الفصل الثامن

قضايا

ثَمَّة عدد من القضايا الحسَّاسة في أمن المعلومات، وسيَستعرِض هذا الفصل بعض هذه القضايا، ويَدرُس أبعادها، ويُقدِّم إجراءات تُسهِم في علاجها، فبعض هذه القضايا تتعلق **ببعدٍ آخر للأمان المتعلق بالمعلومات والاتصالات** غير **أمان المعلومات** الذي تعرضنا له في صلب الكتاب، ألا وهو أمان الأشخاص أنفسهم نتيجة تداولهم للمعلومات على شبكاتها، مثل أمان القُصّر، وأمان الأشخاص نتيجة وجود معلومات على شبكات الاتصال حول تحركاتهم.

1.8 أمان معلومات القُصَّر

مع تَطوُّر وسائل الاتِّصال الحديثة عَبْر الإنترنت، ومع ازدياد تَعلُّق القُصَّر بها، واستخدامِهم لها بوصفها وسائل ترفيه أكثر مِمَّا هي وسائل اتِّصال، ازدادَت عمليات اصطياد هؤلاء القُصَّر بكثافة، والقاصِر بحَسْب تعريفه في الشبكة الدوليَّة لحقوق الطفل CRIN هو من لم يَتجاوَز سن 18[1]، سواء أكان ذكرًا أم أنثى. إنَّ أخطار استعمال القُصَّر

(1) تَدعو CRIN أيضًا القاصر من لم يَتجاوَز سن 18 سنة.

لوسائل الاتِّصال عَبْر الإنترنت كثيرة جدًّا. يُدعَى تطبيق الحلول المثاليَّة لمواجهة أخطار استعمال القُصَّر لوسائل الاتِّصال عَبْر الإنترنت **أمن معلومات القُصَّر**، وسيَتم فيما يأتي تعداد هذه الأخطار، ومن ثم سيَتم الحديث عن أسبابها، وبعدها ستُقدَّم الحلول لمواجَهتها.

تَتضمَّن أخطار استعمال القُصَّر لوسائل الاتِّصال عبر الإنترنت جميع العواقِب السيّئة التي يُمكِن أن تَأتي من ذلك، وتُسمَّى (أخطارًا) لأنَّ القُصَّر لديهم اندفاعات ومجازَفات غير شعوريَّة نحو الخطر، وهي:

1. سَرِقة مجرمين لمعلومات شخصيَّة من القاصِر تَتعلَّق باسمه الكامِل وجنسه وعمره وعنوانه التفصيلي ومعلومات أخرى عن عائلته، مثل أسمائهم ومهنَتَي والديه وأوقات غيابهم جميعًا عن المنزل، وما إلى ذلك من المعلومات المشابِهة، وتُسرَق هذه المعلومات إمّا من خلال غرف الدردشة الكثيرة أو من خلال وجودها أساسًا على صفحة خاصَّة بالقاصِر في أحد مواقع الشبكات الاجتماعيَّة، ويستفيد المجرمون من هذه المعلومات بطُرُق عدة، فقد يَقوم المجرم الذي سَرَق معلومات حقيقيَّة تفصيليَّة من القاصِر دون شعوره، إمّا بخَطْفِ القاصِر وطَلب فدية من أهله، أو سرقة منزله عند معرفة عدم وجود أحد في المنزل، أو بيع هذه المعلومات إلى جهات إجراميَّة أخرى.
2. استدراج القاصِر للانضمام إلى تَنظيم ما، سواء أكان هذا التنظيم عبارة عن شبكة دعارة للقُصَّر أم تَنظيم إرهابي، خاصَّةً إذا كان القاصِر يَتجاوَز سن 15 سنة، ويجري استدراج القاصِر للانضمام إلى أيّ تنظيم عن طريق، إمّا غرف الدردشة أو صفحات الشبكات الاجتماعيَّة، ويَنتُج عن الانضمام إلى شبكة دعارة إقناع القاصِر (سواء أكان ذكرًا أم أنثى) بتصوير نفسه عاريًا وإرسال الصور إلى هذه الشبكة سرًّا، ويَتضمَّن انضمام القاصِر إلى شبكة تَبادُل صور فاحِشة معه، وذلك يُسبِّب أضرارًا نفسيَّة له، وقد يَتجاوَز هذا الأمر

