الأمم المتحدة
الاسكوا
ESCWA

الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية

توصيات سياساتية

اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا)

الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية: توصيات سياساتية

الأمم المتحدة

Distr.
LIMITED

E/ESCWA/TDD/2015/1
9 February 2015
ORIGINAL: ARABIC

اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا)

الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية: توصيات سياساتية

الأمم المتحدة
نيويورك، 2015

15-00097

كلمة شكر

قام فريق عمل قسم الابتكار في إدارة التكنولوجيا من أجل التنمية في الإسكوا بتصميم وتنسيق إعداد هذه الدراسة ومراجعتها، وذلك بإدارة وإشراف السيدة نبال إدلبي، رئيسة قسم الابتكار، ومشاركة كل من السيدة هانيا صبيدين الديماسي، مساعدة أبحاث، والسيدة ليز دينر، مسؤولة معاونة لتكنولوجيا المعلومات.

لقد استندت الدراسة إلى تقرير متخصص أعده السيد وسيم حجار، وهو قاضي وخبير في مجال المعلوماتية القانونية وقانون المعلوماتية ومجاز في هندسة الكمبيوتر. وقام السيد عماد الصابوني، وزير الاتصالات والتقانة سابقاً في الجمهورية العربية السورية والخبير في مجال سياسات واستراتيجيات تكنولوجيا المعلومات والاتصالات، بمراجعة موضوعية علمية لهذه الدراسة.

وقد قامت الإسكوا بمراجعة أقران لهذه الدراسة شارك فيها عدد من خبراء الإسكوا، بالإضافة إلى كل من السيد يوسف نصير، الخبير في سياسات واستراتيجيات مجتمع المعلومات، والسيدة جنان الخوري رئيسة القسم الحقوي في مركز المعلوماتية القانونية في الجامعة اللبنانية.

تم إعداد هذه الدراسة في إطار الجهد المتواصل لإدارة التكنولوجيا من أجل التنمية في الإسكوا، التي يديرها السيد حيدر فريحات، من أجل تطوير مجتمع المعلومات في المنطقة العربية. وقد تم تصميم هذه الدراسة بحيث تكون استكمالاً لجهود الإسكوا في مجال تطوير وتنسيق التشريعات السيبرانية لبناء مجتمع المعرفة في المنطقة العربية، وهي تركز على الإطار التنظيمي والإجرائي للحد من الجرائم السيبرانية وضمان الأمان في الفضاء السيبراني.

وتشكر الإسكوا الدول الأعضاء لتعاونهم مع الإسكوا في استكمال بيانات الاستبيان الخاص بهذه الدراسة.

وترحب الإسكوا بملاحظات وتعليقات القراء عبر البريد الإلكتروني: escwa-tdd@un.org.

المحتويات

المحتويات

الصفحة

قائمة الجداول

قائمة الأشكال

قائمة الأطر

المرفقات

موجز تنفيذي

أضحت تكنولوجيا المعلومات والاتصالات أداةً أساسية في الحياة اليومية، وشاملة لأغلب القطاعات والأنشطة الاقتصادية إضافة إلى فعاليتها في التنمية الاقتصادية والاجتماعية. وقد ساعد التطور التكنولوجي، كانتشار الإنترنت والأجهزة النقالة، وكذلك توافر الحزمة العريضة للإنترنت عبر الأجهزة النقالة وتدني كلفتها، إلى ارتفاع أعداد مستخدمي الإنترنت. وقد وصلت نسبة النفاذ إلى الإنترنت في المنطقة العربية إلى 40 في المائة عام 2014، ونسبة اشتراكات الحزمة العريضة للإنترنت عبر الأجهزة النقالة في المنطقة إلى 24 اشتراك لكل مئة مواطن مقارنة بـ 32 على مستوى العالم[1]. إلا أن الانفتاح الذي يميز شبكة الإنترنت، والفضاء السيبراني عموماً، جعله عرضة للتعديات والانتهاكات والأنشطة الإجرامية والتعدي على حقوق الناس، وجعل من مستخدمي الفضاء السيبراني عرضة للانتهاكات من قبل المجرمين ومخترقي الشبكات، مما يؤثر سلباً على جميع المستخدمين من أفراد وشركات ومؤسسات حكومية ومنظمات. ومن هنا تبرز أهمية مضاعفة الجهود على كافة الأصعدة لضمان أمان الفضاء السيبراني والحد من المخاطر الإلكترونية.

وتكتسب الجهود المشتركة بين القطاعات والفرقاء المعنيين، والتعاون الدولي والإقليمي، في مواجهة الانتهاكات على الفضاء السيبراني ومكافحتها أهمية خاصة نظراً للطبيعة الشمولية للمخاطر السيبرانية. حيث تظهر العديد من الإشكاليات عند تواجد كل من الجاني، والضحية، والأنظمة المستخدمة في عدة دول، إضافة إلى تداخل عناصر أخرى منها ما هو افتراضي ومنها ما هو فعلي عبر الحدود الجغرافية والسياسية. الأمر الذي يدل على مدى صعوبة متابعة ومكافحة مخاطر الفضاء السيبرانية. وقد قدر عدد ضحايا الجرائم السيبرانية بنحو 556 مليون ضحية لعام 2013، أي ما يعادل أكثر من 1,5 مليون ضحية في اليوم، أما الخسائر فقد قدرت بـ 110 بلايين دولار أمريكي[2].

ينص مقترح أهداف التنمية المستدامة Sustainable Development Goals، المزمع أن تحل محل الأهداف الإنمائية للألفية ما بعد عام 2015، على تعزيز النفاذ إلى تكنولوجيا المعلومات والاتصالات بما فيها الإنترنت، وكذلك تقليص كلفة النفاذ في البلدان الأقل نمواً. كما أن نتائج القمة العالمية لمجتمع المعلومات بعد مضي عشر سنوات (WSIS+10) استمرت بالتأكيد على أهمية بناء الثقة والأمن بتكنولوجيا المعلومات والاتصالات، وكذلك نشر ثقافة عالمية حول الأمن السيبراني، وتعاون مختلف الفرقاء المعنيين وطنياً وإقليمياً وعالمياً في حماية مستخدمي الفضاء السيبراني.

تأتي هذه الدراسة استكمالاً لأنشطة الإسكوا التي بدأت عام 2007 بهدف تطوير وتنسيق التشريعات السيبرانية في المنطقة العربية وتطبيقها على أرض الواقع، ويجري التركيز على موضوع الأمان السيبراني ومكافحة الجريمة السيبرانية نظراً لأهمية هذا الموضوع لتطوير وبناء مجتمع المعرفة في المنطقة العربية. فقد قامت الإسكوا بتنفيذ مشروع إقليمي تحت عنوان "تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية" بين عامي 2009 و2012، حيث نتج عنه مجموعة من المخرجات أبرزها إرشادات الإسكوا للتشريعات السيبرانية[3]. وقد توسعت هذه الإرشادات في الشق التشريعي حيث قدمت نصوصاً نموذجية للقوانين السيبرانية تتيح للدول في المنطقة العربية الاستفادة منها وتكييفها أو الاعتماد عليها في صياغة قوانينها الوطنية. كما أصدرت الإسكوا في عام 2013 مذكرة سياساتية حول تطوير وتنسيق التشريعات السيبرانية في المنطقة

---

1 تقديرات الاتحاد الدولي للاتصالات. 2014. قياس مجتمع المعلومات. ISBN 978-92-61-15291-8.

2 Todd Neal, Combat Cybercrime with Compliance and Ethics, http://www.tnwinc.com/2910/information-security-training-2.

3 الإسكوا. 2012. إرشادات الإسكوا للتشريعات السيبرانية. E/ESCWA/ICTD/2011/Technical Paper.5.

العربية[4]، بهدف الانتقال من الجانب النظري التشريعي إلى التنفيذ على المستوى الوطني والإقليمي. وقد استخدمت عشر دول عربية إرشادات الإسكوا للتشريعات السيبرانية من أجل تحديث وتطوير قوانينها السيبرانية بالتعاون مع الإسكوا.

وتهدف هذه الدراسة المعنونة "الأمان السيبراني ومواجهة الجرائم السيبرانية في المنطقة العربية: توصيات سياساتية" إلى توفير نظرة تحليلية للوضع الراهن إقليمياً ودولياً ووسائل تعزيز وتنسيق الجهود لمكافحة جرائم الفضاء السيبراني وضمان سلامته، كما تهدف إلى اقتراح إطار توجيهي سياساتي من أجل تعزيز الأمان السيبراني وبناء الثقة بتكنولوجيا المعلومات والاتصالات والفضاء السيبراني.

تتناول الدراسة التوجهات العالمية في مكافحة الجرائم السيبرانية وضمان الأمان السيبراني. وتركز على التوجهات الخاصة بوضع القوانين وتنفيذها وتنسيقها ما بين البلدان في المناطق المتطورة. وتبين الجانب السياساتي على مستوى العالم، في تعزيز الأمن السيبراني ودور المؤسسات العامة والخاصة في تطوير التقنيات اللازمة للحماية من المخاطر السيبرانية وحتى استباقها والتصدي لها. كما تقوم الدراسة بتحليل معمق لوضع المنطقة العربية والتحديات التي تواجهها والفوارق بينها وبين مناطق العالم الأخرى. وذلك فيما يخص تطور الجرائم عبر الفضاء السيبراني، والاستراتيجيات الوطنية للأمان السيبراني، وسن وتطبيق القوانين السيبرانية، وكذلك الأجهزة القانونية، والتعاون في ما بين دول المنطقة. كما تلقي الدراسة الضوء على التحديات التي تواجه القطاع الخاص وكذلك الفوارق في ثقافة المستخدم ووعيه في المنطقة العربية. لذا يعتبر توجه الدراسة توجهاً قانونياً سياساتياً وليس تقنياً خاصاً بتكنولوجيا المعلومات والاتصالات.

ويهدف الجزء المحوري من هذه الدراسة إلى تقديم إطار عمل للأمان في الفضاء السيبراني في المنطقة العربية. وتحث الإسكوا الحكومات في المنطقة العربية على استخدام هذا الإطار وتكييفه بحسب السياق والحاجات الوطنية لبناء بيئة متكاملة للأمان السيبراني ومواجهة الجريمة على الفضاء السيبراني. كما يمكن للمختصين في الحكومات الاستفادة جزئيا من هذا الإطار لسد مواضع النقص وتحديث الوضع التشريعي والمؤسساتي في المنظومة الوطنية للأمان والأمن السيبراني. وقد تمت صياغة هذه الإطار في ضوء تحليل تحديات وفوارق المنطقة العربية وما تحتاجه للوصول إلى مستوى أفضل من الأمان في الفضاء السيبراني.

يتألف إطار العمل المقترح من عدة أجزاء كما يلي:

1- **وضع استراتيجية وطنية لضمان الأمان السيبراني ومكافحة الجرائم السيبرانية** بحيث تغطي هذه الاستراتيجية الجوانب التشريعية والتنفيذية والتنظيمية والتثقيفية. كما ينبغي أن تغطي الاستراتيجية مسائل التوعية والتدريب المتخصص، والمنهجيات الوطنية للاستجابة للحوادث السيبرانية وما يتطلب ذلك من إنشاء مؤسسات مختصة وتوفير الكوادر المهنية، وقياس مخاطر الفضاء السيبراني ووضع المؤشرات التي تراعي النوع الاجتماعي، وتعزيز الشراكة بين القطاع العام والخاص والتعاون الإقليمي.

2- **الوسائل التشريعية المُقترح اعتمادها للأمان السيبراني في المنطقة العربية** والتي تنطلق من إجراء مسح وطني شامل للقوانين ذات الصلة بحيث يتم تفادي تعارض القوانين مع بعضها. إذ أن القوانين الوطنية تحتاج إلى التحديث دورياً في ظل تطور وتغير الإشكاليات القانونية الناتجة عن طبيعة الفضاء السيبراني. كما يتطلب الجانب التشريعي التعاون الدولي نظراً لطبيعة التعديات على الفضاء السيبراني العابرة للحدود. ويمكن

4 الإسكوا. 2013. مذكرة سياساتية - تطوير وتنسيق التشريعات السيبرانية في المنطقة العربية. E/ESCWA/ICTD/2013/ Technical Paper.1.

للدول في هذا الإطار الاسترشاد باتفاقيات جامعة الدول العربية وإرشادات الإسكوا ودراساتها، وكذلك دراسات إقليمية وعالمية أخرى.

3- **وسائل وأجهزة تطبيق القانون** والتي تشمل إنشاء وحدات للتحقيق في الجرائم السيبرانية إما داخل النيابة العامة، أو كقوة مشتركة بين عدة مؤسسات، أو كوحدات تحقيق مركزية. وينبغي هنا أن تتوفر لدى فرق التحقيق خبرات في التعامل مع الجرائم السيبرانية التي يجب أن تأخذ بالاعتبار العنف القائم على نوع الجنس أو العنف ضد المرأة، خاصة عندما تكون الضحية امرأة. ومن الأهمية بمكان إدخال عناصر نسائية ضمن فرق التحقيق لديها خبرات كافية بالجرائم السيبرانية. كما تشمل وسائل العمل الاستباقي إنشاء مراكز الاستجابة لطوارئ الحاسوب، والتي تعمل كأداة أساسية لحماية البنية الأساسية الحساسة للمعلومات، والتي من مهامها رصد المخاطر المعلوماتية المستجدة، والتصدي لها وإطلاق حملات إعلامية للتحذير منها، وكذلك تزويد الجهات المختلفة بتوجيهات حول سبل حماية الأنظمة المعلوماتية والبيانات.

4- **وسائل التوعية والتثقيف والتدريب المتخصص** والتي تستهدف مستخدمي الإنترنت عموماً عبر مختلف وسائل التواصل الإعلامي والتعليمي المرئي والمسموع. كما ينبغي أن تخصص حملات توعية للفئات المختلفة من المجتمع مثل الأطفال والشباب والنساء. وتشمل أنشطة التوعية والتدريب إطلاق الدورات التدريبية المتخصصة للقضاة والمحققين والشرطة والتقنيين في جهاز الشرطة ومراكز الاستجابة لطوارئ الحاسوب.

5- **التعاون بين القطاعين العام والخاص** لدعم عملية حفظ الأمن السيبراني عبر تبادل المعلومات، وتشارك العبء المادي، والتعاون العملي، وإيجاد ووضع الحلول التقنية، وزيادة الاستثمارات. وتقوم مؤسسات القطاع الخاص، كمزودي خدمات الاتصال ومزودي خدمات الشبكة، بدور هام في الحماية التقنية من المخاطر السيبرانية والبرمجيات الخبيثة إضافة إلى التعاون مع الحكومة في تقديم المعلومات والبيانات المطلوبة خلال التحقيقات والمساعدة في التوعية والالتزام بالتوجيهات الوطنية لناحية التعامل مع بيانات المستخدمين وتطبيق معايير أمن المعلومات والأنظمة المعلوماتية.

6- **التعاون الإقليمي والدولي** والذي له أهمية كبيرة نظراً لطبيعة الجرائم السيبرانية العابرة للحدود. وبالنسبة للمنطقة العربية، ينبغي بذل المزيد من الجهود لتنسيق القوانين والتشريعات السيبرانية الوطنية عن طريق استخدام إرشادات الإسكوا للتشريعات السيبرانية، والتعاون عبر تطبيق الاتفاقيات الإقليمية كالاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010، والعمل على الحلول الإجرائية التعاونية كالاستجابة لطلبات التعاون الموجهة بوسائل الاتصال السريعة وتقديم المساعدة المتبادلة بين الدول، وكذلك تعزيز آليات التعاون القضائي مع التركيز على آليات التعاون غير الرسمية بين الأجهزة المختصة بين الدول.

تجدر الإشارة إلى أن الدراسة تتضمن نصاً لقانون نموذجي متعلق بالقواعد الإجرائية الخاصة بالجرائم السيبرانية والأدلة الرقمية (في المرفق الثالث). ويمكن للدول العربية الاستفادة من هذا النص، وتكييفه أو الاقتباس منه في نص القانون الإجرائي الوطني لها.

قائمة المصطلحات

24/7 network point of contact	شبكة نقاط الاتصال 7/24
Anonymity	الغفلية
Authenticity	الموثوقية
Availability	الإتاحة
Botnets	الحواسيب المُسيطر عليها
Child online protection	حماية الأطفال على الخط
Child pornography	المواد الإباحية للأطفال
Cloud computing	الحوسبة السحابية
Computer emergency response team (CERT)	فريق الاستجابة لطوارئ الحاسوب
Computer forensics	علم الأدلة الجنائية المعلوماتية (الجنائيات الحاسوبية)
Confidentiality	السرية
Content attacks	الاعتداءات المرتبطة بالمحتوى
Content data	محتوى المعلومات
Cyber incident response scheme	منهجيات الاستجابة للحوادث السيبرانية
Cyber legislation	التشريعات السيبرانية
Cyber security strategy	استراتيجية الأمن السيبراني
Cyber terrorism	الإرهاب السيبراني
Cyberattack	هجوم سيبراني
Cybercrime	الجريمة السيبرانية
Cyberharassment	التحرش الجنسي السيبراني
Cyberlaundering	تبييض الأموال عبر الفضاء السيبراني
Cyberlaw	القانون السيبراني
Cybersafety	الأمان في الفضاء السيبراني (الأمان السيبراني)
Cybersafety plan	خطة الأمان السيبراني
Cybersecurity	الأمن السيبراني
Cyberspace	الفضاء السيبراني
Cyberstalking	المطاردة السيبرانية
Cyberwar/cyberwarfare	الحرب السيبرانية

قائمة المصطلحات (تابع)

Data espionage	التجسس المعلوماتي/السيبراني
Data host	مستضيف البيانات
Data interference	الاعتداء على البيانات الرقمية
Defamation	القدح والذم
Denial of service	وقف خدمات مواقع إلكترونية
Digital evidence	الدليل الرقمي
Dual criminality	التجريم المتبادل للفعل
Electronic archive	أرشيف إلكتروني
Electronic identity	الهوية الإلكترونية
Electronic identity theft	انتحال الهوية الإلكترونية
Electronic traces	الآثار الرقمية أو الإلكترونية
Encryption	التشفير
Erotic or pornographic material	المواد الإباحية
Filters	برامج الترشيح
Firewall	جدران الحماية
Formal Mutual Legal Assistant (MLA) request	طلب رسمي للمساعدة القانونية المتبادلة
Fraud	الاحتيال
Gambling online	المقامرة على الخط
Global Positioning System (GPS) locations	إحداثيات النظام العالمي لتحديد المواقع
Hackers	مخترقو الشبكات
Identification data	معلومات التعريف
Illegal access/hacking	الدخول غير القانوني إلى نظام معلوماتي
Illegal interception	اعتراض البيانات والاتصالات المعلوماتية
Illegal treatment of personal data	معالجة البيانات ذات الطابع الشخصي دون ترخيص
Informal police cooperation	تعاون الشرطة غير الرسمي
Integrity	السلامة
Internet of things	إنترنت الأشياء
Internet service provider	مزود خدمات الاتصال

قائمة المصطلحات (تابع)

Interoperability	التشغيلية
IP spoofing	تقليد العنوان الرقمي
Log files	سجلات الدخول
Malicious code	برامج احتيالية
Malicious software/Malware	برامج خبيثة
Misuse of devices and software	إساءة استعمال التجهيزات والبرامج المعلوماتية
Non-repudiation	عدم إمكانية الإنكار
Offline	خارج الخط
Online	على الخط
Phishing	التصيد
Privacy	الخصوصية
Proactive investigators	المحققون الاستباقيون
Procedural law for cybercrime and digital evidence	قانون القواعد الإجرائية الخاصة بالجرائم السيبرانية والأدلة الرقمية
Proxies	المخدّمات الوكيلة
Racism Hate/Violence speech	الحض على الكراهية والعنف والعنصرية
Remote forensic tools	تقنيات البحث عن الأدلة المعلوماتية عن بعد
Service provider	مزود خدمات الشبكة
Sex-disaggregated indicators	المؤشرات التي تراعى النوع الاجتماعى
Social engineering	الهندسة الاجتماعية
Spam	البريد الواغل (البريد غير المرغوب فيه)
System breach	اختراق الأنظمة
System interference	الاعتداء على الأنظمة المعلوماتية
Temporary internet files	ملفات الإنترنت المؤقتة
Traffic data	معلومات حركة البيانات
Victims of cyberattacks	ضحايا الاعتداءات السيبرانية
Voice over Internet Protocol (VoIP)	الصوت عبر الإنترنت

مقدمة

يؤدي الاعتماد المتزايد على تكنولوجيات المعلومات والاتصالات إلى ظهور إمكانات وفرص جديدة للتنمية الثقافية والاجتماعية والاقتصادية والسياسية والقانونية، إلا أنه يترافق أيضاً مع زيادة المخاطر الإلكترونية نتيجة الاستخدام السيئ وغير المسؤول لهذه التكنولوجيات. كما يؤدي التزايد المستمر في أعداد مستخدمي الإنترنت إلى تزايد عدد المستخدمين الذين قد يصبحون ضحايا للمخاطر الإلكترونية إما نتيجة الاستخدام الخاطئ أو غير المسؤول للإنترنت وتطبيقاتها، أو نتيجة الهجمات الموجهة لأجهزتهم الإلكترونية غير المحمية بالشكل الملائم، أو تلك الهجمات الموجهة لهم شخصياً سواء عن قصد أو غير قصد. ويزيد من تعقيد المخاطر الإلكترونية آليات إخفاء المعلومات التي يعتمدها مخترقو الشبكات hackers، وهي ما تعرف بالغفلية anonymity، وكذلك الابتكارات التي يعتمدونها عند توجيه هجماتهم السيبرانية، والتطورات المتسارعة للتكنولوجيا، بالإضافة إلى الطبيعة الدولية للجريمة السيبرانية.

إن الطابع المفتوح للإنترنت هو مصدر قوتها، لكنه أيضاً موضع ضعفها الذي يعرضها لخطر المجرمين ومرتكبي الهجمات الإلكترونية. فلكي تؤدي الإنترنت دورها، يجب أن تحافظ على طابعها المفتوح وقابليتها التشغيلية Interoperability[5] مع التجهيزات والأنظمة الأخرى، إلا أن هذا الانفتاح يساعد مخترقو الشبكات على القيام بأعمالهم الجرمية بشكل أسهل على الإنترنت. وقد أصبحت تطال اليوم أيضاً منصات الهواتف النقالة.

وبالتالي فلا بد من تكاتف الجهود للحدّ من المخاطر على الإنترنت ومنصات الهاتف النقال بهدف حماية مستخدمي تكنولوجيا المعلومات والاتصالات بكافة فئاتهم وشرائحهم سواء كانوا أفراداً أم مؤسسات. وفي هذا السياق، تقدم الإسكوا هذه الدراسة لتحديد الأطر السياساتية الضرورية من أجل تعزيز الأمان السيبراني[6] في المنطقة العربية وتوضيح السبل اللازمة من أجل مكافحة الجرائم السيبرانية على المستويين الوطني والإقليمي وبالتلاؤم مع المستوى الدولي.

تلقي هذه المقدمة نظرة سريعة حول المخاطر السيبرانية والأضرار الناتجة عنها، وستوضح الفروق بين الأمان السيبراني والجرائم السيبرانية والأمن السيبراني. كما ستسلط الضوء على نطاق الجرائم السيبرانية وتبين طابعها الدولي. ويمكن للقارئ مراجعة المرفقات الثلاثة الأولى للدراسة والتي تبين المفاهيم التقنية الأساسية للمخاطر المعلوماتية وتفاصيل حول الجرائم السيبرانية الأكثر انتشاراً اليوم.

ألف- لمحة عن المخاطر السيبرانية والأضرار الناتجة عنها

من غير المرجح اليوم أن تؤدي أية أسباب تقنية، كتوقف الإنترنت، إلى التأثير في الاعتماد على هذه الشبكة وذلك لطبيعة البنية الأساسية للشبكة، ولبروتوكولات الاتصال بين الأجهزة االمتصلة. ولكنّ ازدياد المخاطر التقنية والجرائم السيبرانية وضعف الأمن السيبراني هو ما قد يضعف الثقة بالإنترنت، ويدفع الناس إلى تجنب استعمالها؛ أي إن العامل النفسي هو ما قد يخفض من عدد مستخدمي الإنترنت أو من نطاق استخدامها. وهذا الوضع لا يساعد كثيراً على انتشار التطبيقات المهنية في عدد من الدول التي لم تول بعد

---

5 The White House, *International Strategy for Cyberspace, Prosperity, security and Openness in a networked World*, May 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, p. 7.

6 سنعتمد مصطلح "الأمان السيبراني" ونقصد به "الأمان في الفضاء السيبراني" في الدراسة للسهولة.

الاهتمام الكافي للحماية والأمن والتشريعات السيبرانية؛ ومن ثمّ فلا بد من توفير الأمن على الإنترنت والسعي لمكافحة الجرائم السيبرانية.

فبالقدر الذي تطورت فيه الخدمات الإلكترونية، تطورت المخاطر والجرائم السيبرانية، وظهرت طرق جديدة لارتكاب الجرائم على الفضاء السيبراني. ومن المؤكد أنه على المجتمع بأفراده ومؤسساته التعايش مع وجود الجرائم السيبرانية واتخاذ التدابير اللازمة لمواجهتها، فهي لن تتوقف، لا بل يمكن أن تتطور، ويقع على عاتق الإنسان اتخاذ الاحتياطات اللازمة في هذا المجال. لقد أصبح الفضاء السيبراني واقعاً منذ منذ منتصف التسعينات، وخلق بيئة جديدة تزدهر فيها الجرائم السيبرانية، وقد عجزت القوانين الجزائية عن متابعة هذا التطور[7].

كما ظهرت تقنيات جديدة مثل الصوت عبر الإنترنت Voice-over-IP (VoIP) communication والحوسبة السحابية cloud computing والتي يصعب معها تطبيق القانون التقليدي وإجراء التحقيقات القضائية نظراً لشموليتها. وساهمت تقنيات الغفلية (تقنيات إخفاء الهوية الحقيقية للمستخدم) وتنامي تسويق البرامج المعلوماتية التي يستخدمها المخترقون في تطوّر الجرائم السيبرانية. ولم يعد المخترقون يحتاجون إلى خبرات كبيرة، لأن برامج الاختراق أصبحت متوفرة وجاهزة. وقد أظهرت إحدى الدراسات أن 22 في المائة فقط من الهجمات السيبرانية معقدة وتحتاج إلى محترفين[8].

لقد بدأت الحكومات والشركات تعي تدريجياً مخاطر الجرائم السيبرانية وأهمية الأمن السيبراني على الأمن الاقتصادي والسياسي للبلد وعلى مصالحه العامة. وتبدو الإنترنت جنة لمخترقي الشبكات بسبب ظهورهم عليها ظهوراً افتراضياً مغفلاً دون اسم. وقد بات هؤلاء يعون ارتفاع عوائد الجرائم السيبرانية، وتدني مخاطر ونسب اكتشافها، وصعوبة إثباتها في بعض الدول. وبالفعل، يتأتّى عن الجرائم السيبرانية خسائر مالية قد تكون مباشرة أو غير مباشرة؛ وهي خسائر فادحة تلحق بالأفراد والاقتصاد على حد سواء. فعلى سبيل المثال، جرى في عام 2012 تقدير قيمة الأضرار الناشئة عن الجرائم السيبرانية في أستراليا بقرابة 2 مليار دولار[9]. ويبين الإطار 1 أضرار الشركات في المملكة المتحدة بسبب الجرائم السيبرانية.

الإطار 1- أضرار الشركات في المملكة المتحدة بسبب الجرائم السيبرانية

أفادت 81 في المائة من الشركات الكبيرة و60 في المائة من المؤسسات الصغيرة في المملكة المتحدة بتعرضهم لاختراق معلوماتي في عام 2013، وكانت قيمة الضرر لأسوأ حالات الجرائم السيبرانية تقع بين 600 ألف ومليون جنيه إسترليني للشركات الكبيرة، وبين 65 ألف و115 ألف جنيه إسترليني للشركات الصغرى[أ]. ويرى مسؤولو بنك إنكلترا أن الهجمات السيبرانية هي أكبر تهديد للاستقرار المالي في المملكة المتحدة[ب].

أ Cabinet Office, Office of Cyber Security and Information Assurance, *Keeping the UK safe in cyber space*, https://www.gov.uk/government/policies/keeping-the-uk-safe-in-cyberspace, p. 2, 3.

ب Todd Neal, Security Analyst, *Combat Cybercrime with Compliance and Ethics*, http://www.tnwinc.com/2910/information-security-training-2.

7 Stein Schjolberg, *The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva*, December 2008, http://www.cybercrimelaw.net/documents/cybercrime_history.pdf, p. 1.

8 United Nations Office on Drugs and Crime, UNODC, *Comprehensive study on* cybercrime, draft, February 2013, p. 42.

9 Norton cybercrime report 2012.

وفي منطقة الشرق الأوسط، يعتقد 48 في المائة من خلال استطلاع قامت به شركة PwC عام (2014) أن مخاطر الجرائم السيبرانية في مؤسساتهم قد ازدادت في الـ 24 شهراً الماضية[10]. كما يبين الإطار بعض الإحصاءات الأخرى حول معدلات الجرائم السيبرانية في المنطقة العربية.

الإطار 2- ارتفاع معدلات الجرائم السيبرانية في دول منطقة الشرق الأوسط

ارتفعت نسبة الجرائم السيبرانية في دول منطقة الشرق الأوسط. فعلى سبيل المثال، ارتفع معدل الجريمة الإلكترونية في دولة الإمارات العربية المتحدة بنسبة 25 في المائة في عام 2013 مقارنة بعام 2012[أ]. كما ارتفعت الجرائم السيبرانية في دولة الكويت في عام 2012 من 563 قضية إلى 997 قضية عام 2013[ب]. وازداد عدد الجرائم السيبرانية المبلَّغ عنها في سلطنة عمان لدى سلطة التحقيق من أقل من 200 في نهاية عام 2011 إلى أكثر من 800 قضية في نهاية عام 2013[ج].

أ لواء النعساني، ص 2 http://www.24.ae/article.aspx?ArticleId=77807.

ب جواب الجهاز المركزي لتكنولوجيا المعلومات على الاستبيان المرسل له في إطار هذه الدراسة، إحصاءات نقلاً عن وزارة الداخلية الكويتية إدارة مكافحة الجرائم الإلكترونية، الكويت، أيلول/سبتمبر 2014.

ج جواب المركز الوطني للسلامة المعلوماتية بهيئة تقنية المعلومات على الاستبيان المرسل له من قبل الإسكوا في إطار هذه الدراسة، سلطنة عُمان، أيلول/سبتمبر 2014.

وتمتاز الجرائم السيبرانية بالسرعة التي تتم بها، بحيث تحدث الأضرار حتى قبل أن تعي الضحية باستهدافها، وهو ما قد لا يتيح للضحية الدفاع عن نفسها. ويُقدَّر عدد ضحايا الجرائم السيبرانية بنحو 556 مليون ضحية في العام، أو أكثر من 1,5 مليون ضحية في اليوم[11]. كما تشير بعض الإحصاءات إلى أن 72 في المائة من مستخدمي الإنترنت من الرجال يقعون ضحية هذه الجرائم مقابل 65 في المائة من مستخدمي الإنترنت من النساء[12]. وتدل هذه الإحصاءات إلى أن الرجال هم أكثر عرضة لجرائم الإنترنت من النساء، وخاصة الفئة العمرية ما بين 18 إلى 31 سنة، ويرجع ذلك إلى استخدامهم للإنترنت لفترات زمنية أطول ولجرأتهم بالدخول إلى مواقع مختلفة، وانخراطهم بسلوك محفوف بالمخاطر عبر الإنترنت ما يعرضهم أكثر للاحتيال والسرقات والبرمجيات الخبيثة.

كما يلاحظ ارتفاع الجرائم السيبرانية ضد المرأة وخاصة تلك التي تتعلق بالعنف ضد المرأة حيث أن 95 في المائة من السلوك العدواني على الإنترنت كالتحرش، والمطاردة، واللغة المسيئة، والصور المهينة هي موجهة ضد النساء، وعادة ما تصدر من الشريك أو من شريك سابق. وفي دراسة حديثة أجراها الاتحاد الأوروبي عام 2014، يظهر أن 4 في المائة من النساء ما بين سن 18 و29 عاماً قد عانوا خلال السنة السابقة من ملاحقة عبر الفضاء السيبراني cyberstalking، في حين أن 11 في المائة من النساء اللواتي تمت مقابلتهن لغرض الدراسة، وهم بعمر 15 سنة فما فوق، قد تلقوا نوعاً من الرسائل غير المرغوب فيها، كالرسائل الجنسية الهجومية عبر البريد الإلكتروني أو الرسائل النصية SMS، أو التحرش غير اللائق عبر شبكات التواصل الاجتماعي.

10 John Wilkinson, Tareq Haddad, PWC, *Economic Crime in the Arab World*, February 2014, http://www.pwc.com/m1/en/publications/gecs2014reportme.pdf, p. 16.

11 Todd Neal, Security Analyst, *Combat Cybercrime with Compliance and Ethics*, http://www.tnwinc.com/2910/information-security-training-2.

12 Norton. http://us.norton.com/cybercrimereport.

وتبقى الولايات المتحدة الأمريكية البلد الأول المنتج للبريد الواغل (أو غير المرغوب فيه) Spam[13]. ويقدَّر أن البريد الواغل قد استهلك في عام 2012 قرابة 70 في المائة من مجمل حركة البيانات على الإنترنت[14].

ويعتبر مكتب التحقيقات الفدرالي في الولايات المتحدة الأمريكية جرائم تكنولوجيا المعلومات من أهم الجرائم التي تواجهها الولايات المتحدة[15]. ويعتقد نحو 60 في المائة من أصحاب الأعمال في الولايات المتحدة أن الضرر اللاحق بهم من جراء الجرائم السيبرانية يفوق الضرر الناجم عن الجرائم العادية[16]. كما أكد تقرير صادر عن الأوروبول Europol في عام 2011 حول تقييم مخاطر الجريمة المنظَّمة أن تكنولوجيا الإنترنت أصبحت عاملا أساسياً لتسهيل معظم أنشطة الجريمة المنظمة[17].

وهكذا، لا بدّ من التساؤل عمّا إذا كانت هذه الوسيلة الجديدة للتواصل، أي الإنترنت، تعطي نتائج إيجابية أم أن عيوبها تفوق إمكاناتها. والجواب عن هذا السؤال هو رهن بنجاعة التدابير المتخذة في كل دولة لضمان الأمان والأمن السيبراني.

باء- التمييز بين الأمان في الفضاء السيبراني والجرائم السيبرانية والأمن السيبراني

قد لا تكون جميع الاعتداءات في الفضاء السيبراني مجرّمة في القانون الجزائي في بعض الدول، وذلك بالرغم من الأضرار التي قد تنشأ عنها؛ وفي هذه الحالة، تعتبر المضايقات والهجمات الإلكترونية سلوكاً غير ملائم ويتطلب قواعد وخطط للأمان السيبراني Cyber Safety Plan، حيث يجري التركيز على المخاطر العريضة الشخصية والاجتماعية الناتجة عن استعمال الحاسوب. أما عندما تكون هذه الأفعال مجرمة جزائياً، فتعتبر هذه الهجمات والمضايقات السيبرانية جرائم سيبرانية وتتطلب خطة وطنية لمكافحتها National Plan to Combat Cybercrime. أما حين تتمادى الاعتداءات لتطال الأمن القومي، فنكون في صدد استراتيجية للأمن السيبراني Cyber Security Strategy، حيث يجري العمل على خطة لفضاء سيبراني آمن وموثوق، بحيث تكون الدولة قادرة على مجابهة الهجمات على البيانات والأنظمة، ولا سيما الهجمات التي تطال البنية الأساسية الحساسة والأنظمة المعلوماتية للأمن القومي. ويمكن القول إن العمل على توفير الأمان والأمن في الفضاء السيبراني يساهمان حكماً في مجابهة الجرائم السيبرانية[18]. ويؤكد الاتحاد الدولي للاتصالات في دراسة صادرة عنه أن وضع استراتيجية لمكافحة الجرائم السيبرانية هو عنصر لا يتجزأ من استراتيجية الأمن السيبراني[19].

---

13 Wikipedia, *International Cybercrime*, http://en.wikipedia.org/wiki/International_cybercrime, p. 8.

14 Symantec Intelligence Report, June 2012; Kaspersky Lab Report, June 2012.

15 Steven R. Chabinsky, Deputy Assistant Director, Cyber Division, Federal Bureau of Investigation, GovSec/ FOSE Conference, Washington, DC, http://www.fbi.gov/news/speeches/the-cyber-threat-whos-doing-what-to-whom. Hereinafter: Chabinsky, GovSec/FOSE Conference.

16 IBM survey, published 14.05.2006, available at: www-03.ibm.com/industries/consumerproducts/doc/content/news/pressrelease/1540939123.html.

17 Europol, *EU Organized Threat Assessment: OCTA 2011,* April 28, 2011, http://www.europol.europa.eu/publications/European_Organised_Crime_Threat_Assessment_%28OCTA%29/OCTA_2011.pdf, p. 6.

18 Australian Government, Attorney General's Department, *National Plan to Combat Cybercrime*, http://www.ag.gov.au/CrimeAndCorruption/Cybercrime/Documents/National%20Plan%20to%20Combat%20Cybercrime.pdf, p. 6.

19 ITU, Marco Gercke, *Understanding Cybercrime: Phenomena, Challenges and Legal Response,* September 2012, p. 97.

جيم- الطابع الدولي للجرائم السيبرانية

يعتبر الطابع الدولي للجرائم السيبرانية من أبرز الصفات التي تميزها، وهي بذلك تتحدى النظام القانوني المحلي والدولي. إذ يطغى في كثير من الأحيان الطابعُ الدولي على الجريمة السيبرانية، فهي جريمة عابرة للحدود، وقد تتضمن أكثر من عنصر أجنبي. فالفعل الجرمي قد يحصل في بلد معين وتتحقق النتيجة الجرمية في بلد آخر، مثل حالة اختراق نظام معلوماتي عن بعد. كما قد تتحقق النتيجة الجرمية في جميع البلدان، مثل حالة نشر قدح وذم بحق شخص معين على موقع إلكتروني يمكن الوصول إليه من معظم دول العالم.

ولا تطال الجرائم السيبرانية اليوم الأفراد فقط، بل أصبحت جرائم شاملة قد تأخذ شكل هجمات ضخمة منسقة تطال البنية الأساسية الحساسة للمعلومات في أكثر من دولة، أو شكل نشاطات إرهابية على الإنترنت. وفي عام 1998، عمدت مجموعة الدول الصناعية الثماني التي هي أكثر تطوراً في العالم G8 إلى إطلاق خطة عمل لمحاربة الجرائم السيبرانية وإنشاء شبكة خبراء متاحة 7 أيام في الأسبوع على مدار 24 ساعة في اليوم للمساعدة في التحقيقات المتعلقة بجرائم المعلوماتية، وكذلك تدريب أجهزة الأمن لدى تلك الدول وتجهيزهم.

دال- تحديد موضوع الدراسة وأهدافها

تأتي هذه الدراسة ضمن الجهد المتواصل للإسكوا لتنظيم قطاع تكنولوجيا المعلومات والاتصالات، وهي استكمال لمشروع الإسكوا "تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية"[20]، الذي قامت بتنفيذه إدارة التكنولوجيا من أجل التنمية (إدارة تكنولوجيا المعلومات والاتصالات سابقاً) في الإسكوا في الفترة 2009-2012. وقد نتج عن هذا المشروع "إرشادات الإسكوا للتشريعات السيبرانية"[21] وهي تشكل نماذج تشريعية يمكن الاقتباس منها في دول المنطقة من أجل تطوير التشريعات الوطنية كما تعتبر اللبنة الأساسية لتنسيق التشريعات السيبرانية في المنطقة العربية، إذ تم استخدامها حتى تاريخ هذا التقرير في تطوير أو تعديل التشريعات السيبرانية في عشر دول عربية. وتشمل إرشادات الإسكوا المواضيع التالية: الاتصالات الإلكترونية وحرية التعبير، المعاملات الإلكترونية والتواقيع الإلكترونية، التجارة الإلكترونية وحماية المستهلك، معالجة البيانات ذات الطابع الشخصي، الجرائم السيبرانية، حقوق الملكية الفكرية في المجال المعلوماتي والسيبراني.

واستناداً إلى نتائج هذا المشروع، أصدرت إدارة التكنولوجيا من أجل التنمية في الإسكوا في عام 2013 "مذكرة سياساتية حول تطوير وتنسيق التشريعات السيبرانية في المنطقة العربية"[22]، بهدف الانتقال من الجانب النظري التشريعي إلى الجانب التنفيذي على المستوى الوطني والإقليمي.

تهدف هذه الدراسة إذاً إلى بيان وضع الدول العربية من ناحية الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية، وإلى وضع آليات ومنهجيات عملية لتحسين الإطار القانوني والتنظيمي للأمن السيبراني في المنطقة العربية. وتعتبر الإشكاليات والمفاهيم القانونية والتقنية التي تم استعراضها في هذه المقدمة موضوع هذه الدراسة، مع التركيز على دول المنطقة العربية من حيث الأمان والأمن السيبراني وواقع الجرائم

20 http://isper.escwa.un.org/FocusAreas/CyberLegislation/Projects/tabid/161/language/ar-LB/Default.aspx.

21 http://isper.escwa.un.org/Portals/0/Cyber%20Legislation/Regional%20Harmonisation%20Project/Directives/Cover-Contents.pdf.

22 http://www.escwa.un.org/information/publications/edit/upload/E_ESCWA_ICTD_13_TP-2_A.pdf.

السيبرانية فيها. كما ستبين هذه الدراسة الفوارق بين وضع المنطقة العربية ودول العالم من حيث السياسات والقوانين النافذة، ومن حيث المعايير والقواعد المطبقة، وبرامج التوعية والتدريب المتبعة.

وستقترح الدراسة إطاراً نموذجياً لتعزيز الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية، وهو يشمل النواحي الاستراتيجية والتشريعية والتنظيمية والتنفيذية والتوعية والتدريب. ويشكل هذا الإطار مخططاً توجيهياً يبين الخطوات العملية الواجب اتّباعها في كل دولة لتعزيز الأمان والأمن السيبراني ومكافحة الجرائم السيبرانية. أي أن هذه الدراسة تهدف إلى وضع الإطار التنظيمي والإجرائي للحد من الجرائم السيبرانية وضمان الأمن السيبراني.

تجدر الإشارة إلى أن الإسكوا تفاعلت مع وزارات وهيئات تكنولوجيا المعلومات والاتصالات في الدول الأعضاء في الإسكوا عند إعداد هذه الدراسة، وقد أرسلت استبياناً إلى الدول بغية التعرف عن كثب على الوضع القانوني والتنظيمي للفضاء السيبراني. وسيتضمّن المرفق الرابع من هذه الدراسة جدولاً يلخص نتائج الاستبيان.

ونظراً للحجم المحدّد لهذه الدراسة والرغبة بتفصيل الإطار المقترح لتعزيز الأمان السيبراني، سوف تتناول الدراسة بعض الدول كنماذج عن الدول العربية وهي: دولة الإمارات العربية المتحدة من بلدان مجلس التعاون الخليجي (النموذج الأول)، ومصر من الدول العربية في شمال أفريقيا (النموذج الثاني)، ولبنان من الدول العربية في غرب آسيا (النموذج الثالث) إذ أنه من الصعب إجراء معالجة تفصيلية لوضع الأمان السيبراني في جميع الدول العربية. إلا أن الدراسة تقدّم ملخصاً عن مجمل الأوضاع في المنطقة العربية، وتعرض أمثلة مختارة من الدول العربية الأخرى، ولو باقتضاب، كلما أمكن ذلك.

لقد تمت إضافة بعض الإحصاءات المصنفة حسب النوع الاجتماعي لتسليط الضوء على تأثير الجريمة السيبرانية على كل من الرجال والنساء. إلا أنه يوجد نقص في البيانات والإحصاءات التي تبين أوجه الشبه والاختلاف للجريمة السيبرانية ما بين الرجال والنساء، ليس في المنطقة العربية فحسب، بل على المستوى الدولي أيضاً.

ومن أجل معالجة وافية للدراسة، ستتضمن هذه الدراسة ثلاثة أجزاء أساسية:

1- التوجهات العامة في مكافحة الجرائم السيبرانية وضمان الأمان السيبراني.
2- التحديات الإقليمية وتحليل الفوارق في مجال الأمان السيبراني ومكافحة الجرائم السيبرانية.
3- إطار عمل للأمان السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية.

وأخيراً، تجدر الإشارة إلى أن إعداد هذه الدراسة تم بحيث يستطيع القارئ انتقاء الفصول بشكل منفصل وفقاً لاهتماماته، أو أن يقرأ الدراسة بشكل متكامل للاطلاع والاستفادة من الفصول الثلاثة الرئيسية.

