعال المنصوص عليها في المادة 503-2 لتشمل «عرض أو توفير مواد إباحية يظهر فيها أطفال من خلال نظام حاسوب" أو شراء مواد إباحية يظهر فيها أطفال من خلال نظام حاسوب لاستخدامه الشخصي أو لإعطائها لشخص آخر"، (انظر المادة 1.9 (ب) من اتفاقية بودابست) تشير المادة 503-2 على وجه التحديد إلى الأفعال التي يتم تنفيذها من خلال نظام حاسوب أو شبكة أو جهاز تخزين - انظر القسم 13 من مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية

308. المادة 12 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات والمادة 29 (3) (أ-ج) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية

الجرائم		
أفضل الممارسات الدولية	**التشريع الوطني**	**ملاحظات**
• تقدم أو توفر مواد إباحية للأطفال من خلال نظام حاسوب؛ • توزيع أو نقل المواد الإباحية عن الأطفال من خلال نظام حاسوب؛ • شراء و/ أو الحصول على مواد إباحية للأطفال من خلال نظام حاسوب لاستخدامه الشخصي أو لإعطائها لشخص آخر ؛ • حيازة مواد إباحية للأطفال في نظام حاسوب أو على وسائط تخزين بيانات الحاسوب؛ أو • الوصول عمدًا، من خلال تكنولوجيا المعلومات والاتصالات، إلى المواد الإباحية عن الأطفال، ، يعتبر جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً. 2. يمكن الدفاع أمام تهمة بجريمة منصوص عليها في الفقرة (1) (ب) إلى (1) (و) إذا أثبت الشخص أن المواد الإباحية عن الأطفال كانت بغرض إنفاذ القانون بحسن نية. 3. لا يجوز لدولة ما أن تجرم السلوك الموصوف في القسم 13 (1) (د) - (و).		
المادة 10 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[309] **انتهاك حقوق النشر**	**ظهير شريف رقم 1-00-20 صادر في 9 ذي القعدة 1420 (15فبراير 2000) بتنفيذ القانون رقم 2-00 المتعلق بحقوق المؤلف والحقوق المجاورة** **المادة 64**	هذه الصياغة كافية
المادة 11 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[310] **المساعدة والتحريض** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لتجريم الأفعال التالية بموجب قانونه الداخلي، وذلك عندما يتم التحريض على ارتكاب أي من الجرائم المقررة وفقا للمواد من 2 إلى 10 من هذه الاتفاقية أو المساعدة عليها عمدًا، مع نية أن ترتكب هذه الجريمة. 2. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وتدابير أخرى لتجريم محاولة ارتكاب أي من الأفعال الإجرامية المنصوص عليها في المواد من 3 إلى 5 و 7 و 8 و 1.9 (أ) و (ج) من هذه الاتفاقية عمدًا.	**القانون الجنائي** **المادتان 114 و 129**	**التحليل القانوني** تعتبر مساعدة الآخرين وتحريضهم على ارتكاب جرائم أمرًا ضروريًا لمحاكمة أولئك الذين يكونون قد قدموا المساعدة أو شجعوا على ارتكاب جرائم الإنترنت. **في حالة المساعدة على ارتكاب الجرائم السيبرانية أو التحريض عليها، تنطبق القواعد العامة الواردة في المادة 129 من القانون الجنائي.** **تنص المادة 114 على محاولات ارتكاب جرائم جنائية.**

309. ليس هنالك معادل للمادة 17 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية
٣١٠. المادة ٩٢ (٢) (و) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 19 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - محاولة ارتكاب الجرائم والاشتراك فيها 1. الاشتراك في ارتكاب أية جريمة من الجرائم المنصوص عليها في هذا الفصل مع وجود نية ارتكاب الجريمة في قانون الدولة الطرف. 2. الشروع في ارتكاب الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية. 3. يجوز لأي دولة طرف الاحتفاظ بحقها في عدم تطبيق الفقرة الثانية من هذه المادة كليا أو جزئيا.		
المادة 12 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[311] **مسؤولية الشركات** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وتدابير أخرى لضمان أن الأشخاص الاعتباريين يمكن اعتبارهم مسؤولين عن أي جريمة جنائية منشأة وفقًا لهذه الاتفاقية، إذا ارتكبها أي شخص طبيعي لصالحهم، سواء كان ذلك بصفته الفردية أو باعتباره جزءًا من جهاز الشخص الاعتباري، أو باعتباره شخصًا قياديًا ضمن تنظيم الشخص الاعتباري، بناءً على: • سلطة تمثيل الشخص الاعتباري؛ سلطة اتخاذ القرارات نيابة عن الشخص الاعتباري؛ سلطة ممارسة السيطرة داخل الشخص الاعتباري. 2. بالإضافة إلى الحالات المنصوص عليها بالفعل في الفقرة 1 من هذه المادة، يتخذ كل طرف الإجراءات اللازمة لضمان أن يتحمل الشخص الاعتباري المسؤولية عندما يكون عدم الإشراف أو السيطرة من قبل أي شخص طبيعي مشار إليه في الفقرة 1 قد جعل من الممكن ارتكاب جريمة جنائية منصوص عليها بموجب هذه الاتفاقية لصالح ذلك الشخص الاعتباري من قبل شخص طبيعي يعمل تحت سلطته. 3. مع مراعاة المبادئ القانونية للطرف، قد تكون مسؤولية الشخص الاعتباري جنائية أو مدنية أو إدارية. 4. تكون هذه المسؤولية دون المساس بالمسؤولية الجنائية للأشخاص الطبيعيين الذين ارتكبوا الجريمة.	**لا يوجد معادل**	**التحليل القانوني** هذا الحكم هو عنصر أساسي بحيث يستطيع الأشخاص الاعتباريون (مثلًا الكيانات التجارية) التصرف نيابة عن الأشخاص الطبيعيين الذين تقع عليهم مسؤولية جنائية **تحليل الفجوة** **التوصيات:** استخدم لغة اتفاقية بودابست في المادة 12 باعتبارها دليلًا للتشريعات الوطنية

311. المادة 20 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، والمادة 30 (2) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
البروتوكول الإضافي لاتفاقية الجريمة السيبرانية، المتعلق بتجريم أعمال العنصرية وكراهية الأجانب المرتكبة من خلال أنظمة الحاسوب، المادة 3[312] - نشر المواد التي تحض على العنصرية وكراهية الأجانب من خلال أنظمة الحاسوب يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم السلوك التالي في قوانينه المحلية، عندما يرتكب عمداً وبدون حق: 1. توزيع المواد العنصرية وكراهية الأجانب أو إتاحتها للجمهور من خلال نظام الحاسوب. 2. يجوز لأي طرف أن يحتفظ بالحق في عدم إسناد المسؤولية الجنائية للسلوك على النحو المحدد في يجوز للطرف أن يحتفظ بالحق في عدم إسناد المسؤولية الجنائية بالتصرف على النحو المحدد في الفقرة 1 من هذه المادة، عندما تحض المواد الموزعة، كما هو محدد في الفقرة 1 من المادة 2، وتشجع على التمييز غير المرتبط بالكراهية أو العنف، شريطة أن تتوفر سبل انتصاف فعالة أخرى. 3. بصرف النظر عن الفقرة 2 من هذه المادة، يجوز للطرف أن يحتفظ بالحق في عدم تطبيق الفقرة 1 على حالات التمييز، لأن هذه الفقرة لا يمكن أن تمثل سبل انتصاف فعالة على النحو المشار إليه الفقرة 2، وذلك بسبب مبادئ ثابتة في نظامه القانوني الوطني متعلقة بحرية التعبير.	**لا يوجد معادل**	**التحليل القانوني** لا تتضمن المادة 3 (1) (ه) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية، التي تتضمن إنشاء وتنزيل مواد متعلقة بدافع العنصرية وكراهية الأجانب من نظام حاسوبي بدلاً من مجرد نشر أو إتاحة مثل هذه المواد، القصد أو عبارة «بدون حق" - وتُفضل صياغة اتفاقية بودابست. **تحليل الفجوة** **التوصيات:** استخدم لغة اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست في المادة 3 من البروتوكول الإضافي كدليل للتشريعات الوطنية
البروتوكول الإضافي - المادة 4[313] - التهديد بدافع العنصرية وكراهية الأجانب يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم السلوك التالي في قوانينه المحلية، عندما يرتكب عمداً وبدون حق: التهديد، من خلال نظام الحاسوب، بارتكاب جريمة جنائية خطيرة على النحو المحدد في قانونها الداخلي، (1) ضد أشخاص لسبب أنهم ينتمون إلى جماعة يميزها عرقها أو لونها أو نسبها أو أصلها القومي أو العرقي أو دينها، إذا تم استخدام أي من هذه العوامل ذريعةً، أو (2) ضد مجموعة من الأشخاص تتميز بأي من هذه الخصائص.	**لا يوجد معادل**	**تحليل الفجوة** **التوصيات:** استخدم لغة اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست في المادة 4 من البروتوكول الإضافي كدليل للتشريعات الوطنية

312. المادة 29 (3) (ه) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية لا يوجد ما يعادلها في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات
313. المادة 29 (3) (و) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية لا يوجد ما يعادلها في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
بروتوكول إضافي **المادة 5[314] - الإهانة بدافع العنصرية وكراهية الأجانب** يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم السلوك التالي في قوانينه المحلية، عندما يرتكب عمدا وبدون حق: إهانة الجمهور، من خلال نظام حاسوبي، (1) الأشخاص لكونهم ينتمون إلى مجموعة يميزها عرقها أو لونها أو نسبها أو أصلها القومي أو العرقي أو دينها، إذا تم استخدام أي من هذه العوامل ذريعةً؛ أو (2) مجموعة من الأشخاص تتميز بأي من هذه الخصائص. يجوز للطرف إما: أن يشترط أن يكون للجريمة المشار إليها في الفقرة 1 من هذه المادة أثر على أن الشخص أو مجموعة الأشخاص المشار إليهم في الفقرة 1 والذين يتعرضون للكراهية أو الاحتقار أو السخرية؛ أو أن يحتفظ بالحق في عدم تطبيق الفقرة 1 من هذه المادة بشكل كلي أو جزئي.	**لا يوجد معادل**	**تحليل الفجوة** **التوصيات:** استخدم لغة اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست في المادة 5 من البروتوكول الإضافي كدليل للتشريعات الوطنية
بروتوكول إضافي **المادة 6[315] - إنكار الإبادة الجماعية أو التقليل منها أو الموافقة عليها أو تبريرها** **جرائم ضد الإنسانية** يعتمد كل طرف ما قد يلزم من إجراءات تشريعية لجعل الأفعال التالية يعتبر جرائم جنائية بموجب قوانينها الداخلية، عندما تُرتكب عمداً وبدون حق: 1. توزيع أو توفير عبر نظام الحاسوب بأية طريقة من الطرق للجمهور، مواد تنكر أو تقلل أو تقر أو تقلل بشكل كبير الأفعال التي تشكل إبادة جماعية أو جرائم ضد الإنسانية، على النحو المحدد في القانون الدولي والمعترف بها على هذا النحو في القرارات النهائية والملزمة للمحكمة العسكرية الدولية، المنشأة بموجب اتفاقية لندن المؤرخة في 8 أغسطس 1945، أو أي محكمة دولية أخرى تنشأ بموجب المواثيق الدولية ذات الصلة والتي يعترف هذا الطرف باختصاصها القضائي. يجوز لأي طرف		

314. المادة 29 (3) (ز) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية لا يوجد ما يعادلها في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات
315. المادة 29 (3) (ح) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية لا يوجد ما يعادلها في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

الجرائم		
أفضل الممارسات الدولية	**التشريع الوطني**	**ملاحظات**
2. أن يشترط أن يكون الإنكار أو التقليل إلى الحد الأدنى المشار إليه في الفقرة 1 من هذه المادة قد ارتكب بهدف التحريض على الكراهية أو التمييز أو العنف ضد أي فرد أو مجموعة من الأفراد على أساس العرق أو اللون أو النسب أو الأصل القومي أو العرقي أو الدين أو إذا استخدمت هذه العوامل ذريعة لذلك، أو أن يحتفظ بالحق في عدم تطبيق الفقرة 1 من هذه المادة بشكل كلي أو جزئي.	**لا يوجد معادل**	**تحليل الفجوة** **التوصيات:** استخدم لغة اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست في المادة 6 من البروتوكول الإضافي كدليل للتشريعات الوطنية
جرائم إضافية للمراجعة		
الجرائم المتعلقة بالهوية **القسم 14 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية** يعاقب الشخص الذي يقوم عن قصد ودون عذر أو مبرر قانوني، أو يتجاوز عذرًا قانونيًا أو مبررًا باستخدام نظام حاسوب في أي مرحلة من مراحل الجريمة بنقل أو تملك أو استخدام وسيلة لتحديد الهوية شخص آخر بنية ارتكاب أي نشاط غير قانوني يشكل جريمة أو المساعدة أو التحريض عليها، عند إدانته بهذه الأعمال بالسجن لمدة لا تتجاوز [المدة] أو بغرامة لا يتجاوز [المبلغ]، أو بالعقوبتين معاً.		**التحليل القانوني** تغطي هذه الجريمة مرحلة التحضير لجريمة خيانة الأمانة المتعلقة بالهوية **تحليل الفجوة** **التوصيات:** يستحسن أن تدرج في التشريعات المحلية.
الكشف عن تفاصيل التحقيق **القسم 16 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية** موفر خدمة الإنترنت الذي يتلقى أمرًا يتعلق بتحقيق جنائي ينص صراحةً على الحفاظ على السرية أو على التزام شبيه ينص عليه القانون، ثم يقوم عن عمد ودون عذر أو مبرر قانوني أو بتجاوز لعذر قانوني مبرر، بالإفصاح عن: • حقيقة أنه قد تم إصدار أمر؛ أو • أي شيء تم تنفيذه بموجب الأمر؛ أو • أي بيانات تم جمعها أو تسجيلها بموجب الطلب؛ يعتبر جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً.		**التحليل القانوني** يعاقب على اختراق البيانات والكشف عن المعلومات الحساسة التي يمكن أن تؤثر على التحقيقات الجنائية **تحليل الفجوة** **التوصيات:** يستحسن أن تدرج في التشريعات المحلية.

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
عدم السماح بالمساعدة **القسم 17 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية** أي شخص آخر غير المشتبه فيه فشل عمداً دون عذر أو مبرر قانوني أو بتجاوز عذر أو مبرر قانوني، بمساعدة شخص أو السماح بمساعدته، بناءً على أمر مثلما تحدد المواد 20 إلى 22[316] يرتكب جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة] ، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً. قد يقرر أي بلد عدم تجريم عدم السماح بالمساعدة شرط أن تتوفر سبل انتصاف فعالة أخرى.		**التحليل القانوني** تتعلق هذه الجريمة بالأشخاص الذين لديهم معرفة محددة بالأدلة ذات الصلة والذين يرفضون تقديم المساعدة. غالبًا ما يعتمد تطبيق القانون على هؤلاء الأشخاص لتأمين الأدلة في التحقيقات الإلكترونية. هنالك مخالفة مستقلة وهي عدم توفير كلمات مرور أو الوصول إلى الرموز للأجهزة المشفرة أو البيانات (مثل "مفتاح المعلومات المحمية") - ينص القسم 53 من قانون تنظيم سلطات التحقيق في المملكة المتحدة لعام 2000 (RIPA) [317] على وجود جرم جنائي يتحمله الأشخاص الذين لا يمتثلون للمادة 49 من إخطار RIPA والقاضية بالكشف عن «المفتاح" **تحليل الفجوة** **التوصيات:** يستحسن أن تدرج في التشريعات المحلية.
المطاردة السيبرانية **القسم 18 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية** الشخص الذي يقوم، دون عذر أو مبرر قانوني، أو يتجاوز عذرًا قانونيًا أو مبررًا، ببدء أي اتصال إلكتروني، بقصد إكراه شخص ما أو تخويفه أو مضايقته أو التسبب في ضائقة عاطفية كبيرة له، باستخدام نظام حاسوب لدعم السلوك المتكرر والعدائي والعنيف، يرتكب جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً.		**التحليل القانوني** هذه الجريمة تُجرم من يضايقون الأشخاص عبر الإنترنت - قد تنص بعض الولايات القضائية على جرائم تحرش غير مرتبطة بالحاسوب - لكن يوصى باعتماد هذه الجريمة لمتابعة لتلك الجرائم المرتكبة عبر الإنترنت. **تحليل الفجوة** **التوصيات:** يستحسن أن تدرج في التشريعات المحلية.
رعاية الأطفال على الإنترنت **القانون الجنائي الهولندي 248e** يعاقب الشخص الذي يقترح ترتيب لقاء، بوسائل عمل آلية أو باستخدام خدمة اتصال، مع شخص يعرف، أو ينبغي منطقيًا أن يعرف، أن هذا الشخص لم يصل بعد إلى سن السادسة عشرة، مع نية ارتكاب أفعال غير لائقة مع هذا الشخص أو لعمل صور عن عمل جنسي يشارك فيه هذا الشخص، بالسجن لمدة لا تقل عن سنتين أو بغرامة من الفئة الرابعة، إذا ارتكب أي عمل يقصد به تحقيق اللقاء. **قانون العقوبات الكندي** **القسم 172.1** 1. يرتكب جريمة كل شخص يتواصل عن طريق وسائل الاتصالات مع		**التحليل القانوني** لإثبات الجرم الهولندي، يلزم عقد لقاء لأغراض جنسية مع تقديم أدلة إثبات مأخوذة من تاريخ الدردشة عبر الإنترنت تفصح عن قصد جنسي؛ طلب عقد اللقاء مع الأدلة على أنه تم التخطيط لذلك (أي التاريخ والمكان). الغرض من القانون الكندي هو منع استدراج الكبار المفترسين للأطفال عبر الإنترنت. لا تتطلب هذه الجريمة حدوث جريمة جنسية. وهذا يعني أن المتهم لا يحتاج إلى الذهاب فعلاً لمقابلة الضحية شخصيًا. تكتمل الجريمة قبل اتخاذ أي إجراءات لارتكاب الجريمة الموضوعية. تجرم المادة 2-503 من القانون الجنائي كل من «حرض أو شجع أو سهل استغلال أطفال تقل سنهم عن 18 سنة في مواد إباحية"، وترتبط الجرائم الواردة في القانون الهولندي والكندي بمراودة الأطفال عبر الإنترنت بغرض ارتكاب فعل جنسي. ويختلف ذلك عن الجريمة الواردة في المادة 2-503 من القانون الجنائي والتي ترتبط حصريًا بالمواد الإباحية. **تحليل الفجوة** **التوصيات:** يُنصح بإدراجها في التشريعات المحلية لتجريم هذا السلوك التحضيري قبل ارتكاب جريمة جنسية

316. أوامر البحث والاستيلاء والمساعدة والإنتاج
317. http://www.legislation.gov.uk/ukpga/2000/23/section/53

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
شخص يكون عمره أقل من 18 عامًا، أو يظن المتهم أن عمره أقل من 18 عامًا، بغرض تسهيل ارتكاب جريمة مرتبطة بهذا الشخص، وذلك بموجب المادة الفرعية 153 (1)، المادة 155، 163.1 ، 170 أو 171 أو القسم الفرعي 212 (1) أو (2) أو (1.2) أو (4)؛ شخص يكون عمره أقل من 16 عامًا، أو يظن المتهم أن عمره أقل من 16 عامًا، بغرض تسهيل ارتكاب جريمة مرتبطة بهذا الشخص، وذلك بموجب المواد 151 أو 152، أو الفقرة الفرعية 160(3) أو 173 (2) أو الأقسام 271 أو 272 أو 273 أو 280؛ أو شخص يكون عمره أقل من 14 عامًا، أو يظن المتهم أن عمره أقل من 14 عامًا، بغرض تسهيل ارتكاب جريمة مرتبطة بهذا الشخص بموجب المادة 281.		
عقاب		
2. يعتبر كل شخص يرتكب جريمة بموجب الفقرة الفرعية (1) مذنبًا مذنبًا بارتكاب جريمة ويكون عرضة لعقوبة السجن لمدة تتراوح بين 10 سنوات كحد أقصى وسنة واحدة كحد أدنى؛ أو مذنبًا بارتكاب جريمة يعاقب عليها في ملخص الإدانة بالسجن لمدة تتراوح بين 18 شهرًا كحد أقصى و 90 يومًا كحد أدنى. افتراض إعادة تقدير العمر 3. الأدلة على أن الشخص المشار إليه في الفقرة (1) (أ) أو (ب) أو (ج) قُدِّم للمتهم وعمره أقل من ثمانية عشر عامًا أو ستة عشر عامًا أو أربعة عشر عامًا، حسب الحالة، في حالة عدم وجود أدلة تثبت عكس ذلك تثبت أن المتهم يعتقد أن الشخص كان أقل من تلك السن.		
لا دفاع		
4. لا يقبل دفاع المتهم أمام التهم الموجهة بموجب الفقرة (1) (أ) أو (ب) أو (ج) بأنه كان يعتقد أن الشخص المشار إليه في تلك الفقرة لا يقل عمره عن ثمانية عشر عامًا أو ستة عشر عامًا أو أربعة عشر عامًا، حسب الحالة، إلا في حالة اتخذ المتهم خطوات معقولة للتأكد من عمر الشخص.		

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 19 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[318] **التفتيش والضبط** **بيانات الحاسوب المخزنة** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لتمكين سلطاته المختصة من البحث في أو الوصول إلى: a. نظام الحاسوب أو جزء منه وبيانات الحاسوب المخزنة فيه؛ و وسيلة تخزين بيانات الحاسوب، حيث يمكن تخزين بيانات الحاسوب في أراضيها. 2. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وغيرها من الإجراءات لضمان تستطيع سلطاته عند تفتيشها نظام حاسوب معينًا أو جزءًا منه أو الوصول إليه بطريقة مماثلة، وذلك وفقًا للفقرة 1. أ، ويكون لدها أسباب للاعتقاد بأن البيانات المطلوبة مخزنة في نظام حاسوب آخر أو أن جزءًا منها موجود في إقليمها، وهذه البيانات يمكن الوصول إليها قانونيًا من النظام الأولي أو متاحة لها، فإنها قادرة على توسيع نطاق البحث أو الوصول المشابه للنظام الآخر على وجه السرعة. 3. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وغيرها من الإجراءات لتمكين سلطاته المختصة من مصادرة أو تأمين بيانات الحاسوب التي تم الوصول إليها وفقًا للفقرات 1 أو 2. تشمل هذه التدابير القدرة على: a. ضبط نظام حاسوب أو جزء منه أو وسيلة تخزين بيانات الحاسوب، والقيام بما يلزم لتأمينه؛ b. إنشاء نسخة من بيانات الحاسوب هذه والاحتفاظ بها؛ c. الحفاظ على سلامة بيانات الحاسوب المخزنة ذات الصلة؛ d. أن يجعل الوصول إلى بيانات الحاسوب في نظام الحاسوب الذي تم الوصول إليه غير ممكن أو أن يحذفها.	**قانون المسطرة الجنائية** **المواد 57 و59 و60 و62 و99**	**التحليل القانوني** تتيح المادتان 57 و59 من قانون الإجراءات الجنائية لضباط الشرطة القضائية الذين أشعروا بحالة تلبس بجناية إخبار النيابة العامة فورًا والانتقال إلى مكان ارتكابها لإجراء المعاينات المفيدة. وتحافظ النيابة العامة على الأدلة القابلة للاندثار وعلى كل من يمكن أن يساعد على إظهار الحقيقة. ويشمل ذلك حجز الأدوات التي استعملت في ارتكاب الجريمة أو التي كانت معدة لارتكابها، أي الحاسوب. إذا كان نوع الجناية أو الجنحة مما يمكن إثباته بحجز أوراق ووثائق أو أشياء أخرى في حوزة أشخاص يظن أنهم شاركوا في الجريمة، أو يحوزون مستندات أو أشياء أخرى تتعلق بالأفعال الإجرامية، فإن ضابط الشرطة القضائية ينتقل فورًا إلى منزل هؤلاء الأشخاص ليجري فيه طبقًا لشروط المحددة في المادتين 60 و62 تفتيشًا يحرر محضرًا بشأنه. وفيما عدا حالات المس بأمن الدولة أو إذا تعلق الأمر بجريمة إرهابية، فلا يحق إلا لضابط الشرطة القضائية ومعه الأشخاص المشار إليهم في المادة 60 وحدهم الاطلاع على الأوراق أو المستندات قبل القيام بحجزها. إذا تعين إجراء التفتيش في أماكن معدة لاستعمال مهني يشغلها شخص يلزمه القانون بكتمان السر المهني، فعلى ضابط الشرطة القضائية أن يشعر النيابة العامة المختصة وأن يتخذ مسبقًا جميع التدابير لضمان احترام السر المهني. يقوم ضابط الشرطة القضائية عند الاقتضاء بأخذ البصمات من مكان ارتكاب الجريمة، كما يمكنه أن يطلب إجراء خبرات عليها وعلى بقية أدوات الجريمة والأشياء التي تم العثور عليها وحجزها بمكان ارتكاب الجريمة أو لدى المشتبه فيهم بارتكابها. عملاً بالمادة 99 من قانون الإجراءات الجنائية، يجوز لقاضي التحقيق أن ينتقل إلى أي مكان لإجراء المعاينات المفيدة أو للقيام بتفتيش. ويشعر بذلك النيابة العامة التي لممثلها الخيار في مرافقته. **تحليل الفجوة** **التوصيات:** هذه هي قوة التحقيق الأكثر أهمية ويجب أن تشير إلى الحصول على حق الوصول وليس البحث. في «التقرير التوضيحي لاتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست، يعني «البحث» التفتيش عن البيانات أو قراءتها أو فحصها أو مراجعتها. لا تشير المادتان 60 و62 إلى "المعطيات" وليست خاصة بالحاسوب. وقد يكون من الضروري في تحقيقات الجرائم السيبرانية الوصول إلى الحاسوب والبيانات الواردة فيه. ولا يوضح قانون الإجراءات الجنائية ما إذا كان سيتم اعتبار بيانات الحاسوب المخزنة في حد ذاتها شيئًا ملموسًا وبالتالي يتم حجزها بطريقة متوازية كأشياء ملموسة مثل أجهزة الحاسوب، بخلاف تأمين الحاسوب أو الوسائط التي تخزن فيها البيانات.

318. المادة 3 من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
4. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لتمكين سلطاته المختصة من أن تأمر أي شخص لديه معرفة بعمل نظام الحاسوب أو التدابير المطبقة لحماية البيانات الموجودة فيه بتوفير ما يلزم من المعلومات بما يكفل تنفيذ الإجراءات المشار إليها في الفقرتين 1 و 2. 5. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و 15. **القسم 20 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - البحث والضبط** 1. إذا اقتنع [القاضي] بناء على [معلومات تحت القَسَم] [شهادة خطية] أن هناك أسبابًا معقولة [للاشتباه] [للاعتقاد] أنه قد يكون هناك في مكان ما شيء أو بيانات حاسوب: • قد تكون مادية كدليل في إثبات الجريمة؛ أو • قد اكتسبها شخص نتيجة لجريمة؛ [يجوز] [يأمر] يصدر [القاضي] تفويضًا لضابط [إنفاذ القانون] [الشرطة]، ويزوده بما قد يلزم من مساعدة، لدخول المكان للبحث عن الشيء أو بيانات الحاسوب وضبطها، وعمل ما يلزم بما في ذلك البحث أو عمليات الوصول الشبيهة: i. نظام الحاسوب أو جزء منه وبيانات الحاسوب المخزنة فيه؛ و ii. وسيلة تخزين بيانات الحاسوب، حيث يمكن تخزين بيانات الحاسوب في إقليم البلد.		يتعلق قانون الإجراءات الجنائية بحجز الوثائق أو السجلات وبأدلة الجمع أثناء التفتيش التي تم تدوينها أو تسجيلها في الماضي بشكل ملموس، مثل الحبر على الورق. ويحتاج المحققون في الجرائم السيبرانية إلى التفتيش عن البيانات وفحصها أو الوصول إليها وحجزها أو نقلها فعليًا. علاوةً على ذلك، من الضروري وجود أحكام إجرائية إضافية لضمان إمكانية الحصول على بيانات الحاسوب بطريقة فعالة بنفس القدر مثل التفتيش عن شيء ملموس يحتوي على البيانات، مثل الحاسوب وحجزه. وهذا مهم لضمان سلامة ومصدرَ تلك البيانات. وتوجد العديد من العوامل التي يجب مراعاتها في أي تشريع: أولاً، البيانات التي تكون في صورة غير ملموسة، مثل البيانات الموجودة في شكل كهرومغناطيسي. ثانيًا، على الرغم من أنه يمكن قراءة البيانات باستخدام أجهزة الحاسوب، إلا أنه لا يمكن حجزها ونقلها بنفس الطريقة التي يمكن بها قراءة السجلات الورقية. ويجب حجز الوسائط الفعلية التي تخزن فيها البيانات غير الملموسة (مثل المحرك الصلب بالحاسوب أو القرص المرن)، أو يجب عمل نسخة من البيانات بأي شكل ملموس (مثل المطبوعات الحاسوبية) أو شكل غير ملموس على وسائط فعلية (مثل القرص المرن)، قبل حجز الوسائط الملموسة التي تحتوي على النسخة ونقلها. وفي الحالتين الأخيرتين، حيث يتم إجراء مثل هذه النسخ من البيانات، تظل نسخة من البيانات في نظام الحاسوب أو جهاز التخزين. ويجب أن ينص القانون المحلي على سلطة إجراء مثل هذه النسخ. ثالثًا، نظرًا لقدرة أنظمة الحاسوب على الاتصال، قد لا يتم تخزين البيانات في جهاز حاسوب معين يتم التفتيش فيه، ولكن قد يمكن الوصول إلى هذه البيانات على النظام بسهولة. ويمكن تخزينها في جهاز تخزين بيانات متصل بالحاسوب بطريقة مباشرة غير مباشرة من خلال أنظمة الاتصال، مثل الإنترنت. وقد يقتضي ذلك، أو لا يقتضي، قوانين جديدة لتمديد التفتيش إلى اماكن تخزين البيانات فعليًا (أو استرداد البيانات من هذا الموقع إلى الحاسوب الذي يتم التفتيش فيه)، أو الاستعانة بصلاحيات التفتيش التقليدية بطريقة منسقة وأسرع في كلا الموقعين. تُعد كلمة «الوصول" مهمة نظرًا لأنها تحمل معنى محايد وتعكس بدقة أكثر المصطلحات الحاسوبية - وهذا مستخدم أيضًا في المادتين 26 و 27 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.[319] يمكن أن يقتبس التشريع الوطني اللغة المناسبة من اتفاقية بودابست بشأن الجريمة السيبرانية واتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية وذلك لتضمين تعريفات لنظام الحاسوب[320] وبيانات الحاسوب[321] والإحالة دائمًا إلى الوصول

319. الفقرات 184 إلى 191، الصفحات 31 إلى 33 من التقرير التفسيري لاتفاقية بودابست

320. انظر المادة 1 (أ) من اتفاقية بودابست: «أي جهاز أو مجموعة من الأجهزة المترابطة أو ذات الصلة، أو واحد أو أكثر من هذه الأجهزة يقوم بمعالجة البيانات تلقائيًا وفقًا لبرنامج ما" **أو** القسم 3 (5) من مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية: «جهاز أو مجموعة من الأجهزة المترابطة أو ذات الصلة، بما في ذلك الإنترنت، يقوم واحد منها أو أكثر بمعالجة تلقائية للبيانات أو بأداء أي وظيفة أخرى وفقًا لأحد البرامج".

321. انظر المادة 1.ب. من اتفاقية بودابست: «أي تمثيل للوقائع أو المعلومات أو المفاهيم في نموذج مناسب للمعالجة في نظام حاسوب، بما في ذلك البرامج المناسبة لأن يقوم نظام حاسوب بأداء وظيفة ما"، **أو** القسم 3 (6) من مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية: "تتضمن بيانات الحاسوب أي تمثيل للوقائع أو المعلومات أو المفاهيم (سواء أكانت نصوصًا أو أصواتًا أو صورًا) أو رموز آلة مقروءة أو تعليمات، في نموذج مناسب للمعالجة في نظام الحاسوب، بما في ذلك البرامج المناسبة لأن يقوم نظام الحاسوب بأداء وظيفة ما".

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
2. إذا كان[قوة إنفاذ القانون] [الشرطة] الذي يجري عملية بحث على أساس القسم 20 (1) أسباب للاعتقاد بأن البيانات المطلوبة مخزنة في نظام حاسوب آخر أو جزء منه في إقليمها، وأن هذه البيانات يمكن الوصول إليها قانونيًا أو يمكن أن تكون متاحة من النظام الأولي، فيجب أن يكون قادرًا على توسيع نطاق البحث أو الوصول إلى النظام الآخر بطريقة مماثلة. 3. يتم تمكين ضابط [تطبيق القانون] [الشرطة] الذي يقوم بالبحث من مصادرة أو تأمين بيانات الحاسوب المماثلة التي يتم الوصول إليها وفقًا للفقرات 1 أو 2. **القسم 21 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - المساعدة** يجب على أي شخص لا يشتبه في ارتكابه جريمة ولكن لديه علم بسير عمل نظام الحاسوب أو التدابير المطبقة لحماية بيانات الحاسوب الواردة فيه والتي تخضع لعملية بحث بموجب المادة 20، أن يسمح وأن يساعد إذا لزم الأمر وطلب منه الشخص المسؤول أن يجري البحث عن طريق: • توفير المعلومات التي تمكن من اتخاذ التدابير المشار إليها في المادة 20؛ • الوصول إلى نظام حاسوب أو وسيط تخزين بيانات الحاسوب واستخدامه للبحث في أي بيانات حاسوب متاحة أو في النظام؛ • الحصول على ونسخ بيانات حاسوب هذه؛ • استخدام المعدات لعمل نسخ؛ و • الحصول على معلومات واضحة من نظام حاسوب بشكل مقبول في الإجراءات القانونية. **المادة 26 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - فحص المعلومات المخزنة** 1. تلتزم كل دولة طرف يتبنى الإجراءات الضرورية لتمكين سلطاتها المختصة من التفتيش أو الوصول إلى:		يجب أن يكون هناك تعريف «للحجز" لضمان النزاهة ولتحديد الإجراءات - القسم 3 (16) من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية "يشمل الحجز: • تشغيل أي نظام حاسوب في الموقع ووسائط تخزين بيانات الحاسوب؛ • إنشاء نسخة من بيانات الحاسوب والاحتفاظ بها، بما في ذلك عن طريق استخدام معدات في الموقع؛ • الحفاظ على سلامة بيانات الحاسوب المخزنة ذات الصلة؛ • أن يجعل الوصول غير ممكن إلى بيانات الحاسوب في نظام الحاسوب الذي تم الوصول إليه أو أن يحذفها؛ • أخذ نسخة مطبوعة من بيانات غير ممكن؛ أو • حجز نظام حاسوب أو جزء منه أو وسيلة تخزين بيانات الحاسوب، والقيام بما يلزم لتأمينه» تنص المادة 21 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية على التشريع لضمان تقديم المساعدة من قبل أولئك الذين لديهم معرفة متخصصة بموقع الأدلة ذات الصلة - يمكن استخدام هذا كدليل - انظر أيضًا القسم 17 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية، المتعلق بالجريمة في حال تم رفض المساعدة دون عذر قانوني

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
a. تقنية معلومات أو جزء منها والمعلومات المخزنة فيها أو المخزنة عليها. b. بيئة أو وسيط تخزين معلومات تقنية معلومات والذي قد تكون معلومات التقنية مخزنة فيه أو عليه. 2. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من التفتيش أو الوصول إلى تقنية معلومات معينة أو جزء منها بما يتوافق مع الفقرة (1- أ) إذا كان هناك اعتقاد بأن المعلومات المطلوبة مخزنة في تقنية معلومات أخرى أو جزء منها في إقليمها وكانت هذه المعلومات قابلة للوصول قانونا أو متوفرة في التقنية الأولى فيجوز توسيع نطاق التفتيش والوصول للتقنية الأخرى. **المادة 27 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - ضبط المعلومات المخزنة** 1. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من ضبط وتأمين معلومات تقنية المعلومات التي يتم الوصول إليها حسب الفقرة 1 من المادة 26 من هذه الاتفاقية. هذه الإجراءات تشمل صلاحيات: a. ضبط وتأمين تقنية المعلومات أو جزء منها أو وسيط تخزين معلومات تقنية المعلومات. b. عمل نسخة معلومات تقنية المعلومات والاحتفاظ بها. c. الحفاظ على سلامة معلومات تقنية المعلومات المخزنة. d. إزالة أو منع الوصول إلى تلك المعلومات في تقنية المعلومات التي يتم الوصول إليها. 2. تلتزم كل طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى أي شخص لديه معرفة بوظيفة تقنية المعلومات أو الإجراءات المطبقة لحماية تقنية المعلومات من أجل تقديم المعلومات الضرورية لإتمام تلك الإجراءات المذكورة في الفقرتين 2 و 3 من المادة 26 من هذه الاتفاقية.		

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 16 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[322] **الحفظ المستعجل لبيانات الحاسوب المخزنة والكشف عنها** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وغيرها من الإجراءات لتمكين سلطاته المختصة من طلب الحفظ السريع لبيانات الحاسوب المحددة أو الحصول عليها بشكل مماثل، بما في ذلك حركة البيانات التي تم تخزينها عن طريق نظام حاسوبي، ولا سيما عندما يكون هناك أسباب للاعتقاد بأن بيانات الحاسوب معرضة بشكل خاص للفقد أو التعديل. 2. عندما يقوم أحد الأطراف بتنفيذ الفقرة 1 أعلاه عن طريق أمر شخص بحفظ بيانات الحاسوب المخزنة المحددة وذلك بوضعها في حوزته أو تحت سيطرته، يعتمد هذا الطرف الإجراءات التشريعية وغيرها من الإجراءات التي قد تكون ضرورية لإلزام ذلك الشخص بالحفاظ على سلامة بيانات الحاسوب لفترة زمنية طويلة، حدها الأقصى تسعين يومًا، وذلك لتمكين السلطات المختصة من طلب الكشف عنها. يجوز للطرف أن ينص على تجديد هذا الأمر لاحقًا. 3. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لإلزام الحارس أو أي شخص آخر يحفظ بيانات الحاسوب بالحفاظ على سرية تنفيذ هذه الإجراءات للفترة الزمنية المنصوص عليها في قانونه الداخلي. 4. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و 15.	**لا يوجد معادل**	**التحليل القانوني** هذه القوة الإجرائية مهمة لضمان الحفاظ على البيانات المعرضة للحذف أو الفقد **تحليل الفجوة** **التوصيات:** تعد هذه القدرة المستعجلة للاحتفاظ بمعلومات المشترك الأساسية والبيانات الوصفية والمعاملات والمحتويات المخزنة ضرورية كجزء من تحقيقات جرائم الإنترنت، ولضمان أن تكون الأدلة متاحة للبحث والوصول والضبط والمراجعة. يمكن استخدام لغة المادة 16 من اتفاقية بازل أو القسم 23 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية أو المادة 23 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. سيتطلب ذلك أيضًا تعريفات «بيانات الحاسوب»، و[323] "معلومات المشترك أو معلومات المشترك الأساسية"، و "حركة البيانات" و[324] "مزود خدمة الاتصالات"[325] يجب ملاحظة أن اتفاقية بودابست واتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية لا تقدمان تعريفًا لمعلومات المشترك الأساسية؛ غير أن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات تقدم تعريفًا لمعلومات المشترك:[326] " أي معلومات لدى مزود الخدمة بخصوص المشتركين في الخدمة، باستثناء المعلومات التي يمكن من خلالها معرفة ما يلي: • نوع خدمة الاتصال المستخدمة والأحكام الفنية المتعلقة بها وفترة الخدمة. • هوية المشترك وعنوانه البريدي أو الجغرافي أو رقم الهاتف ومعلومات الدفع المتاحة بموجب اتفاقية الخدمة • أي معلومات أخرى على موقع تركيب معدات الاتصالات بموجب اتفاقية الخدمة." ينبغي إيلاء اهتمام لأن يكون طول مدة الحفظ معقولًا في هذه الظروف، وأن يُسمَح بتطبيق التمديد في الظروف الملحة - تنص اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست والاتفاقية العربية لمكافحة جرائم تقنية المعلومات على 90 يومًا، فيما تنص اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية على 7 أيام. ووفقًا للتجربة فإن مدة 90 يومًا هي مدة قصيرة في التحقيقات عبر الإنترنت ، ويجب أن تكون حوالي 180 يومًا يمكن تمديدها.