مجـرَّد انضمام افتراضي لشـبكة دعارة على الإنترنـت وتَبادُل الصور إلى تَردُّد القاصِـر فعليًّا على شـبكة الدعـارة وانضمامه إليها عمليًّـا. أمّا حالات انضمام القاصِر إلى التنظيمات الإرهابيَّة عبر الإنترنت فهي كثيرة جدًّا، فها هي جميع وسـائل الإعـلام تتحـدث فـي أنحاء العالـم عن انضمـام الكثيرين مـن القُصَّر مِمَّـن غُرِّر بهم بدوافع دينيَّة إلى تنظيمات إرهابيَّة، ويَنتُج عن انضمام القاصِر افتراضيًّـا لهذه التنظيمات الإرهابيَّة في معظم الأحيان اسـتدراجه للانضمام فعليًّـا إليهـا وتَجنيده في عمليات انتحاريَّة وحروب إرهابيَّة ضد دولٍ ما، وهناك أمثلة انضمام القُصَّر للتنظيمات الإرهابيَّة عبر الإنترنت.

3. تَثقيـف القُصَّـر بمعلومـات خاطِئـة، إمّـا عَمْدًا أو عـن غير قَصد، وقـد تَتضمَّن هـذه المعلومـات أمورًا سـيّئة تَتعلَّق بالصحة العامَّة، أو بالحيـاة الاجتماعيَّة، أو بمخالَفـة الأنظمـة والقوانين النافِذة في البلد الذي يَعيش فيـه القاصِر، ويَنتُج عـن التثقيـف بمعلومات خاطِئة ظهور سـلوكيَّات سـيّئة للقاصِـر مرتَبِطة بالأمر الـذي تَـمَّ تَلقّي معلومـات عنه، وأحيانًا قد يُسـيء القاصِر فَهْم هـذه المعلومات بسبب عدم تَوافُقها مع عمره.

أمّا أسباب انتشار أخطار استعمال القُصَّر لوسائل الاتِّصال عبر الإنترنت فهي:

1. فُضول القُصَّر وحُب استطلاعِهم لكل ما هو موجود على شبكة الإنترنت، إذ يَندفِع القُصَّر لرؤية كل شيء ومطالَعته في الإنترنت، ويَتضمَّن هذا الاندفاع مُحاوَلة التفاعُل والتواصُل مع الأشخاص دون النظَر إلى حقيقة أعمارهم وجنسهم وجنسياتهم، ودون معرفة أهدافهم الحقيقيَّة من هذا التَفاعُل، وإنَّ براءَة القاصِر في معظم الأحيان تَجعلُه يُقدِّم معلومات شخصيَّة تفصيليَّة عنه وعن عائلته دون إدراك الخطر الذي يُمكِن أن يَأتي من ذلك الأمر، فالقاصِر يُقدِّم معلوماته الشخصيَّة التفصيليَّة من باب تَكوين أصدقاء، والمجرِم يَستغلُّ هذا الاندفاع من القاصِر ورغبته في تَكوين أصدقاء، ويُقدِّم نفسه للقاصِر على أنه صديق من عمره نفسه وحتَّى جنسه، وله الهوايات نفسها ليَسرِق منه تِلْك المعلومات.
2. الكَبْتُ النفسي ومن ثم الجنسي للقاصِر خاصَّة إذا كان في سِن البلوغ. يَسعى بعض القُصَّر في سِن البلوغ للتخفيف عن كَبْتهم الجنسي إلى شبكة الإنترنت لمُطالَعة المواد الإباحيَّة، وتَنتظِر معظم مواقع الإنترنت الفاحِشة هؤلاء القُصَّر؛ ليُقدِّموا لهم المواد الإباحيَّة ولاستغلالهم.
3. التأثير الإعلامي في القُصَّر، إذ يَتفاعَل القاصِر مع وسائل الإعلام بشكلٍ كبير. فعندما يَتلقَّى القاصِر إعلامًا يُؤثِّر في اندفاعه الديني، يَلجأ إلى الإنترنت، وتستغله الصفحات المتطرِّفة في الشبكات الاجتماعيَّة لحَقْنه بأفكار تُؤدِّي به في النهاية إلى الانضمام إلى أصحابها.
4. عَدَم مُتابَعة الأهل لأبنائهم. كثيرًا ما تَقَع الحوادث التي يَذهَب القُصَّر ضَحيتها من وراء إهمال الأهل لأبنائهم الذين يَمضون ساعات كثيرة ومتواصِلة على شبكة الإنترنت، وأيضًا يَتجلَّى إهمال الأهل في عدم مُتابَعة أبنائهم الذين يَستخدِمون وسائل الاتِّصال التي أصبحت متوافِرة في جميع الأنظمة الحاسوبيَّة والهواتف الخلويَّة.