وتأمل الإسكوا أن يستفيد متخذو القرار في الحكومات من هذه الدراسة وتطبيقها في دولهم، وأن يستفيد منها كذلك أصحاب المصلحة الآخرون المعنيون بتطوير مجتمع المعرفة في المنطقة العربية، كالقطاع الخاص والمنظمات غير الحكومية، وكذلك الأفراد.

أولاً- التوجهات العامة العالمية في مكافحة الجرائم السيبرانية وضمان الأمان السيبراني

من المؤكد أن الجرائم السيبرانية تنمو وتزداد حالياً بدافع تحقيق الأرباح المادية بسهولة وذلك عن طريق استغلال الانتشار الواسع لتكنولوجيا المعلومات والاتصالات ووصولها إلى مستخدمين غير مدركين للمخاطر والحيل التي قد يرتكبها مجرمو المعلوماتية. كما قد يكون الدافع وراء الجرائم السيبرانية التهجم على خصوصيات الأفراد واستغلال الكميات الهائلة من المعلومات بمختلف أشكالها للتجريح بهم أو التحرش بهم. وبالمقابل، ينمو وعي الأفراد في الدول المتقدّمة لهذه الجرائم بفعل التوعية المستمرة والتغطية الإعلامية الدائمة[23] حول المخاطر السيبرانية. ويختلف تقدير مدى خطورة الجريمة السيبرانية بين الأفراد والمؤسسات التجارية والدولة؛ إذ تعتبر المؤسسات التجارية أن جرائم التعرض للأنظمة المعلوماتية هي من أخطر الجرائم السيبرانية.

ومن المؤكد أن الجرائم السيبرانية تزداد وتتطور مع تقدم التكنولوجيا، فحجم التجهيزات المعلوماتية يصغر، في حين تزداد سعات الحفظ وسرعات المعالجة. وقد أصبحت المعالجات جزءاً أساسياً من الأجهزة الكهربائية المعروفة مثل الثلاجة أو الغسالة ومن المتوقع انتشار التحكم الإلكتروني بشكل أوسع مع التوجهات الحديثة نحو إنترنت الأشياء Internet of Things. ويمكن تلخيص تحديات الفضاء السيبراني وفق ما يلي[24]:

- يشرف على إدارة الفضاء السيبراني بشكل أساسي القطاع التجاري، وهذا الفضاء غير مركزي بطبيعته؛
- تتضمن الأجهزة والأنظمة التي تشكّل الفضاء السيبراني عناصر مقدّمة من مورّدين مختلفين؛
- من الصعب التنبؤ بطريقة استخدام الفضاء السيبراني في المستقبل نظراً لسرعة التغير والابتكار؛
- إن سرعة التطور التكنولوجي تجعل وسائل الدفاع والوقاية في الفضاء السيبراني بطيئة وغير ملائمة.

ويتضح مما سبق أن ازدياد الانفتاح والربط بين الشبكات المعلوماتية وعدم وجود أي مركزية يؤدي إلى بروز مكامن ضعف أكبر على هذه الشبكات. ويقدم المرفق الأول شرحاً للمفاهيم التكنولوجية الأساسية المستخدمة في هذه الدراسة.

وفي المقابل، فقد ظهرت في السنوات الأخيرة ملامح توجّهات عامة تعتمدها الدول في مكافحة الجرائم السيبرانية على صعيد العالم، وقد تشكّل هذه التوجهات أساساً لسياسة أو استراتيجية وطنية للأمن السيبراني مع الإشارة إلى ضرورة تكييف هذه التوجهات، مع خصوصية الدولة وإمكانياتها وظروفها ونظامها القانوني والاجتماعي.

ووفقاً لإحدى دراسات الأمم المتحدة[25] من المؤكد أن نمو الربط الإلكتروني بين الأنظمة المعلوماتية يساهم في زيادة الجرائم السيبرانية، مع الإشارة إلى أن الجرائم السيبرانية تركز في الوقت الحاضر على

---

23 United Nations Office on Drugs and Crime, UNODC, *Comprehensive study on cybercrime*, draft, February 2013, p. 6.

24 Cabinet Office, *The UK Cyber Security Strategy, Protecting and promoting the UK in a digital world*, November 2011, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf, p. 18.

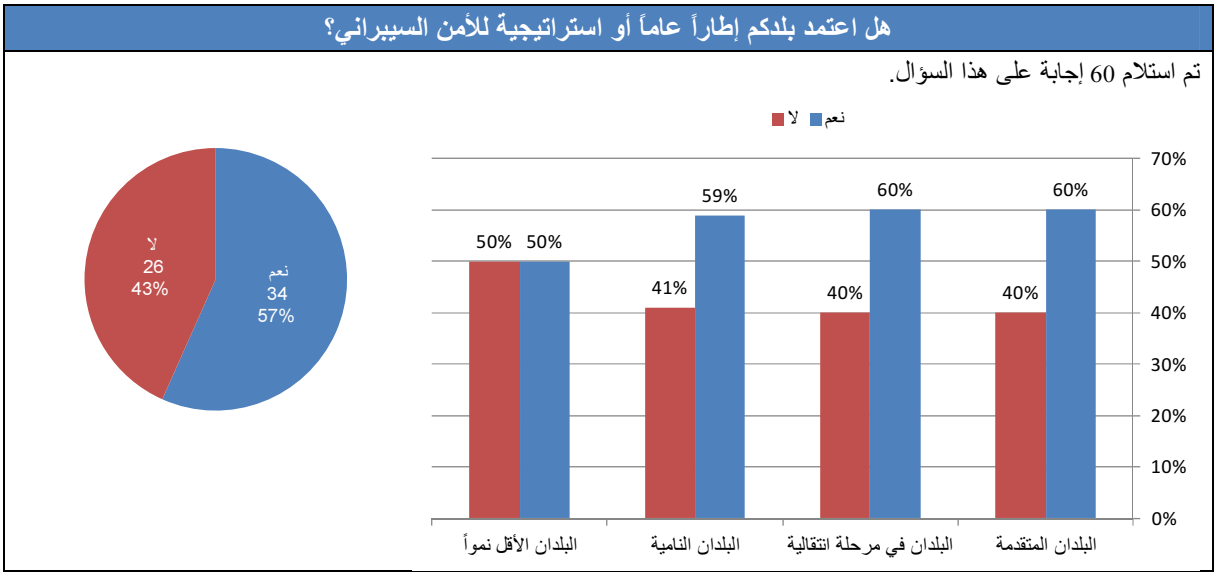
25 United Nations Office on Drugs and Crime, UNODC, *Comprehensive study on cybercrime*, draft, February 2013, p. 4.

الأنظمة المعلوماتية ذات النطاق العالمي Global، وتستهدف بدرجة أدنى الأنظمة المعلوماتية المستقلة غير المترابطة Standalone. وتوجه الدول والمؤسسات نحو اعتماد تقنيات الحوسبة السحابية cloud computing يطرح تحديات جديدة على مستوى الأمن السيبراني. ويبين المرفق الثاني لائحة بالجرائم السيبرانية.

ويعتمد تخفيف المخاطر[26] على اعتماد تقنيات وحلول فاعلة للحوادث، واستخدام تجهيزات وبرمجيات موثوقة، والاعتماد على موردين ذوي سمعة حسنة. كما يعتمد على تطبيق فعال للقانون، وتعاون دولي متوافق عليه، وكذلك تعاون مع القطاع الخاص من أجل إيجاد الحلول التقنية الملائمة، وتطوير قواعد للتصرف لدى الدول. ويجب أيضاً اتخاذ تدابير الحماية الملائمة بإعادة دراسة قواعد التصرف وسياسات الأمن Code of conduct and security policies دورياً، والتوعية حول أهمية تطبيق قواعد الأمن security compliance والتدريب على أمن المعلومات Information security training[27].

وتبين دراسة أجراها الاتحاد الدولي للاتصالات شملت 62 دولة على صعيد العالم[28] أن 57 في المائة من الدول لديها استراتيجية للأمن السيبراني، وأن 67 في المائة من الدول التي ليس لديها استراتيجية هي في طور وضعها. أما معظم الدول العربية، فليس لديها استراتيجية جاهزة للأمن السيبراني، وأن بعضها أيضاً لم يبدأ بعد بصياغة استراتيجية وطنية.

الشكل 1- اعتماد الدول على استراتيجية للأمن السيبراني



المصدر: *2013 ITU survey on measures to raise awareness on cybersecurity*, August 2013. http://www.itu.int/en/ITU-D/Cybersecurity/Documents/22survey.pdf, p. 15.

---

26 The White House, *International Strategy for Cyberspace, Prosperity, security and Openness in a networked World*, May 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, p. 13.

27 Todd Neal, Security Analyst, *Combat Cybercrime with Compliance and Ethics*, http://www.tnwinc.com/2910/information-security-training-2.

28 ITU, *2013 ITU survey on measures to raise awareness on cybersecurity*, August 2013, http://www.itu.int/en/ITU-D/Cybersecurity/Documents/22survey.pdf, p. 15.

يعرض هذا الفصل التوجهات العامة في مكافحة الجرائم السيبرانية وضمان الأمن السيبراني بشيء من التفصيل. وتعرض الفقرة الأولى لمحة عن الجهود المبذولة على الصعيد العالمي لمكافحة الجرائم السيبرانية وضمان الأمن السيبراني، بينما تعرض الفقرة الثانية التوجهات التشريعية، وتوضح الفقرة الثالثة التوجهات الخاصة بتطبيق القانون والتنظيم. وتخصص الفقرة الرابعة للتوجهات المتعلقة بالتعاون بين الدول، أما الفقرة الخامسة فتخصص للتوجهات التقنية والإدارية والتنظيمية الأخرى.

ألف- لمحة حول الجهود المبذولة على الصعيد العالمي

1- قرارات ووثائق الأمم المتحدة

في نطاق العمل الأممي، أصدرت الأمم المتحدة عدة قرارات بخصوص الجرائم السيبرانية أو المعلوماتية، أهمها القرار رقم 63/55 بتاريخ 4 كانون الأول/ديسمبر 2000 والقرار رقم 121/56 بتاريخ 19 كانون الأول/ديسمبر 2001 حول محاربة سوء استخدام تكنولوجيا المعلومات. وقد أوصى القرار رقم 63/55 بأن تضمّن الدول في قوانينها وممارساتها إلغاء أية ملاذات آمنة لكل من يسيء استخدام تكنولوجيا المعلومات، كما أقر بأن الأنظمة القانونية يجب أن تحمي سرية المعلومات وأنظمة الحاسوب وسلامتها وتوفرها من الاعتداء غير المشروع، وأن تضمن معاقبة التصرف الجرمي. ويدعو القرار 121/56 الدول عند صياغة قوانين وطنية أو سياسات أو ممارسات لمحاربة سوء الاستخدام الجزائي لتكنولوجيا المعلومات أن تأخذ في الحسبان أعمال وإنجازات لجنة الوقاية من الجرائم والعدالة الجزائية[29]. وقد أصدرت الهيئة العامة للأمم المتحدة في عام 2005 القرار رقم 60/177 الذي يشجع التعاون لمكافحة الجرائم السيبرانية وتقديم المساعدة للدول الأعضاء في هذا المجال. كما أصدرت الأمم المتحدة في عام 2010 القرار رقم 64/211 الذي يدعو الدول إلى تحديث قوانينها في مجال الجرائم السيبرانية والخصوصية والبيانات الشخصية والتجارة والتواقيع الإلكترونية وإلى اعتماد الاتفاقيات والتجارب الإقليمية في هذه المراجعة.

إضافة إلى ما تقدم، فإن الوثائق العالمية حول حقوق الإنسان، ولا سيما الإعلان العالمي لحقوق الإنسان، والعهد الدولي الخاص بالحقوق المدنية والسياسية لعام 1966، واتفاقية مجلس أوروبا حول حماية حقوق الإنسان والحريات الأساسية، تؤكد حق الإنسان في حرية الرأي دون أي تدخل، وحقه في البحث وتلقي أي معلومات أو أفكار من خلال أية وسيلة بصرف النظر عن الحدود.

بينت وثائق مؤتمر القمة العالمية لمجتمع المعلومات في جنيف في عام 2003 ثم في تونس في عام 2005 أهمية تطوير مجتمع معلومات في مختلف الدول. وأشارت هذه الوثائق والتي تتضمن إعلان مبادئ[30] وخطة عمل جنيف[31] والتزام تونس[32] وأجندة تونس[33] إلى ضرورة بناء الثقة والأمن في مجتمع المعلومات وحددت الأطر التي يجب العمل من أجل تأمين ذلك. وقد اعتمدت 174 دولة مشاركة في القمة العالمية مقررات هذه القمة.

---

29 Stein Schjolberg, *The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva*, December 2008, http://www.cybercrimelaw.net/documents/cybercrime_history.pdf, p. 9.

30 http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1161|0.

31 http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1160|0.

32 http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2266|0.

33 http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2267|0.

2- جهود الاتحاد الدولي للاتصالات

أعلن الأمين العام للاتحاد الدولي للاتصالات عام 2007 إطلاق مبادرة أجندة الاتحاد الشاملة حول الأمن السيبراني Global Cybersecurity Agenda[34]. ويعمل الاتحاد الدولي للاتصالات منذ ذاك العام على هذه الأجندة. وتهدف هذه الأجندة إلى إنشاء إطار أو بروتوكول للتنسيق بين جهود مكافحة الجرائم السيبرانية، وهو يشمل تدابير قانونية وتقنية وتدابير إجرائية وتنظيمية وتدابير تخصّ بناء القدرات والتعاون الدولي. وقد جرى في عام 2008 نشر التقرير النهائي الذي تم إعداده من قبل أكثر من 100 خبير[35]. ويعمل الاتحاد الدولي للاتصالات على تنفيذ آلية لوضع إطار مشترك للأمن السيبراني للأمم المتحدة يعالج الأمن السيبراني على المستوى الوطني والإقليمي والعالمي[36]. هذا وتتضمن الفقرة 14 من إعلان حيدر أباد عام 2010 نصاً حول حماية المرأة على الإنترنت حيث تعتبر إحدى مكونات بناء الثقة بالفضاء السيبراني والثقة في توافر، وموثوقية، وأمن، واستخدام تكنولوجيا المعلومات والاتصالات[37]. وعلى صعيد المنطقة العربية، تستضيف سلطنة عمان المركز الإقليمي للأمن الإلكتروني للمنطقة العربية التابع للاتحاد الدولي للاتصالات. ويهدف هذا المركز إلى تقديم الخدمات والمبادرات للمنطقة العربية لتحسين قدرات الأمن الإلكتروني عن طريق التنسيق وتعزيز التعاون الإقليمي[38].

3- الاتفاقيات والمبادرات الإقليمية

تعتبر اتفاقية مجلس أوروبا حول الجرائم السيبرانية (اتفاقية بودابست) التي دخلت حيز التنفيذ في 1 تموز/يوليو 2004 من أهم الاتفاقيات الإقليمية. وتهدف هذه الاتفاقية إلى تنسيق التشريعات الوطنية حول الجرائم السيبرانية وتحسين القدرات الوطنية للتحقيق في هذه الجرائم والتعاون في هذا المجال؛ وهي تُعنى بجمع الأدلة المعلوماتية في مختلف أنواع الجرائم[39]، وليس في الجرائم السيبرانية فقط. وتتضمن الاتفاقية ثلاثة أجزاء: الجزء الأول حول القواعد الموضوعية للجرائم، والجزء الثاني حول إجراءات التحقيق، والجزء الثالث حول آليات التعاون الدولي. ولغاية بداية شهر تشرين الأول/أكتوبر عام 2014، صادقت 43 دولة على الاتفاقية في حين وقعت 10 دول أخرى عليها لكنها لم تصادق عليها إلى الآن (يُراجع الموقع الإلكتروني لمجلس أوروبا)[40]. وتعدّ الاتفاقية نموذجاً تشريعياً، حيث اقتبست عدة دول في المنطقة العربية من نصوص هذه الاتفاقية عند إعداد قوانينها الوطنية.

---

34 ITU, Marco Gercke, *Understanding Cybercrime: Phenomena, Challenges and Legal Response,* September 2012, p. 120, p. 121.

35 Stein Schjolberg, *The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva*, December 2008, http://www.cybercrimelaw.net/documents/cybercrime_history.pdf, p. 20.

36 Dr. Hamadoun I. Touré Secretary-General, ITU, *CybersecurityGlobal status update*, December 2011, http://www.un.org/en/ecosoc/cybersecurity/itu_sg_20111209_nonotes.pdf, p. 10.

37 ITU. http://www.itu.int/ITU-D/conferences/wtdc/2010/pdf/HyderabadDeclaration.pdf.

38 جواب المركز الوطني للسلامة المعلوماتية بهيئة تقنية المعلومات على الاستبيان المرسل له من قبل الإسكوا في إطار هذه الدراسة، سلطنة عمان، أيلول/سبتمبر 2014.

39 يبين المرفق الثالث جدول بالأدلة المعلوماتية.

40 http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG.

وفي المنطقة العربية تم وضع الاتفاقية العربية في 21 كانون الأول/ديسمبر 2010 لمكافحة جرائم تقنية المعلومات[41]، والتي تضمنت خمسة فصول أساسية منها فصل خاص بالتجريم ويحدد أنواع الجرائم السيبرانية، وفصل يتعلق بالأحكام الإجرائية وفصل خاص بالتعاون القانوني والقضائي في ما بين الدول العربية. وقد وقعت 18 دولة عربية على هذه الاتفاقيات وصادقت عليها سبع دول عربية.

كما أعدت الإسكوا في إطار مشروع "تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية"[42]، المنفذ خلال 2009-2012، "إرشادات الإسكوا للتشريعات السيبرانية"[43] والتي تعتبر بمثابة نماذج تشريعية لدول المنطقة. وهذه الإرشادات تشمل، إضافة إلى الجرائم السيبرانية، الاتصالات الإلكترونية وحرية التعبير، والتواقيع الإلكترونية والمعاملات الإلكترونية، والتجارة الإلكترونية وحماية المستهلك، ومعالجة البيانات ذات الطابع الشخصي، وحقوق الملكية الفكرية في المجال المعلوماتي والسيبراني.

ولتنسيق التشريعات حول جرائم الحاسوب في دول الكومنولث، أعدّت مجموعة من الخبراء قانوناً نموذجياً في عام 2002 مُستوحى من اتفاقية بودابست، سمي "قانون الجرائم المتعلقة بالحاسوب". كما أقر الاتحاد الأوروبي في عام 2003 إطاراً قانونياً حول الاعتداءات على الأنظمة المعلوماتية، ودخل حيز التنفيذ في عام 2005. وقد كانت منظمة التعاون والتنمية في الميدان الاقتصادي Organization for Economic Cooperation and Development (OECD) أول منظمة دولية أصدرت توجيهات حول جرائم الحاسوب وحول أمن أنظمة المعلومات والشبكات[44]. وكذلك اعتمدت العام الماضي اتفاقية الاتحاد الأفريقي الخاصة بمجال الأمن السيبراني وحماية البيانات الشخصية في حزيران/يونيو 2014[45].

وقد عمدت بعض المناطق إلى إنشاء مؤسسات متخصصة لتعزيز التعاون فيما بينها في مجال الأمن السيبراني وذلك بهدف تبادل المعلومات والخبرات والممارسات الفضلى، ومن أهمها وكالة الاتحاد الأوروبي لأمن الشبكات والمعلومات European Union Agency for Network and Information Security (ENISA)، التي تؤدي دور مركز الخبرة للاتحاد الأوروبي ولدوله وللقطاع الخاص فيه وللمواطنين الأوروبيين؛ وهي تقدم نصائح حول الممارسات الفضلى في السلامة المعلوماتية[46]، وتساعد دول الاتحاد الأوروبي على تطبيق إرشاداته وتحصين البنية الأساسية الحساسة للمعلومات والشبكات، وتعزيز قدرات الدول على تفادي المخاطر السيبرانية ومعالجتها. ولهذا الغرض، تقوم بجمع وتحليل البيانات، وبدراسة تقييم المخاطر وإدارتها، وبالتوعية وتعزيز التعاون بين القطاع العام والخاص[47].

---

41 http://www.lasportal.org/wps/wcm/connect/LAS/las/las_ar_aln/arab_legal_network_agreements/?WCM_Page.ResetAll=TRUE.

42 http://isper.escwa.un.org/FocusAreas/CyberLegislation/Projects/tabid/161/language/ar-LB/Default.aspx.

43 http://isper.escwa.un.org/Portals/0/Cyber%20Legislation/Regional%20Harmonisation%20Project/Directives/Directives-Full.pdf.

44 Stein Schjolberg, *The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva*, December 2008, http://www.cybercrimelaw.net/documents/cybercrime_history.pdf, p. 13, 15, 17.

45 http://opennetafrica.org/wp-content/uploads/researchandpubs/African%20Union%20Convention%20on%20Cyber Security%20&%20Personal%20Data%20Protection.pdf.

46 تستخدم بعض الدول العربية مصطلح السلامة المعلوماتية من أجل الدلالة على الأمان في الفضاء السيبراني أو بالإنكليزية Cybersafety.

47 http://www.enisa.europe.eu. ENISA, *Roadmap to provide more proactive and efficient Computer Emergency Response Team training*, http://www.enisa.europa.eu/activities/cert/support/exercise/roadmap-to-provide-more-proactive-and-efficient-cert-training.

وكما ذكر سابقاً تستضيف سلطنة عمان المركز الإقليمي للأمن الإلكتروني للمنطقة العربية، التابع للاتحاد الدولي للاتصالات، والذي يهدف إلى تقديم الخدمات والمبادرات للمنطقة العربية لتحسين قدرات الأمن الإلكتروني عن طريق التنسيق وتعزيز التعاون الإقليمي في هذا المجال[48].

باء- التوجهات التشريعية

1- تطبيق التشريعات التقليدية على الجرائم السيبرانية

من المؤكد أن إدخال أي تكنولوجيا جديدة يؤدي إلى ظهور تحديات قانونية جديدة. غير أنه من الممكن مع التطور التكنولوجي المعلوماتي تطبيق التشريعات التقليدية التي تركز على الأشياء الملموسة ضمن حدود معينة، على أن يصاحبها صياغة نصوص قانونية جديدة لتحكم مفاهيم جديدة غير ملموسة مثل البيانات والأنظمة المعلوماتية، حيث يصعب تحديد صاحب أو حائز المعلومة، ولا سيما على صعيد التجريم والاختصاص القضائي وإجراءات التحقيق والأدلة المعلوماتية. ويبدو من ردود الدول المُستفتاة، ضمن دراسة الأمم المتحدة، أن بعض الجرائم السيبرانية هي مجرّمة وفق النصوص العامة التقليدية، وأن هنالك جرائم سيبرانية أخرى جرى تجريمها بنصوص خاصة[49]. هذا، مع العلم أن النوع الثاني من الجرائم السيبرانية يخضع أيضاً للنصوص العامة وللنظرية العامة لقانون العقوبات في ما يتعلق بتحديد أركان الجريمة والمشتركين والمحاولة الجرمية وأسباب الدفاع المشروع وغيرها. ويبدو أن معظم الدول تحاول توسيع نطاق تطبيق تشريعاتها التقليدية لتشمل الفضاء السيبراني والجرائم السيبرانية. وعلى صعيد الدول العربية، يجهد القضاء لمحاولة تطبيق نصوص قانون العقوبات التقليدي على الجرائم السيبرانية لتدارك النقص في التشريعات السيبرانية.

2- ضرورة تحديث التشريعات

يقتضي التأكيد على أنه بغية تجريم بعض الأفعال بهدف حماية المعلومات والاتصالات في الفضاء السيبراني، يجب سن التشريعات الخاصة والواضحة قدر الإمكان، لا الاعتماد على تفسيرات ملتبسة للقانون العام[50]. ويتبين من ردود الدول المُستفتاة، ضمن دراسة للأمم المتحدة، أن النصوص القانونية المتعلقة بالجرائم السيبرانية ليست مقننة ضمن نص قانوني واحد، بل مبعثرة ضمن عدة قوانين هي: قوانين العقوبات، وقوانين جرائم تكنولوجيا المعلومات، وقوانين الإجراءات الجزائية، وقوانين التنصت، وقوانين الإثبات (البيّنات)، وقوانين الاتصالات الإلكترونية، وقوانين أمن أنظمة تكنولوجيا المعلومات، والقوانين حول البيانات الشخصية وحمايتها، وقوانين المعاملات الإلكترونية، وقوانين الأمن السيبراني، والقوانين حول التعاون الدولي. كما يتبين من ردود الدول أن العمل التشريعي موجه نحو تعزيز العمل على النواحي الأخرى للجرائم السيبرانية، غير التجريم، كالإجراءات وجمع الأدلة والتعاون الدولي. ويتبين أيضاً من الدراسة أن بعض الدول أصدرت قوانين إجرائية خاصة بجمع الأدلة المعلوماتية وحفظها وضمان مصداقيتها، في حين تطبق دول أخرى عليها ذات القوانين الإجرائية الجزائية المطبقة على الجرائم العادية[51].

---

48 جواب المركز الوطني للسلامة المعلوماتية بهيئة تقنية المعلومات على الاستبيان المرسل له من قبل الإسكوا في إطار هذه الدراسة، سلطنة عُمان، أيلول/سبتمبر 2014.

49 United Nations Office on Drugs and Crime, UNODC, *Comprehensive study on cybercrime*, draft, February 2013, p. 51, 52.

50 Stein Schjolberg, *The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva*, December 2008, http://www.cybercrimelaw.net/documents/cybercrime_history.pdf, p. 2.

51 United Nations Office on Drugs and Crime, UNODC, *Comprehensive study on cybercrime*, draft, February 2013, p. 53, 54.

ويبدو أن دولاً عديدة في العالم مازالت تعمل على تحديث تشريعاتها في الجانب الموضوعي وكذلك في الجانب الإجرائي، وذلك لضمان محاربة الجرائم السيبرانية. فبعض الظواهر الإجرامية ازدادت وتعاظمت الأضرار الجرمية الناتجة عنها، وأصبح من المفترض إعداد تشريعات خاصة لتجريمها. وهذه الظواهر تتمثل بالبريد الواغل spam (أو غير المرغوب فيه)، وسرقة الهوية، وتجريم الأعمال التحضيرية، وليس فقط في المحاولات الجرمية والهجمات السيبرانية المنسقة والهائلة ضد البنية الأساسية الحساسة وغيرها. وقد أضيفت إلى الجرائم السيبرانية الجرائم الخاصة بالعنف ضد المرأة والمطاردة والمضايقة على الفضاء السيبراني، وتبين الدراسات أن بعض الإجراءات المرتبطة بالجريمة السيبرانية قد تكون أيضاً موجودة في قوانين العنف المنزلي أو قوانين التحرش بالمرأة[52].

وتضيف بعض الدول على نصوص تجريم الجرائم السيبرانية ظروفاً مشددة للعقوبة في بعض الحالات، منها: ارتكاب الفعل بقصد جلب منفعة غير مشروعة أو بقصد الإضرار بالغير، والتسبب بضرر بالغ، والتسبب بفوضى عامة، ومحو البيانات أو تعديلها، وإعاقة عمل النظام المعلوماتي أو وقف بعض وظائفه، وتسهيل أو دعم الإرهاب، وإعاقة بنية أساسية حساسة، وارتكاب الفعل من قبل مجموعة منظمة، وتزامن الفعل مع سلوك عنيف.

ويقتضي التمييز، في نطاق تحديث التشريع، بين قوانين الجرائم السيبرانية التي تركز على قمع الفعل الجرمي بعد حدوثه وبين القوانين الناظمة للفضاء السيبراني أو قوانين تخفيض المخاطر السيبرانية، وهي قوانين استباقية تهدف إلى تخفيض المخاطر السيبرانية وجعل التحقيقات الجزائية أسهل في حال وقوع افعال جرمية؛ ومن الأمثلة على ذلك عمليات التصفية (الترشيح) على الإنترنت Filtering؛ وحماية البيانات وحفظها، والأعمال الاستباقية ضد البنية التحتية للمجرمين. وهذه الأعمال الاستباقية يجب أن تتم ضمن حدود عدم التعرض لحقوق الأفراد أو الاستخدام المفرط للقوة[53].

ويجب أن يتمتع التشريع بصفة الحياد التقني، بحيث يمكن تطبيقه في المستقبل على التقنيات الحديثة التي تؤدي ذات الوظائف. ويجب أن لا تحدد النصوص صراحة ما يعتبر من التجهيزات أنظمة معلومات أو أنظمة حاسوبية؛ ويعتبر هذا التوجه من الممارسات الجيدة، إذ يحول دون وقوع التقنيات المُستجدة خارج إطار النص القانوني، مما يحتم تعديله باستمرار[54].

أما على صعيد المنطقة العربية، فبالرغم من أن المنطقة العربية بطيئة في تحديث القوانين بشكل عام وقوانين الفضاء السيبراني بشكل خاص، إلا أن الدول العربية اهتمت بشكل جيد بمكافحة الجرائم السيبرانية وقد أصبح لدى العديد من الدول العربية قوانين خاصة بهذه الجرائم، وإن اختلفت مسميات هذه القوانين بين دولة وأخرى. وكما تبين دراسات الإسكوا الأخيرة[55] يوجد قوانين خاصة بالجرائم السيبرانية في كل من الأردن والإمارات العربية المتحدة والبحرين والمملكة العربية السعودية والجمهورية العربية السورية والسودان وعمان، بينما توجد مواد خاصة بالجرائم السيبرانية في التشريعات السيبرانية الأخرى في كل من تونس والمغرب، وتوجد مسودات لقوانين مرتبطة بالجرائم السيبرانية في كل من مصر ولبنان وفلسطين. وقد كانت

52 http://www.genderit.org/sites/default/upload/flowresearch_cnyst_legtrend_august22_1.pdf.

53 United Nations Office on Drugs and Crime, UNODC, *Comprehensive study on cybercrime*, draft, February 2013, p. 55.

54 United Nations Office on Drugs and Crime, UNODC, *Comprehensive study on cybercrime*, draft, February 2013, p. 14.

55 http://www.escwa.un.org/information/publications/edit/upload/E_ESCWA_ICTD_13_6_E.pdf, page 76.

البحرين من آخر الدول العربية التي أصدرت قانوناً خاصاً بـ "جرائم تقنية المعلومات" وهو القانون رقم 60 لسنة 2014 والذي صدر في 30 أيلول/سبتمبر 2014[56].

3- تنسيق التشريعات بين الدول

تناط بالمؤسسات الدولية مسؤولية تنسيق التشريعات السيبرانية بين الدول، وهذا التنسيق ممكن تحقيقه بفضل الاتفاقيات الدولية والتوصيات أو الإرشادات[57] الإقليمية أو الدولية.

وتوصي دراسة للأمم المتحدة بتنسيق التشريعات السيبرانية بين الدول بغية إنهاء وجود الملاذات الآمنة للمرتكبين وضمان جمع الأدلة المعلوماتية، باعتبار أن بعض الدول تشترط التجريم المتبادل للفعل Dual criminality من أجل التعاون قضائياً[58]. وتظهر اختلافات فيما يتعلق بمعظم الجرائم السيبرانية على صعيد تقدير خطورتها، ومن ثمّ تحديد عقوبتها، وكذلك على صعيد العناصر المكونة لها. فمثلاً تربط بعض الدول جرم الدخول غير المشروع إلى نظام معلوماتي بإحداث ضرر أو تغيير بيانات أو بأن يتم ذلك بصورة قصدية أو احتيالية أو دون حق؛ وتربط بعض الدول جرم اعتراض البيانات بكون البيانات غير عامة أي غير مباحة للجمهور أو أن الاعتراض يجري بوسائل تقنية. كما تثار إشكاليات قانونية بين الدول حول بعض الجرائم السيبرانية، مثل جرم إساءة استخدام تجهيزات معلوماتية، من حيث التفريق بين ما هو محاولة جرمية معاقب عليها وما هو عمل تحضيري غير معاقب عليه، ومن حيث ازدواجية استعمال التجهيزات المعلوماتية المباحة بطبيعتها في عمل مشروع أو عمل جرمي، وكذلك فيما يتعلق بتطبيق النصوص التقليدية على جريمة الاحتيال المعلوماتي إذا كانت مرتكبة من قبل المحتال ضد نظام معلوماتي وليس شخص، فإذا لم يلحظ النص هذه الفرضية، فيجب تعديله[59].

ويتبين من دراسة للأمم المتحدة أن معظم الجرائم السيبرانية المعروفة هي مجرّمة في معظم الدول، باستثناء جرائم البريد الواغل، وبدرجة أقل جرم إساءة استعمال التجهيزات المعلوماتية، والعنصرية عبر الإنترنت، وجرم استدراج الأطفال عبر الإنترنت[60]. ومن المفترض أن يؤدي التشريع إلى ضمان تطبيق تدابير فعالة للأمن السيبراني، مثل إعطاء السلطات المختصة الصلاحيات والوسائل الضرورية لتطبيق الدفاع، في الفضاء السيبراني، عن الوظائف الحيوية للمجتمع[61].

وبهدف تنسيق تشريعات الجرائم السيبرانية على مستوى المنطقة العربية، أعدت الإسكوا الإرشاد الخاص بالجرائم السيبرانية والذي يحدد أنواع هذه الجرائم[62] والتي تم حصرها بـ 51 نوع (مادة)، أما الاتفاقية العربية لمكافحة جرائم تقنية المعلومات فقد حددت 13 جريمة عامة خاصة بتقنية المعلومات.

---

56 http://www.legalaffairs.gov.bh/Media/LegalPDF/K6014.pdf.

57 Stein Schjolberg, *The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva*, December 2008, http://www.cybercrimelaw.net/documents/cybercrime_history.pdf, p. 1.

58 United Nations Office on Drugs and Crime, UNODC, *Comprehensive study on cybercrime*, draft, February 2013, p. 56, 60.

59 ITU, Marco Gercke, *Understanding Cybercrime: Phenomena, Challenges and Legal Response,* September 2012, p. 217.

60 United Nations Office on Drugs and Crime, UNODC, *Comprehensive study on cybercrime*, draft, February 2013, p. 77.

61 Secretariat of the Security and Defense Committee, *Finland's Cyber security Strategy*. http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf, p. 10.

62 http://isper.escwa.un.org/Portals/0/Cyber%20Legislation/Regional%20Harmonisation%20Project/Directives/Dir-5-Cybercrimes.pdf.

4- التوازن في التشريع والتنسيق مع الإجراءات التنظيمية

لعل الإشكالية تكمن أيضاً في التوازن بين حماية الأشخاص والممتلكات والبنية الأساسية، والحاجة إلى احترام حقوق الملكية والحقوق المدنية[63]؛ إذ أن زيادة الرقابة على الإنترنت بغرض ضمان الأمن السيبراني يمكن أن يساء استخدامه لمراقبة الأشخاص والتعرض لخصوصياتهم. ومن أجل احترام خصوصية الأفراد، تفرض القوانين في العالم، في معرض الإجراءات الجزائية، قيوداً على بعض البيانات وفق طبيعتها وكيفية الوصول إليها، ووجوب عدم إفشائها من قبل المحققين، وتُلزم، في حالة بعض الإجراءات، بالحصول على إذن قضائي، كما تحدد نطاق الإجراء في الزمان والمكان في ما يخصّ الأشخاص.

ويجب أن يضمن التشريع الذي يحكم أي تصرف غير مشروع على الإنترنت أن السلوكيات "على الخط" online تتم معالجتها بطريقة متوازية مع تلك التي تجري "خارج الخط" offline، في ظل حياد تقني، وفي ظل احترام الخصوصية والحريات الخاصة. ويجب إعطاء الأهمية لمتطلبات تطبيق القانون وتحدياته الناشئة عن الإنترنت، ولا سيما في ما يتعلق بالموارد والتدريب والحاجة إلى خبرات وأدوات تحقيق جديدة، والتعاون بين جهات تطبيق القانون المحلية، ومع الشركاء الدوليين. ويجب أن يكون هناك دعم مستمر لدور القطاع الخاص فيما يتعلق بسلوكيات التعامل وتطوير وسائل تقنية ملائمة والعمل على تثقيف وتوعية مستخدمي الإنترنت لمنع مخاطر النشاطات غير المشروعة على الإنترنت أو للتقليل منها[64]. وقد أوصى مؤتمر القمة العالمية لمجتمع المعلومات الدول بوضع تشريعات تضمن التحقيق وملاحقة جرائم المعلوماتية، كما أوصى باتخاذ التدابير الملائمة لضمان استقرار الإنترنت وسلامتها ومحاربة الجرائم السيبرانية، في ظل احترام الخصوصية وحرية الرأي.

جيم- التوجهات الخاصة بتطبيق القانون والتنظيم

1- وضع سياسة خاصة بالأمن السيبراني

من أولى الخطوات على الصعيد التنفيذي في مجال الأمن السيبراني ومكافحة الجرائم السيبرانية ضرورة وضع سياسة شاملة وعامة من قبل الدولة أو الأجهزة المختصة فيها. وتتضمن هذه السياسة المتطلبات الخاصة بالأمن السيبراني وإجراءاته، والوسائل المعلوماتية والمادية المطبقة، وتدابير الحماية التقنية والتنظيمية والتشغيلية، وكيفية التصرف في مكافحة المخاطر السيبرانية والتبليغ عنها وتقديم الدعم للضحايا. ويجب التوعية بهذه السياسة وتعميمها على إدارات الدولة وعلى الأفراد والشركات.

يتبين من الدراسة التي أعدها مكتب الأمم المتحدة المعني بالمخدرات والجريمة حول الجرائم السيبرانية في العالم[65] أن 70 في المائة من الدول المُستفتاة لديها سياسة، ولو جزئية، للوقاية من الجرائم السيبرانية، أو أنها قيد الإعداد؛ ويدخل ضمنها التوعية والتعاون الدولي وتطبيق القانون. وتنخفض هذه النسبة في المنطقة

63 Steven Titch, *Four principles for effective cybersecurity law and policy*, 25 April 2014, http://www.rstreet.org/2014/04/25/four-principles-for-effective-cybersecurity-law-and-policy, P. 2.

64 A working group established by the U.S. President, *The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet,* March 2000, Stein Schjolberg, *The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva*, December 2008, http://www.cybercrimelaw.net/documents/cybercrime_history.pdf, p. 7.

65 United Nations Office on Drugs and Crime, UNODC, *Comprehensive study on cybercrime*, draft, February 2013, p. 225, 226, 233.

العربية. وقد أفادت 50 في المائة من الدول أن استراتيجياتها تتضمن بناء شراكة مع القطاع الخاص في مجال الأمن السيبراني، وقد ترتكز هذه الشراكة غالباً على تفاهمات غير رسمية، أو رسمية أحيانا، وكذلك بناء على قرارات وزارية أو على التشريع. ويكون موضوع الشراكة: تبادل المعلومات والحالات والمساعدة، والتوعية، وتبادل الممارسات الفضلى للوقاية، وتطوير الحلول التقنية، والتعاون الدولي، والمساعدة في وضع السياسات. ومن الضروري أن تتضمن الخطة الوطنية للأمن السيبراني أهداف وأولويات محددة.

وكمثال على سياسات الأمن السيبراني، يمكن ذكر استراتيجية المملكة المتحدة للأمن السيبراني، التي نشرتها في 25 تشرين الثاني/نوفمبر 2011 واعتمدت بموجبها خطة للوقاية من الجرائم السيبرانية، حيث صنّفت الأمن السيبراني من ضمن أولويات الأمن الوطني. ويمكن للدول الأخرى الاسترشاد بالخطوط العريضة لهذه الخطة الموضحة في الإطار 3.

ووفق دراسة الأمم المتحدة وبناء على الممارسات الجيدة في مجال وضع السياسات الوطنية للأمن السيبراني، يمكن أن تتضمن هذه السياسات: إصدار التشريعات، والقيادة الفعالة، وتطوير قدرات القضاء الجزائي وأجهزة تطبيق القانون، والتعليم والتوعية، وتطوير قاعدة معلومات، والتعاون بين الحكومة والمجتمعات والقطاع الخاص، ومع باقي الدول والمنظمات. ومن الضروري وجود خطة وطنية للوقاية من الجرائم السيبرانية مع أهداف وأولويات محددة[66]، ويبين الإطار 4 أمثلة عن بعض تجارب الدول في وضع سياسة وطنية للأمن السيبراني.

الإطار 3- استراتيجية المملكة المتحدة للأمن السيبراني

تتضمن الاستراتيجية الوطنية للأمن السيبراني في المملكة المتحدة ما يلي:

- إنشاء مركز للاستجابة السريعة لطوارئ الحاسوب CERT-UK؛
- وضع منهجيات للاستجابة للحوادث السيبرانية Cyber Incident Response scheme، لمساعدة الشركات على تدارك الهجمات السيبرانية؛
- إنشاء وحدة وطنية للجريمة السيبرانية National Cyber Crime Unit في عام 2013 ضمن الوكالة الوطنية للجرائم، وتدريب الشرطة على تحقيقات الجرائم السيبرانية وإنشاء وحدات متخصصة بذلك في كل منطقة؛
- توفير المشورة الفنية في مجال الأمن السيبراني للمؤسسات والجمهور، على شكل إرشادات وكتيبات؛
- إرساء شراكة في مجال أمن المعلومات السيبراني مع المؤسسات، لتبادل المعلومات حول المخاطر؛
- اعتماد إرشادات لتثقيف وحماية الزبائن من المخاطر، بالتعاون مع مزودي خدمات الشبكة، وبخاصة مزودي خدمات الاتصال ISP؛
- تطوير مبادئ حول حماية المؤسسات نفسها Cyber Essentials scheme من المخاطر السيبرانية؛
- إنشاء نظام معلوماتي موحد للتبليغ "7/24" عن الجرائم السيبرانية ذات الطابع المالي، وهو ما يسمح بتشارك المعلومات حولها وتحليلها؛
- دعم صناعات البرمجيات والتجهيزات الخاصة بالحماية من المخاطر السيبرانية؛

66 United Nations Office on Drugs and Crime, UNODC, *Comprehensive study on cybercrime*, draft, February 2013, p. 225, 226, 233.

الإطار 3 (تابع)

- التعاون مع الدول الأخرى لتحديد وإدارة المخاطر السيبرانية، ووضع قواعد تصرف للدول والمؤسسات[أ]؛
- العمل مع مزودي خدمات الشبكة لمساعدة المستخدمين لتحديد النشاطات غير المشروعة المتعلقة بأنظمتهم المعلوماتية، ومن ثم الحماية منها؛
- العمل مع الشركات التي تملك وتدير البنية الأساسية بحيث تصبح المعلومات والأنظمة أكثر أمناً؛
- اعتماد مؤشرات للمستهلك بخصوص منتجات الأمن السيبراني الجيدة؛
- العمل على تخفيف مكامن الضعف في الأنظمة المعلوماتية للدولة وبنيتها الأساسية الحساسة؛
- زيادة عدد المتخصصين في الأمن السيبراني؛
- العمل مع مزودي خدمات الشبكة لدراسة إمكانية تطبيق عقوبات فورية على الخط online على الانتهاكات على الخط[ب].

أ Cabinet Office, Office of Cyber Security and Information Assurance, *Keeping the UK safe in cyber space*, https://www.gov.uk/government/policies/keeping-the-uk-safe-in-cyberspace, p. 3, 4, 5.

ب Cabinet Office, *The UK Cyber Security Strategy, Protecting and promoting the UK in a digital world,* November 2011, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf, p. 23, 31.

الإطار 4- بعض تجارب الدول في وضع سياسة وطنية للأمن السيبراني

1- التجربة الروسية

أطلقت روسيا مبادئ أساسية لتحقيق تعاون دولي أكثر فعالية في مكافحة الجرائم السيبرانية، وهذه المبادئ هي: أهمية وضع معاهدة للتعاون في محاربة الجرائم السيبرانية ضمن إطار الأمم المتحدة، وتعزيز التعاون مع تجمعات الدول الكبرى، وزيادة تبادل المعلومات بين الأجهزة الرسمية في مجال التحقيقات، وتعزيز آليات تبادل المعلومات حول تقنيات التحقيق والممارسات القضائية[أ].

2- التجربة الأمريكية

يتبين من التجربة الأميركية أنه ليس من الضروري الاختيار بين حرية سير المعلومات وأداء الشبكة من جهة، وأمن شبكاتها من جهة أخرى. فأفضل الحلول السيبرانية هي متحركة، وقابلة للتكييف، مع تأثير ضئيل على أداء الشبكة. فهناك أدوات تؤمن الأنظمة من دون تعطيل الابتكار وقمع حرية التعبير أو التجمع أو إعاقة الربط العالمي بين أنظمة المعلومات. وفي الحقيقة، فإن الأمن السيبراني الجيد يعزز الخصوصية، والعدالة الفعالة تحمي الحريات الأساسية[ب]. ولعل من الأفضل إقرار تشريعات لمحاربة النشاطات غير المشروعة للجريمة السيبرانية بدلاً من تقييد وصول الأفراد إلى الإنترنت، والعمل على منع المجرمين من استعمال الإنترنت في نشاطاتهم.