322. لا يوجد ما يعادلها في اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية
323. انظر المادة 1.ب. اتفاقية بودابست **أو** القسم 3 (6) من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية
324. انظر المادة 1.د من اتفاقية بودابست: "أي بيانات حاسوب تتعلق باتصال عن طريق نظام حاسوب، يتم إنشاؤها بواسطة نظام حاسوب يشكل جزءًا من سلسلة الاتصال، وتعرض مصدر الاتصال أو وجهته أو مساره أو الوقت أو التاريخ أو حجمه أو مدته أو نوع الخدمة الأساسية"، **أو** القسم 3 (18) من مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية: "حركة البيانات تعني أي بيانات حاسوب تتعلق باتصال عن طريق نظام حاسوب، يتم إنشاؤها بواسطة نظام حاسوب يشكل جزءًا من سلسلة الاتصال، وتعرض مصدر الاتصال أو وجهته أو مساره أو الوقت أو التاريخ أو الحجم أو المدة أو نوع الخدمة الأساسية".
325. انظر المادة 1.ج. من اتفاقية بودابست: "1 أي كيان عام أو خاص يوفر للمستخدمين قدرة الاتصال عن طريق نظام الحاسوب، و 2 أي كيان آخر يعالج أو يخزن بيانات الحاسوب نيابة عن خدمة الاتصال هذه أو مستخدمي هذه الخدمة».
326. انظر المادة 2 (9) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
القسم 23 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الحفظ المستعجل إذا اقتنع ضابط [تطبيق القانون] [الشرطة] بوجود أسباب معقولة للاعتقاد بأن بيانات الحاسوب المطلوبة لأغراض التحقيق الجنائي معرضة للضياع أو التعديل، يجوز لضابط [تطبيق القانون] [الشرطة]، عن طريق إشعار مكتوب مقدم إلى شخص يتحكم في بيانات الحاسوب، أن يطلب من هذا الشخص الحفاظ على البيانات المحددة في الإشعار لمدة تصل إلى سبعة (7) أيام على وفقًا لما هو محدد في الإشعار. يمكن تمديد الفترة إلى ما بعد سبعة (7) أيام إذا سمح [قاضي]، بناءً على طلب من طرف واحد، وذلك لمدة زمنية أخرى محددة. **المادة 23 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات- الحفظ المستعجل للبيانات المخزنة في تكنولوجيا المعلومات** 1. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأمر أو الحصول على الحفظ العاجل للمعلومات المخزنة بما في ذلك معلومات تتبع المستخدمين والتي خزنت على تقنية معلومات وخصوصا إذا كان هناك اعتقاد بأن تلك المعلومات عرضة للفقدان أو التعديل. 2. تلتزم كل دولة طرف بتبني الإجراءات الضرورية فيما يتعلق بالفقرة 1 بواسطة إصدار أمر إلى شخص من أجل حفظ معلومات تقنية المعلومات المخزنة والموجودة بحيازته أو سيطرته ومن أجل إلزامه بحفظ وصيانة سلامة تلك المعلومات لمدة أقصاها 90 يوما قابلة للتجديد، من أجل تمكين السلطات المختصة من البحث والتقصي 3. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لإلزام الشخص المسؤول عن حفظ تقنية معلومات للإبقاء على سرية الإجراءات طوال الفترة القانونية المنصوص عليها في القانون الداخلي.		

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 17 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[327] **الحفظ المستعجل والكشف الجزئي لبيانات المرور** 1. فيما يتعلق ببيانات المرور التي يتعين الحفاظ عليها بموجب المادة 16، يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى من أجل: a. التأكد من أن مثل هذا الحفظ المستعجل لبيانات المرور متاح بغض النظر عما إذا كان هناك واحد أو أكثر من مقدمي الخدمة قد شاركوا في نقل ذلك الاتصال؛ و b. ضمان الكشف السريع للسلطة المختصة لدى الدولة الطرف، أو للشخص المعين من قبل تلك السلطة، عن كمية كافية من حركة البيانات لتمكينه من تحديد مقدمي الخدمات والمسار الذي تم من خلاله نقل الاتصال. 2. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و 15. **القسم 23 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الحفظ المستعجل** إذا اقتنع ضابط [تطبيق القانون] [الشرطة] بوجود أسباب معقولة للاعتقاد بأن بيانات الحاسوب المطلوبة لأغراض التحقيق الجنائي معرضة للضياع أو التعديل، يجوز لضابط [تطبيق القانون] [الشرطة]، عن طريق إشعار مكتوب مقدم إلى شخص يتحكم في بيانات الحاسوب، أن يطلب من هذا الشخص الحفاظ على البيانات المحددة في الإشعار لمدة تصل إلى سبعة (7) أيام على وفقًا لما هو محدد في الإشعار. يمكن تمديد الفترة إلى ما بعد سبعة (7) أيام إذا سمح [قاضي]، بناءً على طلب من طرف واحد، وذلك لمدة زمنية أخرى محددة.	**لا يوجد معادل**	**التحليل القانوني** تعد هذه القوة الإجرائية مهمة بشكل خاص لضمان توفير مقدمي خدمات الإنترنت لعناوين بروتوكول إنترنت يمكنها تحديد موقع مرتكب الجريمة السيبرانية. **تحليل الفجوة** **التوصيات:** يجب تضمين هذه القوة المستعجلة جنبًا إلى جنب مع الكشف عن حركة البيانات في التشريعات لتمكين التحقيقات الفعالة في جرائم الإنترنت. يمكن استخدام لغة المادة 17 من اتفاقية بازل، القسمين 23 و 24 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية أو المادة 24 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. سيتطلب ذلك أيضًا تعريفات لـ «حركة البيانات" و "مزود خدمة الاتصالات"[328]

327. لا يوجد ما يعادلها في اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية
328. انظر التعريفات أعلاه

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
القسم 24 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - جمع بيانات حركة الاتصالات إذا اقتنع ضابط [تطبيق القانون] [الشرطة] بناءً على أسباب معقولة بأن البيانات المخزنة في نظام الحاسوب ضرورية لأغراض التحقيق الجنائي، يجوز له أن يطلب، عبر إشعار خطي، من شخص له السيطرة على نظام الحاسوب كشف بيانات حركة مرور تتعلق باتصال محدد بشكل كافٍ لتحديد: 3. مزودو خدمة الإنترنت؛ و/ أو 4. المسار الذي تم من خلاله نقل الاتصال. **المادة 24 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - لتحفظ العاجل والكشف الجزئي لمعلومات تتبع المستخدمين** تلتزم كل دولة طرف بتبني الإجراءات الضرورية فيما يختص بمعلومات تتبع المستخدمين من أجل: 1. ضمان توفر الحفظ العاجل لمعلومات تتبع المستخدمين بغض النظر عن اشتراك واحد أو أكثر من مزودي الخدمة في بث تلك الاتصالات. 2. ضمان الكشف العاجل للسلطات المختصة لدى الدولة الطرف أو لشخص تعينه تلك السلطات لمقدار كاف من معلومات تتبع المستخدمين لتمكين الدولة الطرف من تحديد مزودي الخدمة ومسار بث الاتصالات.		
المادة 18 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[329] **أمر النسخ** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وتدابير أخرى لتمكين سلطاته المختصة من أن تأمر: a. شخصًا موجودًا في إقليمها بتقديم بيانات حاسوب محددة في حيازته أو تحت سيطرته، وتُخَزّن في نظام حاسوب أو بوسيلة تخزين بيانات الحاسوب؛ و b. مقدم خدمة يقدم خدماته في إقليم الدولة الطرف بتقديم معلومات المشترك المرتبطة بهذه الخدمات، والتي تكون في حيازة أو تحت سيطرة مقدم الخدمة.	**لا يوجد معادل**	**التحليل القانوني** هذا شرط أساسي لإجراء تحقيق فعال في جرائم الإنترنت وسيؤثر غيابه على الملاحقات القضائية والتعاون الدولي.

329. لا يوجد ما يعادلها في اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
2. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و 15. 3. تعني «معلومات المشترك» أي معلومات محفوظة بشكل بيانات حاسوب أو أي شكل آخر ويحتفظ بها مزود الخدمة، وترتبط بالمشتركين في خدماته، بخلاف بيانات الحركة أو المحتوى، والتي يمكن إنشاؤها من خلال: a. نوع خدمة الاتصال المستخدمة والأحكام الفنية المتعلقة بها وفترة الخدمة؛ b. هوية المشترك أو العنوان البريدي أو الجغرافي، ورقم الهاتف وأرقام الاتصال الأخرى ومعلومات الفوترة والدفع المتاحة بناءً على اتفاقية الخدمة؛ c. أي معلومات أخرى متاحة على موقع تركيب معدات الاتصالات بناءً على اتفاقية الخدمة أو الترتيب. **القسم 22 من نظام اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - أمر النسخ** إذا كان [قاض] مقتنعًا بناءً على طلب قدمه [ضابط أنفاذ القانون] [الشرطة] بأن بيانات حاسوب محددة أو نسخة مطبوعة أو غيرها من المعلومات ضرورية لإجراء تحقيق جنائي أو لإجراءات جنائية، يجوز [للقاضي] أن يأمر بما يلي: • أن ينسخ شخص في إقليم [الدولة المشترعة] يتحكم في نظام الحاسوب نسخًا محددة من بيانات الحاسوب أو نسخة مطبوعة أو معلومات أخرى واضحة من تلك البيانات؛ أو • مزود خدمة الإنترنت في [الدولة المشترعة] لتقديم معلومات حول الأشخاص المشتركين في الخدمة أو الذين يستخدمونها بطريقة أخرى.		**تحليل الفجوة** **التوصيات:** تعتبر هذه السلطة الأساسية ضرورية لضمان توفير مزودي خدمة الاتصالات في المغرب لمعلومات المشترك الأساسية وبيانات المرور وبيانات المحتوى المخزنة. سيتطلب ذلك أيضًا تعريفات «بيانات الحاسوب"، و "معلومات المشترك أو معلومات المشترك الأساسية"، و "حركة البيانات" و "مزود خدمة الاتصالات"[330] المادة 25 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات هي نموذج يمكن استخدامه ويستخدم تعريفات مختلفة بما في ذلك «تكنولوجيا المعلومات"، و[331] "مزود الخدمة" و[332] "البيانات"؛[333] غير أنه من المستحسن أن تكون هناك تعريفات لـ «معلومات المشترك أو معلومات المشترك الأساسية" أو "حركة البيانات" لأنها ستكون أنواع مختلفة من الأدلة التي يمكن توليدها في دول الجنوب الشريكة. علاوة على ذلك، سوف تتطلب هذه السلطة من الأفراد وغيرهم (مثل الكيانات المؤسسية والمؤسسات المالية وغيرها من المنظمات) ممن يحملون البيانات أن يقوموا بتوليدها بناء على طلب سلطات إنفاذ القانون. يمكن أن تكون المادة 18 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست والمادة 22 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية بمثابة دليل مع التطبيق الثابت للتعريفات

330. انظر التعريفات أعلاه

331. المادة 2 (1) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات: «أية وسيلة مادية أو معنوية أو مجموعة وسائل مترابطة أو غير مترابطة تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها وفقا للأوامر والتعليمات المخزونة بها. ويشمل ذلك جميع المدخلات والمخرجات المرتبطة بها سلكيًا أو لاسلكيًا في نظام أو شبكة."

332. المادة 2 (2) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات: «أي شخص طبيعي أو معنوي عام أو خاص يزود المشتركين بالخدمات للتواصل بواسطة تقنية المعلومات، أو يقوم بمعالجة أو تخزين المعلومات نيابة عن خدمة الاتصالات أو مستخدميها».

333. المادة 2 (3) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات: «كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة تقنية المعلومات، كالأرقام والحروف والرموز وما إلى ذلك».

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 25 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - أمر تسليم المعلومات تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى: 1. أي شخص في إقليمها لتسليم معلومات معينة في حيازة ذلك الشخص والمخزنة على تقنية معلومات أو وسيط تخزين معلومات. 2. أي مزود خدمة يقدم خدماته في إقليم الدولة الطرف لتسليم معلومات المشترك المتعلقة بتلك الخدمات في حوزة مزود الخدمة أو تحت سيطرته.		
المادة 21 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[334] **اعتراض بيانات المحتوى** 1. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وغيرها من الإجراءات، فيما يتعلق بمجموعة من الجرائم الخطيرة التي يحددها القانون المحلي، لتمكين سلطاته المختصة من: a. الجمع أو التسجيل من خلال تطبيق الوسائل التقنية على أراضي ذلك الطرف، و b. إلزام مزود الخدمة، في حدود قدرته التقنية الحالية: c. الجمع أو التسجيل من خلال تطبيق الوسائل التقنية على أراضي ذلك الطرف؛ أو d. التعاون ومساعدة السلطات المختصة في جمع أو تسجيل بيانات المحتوى في الوقت الحقيقي، لاتصالات محددة تتم في أراضيها وترسل عن طريق نظام حاسوبي. 2. في الحالات التي لا يمكن فيها لأي طرف، بسبب المبادئ المستقرة في نظامه القانوني الداخلي، أن يعتمد التدابير المشار إليها في الفقرة 1.أ، يجوز له بدلا من ذلك اعتماد تدابير تشريعية وتدابير أخرى قد تكون ضرورية لضمان جمع أو تسجيل البيانات المرورية المرتبطة باتصالات محددة مرسلة في أراضيه، في الوقت الحقيقي، من خلال تطبيق الوسائل التقنية على ذلك الإقليم.	**لا يوجد معادل**	**التحليل القانوني** تعتبر هذه السلطة ضرورية للتشريعات الوطنية - ويجب أن تكون هناك ضمانات ومتطلبات/إجراءات لإلزام مزودي خدمة الاتصالات على التعاون في جمع أو تسجيل بيانات المحتوى في الوقت الفعلي لاتصالات محددة تتم في المغرب. **تحليل الفجوة** **التوصيات:** يجب اتخاذ تدابير لإلزام مقدمي الخدمات في المغرب بالتعاون من أجل جمع المحتوى في الوقت الحقيقي؛ وينبغي اتخاذ الضمانات للتأكد من أن جمعها قانوني وضروري ومعقول ومتناسب مع الحالة. يجب مراعاة مراجعة المادة 29 من CITO والمادة 21 BC والقسم 26 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية وإدراج اللغة في التشريعات الوطنية

334. لا يوجد ما يعادلها في اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
3. يعتمد كل طرف التدابير التشريعية والتدابير الأخرى التي قد تكون ضرورية لإلزام مقدم الخدمة بالحفاظ على سرية تنفيذ أي سلطة منصوص عليها في هذه المادة وأي معلومات تتعلق بها. 4. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و 15. **القسم 26 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - اعتراض بيانات المحتوى** 1. إذا تأكد [قاضٍ] بناء على [شهادة تحت القسم] [شهادة خطية] بأن هناك أسباباً معقولة لـ [الاشتباه] [الظن] بأن محتوى البلاغات الإلكترونية هو مطلوب بشكل معقول لأغراض [التحقيق] في تحقيق جنائي، [يجوز] [للقاضي] [يجب] أن: • يطلب من مزود خدمة الإنترنت الذي تتوفر خدمته في [بلد المشرع] جمع أو تسجيل أو السماح أو مساعدة السلطات المختصة في جمع أو تسجيل بيانات المحتوى المرتبطة بالاتصالات المحددة التي يتم إرسالها عن طريق نظام حاسوب، وذلك من خلال استخدام وسائل تقنية؛ أو • السماح لموظف [قوة تنفيذ القانون] [الشرطة] بجمع أو تسجيل تلك البيانات من خلال تطبيق الوسائل التقنية. 2. قد تقرر دولة عدم تنفيذ القسم 26. **المادة CITO 29 - اعتراض معلومات المحتوى** 1. تلتزم كل دولة طرف باعتماد الإجراءات التشريعية اللازمة المتعلقة بسلسلة من الجرائم المنصوص عليها في القانون المحلي، وذلك لتمكين السلطات المختصة من:		

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
a. تسجيل أو جمع المعلومات من خلال الوسائل التقنية في أراضي هذه الدولة الطرف، أو التعاون مع السلطات المختصة ومساعدتها على تسريع جمع وتسجيل معلومات المحتوى الخاصة بالاتصالات ذات الصلة في إقليمها والتي يتم نقلها عن طريق تكنولوجيا المعلومات. 2. إذا تعذر على الدولة الطرف، بسبب النظام القانوني المحلي، اعتماد الإجراءات المبينة في الفقرة 1 (أ)، يجوز لها اعتماد إجراءات أخرى بالشكل الضروري لضمان تسريع جمع وتسجيل معلومات المحتوى المقابلة الاتصالات ذات الصلة في أراضيها باستخدام الوسائل التقنية في ذلك الإقليم. 3. تلتزم كل دولة طرف باعتماد الإجراءات اللازمة لمطالبة مقدم الخدمة بالحفاظ على سرية أي معلومات عند ممارسة السلطة المنصوص عليها في هذه المادة.		
المادة 20 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[335] **جمع بيانات حركة الاتصالات في الوقت الحقيقي** 1. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتمكين سلطاته المختصة من: a. الجمع أو التسجيل من خلال تطبيق الوسائل التقنية على أراضي ذلك الطرف، و إلزام مزود الخدمة، في حدود قدرته التقنية الحالية: الجمع أو التسجيل من خلال تطبيق الوسائل التقنية على أراضي ذلك الطرف؛ أو التعاون ومساعدة السلطات المختصة في جمع أو تسجيل بيانات المحتوى في الوقت الحقيقي، لاتصالات محددة تتم في أراضيها وترسل عن طريق نظام حاسوبي.	**لا يوجد معادل**	**التحليل القانوني** لا توجد سلطة إجرائية فقط لجمع بيانات حركة المرور في الوقت الحقيقي. يمكن أن يكون هناك حد أدنى لجمع بيانات حركة المرور في الوقت الحقيقي، وتعد هذه الحركة أداة تحقيق أساسية. قد تكون هناك حالات لا يضع فيها مقدم الطلب حدًا قانونيًا أعلى لتأمين المحتوى، ولكن يمكن وجود حد أدنى لتأمين حركة المرور. لهذا السبب، يجب أن يكون هناك تمييز بين جمع المحتوى المخزن وبيانات المرور في الوقت الحقيقي. يجب أن تكون هناك ضمانات ومتطلبات/إجراءات لإلزام مزودي خدمة الاتصالات على التعاون في جمع أو تسجيل بيانات المحتوى في الوقت الفعلي لاتصالات محددة تتم في المغرب **تحليل الفجوة** **التوصيات:** ينبغي توفير صلاحية محددة لجمع حركة البيانات في الوقت الفعلي، وينبغي إدراج حكم لإلزام مزودي خدمة الاتصالات في المغرب على التعاون لجمع حركة البيانات في الوقت الفعلي؛ ويجب إدراج ضمانات لضمان أن جمعها قانوني وضروري ومعقول ومتناسب مع الحالة. يمكن اعتماد اللغة من المادة 28 الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لكنها لا تشير إلى الجمع المستعجل في الوقت الحقيقي. يجب استخدام المادة 20 من اتفاقية بودابست والمادة 25 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية باعتبارهما دليلًا للتشريعات الوطنية

335. المادة 31 (3) (هـ) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية - تشير المادة 28 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات إلى الجمع المستعجل بدلاً من الجمع في الوقت الفعلي

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
2. في الحالات التي لا يمكن فيها لأي طرف، بسبب المبادئ المستقرة في نظامه القانوني الداخلي، أن يعتمد التدابير المشار إليها في الفقرة 1.أ، يجوز له بدلا من ذلك اعتماد تدابير تشريعية وتدابير أخرى قد تكون ضرورية لضمان جمع أو تسجيل البيانات المرورية المرتبطة باتصالات محددة مرسلة في أراضيه، في الوقت الفعلي، من خلال تطبيق الوسائل التقنية على ذلك الإقليم. 3. يعتمد كل طرف التدابير التشريعية والتدابير الأخرى التي قد تكون ضرورية لإلزام مقدم الخدمة بالحفاظ على سرية تنفيذ أي سلطة منصوص عليها في هذه المادة وأي معلومات تتعلق بها. 4. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و 15. **القسم 25 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - جمع بيانات حركة الاتصالات** 1. إذا تأكد [قاض] بناء على [شهادة تحت القسم] [شهادة خطية] بأن هناك أسباباً معقولة لـ [الاشتباه] [الظن] بأن بيانات حركة الاتصالات المرتبطة ببلاغ محدد ضرورية بشكل معقول لأغراض [التحقيق] في تحقيق جنائي، [يجوز] [للقاضي] [يجب] أن يأمر شخصًا يتحكم بهذه البيانات بما يلي: • جمع أو تسجيل بيانات حركة الاتصالات المرتبطة باتصالات محددة خلال فترة محددة؛ أو • التصريح ومساعدة ضابط [الشرطة] [قوة تنفيذ القانون] محدد لجمع أو تسجيل تلك البيانات. 2. إذا تأكد [قاض] بناء على [شهادة تحت القسم] [شهادة خطية] بأن هناك أسباباً معقولة لـ [الاشتباه] [الظن] بأن بيانات حركة الاتصالات المرتبطة ببلاغ محدد ضرورية بشكل معقول لأغراض [التحقيق] في تحقيق جنائي، [يجوز] [للقاضي] [يجب] أن يسمح لـ [قوة تنفيذ القانون] [الشرطة] بجمع أو تسجيل بيانات حركة الاتصالات المرتبطة برسالة محددة خلال فترة محددة من خلال تطبيق الوسائل التقنية. 3. قد تقرر دولة عدم تنفيذ القسم 25.		

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
		واجب الكشف عن مفاتيح التشفير مع استخدام الإرهابيين والمجرمين المنظمين بشكل روتيني لتطبيقات الرسائل المشفرة[336] قد يعتبر الكشف عن مفاتيح التشفير قوة ملائمة لإطلاق مفاتيح كلمات المرور لفتح الأجهزة[337] **تحليل الفجوة** **التوصيات:** عدم القدرة على توضيح ما إذا كانت هناك أية صلاحيات في المغرب - لكن هذه الصلاحيات ستتيح لوكالات إنفاذ القوانين إجبار أصحاب الأجهزة على فتحها
		التزامات الاحتفاظ بالبيانات[338] تسمح مثل هذه السلطة لوكالات إنفاذ القانون بـ 1. تتبع وتحديد مصدر الاتصال 2. تحديد وجهة الاتصال؛ 3. تحديد تاريخ ووقت ومدة الاتصال؛ و 4. تحديد نوع الاتصال المغرب ليس لديه هذا النوع من الالتزام[339]

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة BC 22 **الاختصاص القضائي** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وغيرها من الإجراءات لإقامة ولاية قضائية على أي جرم منصوص عليه في المواد من 2 إلى 11 من هذه الاتفاقية، عندما تُرتكب الجريمة: a. في أراضيها؛ أو b. على متن سفينة ترفع علم تلك الدولة الطرف؛ أو c. على متن طائرة مسجلة بموجب قوانين ذلك الطرف؛ أو	**قانون المسطرة الجنائية** **المواد 704 و 705 و 706 و 707 و 708 و 709 و 710 و 711 و 712 و 749**	**التحليل القانوني** يحدد قانون الإجراءات الجنائية بوضوح الاختصاص القضائي - الذي ينطبق بالتساوي على مخالفات الجرائم السيبرانية. **تحليل الفجوة** **التوصيات:** في حالة الجرائم المرتكبة باستخدام أنظمة الحاسوب، ستظهر هناك مواقف يكون فيها لأكثر من طرف اختصاص قضائي على بعض أو كل المشتركين في الجريمة. مثل العديد من هجمات الفيروسات والاحتيال وانتهاكات حقوق الطبع والنشر المرتكبة من خلال استغلال ضحايا الإنترنت الموجودين في أكثر من دولة واحدة. إذا كان هناك تعارض بين السلطات القضائية، فيجب أن تؤخذ في الاعتبار المبادئ التوجيهية المتعلقة بتحديد الولاية القضائية المناسبة لمحاكمة جريمة ما - انظر المبادئ التوجيهية Eurojust لتقرير الولاية القضائية التي في الجرائم التي تجب ملاحقتها (المراجعة 2016)[340]

336. Eleanor Saitta. "Can Encryption Save Us?" Nation 300, no. 24 (15 يونيو 2015): 16-18. Academic Search Premier, EBSCOhost (تمت زيارته في 29 فبراير 2016).

337. انظر مثلاً القسم ٩٤ من القانون الإنجليزي (Regulation of Investigatory Powers Act 2000 (UK) - http://www.legislation.gov.uk/ukpga/2000/23/section/49

338. أصدر الاتحاد الأوروبي في عام 2006 توجيهه بشأن الاحتفاظ بالبيانات - اضطرت الدول الأعضاء في الاتحاد الأوروبي إلى تخزين بيانات الاتصالات الإلكترونية لمدة ستة أشهر على الأقل و 24 شهراً على الأكثر للتحقيق في الجرائم الخطيرة وكشفها ومقاضاة مرتكبيها. أبطلت محكمة العدل الأوروبية في عام 2014 توجيه الاحتفاظ بالبيانات، حيث قررت أنها قدمت ضمانات غير كافية ضد التدخلات في الخصوصية وحماية البيانات. في حالة عدم وجود توجيه صالح للاتحاد الأوروبي بشأن الاحتفاظ بالبيانات، فقد تواصل الدول الأعضاء تقديم خطة للاحتفاظ بالبيانات - للاطلاع على الخطط الوطنية، انظر: http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention

339. تقرير ICMEC العالمي، الصفحة 33

340. http://www.eurojust.europa.eu/Practitioners/operational/Documents/Operational-Guidelines-for-Deciding.pdf

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
d. من قِبَل أحد رعاياها، إذا كانت الجريمة معاقبًا عليها بموجب القانون الجنائي حيث ارتكبت، أو إذا ارتكبت الجريمة خارج الولاية الإقليمية لأي دولة. 2. يجوز لكل طرف أن يحتفظ بالحق في عدم تطبيق أو تطبيق قواعد الاختصاص المنصوص عليها في الفقرات من 1 إلى 1 د من هذه المادة أو أي جزء منها فقط في حالات أو شروط محددة. 3. يعتمد كل طرف ما قد يلزم من إجراءات لإقامة ولاية قضائية على الجرائم المشار إليها في الفقرة 1 من المادة 24 من هذه الاتفاقية، في الحالات التي يكون فيها الجاني المفترض موجودا في إقليمه ولا يسلمه إلى بلد آخر بعد طلب التسليم على أساس جنسيته فقط. 4. لا تستبعد هذه الاتفاقية أي ولاية قضائية جنائية يمارسها أي طرف وفقًا لقانونه الداخلي. 5. عندما يطالب أكثر من طرف بالولاية القضائية على جريمة مفترضة تم النص عليها في هذه الاتفاقية، يتشاور الطرفان المعنيان، عند الضرورة من أجل تحديد الولاية القضائية الأنسب. **القسم 19من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الولاية القضائية** ينطبق هذا القانون على أي فعل أو تقصير: • في إقليم [الدولة المشترعة]؛ أو • على سفينة أو طائرة مسجلة في [الدولة المشترعة]؛ أو • من قبل أحد مواطني [الدولة المشترعة] خارج الولاية القضائية لأي بلد؛ أو من قبل أحد مواطني [الدولة المشترعة] خارج إقليم [الدولة المشترعة]، إذا كان سلوك هذا الشخص يشكل أيضًا جريمة بموجب قانون البلد الذي ارتكبت فيه الجريمة. **المادة 30 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - الاختصاص** 1. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد اختصاصها على أي من الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية وذلك إذا ارتكبت الجريمة كلياً أو جزئياً أو تحققت:		

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
في إقليم الدولة الطرف على متن سفينة تحمل علم الدولة الطرف. على متن طائرة مسجلة تحت قوانين الدولة الطرف. من قبل أحد مواطني الدولة الطرف إذا كانت الجريمة يعاقب عليها حسب القانون الداخلي في مكان ارتكبها أو إذ ارتكبت خارج منطقة الاختصاص القضائي لأية دولة. إذا كانت الجريمة تمس أحد المصالح العليا للدولة. 2. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد الاختصاص الذي يغطي الجرائم المنصوص عليها في المادة 31 الفقرة 1 من هذه الاتفاقية في الحالات التي يكون فيها الجاني المزعوم حاضرا في إقليم تلك الدولة الطرف ولا يقوم بتسليمه إلى طرف آخر بناء على جنسيته بعد طلب التسليم. 3. إذا ادعت أكثر من دولة بالاختصاص القضائي لجريمة منصوص عليها في هذه الاتفاقية فيقدم طلب الدولة التي أخلت الجريمة بأمنها أو بمصالحها ثم الدولة التي وقعت الجريمة في إقليم ثم الدولة التي يكون الشخص المطلوب من رعاياها وإذا اتحدت الظروف فتقدم الدولة الأسبق في طلب التسليم. في حالة وجود ظروف مماثلة، تُعطى الأولوية لأول دولة تطلب التسليم.		
	لا يوجد معادل	**التحليل القانوني** تُعد هذه آلية أساسية لتحقيق قدرة فعالة في مجال التحقيق في الجرائم السيبرانية وهي مطلب في اتفاقية بودابست. **تحليل الفجوة** **التوصيات:** لا ينبغي أن يتطلب ذلك تشريعًا خاصًا لتنفيذه، وفيما يتعلق بالموارد يجب أن تُعطى الأولوية. يجب مشاركة تفاصيل الاتصال لنقطة الاتصال الوحيدة المعينة (SPOC) على المستوى الوطني ومع السلطات المركزية على المستوى الدولي والإنتربول. ينبغي أيضًا النظر في صياغة مذكرة تفاهم مع الوكالات الوطنية بحيث يكون لدى نقطة الاتصال الوحيدة المعينة سلطة القيام بالإجراءات المطلوبة كجزء من تحقيق دولي في جرائم الإنترنت وتطبيق القوانين والمعاهدات الوطنية. ستتضمن مذكرة التفاهم هذه الطلبات الواردة والصادرة وتضمن عملية فعالة وكفؤة.

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 35 من اتفاقية بودابست[341] **شبكة تعمل على مدار اليوم والساعة** 1. يعين كل طرف جهة اتصال متاحة على مدار أربع وعشرين ساعة وطوال أيام الأسبوع، من أجل ضمان تقديم مساعدة فورية بغرض إجراء تحقيقات أو إجراءات تتعلق بالجرائم الجنائية المتعلقة بأنظمة الحاسوب والبيانات، أو لجمع أدلة عن الجرائم الجنائية في شكل إلكتروني. يجب أن تشمل هذه المساعدة تيسير الإجراءات التالية، أو تنفيذها مباشرة إذا سمح القانون الداخلي بذلك: a. تقديم المشورة الفنية؛ الحفاظ على البيانات وفقا للمادتين 29 و 30؛ جمع الأدلة وتوفير المعلومات القانونية وتحديد مكان المشتبه به. 2. يجب أن يكون لدى جهة الاتصال التابعة لكل طرف القدرة على إجراء الاتصالات مع جهة اتصال الطرف الآخر على وجه السرعة. إذا لم تكن نقطة الاتصال التي حددها أحد الأطراف جزءًا من سلطة أو سلطات ذلك الطرف المسؤولة عن المساعدة أو التسليم المتبادلين الدوليين، فيجب أن تضمن قدرتها على التنسيق مع هذه السلطة أو السلطات على وجه السرعة. 3. يجب على كل طرف التأكد من توفر الأفراد المدربين والمجهزين من أجل تسهيل تشغيل الشبكة.		
المادة 25 من اتفاقية بودابست **المبادئ العامة المتعلقة بالمساعدة المتبادلة** 1. يقدم الطرفان المساعدة المتبادلة إلى أقصى حد ممكن لغرض إجراء التحقيقات أو الإجراءات المتعلقة بالجرائم الجنائية المتعلقة بأنظمة الحاسوب والبيانات، أو لجمع الأدلة المتعلقة بالجرائم الجنائية في شكل إلكتروني. 2. يعتمد كل طرف أيضًا الإجراءات التشريعية وغيرها من الإجراءات التي قد تكون ضرورية لتنفيذ الالتزامات المنصوص عليها في المواد من 27 إلى 35.		**التحليل القانوني** تضمن المادة 25 من اتفاقية بودابست إمكانية استخدامها كأداة لتسهيل المساعدة القانونية المتبادلة. صادق المغرب على اتفاقية بودابست، وسيكون هذا الأساس للتعاون مع الدول الأخرى التي صادقت على الاتفاقية. بدون التشريعات الوطنية، لا يمكن للدول غير الموقعة على اتفاقية بودابست تقديم طلبات للحفظ المستعجل لبيانات الحاسوب المخزنة والحفظ المستعجل والكشف الجزئي لبيانات الحركة والكشف عن البيانات المخزنة وبيانات الحركة، بمعنى وجود قيود على التعاون الدولي الذي يمكن أن يوفره المغرب للدول مقدمة الطلب.

341. المادة 43 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
3. يجوز لكل طرف في الظروف العاجلة تقديم طلبات للمساعدة المتبادلة أو الاتصالات المتعلقة بها عن طريق وسائل الاتصال العاجلة، بما في ذلك الفاكس أو البريد الإلكتروني، إلى الحد الذي توفر فيه هذه الوسائل مستويات مناسبة من الأمن والمصادقة (بما في ذلك استخدام التشفير، عند الضرورة)، مع تأكيد رسمي لاحق، حيثما يطلب ذلك الطرف متلقي الطلب. يجب على الطرف متلقي الطلب قبول الطلب والرد عليه بأي وسيلة اتصال سريعة. 4. باستثناء ما هو منصوص عليه على وجه التحديد في المواد الواردة في هذا الفصل، تخضع المساعدة المتبادلة للشروط المنصوص عليها في قانون الطرف متلقي الطلب أو معاهدات المساعدة المتبادلة المطبقة، بما في ذلك الأسباب التي تُجيز للطرف متلقي الطلب أن يرفض التعاون. لا يجوز للطرف متلقي أن يبني حقه في رفض المساعدة المتبادلة المتعلقة بالجرائم المشار إليها في المواد من 2 إلى 11، فقط على أساس أن الطلب يتعلق بجريمة يعتبرها جريمة مالية. 5. عندما تسمح أحكام هذا الفصل للطرف متلقي الطلب بتقييد المساعدة المتبادلة بشرط ازدواجية التجريم، يعتبر هذا الشرط مستوفيًا، بصرف النظر عما إذا كانت قوانينه تضع الجريمة في نفس الفئة الجرمية، أو إذا أعطيت الجريمة نفس التسمية عند الطرف الطالب، وذلك إن كان السلوك الكامن وراء الجريمة التي طلبت المساعدة من أجلها جريمة جنائية بموجب قوانينه. **المادة 34 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - الإجراءات المتعلقة بطلبات التعاون والمساعدة المتبادلة** 1. تطبق أحكام الفقرات 9-2 من هذه المادة في حالة عدم وجود معاهدة أو اتفاقية تعاون ومساعدة متبادلة وفقًا للتشريعات المعمول بها بين الدول الأطراف التي تطلب المساعدة وتلك التي تُطلَب منها المساعدة. في حال وجوده جود معاهدة أو اتفاقية فلا تطبق الفقرات المشار إليها إلا إذا اتفقت الأطراف المعنية على تطبيقها كاملة أو بشكل جزئي .		**تحليل الفجوة** **التوصيات:** يُطلب من القانون المحلي الحفاظ على بيانات الحاسوب المخزنة على وجه السرعة، والحفظ المستعجل والكشف الجزئي لبيانات الحركة وطلبات النسخ. يمكن استخدام اتفاقية بودابست كسوابق للحفظ المستعجل لبيانات الحاسوب المخزنة[342] والحفظ المستعجل والكشف الجزئي لبيانات الحركة[343] والكشف عن البيانات المخزنة[344] وبيانات الحركة[345]. ينبغي النظر في السماح للسلطات المختصة بإعطاء الإذن لهيئات إنفاذ القانون المحلي بإجراء تحقيق في الدولة التي تأكد فيها الوصول إلى الجهاز. يعد الوصول إلى المعلومات هو المعيار الأساسي لبدء التحقيق في الحالات التي يتعذر فيها معرفة مكان تخزين البيانات (أي في التخزين السحابي). يمكن أن يشمل ذلك "اعترافًا متبادلًا" بأوامر المحكمة الصادرة تجاه مقدمي خدمات الاتصالات في دولة معينة، والتي يمكن تقديمها إلى فروع مقدمي خدمة العملاء الموجودين في دول أخرى، اعتمادًا على مكان تخزين البيانات.

342. المادة 29 من اتفاقية بودابست
343. المادة 30 من اتفاقية بودابست
344. المادة 31 من اتفاقية بودابست
345. المادة 33 من اتفاقية بودابست

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
2. على كل دولة طرف تحديد سلطة مركزية تكون مسؤولة عن إرسال وإجابة طلبات المساعدة المتبادلة وتنفيذ هذه الطلبات وإيصالها إلى السلطات المعنية لتنفيذها. a. على السلطات المركزية أن تتصل ببعضها مباشرة. b. على كل دولة طرف - وقت التوقيع أو إيداع أدوات التصديق أو القبول أو الموافقة - أن تتصل بالأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس العدل العرب وتنقل إليهما أسماء وعناوين السلطات المحددة خصيصا لغايات هذه الفقرة. c. تقوم الأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس وزراء العدل العرب بإنشاء وتحديث سجل للسلطات المركزية والمعينة من قبل الدول الأطراف. وعلى كل دولة طرف أن تتأكد من أن التفاصيل الموجودة في السجل صحيحة دائما 3. يتم تنفيذ طلبات المساعدة المتبادلة في هذه المادة وفقًا للإجراءات التي تحددها الدولة الطرف الطالبة، إلا في حالة عدم الامتثال لقانون الدولة الطرف متلقية طلب المساعدة. 4. يجوز للدولة الطرف المطلوب منها المساعدة أن تؤجل الإجراءات المتخذة بشأن الطلب إذا كانت هذه الإجراءات تؤثر على التحقيقات الجنائية التي تجري من قبل سلطاتها. 5. قبل رفض أو تأجيل المساعدة يجب على الدولة الطرف المطلوب منها المساعدة بعد استشارة الدولة الطرف الطالبة لها أن تقرر فيما إذ سيتم تلبية الطلب جزئيا أو يكون خاضعا للشروط التي قد ترها ضرورية. 6. تلتزم الدولة الطرف التي تطلب منها المساعدة بإبلاغ الدولة الطرف الطالبة بنتيجة تنفيذ الطلب. وإذا تم رفض أو تأجيل الطلب، يجب إعطاء أسباب هذا الرفض أو التأجيل. ويجب على الدولة الطرف المطلوب منها المساعدة أن تعلم الدولة الطرف الطالبة لها بالأسباب التي تمنع تنفيذ الطلب بشكل نهائي أو الأسباب التي تؤخره بشكل كبير.		

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
7. يجوز للدولة الطرف الطالبة للمساعدة أن تطلب من الدولة الطرف المطلوب منها المساعدة الإبقاء على سرية حقيقة ومضمون أي طلب يندرج في هذا الفصل ما عدا القدر لكافي لتنفيذ الطلب. وإذا لم تستطع الدولة الطرف المطلوب منها المساعدة الالتزام بهذا الطلب للسرية، يجب عليها إعلام الدولة الطرف الطالبة والتي ستقرر مدى إمكانية تنفيذ الطلب. 8. • في الحالات العاجلة، يجوز إرسال طلبات المساعدة المتبادلة مباشرة إلى السلطات القضائية في الدولة الطرف المطلوب منها المساعدة من نظيرتها في الدولة الطرف الطالبة لها. وفي مثل هذه الحالات، يجب إرسال نسخة الوقت من السلطة المركزية في الدولة الطرف الطالبة إلى نظيرتها في الدولة الطرف المطلوب منها. • يجوز إجراء الاتصالات وتقديم الطلبات حسب هذه الفقرة بواسطة الإنتربول. • حيثما يتم تقديم طلب حسب الفقرة أ ولم تكن السلطة مختصة بالتعامل مع الطلب، فيجب عليها إحالة الطلب إلى السلطة المختصة وإعلام الدولة الطرف الطالبة للمساعدة مباشرة بذلك. • إن الاتصالات والطلبات التي تتم حسب هذه الفقرة والتي لا تشمل الإجراء القسري يمكن بثها مباشرة من قبل السلطات المختصة في الدولة الطرف الطالبة للمساعدة إلى نظيرتها في الدولة الطرف المطلوب منها المساعدة. • يجوز لكل دولة طرف، وقت التوقيع أو التصديق أو القبول أو الإقرار أو الانضمام إبلاغ الأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس وزراء العدل العرب بأن الطلبات حسب هذه الفقرة يجب توجيهها إلى السلطة المركزية لغايات الفعالية.		