إنَّ الحلول المثاليَّة لمواجَهة أخطار استعمال القُصَّر لوسائل الاتِّصال عَبْر الإنترنت ليسَت كثيرة، ولكنَّها تَشمَل الأساليب لاستباق حدوث أي أخطار واحتوائها عند حدوثها، والحلول المثاليَّة لمواجَهة أخطار استعمال القُصَّر لوسائل الاتِّصال عَبْر الإنترنت هي:

1. تَركيب برامج حاسوبيَّة متخصِّصة تَمْنَع الأطفال من الولوج إلى أي موقع إنترنت باستثناء مواقع الإنترنت المَسموحَة من قِبَل الأهل. تَستطيع هذه البرامج أن تَضَع حاجزًا بين ولوج الطفل وأي موقع إنترنت يَرغَب الأهل في حَجْبه، وتَستطيع بعض هذه البرامج أن تُسجِّل جميع أنشطة الطفل في أثناء عَمَله على الإنترنت للاطِّلاع عليها فيما بعد، ويَبقى على الأهل التأكُّد من سلامة مواقع الإنترنت التي يَسمَحون لأطفالهم بالولوج إليها، وهذه المهمَّة ليسَت بالأمر الصعب، حيث يَستطيع الوالدان أن يُلقيا نظرة سريعة على هذه المواقع قبل البَتّ في السماح بالولوج إليها، ويُمكِن اختصار الطريق على الأهل من خلال إتاحَة مواقع الأطفال، كالألعاب والترفيه والرسوم المتحرِّكة فقط ضمن المواقع المَسموح بالدخول إليها في إعدادات تِلْك البرامج، وفي الواقع طُبِّقَت بعض القيود على استخدام الأطفال للإنترنت في بعض البلدان، وأشهرها الولايات المتَّحدة الأمريكيَّة، فعام 2000 سَنَّ الكونغرس الأمريكي قانون CIPA الذي يَنصُّ على أنه يجب على المدارس والمكتبات الحاصِلة على حسوم من استعمال خدمة الإنترنت فَرْض قيود على الإنترنت لمَنْع الأطفال من الولوج إلى مواقع الإنترنت المؤذية والفاحِشة (4).
2. مراقَبة سلوك القاصِر بعد استعماله الإنترنت على المدى القصير. إنَّ أي تَغيُّر في سلوك القاصِر بالتزامُن مع جلوسه الطويل على الإنترنت يَدلُّ على حدوث تأثير فيه يُمكِن أن يُؤذيه فيما بعد، ويَجب على الأهل اتِّباع أسلوب يُمكِّنهم من استدراج القاصِر لإخبارهم عن أنشطته في الإنترنت واتِّصالاته مع أصدقائه، وإذا كان الأهل على دراية تقنيَّة لا بأس بها في الحاسوب، يَستطيعون زراعة

برنامج تَجسُّس خَفي في حاسوب القاصِر لمتابَعة أنشطته كاملةً، وهناك برامج تجاريَّة لهذا الغرض موجودة بكثرة على الإنترنت.