ويمكن الاسترشاد بالتجربة الأميركية، إذ أوصت الإدارة الأمريكية في عام 2011 في تقريرها حول "استراتيجية وطنية لهويات موثوق بها في الفضاء السيبراني" باعتماد نظام للهوية الإلكترونية، حيث يلتزم الأفراد والمؤسسات بمعايير وقواعد معينة لتوثيق هوياتهم على الإنترنت، وهو ما يوفر أماناً أكبر للمعاملات الإلكترونية، ويصعب الأمر على المرتكبين، ويساعد في كشف هوية المجرمين[ج].

الإطار 4 (تابع)

ويتبين أيضاً من التقرير الصادر عن الإدارة الأمريكية في أيار/مايو 2011 حول "استراتيجية دولية حول الفضاء السيبراني: ازدهار وأمان وانفتاح في عالم مترابط" أن الاستراتيجية الأمريكية تتمحور حول ضمان الحريات الأساسية والخصوصية وحرية سير المعلومات مع ضمان أمن الشبكات ووضع قواعد دولية للتصرف وتعزيز الربط بين الأنظمة المعلوماتية والتحقيق في الجرائم السيبرانية وملاحقة مرتكبيها وتعزيز التعاون الدولي ووضع استراتيجية دولية[ج].

3- التجربة الأسترالية

تعتمد التجربة الأسترالية مقاربة تستند إلى المبادئ التالية: فهم المشكلة الحقيقة عن طريق جمع المعلومات الكافية، والشراكة وتحمل المسؤولية بين القطاعين العام والخاص والأفراد، والتركيز على الوقاية باعتبارها أسهل وأقل كلفة، وإيجاد توازن بين الحماية وبين الخصوصية والحرية على الإنترنت[هـ].

4- التجربة الأسترالية

تعتمد التجربة الأسترالية مقاربة تستند إلى المبادئ التالية: فهم المشكلة الحقيقة عن طريق جمع المعلومات الكافية، والشراكة وتحمل المسؤولية بين القطاعين العام والخاص والأفراد، والتركيز على الوقاية باعتبارها أسهل وأقل كلفة، وإيجاد توازن بين الحماية وبين الخصوصية والحرية على الإنترنت[و].

أ *Basic principles for State Policy of the Russian Federation in the field of International Information Security to 2020,* Press release, 16 September 2013, http://www.veleposlanistvorusije.mid.ru/doc/pr_20130916_en.pdf, p. 6, 7.

ب The White House, *International Strategy for Cyberspace, Prosperity, security and Openness in a networked World*, May 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, p. 9.

ج The White House, *National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy*, April 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

د The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a NetworkedWorld*, May 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf.

هـ Australian Government, Attorney General's Department, *National Plan to Combat Cybercrime*, http://www.ag.gov.au/CrimeAndCorruption/Cybercrime/Documents/National%20Plan%20to%20Combat%20Cybercrime.pdf, p. 7.

و Australian Government, Attorney General's Department, *National Plan to Combat Cybercrime*, http://www.ag.gov.au/CrimeAndCorruption/Cybercrime/Documents/National%20Plan%20to%20Combat%20Cybercrime.pdf, p. 7.

2- إنشاء المحاكم وأجهزة التحقيق المتخصصة

في ما يخصّ تطبيق التشريعات السيبرانية، هناك حاجة إلى وجود جهاز تحقيق رسمي متخصص يضطلع بدور مهم من ناحية إجراء التحقيقات في الجرائم السيبرانية، وكذلك في الجرائم التقليدية التي تستند إلى أدلة معلوماتية معقدة. ويجب أن يكون الهدف من وجود هذا الجهاز تدعيم إجراءات التحقيق، التي هي قانونية في المبدأ، بخبرات فنية تمكنها من جمع الأدلة الرقمية من مسرح الجريمة أو من خارجه وحفظ هذه الأدلة مع ضمان موثوقيتها وصدقيتها وتحليلها واستخراج الاستنتاجات القانونية منها وتقديمها للقضاء ضمن تقرير متكامل، مع تقديم الشروح اللازمة عنها عند الضرورة. ويجب أن يتكون هذا الجهاز من فنيين متخصصين في مختلف فروع تكنولوجيا المعلومات، كالشبكات المعلوماتية والتجهيزات المعلوماتية وقواعد المعلومات وبرامج الحماية وجدران الحماية Firewall والأمن السيبراني وغيرها من البرامج. ويمكن لكل قسم من أقسام الشرطة الاستعانة بهذا الجهاز المتخصص في التحقيقات التي يجريها، والمتضمنة الأدلة المعلوماتية.

ويتبين، وفق دراسة أجرتها الأمم المتحدة، أن 90 في المائة من الدول قد أنشأت أو تعمل على إنشاء وحدات متخصصة في تحقيقات الجرائم السيبرانية والأدلة المعلوماتية، مع العلم أن عدد عناصرها لا يتجاوز في معظم الدول، حتى المتقدمة منها، 1 في المائة من مجموع أفراد الشرطة[67]. ويبدو أن معظم الدول العربية قد أقامت مكاتب متخصصة للتحقيق في الجرائم السيبرانية[68].

ويفترض أيضاً تدريب العناصر غير المتخصصة من الشرطة على المهارات الأساسية في مجال الأدلة الجنائية المعلوماتية، باعتبارها قد تدخل ضمن إطار أي تحقيق جزائي متعلق حتى بجريمة تقليدية. ومن المتعارف عليه أن يتولى التدريب في هذه الحالة عناصر متخصصون من الشرطة نفسها.

يواجه القضاء تحديات عديدة لملاحقة الجرائم السيبرانية، منها ما يتعلق بالتشريعات السيبرانية وتطبيقها، وأخرى تتعلق بالأدلة المعلوماتية، وكذلك ما يتعلق بصعوبة جمع هذه الأدلة من الخارج، وأيضاً ما يتعلق باسترداد المتهمين.

ويتبين وفق دراسة للأمم المتحدة أن 60 في المائة من الدول المُستفتاة قد أنشأت نيابات عامة أو محققين متخصصين لملاحقة الجرائم السيبرانية، ويتمتعون بمستوى عال من التخصص في الدول المتقدمة، على عكس أقرانهم في الدول النامية، حيث لا تتوفر لدى المحقق أحياناً أية تجهيزات معلوماتية أو أية خبرة معلوماتية. أما في ما يخصّ المحاكم، فيتبين من الدراسة أن 10 في المائة فقط من الدول قد أنشأت محاكم متخصصة في الجرائم السيبرانية، في حين تتولى المحاكم العادية في الدول الباقية الحكم في هذه القضايا، ولم يتلق القضاة فيها، في 40 في المائة من الدول، أي تدريب على مكافحة الجرائم السيبرانية والأدلة المعلوماتية[69]. ويفترض بالقاضي المتخصص في هذه الحالة فهم المفاهيم التقنية والإنترنت ومعرفة قوانين المعلوماتية والأدلة المعلوماتية. وفي الخلاصة، يجب أن يكون لدى أي دولة جهاز شرطة يملك قدرات للحد من الجرائم السيبرانية وكشفها وحلها[70].

وتجدر الإشارة إلى أنه، على صعيد دول المنطقة العربية، لا يوجد حتى الآن محاكم متخصصة في الجرائم السيبرانية، بينما يوجد بعض مراكز الشرطة التي تحقق في الجرائم السيبرانية (انظر الفصل الثاني- دال).

3- استعمال الأدلة الرقمية في التحقيقات الجزائية

من الطبيعي القول إن أنسب الأدلة لإثبات الجرائم السيبرانية هي الأدلة المعلوماتية أو الرقمية أو الإلكترونية، إلا أن إثبات هذه الجرائم لا يقتصر على هذ النوع من الأدلة، فمن الممكن إثباتها بأدلة تقليدية كالاستجواب والشهود والاعتراف وغيرها. ويجب التنويه إلى أن الأدلة المعلوماتية تؤدي دوراً كبيراً في يومنا هذا في إثبات جرائم تقليدية كالقتل والسرقة وغيرها.

---

67 United Nations Office on Drugs and Crime, UNODC, *Comprehensive study on cybercrime*, draft, February 2013, p. 152, 154.

68 أنظر: المرفق الخامس من هذه الدراسة المتعلق بنتائج الاستبيان المُرسل لدول المنطقة في إطار هذه الدراسة.

69 United Nations Office on Drugs and Crime, UNODC, *Comprehensive study on cybercrime*, draft, February 2013, p. 172.

70 Secretariat of the Security and Defense Committee, *Finland's Cyber security Strategy*. http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf, p. 8.

ومن أجل الحصول على الأدلة الرقمية وضبطها يجب اتباع الإجراءات القانونية المنصوص عليها في القانون (قانون أصول المحاكمات الجزائية أو غيره من القوانين) وذلك عند التفتيش من قبل الأشخاص المختصين والمخولين قانوناً بجمع الأدلة وهو ما يدعى بالضابطة العدلية. ويتم التحقق عادةً من صحة الدليل عن طريق السلامة الفنية للإجراءات المستخدمة في الحصول عليه، وعن طريق التأكد من سلامة الدليل الرقمي من العبث الفني (فكرة التحليل التناظري الرقمي، حيث تتم مقارنة الدليل الرقمي المقدم للقضاء بالأصل المحفوظ في الحاسوب أو بواسطة استخدام خوارزميات خاصة، أو بتقنية الدليل المحايد)[71].

ومن ثم يجري العمل على تحليل الدليل المعلوماتي في مختبر متخصص يتم إنشاؤه لهذه الغاية، ويمكن بناؤه في بيئة افتراضية Virtual Environment على نظامي التشغيل ويندوز ولينكس، وذلك نظراً لوجود برامج مختلفة للتحقيق الجنائي المعلوماتي على كل من نظامي التشغيل؛ هذا مع العلم أن أدوات التحقيق الجنائي المعلوماتي لا تحتاج غالباً إلى موارد كبيرة، ويمكن للدول ذات الإمكانات المحدودة، كما هو الوضع في بعض دول المنطقة، أن تمولها ذاتياً[72].

4- مراكز الاستجابة لطوارئ الحاسوب

عمدت الدول المتقدمة إلى إنشاء مركز للاستجابة السريعة لطوارئ الحاسوب Computer Emergency Response Team (CERT). ويشكل المركز الأداة الأساسية لحماية البنية الأساسية الحساسة للمعلومات؛ ومن مهامه العمل بسرعة على رصد المخاطر المعلوماتية المستجدة، مثل الفيروسات والديدان وبرامج التجسس ومكامن الضعف في الأنظمة التشغيلية، والتعامل معها، وإعطاء الحلول والتدابير اللازمة بشأنها، ونشر المخاطر المعلوماتية على موقعه على الإنترنت، وإطلاق حملات إعلامية عنها، وتحذير المواطنين منها، وإعطائهم الإرشادات والتوجيهات حول سبل حماية أنظمتهم المعلوماتية وبياناتهم، وتنفيذ برامج توعية شاملة للمواطنين. وتتعاون في بعض الدول مراكز الاستجابة لطوارئ الحاسوب مع بعض المؤسسات المتخصصة، كمكاتب المدعين العامين أو أجهزة التحقيق القضائي المتخصصة أو مراكز الأبحاث والجامعات، من أجل إعداد قواعد سلوكية للأفراد والشركات لاتّباعها بغية حماية أنظمتهم المعلوماتية وبياناتهم.

وتهدف مراكز الاستجابة لطوارئ الحاسوب أيضاً إلى تمكين الأفراد والشركات من استباق الهجمات السيبرانية وتفادي الأضرار قبل حدوثها؛ كما يهدف إلى تثقيفهم تقنياً لحماية حواسيبهم من حوادث قد لا توصف بالجرائم، مثل الأعطال التقنية، وإلى التعرف على مكامن الضعف في الأنظمة التشغيلية والبرامج المعلوماتية، وتوضيح متطلبات تحديث البرامج والربط بينها.

ويبدو أن العديد من الدول العربية قد أنشأت هذا النوع من المراكز أو هي في طور إنشائه[73] (انظر الفصل الثاني- هاء).

---

71 أنظر: طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي، ص 17. www.startimes.com/f.aspx?t=30245909.

72 مقدمة لمراحل التحقيق الجنائي الرقمي ومراحله، ص 5. http://www.ofpcss.com/2014/04/Introduction-of-the-stages-of-the-criminal-investigation-and-the-steps.html.

73 أنظر المرفق الخامس من هذه الدراسة المتعلق بنتائج الاستبيان المُرسل لدول المنطقة في إطار هذه الدراسة.

دال- التوجهات الخاصة بالتعاون بين الدول

1- التعاون القضائي الرسمي وغير الرسمي بين الدول

توصي دراسة الأمم المتحدة بضرورة إيجاد آليات رسمية وغير رسمية للتعاون القضائي بين الدول، إما بموجب اتفاقيات دولية أو ثنائية، أو بموجب القانون الوطني، أو وفق مبدأ المعاملة بالمثل، وذلك تفادياً للتعرض لسيادة الدول. إذ قد يكون من الضروري تمكين الدول من القيام بأعمال تحقيق في أراضي دول أخرى، باعتبار أن 50 في المائة من الدول المُستفتاة أفادت بأن أكثر من 50 في المائة من الجرائم السيبرانية تتضمن عنصراً دولياً. ويبدو أن الآليات الرسمية للتعاون هي الطاغية، إلا أنها تتطلب وقتاً قد يصل إلى عدة أشهر في حالة استرداد المجرمين. كما يمكن الاستفادة من خدمة "7/24" للتعاون بين الدول بواسطة مكاتب الإنتربول الموجودة فيها.

أما في نطاق الآليات غير الرسمية للتعاون، فيجري عادة تعيين نقطة اتصال من كل جهة، ويتم الاتصال مباشرةً بين وحدات الشرطة لتبادل المعلومات والمستندات، ولتحديد أماكن وجود المتهمين والشهود، ولإجراء المقابلات. ويُتبع الإجراء غير الرسمي بإجراء آخر أكثر رسمية؛ وهذا ما تنص عليه اتفاقية بودابست والاتفاقية العربية لمكافحة جرائم تقنية المعلومات من حيث إجراء المراسلة غير الرسمية التي تتبع بتأكيد رسمي.

ووفقاً لدراسة الأمم المتحدة[74] تشكل الآليات الرسمية 70 في المائة من تبادلات التعاون واستناداً إلى اتفاقيات ثنائية في أغلب الأحيان (60 في المائة من الحالات)، في حين تشكل حالات استعمال خدمة "7/24" 6 في المائة. ويشكل التعاون غير الرسمي مباشرةً بين أجهزة الشرطة 9 في المائة، في حين يشكل الاتصال المباشر مع مزود خدمات الشبكة 8 في المائة. غير أن طلبات التعاون والاسترداد قد أكدت رسمياً وفق ما أفادت به الدول المستفتاة، والتي استعمل بعضها (50 في المائة) البريد الإلكتروني أو الفاكس أو الأنظمة المعلوماتية على الخط (5 في المائة) في هذه الطلبات. وقد أفادت 70 في المائة من دول آسيا أن التعاون غير الرسمي ممكن لديها عن طريق اتفاقيات ثنائية أو إقليمية أو عن طريق الإنتربول أو شبكات التعاون القائمة.

وإضافة إلى التعاون في مجال التحقيقات القضائية، يهدف التعاون الدولي أيضاً إلى تبادل المعلومات والدروس المستفادة من التجارب والممارسات الفضلى في دول أخرى لرفع مستوى الأمن السيبراني في الدولة[75].

إن الهدف الأساسي من آليات التعاون غير الرسمية هو تفادي البيروقراطية وتفادي ضياع الأدلة المعلوماتية السريعة الزوال. وتخضع طلبات التعاون إلى شروط موضوعية تتعلق بتجريم الأعمال المرتكبة في مختلف الدول وهو ما يدعى بـ "التجريم المزدوج" وإلى شروط إجرائية ملائمة. وقد أنشأت اتفاقية بودابست شبكة تعاون "7/24"، وكذلك فعلت مجموعة الدول الصناعية G8. وتجدر الإشارة إلى اتفاقية الأمم المتحدة حول الجريمة المنظمة العابرة للدول[76] وبروتوكولاتها الثلاثة التي تتضمن آليات للتعاون، وهي غير مخصّصة

---

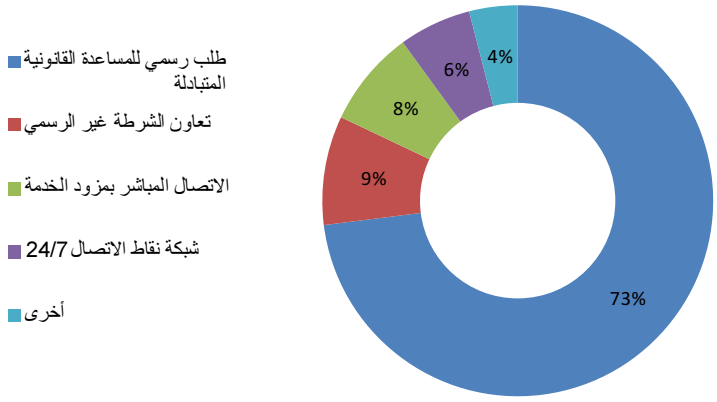
74 United Nations Office on Drugs and Crime, UNODC, *Comprehensive study on cybercrime*, draft, February 2013, p. 55, 187, 197, 201, 210.

75 Secretariat of the Security and Defense Committee, *Finland's Cyber security Strategy*. http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf, p. 9.

76 .http://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-a.pdf

للجرائم السيبرانية، ولكنها قابلة للتطبيق في هذا السياق على الجرائم التي ترتكبها مجموعات منظمة، وتكون داخلة ضمن نطاق الاتفاقية.

الشكل 2- طرق الحصول على أدلة من خارج إقليم الدولة (مصدر)



المصدر: United Nations Office on Drugs and Crime, UNODC, *Comprehensive study on cybercrime*.

2- تنازع الاختصاص القضائي

غالباً ما تدخل الأفعال الجرمية المرتكبة ضمن الاختصاص القضائي لعدة دول، إذ أن الفضاء السيبراني لا يلتزم بالحدود الجغرافية. ويتم تحديد الاختصاص القضائي لدولة ما بالأفعال الجرمية التي تقع ضمن إقليمها أو بالأفعال التي يرتكبها مواطنوها خارج أراضيها (مبدأ الجنسية الإيجابية "Principle of active nationality") أو تقع على مواطنيها في الخارج (مبدأ الجنسية السلبية "Principle of passive nationality")، أو بالأفعال الجرمية التي تطال مصالحها الأساسية كدولة. ويكفي في بعض الأحيان توفر أحد عناصر الفعل الجرمي أو أحد آثاره أو نتائجه الجرمية أو نظام معلوماتي أو بيانات ضمن الإقليم الوطني لربط اختصاص المحاكم الوطنية. ويكفي لربط اختصاص المحاكم الإقليمي أن يكون أحد عناصر الفعل الجرمي قد حصل في إقليم الدولة، كالنتيجة الجرمية مثلاً، ويسمى ذلك "مبدأ الإقليمية الموضوعية" "Principle of objective territory"، ويثير ذلك تنازع الاختصاص القضائي بين محاكم عدة دول. فعلى سبيل المثال، يكفي استعمال البنية الأساسية لدولة ما، كاستضافة البيانات أو تقديم خدمة البريد الإلكتروني أو تقديم خدمات الاتصالات ونقل المعلومات، ولو انتقاليا، لتعتبر الجريمة ضمن الدولة حتى ولو كان المجرم أو الضحية خارجها. كما يمكن في بعض الدول إعطاء المحاكم صلاحية النظر في الأفعال الجرمية التي تمس مصالح المجتمع الدولي (مبدأ العالمية Principle of universality)، كالجرائم ضد الإنسانية أو جرائم الحرب أو جرائم الاتجار بالبشر أو الاستغلال الجنسي للمرأة خلال فترة الأزمات والحروب. ويتم حل النزاعات حول الاختصاص القضائي بين الدول بالتشاور بالطرق الرسمية أو غير الرسمية. وتقدر دراسة الأمم المتحدة أن بين 30 و70 في المائة من الجرائم السيبرانية تتضمن عنصراً دولياً[77].

77 United Nations Office on Drugs and Crime, UNODC, *Comprehensive study on cybercrime*, draft, February 2013, p. 183, 189 236, 237, 238.

هاء- التوجهات التقنية والإدارية الأخرى

1- التوجهات التقنية الخاصة بمزودي خدمات الشبكة والشركات

كما ذكر سابقاً، فقد أفادت 50 في المائة من الدول أن استراتيجياتها تتضمن بناء شراكة مع القطاع الخاص في مجال الأمن السيبراني. وتتضمن بنود هذه الشراكة: تبادل المعلومات والحالات والمساعدة، والتوعية، وتبادل الممارسات الفضلى للوقاية، وتطوير الحلول التقنية، والتعاون الدولي، والمساعدة في وضع السياسات.

ويمكن التعاون أيضاً مع مزودي خدمات الاتصال Internet Service Provider (ISP) من أجل حجب بعض المواقع غير المشروعة أو منع نقل البيانات التي ترد من عناوين إلكترونية مشبوهة، إذ أن كل رزمة بيانات packet تحمل ترويسة header تتضمن العنوان الرقمي للمصدر. ويؤدي مزودو خدمات الاتصال دوراً حيوياً أيضاً في حفظ سجلات الدخول لزبائنهم والبيانات الشخصية عنهم (الاسم، العنوان، رقم الهاتف) ومنع المحتوى غير المشروع، ومساعدة الزبائن في اكتشاف الحواسيب المعرضة للخطر أو الملوثة (مثل حالة Botnet)، وإعلامهم، وضمان اتصالات آمنة وتصفية البيانات المنقولة على الإنترنت Internet traffic، مثل البريد الواغل والبرمجيات الخبيثة والمحتوى غير المشروع، وعدم تمريرها. كما يمكن لشركات استضافة البيانات والمواقع ممارسة رقابة على الخدمات المقدمة من المواقع المُستضافة لديهم (محتوى غير مشروع، أو مخالف لقوانين الملكية الفكرية)، ومنع الاستخدام غير المشروع لهذه الخدمات. علماً أنه يمكن دوماً لمرتكبي مثل هذه الأعمال إخفاء هويتهم باستخدام خدمات شركات لا تتطلب التسجيل أو العمل من دول لا تفرض حفظ معلومات حركة البيانات. وقد اتخذت بعض شركات تكنولوجيا المعلومات خطوات استباقية، قانونية وغيرها، لمكافحة الجرائم السيبرانية.

تجدر الإشارة إلى أنه وفق المبادئ القانونية السائدة عالمياً، ليس هناك، من إلزام بالرقابة على المعلومات وذلك نظراً للحجم الهائل للبيانات المنقولة، ولا توجد مسؤولية على مزود خدمات الاتصال إلا في حال امتناعه عن وقف البيانات أو سحبها بناء على قرار قضائي أو بناء على طلب مرسل البيانات. وكذلك لا يوجد إلزام على مزودي خدمات الاتصال بالرقابة على البيانات المخزنة إلا إذا علم بطابعها غير المشروع الظاهر.

ومن الأمور التقنية المطروحة أيضاً، إلزام شركات تكنولوجيا المعلومات بتطبيق معايير أمن المعلومات والأنظمة المعلوماتية عند تصميم الخدمات والتطبيقات المعلوماتية الذكية. كما يجب تحسين قدرات الشركات التي تؤدي خدمات حيوية للمجتمع لكشف ودفع المخاطر السيبرانية التي تتسبب بإعاقة خدمة حيوية[78].

هذا ويمكن أن تؤدي الهيئات الناظمة لقطاع الاتصالات أو لقطاع تكنولوجيا المعلومات دوراً مهماً في مجال الأمن السيبراني وخاصة في ما يتعلق بتنظيم المحتوى وحماية المستهلك وضمان أمن الشبكات[79]. وتؤدي

78 Secretariat of the Security and Defense Committee, *Finland's Cyber security Strategy*. http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf, p. 10.

79 ITU, Marco Gercke, *Understanding Cybercrime: Phenomena, Challenges and Legal Response,* September 2012, p. 101.

كذلك الجامعات ومؤسسات الأبحاث دوراً مهماً بالمساعدة في تطوير المعرفة وفي وضع السياسات والتشريع والتقنيات والمعايير والمساعدة التقنية والتعاون مع أجهزة تطبيق القانون[80].

2- التوجهات المرتبطة بالعوامل الاجتماعية والاقتصادية

فيما يتعلق بالعوامل الأخرى المؤثرة، لا ينبغي إهمال العوامل الاجتماعية والاقتصادية. فبالرغم من أن الخسائر الناجمة عن الجرائم السيبرانية تزيد عن 1 تريليون دولار سنوياً على صعيد العالم[81]، فقد تؤدي الضغوط على الشركات لتخفيض النفقات إلى خفض مستوى الأمن السيبراني. كما أن توظيف أشخاص برواتب أقل أو لمدد مؤقتة أو إنهاء عقود بعضهم يجعل ولاؤهم للشركة أقل، ويمكن حينها لمخترقي الأنظمة إغراؤهم. وفي الدول النامية، يعتبر بعض العاطلين عن العمل الجرائم السيبرانية مورد رزق لهم[82].

تجدر الإشارة إلى أنه ينتج عن أعمال العنف التي تحدث على الخط، بما فيها العنف ضد المرأة (انظر الإطار 5)، آثار نفسية واجتماعية سلبية، قد تسيء إلى سمعة الضحايا، كما قد تؤثر على علاقة الضحايا بالعائلة والأصدقاء، وقد تكون نتائجها مدمرة. لذا فلا بد من الاعتماد على الأخصائيين الاجتماعيين من أجل معالجة الضحايا كما هو الحال في الجرائم التقليدية. وقد يكون وضع ضحايا الجرائم السيبرانية أسوأ من ضحايا الجرائم التقليدية خاصة إذا ما كانت القوانين المحلية لا تشمل نصوصاً خاصة بالجرائم السيبرانية.

الإطار 5- مثال حول استخدام تكنولوجيا المعلومات والاتصالات في تضخيم أثر العنف ضد المرأة

قامت مجموعة من المجرمين في أفريقيا بتخدير امرأة واغتصابها في إحدى الليالي، ومن ثم قام أحد المغتصبين بإرسال رسالة نصية لها يعلمها فيها بما تم خلال هذه الليلة. وعندما استيقظت وجدت هذه الرسالة النصية على هاتفها وشكل ذلك صدمة بالنسبة لها. ولكن الجاني لم يكتف فقط بإرسال الرسالة لها، بل أرسلها أيضاً إلى جميع الأشخاص الموجودة أرقام هواتفهم في قائمتها الهاتفية ومنهم أفراد عائلتها وأصدقائها. وقد اعتبرت عائلة الضحية ما حدث مع ابنتهم عاراً على العائلة فتبروا منها، وتركها أصدقاؤها أيضاً. وبالتالي بقيت هذه السيدة تواجه مشكلتها وحيدة، ونفاها مجتمعها وعائلتها. ولم يكن أمامها إلا أن تترك بلدها وتفر لمكان آخر تسعى فيه لبناء حياة جديدة.

المصدر: http://www.genderit.org/sites/default/upload/casesummaries_tbtt.pdf.

واو- التوجهات المتعلقة بالتوعية والتدريب

3- توعية المستخدمين

إن توعية وتدريب المستخدمين على المبادئ الأساسية للأمن السيبراني يجب أن تكون جزءاً أساسياً من أي استراتيجية أو مبادرة وطنية أو إقليمية لمكافحة الجرائم السيبرانية[83]. وقد تنبهت معظم الدول في العالم إلى

80 United Nations Office on Drugs and Crime, UNODC, *Comprehensive study on cybercrime*, draft, February 2013, p. 239, p. 247.

81 Dr. Hamadoun I. Touré Secretary-General, ITU, *CybersecurityGlobal status update*, December 2011, http://www.un.org/en/ecosoc/cybersecurity/itu_sg_20111209_nonotes.pdf, p. 7.

82 United Nations Office on Drugs and Crime, UNODC, *Comprehensive study on cybercrime*, draft, February 2013, p. 10.

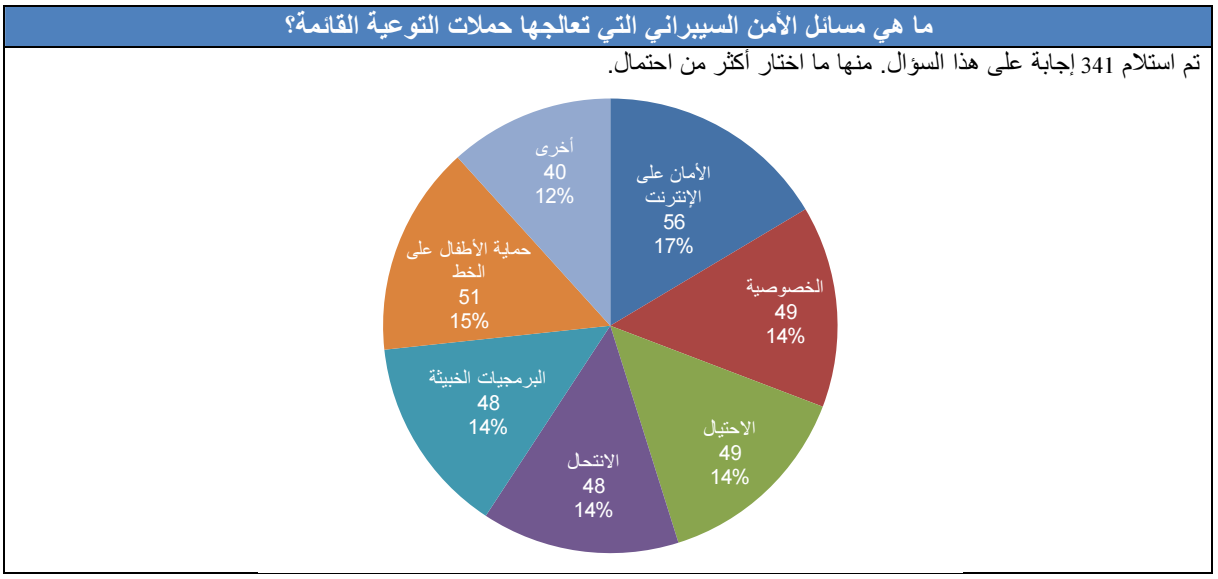
83 ITU, Marco Gercke, *Understanding Cybercrime: Phenomena, Challenges and Legal Response,* September 2012, p. 18.

ذلك، وهي تعمل على توعية المستخدمين بالمخاطر السيبرانية والجرائم السيبرانية وكيفية تفاديها. ويكون الهدف من التوعية والتدريب الموجه للأفراد تمكينهم من تعلم الوسائل التي تتيح لهم حماية أنفسهم في الفضاء السيبراني، ومن ثمّ الوقاية من الجرائم السيبرانية، وكذلك معرفة آليات المساعدة في حال الوقوع ضحية لجريمة سيبرانية وكيفية التصرف عند حدوث ذلك، والإجراءات القانونية المفروض اتخاذها من قبل المراجع الرسمية المختصة. ويساهم ممثلو القضاء ومكاتب المدعين العامين وأجهزة التحقيق في عدد من الدول في عمليات التوعية والتدريب، باعتبار أن ذلك من شأنه تغيير سلوك الأفراد والتخفيف من تأثير الجرائم السيبرانية ودعم جهود مكافحة هذه الجرائم[84].

وقد تكون طرق الوقاية من الجريمة السيبرانية بسيطة وسهلة في عدة حالات إلا أن المستخدم لا يعرفها، وبالتالي لا بد من بيان هذه الطرق والآليات. ويجب التنبه إلى ضرورة التوعية بشكل يتلاءم مع المستوى التقني للمستخدمين العاديين، إذ أن هناك حدوداً لما قد يقوم به مستخدمو المعلوماتية من أجل السلامة المعلوماتية، فهم لن يتحملوا عبء القيام بإجراءات معقدة ولا حفظ كلمات سر طويلة لكل نظام معلوماتي. ومن الحلول الممكنة وجود أنظمة معلوماتية مساعدة في مجال الأمن السيبراني لتنبيه المستخدم ومساعدته.

ووفق دراسة للاتحاد الدولي للاتصالات أجريت على 62 دولة على صعيد العالم، يمكن تقسيم المواضيع المشمولة بالتوعية، وفق ما يلي: الاحتيال (28 في المائة)، الأمان على الإنترنت (17 في المائة)، حماية الأطفال على الخط (15 في المائة)، الخصوصية (14 في المائة)، الفيروسات (14 في المائة)، المسائل الأخرى (12 في المائة)[85].

الشكل 3- مواضيع حملات التوعية حول الأمن السيبراني



المصدر: http://www.itu.int/en/ITU-D/Cybersecurity/Documents/22survey.pdf, p. 22.

84 University of Mississippi, School of Law, National Center for Justice and the Rule of law, *Combating cyber crime: essential tools and effective organizational structures, A guide for policy makers and managers*, http://www.olemiss.edu/depts/ncjrl/pdf/CyberCrimebooklet.pdf, p. 47.

85 ITU, *2013 ITU survey on measures to raise awareness on cybersecurity*, August 2013, http://www.itu.int/en/ITU-D/Cybersecurity/Documents/22survey.pdf, p. 22.

وبالتأكيد، فإن مستخدمي الحاسوب المثقفين معلوماتياً ليسوا ضحايا سهلة لمخترقي الشبكات ولا هم ضحايا محتملين لمرتكبي الجرائم عن طريق وسائل التواصل الاجتماعي. فالمعرفة والتوعية التقنية هامة جداً، فبنتيجة حملات التوعية، تزداد المعرفة لدى المستخدمين لحماية أنفسهم. ويُقدر أنه قد يمكن للأشخاص تفادي أكثر من 80 في المائة من الهجمات بتطبيق ممارسات فُضلى، كالتحديث الدوري لبرامج مكافحة التجسس أو الفيروسات[86].

ويساهم القضاء ومكاتب المدعين العامين وأجهزة التحقيق في عمليات التوعية والتدريب، باعتبار أن ذلك من شأنه تغيير سلوك الأفراد والتخفيف من تأثيرات الجرائم السيبرانية ودعم جهود مكافحة هذه الجرائم[87].

2- توعية فئات خاصة في المجتمع

تستهدف بعض حملات التوعية فئات محددة في المجتمع كالأطفال والطلاب والمؤسسات الخاصة والهيئات الحكومية والمسنين والفئات المهمشة وذوي الاحتياجات الخاصة، وهذا يساعد في مواءمة التدريب مع الاحتياجات الخاصة لكل فئة. ووفق دراسة للاتحاد الدولي للاتصالات على 62 دولة على صعيد العالم، تبين أن الفئات المستهدفة بحملات التوعية تتضمن حسب ترتيب الأهمية: المراهقون (18 في المائة)، والطلاب (17 في المائة)، والأطفال (17 في المائة)، والهيئات الحكومية (16 في المائة)، والمؤسسات الخاصة (13 في المائة)، والأشخاص المسنون (9 في المائة)، والأشخاص ذوي الإعاقات (7 في المائة)، وغيرهم (3 في المائة)[88]. انظر الشكل 4.

3- تدريب خاص للقضاة ومحققي الشرطة

إن الطبيعة التقنية الخاصة والمعقدة للمعلوماتية، وما تتطلبه من قواعد خاصة لحكمها، سواء على الصعيد الإجرائي أو على الصعيد الموضوعي، واللغة التقنية الخاصة التي قد يضطر القاضي لاستعمالها، تفرض إجراء دورات تدريبية خاصة للقضاة والمحققين ورجال الشرطة للتعامل مع الجرائم السيبرانية والأدلة المعلوماتية.

وبالتالي يجب رفد برامج التوعية ببرامج خاصة بتدريب القضاة ومحققي الشرطة بحيث تتضمن كيفية مباشرة التحقيقات الجزائية في الجرائم السيبرانية وفهم ماهية هذه الجرائم وكيفية جمع الأدلة المعلوماتية الجرمية حولها. ولا بد من وجود جهاز تقني مساعد للشرطة مؤلف من تقنيين يتمتعون بالكفاءة بحيث يتم تدريبهم وتجهيزهم بالبرامج والأدوات المعلوماتية الخاصة بالتحقيقات، ومنحهم الرواتب الملائمة لتجنب استقطابهم من القطاع الخاص الذي قد يغريهم برواتب أعلى. كما ينبغي إدخال النساء والرجال سوية في البرامج التدريبية نظراً للحاجة إلى محققين من الجنسين للتعامل مع مرتكبي الجرائم السيبرانية أو مع الضحايا من الجنسين. ويجب التنويه إلى أن وجود النساء في طاقم التحقيق يسهل التعامل مع الضحايا من النساء. ففي الكثير من الدول العربية، ونظراً للعادات الاجتماعية والثقافية، قد تفضل المرأة، إذا وقعت ضحية جريمة

86 Cabinet Office, *The UK Cyber Security Strategy, Protecting and promoting the UK in a digital world.* November 2011, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf, p. 31.

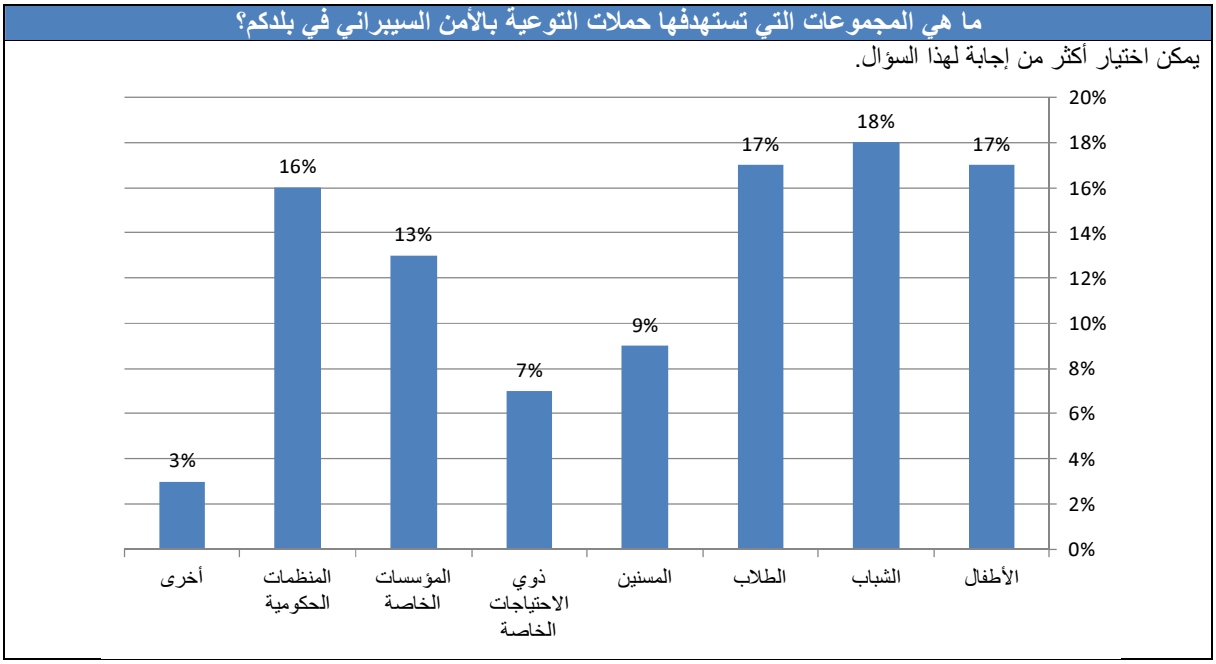
87 University of Mississippi, School of Law, National Center for Justice and the Rule of law, *Combating cyber crime: essential tools and effective organizational structures, A guide for policy makers and managers*, http://www.olemiss.edu/depts/ncjrl/pdf/CyberCrimebooklet.pdf, p. 47.

88 ITU, *2013 ITU survey on measures to raise awareness on cybersecurity*, August 2013, http://www.itu.int/en/ITU-D/Cybersecurity/Documents/22survey.pdf, p. 19.

سيبرانية، أن تبلغ عنها امرأة أخرى في الشرطة أو السلك القضائي بدلاً من تبليغ الرجال، أو قد تختار الكتمان خوفاً من التشهير وحفاظاً على السمعة الشخصية.

ومن الممارسات الفضلى في العالم، مساهمة المدعين العامين والمحققين في مجال الجرائم السيبرانية في تنبيه المشرّع إلى بعض الإشكاليات الإجرائية والموضوعية في هذا المجال، ومساعدته في صياغة القواعد القانونية الملائمة بصددها[89].

الشكل 4- الفئات المستهدفة بحملات التوعية حول الأمن السيبراني



المصدر: http://www.itu.int/en/ITU-D/Cybersecurity/Documents/22survey.pdf, p 19.

89 University of Mississippi, School of Law, National Center for Justice and the Rule of law, *Combating cyber crime: essential tools and effective organizational structures, A guide for policy makers and managers*, http://www.olemiss.edu/depts/ncjrl/pdf/CyberCrimebooklet.pdf, p. 47.

ثانياً- التحديات الإقليمية في مجال الأمن السيبراني ومكافحة الجرائم السيبرانية

تم تحديد مجموعة من التحديات التي تواجه الأمن السيبراني ومكافحة الجرائم السيبرانية على صعيد العالم، ومنها الانتشار الواسع لتكنولوجيا المعلومات والاتصالات، واعتماد معظم النشاطات البشرية لهذه التكنولوجيا، والارتهان لها، وكذلك ارتفاع عدد مستخدمي الحاسوب والإنترنت مايؤدي بالتالي الى ارتفاع عدد الضحايا المحتملين، وأيضا توفر الأجهزة والبرامج المتطورة فنياً وقدرة المرتكبين على الوصول إليها بسهولة، وتوفر المعلومات لهم حول أنظمة الأمن، وعدم وجود آليات للرقابة على الإنترنت. وفيما يتعلق بالجانب الإجرامي والتنظيمي، فالتحديات تظهر في البعد الدولي للمشكلة، وفك الارتباط بين موقع المجرم وموقع الجريمة، وإمكانية أتمتة الهجمات على الحواسيب لتطال الآلاف منها آلياً، وسرعة انتقال المعلومات وآنيتها، وسرعة التطور التقني الذي يؤدي إلى تنامي تعقيد الهجمات السيبرانية، والغفلية، أي إمكانية إخفاء الشخص لهويته على الإنترنت، وتشفير المعلومات من قبل مرتكبي الجرائم. وفيما يتعلق بالتحقيق، تبرز تحديات تواجه أدوات التحقيق التقليدية مما يشير إلى الحاجة إلى أدوات معلوماتية حديثة، وتحديات التشريع وتجريم أفعال جديدة، وسن إجراءات جديدة للأدلة المعلوماتية[90]. ولا تختلف كثيراً التحديات في المنطقة عن تلك التي تواجه عدداً من الدول النامية في العالم، مع بعض الفوارق والخصوصيات التي نبينها في القسم التالي.

أما في المنطقة العربية، فمن أهم التحديات الاستراتيجية للمخاطر السيبرانية ضعف الإطار التنظيمي والقانوني وصعوبة تحذير المستخدمين في الوقت المناسب من المخاطر والحوادث السيبرانية المرتقبة لكون معظم المستخدمين لا يتابعون تطوراتها، ومكامن الضعف المعقدة في توريد التجهيزات المعلوماتية للشبكات التي تأتي من دول أخرى، وانخفاض الوعي حول المخاطر الإلكترونية. وتنعكس التحديات والفوارق في المنطقة العربية على الجوانب الاستراتيجية، والتشريعية، وتطبيق القانون وأجهزته، والقطاع العام، والقطاع الخاص، وتلك المتعلقة بثقافة المستخدم.

ألف- التحديات والفوارق المتعلقة بتطور الجرائم السيبرانية في المنطقة العربية

1- تطور استخدام الإنترنت وازدياد الجرائم السيبرانية

أولى الخصائص التي تشهدها المنطقة العربية هي النمو السريع لاستخدامات الإنترنت. فهذا النمو شهدته الدول المتقدمة في مراحل سابقة، والآن تتبع دول المنطقة مسار التطور التاريخي ذاته. وعلى سبيل المثال، زاد عدد مستخدمي الإنترنت في الإمارات العربية المتحدة بنسبة 212 في المائة خلال السنوات العشر الماضية[91]. كما بينت الإحصاءات أن 40 في المائة من مستخدمي الإنترنت في دول منطقة الشرق الأوسط وشمال أفريقيا يستخدمون الإنترنت أكثر من 20 ساعة في الأسبوع، وهو ما يتوافق مع المعدل العالمي[92]. ويؤدي ازدياد أعداد مستخدمي الإنترنت في المنطقة العربية بطبيعة الحال إلى ازدياد الأشخاص المعرضين للمخاطر السيبرانية، ومن ثمّ ازدياد الجرائم السيبرانية.

---

90 ITU, Marco Gercke, *Understanding Cybercrime: Phenomena, Challenges and Legal Response,* September 2012, p. 75-84.

91 جريدة دار الخليج، دبي، الثلاثاء 14 كانون الأول/ديسمبر 2010، المشاركون في اجتماع الإنتربول يشيدون بإنشاء محاكم للجريمة الإلكترونية، http://www.mohamoon-uae.com/default.aspx?Action=DisplayNews&type=3&ID=12864، ص 1.

