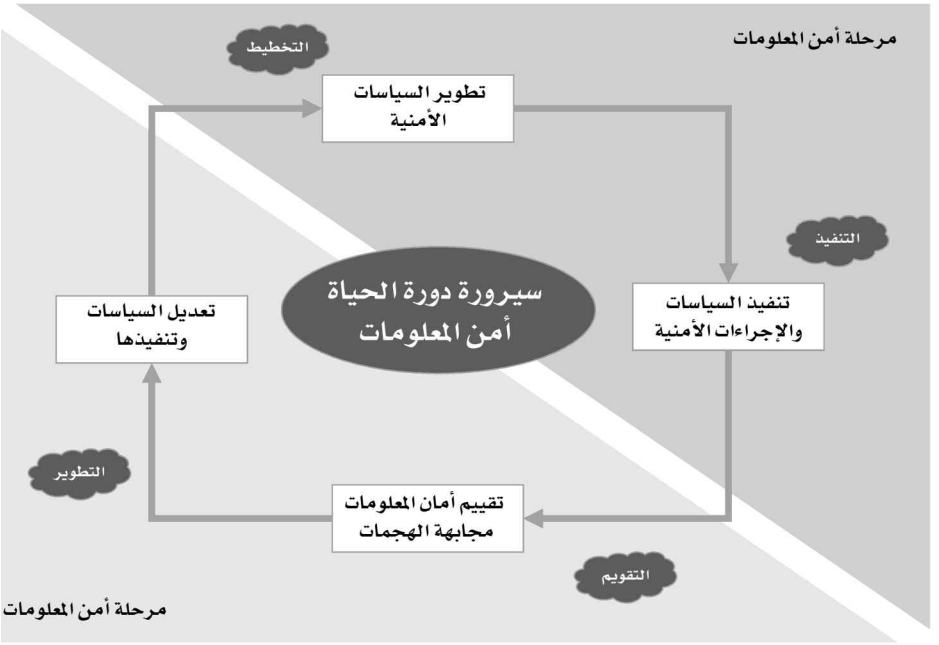
# الفصل الرابع

## أمان المعلومات ومستوياته ومقاييسه


كما ذكرنا سابقًا، ثمة مرحلتان في عملية حماية المعلومات هما: مرحلة التعامل مع أمن المعلومات، ومرحلة التعامل مع أمان المعلومات، ويبيّن الشكل أدناه عناصر هاتين المرحلتين، وعادة لا يتطرق كثير من العاملين في حقل أمن المعلومات إلى آليَّةٍ لتقييس تفاصيل ومراتِب الحالة الأمنية التي تَدخُل فيها المعلومات بعد حمايتها، أو الحالة التي يجب أن تكون عليها المعلومات من حيث أمنها واستمرار هذا الأمن مع المستجدات والتطورات المضادة؛ أي مرحلة (أمان المعلومات)، فمعظم الألفاظ التي تُطلَق على المعلومات بعد حمايتها في هذا الحقل هي (آمنة) و(مؤمَّنة) و(مَحميَّة) و(حصينة) وما إلى ذلك من الألفاظ المرادِفة، ويُقدِّم هذا الفصل مقاييس لتقييم أمان المعلومات المَحميَّة، ولا تَرتبِط هذه المقاييس بطبيعة المعلومات، سواء أكانت رقميَّة أم ورقيَّة، فهي تسري على كلتا الطبيعتين.

يَعتمِد المقياس الأول على (**مستويات** أمان المعلومات) لقياس أمان المعلومات المَحميَّة تبعًا لفئات المجتمع أو تبعًا لفئات مالك المعلومات أو الطرف المعني بأمنها، ويُقيِّم المقياس الثاني (**درجات** أمان المعلومات) المَحميَّة من منظور أهميَّتها ومستوى حساسيَّتها أو مستوى سريتها أو خصوصيتها. أمّا المقياس الثالث فيُحدِّد **وَضْع** المعلومات المَحميَّة أو حالتها، آمنة أو غير آمنة، استنادًا إلى التكلفة الماليَّة والمدَّة الزمنيَّة لاختراق حمايتها بغَضِّ النَظر عن مراتِب هذا الأمان.