3. تَوعيـة القُصَّـر اجتماعيًّـا ودينيًّا. تَتضمَّن تَوعية القاصِـر اجتماعيًّا تَعليمه عدم التعاطي مع أشخاص قد يكونون مشبوهين أو غير معروفين لديه، وعدم إعطائهم معلومـات شَـخصيَّة تفصيليَّة عنه، ويَندرِج تحـت تَوعية القاصِر اجتماعيًّا عدم تَزويد مواقع الإنترنت بالمعلومات الشخصَّية حتَّى ولو كان ذلك اختياريًّا، ولقد طُبّقت فعلًا قوانين تَمْنع أصحاب مواقع الإنترنت طَلَب معلومات من الأطفال إلا بموافقة الأهل، فعام 1998م أحدَثَت الولايات المتَّحدة الأمريكيَّة قانون COPPA الـذي يُلـزِم مديري مواقـع الإنترنت ومشـغِّليها بالحصـول على موافَقـة والدَي الطفل الذي يَقلُّ عمره عن 13 عامًا قبل تَجميعهم معلومات شخصيَّة منه (5). أمّـا تَوعيـة القاصِر دينيًّا فتَتضمَّن تَذكيره بوجوب التحلِّي بالأخلاق الإسـلاميَّة والتقيُّد بالتعاليم التي تُحرِّم مشـاهدة المواد الإباحيَّة ومخالَفة شَرْع الله – عز وجـل – وإشـعاره بأنَّـه مراقَـب مـن الله – عـز وجل – حتَّـى ولـو كان مختليًا مع نفسه، وتَتضمَّن تَوعية القاصِر دينيًّا تَذكيره بالإثم الذي يُمكِن ارتكابه من وراء تَصديق الجماعات المتطرِّفة والالتحاق بها.

2.8 أمان المعلومات الحَركيَّة

ثَمَّة معلومات خاصَّة تَتضمَّن تفاصيل عن انتقال فرد أو أفراد عدَّة أو نَقْل مادة ما من مكان إلى آخر، وتُدعَى **المعلومات الحَركيَّة**، وتَتألَّف المعلومات الحَركيَّة من ستَّة عناصر، هي:

- الهَدَف، وهو إمّا فردًا أو أفرادًا أو مادة ما.
- المكان الأصل الذي يُوجَد فيه الهَدَف.
- المكان المَقصود الذي سيَنتقِل إليه الهَدَف.

- مخطَّط الطريق الكامِل الذي سيَسلُكه الهدف من المكان الأصل إلى المكان المقصود.
- وسيلة الانتقال (أو النقْل) سواء أكانت سيَّارة أم قطارًا أم باخرة أم طائرة.
- موعد الانتقال (أو النقْل) محدَّدًا بالتاريخ (اليوم، والشهر، والسنة) وبالوقت (الساعة، والدقيقة).

صفة المعلومات الحَركيَّة أنَّها مؤقَّتة، بمعنى أنَّه يَنتهي الاهتمام بحمايتها بمجرَّد وصول الهدف إلى المكان المَقصود، ويَقتضي ذلك أنَّ الأمان الذي يُمكِن أن نُدخِل فيه هذه المعلومات هو الأمان العادي ذو الدرجة الثانية، وعليه، فإنَّ صفة الأمان في هذه الدرجة (ثابِتة وآنية)، وذلك يَعني أنَّ مستوى حماية المعلومات الحَركيَّة ثابِت، ولكنَّه يَستمرُّ مدة زمنيَّة إلى حين وصول الهَدَف إلى المكان المَقصود، ومن أمثلة المعلومات الحَركيَّة المتعلِّقة بفرد، المعلومات الخاصَّة التي تَتضمَّن انتقال موكب رئيس دولة من مكان إلى آخر، أو سَفَر مسؤولين كبار من مكان إلى آخر، وعُبورهم بالطائرة أجواء بلدان محدَّدة، وما إلى ذلك، ومن أمثلة المعلومات الحَركيَّة المتعلِّقة بمادة ما المعلومات الخاصَّة التي تَتضمَّن نَقْل أسلحة من مكان إلى آخر (أو من بلد إلى آخر)، أو المعلومات الخاصَّة التي تَتضمَّن نَقْل أموال نقديَّة من مكان إلى آخر، وثَمَّة أمرٌ مهم يَنبغي التركيز عليه فيما يَخصُّ المعلومات الحَركيَّة، وهو أنَّ هذه المعلومات قد تُستخدَم نفسها على نحوٍ متكرِّر، أو قد يَتغيَّر فيها واحد أو أكثر من عناصرها، فعلى سبيل المثال، قد يُعاد استخدام المعلومات الحركيَّة المتعلِّقة بانتقال موكب مسؤول كبير من منزله إلى مقرِّ عمله (أو بالعكس) يوميًّا بالعناصر نفسها؛ أي إنَّه سيَنتقِل من منزله (المكان الأصل) إلى مقرِّ عمله (المكان المقصود) أو بالعكس، وسيَسلُك الطريق نفسه المخصَّص لذلك وبوسيلة الانتقال نفسها وتمامًا موعد هذا الانتقال نفسه، وأحيانًا ولأسباب أمنيَّة، قد يَقوم المَعنيُّون بحماية موكبه بتَغيير أحد العناصر، مثل مخطَّط الطريق أو موعد الانتقال أو أحيانًا وسيلة الانتقال.