92 Ministry of information and communications technology, Qatar, Rassed, *The attitudes of online users in the MENA region cybersafety, security and data privacy*, May 2014, http://www.ictqatar.qa/sites/default/files/Cybersafety,%20security%20and%20data%20privacy.pdf, p. 9.

وتظهر الدراسات أن نسبة مستخدمي الإنترنت الذين يقعون ضحايا الجرائم السيبرانية تتراوح ما بين 1 و17 في المائة، وهذه النسبة تزداد في الدول الأقل نمواً[93]. ووفق دراسة للأمم المتحدة[94]، فقد أكد مسؤولو تطبيق القانون في دول آسيا، أن الجرائم السيبرانية في ازدياد، وبدرجات تتفاوت بين ازدياد عادي وازدياد كبير. كما يعتقد 48 في المائة من المستطلعين في منطقة الشرق الأوسط، في مسح صدر أوائل عام 2014، أن مخاطر الجرائم السيبرانية في مؤسساتهم قد ازدادت في الأشهر الأربعة والعشرين الماضية[95]. ويبدي 44 في المائة من المستخدمين في دول منطقة الشرق الأوسط وشمال أفريقيا مخاوف كبيرة من تعرض حسابات بريدهم الإلكتروني أو غيره من الحسابات على الإنترنت للاختراق، وهذه النسبة هي أعلى قليلاً مما هي عليه في العالم عموماً (41 في المائة)[96].

ويبدو في دول المنطقة العربية أن الغالبية العظمى من الجرائم السيبرانية هي تلك التي تكون المعلوماتية فيها وسيلة ارتكاب الجريمة وليس محلها. فوفق إحدى الدراسات لعام 2011، احتلت دولة الإمارات العربية المتحدة المرتبة 19 عالمياً، في حين جاء لبنان في المرتبة 25 عالمياً من حيث ترتيب الدول التي تتعرض لهجمات سيبرانية[97]. وفي لبنان تحديداً، لا تتجاوز جرائم التعدي على الأنظمة والبيانات 5 في المائة من المجموع، في حين أن 95 في المائة منها هي جرائم تقليدية بوسيلة معلوماتية، مثل الاحتيال والقدح. وكذلك في السودان، حيث لا تتجاوز نسبة جرائم التعدي على الأنظمة والبيانات 8 في المائة، في حين تزيد نسبة جرائم شبكات التواصل الاجتماعي عن 70 في المائة[98].

وقد ارتفع معدل الجريمة السيبرانية في الإمارات العربية المتحدة بنسبة 25 في المائة عام 2013 مقارنة بعام 2012، وتصدرت قضايا الاحتيال والابتزاز بهدف الحصول على المال ولأهداف غير أخلاقية قائمة الجرائم المرتكبة، وذلك بحسب إحصاءات صادرة عن شرطة دبي. وقد ورد عن الإدارة العامة للتحريات والبحث الجنائيان "البلاغات ترد من كلا الجنسين ومن أعمار مختلفة، وتتركز بالنسبة للنساء على مواقع الزواج الإلكترونية، حيث يستغل الجاني إقبال الإناث من مختلف الأعمار على هذه المواقع لأغراض متعددة"[99].

كما ارتفعت الجرائم السيبرانية في دولة الكويت في عام 2012 من 563 قضية إلى 997 قضية في عام 2013[100]. وازداد عدد الجرائم السيبرانية المبلغ عنها في سلطنة عُمان لدى سلطة التحقيق من أقل من 200 في نهاية عام 2011 إلى أكثر من 800 قضية في نهاية عام 2013[101].

---

93 United Nations Office on Drugs and Crime, UNODC, *Comprehensive study on cybercrime*, draft, February 2013, p. 25.

94 United Nations Office on Drugs and Crime, UNODC, *Comprehensive study on cybercrime*, draft, February 2013, p. 7.

95 John Wilkinson, Tareq Haddad, PWC, *Economic Crime in the Arab World*, February 2014, http://www.pwc.com/m1/en/publications/gecs2014reportme.pdf, p. 16.

96 Ministry of information and communications technology, Qatar, Rassed, *The attitudes of online users in the MENA region cybersafety, security and data privacy*, May 2014, http://www.ictqatar.qa/sites/default/files/Cybersafety,%20security%20and%20data%20privacy.pdf, p. 22.

97 Dr. Hamadoun I. Touré Secretary-General, ITU, *Cybersecurity Global status update*, December 2011, http://www.un.org/en/ecosoc/cybersecurity/itu_sg_20111209_nonotes.pdf, p. 5.

98 القاضي حسن محمد علي حسن، المشرف على قسم الحاسوب، تجربة المركز السوداني لأمن المعلومات، المؤتمر الثالث لأمن وسلامة الفضاء السيبراني، بيروت، 25-27 آب/أغسطس 2014، ص 16.

99 لواء النعساني، ص 2 http://www.24.ae/article.aspx?ArticleId=77807.

100 جواب الجهاز المركزي لتكنولوجيا المعلومات على الاستبيان المرسل له في إطار هذه الدراسة، إحصاءات نقلاً عن وزارة الداخلية الكويتية- إدارة مكافحة الجرائم الإلكترونية، الكويت، أيلول/سبتمبر 2014.

101 جواب المركز الوطني للسلامة المعلوماتية بهيئة تقنية المعلومات على الاستبيان المرسل له من قبل الإسكوا في إطار هذه الدراسة، سلطنة عُمان، أيلول/سبتمبر 2014.

وتأتي جرائم الاحتيال المعلوماتي وجرائم التعرض للشخص بواسطة الحاسوب في دول آسيا في طليعة الجرائم السيبرانية، في حين تقل نسبة جرائم المواد الإباحية للأطفال في دول آسيا عنها في دول أوروبا وأمريكا[102]. كما ترتفع المطالبات بإزالة محتوى موقع إلكتروني في دول الشرق الأوسط مقارنة بالنسب العامة تبعاً للتعرض لخصوصية الفرد، وذلك نظراً لطبيعة المجتمع الشرقي المحافظ وتقاليده.

ويتبين من الأرقام السابقة أن معدّل الجرائم السيبرانية هو أعلى نسبياً في منطقة الشرق الأوسط من المعدّل العالمي، وهذا ناتج عن ضعف آليات محاربة هذه الجرائم، سواء على صعيد السياسات المطبقة، أو على الصعيد التقني أو التشريعي أو التوعوي. ويبدو أن المجرمين بدأوا يلجأون أكثر فأكثر في دول المنطقة إلى تكنولوجيا المعلومات لارتكاب أفعالهم لارتفاع عوائدها وتدني مخاطرها وإمكان القيام بها عن بعد وصعوبة إثباتها نسبياً. وفي هذا السياق، ووفقاً لإحصائية صادرة عن أبو ظبي، فإن نسبة 70 في المائة من الجرائم التي وقعت فيها خلال الأشهر الستة الأخيرة من عام 2010 استخدمت في ارتكابها تكنولوجيا المعلومات والاتصالات[103].

وقد أدى تزايد الجرائم السيبرانية في دول المنطقة إلى ارتفاع في أرقام بعض الجرائم التقليدية، باعتبار أن الجرائم السيبرانية يمكن أن تكون وسيلة لتسهيل ارتكاب الجرائم التقليدية. فعلى سبيل المثال، أثبتت بعض الدراسات في المجتمع السعودي أن 68.8 في المائة من المستطلعين يرون أن هناك علاقة بين الانحراف والجرائم المرتبكة، ومشاهدة محتوى الفيديو الجنسي. كما أثبتت إحدى الدراسات المتخصصة بتفسير ارتكاب الجريمة الجنسية في المجتمع السعودي والتي أجريت في الاصلاحيات المركزية في المملكة أن 53.7 في المائة من مرتكبي الجرائم الجنسية كان لهم اهتمامات بالصور الجنسية[104].

2- قلة الإحصاءات والدراسات حول الجرائم السيبرانية

يصعب في بعض الأحيان إجراء دراسات إقليمية مقارنة بين مختلف الدول العربية حول الجرائم السيبرانية والأمان السيبراني، وذلك لعدة أسباب، منها: (1) عدم وجود تعاريف موحدة للجريمة السيبرانية ولبعض المفاهيم القانونية والتقنية، (2) محدودية مصادر المعلومات لوضع دراسات تحليلة بسبب عدم وجود الوعي الكاف لدى الرأي العام وعدم إلمام القضاء أو الضابطة العدلية بالنواحي التقنية في الجرائم السيبرانية وكذلك عدم وجود أجهزة رسمية توثق الشكاوى أو تصدر إحصاءات موثوقة عن الجرائم السيبرانية، (3) امتناع ضحايا الاعتداءات السيبرانية عن تقديم الشكاوى أو الإفصاح عن تجربتهم، (4) وعدم وجود أجهزة تحقيق متخصصة لاكتشاف الجرم.

ومن اللافت ضعف إحصاءات الجرائم السيبرانية وندرتها وتضارب أرقامها في دول المنطقة العربية، خاصة إذا ما تمت مقارنتها مع تلك المتاحة في الدول المتقدمة. وهذا الضعف هو مؤشر خطير يدل على عدم إيلاء الموضوع الاهتمام اللازم من الجهات المعنية، وهو لا يساعد في وضع سياسات واستراتيجيات فعالة في

---

102 United Nations Office on Drugs and Crime, UNODC, *Comprehensive study on cybercrime*, draft, February 2013, p. 26, 36.

103 جريدة دار الخليج، الأحد 9 كانون الأول/يناير 2011، جيهان شعيب، خلال ندوة تقصي جرائم تقنية المعلومات د. محمد الكمالي: 80 في المائة من الجرائم أصبحت إلكترونية، http://www.mohamoon-uae.com/default.aspx?Action=DisplayNews&type=3&ID=13154، ص 1.

104 محمد عبد الله منشاوي، جرائم الانترنت من منظور شرعي وقانوني، 1-11-1423هـ، http://www.khayma.com/education-technology/Study33.htm، ص 16.

هذا المجال، مبنية على أسس سليمة وواقعية. ويتضح ذلك في استناد معظم الدراسات في دول المنطقة إلى إحصاءات عائدة لدول أخرى، وكذلك من عدم استناد سياسات الدول في مجال الجرائم السيبرانية إلى معلومات علمية دقيقة ومعطيات إحصائية واضحة ومفصلة. وتشير دراسة للأمم المتحدة أنه بسبب الصعوبة في تعريف وتحديد الجرائم السيبرانية، فإن أية تقارير إحصائية مقارنة بين عدة دول حول هذه الجرائم هي أقل بكثير من تلك العائدة للجرائم الأخرى[105]. ويقل بنتيجة ذلك توافر البيانات والإحصاءات حول الجرائم السيبرانية المصنفة بحسب النوع الاجتماعي، مما يجعل دراسة آثار الجرائم على كل من الرجل والمرأة عملية صعبة. وبالتالي فإنه من الصعوبة بمكان تحليل توجهات الجرائم السيبرانية الموجهة تجاه الرجال أو النساء أو الأطفال على الفضاء السيبراني. وتجدر الإشارة إلى أن إعداد هذه الدراسة قد واجه صعوبة في الحصول على إحصاءات مفصلة حول دول المنطقة تخصّ واقع الأمان السيبراني والجرائم السيبرانية فيها.

باء- التحديات الاستراتيجية في المنطقة العربية

يتيح وضع استراتيجية شاملة للأمان السيبراني تحديد الأهداف المرجوة، وبيان الأنشطة المطلوبة لبلوغها، وتقسيمها على مراحل، وتحديد متطلباتها البشرية والمالية والتنظيمية والتقنية، وتنظيم وسائل تمويلها وفق خطط محدّدة. كما يساعد وضع الاستراتيجيات على تحديد آليات التنفيذ ووضع مخطط زمني للتنفيذ بالإضافة إلى تحديد المعنيين بالتنفيذ وإيجاد آليات لتنسيق الجهود في ما بينهم. وتفتقر معظم الدول العربية، إلى وجود استراتيجية متكاملة للأمان السيبراني. ويبدو أن بعض دول المنطقة بدأت بوضع مثل هذه الاستراتيجيات بناء على بعض التجارب الدولية، وهي في طور استكمالها. أما الدول الأخرى، فلديها فقط استراتيجيات عامة لقطاع تكنولوجيا المعلومات والاتصالات. ويبين الإطار 6 الاستراتيجيات في بعض دول المنطقة العربية وهي مصر والإمارات العربية المتحدة والجمهورية العربية السورية.

أقر الأردن استراتيجية وطنية لأمن المعلومات والأمن السيبراني عام 2012 وحدد لها خمسة أهداف وتسع أولويات. وتتركز أهداف هذه الاستراتيجية على دعم الأمن الوطني والحماية من الهجمات السيبرانية والتقليل من الأخطار التي يمكن أن تتعرض لها الشبكات الحكومية والبنى الأساسية للمعلومات، وزيادة الثقة بالحكومة وأمن منظومات المعلومات الخاصة. أما الأولويات التسع الخاصة بتحقيق هذه الأهداف، فكانت من بينها إقامة الفريق الوطني للاستجابة لطوارئ الحاسوب الأردني JOCERT المجهز بأكمل التجهيزات والذي يضم محترفي أمن عاليّ المهارة لمعالجة قضايا التهديد وعمليات محاولة اختراق المؤسسات. وقد أوكلت مهمة إنشاء هذا الفريق الوطني إلى مركز تكنولوجيا المعلومات الوطني، وتم إنشاءه عام 2013. ومن بين أولويات الاستراتيجية وضع برامج لبناء القدرات والتوعية الأمنية، والسياسات والمعايير الوطنية لأمن المعلومات، وتحديث النظام التشريعي والقانوني ونظام التشفير الوطني.

الإطار 6- بعض الاستراتيجيات من دول المنطقة العربية

1- استراتيجية وزارة الاتصالات وتكنولوجيا المعلومات في مصر

وضعت وزارة الاتصالات وتكنولوجيا المعلومات في مصر ضمن استراتيجيتها الجديدة للفترة 2012-2017 موضوع أمن المعاملات الإلكترونية والشبكات المعلوماتية، مثل تطوير أنظمة أمن الشبكات، وذلك لدعم القطاع المصرفي وأنظمة الدفع الإلكتروني، وكذلك مسألة الخصوصية والحماية على الإنترنت. وقد أنشأت وزارة الاتصالات وتكنولوجيا المعلومات في آخر 2011 لجنة من الخبراء الفنيين والقانونيين لصياغة قانون للأمن السيبراني[أ].

105 United Nations Office on Drugs and Crime, UNODC, *Comprehensive study on cybercrime*, draft, February 2013, p. 6.

الإطار 6 (تابع)

2- استراتيجية دولة الإمارات العربية المتحدة لقطاع تكنولوجيا المعلومات

تهدف استراتيجية دولة الإمارات العربية المتحدة إلى بناء مجتمع معلومات مستدام، وقد تضمنت هذه الاستراتيجية للأعوام 2011-2013 تعزيز التحول الإلكتروني لجميع الخدمات الحكومية خلال ثلاث سنوات، وتطوير مشروع البنية الأساسية لإدارة الهوية الوطنية. وتستكمل استراتيجية الإمارات للأعوام 2012-2014 الاستراتيجية السابقة، وترمي إلى بناء البنية الأساسية لتكنولوجيا المعلومات لتوفير الخدمات الإلكترونية للمواطنين عبر قنوات إلكترونية متعددة[ب].

3- استراتيجية تقانة المعلومات والاتصالات في الجمهورية العربية السورية

قامت الجمهورية العربية السورية منذ عام 2004 بوضع استراتيجية وطنية لتقانات (تكنولوجيات) المعلومات والاتصالات. ولكن هذه الاستراتيجية لم تتطرّق صراحة إلى قضايا الأمن السيبراني. وفي 2009-2010، وضعت وزارة الاتصالات والتقانة استراتيجية مفصّلة للحكومة الإلكترونية[ج] تضمّنت الإشارة إلى قضايا أمن النظم المعلوماتية الحكومية وسبُل حمايتها. ويبقى أن الجمهورية العربية السورية ليس لديها حتى الآن (2014) استراتيجية خاصة بالأمن السيبراني، لكن وزارة الاتصالات والتقانة أصدرت بالمقابل في عام 2014 وثيقة "السياسة الوطنية لأمن المعلومات"[د] التي حدّدت مجالات ومتطلبات العمل في هذا الشأن.

أ الإسكوا، الملامح الوطنية لمجتمع المعلومات لجمهورية مصر العربية، 2013، ص 8.
ب الإسكوا، الملامح الوطنية لمجتمع المعلومات في الإمارات العربية المتحدة، 2013، ص 3.
ج استراتيجية الحكومة الإلكترونية في سورية http://www.moct.gov.sy/moct/?q=ar/node/61.
د السياسة الوطنية لأمن المعلومات في سورية http://nans.gov.sy/images/stories/doc/isc_doc/finalpolicy.pdf.

جيم- التحديات التشريعية الخاصة بالفضاء السيبراني في المنطقة العربية

1- التشريعات المتعلقة بالجرائم السيبرانية في بعض دول المنطقة العربية

يتفاوت وضع التشريعات الخاصة بالجرائم السيبرانية (أو جرائم تقنية المعلومات) في الدول العربية، إذ قامت بعض الدول بإصدار تشريعات خاصة بهذه الجرائم، في حين ضمنت بعض الدول الأخرى مواداً خاصة بالجريمة السيبرانية في تشريعاتها الأخرى وبخاصة قوانين المعاملات الإلكترونية أو التجارة الإلكترونية وقوانين حماية حقوق الملكية الفكرية في الفضاء السيبراني. وقامت بعض الدول الأخرى بإدراج مواد خاصة بالجريمة السيبرانية في قانون العقوبات. وفي ما يلي ملخص لوضع تشريعات الجرائم السيبرانية في بعض الدول العربية.

(أ) الأردن

أقر الأردن قانون جريمة أنظمة المعلومات رقم 30 عام 2010. ويحدد هذا القانون عناصر جرائم نظم المعلومات ويبين الثغرات في التشريعات القائمة من حيث التعامل مع نظم المعلومات وجرائم الإنترنت. وقد تعامل القانون مع نمطين من الجرائم: الجرائم الجديدة، التي تتضمن النفاذ إلى نظم المعلومات والشبكات بدون إذن ومسح ونسخ وإضافة وتغيير في المعلومات ونشر الفيروسات وسرقة البيانات المستعملة في المداولات المالية الإلكترونية. والنوع الثاني هو استعمال نظم المعلومات والشبكات في الجريمة التقليدية مثل التأثير في القاصرين أو المتخلفين عقلياً لارتكاب جريمة، أو الترويج للدعارة وغير ذلك.

(ب) الإمارات العربية المتحدة

على الصعيد التشريعي، فقد كانت دولة الإمارات العربية المتحدة سبّاقة في المنطقة إلى إقرار قانون لمكافحة جرائم تقنية المعلومات (رقم 2) في شباط/فبراير عام 2006. كما أوصى مجلس التعاون الخليجي في مؤتمر انعقد في حزيران/يونيو 2007 بوضع اتفاقية حول الجرائم السيبرانية تجمع بين أعضائه. وقد عادت الإمارات العربية المتحدة وحدّثت قانونها، بإلغاء القانون رقم 2 لعام 2006 واستبداله بالقانون الاتحادي رقم 5 لسنة 2012، الذي هو أكثر تفصيلاً وعصريا ويراعي الأوجه المستجدة في ارتكاب الجرائم السيبرانية، إلا إن هذا القانون الجديد لم يتضمن قواعد إجرائية مفصلة خاصة بالتحقيقات الجزائية المتعلقة بالجرائم السيبرانية.

(ج) تونس

أصدرت تونس مجموعة من التشريعات المتعلقة مباشرةً أو غير مباشرةً بالأمان السيبراني، وهي: القانون رقم 5 لسنة 2004 المتعلق بتنظيم مجال السلامة المعلوماتية وضبط القواعد العامة لحماية النظم المعلوماتية والشبكات، والقانون رقم 89 لسنة 1999 المتعلق بتنقيح وإتمام بعض أحكام المجلة الجنائية وإضافة فصل خاص بالجرائم المعلوماتية، والقانون التوجيهي رقم 13 لسنة 2007 المتعلق بإرساء الاقتصاد الرقمي، والقانون الأساسي رقم 63 لسنة 2004 المتعلق بحماية المعطيات الشخصية، والقانون رقم 83 لسنة 2000 المتعلق بالمبادلات والتجارة الإلكترونية، والقانون رقم 57 لسنة 2000 المتعلق بتنقيح وإتمام بعض فصول مجلة الالتزامات والعقود للاعتراف بالسندات والتواقيع الإلكترونية، والقانون رقم 75 لسنة 2003 المتعلق بدعم الجهود الدولية لمكافحة الإرهاب ومنع غسل الأموال، وقانون الاتصالات لعام 2001 وتعديلاته[106].

(د) مصر

حاولت مصر، على غرار دول أخرى في المنطقة العربية، إقرار قانون خاص بالجرائم السيبرانية، لكن مشروع القانون ما زال عالقاً في البرلمان بانتظار إقراره. غير أن مصر أقرت بعض النصوص المتعلقة ببعض الجرائم السيبرانية في قوانين متفرقة. فقد سبق لمصر أن أقرت القانون رقم 15 لعام 2004 حول التوقيع الإلكتروني الذي ينص في مادته رقم 23 على تجريم فعل التزوير الإلكتروني للمحرر الإلكتروني والتوقيع الإلكتروني واستعمال المزور الإلكتروني وإتلاف محرر إلكتروني أو تعديله، وكذلك أقرت تعديل المادة 116 من قانون الطفل رقم 129 لعام 2008 حول الاستغلال الجنسي للأطفال عبر الإنترنت، هذا إضافة إلى بعض النصوص المتفرقة في عدة قوانين مثل قانون العقوبات، بخصوص حماية الحق في الحياة الخاصة، والمادة 171 المتعلقة بوسائل العلانية، وقانون الأحوال المدنية رقم 143 لسنة 1994، بخصوص الجرائم المتعلقة بحماية الحق في الخصوصية أو في الحياه الخاصة، وقانون تنظيم الاتصالات رقم 10 لسنة 2003 الذي يهدف الي تحقيق سلامة وأمن نظم وشبكات الاتصالات ويجرم الافعال التي من شأنها الحاق الضرر بشبكات الاتصالات أو تعطيلها أو التنصت على الاتصالات، والقانون رقم 82 لسنة 2002 بإصدار قانون حماية الملكية الفكرية.

ومن اللافت أن الدستور المصري الجديد، على غرار دساتير بعض الدول، يورد بعض المبادئ القانونية في ما يخص استخدام المعلوماتية. فينص في مادته رقم 31 على أن أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه على النحو الذي ينظمه القانون؛ كما تنص المادة 57 منه على أن للحياة الخاصة حرمة، وهي مصونة لا تمس. وللمراسلات البريدية والبرقية والإلكترونية والمحادثات الهاتفية، وغيرها من وسائل الاتصال، حرمة وسريتها مكفولة،

106 المصدر: المعلومات التي زودتها الوكالة الوطنية للسلامة المعلوماتية - وزارة التعليم العالي والبحث العلمي وتكنولوجيا المعلومات والإتصال على الاستبيان المرسل لها في إطار هذه الدراسة، تونس، أيلول/سبتمبر 2014.

ولا تجوز مصادرتها، أو الاطلاع عليها، أو رقابتها إلا بأمر قضائي، ولمدة محددة، وفى الأحوال التي يبينها القانون؛ كما تلتزم الدولة بحماية حق المواطنين في استخدام وسائل الاتصال العامة بكافة أشكالها ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها بشكل تعسفي.

(هـ) لبنان

أما في لبنان، فقد انتهت في عام 2012 لجنة مشكلة من قبل رئاسة مجلس الوزراء، تضم ممثلين عن جميع الوزارات المعنية والقطاع الخاص، من إعداد مشروع قانون متكامل حول المعاملات الإلكترونية والتواقيع الإلكترونية وحماية البيانات ذات الطابع الشخصي وأسماء المواقع وكذلك حول جرائم المعلوماتية، غير أن المشروع ما زال في أدراج المجلس النيابي اللبناني بانتظار إقراره. وقد سبق للبنان أن أقر القانون رقم 75 بتاريخ 3 نيسان/أبريل 1999 المتعلق بحماية الملكية الادبية والفنية وكذلك القانون رقم 140 بتاريخ 27 تشرين الأول/أكتوبر 1999 المتعلق بصون الحق بسرية المكالمات الهاتفية، إضافة إلى بعض النصوص التقليدية في قانون العقوبات التي يمكن تطبيقها في مجال الجرائم السيبرانية، مثل الاحتيال والسب والتخريب.

(و) الجمهورية العربية السورية

صدر في الجمهورية العربية السورية المرسوم التشريعي رقم 17 بتاريخ 8 شباط/فبراير 2012 المتعلق بتنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية، وهو ينظم مسؤوليات مزودي خدمات الشبكة وواجباتهم، والتعريف عن مزود خدمات الاتصال على الشبكة، والإخبار عن الطابع غير المشروع للمحتوى، وحجب المواقع الإلكترونية، ويحدّد أصناف الجرائم السيبرانية وعقوباتها وحالات تشديدها، كما ينص على إحداث ضابطة عدلية متخصصة. وصدر عن وزارة الاتصالات والتقانة القرار رقم 290 لعام 2012 بتطبيق التعليمات التوضيحية والتنفيذية لهذا القانون.

وقبل هذا المرسوم التشريعي، كان قد صدر القانون رقم 4 بتاريخ 25 شباط/فبراير 2009 الخاص بالتوقيع الإلكتروني وخدمات الشبكة، والذي تضمن بوجه خاص تنظيم التوقيع الإلكتروني وشروط إنشائه وإصداره وتصديقه، وأحدث هيئة مختصة هي الهيئة الوطنية لخدمات الشبكة[107]، كما تضمّن النصّ على المخالفات والعقوبات المتعلقة بتزوير التوقيع الإلكتروني واستعمال التوقيع الإلكتروني المزوّر. وصدر بتاريخ 9 حزيران/يونيو 2010 القانون رقم 18 الخاص بتنظيم قطاع الاتصالات، الذي أحدث هيئة مختصّة هي الهيئة الناظمة لقطاع الاتصالات[108]، كما نصّ على إحداث ضابطة عدلية مختصة بالمخالفات والجرائم المتعلقة بخدمات الاتصالات. وصدر أيضاً قانون الإعلام بالمرسوم التشريعي رقم 108 بتاريخ 8 آب/أغسطس 2011، الذي تضمّن تنظيم وسائل التواصل على الشبكة (الإعلام الإلكتروني) والمخالفات والجرائم المرتبطة بها. وصدر أيضاً المرسوم التشريعي رقم 62 بتاريخ 16 أيلول/سبتمبر 2013 الخاص بتنظيم حقوق المؤلف والحقوق المجاورة (الملكية الفكرية)، الذي تضمّن النص على حماية المصنّفات المعلوماتية.

(ز) بعض الدول العربية الأخرى

أقرت المملكة العربية السعودية نظام مكافحة جرائم المعلوماتية عام 2007. كما أصدرت البحرين مؤخراً القانون رقم 60 لسنة 2014 بشأن جرائم تقنية المعلومات. أما الكويت، فقد أعدت مسودة مشروع قانون

107 www.nans.gov.sy.

108 www.sytra.gov.sy.

حول الجرائم السيبرانية[109]. وتعمل دول عربية أخرى على إعداد وإقرار قوانين خاصة بالجرائم السيبرانية. وتجدر الإشارة إلى أن لدى الإسكوا العديد من الدراسات حول وضع التشريعات السيبرانية ومنها الجرائم السيبرانية في المنطقة العربية لغاية عام 2013[110].

2- معوقات وضع التشريعات السيبرانية وتحديثها

يلاحظ في بعض بلدان المنطقة العربية أن المشرّع، إنفاذاً لقرارات من أعلى السلطات في البلاد، قد حزم أمره بإقرار التشريعات في مجال الجرائم السيبرانية ثم تطويرها، كما هو الحال في دولة الإمارات العربية المتحدة. أما في دول أخرى، فالتشريعات المتعلقة بالجرائم السيبرانية لم تصدر لغاية تاريخه (2014)، وذلك إما بفعل عدم وجود استقرار سياسي وإعطاء الأولوية لملفات أخرى، أو بسبب عدم وجود ثقافة المعلوماتية لدى المسؤولين وعدم وعيهم لأهمية الموضوع. وبالانتظار يتم تطبيق بعض نصوص قانون العقوبات التقليدي وبعض النصوص الواردة في قوانين متفرقة أخرى على بعض الجرائم السيبرانية، فيما تبقى جرائم سيبرانية عديدة غير مجرمة. ونجد، أيضاً، تفاوتاً بين دول المنطقة من حيث تحديث تشريعاتها لتتلاءم مع المفاهيم المستجدة؛ فبعض هذه الدول، كدولة الإمارات العربية المتحدة، بلغت مرحلة متقدمة، ليس فقط بإقرار قانون منذ عدة سنوات، بل مراجعته وتحديثه عقب اختبار تطبيقه سنوات عدة، ومواكبة التطور التقني الحاصل والانتهاكات في هذا المجال.

ومن معوقات التشريع في دول المنطقة أيضاً وجود ضوابط مختلفة له في كل دولة، وكذلك الضوابط والمعايير العالمية التي لا تساعد على ضمان تناسقه بين الدول، وما يتعارض منها مع قواعد قانونية أساسية أو دستورية أو دينية في البلاد أو مع تقاليد المجتمع أو غيرها[111].

من ناحية أخرى، قد تكون النصوص المتعلقة بالجرائم السيبرانية مبعثرة في قوانين عدة، وليست مقننة ضمن قانون واحد يشكل مرجعاً يسهل الرجوع إليه. وبالفعل، يتبين من دراسة للأمم المتحدة أن جرائم التعدي على سلامة وسرية وتوفر أنظمة المعلوماتية هي مجرمة في معظم دول العالم بنصوص خاصة، أما الأفعال الجرمية المرتبطة بالحاسوب، حيث تكون المعلوماتية وسيلة ارتكاب الجرم، كالاحتيال والتزوير والابتزاز وخرق الخصوصية والاعتداء على الحياة الخاصة وانتحال الهوية، فهي مجرمة بمقتضى النصوص العقابية العامة التقليدية[112].

تبين الدراسات والتجارب في العديد من الدول والمناطق إمكانية تحديث التشريعات وفق عدة منهجيات وهي:

(أ) إما وضع قانون واحد متكامل يتناول كامل أو معظم أوجه المواضيع الإلكترونية أو السيبرانية، ومنها الجرائم السيبرانية والتواقيع الإلكترونية والتجارة الإلكترونية والبيانات الشخصية وأسماء المواقع. وهذه هي حالة لبنان في مشروع القانون الأخير العالق لدى المجلس النيابي اللبناني؛

109 جواب الجهاز المركزي لتكنولوجيا المعلومات على الاستبيان المرسل له في إطار هذه الدراسة، الكويت، أيلول/سبتمبر 2014.

110 Regional Profile of Information Society in the Arab region, 2013: http://www.escwa.un.org/information/publications/edit/upload/E_ESCWA_ICTD_13_6_E.pdf, chapter 5 and 6.

111 United Nations Office on Drugs and Crime, UNODC, *Comprehensive study on cybercrime*, draft, February 2013, p. 59.

112 United Nations Office on Drugs and Crime, UNODC, *Comprehensive study on cybercrime*, draft, February 2013, p. 77.

(ب) وإما صياغة عدة قوانين لكل موضوع على حدة، مثل حالة الإمارات العربية المتحدة في قانون مكافحة جرائم تقنية المعلومات؛ وحالة الجمهورية العربية السورية في التشريعات الخاصة بالاتصالات والتوقيع الإلكتروني والمراسلات الإلكترونية والإعلام الإلكتروني وحماية الملكية الفكرية وتنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية؛

(ج) أو إجراء تعديلات موضوعية على النصوص النافذة حالياً، مثل القانون المدني وقانون العقوبات وغيرها لتضاف إليها الأحكام المتعلقة بالفضاء السيبراني[113]، كالجرائم السيبرانية والتوقيع الإلكتروني وغيرها. وأبرز مثال على هذه الحالة هو فرنسا.

3- القواعد الإجرائية الجزائية في قضايا الجرائم السيبرانية

لقد فات المشرّع في معظم دول المنطقة وضع قواعد إجرائية تنظم مسألة التحقيق وجمع الأدلة المعلوماتية في قضايا الجرائم السيبرانية، والتي تتطلب، نظراً لطبيعتها، قواعد إجرائية خاصة.

ولكن بالمقابل، وعلى سبيل المثال، فقد تضمن المرسوم التشريعي السوري رقم 17 الصادر في 8 شباط/فبراير 2012 المتعلق بتنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية، بعض القواعد الإجرائية، ولا سيما ما يخص التزامات مزودي خدمات الاتصال مثل حفظ معلومات حركة البيانات وبيانات التعريف عن صاحب الموقع الإلكتروني وتقديمها للسلطة القضائية؛ وكذلك إنشاء ضابطة عدلية في وزارة الداخلية متخصصة في الجرائم المعلوماتية، وتحديد صلاحياتها في التقصي الإلكتروني والتفتيش والضبط، بإجازة أن تكون البرمجيات الحاسوبية خاضعة للتفتيش والضبط، إلى جانب الأشياء المادية الأخرى (كالتجهيزات الحاسوبية). وينصّ القانون على أن الأحكام المتعلقة بتنظيم التواصل على الشبكة ونشاطات مزودي خدمات الشبكة تطبّق على أي مزود خدمات اتصال في الجمهورية العربية السورية له مركز إدارة فعلي أو مركز ثابت يمارس فيه نشاطاً اقتصادياً راهناً، وذلك بصرف النظر عن جنسيته وعن مكان تأسيسه ومقره الرئيسي إذا كان شخصاً اعتبارياً، وعن المكان الذي توجد فيه التجهيزات التقنية التي يستخدمها. وينصّ هذا المرسوم التشريعي أيضاً على حجية الدليل الرقمي، وشروط التحقق من سلامة الأدلة الرقمية المقدّمة إلى المحكمة. ويحدّد المرسوم التشريعي الاختصاص القضائي في حالات الجرائم السيبرانية بغرض توسيع الاختصاص القضائي حسب الصلاحيات الإقليمية والذاتية والشخصية والشاملة المنصوص عليها في قانون العقوبات النافذ؛ ويسمح ذلك بالنظر في كثير من القضايا المنصوص عليها في القانون أمام القضاء السوري، سواء أكانت الأفعال قد ارتكبت داخل أو خارج الأرض السورية، من قبل السوريين أو الأجانب. وينصّ المرسوم التشريعي أيضاً، في معرض تطبيقه، على اعتبار النطاق العُلوي السوري على الإنترنت (.sy) في حكم الأرض السورية.

عموماً، يتبين من دراسة للأمم المتحدة أن 60 في المائة من الدول المُستفتاة في المنطقة تفيد بأن النصوص القانونية الوطنية المتعلقة بالجرائم السيبرانية غير كافية، أو هي كافية جزئياً فقط، ولا سيما من ناحية إجراءات التحقيق وتقنياته الحديثة، كجمع الأدلة المعلوماتية عن بعد. فنصوص الإجراءات الجزائية التقليدية قد لا يمكن تفسيرها لتستوعب مسائل غير ملموسة كالبيانات وطبيعتها الآنية volatile أو العناوين الرقمية، إضافة إلى عدم قدرتها على تدارك قيام المرتكبين باستعمال وسائل تقنية لإعاقة التحقيق كالتشفير encryption والمخدّمات الوكيلة proxies والحوسبة السحابية cloud computing وتعدد المسارات routing في الإنترنت.

113 قانون مكافحة جرائم الإنترنت. متى يخرج إلي النور؟ http://www.aim-council.org/arabSecurityInfoOffice/emagazine/issue21/ecrime/Pages/Anti-cyber-crime-law.aspx، ص 1.

إضافة إلى عدم احتفاظ المؤسسات بالبيانات لعدم وجود نص قانوني يلزمها بذلك، أو احتفاظها بالبيانات لمدد قصيرة. وتستعمل بعض الدول القواعد الإجرائية الجزائية التقليدية في البحث عن بيانات الحاسوب أو طلب معلومات حركة البيانات أو المحتوى أو البيانات الشخصية للزبائن من الغير أو اعتراضها على الخط[114]. ومن الضروري تنظيم إجراءات التحقيق الجزائي من حيث البحث عن البيانات المعلوماتية وحجزها وطلبها من الغير وحفظها واعتراضها في وقت إرسالها أو إنشائها في زمنها الحقيقي real time. وفي معظم دول المنطقة، يرفض مزودو خدمات الشبكة وباقي الشركات في أغلب الأحيان تقديم أية بيانات للتحقيقات الجزائية دون طلب رسمي.

4- إصدار اللوائح أو المراسيم التنفيذية تطبيقاً للقوانين

عمدت بعض دول المنطقة إلى وضع نصوص تنفيذية تطبيقاً للقانون، يسهل إصدارها وتعديلها لمواكبة التطور التقني بسرعة ولتفصيل القانون، وذلك نظراً لبطء العملية التشريعية ولاكتفاء القانون بالمبادئ العامة في أغلب الأحيان، تاركاً التفاصيل للوائح التنفيذية أو التعاميم أو المراسيم.

وعلى سبيل المثال، فقد أصدرت الإمارات العربية المتحدة التعميم رقم (6) لسنة 2013 بشأن سياسة ومعايير حكومة أبو ظبي لأمن المعلومات. كما أصدر مجلس الوزراء الإماراتي القرار رقم 21 لسنة 2013 بشأن لائحة أمن المعلومات في الجهات الاتحادية، والتي تسري على الجهات الاتحادية وعلى الموظفين العاملين لديها، وتهدف الى تعزيز مفهوم أمن المعلومات لدى الجهات الاتحادية والمستخدمين، وتوفير إطار قانوني للجهات الاتحادية لضمان أمن الأصول المعلوماتية وتحديد معايير الاستخدام الأمثل لها، وتشجيع التطبيق الفعال للأمن الإلكتروني، وإيجاد بيئة آمنة في الجهات الاتحادية لحفظ المعلومات عن طريق ضمان سرية المعلومات والبنية الأساسية للشبكة، وحمايتها بمنع الدخول أو التعديل أو التغيير غير المصرح به لتلك المعلومات، وتحديد المخاطر المحتملة، وكيفية مواجهتها لضمان استمرارية سير العمل في الجهات الاتحادية، ودرجات السرية المتعلقة بوثائق ومستندات الجهات الاتحادية (وهي سري للغاية وسري ومحظور وعام)، والنفاذ عبر الشبكة المحلية اللاسلكية (WiFi) وشروطه، والمسؤوليات والجزاءات عن المخالفات. يضاف إلى ذلك قرار المجلس التنفيذي رقم (13) لسنة 2012 بشأن أمن المعلومات في حكومة دبي[115].

أما في الجمهورية العربية السورية، فقد أعطيت وزارة الاتصالات والتقانة، ممثلة بالهيئة الوطنية لخدمات الشبكة والهيئة الناظمة لقطاع الاتصالات، صلاحية وضع اللوائح التنظيمية المتعلقة بتنظيم التواصل على الشبكة والجرائم المعلوماتية والمخالفات والجرائم في قطاع الاتصالات. وقد صدرت بموجب ذلك مجموعة من اللوائح التنظيمية[116] المتعلقة بالسلامة المعلوماتية؛ كما صدرت اللوائح التنظيمية المتعلقة بالسياسة الوطنية لأمن المعلومات[117]. ويمكن أيضاً الإشارة هنا إلى اعتماد وزارة الاتصالات والتقانة مجموعة من المعايير الخاصة بتكنولوجيا المعلومات، منها ما يتعلق بحماية أنظمة تقانات المعلومات والاتصالات[118].

---

114 United Nations Office on Drugs and Crime, UNODC, *Comprehensive study on cybercrime*, draft, February 2013, p. 77, 122, 128, 147.

115 جريدة البيان، أبو ظبي، عدد 14 آب/أغسطس 2013، تهدف لتحديد معايير الاستخدام الأمثل للأصول المعلوماتية، لائحة أمن المعلومات الاتحادية، http://www.mohamoon-uae.com/default.aspx?action=DisplayNews&type=1&id=20981&Catid=2659، ص 1.

116 http://nans.gov.sy/index.php/nansdocuments.

117 http://nans.gov.sy/images/stories/doc/isc_doc/policy-isc.pdf.

118 http://www.moct.gov.sy/ICTSandards/ar_pdf/2.pdf.

5- الأدلة الرقمية (أو الإلكترونية أو المعلوماتية) في التشريعات

تبرز في المنطقة العربية مشكلة مدى مشروعية الأدلة الرقمية أو مدى قبولها في المحاكم كوسيلة إثبات في الجرائم السيبرانية أو حتى التقليدية، في حال لم ينص القانون صراحة عليها. ففي بعض الدول التي تتبع نظام الإثبات المقيد أو نظام الأدلة القانونية أو نظام قريب كالنظام المختلط، حيث ينص القانون حصراً على وسائل الإثبات المقبولة قانوناً ويحدد قوتها الثبوتية، كما هي الحال في ليبيا، تثار إشكالية مدى قبول الأدلة المعلوماتية لدى المحاكم[119]. أما في دول أخرى تعتمد النظام القانوني اللاتيني، ولا يوجد لديها نص ضمن قانون أصول المحاكمات الجزائية يشرع الأدلة المعلوماتية، وتعتمد نظام الإثبات الحر، حيث يعود للقاضي تكوين قناعته عن أي دليل يجده، كما هو الحال في لبنان، فالوضع مختلف ولا يوجد إشكال قانوني كبير. ففي معظم دول المنطقة، لا يميز بين الأدلة المادية والأدلة المعلوماتية، في حين أن هذا التمييز قائم في أقل من 40 في المائة من دول آسيا، وفق دراسة للأمم المتحدة[120].

ولا تتيح القوانين الإجرائية في بعض الدول سوى ضبط الأدلة المادية، وعليه يتم ضبط جهاز الحاسوب ولا يمكن نقل محتواه على قرص. كما تبرز مشكلة تحديد نطاق البحث بمسرح الجريمة أو مكان إقامة المشتبه به، وعدم وجود مرونة في مد نطاق البحث عن البيانات، ولا سيما إذا كان المشتبه به قد خزنها عن بعد على حواسيب بعيدة. كما قد لا يعرف المحققون مكان حفظ البيانات أو لا يستطيعون الوصول إليها لأسباب تقنية. وينبغي أن يمكّن التشريع المحققين من إلزام أشخاص آخرين قادرين على تخطي هذه الأسباب التقنية بتقديم المساعدة أو إلزام أي شخص ثالث بتقديم البيانات المطلوبة الموجودة في حيازته أو تحت سلطته[121]. وكذلك تُثار مشروعية تقنيات البحث عن الأدلة المعلوماتية عن بعد Remote forensic tools دون الحضور المادي إلى منزل المشتبه به. وهذه التقنية تثير عدة إشكاليات قانونية تتعلق بالحق بالخصوصية وانتهاك سيادة دول أخرى وصعوبة تنزيل هذه البرامج على حاسوب المشتبه به المحمي تقنياً.

وتظهر أيضاً إشكاليات قانونية أخرى، فمن المتعارف عليه أنه لا يتم إجبار المتهم على تقديم دليل ضد نفسه، خلافاً لما هو جار في حالة الأدلة المعلوماتية من إلزامه بتقديم بيانات أو كلمات سر حساب بريده الإلكتروني أو تقديم مفتاح التشفير. كذلك تبرز في دول المنطقة، كما هو في كثير من المناطق الأخرى، مشكلة توسع مسرح الجريمة ليشمل أكثر من دولة، وضرورة جمع الأدلة من أماكن خارج سيادة الدولة التي تتولى التحقيق في الجريمة السيبرانية. كما تعاني التحقيقات من مشاكل أخرى منها إخفاء مرتكب الجريمة لهويته الحقيقية ولمعلوماته steganography or information hiding ضمن ملفات قد تبدو بريئة، أو بواسطة التشفير أو غيرها من التقنيات، أو تهيئة جهازه لتدمير نفسه أو لمحو المعلومات عند القبض عليه.

دال- تحديات تطبيق القانون وأجهزته في المنطقة العربية

1- تعويض النقص في التشريعات

لجأت بعض الدول في المنطقة العربية إلى عدة حلول مختلفة لتعويض النقص في التشريعات السيبرانية. وعلى سبيل المثال، تولت النيابة العامة التمييزية في لبنان إصدار تعاميم موجهة إلى مزودي خدمات الاتصال لإلزامهم بحفظ معلومات حركة البيانات لمدة معينة، وذلك بانتظار إقرار سلة التشريعات

119 طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي، www.startimes.com/f.aspx?t=30245909، ص 7 وما يليها.

