**المعاهدات الدولية للإنترنت: حقائق وتحدّيات**

[**العدد 83 - كانون الثاني 2013**](https://www.lebarmy.gov.lb/ar/content/83-d)

**المعاهدات الدولية للإنترنت: حقائق وتحدّيات**   
إعداد: د. جورج لبكي   
محلل وباحث استراتيجي

تشكّل ثورة الإتصالات أبرز نتائج العولمة، خصوصًا، من ناحية آنية، الإتصالات وسرعتها الكبيرة التي لم يعرفها تاريخ الانسانية من قبل. إن التطور التكنولوجي الحاصل لأنظمة الإتصال أثّر تأتيرًا مباشرًا على الأمم على المستويات السياسية والثقافية والإجتماعية. من المهم جدًا معالجة موضوع القوانين التي تحكم شبكة الإنترنت وتأثيرها على المجتمعات لأن اختراق شبكة الإنترنت لحدود الدول يجعل من المستحيل تنظيمها أو مراقبتها، وبخاصةٍ من دون تعاون دولي وثيق. للشبكة العنكبوتية حسنات كبيرة من حيث نشر المعرفة ومبادىء الحرية حتى قيل أنه «إذا كنت ترغب في تحرير مجتمع ما إعطه فقط إمكان الوصول إلى الانترنت». لكن للإنترنت محاذير أهمها استعمالها للأعمال الإرهابية ولاختراق خصوصيات الأفراد ولتدمير قيم المجتمعات الإنسانية. لذلك، سعى عدد من الإتفاقيات الدولية إلى تشكيل نوعٍ من الإطار الواسع لمعالجة كل هذه التحديات.

**ظهور الانترنت كشبكة إعلام اجتماعي**

مع ظهور الإنترنت، صار تناقل الخبر أسرع وأقل كلفة من أي وقتٍ مضى في تاريخ الإتصالات. وقد تسبّبت الإنترنت بحصول تغييرات جذرية في حياة جميع شرائح المجتمع الانساني. وهنا لا بد من الإشارة الى أن الإنترنت أضحت في حالة تنافس مع المصادر التقليدية للإعلام مثل الراديو والتلفزيون، وحتى أن بعض الصحف آثر أن يلغي طبعته الورقية ليتستبدلها بطبعة على الشبكة العنكبوتية.

ويعود تاريخ الإنترنت للعام 1960 عندما بدأت أبحاث علمية في هذا المجال بتكليفٍ من الحكومة في الولايات المتحدة بالتعاون مع شركات تجارية من القطاع الخاص. والعام 1990، بدأ تسويق الإنترنت لتصبح شبكة عالمية تطال تقريبًا كل جانب من الحياة البشرية المعاصرة. ومنذ العام 2009، أضحى أكثر من ربع سكان العالم موصولاً على الشبكة العنكبوتية، والأرقام بارتفاعٍ مستمر.

ليس للإنترنت إدارة مركزية تدير عملية استخدامها بشكل مركزي مباشر يتحكّم بقواعد استخدامها أو بالنواحي التقنية للشبكة. إن ما يتم إدارته مركزيًا يشمل فقط بروتوكول العناوين[[1]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%85%D8%B9%D8%A7%D9%87%D8%AF%D8%A7%D8%AA-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A%D8%A9-%D9%84%D9%84%D8%A5%D9%86%D8%AA%D8%B1%D9%86%D8%AA-%D8%AD%D9%82%D8%A7%D8%A6%D9%82-%D9%88%D8%AA%D8%AD%D8%AF%D9%91%D9%8A%D8%A7%D8%AA" \l "_ftn1" \o ") على الإنترنت ونظام إسم النطاق[[2]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%85%D8%B9%D8%A7%D9%87%D8%AF%D8%A7%D8%AA-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A%D8%A9-%D9%84%D9%84%D8%A5%D9%86%D8%AA%D8%B1%D9%86%D8%AA-%D8%AD%D9%82%D8%A7%D8%A6%D9%82-%D9%88%D8%AA%D8%AD%D8%AF%D9%91%D9%8A%D8%A7%D8%AA" \l "_ftn2" \o "). ويتم ذلك بتوجيه من قبل مؤسسة الإنترنت للأسماء والأرقام المخصصة (ICANN)[[3]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%85%D8%B9%D8%A7%D9%87%D8%AF%D8%A7%D8%AA-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A%D8%A9-%D9%84%D9%84%D8%A5%D9%86%D8%AA%D8%B1%D9%86%D8%AA-%D8%AD%D9%82%D8%A7%D8%A6%D9%82-%D9%88%D8%AA%D8%AD%D8%AF%D9%91%D9%8A%D8%A7%D8%AA" \l "_ftn3" \o ") ومقرها في ولاية كاليفورنيا في الولايات المتحدة منذ العام 1998.

في أواخر 1990، أشارت الإحصاءات إلى أن الحركة على شبكة الإنترنت العامة تتضاعف كل عام، وذلك يعود للنموّ المتزايد لعدد مستخدمي الشبكة ولعدم وجود إدارة مركزية تتحكّم باستخدام الشبكة، الأمر الذي يسمح بالتوسّع الطبيعي لاستخدامها من دون قيود أو موانع. فأي مستخدم جديد يستطيع الإنضمام إلى الشبكة من دون قيود تذكر. وقد قدّر عدد مستخدمي الإنترنت بحوالى المليارين العام 2011.

تنبع أهمية إدخال الإنترنت الى أي بلد من حقيقة أساسية وهي أن شبكة الانترنت تتحدى الحدود والرقابة الحكومية التقليدية على وسائل الإعلام، وتوفر صوتًا بديلاً عن وسائل الإعلام التقليدية، التي تشكّل عادةً الصدى الرئيس للسلطات الرسمية وللمجموعات الضاغطة. بعبارة أخرى، إنه يؤمّن تدفّق المعلومات من دون وجود حدود فعلية، وبالتالي يوفّر فرصًا لا تقدّر بثمن لتحريك الجمهور لعبور الحدود الوطنية، وخصوصًا بين الشباب من خلال إقامة مناطق تلاقٍ غير مكانية (virtual space).

ان استخدام الإنترنت هو أكثر انتشارًا بين الفئات الشبابية في العالم، خصوصًا الشباب ما بين العشرين والثلاثين من العمر. فهؤلاء يستخدمون شبكة الإنترنت على نطاقٍ أوسع مقارنةً ببقية النشطاء. وعلى سبيل المثال فقد شكّل هذا العامل سببًا رئيسًا لتنشيط الشارع العربي من خلال المساعدة على التحرّكات وتنظيم احتجاجات وتعزيز شكل جديد من الصحافة التي توفّر منصة للمواطنين العاديين للتعبير عن آرائهم وعرض الحقائق من وجهة نظرهم. كما سهّل استعمال خدمات مواقع الفيسبوك والتويتر الاجتماعية في الترويج للنشاطات الشبابية المختلفة الأشكال. كذلك، تم إنشاء مواقع جديدة خاصة بالمواطنين على شبكة الإنترنت لتوفير منتديات للنقاش السياسي والإجتماعي. من ناحية أخرى، لا بد من الإشارة الى أن الإنترنت والأقمار الصناعية تعمل بشكلٍ متواصل على بث تحرّكات المواطنين والسلطات العامة وكذلك للعالم بأسره، لذلك لم يعد بالإمكان إخفاء الكثير من الحقائق لفترةٍ طويلة.