يُمكِن حماية المعلومات الحَركيَّة وإدخالها في وَضْع الأمان من خلال تَطبيق أمن معلومات عليها، يُدعَى **أمن المعلومات الحَركيَّة**، ويَتمثَّل أمن المعلومات الحَركيَّة في حمايتها من أجل حماية الهَدَف من أي خطر قد يُوجَّه إليه عند انتقاله (أو نَقْله) المتمثل في سَعي مجرمين لإيذاء الهَدَف إذا كان فردًا أو إيذاء الهَدَف أو سَرقته إذا كان عبارة عن مادَّة ما، ويُقَاس نجاح أمن المعلومات الحَركيَّة بالسلامة التامَّة لوصول الهدف إلى المكان المَقصود على نحوٍ متكرِّر، ويَتم تَحقيق أمن المعلومات الحَركيَّة من خلال تطبيق الإجراءات الآتية:

1. وَضْع الخطَّة الكامِلة لانتقال (أو نَقْل) الهَدَف من قِبَل خبراء متخصِّصين في مجال أمن الهَدَف وسلامة انتقاله (أو نَقْله). يُفتَرَض في الخبراء المتخصِّصين في مجال أمن الهَدَف وسلامته أنَّهم يَستطيعون رَسْم مخطَّط الطريق الكامِل ووسيلة الانتقال (أو النقْل) الملائمة وموعد الانتقال (أو النقْل) بما يَتناسَب مع أهميَّة الهَدَف وأخطار الطريق واعتبارات أخرى، مثل إطلاق تهديدات سابقة للهَدَف.
2. عَدَم تَسجيل المعلومات الحَركيَّة رقميًّا أو ورقيًّا، في وسائل أو وسائط معلوماتية يمكن النفاذ إليها.
3. الاحتفاظ بالمعلومات الحَركيَّة بين مجموعة صغيرة جدًّا من الأفراد ذوي العلاقة بانتقال (أو نَقْل) الهَدَف، ويَجب أن يُختار هؤلاء الأفراد على أساس الثقة التامَّة بأمانتهم، ويَجب أن يُغيَّروا باستمرار؛ لكيلا يَحدُث تَسريب للمعلومات الحَركيَّة من قِبَل أحدهم لأي سببٍ كان، مثل إقدام واحد منهم أو بعضهم على الخيانة.
4. تَغيير واحد أو أكثر من عناصر المعلومات الحَركيَّة باستمرار.
5. استعمال وسائط اتصالات مشفرة (معماة) بمستوى آمن من مستويات التشفير (التعمية).

3.8 حوادث الأمان

لا يَعني أنَّ تطبيق إجراءات الأمن ثمَّ إجراءات الأمان على المعلومات خاصَّة (مهما كان نموذجها) يَجعلها آمنة دومًا، فمن المُمكِن أن يَحدُث اختراق لأمان المعلومات حتَّى بعد تطبيق جميع إجراءات الأمن وجميع إجراءات الأمان بحذافيرها وبمهنيَّة عالية، فلا يوجَد وَضْعٌ مثالي لأمان المعلومات، بحيث تَكون هذه المعلومات آمنة بشكل تام، وإذا كانت الإجراءات المضادَّة مطبَّقة على نحوٍ عالٍ من الاحتراف وبمتابعة مستمرَّة، فعندها لا يَصِل أمان المعلومات إلى الوضع المثالي، وإنَّما إلى حَدٍّ قريب منه، وإذا حَدثَت اختراقات لأمان المعلومات المماثِّلة، إمّا بسرقة هذه المعلومات أو إفشائها أو تخريبها، فنحن بصَدَد مفهوم حوادث الأمان Safety incident، وقد يَتساءَل القارئ عن سَبَب تَسمية هذه الحوادث بـ (حوادث الأمان) بدلًا من (حوادث الأمن)، فلا يوجَد في حقل أمن المعلومات حوادث أمن؛ لأنَّ وقوع أي سرقة أو إفشاء أو تخريب للمعلومات الخاصَّة قبل تطبيق إجراءات الأمن تحديدًا سَبَبه عدم تطبيق أمن معلومات رسميًّا عليها، فوقوع أي سرقة أو إفشاء أو تخريب للمعلومات الخاصَّة قبل تطبيق أمن معلومات لا يَمتُّ بصِلة لحقل أمن المعلومات، وإنَّ السَبَب الرئيس لوقوع حوادث الأمان هو عَدَم تطبيق إدارة أمن المعلومات بشكلٍ مناسِب، ولقد وُضِعَت مراحل إدارة أمن المعلومات لكل نموذج من نماذج المعلومات الخاصَّة على نحوٍ مثالي، ولكن سوء التطبيق لجميع هذه المراحل يُمهِّد لوقوع حوادث الأمان.