120 United Nations Office on Drugs and Crime, UNODC, Comprehensive study on cybercrime, draft, February 2013, p. 166.

121 ITU, Marco Gercke, *Understanding Cybercrime: Phenomena, Challenges and Legal Response,* September 2012, p. 252, 253.

المعروضة على المجلس النيابي اللبناني في هذا المجال. وكذلك فقد نظم النائب العام في مصر بموجب تعليمات صادرة عنه صلاحيات النيابة العامة لإصدار قرارات أثناء التحقيقات في القضايا، وبحيث تلتزم الشركات المصرية بذلك[122]. ويبين الإطار 7 مزيداً من التفاصيل حول حالة مصر.

كما عمد القضاء في بعض الدول إلى تطبيق النصوص التقليدية لقانون العقوبات على الجرائم السيبرانية المستجدة؛ فصدرت أحكام في لبنان تدين بجرم التخريب العادي الاعتداء على جهاز حاسوب، وبجرم التعرض للآداب العامة نشر المواد الإباحية على الإنترنت، وبجرم الاحتيال الأفعال الاحتيالية عبر شبكة الإنترنت. غير أن هذه الحلول تبقى قاصرة، ولا سيما في حالة الجرائم السيبرانية، حيث تكون المعلوماتية هي محل الاعتداء، باعتبار أن هذا النوع من الجرائم لم يظهر إلا مع المعلوماتية. ولا ينبغي القياس في النصوص العقابية (الجزائية) والتوسع في تفسيرها عملاً بمبدأ حصرية تفسيرها ومبدأ "لا جريمة ولا عقوبة دون نص". ولذلك، لم يستطع القضاء اللبناني في كثير من القضايا تجريم بعض الأفعال وأحال المرتكبين والضحية أمام القضاء المدني للمطالبة بالتعويض عن الضرر الحاصل، مثل حالة سرقة حساب بريد إلكتروني أو اختراق نظام معلوماتي.

أما في الجمهورية العربية السورية، فقد قامت فلسفة المشرّع عند وضع قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية على تقسيم الجرائم المعلوماتية إلى نوعين: الأول هو الذي يكون فيه الحاسوب أو الشبكة مجرد وسيلة تسمح بارتكاب الجريمة، وهي غالباً جرائم اعتيادية (مثل جريمة التهديد عن طريق الإنترنت)، لكنّ الضرر منها عادة ما يكون أعظم؛ والثاني هو الذي تكون فيه المنظومة المعلوماتية أو الشبكة موضوعاً للجريمة (مثل اختراق المنظومات المعلوماتية وتخريبها)، وهي غالباً جرائم مستحدثة لا بدّ من النصّ على أركانها ومعاقبتها. وقد نصّ القانون صراحة على النوع الثاني من الجرائم، وحدّد عقوباتها. أما في حالة الجرائم المنصوص عليها في القوانين الجزائية النافذة الأخرى، فقد نصّ القانون على مضاعفة الحدّ الأدنى للعقوبة المقرّرة لها إذا ارتُكب النشاط الجرمي باستخدام الشبكة أو وقع على الشبكة، أو إذا وقع النشاط الجرمي على جهاز حاسوبي أو منظومة معلوماتية بقصد التأثير على عملها أو على المعلومات أو البيانات المخزّنة فيها؛ والهدف من ذلك توحيد النصّ التشريعي وعدم تكرار أشكال الجرائم الاعتيادية عندما تُرتكب بالوسائل المعلوماتية أو تقع على المنظومات المعلوماتية. ومن أشكال النوع الثاني من الجرائم المعلوماتية، على سبيل المثال لا الحصر: الذم والقدح، وإنتاج محتوى يتعلق بإباحية القاصرين على منظومة معلوماتية، أو توزيعه أو حيازته، والترويج لجرائم الاتّجار بالأشخاص، والتحريض على ارتكاب الجرائم بوسيلة معلوماتية.

الإطار 7- تطبيق التشريعات العامة من قبل القضاء المصري على الجرائم السيبرانية

اعتمد القضاء المصري حلولاً مشابهة لتلك التي توصل إليها القضاء في لبنان. فعلى سبيل المثال، يبدو من الواضح خلو بعض التشريعات العربية من إدراج ثبوت جريمة القدح والذم عبر المراسلات الإلكترونية كأحد وسائل التعبير التي تقوم معها جريمة القدح والذم. لكن نص المادة 171 من قانون العقوبات المصري ترك الباب مفتوحاً للاجتهاد بإدراجه عبارة "وبأية طريقة أخرى"، فيستفاد منها أن البريد الإلكتروني يعد من الوسائل التي تستخدم في التعبير ومعها تقوم جريمة القدح والذم إذا ما توافرت أركان الجريمة[أ]. كما قضى القضاء المصري أن قانون براءات الاختراع ينطبق على الجانب المادي من نظام المعالجة الآلية للمعلومات، وطبّق نصوص قانون حماية الحياة الخاصة وقانون تجريم إفشاء الأسرار على بعض الجرائم المعلوماتية[ب].

أ بهنسي سمير بهنسي، جرائم الحاسب الآلي والإنترنت، بحث مقدم الى قسم الدراسات العليا، دبلوم القانون العام - جامعة الاسكندرية - كلية الحقوق، ص 12.

ب محمد عبد الله منشاوي، جرائم الانترنت من منظور شرعي وقانوني، 1-11-1423هـ، http://www.khayma.com/education-technology/Study33.htm ص 11.

122 جواب الجمعية العربية للتحكيم الإلكتروني على الاستبيان المرسل لها من قبل الإسكوا في إطار هذه الدراسة، أيلول/سبتمبر 2014.

2- ضعف أجهزة التحقيق

تبقى الكثير من الجرائم السيبرانية في المنطقة العربية دون تحقيق فعال ولا يكتشف فيها المجرم بسبب محدودية الموارد المتوفرة لدى أجهزة التحقيق، ولا سيما في الدول ذات الإمكانيات المادية القليلة. وحتى على صعيد العالم، تبين، في دراسة موّلتها شركة الدفع الإلكتروني على الخط Paypal، أن الجريمة السيبرانية المتعلقة بقيمة تقل عن 25000 دولار لا يتم التحقيق فيها ولا ملاحقة فاعليها، خلافاً للجرائم التقليدية التي تتولى التحقيق فيها الشرطة بسرعة وفعالية. وتعود أسباب ذلك إلى النقص في التمويل وعدم توفر الخبرات في مجال الجرائم السيبرانية في الأجهزة الرسمية وعدم وجود مستوى عالٍ من التعاون على الصعيد الدولي وتبادل المعلومات، ونظراً للطابع الدولي العابر للحدود للجريمة السيبرانية، وللحد الأدنى المطلوب لقيمة فتح ملف شكوى[123].

ومن المعوقات أيضاً في بعض دول المنطقة، ضعف تجهيز وحدات الشرطة المتخصصة في الجرائم السيبرانية. وقد أوردت دراسة صادرة عن الأمم المتحدة أن الدول النامية في آسيا أبدت حاجتها إلى أدوات لفحص الأدلة الجنائية المعلوماتية، وأن ما لديها قد تخطاه الزمن[124]. كما يبرز التحدي عند تحليل كميات هائلة من البيانات المعلوماتية أو أجهزة أو برامج معلوماتية حديثة.

ويلاحظ أيضاً وجود تفاوت بين الأجهزة المتخصصة للشرطة في مجال الجرائم السيبرانية، ففي الدول النامية، تفتقر هذه الوحدات إلى الخبرات والتجهيز، ويقدر عددها بنحو 0.2 لكل 100,000 مستخدم إنترنت، أي أقل بنحو ضعفين إلى خمسة أضعاف من الدول الأكثر تقدماً. وفي بعض الحالات، لا تتوفر لدى عناصر الشرطة المتخصصة إلا تجهيزات معلوماتية بدائية وخبرات معلوماتية أساسية غير متقدمة. أما في الدول المتقدمة، تبلغ نسبة العناصر ذات الكفاءة العالية المزودة بتجهيزات معلوماتية معقدة ومتطورة 70 في المائة من مجموع العناصر المتخصصة[125].

3- غياب أو ضعف وحدات التحقيق المتخصصة

تظهر بعض ملامح التقدم في بعض الدول العربية بإنشاء وحدات متخصصة في الشرطة للتحقيق في قضايا الجرائم السيبرانية وفي جمع الأدلة المعلوماتية وتحليلها. وتضم هذه الوحدات فنيين مختصين في المعلوماتية يتلقون تدريباً مناسباً، ويعملون على تجهيزات وبرامج لمعالجة الأدلة المعلوماتية. ولهذه الوحدات صلاحيات محددة وواضحة لا تتعارض مع صلاحيات وحدات أخرى. ومن هذه الوحدات إدارة المباحث الإلكترونية التي أسست في دبي في عام 2008، وقسم الإسناد والتحقيق في الجرائم السيبرانية في مديرية الأمن العام في إدارة البحث الجنائي في الأردن[126]. إضافة إلى مكتب مكافحة جرائم المعلوماتية وحماية الملكية الفكرية في لبنان الذي تم إنشاؤه عام 2006 ضمن إطار قسم المباحث الجنائية الخاصة في الشرطة القضائية في قوى الأمن الداخلي، والذي يضمّ نحو 40 عنصراً، البعض منهم متخصص في تكنولوجيا المعلومات، وقد نجح المكتب في حل العديد من قضايا الجرائم السيبرانية.

123 Robert Winters, *Practical steps to combat computer crime*, August 2013, http://cjfocus.com/2013/08/06/practical-steps-to-combat-computer-crime, p. 1.

124 United Nations Office on Drugs and Crime, UNODC, *Comprehensive study on cybercrime*, draft, February 2013, p. 153.

125 United Nations Office on Drugs and Crime, UNODC, *Comprehensive study on cybercrime*, draft, February 2013, p. 152, 154.

126 جواب مركز تكنولوجيا المعلومات الوطني على الاستبيان المرسل له في إطار هذه الدراسة، الأردن، أيلول/سبتمبر 2014.

ومن الأمثلة الأخرى، أنشأت وزارة الداخلية المصرية عام 2002 إدارة لمكافحة جرائم الحاسب الآلي وشبكة المعلومات "وحدة شبكات البيانات والجريمة السيبرانية"، لتتولى رصد جرائم تكنولوجيا المعلومات وتعقب مرتكبيها باستخدام أحدث النظم الفنية والتقنية الحديثة. وقد خصصت الوحدة خط الهاتف الساخن 108 لتقصي الجرائم السيبرانية[127]. ونشير أيضاً إلى مبادرة دولة الإمارات العربية المتحدة، السباقة في المنطقة، حول مشروعها المستقبلي بإنشاء محاكم خاصة بالجريمة الإلكترونية، وتدريب القضاة ووكلاء الادّعاء على استقصائها وتبيان عناصرها وأدلتها الجرمية المعلوماتية[128].

أما في الجمهورية العربية السورية، فقد نص قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية على أن تُحدث في وزارة الداخلية ضابطة عدلية مختصّة تكلّف باستقصاء الجرائم المعلوماتية، وجمع أدلتها الرقمية، والقبض على فاعليها، وإحالتهم على المحاكم الموكلة بمحاكمتهم. وتستعين هذه الضابطة العدلية بخبراء دائمين أو مؤقتين، من وزارة الدفاع، ووزارة العدل، ووزارة الاتصالات والتقانة، لتنفيذ المهام الموكلة إليها. ويسمح لهذه لضابطة العدلية القيام بعمليات التقصي الإلكتروني، بناءً على إذن من السلطة القضائية المختصّة؛ وعلى كل صاحب أو مدير أي منظومة معلوماتية تُرتكب جريمة معلوماتية باستخدام منظومته، أن يتيح للضابطة العدلية تفتيش وضبط البيانات والمعلومات والبرمجيات الحاسوبية، والحصول على نسخة منها؛ ويمكن في حالات الضرورة ضبط الأجهزة والبرمجيات الحاسوبية المستخدمة أو جزء من مكوّناتها. كما أطلقت وزارتا العدل والاتصالات والتقانة في الجمهورية العربية السورية، في عام 2014، مشروعاً مشتركاً لتدريب القضاة على تطبيق القوانين الإلكترونية، وفي مقدمتها قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية، وقانون التوقيع الإلكتروني، وقانون الاتصالات.

4- إشكالية الاختصاص القضائي

تواجه أجهزة تطبيق القانون تحديات، ليست فقط تقنية، بل ما يتعلق منها بالاختصاص القضائي من حيث ملاحقة الجرائم السيبرانية والتحقيق فيها. فمرتكبي الجرائم والضحايا يوجدون في العالم المادي، في حين ترتكب الجرائم في العالم الافتراضي، كذلك توجد المخدّمات الحاسوبية وأجهزة الاتصال في أماكن مادية مختلفة عن تلك العائدة للمرتكبين أو الضحايا[129]. كما قد يتوزع الركن المادي للجريمة السيبرانية في دول عدة مما يثير إشكاليات تحديد مكان هذه الجرائم. وبشكل عام تثير بعض الجرائم السيبرانية إشكالية تعيين مكان إرتكاب هذه الجرائم السيبرانية نظراً لطبيعتها العابرة للحدود الجغرافية.

ومن الناحية القضائية يشكل موضوع "التجريم المزدوج"، والذي يعني تجريم الفعل في دولة وعدم تجريمه في دولة أخرى، إشكالية أيضاً عند البت في الجرائم السيبرانية ومحاكمة أو متابعة الجناة. هذا وقد تظهر مشكلة أخرى في هذه الجرائم العابرة للحدود وذلك عند الانتقال من نظام قانوني إلى نظام قانوني آخر، كالانتقال من النظام Anglo-saxon إلى النظام Roman-Germanique، في الدول التي يجري فيها معالجة الجريمة السيبرانية. وهذه الإشكاليات خاصة بانعقاد الاختصاص لدولة دون أخرى، مما قد يثير التنازع الإيجابي أو السلبي لتحديد القضاء الأكثر ملاءمة للفصل في الدعوى قضائياً.

---

127 الإسكوا، الملامح الوطنية لمجتمع المعلومات لجمهورية مصر العربية، 2013.

128 جريدة دار الخليج، دبي، الثلاثاء 14 كانون الأول/ديسمبر 2010، المشاركون في اجتماع الإنتربول يشيدون بإنشاء محاكم للجريمة الإلكترونية، http://www.mohamoon-uae.com/default.aspx?Action=DisplayNews&type=3&ID=12864، ص 1.

129 Kristin M. Finklea, Catherine A. Theohary, *Cybercrime: Conceptual issues for Congress and U.S. law enforcement*, January 2013, http://fas.org/sgp/crs/misc/R42547.pdf, p. 10.

هاء- مراكز الاستجابة لطوارئ الحاسوب في المنطقة العربية

تماشياً مع التوجه العالمي نحو إنشاء هيئات من قبل الدولة للعمل في مجال الأمن السيبراني، بادر عدد من الدول في المنطقة إلى إنشاء مركز وطني للاستجابة لطوارئ الحاسوب. وتجدر الإشارة إلى ضرورة التمييز بين دور مراكز الاستجابة لطوارئ الحواسيب والضابطة العدلية. ومركز الاستجابة لطوارئ الحاسوب له دور وقائي توعوي تقني، وقد يتدخل حتى في حال عدم حصول جرم جزائي. أما الضابطة العدلية فتتولى التحقيق بعد حصول الفعل الجرمي، أي بصورة لاحقة علاجية عقابية لا وقائية، ولا تتدخل إلا عند حصول جرم جزائي، إلا أنها في بعض الأحيان قد تستعين في تحقيقاتها بالخبرات التقنية لمركز الاستجابة لطوارئ الحاسوب.

تم إنشاء مركز الاستجابة لطوارئ الحاسب الآلي (aeCERT)[130] في الإمارات العربية المتحدة بهدف تحسين معايير وممارسات أمن المعلومات وحماية البنية الأساسية لتقنية المعلومات من المخاطر والهجمات السيبرانية، وكذلك من أجل نشر أفضل الممارسات والتجارب ومكافحة جرائم الإنترنت ومساعدة الجهات المختصة في التحقيقات العدلية والتوعية حول أمن المعلومات وتقديم المشورة الفنية، وكذلك أيضا لإنشاء مركز للإبلاغ عن الجرائم السيبرانية وجمع المعلومات عنها وعن مخاطر الأمن السيبراني ورصدها وتحليلها واختبارها وتتبعها والعمل كآلية إنذار مبكر. كما أنشأت إمارة دبي بموجب قانون صدر عام 2014 مركزاً للأمن الإلكتروني ومكافحة جرائم المعلوماتية. كما أن هناك دول في المنطقة مثل لبنان بصدد إنشاء مركز كهذا، إدراكاً منها لأهميته.

كما أنشأ السودان في 1 كانون الثاني/يناير 2010، بمبادرة من الهيئة القومية للاتصالات، المركز السوداني لأمن المعلومات للاستجابة لحوادث أمن المعلومات، ولتقديم المشورة الفنية للمواطنين والشركات في هذا المجال ومساعدة الجهات العدلية في تتبع الجريمة الإلكترونية[131]. وقد سبق للسودان أن أقر قانون مكافحة جرائم المعلوماتية عام 2007 وقانون المعاملات الإلكترونية وقانون المصنفات الفنية والأدبية في عام 2001.

وأنشأت سلطنة عُمان المركز الوطني للسلامة المعلوماتية (OCERT) في نيسان/أبريل 2010[132]. كما تستضيف سلطنة عمان المركز الإقليمي للأمن الإلكتروني للمنطقة العربية، التابع للاتحاد الدولي للاتصالات. ويهدف المركز الإقليمي للأمن الإلكتروني للمنطقة العربية، والذي يديره المركز الوطني للسلامة المعلوماتية بسلطنة عمان، إلى تقديم الخدمات والمبادرات للمنطقة العربية لتحسين قدرات الأمن الإلكتروني عن طريق التنسيق وتعزيز التعاون الإقليمي في هذا المجال[133].

وكذلك أنشأت قطر في كانون الأول/ديسمبر 2005 ضمن المجلس الأعلى لتكنولوجيا المعلومات والاتصالات (ictQATAR) مركز الاستجابة لطوارئ الحاسب الآلي (Q-CERT)[134]. كذلك فعلت المملكة العربية

130 يراجع الموقع الإلكتروني للمركز www.aecert.ae.

131 يراجع الموقع الإلكتروني للمركز www.cert.sd.

132 يراجع الموقع الإلكتروني للمركز www.cert.gov.om.

133 جواب المركز الوطني للسلامة المعلوماتية بهيئة تقنية المعلومات على الاستبيان المرسل له من قبل الإسكوا في إطار هذه الدراسة، سلطنة عُمان، أيلول/سبتمبر 2014.

134 يراجع الموقع الإلكتروني للمركز www.qcert.org.

السعودية[135]. كما سبق للوكالة الوطنية للسلامة المعلوماتية في تونس أن أسست مركز الاستجابة لطوارئ الحاسب الآلي (tunCERT) لديها عام 2007[136]. كما توجد في مصر إدارة عليا فى الجهاز القومي لتنظيم الاتصالات ومركز للاستعداد لطوارئ الحاسبات والشبكات EG CERT، وتتولى أيضاً تقديم الخبرة الفنية في فحص الأدلة في الجرائم السيبرانية[137]. وفي الأردن، تم إنشاء مركز للاستجابة لطوارئ الحاسوب، إلا أنه بحاجة للتدريب والتجهيز[138]. كما تعمل دولة الكويت حالياً على تنفيذ مركز الاستجابة لطوارئ الحاسوب تحت مظلة الجهاز المركزي لتكنولوجيا المعلومات[139].

وفي الجمهورية العربية السورية، تم في الهيئة الوطنية لخدمات الشبكة إحداث مركز أمن المعلومات، الذي سيحتضن لاحقاً مركز الاستجابة لطوارئ الحاسوب SyCERT. ويقوم مركز أمن المعلومات حالياً بإصدار نشرات دورية عن التنبيهات الأمنية، وأدلة عن الثغرات الأمنية، ويقدّم للمؤسسات خدمات في أمن المعلومات مثل خدمة المسح الأمني للمواقع الإلكترونية لاختبار وجود الثغرات الأمنية، وتقديم الدعم الفني للجهات الحكومية في حال اختراق موقعها الإلكتروني أو نشر بيانات ومعلومات خاصة بها دون تصريح[140].

وقد قامت بعض مراكز الاستجابة لطوارئ الحاسوب العربية بإنجازات ملموسة. مثلاً، تولى المركز السوداني لأمن المعلومات تحليل الدودة المعلوماتية الخطيرة دوكو Duku والتصدي لها، وأشادت شركة كاسبرسكي للبرمجيات بأعماله على صفحتها على الفيسبوك[141]. وتتمتع بعض المراكز بصلاحيات كبيرة للقيام بعملها. فعلى سبيل المثال، وطبقا لقانون السلامة المعلوماتية في تونس رقم 5 لسنة 2004 في مادته الخامسة تخضع النظم المعلوماتية والشبكات الراجعة بالنظر إلى مختلف الهياكل العمومية، باستثناء النظم المعلوماتية وشبكات وزارتي الدفاع الوطني والداخلية والتنمية المحلية، لنظام تدقيق إجباري ودوري للسلامة المعلوماتية. كما تنص المادة 11 من ذات القانون على أنه يمكن للوكالة الوطنية للسلامة المعلوماتية، من أجل حماية النظم المعلوماتية والشبكات، في حالة الهجمات والاختراقات، اقتراح عزل النظام المعلوماتي أو الشبكة المعنية إلى أن تتوقف هذه الاختراقات ويتم هذا العزل بمقتضى قرار من الوزير المكلف بتكنولوجيات الاتصال. ويتضمن الجدول 1 قائمة بأسماء مراكز الاستجابة لطوارئ الحاسوب في المنطقة العربية وسنة إنشاء كل منها.

أما على الصعيد العملي وآليات الرقابة الروتينية، فمعظم دول المنطقة العربية لديها نسب مختلفة، ومتدنية قياساً بتلك النسب السائدة في العالم، والخاصة بالحفاظ على الأمان السيبراني. إذ يتبين عدم وجود آليات فعالة لمراقبة تطور الوضع على صعيد الأمان السيبراني ومكافحة الجرائم السيبرانية، فقد تم اكتشاف فقط 5 في المائة من عمليات الاحتيال بفضل آليات الرقابة الروتينية[142]. كما أن محاربة الجرائم السيبرانية

---

135 يراجع الموقع الإلكتروني للمركز www.cert.gov.sa.

136 يراجع الموقع الإلكتروني للمركز tuncert.ansi.tn.

137 جواب على الاستبيان المرسل من قبل الإسكوا في إطار هذه الدراسة، مصر، أيلول/سبتمبر 2014.

138 جواب مركز تكنولوجيا المعلومات الوطني على الاستبيان المرسل له في إطار هذه الدراسة، الأردن، أيلول/سبتمبر 2014.

139 جواب الجهاز المركزي لتكنولوجيا المعلومات على الاستبيان المرسل له في إطار هذه الدراسة، الكويت، أيلول/سبتمبر 2014.

140 http://nans.gov.sy/index.php/nansdocuments/99-docsisc.

141 القاضي حسن محمد علي حسن، تجربة المركز السوداني لأمن المعلومات، المؤتمر الثالث لأمن وسلامة الفضاء السيبراني، بيروت، آب/أغسطس 2014، ص 20.

142 John Wilkinson, Tareq Haddad, PWC, Economic Crime in the Arab World, February 2014, http://www.pwc.com/m1/en/publications/gecs2014reportme.pdf, p. 1.

تكون من خلال التطبيق الفعال للقانون لا بتقييد الوصول الشرعي إلى الإنترنت. ومن المفيد منع المرتكبين من الوصول إلى مخترقي الشبكة المحترفين Hacker الذين يؤجرون خدماتهم[143].

الجدول 1- مراكز الاستجابة لطوارئ الحواسيب في المنطقة العربية

الدولة	اسم المركز	الموقع الإلكتروني	سنة الإنشاء
الإمارات العربية المتحدة	مركز الاستجابة لطوارئ الحاسب الآلي aeCERT	www.aecert.ae	2008
الأردن	فريق الاستجابة لطوارئ الحاسوب		2013
الكويت	مركز الاستجابة لطوارئ الحاسبات		قيد الإنشاء
المملكة العربية السعودية	المركز الوطني الإرشادي لأمن المعلومات	www.cert.gov.sa	
الجمهورية العربية السورية	مركز الاستجابة لطوارئ الحاسوب SyCERT في مركز أمن المعلومات التابع للهيئة الوطنية لخدمات الشبكة		قيد الإنشاء
السودان	المركز السوداني لأمن المعلومات	www.cert.sd	2010
تونس	مركز الاستجابة لطوارئ الحاسب الآلي tunCERT	www.tuncert.ansi.tn	2007
سلطنة عمان	المركز الوطني للسلامة المعلوماتية OCERT	www.cert.gov.om	2010
قطر	مركز الاستجابة لطوارئ الحاسب الآلي Q-CERT	www.qcert.org	2005
مصر	مركز الاستعداد لطوارئ الحاسبات والشبكات EG CERT		2010

واو- التنسيق الإقليمي والتعاون بين الدول في المنطقة العربية

تفتقر دول المنطقة العربية إلى التعاون القضائي الفعال في مجال تحقيقات الجرائم السيبرانية. وعلى الرغم من وضع واعتماد الاتفاقية العربية بتاريخ 2 كانون الأول/ديسمبر 2010 المتعلقة بمكافحة جرائم تقنية المعلومات، والتي تضمنت فصلاً كاملاً (الفصل الرابع) حول التعاون القانوني والقضائي، والذي ينص على تلبية طلبات الدول بخصوص تسليم المجرمين وجمع الأدلة وحفظ وتسليم البيانات والمعلومات وحركة البيانات والمحتوى، وكذلك إنشاء نقطة اتصال للمساعدة وإمكانية إرسال طلب المساعدة العاجل بالفاكس أو البريد الإلكتروني؛ لا يزال التعاون غير فعال بين الدول العربية. وتشير الدراسات إلى أن أحد أسباب ارتفاع الجرائم السيبرانية هو عدم التعاون في ما بين الدول، ففي الإمارات العربية المتحدة، ارتفعت نسبة الجرائم السيبرانية بمعدل 25 في المائة عام 2014 عن الأعوام السابقة، وأحد أسباب هذا الارتفاع ضعف التعاون مع دول الشرق الأوسط والعالم[144].

أما القانون العربي الاسترشادي لمكافحة جرائم تقنية المعلومات[145] وما يتعلق بها، فلم يتضمن نصوصاً ذات طابع إجرائي، أو نصوصاً حول التنسيق والتعاون الدولي، بل تضمن فقط قواعد موضوعية تفصّل جرائم تقنية المعلومات. وتجدر الإشارة أيضاً إلى أهمية القانون العربي الاسترشادي للإثبات بالتقنيات الحديثة لعام 2008 والقانون العربي الاسترشادي للمعاملات والتجارة الإلكترونية لعام 2009، حيث أنهما يساهمان حكماً في الأمان السيبراني من خلال تأكيد هوية المتعامل بالتوقيع الإلكتروني وشهادات التصديق، وكذلك حماية المستهلك في مجال التجارة الإلكترونية وإثبات تعاملاته الإلكترونية.

143 The White House, *International Strategy for Cyberspace, Prosperity, security and Openness in a networked World*, May 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, p. 24.

144 لواء النعساني، ص 3 http://www.24.ae/article.aspx?ArticleId=77807.

145 http://www.carjj.org/node/246.

وعدم وجود تعاريف موحدة للجرائم السيبرانية يعيق التعاون بين دول المنطقة، فبعض الأفعال قد تكون مجرمة في دولة وغير مجرمة في دولة أخرى، وهو ما يدعى في المجال القضائي بالتجريم المزدوجة. كما أن العقوبات المقررة لكل فعل جرمي في كل دولة قد تكون مختلفة ومتباينة، فبعضها قد يكتفي بالغرامات (مخالفة) أو بالحبس البسيط (جنحة) وبعضها قد يشدد العقوبات (جنحة مشددة أو جناية).

زاي- التحديات الخاصة بالقطاع الخاص في المنطقة العربية

تجهد مؤسسات القطاع الخاص في المنطقة العربية في محاولة فهم الجرائم السيبرانية وادراك مخاطرها وكيفية الوقاية منها، وتفادي وقوعها ضحية للهجمات السيبرانية. ويبدو أنه من الصعب إجراء تقديرات دقيقة حول حجم الخسارة المادية الناتجة عن الجرائم السيبرانية في المنطقة العربية. ومن التحديات التي تواجه الأمن السيبراني في القطاع الخاص: تكاليف اعتماد أنظمة الأمان وتوقف الأعمال، والخسائر المترتبة عن الجرائم السيبرانية على الدخل، وكذلك على الأنظمة الالكترونية، وتشويه السمعة، وإضاعة الفرص نتيجة تجنب بعض البضائع والأسواق بفعل الجرائم السيبرانية. وقد بينت بعض الدراسات[146]، أن 40 في المائة من المؤسسات المشاركة في المسح لم تتكبد أية خسائر نتيجة الجرائم السيبرانية التي تعرضت لها، وهي نسبة مقلقة حيث أنه في كثير من الأحيان لا يُكتشف الضرر إلا لاحقاً، أو لا يتم تقييمه بدقة. بينما قدرت 6 في المائة من المؤسسات خسائرها نتيجة الجرائم السيبرانية، بأكثر من مليون دولار أمريكي، و2 في المائة منها بين 5 و100 مليون دولار. كما تم تقدير حجم الأضرار السنوية الناتجة عن الجرائم السيبرانية في الولايات المتحدة الأمريكية بأكثر من 67 مليار دولار[147].

ويؤدي الوضع الاقتصادي في بعض دول المنطقة وانخفاض دخل الفرد إلى تفاقم التعدي على الملكية الفكرية ونسخ البرامج المعلوماتية والأفلام والأغاني الرقمية. ويتفاوت حجم هذه الانتهاكات بين دول المنطقة وبين المناطق التي تطبق قوانين صارمة في هذا المجال وتوفر موارد بشرية كافية، تكون مدربة على تقصي هذا النوع من الانتهاكات القانونية. وفي الإمارات العربية المتحدة، على سبيل المثال، كشفت شرطة أبو ظبي في عام 2008 عن ازدياد عمليات ضبط البرمجيات غير القانونية والمنسوخة خلال عام 2007، بنسب غير مسبوقة، وصلت إلى 107 في المائة مقارنة بالعام الذي سبقه[148].

وفي الواقع يبحث مجرمو الفضاء السيبراني عن أماكن الضعف في البلدان النامية، كما هو الحال في المنطقة العربية، حيث لا تتوفر آليات فعالة لمكافحة الجرائم السيبرانية، ويقومون بالتالي باستغلال الثغرات في النظام القانوني أو ضعف إمكانات أجهزة إنفاذ القانون. كما يبدو أن المرتكبين يلجؤون إلى تبادل المعلومات والبيانات لمساعدة بعضهم في أعمالهم الإجرامية. مما يؤدي إلى تزايد الخوف لدى المستخدمين والقطاع الخاص من الجرائم السيبرانية في منطقة الشرق الأوسط بشكل أكبر مما هو في الدول المتقدمة لضعف الثقة بالإجراءات القانونية والإجرائية المطبقة للحفاظ على الأمان السيبراني.

---

146 John Wilkinson, Tareq Haddad, PWC, Economic Crime in the Arab World, February 2014, http://www.pwc.com/m1/en/publications/gecs2014reportme.pdf, p. 16.

147 See 2005 FBI Computer Crime Survey, page 10.

148 جريدة الإمارات اليوم، الإثنين 16 حزيران/يونيو 2008، أحمد عابد، شرطة أبو ظبي حذّرت من شرائها أو استخدامها، قضايا البرمجيات المقلدة ترتفع 107 في المائة، http://www.mohamoon-uae.com/default.aspx?Action=DisplayNews&type=3&ID=4527، ص 1.

ومن مكامن الضعف على صعيد مزودي خدمات الشبكة في المنطقة العربية، أن السياسات أو القواعد القانونية قد تشكل عائقاً أمام تدخلهم لإيقاف نقل البيانات العائد للمجرمين من شبكتهم، بسبب مبدأ حياد الشبكة Network Neutrality، أو منعهم من مراقبة المحتوى احتراما للخصوصية أو تبادل المعلومات حول هذا النشاط الإجرامي مع مشغلين آخرين[149]. وتعاني بعض دول المنطقة، ومنها لبنان، من وجود فوضى في قطاع الاتصالات والإنترنت، فعدد من مزودي خدمات شبكة الإنترنت يعملون من دون ترخيص أو مراقبة من قبل وزارة الاتصالات ولا يحفظون معلومات حول حركة البيانات أو سجلات عن هوية المستخدمين.

حاء- التحديات المتعلقة بالثقافة والتوعية حول الأمان السيبراني في المنطقة العربية

وفيما يتعلق بممارسات مرتكبي الجرائم السيبرانية في دول المنطقة وردّات فعل الرأي العام عليها، فهي تبدو مشابهة أحياناً لتلك السائدة في العالم وتتفاوت معها أحياناً أخرى. إذ تتداخل معها عوامل اجتماعية أو ثقافية أو دينية أو اقتصادية، مرتبطة بخصوصيات المنطقة العربية. وتبرز تحديات تتعلق بالمفاهيم الاجتماعية والدينية والإنسانية السائدة في مجتمعاتنا الشرقية، والتي تفرض قواعد خاصة تختلف عن تلك المطبقة في دول الغرب. وهنا يتضح دور قواعد السلوك والتصرف المفترض مراعاتها من قبل الجميع في تعاملاتهم على الإنترنت، أي من قبل مزودي خدمات الاتصال والمستخدمين على حد سواء. إلا أن قواعد السلوك والتصرف هذه ما زالت غير مقننة وغير منشورة في كثير من دول المنطقة.

وعلى سبيل المثال، يميل المستخدمون في المنطقة العربية في بعض الحالات إلى استعمال الإنترنت لتوسيع دائرة معارفهم الاجتماعية والمهنية، عبر الاتصال بأشخاص لم يعرفوهم من قبل، مما يعرضهم للمخاطر. وتظهر بين الحين والآخر إشكاليات عديدة تنتج عن عدم مراعاة قاعدة سلوكية معينة، فمثلاً قامت دولة الإمارات العربية المتحدة في الآونة الأخيرة بإلزام جميع المشتركين في موقع فيسبوك التقيّد بشروط قد تخالف قواعد الموقع ولكنها تلبي القانون الإماراتي، ومنها ألاّ يرفق المستخدم أسماء المستخدمين الآخرين عند نشر المحتوى دون الحصول على موافقتهم، وذلك باعتبار أن القانون الإماراتي يحمي خصوصية الأفراد وسمعتهم[150].

1- إدراك المخاطر السيبرانية في دول المنطقة

أشارت دراسة أجرتها وزارة الاتصالات وتكنولوجيا المعلومات في قطر عام 2014 في 14 بلداً[151]، أن الأشخاص في المنطقة العربية لا يعون كثيراً المخاطر السيبرانية. فالأشخاص في دول منطقة الشرق الأوسط وشمال أفريقيا، وبالرغم من أن عدداً كبيراً منهم (45 في المائة) يصرح أنه يتوخى الحذر بتصرفاته على الإنترنت، وأنه يتفحص ضبط الخصوصية والأمن على الخط، هم أكثر انفتاحاً من أولئك الذين هم في مناطق أخرى لإقامة اتصال على الخط مع أشخاص لا يعرفونهم أو لم يلتقوا بهم فعلياً، كما أنهم يميلون أكثر من غيرهم إلى فتح رسائل بريد إلكتروني وملحقاتها الصادرة عن مصادر مجهولة، وإلى تنزيل ملفات عن

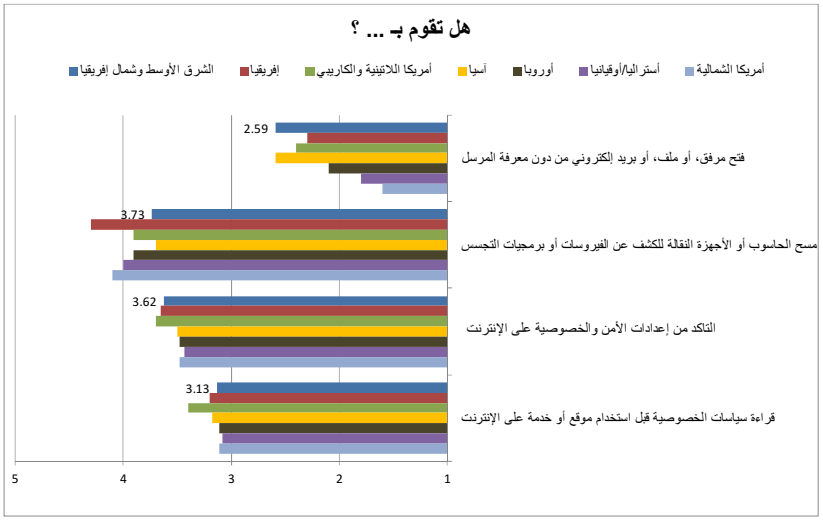
149 Micheal Barrett, Andy Steingruebl, Bill Smith, *Combating Cybercrime: Principles, Policies and Programs*, April 2011, https://www.paypal-media.com/assets/pdf/fact_sheet/PayPal_CombatingCybercrime_WP_0411_v4.pdf, p. 5.

150 دولة الإمارات العربية المتحدة "ورقة عمل" حول استخدام موقع التواصل الاجتماعي "فيسبوك"، http://arabic.cnn.com/middleeast/2014/05/21/facebook-uae-law، ص 1.

151 Ministry of information and communications technology, Qatar, Rassed, *The attitudes of online users in the MENA region cybersafety, security and data privacy*, May 2014, http://www.ictqatar.qa/sites/default/files/Cybersafety,%20security%20and%20data%20privacy.pdf, p. 3, 10, 31.

الإنترنت، ولا يجرون مسحاً لحواسيبهم بالبرامج المضادة للفيروسات المعلوماتية وبرامج التجسس، مع أنهم أكثر تخوفاً من الإنترنت وأقل ميلاً لإجراء معاملات التجارة الإلكترونية أو العمليات المصرفية على الخط. وهم يعتقدون كباقي المستخدمين في العالم أن خدمات المصارف والمؤسسات المالية الإلكترونية على الإنترنت هي أكثر أمناً من غيرها من الخدمات، تليها الخدمات الصحية ومن ثم خدمات السلطات الحكومية (انظر الشكل 5 لمزيد من التفاصيل).

الشكل 5- تصرفات الأشخاص على الإنترنت في ما يخص الأمان السيبراني



المصدر: http://www.ictqatar.qa/sites/default/files/Cybersafety.20privacy.pdf في المائة20data في المائة20and في المائة20security في المائة

ومن المعتقدات الشائعة لدى الرأي العام أن المخاطر على الأنظمة المعلوماتية تأتي من داخل المؤسسة لا من خارجها، فـ 9 في المائة من المستطلعين في منطقة الشرق الأوسط هم من هذا الرأي[152]. كذلك يعتقد مستخدمو الهواتف النقالة أو الذكية والألواح الإلكترونية خطأً أنها أكثر أمناً من الحواسيب. وتدل الدراسات على أن معظم مستخدمي الإنترنت في الدول المتقدمة والنامية يطبقون تدابير الأمن الأساسية؛ ويشذ عن ذلك القاصرون والأطفال الذين نادراً ما يستخدمون هذه التدابير، وكذلك الشركات الصغيرة والمتوسطة التي تعتقد أنها غير مستهدفة أو قلما تتخذ هذه التدابير[153].

ولعل بعض الأشخاص في المنطقة العربية الذين لا يستعملون الحاسوب يعتقدون أنهم بغنى عن التعرف على هذا الحقل المستجد وكيفية الحماية فيه، إلا أنهم، كالغالبية العظمى من الناس، يستعملون أجهزة هاتف نقال ذكية، وقد يقومون بتحميل تطبيقات عليها. إن مخاطر الهواتف النقالة الذكية هي أكبر من مخاطر أجهزة الحاسوب التي تتمتع بحماية ضد الفيروسات والتجسس، في حين أن برامج الحماية في الهواتف هي ضعيفة حالياً؛ لا بل إن معظم التطبيقات على الهواتف الذكية هي من صنع أفراد لا شركات، وقد يخفون داخلها برامج احتيالية malicious code. كما أن شركات البرمجة هي أكثر سرعة في صنع التعديلات والتحديثات للبرامج، وتوجيه التنبيهات للمستخدم على صعيد الحواسيب منها على صعيد الهواتف الذكية.

152 John Wilkinson, Tareq Haddad, PWC, *Economic Crime in the Arab World,* February 2014, http://www.pwc.com/m1/en/publications/gecs2014reportme.pdf, p. 18.

153 United Nations Office on Drugs and Crime, UNODC, *Comprehensive study on cybercrime*, draft, February 2013, p. 234, 237.

2- عدم ملاءمة أو كفاية برامج التوعية في دول المنطقة العربية

بالرغم من عدم وجود وعي كافٍ في المنطقة العربية للمخاطر السيبرانية، يتبين أن دولاً عديدة قد أطلقت حملات توعية أو حملات لتدريب المستخدمين. إلا أن هذه الحملات تعاني من الضعف أو عدم النجاح نسبياً نظراً لضعف التغطية أو التسويق، ولعدم تكرارها وكذلك عدم استهدافها الفئات المعنية حقيقةً، وعدم استقطابها اهتمام الجمهور، وتعاني أيضا من حداثة مواضيعها وتقنيتها، أو سوء اختيار المحاضرين.

أما المناهج التعليمية، فلا تتضمن في كثير من المدارس والجامعات أية مواد حول الأمان السيبراني؛ ولا يجري تنظيم حملات إعلامية في وسائل الإعلام تعويضاً عن ذلك. كما يلاحظ ضعف في حملات التوعية الموجهة للنساء تحديداً، أو التوعية بالجرائم التي تطال النساء أكثر من الرجال.

ويوجد بعض المبادرات الناجحة في عدد من الدول العربية، إذ تتبنى اللجنة الوطنية لحماية النشء على الإنترنت في مصر مبادرات عديدة، وترعاها وتنفذها وزارة التربية والتعليم. وفي لبنان، يقوم المجلس الأعلى للطفولة في وزارة الشؤون الإجتماعية بدور مشابه. وفي عام 2011، أطلقت هيئة تقنية المعلومات في سلطنة عمان، متمثلة بالمركز الوطني للسلامة المعلوماتية، حملة لحماية الطفل من مخاطر الإنترنت، وبرنامج الأمان السيبراني للمرأة والأسرة.

3- التبليغ عن الجرائم السيبرانية

يحجم الضحايا في الدول العربية عن التبليغ عن الجرائم السيبرانية لأسباب عديدة، منها اعتقادهم بعدم جدوى تقديم الشكوى واستحالة اكتشاف الجاني، أو خوفهم من تضرر سمعتهم التجارية وخسارة الزبائن، أو لضعف المعرفة التقنية لديهم وعدم ثقتهم بالكفاءات التقنية لأجهزة الشرطة، أو لشعورهم بالإحراج من وقوعهم في الخطأ. وهناك حالات عديدة لنساء تعرضن للعنف الفعلي عبر الفضاء السيبراني ولكن اخترن عدم رفع تقرير بذلك الى السلطات المعنية عن حالاتهن. وقد بينت دراسة حديثة أجريت في الولايات المتحدة عام 2014، أن 13-14 في المائة فقط من النساء أبلغن عن تعرضهن للعنف[154]. ففي البلدان التي لا تعالج قضايا العنف ضد المرأة بشكل عام، تنخفض نسب واحتمالات إبلاغ النساء عن تعرضهن للعنف عبر الفضاء السيبراني.

وبشكل عام من الضروري تحفيز الضحية وإقناعها بالإبلاغ عن الجريمة السيبرانية للعمل على توقيف المرتكبين ومنعهم من تكرار فعلتهم، فمعظم الجرائم السيبرانية لا يرتكبها أفراد يجربون حظهم مرة، بل عصابات محترفة، قد تتنقل من بلد إلى آخر لإخفاء آثارها. ويتبين من دراسة أجريت على عينة من 20,000 شخص في 24 دولة أن 21 في المائة فقط من ضحايا الجرائم السيبرانية قد تقدموا بشكاوى حولها للشرطة[155].

طاء- خلاصة

يتبين من الفقرات السابقة وجود فجوات قانونية وإجرائية وتنظيمية وتوعوية في المنطقة العربية في مجال الأمن السيبراني ومكافحة الجرائم السيبرانية وذلك بالمقارنة مع الدول المتقدمة أو بعض الدول النامية. ولا يخفى أن العديد من الدول العربية قامت ببعض المبادرات الناجحة إلا أن معظم هذه النجاحات لم تعمم

154 http://fra.europa.eu/sites/default/files/fra-2014-vaw-survey-main-results-apr14_en.pdf.