ولكن هذا التطوّر الكبير لشبكة الإنترنت لم يكن مصحوبًا بقواعد قانونية واضحة، الأمر الذي أثار عددًا من المخاوف المتعلقة بجرائم الإنترنت، وخصوصيات الافراد، وحدود الرقابة والثغرات العديدة الأخرى. وقد استحوذ الخطر المتزايد للجرائم المرتكبة عن طريق الانترنت على اهتمام جميع الدول. ولا تزال حتى هذا اليوم الجهود المبذولة لمكافحة الجريمة السيبرانية[[4]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%85%D8%B9%D8%A7%D9%87%D8%AF%D8%A7%D8%AA-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A%D8%A9-%D9%84%D9%84%D8%A5%D9%86%D8%AA%D8%B1%D9%86%D8%AA-%D8%AD%D9%82%D8%A7%D8%A6%D9%82-%D9%88%D8%AA%D8%AD%D8%AF%D9%91%D9%8A%D8%A7%D8%AA" \l "_ftn4" \o ") قائمة بشكلٍ جديّ في معظم البلدان. ولكن في الواقع، إن القوانين الوطنية القائمة لا تزال متأخّرة في موضوع تنظيم الشبكة العنكبوتية، إذ أنها لا تغطي مجموعة واسعة من الجرائم عبر الإنترنت ولا تقيم  حدودًا واضحة لما هو مقبول أو مرفوض. هذا النقص في الحماية القانونية يجبر الشركات والحكومات على الإعتماد بشكلٍ فردي على تدابير تقنية محدودة لحماية مصالحها من قراصنة الإنترنت الذين يحاولون الوصول إليها، أو تدمير المعلومات القيّمة الموجودة لدى الشركات او المؤسسات العامة أو الافراد.

هذا التطبيق الضعيف لقوانين مكافحة هذا النوع من الجرائم وخطورة هذه المسألة يتطلب المزيد من التشريعات والتعاون الدولي.

أمام هذا الواقع القانوني الذي يتخطى الحدود الوطنية، حاولت مؤخرًا عدة دول، من خلال عدد من المعاهدات، معالجة هذه التحديات لأنه لا يوجد حتى هذه اللحظة نظام عالمي لمكافحة مساوئ الإنترنت كالرسائل الملغومة (spam) أو الأمور التي تتعلّق بالأخلاق العامة.

في الواقع، لا يمكن معالجة التحديات القانونية والفنية والتنظيمية المتعلّقة بالأمن السيبراني بشكلٍ صحيح إلا من خلال اعتماد استراتيجية على المستوى الدولي يشارك فيها جميع ذوي العلاقة لمعالجة الأمر.

وقد اتخذت مبادرات من قبل العديد من المنظمات منها: الجمعية العامة للأمم المتحدة، الاتحاد الدولي للاتصالات (ITU)، الإنتربول/يوروبول، منظمة التعاون الاقتصادي والتنمية (OECD)، ومنظمات الأمم المتحدة المعنية بمشاكل المخدرات والجريمة (UNODC)، معهد الأمم المتحدة الأقليمي لدراسة شؤون الجريمة والعدالة، معهد بحوث (UNICRI) ومؤسسة الإنترنت للأسماء والأرقام المخصصة (ICANN) والمنظمة الدولية لتوحيد المقاييس (ISO)، واللجنة الكهروتقنية الدولية (IEC) وفرق عمل هندسة الإنترنت وFIRST منتدى الاستجابة للأحداث ومجموعات الأمن لآسيا والمحيط الهادئ، ومنظمة التعاون الإقتصادي للمحيط الهادىء وآسيا (APEC) ومنظمة الدول الأميركية (OAS) ورابطة دول جنوب شرق آسيا (ASEAN) وجامعة الدول العربية، والإتحاد الأفريقي. ومبادرات فردية من جانب دول نامية أوفي طور النمو.

اما المبادرة الأكثر تقدمًا لتنظيم الشبكة العنكبوتية ومحاربة الجرائم الإلكترونية فهي إتفاقية المجلس الأوروبي (European Council) بشأن الجريمة السيبرانية[[5]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%85%D8%B9%D8%A7%D9%87%D8%AF%D8%A7%D8%AA-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A%D8%A9-%D9%84%D9%84%D8%A5%D9%86%D8%AA%D8%B1%D9%86%D8%AA-%D8%AD%D9%82%D8%A7%D8%A6%D9%82-%D9%88%D8%AA%D8%AD%D8%AF%D9%91%D9%8A%D8%A7%D8%AA" \l "_ftn5" \o ")، وقرارات الأمم المتحدة المختلفة لمنع جرائم الكمبيوتر ومكافحتها، وخطة عمل مؤتمر دول الـ G8 (الدول الصناعية الثمانية)، وجهود الإتحاد الدولي للإتصالات بشأن توحيد آليات تطوير الإتصالات السلكية واللاسلكية.

**جرائم الإنترنت**

وفق الاتفاقية الأوروبية بشأن الجريمة السيبرانية التي عقدت في بودابست العام 2001، إن مصطلح «جرائم الإنترنت» يتناول النشاطات غير القانونية أو غير المشروعة المرتبطة بأجهزة الكومبيوتر وباستخدام الشبكة العنكبوتية، مع استثناء استخدام آلة الكمبيوتر كآلة مادية لارتكاب الجريمة، عندها يعتبر الجرم عاديًا.  
وفي المقابل، يعتبر حذف المعلومات بواسطة جهاز الكمبيوتر من دون استخدام الشبكة العنكبوتية مشمولاً بجرائم الإنترنت وفق الاتفاقيات الدولية كاتفاقية المجلس الأوروبي بشأن الجريمة السيبرانية.