ثَمَّة إجراءان علاجيّان للتعامُل مع حوادث الأمان، هما:

1. مراجعة الآليَّة التي تَمَّ عَبْرها تطبيق إدارة أمن المعلومات، ومن ثم تَغييرها، فالإجراء العلاجي الأول يَنبغي أن يَكون مراجعة هذه الآليَّة لاكتشاف مواضِع الخطأ في التطبيق ومعرفتها، فوَضْعُ آليَّة جديدة لتطبيق مراحل إدارة أمن المعلومات تَتفادَى مواضِع خطأ التطبيق تِلْك.

2. تغيير مضامين جميع المعلومات الخاصَّة فَوْر وقوع حادث الأمان. سوف يَتعرَّض مالِك المعلومات الخاصَّة إلى أذى وخسارة كبيرين بمجرَّد وقوع حادث الأمان؛ لـذا يَجـب عليـه أن يُغيِّر عند وقوع حـادث الأمان مضامين المعلومات الخاصَّة فورًا، وعند ذلك ستَفقِد مضامين هذه المعلومات القديمة أهميَّتها بعد تغييرها، وتَتراوَح عملية تغيير مضامين المعلومات الخاصَّة ما بين السـهولة والصعوبة، وذلك بحسـب كل نموذج من نمـاذج المعلومات، فمن أمثلة المعلومات الخاصَّة ذات القيمـة الماديَّـة التـي يُمكِن تغييـر مضامينها معلومات الأعمـال الخاصَّة، وأرقـام التعريف الشـخصي، وتُغيَّر مضامين معلومات الأعمـال الخاصَّة مثلًا بتغيير الخطَط المسـتقبليَّة لمشروعات تجاريَّة أو التصاميم الرئيسة لمنتجات صناعيَّة.

أمّـا أرقـام التعريـف الشـخصي فتُغيَّـر بـكل سـهولة من خـلال تبديلهـا بأرقام أخـرى، وأمّا تغيير مضامين المعلومات الخاصَّـة ذات القيمة المعنويَّة فيَتطلَّب جهودًا كبيرة وصعبة، إذ سيَشـمَل تغيير مضامين المعلومات المصنَّفة سـريَّة، كتصاميم الأسلحة، ومواعيد الهجمات الحربيَّة، وتغيير في مضامين المعلومات الدوليَّـة المصنَّفـة سـريَّة، كمحتويـات معلومـات اسـتخباراتيَّة مشـتَرَكة، وأمّا تغييـر مضامين المعلومـات الخاصَّة ذات القيمـة المَجازيَّة فلا يَحتـاج إلا إلى جهـدٍ يَتمثَّـل في تغييـر محتويات مِثْل كلمـات المرور لحسـابات صناديق البريد الإلكترونـي، وما إلى ذلك، وإنَّ تغيير مضامين جميع المعلومات الخاصَّة يَقطَع الطريق في أغلب الأحيان أمام الخصم للاسـتفادة من المعلومات التي حَصَل عليهـا؛ لـذا فـإنَّ أهم شـيئين في هـذا الإجراء همـا الحِرص على سـريَّة عمليَّة تغييـر مضامين المعلومات الخاصَّة، والإسـراع في تطبيـق إدارة أمن معلومات عليها من جديد.