155 Symantec, 2011, Norton Cybercrime Report 2011.

لتشمل الدولة بكاملها أو المنطقة العربية. وتجدر الإشارة إلى أهمية توفر الثقة بين أصحاب المصلحة المختلفين في الدولة الواحدة من أجل التعاون وتبادل المعلومات والبيانات والمعرفة من أجل مكافحة المخاطر السيبرانية، إلا أن الدول العربية ما زالت تفتقر إلى وجود ثقة كافية في ما بين المؤسسات كما تفتقر إلى آليات تنسيق هذا التعاون. ونظراً للطبيعة الشمولية للجرائم السيبرانية وعدم وجود حدود فيما بين الفضاءات السيبرانية على الإنترنت، فإن للتعاون الإقليمي ودون الإقليمي والدولي في ما بين الدول أهمية استثنائية. وبالتالي يجب على الدول العربية التنبه إلى أهمية التعاون لمكافحة الجرائم السيبرانية وإلى إيجاد الأساليب العملية لتحقيق مثل هذا التعاون. وبناء على ما تقدم، يلخص الجدول 2 وضع الأمن السيبراني في ثلاث دول من المنطقة العربية: الإمارات العربية المتحدة والتي تمثل نموذج عن دول مجلس التعاون الخليجي، ومصر كنموذج عن دول شمال أفريقيا، ولبنان كنموذج عن دول الشرق الأوسط.

الجدول 2- ملخص لوضع الأمن السيبراني في ثلاث دول عربية

	النموذج الأول (الإمارات)	النموذج الثاني (مصر)	النموذج الثالث (لبنان)
الإرادة السياسة للتحديث	وجود إرادة واضحة	تعاني أحياناً من عدم وجود استقرار سياسي وأمني ووجود أولويات أخرى	تعاني من عدم وجود استقرار سياسي وأمني ووجود أولويات أخرى
استراتيجية للأمن السيبراني	يوجد استراتيجية بحاجة للتحديث والتفصيل	يوجد استراتيجية بحاجة للتحديث والتفصيل	لا يوجد استراتيجية
التشريعات السيبرانية	- تم إصدار التشريعات - يتم تحديثها باستمرار - تنقص بعض التشريعات	- تم إصدار بعض التشريعات - لا تزال تنقص تشريعات أساسية - لا يتم التحديث بالوتيرة المطلوبة	- تم إصدار تشريعات محدودة - تم إعداد مشاريع قوانين - بحاجة لورشة تشريعية
القواعد الإجرائية للقوانين	بحاجة لقواعد إجرائية خاصة	بحاجة لقواعد إجرائية خاصة	بحاجة لقواعد إجرائية خاصة
تطبيق التشريعات	تشريعات خاصة كافية سهلة التطبيق	يجتهد القضاء لتطبيق نصوص قانون العقوبات التقليدي	يجتهد القضاء لتطبيق نصوص قانون العقوبات التقليدي
التنظيم	- يوجد أجهزة تحقيق متخصصة - عدم وجود محاكم متخصصة	- يوجد أجهزة تحقيق متخصصة - عدم وجود محاكم متخصصة	- يوجد أجهزة تحقيق متخصصة - عدم وجود محاكم متخصصة
مركز للاستجابة لطوارئ الحاسوب	يوجد مركز للاستجابة لطوارئ الحاسوب	يوجد مركز للاستجابة لطوارئ الحاسوب	لا يوجد مركز للاستجابة لطوارئ الحاسوب
قواعد سلوكية للأمن السيبراني	يوجد قواعد سلوكية بحاجة للتحديث	لا يوجد قواعد سلوكية	لا يوجد قواعد سلوكية
تعاون القطاع الخاص	يتعاون القطاع الخاص مع أجهزة التحقيق	يتعاون القطاع الخاص مع أجهزة التحقيق	يتعاون القطاع الخاص مع أجهزة التحقيق مع وجود معوقات
التوعية	يوجد حملات توعية عامة ومتخصصة (بحاجة للاستكمال)	يوجد حملات توعية عامة ومتخصصة غير كافية	يوجد حملات توعية عامة ومتخصصة غير كافية
التدريب	تم إجراء دورات تدريبية للقضاة وللشرطة المتخصصة (بحاجة للاستكمال)	تم إجراء دورات تدريبية للقضاة وللشرطة المتخصصة على نحو غير كاف	تم إجراء دورات تدريبية للقضاة وللشرطة المتخصصة على نحو غير كاف
إحصاءات	يوجد إحصاءات حول الجرائم السيبرانية والسلامة المعلوماتية	يوجد إحصاءات غير كافية حول الجرائم السيبرانية والسلامة المعلوماتية	يوجد إحصاءات غير كافية حول الجرائم السيبرانية والسلامة المعلوماتية

ثالثاً- إطار عمل للأمان السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية

عَرض الفصل الأول من هذه الدراسة تحليلاً مفصلاً للتوجهات العامة لضمان الأمان السيبراني والممارسات والأمثلة العالمية في هذا المجال. ومن ثم ركز الفصل الثاني على وضع المنطقة العربية تحديداً، والتحديات والمعوقات التي تواجهها، وبالتالي قدمت الدراسة تحليلاً للفجوة التي تعاني منها المنطقة العربية لناحية توفير الأمان السيبراني إذا ما قورنت بباقي مناطق وبلدان العالم الأكثر نمواً. ومن أبرز أهداف هذه الدراسة هو وضع إطار عمل للأمن السيبراني ومكافحة الجرائم السيبرانية بناء على ما سبق من تحليل ونقاش لحاجات المنطقة. يمكن لحكومات الدول العربية استخدام هذا الإطار على المستوى الوطني كسلة متكاملة لتأمين الأمن السيبراني، أو يمكنها اختيار أجزاء منه وتكييفها بحسب البيئة والحاجة الوطنية.

ألف- وضع استراتيجية وطنية للأمان السيبراني ومكافحة الجرائم السيبرانية

تتمثل الخطوة الأولى في هذا الإطار بوضع استراتيجية متكاملة للأمان السيبراني ولمكافحة الجرائم السيبرانية. وتتضمن هذه الاستراتيجية نواحي مختلفة، منها التشريعي والتنفيذي والتنظيمي والتثقيفي. تجدر الإشارة إلى أنه إذا كان قد سبق لبعض دول المنطقة أن وضعت استراتيجية مماثلة، فينبغي عليها تحديثها وإعادة النظر فيها دورياً في ظل المتغيرات وسرعة التطور التقني وما اختبرته في ظل الاستراتيجية القديمة. وعلى كل دولة وضع خطط عمل مفصلة لتطبيق استراتيجيتها عن طريق تحديد الأهداف الجزئية والمشاريع والإجراءات والتحديثات المنوي تنفيذها والهوامش الزمنية لها والترابط بينها.

ويمكن، كفكرة أولية، اعتماد الدول النامية، ومنها دول المنطقة، نفس استراتيجيات مكافحة الجرائم السيبرانية المقررة في الدول المتقدمة، لما في ذلك من توفير للوقت وللمال؛ غير أن اعتماد هذه المقاربة يثير عدة إشكاليات، فبالرغم من أوجه الشبه في المخاطر السيبرانية بين الدول النامية والمتقدمة، فإن أفضل الحلول لأي بلد ترتبط بموارده وإمكاناته وبالنظام القانوني المطبق فيه وبعقلية المجتمع ومدى تعاون القطاع الخاص[156]. ويمكن العودة إلى الإطارين 3 و4 الذين يوضحان بعض التجارب العالمية في مجال استراتيجيات الأمن السيبراني، والتي يمكن لدول المنطقة أن تستنير بها، مع اقتباس ما قد ينسجم مع واقع كل دولة وإمكاناتها وتشريعاتها، بعد تكييفها بناء على احتياجاتها وأولوياتها. وتجدر الإشارة أنه في محاولة لتحديد أنجع الوسائل للأمان السيبراني، أظهرت نتائج استطلاع للرأي أجري في عام 2011 على 1861 مختصّا في تكنولوجيا المعلومات، أن 58 في المائة منهم يرون أن تطبيق ممارسات وسياسات أمن فعالة له أكبر وقع على الأمان السيبراني، في حين أفاد 15 في المائة فقط أنه يمكن زيادة مستوى الأمان السيبراني بالدرجة الأولى بواسطة التكنولوجيا، وأقرّ 7 في المائة فقط أن القوانين هي الحل الأول[157].

وبناء على التجارب الدولية وعلى احتياجات المنطقة العربية، يوصَى بأن تتضمّن استراتيجية الأمان السيبراني ومكافحة الجريمة السيبرانية في كل دولة عربية البنود التالية كحد أدنى:

- وضع التشريعات السيبرانية الضرورية وتحديثها (كما هو وارد في الفقرة باء)؛
- وضع منهجية للاستجابة للحوادث السيبرانية، وبوجه خاص إنشاء مراكز للاستجابة السريعة لطوارئ الحاسوب، ووضع أسس التواصل والتعاون بين هذه المراكز في المنطقة العربية؛

156 ITU, Marco Gercke, *Understanding Cybercrime: Phenomena, Challenges and Legal Response,* September 2012, p. 98.

157 Steven Titch, *Four principles for effective cybersecurity law and policy*, 25 April 2014, http://www.rstreet.org/2014/04/25/four-principles-for-effective-cybersecurity-law-and-policy, p. 4.

- دعم صناعة البرمجيات والتجهيزات والحلول التقنية الخاصة بالحماية من المخاطر السيبرانية؛
- تعزيز الشراكة بين القطاع العام والخاص، وبخاصة فيما يتعلق بحملات التوعية، وتطوير الحلول التقنية، وحفظ معلومات حركة البيانات وبيانات التعريف عن المستخدمين، والتمويل؛
- تشجيع اعتماد الهوية الإلكترونية للمستخدمين على الشبكة، وبوجه خاص عند الدخول إلى الأنظمة ذات الطبيعة الحساسة، كالأنظمة المالية؛
- تطوير نظام للتبليغ السريع عن الجرائم السيبرانية بحيث يعتمد على السرية ويضمن حقوق المرأة والطفل؛
- اعتماد المؤشرات التي تراعى النوع الاجتماعى وتسمح بتقصي مستوى الجريمة السيبرانية، وتحديثها دورياً؛
- التوعية الحثيثة والمستمرة حول الأمان السيبراني والجرائم السيبرانية للمؤسسات والأفراد؛
- تعزيز التدريب والتأهيل في مجال الأمن السيبراني، بغية زيادة عدد المتخصصين في هذا المجال؛
- إقرار مبدأ التعاون في محاربة الجرائم السيبرانية ضمن إطار جامعة الدول العربية، بغية زيادة تبادل المعلومات بين الأجهزة الرسمية.

ويجب أيضاً على كل دولة من دول المنطقة تطبيق مجموعة من الوسائل، كما هو مبين في الأجزاء اللاحقة، يكون فيها إطار عمل للأمان والأمن السيبراني ولمكافحة الجرائم السيبرانية. وهذه الوسائل هي تشريعية وتنظيمية وتوعوية وتثقيفية وتقنية وتعاونية فيما بين القطاع العام والقطاع الخاص في ذات الدولة.

باء- الوسائل التشريعية المُقترح اعتمادها للأمان السيبراني في دول المنطقة العربية

بداية، ينبغي على كل دولة من دول المنطقة العمل على تحديث تشريعاتها، وسن قوانين لتجريم الجرائم السيبرانية؛ فقوانين العقوبات التقليدية ليست صالحة على الدوام لحكم هذه الأفعال الجرمية الجديدة، على الأقل في حالة الأفعال التي تكون فيها المعلوماتية محل الاعتداء. وكذلك ينبغي العمل باستمرار على تحديث التشريعات لمواكبة التطور التقني والأساليب المبتكرة التي يعتمدها المجرمون وإعادة النظر في العقوبات وفي ظروف تشديدها وفق ما يظهر من ممارسات إجرامية.

1- إجراء مسح وطني شامل للتشريعات ذات الصلة

بغية وضع سياسة تشريعية فعالة ومستندة إلى معطيات علمية ودقيقة، ينبغي للدولة القيام بدراسة شاملة وتفصيلية للقوانين الموجودة فيها قبل المسارعة إلى وضع قوانين جديدة. فهذا يحول دون إصدار قوانين غامضة قد تتعارض مع القوانين السابقة النافذة، ويحول دون الاستنسابية في تفسير المصطلحات والتعابير المبهمة من قبل النيابة العامة للتوسع في الادّعاء[158]. وهذا يعني ضرورة النظر إلى بعض الأفعال الجرمية على الإنترنت باعتبارها جرائم عادية كلاسيكية ولكنها تستعمل وسيلة جديدة هي الإنترنت أو المعلوماتية.

158 Steven Titch, *Four principles for effective cybersecurity law and policy*, 25 April 2014, http://www.rstreet.org/2014/04/25/four-principles-for-effective-cybersecurity-law-and-policy, p. 2.

2- تحديث تشريعات الجرائم السيبرانية وإيجاد حلول لبعض إشكالياتها

تحتاج التشريعات الوطنية إلى التحديث دورياً خاصة في مكافحة الإشكاليات القانونية الناتجة عن طبيعة الفضاء السيبراني. ومن تلك الإشكاليات، عدم وضع تعريف واضح وموحد للجرائم السيبرانية عامة في دولة معينة، حيث يبدو غير ذي أولوية، باعتبار أنه من الأهم وضع تعريفات محددة في التشريع الداخلي لكل جريمة سيبرانية تبين أركانها وعناصرها، تطبيقاً لمبدأ "لا جريمة ولا عقوبة دون نص قانوني". ومن المسلّم به أن القواعد القانونية الإجرائية التقليدية في الدول العربية المتعلقة بتنظيم آليات التحقيق في الجرائم الجزائية عاجزة عن حكم قضايا جرائم المعلوماتية نظراً للطبيعة الخاصة لها، فالمعلوماتية تمتاز بالطابع اللامادي والتقني المتخصص وبالقدرة على الزوال بسرعة وباختراق الحدود وبوجود هوية إلكترونية مختلفة عن الهوية الحقيقية وبالقدرة على إحداث أضرار جسيمة عن بعد، فلا بد من تحديث هذه القواعد.

وعلى سبيل المثال، تعتبر البيانات المعلوماتية في حيازة الشخص إذا كان يحوز مادياً جهاز الحاسوب الذي يخزنها، أو هو قادر على الوصول عن بعد إلى هذه المعلومات المخزنة على وسائط حفظ إلكترونية، حتى خارج البلاد، عبر شبكات نقل المعلومات. كما أن الإذن بالبحث عن بيانات ضمن نظام معلوماتي يمكن توسيعه ليشمل بيانات مخزنة في نظام آخر، ولكن يمكن الوصول إليها من النظام المعلوماتي الأول[159].

ومن الإشكاليات لتي تواجه تحديث أو وضع القوانين السيبرانية تحديد المسؤوليات الجزائية على نحو متناسق بين القوانين. وفي هذه الحالة، لا بد من إطار قانوني إجرائي في دول المنطقة ينظم جمع الأدلة المعلوماتية، مثل مراقبة الشبكات واعتراض الاتصالات وضبط أجهزة الحاسوب والبيانات المعلوماتية، ولاسيما تلك التي تزول بسرعة، وإلزام مزودي خدمات الاتصال بحفظ معلومات حركة البيانات وبيانات التعريف عن أصحاب مواقع الإنترنت التي يستضيفونها وتزويد أجهزة التحقيق بها عند الحاجة. كذلك ينبغي وضع حلول لمشاكل الاختصاص القضائي، كالتنازع الإيجابي على الصلاحية، أي عندما تدلي محاكم الدول المعنية باختصاصها بالموضوع، أو التنازع السلبي على الصلاحية، أي عندما تدلي محاكم الدول المعنية بعدم اختصاصها، وتحديد القانون الذي ينبغي تطبيقه.

إضافة إلى ما تقدم، يمكن لكل دولة عربية تطبيق مجموعة من الممارسات الفضلى التي ثبت نجاحها نتيجة لتجارب الدول الأخرى. وضمن التوصيات المهمة حول التغييرات المفترض اعتمادها لمكافحة الجرائم السيبرانية، ينبغي القيام بما يلي (لمزيد من التفاصيل أنظر التوصيات)[160]:

- إجراء التغييرات التشريعية بالحد الأدنى الكافي لضمان مستويات ملائمة من الأمن السيبراني؛
- تفسير القوانين وفق طرق تسمح لأصحاب الشأن بإعطاء الأولوية للأمان السيبراني؛
- تجنب الخلط بين الجرائم السيبرانية وغيرها من المسائل، مثل الملكية الفكرية والخصوصية وحرية التعبير؛
- وضع التشريعات التي تسمح لأجهزة الدولة بمهاجمة مراكز التحكم (الحواسيب الرئيسية) التي تسيطر على حواسيب الأشخاص؛

159 Michael A. Vatis, *The Council of Europe Convention on Cybercrime*, http://cs.brown.edu/courses/csci1950-p/sources/lec16/Vatis.pdf, p. 6, 7.

160 Micheal Barrett, Andy Steingruebl, Bill Smith, *Combating Cybercrime: Principles, Policies and Programs*, April 2011, https://www.paypal-media.com/assets/pdf/fact_sheet/PayPal_CombatingCybercrime_WP_0411_v4.pdf, p. 7 to 25.

- تسريع إجراءات التعاون بين أجهزة التحقيق في الدول عن طريق الربط الإلكتروني بينها (مثل حفظ وتبادل البيانات المعلوماتية)؛
- إمكانية محاكمة الجاني في بلد إقامته لا في بلد إقامة الضحية، وذلك في حال رفض طلب استرداده.

في هذا الإطار، تقترح الإسكوا، استكمالا لـ "إرشادات الإسكوا للتشريعات السيبرانية" الصادرة في عام 2012، قانوناً نموذجياً جديداً متعلقاً بالقواعد الإجرائية الخاصة بالجرائم السيبرانية والأدلة الرقمية، وهو مقتبس من اتفاقية بودابست. (أنظر المرفق الثالث للاطلاع على النص النموذجي المقترح).

3- تنسيق التشريعات بين الدول العربية والاسترشاد بإرشادات الإسكوا للتشريعات السيبرانية

ينبغي توحيد المقاربة التشريعية بين الدول العربية، أو على الأقل تنسيقها. كما ينبغي وضع تعاريف موحدة أو متناسقة، للجرائم السيبرانية. وكذلك ينبغي وضع سلّم متناسق للعقوبات؛ إذ يمكن التفلّت من الملاحقة إذا كانت دولة عربية معينة تجرّم فعلاً معيناً في حين لا تجرّمه دولة أخرى. كما أن التعاون بين الأجهزة الرسمية في الدول العربية لا يكفي لوحده، بل يعتبر إشراك القطاع الخاص ذا أهمية، خاصة الشركات التي توفر التجهيزات والبرامج المعلوماتية وكذلك شركات الاتصالات[161].

إن معظم الدول ترفض التعاون إذا كان الفعل الجرمي المُرتكب في دولة أخرى غير مجرّم في قانونها الداخلي (التجريم المزدوج)، فالتعاون بين الدول يقتصر على الجرائم المجرّمة في جميع هذه الدول. فطالما أن التقنيات المستخدمة في مجال تكنولوجيا المعلومات هي نفسها على مستوى العالم، فمن الأولى أن تكون تعاريف الانتهاكات المُستندة إلى هذه التقنيات هي ذاتها.

كما يمكن للدول العربية الاسترشاد في سن تشريعاتها المتعلقة بالجانب الموضوعي وبقسم من الجانب الإجرائي بإرشادات الإسكوا للتشريعات السيبرانية التي صدرت عام 2012، وهي ملائمة للتطبيق في الدول العربية ذات النظام القانوني المبني على القانون اللاتيني، وذلك باعتبار أن هذه الإرشادات مستوحاة من إرشادات الاتحاد الأوروبي والقوانين الفرنسية والأوروبية. كما يمكن للدول العربية الاسترشاد بالاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010، وبالقانون العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها لعام 2003، والقانون العربي الاسترشادي للإثبات بالتقنيات الحديثة لعام 2008، والقانون العربي الاسترشادي للمعاملات والتجارة الإلكترونية لعام 2009.

وقد تضمنت إرشادات الإسكوا للتشريعات السيبرانية لعام 2012 القواعد الموضوعية المتعلقة بهذه الجرائم، ومنها التعدي على البيانات المعلوماتية، والتعدي على الأنظمة المعلوماتية وإساءة استعمال الأجهزة أو البرامج المعلوماتية، والتعدي على الأموال والمعاملات بوسائل إلكترونية، وجرائم الاستغلال الجنسي للقاصرين بوسائل معلوماتية، والتعدي على الملكية الفكرية للأعمال الرقمية، وجرائم البطاقات المصرفية والنقود الإلكترونية، وجرائم المعلومات الشخصية، وجرائم العنصرية والجرائم ضد الإنسانية بوسائل معلوماتية، والمقامرة وترويج المواد المخدرة بوسائل معلوماتية، وجرائم المعلوماتية ضد الدولة والسلامة

161 About that review: Fausto Pocar, *New Challenges for international rules against cyber-crime*, http://link.springer.com/article/10.1023/B:CRIM.0000037565.32355.10#page-1.

العامة، وتشفير المعلومات. ومن ثمّ فقد تضمن الإرشاد النوع الأول من جرائم المعلوماتية، حيث تكون المعلوماتية موضوع الفعل الجرمي، كالاعتداء على الأنظمة المعلوماتية، وكذلك النوع الثاني من الجرائم المعلوماتية، حيث تكون المعلوماتية هي وسيلة ارتكاب فعل جرمي تقليدي كالاحتيال أو السرقة أو السب.

ولم ينظم الإرشاد القضايا الإجرائية في التحقيقات القضائية، بل أشار فقط في مادة وحيدة إلى التعاون الدولي في هذا المجال، حيث تنص المادة 56 على أنه على الدول الأعضاء أن تلتزم المعاهدات والاتفاقيات الدولية ذات الطابع الجماعي أو الثنائي المتعلقة بمكافحة الجرائم عموماً، مع مراعاة طبيعة الجرائم السيبرانية، وذلك من حيث تسهيل وتسريع الإجراءات الخاصة بجمع الأدلة وضبطها وتبادل المعلومات حول الجرائم المذكورة وملاحقة مرتكبيها؛ كما تحرص الدول الأعضاء على التعاون فيما بينها في مجال التحقيقات القضائية في جرائم المعلوماتية، وأعمال رصدها ومكافحتها. (أنظر المرفق الثالث للاطلاع على الجانب الإجرائي للجرائم السيبرانية).

4- الاسترشاد باتفاقية بودابست

يمكن الاسترشاد في المنطقة العربية بالقواعد الإجرائية الأساسية في مجال تحقيقات جرائم المعلوماتية، التي يمكن العودة إليها أيضاً في اتفاقية بودابست، حيث تقوم الدول العربية بإدخال مبادئها ضمن أنظمتها القانونية. وتتمحور القواعد الإجرائية حول إعطاء أجهزة التحقيق الصلاحيات التالية:

- إلزام أي شخص بحفظ بيانات معلوماتية، ومنها معلومات حركة البيانات (Traffic data)؛
- إلزام مزودي خدمات الاتصال بتزويد أجهزة التحقيق بمعلومات حركة البيانات وببيانات التعريف الشخصية حول أصحاب المواقع الإلكترونية Subscriber information التي يستضيفونها، وإلزام أي شخص بتزويدها ببيانات معلوماتية محددة هي بحوزته؛
- الوصول إلى أنظمة الحاسوب والمعلومات وضبطها؛
- الوصول إلى معلومات حركة البيانات في زمن الإرسال الحقيقي، إما مباشرة أو عن طريق مزودي خدمات الاتصال؛
- الوصول إلى محتوى الاتصال أو المعلومات بذاتها content data في زمن الإرسال الحقيقي، إما مباشرة أو عن طريق مزودي خدمات الاتصال؛
- إلزام أي شخص لديه معلومات حول طرق عمل نظام معلوماتي والتدابير التقنية لحمايته بالمساعدة على ضبط البيانات أو النظام؛
- إعطاء الصلاحية القضائية لمحاكم البلد الذي وقع فيه الجرم أو في حال وجود المتهم على أراضي هذا البلد، وعدم إجابة طلب الاسترداد المقدم من بلد آخر بسبب جنسية المتهم التابع للبلد الأول.

ومن المفيد إعطاء الصلاحية لمحاكم البلد الذي نشأ منه الاعتداء المعلوماتي ومكان وجود المرتكب (محل وإقامة المجرم)، وإن كانت آثار الفعل قد لحقت بنظام معلوماتي خارج البلد، وذلك نظراً لسهولة السير بالتحقيق وإمكانية توقيف الفاعل.

جيم- وسائل تطبيق القانون وأجهزته في دول المنطقة العربية من أجل الأمان السيبراني

1- إنشاء وحدات متخصصة لتطبيق القانون

أشارت إرشادات الإسكوا للتشريعات السيبرانية بمادة وحيدة إلى التطويرات البنيوية في الهياكل التنظيمية للسلطات بهدف محاربة جرائم المعلوماتية، عن طريق إنشاء وحدات متخصصة في أجهزة الشرطة التي تتولى التحقيقات الجزائية، حيث تنص المادة 55 على أنه "تحرص الدول الأعضاء على إنشاء وحدة متخصصة في جرائم المعلوماتية في الأجهزة الأمنية المولجة بالتحقيقات القضائية تحت إشراف القضاء، كالضابطة العدلية. تتولى هذه الوحدة أعمال التحقيق في هذه الجرائم ورصدها تحت إشراف القضاء. ويتألف الجهاز البشري لهذه الوحدة من عناصر فنية متخصصة ذات كفاءة في مجال المعلوماتية والاتصالات".

وتوجد عدة نماذج معتمدة في الدول لتنظيم وحدات التحقيقات في مجال الأدلة المعلوماتية: (1) لجأت بعض الدول إلى إنشاء وحدات متخصصة داخل النيابات العامة لتتولى التحقيق في الجرائم السيبرانية، فيرأس الوحدة مدعٍ عام ويتشكل فريق من محققين وتقنيين؛ (2) أو كخيار آخر، يمكن تكوين قوة مشتركة بين عدة مؤسسات تتضمن محققين وفنيين ورجال شرطة؛ (3) وفي الخيار الأخير، يمكن إنشاء وحدات مركزية للتحقيق في مجال الأدلة المعلوماتية أو وحدات لامركزية في المناطق[162]، ويمكن اعتماد أي من هذه النماذج من قبل الدول العربية. وقد يدخل الأمن السيبراني، وفق توزيع الصلاحيات في كل دولة عربية، ضمن اختصاص عدة وحدات أو أقسام في وزارات مختلفة، منها ما يتعلق بحماية المستهلك (من الاحتيال المعلوماتي) أو أجهزة الأمن القومي ضمن وزارة الدفاع، إضافة إلى مراكز الاستجابة لطوارئ الحاسوب.

ومن الأهمية بمكان التنسيق فيما بين الوزارات والهيئات المتخصصة في البلد الواحد من أجل مكافحة الجرائم السيبرانية وخاصة وزارة العدل ووزارة الاقتصاد ووزارة الاتصالات ووزارة الداخلية وذلك بهدف منع التضارب في الصلاحيات والاختصاصات وتعزيز التعاون فيما بينها وتدريب العاملين المعنيين فيها على التشريعات السيبرانية وصولاً إلى التعاون لمكافحة الجرائم السيبرانية.

وبهدف التعامل مع خصوصيات المرأة، ينبغي أن تتوفر لدى فرق التحقيق خبرات في التعامل مع الجرائم السيبرانية التي يمكن أن تركز على العنف القائم على النوع الاجتماعي أو العنف ضد المرأة، خاصة عندما تكون الضحية امرأة. إضافة إلى إدخال عناصر نسائية ضمن فرق التحقيق لديها خبرات كافية بالجرائم السيبرانية. وينبغي أيضاً أن يكون لدى أعضاء النيابة العامة خبرة في هذا الموضوع حتى يتمكنوا من ملاحقة المذنبين بارتكاب جرائم سيبرانية ترتبط بالنوع الاجتماعي، دون التأثير على الصحة البدنية والعقلية للضحايا.

وفي جميع الأحوال، تكمن مهمة النيابات العامة في توجيه المحققين خلال التحقيقات وتحديد الأدلة المعلوماتية المطلوب جمعها لإثبات الوقائع الجرمية وتطوير الآليات والنماذج لمذكرات التفتيش والتوقيف والعمل على توعية الجمهور من الجريمة المعلوماتية. وينبغي أن يكون المدعي العام المشرف على هذه التحقيقات مطّلعاً على التشريعات السيبرانية وعلى دراية بالتقنيات المعلوماتية[163].

---

162 University of Mississippi, School of Law, National Center for Justice and the Rule of law, *Combating cyber crime: essential tools and effective organizational structures, A guide for policy makers and managers*, http://www.olemiss.edu/depts/ncjrl/pdf/CyberCrimebooklet.pdf, p. 17.

163 University of Mississippi, School of Law, National Center for Justice and the Rule of law, *Combating cyber crime: essential tools and effective organizational structures, A guide for policy makers and managers*, http://www.olemiss.edu/depts/ncjrl/pdf/CyberCrimebooklet.pdf, p. 31.

2- تعزيز الإجراءات الاستباقية للأمان السيبراني

إن رصد الجرائم السيبرانية والاحاطة الكاملة بتقنياتها واستبقاها، وضبطها وإعاقتها على الخط، دونه صعوبة الوتيرة السريعة والطابع العابر للحدود للجريمة السيبرانية، الذي يطرح تحديات جديدة على صعيد تطبيق القانون، ويتطلب آليات قانونية مبتكرة تفوق تلك المتبعة بخصوص الجرائم التقليدية[164]. ويتبين من دراسة للأمم المتحدة أن نسبة الجرائم السيبرانية المكتشفة من خلال تحقيق استباقي متدنية، لكن بعض الدول تركز على استراتيجية الأعمال المخفية ضد المخاطر السيبرانية[165].

ومن هنا تنبع أهمية بناء قدرات الأجهزة الرسمية في الدول العربية لاستباق أي اعتداء على الأمن السيبراني والاستعداد له وإعاقته. وفي هذا الإطار، يتم إعداد ما يعرف بالمحققين الاستباقيين proactive investigators القادرين على التواصل مع المرتكبين المرتقبين، حيث يمكن للمحقق أن ينتحل شخصية الضحية للإيقاع بالمرتكب. كذلك تقوم وحدات متخفية بمراقبة مواقع التواصل الاجتماعي وبعض منتديات النقاش والرسائل الفورية وخدمات الند للند peer-to-peer ومراقبة أجهزة التحكم لبعض البرمجيات الخبيثة. ويتوقف هذا الأمر على إجازة القانون في كل دولة لهذا العمل التحقيقي الاستباقي.

ففي نظام غير مركزي كالإنترنت، يؤدي نظام الإنذار المبكر عن المخاطر دوراً حاسماً في الأمن السيبراني؛ ومن هنا تبرز أهمية وضع خطط للاستجابة السريعة للأحداث التي قد تحصل على الشبكة وللدفاع عن البلد ضد الهجمات السيبرانية. وعلى الدول العربية الاستثمار في مراكز الاستجابة لطوارئ الحاسوب وإعطائها دوراً قيادياً على صعيد استباق وتحديد المخاطر السيبرانية وكذلك إعطائها صلاحية تنسيق المعالجات المطلوبة لدى أجهزة الدولة كافة. ويتطلب دعم هذه المراكز توظيف كفاءات تقنية عالية وتطوير قدراتها الدفاعية في الفضاء السيبراني، وتأمين الإمكانيات لإعادة الوضع إلى ما كان عليه قبل حصول الخلل المعلوماتي recovery. وقد تبين أن أداء المراكز الحالية للاستجابة لطوارئ الحاسوب في المنطقة العربية لا يوفر الفعالية المطلوبة في بعض الأحيان، بسبب ضعف آليات التواصل مع المجتمع، ومحدودية الموارد البشرية الفنية المؤهلة، أو الحاجة لمزيد من التمويل أو التنظيم أو التنسيق مع باقي وزارات الدولة المعنية.

دال- اعتماد وسائل ناجعة للتوعية والتدريب حول الأمان السيبراني

1- اعتماد آليات ناجحة للتوعية ونشر ثقافة إدارة مخاطر تكنولوجيا المعلومات

يفتقد المجتمع العربي اليوم إلى ثقافة إدارة مخاطر تكنولوجيا المعلومات. فالمواطن العربي نادراً ما يهتم لهذا الأمر، إما لعدم المعرفة أو الإهمال أو رمي المسؤولية على عاتق الدولة. إلا أن إدراك الأشخاص ووعيهم لمخاطر التعاملات على الإنترنت هو خط الدفاع الأول في مكافحة الجرائم السيبرانية. لقد كان المحتالون يستعملون برامج لمسح بوابات أجهزة الحاسوب والعثور على غير المحمي منها أو اختراق كلمات السر. ومع تطور برامج مكافحة الفيروسات والتجسس المعلوماتي وبرامج مكافحة البرمجيات الخبيثة عموماً، وازدياد فعاليتها، أصبح المعتدون يلجأون أكثر إلى ما يسمّى "الهندسة الاجتماعية" للوصول إلى ضحاياهم. وهذه الطريقة ترتكز على التفاعل الإنساني عن طريق منتديات النقاش أو رسائل البريد الإلكتروني، وتهدف

164 Australian Government, Attorney General's Department, *National Plan to Combat Cybercrime*, http://www.ag.gov.au/CrimeAndCorruption/Cybercrime/Documents/National%20Plan%20to%20Combat%20Cybercrime.pdf, p. 16.

165 United Nations Office on Drugs and Crime, UNODC, *Comprehensive study on cybercrime*, draft, February 2013, p. 117.

إلى خداع الضحية لتنزيل برامج تحكم على حواسيبها أو فضح معلومات شخصية عنها. وهذه الطريقة غير التقنية لاستهداف الضحايا تنجح حتى في حالة الحواسيب المحمية تقنياً.

ومن هنا تظهر أهمية دور الحكومات العربية في اعتماد وسائل تواصل فعالة مع المجتمع لنشر التوعية. ويمكن تنبيه وتوعية المستخدم على بعض المخاطر المستجدة عن طريق شبكات التواصل الاجتماعي، التي يرتادها الأشخاص ارتياداً شبه يومي مما يسرع عملية الاستجابة للخطر المستجد. كما يمكن الاسترشاد بما يقوم به مكتب التحقيقات الفدرالية في الولايات المتحدة الأمريكية، من حيث نشره على موقعه الإلكتروني[166] حالات الاحتيال الإلكتروني التي يتم الإبلاغ عنها، وذلك لتنبيه الجمهور من التعرض لها، وكذلك لإعلامه بالخطوات المطلوبة من قبل الأفراد لحماية أنفسهم. كما تقوم مراكز الاستجابة السريعة لطوارئ الحاسوب بتوعية مستخدمي الإنترنت عبر نشر الأخطار السيبرانية التي يتم اكتشافها أو الإبلاغ عنها حديثاً بما فيها جرائم العنف ضد المرأة على الفضاء السيبراني، مع طرق تفاديها من الناحية التقنية والعملانية.

ويمكن أيضاً اعتماد عدة وسائل لنشر الوعي حول المخاطر في الفضاء السيبراني عن طريق: البرامج التلفزيونية، والمقابلات الإعلامية، وتوزيع الكتيبات، والمحاضرات في الجامعات والمدارس، والأفلام القصيرة، واللعب التفاعلية، وإنشاء مواقع إلكترونية أو صفحات على الإنترنت أو الفيسبوك للتوعية، والرسائل النصية القصيرة، والمؤتمرات، والخطابات الموجهة للجمهور. ويمكن أن تتضمن هذه البرامج وصفا لأشكال وأنواع الجرائم السيبرانية بما فيها تلك التي تستهدف النساء والأطفال.

كما ينبغي للدول العربية الاهتمام بالتوعية بمخاطر العنف ضد المرأة على الفضاء السيبراني، ويحبذ أن تتفاعل السلطات الحكومية مع المنظمات غير الحكومية ومنظمات المجتمع المدني المعنية بشؤون المرأة لتثقيف النساء حول الجريمة الإلكترونية وآليات الحماية والأمن في الفضاء السيبراني وذلك نظراً لكونها موضع ثقة للنساء في المجتمع، ولكونها وسيلة جيدة للوصول إلى أكبر طيف من النساء سواء في المدينة أو في الريف. كما يمكن زيادة التوعية وبشكل خاص عند النساء عن طريق نشر بعض التجارب أو القصص التي قامت فيها السيدات بإبلاغ عن جرائم سيبرانية خاصة بهن مع ضرورة الحفاظ على السرية والخصوصية عند سرد مثل هذه التجارب. ويمكن للدول الأقل نمواً طلب المساعدة في مجال التوعية والتدريب من الدول الأكثر نمواً، خاصة تلك التي لها مصلحة في ذلك، والاستفادة من الخبرات التي اكتسبتها في مجال التوعية.

2- توعية مختلف الفئات في المجتمع

(أ) المستخدمون

يجب أن تكون برامج التوعية موجهة إلى فئات محددة من المجتمع، منها: الأطفال، والطلاب، والهيئات الحكومية، والمؤسسات الخاصة، والأشخاص المسنون، والأشخاص ذوي الإعاقة. فهكذا، يمكن تحديد هدف برنامج التوعية وآليته وأنشطته بحسب الفئة المستهدفة وحاجاتها ومستوى المعرفة فيها. وتؤكد دراسة للأمم المتحدة أهمية حملات التوعية المستمرة، ولا سيما تلك التي تتعلق بالمخاطر السيبرانية التي تستجد، وكذلك التي تستهدف فئات معينة كالأطفال مثلاً[167].

166 www.fbi.gov.

167 United Nations Office on Drugs and Crime, UNODC, *Comprehensive study on cybercrime*, draft, February 2013, p. 234.

وتعتبر التوعية محورية لطلاب المدارس والجامعات، حيث أن نسبة كبيرة من هؤلاء الطلاب أصبحوا مستخدمين معتادين للإنترنت بحكم دراستهم ونمط حياتهم اليومي على شبكات التواصل الاجتماعي ومنتديات النقاش والبريد الإلكتروني. وينبغي التركيز على الفروق الجنسية بين الفتيات والفتيان في حملات التوعية.

كما يمكن حثّ الشركات في الدول العربية على اعتماد الخطوات العملية التالية لتوعية الموظفين: إشراك الإدارة العليا ومجلس الإدارة بهذه المخاطر ومدى تأثيرها على وضع السياسات الاستراتيجية للأعمال، وإعادة النظر دورياً وبسرعة في مدى استعداد المؤسسة لهذه الجرائم، وإنشاء فريق عمل سيبراني للتدخل السريع، وتوظيف كفاءات تقنية، واتخاذ الإجراءات القانونية الحازمة بحق المنتهكين، والتواصل المستمر مع الآخرين لمعرفة اتجاهات الجرائم السيبرانية الحالية.

فالخبراء مدعوون إلى بذل جهد متواصل وإلى إدخال مواد التدريب حول الأمن السيبراني في مناهج المدارس والجامعات وسائر المؤسسات التربوية لتثقيف المجتمع برمته، إضافة إلى تدريب مركز للمديرين ومتخذي القرارات في الشركات وتدريب مستمر متخصص للفنيين المعلوماتيين[168].

(ب) المشرعون والقضاة والمحامون

إن التوعية اللازمة من أجل تحسين الأمان السيبراني تشمل بالإضافة إلى المستخدمين المختلفين المشرعون أيضاً، إذ لا بد من توعية المشرّع حول مخاطر الجرائم السيبرانية لحثه على تحديث التشريعات الضرورية في هذا المجال، مع العلم أن العملية التشريعية عملية بطيئة وغير مواكبة عادة التقدم السريع للتكنولوجيا. كما لا بد من توعية القضاة حول مخاطر الجرائم السيبرانية والأضرار الجسيمة التي تنشأ عنها، وبيان الأبعاد المختلفة للاستخدام المسيء لتكنولوجيا المعلومات والاتصالات وآلياته ونتائجه الاجتماعية والاقتصادية. كما لا بد من إعلام المشرعين أيضاً بالدليل الرقمي وإمكانيات الاستفادة منه. وبالإضافة إلى برامج التوعية للمشرعين، لا بد من وضع خطة عمل لبرامج تدريبية متخصصة للقضاة والمحامين كما هو مبين في الفقرة التالية.

3- تشجيع النساء والرجال على التبليغ عن الجرائم السيبرانية

ينبغي أن تتخذ الحكومات خطوات عملية لتشجيع النساء والرجال والمؤسسات في الدول العربية على التبليغ عن الجرائم السيبرانية لعدة أهداف، منها بناء قاعدة معلومات وطنية تصلح لرسم استراتيجية للتعامل في المستقبل مع هذا النوع من الجرائم. وتحتاج هذه العملية إلى تحديد مرجع موحد لتلقي شكاوى الجرائم السيبرانية، ومن الأفضل أن يتم ذلك على الخط بحيث يستطيع جميع الأفراد التبليغ عن الانتهاكات التي تعرضوا لها حتى ولو كانوا يقطنون مناطق ريفية أو نائية.

وتجدر الإشارة إلى أنه قد يكون من الصعب على بعض الفئات الاجتماعية، مثل المرأة أو الطفل، تقديم تقرير أو الإبلاغ عن الجرائم السيبرانية التي تعرضوا لها، ولذلك فإنه من الأهمية بمكان إنشاء وحدات خاصة تتضمن بالإضافة إلى ضباط الشرطة أخصائيين اجتماعيين ومستشارين في شؤون المرأة أو الطفل للمساعدة في التبليغ عن الجرائم السيبرانية وبيان ملابساتها. وفي حالات التبليغ عن الجرائم على الخط، يمكن إضافة خيارات تسمح للأشخاص بالتبليغ دون التصريح عن هويتهم من أجل زيادة السرية.

168 National French Police, *Prospective analysis on trends on cybercrime from 2011 to 2020*, http://www.mcafee.com/sg/resources/white-papers/wp-trends-in-cybercrime-2011-2020.pdf, p. 39.

وينبغي أيضاً إنشاء قاعدة بيانات وطنية حول الجرائم السيبرانية لتجميع المعلومات والإحصاءات عنها بالتفصيل بحيث تكون هذه الإحصاءات دقيقة ومعبرة فعلياً عن الاعتداءات السيبرانية ومصنفة حسب النوع الاجتماعي. ويجدر، بعد تحليل قاعدة البيانات، تحديث النماذج التي يملؤها الضحايا. وفي كثير من الدول، لا يتم التمييز في تقارير الشرطة بين الجرائم التقليدية التي تتم على الخط Online أو خارج الخط Offline. لذا، من المهم اتباع نماذج جديدة لتقارير الشرطة تفرّق بين هذين النوعين من الجرائم[169].

4- إطلاق الدورات التدريبية المتخصصة

(أ) دورات للقضاة والمحققين والشرطة (الضابطة العدلية)

يعتبر بناء قدرات القانونين من أهم الأنشطة التي تقوم بها الدول للحفاظ على الأمان السيبراني. ويتم ذلك عبر إطلاق دورات تدريبية تخصصية للعاملين في مجال السلامة المعلوماتية ومكافحة الجرائم السيبرانية لتمكينهم من القيام بمهامهم على أكمل وجه، وتحديث معارفهم، ولا سيما مع تسارع التطور التقني وابتكارات المجرمين والمخترقين. ويهدف التدريب الموجه إلى القضاة والمحققين وإلى الرجال والنساء العاملين في الشرطة إلى بناء قدراتهم ومعارفهم لمحاربة الجرائم السيبرانية، وتدريبهم على استخدام الأدوات المعلوماتية في التحقيقات الجزائية.

وتتضمن مواضيع التدريب الموجهة إلى المحققين الإطار القانوني للجرائم والتحقيقات وضبط أو جمع الأدلة الرقمية وحفظها وتحليلها، والتحقيقات المتوفرة على الإنترنت، وضبط أجهزة الهاتف النقال وتحليلها[170]، إضافة إلى كيفية التعامل مع القضايا الحساسة وتلك المتعلقة بالعنف ضد المرأة. ويتم التدريب بواسطة متخصص بالتدريب ضمن القضاء ووحدات الشرطة، كمعهد القضاة وأكاديمية الشرطة، وبالاستعانة بخبراء محليين ودوليين. أما الحالات الأكثر تعقيداً من الجرائم السيبرانية، أو تلك التي تستخدم تقنيات متقدمة، فتترك لوحدات متخصصة من الشرطة[171].

ومن الأهمية بمكان إدراج مواضيع الجرائم السيبرانية المتعلقة بالنوع الاجتماعي والجرائم التي تستهدف النساء بشكل خاص ضمن برامج الدورات التدريبية. ويبين التدريب كيفية مقاربة الجرائم التقليدية ضد المرأة بجرائم سيبرانية، والآليات المطلوب اعتمادها لمعالجة هذه الجرائم. وينبغي أن تشمل حملات التوعية والتدريب جميع المعنيين بالأمان السيبراني من الرجال أو النساء، سواء في السلك القضائي أو الإجرائي والجزائي، حتى لو تلقوا دورات سابقة، وذلك لمواكبة التطور التقني وتطور الأساليب التي يتبعها المرتكبون.