التعاون الدولي		
أفضل الممارسات الدولية	**التشريع الوطني**	**ملاحظات**
المادة 26 من اتفاقية بودابست **المعلومات التلقائية** 1. يجوز للطرف، في حدود قانونه الداخلي ودون طلب مسبق، أن يحيل إلى الطرف الآخر المعلومات التي تم الحصول عليها في إطار تحقيقاته، عندما يرى أن الكشف عن هذه المعلومات قد يساعد الطرف المتلقي في بدء أو التحقيقات أو الإجراءات المتعلقة بالجرائم الجنائية المنصوص عليها في هذه الاتفاقية، أو قد تؤدي إلى طلب تعاون من جانب هذا الطرف بموجب هذا الفصل. 2. قبل تقديم هذه المعلومات، يجوز للطرف المقدم أن يطلب الحفاظ على سريتها أو استخدامها فقط وفقًا للشروط. إذا لم يستطع الطرف المتلقي الامتثال لهذا الطلب، فيجب عليه إخطار الطرف المقدم الذي يحدد بعد ذلك ما إذا كان ينبغي تقديم المعلومات. إذا قبل الطرف المتلقي المعلومات وفقًا لهذه الشروط فعليه أن يلتزم بها. **المادة 33 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - المعلومات العرضية المتلقاة** 1. يجوز لأي دولة طرف - ضمن حدود قانونها الداخلي - وبدون طلب مسبق أن تعطي لدولة أخرى معلومات حصلت عليها من خلال تحقيقاتها إذا اعتبرت أن كشف مثل هذه المعلومات يمكن أن تساعد الدولة الطرف المرسلة إليها في إجراء الشروع أو القيام بتحقيقات في الجرائم المنصوص عليها في هذه الاتفاقية أو قد تؤدي إلى طلب للتعاون من قبل تلك الدولة الطرف. 2. قبل إعطاء مثل هذه المعلومات يجوز للدولة الطرف المزودة أن تطلب الحفاظ على سرية المعلومات، وإذا لم تستطع الدولة الطرف المستقبلة الالتزام بهذا الطلب يجب عليها إبلاغ الدولة الطرف المزودة بذلك والتي تقرر بدورها مدى إمكانية التزويد بالمعلومات. وإذا قبلت الدولة الطرف المستقبلة المعلومات مشروطة بالسرية فيجب أن تبقى المعلومات بين الطرفين.	**لا يوجد معادل**	**التحليل القانوني** يعد هذا إجراءً هامًا لتمكين الدولة من الاحتفاظ بمعلومات من شأنها أن تساعد دولة أخرى على منع جريمة الإنترنت أو التحقيق فيها. وعلى الرغم من أن ذلك متاحًا بين الدول التي صادقت على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الوارد ذكرهم في المادة 33 من الاتفاقية، فليس للمغرب أي أساس قانوني محلي يجبره بمشاركة هذه المعلومات مع الدول غير الموقعة على الاتفاقية ما لم يتم إرسال طلب رسمي عبر قنوات المساعدة القانونية المتبادلة المعتادة. تنص المادة 18 (4) - (5) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة على تبادل المعلومات الاستخباراتية تلقائيًا في الأمور التي تفي بتعريف جريمة خطيرة[346]، ذات طابع عبر وطني[347] وأن جماعة إجرامية منظمة ضالعة في ارتكاب الجرم[348]. دون استيفاء هذا التعريف، يجب إرسال طلب رسمي عبر قنوات المساعدة القانونية المتبادلة المعتادة إلى الدول التي ليست عضوًا في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. وبسبب الطبيعة السريعة الحركة للجريمة السيبرانية، فإن المشاركة التلقائية هي وسيلة فعالة للتعاون مع الدول الأخرى، وغياب هذه المشاركة يمنع التعاون الدولي الفعال مع الدول غير العضو في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. **تحليل الفجوة** **التوصيات:** استخدمت اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة المادة 18 (4) - (5) أساسًا لمشاركة المعلومات التي تدخل ضمن مجال هذه الاتفاقية بشكل تلقائي (مع ضمانات مقدمة حول الاستخدام في الأدلة أو الكشف عن المعلومات الحساسة لطرف ثالث (بما في ذلك دولة أخرى).[349] النظر في التشريعات القائمة على المادة 33 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات أو المادة 26 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست.

346. يقصد بتعبير "جريمة خطيرة" في المادة 2 (ب) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة أي سلوك يمثل جرما يعاقب عليه بالحرمان التام من الحرية لمدة لا تقل عن أربع سنوات أو بعقوبة أشد"

347. المادة 3 (1) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية

348. تُعرّف المادة 2 (أ) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية «الجماعة الإجرامية المنظمة» بأنها جماعة ذات هيكل تنظيمي، مؤلفة من ثلاثة أشخاص أو أكثر، موجودة لفترة من الزمن وتعمل بصورة متضافرة بهدف ارتكاب واحدة أو أكثر من الجرائم الخطيرة أو الأفعال المجرمة وفقًا لهذه الاتفاقية، من أجل الحصول، بشكل مباشر أو غير مباشر، على منفعة مالية أو منفعة مادية أخرى"

349. انظر المادة 33 (2) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 32 من اتفاقية بودابست **الوصول عبر الحدود إلى بيانات الحاسوب المخزنة بموافقة أو عندما تكون متاحة للجمهور** يجوز للطرف، دون إذن من طرف آخر: الوصول إلى بيانات الحاسوب المخزنة (مفتوحة المصدر) المتاحة للجمهور، بغض النظر عن مكان وجود البيانات جغرافيا؛ أو الوصول إلى بيانات الحاسوب المخزنة الموجودة لدى طرف آخر أو استلامها، من خلال نظام حاسوب في إقليمها، إذا حصل الطرف على موافقة مشروعة وطوعية من الشخص الذي لديه السلطة القانونية للكشف عن البيانات للطرف من خلال نظام الحاسوب هذا. **القسم 27 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - البرامج الشرعية** 1. إذا كان [القاضي] [قاضي التحقيق] مقتنعًا بناءً على [معلومات مقدمة تحت القَسَم] [شهادة خطية] أنه في سياق تحقيق متعلق بجريمة مدرجة في الفقرة 7 أدناه، توجد أسباب معقولة للاعتقاد بأنه لا يمكن جمع الأدلة الأساسية عن طريق تطبيق أحكام أخرى مدرجة في الجزء الرابع ولكنها ضرورية لأغراض التحقيق الجنائي، فإن [القاضي] [القاضي] [أن] يأذن لضابط [إنفاذ القانون] [الشرطة] بناءً على طلب باستخدام برنامج شرعي عن بعد في مهمة محددة ضرورية للتحقيق وتثبيته في نظام الحاسوب المشتبه به من أجل جمع الأدلة ذات الصلة. يجب أن يحتوي الطلب على المعلومات التالية: • المشتبه في ارتكابه الجريمة، إذا كان ذلك ممكنا مع الاسم والعنوان؛ و • وصف نظام الحاسوب المستهدف؛ و • وصف الوسيلة المقصود ومدى ومدة الاستخدام؛ و • أسباب ضرورة الاستخدام. 2. من الضروري التأكد في مثل هذا التحقيق من أن التعديلات التي يتم إدخالها على نظام الحاسوب الخاص بالمشتبه به مقصورة على تلك الضرورية للتحقيق وأن أي تغييرات يمكن التراجع عنها إذا أمكن بعد نهاية التحقيق. أثناء التحقيق، من الضروري تسجيل الدخول	**لا يوجد معادل**	**التحليل القانوني** تمكن هذه السلطة الإجرائية الدولة من تأمين المحتوى المخزن في دولة أخرى في ظروف محدودة. المادة 32 ب. إن اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست والمادة 40 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات هما استثناء من مبدأ الإقليمية وتسمحان بوصول منفرد عبر الحدود دون الحاجة إلى مساعدة قانونية متبادلة عندما تكون هناك موافقة أو تكون المعلومات متاحة للجمهور. أمثلة على استخدام هذه السلطة الإجرائية بموجب المادة 32 من اتفاقية بودابست تتضمن: قد يتم تخزين البريد الإلكتروني لشخص ما في بلد آخر بواسطة مزود خدمة، أو قد يقوم شخص ما بتخزين البيانات عن قصد في بلد آخر. يجوز لهؤلاء الأشخاص استرداد البيانات بشرط أن يكون لديهم السلطة القانونية التي تخولهم ذلك، ويجوز لهم الكشف طوعًا عن البيانات لموظفي إنفاذ القانون أو السماح لهؤلاء المسؤولين بالوصول إلى البيانات[350] يمكن اعتقال إرهابي مشتبه به بشكل قانوني عندما يكون بريده الإلكتروني، الذي قد يحوي دليلًا على ارتكاب جريمة، مفتوحًا على الجهاز اللوحي أو الهاتف الذكي أو أي جهاز آخر. إذا وافق المشتبه طوعًا على وصول الشرطة إلى الحساب وإذا كانت الشرطة متأكدة من وجود بيانات صندوق البريد في ولاية أخرى، يجوز للشرطة الوصول إلى البيانات بموجب المادة 32. ب. **تحليل الفجوة** **التوصيات:** تم تضمين هذه السلطة التي تؤمن الأدلة من طرف واحد في التشريعات مع ضمانات الحصول على الموافقة بشكل قانوني من المستخدم.[351] يمكن استخدام لغة المادة 32 من اتفاقية بودابست والمادة 40 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. تم انتقاد المادة 32.ب بشدة، ويمكن اعتبار أن موافقة الدولة حيث تُخزَّن بيانات الحاسوب قد تم الحصول عليها بالإضافة إلى المستخدم. ينص القسم 27 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية على البرامج الشرعية وهذا قد يسمح بالوصول إلى جهاز حاسوب في دولة أخرى. هناك عدد من القيود التي تشترط عدم إمكانية الحصول على الأدلة بوسائل أخرى، وتتطلب أمرًا قضائيًا، ويمكن أن تُطبَّق على جرائم معينة فقط ضمن مدة مقيدة (3 أشهر). يجب أيضًا إيلاء الاعتبار لموافقة الدولة الأخرى التي قد يتطفل عليها البرنامج الشرعي.

350. الفقرة 294، الصفحة 53 من التقرير الإيضاحي في اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست
351. يجب الانتباه لمواقف مثل عدم وجود المستخدم (في حالة الوفاة) وإذا كان يمكن الحصول على موافقة في دولة أخرى

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
• الوسيلة الفنية المستخدمة ووقت وتاريخ التطبيق؛ و • تحديد نظام الحاسوب وتفاصيل التعديلات التي أجريت في التحقيق؛ • أي معلومات تم الحصول عليها. يجب حماية المعلومات التي يتم الحصول عليها عن طريق استخدام هذا البرنامج من أي تعديل أو حذف غير مصرح به أو وصول غير مصرح به. 3. تقتصر مدة الترخيص في القسم 27 (1) على [3 أشهر]. يتم إيقاف الإجراء المتخذ على الفور إذا لم تعد شروط الترخيص مستوفاة. 4. يتضمن ترخيص تثبيت البرنامج الوصول عن بُعد إلى نظام الحاسوب المشتبه به. 5. إذا كانت عملية التثبيت تتطلب الوصول الفعلي إلى مكان ما، يجب استيفاء متطلبات القسم 20. 6. يجوز لضابط [تطبيق القانون] [الشرطة] أن يطلب من المحكمة أن تأمر مقدم خدمة بالمساعدة في عملية التسليم إذا لزم الأمر، وذلك بموجب أمر المحكمة الممنوح في (1) الطلب المذكور أعلاه. 7. [قائمة الجرائم]. 8. قد تقرر دولة عدم تنفيذ القسم 27. **المادة 40 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - الوصول إلى معلومات تقنية المعلومات عبر الحدود** يجوز لأي دولة طرف، وبدون الحصول على تفويض من دولة طرف أخرى: 1. أن تصل إلى معلومات تقنية المعلومات المتوفرة للعامة (مصدر مفتوح) بغض النظر عن الموقع الجغرافي للمعلومات. 2. أن تصل أو تستقبل- من خلال تقنية المعلومات في إقليمها- معلومات تقنية المعلومات الموجودة لدى الدولة الطرف الأخرى وذلك إذا كانت حاصلة على الموافقة الطوعية والقانونية من الشخص الذي يملك السلطة القانونية لكشف المعلومات إلى تلك الدولة الطرف بواسطة تقنية المعلومات المذكورة.		

فلسطين

صادقت السلطة الفلسطينية على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات وتم إصدار القانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية في 9 يوليو 2017.[352]

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 2 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست - الوصول غير المشروع يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لتجريم الوصول إلى النظام الكلي أو أي جزء من نظام الحاسوب، إذا ارتكب عمدًا، دون أي حق. قد يشترط طرف ما ارتكاب الجريمة عن طريق انتهاك إجراءات أمنية بقصد الحصول على بيانات الحاسوب أو نية أخرى غير نزيهة، أو فيما يتعلق بنظام كمبيوتر متصل بنظام كمبيوتر آخر. **المادة 6 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - جريمة الدخول غير المشروع** 1. الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به. 2. تشدد العقوبة إذا ترتب على هذا الدخول أو البقاء أو الاتصال أو الاستمرار بهذا الاتصال: محو أو تعديل أو تشويه أو نسخ أو نقل أو محو للبيانات المحفوظة وللأجهزة والأنظمة الالكترونية وشبكات الاتصال وإلحاق الضرر بالمستخدمين والمستفيدين. الحصول على معلومات حكومية سرية.	**القانون رقم 16 لعام 2017 بشأن الجرائم الإلكترونية** **المادة 4 (1)**	**التحليل القانوني** تتفق المادة 4 (1) مع المادة 6 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الي تشير إلى «الدخول أو البقاء أو الاتصال غير المشروع" دون تعريف معنى هذه الأفعال. تشير اتفاقية بودابست إلى «بدون حق" في المادة 2 على أساس أن الوصول غير مصرح به. أكد التقرير التفسيري لاتفاقية بودابست اشتقاق عبارة "بدون حق" مثل، "التصرف الذي تم دون سلطة (سواء كانت تشريعية أو تنفيذية أو إدارية أو قضائية أو تعاقدية أو توافقية) أو تصرفًا لا يشمله، بأي حال، الدفوع القانونية أو الأعذار أو المبررات أو المبادئ ذات الصلة بموجب القانون المحلي". كما تتضمن المادة 4 (1) من القانون الوطني جريمة التواجد غير القانوني. لا يتضمن التشريع الوطني البرامج ضمن تعريف «البيانات» **تحليل الفجوة** **التوصيات:** يمكن أن يتضمن التشريع الوطني إدراج البرامج ضمن تعريف البيانات لأن بعض البيانات تشمل البرامج والبعض الآخر لا تشملها. علاوةً على ذلك، يمكن أن يوفر التشريع الوطني تعريفًا لعبارة «الدخول غير المشروع" للتأكد من أنها ليست سوى جريمة دون مبرر أو عذر معقول. وهذا هو سبب إدراج اتفاقية بودابست لعبارة "بدون حق" والتي تضمن، على سبيل المثال، تبرير دخول مسؤولي إنفاذ القوانين إلى نظام الحاسوب لإجراء تحقيق.

352. النص متوفر باللغة العربية فقط

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 3 من اتفاقية بودابست **اعتراض غير قانوني** يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وتدابير أخرى لتجريم اعتراض عمليات نقل البيانات الحاسوبية غير العامة من نظام حاسوب وإليه وداخله، بما في ذلك الانبعاثات الكهرومغناطيسية من نظام الحاسوب الذي يحمل مثل هذه البيانات، وذلك عند ارتكاب هذا العمل عمدًا بوسائط تقنية، ويعتبر جريمة جنائية بموجب القانون الداخلي. قد يشترط الطرف أن تكون الجريمة قد ارتكبت بنية غير نزيهة، أو أن تتم ضد نظام حاسوب متصل بنظام حاسوب آخر. **المادة 7 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات** **اعتراض غير قانوني** الاعتراض غير القانوني المتعمد لحركة البيانات بأي وسيلة تقنية، وتعطيل نقل أو استقبال بيانات تكنولوجيا المعلومات.	**القانون رقم 16 لعام 2017 بشأن الجرائم الإلكترونية** **المادة 7**	**التحليل القانوني** يُعتبر تجريم هذا الفعل ضروريًا لمقاضاة عمليات نقل بيانات الحاسوب من وإلى وداخل نظام الحاسوب الذي قد يتم اعتراضه بشكل غير قانوني للحصول على معلومات (مثل wikileaks أو PanamaPapers). **تحليل الفجوة** **التوصيات:** من المفهوم أنه تم استخدام الصياغة من المادة 7 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - لا تحتوي الاتفاقية على تعريف لعبارة «بيانات تكنولوجيا المعلومات" والتي يجب أن تُدرج للفصل بينها وبين كلمة البيانات. يمكن أن يتضمن التشريع الوطني تعريفًا للبيانات أو بيانات الحاسوب فقط - تشير المادة 3 من اتفاقية بودابست إلى اعتراض «بيانات الحاسوب"التي تم تعريفها في المادة 1.ب من اتفاقية بودابست بأنها "أي بيانات حاسوب تتعلق باتصال عن طريق نظام حاسوب، يتم إنشاؤها بواسطة نظام حاسوب يشكل جزءًا من سلسلة الاتصال، وتعرض مصدر الاتصال أو وجهته أو مساره أو الوقت أو التاريخ أو حجمه أو مدته أو نوع الخدمة الأساسية."
المادة 4 من اتفاقية بودابست **التشويش على البيانات** يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لكي تجرم قوانينها الوطنية محو بيانات الحاسوب أو إتلافها أو تغييرها أو حذفها دون حق، وذلك عند ارتكابها عمدًا. 2 يجوز لأي طرف الاحتفاظ بالحق في المطالبة بأن السلوك الموصوف في الفقرة 1 يؤدي إلى ضرر جسيم. **القسم 7 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية- التشويش غير القانوني على البيانات** الشخص الذي يقوم بأي من الأفعال التالية عمدا ودون عذر أو مبرر قانوني أو يتجاوز عذرًا أو مبررًا قانونيًا: • محو أو إتلاف بيانات الحاسوب؛ أو • يحذف بيانات الحاسوب؛ أو • تغيير بيانات الحاسوب؛ أو • جعل بيانات الحاسوب بلا معنى لها أو غير ذات فائدة أو غير فعالة؛ أو • يعوق أو يقاطع أو يشوش على الاستخدام القانوني لبيانات الحاسوب؛ أو • يعوق أو يقاطع أو يشوش على أي شخص في استخدامه القانوني لبيانات الحاسوب؛ أو	**القانون رقم 16 لعام 2017 بشأن الجرائم الإلكترونية** **المادة 4 (3)**	**التحليل القانوني** إذا تم استخدام نفس الصياغة مع التشريع الوطني، على النحو المشار إليه في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، فلا تتم الإشارة إلى عبارة «بدون حق." علاوةً على ذلك، لا تتضمن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات إلغاء بيانات الحاسوب التي تعد عنصرًا من عناصر التصيد الاحتيالي للحصول على إمكانية الوصول غير القانوني عن طريق تثبيت برنامج Keylogger للحصول على معلومات حساسة.[353] **تحليل الفجوة** **التوصيات:** يمكن تصحيح نقص بعض العناصر الرئيسة المتعلقة بهذه الجريمة في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات باستخدام لغة المادة 4 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست أو القسم 7 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية. من شأن استخدام عبارة «بدون حق" (انظر أعلاه بشأن الدخول غير المشروع) أن يضمن لمسؤولي إنفاذ القوانين، على سبيل المثال، إمكانية التدخل في البيانات، إذا كان ذلك مناسبًا ومبررًا لغايات إجراء التحقيقات.

353. http://www.coe.int/en/web/cybercrime/guidance-notes

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
• يمنع الوصول إلى بيانات الحاسوب لأي شخص مصرح له بالوصول إليها؛ يعتبر جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً. **المادة 8 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات** **جريمة ضد سلامة البيانات** 1. تعمد محو أو حذف أو منع أو تعديل أو إخفاء بيانات تكنولوجيا المعلومات بشكل غير قانوني. 2. قد يطلب أحد الأطراف أن يتسبب الفعل بأضرار جسيمة من أجل تجريم الأفعال المذكورة في الفقرة 1.		
المادة 5 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[354] **التشويش على النظام** يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لكي تُجرّم في قانونها الداخلي أعمال الإعاقة الخطيرة التي ترتكب عمدًا ودون وجه حق من أجل إعاقة عمل نظام حاسوب من خلال إدخال بيانات حاسوب أو نقلها أو محوها أو حذفها أو إتلافها أو تغييرها أو منعها. **القسم 9 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - التشويش غير القانوني على النظام** 1. الشخص الذي يقوم عن قصد، ودون عذر أو مبرر قانوني، أو بتجاوز عذر أو مبرر قانوني: • أعاقة عمل نظام الحاسوب أو التشويش عليه؛ أو • إعاقة شخص يستخدم أو يشغل بشكل قانوني نظام الحاسوب أو التشويش عليه؛ يعتبر جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً.	**القانون رقم 16 لعام 2017 بشأن الجرائم الإلكترونية** **المادة 4 (3)**	**التحليل القانوني** لا تحتوي الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على جريمة التدخل في النظم، ولا تتضح الصيغة المستخدمة في التشريع الوطني. تشير المادة 11 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات إلى «التدخل في وظيفة أنظمة التشغيل وأنظمة الاتصالات أو محاولة تعطيلها أو تغييرها.» و«تعطيل الأجهزة والبرامج والمواقع الإلكترونية. وإن كان هذا بهدف ارتكاب جريمة «احتيال". هذه الجريمة من شأنها أن تمنع البرمجيات الخبيثة التي تتداخل مع عمل الحاسوب التي يقوم بها المناضل المقرصن دون هدف ارتكاب جريمة احتيال. **تحليل الفجوة** **التوصيات:** إن صياغة اتفاقية بودابست في المادة 5 أو القسم 9 من مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية تُعد سابقة مفيدة. ضع في اعتبارك أيضًا ما إذا كان منع الهجمات ضد البنية التحتية الحيوية ومحاكمة مرتكبيها يحتاج إلى جريمة منفصلة أو مشددة (انظر القسم 9 (2) من مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية). وستكون هذه الجريمة المشددة ذات صلة عندما يعيق الإرهابيون عمل أنظمة الحاسوب في المستشفيات خلال هجوم قطع الخدمة.[355]

354. لا يوجد ما يعادلها في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات
355. http://www.coe.int/en/web/cybercrime/guidance-notes

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
2. يعاقب أي شخص الذي يتعمد دون عذر أو مبرر قانوني، أو بتجاوز عذر قانوني أو مبرر، إعاقة نظام حاسوب مخصص حصريًا لاستخدام عمليات البنية التحتية الحيوية أو التشويش عليه، أو في الحالات التي لا يكون فيها هذا النظام مخصصًا للاستخدام الحصري في عمليات البنية التحتية الحيوية، ولكنه يستخدم في عمليات البنية التحتية الحيوية وتؤثر هذه الإعاقة على استخدام عمليات البنية التحتية الحيوية، بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً.		
المادة 6 من اتفاقية بودابست **سوء استخدام الأجهزة** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لتجريم الأفعال الإجرامية بموجب قوانينه الداخلي، عندما تُرتكب عمداً ودون حق: a. إنتاج أو بيع أو الشراء بغرض الاستخدام أو الاستيراد أو التوزيع أو توفير ما يلي بأية طريقة: i. أي جهاز، بما في ذلك برنامج الحاسوب، تم تصميمه أو تكييفه بشكل أساسي بغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من 2 إلى 5؛ كلمة مرور الحاسوب أو رمز الوصول أو البيانات المماثلة التي يمكن من خلالها الوصول إلى نظام الحاسوب كله أو جزء منه، بقصد استخدامه لغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من 2 إلى 5؛ و ii. حيازة عنصر مشار إليه في الفقرتين أ.1 أو 2 أعلاه، بقصد استخدامه لغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من 2 إلى 5. يجوز لأي طرف أن يشترط بموجب القانون امتلاك عدد من هذه العناصر قبل إسناد المسؤولية الجنائية.	**القانون رقم 16 لعام 2017 بشأن الجرائم الإلكترونية** **المادة 26**	**التحليل القانوني** كما ذكر أعلاه للوصول غير المشروع، لا توجد إشارة إلى «بدون حق" في المادة 9 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ستمكّن تجريم هذه الأفعال من ملاحقة إنتاج وبيع والشراء من أجل الاستخدام واستيراد وتوزيع رموز الوصول والبيانات المحوسبة الأخرى المستخدمة في ارتكاب جرائم الإنترنت - فمثلاً، يمكن الوصول إلى أنظمة الحاسوب لتسهيل أي هجوم إرهابي بالتدخل في شبكة الطاقة الكهربائية للبلد. **تحليل الفجوة** **التوصيات:** إذا تم استخدام الصياغة في المادة 9 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، فهذا لا يوضح ما إذا كانت تلك الأجهزة التي لها استخدام شرعي وكذلك استخدام جنائي («الاستخدام المزدوج") محظورة من عدمه - يمكن معالجة ذلك من خلال إدراج صياغة اتفاقية بودابست لعبارة "المكيف بشكل أساسي" يجب أن يوفر القانون الوطني عذرًا معقولًا حتى تتمكن أجهزة إنفاذ القانون من استخدام الأجهزة لتقنيات التحقيق الخاصة - راجع اللغة في المادة 2.6. اتفاقية بودابست أو القسم 10 (2) من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية باعتبارهما دليلًا.	

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
2. لا يجوز تفسير هذه المادة على أنها تفرض مسؤولية جنائية عندما لا يكون الغرض من الإنتاج أو البيع أو الشراء بغرض الاستخدام أو الاستيراد أو التوزيع أو التوفير أو حيازة المشار إليه في الفقرة 1 من هذه المادة ارتكاب جريمة منصوص عليها وفقًا للشروط المواد من 2 إلى 5 من هذه الاتفاقية، مثل الاختبارات المسموح بها أو حماية نظام الحاسوب. 3. يجوز لكل طرف أن يحتفظ بالحق في عدم تطبيق الفقرة 1 من هذه المادة، شريطة أن لا يتعلق التحفظ ببيع أو توزيع أو توفير المواد المشار إليها في الفقرة 1 أ من هذه المادة بطريقة أخرى **المادة 9 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات: جريمة إساءة استخدام وسائل تقنية المعلومات** 1. إنتاج أو بيع أو شراء أو استيراد أو توزيع أو توفير: a. أية أدوات أو برامج مصممة أو مكيفة لغايات ارتكاب الجرائم المبينة في المادة 6 إلى 8. b. كلمة سر نظام معلومات أو شيفرة دخول أو معلومات مشابهة يتم بواسطتها دخول نظام معلومات ما بقصد استخدامها لأية من الجرائم المبينة في المادة 6 إلى 8. c. حيازة أية أدوات أو برامج مذكورة في الفقرتين أعلاه، بقصد استخدامها لغايات ارتكاب أي من الجرائم المذكورة في المادة 6 إلى 8 **القسم 10 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الأجهزة غير القانونية** 1. يرتكب الشخص جريمة إذا: a. أنتج أو باع أو اشترى بغرض الاستخدام أو استورد أو صدّر أو وزع أو وفّر بأي طريقة، عن قصد ودون عذر أو مبرر قانوني أو بتجاوز عذر أو مبرر قانوني:		

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
i. جهاز، بما في ذلك برنامج حاسوب، تم تصميمه أو تكييفه بغرض ارتكاب جريمة محددة بموجب أحكام أخرى من الجزء الثاني من هذا القانون؛ أو كلمة مرور الحاسوب أو رمز الوصول أو البيانات المماثلة التي يمكن من خلالها الوصول إلى نظام الحاسوب كله أو جزء منه بقصد استخدامه من قبل أي شخص لغرض ارتكاب جريمة محددة بموجب أحكام أخرى من الجزء الثاني من هذا القانون؛ أو ii. كان في حوزته غرض مشار إليه في الفقرة الفرعية «1» أو «2»، وكان القصد هو استخدامه من قبل أي شخص لارتكاب جريمة محددة بموجب أحكام أخرى من الجزء الثاني من هذا القانون، فإنه يعاقب عند إدانته بارتكاب هذه الجريمة بالسجن لمدة لا تزيد عن [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً. 2. لا يجوز تفسير هذا الحكم على أنه يفرض مسؤولية جنائية عندما لا يكون الغرض من الإنتاج أو البيع أو الشراء للاستخدام أو الاستيراد أو التوزيع أو التوفير أو الحيازة المشار إليها في الفقرة 1 هو ارتكاب جريمة منصوص عليها وفقًا لأحكام أخرى من الجزء الثاني من هذا القانون، كأن تكون الأغراض مثل الاختبار أو الحماية المعتمدين لنظام الحاسوب. 3. قد يقرر بلد ما عدم تجريم الأجهزة غير القانونية أو قصر التجريم على الأجهزة المدرجة في الجدول.		

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 7 من اتفاقية بودابست **أعمال التزوير المرتبطة بالحاسوب** يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم إدخال بيانات الحاسوب أو تغييرها أو حذفها أو محوها، عند ارتكاب ذلك عن قصد وبدون حق، مما يؤدي إلى بيانات غير موثوقة بهدف أن يتم التعامل معها أو التصرف فيها لأغراض قانونية كما لو كانت أصلية، بصرف النظر عما إذا كانت البيانات قابلة للقراءة ومقروءة مباشرة أم لا. قد يطلب طرف ما وجود نية الاحتيال، أو نية غير شريفة مماثلة، قبل إسناد المسؤولية الجنائية. **القسم 11 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - أعمال التزوير المتعلقة بالحاسوب** 1. كل شخص يقوم عن قصد ودون عذر أو مبرر قانوني أو بتجاوز عذر قانوني أو مبرر، بإدخال أو تبديل أو حذف أو منع بيانات الحاسوب، مما ينتج عنه بيانات غير موثوقة بقصد التعامل معها أو التصرف فيها لأغراض قانونية كما لو كانت صحيحة، بصرف النظر عما إذا كانت البيانات قابلة للقراءة مباشرة أم لا، يعاقب عند الإدانة بهذه الأعمال بالسجن لمدة لا تزيد عن [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً. 2. تكون العقوبة إذا ارتكبت الجريمة المذكورة أعلاه عن طريق إرسال رسائل بريد إلكتروني متعددة من أنظمة الحاسوب أو من خلالها هي السجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً. **المادة 10 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات** **جريمة التزوير** يعني استخدام تقنية المعلومات تغيير حقيقة البيانات بطريقة تسبب الضرر بغرض استخدامها كبيانات حقيقية.	**القانون رقم 16 لعام 2017 بشأن الجرائم الإلكترونية** **المادة 11**	**التحليل القانوني** لا تشير الصياغة في المادة 10 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات إلى أي قصد غير شريف وتشترط التسبب في ضرر **تحليل الفجوة** **التوصيات:** لا تتطلب الصياغة في مادة اتفاقية بودابست ومواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية حدوث ضرر. تشترط اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست ومواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية فقط أن "البيانات الزائفة" "تعتبر" حقيقية المادة 7 من اتفاقية بودابست أو القسم 11 من مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية، لذلك، يتطلب الحماية من التزوير المرتبط بالحاسوب والذي قد يشمل التصيُّد الاحتيالي والتصيُّد الاحتيالي الموجَّه عند تلقي الضحية له دون حدوث أي ضرر. على سبيل المثال، قد يتم إدخال بيانات الحاسوب (مثل البيانات المستخدمة في جوازات السفر الإلكترونية) أو تغييرها أو حذفها أو إلغاؤها، مما يؤدي إلى اعتبار البيانات غير الموثوقة على أنها بيانات أصلية[356] دون حدوث أي ضرر. وبموجب الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لا يشكل ذلك جريمة. ضع في اعتبارك أيضًا القسم 11 (2) من مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية (غير مشمول في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات) الذي ينص على إرسال رسائل بريد إلكتروني متعددة باعتبارها جريمة مشددة.

356. http://www.coe.int/en/web/cybercrime/guidance-notes

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 8 من اتفاقية بودابست **الاحتيال المرتبط بالحاسوب** يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وتدابير أخرى لتجريم الأفعال التالية بموجب قوانينه الداخلية، عند ارتكابها عمداً ودون حق، بما يسبب فقدان الممتلكات لشخص آخر عن طريق: أي إدخال أو تغيير أو حذف أو إلغاء لبيانات الحاسوب، أي تدخل في عمل نظام الحاسوب، مع نية احتيال أو نية غير شريفة من أجل الحصول، دون حق، على منفعة اقتصادية لنفسه أو لشخص آخر. **المادة 11 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات: جريمة الاحتيال** التسبب بإلحاق الضرر بالمستفيدين والمستخدمين عن قصد وبدون وجه حق بنية الاحتيال لتحقيق المصالح والمنافع بطريقة غير مشروعة، للفاعل أو للغير، عن طريق: 1. إدخال أو تعديل أو محو أو حجب للمعلومات والبيانات. 2. التدخل في وظيفة أنظمة التشغيل وأنظمة الاتصالات أو محاولة تعطيلها أو تغييرها. 3. تعطيل الأجهزة والبرامج والمواقع الإلكترونية. **القسم 12 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الاحتيال المرتبط بالحاسوب** الشخص الذي يتسبب في فقدان الممتلكات لشخص آخر، عن قصد، ودون عذر أو مبرر قانوني أو بتجاوز عذر أو مبرر قانوني، وذلك عن طريق: • أي إدخال أو تغيير أو حذف أو إلغاء لبيانات الحاسوب؛ • أي تدخل في عمل نظام الحاسوب، بقصد احتيالي أو غير شريف للحصول، دون حق، على منفعة اقتصادية لنفسه أو لشخص آخر، وتكون عقوبة هذه الأعمال السجن لمدة لا تتجاوز [المدة] ، أو غرامة لا تتجاوز [المبلغ]، أو العقوبتين معاً.	**القانون رقم 16 لعام 2017 بشأن الجرائم الإلكترونية** **المادة 14**	**التحليل القانوني** الصياغة في المادة 11 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات غامضة مع عدم وجود إشارة إلى أي نية غير شريفة وتتطلب وقوع شكل من أشكال «الضرر" دون تعريف ماهيته **تحليل الفجوة** **التوصيات:** لا تتطلب الاتفاقية العربية لمكافحة جرائم تقنية المعلومات سوى النية - تتضمن الصياغة في اتفاقية بودابست أو مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية شرط وجود نية غير شريفة.

الجرائم		
أفضل الممارسات الدولية	**التشريع الوطني**	**ملاحظات**
المادة 9 من اتفاقية بودابست **الجرائم ذات الصلة بالمحتوى (مثل المواد الإباحية للأطفال)** 1. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم السلوك التالي في قوانينه المحلية، عندما يرتكب عمدا وبدون حق: a. إنتاج مواد إباحية للأطفال بغرض توزيعها من خلال نظام حاسوب؛ b. عرض أو إتاحة مواد إباحية للأطفال من خلال نظام الحاسوب؛ c. توزيع أو نقل المواد الإباحية للأطفال من خلال نظام الحاسوب؛ d. شراء مواد إباحية للأطفال من خلال نظام حاسوب بقصد الاستخدام الشخصي أو لإعطائها لشخص آخر؛ امتلاك مواد إباحية للأطفال في نظام حاسوب أو على وسائط تخزين بيانات الحاسوب. 2. لأغراض الفقرة 1 أعلاه، يجب أن يشمل مصطلح «استغلال الأطفال في المواد الإباحية» أية مواد إباحية تصور بصريًا: a. قاصر مشترك في سلوك جنسي صريح؛ b. شخص يبدو أنه قاصر يشارك في سلوك جنسي صريح؛ c. صور واقعية تمثل قاصرًا مشاركًا في سلوك جنسي صريح. 3. لأغراض الفقرة 2 أعلاه، يشمل مصطلح «القاصر» جميع الأشخاص الذين تقل أعمارهم عن 18 عامًا. ومع ذلك، يجوز لأي طرف أن يطلب حدًا أدنى للسن، لا يقل عن 16 عامًا. 4. يجوز لكل طرف أن يحتفظ بالحق في عدم تطبيق الفقرات الفرعية 1 ، د. و هـ ، و2، الفقرتين الفرعيتين ب. و ج كليًا أو جزئيًا. **المادة 12 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات: جريمة الإباحية** 1. إنتاج أو عرض أو توزيع أو توفير أو نشر أو شراء أو بيع أو استيراد مواد إباحية أو مخلة بالحياء بواسطة تقنية المعلومات. 2. يجب زيادة العقوبة على جرائم المواد الإباحية المتعلقة بالأطفال والقصر.	**القانون رقم 16 لعام 2017 بشأن الجرائم الإلكترونية** **المادة 16**	**التحليل القانوني** تجريم هذه الأعمال يعتبر أساسيًا من أجل حماية الأطفال من الأذى، وذلك من خلال تجريم توزيع الصور غير اللائقة للأطفال ونقلها وتوفيرها وعرضها وحيازتها. **تحليل الفجوة** **التوصيات:** إذا استُخدمت اللغة الواردة في المادة 12 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، فلا يوجد تعريف للطفل أو القاصر - ينبغي أن يكون هذا متسقًا مع التشريعات الوطنية الموجودة. تقدم المادة 9.3 من اتفاقية بودابست تعريف «القاصر" علاوة على ذلك، لا يوجد تعريف لمصطلح «الإخلال بالآداب العامة" بينما تعرف المادة 9.2 "المواد الإباحية المتعلقة بالأطفال" وترتكب الجريمة وفقًا للاتفاقية العربية لمكافحة جرائم تقنية المعلومات من خلال «تقنية المعلومات" المُعرفة في المادة 2 (1) من الاتفاقية ذاتها بأنها "أية وسيلة مادية أو معنوية أو مجموعة وسائل مترابطة أو غير مترابطة تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها وفقًا للأوامر والتعليمات المخزنة بها. ويشمل ذلك جميع المدخلات والمخرجات المرتبطة بها سلكيا أو لا سلكيا في نظام أو شبكة». كما تتم الإشارة إلى «مترابطة"لن يشمل ذلك وسائط التخزين على النحو المحظور في المادة 1.9 ه من اتفاقية بودابست ولا تغطي الاتفاقية العربية لمكافحة جرائم تقنية المعلومات جرائم «عرض" أو "إتاحة» أو «شراء للغير» صور إباحية للأطفال على النحو المحظور في المادة 1.9 من اتفاقية بودابست أو القسم 13 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
3. تغطي الزيادة المذكورة في الفقرة 2 من هذه المادة الحصول على المواد الإباحية المواد الإباحية المتعلقة بالأطفال والقصر أو المواد الخاصة بالأطفال والقصر المخلة بالحياء، من خلال وسائل تكنولوجيا المعلومات أو وسيلة تخزين لهذه التكنولوجيا. **القسم 13 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - المواد الإباحية للأطفال** 1. الشخص الذي يقوم عن قصد ودون عذر أو مبرر قانوني بـ: • إنتاج مواد إباحية للأطفال بغرض توزيعها من خلال نظام حاسوب؛ • تقديم أو توفير مواد إباحية للأطفال من خلال نظام حاسوب؛ • توزيع أو نقل المواد الإباحية عن الأطفال من خلال نظام حاسوب؛ • شراء و/ أو الحصول على مواد إباحية للأطفال من خلال نظام حاسوب لاستخدامه الشخصي أو لإعطائها لشخص آخر؛ • حيازة مواد إباحية للأطفال في نظام حاسوب أو على وسائط تخزين بيانات الحاسوب؛ أ • الوصول عمدًا، من خلال تكنولوجيا المعلومات والاتصالات، إلى المواد الإباحية عن الأطفال، يعتبر جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً. 2. يمكن الدفاع أمام تهمة بجريمة منصوص عليها في الفقرة (1) (ب) إلى (1) (و) إذا أثبت الشخص أن المواد الإباحية عن الأطفال كانت بغرض إنفاذ القانون بحسن نية. 3. لا يجوز لدولة ما أن تجرم السلوك الموصوف في القسم 13 (1) (د) - (و).		