**وقد صنّف المجلس الأوروبي جرائم الإنترنت بأربعة أنواع مختلفة هي:**

- الجرائم ضد سلامة المعلومات وخصوصيتها

- الجرائم ذات الصلة بالكمبيوتر

- الجرائم المتعلقة بمحتوى الكمبيوتر

- الجرائم التي تتعلّق بالعلامات التجارية والملكية الفكرية:

**الجرائم ضد سلامة المعلومات وخصوصيتها**

**تشمل هذه الجرائم:**

أ. الدخول غير المشروع (أعمال القرصنة)

ب. التجسس على البيانات والمعلومات

ج. الإعتراض غيرالقانوني

د. التدخل في البيانات والمعلومات

ﻫ. التدخل في أنظمة الكمبيوتر وبرامجه

**الجرائم المتصلة بالكمبيوتر وتشمل:**

أ. الغش والإحتيال ذات الصلة بالكمبيوتر

ب.استخدام الكمبيوتر للتزوير

ج. سرقة الهوية

الجرائم المتصلة بالمحتوى وتشمل:

أ. وجود مضمون جنسي أو إباحي

ب. مواد إباحية ذات علاقة بالأطفال

ج. بيانات التحريض على العنصرية، الكراهية وتمجيد العنف

د. التعرّض للأديان

ﻫ.ألعاب القمار غير المشروعة والألعاب على الإنترنت

و. التشهير والمعلومات الكاذبة

ز. البريد المزعج (spam)

ح. مواد أخرى

**الجرائم ذات الصلة بحقوق الطبع والنشر والعلامات التجارية وتشمل:**

أ. تبادل الأغاني والملفات والبرامج المحمية في حقوق التأليف والنشر من خلال برامج تبادل المعلومات

ب. التحايل على نظم إدارة الحقوق الرقمية

ج. إستخدام العلامات التجارية في أنشطة إجرامية بهدف التضليل

د. الجرائم ذات الصلة بإسم المواقع الإلكترونية

**وبالإضافة إلى ذلك، يتم استخدام بعض المصطلحات لوصف الأعمال الإجرامية التي تقع ضمن فئات عدة كالمذكورة أعلاه، مثل:**

أ. الإرهاب السيبراني

ب. الحرب الإلكترونية

ج. غسل الأموال السيبراني

د. الخداع (philsing)

**التحديات القانونية الوطنية والدولية**

حتى وقتٍ قريب، كان للحكومات مقاربات مختلفة بشأن التشريعات الخاصة بالإنترنت. فمعظم دول العالم تنظّم الإنترنت ضمن حدود قيمها السياسية والقانونية والأخلاقية والثقافية. لكن بما أن تطوّر تكنولوجيا الإتصالات والمعلومات يجري على مستوى دولي خارجًا عن نطاق سيطرة هذه الدول، فإن اعتماد تشريعات فعالة وتنفيذها لمكافحة جرائم الإنترنت يشكّل تحديًا كبيرًا للحكومات. وبالتالي، إن جرائم الإنترنت تمثّل تحديًا كبيرًا للأجهزة القانونية في كلّ من البلدان المتقدمة والنامية، ذلك أن عملية التشريع تستغرق وقتًا طويلاً يمنع مكافحة جرائم المعلوماتية بسرعة.

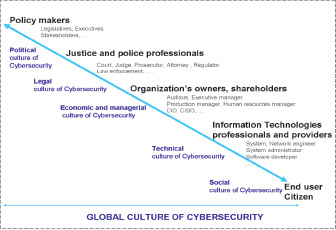
في الواقع، فإن المحاكم الجزائية الوطنية تواجه اليوم صعوبة أساسية وهي الوقت الضائع بين اكتشاف الإنتهاكات للتقنيات الجديدة، وبين تعديل القوانين الجزائية لمكافحتها. فالتعديلات الضرورية للقانون الجزائي الوطني غالبًا ما تكون بطيئة لأنها تتطلب تحقيق الخطوات الآتية:

اكتشاف محتوى المخالفات في التكنولوجيا الجديدة، وإيجاد الثغرات في القانون الجزائي لمعالجتها واعتماد قوانين جديدة تجرِّم التعديات المتعلقة بالكمبيوتر. وما يزيد من التأخير في عملية مكافحة جرائم الإنترنت الحاجة إلى معدات وتقنيات قد لا تكون متوافرة للتحقيق في الأعمال الإجرامية المحتملة.

فالتعامل بالأدلة الرقمية يترافق مع تحديات كبيرة ويتطلّب إجراءات محدّدة للحفاظ على سلامة المعلومات، وتجنّب تعديل الأدلة أو حذفها، أو التعدي على حقوق مستخدمي الإنترنت الأبرياء. ومن بين التحديات الأخرى الأساسية نذكر:

صعوبة كشف الأجهزة والبرامج التي يستخدمها المشتبه بهم، وكشف هوية مستخدمي الإنترنت عن طريق تحليل الرسائل الالكترونية، واستعادة الملفات المحذوفة، وتحديد الأدلة ذات الصلة بالجرائم، وفك تشفير الملفات.

من ناحية أخرى، إن انتشار الإنترنت خارج حدود الدولة يطرح تحديات قانونية تتعلّق بسيادة الدول وصلاحية محاكمها التي تمتد فقط على مساحتها الجغرافية (ضمن حدودها). ولكن بما أن جرائم الإنترنت ظاهرة عالمية جديدة تمتدّ خارج نطاق الحدود الوطنية فإن ذلك يستلزم لنجاح مكافحة تلك الجرائم تنسيقًا (harmonization) كبيرًا بين القوانين الداخلية والمعاهدات الدولية والتعاون بين مختلف البلدان. فمنذ العام 1995، تواجه الحكومات في جميع أنحاء العالم عددًا من المشاكل على شبكة الانترنت كتحميل المواد التي تعتبر غير قانونية ووجود محتوى غير أخلاقي مضر بالشباب، بالإضافة إلى الجرائم الأخرى.



**المصدر: الاتحاد الدولي للاتصالات دليل مكافحة الجريمة الإلكتروني**

**التشريعات الدولية في مجال الانترنت**

يعمل عدد من المنظمات الدولية باستمرار لمواكبة التطورات في شأن أمن الفضاء الإلكتروني وقد أسّست مجموعات عمل لوضع استراتيجيات لمكافحة جرائم الإنترنت. ويستخدم مصطلح «الأمن السيبراني» لتلخيص أنشطة مختلفة كجمع المعلومات ووضع السياسات العامة والتدابير الأمنية، والمبادئ التوجيهية، وطرق إدارة المخاطر، والحماية، والتدريب، ودليل لأفضل الممارسات المهنية، ومختلف التقنيات التي يمكن استخدامها لحماية شبكة الإنترنت. وتشمل هذه السياسات المعلومات وأجهزة الكمبيوتر، والأفراد، والبنية التحتية، وبرامج المعلوماتية، والخدمات، ونظم الاتصالات السلكية واللاسلكية، ومجمل المعلومات المنقولة و/أو المخزنة في الاجهزة الإلكترونية. يهدف الأمن السيبراني جاهدًا لضمان تحقيق سلامة المؤسسات والأفراد في مواجهة المخاطر الأمنية وكل ما يتعلق بشبكة الانترنت[[6]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%85%D8%B9%D8%A7%D9%87%D8%AF%D8%A7%D8%AA-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A%D8%A9-%D9%84%D9%84%D8%A5%D9%86%D8%AA%D8%B1%D9%86%D8%AA-%D8%AD%D9%82%D8%A7%D8%A6%D9%82-%D9%88%D8%AA%D8%AD%D8%AF%D9%91%D9%8A%D8%A7%D8%AA" \l "_ftn6" \o ").