### 1.4 مستويات أمان المعلومات بحسب الجهة المالكة لها

تعتمد مستويات أمان المعلومات على الجهة المالكة لها، ويُمكِن التمييز بين أربع فئات رئيسة: الفرد – والمؤسسة أو المنظَّمة – والدولة – والعالم. الفرد هو المكوِّن الرئيس للمنظَّمة والدولة، والمنظَّمة قد تكون أحد مكوِّنات الدولة، وإن هناك تجمعات وتكتلات دولية لها معلومات خاصة بها، وتَحتاج المعلومات المرتَبِطة بكل فئة من هذه الفئات إلى

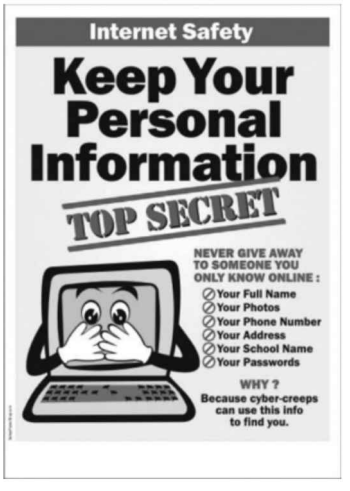
مستوى محدَّد من الأمان، إذْ ليسَ من الضروري توفير أمان تام وموحَّد الدرجة لكل الفئات، إذ إن لكل فئة متطلَّبات أمان معلومات معيَّنة تَختلِف عن تلك المطلوبة لبقيَّة الفئات.

ثَمَّة أربعة مستويات لأمان المعلومات تَشمَل جميع فئات المجتمع، وهي: **أمان المعلومات على مستوى الفرد، والمنظَّمة، والدولة، والعالَم.**

### 1.1.4 أمان المعلومات على مستوى الفرد

الفرد هو أصغر وحدة فاعِلة في المجتمع، وتَنحصِر أهميَّة أمان المعلومات في هذا المستوى ضِمْن نطاق الفرد فقط، وصفة بعض المعلومات في هذا المستوى أنَّها خاصَّة للفرد وغير مشتَرَكة مع الآخرين، والفرد هو الشخص الوحيد المخوَّل بقراءتها واستعمالها والاستفادة منها، والتخويل هنا مَمنوح من الفرد نفسه (أي مِنْه وإليه).

من الصعوبة تحديد جميع أشكال المعلومات المَطلوب حمايتها بالنسبة إلى الفرد، ولكن يُمكِن تعريف أنواع عامَّة للمعلومات التي تَخصُّ الفرد، ويَندرِج تحتها أيُّ شكل من تِلْك المعلومات. عمومًا، ثَمَّة نوعان من المعلومات التي تَخصُّ الفرد، هما: **معلومات فرديَّة خاصَّة غير حسَّاسة، ومعلومات فرديَّة خاصَّة حسَّاسة.**



المعلومات الفرديَّة الخاصَّة غير الحسَّاسة هي المعلومات المرتَبِطة بشخصٍ واحد فقط، وهو الطرف الوحيد المخوَّل بقراءتها واستعمالها والاستفادة منها، ولا تَحمِل في مضامينها أيَّ مظهر حسَّاس، بحيث إنَّ كتمانها لا يُؤدِّي إلى الجريمة المباشرة بحقِّ أيّ فرد آخر أو تهديد الأمن لدولة ما، وإنَّ إفشاءها يُؤدِّي إلى إيذاء مالِكها، ومن أمثلة المعلومات لهذا النوع: المذكِّرات اليوميَّة، وكلمات السرّ الخاصَّة بصناديق البريد الإلكتروني، وأرقام الحسابات المصرفيَّة، ورقم التعريف الشخصي PIN، وخطط شخصيَّة مستقبليَّة، وكما هو واضحٌ من التعريف، فإنَّ هذا النوع من المعلومات لا يَتضمَّن معلومات تُؤدِّي بتطبيقها إلى إيذاء أيّ فرد آخر جسديًّا، كالتخطيط مثلًا لعمليَّة قَتْل، أو اغتيالات سياسيَّة أو عسكريَّة، ولا تُؤدِّي إلى تهديد أمن دولة ما.

ولأن المعلومات الفرديَّة الخاصَّة غير الحسَّاسة لا تَحتوي على أيّ شكل من أشكال الجريمة المباشرة تجاه أيّ فرد آخر أو تهديد أمن دولة ما، فمن حقِّ الفرد الذي يَمتلِكها أن يَحميها بالطريقة التي يَختارها، وهذا الحقُّ الذي يَمتلِكه الفرد مبرَّر.