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 10 من اتفاقية بودابست **انتهاك حقوق النشر** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وغيرها من التدابير لاعتبار انتهاك حقوق الطبع والنشر، جرائم جنائية بموجب قوانينه الداخلية، وفقًا للالتزامات التي تعهد بها بموجب قانون باريس الصادر في 24 يوليو 1971، مراجعة اتفاقية برن لحماية المصنفات الأدبية والفنية، والاتفاق المتعلق بجوانب حقوق الملكية الفكرية المتصلة بالتجارة ومعاهدة الويبو بشأن حق المؤلف، باستثناء أي حقوق معنوية ممنوحة بموجب هذه الاتفاقيات، عندما تُرتكب هذه الانتهاكات عمدا وعلى نطاق تجاري وعن طريق نظام الحاسوب. 2. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لاعتبار أي انتهاك للحقوق أدناه جرائم جنائية بموجب قوانينه الداخلية، وذلك عملاً بالالتزامات التي تعهد بها بموجب الاتفاقية الدولية لحماية فناني الأداء ومنتجي التسجيلات الصوتية وهيئات الإذاعة (اتفاقية روما) واتفاق جوانب حقوق الملكية الفكرية المتصلة بالتجارة ومعاهدة المنظمة العالمية للملكية الفكرية بشأن الأداء والتسجيل الصوتي، باستثناء أي حقوق معنوية ممنوحة بموجب هذه الاتفاقيات، حيثما ارتكبت هذه الانتهاكات عمدا وعلى نطاق تجاري وعن طريق نظام الحاسوب. 3. يجوز لأي طرف أن يحتفظ بالحق في عدم فرض مسؤولية جنائية بموجب الفقرتين 1 و 2 من هذه المادة في ظروف محدودة، شريطة توفر سبل انتصاف فعالة أخرى، وأن لا ينتقص هذا التحفظ من التزامات الطرف الدولية المنصوص عليها في المواثيق الدولية المشار إليها في الفقرتين 1 و 2 من هذه المادة. **المادة 17 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - الجرائم المتعلقة بحق المؤلف والحقوق المرتبطة بها** انتهاك حقوق النشر كما هو محدد وفقًا لقانون الدولة الطرف، إذا كان الفعل قد ارتكب عمداً وليس لغرض الاستخدام الشخصي، وانتهاك الحقوق المرتبطة بحقوق الطبع والنشر ذات الصلة على النحو المحدد وفقًا لقانون الدولة الطرف، إذا كان الفعل ارتكب عمدا وليس لهدف الاستخدام الشخصي.	**القانون رقم 16 لعام 2017 بشأن الجرائم الإلكترونية** **المادة 8**	**التحليل القانوني** تستخدم هيئات تطبيق القانون على الصعيد الدولي جرائم حقوق النشر الرقمية باعتبارها سلوكًا إجراميًا إضافيًا للتحقيق في العديد من أشكال جرائم الإنترنت ومحاكمة مرتكبيها (بما في ذلك جرائم مثل التصيّد الاحتيالي والاحتيال الإلكتروني والتزوير الإلكتروني ومواقع الويب الاحتيالية وانتهاكات البيانات وسرقتها). تميل إحدى هذه الجرائم الأساسية في العديد من الحالات إلى أن تكون انتهاكًا لحقوق النشر الرقمية. هجوم Sony الإلكتروني[357] ليس إلا مثالاً حديث العهد تضافرت فيه المنظمات الإجرامية والقوى المرتبطة بجرائم الإنترنت وسرقة البيانات/التجسس على الشركات وانتهاك حقوق الطبع والنشر لتكمل عمل بعضها البعض. إن عدم وجود أي أحكام تتعلق بالملكية الفكرية يشكل إخفاقًا في حماية الابتكار في القرن الحادي والعشرين لدول الجنوب الشريكة والشركات والمواطنين. قد تكون هذه الحقوق محمية في تشريعات أخرى لم تتم مراجعتها كجزء من هذا التحليل **تحليل الفجوة** **التوصيات:** يجب التأكد من وجود حماية ضد انتهاك حقوق النشر التي تتوافق مع الالتزامات الدولية.

357. https://en.wikipedia.org/wiki/Sony_Pictures_hack

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 11 من اتفاقية بودابست **المساعدة والتحريض** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لتجريم الأفعال التالية بموجب قانونه الداخلي، وذلك عندما يتم التحريض على ارتكاب أي من الجرائم المقررة وفقا للمواد من 2 إلى 10 من هذه الاتفاقية أو المساعدة عليها عمدًا، مع نية أن ترتكب هذه الجريمة. 2. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وتدابير أخرى لتجريم محاولة ارتكاب أي من الأفعال الإجرامية المنصوص عليها في المواد من 3 إلى 5 و 7 و 8 و 1.9 (أ) و (ج) من هذه الاتفاقية عمدًا. **المادة 19 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - محاولة ارتكاب الجرائم والاشتراك فيها** 1. الاشتراك في ارتكاب أية جريمة من الجرائم المنصوص عليها في هذا الفصل مع وجود نية ارتكاب الجريمة في قانون الدولة الطرف. 2. الشروع في ارتكاب الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية. 3. يجوز لأي دولة طرف الاحتفاظ بحقها في عدم تطبيق الفقرة الثانية من هذه المادة كليا أو جزئيا.	**القانون رقم 16 لعام 2017 بشأن الجرائم الإلكترونية** **المادة 52**	**التحليل القانوني** لا يوجد في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات مادة لتجريم أولئك الذين يساعدون ويحرضون على جرائم الإنترنت. وتنص المادة 19 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على الشروع في الفعل أيضًا **تحليل الفجوة** **التوصيات:** تشير المادة 19 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات فقط إلى الشروع في الفعل، وينبغي أن يستخدم التشريع الوطني المادة 11 من اتفاقية بودابست كسابقة لضمان إمكانية محاكمة من قاموا بتقديم المساعدة أو التحريض على ارتكاب الجرائم السيبرانية.
المادة 12 من اتفاقية بودابست **مسؤولية الشركات** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وتدابير أخرى لضمان أن الأشخاص الاعتباريين يمكن اعتبارهم مسؤولين عن أي جريمة جنائية منشأة وفقًا لهذه الاتفاقية، إذا ارتكبها أي شخص طبيعي لصالحهم، سواء كان ذلك بصفته الفردية أو باعتباره جزءًا من جهاز الشخص الاعتباري، أو باعتباره شخصًا قياديًا ضمن تنظيم الشخص الاعتباري، بناءً على: a. سلطة تمثيل الشخص الاعتباري؛ b. سلطة اتخاذ القرارات نيابة عن الشخص الاعتباري؛ c. سلطة ممارسة السيطرة داخل الشخص الاعتباري.	**القانون رقم 16 لعام 2017 بشأن الجرائم الإلكترونية** **المادة 52**	**التحليل القانوني** هذا الحكم هو عنصر أساسي بحيث يستطيع الأشخاص الاعتباريون (مثلًا الكيانات التجارية) التصرف نيابة عن الأشخاص الطبيعيين الذين تقع عليهم مسؤولية جنائية **تحليل الفجوة** **التوصيات:** لا تتضمن المادة 20 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات حكمًا يكون من الممكن فيه لكيان اعتباري أن يكون مسؤولاً عن الفعل عندما يكون الشخص الطبيعي المعني غير خاضعًا للإشراف أو الرقابة ويرتكب جريمة جنائية متصرفًا تحت سلطته - انظر المادة 2.12 من اتفاقية بودابست

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
2. بالإضافة إلى الحالات المنصوص عليها بالفعل في الفقرة 1 من هذه المادة، يتخذ كل طرف الإجراءات اللازمة لضمان أن يتحمل الشخص الاعتباري المسؤولية عندما يكون عدم الإشراف أو السيطرة من قبل أي شخص طبيعي مشار إليه في الفقرة 1 قد جعل من الممكن ارتكاب جريمة جنائية منصوص عليها بموجب هذه الاتفاقية لصالح ذلك الشخص الاعتباري من قبل شخص طبيعي يعمل تحت سلطته. 3. مع مراعاة المبادئ القانونية للطرف، قد تكون مسؤولية الشخص الاعتباري جنائية أو مدنية أو إدارية. 4. تكون هذه المسؤولية دون المساس بالمسؤولية الجنائية للأشخاص الطبيعيين الذين ارتكبوا الجريمة. **المادة 20 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات: المسؤولية الجنائية للأشخاص الطبيعيين أو الاعتباريين** تلتزم كل دولة طرف، مع مراعاة قانونها الداخلي، بترتيب المسؤولية الجنائية للأشخاص الاعتباريين عن الجرائم التي يرتكبها ممثلوها نيابة عنهم أو لصالحهم، دون الإخلال بفرض عقوبة على الشخص الذي ارتكب جريمة شخصيًا.		
البروتوكول الإضافي لاتفاقية الجريمة السيبرانية، المتعلق بتجريم أعمال العنصرية وكراهية الأجانب المرتكبة من خلال أنظمة الحاسوب **المادة 3[358] - نشر المواد التي تحض على العنصرية وكراهية الأجانب من خلال أنظمة الحاسوب** يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم السلوك التالي في قوانينه المحلية، عندما يرتكب عمدا وبدون حق: 1. توزيع المواد العنصرية وكراهية الأجانب أو إتاحتها للجمهور من خلال نظام الحاسوب. 2. يجوز لأي طرف أن يحتفظ بالحق في عدم إسناد المسؤولية الجنائية للسلوك على النحو المحدد في يجوز للطرف أن يحتفظ بالحق في عدم إسناد المسؤولية الجنائية بالتصرف على النحو المحدد في الفقرة 1 من هذه المادة، عندما تحض المواد الموزعة، كما هو محدد في الفقرة 1 من المادة 2، وتشجع على التمييز غير المرتبط بالكراهية أو العنف، شريطة أن تتوفر سبل انتصاف فعالة أخرى.	**القانون رقم 16 لعام 2017 بشأن الجرائم الإلكترونية** **المادة 24**	**التحليل القانوني** إذا تم استخدام المادة 3 من البروتوكول الإضافي، فهذه سابقة مناسبة

358. لا يوجد ما يعادلها في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

الجرائم		
أفضل الممارسات الدولية	**التشريع الوطني**	**ملاحظات**
3. بصرف النظر عن الفقرة 2 من هذه المادة، يجوز للطرف أن يحتفظ بالحق في عدم تطبيق الفقرة 1 على حالات التمييز، لأن هذه الفقرة لا يمكن أن تمثل سبل انتصاف فعالة على النحو المشار إليه الفقرة 2، وذلك بسبب مبادئ ثابتة في نظامه القانوني الوطني متعلقة بحرية التعبير.		
بروتوكول إضافي **المادة 4[359] - التهديد بدافع العنصرية وكراهية الأجانب** يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم السلوك التالي في قوانينه المحلية، عندما يرتكب عمدا وبدون حق: التهديد، من خلال نظام الحاسوب، بارتكاب جريمة جنائية خطيرة على النحو المحدد في قانونها الداخلي، (1) ضد أشخاص لسبب أنهم ينتمون إلى جماعة يميزها عرقها أو لونها أو نسبها أو أصلها القومي أو العرقي أو دينها، إذا تم استخدام أي من هذه العوامل ذريعةً، أو (2) ضد مجموعة من الأشخاص تتميز بأي من هذه الخصائص.	**القانون رقم 16 لعام 2017 بشأن الجرائم الإلكترونية** **المادة 24**	**التحليل القانوني** إذا تم استخدام المادة 4 من البروتوكول الإضافي، فهذه سابقة مناسبة
بروتوكول إضافي **المادة 5[360] - الإهانة بدافع العنصرية وكراهية الأجانب** يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم السلوك التالي في قوانينه المحلية، عندما يرتكب عمدا وبدون حق: 1. إهانة الجمهور، من خلال نظام حاسوبي، (1) الأشخاص لكونهم ينتمون إلى مجموعة يميزها عرقها أو لونها أو نسبها أو أصلها القومي أو العرقي أو دينها، إذا تم استخدام أي من هذه العوامل ذريعةً؛ أو (2) مجموعة من الأشخاص تتميز بأي من هذه الخصائص. 2. يجوز للطرف 2A إما: a. أن يشترط أن يكون للجريمة المشار إليها في الفقرة 1 من هذه المادة أثر على أن الشخص أو مجموعة الأشخاص المشار إليهم في الفقرة 1 والذين يتعرضون للكراهية أو الاحتقار أو السخرية؛ أو أن يحتفظ بالحق في عدم تطبيق الفقرة 1 من هذه المادة بشكل كلي أو جزئي.	**لا يوجد معادل**	**تحليل الفجوة** **التوصيات:** استخدم لغة اتفاقية بودابست في المادة 5 من البروتوكول الإضافي كدليل للتشريعات الوطنية

359. لا يوجد ما يعادلها في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات
360. لا يوجد ما يعادلها في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

الجرائم		
أفضل الممارسات الدولية	**التشريع الوطني**	**ملاحظات**
بروتوكول إضافي **المادة 6[361] - إنكار الإبادة الجماعية أو التقليل منها أو الموافقة عليها أو تبريرها** **جرائم ضد الإنسانية** يعتمد كل طرف ما قد يلزم من إجراءات تشريعية لجعل الأفعال التالية يعتبر جرائم جنائية بموجب قوانينها الداخلية، عندما تُرتكب عمداً وبدون حق: 1. توزيع أو توفير عبر نظام الحاسوب بأية طريقة من الطرق للجمهور، مواد تنكر أو تقلل أو تقر أو تقلل بشكل كبير الأفعال التي تشكل إبادة جماعية أو جرائم ضد الإنسانية، على النحو المحدد في القانون الدولي والمعترف بها على هذا النحو في القرارات النهائية والملزمة للمحكمة العسكرية الدولية، المنشأة بموجب اتفاقية لندن المؤرخة في 8 أغسطس 1945، أو أي محكمة دولية أخرى تنشأ بموجب المواثيق الدولية ذات الصلة والتي يعترف هذا الطرف باختصاصها القضائي. 2. 2A يجوز للطرف إما a. أن يشترط أن يكون الإنكار أو التقليل إلى الحد الأدنى المشار إليه في الفقرة 1 من هذه المادة قد ارتكب بهدف التحريض على الكراهية أو التمييز أو العنف ضد أي فرد أو مجموعة من الأفراد على أساس العرق أو اللون أو النسب أو الأصل القومي أو العرقي أو الدين أو إذا استخدمت هذه العوامل ذريعة لذلك، أو أن يحتفظ بالحق في عدم تطبيق الفقرة 1 من هذه المادة بشكل كلي أو جزئي.	**القانون رقم 16 لعام 2017 بشأن الجرائم الإلكترونية** **المادة 25**	**التحليل القانوني** إذا تم استخدام المادة 6 من البروتوكول الإضافي، فهذه سابقة مناسبة
جرائم إضافية للمراجعة		
الجرائم المتعلقة بالهوية **القسم 14 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية** يعاقب الشخص الذي يقوم عن قصد ودون عذر أو مبرر قانوني، أو يتجاوز عذرًا قانونيًا أو مبررًا باستخدام نظام حاسوب في أي مرحلة من مراحل الجريمة بنقل أو تملك أو استخدام وسيلة لتحديد الهوية شخص آخر بنية ارتكاب أي نشاط غير قانوني يشكل جريمة أو المساعدة أو التحريض عليها، عند إدانته بهذه الأعمال بالسجن لمدة لا تتجاوز [المدة] أو بغرامة لا يتجاوز [المبلغ]، أو بالعقوبتين معاً.	**القانون رقم 16 لعام 2017 بشأن الجرائم الإلكترونية** **المادة 10**	**التحليل القانوني** تغطي هذه الجريمة مرحلة التحضير لجريمة خيانة الأمانة المتعلقة بالهوية **تحليل الفجوة** **التوصيات:** إذا تم إدراج القسم 14 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية، فهذه سابقة مناسبة

361. لا يوجد ما يعادلها في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
الكشف عن تفاصيل التحقيق **القسم 16 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية** موفر خدمة الإنترنت الذي يتلقى أمرًا يتعلق بتحقيق جنائي ينص صراحةً على الحفاظ على السرية أو على التزام شبيه ينص عليه القانون، ثم يقوم عن عمد ودون عذر أو مبرر قانوني أو بتجاوز لعذر قانوني مبرر، بالإفصاح عن: • حقيقة أنه قد تم إصدار أمر؛ أو • أي شيء تم تنفيذه بموجب الأمر؛ أو • أي بيانات تم جمعها أو تسجيلها بموجب الطلب؛ يعتبر جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً.	**القانون رقم 16 لعام 2017 بشأن الجرائم الإلكترونية** **المادة 48**	**التحليل القانوني** يعاقب على اختراق البيانات والكشف عن المعلومات الحساسة التي يمكن أن تؤثر على التحقيقات الجنائية **تحليل الفجوة** **التوصيات:** إذا تم إدراج القسم 16 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية، فهذه سابقة مناسبة
عدم السماح بالمساعدة **القسم 17 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية** أي شخص آخر غير المشتبه فيه فشل عمداً دون عذر أو مبرر قانوني أو بتجاوز عذر أو مبرر قانوني، بمساعدة شخص أو السماح بمساعدته، بناءً على أمر مثلما تحدد المواد 20 إلى 22[362] يرتكب جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة] ، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً. قد يقرر أي بلد عدم تجريم عدم السماح بالمساعدة شرط أن تتوفر جزاءات فعالة أخرى.	**القانون رقم 16 لعام 2017 بشأن الجرائم الإلكترونية** **المادة 41**	**التحليل القانوني** تتعلق هذه الجريمة بالأشخاص الذين لديهم معرفة محددة بالأدلة ذات الصلة والذين يرفضون تقديم المساعدة. غالبًا ما يعتمد تطبيق القانون على هؤلاء الأشخاص لتأمين الأدلة في التحقيقات الإلكترونية. هنالك مخالفة مستقلة وهي عدم توفير كلمات مرور أو الوصول إلى الرموز للأجهزة المشفرة أو البيانات (مثل «مفتاح المعلومات المحمية") - ينص القسم 53 من قانون تنظيم سلطات التحقيق في المملكة المتحدة لعام 2000 (RIPA)[363] على وجود جرم جنائي يتحمله الأشخاص الذين لا يمتثلون للمادة 49 من إخطار RIPA والقاضية بالكشف عن «المفتاح" **تحليل الفجوة** **التوصيات:** إذا تم إدراج القسم 17 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية، فهذه سابقة مناسبة هنالك مخالفة مستقلة وهي عدم توفير كلمات مرور أو الوصول إلى الرموز للأجهزة المشفرة أو البيانات (مثل «مفتاح المعلومات المحمية") - ينص القسم 53 من قانون تنظيم سلطات التحقيق في المملكة المتحدة لعام 2000 (RIPA)[364] على وجود جرم جنائي يتحمله الأشخاص الذين لا يمتثلون للمادة 49 من إخطار RIPA والقاضية بالكشف عن «المفتاح"

362. أوامر البحث والاستيلاء والمساعدة والإنتاج
363. http://www.legislation.gov.uk/ukpga/2000/23/section/53
364. http://www.legislation.gov.uk/ukpga/2000/23/section/53

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المطاردة السيبرانية **القسم 18 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية** الشخص الذي يقوم، دون عذر أو مبرر قانوني، أو يتجاوز عذرًا قانونيًا أو مبررًا، ببدء أي اتصال إلكتروني، بقصد إكراه شخص ما أو تخويفه أو مضايقته أو التسبب في ضائقة عاطفية كبيرة له، باستخدام نظام حاسوب لدعم السلوك المتكرر والعدائي والعنيف، يرتكب جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً.	**القانون رقم 16 لعام 2017 بشأن الجرائم الإلكترونية** **المادة 15**	**التحليل القانوني** هذه الجريمة تُجرم من يضايقون الأشخاص عبر الإنترنت - قد تنص بعض الولايات القضائية على جرائم تحرش غير مرتبطة بالحاسوب - لكن يوصى باعتماد هذه الجريمة لمتابعة لتلك الجرائم المرتكبة عبر الإنترنت. **تحليل الفجوة** **التوصيات:** إذا تم إدراج القسم 18 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية، فهذه سابقة مناسبة
رعاية الأطفال على الإنترنت **القانون الجنائي الهولندي 248e** يعاقب الشخص الذي يقترح ترتيب لقاء، بوسائل عمل آلية أو باستخدام خدمة اتصال، مع شخص يعرف، أو ينبغي منطقيًا أن يعرف، أن هذا الشخص لم يصل بعد إلى سن السادسة عشرة، مع نية ارتكاب أفعال غير لائقة مع هذا الشخص أو لعمل صور عن عمل جنسي يشارك فيه هذا الشخص، بالسجن لمدة لا تقل عن سنتين أو بغرامة من الفئة الرابعة، إذا ارتكب أي عمل يقصد به تحقيق اللقاء. **قانون العقوبات الكندي** **القسم 172.1** 1. كل شخص يرتكب جريمة عن طريق وسائل الاتصالات أو يتواصل مع شخص يكون عمره 18 عامًا أو أقل، بغرض تسهيل ارتكاب جريمة مرتبطة بهذا الشخص، وذلك بموجب المادة الفرعية 153 (1)، أو القسم 155، أو 163.1، أو 170، أو 171، أو القسم الفرعي 212 (1) أو (2) أو (2.1) أو (4)؛ شخص يكون عمره أقل من 16 عامًا، أو يظن المتهم أن عمره أقل من 16 عامًا، بغرض تسهيل ارتكاب جريمة مرتبطة بهذا الشخص، وذلك بموجب المواد 151 أو 152، أو الفقرة الفرعية 160(3) أو 173 (2) أو الأقسام 271 أو 272 أو 273 أو 280؛ أو 2. شخص يكون عمره أقل من 14 عامًا، أو يظن المتهم أن عمره أقل من 14 عامًا، بغرض تسهيل ارتكاب جريمة مرتبطة بهذا الشخص بموجب المادة 281.	**القانون رقم 16 لعام 2017 بشأن الجرائم الإلكترونية** **المواد 61 (3) و (4) و 56**	**التحليل القانوني** لإثبات الجرم الهولندي، يلزم عقد لقاء لأغراض جنسية مع تقديم أدلة إثبات مأخوذة من تاريخ الدردشة عبر الإنترنت تفصح عن قصد جنسي؛ طلب عقد اللقاء مع الأدلة على أنه تم التخطيط لذلك (أي التاريخ والمكان). الغرض من القانون الكندي هو منع استدراج الكبار المفترسين للأطفال عبر الإنترنت. لا تتطلب هذه الجريمة حدوث جريمة جنسية. وهذا يعني أن المتهم لا يحتاج إلى الذهاب فعلاً لمقابلة الضحية شخصيًا. تكتمل الجريمة قبل اتخاذ أي إجراءات لارتكاب الجريمة الموضوعية. **تحليل الفجوة** **التوصيات:** إذا كان التشريع الوطني يحظر الاستدراج، دون اشتراط حدوث لقاء، فهذا مناسب.

الجرائم		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
العقوبة 3. يعتبر كل شخص يرتكب جريمة بموجب الفقرة الفرعية (1) مذنبًا مذنبًا بارتكاب جريمة ويكون عرضة لعقوبة السجن لمدة تتراوح بين 10 سنوات كحد أقصى وسنة واحدة كحد أدنى؛ أو مذنبًا بارتكاب جريمة يعاقب عليها في ملخص الإدانة بالسجن لمدة تتراوح بين 18 شهرًا كحد أقصى و 90 يومًا كحد أدنى. افتراض إعادة تقدير العمر 4. الأدلة على أن الشخص المشار إليه في الفقرة (1) (أ) أو (ب) أو (ج) قُدِّم للمتهم وعمره أقل من ثمانية عشر عامًا أو ستة عشر عامًا أو أربعة عشر عامًا، حسب الحالة، في حالة عدم وجود أدلة تثبت عكس ذلك تثبت أن المتهم يعتقد أن الشخص كان أقل من تلك السن. لا دفاع 5. لا يقبل دفاع المتهم أمام التهم الموجهة بموجب الفقرة (1) (أ) أو (ب) أو (ج) بأنه كان يعتقد أن الشخص المشار إليه في تلك الفقرة لا يقل عمره عن ثمانية عشر عامًا أو ستة عشر عامًا أو أربعة عشر عامًا، حسب الحالة، إلا في حالة اتخذ المتهم خطوات معقولة للتأكد من عمر الشخص.		

الإجراء		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
	مرسوم القانون رقم 20 لعام 2015 بشأن مكافحة غسيل الأموال وتمويل الإرهاب **المادة 33** صلاحيات النائب العام: يجوز للنائب العام، بناءً على قرار من المحكمة المختصة...الوصول إلى أنظمة الحاسوب والشبكات وأجهزة الحاسوب الرئيسية **القانون رقم 16 لعام 2017 بشأن الجرائم الإلكترونية** **المادة 33** **المادة 34:** يجوز للنيابة العامة الوصول إلى الأجهزة، أو الأدوات، أو الوسائل، أو البيانات، أو المعلومات الإلكترونية، أو بيانات الحركة، أو البيانات المتعلقة بحركة الاتصالات، أو بمستعمليها أو معلومات المحتوى ذات الصلة بالجريمة الإلكترونية.	**التحليل القانوني** هذه هي صلاحية التحقيق الأكثر أهمية ويجب أن تشير إلى الحصول على حق الوصول وليس التفتيش. في «التقرير التوضيحي لاتفاقية بودابست، يعني «البحث» التفتيش عن البيانات أو قراءتها أو فحصها أو مراجعتها. ويشمل ذلك مفهوم البحث عن البيانات والبحث عن (فحص) البيانات. لكلمة "الوصول" معنى محايد وتعكس بدقة أكثر المصطلحات الحاسوبية؛ يتم استخدامها كذلك في المادتين 26 و 27 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.[365] تتعلق المادة 33 من مرسوم القانون رقم 20 لعام 2015 بالحصول على المعلومات، لكنها لا تتوفر إلا لغسل الأموال وتمويل الإرهاب. ستكون المادة 33 من القانون رقم 16 لعام 2017 أكثر شمولاً وتنطبق على الجرائم السيبرانية التي تجرمها. تؤكد المادة 34 (1) الوصول إلى أجهزة الحاسوب والبيانات ذات الصلة بالجرائم في القانون رقم 16. تتيح المادة 34 (3) نسخ البيانات ذات الصلة إذا لم يتم حجزها. تمنع المادة 34 (4) الوصول إلى البيانات إذا لم يتم حجزها وتقتضي المادة 34 (5) الحفاظ على سلامة البيانات المحتجزة. تتوافق هذه الأحكام مع الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

365. الفقرة 191، الصفحة 33 التقرير التوضيحي لاتفاقية بودابست

الإجراء		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 26 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - فحص المعلومات المخزنة 1. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين سلطاتها المختصة من التفتيش أو الوصول إلى: a. تقنية معلومات أو جزء منها والمعلومات المخزنة فيها أو المخزنة عليها. b. بيئة أو وسيط تخزين معلومات تقنية معلومات والذي قد تكون معلومات التقنية مخزنة فيه أو عليه. 2. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من التفتيش أو الوصول إلى تقنية معلومات معينة أو جزء منها بما يتوافق مع الفقرة (-1 أ) إذا كان هناك اعتقاد بأن المعلومات المطلوبة مخزنة في تقنية معلومات أخرى أو جزء منها في إقليمها وكانت هذه المعلومات قابلة للوصول قانونا أو متوفرة في التقنية الأولى فيجوز توسيع نطاق التفتيش والوصول للتقنية الأخرى. **المادة 27 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - ضبط المعلومات المخزنة** 1. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من ضبط وتأمين معلومات تقنية المعلومات التي يتم الوصول إليها حسب الفقرة 1 من المادة 26 من هذه الاتفاقية. هذه الإجراءات تشمل صلاحيات: a. ضبط وتأمين تقنية المعلومات أو جزء منها أو وسيط تخزين معلومات تقنية المعلومات. b. عمل نسخة معلومات تقنية المعلومات والاحتفاظ بها. c. الحفاظ على سلامة معلومات تقنية المعلومات المخزنة. d. إزالة أو منع الوصول إلى تلك المعلومات في تقنية المعلومات التي يتم الوصول إليها. 2. تلتزم كل طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى أي شخص لديه معرفة بوظيفة تقنية المعلومات أو الإجراءات المطبقة لحماية تقنية المعلومات من أجل تقديم المعلومات الضرورية لإتمام تلك الإجراءات المذكورة في الفقرتين 2 و 3 من المادة 26 من هذه الاتفاقية.	يجوز للنيابة العامة الإذن بالضبط والتحفظ على كامل نظام المعلومات، أو جزء منه، أو أية وسيلة من وسائل تكنولوجيا المعلومات التي من شأنها أن تساعد على كشف الحقيقة. إذا لم يكن الضبط والتحفظ على نظام المعلومات ضروريًا أو تعذر إجراؤه، تنسخ البيانات أو المعلومات التي لها علاقة بالجريمة والبيانات التي تؤمن قراءتها وفهمها على وسيلة من وسائل تكنولوجيا المعلومات. إذا استحال إجراء الضبط والتحفظ عليه بصفة فعلية، وحفاظًا على أدلة الجريمة يتعين استعمال كافة الوسائل المناسبة لمنع الوصول والنفاذ إلى البيانات المخزنة بنظام المعلومات والوصول إليها. تتخذ الاحتياطات الضرورية للحفاظ على سلامة المضبوط المتحفظ عليه بما في ذلك الوسائل الفنية لحماية محتواها. تحرر قدر الإمكان قائمة بالمضبوط المتحفظ عليه بحضور المتهم أو من وجد لديه المضبوط المتحفظ عليه ويحرر تقرير بذلك. ويُحفظ لمضبوط المتحفظ عليه حسب الحالة في ظرف، أو مغلق مختوم، وتكتب عليه ورقة مع بيان تاريخ التحفظ وساعته وعدد المحاضر والقضية.	

الإجراء		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 16 من اتفاقية بودابست **الحفظ المستعجل لبيانات الحاسوب المخزنة والكشف عنها** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وغيرها من الإجراءات لتمكين سلطاته المختصة من طلب الحفظ السريع لبيانات الحاسوب المحددة أو الحصول عليها بشكل مماثل، بما في ذلك بيانات الحركة التي تم تخزينها عن طريق نظام حاسوبي، ولا سيما عندما يكون هناك أسباب للاعتقاد بأن بيانات الحاسوب معرضة بشكل خاص للفقد أو التعديل. 2. عندما يقوم أحد الأطراف بتنفيذ الفقرة 1 أعلاه عن طريق أمر شخص بحفظ بيانات الحاسوب المخزنة المحددة وذلك بوضعها في حوزته أو تحت سيطرته، يعتمد هذا الطرف الإجراءات التشريعية وغيرها من الإجراءات التي قد تكون ضرورية لإلزام ذلك الشخص بالحفاظ على سلامة بيانات الحاسوب لفترة زمنية طويلة، حدها الأقصى تسعين يومًا، وذلك لتمكين السلطات المختصة من طلب الكشف عنها. يجوز للطرف أن ينص على تجديد هذا الأمر لاحقًا. 3. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لإلزام الحارس أو أي شخص آخر يحفظ بيانات الحاسوب بالحفاظ على سرية تنفيذ هذه الإجراءات للفترة الزمنية المنصوص عليها في قانونه الداخلي. 4. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و 15.	**القانون رقم 16 لعام 2017 بشأن الجرائم الإلكترونية** **المادة 34**	**التحليل القانوني** هذه السلطة الإجرائية مهمة لضمان الحفاظ على البيانات المعرضة للحذف أو الفقد. **تحليل الفجوة** **التوصيات:** تعد هذه الصلاحية المعجلة للاحتفاظ بمعلومات المشترك الأساسية والبيانات الوصفية والمعاملات والمحتويات المخزنة ضرورية كجزء من تحقيقات جرائم الإنترنت لضمان أن تكون الأدلة متاحة للبحث والوصول والضبط والمراجعة. يتطلب التشريع الوطني تعريفات كافية لـ «معلومات المشترك أو BSI»،[366] و "بيانات الحركة"،[367] و "مزود خدمة الاتصالات"[368] للتأكد من أنه يمكن الحفاظ عليها. ينبغي إيلاء اهتمام لأن يكون طول مدة الحفظ معقولًا في هذه الظروف، وأن يُسمَح بتطبيق التمديد في الظروف الملحة - تنص اتفاقية بودابست والاتفاقية العربية لمكافحة جرائم تقنية المعلومات على 90 يومًا، فيما تنص اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية على 7 أيام. ووفقًا للتجربة فإن مدة 90 يومًا هي مدة قصيرة في التحقيقات عبر الإنترنت ، ويجب أن تكون حوالي 180 يومًا يمكن تمديدها.

366. انظر التعريف الوارد في قاموس المصطلحات أعلاه أو المادة 2(9) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات: «أي معلومات متعلقة بمشتركي الخدمة وتوجد لدى موفر الخدمة باستثناء المعلومات التي يمكن من خلالها معرفة ما يلي: نوع خدمة الاتصال المستخدمة والمتطلبات الفنية وفترة الخدمة. ب. هوية المشترك وعنوانه البريدي أو الجغرافي أو رقم الهاتف ومعلومات الدفع المتاحة بموجب اتفاقية الخدمة. ج. أي معلومات أخرى موجودة على موقع تركيب معدات الاتصالات بموجب اتفاقية الخدمة".

367. انظر المادة 1.د من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست: «أي بيانات حاسوب تتعلق باتصال عن طريق نظام حاسوب، يتم إنشاؤها بواسطة نظام حاسوب يشكل جزءًا من سلسلة الاتصال، وتعرض مصدر الاتصال أو وجهته أو مساره أو الوقت أو التاريخ أو حجمه أو مدته أو نوع الخدمة الأساسية"، **أو** القسم 3 (18) من مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية: «حركة البيانات تعني أي بيانات حاسوب تتعلق باتصال عن طريق نظام حاسوب، يتم إنشاؤها بواسطة نظام حاسوب يشكل جزءًا من سلسلة الاتصال، وتعرض مصدر الاتصال أو وجهته أو مساره أو الوقت أو التاريخ أو الحجم أو المدة أو نوع الخدمة الأساسية».

368. انظر المادة 1.ج. من اتفاقية بودابست: "1 أي كيان عام أو خاص يوفر للمستخدمين قدرة الاتصال عن طريق نظام الحاسوب، و 2 أي كيان آخر يعالج أو يخزن بيانات الحاسوب نيابة عن خدمة الاتصال هذه أو مستخدمي هذه الخدمة" **أو** المادة 2 (2) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات:»أي شخص طبيعي أو معنوي عام أو خاص يزود المشتركين بالخدمات للتواصل بواسطة تقنية المعلومات، أو يقوم بمعالجة أو تخزين المعلومات نيابة عن خدمة الاتصالات أو مستخدميها".

الإجراء		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
القسم 23 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الحفظ المستعجل إذا اقتنع ضابط [تطبيق القانون] [الشرطة] بوجود أسباب معقولة للاعتقاد بأن بيانات الحاسوب المطلوبة لأغراض التحقيق الجنائي معرضة للضياع أو التعديل، يجوز لضابط [تطبيق القانون] [الشرطة]، عن طريق إشعار مكتوب مقدم إلى شخص يتحكم في بيانات الحاسوب، أن يطلب من هذا الشخص الحفاظ على البيانات المحددة في الإشعار لمدة تصل إلى سبعة (7) أيام على وفقًا لما هو محدد في الإشعار. يمكن تمديد الفترة إلى ما بعد سبعة (7) أيام إذا سمح [قاضي]، بناءً على طلب من طرف واحد، وذلك لمدة زمنية أخرى محددة. **المادة 23 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات- الحفظ المستعجل للبيانات المخزنة في تكنولوجيا المعلومات** 1. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأمر أو الحصول على الحفظ العاجل للمعلومات المخزنة بما في ذلك معلومات تتبع المستخدمين والتي خزنت على تقنية معلومات وخصوصا إذا كان هناك اعتقاد بأن تلك المعلومات عرضة للفقدان أو التعديل. 2. تلتزم كل دولة طرف بتبني الإجراءات الضرورية فيما يتعلق بالفقرة 1 بواسطة إصدار أمر إلى شخص من أجل حفظ معلومات تقنية المعلومات المخزنة والموجودة بحيازته أو سيطرته ومن أجل إلزامه بحفظ وصيانة سلامة تلك المعلومات لمدة أقصاها 90 يوما قابلة للتجديد، من أجل تمكين السلطات المختصة من البحث والتقصي 3. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لإلزام الشخص المسؤول عن حفظ تقنية معلومات للإبقاء على سرية الإجراءات طوال الفترة القانونية المنصوص عليها في القانون الداخلي.		

الإجراء		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 24 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - لتحفظ العاجل والكشف الجزئي لمعلومات تتبع المستخدمين تلتزم كل دولة طرف بتبني الإجراءات الضرورية فيما يختص بمعلومات تتبع المستخدمين من أجل: 1. ضمان توفر الحفظ العاجل لمعلومات تتبع المستخدمين بغض النظر عن اشتراك واحد أو أكثر من مزودي الخدمة في بث تلك الاتصالات. 2. ضمان الكشف العاجل للسلطات المختصة لدى الدولة الطرف أو لشخص تعينه تلك السلطات لمقدار كاف من معلومات تتبع المستخدمين لتمكين الدولة الطرف من تحديد مزودي الخدمة ومسار بث الاتصالات.	**القانون رقم 16 لعام 2017 بشأن الجرائم الإلكترونية** **المادة 34**	**التحليل القانوني** تعد هذه الصلاحية الإجرائية مهمة بشكل خاص لضمان توفير مزودي خدمات الاتصالات لعناوين بروتوكول إنترنت التي يمكن من خلالها تحديد موقع مرتكب الجريمة السيبرانية. لا تحتوي الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على تعريف «تتبع المعلومات" - سيكون هذا مختلفًا عن بيانات حركة البيانات حيث أن الأخيرة ستشمل مصدر الاتصال أو وجهته أو مساره أو وقته أو تاريخه أو حجمه أو المدة أو نوع الخدمة الأساسية (انظر المادة 1.د. من اتفاقية بودابست أو القسم 3(18) من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية **تحليل الفجوة** **التوصيات:** يجب أن تتضمن هذه الصلاحية المعجلة، إلى جانب الكشف عن بيانات الحركة، تعريف «بيانات الحركة"و"مزود خدمة الاتصالات"[369]
المادة 25 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - أمر تسليم المعلومات تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى: 1. أي شخص في إقليمها لتسليم معلومات معينة في حيازة ذلك الشخص والمخزنة على تقنية معلومات أو وسيط تخزين معلومات. 2. أي مزود خدمة يقدم خدماته في إقليم الدولة الطرف لتسليم معلومات المشترك المتعلقة بتلك الخدمات في حوزة مزود الخدمة أو تحت سيطرته.	**القانون رقم 16 لعام 2017 بشأن الجرائم الإلكترونية** **المادة 32** **أمر النسخ**	**التحليل القانوني** هذا شرط أساسي لإجراء تحقيق فعال في جرائم الإنترنت وسيؤثر غيابه على الملاحقات القضائية والتعاون الدولي. **تحليل الفجوة** **التوصيات:** تعد هذه الصلاحية الأساسية ضرورية لضمان تقديم مزودي خدمة الاتصالات في السلطة الفلسطينية لمعلومات المشترك الأساسية وبيانات الحركة وبيانات المحتوى المخزنة. سيتطلب ذلك أيضًا تعريفات «معلومات المشترك أو معلومات المشترك الأساسية"، و "حركة البيانات" و "مزود خدمة الاتصالات".[370] المادة 25 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات تستخدم تعريفات مختلفة بما في ذلك «تكنولوجيا المعلومات"،[371] و"مزود الخدمة"[372] و"البيانات";[373] غير أنه من المستحسن أن تكون هناك تعريفات لـ «معلومات المشترك أو معلومات المشترك الأساسية" أو "حركة البيانات" لأنها ستكون أنواع مختلفة من الأدلة التي يمكن توليدها في دول الجنوب الشريكة. علاوة على ذلك، سوف تتطلب هذه السلطة من الأفراد وغيرهم (مثل الكيانات المؤسسية والمؤسسات المالية وغيرها من المنظمات) ممن يحملون البيانات أن يقوموا بتوليدها بناء على طلب سلطات إنفاذ القانون.

369. انظر التعريفات أعلاه

370. المرجع السابق

371. المادة 2 (1) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات: "أية وسيلة مادية أو معنوية أو مجموعة وسائل مترابطة أو غير مترابطة تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها وفقا للأوامر والتعليمات المخزونة بها. ويشمل ذلك جميع المدخلات والمخرجات المرتبطة بها سلكيا أو لا سلكيا في نظام أو شبكة".

372. المادة 2 (2) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات: «أي شخص طبيعي أو معنوي عام أو خاص يزود المشتركين بالخدمات للتواصل بواسطة تقنية المعلومات، أو يقوم بمعالجة أو تخزين المعلومات نيابة عن خدمة الاتصالات أو مستخدميها».