**وأبرز المجموعات والمنظمات الدولية التي عملت في موضوع جرائم شبكة الانترنت نذكر:**

أ.مجموعة الدول الثماني G8

ب. الأمم المتحدة ومنظماتها

ج. الاتحاد الدولي للاتصالات

د. مجلس أوروبا

**أ. مجموعة الدول الثماني: G8**

إعتمد وزراء العدل والداخلية التابعين لبلدان الـ G8 في اجتماعاتهم المختلفة سياسات لمكافحة العديد من جرائم الإنترنت تستند إلى المبادئ التالية: عدم إتاحة ملاذات آمنة للمعتدين على تكنولوجيا المعلومات، التنسيق بين جميع الدول المعنية في ملاحقة مرتكبي جرائم الإنترنت ومحاكمتهم بغض النظر عن مكان حدوث الضرر، تدريب الموظّفين المكلفين تنفيذ القوانين، وتجهيزهم بالمعدات الضرورية للتعامل مع الجرائم ذات التقنية العالية.

بالإضافة الى ذلك، دعت دول الـ G8 إلى مواصلة العمل حتى التوصّل إلى حلول دولية ناجحة، من خلال عقد إتفاقات دولية، لمعالجة الجريمة ذات التقنية العالية والاستفادة من عمل المنظمات الدولية المختلفة ومن تثمير الدراسات العديدة التي وضعتها دول الـ G8 ومن بينها: مبادىء وخطة العمل بشأن الجريمة ذات التكنولوجيا العالية وجرائم الكمبيوتر (1997) ومبادئ بشأن الحصول على المعلومات المخزّنة على الكمبيوتر خارج حدود الدول (1999) وتوصيات لتعقّب الاتصالات على الشبكة خارج الحدود الوطنية في التحقيقات الإرهابية والإجرامية (2002) ومبادئ توافر البيانات الأساسية لحماية السلامة العامة (2002) وإعلان بيان دول G8 على نظم حماية المعلومات (2002).

وترى دول الـ G8 أن الحماية الفعالة ضد الجرائم ذات التقنية العالية تتطلّب الاتصال والتنسيق والتعاون داخليًا ودوليًا بين جميع أصحاب المصلحة في القطاع الخاص والأوساط الأكاديمية، والمؤسسات الحكومية. بناءً على ذلك، فإن دول الـ G8 إلتزمت تدريب جميع العاملين في مجال تطبيق القانون وتجهيزهم بالمعدات الضرورية لمكافحة جرائم الإنترنت. كما تعهّدت بمساعدة جميع البلدان الأعضاء على إقامة مراكز إتصال تعمل على مدار 24 ساعة سبعة أيام في الأسبوع. إن وجود جرائم تعتمد التكنولوجيا المتقدّمة تطرح تحديات كبيرة على الأجهزة القضائية. فغالبًا ما يكون من الصعب على المحققين ذات المهارة العالية العمل بسرعة فائقة لحماية البيانات الالكترونية وتحديد المتهمين بخرق القانون. من هنا أهمية الشبكة التي طرحت دول الـ G8 إنشاءها لأنها ستمكّن من الاستجابة بسرعة كبيرة لطلبات السلطات الرسمية أو مستخدمي شبكات الانترنت.

**إن توصيات الـ G8 بالنسبة لجرائم التكنولوجيا المتقدمة والجرائم ذات الصلة بالكمبيوتر موجودة في إطار الباب D من المعاهدة وتتلخص بما يلي:**

- يتعيّن على الدول أن تُجرِّم الانتهاكات على حقوق الغير الشبكة العنكبوتية التي تستوجب العقوبات الجزائية وأن تعالج المشاكل المتعلقة بالتحقيقات القضائية بالتدريب الفعال لمنع الجريمة، وإقامة تعاون دولي في ما يتعلّق بمكافحة هذه الانتهاكات.

- ينبغي للدول أن تتخذ خطوات رادعة لمنع الجريمة ذات التقنية العالية، ويشمل ذلك:

• التعاون مع القطاع الصناعي لضمان أمن شبكات الكمبيوتر ونظم الاتصالات، وإيجاد الآليات المناسبة عند تعرّض المواقع الالكترونية للهجمات.

• سن قوانين وتدابير أخرى وتنفيذها لضمان حماية ملائمة لحقوق الملكية الفكرية ضد التزوير والقرصنة.

• تحديد المشاكل المحتملة ومعالجتها في المستقبل التي قد تنتج عن التطورات في مجال تكنولوجيا المعلومات.

• نشر الوعي العام في ما يتعلق بموضوع الجريمة ذات التقنية العالية.

- يتوجب على الدول العمل المستمر على اقتناء التكنولوجيات الملائمة والتطوير المستمر للخبرات والقدرات في مجال التحقيق والادعاء العام، من أجل ملاحقة المجرمين الذين يستخدمون تكنولوجيا الكمبيوتر لارتكاب جرائمهم. ويتوجّب على الدول تشجيع قيام المزيد من الأبحاث من أجل زيادة فعالية تقنيات تطبيق القانون.

- ينبغي تحسين التواصل بين الموظفين المكلّفين تطبيق القوانين في مختلف الدول، بما في ذلك تبادل الخبرات في معالجة هذه المشاكل.

- يتوجب على الدول الحفاظ على التوازن المناسب بين حماية الحق في الخصوصية، ولا سيما بالنظر إلى الخطر الذي تخلقه التكنولوجيات المستجدة، والحفاظ على قدرة تطبيق القانون لحماية السلامة العامة والقيم الاجتماعية الأخرى.

- على الدول تشجيع وضع القوانين وتنفيذ تدابير لتوفير حماية فعالة للأطفال من جميع أشكال الاستغلال الجنسي على الإنترنت.

- على الدول أن تتعاون من أجل التطوير المستمر للموارد والتقنيات والتدريب للمساعدة في تطبيق القانون ومكافحة الاستغلال الجنسي للأطفال عبر الإنترنت. كما ينبغي العمل مع مقدمي خدمة الإنترنت والمنظمات غير الحكومية لتطوير الطرق التي يمكن أن تساعد هذه المنظمات من أجل تطبيق قوانين مكافحة الاستغلال الجنسي للأطفال على شبكة الإنترنت.

وأخيرًا، على الدول أن تشجّع التعاون في مجال تطوير الاستراتيجيات المناسبة لرفع الوعي العام في هذا الشأن، وكذلك التقييم المستمر لبرامج المكافحة والوسائل القانونية المتبعة[[7]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%85%D8%B9%D8%A7%D9%87%D8%AF%D8%A7%D8%AA-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A%D8%A9-%D9%84%D9%84%D8%A5%D9%86%D8%AA%D8%B1%D9%86%D8%AA-%D8%AD%D9%82%D8%A7%D8%A6%D9%82-%D9%88%D8%AA%D8%AD%D8%AF%D9%91%D9%8A%D8%A7%D8%AA" \l "_ftn7" \o ").