(ب) دورات تدريبية للتقنيين في جهاز الشرطة أو مراكز الاستجابة لطوارئ الحاسوب

ينبغي أن تجري الدولة دورات تدريبية تخصصية دورياً للتقنيين في جهاز الشرطة أو مراكز الاستجابة لطوارئ الحاسوب، لتمكينهم من القيام بعملهم على أكمل وجه، وتحديث معارفهم في ظل التطور التقني المتسارع.

---

169 Australian Government, Attorney General's Department, *National Plan to Combat Cybercrime*, http://www.ag.gov.au/CrimeAndCorruption/Cybercrime/Documents/National%20Plan%20to%20Combat%20Cybercrime.pdf, p. 15.

170 United Nations Office on Drugs and Crime, UNODC, *Comprehensive study on cybercrime*, draft, February 2013, p. 175.

171 Australian Government, Attorney General's Department, *National Plan to Combat Cybercrime*, http://www.ag.gov.au/CrimeAndCorruption/Cybercrime/Documents/National%20Plan%20to%20Combat%20Cybercrime.pdf, p. 17.

وتشمل هذه الدورات المواضيع التالية: جمع الأدلة الرقمية وحفظها، والتحليل المتقدم للأدلة الرقمية، واكتشاف الحوادث السيبرانية والإنذار المبكر، والمعالجة أو الإدارة المتقدمة للحوادث السيبرانية، وكيفية إنشاء مركز للاستجابة لطوارئ الحاسوب، وتحليل الفيروسات وبرامج التجسس والاختراق، ومكامن الضعف للبرامج، وأمن الشبكات والمعلومات، وأمن الإنترنت والسيناريوهات المختلفة للهجمات، وكتابة البرمجيات الآمنة، والضمان المتعلق بموردي البرامج [172].

(ج) إدخال موضوع الجرائم السيبرانية في المناهج التعليمية

يجب حث الجامعات على إدخال مناهج حول تعزيز آليات الأمن السيبراني ومكافحة الجرائم السيبرانية في الجامعات المتخصصة وخاصة في كليات المعلوماتية والحقوق وفي المعاهد القضائية والإدارية. كما يجب إدراج برامج خاصة للدراسات العليا وإنشاء اختصاصات في هذا المجال وذلك من أجل توفير خبرات متخصصة في الدول العربية. كما يجب أيضاً إدراج موضوع الأمان السيبراني في برامج المعلوماتية في المدارس والمعاهد كافة.

هاء- التعاون بين القطاعين العام والخاص والمجتمع المدني

1- التعاون بين القطاعين العام والخاص ومبرراته ومواضيعه

تدعم الشراكة بين القطاع العام والخاص عملية حفظ الأمان والأمن السيبراني عبر تبادل المعلومات وتشارك العبء المادي والتعاون العملي والإجرائي (التحقيقات، التتبع، الإنذار، إدارة الأزمة) [173]. فإنشاء الشراكة بين هذين القطاعين في مجال الأمان والأمن السيبراني هو أمر هام وواعد، وقد تم تطبيقه في عدة دول متقدمة مثل الولايات المتحدة الأمريكية والاتحاد الأوروبي[174].

لذا يجدر بالدول العربية وضع وتحفيز آليات التعاون والشراكة بين القطاعين العام والخاص وخاصة مع مزودي خدمات الاتصال وفي ما يخص تبادل المعلومات حول الجرائم السيبرانية، وحفظ معلومات حركة البيانات وبيانات التعريف عن المستخدمين، وتقديمها لأجهزة التحقيق. كما أن للقطاع الخاص ومزودو خدمات الشبكة دور هام في تطوير وتشجيع البرمجيات الآمنة، ونشر وتحفيز طرق الوقاية من الجرائم والمخاطر السيبرانية، وكذلك في وضع برامج التوعية الملائمة لكافة أفراد المجتمع. ويجب حكماً في هذا النوع من الشراكة إيجاد توازن بين مصالح كل من الطرفين.

فكثيراً ما تكون الشركات الخاصة سباقة في كشف الطرق المستجدة لارتكاب الجرائم السيبرانية واختراق الأنظمة المعلوماتية، وكيفية الوقاية منها؛ غير أنها غالباً ما تحجم عن التعاون لأسباب تتعلق بالخصوصية، والأسرار التجارية، أو عدم المبالاة. ومن ناحية ثانية، ترفض الدول تزويد الشركات الخاصة بالمعلومات لأسباب تتعلق بالأمن القومي. ويعود لكل دولة عربية تمويل الأبحاث في مجالات الأمن السيبراني

---

172 ENISA, Roadmap to provide more proactive and efficient Computer Emergency Response Team training, http://www.enisa.europa.eu/activities/cert/support/exercise/roadmap-to-provide-more-proactive-and-efficient-cert-training.

173 National French Police, *Prospective analysis on trends on cybercrime from 2011 to 2020*, http://www.mcafee.com/sg/resources/white-papers/wp-trends-in-cybercrime-2011-2020.pdf, p. 42, 43.

174 ENISA مثل لجنة التجارة الفيدرالية في الولايات المتحدة الأمريكية وفي الاتحاد الأوروبي.

لابتكار حلول جديدة ومبتكرة في هذا المجال. كما ينبغي تشجيع الشركات والمعاهد والجامعات على الاستثمار في مجال أبحاث الأمن السيبراني، من حيث صناعة التجهيزات والبرمجيات المعلوماتية.

2- تنسيق دور القطاعين العام والخاص كمزودي خدمات الشبكة

نشأت، نتيجة التجربة في بعض الدول، مجموعة من الممارسات الفضلى في مجال الأمان السيبراني التي يمكن الاسترشاد بها، ومنها[175]:

- تولي الحكومات بنفسها الرقابة التقنية في مجال الأمن السيبراني، لا تفويضها إلى القطاع الخاص؛
- إيجاد حلول تضمن الأمن السيبراني من دون التعرض للخصوصية؛
- جعل المؤسسات التي تتولى إدارة الإنترنت شريكة في وضع الحلول؛
- جمع المعلومات حول الجرائم السيبرانية وبناء قاعدة معلومات وطنية/إقليمية/عالمية عنها؛
- إلزام مصنعي التجهيزات المعلوماتية بجعل منتجاتهم آمنة، عن طريق جعل تحديثات البرامج المتعلقة بالأمان السيبراني آلية، وأن لا تتم (لا تفعّل) الصيانة عن بعد إلا من قبل المستخدم بعد اعتماد كلمات سر معقدة؛
- إجراء تغييرات لدى كل شخص ليس فقط لحماية نفسه بل لحماية الأشخاص الآخرين؛
- النظر إلى موضوع الأمان السيبراني من منظور دولي بسبب عالمية الإنترنت (الحيز العالمي) وبالتالي يجب إجراء التعديلات الفنية والتقنية في كل بلد ضمن إطار عمل متناسق؛
- حفظ بيانات التعريف الخاصة بالموردين في مجال التجارة الإلكترونية؛ فالغفلية لا تساعد في مكافحة الجرائم السيبرانية؛
- زيادة الاستثمارات في مجال تطبيق القانون لمكافحة الجرائم السيبرانية، علماً أنها تبقى أقل من تلك المخصصة للجرائم التقليدية؛
- مراقبة الشبكات والتعاون مع مزودي خدمات الاتصال، وتزويدهم بالعناوين الرقمية IP للحواسيب المسيطر عليها لإبلاغ اصحابها؛
- تخويل مزودي خدمات الشبكة الذين يقومون بالنقل العابر للبيانات Transit Providers وقف البيانات الصادرة عن الحواسيب المُسيطر عليها Botnet بعد فحص البيانات التقنية لرزم المعلومات packet headers؛
- تمكين مزودي خدمات الاتصال من منع رزم المعلومات من الخروج من شبكتهم إذا كان العنوان الرقمي المذكور فيها للمُرسل غير صحيح، وهو ما يعرف بتقليد العنوان الرقمي IP Spoofing؛
- زيادة التمويل من القطاع الخاص والعام للجهود الرامية إلى تثقيف المستهلك حول الأمان السيبراني؛
- عدم السماح للحواسيب غير المحمية تقنياً من الاتصال بالإنترنت؛

175 Micheal Barrett, Andy Steingruebl, Bill Smith, *Combating Cybercrime: Principles, Policies and Programs*, April 2011, https://www.paypal-media.com/assets/pdf/fact_sheet/PayPal_CombatingCybercrime_WP_0411_v4.pdf, p. 7 to 25.

- إنشاء وسائل آمنة للشركات الخاصة من أجل تبادل المعلومات حول المستخدمين المخترقين معلوماتياً وذلك خارج إطار القواعد التقليدية؛
- حثّ مسجلي مواقع الإنترنت registries/registrars للتدقيق في بيانات التعريف حول أصحاب المواقع والتأكد من صحتها، وحثّ الأيكان (ICANN The Internet Corporation for Assigned Names and Numbers) على تطبيق قواعد السلامة لديها.

3- تعاون الدولة مع المجتمع المدني ومزودي خدمات الشبكة

يقتضي على الدولة محاورة جمعيات المجتمع المدني التي قد تعارض الإجراءات الجزائية في مجال تحقيقات القضايا السيبرانية. ومن هذه الجهات، جمعيات الدفاع عن الحريات العامة، التي قد تتسبب بتعريض الخصوصيات والحريات الخاصة للانتهاك بفعل ضبط معلومات حركة البيانات ومحتوى الرسائل. ومن هذه الجهات أيضاً، مزودو خدمات الاتصال والذين قد يعترضون على الأعباء الإضافية التي ألقيت على عاتقهم من حيث حفظ معلومات حركة البيانات ومحتوى الرسائل.

واو- التعاون بين الدول العربية من أجل تعزيز الأمان السيبراني

1- تعزيز التعاون البيني في المنطقة العربية ومبرراته ومضامينه

يشكل تعزيز التعاون بين الدول العربية، وبينها وبين بقية الدول، حجر الأساس لمكافحة الجرائم السيبرانية ولتعزيز الأمان السيبراني، نظراً للطابع العابر للحدود لهذه الجرائم. ويمكن البدء بتفعيل الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010 وتطبيقها؛ وقد تضمنت هذه الاتفاقية تنظيماً حديثاً لآليات التعاون. ويمكن كذلك الاسترشاد بإرشادات الإسكوا الخاصة بالتشريعات السيبرانية ومنها الاسترشاد الخاص بالجرائم الإلكترونية مضافاً إليه الجزء الإجرائي الموضح في المرفق الثالث لهذه الدراسة والمقتبس من اتفاقية بودابست. وتفيد هذه الاتفاقيات/الإرشادات في إعداد واعتماد اتفاقيات ثنائية أو صياغة تفاهمات بين الدول العربية أو في مراجعة الاتفاقية العربية لجرائم تقنية المعلومات. وقد تضمنت الاتفاقيات المذكورة قواعد خاصة حول التعاون القضائي بين الدول بخصوص جمع الأدلة المعلوماتية والتحقيق في الجرائم السيبرانية، وهذه القواعد تتلخص بالآتي:

- التعاون إلى أقصى الحدود بين الدول في التحقيقات الجزائية وجمع الأدلة المعلوماتية، حتى في الجرائم التقليدية؛
- اعتبار الجرائم السيبرانية من الجرائم التي يقبل فيها استرداد المتهمين إذا كان معاقباً عليها في الدولتين بعقوبة سالبة للحرية لمدة تزيد على سنة، أو بعقوبة أشد؛
- الاستجابة لطلبات التعاون الموجهة بوسائل الاتصال السريعة، كالبريد الإلكتروني أو الفاكس، بشرط ضمان مستوى ملائم من الأمن والمصادقة على المصدر، ويمكن اشتراط تأكيد الطلب بمراسلة رسمية؛
- إرسال معلومات إلى دولة أخرى قد تفيدها في التحقيق في جريمة سيبرانية؛
- تسمية نقطة اتصال لدى كل دولة لإرسال طلبات المساعدة المتبادلة أو للإجابة عليها أو لتنفيذها؛
- حفظ البيانات المعلوماتية الموجودة على أراضي دولة مدة لا تقل عن 60 يوماً، بناءً على طلب دولة أخرى، على أن يتم ضبط هذه البيانات بصورة لاحقة بناء على طلب الدولة الأخرى؛

- الاستجابة لطلبات المساعدة المتبادلة المقدمة من دولة أخرى للبحث عن بيانات معلوماتية أو لضبطها أو لإعطائها، عندما تكون موجودة على أراضي الدولة الموجه اليها الطلب؛
- السماح لسلطات دولة بالوصول، عن طريق نظام معلوماتي موجود على أراضيها، إلى بيانات معلوماتية مخزنة على أراضي دولة أخرى، وذلك في حال موافقة الشخص صاحب السلطة على البيانات؛
- تقديم المساعدة المتبادلة، عن طريق تقديم معلومات حركة البيانات الجارية traffic data على أراضي إحدى الدول في زمن الإرسال الحقيقي real time؛
- تقديم المساعدة المتبادلة، عن طريق تقديم أو تسجيل محتوى الرسالة أو المعلومات المنقولة بواسطة نظام معلوماتي على أراضي إحدى الدول في زمن الإرسال الحقيقي real time، بالقدر الذي تسمح به قوانين تلك الدولة؛
- تسمية نقطة اتصال متاحة 24/24 ساعة، سبعة أيام في الأسبوع، لتقديم المساعدة المتبادلة.

من ناحية أخرى يجب أيضاً العمل على توحيد المصطلحات الخاصة بالأمان والأمن السيبراني وكذلك التشريعات السيبرانية من أجل تسهيل تبادل المعرفة والخبرات، وكذلك من أجل التنسيق بين التشريعات، وتسهيل التعاون والتفاعل فيما بين القضاة ورجال الشرطة وخاصة عند مكافحة الجرائم السيبرانية.

2- تحسين آليات التعاون القضائي بين الدول العربية

يبدو في التحقيقات الجزائية المهمة، حيث يكون عامل الوقت حاسماً، أن التعاون القضائي في مجال الجرائم السيبرانية قد تحسن تحسّناً ملحوظاً في السنوات الأخيرة، وذلك نتيجة لاتفاقية بودابست وللاتفاقية العربية لمكافحة جرائم تقنية المعلومات. غير أن نقاط ضعف اتفاقية بودابست هي عدم اعتمادها لدى أطراف أساسيين في العالم في هذا المجال، كروسيا والصين، وكذلك بعض دول آسيا وأفريقيا وأمريكا الجنوبية وقد يرد على ذلك بتبني دول عديدة محتوى اتفاقية بودابست ضمن قانونها الداخلي. ومن نقاط الضعف الأخرى عدم وجود آلية لإجبار أي دولة موقعة على الاتفاقية على تنفيذ التعاون، وإتاحة المجال لأية دولة موقعة عليها لرفض طلب المساعدة، لأسباب خاصة مثل وجود ضرر لاحق بسيادتها أو أمنها أو نظامها العام أو مصالحها الأساسية[176]. وتجدر الإشارة إلى أن الدول العربية لم توقع على اتفاقية بودابست، باستثناء المملكة المغربية، والتي ليست ملزمة بها.

وفي هذا الإطار يجدر التركيز على آليات التعاون غير الرسمية بين الأجهزة المختصة بين الدول، باعتبار أن اتّباع الإجراءات الرسمية في مجال التعاون القضائي يتطلب وقتاً طويلاً، قد يؤدي إلى ضياع الأدلة المعلوماتية وفرار المجرمين.

وقد ظهرت في مؤتمرات كثيرة رغبة قوية للتعاون بين الدول. فعلى سبيل المثال، أوصى المشاركون في المؤتمر الإقليمي السادس للجمعية الدولية لأعضاء النيابة العامة لدول الشرق الأوسط وآسيا والمحيط الهادئ، تحت عنوان "النيابات العامة في القرن 21"، الذي انعقد بدبي في عام 2009، بضرورة تعاون أعضاء

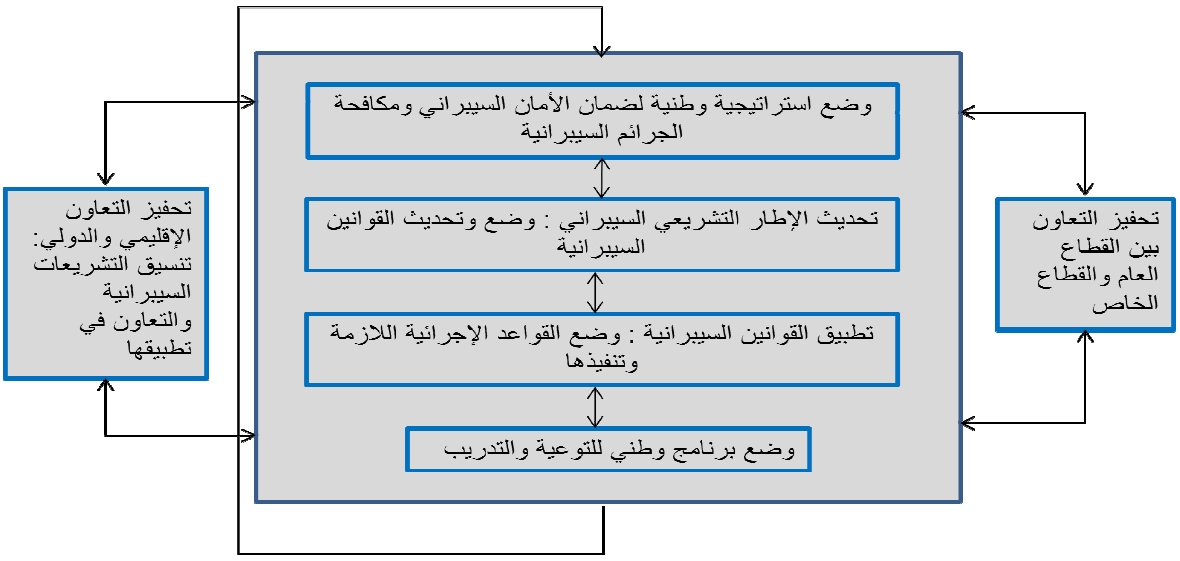
176 Michael A. Vatis, *The Council of Europe Convention on Cybercrime*, http://cs.brown.edu/courses/csci1950-p/sources/lec16/Vatis.pdf, p. 14.

النيابة العامة في جميع أنحاء العالم بصورة فاعلة لمكافحة العدد المتزايد من الجرائم السيبرانية، عن طريق الدعم والمساعدة القانونية المتبادلة، ونقل أفضل الممارسات، وتدريب النيابات العامة[177].

أخيراً، يدخل ضمن مفهوم التعاون، العمل بين دول المنطقة على تطوير آليات تبادل الخبرات والمعارف العلمية والتقنية والتجارب والحلول، عن طريق الزيارات المتبادلة والمؤتمرات الدورية وإنشاء قنوات اتصال دائمة. ويمكن أن يتم ذلك عن طريق توقيع بروتوكولات تعاون وتنسيق بين دول المنطقة العربية.

ويلخص الشكل 6 المكونات الأساسية لإطار العمل المقترح لضمان الأمان السيبراني ومكافحة الجرائم السيبرانية.

الشكل 6- إطار العمل المقترح لضمان الأمان السيبراني ومكافحة الجرائم السيبرانية



177 جريدة دار الخليج، محمد رباح، طارق زياد، الثلاثاء 17 تشرين الثاني/نوفمبر 2009، دعا إلى ضمان أمن وسلامة أعضاء النيابة العامة مؤتمر النيابات العامة في القرن 21 يوصي بالتعاون لمكافحة الجريمة الإلكترونية، http://www.mohamoonuae.com/default.aspx?Action=DisplayNews&type=3&ID=9216، ص 1.

رابعاً- الخاتمة

غيّر الفضاء السيبراني الكثير من الجوانب الحياتية، الاقتصادية والاجتماعية، لكن كما نشأت عنه المنافع، شابته الكثير من المخاطر التي تتطلب مقاربة جديدة لحماية مستخدمي الإنترنت وبناء ثقتهم بالفضاء السيبراني وبالتالي تعظيم الاستفادة منه. فمن أجل الاستفادة من الإمكانات التي وفرتها تكنولوجيا المعلومات والاتصالات، لا بد من أن تبقى التكنولوجيا آمنة وفعالة، دون اعتراض للمعلومات في خط سيرها، مع ضمان خصوصيتها وسلامتها من التحوير، وذلك أساسي لطمأنة الناس وبث الثقة في نفوسهم حول الإنترنت. غير أن الأعمال الإجرامية قد تطورت بفعل تكنولوجيا المعلومات، حيث أصبح المجرمون أكثر احترافاً وبل منهم أصحاب الأعمال والخبرات الخاصة. ومن الغريب كيف أن التكنولوجيا التي تعتمد عليها الضحية أصبحت هي ذاتها الأداة التي يستخدمها المرتكب المحترف القادر على إخفاء هويته أو تغييرها.

إن للجرائم السيبرانية ولانتهاكات الأمان في الفضاء السيبراني عواقب عديدة على الصعيد الاقتصادي والاجتماعي والفكري وعلى الصحة العامة وكذلك على الأمن القومي. وقد تطال الجرائم السيبرانية الأمن الاقتصادي أو قد تطال سمعة الأفراد أو الشركات وفي كلتا الحالتين تؤثر هذه الجرائم على ثقة المستخدم بالفضاء السيبراني. ومن أبرز مظاهرها غفلية الفاعل وإخفاء الهوية والتزوير وانتهاك الخصوصية والتهرب الضريبي. ويعتقد كثيرون أن الجرائم السيبرانية وانتهاكات السلامة المعلوماتية في ازدياد، ولو تدريجي، وأن التدابير التقنية وحدها، بالرغم من ضرورتها وأهميتها، غير قادرة على مكافحة هذا النوع من الأفعال. وهنا تبرز أهمية وضع إطار تشريعي وطني، في ظل تنسيق إقليمي، يستكمل بتعاون دولي[178].

قدمت هذه الدراسة إطاراً عاماً وطنياً استراتيجياً للأمان السيبراني ومكافحة الجرائم السيبرانية. ومن المؤمل أن تستفيد دول المنطقة العربية من هذه الدراسة، ولا سيما من القسم الثالث منها المتعلق بإطار العمل للأمان السيبراني في المنطقة العربية، والمرفق الثالث والذي يتضمن إرشادا خاصا بالقواعد الإجرائية للجرائم السيبرانية، والذي يتضمن أيضا مواد خاصة بعمل السلطات القضائية وأخرى خاصة بالأدلة الرقمية. ويتطرق الإطار إلى الجانب التشريعي وإلى آليات تطبيق القانون مع الإشارة إلى أهمية تنسيق الجهود والتعاون على المستوى الوطني في ما بين أجهزة الدولة المختلفة وكذلك التعاون مع القطاع الخاص والمجتمع المدني. ويولي أيضاً هذا الإطار أهمية خاصة إلى حملات التوعية للمستخدمين وإلى ضرورة التدريب التخصصي للعاملين في مجال الأمن السيبراني والتحقيقات القضائية. ويوضح الإطار أهمية التكامل في ما بين القوانين التشريعية السيبرانية في البلد الواحد وإلى ضرورة التنسيق حول هذه القوانين على الصعيدين الإقليمي والدولي. وتشير الدراسة إلى أهمية دور الأفراد في ضمان الأمان السيبراني، إذ يقع على عاتق كل شخص المساهمة في هذا الجهد عن طريق أفعاله الشخصية اليومية وما يحمله من الإنترنت أو ما يرسله عبرها. ولا يجب أن يتعارض حق أي شخص بالوصول إلى المعلومات على الإنترنت مع واجباته باتخاذ وسائل الحماية التقنية منعاً للإضرار بنفسه وكذلك بغيره على الشبكة. ويشكل ما تقدم استراتيجية وطنية للأمن السيبراني ومكافحة الجرائم السيبرانية، ويجب على كل دولة من دول المنطقة العربية وضع هكذا استراتيجية وأن تنفذها وأن تراجعها دورياً.

كما بينت الدراسة واقع بعض الدول العربية في مكافحة المخاطر السيبرانية، والتفاوت الذي تشهده حيث أن بعض هذه الدول قد بلغ مرحلة متقدمة من ناحية التشريع وتطبيقه والتوعية والتدريب، في حين أن دولاً أخرى ما زالت تعمل على إقرار تشريعات أو تسعى لتطبيقها أو لوضع برامج توعية وتدريب أو لتوفير

178 Micheal Barrett, Andy Steingruebl, Bill Smith, *Combating Cybercrime: Principles, Policies and Programs*, April 2011, https://www.paypal-media.com/assets/pdf/fact_sheet/PayPal_CombatingCybercrime_WP_0411_v4.pdf, p. 2.

الموارد المادية اللازمة لذلك. وقد تم الاعتماد في تحليل واقع المنطقة العربية على نتائج الاستبيان الذي أرسل إلى الدول الأعضاء في الإسكوا، وإلى المعلومات المتوفرة في العديد من المصادر والمراجع العلمية وإلى دراسات الإسكوا السابقة في هذا المجال. ويوضح المرفق الرابع ملخص أجوبة الاستبيان المرسل إلى دول الإسكوا بموجب هذه الدراسة.

وفي الختام، يعد توفير الأمان في الفضاء السيبراني عملية معقدة وصعبة ومكلفة[179]، كما أنها عملية تحتاج إلى تضافر الجهود خاصة في ظل تعدد الحلول وتنوعها في مكافحة الجرائم السيبرانية[180]. لذا يوصى باعتماد سلة متكاملة من الحلول، تعالج جميع الجوانب التي تطرق إليها الإطار العام في القسم الثالث من الدراسة، واعتماد القدر الأكبر من التوصيات المذكورة في مختلف أقسام الدراسة. إذ يبدو من الاستراتيجيات المختلفة المعتمدة في العالم أن مقاربة الجرائم السيبرانية تتم ضمن الإطار الأوسع للأمان السيبراني.

179 Cabinet Office, *The UK Cyber Security Strategy, Protecting and promoting the UK in a digital world*, November 2011, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf, p. 16.

180 Micheal Barrett, Andy Steingruebl, Bill Smith, *Combating Cybercrime: Principles, Policies and Programs*, April 2011, https://www.paypal-media.com/assets/pdf/fact_sheet/PayPal_CombatingCybercrime_WP_0411_v4.pdf, p. 7.

المرفق الأول

شرح المفاهيم التكنولوجية الأساسية المعتمدة في هذه الدراسة

كان أول الباحثين الذين تناولوا موضوع جرائم الحاسوب هو دون باركر (Donn B. Parker) منذ أوائل السبعينيات من القرن الماضي، في معهد ستافورد للبحوث، وقد كتب أول دليل أساسي فدرالي حول تطبيق القانون Computer Crime- Criminal Justice Resource Manual. كما كانت منظمة الإنتربول السبّاقة على الصعيد الدولي في إثارة موضوع جرائم الحاسوب والتشريع الجزائي في مؤتمر عقد في باريس في عام 1970[181]. أما أولى جرائم المعلوماتية التي عرفت فهي الضرر المادي الحاصل على جهاز حاسوب رئيسي mainframe. وقد تطورت تاريخياً المفاهيم التقنية والقانونية في مجال الأمن السيبراني، ويمكن إيراد تعاريفها لفهم أكبر.

يمكن تعريف المخاطر المعلوماتية أو السيبرانية، وفق المعايير الفدرالية لمعالجة المعلومات - متطلبات الأمن الدنيا لأنظمة المعلومات الفيديرالية في الولايات المتحدة الأمريكية *Federal Information Processing Standards (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems*، بأنها أي حدث أو ظرف يمكنه التأثير على عمليات المؤسسات وممتلكات المؤسسات والأفراد، عبر نظام معلومات، عن طريق الدخول غير المشروع أو تدمير المعلومات أو إفشائها أو تعديلها أو وقف الخدمات. وتشمل المخاطر كذلك إمكانية استغلال مكامن ضعف نظام المعلومات. وتصنف المخاطر بأنها إما قصدية وإما عرضية (عطل في الحاسوب أو البرنامج) أو بيئية (هزة أرضية، حريق أو غيرها). ويعتبر الهجوم المعلوماتي إيجابياً عندما يرمي إلى تعديل وظائف النظام أو البيانات، وسلبياً عندما يرمي إلى الاطّلاع على معلومات[182].

ويمكن تعريف الأمن السيبراني كمجموعة الأدوات والسياسات ومبادئ الأمن والاحتياطات والتوجيهات ومقاربات إدارة المخاطر والأعمال والتدريب والممارسات الفُضلى والضمانات التي يمكن استخدامها لحماية البيئة السيبرانية وممتلكات المؤسسات والمستخدمين. وتضم هذه الممتلكات أجهزة الحاسوب المربوطة بالشبكة، والبنية الأساسية الشخصية، والأنظمة المعلوماتية، والخدمات، وأنظمة الاتصالات، والبيانات المخزنة أو المنقولة. ويجهد الأمن السيبراني لضمان أمن هذه الممتلكات في البيئة السيبرانية. أما الأهداف العامة للأمن السيبراني فتتضمن: الإتاحة availability، والسلامة integrity، والموثوقية authenticity وعدم إمكانية الإنكار non-repudiation، والسرية confidentiality[183].

ومن مسؤولية كل شركة أو شخص أن يحمي بياناته ليس فقط من أجل سلامة عملياته التجارية بل أيضاً من أجل أمن زبائنه. فالقراصنة يبحثون عن الشركات التي لا تتخذ تدابير حماية تكنولوجية.

ومن أجل فهم أعمق للجرائم السيبرانية، ينبغي فهم تعريف الفضاء السيبراني، فهو شبكات المعلومات والبنية الأساسية المترابطة، متضمّنة الإنترنت، وشبكات الاتصالات، وأنظمة الحاسوب، ووحدات معالجة المعلومات والتحكم في الصناعات الحساسة. أي أن الفضاء السيبراني هو البيئة الافتراضية للمعلومات والترابط بين الناس[184]. والفضاء السيبراني هو نطاق تفاعلي مؤلف من شبكات رقمية تستخدم لحفظ وتعديل وتوصيل المعلومات، وهو يتضمن الإنترنت، لكنه يتضمّن أيضاً أنظمة المعلومات التي تستخدم في نشاطاتنا الاقتصادية والخدماتية والبنية الأساسية[185]. ويمكن إعطاء تعريف أولي للجريمة السيبرانية أو المعلوماتية، بأنها أي تصرف غير قانوني أو غير أخلاقي أو غير مرخص يرتبط بالمعالجة الآلية للبيانات أو بنقلها[186].

---

181 Stein Schjolberg, *The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva*, December 2008, http://www.cybercrimelaw.net/documents/cybercrime_history.pdf, p. 2, 3.

182 Wikipedia, Threat (computer), http://en.wikipedia.org/wiki/Threat_(computer), p. 2, 4.

183 ITU, Marco Gercke, *Understanding Cybercrime: Phenomena, Challenges and Legal Response,* September 2012, p. 7.

184 National Security Agency, USA, *Statement for the Record, Lieutenant General Keith Alexander, Commander, Joint Functional Component Command for Network Warfare*, Before the House Armed Services Committee, Terrorism, Unconventional Threats, and Capabilities Subcommittee, May 5, 2009, http://www.nsa.gov/public_info/speechestestimonies/5may09_dir.shtml.

185 Cabinet Office, *The UK Cyber Security Strategy, Protecting and promoting the UK in a digital world*, November 2011, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf, p. 11.

186 Organization for Economic Cooperation and Development (OECD), OECD recommendations of 1986.

وبالمعنى العام، فإن الجرائم السيبرانية تم تعريفها على أنها نشاطات غير مشروعة أو غير قانونية تحدث على شبكة الإنترنت. كما يمكن تعريف الجريمة السيبرانية بأنها نشاط إجرامي يستخدم الحواسيب والإنترنت للاعتداء، إما مباشرةً أو غير مباشرةً، على المستهلكين أو الأعمال. وهناك عدة فئات ضمن الجرائم السيبرانية، منها سرقة الأموال مباشرةً من البنوك أو البطاقات المصرفية، وانتحال الهوية Identity Theft، والتعدي على الملكية الفكرية[187]. يدخل ضمن سرقة الهوية الإلكترونية سرقة رقم الضمان الاجتماعي ورقم جواز السفر وتاريخ الميلاد والعنوان وأرقام الهاتف وكلمات السر وأرقام الحسابات.

وتختلف نية الفاعل الجرمية في الجرائم السيبرانية من حالة إلى أخرى، فقد تكون بدافع الربح المادي أو الشهرة، أو بدافع أهداف سياسية كمهاجمة المواقع الإلكترونية لدولة عدوة، أو الحصول على حظوات لدى الآخرين أو شكرهم، أو إثبات الذات والمعرفة التقنية، أو التنافس مع الآخرين. وفي ضوء هذه التعاريف، تتنوع جرائم المعلوماتية وتتعدد، لدرجة يصعب معها حصرها، ما بين التزوير والتزييف الرقمي أو المعلوماتي، وتدمير وإتلاف البرامج والبيانات والمعلومات، والسطو على البيانات والمعلومات، والاحتيال الرقمي، والتجسس[188]. وقد تكون المعلوماتية هدف الجريمة أو موضوعها أو محل الاعتداء، كالتعدي على البيانات أو الأنظمة، أو قد تكون المعلوماتية أداة أو وسيلة لارتكاب جريمة تقليدية كالاحتيال المعلوماتي، أو قد تكون المعلوماتية موضع وجود أدلة معلوماتية لجريمة تقليدية[189].

أما التعريف الضيق للجرائم السيبرانية، فيربطها باستخدام شبكة معلوماتية، فالتعرض لنظام معلوماتي غير مرتبط بشبكة معلوماتية لا يعتبر جريمة سيبرانية[190]، وهذا التعريف الضيق منتقد إذ لا يتوافق مع اتفاقية بودابست، ويخرج كثير من جرائم الحاسوب من نطاقه. ويمكن تجاوز أمر تعريف الجرائم السيبرانية وعدم الحاجة لوجود تعريف كهذا، طالما أن هناك تعريفات مفصلة لكل جريمة من الجرائم المرتبطة بالحاسوب والشبكات المعلوماتية. لذا، فهناك عدة إشكاليات حول ما يدخل ضمن نطاق الجرائم السيبرانية، فالبعض يعتبر بعض النشاطات الجرمية خارج الخط لا تشكل جرائم سيبرانية، أو أن الجرائم التي تتم بوسيلة معلوماتية تبقى جريمة تقليدية. كما أن بعض الأفعال قد تكون مجرّمة في بلد وغير مجرّمة في بلد آخر (التجريم المزدوج) مثل المقامرة على الخط Online gambling.

وترتبط الأدلة الرقمية أو المعلوماتية بالجرائم السيبرانية التي تشكل عنصراً أساسياً في إثبات الجريمة. فالأدلة المعلوماتية هي معلومات في شكل رقمي يمكن اعتمادها كدليل على وقائع أو تصرفات في المحكمة. مجموعة المجالات أو النبضات المغناطيسية أو الكهربائية التي يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات خاصة لتظهر في شكل صور أو تسجيلات صوتية أو مرئية[191]. كما يمكن تعريف الدليل المعلوماتي أو الرقمي بأنه ذلك الدليل المشتق من النظم البرامجية المعلوماتية الحاسوبية، وأجهزة ومعدات وأدوات الحاسوب، أو شبكات الاتصالات، أو بواسطتها، عن طريق إجراءات قانونية وفنية، لتقديمها للقضاء بعد تحليلها علمياً أو تفسيرها ووضعها في شكل نصوص مكتوبة، أو رسوم أو صور أو أشكال أو أصوات، لإثبات وقوع الجريمة ولتقرير البراءة أو الإدانة فيها[192].

ويُعرف علم الأدلة الجنائية المعلوماتية (أو الجنائيات الحاسوبية) Computer forensics بأنه التحليل المُمنهج للتجهيزات المعلوماتية بهدف البحث عن دليل معلوماتي أو رقمي، حيث يتم عبر مرحلتين: مرحلة التحقيق (البحث عن الأدلة، تجميع الأدلة وحفظها وتحليلها) ومرحلة تقديمها أثناء المحاكمة للمحكمة[193].

---

187 Micheal Barrett, Andy Steingruebl, Bill Smith, *Combating Cybercrime: Principles, Policies and Programs*, April 2011, https://www.paypal-media.com/assets/pdf/fact_sheet/PayPal_CombatingCybercrime_WP_0411_v4.pdf, p. 3.

188 عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، الرياض، 12-14 تشرين الثاني/نوفمبر 2007، ص 6.

189 University of Mississippi, School of Law, National Center for Justice and the Rule of law, *Combating cyber crime: essential tools and effective organizational structures, A guide for policy makers and managers*, http://www.olemiss.edu/depts/ncjrl/pdf/CyberCrimebooklet.pdf, p. 2, 3.

190 ITU, Marco Gercke, *Understanding Cybercrime: Phenomena, Challenges and Legal Response,* September 2012, p. 11.

191 طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي، ص 18، www.startimes.com/f.aspx?t=30245909.

192 عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، الرياض، 12-14 تشرين الثاني/نوفمبر 2007، ص 13.

193 ITU, Marco Gercke, *Understanding Cybercrime: Phenomena, Challenges and Legal Response*, September 2012, p. 235, 240.

وقد قسمت الجرائم السيبرانية إلى فئات: فئة اختراق الأنظمة، وفئة الاعتداءات المرتبطة بالمحتوى، وفئة التعديات على الملكية الفكرية والعلامات التجارية، والتعديات المرتبطة بالحاسوب، والإرهاب السيبراني والحرب السيبرانية. ويبين المرفق الثاني من هذه الدراسة لائحة مفصلة بالجرائم السيبرانية المختلفة، ويمكن أيضاً مراجعة النصوص القانونية المتعلقة بالجرائم السيبرانية، التي تبين عناصر كل جرم وأركانه، في إرشاد الإسكوا المتعلق بالجرائم السيبرانية.

وتتنوع فئات المرتكبين من أفراد إلى مجموعات منظمة إلى نشاطات مدعومة من دول. وتختلف النية الجرمية وفق هذه الفئات. فنية الفرد المرتكب هي عادة تحقيق الربح أو الشهرة أو إثبات الذات، في حين تسعى المجموعات المنظمة إلى الربح، وتحاول أنشطة الدول انتهاك سلامة وأمن دول عدوة أو تحقيق أهداف اقتصادية، أو للتجسس الصناعي أو التجاري. ويقدر أن نسبة 80 في المائة من الجرائم السيبرانية أساسها نشاطات منظمة، ولا سيما جرائم الاحتيال والتزوير المعلوماتي وسرقة الهوية[194].

وكتطبيق عملي، يمكن إيراد عدة أمثلة على الجرائم السيبرانية، منها حالات عمليات الاحتيال المعلوماتي، فمثلاً قد يعمد المحتال إلى وضع جهاز معلوماتي فوق جهاز قارئ البطاقة المصرفية أو بطاقة الائتمان، وينسخ هذا الجهاز معلومات الشريطة الممغنطة للبطاقة المصرفية، ومنها رقم البطاقة والرقم السري[195].

ومن الأمثلة على الحرب السيبرانية، الهجمات السيبرانية لتعطيل خدمات مواقع إلكترونية Denial of service في عام 2007 في أستونيا، حيث تم إغراق الموقع بطلبات لا يستطيع تلبيتها، وكذلك الهجمات على الأنظمة المعلوماتية للقيادة والتحكم في جورجيا في عام 2008، وإصابة الفيروس المعلوماتي Stuxnet لمشغلات المفاعلات النووية الإيرانية.

الأدلة المعلوماتية

يوجد العديد من العناصر التي يمكن أن تكون بمثابة أدلة معلوماتية، وهذه العناصر بعضها معروف بالنسبة للمستخدم العادي مثل الملفات المعلوماتية والصور الرقمية والأفلام الرقمية، وبعضها الآخر مرتبط بتفاعله مع محيطه الخارجي مثل لائحة الأشخاص contact list وأرقام هواتفهم، والرسائل النصية القصيرة. وتتضمن الأدلة الرقمية أيضاً معلومات مخبئة بالنسبة للمستخدم العادي وموجودة إما في ملفات النظام مثل سجلات الدخول log files، أو مرتبطة بتبادل المعلومات والبيانات عبر الشبكة ومنها معلومات حركة البيانات، وملفات الإنترنت للنظام العالمي لتحديد المواقع GPS internet files. ويبين الجدول 3 الأدلة المعلوماتية المستخدمة اليوم.

الجدول 3- الأدلة المعلوماتية

الأدلة المعلوماتية	المرادف باللغة الإنكليزية
ملفات معلوماتية	files
صور	pictures
أفلام رقمية	videos
أرشيف إلكتروني	electronic archive
رسائل البريد الإلكتروني	emails
رسائل صوتية	voice messages
رسائل نصية قصيرة	SMS
لائحة الأشخاص وأرقام الهواتف	contact list
سجل المواعيد	calendar
سجلات الدخول	log files
معلومات حركة البيانات	traffic data
محتوى المعلومات	content data
معلومات التعريف	identification data
ملفات الإنترنت المؤقتة	temporary internet files
إحداثيات النظام العالمي لتحديد المواقع	GPS locations
كلمات السر	passwords/user names
الآثار الرقمية أو (المعلوماتية أو الإلكترونية)	electronic traces

194 United Nations Office on Drugs and Crime, UNODC, *Comprehensive study on cybercrime*, draft, February 2013, p. 17, 44.

195 Kristin M. Finklea, Catherine A. Theohary, Cybercrime: Conceptual issues for Congress and U.S. law enforcement, January 2013, http://fas.org/sgp/crs/misc/R42547.pdf, p. 7.

المرفق الثاني

قائمة الجرائم السيبرانية

فيما يلي قائمة بما تم تصنيفه كجريمة سيبرانية[196]، (أنظر المرجع)[197].

- التجسس المعلوماتي/السيبراني (Data Espionage) حيث يتم اختراق الأنظمة المعلوماتية للآخرين لسرقة المعلومات. وقد يعترض المرتكبون خطوط الاتصالات السلكية واللاسلكية (البريد الإلكتروني أو اتصالات الصوت على الإنترنت). ويتم هذا الأمر إما لغرض المتعة وإثبات المهارة، وإما لكشف أمور سرية وفضحها أمام الجمهور، وإما لبيع المعلومات نظراً لقيمتها التجارية أو لكشف أسرار مالية أو صناعية عن الشركات المنافسة، وإما لسرقة كلمات السر للحسابات المصرفية أو البريد الإلكتروني، أو لأسباب سياسية إذا كان موجهاً ضد دولة معينة؛

- الإرهاب السيبراني (cyberterrorism)، ويتمثل بالاعتداء على شبكة الإنترنت بغية تعطيل خدماتها وإشاعة عدم الثقة في الإنترنت في صفوف المستخدمين. والأهم من ذلك هو الهجمات على البنية الأساسية المعلوماتية التي تشغل كثيراً من القطاعات الحساسة، كالنقل والطاقة والطيران. ويمكن أيضاً استخدام الإنترنت للترويج للأفكار الإرهابية أو لجمع المعلومات أو للتحضير لهجمات مادية أو لنشر مواد تدريبية (كصنع متفجرات) أو لجمع التمويل أو لتجنيد أشخاص أو للتواصل بين الشبكات الإرهابية؛

- الحرب السيبرانية (cyberwarfare)، وتتمثل باستخدام تكنولوجيا المعلومات في تدمير أو تعطيل أو كشف معلومات أو أنظمة معلومات ذات قيمة للعدو. حيث قد تتعرض المواقع والأنظمة الإلكترونية لدولة معنية لهجمات من دولة أخرى أو جهات مرتبطة بها. وقد تقع هذه الهجمات ضمن حرب حقيقية بين الدولتين، مثال حالة أستونيا عام 2007 وحالة جورجيا عام 2008 وفيروس Stuxnet؛

- الدخول غير المشروع إلى نظام معلوماتي (Illegal Access/Hacking)، وتشترط بعض القوانين لتجريم الفعل وجود حماية تقنية للنظام المعلوماتي المخترق أو حصول تعديل على البيانات المعلوماتية أو وجود نية جرمية لدى الفاعل؛

- الاعتراض غير المشروع للبيانات والاتصالات المعلوماتية (Illegal interception) ولا سيما اللاسلكية منها (wireless)، كاعتراض رسائل البريد الإلكتروني أو المعلومات المدخلة على مواقع إلكترونية أو قاعدة معلومات على الخط، أو الصوت على الإنترنت (VoIP communications). ولا تدخل المعلومات المُخزنة على وسيط إلكتروني كقرص صلب ضمن موضوع هذا الجرم؛

- الاعتداء على البيانات الرقمية (Data Interference)، حيث يقوم المرتكبون بمحو البيانات أو تعديلها أو منع الوصول إليها، وهو ما يعرف بالاعتداء على سلامة البيانات integrity وتوفرها availability؛

- الاعتداء على الأنظمة المعلوماتية (System interference)، وقد تكون الهجمات على الحواسيب مادية لتحطيم الأجهزة؛

- إساءة استعمال التجهيزات والبرامج المعلوماتية (misuse of devices) لارتكاب أفعال جرمية؛

- انتحال الهوية الإلكترونية (identity theft)، وأهم عناصرها رقم الضمان الصحي ورقم جواز السفر وتاريخ الولادة وعنوان السكن ورقم الهاتف وكلمات السر. قد يستعمل المُرتكب هذه المعلومات لفتح حسابات مصرفية أو للاستيلاء عليها أو لتجاوز آليات التحقق من الهوية؛

---

196 قامت الإسكوا بوضع نموذج موضوعي للجرائم السيبرانية عام 2012 والذي يتضمن أنواع الجرائم السيبرانية. يرجى مراجعة الإرشاد الخامس من إرشادات الإسكوا للتشريعات السيبرانية والخاص بالجرائم السيبرانية: http://isper.escwa.un.org/Portals/0/Cyber%20Legislation/Regional%20Harmonisation%20Project/Directives/Dir-5-Cybercrimes.pdf.