373. المادة 2 (3) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات: «كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة تقنية المعلومات، كالأرقام والحروف والرموز وما إلى ذلك». المادة 1.ب وتتضمن اتفاقية بودابست أيضًا برنامجًا مناسبًا لجعل نظام الحاسوب يقوم بأداء الوظيفة

الإجراء		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 29 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - اعتراض معلومات المحتوى 1. تلتزم كل دولة طرف باعتماد الإجراءات التشريعية اللازمة المتعلقة بسلسلة من الجرائم المنصوص عليها في القانون المحلي، وذلك لتمكين السلطات المختصة من: a. تسجيل أو جمع المعلومات من خلال الوسائل التقنية في أراضي هذه الدولة الطرف، أو b. التعاون مع السلطات المختصة ومساعدتها على تسريع جمع وتسجيل معلومات المحتوى الخاصة بالاتصالات ذات الصلة في إقليمها والتي يتم نقلها عن طريق تكنولوجيا المعلومات. 2. إذا تعذر على الدولة الطرف، بسبب النظام القانوني المحلي، اعتماد الإجراءات المبينة في الفقرة 1 (أ)، يجوز لها اعتماد إجراءات أخرى بالشكل الضروري لضمان تسريع جمع وتسجيل معلومات المحتوى المقابلة الاتصالات ذات الصلة في أراضيها باستخدام الوسائل التقنية في ذلك الإقليم. 3. تلتزم كل دولة طرف باعتماد الإجراءات اللازمة لمطالبة مقدم الخدمة بالحفاظ على سرية أي معلومات عند ممارسة السلطة المنصوص عليها في هذه المادة.	**مرسوم القانون رقم 20 لعام 2015 بشأن مكافحة غسيل الأموال وتمويل الإرهاب** **المادة 33** بناء على قرار من المحكمة المختصة، يجوز للنائب العام: 1. الرقابة على الحسابات المصرفية وغيرها من الحسابات المماثلة. 2. الوصول إلى أنظمة الحاسوب والشبكات وأجهزة الحاسوب الرئيسية 3. الإخضاع لمراقبة أو تتبع الاتصالات. 4. التسجيل الصوتي والمرئي أو تصوير أعمال أو سلوك أو محادثات. 5. اعتراض وحجز المراسلات. **القانون رقم 16 لعام 2017 بشأن الجرائم الإلكترونية** **المادة 35 (2)** للنيابة العامة أن تأمر بالجمع والتزويد الفوري لأي بيانات بما فيها حركات الاتصالات، أو معلومات إلكترونية، أو بيانات مرور، أو معلومات المحتوى التي تراها لازمة لمصلحة التحقيقات، باستعمال الوسائل الفنية المناسبة والاستعانة في ذلك عند الاقتضاء بمزودي الخدمة حسب نوع الخدمة التي يقدمها.	**التحليل القانوني** هذه الصلاحية ضرورية للتشريع الوطني لإلزام مزودي خدمة الاتصالات بالتعاون في جمع أو تسجيل بيانات المحتوى في الوقت الحقيقي في فلسطين. المادة 33 - يتعلق مرسوم القانون رقم 20 لعام 2015 فقط بتحقيقات غسل الأموال وتمويل الإرهاب. ستكون المادة 35 من القانون رقم 16 لعام 2017 أكثر شمولاً وتنطبق على الجرائم الإلكترونية التي تجرمها.
المادة 28 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست **الجمع السريع لمعلومات تتبع المستخدمين**	**القانون رقم 16 لعام 2017 بشأن الجرائم الإلكترونية** **المادة 35 (2)** للنيابة العامة أن تأمر بالجمع والتزويد الفوري لأي بيانات **بما فيها حركات الاتصالات، أو معلومات إلكترونية، أو بيانات مرور**، أو معلومات المحتوى التي تراها لازمة لمصلحة التحقيقات، باستعمال الوسائل الفنية المناسبة والاستعانة في ذلك عند الاقتضاء بمزودي الخدمة حسب نوع الخدمة التي يقدمها.	**التحليل القانوني** المادة 35 (2) لها نفس العتبة لمعلومات المحتوى - وهي جمع بيانات الحركة إذا اقتضى إجراء التحقيق ذلك. **تحليل الفجوة** **التوصيات:** يمكن إيلاء النظر إلى عتبة مختلفة. قد تكون هناك حالات لا يضع فيها مقدم الطلب عتبة قانونيةً أعلى لتأمين المحتوى، ولكن يمكن وجود عتبة أدنى لتأمين حركة المرور. ولهذا السبب، يجب أن يكون هناك تمييز بين جمع المحتوى المخزن وبيانات الحركة في الوقت الحقيقي.

الإجراء		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
		التزامات الاحتفاظ بالبيانات[374] تسمح مثل هذه السلطة لوكالات إنفاذ القانون بـ 1. تتبع وتحديد مصدر الاتصال 2. تحديد وجهة الاتصال؛ 3. تحديد تاريخ ووقت ومدة الاتصال؛ و 4. تحديد نوع الاتصال غير قادر على تحديد ما إذا كانت السلطة الفلسطينية لديها مثل هذا الالتزام[375]

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 30 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - الاختصاص 1. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد اختصاصها على أي من الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية وذلك إذا ارتكبت الجريمة كلياً أو جزئياً أو تحققت: a. في إقليم الدولة الطرف b. على متن سفينة تحمل علم الدولة الطرف. c. على متن طائرة مسجلة تحت قوانين الدولة الطرف. d. من قبل أحد مواطني الدولة الطرف إذا كانت الجريمة يعاقب عليها حسب القانون الداخلي في مكان ارتكبها أو إذ ارتكبت خارج منطقة الاختصاص القضائي لأية دولة. e. إذا كانت الجريمة تمس أحد المصالح العليا للدولة. 2. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد الاختصاص الذي يغطي الجرائم المنصوص عليها في المادة 31، الفقرة 1 من هذه الاتفاقية في الحالات التي يكون فيها الجاني المزعوم حاضرا في إقليم تلك الدولة الطرف ولا يقوم بتسليمه إلى طرف آخر بناء على جنسيته بعد طلب التسليم.	**القانون رقم 16 لعام 2017 بشأن الجرائم الإلكترونية** **المادة 2**	**التحليل القانوني** تضمن المادة نطاقًا واضحًا للجرائم السيبرانية ذات الطابع الدولي. **تحليل الفجوة** **التوصيات:** يضمن التشريع الوطني تحديد الاختصاص. إذا كان هناك تعارض بين السلطات القضائية، فيجب أن تؤخذ في الاعتبار المبادئ التوجيهية المتعلقة بتحديد الولاية القضائية المناسبة لمحاكمة جريمة ما - انظر المبادئ التوجيهية Eurojust لتقرير الولاية القضائية التي في الجرائم التي تجب ملاحقتها (المراجعة 2016)[376]

374. أصدر الاتحاد الأوروبي في عام 2006 توجيهه بشأن الاحتفاظ بالبيانات - اضطرت الدول الأعضاء في الاتحاد الأوروبي إلى تخزين بيانات الاتصالات الإلكترونية لمدة ستة أشهر على الأقل و 24 شهراً على الأكثر للتحقيق في الجرائم الخطيرة وكشفها ومقاضاة مرتكبيها. أبطلت محكمة العدل الأوروبية في عام 2014 توجيه الاحتفاظ بالبيانات، حيث قررت أنها قدمت ضمانات غير كافية ضد التدخلات في الخصوصية وحماية البيانات. في حالة عدم وجود توجيه صالح للاتحاد الأوروبي بشأن الاحتفاظ بالبيانات، يجوز للدول الأعضاء تقديم خطة للاحتفاظ بالبيانات - للاطلاع على الخطط الوطنية، انظر: http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention

375. تقرير ICMEC العالمي ، الصفحة 30

376. http://www.eurojust.europa.eu/Practitioners/operational/Documents/Operational-Guidelines-for-Deciding.pdf

التعاون الدولي		
أفضل الممارسات الدولية	**التشريع الوطني**	**ملاحظات**
3. إذا ادعت أكثر من دولة بالاختصاص القضائي لجريمة منصوص عليها في هذه الاتفاقية فيقدم طلب الدولة التي أخلت الجريمة بأمنها أو بمصالحها ثم الدولة التي وقعت الجريمة في إقليم ثم الدولة التي يكون الشخص المطلوب من رعاياها وإذا اتحدت الظروف فتقدم الدولة الأسبق في طلب التسليم. في حالة وجود ظروف مماثلة، تُعطى الأولوية لأول دولة تطلب التسليم.		
المادة 43 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات **الهيئات المتخصصة**[377] 1. تضمن كل دولة طرف، وفقا للمبادئ الأساسية لنظامها القانوني، وجود هيئة متخصصة مكرسة على مدار 24 ساعة في اليوم لضمان تقديم المساعدة العاجلة لأغراض التحقيق أو الإجراءات المتعلقة بجرائم تكنولوجيا المعلومات أو جمع الأدلة بشكل إلكتروني بشأن جريمة محددة. تتضمن هذه المساعدة تسهيل أو تنفيذ: a. تقديم المشورة الفنية. b. حماية المعلومات على أساس المادتين 37 و 38. c. جمع الأدلة وتقديم المعلومات القانونية وتحديد مكان المشتبه بهم. 2. a. يجب أن تكون هذه الهيئة في جميع الدول الأطراف قادرة على التواصل الفوري مع الهيئة المقابلة في أي دولة طرف أخرى b. إذا كانت الهيئة المذكورة، المعينة من قبل دولة طرف، ليست جزءًا من السلطات المسؤولة عن المساعدة الثنائية الدولية في تلك الدولة، يجب أن تضمن تلك الهيئة قدرتها على التنسيق الفوري مع تلك السلطات. c. تضمن كل دولة طرف توافر موارد بشرية قادرة على تيسير عمل الهيئة المذكورة أعلاه.	**لا يوجد معادل**	**التحليل القانوني** هذه آلية أساسية لتحقيق قدرة فعالة على التحقيق في الجرائم الإلكترونية. **تحليل الفجوة** **التوصيات:** لا ينبغي أن يتطلب ذلك تشريعًا خاصًا لتنفيذه، وفيما يتعلق بالموارد يجب أن تُعطى الأولوية. يجب مشاركة تفاصيل الاتصال لنقطة الاتصال الوحيدة المعينة (SPOC) على المستوى الوطني ومع السلطات المركزية على المستوى الدولي والإنتربول. ينبغي أيضًا النظر في صياغة مذكرة تفاهم مع الوكالات الوطنية بحيث يكون لدى نقطة الاتصال الوحيدة المعينة سلطة القيام بالإجراءات المطلوبة كجزء من تحقيق دولي في جرائم الإنترنت وتطبيق القوانين والمعاهدات الوطنية. ستتضمن مذكرة التفاهم هذه الطلبات الواردة والصادرة وتضمن عملية فعالة وكفؤة.

377. المادة 35 من اتفاقية بودابست

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 34 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - الإجراءات المتعلقة بطلبات التعاون والمساعدة المتبادلة 1. تطبق أحكام الفقرات 2-9 من هذه المادة في حالة عدم وجود معاهدة أو اتفاقية تعاون ومساعدة متبادلة وفقًا للتشريعات المعمول بها بين الدول الأطراف التي تطلب المساعدة وتلك التي تُطلب منها المساعدة. في حال وجوده جود معاهدة أو اتفاقية فلا تطبق الفقرات المشار إليها إلا إذا اتفقت الأطراف المعنية على تطبيقها كاملة أو بشكل جزئي. 2. a. على كل دولة طرف تحديد سلطة مركزية تكون مسؤولة عن إرسال وإجابة طلبات المساعدة المتبادلة وتنفيذ هذه الطلبات وإيصالها إلى السلطات المعنية لتنفيذها. b. على السلطات المركزية أن تتصل ببعضها مباشرة. c. على كل دولة طرف - وقت التوقيع أو إيداع أدوات التصديق أو القبول أو الموافقة - أن تتصل بالأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس العدل العرب وتنقل إليهما أسماء وعناوين السلطات المحددة خصيصا لغايات هذه الفقرة. d. تقوم الأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس وزراء العدل العرب بإنشاء وتحديث سجل للسلطات المركزية والمعينة من قبل الدول الأطراف. وعلى كل دولة طرف أن تتأكد من أن التفاصيل الموجودة في السجل صحيحة دائما 3. يتم تنفيذ طلبات المساعدة المتبادلة في هذه المادة وفقًا للإجراءات التي تحددها الدولة الطرف الطالبة، إلا في حالة عدم الامتثال لقانون الدولة الطرف متلقية طلب المساعدة. 4. يجوز للدولة الطرف المطلوب منها المساعدة أن تؤجل الإجراءات المتخذة بشأن الطلب إذا كانت هذه الإجراءات تؤثر على التحقيقات الجنائية التي تجري من قبل سلطاتها. 5. قبل رفض أو تأجيل المساعدة يجب على الدولة الطرف المطلوب منها المساعدة بعد استشارة الدولة الطرف الطالبة لها أن تقرر فيما إذ سيتم تلبية الطلب جزئيا أو يكون خاضعا للشروط التي قد ترها ضرورية.	**القانون رقم 16 لعام 2017 بشأن الجرائم الإلكترونية** **المادتان 43 و 44**	**التحليل القانوني** تضمن المادتان 32 و 34 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات إمكانية استخدامها كأداة لتسهيل المساعدة القانونية المتبادلة وينص القانون الوطني الآن على الحفظ المعجل لبيانات الحاسوب المخزنة والحفظ المعجل والكشف الجزئي لبيانات الحركة والكشف عن البيانات المخزنة وبيانات الحركة، واعتراض بيانات المحتوى، وجمع بيانات الحركة في الوقت الحقيقي ، أوامر الإنتاج، البحث والاحتجاز في حالات الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. كذلك، من خلال مبدأ المعاملة بالمثل، يمكن للسلطة الفلسطينية تنفيذ طلبات من تلك الدول الموقعة على اتفاقية بودابست وغيرها من الدول التي لديها نفس الإجراءات الإجرائية.

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
6. تلتزم الدولة الطرف المطلوب منها المساعدة أن تُعلِم الدولة الطرف الطالبة لها بنتيجة تنفيذ الطلب. وإذا تم رفض أو تأجيل الطلب، يجب إعطاء أسباب هذا الرفض أو التأجيل. ويجب على الدولة الطرف المطلوب منها المساعدة أن تعلم الدولة الطرف الطالبة لها بالأسباب التي تمنع تنفيذ الطلب بشكل نهائي أو الأسباب التي تؤخره بشكل كبير. 7. يجوز للدولة الطرف الطالبة للمساعدة أن تطلب من الدولة الطرف المطلوب منها المساعدة الإبقاء على سرية حقيقة ومضمون أي طلب يندرج في هذا الفصل ما عدا القدر لكافي لتنفيذ الطلب. وإذا لم تستطع الدولة الطرف المطلوب منها المساعدة الالتزام بهذا الطلب للسرية، يجب عليها إعلام الدولة الطرف الطالبة والتي ستقرر مدى إمكانية تنفيذ الطلب. 8. a. في الحالات العاجلة، يجوز إرسال طلبات المساعدة المتبادلة مباشرة إلى السلطات القضائية في الدولة الطرف المطلوب منها المساعدة من نظيرتها في الدولة الطرف الطالبة لها. وفي مثل هذه الحالات، يجب إرسال نسخة الوقت من السلطة المركزية في الدولة الطرف الطالبة إلى نظيرتها في الدولة الطرف المطلوب منها. b. يجوز إجراء الاتصالات وتقديم الطلبات حسب هذه الفقرة بواسطة الإنتربول. c. حيثما يتم تقديم طلب حسب الفقرة أ ولم تكن السلطة مختصة بالتعامل مع الطلب فيجب عليها إحالة الطلب إلى السلطة المختصة وإعلام الدولة الطرف الطالبة للمساعدة مباشرة بذلك. d. إن الاتصالات والطلبات التي تتم حسب هذه الفقرة والتي لا تشمل الإجراء القسري يمكن بثها مباشرة من قبل السلطات المختصة في الدولة الطرف الطالبة للمساعدة إلى نظيرتها في الدولة الطرف المطلوب منها المساعدة. e. يجوز لكل دولة طرف، وقت التوقيع أو التصديق أو القبول أو الإقرار أو الانضمام إبلاغ الأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس وزراء العدل العرب بأن الطلبات حسب هذه الفقرة يجب توجيهها إلى السلطة المركزية لغايات الفعالية.		

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 33 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - المعلومات العرضية المتلقاة 1. يجوز لأي دولة طرف - ضمن حدود قانونها الداخلي - وبدون طلب مسبق أن تعطي لدولة أخرى معلومات حصلت عليها من خلال تحقيقاتها إذا اعتبرت أن كشف مثل هذه المعلومات يمكن أن تساعد الدولة الطرف المرسلة إليها في إجراء الشروع أو القيام بتحقيقات في الجرائم المنصوص عليها في هذه الاتفاقية أو قد تؤدي إلى طلب للتعاون من قبل تلك الدولة الطرف. 2. قبل إعطاء مثل هذه المعلومات يجوز للدولة الطرف المزودة أن تطلب الحفاظ على سرية المعلومات، وإذا لم تستطع الدولة الطرف المستقبلة الالتزام بهذا الطلب يجب عليها إبلاغ الدولة الطرف المزودة بذلك والتي تقرر بدورها مدى إمكانية التزويد بالمعلومات. وإذا قبلت الدولة الطرف المستقبلة المعلومات مشروطة بالسرية، فيجب أن تبقى المعلومات بين الطرفين.	**القانون رقم 16 لعام 2017 بشأن الجرائم الإلكترونية** **المادة 43**	**التحليل القانوني** يعد هذا إجراءً هامًا لتمكين الدولة من الاحتفاظ بمعلومات من شأنها أن تساعد دولة أخرى على منع جريمة الإنترنت أو التحقيق فيها. ليس للسلطة الفلسطينية الآن أي أساس قانوني محلي لتبادل هذه المعلومات **تحليل الفجوة** **التوصيات:** ينبغي النظر في ضمانات بشأن استخدام المعلومات المقدمة تلقائيًا في الأدلة، أو الكشف عن المعلومات الحساسة لطرف ثالث (بما في ذلك دولة أخرى).[378]
المادة 40 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - الوصول إلى معلومات تقنية المعلومات عبر الحدود يجوز لأي دولة طرف، وبدون الحصول على تفويض من دولة طرف أخرى: 1. أن تصل إلى معلومات تقنية المعلومات المتوفرة للعامة (مصدر مفتوح) بغض النظر عن الموقع الجغرافي للمعلومات. 2. أن تصل إلى أو تتلقى - من خلال تقنية المعلومات في إقليمها - معلومات تقنية المعلومات الموجودة لدى الدولة الطرف الأخرى، وذلك بعد حصولها على الموافقة الطوعية والقانونية من الشخص الذي يملك السلطة القانونية لكشف المعلومات إلى تلك الدولة الطرف بواسطة تقنية المعلومات المذكورة.		**التحليل القانوني** تمكن هذه السلطة الإجرائية الدولة من تأمين المحتوى المخزن في دولة أخرى في ظروف محدودة. تعد المادة 40 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات استثناءً من مبدأ الإقليمية وتسمح بوصول منفرد عبر الحدود دون الحاجة إلى مساعدة قانونية متبادلة عندما تكون هناك موافقة من المستخدم أو تكون المعلومات متاحة للجمهور. تتضمن الأمثلة على استخدام هذه الصلاحية الإجرائية ما يلي: قد يتم تخزين البريد الإلكتروني لشخص ما في بلد آخر بواسطة مزود خدمة، أو قد يقوم شخص ما بتخزين البيانات عن قصد في بلد آخر. يجوز لهؤلاء الأشخاص استرداد البيانات بشرط أن يكون لديهم السلطة القانونية التي تخولهم ذلك، ويجوز لهم الكشف طوعًا عن البيانات لموظفي إنفاذ القانون أو السماح لهؤلاء المسؤولين بالوصول إلى البيانات[379] أو يمكن اعتقال إرهابي مشتبه به بشكل قانوني عندما يكون بريده الإلكتروني، الذي قد يحوي دليلًا على ارتكاب جريمة، مفتوحًا على الجهاز اللوحي أو الهاتف الذكي أو أي جهاز آخر. إذا وافق المشتبه طوعًا على وصول الشرطة إلى الحساب وإذا كانت الشرطة متأكدة من وجود بيانات صندوق البريد في ولاية أخرى، يجوز للشرطة الوصول إلى البيانات.

378. انظر المادة 33 (2) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات
379. الفقرة 294، الصفحة 52 من التقرير الإيضاحي في اتفاقية بودابست

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
القسم 27 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - برامج الخبرة الشرعية 1. إذا كان [القاضي] [قاضي التحقيق] مقتنعًا بناءً على [معلومات مقدمة تحت القَسَم] [شهادة خطية] أنه في سياق تحقيق متعلق بجريمة مدرجة في الفقرة 7 أدناه، توجد أسباب معقولة للاعتقاد بأنه لا يمكن جمع الأدلة الأساسية عن طريق تطبيق أحكام أخرى مدرجة في الجزء الرابع ولكنها ضرورية لأغراض التحقيق الجنائي، فإن [القاضي] [القاضي] [أن] يأذن لضابط [إنفاذ القانون] [الشرطة] بناءً على طلب باستخدام برنامج شرعي عن بعد في مهمة محددة ضرورية للتحقيق وتثبيته في نظام الحاسوب المشتبه به من أجل جمع الأدلة ذات الصلة. يجب أن يحتوي الطلب على المعلومات التالية: • المشتبه في ارتكابه الجريمة، إذا كان ذلك ممكنا مع الاسم والعنوان؛ و • وصف نظام الحاسوب المستهدف؛ و • وصف الوسيلة المقصود ومدى ومدة الاستخدام؛ و • أسباب ضرورة الاستخدام. 2. من الضروري التأكد في مثل هذا التحقيق من أن التعديلات التي يتم إدخالها على نظام الحاسوب الخاص بالمشتبه به مقصورة على تلك الضرورية للتحقيق وأن أي تغييرات يمكن التراجع عنها إذا أمكن بعد نهاية التحقيق. أثناء التحقيق، من الضروري تسجيل الدخول a. الوسيلة الفنية المستخدمة ووقت وتاريخ التطبيق؛ و b. تحديد نظام الحاسوب وتفاصيل التعديلات التي أجريت في التحقيق؛ c. أي معلومات تم الحصول عليها. يجب حماية المعلومات التي يتم الحصول عليها عن طريق استخدام هذا البرنامج من أي تعديل أو حذف غير مصرح به أو وصول غير مصرح به.		**تحليل الفجوة** **التوصيات:** تم تضمين هذه الصلاحية المقيدة التي تؤمن الأدلة من طرف واحد في التشريعات مع ضمانات الحصول على الموافقة بشكل قانوني من المستخدم.[380] لا تنص المادة 40 على موافقة الدولة التي تتلقى الطلب. ينص القسم 27 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية وجود عدد من القيود التي تشترط عدم إمكانية الحصول على الأدلة بوسائل أخرى، وتتطلب أمرًا قضائيًا، ولا يمكن أن تُطبَّق إلا على جرائم معينة فقط وضمن مدة مقيدة (3 أشهر). يجب أيضًا إيلاء الاعتبار لموافقة الدولة الأخرى التي قد يتطفل عليها البرنامج الشرعي.

380. يجب الانتباه لمواقف مثل عدم وجود المستخدم (في حالة الوفاة) وإذا كان يمكن الحصول على موافقة في دولة أخرى

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
3. تقتصر مدة الترخيص في القسم 27 (1) على [3 أشهر]. يتم إيقاف الإجراء المتخذ على الفور إذا لم تعد شروط الترخيص مستوفاة. 4. يتضمن ترخيص تثبيت البرنامج الوصول عن بُعد إلى نظام الحاسوب المشتبه به. 5. إذا كانت عملية التثبيت تتطلب الوصول الفعلي إلى مكان ما، يجب استيفاء متطلبات القسم 20. 6. يجوز لضابط [تطبيق القانون] [الشرطة] أن يطلب من المحكمة أن تأمر مقدم خدمة بالمساعدة في عملية التسليم إذا لزم الأمر، وذلك بموجب أمر المحكمة الممنوح في (1) الطلب المذكور أعلاه. 7. [قائمة الجرائم]. 8. قد تقرر دولة عدم تنفيذ القسم 27.		

تونس

تجدر الإشارة إلى أنه على الرغم من أن تونس ليس لديها بعد تشريع بشأن الجرائم السيبرانية، إلا أنه يجري إعداد مشروع قانون. انضمت تونس إلى الاتفاقية رقم 108 لمجلس أوروبا بشأن اتفاقية حماية الأفراد فيما يتعلق بالمعالجة التلقائية للبيانات الشخصية وبروتوكولها الإضافي رقم 181 لحماية الأفراد فيما يتعلق بالمعالجة التلقائية للبيانات الشخصية، بشأن سلطات الإشراف وتدفق البيانات عبر الحدود.[381] تحتل هذه الاتفاقيات المصدق عليها المرتبة الثانية في هرم النصوص القانونية في تونس بعد الدستور مباشرة وقبل القوانين والمراسيم.

الجرائم		
اتفاقية بودابست بشأن الجرائم السيبرانية ("اتفاقية بودابست")	التشريع الوطني	ملاحظات
المادة 2 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست - الوصول غير المشروع[382] يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لإثبات الجرائم الجنائية بموجب قانونه المحلي، عندما ترتكب عمدا، والوصول إلى نظام الحاسوب بالكامل أو أي جزء منه دون حق. قد يشترط طرف ما ارتكاب الجريمة عن طريق انتهاك إجراءات أمنية بقصد الحصول على بيانات الحاسوب أو نية أخرى غير نزيهة، أو فيما يتعلق بنظام حاسوب متصل بنظام حاسوب آخر.	**المجلة الجنائية** **المادة 199 مكرر** أي شخص قام، عن طريق الاحتيال، بالانضمام أو الإبقاء على نفسه في نظام معالجة البيانات بالكامل أو جزء منه،	**التحليل القانوني** يتضمن الحكم الوطني إشارة إلى «عن طريق الاحتيال"، وهذا يشير إلى أن الجاني قد وصل إلى البيانات بطريقة غير شريفة؛ في حين تشير اتفاقية بودابست إلى "بدون حق" وذلك للدلالة على الوصول غير المصرح به. تشير اتفاقية بودابست إلى "نية غير شريفة"، ولكن هذا يتعلق بتأمين البيانات بدلاً من فعل الوصول غير القانوني. في الوقت الحالي، يمكن ارتكاب هذه الجريمة على المستوى الوطني فقط في حالة كان لدى مرتكب الجريمة غرضًا غير شريف من الوصول. من غير الواضح إن كان تعريف "احتيالي" يستلزم وجود عمل صريح محدد أو إذا كان أي وصول غير قانوني يعتبر احتياليًا. ولهذا السبب يجب تعريف "الاحتيال".

381. القانون الأساسي رقم 42 لسنة 2017 المؤرخ في 30 ماي 2017 بشأن الموافقة على انضمام الجمهورية التونسية للاتفاقية رقم 108 لمجلس أوروبا بشأن حماية الأفراد فيما يتعلق بالمعالجة التلقائية للبيانات الشخصية وبروتوكولها الإضافي رقم 181 بشأن السلطات الإشرافية وتدفق البيانات عبر الحدود

382. المادة 29 (1) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية

الجرائم		
اتفاقية بودابست بشأن الجرائم السيبرانية ("اتفاقية بودابست")	**التشريع الوطني**	**ملاحظات**
المادة 6 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - جريمة الدخول غير المشروع 1. الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به. 2. تشدد العقوبة إذا ترتب على هذا الدخول أو البقاء أو الاتصال أو الاستمرار بهذا الاتصال: a. محو أو تعديل أو تشويه أو نسخ أو نقل أو محو للبيانات المحفوظة وللأجهزة والأنظمة الالكترونية وشبكات الاتصال وإلحاق الضرر بالمستخدمين والمستفيدين. b. الحصول على معلومات حكومية سرية. **القسم 4 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الوصول غير القانوني** 1. يعاقب بالسجن لمدة لا تتجاوز [المدة] أو غرامة لا تتجاوز [المبلغ] أو بالعقوبتين معاً أي شخص يدان بجريمة الوصول إلى نظام حاسوب كله أو جزء منه عن قصد ودون عذر مبرر قانونًا أو بتجاوز لسبب قانوني. 2. قد تقرر أي دولة عدم تجريم الوصول غير المصرح به بشرط توفر سبل انتصاف فعالة أخرى. علاوة على ذلك، قد يشترط بلد ما ارتكاب الجريمة عن طريق انتهاك الإجراءات الأمنية أو بقصد الحصول على بيانات الحاسوب أو بنية أخرى غير نزيهة. **القسم 5 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الآثار غير القانونية** 1. أي شخص يظل مسجلاً في نظام حاسوب أو جزء من نظام حاسوب أو يواصل استخدام نظام حاسوب عن قصد ودون عذر أو مبرر قانوني، أو يتجاوز عذرًا أو مبررًا قانونيًا يعاقب عند إدانته بالسجن لمدة لا تتجاوز [المدة]، أو غرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً. 2. قد تقرر أي دولة عدم تجريم الآثار غير المصرح بها فقط، شرط أن تتوفر سبل انتصاف فعالة أخرى. بدلاً من ذلك، قد يشترط البلد ارتكاب الجرم عن طريق انتهاك الإجراءات الأمنية أو بقصد الحصول على بيانات الحاسوب أو بنية أخرى غير نزيهة.		يشير نص الجريمة أيضًا إلى «نظام معالجة البيانات المؤتمتة" دون وجود تعريف له. من غير الواضح ما إذا كان هذا يتعلق بـ «نظام حاسوب" (أي يعني أي جهاز أو مجموعة من الأجهزة المترابطة أو ذات الصلة، يقوم واحد أو أكثر منها، وفقًا لبرنامج ما، بمعالجة تلقائية للبيانات - المادة 1 من اتفاقية بودابست) أو "البيانات المحوسبة" (أي تمثيل للوقائع أو المعلومات أو المفاهيم في شكل مناسب للمعالجة في نظام الحاسوب، بما في ذلك برنامج مناسب لكي يقوم نظام الحاسوب بأداء وظيفة ما - المادة 1 من اتفاقية بودابست) تشير المادة 6 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات إلى «الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به." دون تحديد ماهية هذه الأفعال، يستحسن لذلك استخدام تعريفات اتفاقية بودابست ومواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية. **التوصيات:** يمكن أن يتضمن التشريع الوطني اللغة ذات الصلة من اتفاقية بودابست و/أو مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية لتضمين تعريفات لنظام الحاسوب وإدراج البرامج في تعريف البيانات لأن بعض البيانات تشمل البرامج وبعضها لا تشملها. علاوة على ذلك، ولكي تتماشى التشريعات مع اتفاقية بودابست/مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية، ينبغي أن يشير التشريع إلى الوصول "دون حق" "بدلاً من الاحتيال" ينبغي النظر في أي جريمة مشددة إذا وقع وصول غير قانوني إلى نظام حاسوبي أساسي أو بيانات حاسوبية

الجرائم		
اتفاقية بودابست بشأن الجرائم السيبرانية ("اتفاقية بودابست")	**التشريع الوطني**	**ملاحظات**
المادة 3 من اتفاقية بودابست[383] **-** **اعتراض غير قانوني** يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وتدابير أخرى لتجريم اعتراض عمليات نقل البيانات الحاسوبية غير العامة من نظام حاسوب وإليه وداخله، بما في ذلك الانبعاثات الكهرومغناطيسية من نظام الحاسوب الذي يحمل مثل هذه البيانات، وذلك عند ارتكاب هذا العمل عمدًا بوسائط تقنية، ويعتبر جريمة جنائية بموجب القانون الداخلي. قد يشترط الطرف أن تكون الجريمة قد ارتكبت بنية غير نزيهة، أو أن تتم ضد نظام حاسوب متصل بنظام حاسوب آخر. **القسم 6 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - اعتراض غير قانوني** 1. الشخص الذي يتعمد اعتراض الوسائل التقنية دون عذر أو مبرر قانوني أو يتجاوز عذرًا أو مبررًا قانونيًا: • أي نقل غير عام إلى نظام الحاسوب أو منه أو داخله؛ أو • الانبعاثات الكهرومغناطيسية من نظام الحاسوب يعتبر جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً. 2. قد يشترط البلد ارتكاب الجرم بنية غير شريفة، أو ضد نظام حاسوب متصل بنظام حاسوب آخر أو عن طريق التحايل على إجراءات الحماية المطبقة لمنع الوصول إلى محتوى الإرسال غير العام. **المادة 7 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات** **الاعتراض غير القانوني** الاعتراض غير القانوني المتعمد لحركة البيانات بأي وسيلة تقنية، وتعطيل نقل أو استقبال بيانات تكنولوجيا المعلومات.	**لا يوجد معادل**	**التحليل القانوني** تعتبر هذه الجريمة أساسية لملاحقة عمليات النقل غير العامة لبيانات الحاسوب إلى نظام حاسوبي أو منه أو داخله، والتي قد يتم اعتراضها بشكل غير قانوني للحصول على معلومات حول موقع الشخص (على سبيل المثال استهداف ذلك الشخص).[384] انضمت تونس إلى الاتفاقية رقم 108 لمجلس أوروبا لحماية الأفراد، فيما يتعلق بالمعالجة التلقائية للبيانات الشخصية وبروتوكولها الإضافي رقم 181 بشأن السلطات الإشرافية وتدفق البيانات عبر الحدود.[385] سيحمي هذا التشريع الأفراد من الانتهاكات التي قد تصاحب جمع ومعالجة البيانات الشخصية على النحو المنصوص عليه في الاتفاقية. وعلى الرغم من أن هذا غير صريح، فإنه يشمل البيانات التي تم الحصول عليها من خلال اعتراض غير قانوني. بالإضافة إلى ذلك، توفر الاتفاقية ضمانات فيما يتعلق بجمع البيانات الشخصية ومعالجتها، وتحظر معالجة البيانات «الحساسة" المتعلقة بعرق الشخص أو آرائه السياسية أو صحته أو دينه أو حياته الجنسية أو سجله الجنائي، وما إلى ذلك، في حالة عدم وجود ضمانات قانونية مناسبة. كما تنص الاتفاقية على حق الفرد في معرفة تخزين معلوماته، وتصحيحها إذا لزم الأمر. لا يمكن تقييد الحقوق المنصوص عليها في الاتفاقية إلا عندما تكون المصالح الغالبة (مثل أمن الدولة والدفاع وما إلى ذلك) مهددة. هذا يعني أنه إذا كان هناك اعتراض قانوني[386] سيتم جمع البيانات ومعالجتها بشكل قانوني. كما تفرض الاتفاقية بعض القيود على تدفق البيانات الشخصية عبر الحدود إلى الدول التي لا يوفر التنظيم القانوني فيها حماية مماثلة.[387] **تحليل الفجوة** **التوصيات:** استخدم لغة اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست في المادة 3، والقسم 6 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية باعتبارهما دليلًا؛ اللغة المستخدمة في المادة 7 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات مناسبة، وإن لم يكن هناك تعريف لـ «بيانات تكنولوجيا المعلومات"

383. المادة 29 (2) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية
384. http://www.coe.int/en/web/cybercrime/guidance-notes
385. المرجع السابق
386. القانون الأساسي رقم 26-2015 المؤرخ في 7 أغسطس 2015 بشأن مكافحة الإرهاب ومنع غسل الأموال المادة 54 أو القانون الأساسي رقم 61-2016 المؤرخ في 3 أغسطس 2016 المتعلق بمنع ومكافحة الاتجار بالبشر المادة 32
387. يوجد ملخص الاتفاقية رقم 108 في: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

الجرائم		
اتفاقية بودابست بشأن الجرائم السيبرانية ("اتفاقية بودابست")	**التشريع الوطني**	**ملاحظات**
المادة 4 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[388] **التشويش على البيانات** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لكي تجرم قوانينها الوطنية محو بيانات الحاسوب أو إتلافها أو تغييرها أو حذفها دون حق، وذلك عند ارتكابها عمدًا. 2. يجوز لأي طرف الاحتفاظ بالحق في المطالبة بأن السلوك الموصوف في الفقرة 1 يؤدي إلى ضرر جسيم. **القسم 7 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - التشويش غير القانوني على البيانات** الشخص الذي يقوم بأي من الأفعال التالية عمدا ودون عذر أو مبرر قانوني أو يتجاوز عذرًا أو مبررًا قانونيًا: • محو أو إتلاف بيانات الحاسوب؛ أو • يحذف بيانات الحاسوب؛ أو • تغيير بيانات الحاسوب؛ أو • جعل بيانات الحاسوب بلا معنى لها أو غير ذات فائدة أو غير فعالة؛ أو • يعوق أو يقاطع أو يشوش على الاستخدام القانوني لبيانات الحاسوب؛ أو • يعوق أو يقاطع أو يشوش على أي شخص في استخدامه القانوني لبيانات الحاسوب؛ أو • يمنع الوصول إلى بيانات الحاسوب لأي شخص مصرح له بالوصول إليها؛ يرتكب جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة]، أو غرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً. **المادة 8 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات** **جريمة ضد سلامة البيانات** 1. تعمد محو أو حذف أو منع أو تعديل أو إخفاء بيانات تكنولوجيا المعلومات بشكل غير قانوني. 2. قد يطلب أحد الأطراف أن يتسبب الفعل بأضرار جسيمة من أجل تجريم الأفعال المذكورة في الفقرة 1.	**المجلة الجنائية** **المادة 199 مكرر**: وترفع العقوبة إلى عامين سجنا والخطية إلى ألفي دينار إذا نتج عن ذلك ولو عن غير قصد إفساد أو تدمير البيانات الموجودة بالنظام المذكور. ويعاقب بالسجن مدة خمسة أعوام وبخطية قدرها خمسة آلاف دينار كل من يدخل بصفة غير شرعية بيانات بنظام معالجة معلوماتية من شأنها إفساد البيانات التي يحتوي عليها البرنامج أو طريقة تحليلها أو تحويلها. وتضاعف العقوبة إذا ارتكبت الفعلة المذكورة من طرف شخص بمناسبة مباشرته لنشاطه المهني.	**التحليل القانوني** الاستخدام «عن طريق الاحتيال" هو غير متناسقة (تتعارض في الواقع مع) المعيار 1.4 الذي نصت عليه اتفاقية بودابست "... عندما يقوم عن قصد بإتلاف بيانات الحاسوب أو حذفها أو محوها أو تغييرها أو العبث بها دون حق" والذي لا يشترط إثبات الاحتيال. يعني ذلك أن السلوك الذي يشكل جريمة تدخل في البيانات وفقًا للمادة 1.4 من اتفاقية بودابست لن يتم تجريمه بموجب المادة 199 مكرر. لا تشمل هذه المادة عنصر محو بيانات الحاسوب **تحليل الفجوة** **التوصيات:** استخدم المادة 4 من اتفاقية بودابست أو القسم 7 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية باعتبارهما دليلًا للتشريعات الوطنية

388. المادة 29 (1) (هـ - و) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية

الجرائم		
اتفاقية بودابست بشأن الجرائم السيبرانية ("اتفاقية بودابست")	**التشريع الوطني**	**ملاحظات**
المادة 5 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[389] **التشويش على النظام** يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لكي تُجرّم في قانونها الداخلي أعمال الإعاقة الخطيرة التي ترتكب عمدًا ودون وجه حق من أجل إعاقة عمل نظام حاسوب من خلال إدخال بيانات حاسوب أو نقلها أو محوها أو حذفها أو إتلافها أو تغييرها أو منعها. **القسم 9 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - التشويش غير القانوني على النظام** 1. الشخص الذي يقوم عن قصد، ودون عذر أو مبرر قانوني، أو بتجاوز عذر أو مبرر قانوني: • إعاقة عمل نظام الحاسوب أو التشويش عليه؛ أو • إعاقة شخص يستخدم أو يشغل بشكل قانوني نظام الحاسوب أو التشويش عليه؛ يعتبر جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً. 2. يعاقب الشخص الذي يتعمد دون عذر أو مبرر قانوني، أو بتجاوز عذر قانوني أو مبرر، إعاقة نظام حاسوب مخصص حصريًا لاستخدام عمليات البنية التحتية الحيوية أو التشويش عليه، أو في الحالات التي لا يكون فيها هذا النظام مخصصًا للاستخدام الحصري في عمليات البنية التحتية الحيوية، ولكنه يستخدم في عمليات البنية التحتية الحيوية وتؤثر هذه الإعاقة على استخدام عمليات البنية التحتية الحيوية، بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً.	**المجلة الجنائية** **المادة 199 مكرر** أي شخص يغير عن عمد أو يدمر تشغيل المعالجة الآلية	**التحليل القانوني** تجريم هذه الأعمال من شأنه أن يمنع البرامج الضارة التي تتداخل مع عمل جهاز الحاسوب - على سبيل المثال ديدان الحاسوب - مجموعة فرعية من البرامج الضارة (مثل فيروسات الحاسوب). إنها برامج حاسوب ذاتية النسخ المتماثل تضر بالشبكة من خلال بدء عمليات نقل البيانات المتعددة. يمكن أن تؤثر على أنظمة الحاسوب عن طريق إعاقة التشغيل السلس لنظام الحاسوب، أو استخدام موارد النظام لتكرار نفسها عبر الإنترنت أو توليد حركة مرور في الشبكة يمكن أن تغلق بعض الخدمات (مثل المواقع الإلكترونية) لا تشير المادة 199 مكرر إلى نية التغيير أو التدمير «بدون حق" علاوة على ذلك، لا تشير المادة 199 مكرر إلى أفعال العرقلة أو الإخلال عمدًا من خلال «إدخال بيانات حاسوب أو نقلها أو محوها أو حذفها أو إتلافها أو تغييرها أو منعها " سيضمن الرجوع إلى هذه الأفعال أن تصف الجريمة معنى العرقلة أو الإخلال عمدًا. **تحليل الفجوة** **التوصيات:** استخدم لغة اتفاقية بودابست في المادة 5 أو القسم 9 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية بإضافة «العرقلة أو الإخلال عمدًا" بدون وجه حق" وأفعال إدخال بيانات حاسوب أو نقلها أو محوها أو حذفها أو إتلافها أو تغييرها أو منعها" ضع في اعتبارك أيضًا ما إذا كان منع ومكافحة الهجمات ضد البنية التحتية الحيوية يحتاج إلى جريمة منفصلة أو مشددة، على سبيل المثال، قد يتم إعاقة عمل نظام الحاسوب لأغراض إرهابية (يمكن أن تؤدي إعاقة النظام الذي يخزن سجلات البورصة إلى أن تكون البيانات غير دقيقة، أو أن تعيق عمل البنية التحتية الحيوية)[390] – القسم 9 (2) من مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية للصياغة المقترحة

389. لا يوجد ما يعادل المادة 29 (1) (د) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

390. http://www.coe.int/en/web/cybercrime/guidance-notes

الجرائم		
اتفاقية بودابست بشأن الجرائم السيبرانية ("اتفاقية بودابست")	**التشريع الوطني**	**ملاحظات**
المادة 6 من اتفاقية بودابست[391] **سوء استخدام الأجهزة** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لتجريم الأفعال الإجرامية بموجب قوانينه الداخلي، عندما تُرتكب عمداً ودون حق: a. إنتاج أو بيع أو شراء بغرض الاستخدام أو استيراد أو توزيع أو توفير ما يلي بأية طريقة: i. أي جهاز، بما في ذلك برنامج الحاسوب، تم تصميمه أو تكييفه بشكل أساسي بغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من 2 إلى 5؛ كلمة مرور الحاسوب أو رمز الوصول أو البيانات المماثلة التي يمكن من خلالها الوصول إلى نظام الحاسوب كله أو جزء منه، بقصد استخدامه لغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من 2 إلى 5؛ و ii. حيازة عنصر مشار إليه في الفقرتين أ.1 أو 2 أعلاه، بقصد استخدامه لغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من 2 إلى 5. يجوز لأي طرف أن يشترط بموجب القانون امتلاك عدد من هذه العناصر قبل إسناد المسؤولية الجنائية. 2. لا يجوز تفسير هذه المادة على أنها تفرض مسؤولية جنائية عندما لا يكون الغرض من الإنتاج أو البيع أو الشراء بغرض الاستخدام أو الاستيراد أو التوزيع أو التوفير أو حيازة المشار إليه في الفقرة 1 من هذه المادة ارتكاب جريمة منصوص عليها وفقًا للشروط المواد من 2 إلى 5 من هذه الاتفاقية، مثل الاختبارات المسموح بها أو حماية نظام الحاسوب. 3. يجوز لكل طرف أن يحتفظ بالحق في عدم تطبيق الفقرة 1 من هذه المادة، شريطة أن لا يتعلق التحفظ ببيع أو توزيع أو توفير المواد المشار إليها في الفقرة 1 أ من هذه المادة بطريقة أخرى.	**لا يوجد معادل**	**التحليل القانوني** سيُمكِّن تجريم هذه الأفعال من ملاحقة إنتاج وبيع والشراء من أجل الاستخدام واستيراد وتوزيع رموز الوصول والبيانات المحوسبة الأخرى المستخدمة في ارتكاب جرائم الإنترنت. - على سبيل المثال، يمكن الوصول إلى أنظمة الحاسوب لتسهيل أي هجوم إرهابي بالتدخل في شبكة الطاقة الكهربائية للبلد. سيُمكِّن تجريم هذه الأفعال من ملاحقة إنتاج وبيع والشراء من أجل الاستخدام واستيراد وتوزيع رموز الوصول والبيانات المحوسبة الأخرى المستخدمة في ارتكاب جرائم الإنترنت. هذه هي العناصر الموجودة في كثير من الأحيان في ملاحقة البرمجيات الخبيثة. لا توجد إشارة في المادة 9 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات إلى عبارة «بدون حق" - لذلك - تُفضل صياغة اتفاقية بودابست ومواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية. يجب أن تأخذ أي جريمة في الاعتبار تلك الأجهزة التي لها استخدام شرعي وكذلك للاستخدام الجنائي («الاستخدام المزدوج") – ينبغي أن يشمل ذلك اللغة المستخدمة في اتفاقية بودابست "المكيف بشكل أساسي" **تحليل الفجوة** **التوصيات:** استخدم لغة اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست في المادة 6 أو القسم 10 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية باعتبارهما دليلًا للتشريعات الوطنية. يرجى ملاحظة أن مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية توفر خيار إدراج الأجهزة في جدول إذا كان ذلك مناسبًا - قد يكون هذا تقييدًا ويتطلب تحديثًا يتوافق مع التقدم التكنولوجي. يجب أن يوفر القانون الوطني عذرًا معقولًا حتى تتمكن أجهزة إنفاذ القانون من استخدام الأجهزة لتقنيات التحقيق الخاصة - راجع اللغة في المادة 2.6. اتفاقية بودابست أو القسم 10 (2) من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية باعتبارهما دليلًا.