**ب. قرارات الجمعية العامة للأمم المتحدة**

تعمل الأمم المتحدة منذ فترة طويلة في مجال تأمين سلامة استخدام التكنولوجيا وشبكات المعلوماتية (الانترنت). وتشارك وكالات الأمم المتحدة المختلفة في مختلف المفاوضات لإيجاد توافق في الآراء بشأن عدد من القضايا، بما في ذلك وضع معايير توفير الحماية لشبكات الانترنت. أما أبرز قرارات الجمعية العامة للامم المتحدة في هذا المجال فهي:

- القرار 45/121 العام 1990، وكذلك نشر دليل منع الجرائم المتصلة بأجهزة الكمبيوتر ومكافحتها في العام 1994.

- القرارات 53/70 في 4 كانون الأول/ديسمبر 1998، و54/49 في 1 كانون الاول/ديسمبر 1999، 55/28 في 20 تشرين الثاني/نوفمبر 2000 و56/19 في 29 تشرين الثاني/نوفمبر 2001 و57/53 في 22 تشرين الثاني/نوفمبر 2002 و58/32  في 18 كانون الأول/ديسمبر 2003 حول موضوع «التطورات في ميدان المعلومات والاتصالات في سياق الأمن الدولي».

- القرارات 55/63 في 4 كانون الأول/ديسمبر 2000، و56/121 في 19 كانون الأول/ديسمبر 2001 بشأن «مكافحة استخدام نظم المعلومات الإدارية الجنائية لتقنية المعلومات». يدعو هذا القرار الدول الأعضاء، عند وضع التشريعات الوطنية لمكافحة إساءة استعمال تكنولوجيا المعلومات، على أن تأخذ بالاعتبار عمل لجنة منع الجريمة والعدالة الجنائية.

- القرار 57/239 في 20 كانون الاول/ديسمبر 2002 بشأن «إنشاء ثقافة عالمية للأمن السيبراني».

- قرارات الجمعية العامة 57/239 في 31 كانون الثاني/يناير 2003 و58/199 في 30 كانون الثاني/يناير 2004 بشأن «إنشاء ثقافة عالمية للأمن السيبراني»، والذي يدعو الدول الأعضاء إلى التعاون وتعزيز ثقافة الأمن السيبراني.

من ناحية أخرى، هناك العديد من القرارات الصادرة عن منظمة الأمم المتحدة في مجموعة من المجالات ذات الصلة بأمن الفضاء الإلكتروني مثل:

• القرار CCPCJ 16/2/2007 من نيسان/أبريل 2007 «المنع الفعال للجريمة والعدالة الجنائية لمكافحة الاستغلال الجنسي للأطفال» (الفقرات 7، 16).

• قرار المجلس الاقتصادي والاجتماعي E/2007/20 بتاريخ 26 تموز/يوليو 2007 بعنوان «التعاون الدولي من أجل منع وتحري ومقاضاة ومعاقبة جرائم الاحتيال الاقتصادي والجرائم المتصلة بالهوية» (E/2007/30 وE/2007/SR.45).

• قرار المجلس الاقتصادي والاجتماعي 2004/26 بتاريخ 21 تموز/يوليو 2004 بعنوان «التعاون الدولي لمنع التحقيق والمقاضاة والمعاقبة على الاحتيال، وإساءة استعمال الهوية وتزييفها والجرائم ذات الصلة».

• الفقرة 18 من «إعلان فيينا بشأن الجريمة والعدالة: مواجهة تحديات القرن الحادي والعشرين»، التي أقرتها الجمعية العامة في القرار 55/59 المؤرخ 4 كانون الاول/ديسمبر 2000 والفقرة 36 المرفقة بقرار الجمعية العامة 56/261 المؤرخ 31 كانون الثاني/يناير 2002 حول: «خطط العمل لتنفيذ إعلان فيينا بشأن الجريمة والعدالة: مواجهة تحديات القرن الحادي والعشرين».

• الفقرتان 15 و16 من إعلان بانكوك بشأن «أوجه التآزر والتعاون: التحالفات الاستراتيجية في مجال منع الجريمة وتحقيق العدالة الجنائية»، الذي أقرّه قرار الجمعية العامة 60/177 بتاريخ 16 كانون الاول/ديسمبر2005.

• توصيات مؤتمر ورشة العمل على «التدابير الرامية إلى مكافحة الجريمة المتصلة بأجهزة الكمبيوتر»، الذي عقد في بانكوك في 22 نيسان/أبريل 2005 كجزء من مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية. الفقرة 2 من قرار الجمعية العامة 60/177 التي دعت الحكومات لتنفيذ جميع التوصيات التي اعتمدها المؤتمر الحادي عشر.

• قرار لجنة مكافحة المخدرات 48/5 حول «تعزيز التعاون الدولي من أجل منع استخدام شبكة الإنترنت لارتكاب الجرائم المتصلة بالمخدرات».

• الفقرة 17 من قرار الجمعية العامة 60/178 المؤرخ 16 كانون الاول/ديسمبر 2005 بخصوص «التعاون الدولي لمكافحة مشكلة المخدرات العالمية».

• قرار لجنة مكافحة المخدرات 43/8 في 15 آذار/مارس 2000 عبر الإنترنت.

• قرار المجلس الاقتصادي والاجتماعي 2004/42 بشأن «بيع المخدرات المشروعة الخاضعة للمراقبة الدولية إلى الأفراد عن طريق الإنترنت».

• مختلف توصيات الهيئات الفرعية التابعة للجنة مكافحة المخدرات واللجنة الفرعية المعنية بالاتجار غير المشروع بالمخدرات والمسائل المتعلقة بالشرقين الأدنى والأوسط.

• التوصيات والمبادئ التوجيهية للهيئة الدولية لمراقبة المخدرات (INCB) التي نشرت العام 2005 وتوصيات للحد من انتشار المبيعات غير المشروعة من المواد الخاضعة للرقابة ولا سيما المستحضرات الصيدلانية، عبر الإنترنت.

تدعو الجمعية العامة في قراراتها المختلفة - التي غالبًا ما تكون مماثلة لقرارات الاتحاد الدولي للاتصالات - الدول الأعضاء، عند وضع القوانين الوطنية والسياسات العامة لمكافحة إساءة استعمال تكنولوجيا المعلومات، وأن تأخذ في الاعتبار أعمال لجنة منع الجريمة ولجنة العدالة الجنائية وغيرها من المنظمات الدولية والإقليمية.

**ج. الاتحاد الدولي للاتصالات**

يوفّر الاتحاد الدولي للاتصالات الذي يضم 192 دولة و700 شركة من القطاع الخاص والمؤسسات الأكاديمية منبرًا «استراتيجيا» للتعاون بين أعضائه باعتباره وكالة متخصصة داخل الأمم المتحدة. ويعمل الاتحاد على مساعدة الحكومات في الاتفاق على مبادئ مشتركة تفيد الحكومات والصناعات التي تعتمد على تكنولوجيا المعلومات والبنية التحتية للاتصالات. وقد وضع الاتحاد الدولي للاتصالات مخططًا «لتعزيز الأمن السيبراني العالمي يتكوّن من سبعة أهداف رئيسة، والأهداف السبعة هي:

- وضع استراتيجيات لتطوير نموذج التشريعات السيبرانية يكون قابلاً للتطبيق محليًا وعالميًا بالتوازي مع التدابير القانونية الوطنية والدولية المعتمدة.