197 Wikipedia, International Cybercrime,http://en.wikipedia.org/wiki/International_cybercrime, p. 2-4. Micheal Barrett, Andy Steingruebl, Bill Smith, *Combating Cybercrime: Principles, Policies and Programs*, April 2011, https://www.paypal-media.com/assets/pdf/fact_sheet/PayPal_CombatingCybercrime_WP_0411_v4.pdf, p. 3, 4. ITU, Marco Gercke, *Understanding Cybercrime: Phenomena, Challenges and Legal Response,* September 2012, p. 17 and following.

- المواد الإباحية للأطفال (Child Pornography)، وقد أصبحت شبكة الإنترنت الوسيلة الأولى لعرضها وترويجها، ويأتي الاتجار بهذه المواد بأرباح كبيرة لأصحابها؛

- المعالجة الآلية للبيانات ذات الطابع الشخصي (treatment of personal data) دون ترخيص، أو مخالفة القواعد الخاصة بهذه المعالجات؛

- المواد الإباحية بوجه عام (Erotic or pornographic material)، حيث يتم نقلها عبر المواقع الإلكترونية أو أنظمة مشاركة الملفات (file sharing) أو الرسائل القصيرة (instant messaging)؛

- الحض على الكراهية والعنف والعنصرية (Racism Hate/Violence speech)، حيث تستخدم مجموعات متطرفة المواقع الإلكترونية لنشر أفكارها، وهذه المواقع في ازدياد مستمر؛

- القدح والذم defamation والتشهير والتهديد والابتزاز عبر شبكة الإنترنت، ولا سيما على المواقع الإلكترونية ومواقع التواصل الاجتماعي ومنتديات النقاش forums/chat rooms؛

- البريد الواغل (أو غير المرغوب فيه) Spam، الذي يتضمن إعلانات لبضائع أو خدمات أو حتى برامج خبيثة malicious software، ويتم إرساله عادةً من عناوين رقمية مختلفة مثل Botnets لتفادي برامج الترشيح filters؛

- ألعاب المقامرة على الخط غير المشروعة illegal gambling؛

- الاحتيال المعلوماتي، عن طريق المناورات على الإنترنت، وعن طريق البطاقات المصرفية والعمليات المصرفية على الإنترنت Credit card/Internet banking. ونذكر حالة التصيد phishing، حيث يتم إيقاع الضحية في الغلط لإفشاء معلومات شخصية حساسة كأرقام الحسابات وكلمات السر، إذ يقوم المحتال بإنشاء موقع مشابه للموقع الأصلي للشركة أو المصرف الذي يتعامل معه العميل الذي يدخل كلمة السر العائدة له على هذا الموقع الوهمي، أو قد يرسل المحتال رسالة بريد إلكتروني وهمية شبيهة بتلك الصادرة عن المصدر الأصلي ليطلب من الضحية تأكيد كلمة السر. وكذلك نذكر التصيد عن طريق الرسائل القصيرة على الهاتف النقال أو بتقنية نقل الصوت على الإنترنت SMS phishing وVoIP؛

- الاعتداء على الملكية الفكرية والعلامات التجارية وبراءات الاختراع Software/music/movies piracy، مثل النسخ غير المشروع للأغاني والأفلام والبرامج، أو تنزيلها من مواقع إلكترونية، أو تبادلها بتقنية مشاركة الملفات file-sharing software؛

- جرائم الإساءة إلى الأديان xenophobic material or insults related to religious symbols؛

- تزوير السندات الإلكترونية Forgery والبطاقات المصرفية credit/debit cards واستخدامها، وسرقة أرقام البطاقات المصرفية العائدة لعملاء على مواقع التجارة الإلكترونية وبيعها لآخرين؛

- تبييض الأموال cyberlaundering عن طريق الإنترنت، ولا سيما عن طريق المقامرة الإلكترونية والتحاويل الإلكترونية والنقود الإلكترونية الافتراضية وإخفاء الهوية؛

- المطاردة السيبرانية cyberstalking وهي المطاردة التي تنطوي على استخدام الإنترنت أو البريد الإلكتروني أو الهواتف المحمولة، ويمكن أن تشمل إرسال رسائل البريد الإلكتروني والرسائل النصية (SMS) أو الرسائل الفورية التي تسيء أو تهدد، أوتنشر تعليقات مسيئة. كما قد تتضمن هذه الرسائل إرسال الصور الحميمة أو أشرطة الفيديو. ولاعتبار هذا التبادل الإلكتروني مطاردة يجب أن يتم إجراء هذا الإرسال عدة مرات وأن ترتكب من قبل الشخص نفسه؛

- التحرش الجنسي السيبراني cyberharassment وهو استخدام تكنولوجيا المعلومات والاتصالات للتحرش الجنسي في النساء، عن طريق إرسال رسائل البريد الإلكتروني الواغل أو غير المرغوب فيه أو الرسائل القصيرة SMS أو عن طريق التفاعل غير الملائم عبر مواقع شبكات التواصل الاجتماعي.

المرفق الثالث[198]

قانون نموذجي متعلق بالقواعد الإجرائية الخاصة بالجرائم السيبرانية والأدلة الرقمية

المادة 1

يطبَّق هذا القانون على الجرائم السيبرانية وعلى كل جريمة مرتكبة بواسطة نظام معلوماتي، وعلى ضبط الأدلة الرقمية (أو الإلكترونية) لكل جريمة، وعلى التحقيقات الجزائية المتعلقة بها.

المادة 1 (مكرر)

تصلح الأدلة الرقمية لإثبات الجرائم السيبرانية وغيرها من الجرائم أمام القضاء.

ويعود للمحكمة تقدير قيمة الدليل الرقمي وحجيته في الإثبات، ويجب أن لا يكون قد تعرض لأي تغيير خلال ضبطه وحفظه.

المادة 2

تطبق فيما يتعلق بالالتزامات المفروضة على مزودي خدمات الشبكة، المتعلقة بحفظ مضمون المعلومات أو معلومات حركة البيانات وتقديمها إلى القضاء، أحكام الباب الثاني المعنون "النظام القانوني لمزودي خدمات الشبكات الإلكترونية"، وأحكام الباب الرابع المعنون "التنصّت على الاتصالات الخاصة والشخصية"، وكذلك الباب الخامس المتعلق بالأحكام الجزائية، من إرشاد الإسكوا حول الاتصالات الإلكترونية وحرية التعبير.

وتُطبَّق هذه الالتزامات على أي مزوّد خدمات للشبكة له على أراضي الدولة مركز إدارة فعلي أو محل إقامة يمارس فيه نشاطاً اقتصادياً راهناً، وذلك بصرف النظر عن جنسيته، وعن مكان تأسيسه ومقرّه الرئيسي إذا كان شخصاً اعتبارياً، وعن المكان الذي توجد فيه التجهيزات التقنية التي يستخدمها.

المادة 3

يعود للسلطات القضائية أن تلزم:

- أي شخص بتسليم أيه بيانات معلوماتية معينة في حوزته أو تحت سيطرته، تكون مخزنة في نظام معلوماتي أو على دعامة إلكترونية؛
- أي مزوّد خدمة شبكة بتسليم أيه بيانات معلوماتية معينة في حوزته أو تحت سيطرته، تكون متعلقة بالمستفيدين من خدماته.

المادة 4

للسلطات القضائية الحق أن تدخل إلى أي نظام معلوماتي أو جزء منه، أو تفتش عليه، وكذلك على البيانات المخزنة فيه أو على أي دعامة إلكترونية.إذا كانت البيانات مخزّنة في نظام معلوماتي آخر موجود على أراضي الدولة، ويمكن الوصول إليها من النظام المعلوماتي الأول المقرر تفتيشه، فيمكن توسيع نطاق التفتيش بسرعة ليشمل النظام المعلوماتي الثاني.

وبهذا الخصوص، يمكن ضبط نظام معلوماتي أو جزء منه، أو دعامة إلكترونية، وحفظ نسخة عن البيانات المعلوماتية، واتخاذ التدابير لحفظ سلامة البيانات المعلوماتية، ومنع أي مستخدم من الوصول إلى بيانات النظام المعلوماتي.

---

198 قامت الإسكوا بوضع نموذج موضوعي للجرائم السيبرانية عام 2012 وهذا الجزء يتضمن الجزء الإجرائي للنموذج يرجى مراجعة الإرشاد الخامس من إرشادات الإسكوا للتشريعات السيبرانية والخاص بالجرائم السيبرانية: http://isper.escwa.un.org/Portals/0/Cyber%20Legislation/Regional%20Harmonisation%20Project/Directives/Dir-5-Cybercrimes.pdf.

المادة 5

للسلطات القضائية أن تلزم أي شخص له معرفة بطرق عمل نظام معلوماتي أو التدابير المطبقة لحماية البيانات المعلوماتية المخزنة بأن يقدم المعلومات المطلوبة من أجل تمكينها من الوصول إلى البيانات المعلوماتية المخزنة، وفق ما تتيحه المادة 4 من هذا القانون.

المادة 6

للسلطات القضائية، في إطار تحقيقات قضائية، أن تلزم مزود خدمات الشبكة، بجمع وتسجيل وتقديم مضمون المعلومات المنقولة بواسطة نظام معلوماتي خلال زمن الإرسال الحقيقي، أو أن يساعدها في ذلك.

يلتزم مزوّد خدمات الشبكة بالسرية المهنية فيما يخص التعليمات التي ينفذها في هذا السياق، وكذلك فيما يخص المعلومات.

المادة 7

تكون محاكم الدول مختصة:

- إذا وقعت الجريمة على أراضيها أو على مركب يرفع علمها أو على متن طائرة مسجلة وفق قوانينها؛
- إذا وقعت الجريمة من قبل أحد مواطنيها، وذلك إذا كان معاقباً عليها جزائياً في البلد الذي ارتكبت فيه، أو إذا كانت الجريمة لا تقع ضمن الاختصاص الإقليمي لأية دولة؛
- إذا وجد فاعل الجريمة على أراضيها ولا يمكن استرداده لمحاكمته في دولة أخرى بسبب جنسيته.

ويُطبَّق على الجرائم السيبرانية الأحكام المتعلقة بالصلاحيات الإقليمية والذاتية والشخصية والشاملة المنصوص عليها في قانون العقوبات.

ويُعدّ النطاق العُلوي للدولة على الإنترنت في حكم أرض الدولة في معرض تطبيق هذا القانون.

التعاون الدولي

المادة 8

تتعاون الدولة مع الدول الأخرى، بناءً على اتفاقيات موقعة معها أو استناداً إلى مبدأ المعاملة بالمثل، في سياق التحقيقات القضائية المتعلقة بالجرائم السيبرانية أو لضبط أدلة معلوماتية متعلقة بجريمة.

المادة 9

تعتبر الجرائم السيبرانية من الجرائم التي يتم فيها استرداد المجرمين استناداً إلى نصوص القانون الوطني أو المعاهدات الدولية المبرمة مع الدول الأخرى. ويخضع الاسترداد لهذه النصوص.

المادة 10

تقبل السلطات القضائية، في حالة الاستعجال، وبناءً على اتفاق ثنائي أو متعدد الأطراف، طلبات المساعدة المتعلقة بالتحقيقات القضائية والمُرسلة بوسائل الاتصال السريعة، مثل الفاكس والبريد الإلكتروني، من سلطات قضائية في دولة أخرى، شريطة ضمان صحة المراسلة ومصدرها وموثوقيتها؛ ويتم تأكيد المراسلة بالشكل الرسمي لاحقاً.

تطبق على طلبات المساعدة القضائية المرسلة من دول أخرى أحكام القانون الوطني.

المادة 11

يمكن للسلطات القضائية، بناءً على اتفاق ثنائي أو متعدد الأطراف، أن ترسل إلى سلطات قضائية في دولة أخرى معلومات ناتجة عن تحقيقات قضائية قد تساعدها في مباشرة تحقيقات قضائية خاصة بها.

يمكن اشتراط أن تبقى هذه المعلومات سرية أو ألاّ تستعمل إلا وفق شروط معينة.

المادة 12

يُرفض طلب المساعدة القضائية المُرسل من دولة أخرى إذا اعتبر متعلقاً بجريمة من طبيعة سياسية أو إذا كانت تلبية الطلب تتعرض لسيادة الدولة أو لأمنها أو لنظامها العام أو لمصالحها الأساسية.

يمكن أن تشترط السلطات القضائية على سلطات الدولة الأخرى أن تبقى المعلومات أو المضبوطات المُرسلة، بناء على طلب مساعدة قضائية، سرية أو ألاّ تُستعمل في تحقيقات قضائية مختلفة عن تلك موضوع طلب المساعدة.

كما يمكن للسلطات القضائية أن توقف كلياً أو جزئياً تنفيذ طلب المساعدة القضائية إذا كان من شأنه المساس بتحقيقات قضائية جارية. ويتم إعلام السلطات القضائية في الدولة الأخرى بموجب قرار معلل.

يمكن إبقاء موضوع طلب المساعدة سرياً بناء على طلب السلطات القضائية في الدولة الأخرى.

المادة 13

يمكن للسلطات القضائية أن تأمر بحفظ البيانات المخزنة في نظام معلوماتي، والتي قد تستعمل كدليل في تحقيقات قضائية. ويمكن أن يتم ذلك بموجب طلب مقدم من سلطات قضائية في دولة أخرى، بناء على اتفاق ثنائي أو متعدد الأطراف، على أن تتقدم بطلب لاحق لضبط هذه البيانات ولتسلمها.

يجب أن يتضمن طلب حفظ البيانات المعلومات الآتية: السلطات القضائية الطالبة، والجريمة والوقائع الجرمية موضوع التحقيقات، وماهية البيانات المطلوب حفظها وعلاقتها بالجريمة، وحائز البيانات المطلوبة أو موضع النظام المعلوماتي، وتبرير الطلب.

يمكن للسلطات القضائية رفض طلب حفظ بيانات في الأحوال المبينة في الفقرة الأولى من المادة 12 من هذا القانون.

المادة 14

إذا تعلق طلب المساعدة القضائية بمعلومات حركة البيانات، وتبين أن نقل البيانات يشارك فيه جزئياً مزوّد خدمة شبكة في دولة ثالثة، تقدم السلطات القضائية للسلطات الأخرى مقدّمة الطلب، معلومات كافية لتحديد مزوّد خدمة الشبكة الأجنبي ومسار حصول نقل البيانات.

يمكن للسلطات القضائية رفض طلب تسليم معلومات حركة البيانات في الأحوال المبينة في الفقرة الأولى من المادة 12 من هذا القانون.

المادة 15

يمكن للسلطات القضائية أن تأمر بضبط بيانات محفوظة في نظام معلوماتي من أجل تسليمها إلى سلطات قضائية في دولة أخرى بموجب طلب مساعدة، بناءً على اتفاق ثنائي أو متعدد الأطراف.

يجب تلبية الطلب بأقصى سرعة إذا كانت البيانات عرضة لمخاطر الضياع أو التعديل.

المادة 16

يمكن للسلطات القضائية أن تأمر:

- بالوصول إلى بيانات معلوماتية مخزّنة موضوعة في تصرف الجمهور أياً كان الموقع الجغرافي لهذه البيانات؛
- بالوصول إلى بيانات معلوماتية مخزّنة في دولة أخرى، وذلك بواسطة نظام معلوماتي واقع في الإقليم الوطني، وفي حال موافقة الشخص المخول قانوناً بإفشاء هذه البيانات.

المادة 17

يمكن للسلطات القضائية أن تقبل طلب مساعدة قضائية مقدم من سلطة قضائية لدولة أخرى، بناءً على اتفاق ثنائي أو متعدد الأطراف، وذلك فيما يتعلق بجمع معلومات حركة البيانات أو ضبط مضمون البيانات وتسجيلها في زمن الإرسال الحقيقي.

المادة 18

تحدد السلطات القضائية نقطة اتصال جاهزة 24 ساعة في اليوم و7 أيام في الأسبوع، وذلك للتعاون القضائي مع السلطات في الدول الأخرى في مجال تحقيقات الجرائم السيبرانية وضبط الأدلة الإلكترونية.

الإطار 8- إرشاد الإسكوا حول الاتصالات الإلكترونية وحرية التعبير
(الأبواب المُحال إليها بموجب هذا القانون)

الباب الثاني: النظام القانوني لمزودي خدمات الشبكات الإلكترونية

المادة 3: تقييد الوصول إلى بعض المواقع والخدمات الإلكترونية

يجب على مزود خدمة الاتصال أن يُعلم المستخدمين بوجود وسائل تقنية تسمح بتقييد الوصول إلى بعض المواقع الإلكترونية أو الخدمات الإلكترونية أو بالاختيار منها، وعلى مزود خدمة الاتصال تقديم هذه الوسائل التقنية للمستخدمين.

المادة 4: رقابة مزود خدمة الاتصال ومستضيف البيانات على المعلومات

لا يخضع مزود خدمة الاتصال ومستضيف البيانات لموجب رقابة على مضمون المعلومات التي يرسلها أو يخزنها، ولا لموجب عام بالبحث عن الأعمال المتعلقة بنشاطات غير مشروعة. يُستثنى من ذلك حالة صدور قرار قضائي يُلزم مزود خدمة الاتصال أو مستضيف البيانات بإجراء مراقبة مؤقتة ومحدودة لمعلومات محدّدة.

ولا يكون مستضيف البيانات مسؤولاً عن المعلومات المخزّنة:

- اذا لم يكن يعلم بطابعها غير المشروع الظاهر؛
- أو إذا أقدم على سحب هذه المعلومات أو جعل الوصول إليها مستحيلا منذ اللحظة التي يعلم فيها بطابعها غير المشروع الظاهر.

يكون مزود خدمة الاتصال مسؤولاً إذا لم يمحُ المعلومات المخزّنة مؤقتاً بناءً على طلب مُرسل هذه المعلومات، وكذلك بناءً لقرار قضائي.

المادة 5: إجراءات الإبلاغ بعدم مشروعية المعلومات

يُعتبر مستضيف البيانات أنّه قد عَلِمَ بالطابع غير المشروع للمعلومات التي يخزّنها عندما يتم إبلاغه المعلومات التالية:

- تاريخ التبليغ؛
- إذا كان المُبلّغ شخصاً طبيعياً: اسمه ومهنته ومقره وجنسيته وتاريخ ومكان الولادة؛
- إذا كان المُبلّغ شخصاً معنوياً: شكله القانوني، مركزه القانوني، واسم المفوض بتمثيله؛
- اسم المُرسل إليه ومقره؛
- وصف الأعمال المُنازع بها ومكان تمركزها؛
- الأسباب التي تدعو لسحب المعلومات مع ذكر القواعد القانونية والتعليل.

المادة 6: عدم إفشاء هوية الناشر وحفظ بيانات التعريف الشخصية له

يحق لكل شخص ينشر معلومات، بصفة غير مهنية أو غير محترفة، للجمهور عبر الاستفادة من خدمات مستضيف بيانات، أن يبقي هويته سرية وأن يقدم إلى الجمهور عناصر التعريف العائدة فقط لمستضيف البيانات، شرط تقديم عناصر التعريف الشخصية عنه لمستضيف البيانات.

أما الناشر المحترف، فيجب عليه دوماً تقديم عناصر التعريف الشخصية به للجمهور.

يجب على مستضيف البيانات أن يحتفظ بالبيانات التي تعرّف بهوية كل ناشر لمدة لا تقل عن عشر سنوات.
كما يخضع مستضيف البيانات لموجب السر المهني بخصوص عناصر التعريف الشخصية باستثناء حالة وجود قرار قضائي.

المادة 7: حفظ معلومات حول حركة البيانات

يجب على كل من مزود خدمة الاتصال ومستضيف البيانات حفظ المعلومات المتعلقة بحركة البيانات والعائدة لجميع المستخدمين الذي يستفيدون من خدماته، وذلك لمدة لا تقل عن خمس سنوات. لا يخضع لموجب الحفظ مضمون المعلومات ذاتها المُرسلة أو المخزّنة أو المراسلات المُتبادلة.

الإطار 8 (تابع)

يخضع مزود خدمة الاتصال ومستضيف البيانات لموجب السر المهني بخصوص معلومات حركة البيانات باستثناء حالة وجود قرار قضائي.

يلتزم مزود خدمة الاتصال ومستضيف البيانات بصون المعلومات حول حركة البيانات من التدمير أو المحو أو التعديل أو الإفشاء، كما يلتزم بمحوها بعد انقضاء مدة الحفظ القانونية المحدّدة بخمس سنوات.

المادة 8: تقديم معلومات حركة البيانات للسلطات القضائية والأمنية

يجب على كل من مزود خدمة الاتصال ومستضيف البيانات تقديم المعلومات المتعلقة بحركة البيانات وبهوية الأشخاص الذين يستفيدون من خدماتهم، وذلك إلى السلطات القضائية والأمنية المختصة العاملة تحت إشرافها. وكذلك يجب عليهم تمكين هذه السلطات من الوصول إلى المعلومات المنوه عنها وفقاً لوقت الإرسال الحقيقي لها عند حصول أي عملية اتصال.

المادة 9: مساهمة مزود خدمة الاتصال ومستضيف البيانات في مكافحة بعض الجرائم

يجب أن يساهم كل من مزود خدمة الاتصال ومستضيف البيانات بمحاربة الجرائم ولا سيما الجرائم ضد الإنسانية أو الجرائم الإباحية للقاصرين أو بالتحريض على العنف أو التعرض لكرامة الإنسان. وعلى مزود خدمة الاتصال أو مستضيف البيانات بالتالي أن يضع بتصرف الجمهور آلية واضحة وسهلة للإبلاغ عن الأفعال المذكورة في هذه المادة، وعليه بعد حصول التبليغ إعلام السلطات العامة بذلك.

المادة 10: المسؤولية التعاقدية لمزود خدمة الاتصال ومستضيف البيانات

يكون كل من مزود خدمة الاتصال ومستضيف البيانات مسؤولاً عن حسن تنفيذ موجباته المنصوص عنها في العقود الموقعة مع عملائه. ويجب أن تتضمن هذه العقود تحديد نوعية الخدمة المقدمة ومواصفاتها ومدتها.

تنتفي مسؤولية مزود خدمة الاتصال ومستضيف البيانات إذا أثبت أن عدم تنفيذ العقد تجاه عميله أو سوء تنفيذه هو ناتج عن خطأ العميل أو عن القوة القاهرة أو عن فعل الغير.

المادة 11: حق الرد للشخص المعني المذكور في عملية نقل المعلومات للجمهور

يتمتع كل شخص تم ذكر اسمه في عملية نقل للمعلومات إلى الجمهور على الخط بحق الرد، مع عدم الإخلال بطلبات التصحيح أو الإلغاء التي يستطيع توجيهها لمزود الخدمة. توجه طلبات ممارسة حق الرد خلال ثلاثة أشهر من تاريخ النشر إلى مدير النشرة، وفي حال عدم إفشائه لاسمه للجمهور، توجه الطلبات المنوه عنها إلى مستضيف البيانات الذي يخزّن المعلومات موضوع طلب الرد. وعلى مستضيف البيانات إرسال طلب الرد دون تأخير إلى مدير النشرة.

الباب الرابع: التنصّت على الاتصالات الخاصة والشخصية

المادة 14: عدم جواز التنصّت على الاتصالات الخاصة والشخصية

تضمن الدول الأعضاء الحق في سرية الاتصالات الإلكترونية الخاصة والشخصية، بحيث لا تخضع هذه الاتصالات لأي نوع من أنواع التنصّت أو المراقبة أو الاعتراض أو الإفشاء إلا في الأحوال التي يجيزها القانون.

المادة 15: جواز التنصّت بإذن قضائي أو لضرورات الأمن الوطني

يمكن لكل دولة عضو أن تجيز التنصّت أو مراقبة أو اعتراض أو إفشاء اتصالات خاصة أو شخصية في الحالتين التاليتين:

- بإذن قضائي، من أجل ضرورات التحقيقات القضائية الجزائية؛
- بإذن من السلطات الأمنية أو الدستورية المختصة تحت إشراف القضاء، من أجل تجميع المعلومات لمكافحة الإرهاب والجرائم الواقعة على أمن الدولة والجرائم المنظّمة.

الإطار 8 (تابع)

الباب الخامس: أحكام جزائية

المادة 16: أحكام جزائية

ضماناً للفعالية في تطبيق أحكام هذا الإرشاد، تحرص الدول الأعضاء على تجريم الأفعال التالية:

- عدم تعاون مزود خدمات الشبكات الإلكترونية مع القضاء بتقديم معلومات حركة البيانات أو بسحب بيانات أو بمنع الوصول إليها متى طلب منه ذلك؛
- قيام مزود خدمة الاتصال أو مستضيف البيانات بعدم حفظ معلومات حركة البيانات وبيانات التعريف الشخصية وفق ما يفرضه القانون؛
- قيام شخص بتقديم معلومات غير صحيحة عن قصد لمزود خدمات الشبكات الإلكترونية لحمله على سحب معلومات أو منع الوصول إليها؛
- عدم قيام مدير النشرة بنشر رد الشخص المعني وفقاً للمادة 11 من هذا الإرشاد؛
- تقديم أو تصدير أو استيراد وسائل تشفير بصورة غير مشروعة دون الحصول على الترخيص المطلوب من السلطات الرسمية؛
- التنصّت على الاتصالات الإلكترونية الخاصة والشخصية بصورة غير مشروعة خارج الحالات التي يجيزها القانون.

المرفق الرابع

ملخص أجوبة الاستبيان المرسل إلى الدول العربية بموجب هذه الدراسة

الجدول 4- ملخص الأجوبة حول الجانب التشريعي في الدول

	تشريع خاص بالأمان السيبراني	تشريع خاص بالجرائم السيبرانية	تطبيق القوانين التقليدية على الجرائم السيبرانية	تحديث مستمر للتشريع السيبراني	قانون إجراءات خاص بالجرائم السيبرانية	تعاون دولي	أجهزة تحقيق متخصصة	محاكم متخصصة	قواعد سلوكية	حفظ مزودي خدمات الاتصال معلومات حركة البيانات	حفظ مزودي خدمات الاتصال بيانات المحتوى	حفظ مزودي خدمات الاتصال بيانات المشتركين	تعاون مزودي خدمات الاتصال	برامج توعية	برامج تدريب متخصصة	مركز لطوارئ الحاسوب	تعاون القطاع الخاص مع القطاع العام
مصر	كلا فقط بعض النصوص المتفرقة	كلا	نعم	كلا	كلا	نعم	نعم	كلا	نعم	نعم	نعم	نعم	نعم	نعم	نعم جزئياً	نعم	نعم
الأردن	كلا استراتيجية وطنية فقط	نعم	نعم	كلا	-	-	نعم	-	-	-	-	-	-	نعم جزئياً	كلا	نعم قيد التجهيز	نعم
الكويت	كلا	كلا	نعم	كلا	كلا	نعم	نعم	كلا	كلا	كلا	كلا	كلا	نعم	نعم	نعم	نعم قيد التنفيذ	نعم
تونس	نعم	نعم	نعم أحياناً (اجتهاد محاكم منضارب)	نعم	-	-	-	-	نعم	-	-	-	-	نعم جزئياً	نعم	نعم	-
لبنان	كلا	كلا	نعم	كلا	كلا	نعم	نعم	كلا	كلا	نعم	نعم	نعم	نعم	نعم جزئياً	نعم جزئياً	كلا	نعم جزئياً
سوريا	كلا – فقط سياساتٌ	نعم	نعم بعد مضاعفة العقوبة	كلا (حتى الآن)	نعم جزئياً	كلا	نعم - قيد التنفيذ	كلا	نعم	نعم	نعم	نعم	نعم	كلا	نعم	نعم – قيد التطوير	نعم
فلسطين	كلا فقط تعليمات وزارة الاتصالات	كلا	نعم	كلا	كلا	نعم	كلا	كلا	كلا	كلا	كلا	كلا	نعم	نعم	كلا	قيد الإنشاء	نعم
عمان	نعم جزئياً	نعم	كلا	نعم	كلا	نعم	نعم	كلا	نعم	نعم	نعم	نعم	نعم	نعم	نعم	نعم	نعم
اليمن	كلا	كلا	نعم	كلا	كلا	كلا	كلا	كلا	كلا	كلا	كلا	نعم	كلا	نعم	نعم جزئياً	كلا	كلا
الإمارات	نعم	نعم	نعم	نعم	كلا	نعم	نعم	كلا	نعم	نعم	نعم	نعم	نعم	نعم	نعم	نعم	نعم

الجدول 5- ملخص حول أنواع التعديات السيبرانية

	جرائم الاحتيال المعلوماتي	جرائم سرقة الهوية الإلكترونية	التعدي على البيانات والأنظمة المعلوماتية	جرائم البطاقات المصرفية	التعدي على الملكية الفكرية	المواد الإباحية للأطفال وجرائم الاستغلال الجنسي	جرائم معلوماتية أخرى هامة	ازدياد الجرائم السيبرانية
مصر	مرتفعة	مرتفعة	مرتفعة	متوسطة	متوسطة	متوسطة	متوسطة	نعم
الأردن	متوسطة	منخفضة	مرتفعة	مرتفعة	متوسطة	مرتفعة	متوسطة	نعم
الكويت	متوسطة	متوسطة	قليلة	متوسطة	قليلة	نادرة	مرتفعة (السباب) متوسطة (التهديد والابتزاز)	نعم
تونس	-	-	-	-	-	-	-	نعم
لبنان	مرتفعة	متوسطة	قليلة	متوسطة	مرتفعة	قليلة	مرتفعة (القدح والذم)	نعم
سوريا	قليلة	قليلة	مرتفعة	قليلة	-	قليلة	قليلة	نعم
فلسطين	قليلة	قليلة	مرتفعة	قليلة	قليلة	قليلة	-	كلا
عمان	مرتفعة	متوسطة	متوسطة	مرتفعة	قليلة	متوسطة	متوسطة	نعم
اليمن	نادرة	قليلة	قليلة	نادرة	نادرة	نادرة	نادرة	نعم
الإمارات	متوسطة	قليلة	مرتفعة	متوسطة	قليلة	نادرة	-	نعم

المراجع

ألف- المرجع العربية

الإسكوا، الملامح الوطنية لمجتمع المعلومات في الإمارات العربية المتحدة، 2013.

الإسكوا، الملامح الوطنية لمجتمع المعلومات لجمهورية مصر العربية، 2013.

الإسكوا، الملامح الوطنية لمجتمع المعلومات في الجمهورية اللبنانية، 2013.

الإسكوا، إرشادات الإسكوا للتشريعات السيبرانية، 2012.

بهنسي سمير بهنسي، جرائم الحاسب الآلي والإنترنت، بحث مقدم الى قسم الدراسات العليا، دبلومة القانون العام – جامعة الاسكندرية – كلية الحقوق.

عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، الرياض، 12-14 تشرين الثاني/نوفمبر 2007.

طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي، www.startimes.com/f.aspx?t=30245909.

القاضي حسن محمد علي حسن، المشرف على قسم الحاسوب، تجربة المركز السوداني لأمن المعلومات، المؤتمر الثالث لأمن وسلامة الفضاء السيبراني، بيروت، 25-27 آب/أغسطس 2014.

محمد عبد الله منشاوي، جرائم الانترنت من منظور شرعي وقانوني، 1-11-1423هـ، http://www.khayma.com/education-technology/Study33.htm.

دولة الإمارات العربية المتحدة "ورقة عمل" حول استخدام موقع التواصل الاجتماعي "فيسبوك"، http://arabic.cnn.com/middleeast/2014/05/21/facebook-uae-law.

قانون مكافحة جرائم الإنترنت. متى يخرج إلى النور؟ http://www.aim-council.org/arabSecurityInfoOffice/emagazine/issue21/ecrime/Pages/Anti-cyber-crime-law.aspx.

مقدمة لمراحل التحقيق الجنائي الرقمي ومراحله، http://www.ofpcss.com/2014/04/Introduction-of-the-stages-of-the-criminal-investigation-and-the-steps.html.

مؤتمر تقنية المعلومات، دولة الإمارات العربية المتحدة، أبو ظبي، 5 نيسان/أبريل 2014، http://me-newswire.net/ar/news.

جريدة دار الخليج، دبي، الثلاثاء 14 كانون الثاني/يناير 2010، المشاركون في اجتماع الإنتربول يشيدون بإنشاء محاكم للجريمة الإلكترونية، http://www.mohamoon-uae.com/default.aspx?Action=DisplayNews&type=3&ID=12864.

جريدة البيان، أبو ظبي، عدد 14 آب/أغسطس 2013، تهدف لتحديد معايير الاستخدام الأمثل للأصول المعلوماتية لائحة أمن المعلومات الاتحادية، http://www.mohamoon-uae.com/default.aspx?action=DisplayNews&type=1&id=20981&Catid=2659.

لواء النعساني، http://www.24.ae/article.aspx?ArticleId=77807.

جريدة الخليج، أبو ظبي، عدد 29 أيار/مايو 2013، "تنفيذي أبو ظبي" يصدر تعميماً حول معايير "أمن المعلومات"، http://www.mohamoon-uae.com/default.aspx?action=DisplayNews&type=1&id=20426&Catid=2659.

جريدة دار الخليج، الأحد 9 كانون الثاني/يناير 2011، جيهان شعيب، خلال ندوة تقصي جرائم تقنية المعلومات د. محمد الكمالي: 80 في المائة من الجرائم أصبحت إلكترونية، http://www.mohamoon-uae.com/default.aspx?Action=DisplayNews&type=3&ID=13154.

جريدة الإمارات اليوم، الإثنين 16 حزيران/يونيو 2008، أحمد عابد، شرطة أبو ظبي حذّرت من شرائها أو استخدامها قضايا البرمجيات المقلّدة ترتفع 107 في المائة، http://www.mohamoon-uae.com/default.aspx?Action=DisplayNews&type=3&ID=4527.

جريدة دار الخليج، محمد رباح، طارق زياد، الثلاثاء 17 تشرين الثاني/نوفمبر 2009، دعا إلى ضمان أمن وسلامة أعضاء النيابة العامة مؤتمر النيابات العامة في القرن 21 يوصي بالتعاون لمكافحة الجريمة الإلكترونية، http://www.mohamoon-uae.com/default.aspx?Action=DisplayNews&type=3&ID=9216.

جريدة دار الخليج - الأحد 26 أيار/مايو 2013، محاضرات توعوية حول الجرائم الإلكترونية، http://www.mohamoon-uae.com/default.aspx?action=DisplayNews&type=1&id=20394&Catid=2659.

جريدة البيان، الثلاثاء 17 نيسان/أبريل 2012، «نيابة دبي» تناقش التحقيق والتصرف في جرائم المعلومات، http://www.mohamoon-uae.com/default.aspx?action=DisplayNews&type=1&id=17175&Catid=2659.

جريدة دار الخليج، دبي، السبت 18 أيار/مايو 2013، المنصوري: برنامج التواصل مع الضحية تفاعل مع 83037 شخصاً من ذوي العلاقة العام الماضي، http://www.mohamoon-uae.com/default.aspx?action=DisplayNews&type=1&id=20318&Catid=2659.

جريدة الاتحاد، الثلاثاء 29 حزيران/يونيو 2010، حملة لتعزيز الوعي الأمني للقضاة في قضايا الجرائم الإلكترونية، http://www.mohamoon-uae.com/default.aspx?Action=DisplayNews&type=3&ID=11531.

ألف- المراجع الأجنبية

Australian Government, Attorney General's Department, *National Plan to Combat Cybercrime*, http://www.ag.gov.au/CrimeAndCorruption/Cybercrime/Documents/National%20Plan%20to%20Combat%20Cybercrime.pdf.

Michael Barrett, Andy Steingruebl, Bill Smith, *Combating Cybercrime: Principles, Policies and Programs*, April 2011, https://www.paypal-media.com/assets/pdf/fact_sheet/PayPal_CombatingCybercrime_WP_0411_v4.pdf.

Alain BENSOUSSAN, *Informatique télécoms Internet*, Francis Lefebvre, 2001.

Cabinet Office, *The UK Cyber Security Strategy, Protecting and promoting the UK in a digital world*, November 2011, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.

Cabinet Office, Office of Cyber Security and Information Assurance, *Keeping the UK safe in cyber space*, https://www.gov.uk/government/policies/keeping-the-uk-safe-in-cyberspace.

Steven R. Chabinsky, Deputy Assistant Director, Cyber Division, Federal Bureau of Investigation, GovSec/FOSE.

Conference, Washington, DC, http://www.fbi.gov/news/speeches/the-cyber-threat-whos-doing-what-to-whom.

ENISA, Roadmap to provide more proactive and efficient Computer Emergency Response Team training, http://www.enisa.europa.eu/activities/cert/support/exercise/roadmap-to-provide-more-proactive-and-efficient-cert-training.

Esteve/Machin, *Devices to access Internet in developing countries*, available at: www2007.org/workshops/paper_106.pdf.

Europol, *EU Organized Threat Assessment: OCTA 2011,* April 28, 2011, http://www.europol.europa.eu/publications/European_Organised_Crime_Threat_Assessment_%28OCTA%29/OCTA_2011.pdf.

Federal Bureau of Investigation FBI, *Internet fraud,* http://www.fbi.gov/scams-safety/peertopeer.

Federal Bureau of Investigation FBI, *New E-scams and warnings*, http://www.fbi.gov/scams-safety/e-scams.

Federal Bureau of Investigation FBI, *How to protect your computer,* http://www.fbi.gov/scams-safety/computer_protect.

Federal Bureau of Investigation FBI, *Internet fraud,* http://www.fbi.gov/scams-safety/fraud/internet_fraud.

Basic principles for State Policy of the Russian Federation in the field of International Information Security to 2020, Press release, 16 September 2013, http://www.veleposlanistvorusije.mid.ru/doc/pr_20130916_en.pdf.

Kristin M. Finklea, Catherine A. Theohary, *Cybercrime: Conceptual issues for Congress and U.S. law enforcement*, January 2013, http://fas.org/sgp/crs/misc/R42547.pdf.

Dr. Hamadoun I. Touré Secretary-General, ITU, *CybersecurityGlobal status update*, December 2011, http://www.un.org/en/ecosoc/cybersecurity/itu_sg_20111209_nonotes.pdf.

IBM survey, published 14.05.2006, available at: www-03.ibm.com/industries/consumerproducts/doc/content/news/pressrelease/1540939123.html.

ITU, Marco Gercke, *Understanding Cybercrime: Phenomena, Challenges and Legal Response,* September 2012.

ITU, *2013 ITU survey on measures to raise awareness on cybersecurity*, August 2013, http://www.itu.int/en/ITU-D/Cybersecurity/Documents/22survey.pdf.

Marco Gercke, *Understanding cybercrime: phenomena, challenges and legal response, ITU, Sep 2012*, www.itu.int/ITU-D/cyb/cybersecurity/legislation.html.

Internet World Stats, *Internet Usage Statistics, The Internet Big Picture, World Internet Users and Population Stats*, http://www.internetworldstats.com/stats.htm.

Ministry of information and communications technology, Qatar, Rassed, *The attitudes of online users in the MENA region cybersafety, security and data privacy*, May 2014, http://www.ictqatar.qa/sites/default/files/Cybersafety,%20security%20and%20data%20privacy.pdf.

National French Police, *Prospective analysis on trends on cybercrime from 2011 to 2020*, http://www.mcafee.com/sg/resources/white-papers/wp-trends-in-cybercrime-2011-2020.pdf.

National Security Agency, USA, *Statement for the Record, Lieutenant General Keith Alexander, Commander, Joint Functional Component Command for Network Warfare*, Before the House Armed Services Committee, Terrorism, Unconventional Threats, and Capabilities Subcommittee, May 5, 2009, http://www.nsa.gov/public_info/speeches_testimonies/5may09_dir.shtml.

Todd Neal, Security Analyst, *Combat Cybercrime with Compliance and Ethics*, http://www.tnwinc.com/2910/information-security-training-2.

Fausto Pocar, *New Challenges for international rules against cyber-crime*. http://link.springer.com/article/10.1023/B:CRIM.0000037565.32355.10#page-1.

Secretariat of the Security and Defense Committee, *Finland´s Cyber security Strategy* http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf.

Stein Schjolberg, *The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva*, December 2008, http://www.cybercrimelaw.net/documents/cybercrime_history.pdf.

Symantec Corporation, *What is Cybercrime?*, http://us.norton.com/cybercrime/definition.jsp.

Symantec Intelligence Report, June 2012; Kaspersky Lab Report, June 2012.

Steven Titch, *Four principles for effective cybersecurity law and policy*, 25 April 2014, http://www.rstreet.org/2014/04/25/four-principles-for-effective-cybersecurity-law-and-policy.

Types of Threats - Computer Definition http://www.yourdictionary.com/types-of-threats.

The White House, *International Strategy for Cyberspace, Prosperity, security and Openness in a networked World*, May 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

Wikipedia, *Threat (computer),* http://en.wikipedia.org/wiki/Threat_(computer).

Wikipedea, *International Cybercrime*,http://en.wikipedia.org/wiki/International_cybercrime.

John Wilkinson, Tareq Haddad, PWC, *Economic Crime in the Arab World*, February 2014, http://www.pwc.com/m1/en/publications/gecs2014reportme.pdf.

Robert Winters, *Practical steps to combat computer crime*, August 2013, http://cjfocus.com/2013/08/06/practical-steps-to-combat-computer-crime.

United Nations Office on Drugs and Crime, UNODC, *Comprehensive study on cybercrime*, draft, February 2013.

University of Mississippi, School of Law, National Center for Justice and the Rule of law, *Combating cyber crime: essential tools and effective organizational structures, A guide for policy makers and managers*, http://www.olemiss.edu/depts/ncjrl/pdf/CyberCrimebooklet.pdf.

Michael A. Vatis, *The Council of Europe Convention on Cybercrime*, http://cs.brown.edu/courses/csci1950-p/sources/lec16/Vatis.pdf.

Michel VIVANT, Lucien RAPP, Michel GUIBAL, *Droit de l'informatique et des réseaux*, Lamy.

ساعد التطور التكنولوجي وانتشار الإنترنت والأجهزة النقالة وتوافر الحزمة العريضة للإنترنت عبر الأجهزة النقالة وتدني كلفتها، إلى ارتفاع أعداد مستخدمي الإنترنت وتزايد الاعتماد على هذه التكنولوجيات في التنمية الاقتصادية والاجتماعية. إلا أن الانفتاح الذي يميّز شبكة الإنترنت، والفضاء السيبراني عموماً، جعلها عرضة للتعديات والأنشطة الإجرامية، فصار مستخدمو الفضاء السيبراني عرضة للانتهاكات من قبل مخترقي الشبكات. ولذلك من الضروري وضع الأطر القانونية والتنظيمية والإجرائية لمواجهة المخاطر السيبرانية وتوعية المؤسسات والأفراد حول هذه المخاطر وآثارها على أعمالهم وحياتهم الشخصية.

تأتي هذه الدراسة استكمالاً لأنشطة الإسكوا التي بدأت في عام 2007 بهدف تطوير وتنسيق التشريعات السيبرانية في المنطقة العربية وتطبيقها على أرض الواقع. وهي تركّز على موضوع الأمان السيبراني ومكافحة الجريمة السيبرانية من أجل بناء مجتمع المعرفة وتطويره في المنطقة العربية. وتهدف الدراسة إلى تحليل الوضع الراهن إقليمياً ودولياً واستعراض وسائل تعزيز وتنسيق الجهود لمكافحة جرائم الفضاء السيبراني وضمان سلامته. وتتضمّن اقتراحاً لإطار توجيهي سياساتي من أجل تعزيز الأمان السيبراني وبناء الثقة بتكنولوجيا المعلومات والاتصالات والفضاء السيبراني. وتحث الإسكوا الحكومات في المنطقة العربية على استخدام الإطار التوجيهي المدرج في الدراسة وتكييفه حسب السياق والحاجات الوطنية لبناء بيئة متكاملة للأمان السيبراني ومواجهة الجرائم السيبرانية. ويمكن للخبراء في الحكومات الاستفادة من أجزاء من هذا الإطار لسدّ مواضع النقص وتحديث الوضع التشريعي والمؤسساتي في المنظومة الوطنية للأمان والأمن السيبراني.

15-00097