391. المادة 9 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات والمادة 29 (1) (ح) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية

الجرائم		
اتفاقية بودابست بشأن الجرائم السيبرانية ("اتفاقية بودابست")	**التشريع الوطني**	**ملاحظات**
القسم 10 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الأجهزة غير القانونية 1. يرتكب الشخص جريمة إذا: a. أنتج أو باع أو اشترى بغرض الاستخدام أو استورد أو صدّر أو وزع أو وفّر بأي طريقة، عن قصد ودون عذر أو مبرر قانوني أو بتجاوز عذر أو مبرر قانوني: i. جهاز، بما في ذلك برنامج حاسوب، تم تصميمه أو تكييفه بغرض ارتكاب جريمة محددة بموجب أحكام أخرى من الجزء الثاني من هذا القانون؛ أو ii. كلمة مرور الحاسوب أو رمز الوصول أو البيانات المماثلة التي يمكن من خلالها الوصول إلى نظام الحاسوب كله أو جزء منه بقصد استخدامه من قبل أي شخص لغرض ارتكاب جريمة محددة بموجب أحكام أخرى من الجزء الثاني من هذا القانون؛ أو كان في حوزته غرض مشار إليه في الفقرة الفرعية «1» أو «2»، وكان القصد هو استخدامه من قبل أي شخص لارتكاب جريمة محددة بموجب أحكام أخرى من الجزء الثاني من هذا القانون، فإنه يعاقب عند إدانته بارتكاب هذه الجريمة بالسجن لمدة لا تزيد عن [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً. 2. لا يجوز تفسير هذا الحكم على أنه يفرض مسؤولية جنائية عندما لا يكون الغرض من الإنتاج أو البيع أو الشراء للاستخدام أو الاستيراد أو التوزيع أو التوفير أو الحيازة المشار إليها في الفقرة 1 هو ارتكاب جريمة منصوص عليها وفقًا لأحكام أخرى من الجزء الثاني من هذا القانون، كأن تكون الأغراض مثل الاختبار أو الحماية المعتمدين لنظام الحاسوب. 3. قد يقرر بلد ما عدم تجريم الأجهزة غير القانونية أو قصر التجريم على الأجهزة المدرجة في الجدول.		

الجرائم		
اتفاقية بودابست بشأن الجرائم السيبرانية ("اتفاقية بودابست")	**التشريع الوطني**	**ملاحظات**
المادة 7 من اتفاقية بودابست **أعمال التزوير المرتبطة بالحاسوب** يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم إدخال بيانات الحاسوب أو تغييرها أو حذفها أو محوها، عند ارتكاب ذلك عن قصد وبدون حق، مما يؤدي إلى بيانات غير موثوقة بهدف أن يتم التعامل معها أو التصرف فيها لأغراض قانونية كما لو كانت أصلية، بصرف النظر عما إذا كانت البيانات قابلة للقراءة ومقروءة مباشرة أم لا. قد يطلب طرف ما وجود نية الاحتيال، أو نية غير شريفة مماثلة، قبل إسناد المسؤولية الجنائية. **القسم 11 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - أعمال التزوير المتعلقة بالحاسوب** 1. كل شخص يقوم عن قصد ودون عذر أو مبرر قانوني أو بتجاوز عذر قانوني أو مبرر، بإدخال أو تبديل أو حذف أو منع بيانات الحاسوب، مما ينتج عنه بيانات غير موثوقة بقصد التعامل معها أو التصرف فيها لأغراض قانونية كما لو كانت صحيحة، بصرف النظر عما إذا كانت البيانات قابلة للقراءة مباشرة أم لا، يعاقب عند الإدانة بهذه الأعمال بالسجن لمدة لا تزيد عن [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً. 2. تكون العقوبة إذا ارتكبت الجريمة المذكورة أعلاه عن طريق إرسال رسائل بريد إلكتروني متعددة من أنظمة الحاسوب أو من خلالها هي السجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً. **المادة 10 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات** **جريمة التزوير** يعني استخدام تقنية المعلومات تغيير حقيقة البيانات بطريقة تسبب الضرر بغرض استخدامها كبيانات حقيقية.	**المجلة الجزائية** **المادة 172** يعاقب بالسجن بقية العمر وبخطية قدرها ألف دينار كل موظف عمومي أو شبهه وكل عدل يرتكب في مباشرة وظيفته زورًا من شأنه إحداث ضرر عام أو خاص وذلك في الصور التالية: - بصنع كل أو بعض كتب أو عقد مكذوب أو بتغيير أو تبديل أصل كتب بأي وسيلة كانت سواء كان ذلك بوضع علامة طابع مدلس به أو إمضاء مدلس أو كان بالشهادة زورًا بمعرفة الأشخاص وحالتهم. - بصنع وثيقة مكذوبة أو تغيير متعمّد للحقيقة بأي وسيلة كانت في كل سند سواء كان ماديًا أو غير مادي من وثيقة معلوماتية أو إلكترونية وميكروفيلم وميكروفيش ويكون موضوعه إثبات حق أو واقعة منتجة لآثار قانونية.	**التحليل القانوني** لا تتعلق الجريمة الوطنية سوى بالموظفين العموميين أو كاتب العدل. يُنصح بإدراج المادة 7 من اتفاقية بودابست للحماية من المخالفات التي قد تشمل التصيُّد الاحتيالي والتصيُّد الاحتيالي الموجَّه. يجب استخدام اللغة المتعلقة بالاحتيال بالحاسوب - على سبيل المثال، قد يتم إدخال بيانات الحاسوب" (مثل البيانات المستخدمة في جوازات السفر الإلكترونية) أو تغييرها أو حذفها أو إلغاؤها، مما يؤدي إلى تصديق البيانات غير الموثوقة أو التعامل معها لأغراض قانونية كما لو كانت صحيحة.[392] اللغة المستخدمة في التشريع الوطني غامضة مع عدم وجود إشارة إلى أي نية غير شريفة وتتطلب وقوع شكل من أشكال «الضرر" دون تعريف ماهيته - وهذا هو الحال أيضًا مع المادة 10 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات وتُفضل الصياغة المستخدمة في اتفاقية بودابست في المادة 7 والقسم 11 من مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية. ينص القسم 11 (2) من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية أيضًا على إرسال رسائل بريد إلكتروني متعددة باعتبارها جريمة مشددة. لا تشير اللغة في المادة 10 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات إلى أي نية غير شريفة وتشترط التسبب في ضرر - اللغة المستخدمة في اتفاقية بودابست ومواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية هي الأفضل لأنها لا تشترط حدوث ضرر. تشترط اتفاقية بودابست ومواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية فقط أن "البيانات الزائفة" "تعتبر" حقيقية **تحليل الفجوة** **التوصيات:** استخدم لغة اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست في المادة 7 أو القسم 11 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية باعتبارهما دليلًا للتشريعات الوطنية. مراجعة ما إذا كان الضرر يجب أن يكون ركنًا من أركان الجريمة - من الأفضل عدم استخدام لفظ الضرر حتى يتم ارتكاب التزوير بمجرد إنشاء البيانات غير الموثوقة والنظر فيها. وقد يعني هذا أنه في حالة إرسال رابط مزور أو وثيقة مزورة كجزء من عملية تصيد احتيالي، تكون الجريمة مكتملة بمجرد نظر المستلم فيها (أي يفتح البريد الإلكتروني الذي يحتوي على الرابط أو يفتح الوثيقة المرفقة) - بدلاً من الاضطرار إلى إثبات وقوع أي ضرر أو أذى على المستلم

392. http://www.coe.int/en/web/cybercrime/guidance-notes

الجرائم		
اتفاقية بودابست بشأن الجرائم السيبرانية ("اتفاقية بودابست")	**التشريع الوطني**	**ملاحظات**
المادة 29 (2) (ب) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية تعمد إدخال بيانات الحاسوب أو تغييرها أو حذفها أو منعها، مما يؤدي إلى بيانات غير موثوقة بقصد التعامل معها أو التصرف فيها لأغراض قانونية كما لو كانت أصلية، بصرف النظر عما إذا كانت البيانات قابلة للقراءة أو واضحة بشكل مباشر أم لا. يجوز للطرف أن يشترط النية للاحتيال، أو نية غير شريفة مماثلة، قبل إسناد المسؤولية الجنائية		
المادة 8 من اتفاقية بودابست[393] **أعمال الاحتيال المرتبطة بالحاسوب** يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وتدابير أخرى لتجريم الأفعال التالية بموجب قوانينه الداخلية، عند ارتكابها عمداً ودون حق، بما يسبب فقدان الممتلكات لشخص آخر عن طريق: أي إدخال أو تغيير أو حذف أو إلغاء لبيانات الحاسوب، أي تدخل في عمل نظام الحاسوب، مع نية احتيال أو نية غير شريفة من أجل الحصول، دون حق، على منفعة اقتصادية لنفسه أو لشخص آخر. **القسم 12 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الاحتيال المرتبط بالحاسوب** الشخص الذي يتسبب في فقدان الممتلكات لشخص آخر، عن قصد، ودون عذر أو مبرر قانوني أو بتجاوز عذر أو مبرر قانوني، وذلك عن طريق: • أي إدخال أو تغيير أو حذف أو إلغاء لبيانات الحاسوب؛ • أي تدخل في عمل نظام الحاسوب، بقصد احتيالي أو غير شريف للحصول، دون حق، على منفعة اقتصادية لنفسه أو لشخص آخر، وتكون عقوبة هذه الأعمال السجن لمدة لا تتجاوز [المدة]، أو غرامة لا تتجاوز [المبلغ]، أو العقوبتين معاً.	**المجلة الجزائية** **المادة 199** كل من يدخِل تغييرًا بأي شكل كان على محتوى وثائق معلوماتية أو إلكترونية أصلها صحيح شريطة حصول ضرر للغير....	**التحليل القانوني** لا يوجد تعريف لعبارات «معلوماتية" أو " وثائق إلكترونية" أو "ضرر" في التشريعات الوطنية وقد يؤدي إلى عدم اليقين. لا تشير المادة 199 ثالثًا إلى قصد احتيالي أو قصد غير شريف بدون حق - فالاحتيال بالحاسوب يرتبط بمرتكب الجريمة الذي يقصد الحصول على منفعة اقتصادية لنفسه أو لشخص آخر. فالسلوك الاحتيالي دون تصريح في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات مفقود وقد يؤدي إلى عدم اليقين. لا يوجد تعريف لعبارات «ضرر" أو "المستفيدين" أو "بطريقة غير مشروعة" في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، مما قد يخلق المزيد من عدم اليقين ويفشل في تجريم السلوك المقصود. يُفضل لغة المادة 8 من اتفاقية بودابست أو القسم 12 من مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية **تحليل الفجوة** **التوصيات:** توفير تعاريف لعبارات «معلوماتية" أو "وثائق إلكترونية" أو "ضرر" والتأكد من وجود قصد احتيالي أو قصد غير شريف بدون حق - استخدام الصياغة المستخدمة في اتفاقية بودابست أو مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية

393. المادة 11 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات والمادة 29 (2) (د) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية

الجرائم		
اتفاقية بودابست بشأن الجرائم السيبرانية ("اتفاقية بودابست")	**التشريع الوطني**	**ملاحظات**
المادة 9 من اتفاقية بودابست[394] **الجرائم ذات الصلة بالمحتوى (مثل المواد الإباحية للأطفال)** 1. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم السلوك التالي في قوانينه المحلية، عندما يرتكب عمدا وبدون حق: a. إنتاج مواد إباحية للأطفال بغرض توزيعها من خلال نظام حاسوب؛ b. عرض أو إتاحة مواد إباحية للأطفال من خلال نظام الحاسوب؛ c. توزيع أو نقل المواد الإباحية للأطفال من خلال نظام الحاسوب؛ d. شراء مواد إباحية للأطفال من خلال نظام حاسوب بقصد الاستخدام الشخصي أو لإعطائها لشخص آخر؛ 2. امتلاك مواد إباحية للأطفال في نظام حاسوب أو على وسائط تخزين بيانات الحاسوب. لأغراض الفقرة 1 أعلاه، يجب أن يشمل مصطلح «استغلال الأطفال في المواد الإباحية» أية مواد إباحية تصور بصريًا: a. قاصر مشترك في سلوك جنسي صريح؛ b. شخص يبدو أنه قاصر يشارك في سلوك جنسي صريح؛ c. صور واقعية تمثل قاصرًا مشاركًا في سلوك جنسي صريح. 3. لأغراض الفقرة 2 أعلاه، يشمل مصطلح «القاصر» جميع الأشخاص الذين تقل أعمارهم عن 18 عامًا. ومع ذلك، يجوز لأي طرف أن يطلب حدًا أدنى للسن، لا يقل عن 16 عامًا. 4. يجوز لكل طرف أن يحتفظ بالحق في عدم تطبيق الفقرات الفرعية 1، (د) و (ه) ، و 2، الفقرتين الفرعيتين (ب) و (ج) كليًا أو جزئيًا. **القسم 13 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - المواد الإباحية للأطفال** 1. الشخص الذي يقوم عن قصد ودون عذر أو مبرر قانوني بـ: • إنتاج مواد إباحية للأطفال بغرض توزيعها من خلال نظام حاسوب؛	**المجلة الجزائية** **المادة 226 مكرر** يعاقب بالسجن مدة ستة أشهر وبخطية قدرها ألف دينار كل من يعتدي علنًا على الأخلاق الحميدة أو الآداب العامة بالإشارة أو القول أو يعمد علنًا إلى مضايقة الغير بوجه يخل بالحياء. ويستوجب نفس العقوبات المذكورة بالفقرة المتقدمة كل من يلفت النظر علنًا إلى وجود فرصة لارتكاب فجور وذلك بكتابات أو تسجيلات أو إرساليات سمعية أو بصرية أو الكترونية أو ضوئية. **القانون الأساسي رقم 61-2016، بتاريخ 3 أغسطس 2016، بشأن منع ومكافحة الاتجار بالبشر (الاتجار بالأشخاص).** **المادة 1** يهدف هذا القانون إلى منع كل أشكال الاستغلال التي يمكن أن يتعرض لها الأشخاص وخاصة النساء والأطفال ومكافحتها بالوقاية من الاتجار بهم وزجر مرتكبيه وحماية ضحاياه ومساعدتهم. كما يهدف إلى دعم التنسيق الوطني والتعاون الدولي في مجال مكافحة الاتجار بالأشخاص في إطار الاتفاقيات الدولية والإقليمية والثنائية المصادق عليها من قبل الجمهورية التونسية. المادة 2 يُقصد بالمصطلحات التالية على معنى هذا القانون: 5..... الاستغلال الاقتصادي أو الجنسي للأطفال بمناسبة تشغيلهم. 6 ..... 7. الاستغلال الجنسي: الحصول على منافع أيًا كانت طبيعتها من خلال توريط شخص في أعمال دعارة أو بغاء أو في تقديم أي أنواع أخرى من الخدمات الجنسية بما في ذلك استغلاله في المشاهد الإباحية بإنتاج مشاهد ومواد إباحية أو مسكها أو ترويجها بأي وسيلة كانت.	**التحليل القانوني** تحمي المادة 9 من اتفاقية بودابست والقسم 13 من مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية الأطفال من الأذى، وذلك من خلال تجريم توزيع الصور غير اللائقة للأطفال ونقلها وتوفيرها وعرضها وحيازتها. لا تشير المادة 226 مكرر إلى صور غير لائقة للأطفال **لا يشير «القانون الأساسي رقم 61 لسنة 2016 المؤرخ في 3 أغسطس 2016، المتعلق بمنع الاتجار بالأشخاص ومكافحته (الاتجار بالأشخاص)» على وجه التحديد إلى استغلال الأطفال في المواد الإباحية التي يظهر فيها أطفال - بل إلى بغاء الأطفال واستغلالهم في المشاهد الإباحية. وهذا يعني أن الجريمة قد تكون مرتبطة بأولئك المتورطين في بغاء الأطفال المتَّجر بهم لتسهيل الصور غير اللائقة.** **لا يوجد تعريف لعبارة** «الحصول على منافع أيًا كانت طبيعتها" **تحليل الفجوة** **التوصيات:** يجب استخدام المادة 9 من اتفاقية بودابست أو القسم 13 من مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية كسوابق للتشريعات الوطنية

394. المادة 12 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات والمادة 29 (3) (أ-ج) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية

الجرائم		
اتفاقية بودابست بشأن الجرائم السيبرانية ("اتفاقية بودابست")	**التشريع الوطني**	**ملاحظات**
• تقديم أو توفير مواد إباحية للأطفال من خلال نظام حاسوب؛ • توزيع أو نقل مواد إباحية عن الأطفال من خلال نظام حاسوب؛ • شراء و/ أو الحصول على مواد إباحية للأطفال من خلال نظام حاسوب لاستخدامه الشخصي أو لإعطائها لشخص آخر؛ • حيازة مواد إباحية للأطفال في نظام حاسوب أو على وسائط تخزين بيانات الحاسوب؛ أو • الوصول عمدًا، من خلال تكنولوجيا المعلومات والاتصالات، إلى المواد الإباحية عن الأطفال، ، يعتبر جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً. 2. يمكن الدفاع أمام تهمة بجريمة منصوص عليها في الفقرة (1) (ب) إلى (1) (و) إذا أثبت الشخص أن المواد الإباحية عن الأطفال كانت بغرض إنفاذ القانون بحسن نية. 3. لا يجوز لدولة ما أن تجرم السلوك الموصوف في القسم 13 (1) (د) - (و).		
المادة 10 من اتفاقية بودابست [395] **انتهاك حقوق النشر** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وغيرها من التدابير لاعتبار انتهاك حقوق الطبع والنشر، جرائم جنائية بموجب قوانينه الداخلية، وفقًا للالتزامات التي تعهد بها بموجب قانون باريس الصادر في 24 يوليو 1971، مراجعة اتفاقية برن لحماية المصنفات الأدبية والفنية، والاتفاق المتعلق بجوانب حقوق الملكية الفكرية المتصلة بالتجارة ومعاهدة المنظمة العالمية للملكية الفكرية بشأن حق المؤلف، باستثناء أي حقوق معنوية ممنوحة بموجب هذه الاتفاقيات، عندما تُرتكب هذه الانتهاكات عمدا وعلى نطاق تجاري وعن طريق نظام الحاسوب.	**القانون رقم 33 لسنة 2009 المؤرخ في 23 يونيو 2009، المتعلق بتنقيح وإتمام القانون رقم 36 لسنة 1994 المؤرخ في 24 فبراير 1994 المتعلق بالملكية الأدبية والفنية**[396]	**التحليل القانوني** تستخدم هيئات تطبيق القانون على الصعيد الدولي جرائم حقوق النشر الرقمية باعتبارها سلوكًا إجراميًا إضافيًا للتحقيق في العديد من أشكال جرائم الإنترنت ومحاكمة مرتكبيها (بما في ذلك جرائم مثل التصيّد الاحتيالي والاحتيال الإلكتروني والتزوير الإلكتروني ومواقع الويب الاحتيالية وانتهاكات البيانات وسرقتها). تميل إحدى هذه الجرائم الأساسية في العديد من الحالات إلى أن تكون انتهاكًا لحقوق النشر الرقمية. هجوم Sony الإلكتروني[397] ليس إلا مثالًا حديث العهد تضافرت فيه المنظمات الإجرامية والقوى المرتبطة بجرائم الإنترنت وسرقة البيانات/التجسس على الشركات وانتهاك حقوق الطبع والنشر لتكمل عمل بعضها البعض. **يحمي القانون رقم 33 لسنة 2009 المؤرخ في 23 يونيو 2009، المتعلق بتنقيح وإتمام القانون رقم 36 لسنة 1994، المؤرخ في 24 فبراير 1994** الابتكار في القرن الحادي والعشرين والشركات والمواطنين التونسيين

395. ليس هنالك معادل للمادة 17 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية
396. النص الكامل باللغة الإنجليزية:http://www.legislation.tn/sites/default/files/fraction-journal-officiel/2009/2009G/052/Tg2009331.pdf أو http:// www.jurisitetunisie.com/tunisie/codes/prop_int/prop_int1000.html
397. https://en.wikipedia.org/wiki/Sony_Pictures_hack

الجرائم		
اتفاقية بودابست بشأن الجرائم السيبرانية ("اتفاقية بودابست")	**التشريع الوطني**	**ملاحظات**
2. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لاعتبار أي انتهاك للحقوق أدناه جرائم جنائية بموجب قوانينه الداخلية، وذلك عملاً بالالتزامات التي تعهد بها بموجب الاتفاقية الدولية لحماية فناني الأداء ومنتجي التسجيلات الصوتية وهيئات الإذاعة (اتفاقية روما) واتفاق جوانب حقوق الملكية الفكرية المتصلة بالتجارة ومعاهدة المنظمة العالمية للملكية الفكرية بشأن الأداء والتسجيل الصوتي، باستثناء أي حقوق معنوية ممنوحة بموجب هذه الاتفاقيات، حيثما ارتكبت هذه الانتهاكات عمدا وعلى نطاق تجاري وعن طريق نظام الحاسوب. 3. يجوز لأي طرف أن يحتفظ بالحق في عدم فرض مسؤولية جنائية بموجب الفقرتين 1 و 2 من هذه المادة في ظروف محدودة، شريطة توفر سبل انتصاف فعالة أخرى، وأن لا ينتقص هذا التحفظ من التزامات الطرف الدولية المنصوص عليها في المواثيق الدولية المشار إليها في الفقرتين 1 و 2 من هذه المادة. **المادة 17 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - الجرائم المتعلقة بحق المؤلف والحقوق المرتبطة بها** انتهاك حقوق النشر كما هو محدد وفقًا لقانون الدولة الطرف، إذا كان الفعل قد ارتكب عمداً وليس لغرض الاستخدام الشخصي، وانتهاك الحقوق المرتبطة بحقوق الطبع والنشر ذات الصلة على النحو المحدد وفقًا لقانون الدولة الطرف، إذا كان الفعل ارتكب عمدا وليس لهدف الاستخدام الشخصي.		
المادة 11 من اتفاقية بودابست[398] **المساعدة والتحريض** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لتجريم الأفعال التالية بموجب قانونه الداخلي، وذلك عندما يتم التحريض على ارتكاب أي من الجرائم المقررة وفقا للمواد من 2 إلى 10 من هذه الاتفاقية أو المساعدة عليها عمدًا، مع نية أن ترتكب هذه الجريمة. 2. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وتدابير أخرى لتجريم محاولة ارتكاب أي من الأفعال الإجرامية المنصوص عليها في المواد من 3 إلى 5 و 7 و 8 و 1.9 (أ) و (ج) من هذه الاتفاقية عمدًا.	**لا يوجد معادل**	**التحليل القانوني** تعتبر مساعدة الآخرين وتحريضهم على ارتكاب جرائم أمرًا ضروريًا لمحاكمة أولئك الذين يكونون قد قدموا المساعدة أو شجعوا على ارتكاب جرائم الإنترنت. تنص المادة 19 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على الشروع أيضًا **تحليل الفجوة** **التوصيات:** استخدم المادة 11 من اتفاقية بودابست والمادة 19 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات (حيث لا توجد إشارة إلى عبارة المحاولة) باعتبارهما دليلاً للتشريعات الوطنية

398. المادة 29 (2) (و) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية

الجرائم		
اتفاقية بودابست بشأن الجرائم السيبرانية ("اتفاقية بودابست")	**التشريع الوطني**	**ملاحظات**
المادة 19 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - محاولة ارتكاب الجرائم والاشتراك فيها 1. الاشتراك في ارتكاب أية جريمة من الجرائم المنصوص عليها في هذا الفصل مع وجود نية ارتكاب الجريمة في قانون الدولة الطرف. 2. الشروع في ارتكاب الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية. 3. يجوز لأي دولة طرف الاحتفاظ بحقها في عدم تطبيق الفقرة الثانية من هذه المادة كليا أو جزئيا.		

الجرائم		
اتفاقية بودابست بشأن الجرائم السيبرانية ("اتفاقية بودابست")	**التشريع الوطني**	**ملاحظات**
المادة 12 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[399] **مسؤولية الشركات** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وتدابير أخرى لضمان أن الأشخاص الاعتباريين يمكن اعتبارهم مسؤولين عن أي جريمة جنائية منشأة وفقًا لهذه الاتفاقية، إذا ارتكبها أي شخص طبيعي لصالحهم، سواء كان ذلك بصفته الفردية أو باعتباره جزءًا من جهاز الشخص الاعتباري، أو باعتباره شخصًا قياديًا ضمن تنظيم الشخص الاعتباري، بناءً على: a. سلطة تمثيل الشخص الاعتباري؛ b. سلطة اتخاذ القرارات نيابة عن الشخص الاعتباري؛ c. سلطة ممارسة السيطرة داخل الشخص الاعتباري. 2. بالإضافة إلى الحالات المنصوص عليها بالفعل في الفقرة 1 من هذه المادة، يتخذ كل طرف الإجراءات اللازمة لضمان أن يتحمل الشخص الاعتباري المسؤولية عندما يكون عدم الإشراف أو السيطرة من قبل أي شخص طبيعي مشار إليه في الفقرة 1 قد جعل من الممكن ارتكاب جريمة جنائية منصوص عليها بموجب هذه الاتفاقية لصالح ذلك الشخص الاعتباري من قبل شخص طبيعي يعمل تحت سلطته. 3. مع مراعاة المبادئ القانونية للطرف، قد تكون مسؤولية الشخص الاعتباري جنائية أو مدنية أو إدارية. 4. تكون هذه المسؤولية دون المساس بالمسؤولية الجنائية للأشخاص الطبيعيين الذين ارتكبوا الجريمة.	**لا يوجد معادل**	**التحليل القانوني** هذا الحكم هو عنصر أساسي بحيث يستطيع الأشخاص الاعتباريون (مثلًا الكيانات التجارية) التصرف نيابة عن الأشخاص الطبيعيين الذين تقع عليهم مسؤولية جنائية **تحليل الفجوة** **التوصيات:** استخدم لغة اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست في المادة 12 باعتبارها دليلًا للتشريعات الوطنية

399. المادة 20 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، والمادة 30 (2) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية

الجرائم		
اتفاقية بودابست بشأن الجرائم السيبرانية ("اتفاقية بودابست")	**التشريع الوطني**	**ملاحظات**
البروتوكول الإضافي لاتفاقية الجريمة السيبرانية، المتعلق بتجريم أعمال العنصرية وكراهية الأجانب المرتكبة من خلال أنظمة الحاسوب **المادة 3[400] - نشر المواد التي تحض على العنصرية وكراهية الأجانب من خلال أنظمة الحاسوب** 1. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم السلوك التالي في قوانينه المحلية، عندما يرتكب عمدا وبدون حق: توزيع المواد العنصرية وكراهية الأجانب أو إتاحتها للجمهور من خلال نظام الحاسوب. 2. 2A يجوز للطرف أن يحتفظ بالحق في عدم إسناد المسؤولية الجنائية بالتصرف على النحو المحدد في الفقرة 1 من هذه المادة، عندما تحض المواد الموزعة، كما هو محدد في الفقرة 1 من المادة 2، وتشجع على التمييز غير المرتبط بالكراهية أو العنف، شريطة أن تتوفر سبل انتصاف فعالة أخرى. 3. بصرف النظر عن الفقرة 2 من هذه المادة، يجوز للطرف أن يحتفظ بالحق في عدم تطبيق الفقرة 1 على حالات التمييز، لأن هذه الفقرة لا يمكن أن تمثل سبل انتصاف فعالة على النحو المشار إليه الفقرة 2، وذلك بسبب مبادئ ثابتة في نظامه القانوني الوطني متعلقة بحرية التعبير.	**القانون الأساسي رقم 26-2015، بتاريخ 7 أغسطس 2015، بشأن مكافحة الإرهاب ومنع غسل الأموال.** **المادة 14** يُعد مرتكبًا لجريمة إرهابية كل من يرتكب فعلاً من الأفعال الآتية، أولاً:..... سابعًا: الإضرار بالممتلكات العامة أو الخاصة أو بالموارد الحيوية أو بالبنية الأساسية أو بوسائل النقل أو الاتصالات أو بالمنظومات المعلوماتية أو بالمرافق العمومية، ثامنًا: التكفير أو الدعوة إليه أو التحريض على الكراهية أو التباغض بين الأجناس والأديان والمذاهب أو الدعوة إليهما.	**التحليل القانوني** لا تشير المادة 14 من التشريع الوطني على وجه التحديد إلى النشر من نظام حاسوبي. لا تتضمن - المادة 3 (1) (ه) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية، التي تتضمن إنشاء وتنزيل مواد متعلقة بدافع العنصرية وكراهية الأجانب من نظام حاسوبي بدلاً من مجرد نشر أو إتاحة مثل هذه المواد - القصد أو عبارة «بدون حق" - وتُفضل لغة اتفاقية بودابست. **تحليل الفجوة** **التوصيات:** استخدام لغة اتفاقية بودابست في المادة 3 من البروتوكول الإضافي كسوابق مقترحة للتشريعات الوطنية
بروتوكول إضافي **المادة 4[401] - التهديد بدافع العنصرية وكراهية الأجانب** يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم السلوك التالي في قوانينه المحلية، عندما يرتكب عمدا وبدون حق: التهديد، من خلال نظام الحاسوب، بارتكاب جريمة جنائية خطيرة على النحو المحدد في قانونها الداخلي، (1) ضد أشخاص لسبب أنهم ينتمون إلى جماعة يميزها عرقها أو لونها أو نسبها أو أصلها القومي أو العرقي أو دينها، إذا تم استخدام أي من هذه العوامل ذريعةً، أو (2) ضد مجموعة من الأشخاص تتميز بأي من هذه الخصائص.	**لا يوجد معادل**	**تحليل الفجوة** **التوصيات:** استخدم لغة اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست في المادة 4 من البروتوكول الإضافي كدليل للتشريعات الوطنية

400. المادة 29 (3) (ه) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية لا يوجد ما يعادلها في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات
401. المادة 29 (3) (و) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية لا يوجد ما يعادلها في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

الجرائم		
اتفاقية بودابست بشأن الجرائم السيبرانية ("اتفاقية بودابست")	**التشريع الوطني**	**ملاحظات**
بروتوكول إضافي **المادة 5[402] - الإهانة بدافع العنصرية وكراهية الأجانب** يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم السلوك التالي في قوانينه المحلية، عندما يرتكب عمدا وبدون حق: إهانة الجمهور، من خلال نظام حاسوبي، (1) الأشخاص لكونهم ينتمون إلى مجموعة يميزها عرقها أو لونها أو نسبها أو أصلها القومي أو العرقي أو دينها، إذا تم استخدام أي من هذه العوامل ذريعةً؛ أو (2) مجموعة من الأشخاص تتميز بأي من هذه الخصائص. يجوز للطرف 2A إما: أن يشترط أن يكون للجريمة المشار إليها في الفقرة 1 من هذه المادة أثر على الشخص أو مجموعة الأشخاص المشار إليهم في الفقرة 1 والذين يتعرضون للكراهية أو الاحتقار أو السخرية؛ أو أن يحتفظ بالحق في عدم تطبيق الفقرة 1 من هذه المادة بشكل كلي أو جزئي.	**لا يوجد معادل**	**تحليل الفجوة** **التوصيات:** استخدم لغة اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست في المادة 5 من البروتوكول الإضافي كدليل للتشريعات الوطنية
بروتوكول إضافي **المادة 6[403] - إنكار الإبادة الجماعية أو التقليل منها أو الموافقة عليها أو تبريرها** **جرائم ضد الإنسانية** يعتمد كل طرف ما قد يلزم من إجراءات تشريعية لجعل الأفعال التالية يعتبر جرائم جنائية بموجب قوانينها الداخلية، عندما تُرتكب عمداً وبدون حق: توزيع أو توفير عبر نظام الحاسوب بأية طريقة من الطرق للجمهور، مواد تنكر أو تقلل أو تقر أو تقلل بشكل كبير الأفعال التي تشكل إبادة جماعية أو جرائم ضد الإنسانية، على النحو المحدد في القانون الدولي والمعترف بها على هذا النحو في القرارات النهائية والملزمة للمحكمة العسكرية الدولية، المنشأة بموجب اتفاقية لندن المؤرخة في 8 أغسطس 1945، أو أي محكمة دولية أخرى تنشأ بموجب المواثيق الدولية ذات الصلة والتي يعترف هذا الطرف باختصاصها القضائي.	**لا يوجد معادل**	**تحليل الفجوة** **التوصيات:** استخدم لغة اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست في المادة 6 من البروتوكول الإضافي كدليل للتشريعات الوطنية

402. المادة 29 (3) (ز) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية لا يوجد ما يعادلها في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات
403. المادة 29 (3) (ح) من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية لا يوجد ما يعادلها في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

الجرائم		
اتفاقية بودابست بشأن الجرائم السيبرانية ("اتفاقية بودابست")	**التشريع الوطني**	**ملاحظات**
2A يجوز للحزب إما أن يشترط أن يكون الإنكار أو التقليل إلى الحد الأدنى المشار إليه في الفقرة 1 من هذه المادة قد ارتكب بهدف التحريض على الكراهية أو التمييز أو العنف ضد أي فرد أو مجموعة من الأفراد على أساس العرق أو اللون أو النسب أو الأصل القومي أو العرقي أو الدين أو إذا استخدمت هذه العوامل ذريعة لذلك، أو أن يحتفظ بالحق في عدم تطبيق الفقرة 1 من هذه المادة بشكل كلي أو جزئي.		
جرائم إضافية للمراجعة		
الجرائم المتعلقة بالهوية **القسم 14 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية** يعاقب الشخص الذي يقوم عن قصد ودون عذر أو مبرر قانوني، أو يتجاوز عذرًا قانونيًا أو مبررًا باستخدام نظام حاسوب في أي مرحلة من مراحل الجريمة بنقل أو تملك أو استخدام وسيلة لتحديد الهوية شخص آخر بنية ارتكاب أي نشاط غير قانوني يشكل جريمة أو المساعدة أو التحريض عليها، عند إدانته بهذه الأعمال بالسجن لمدة لا تتجاوز [المدة] أو بغرامة لا يتجاوز [المبلغ]، أو بالعقوبتين معاً.		**التحليل القانوني** تغطي هذه الجريمة مرحلة التحضير لجريمة خيانة الأمانة المتعلقة بالهوية **تحليل الفجوة** **التوصيات:** يستحسن أن تدرج في التشريعات المحلية.
الكشف عن تفاصيل التحقيق **القسم 16 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية** موفر خدمة الإنترنت الذي يتلقى أمرًا يتعلق بتحقيق جنائي ينص صراحةً على الحفاظ على السرية أو على التزام شبيه ينص عليه القانون، ثم يقوم عن عمد ودون عذر أو مبرر قانوني أو بتجاوز لعذر قانوني مبرر، بالإفصاح عن: • حقيقة أنه قد تم إصدار أمر؛ أو • أي شيء تم تنفيذه بموجب الأمر؛ أو • أي بيانات تم جمعها أو تسجيلها بموجب الطلب؛ يعتبر جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً.		**التحليل القانوني** يعاقب على اختراق البيانات والكشف عن المعلومات الحساسة التي يمكن أن تؤثر على التحقيقات الجنائية **تحليل الفجوة** **التوصيات:** يستحسن أن تدرج في التشريعات المحلية.