- وضع استراتيجيات لتهيئة الأرضية الوطنية والإقليمية المناسبة لوضع الهيكليات التنظيمية والسياسات المتعلّقة بجرائم الانترنت.

- وضع استراتيجية لتحديد الحد الأدنى المقبول عالميًا في موضوع معايير الأمن ونظم تطبيقات البرامج والأنظمة.

- وضع استراتيجيات لوضع آلية عالمية للمراقبة والإنذار والرد المبكر مع ضمان قيام التنسيق عبر الحدود.

- وضع استراتيجيات لإنشاء نظام هوية رقمي عالمي وتطبيقه، وتحديد الهيكليات التنظيمية اللازمة لضمان الاعتراف بالوثائق الرقمية للأفراد عبر الحدود الجغرافية.

- تطوير استراتيجية عالمية لتسهيل بناء القدرات البشرية والمؤسسية لتعزيز المعرفة والدراية في مختلف القطاعات وفي جميع المجالات المعلوماتية.

- تقديم المشورة بشأن إمكانية اعتماد إطار استراتيجي عالمي لأصحاب المصلحة من أجل التعاون الدولي والحوار والتعاون والتنسيق في جميع المجالات التي سبق ذكرها[[8]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%85%D8%B9%D8%A7%D9%87%D8%AF%D8%A7%D8%AA-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A%D8%A9-%D9%84%D9%84%D8%A5%D9%86%D8%AA%D8%B1%D9%86%D8%AA-%D8%AD%D9%82%D8%A7%D8%A6%D9%82-%D9%88%D8%AA%D8%AD%D8%AF%D9%91%D9%8A%D8%A7%D8%AA" \l "_ftn8" \o ").

**د. إتفاقية المجلس الأوروبي بشأن جرائم الإنترنت**

إعتمد المجلس الأوروبي الطابع الدولي لجرائم الكمبيوتر منذ العام 1976. وفي العام 1996، أنشأت اللجنة الأوروبية لمشاكل الجريمة (CDPC) لجنة خبراء للتعامل مع مشكلة الجريمة السيبرانية. عملت اللجنة بين العامين 1997 و2000 على مشروع الاتفاقية التي اعتمدها البرلمان الأوروبي في الجزء الثاني من جلسته العامة في شهر نيسان/أبريل 2001. وتم التصديق على الاتفاقية من قبل 30 دولة بحلول العام 2010.

إن إتفاقية جرائم الانترنت هي المعاهدة الدولية الأولى التي تسعى لمعالجة الجرائم المتعلقة بالكمبيوتر والإنترنت عبر التنسيق بين القوانين الوطنية وقوانين الدول الأخرى.

تهدف الاتفاقية إلى:

- توحيد عناصر القانون الجزائي المحلي مع الأحكام المتعلقة بالجرائم الإلكترونية.

- توفير الاجراءات القانونية اللازمة للتحري وملاحقة الجرائم المرتكبة الكترونيًا بواسطة الكمبيوتر.

- تعيين نظام سريع وفعال للتعاون الدولي.

- الحفاظ بشكل سريع على البيانات المخزّنة على أجهزة الكمبيوتر وحفظها والإفصاح الجزئي عن حركة هذه البيانات المخزنة على الكمبيوتر.

- جمع معلومات عن حركة البيانات وعن إمكان وجود تدخّل في محتواها.

- تتضمن أيضًا الاتفاقية المبادئ العامة المتعلّقة بالتعاون الدولي في المواضيع التالية: تسليم المجرمين، المساعدة الدولية المتبادلة، إعطاء المعلومات بصورة آلية، وإنشاء الولاية القضائية على أي جريمة.

- المساعدة المتبادلة في جمع حركة المعلومات واعتراضها.

- الإجراءات المتعلقة بطلبات المساعدة المتبادلة في غياب الاتفاقات الدولية.

**لبنان والجريمة السيبرانية**

لم يصادق لبنان على الاتفاقية المتعلقة بجرائم المعلوماتية الالكترونية حتى اليوم. فهذا الموضوع لا يزال معلّقًا منذ العام 2005. وعلى الرغم من تزايد جرائم الإنترنت التي تؤثّر على لبنان بشكلٍ كبير فإن القوانين الحالية المطبّقة تستنتد إلى نصوصٍ تقليدية من قانون العقوبات وهي ليست مناسبة للجرائم المتعلّقة بالإنترنت.

ولكن يجدر بالاشارة أن لدى لبنان قسمًا خاصًا بجرائم الإنترنت تابعًا لقوى الأمن الداخلي يتعقّب عناوين المجرمين من خلال استخدام أدوات متقدمة للعثورعلى أدلّة رقمية متصلة بجرائم شبكة الانترنت، ولكن هناك حاجة مستمرّة الى تطوير هذه التقنيات. بالإضافة إلى ذلك فإن لبنان هو عضو في شبكة الانتربول، ويسعى حاليًا إلى الانضمام إلى شبكة دول الـ G8.

**الخلاصة: الإنترنت حق من حقوق الإنسان**

أصبحت شبكة الإنترنت تشكّل قوة إجتماعية وإقتصادية وسياسية مؤثّرة في العالم الحديث. وبالمقابل، إن التحديات القانونية الناتجة عن شبكة الانترنت قد كثرت وازدادت بحيث أصبحت الجرائم السيبرانية من الجرائم الكبرى في القرن الـ 21. وإن أحدث تقرير صدر عن الأمم المتحدة حول شبكة الإنترنت في3 حزيران/يونيو 2011. إعتبر أن الحصول على خدمة الإنترنت حق من حقوق الإنسان الأساسية.

ويذكر التقرير أن شبكة الإنترنت هي واحدة من أقوى أدوات القرن التي تمكّن من زيادة الشفافية ومن سرعة الحصول على المعلومات، وتسهيل مشاركة المواطنين في بناء مجتمع ديموقراطي. واستنادًا إلى وقائع من المظاهرات الأخيرة في جميع بلدان الشرق الأوسط وشمال أفريقيا، أدّت شبكة الإنترنت دورًا رئيسًا في تعبئة السكان للدعوة للتظاهر من أجل العدالة والمساواة والمساءلة واحترام أفضل لحقوق الإنسان. ويدعو التقرير جميع الدول إلى تجنّب اعتماد القوانين التي تحظّر الدخول إلى شبكة الإنترنت بحجج زائفة كالحاجة إلى حماية خصوصية الأفراد، والأمن القومي أو مكافحة الإرهاب.

ويدعو التقرير أيضًا الدول إلى تبني سياسات فعالة وملموسة والاستراتيجيات التي يجب أن توضع بالتعاون مع الأفراد من جميع شرائح المجتمع، لجعل الإنترنت متاحة على نطاق واسع وميسرة وبأسعار معقولة للجميع. ويضيف التقرير: «وبالنظر إلى أن الإنترنت أصبحت أداة لا غنى عنها لتحقيق عدد من مبادىء حقوق الإنسان، ومكافحة عدم المساواة، وتسريع التنمية والتقدم الإنساني، ينبغي ضمان حصول الجميع على خدمة شبكة الإنترنت وأن يكون من أولويات جميع الدول»[[9]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%85%D8%B9%D8%A7%D9%87%D8%AF%D8%A7%D8%AA-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A%D8%A9-%D9%84%D9%84%D8%A5%D9%86%D8%AA%D8%B1%D9%86%D8%AA-%D8%AD%D9%82%D8%A7%D8%A6%D9%82-%D9%88%D8%AA%D8%AD%D8%AF%D9%91%D9%8A%D8%A7%D8%AA" \l "_ftn9" \o ").

وفي النهاية، على الرغم من التقدم الكبير في العديد من البلدان لمحاكمة الجرائم المتعلقة بالإنترنت، إن غالبية البلدان لا تزال تعوّل على القوانين القديمة التي سبقت ولادة شبكة الانترنت. ولكن لكي تكون هذه الدول قادرة على محاربة جرائم الإنترنت يجب أن تقوم بما يلي:

- تحديث دوري للقوانين لتتلاءم مع التكنولوجيات الجديدة. على سبيل المثال، إن القوانين التي تنظم عمليات مزودي خدمات الإنترنت تحتاج إلى تحديث بشكل منتظم.

- التعاون فيما بينها لاعتماد معيار موحّد لمكافحة جرائم الفضاء الالكتروني لمنع المجرمين من استغلال البلدان التي لديها قوانين أقل صرامة لأنهم يميلون إلى ارتكاب الجرائم الإلكترونية في البلدان ذات القوانين الأقل تشددًا، حيث يجد المجرم أنه من الأسهل ارتكاب الجرائم الإلكترونية في هذه البلدان.

- توظيف محققين ذات معرفة تقنية عالية ومواكبة أحدث التقنيات في هذا المجال. وينبغي إنشاء مختبرات الطب الشرعي على الكمبيوتر لجمع الأدلة الرقمية من أجهزة الحاسوب وتوفير التدريب للمحققين.

- توظيف الخبراء وتدريبهم لمواكبة أحدث التطورات التكنولوجية وفهمها وتطويرالقوانين الوطنية وفق ذلك.

- إعتماد نظام عقوبات صارم على الجرائم التي يمكن أن يكون لها تأثير كبير على المجتمع.

- إشراك القطاع الخاص في مكافحة جرائم الإنترنت لأنها ضرورية لمساعدة السلطات العامة من خلال تحسين الحماية الذاتية كخط دفاع أول لهذا القطاع، واعتماد الحلول التقنية المتقدمة والخطوات الإدارية الضرورية لحماية أمن المعلومات.

- التطوير المستمر للتعاون بين الدول، ولاسيما أنه لا يوجد إجماع بين هذه الدول بشأن تعريف جرائم المعلوماتية وتحديدها بصورة دقيقة. إن عدم تعريف هذه الجرائم بطريقة موحدة سوف يعقد الجهود المبذولة من قبل المكلفين بتطبيق القانون لمكافحة الجريمة السيبرانية.

- تزويد البلدان النامية الموارد والتقنيات اللازمة لمعالجة جرائم الإنترنت ومكافحتها.

- إعتماد القانون النموذجي المتعلق بجرائم الإنترنت وخصوصًا بالنسبة لبلدان العالم الثالث من خلال إشراك القطاعين العام والخاص في هذا الأمر والشروع إلى اعتماد استراتجيات تساعد في القضاء على الخطر المحتمل من جرائم الانترنت.

ختامًا لا يمكن معالجة موضوع الشبكة العنكبوتية إلا من خلال تعاون دولي وثيق لأن هذه الجرائم المرتكبة على هذه الشبكة تتخطّى حدود البلدان ومن جهة أخرى هنالك صعوبة بتحديد مفهوم هذه الجرائم لأن لكل دولة مفاهيم خاصة بها تنبع من قيمها وتقاليدها الخاصة. إن الاتفاقيات الدولية الحالية في هذا المجال ما زالت في مراحلها الأولى وينبغي تطويرها للحفاظ على أمن المجتمعات والأوطان وعلى الديمقراطية وحقوق الانسان.

**المراجع**

1.   Arthur, C. (2011). Guardian.co.uk. available at: http://www.guardian.co.uk

2.   Posetti, J. (2011). Twitter. Available at: http://twitter.com

3.   Tinker, T., Mc Laughlin, G., & Dumlao, M. (2009-2010), «**Crisis Communication and Response**», Retrieved April 4, 2011, from Disaster Resource Guide:, available at: http://www.disaster-resource.com

4.   Council of Europe Organized Crime Report 2004 available at: http://www.coe.int

5.   ITU WTSA Resolution 50: Cybersecurity (Rev. Johannesburg, 2008) available at: http://www.itu.int

   - ITU, ICT Applications and Cybersecurity Background Note to the 2009 Pacific ICT Ministerial Forum held in Tonga 17-20 February2009. available at: http://www.itu.int

6.   United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: http://www.unctad.org

7.   O'Connell, Cyber-Crime hits $ 100 Billion in 2007, ITU News related to ITU Corporate Strategy, 17.10.2007, available at: http://www.ibls.com

8.   Schjolberg and Hubbard, «**Harmonizing National Legal Approaches on Cybercrime**», 2005, page 5. available at: http://www.itu.int

9.   Simon and Slay, «**Voice over IP: Forensic Computing Implications**», 2006, available at: http://scissec.scis.ecu.edu.au

10. Sofaer and Goodman, «**The Transnational Dimension of Cyber Crime and Terrorism**», 2001, page 14, available at: http://media.hoover.org

11. The 2002 OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. available at: http://www.oecd.org

12. WSIS Geneva Plan of Action, 2003, available at: http://www.itu.int/

13. WSIS Tunis Agenda for the Information Society, 2005, available at: http://www.itu.int

14. ITU Global Cybersecurity Agenda, High-Level Experts Group, Global Strategic Report, 2008..

15. UN report on the Internet, available at: http://documents.latimes.com//

[[1]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%85%D8%B9%D8%A7%D9%87%D8%AF%D8%A7%D8%AA-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A%D8%A9-%D9%84%D9%84%D8%A5%D9%86%D8%AA%D8%B1%D9%86%D8%AA-%D8%AD%D9%82%D8%A7%D8%A6%D9%82-%D9%88%D8%AA%D8%AD%D8%AF%D9%91%D9%8A%D8%A7%D8%AA" \l "_ftnref1" \o ")-    Protocol Address Space