الجرائم		
اتفاقية بودابست بشأن الجرائم السيبرانية ("اتفاقية بودابست")	التشريع الوطني	ملاحظات
عدم السماح بالمساعدة **القسم 17 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية** 1. أي شخص آخر غير المشتبه فيه فشل عمداً دون عذر أو مبرر قانوني أو بتجاوز عذر أو مبرر قانوني، بمساعدة شخص أو السماح بمساعدته، بناءً على أمر مثلما تحدد المواد 20 إلى 22[404] يرتكب جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة] ، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً. 2. قد يقرر أي بلد عدم تجريم عدم السماح بالمساعدة شرط أن تتوفر سبل انتصاف فعالة أخرى.		**التحليل القانوني** تتعلق هذه الجريمة بالأشخاص الذين لديهم معرفة محددة بالأدلة ذات الصلة والذين يرفضون تقديم المساعدة. غالبًا ما يعتمد تطبيق القانون على هؤلاء الأشخاص لتأمين الأدلة في التحقيقات الإلكترونية. هنالك مخالفة مستقلة وهي عدم توفير كلمات مرور أو الوصول إلى الرموز للأجهزة المشفرة أو البيانات (مثل «مفتاح المعلومات المحمية") - ينص القسم 53 من قانون تنظيم سلطات التحقيق في المملكة المتحدة لعام 2000 (RIPA) [405] على وجود جرم جنائي يتحمله الأشخاص الذين لا يمتثلون للمادة 49 من إخطار RIPA والقاضية بالكشف عن «المفتاح" **تحليل الفجوة** **التوصيات:** يستحسن أن تدرج في التشريعات المحلية.
المطاردة السيبرانية **القسم 18 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية** الشخص الذي يقوم، دون عذر أو مبرر قانوني، أو يتجاوز عذرًا قانونيًا أو مبررًا، ببدء أي اتصال إلكتروني، بقصد إكراه شخص ما أو تخويفه أو مضايقته أو التسبب في ضائقة عاطفية كبيرة له، باستخدام نظام حاسوب لدعم السلوك المتكرر والعدائي والعنيف، يرتكب جريمة يعاقب عليها عند الإدانة بالسجن لمدة لا تتجاوز [المدة]، أو بغرامة لا تتجاوز [المبلغ]، أو بالعقوبتين معاً.		**التحليل القانوني** هذه الجريمة تُجرم من يضايقون الأشخاص عبر الإنترنت - قد تنص بعض الولايات القضائية على جرائم تحرش غير مرتبطة بالحاسوب - لكن يوصى باعتماد هذه الجريمة لمتابعة لتلك الجرائم المرتكبة عبر الإنترنت. **تحليل الفجوة** **التوصيات:** يستحسن أن تدرج في التشريعات المحلية.
رعاية الأطفال على الإنترنت **القانون الجنائي الهولندي 248e** يعاقب الشخص الذي يقترح ترتيب لقاء، بوسائل عمل آلية أو باستخدام خدمة اتصال، مع شخص يعرف، أو ينبغي منطقيًا أن يعرف، أن هذا الشخص لم يصل بعد إلى سن السادسة عشرة، مع نية ارتكاب أفعال غير لائقة مع هذا الشخص أو لعمل صور عن عمل جنسي يشارك فيه هذا الشخص، بالسجن لمدة لا تقل عن سنتين أو بغرامة من الفئة الرابعة، إذا ارتكب أي عمل يقصد به تحقيق اللقاء.		**التحليل القانوني** لإثبات الجرم الهولندي، يلزم عقد لقاء لأغراض جنسية مع تقديم أدلة إثبات مأخوذة من تاريخ الدردشة عبر الإنترنت تفصح عن قصد جنسي؛ طلب عقد اللقاء مع الأدلة على أنه تم التخطيط لذلك (أي التاريخ والمكان). الغرض من القانون الكندي هو منع استدراج الكبار المفترسين للأطفال عبر الإنترنت. لا تتطلب هذه الجريمة حدوث جريمة جنسية. وهذا يعني أن المتهم لا يحتاج إلى الذهاب فعلاً لمقابلة الضحية شخصيًا. تكتمل الجريمة قبل اتخاذ أي إجراءات لارتكاب الجريمة الموضوعية. **تحليل الفجوة** **التوصيات:** يُنصح بإدراجها في التشريعات المحلية لتجريم هذا السلوك التحضيري قبل ارتكاب جريمة جنسية

404. أوامر البحث والاستيلاء والمساعدة والإنتاج
405. http://www.legislation.gov.uk/ukpga/2000/23/section/53

الجرائم		
اتفاقية بودابست بشأن الجرائم السيبرانية ("اتفاقية بودابست")	**التشريع الوطني**	**ملاحظات**
قانون العقوبات الكندي **القسم 172.1** 1. يرتكب جريمة كل شخص يتواصل عن طريق وسائل الاتصالات مع شخص يكون عمره أقل من 18 عامًا، أو يظن المتهم أن عمره أقل من 18 عامًا، بغرض تسهيل ارتكاب جريمة مرتبطة بهذا الشخص، وذلك بموجب المادة الفرعية 153 (1) ، المادة 155، 163.1 ، 170 أو 171 أو القسم الفرعي 212 (1) أو (2) أو (2.1) أو (4)؛ شخص يكون عمره أقل من 16 عامًا، أو يظن المتهم أن عمره أقل من 16 عامًا، بغرض تسهيل ارتكاب جريمة مرتبطة بهذا الشخص، وذلك بموجب المواد 151 أو 152، أو الفقرة الفرعية 160(3) أو 173(2) أو الأقسام 271 أو 272 أو 273 أو 280؛ أو شخص يكون عمره أقل من 14 عامًا، أو يظن المتهم أن عمره أقل من 14 عامًا، بغرض تسهيل ارتكاب جريمة مرتبطة بهذا الشخص بموجب المادة 281. عقاب 2. يعتبر كل شخص يرتكب جريمة بموجب الفقرة الفرعية (1) مذنبًا مذنبًا بارتكاب جريمة ويكون عرضة لعقوبة السجن لمدة تتراوح بين 10 سنوات كحد أقصى وسنة واحدة كحد أدنى؛ أو مذنبًا بارتكاب جريمة يعاقب عليها في ملخص الإدانة بالسجن لمدة تتراوح بين 18 شهرًا كحد أقصى و90 يومًا كحد أدنى. افتراض إعادة تقدير العمر 3. الأدلة على أن الشخص المشار إليه في الفقرة (1) (أ) أو (ب) أو (ج) قُدِّم للمتهم وعمره أقل من ثمانية عشر عامًا أو ستة عشر عامًا أو أربعة عشر عامًا، حسب الحالة، في حالة عدم وجود أدلة تثبت عكس ذلك تثبت أن المتهم يعتقد أن الشخص كان أقل من تلك السن. لا دفاع 4. لا يقبل دفاع المتهم أمام التهم الموجهة بموجب الفقرة (1) (أ) أو (ب) أو (ج) بأنه كان يعتقد أن الشخص المشار إليه في تلك الفقرة لا يقل عمره عن ثمانية عشر عامًا أو ستة عشر عامًا أو أربعة عشر عامًا، حسب الحالة، إلا في حالة اتخذ المتهم خطوات معقولة للتأكد من عمر الشخص.		

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 19 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[406] **التفتيش والضبط** **بيانات الحاسوب المخزنة** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لتمكين سلطاته المختصة من البحث في أو الوصول إلى: a. نظام الحاسوب أو جزء منه وبيانات الحاسوب المخزنة فيه؛ و b. وسيلة تخزين بيانات الحاسوب، حيث يمكن تخزين بيانات الحاسوب في أراضيها. 2. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وغيرها من الإجراءات لضمان تستطيع سلطاته عند تفتيشها نظام حاسوب معينًا أو جزءًا منه أو الوصول إليه بطريقة مماثلة، وذلك وفقًا للفقرة 1. أ، ويكون لدها أسباب للاعتقاد بأن البيانات المطلوبة مخزنة في نظام حاسوب آخر أو أن جزءًا منها موجود في إقليمها، وهذه البيانات يمكن الوصول إليها قانونيًا من النظام الأولي أو متاحة لها، فإنها قادرة على توسيع نطاق البحث أو الوصول المشابه للنظام الآخر على وجه السرعة. 3. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وغيرها من الإجراءات لتمكين سلطاته المختصة من مصادرة أو تأمين بيانات الحاسوب التي تم الوصول إليها وفقًا للفقرات 1 أو 2. تشمل هذه التدابير القدرة على: a. ضبط نظام حاسوب أو جزء منه أو وسيلة تخزين بيانات الحاسوب، والقيام بما يلزم لتأمينه؛ b. إنشاء نسخة من بيانات الحاسوب هذه والاحتفاظ بها؛ c. الحفاظ على سلامة بيانات الحاسوب المخزنة ذات الصلة؛ d. أن يجعل الوصول إلى بيانات الحاسوب في نظام الحاسوب الذي تم الوصول إليه غير ممكن أو أن يحذفها.	**لا يوجد معادل**	**التحليل القانوني** هذه هي قوة التحقيق الأكثر أهمية ويجب أن تشير إلى الحصول على حق الوصول وليس البحث. في «التقرير التوضيحي لاتفاقية بودابست، يعني «البحث" التفتيش عن البيانات أو قراءتها أو فحصها أو مراجعتها. ويشمل ذلك مفهوم البحث عن البيانات والبحث عن (فحص) البيانات. لكلمة "الوصول" معنى محايد وتعكس بدقة أكثر المصطلحات الحاسوبية؛ يتم استخدامها كذلك في المادتين 26 و 27 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.[407] **تحليل الفجوة** **التوصيات:** يمكن أن يقتبس التشريع الوطني اللغة المناسبة من اتفاقية بودابست بشأن الجريمة السيبرانية واتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية وذلك لتضمين تعريفات لنظام الحاسوب[408] وبيانات الحاسوب[409] والإحالة دائمًا إلى الوصول يجب أن يكون هناك تعريف «للحجز" لضمان النزاهة ولتحديد الإجراءات - القسم 3 (16) من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية "يشمل الحجز: • تشغيل أي نظام حاسوب في الموقع ووسائط تخزين بيانات الحاسوب؛ • إنشاء نسخة من بيانات الحاسوب والاحتفاظ بها، بما في ذلك عن طريق استخدام معدات في الموقع؛ • الحفاظ على سلامة بيانات الحاسوب المخزنة ذات الصلة؛ • أن يجعل الوصول غير ممكن إلى بيانات الحاسوب في نظام الحاسوب الذي تم الوصول إليه أو أن يحذفها؛ • أخذ نسخة مطبوعة من بيانات غير ممكن؛ أو • حجز نظام حاسوب أو جزء منه أو وسيلة تخزين بيانات الحاسوب، والقيام بما يلزم لتأمينه» تنص المادة 21 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية على التشريع لضمان تقديم المساعدة من قبل أولئك الذين لديهم معرفة متخصصة بموقع الأدلة ذات الصلة - يمكن استخدام هذا كدليل - انظر أيضًا القسم 17 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية، المتعلق بالجريمة في حال تم رفض المساعدة دون عذر قانوني

406. المادة 3 من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية
407. الفقرة 191، الصفحة 33 التقرير التوضيحي لاتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية
408. انظر المادة 1.أ. من اتفاقية بودابست: «أي جهاز أو مجموعة من الأجهزة المترابطة أو ذات الصلة، أو واحد أو أكثر من هذه الأجهزة يقوم بمعالجة البيانات تلقائيًا وفقًا لبرنامج ما" **أو** القسم 3 (5) من مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية: «جهاز أو مجموعة من الأجهزة المترابطة أو ذات الصلة، بما في ذلك الإنترنت، أو واحد أو أكثر من هذه الأجهزة يقوم بمعالجة تلقائية للبيانات أو بأداء أي وظيفة أخرى وفقًا لبرامج ما."
409. انظر المادة 1.ب. من اتفاقية بودابست: «أي تمثيل للوقائع أو المعلومات أو المفاهيم في نموذج مناسب للمعالجة في نظام حاسوب، بما في ذلك البرامج المناسبة لأن يقوم نظام حاسوب بأداء وظيفة ما"، **أو** القسم 3 (6) من مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية: "تتضمن بيانات الحاسوب أي تمثيل للوقائع أو المعلومات أو المفاهيم (سواء أكانت نصوصًا أو أصواتًا أو صورًا) أو رموز آلة مقروءة أو تعليمات، في نموذج مناسب للمعالجة في نظام الحاسوب، بما في ذلك البرامج المناسبة لأن يقوم نظام الحاسوب بأداء وظيفة ما".

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
4. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى لتمكين سلطاته المختصة من أن تأمر أي شخص لديه معرفة بعمل نظام الحاسوب أو التدابير المطبقة لحماية البيانات الموجودة فيه بتوفير ما يلزم من المعلومات بما يكفل تنفيذ الإجراءات المشار إليها في الفقرتين 1 و 2. 5. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و 15. **القسم 20 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - البحث والضبط** 1. إذا اقتنع [القاضي] بناء على [معلومات تحت القَسَم] [شهادة خطية] أن هناك أسبابًا معقولة [للاشتباه] [للاعتقاد] أنه قد يكون هناك في مكان ما شيء أو بيانات حاسوب: • قد تكون مادية كدليل في إثبات الجريمة؛ أو • قد اكتسبها شخص نتيجة لجريمة؛ [يجوز] [يأمر] يصدر [القاضي] تفويضًا لضابط [إنفاذ القانون] [الشرطة]، ويزوده بما قد يلزم من مساعدة، لدخول المكان للبحث عن الشيء أو بيانات الحاسوب وضبطها، وعمل ما يلزم بما في ذلك البحث أو عمليات الوصول الشبيهة: i. نظام الحاسوب أو جزء منه وبيانات الحاسوب المخزنة فيه؛ و ii. وسيلة تخزين بيانات الحاسوب، حيث يمكن تخزين بيانات الحاسوب في إقليم البلد. 2. إذا كان[قوة إنفاذ القانون] [الشرطة] الذي يجري عملية بحث على أساس القسم 20 (1) أسباب للاعتقاد بأن البيانات المطلوبة مخزنة في نظام حاسوب آخر أو جزء منه في إقليمها، وأن هذه البيانات يمكن الوصول إليها قانونيًا أو يمكن أن تكون متاحة من النظام الأولي، فيجب أن يكون قادرًا على توسيع نطاق البحث أو الوصول إلى النظام الآخر بطريقة مماثلة. 3. يتم تمكين ضابط [تطبيق القانون] [الشرطة] الذي يقوم بالبحث من مصادرة أو تأمين بيانات الحاسوب المماثلة التي يتم الوصول إليها وفقًا للفقرات 1 أو 2.		

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
القسم 21 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - المساعدة يجب على أي شخص لا يشتبه في ارتكابه جريمة ولكن لديه علم بسير عمل نظام الحاسوب أو التدابير المطبقة لحماية بيانات الحاسوب الواردة فيه والتي تخضع لعملية بحث بموجب المادة 20، أن يسمح وأن يساعد إذا لزم الأمر وطلب منه الشخص المسؤول أن يجري البحث عن طريق: • توفير المعلومات التي تمكن من اتخاذ التدابير المشار إليها في المادة 20؛ • الوصول إلى نظام حاسوب أو وسيط تخزين بيانات الحاسوب واستخدامه للبحث في أي بيانات حاسوب متاحة أو في النظام؛ • الحصول على ونسخ بيانات حاسوب هذه؛ • استخدام المعدات لعمل نسخ؛ و • الحصول على معلومات واضحة من نظام حاسوب بشكل مقبول في الإجراءات القانونية. **المادة 26 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - فحص المعلومات المخزنة** 1. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين سلطاتها المختصة من التفتيش أو الوصول إلى: a. تقنية معلومات أو جزء منها والمعلومات المخزنة فيها أو المخزنة عليها. b. بيئة أو وسيط تخزين معلومات تقنية معلومات والذي قد تكون معلومات التقنية مخزنة فيه أو عليه. 2. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من التفتيش أو الوصول إلى تقنية معلومات معينة أو جزء منها بما يتوافق مع الفقرة (1-أ) إذا كان هناك اعتقاد بأن المعلومات المطلوبة مخزنة في تقنية معلومات أخرى أو جزء منها في إقليمها وكانت هذه المعلومات قابلة للوصول قانونا أو متوفرة في التقنية الأولى فيجوز توسيع نطاق التفتيش والوصول للتقنية الأخرى.		

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 27 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - ضبط المعلومات المخزنة 1. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من ضبط وتأمين معلومات تقنية المعلومات التي يتم الوصول إليها حسب الفقرة 1 من المادة 26 من هذه الاتفاقية. هذه الإجراءات تشمل صلاحيات: a. ضبط وتأمين تقنية المعلومات أو جزء منها أو وسيط تخزين معلومات تقنية المعلومات. b. عمل نسخة معلومات تقنية المعلومات والاحتفاظ بها. c. الحفاظ على سلامة معلومات تقنية المعلومات المخزنة. إزالة أو منع الوصول إلى تلك المعلومات في تقنية المعلومات التي يتم الوصول إليها. 2. تلتزم كل طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى أي شخص لديه معرفة بوظيفة تقنية المعلومات أو الإجراءات المطبقة لحماية تقنية المعلومات من أجل تقديم المعلومات الضرورية لإتمام تلك الإجراءات المذكورة في الفقرتين 2 و 3 من المادة 26 من هذه الاتفاقية.		
المادة 16 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[410] **الحفظ المستعجل لبيانات الحاسوب المخزنة والكشف عنها** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وغيرها من الإجراءات لتمكين سلطاته المختصة من طلب الحفظ السريع لبيانات الحاسوب المحددة أو الحصول عليها بشكل مماثل، بما في ذلك بيانات المرور التي تم تخزينها عن طريق نظام حاسوبي، ولا سيما عندما يكون هناك أسباب للاعتقاد بأن بيانات الحاسوب معرضة بشكل خاص للفقد أو التعديل.	**لا يوجد معادل**	**التحليل القانوني** هذه القوة الإجرائية مهمة لضمان الحفاظ على البيانات المعرضة للحذف أو الفقد

410. لا يوجد ما يعادلها في اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
2. عندما يقوم أحد الأطراف بتنفيذ الفقرة 1 أعلاه عن طريق أمر شخص بحفظ بيانات الحاسوب المخزنة المحددة وذلك بوضعها في حوزته أو تحت سيطرته، يعتمد هذا الطرف الإجراءات التشريعية وغيرها من الإجراءات التي قد تكون ضرورية لإلزام ذلك الشخص بالحفاظ على سلامة بيانات الحاسوب لفترة زمنية طويلة، حدها الأقصى تسعين يومًا، وذلك لتمكين السلطات المختصة من طلب الكشف عنها. يجوز للطرف أن ينص على تجديد هذا الأمر لاحقًا. 3. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لإلزام الحارس أو أي شخص آخر يحفظ بيانات الحاسوب بالحفاظ على سرية تنفيذ هذه الإجراءات للفترة الزمنية المنصوص عليها في قانونه الداخلي. 4. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و 15. **القسم 23 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الحفظ المستعجل** إذا اقتنع ضابط [تطبيق القانون] [الشرطة] بوجود أسباب معقولة للاعتقاد بأن بيانات الحاسوب المطلوبة لأغراض التحقيق الجنائي معرضة للضياع أو التعديل، يجوز لضابط [تطبيق القانون] [الشرطة]، عن طريق إشعار مكتوب مقدم إلى شخص يتحكم في بيانات الكمبيوتر، أن يطلب من هذا الشخص الحفاظ على البيانات المحددة في الإشعار لمدة تصل إلى سبعة (7) أيام على وفقًا لما هو محدد في الإشعار. يمكن تمديد الفترة إلى ما بعد سبعة (7) أيام إذا سمح [قاضي]، بناءً على طلب من طرف واحد، وذلك لمدة زمنية أخرى محددة.		**تحليل الفجوة** **التوصيات:** تعد هذه القدرة المستعجلة للاحتفاظ بمعلومات المشترك الأساسية والبيانات الوصفية والمعاملات والمحتويات المخزنة ضرورية كجزء من تحقيقات جرائم الإنترنت، ولضمان أن تكون الأدلة متاحة للبحث والوصول والضبط والمراجعة. يمكن استخدام لغة المادة 16 من اتفاقية بازل أو القسم 23 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية أو المادة 23 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. يتطلب التشريع الوطني تعريفات كافية لـ «معلومات المشترك أو BSI"،[411] و "بيانات الحركة"،[412] و "مزود خدمة الاتصالات"[413] للتأكد من أنه يمكن الحفاظ عليها. ينبغي إيلاء اهتمام لأن يكون طول مدة الحفظ معقولًا في هذه الظروف، وأن يُسمَح بتطبيق التمديد في الظروف الملحة - تنص اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست والاتفاقية العربية لمكافحة جرائم تقنية المعلومات على 90 يومًا، فيما تنص اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية على 7 أيام. ووفقًا للتجربة فإن مدة 90 يومًا هي مدة قصيرة في التحقيقات عبر الإنترنت ، ويجب أن تكون حوالي 180 يومًا يمكن تمديدها.

411. انظر المادة 2 (9) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات: «أي معلومات متعلقة بمشتركي الخدمة وتوجد لدى موفر الخدمة باستثناء المعلومات التي يمكن من خلالها معرفة ما يلي: نوع خدمة الاتصال المستخدمة والمتطلبات الفنية وفترة الخدمة. ب. هوية المشترك وعنوانه البريدي أو الجغرافي أو رقم الهاتف ومعلومات الدفع المتاحة بموجب اتفاقية الخدمة. ج. أي معلومات أخرى موجودة على موقع تركيب معدات الاتصالات بموجب اتفاقية الخدمة".

412. انظر المادة 1.د من اتفاقية بودابست: «أي بيانات حاسوب تتعلق باتصال عن طريق نظام حاسوب، يتم إنشاؤها بواسطة نظام حاسوب يشكل جزءًا من سلسلة الاتصال، وتعرض مصدر الاتصال أو وجهته أو مساره أو الوقت أو التاريخ أو حجمه أو مدته أو نوع الخدمة الأساسية"، **أو** القسم 3 (18) من مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية: «بيانات الحركة تعني أي بيانات حاسوب تتعلق باتصال عن طريق نظام حاسوب، يتم إنشاؤها بواسطة نظام حاسوب يشكل جزءًا من سلسلة الاتصال، وتعرض مصدر الاتصال أو وجهته أو مساره أو الوقت أو التاريخ أو الحجم أو المدة أو نوع الخدمة الأساسية».

413. انظر المادة 1.ج من اتفاقية بودابست: "1 أي كيان عام أو خاص يوفر للمستخدمين قدرة الاتصال عن طريق نظام الحاسوب، و 2 أي كيان آخر يعالج أو يخزن بيانات الحاسوب نيابة عن خدمة الاتصال هذه أو مستخدمي هذه الخدمة" **أو** المادة 2 (2) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات:»أي شخص طبيعي أو معنوي عام أو خاص يزود المشتركين بالخدمات للتواصل بواسطة تقنية المعلومات، أو يقوم بمعالجة أو تخزين المعلومات نيابة عن خدمة الاتصالات أو مستخدميها".

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 23 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات- الحفظ المستعجل للبيانات المخزنة في تكنولوجيا المعلومات 1. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأمر أو الحصول على الحفظ العاجل للمعلومات المخزنة بما في ذلك معلومات تتبع المستخدمين والتي خزنت على تقنية معلومات وخصوصا إذا كان هناك اعتقاد بأن تلك المعلومات عرضة للفقدان أو التعديل. 2. تلتزم كل دولة طرف بتبني الإجراءات الضرورية فيما يتعلق بالفقرة 1 بواسطة إصدار أمر إلى شخص من أجل حفظ معلومات تقنية المعلومات المخزنة والموجودة بحيازته أو سيطرته ومن أجل إلزامه بحفظ وصيانة سلامة تلك المعلومات لمدة أقصاها 90 يوما قابلة للتجديد، من أجل تمكين السلطات المختصة من البحث والتقصي 3. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لإلزام الشخص المسؤول عن حفظ تقنية معلومات للإبقاء على سرية الإجراءات طوال الفترة القانونية المنصوص عليها في القانون الداخلي.		
المادة 17 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[414] **الحفظ المستعجل والكشف الجزئي لبيانات المرور** 1. فيما يتعلق ببيانات المرور التي يتعين الحفاظ عليها بموجب المادة 16، يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وإجراءات أخرى من أجل: a. التأكد من أن مثل هذا الحفظ المستعجل لبيانات المرور متاح بغض النظر عما إذا كان هناك واحد أو أكثر من مقدمي الخدمة قد شاركوا في نقل ذلك الاتصال؛ و b. ضمان الكشف السريع للسلطة المختصة لدى الدولة الطرف، أو للشخص المعين من قبل تلك السلطة، عن كمية كافية من بيانات المرور لتمكينه من تحديد مقدمي الخدمات والمسار الذي تم من خلاله نقل الاتصال. 2. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و 15.	**لا يوجد معادل**	**التحليل القانوني** هذه السلطة الإجرائية مهمة بشكل خاص لضمان توفير مزودي خدمة الاتصالات لعناوين بروتوكول الإنترنت التي يمكنها تحديد موقع مرتكب الجريمة السيبرانية. **تحليل الفجوة** **التوصيات:** يجب تضمين هذه القوة المستعجلة جنبًا إلى جنب مع الكشف عن بيانات المرور في التشريعات لتمكين التحقيقات الفعالة في جرائم الإنترنت. يمكن استخدام لغة المادة 17 من اتفاقية بازل، القسمين 23 و 24 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية أو المادة 24 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. سيتطلب ذلك أيضًا تعريفات لـ «حركة البيانات" و "مزود خدمة الاتصالات"[415]

414. لا يوجد ما يعادلها في اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية
415. انظر التعريفات أعلاه

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
القسم 23 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الحفظ المستعجل إذا اقتنع ضابط [تطبيق القانون] [الشرطة] بوجود أسباب معقولة للاعتقاد بأن بيانات الحاسوب المطلوبة لأغراض التحقيق الجنائي معرضة للضياع أو التعديل، يجوز لضابط [تطبيق القانون] [الشرطة]، عن طريق إشعار مكتوب مقدم إلى شخص يتحكم في بيانات الكمبيوتر، أن يطلب من هذا الشخص الحفاظ على البيانات المحددة في الإشعار لمدة تصل إلى سبعة (7) أيام على وفقًا لما هو محدد في الإشعار. يمكن تمديد الفترة إلى ما بعد سبعة (7) أيام إذا سمح [قاضي]، بناءً على طلب من طرف واحد، وذلك لمدة زمنية أخرى محددة. **القسم 24 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - جمع بيانات حركة الاتصالات** إذا اقتنع ضابط [تطبيق القانون] [الشرطة] بناءً على أسباب معقولة بأن البيانات المخزنة في نظام الحاسوب ضرورية لأغراض التحقيق الجنائي، يجوز له أن يطلب، عبر إشعار خطي، من شخص له السيطرة على نظام الحاسوب كشف بيانات حركة مرور تتعلق باتصال محدد بشكل كافٍ لتحديد: • مزودو خدمة الإنترنت؛ و/ أو المسار الذي تم من خلاله نقل الاتصال. **المادة 24 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - لتحفظ العاجل والكشف الجزئي لمعلومات تتبع المستخدمين** تلتزم كل دولة طرف بتبني الإجراءات الضرورية فيما يختص بمعلومات تتبع المستخدمين من أجل: 1. ضمان توفر الحفظ العاجل لمعلومات تتبع المستخدمين بغض النظر عن اشتراك واحد أو أكثر من مزودي الخدمة في بث تلك الاتصالات. 2. ضمان الكشف العاجل للسلطات المختصة لدى الدولة الطرف أو لشخص تعينه تلك السلطات لمقدار كاف من معلومات تتبع المستخدمين لتمكين الدولة الطرف من تحديد مزودي الخدمة ومسار بث الاتصالات.		

إجراءات		
أفضل الممارسات الدولية	**التشريع الوطني**	**ملاحظات**
المادة 18 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[416] **أمر النسخ** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وتدابير أخرى لتمكين سلطاته المختصة من أن تأمر: a. شخصًا موجودًا في إقليمها بتقديم بيانات حاسوب محددة في حيازته أو تحت سيطرته، وتُخَزّن في نظام حاسوب أو بوسيلة تخزين بيانات الحاسوب؛ و b. مقدم خدمة يقدم خدماته في إقليم الدولة الطرف بتقديم معلومات المشترك المرتبطة بهذه الخدمات، والتي تكون في حيازة أو تحت سيطرة مقدم الخدمة. 2. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و 15. 3. تعني «معلومات المشترك» أي معلومات محفوظة بشكل بيانات حاسوب أو أي شكل آخر ويحتفظ بها مزود الخدمة، وترتبط بالمشتركين في خدماته، بخلاف بيانات المرور أو المحتوى، والتي يمكن إنشاؤها من خلال: a. نوع خدمة الاتصال المستخدمة والأحكام الفنية المتعلقة بها وفترة الخدمة؛ b. هوية المشترك أو العنوان البريدي أو الجغرافي، ورقم الهاتف وأرقام الاتصال الأخرى ومعلومات الفوترة والدفع المتاحة بناءً على اتفاقية الخدمة؛ c. أي معلومات أخرى متاحة على موقع تركيب معدات الاتصالات بناءً على اتفاقية الخدمة أو الترتيب.	**لا يوجد معادل**	**التحليل القانوني** هذا شرط أساسي لإجراء تحقيق فعال في جرائم الإنترنت وسيؤثر غيابه على الملاحقات القضائية والتعاون الدولي. **تحليل الفجوة** **التوصيات:** تعتبر هذه السلطة الأساسية ضرورية لضمان توفير مزودي خدمة الاتصالات في تونس لمعلومات المشترك الأساسية وبيانات المرور وبيانات المحتوى المخزنة. سيتطلب ذلك أيضًا تعريفات «بيانات الحاسوب"، و "معلومات المشترك أو معلومات المشترك الأساسية"، و "حركة البيانات" و "مزود خدمة الاتصالات"[417] المادة 25 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات هي نموذج يمكن استخدامه ويستخدم تعريفات مختلفة بما في ذلك «تكنولوجيا المعلومات"، و[418] "مزود الخدمة" و[419] "البيانات"؛[420] غير أنه من المستحسن أن تكون هناك تعريفات لـ «معلومات المشترك أو معلومات المشترك الأساسية" أو "حركة البيانات" لأنها ستكون أنواع مختلفة من الأدلة التي يمكن توليدها في دول الجنوب الشريكة. علاوة على ذلك، سوف تتطلب هذه السلطة من الأفراد وغيرهم (مثل الكيانات المؤسسية والمؤسسات المالية وغيرها من المنظمات) ممن يحملون البيانات أن يقوموا بتوليدها بناء على طلب سلطات إنفاذ القانون. يمكن أن تكون المادة 18 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست والمادة 22 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية بمثابة دليل مع التطبيق الثابت للتعريفات

416. لا يوجد ما يعادلها في اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية
417. انظر التعريفات أعلاه
418. المادة 2 (1) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات: "أية وسيلة مادية أو معنوية أو مجموعة وسائل مترابطة أو غير مترابطة تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها وفقا للأوامر والتعليمات المخزونة بها. ويشمل ذلك جميع المدخلات والمخرجات المرتبطة بها سلكيا أو لا سلكيا في نظام أو شبكة".
419. المادة 2 (2) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات انظر أعلاه
420. المادة 2 (3) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات: «كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة تقنية المعلومات، كالأرقام والحروف والرموز وما إلى ذلك».

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
القسم 22 من نظام اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - أمر النسخ إذا كان [قاض] مقتنعًا بناءً على طلب قدمه [ضابط إنفاذ القانون] [الشرطة] بأن بيانات حاسوب محددة أو نسخة مطبوعة أو غيرها من المعلومات ضرورية لإجراء تحقيق جنائي أو لإجراءات جنائية، يجوز [للقاضي] أن يأمر بما يلي: • أن ينسخ شخص في إقليم [الدولة المشترعة] يتحكم في نظام الحاسوب نسخًا محددة من بيانات الحاسوب أو نسخة مطبوعة أو معلومات أخرى واضحة من تلك البيانات؛ أو • مزود خدمة الإنترنت في [الدولة المشترعة] لتقديم معلومات حول الأشخاص المشتركين في الخدمة أو الذين يستخدمونها بطريقة أخرى. **المادة 25 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - أمر تسليم المعلومات** تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى: 1. أي شخص في إقليمها لتسليم معلومات معينة في حيازة ذلك الشخص والمخزنة على تقنية معلومات أو وسيط تخزين معلومات. 2. أي مزود خدمة يقدم خدماته في إقليم الدولة الطرف لتسليم معلومات المشترك المتعلقة بتلك الخدمات في حوزة مزود الخدمة أو تحت سيطرته.		
المادة 21 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[421] **اعتراض بيانات المحتوى** 1. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وغيرها من الإجراءات، فيما يتعلق بمجموعة من الجرائم الخطيرة التي يحددها القانون المحلي، لتمكين سلطاته المختصة من: a. الجمع أو التسجيل من خلال تطبيق الوسائل التقنية على أراضي ذلك الطرف، و إلزام مزود الخدمة، في حدود قدرته التقنية الحالية:	**القانون الأساسي رقم 61-2016، بتاريخ 3 أغسطس 2016، بشأن منع ومكافحة الاتجار بالبشر (الاتجار بالأشخاص).** **المادة 42** يعاقب بالسجن مدة خمسة أعوام و بخطية قدرها خمسة آلاف دينار كل من يتعمد اعتراض الاتصالات والمراسلات أو المراقبة السمعية البصرية في غير الأحوال المسموح بها قانونا و دون احترام الموجبات القانونية.	**التحليل القانوني** تعتبر هذه السلطة ضرورية للتشريعات الوطنية؛ ويجب أن تكون هناك ضمانات ومتطلبات / إجراءات لإلزام مقدمي الخدمة على التعاون في جمع أو تسجيل بيانات المحتوى في الوقت الحقيقي لاتصالات محددة تتم في تونس. لا يحتوي التشريع الوطني على أحكام صريحة تتعلق بجمع البيانات في الوقت الحقيقي. على الرغم من أن التقييد على استخدام تقنية اعتراض الاتصالات تم تجريمه في المادة 42 من القانون الأساسي رقم 61-2016 والمادة 64 من القانون الأساسي رقم 26-2015

421. لا يوجد ما يعادلها في اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية

إجراءات		
أفضل الممارسات الدولية	**التشريع الوطني**	**ملاحظات**
i. الجمع أو التسجيل من خلال تطبيق الوسائل التقنية على أراضي ذلك الطرف؛ أو ii. التعاون ومساعدة السلطات المختصة في جمع أو تسجيل بيانات المحتوى في الوقت الحقيقي، لاتصالات محددة تتم في أراضيها وترسل عن طريق نظام حاسوبي. 2. في الحالات التي لا يمكن فيها لأي طرف، بسبب المبادئ المستقرة في نظامه القانوني الداخلي، أن يعتمد التدابير المشار إليها في الفقرة 1.أ، يجوز له بدلا من ذلك اعتماد تدابير تشريعية وتدابير أخرى قد تكون ضرورية لضمان جمع أو تسجيل البيانات المرورية المرتبطة باتصالات محددة مرسلة في أراضيه، في الوقت الحقيقي، من خلال تطبيق الوسائل التقنية على ذلك الإقليم. 3. يعتمد كل طرف التدابير التشريعية والتدابير الأخرى التي قد تكون ضرورية لإلزام مقدم الخدمة بالحفاظ على سرية تنفيذ أي سلطة منصوص عليها في هذه المادة وأي معلومات تتعلق بها. 4. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و 15. **القسم 26 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - اعتراض بيانات المحتوى** 1. إذا تأكد [قاض] بناء على [شهادة تحت القسم] [شهادةً خطية] بأن هناك أسباباً معقولة لـ [الاشتباه] [الظن] بأن محتوى البلاغات الإلكترونية هو مطلوب بشكل معقول لأغراض [التحقيق] في تحقيق جنائي، [يجوز] [للقاضي] [يجب] أن: • يطلب من مزود خدمة الإنترنت الذي تتوفر خدمته في [بلد المشرع] جمع أو تسجيل أو السماح أو مساعدة السلطات المختصة في جمع أو تسجيل بيانات المحتوى المرتبطة بالاتصالات المحددة التي يتم إرسالها عن طريق نظام حاسوب، وذلك من خلال استخدام وسائل تقنية؛ أو • السماح لموظف [قوة تنفيذ القانون] [الشرطة] بجمع أو تسجيل تلك البيانات من خلال تطبيق الوسائل التقنية. 2. قد تقرر دولة عدم تنفيذ القسم 26.	والمحاولة موجبة للعقاب. **القانون الأساسي رقم 26-2015، بتاريخ 7 أغسطس 2015، بشأن مكافحة الإرهاب ومنع غسل الأموال.** **المادة 64** يعاقب بالسجن مدة خمسة أعوام و بخطية قدرها خمسة آلاف دينار كل من يتعمد اعتراض الاتصالات والمراسلات أو المراقبة السمعية البصرية في غير الأحوال المسموح بها قانونا و دون احترام الموجبات القانونية. والمحاولة موجبة للعقاب.	**تحليل الفجوة** **التوصيات:** يجب اتخاذ تدابير لإلزام مقدمي الخدمات في تونس بالتعاون من أجل جمع المحتوى في الوقت الحقيقي؛ وينبغي اتخاذ الضمانات للتأكد من أن جمعها قانوني وضروري ومعقول ومتناسب مع الحالة. يجب مراعاة مراجعة المادة 29 من CITO والمادة 21 من اتفاقية بودابست والقسم 26 من **مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية** وإدراج اللغة في التشريعات الوطنية

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة CITO 29 - اعتراض معلومات المحتوى 1. تلتزم كل دولة طرف باعتماد الإجراءات التشريعية اللازمة المتعلقة بسلسلة من الجرائم المنصوص عليها في القانون المحلي، وذلك لتمكين السلطات المختصة من: a. تسجيل أو جمع المعلومات من خلال الوسائل التقنية في أراضي هذه الدولة الطرف، أو b. التعاون مع السلطات المختصة ومساعدتها على تسريع جمع وتسجيل معلومات المحتوى الخاصة بالاتصالات ذات الصلة في إقليمها والتي يتم نقلها عن طريق تكنولوجيا المعلومات. 2. إذا تعذر على الدولة الطرف، بسبب النظام القانوني المحلي، اعتماد الإجراءات المبينة في الفقرة 1 (أ)، يجوز لها اعتماد إجراءات أخرى بالشكل الضروري لضمان تسريع جمع وتسجيل معلومات المحتوى المقابلة الاتصالات ذات الصلة في أراضيها باستخدام الوسائل التقنية في ذلك الإقليم. 3. تلتزم كل دولة طرف باعتماد الإجراءات اللازمة لمطالبة مقدم الخدمة بالحفاظ على سرية أي معلومات عند ممارسة السلطة المنصوص عليها في هذه المادة.		
المادة 20 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست[422] **جمع بيانات حركة الاتصالات في الوقت الحقيقي** 1. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتمكين سلطاته المختصة من: a. الجمع أو التسجيل من خلال تطبيق الوسائل التقنية على أراضي ذلك الطرف، و إلزام مزود الخدمة، في حدود قدرته التقنية الحالية: i. الجمع أو التسجيل من خلال تطبيق الوسائل التقنية على أراضي ذلك الطرف؛ أو ii. التعاون ومساعدة السلطات المختصة في جمع أو تسجيل بيانات المحتوى في الوقت الحقيقي، لاتصالات محددة تتم في أراضيها وترسل عن طريق نظام حاسوبي.		**التحليل القانوني** لا توجد سلطة إجرائية فقط لجمع بيانات حركة المرور في الوقت الحقيقي. يمكن أن يكون هناك حد أدنى لجمع بيانات حركة المرور في الوقت الحقيقي، وتعد هذه الحركة أداة تحقيق أساسية. قد تكون هناك حالات لا يضع فيها مقدم الطلب حدًا قانونيًا أعلى لتأمين المحتوى، ولكن يمكن وجود حد أدنى لتأمين حركة المرور. لهذا السبب، يجب أن يكون هناك تمييز بين جمع المحتوى المخزن وبيانات المرور في الوقت الحقيقي. يجب أن تكون هناك ضمانات ومتطلبات/إجراءات لإلزام مزودي خدمة الاتصالات على التعاون في جمع أو تسجيل بيانات المحتوى في الوقت الفعلي لاتصالات محددة تتم في تونس

422. المادة 31 (3) (ه) - تشير المادة 28 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات إلى الجمع المستعجل بدلًا من الجمع في الوقت الفعلي

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
2. في الحالات التي لا يمكن فيها لأي طرف، بسبب المبادئ المستقرة في نظامه القانوني الداخلي، أن يعتمد التدابير المشار إليها في الفقرة 1.أ، يجوز له بدلا من ذلك اعتماد تدابير تشريعية وتدابير أخرى قد تكون ضرورية لضمان جمع أو تسجيل البيانات المرورية المرتبطة باتصالات محددة مرسلة في أراضيه، في الوقت الفعلي، من خلال تطبيق الوسائل التقنية على ذلك الإقليم. 3. يعتمد كل طرف التدابير التشريعية والتدابير الأخرى التي قد تكون ضرورية لإلزام مقدم الخدمة بالحفاظ على سرية تنفيذ أي سلطة منصوص عليها في هذه المادة وأي معلومات تتعلق بها. 4. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و 15. **القسم 25 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - جمع بيانات حركة الاتصالات** 1. إذا تأكد [قاض] بناء على [شهادة تحت القسم] [شهادة خطية] بأن هناك أسباباً معقولة لـ [الاشتباه] [الظن] بأن بيانات حركة الاتصالات المرتبطة ببلاغ محدد ضرورية بشكل معقول لأغراض [التحقيق] في تحقيق جنائي، [يجوز] [للقاضي] [يجب] أن يأمر شخصًا يتحكم بهذه البيانات بما يلي: • جمع أو تسجيل بيانات حركة الاتصالات المرتبطة باتصالات محددة خلال فترة محددة؛ أو التصريح ومساعدة ضابط [الشرطة] [قوة تنفيذ القانون] محدد لجمع أو تسجيل تلك البيانات. 2. إذا تأكد [قاض] بناء على [شهادة تحت القسم] [شهادة خطية] بأن هناك أسباباً معقولة لـ [الاشتباه] [الظن] بأن بيانات حركة الاتصالات المرتبطة ببلاغ محدد ضرورية بشكل معقول لأغراض [التحقيق] في تحقيق جنائي، [يجوز] [للقاضي] [يجب] أن يسمح لـ [قوة تنفيذ القانون] [الشرطة] بجمع أو تسجيل بيانات حركة الاتصالات المرتبطة برسالة محددة خلال فترة محددة من خلال تطبيق الوسائل التقنية. 3. قد تقرر دولة عدم تنفيذ القسم 25.	**لا يوجد معادل**	**تحليل الفجوة** **التوصيات:** ينبغي توفير صلاحية محددة لجمع بيانات المرور في الوقت الفعلي، وينبغي إدراج حكم لإلزام مزودي خدمة الاتصالات في تونس على التعاون لجمع بيانات المرور في الوقت الفعلي؛ ويجب إدراج ضمانات لضمان أن جمعها قانوني وضروري ومعقول ومتناسب مع الحالة. يمكن اعتماد اللغة من المادة 28 الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لكنها لا تشير إلى الجمع المستعجل في الوقت الحقيقي. يجب استخدام المادة 20 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست والمادة 25 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية باعتبارهما دليلًا للتشريعات الوطنية

إجراءات		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
		واجب الكشف عن مفاتيح التشفير مع استخدام الإرهابيين والمجرمين المنظمين بشكل روتيني لتطبيقات الرسائل المشفرة[423]، قد يعتبر الكشف عن مفاتيح التشفير قوة ملائمة لإطلاق مفاتيح كلمات المرور لفتح الأجهزة[424] **تحليل الفجوة** **التوصيات:** عدم القدرة على توضيح ما إذا كانت هناك أية صلاحيات في تونس - لكن هذه الصلاحيات ستتيح لوكالات إنفاذ القوانين إجبار أصحاب الأجهزة على فتحها
		التزامات الاحتفاظ بالبيانات[425] تسمح مثل هذه السلطة لوكالات إنفاذ القانون بـ 1. تتبع وتحديد مصدر الاتصال 2. تحديد وجهة الاتصال؛ 3. تحديد تاريخ ووقت ومدة الاتصال؛ و 4. تحديد نوع الاتصال تونس لديها هذا النوع من الالتزام[426]

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
المادة 22 من اتفاقية بودابست **الاختصاص القضائي** 1. يعتمد كل طرف ما قد يلزم من إجراءات تشريعية وغيرها من الإجراءات لإقامة ولاية قضائية على أي جرم منصوص عليه في المواد من 2 إلى 11 من هذه الاتفاقية، عندما تُرتكب الجريمة: a. في أراضيها؛ أو b. على متن سفينة ترفع علم تلك الدولة الطرف؛ أو c. على متن طائرة مسجلة بموجب قوانين ذلك الطرف؛ أو d. من قِبَل أحد رعاياها، إذا كانت الجريمة معاقبًا عليها بموجب القانون الجنائي حيث ارتكبت، أو إذا ارتكبت الجريمة خارج الولاية الإقليمية لأي دولة.	**لا يوجد معادل**	**التحليل القانوني** بدون وجود نطاق محدد بوضوح للجرائم الإلكترونية ، وهي دولية بطبيعتها سيبقى أي تشريع مقيدًا. **تحليل الفجوة** **التوصيات:** يضمن التشريع الوطني أن يتم تعريف الاختصاص باستخدام لغة المادة 22 من اتفاقية بودابست، القسم 19 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية أو المادة 30 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. إذا كان هناك تعارض بين السلطات القضائية، فيجب أن تؤخذ في الاعتبار المبادئ التوجيهية المتعلقة بتحديد الولاية القضائية المناسبة لمحاكمة جريمة ما - انظر المبادئ التوجيهية Eurojust لتقرير الولاية القضائية التي في الجرائم التي تجب ملاحقتها (المراجعة 2016)[427]

423. Eleanor Saitta. “Can Encryption Save Us?” Nation 300, no. 24 (15 يونيو 2015): 16-18. Academic Search Premier, EBSCOhost (تمت زيارته في 29 فبراير 2016)

424. انظر مثلاً القسم 49 من القانون الإنجليزي (Regulation of Investigatory Powers Act 2000 (UK - http://www.legislation.gov.uk/ukpga/2000/23/section/49

425. أصدر الاتحاد الأوروبي في عام 2006 توجيهه بشأن الاحتفاظ بالبيانات - اضطرت الدول الأعضاء في الاتحاد الأوروبي إلى تخزين بيانات الاتصالات الإلكترونية لمدة ستة أشهر على الأقل و 24 شهراً على الأكثر للتحقيق في الجرائم الخطيرة وكشفها ومقاضاة مرتكبيها. أبطلت محكمة العدل الأوروبية في عام 2014 توجيه الاحتفاظ بالبيانات، حيث قررت أنها قدمت ضمانات غير كافية ضد التدخلات في الخصوصية وحماية البيانات. في حالة عدم وجود توجيه صالح للاتحاد الأوروبي بشأن الاحتفاظ بالبيانات، يجوز للدول الأعضاء تقديم خطة للاحتفاظ بالبيانات - للاطلاع على الخطط الوطنية، انظر: http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention

426. تقرير ICMEC العالمي، الصفحة 40

427. http://www.eurojust.europa.eu/Practitioners/operational/Documents/Operational-Guidelines-for-Deciding.pdf

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
2. يجوز لكل طرف أن يحتفظ بالحق في عدم تطبيق أو تطبيق قواعد الاختصاص المنصوص عليها في الفقرات من 1 إلى 1 د من هذه المادة أو أي جزء منها فقط في حالات أو شروط محددة. 3. يعتمد كل طرف ما قد يلزم من إجراءات لإقامة ولاية قضائية على الجرائم المشار إليها في الفقرة 1 من المادة 24 من هذه الاتفاقية، في الحالات التي يكون فيها الجاني المفترض موجودا في إقليمه ولا يسلمه إلى بلد آخر بعد طلب التسليم على أساس جنسيته فقط. 4. لا تستبعد هذه الاتفاقية أي ولاية قضائية جنائية يمارسها أي طرف وفقًا لقانونه الداخلي. 5. عندما يطالب أكثر من طرف بالولاية القضائية على جريمة مفترضة تم النص عليها في هذه الاتفاقية، يتشاور الطرفان المعنيان، عند الضرورة من أجل تحديد الولاية القضائية الأنسب. **القسم 19من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - الولاية القضائية** ينطبق هذا القانون على أي فعل أو تقصير: • في إقليم [الدولة المشترعة]؛ أو • على سفينة أو طائرة مسجلة في [الدولة المشترعة]؛ أو • من قبل أحد مواطني [الدولة المشترعة] خارج الولاية القضائية لأي بلد؛ أو من قبل أحد مواطني [الدولة المشترعة] خارج إقليم [الدولة المشترعة]، إذا كان سلوك هذا الشخص يشكل أيضًا جريمة بموجب قانون البلد الذي ارتكبت فيه الجريمة. **المادة 30 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - الاختصاص** 1. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد اختصاصها على أي من الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية وذلك إذا ارتكبت الجريمة كلياً أو جزئياً أو تحققت: a. في إقليم الدولة الطرف على متن سفينة تحمل علم الدولة الطرف. b. على متن طائرة مسجلة تحت قوانين الدولة الطرف.		

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
c. من قبل أحد مواطني الدولة الطرف إذا كانت الجريمة يعاقب عليها حسب القانون الداخلي في مكان ارتكابها أو إذ ارتكبت خارج منطقة الاختصاص القضائي لأية دولة. d. إذا كانت الجريمة تمس أحد المصالح العليا للدولة. 2. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد الاختصاص الذي يغطي الجرائم المنصوص عليها في المادة 31، الفقرة 1 من هذه الاتفاقية في الحالات التي يكون فيها الجاني المزعوم حاضرا في إقليم تلك الدولة الطرف ولا يقوم بتسليمه إلى طرف آخر بناء على جنسيته بعد طلب التسليم. 3. إذا ادعت أكثر من دولة بالاختصاص القضائي لجريمة منصوص عليها في هذه الاتفاقية فيقدم طلب الدولة التي أخلت الجريمة بأمنها أو بمصالحها ثم الدولة التي وقعت الجريمة في إقليم ثم الدولة التي يكون الشخص المطلوب من رعاياها وإذا اتحدت الظروف فتقدم الدولة الأسبق في طلب التسليم. في حالة وجود ظروف مماثلة، تُعطى الأولوية لأول دولة تطلب التسليم.		
المادة 35 من اتفاقية بودابست[428] **شبكة تعمل على مدار اليوم والساعة** 1. يعين كل طرف جهة اتصال متاحة على مدار أربع وعشرين ساعة وطوال أيام الأسبوع، من أجل ضمان تقديم مساعدة فورية بغرض إجراء تحقيقات أو إجراءات تتعلق بالجرائم الجنائية المتعلقة بأنظمة الحاسوب والبيانات، أو لجمع أدلة عن الجرائم الجنائية في شكل إلكتروني. يجب أن تشمل هذه المساعدة تيسير الإجراءات التالية، أو تنفيذها مباشرة إذا سمح القانون الداخلي بذلك: a. تقديم المشورة الفنية؛ b. الحفاظ على البيانات وفقا للمادتين 29 و 30؛ c. جمع الأدلة وتوفير المعلومات القانونية وتحديد مكان المشتبه به.	**لا يوجد معادل**	**التحليل القانوني** هذه آلية أساسية لتحقيق قدرة فعالة على التحقيق في الجرائم الإلكترونية. **تحليل الفجوة** **التوصيات:** لا ينبغي أن يتطلب ذلك تشريعًا خاصًا لتنفيذه، وفيما يتعلق بالموارد يجب أن تُعطى الأولوية. يجب مشاركة تفاصيل الاتصال لنقطة الاتصال الوحيدة المعينة (SPOC) على المستوى الوطني ومع السلطات المركزية على المستوى الدولي والإنتربول. ينبغي أيضًا النظر في صياغة مذكرة تفاهم مع الوكالات الوطنية بحيث يكون لدى نقطة الاتصال الوحيدة المعينة سلطة القيام بالإجراءات المطلوبة كجزء من تحقيق دولي في جرائم الإنترنت وتطبيق القوانين والمعاهدات الوطنية. ستتضمن مذكرة التفاهم هذه الطلبات الواردة والصادرة وتضمن عملية فعالة وكفؤة.

428. المادة 43 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
2. a. يجب أن يكون لدى جهة الاتصال التابعة لكل طرف القدرة على إجراء الاتصالات مع جهة اتصال الطرف الآخر على وجه السرعة. b. إذا لم تكن نقطة الاتصال التي حددها أحد الأطراف جزءًا من سلطة أو سلطات ذلك الطرف المسؤولة عن المساعدة أو التسليم المتبادلين الدوليين، فيجب أن تضمن قدرتها على التنسيق مع هذه السلطة أو السلطات على وجه السرعة. 3. يجب على كل طرف التأكد من توفر الأفراد المدربين والمجهزين من أجل تسهيل تشغيل الشبكة.		
المادة 25 من اتفاقية بودابست **المبادئ العامة المتعلقة بالمساعدة المتبادلة** 1. يقدم الطرفان المساعدة المتبادلة إلى أقصى حد ممكن لغرض إجراء التحقيقات أو الإجراءات المتعلقة بالجرائم الجنائية المتعلقة بأنظمة الحاسوب والبيانات، أو لجمع الأدلة المتعلقة بالجرائم الجنائية في شكل إلكتروني. 2. يعتمد كل طرف أيضًا الإجراءات التشريعية وغيرها من الإجراءات التي قد تكون ضرورية لتنفيذ الالتزامات المنصوص عليها في المواد من 27 إلى 35. 3. يجوز لكل طرف في الظروف العاجلة تقديم طلبات للمساعدة المتبادلة أو الاتصالات المتعلقة بها عن طريق وسائل الاتصال العاجلة، بما في ذلك الفاكس أو البريد الإلكتروني، إلى الحد الذي توفر فيه هذه الوسائل مستويات مناسبة من الأمن والمصادقة (بما في ذلك استخدام التشفير، عند الضرورة)، مع تأكيد رسمي لاحق، حيثما يطلب ذلك الطرف متلقي الطلب. يجب على الطرف متلقي الطلب قبول الطلب والرد عليه بأي وسيلة اتصال سريعة.		**التحليل القانوني** تضمن المادة 25 من اتفاقية بودابست إمكانية استخدامها كأداة لتسهيل المساعدة القانونية المتبادلة.[429] تونس ليست طرفًا في اتفاقية بودابست أو الاتفاقية العربية لمكافحة جرائم تقنية المعلومات أو اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية. هذا يعني أن تونس ليست طرفًا في أي اتفاقية دولية مخصصة للجرائم السيبرانية، وسيعيق ذلك التحقيقات الدولية لأن السلطات الإجرائية لن يكون لها أساس قانوني. بخلاف أي اتفاقية ثنائية - تونس من الدول الموقعة على اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية[430] لذلك فإن المادة 18 من تلك الاتفاقية هي أساس المساعدة القانونية المتبادلة والتبادلية/مبدأ المعاملة بالمثل.[431] وهذا يعني أنه بدون التشريعات الوطنية لا يمكن تقديم طلبات للحفظ المستعجل لبيانات الحاسوب المخزنة والحفظ المستعجل والكشف الجزئي لبيانات الحركة والكشف عن البيانات المخزنة وبيانات الحركة، بمعنى وجود قيود على التعاون الدولي الذي يمكن أن توفره تونس للدول مقدمة الطلب. انظر الملحق أ للاطلاع على أنواع الطلبات الدولية المرسلة من تونس.

429. لا يوجد حكم مماثل في اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية
430. تم التصديق في 19 يونيو 2003
431. يمكن للمادة 18 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة أن تكون أساس قانون مكافحة غسل الأموال إذا كان تعريف الجريمة المنظمة عبر الوطنية مصدقًا عليه، ويمكن أن تكون اتفاقية الرياض بشأن التعاون القضائي أساسًا تشريعيًا للدول التي صادقت عليها

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
4. باستثناء ما هو منصوص عليه على وجه التحديد في المواد الواردة في هذا الفصل، تخضع المساعدة المتبادلة للشروط المنصوص عليها في قانون الطرف متلقي الطلب أو معاهدات المساعدة المتبادلة المطبقة، بما في ذلك الأسباب التي تُجيز للطرف متلقي الطلب أن يرفض التعاون. لا يجوز للطرف متلقي أن يبني حقه في رفض المساعدة المتبادلة المتعلقة بالجرائم المشار إليها في المواد من 2 إلى 11، فقط على أساس أن الطلب يتعلق بجريمة يعتبرها جريمة مالية. 5. عندما تسمح أحكام هذا الفصل للطرف متلقي الطلب بتقييد المساعدة المتبادلة بشرط ازدواجية التجريم، يعتبر هذا الشرط مستوفًيا، بصرف النظر عما إذا كانت قوانينه تضع الجريمة في نفس الفئة الجرمية، أو إذا أعطيت الجريمة نفس التسمية عند الطرف الطالب، وذلك إن كان السلوك الكامن وراء الجريمة التي طلبت المساعدة من أجلها جريمة جنائية بموجب قوانينه. **المادة 34 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - الإجراءات المتعلقة بطلبات التعاون والمساعدة المتبادلة** 1. 1 تطبق أحكام الفقرات 9-2 من هذه المادة في حالة عدم وجود معاهدة أو اتفاقية تعاون ومساعدة متبادلة وفقًا للتشريعات المعمول بها بين الدول الأطراف التي تطلب المساعدة وتلك التي تُطلَب منها المساعدة. في حال وجوده جود معاهدة أو اتفاقية فلا تطبق الفقرات المشار إليها إلا إذا اتفقت الأطراف المعنية على تطبيقها كاملة أو بشكل جزئي. 2. a. على كل دولة طرف تحديد سلطة مركزية تكون مسؤولة عن إرسال وإجابة طلبات المساعدة المتبادلة وتنفيذ هذه الطلبات وإيصالها إلى السلطات المعنية لتنفيذها.		**تحليل الفجوة** **التوصيات:** يُطلب من القانون المحلي الحفاظ على بيانات الحاسوب المخزنة على وجه السرعة، والحفظ المستعجل والكشف الجزئي لبيانات الحركة وطلبات النسخ. يمكن استخدام اتفاقية بودابست واتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية و الاتفاقية العربية لمكافحة جرائم تقنية المعلومات كسوابق من أجل المحافظة المستعجلة على بيانات الحاسوب المخزنة،[432] والحفظ المستعجل والكشف الجزئي لبيانات المرور،[433] والكشف عن البيانات المخزنة[434] والجمع المستعجل لبيانات المرور[435] - هناك حاجة أيضًا للنظر في إمكانية السماح باعتراض بيانات ومحتويات حركة المرور في الوقت الحقيقي[436]. علاوة على ذلك، يجب أن يكون هناك إطار للتعاون في تحقيقات جرائم الإنترنت التي تنص عليها اتفاقيات متعددة الأطراف مثل المادة 27 من اتفاقية بودابست والمادة 32 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.[437] ينبغي النظر في السماح للسلطات المختصة بإعطاء الإذن لهيئات إنفاذ القانون المحلي بإجراء تحقيق في الدولة التي تأكد فيها الوصول إلى الجهاز. يعد الوصول إلى المعلومات هو المعيار الأساسي لبدء التحقيق في الحالات التي يتعذر فيها معرفة مكان تخزين البيانات (أي في التخزين السحابي). يمكن أن يشمل ذلك "اعترافًا متبادلًا" بأوامر المحكمة الصادرة تجاه مقدمي خدمات الاتصالات في دولة معينة، والتي يمكن تقديمها إلى فروع مقدمي خدمة العملاء الموجودين في دول أخرى، اعتمادًا على مكان تخزين البيانات.

432. المادة 29 من اتفاقية بودابست، القسم 23 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية والمادة 37 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

433. المادة 30 من اتفاقية بودابست، القسمان 23 و 24 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية والمادة 38 الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

434. المادة 31 من اتفاقية بودابست والمادة 39 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

435. المادة 41 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

436. المادتان 33 و 34 من اتفاقية بودابست، والقسمان 25 و 26 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية

437. لا توجد أحكام مكافئة بشأن إجراءات المساعدة القانونية المتبادلة في اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
b. على السلطات المركزية أن تتصل ببعضها مباشرة. c. على كل دولة طرف - وقت التوقيع أو إيداع أدوات التصديق أو القبول أو الموافقة - أن تتصل بالأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس العدل العرب وتنقل إليهما أسماء وعناوين السلطات المحددة خصيصا لغايات هذه الفقرة. d. تقوم الأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس وزراء العدل العرب بإنشاء وتحديث سجل للسلطات المركزية والمعينة من قبل الدول الأطراف. وعلى كل دولة طرف أن تتأكد من أن التفاصيل الموجودة في السجل صحيحة دائما 3. يتم تنفيذ طلبات المساعدة المتبادلة في هذه المادة وفقًا للإجراءات التي تحددها الدولة الطرف الطالبة، إلا في حالة عدم الامتثال لقانون الدولة الطرف متلقية طلب المساعدة. 4. يجوز للدولة الطرف المطلوب منها المساعدة أن تؤجل الإجراءات المتخذة بشأن الطلب إذا كانت هذه الإجراءات تؤثر على التحقيقات الجنائية التي تجري من قبل سلطاتها. 5. قبل رفض أو تأجيل المساعدة يجب على الدولة الطرف المطلوب منها المساعدة بعد استشارة الدولة الطرف الطالبة لها أن تقرر فيما إذ سيتم تلبية الطلب جزئيا أو يكون خاضعا للشروط التي قد ترها ضرورية. 6. تلتزم الدولة الطرف المطلوب منها المساعدة أن تُعلِم الدولة الطرف الطالبة لها بنتيجة تنفيذ الطلب. وإذا تم رفض أو تأجيل الطلب، يجب إعطاء أسباب هذا الرفض أو التأجيل. ويجب على الدولة الطرف المطلوب منها المساعدة أن تعلم الدولة الطرف الطالبة لها بالأسباب التي تمنع تنفيذ الطلب بشكل نهائي أو الأسباب التي تؤخره بشكل كبير. 7. يجوز للدولة الطرف الطالبة للمساعدة أن تطلب من الدولة الطرف المطلوب منها المساعدة الإبقاء على سرية حقيقة ومضمون أي طلب يندرج في هذا الفصل ما عدا القدر لكافي لتنفيذ الطلب. وإذا لم تستطع الدولة الطرف المطلوب منها المساعدة الالتزام بهذا الطلب للسرية، يجب عليها إعلام الدولة الطرف الطالبة والتي ستقرر مدى إمكانية تنفيذ الطلب.		

التعاون الدولي		
أفضل الممارسات الدولية	**التشريع الوطني**	**ملاحظات**
8. a. في الحالات العاجلة، يجوز إرسال طلبات المساعدة المتبادلة مباشرة إلى السلطات القضائية في الدولة الطرف المطلوب منها المساعدة من نظيرتها في الدولة الطرف الطالبة لها. وفي مثل هذه الحالات، يجب إرسال نسخة الوقت من السلطة المركزية في الدولة الطرف الطالبة إلى نظيرتها في الدولة الطرف المطلوب منها. b. يجوز إجراء الاتصالات وتقديم الطلبات حسب هذه الفقرة بواسطة الإنتربول. c. حيثما يتم تقديم طلب حسب الفقرة أ ولم تكن السلطة مختصة بالتعامل مع الطلب فيجب عليها إحالة الطلب إلى السلطة المختصة وإعلام الدولة الطرف الطالبة للمساعدة مباشرة بذلك. d. إن الاتصالات والطلبات التي تتم حسب هذه الفقرة والتي لا تشمل الإجراء القسري يمكن بثها مباشرة من قبل السلطات المختصة في الدولة الطرف الطالبة للمساعدة إلى نظيرتها في الدولة الطرف المطلوب منها المساعدة. e. يجوز لكل دولة طرف، وقت التوقيع أو التصديق أو القبول أو الإقرار أو الانضمام إبلاغ الأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس وزراء العدل العرب بأن الطلبات حسب هذه الفقرة يجب توجيهها إلى السلطة المركزية لغايات الفعالية.		
المادة 26 من اتفاقية بودابست **المعلومات التلقائية** 1. يجوز للطرف، في حدود قانونه الداخلي ودون طلب مسبق، أن يحيل إلى الطرف الآخر المعلومات التي تم الحصول عليها في إطار تحقيقاته، عندما يرى أن الكشف عن هذه المعلومات قد يساعد الطرف المتلقي في بدء أو التحقيقات أو الإجراءات المتعلقة بالجرائم الجنائية المنصوص عليها في هذه الاتفاقية، أو قد تؤدي إلى طلب تعاون من جانب هذا الطرف بموجب هذا الفصل.	**لا يوجد معادل**	**التحليل القانوني** يعد هذا إجراءً هامًا لتمكين الدولة من الاحتفاظ بمعلومات من شأنها أن تساعد دولة أخرى على منع جريمة الإنترنت أو التحقيق فيها. وعلى الرغم من أن ذلك متاحًا بين الدول التي صدقت على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الوارد ذكرهم في المادة 33 من الاتفاقية، فليس لتونس أي أساس قانوني محلي يجبره بمشاركة هذه المعلومات مع الدول غير الموقعة على الاتفاقية ما لم يتم إرسال طلب رسمي عبر قنوات المساعدة القانونية المتبادلة المعتادة.

التعاون الدولي		
أفضل الممارسات الدولية	**التشريع الوطني**	**ملاحظات**
2. قبل تقديم هذه المعلومات، يجوز للطرف المقدم أن يطلب الحفاظ على سريتها أو استخدامها فقط وفقًا للشروط. إذا لم يستطع الطرف المتلقي الامتثال لهذا الطلب، فيجب عليه إخطار الطرف المقدم الذي يحدد بعد ذلك ما إذا كان ينبغي تقديم المعلومات. إذا قبل الطرف المتلقي المعلومات وفقًا لهذه الشروط فعليه أن يلتزم بها. **المادة 33 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - المعلومات العرضية المتلقاة** 1. يجوز لأي دولة طرف - ضمن حدود قانونها الداخلي - وبدون طلب مسبق أن تعطي لدولة أخرى معلومات حصلت عليها من خلال تحقيقاتها إذا اعتبرت أن كشف مثل هذه المعلومات يمكن أن تساعد الدولة الطرف المرسلة إليها في إجراء الشروع أو القيام بتحقيقات في الجرائم المنصوص عليها في هذه الاتفاقية أو قد تؤدي إلى طلب للتعاون من قبل تلك الدولة الطرف. 2. قبل إعطاء مثل هذه المعلومات، يجوز للدولة الطرف المزودة أن تطلب الحفاظ على سرية المعلومات، وإذا لم تستطع الدولة الطرف المستقبلة الالتزام بهذا الطلب يجب عليها إبلاغ الدولة الطرف المزودة بذلك والتي تقرر بدورها مدى إمكانية التزويد بالمعلومات. وإذا قبلت الدولة الطرف المستقبلة المعلومات مشروطة بالسرية، فيجب أن تبقى المعلومات بين الطرفين.		تنص المادة 18 (4) - (5) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة على تبادل المعلومات الاستخباراتية تلقائيًا في الأمور التي تفي بتعريف جريمة خطيرة[438]، ذات طابع عبر وطني[439] وأن جماعة إجرامية منظمة ضالعة في ارتكاب الجرم[440]. دون استيفاء هذا التعريف، يجب إرسال طلب رسمي عبر قنوات المساعدة القانونية المتبادلة المعتادة إلى الدول التي ليست عضوًا في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. وبسبب الطبيعة السريعة الحركة للجريمة السيبرانية، فإن المشاركة التلقائية هي وسيلة فعالة للتعاون مع الدول الأخرى، وغياب هذه المشاركة يمنع التعاون الدولي الفعال مع الدول غير العضو في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. **تحليل الفجوة** **التوصيات:** استخدمت اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة المادة 18 (4) - (5) أساسًا لمشاركة المعلومات التي تدخل ضمن مجال هذه الاتفاقية بشكل تلقائي (مع ضمانات مقدمة حول الاستخدام في الأدلة أو الكشف عن المعلومات الحساسة لطرف ثالث (بما في ذلك دولة أخرى).[441] النظر في التشريعات القائمة على المادة 33 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات أو المادة 26 من اتفاقية بودابست.
المادة 32 من اتفاقية بودابست **الوصول عبر الحدود إلى بيانات الحاسوب المخزنة بموافقة أو عندما تكون متاحة للجمهور** 1. يجوز للطرف، دون إذن من طرف آخر: a. الوصول إلى بيانات الحاسوب المخزنة (مفتوحة المصدر) المتاحة للجمهور، بغض النظر عن مكان وجود البيانات جغرافيا؛ أو	**لا يوجد معادل**	**التحليل القانوني** تمكن هذه السلطة الإجرائية الدولة من تأمين المحتوى المخزن في دولة أخرى في ظروف محدودة. إن المادة 32.ب من اتفاقية بودابست والمادة 40 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات هما استثناء من مبدأ الإقليمية وتسمحان بوصول منفرد عبر الحدود دون الحاجة إلى مساعدة قانونية متبادلة عندما تكون هناك موافقة أو تكون المعلومات متاحة للجمهور.

438. يقصد بتعبير «جريمة خطيرة» في المادة 2 (ب) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة أي سلوك يمثل جرما يعاقب عليه بالحرمان التام من الحرية لمدة لا تقل عن أربع سنوات أو بعقوبة أشد"

439. المادة 3 (1) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية

440. تُعرّف المادة 2 (أ) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة «الجماعة الإجرامية المنظمة» بأنها جماعة ذات هيكل تنظيمي، مؤلفة من ثلاثة أشخاص أو أكثر، موجودة لفترة من الزمن وتعمل بصورة متضافرة بهدف ارتكاب واحدة أو أكثر من الجرائم الخطيرة أو الأفعال المجرمة وفقا لهذه الاتفاقية، من أجل الحصول، بشكل مباشر أو غير مباشر، على منفعة مالية أو منفعة مادية أخرى"

441. انظر المادة 33 (2) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
b. الوصول إلى بيانات الحاسوب المخزنة الموجودة لدى طرف آخر أو استلامها، من خلال نظام حاسوب في إقليمها، إذا حصل الطرف على موافقة مشروعة وطوعية من الشخص الذي لديه السلطة القانونية للكشف عن البيانات للطرف من خلال نظام الحاسوب هذا. **القسم 27 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية - البرامج الشرعية** 1. إذا كان [القاضي] [قاضي التحقيق] مقتنعًا بناءً على [معلومات مقدمة تحت القَسَم] [شهادة خطية] أنه في سياق تحقيق متعلق بجريمة مدرجة في الفقرة 7 أدناه، توجد أسباب معقولة للاعتقاد بأنه لا يمكن جمع الأدلة الأساسية عن طريق تطبيق أحكام أخرى مدرجة في الجزء الرابع ولكنها ضرورية لأغراض التحقيق الجنائي، فإن [القاضي] [القاضي] [أن] يأذن لضابط [إنفاذ القانون] [الشرطة] بناءً على طلب باستخدام برنامج شرعي عن بعد في مهمة محددة ضرورية للتحقيق وتثبيته في نظام الحاسوب المشتبه به من أجل جمع الأدلة ذات الصلة. يجب أن يحتوي الطلب على المعلومات التالية: • المشتبه في ارتكابه الجريمة، إذا كان ذلك ممكنا مع الاسم والعنوان؛ و • وصف نظام الحاسوب المستهدف؛ و • وصف الوسيلة المقصودة ومدى ومدة الاستخدام؛ • أسباب ضرورة الاستخدام. 2. من الضروري التأكد في مثل هذا التحقيق من أن التعديلات التي يتم إدخالها على نظام الحاسوب الخاص بالمشتبه به مقصورة على تلك الضرورية للتحقيق وأن أي تغييرات يمكن التراجع عنها إذا أمكن بعد نهاية التحقيق. يكون من الضروري تسجيل الدخول أثناء التحقيق		من أمثلة استخدام هذه الصلاحية الإجرائية بموجب المادة 32 من اتفاقية بودابست: قد يتم تخزين البريد الإلكتروني لشخص ما في دولة أخرى بواسطة مزود خدمة، أو قد يقوم شخص ما بتخزين البيانات عن قصد في دولة أخرى. يجوز لهؤلاء الأشخاص استرداد البيانات بشرط أن يكون لديهم السلطة القانونية التي تخولهم ذلك، ويجوز لهم الكشف طوعًا عن البيانات لموظفي إنفاذ القانون أو السماح لهؤلاء المسؤولين بالوصول إلى البيانات[442] أو يمكن اعتقال إرهابي مشتبه به بشكل قانوني عندما يكون بريده الإلكتروني، الذي قد يحوي دليلًا على ارتكاب جريمة، مفتوحًا على الجهاز اللوحي أو الهاتف الذكي أو أي جهاز آخر. إذا وافق المشتبه طوعًا على وصول الشرطة إلى الحساب وإذا كانت الشرطة متأكدة من وجود بيانات صندوق البريد في دولة أخرى، يجوز للشرطة الوصول إلى البيانات بموجب المادة 32. ب. **تحليل الفجوة** **التوصيات:** تم تضمين هذه الصلاحية التي تؤمن الأدلة من طرف واحد في التشريعات مع ضمانات الحصول على الموافقة بشكل قانوني من المستخدم.[443] يمكن استخدام لغة المادة 32 من اتفاقية بودابست والمادة 40 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. تم انتقاد المادة 32.ب بشدة، ويمكن اعتبار أن موافقة الدولة حيث تُخزَّن بيانات الحاسوب قد تم الحصول عليها بالإضافة إلى المستخدم. ينص القسم 27 من اتفاقية مواءمة سياسات تكنولوجيا المعلومات والاتصالات والتشريعات والإجراءات التنظيمية على البرامج الشرعية وهذا قد يسمح بالوصول إلى جهاز حاسوب في دولة أخرى. هناك عدد من القيود التي تشترط عدم إمكانية الحصول على الأدلة بوسائل أخرى، وتتطلب أمرًا قضائيًا، ويمكن أن تُطبَّق على جرائم معينة فقط ضمن مدة مقيدة (3 أشهر). يجب أيضًا إيلاء الاعتبار لموافقة الدولة الأخرى التي قد يتطفل عليها البرنامج الشرعي.

442. الفقرة 294، الصفحة 53 من التقرير الإيضاحي في اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الموقعة في بودابست
443. يجب الانتباه لمواقف مثل عدم وجود المستخدم (في حالة الوفاة) وإذا كان يمكن الحصول على موافقة في دولة أخرى

التعاون الدولي		
أفضل الممارسات الدولية	التشريع الوطني	ملاحظات
• الوسيلة الفنية المستخدمة ووقت وتاريخ التطبيق؛ و • تحديد نظام الحاسوب وتفاصيل التعديلات التي أجريت في التحقيق؛ • أي معلومات تم الحصول عليها. يجب حماية المعلومات التي يتم الحصول عليها عن طريق استخدام هذا البرنامج من أي تعديل أو حذف أو وصول غير مصرح بهما. 3. تقتصر مدة الترخيص في القسم 27 (1) على [3 أشهر]. يتم إيقاف الإجراء المتخذ على الفور إذا لم تعد شروط الترخيص مستوفاة. 4. يتضمن ترخيص تثبيت البرنامج الوصول عن بُعد إلى نظام الحاسوب المشتبه به. 5. إذا كانت عملية التثبيت تتطلب الوصول الفعلي إلى مكان ما، يجب استيفاء متطلبات القسم 20. 6. يجوز لضابط [تطبيق القانون] [الشرطة] أن يطلب من المحكمة أن تأمر مقدم خدمة بالمساعدة في عملية التسليم إذا لزم الأمر، وذلك بموجب أمر المحكمة الممنوح في (1) الطلب المذكور أعلاه. 7. [قائمة الجرائم]. 8. قد تقرر دولة عدم تنفيذ القسم 27. **المادة 40 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - الوصول إلى معلومات تقنية المعلومات عبر الحدود** يجوز لأي دولة طرف، وبدون الحصول على تفويض من دولة طرف أخرى: 1. أن تصل إلى معلومات تقنية المعلومات المتوفرة للعامة (مصدر مفتوح) بغض النظر عن الموقع الجغرافي للمعلومات. 2. أن تصل إلى أو تتلقى - من خلال تقنية المعلومات في إقليمها - معلومات تقنية المعلومات الموجودة لدى الدولة الطرف الأخرى، وذلك بعد حصولها على الموافقة الطوعية والقانونية من الشخص الذي يملك السلطة القانونية لكشف المعلومات إلى تلك الدولة الطرف بواسطة تقنية المعلومات المذكورة.		

خلاصة

يظهر التحليل القانوني وتحليل الفجوة أعلاه أن دول الجنوب الشريكة في حاجة إلى تكييف وتحديث تشريعاتهم لتمكين التحقيقات الفعالة وضمان إمكانية قانونهم الوطني من الاستجابة لتهديدات الجرائم السيبرانية. ويمكن أن تكون العملية التشريعية بطيئة وهذا يزيد من التهديد والأضرار الناجمة عن الجرائم السيبرانية. والأولوية هي سن تشريعات لتلك الجرائم التي لا تمثل أي جريمة أخرى محتملة في التشريعات الوطنية ولضمان تزويد وكالات إنفاذ القوانين بالأدوات اللازمة لمقاضاة الجناة على نحو فعال. ويجب استخدام اتفاقية بودابست ومواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية والاتفاقية العربية لمكافحة جرائم تقنية المعلومات لصياغة وتعديل التشريعات لتوفير تطبيق متسق في دول الجنوب الشريكة والسماح للدول الأعضاء في الاتحاد الأوروبي بالاستخدام المتبادل. وسيؤدي ذلك إلى تمكين الحفظ المستعجل وجمع المحتوى وبيانات المرور في الوقت الفعلي. على سبيل الأولوية الفورية، يجب إنشاء نقاط اتصال واحدة (SPOC) على مدار الساعة، لضمان التعاون الدولي بشكل فعال واستباقي.

التوصيات الرئيسية من تحليل الفجوة هي كما يلي:

1. **يُوصى** بأن تقوم دول الجنوب الشريكة، في حالة عدم قيامها بذلك، بالتوقيع على اتفاقية بودابست و/أو والاتفاقية العربية لمكافحة جرائم تقنية المعلومات والتصديق عليها وتنفيذها لتمكين طلبات المساعدة القانونية المتبادلة من جمع بيانات المرور واعتراض المحتوى وأوامر التقديم والتبادل التلقائي للمعلومات في الوقت الفعلي.
2. **يُوصى** بتخصيص كل دولة من دول الجنوب الشريكة نقاط اتصال واحدة (SPOC) للتعامل مع طلبات المساعدة القانونية المتبادلة الصادرة والواردة العاجلة ومواصلة تحديث العمليات لتأمين بيانات مزودي خدمة الاتصالات من خلال الوسائل الرسمية وغير الرسمية.
3. **يُوصى بدرجة كبيرة** وضع عمليات لحفظ البيانات لتمكين إرسال طلب المساعدة القانونية المتبادلة - فبدون الحفظ - سيتم حذف البيانات ولا يمكن تنفيذ طلب المساعدة القانونية المتبادلة

المرفق (أ)

الاحصائيات التونسية على طلبات الإنابة القضائية

أصل طلبات الإنابة القضائية التي استلمتها الوكالة الفنية للاتصالات التونسية خلال الفترة من 16 أبريل 2014 إلى 10 يونيو 2017	
النوع	**العدد**
فرع إدارتي الاستخبارات والتحقيقات بالحرس الوطني	836
مراكز الشرطة الوطنية	1372
مديرية الشرطة القضائية	454
الفرع المعاون للقضايا الجنائية	271
العدل	223
مديرية الرعاية الاجتماعية	65
المديرية المعاونة للبحوث والدراسات الاقتصادية والمالية	43
الوحدة الوطنية للبحث في الجرائم الارهابية	204
أخرى	42
المجموع	3510

الموضوعات المتعلقة بطلبات الإنابة القضائية التي استلمتها الوكالة التونسية لتقنيات الاتصالات خلال الفترة من 16 أبريل 2014 إلى 10 يونيو 2017	
تسجيل دخول صاحب حساب الفيسبوك	1290
التعرف على مستخدم الهاتف المحمول	1731
التعرف على هوية لص الحاسوب	193
تحديد مستغل عنوان بروتوكول الإنترنت	107
تحديد صاحب حساب سكايب	7
تحديد صاحب حساب البريد الإلكتروني	70
تحديد صاحب الموقع الإلكتروني	51
تسجيل دخول صاحب حساب تويتر	16
تحديد صاحب حساب يوتيوب	2
استخراج المحتوى من الهاتف المحمول أو الحاسوب	26
المشغلين	17
المجموع	3510

قائمة المراجع

1. African Union, Oliver Tambo Declaration, Johannesburg 2009
2. اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية
3. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات
4. اتفاقية بودابست بشأن الجريمة السيبرانية التابعة لمجلس أوروبا
5. Andy Greenberg (20 April 2011) Crypto Currency
6. Andy Greenberg (19 November 2014) Hacker Lexicon: What is the dark web?
7. Arab Social Media Report 2017 Debbie Stephenson (27 July 2014) Spear Phishing: Who's Getting Caught?
8. Comparative Analysis of the Malabo Convention of the African Union and the Budapest اتفاقية الجريمة السيبرانية 20 نوفمبر 2016
9. Eric Tamarkin, (20 January 2015) The AU's Cybercrime Response. A Positive Start, but Substantial Challenges Ahead, Policy Brief 73
10. التقرير التفسيري لاتفاقية بودابست (185) رقم 10
11. التقرير التفسيري لاتفاقية مكافحة الجرائم السيبرانية، رقم 298.
12. Gercke, 10 Years Convention on Cybercrime, Computer Law Review International, 2011
13. ICMEC Model Legislation and Global Review 8th EditionITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008
14. Strategic Seminar "Keys to Cyberspace" Eur ojust, The Hague, 2 June 2016 Outcome Report.
15. Lange/Nimsger (2004) Electronic Evidence and Discovery and Whitcomb, An Historical Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, No. 1.
16. Mohamed N. El-Guindy (2012) Cybercrime Challenges in the Middle East.
17. Mohamed N. El-Guindy (2014) Middle East Security Threat Report
18. R. Moore (2005) Cyber crime: Investigating High-Technology Computer Crime
19. Ramzan, Zulfikar (2010) Phishing attacks and countermeasures - In Stamp, Mark & Stavroulakis, Peter Handbook of Information and Communication Security Springer.
20. ملاحظات توجيهية T-CY - فاتح مارس 2017
21. تعزيز القدرة التنافسية في منطقة البحر الكاريبي من خلال مواءمة سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية
22. مشروع تور: الأسئلة الشائعة
23. Verdelho (2008) The effectiveness of international cooperation against cybercrime.
24. Warren G. Kruse, Jay G. Heiser (2002) Computer forensics: incident response essentials.
25. شكر وتقدير
26. شكر خاص لالتزام وتفاني المستشارين العلميين الذين كانت مساهمتهم أساسية في إنتاج هذا البحث.