[[2]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%85%D8%B9%D8%A7%D9%87%D8%AF%D8%A7%D8%AA-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A%D8%A9-%D9%84%D9%84%D8%A5%D9%86%D8%AA%D8%B1%D9%86%D8%AA-%D8%AD%D9%82%D8%A7%D8%A6%D9%82-%D9%88%D8%AA%D8%AD%D8%AF%D9%91%D9%8A%D8%A7%D8%AA" \l "_ftnref2" \o ")-    Assigned Names and Numbers

[[3]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%85%D8%B9%D8%A7%D9%87%D8%AF%D8%A7%D8%AA-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A%D8%A9-%D9%84%D9%84%D8%A5%D9%86%D8%AA%D8%B1%D9%86%D8%AA-%D8%AD%D9%82%D8%A7%D8%A6%D9%82-%D9%88%D8%AA%D8%AD%D8%AF%D9%91%D9%8A%D8%A7%D8%AA" \l "_ftnref3" \o ")-    The Internet Corporation for Assigned Names

[[4]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%85%D8%B9%D8%A7%D9%87%D8%AF%D8%A7%D8%AA-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A%D8%A9-%D9%84%D9%84%D8%A5%D9%86%D8%AA%D8%B1%D9%86%D8%AA-%D8%AD%D9%82%D8%A7%D8%A6%D9%82-%D9%88%D8%AA%D8%AD%D8%AF%D9%91%D9%8A%D8%A7%D8%AA" \l "_ftnref4" \o ")-     لكلمة الجرائم على الشبكة العنكبوتية التعبير الرسمي باللغة العربية Cybercrime

[[5]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%85%D8%B9%D8%A7%D9%87%D8%AF%D8%A7%D8%AA-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A%D8%A9-%D9%84%D9%84%D8%A5%D9%86%D8%AA%D8%B1%D9%86%D8%AA-%D8%AD%D9%82%D8%A7%D8%A6%D9%82-%D9%88%D8%AA%D8%AD%D8%AF%D9%91%D9%8A%D8%A7%D8%AA" \l "_ftnref5" \o ")-    The European Cybercrime Council Convention

[[6]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%85%D8%B9%D8%A7%D9%87%D8%AF%D8%A7%D8%AA-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A%D8%A9-%D9%84%D9%84%D8%A5%D9%86%D8%AA%D8%B1%D9%86%D8%AA-%D8%AD%D9%82%D8%A7%D8%A6%D9%82-%D9%88%D8%AA%D8%AD%D8%AF%D9%91%D9%8A%D8%A7%D8%AA" \l "_ftnref6" \o ")-    ITU: Understanding Cyber Crime : A guide for developing countries, draft, April 2009,cybmai@itu.int

تمت الزيارة في 23 حزيران 2012

[[7]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%85%D8%B9%D8%A7%D9%87%D8%AF%D8%A7%D8%AA-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A%D8%A9-%D9%84%D9%84%D8%A5%D9%86%D8%AA%D8%B1%D9%86%D8%AA-%D8%AD%D9%82%D8%A7%D8%A6%D9%82-%D9%88%D8%AA%D8%AD%D8%AF%D9%91%D9%8A%D8%A7%D8%AA" \l "_ftnref7" \o ")-    G8 recommandations on transnational crimes, 2011¡ www.Canadainternationalgc.ca/G8/  (تمت الزيارة في 23 حزيران 2012)

[[8]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%85%D8%B9%D8%A7%D9%87%D8%AF%D8%A7%D8%AA-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A%D8%A9-%D9%84%D9%84%D8%A5%D9%86%D8%AA%D8%B1%D9%86%D8%AA-%D8%AD%D9%82%D8%A7%D8%A6%D9%82-%D9%88%D8%AA%D8%AD%D8%AF%D9%91%D9%8A%D8%A7%D8%AA" \l "_ftnref8" \o ")-    ITU Global Cybersecurity Agenda, High-Level Experts Group, Global Strategic Report,[.](http://www.itu.int/osg/csd/cybersecurity/gca/global-strategic-report/index.html.%C3%8A%C3%A3%C3%8A)  ( تمت الزيارة في 23 ايلول/سبتمبر 2012)

[[9]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%85%D8%B9%D8%A7%D9%87%D8%AF%D8%A7%D8%AA-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A%D8%A9-%D9%84%D9%84%D8%A5%D9%86%D8%AA%D8%B1%D9%86%D8%AA-%D8%AD%D9%82%D8%A7%D8%A6%D9%82-%D9%88%D8%AA%D8%AD%D8%AF%D9%91%D9%8A%D8%A7%D8%AA" \l "_ftnref9" \o ")-    UN report on the Internet, available at: http://documents.latimes.com/un-report-internet-rights/

**Internet related International treaties Facts and Challenges**

The communication revolution constitutes one of the major results of globalization especially with regard to the communication’s great and unprecedented speed and instantaneous aspect.  
The ongoing technological development of communication systems has directly affected nations on the political, cultural and social levels.  
It is crucial to tackle the issue of laws governing the internet and their impact over societies since the internet’s infiltration into State borders makes it impossible to organize or control this web especially with the absence of close international cooperation. The Web has many advantages in terms of spreading knowledge and the principles of freedom to the extent that it is widely said that «If you wish to free any society give it internet access». However, the Internet also has inconveniences mainly its use for terrorist acts and for violating individual privacy and ruining the values of human societies. Therefore, a number of international treaties attempted to set up a broad legal framework to handle these challenges.

**Les conventions internationales de l’Internet: vérités et défis**

La révolution au niveau des télécommunications est le principal résultat de la mondialisation, surtout du côté des communications instantanées et leur grande rapidité sans précédent dans l’histoire de l’humanité. Le développement technologique au niveau des systèmes de communication a influencé directement les nations, aux niveaux politique, culturel et social. Il est très important de traiter l’affaire des lois qui contrôlent le réseau de l’Internet et son influence sur les sociétés car l’invasion du réseau de l’Internet des frontières des états rend impossible le fait de son organisation et de son contrôle, surtout sans coopération internationale étroite. Le réseau a de grands avantages au niveau de la diffusion de la connaissance et les principes de la liberté jusqu’au point de dire que «si on veut libérer une société, accorder-lui un accès sur Internet». Or l’Internet a des précautions, notamment son emploi lors des actes terroristes et la violation de l’intimité des individus et détruire les valeurs des sociétés humaines. C’est alors qu’un certain nombre de conventions internationales ont essayé de former un cadre large pour traiter tous ces défis.

- See more at: https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%85%D8%B9%D8%A7%D9%87%D8%AF%D8%A7%D8%AA-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A%D8%A9-%D9%84%D9%84%D8%A5%D9%86%D8%AA%D8%B1%D9%86%D8%AA-%D8%AD%D9%82%D8%A7%D8%A6%D9%82-%D9%88%D8%AA%D8%AD%D8%AF%D9%91%D9%8A%D8%A7%D8%AA#sthash.pWE40Ezt.dpuf