النوع الثاني من المعلومات التي تَخصُّ الفرد هو المعلومات الفرديَّة الخاصَّة والحسَّاسة، وهي المعلومات المرتَبِطة بشخصٍ (أو عدد من الأشخاص)، وهو الطرف الوحيد المخوَّل بقراءتها واستعمالها والاستفادة منها (من وجهة نَظَره الخاصَّة)، التي تَحمِل مظاهر حسَّاسة أو خطيرة، بحيث إنَّ كتمانها يُؤدِّي إلى إمكانية القيام بجرائم مباشرة أو تهديدات جديَّة لأمن أي دولة، وإنَّ إفشاءها يُؤدِّي إلى إحباط هذه الجريمة، وإنَّ المعلومات الفرديَّة الخاصَّة والحسَّاسة قد يشترك فيها أكثر من طرف (مجموعة من الأفراد يرتبطون بفرد)، خاصَّةً إذا كانوا يُشكِّلون عصابة، وتندرج مثل هذه العصابات تحت فئة الفرد؛ لأنها لم تَتكوَّن بطريقة نظاميَّة وشرعيَّة، فقد تَشكَّلت من خلال دعوة شخصٍ واحدٍ (هو الأصل) عددًا من الأفراد للانضمام إلى تنظيمه والائتمار بأوامره؛ ولذلك فهدف حماية المعلومات الخاصَّة الحسَّاسة من قِبَل هؤلاء الأفراد هو في النهاية هَدَف زَعيمهم نفسه؛ لأنَّهم يَعملون بتفكيره ومذهبه نفسه، وإنَّ إبقاء هذه المعلومات

الفرديَّة الخاصَّة الحسَّاسة (سريَّةً) يُؤدِّي إلى عواقِب وخيمة تَصِل درجة خطورتها إلى مستويات عالية إنْ لم يَتم إفشاؤها للمَعنيين.

لا يَمتلِك الفرد حق حماية معلوماته الخاصَّة الحسَّاسة مهما كانت ظروفه أو مَكانته الاجتماعيَّة، وإنَّ أفضل إجراء للتّعامُل مع هذه المعلومات هو القيام بإفشائها للمَعنيين وإجبار مالِكها على ذلك، أو اختراق أمانها إنْ لم يَكُن بالإمكان إفشاؤها مباشرةً.

### 2.1.4 أمان المعلومات على مستوى المنظَّمة

يُطلَق اسم (المنظَّمة) على أي منشأة أو شركة أو مؤسسة تَعود ملكيَّتها إلى فردٍ واحد أو عدد من الأفراد، وقد تَعود ملكيَّة المنظَّمة إلى الدولة، فثَمَّة نوع واحد من المعلومات التي تَخصُّ المنظَّمات (سواء أكانت تجاريَّة أم صناعيَّة أم خدمية) هو معلومات **الأعمال الخاصَّة** Private Business Information، وصفة معلومات الأعمال الخاصَّة في مستوى المنظَّمة أنَّها خاصَّة بالنسبة إلى المالِك (أو الأفراد المالِكين) وغير مشتَرَكة مع الآخرين، وهذا يَدلُّ على أنَّ مالِكي المنظَّمة هم المخوَّلون فقط بقراءة معلومات الأعمال الخاصَّة واستعمالها والاستفادة منها، ولا يَقتصِر التّخويل على المالِكين فقط، بل إنَّ موظَّفي المنظَّمة المخوَّلين من قبل مالِكيها يُمكِنهم قراءة معلومات الأعمال الخاصَّة واستعمالها أيضًا.

إنَّ معلومات الأعمال الخاصَّة التي تَمتلِكها المنظَّمة حسَّاسة بطبيعتها، وحساسيتها تَنبُع من أهميَّتها بالنسبة إلى مالِكيها؛ لأن فقدان هذه المعلومات أو إفشاءها أو تخريب جزء منها أو جميعها يُؤدِّي إلى خسائر كبيرة بالنسبة إلى المنظَّمة، وحجم هذه الخسائر يَعتمِد على درجة حساسيَّة معلومات الأعمال الخاصَّة ومقدار التخريب أو الإفشاء، ويَختلِف مضمون معلومات الأعمال الخاصَّة من منظَّمة إلى أخرى، فالمنشأة الصغيرة (كمكتب سياحة مثلًا) تَحتفِظ بأسماء العملاء المتعامِلِين معها، والشركة التجاريَّة (استيراد وتصدير مثلًا) تَحتفِظ بالعمليات والصفقات التجاريَّة التي أجرتها

أو ستَجريها مستقبلًا، والشركة الصناعية (معمل مثلًا) تَحتفِظ بالتصاميم والخطط المستقبليَّة لعمليات الإنتاج.

ومن حَقِّ المنظَّمة أن تَحمي معلومات الأعمال الخاصَّة التي تَمتلِكها مهما كان مضمونها أو درجة حساسيَّتها، وهذا الحقُّ مَكفول لأيّ منظَّمة، طالما أنها تَعمَل ضِمْن الإطار المشروع، والإطار المشروع يَعني أنَّ جميع معلومات الأعمال الخاصَّة التي تَحتفِظ بها المنظَّمة تَخصُّ مصالحها، ولا تَنطَوي على أي شكل من أشكال الجريمة المباشرة تجاه أي فرد أو تهديدات أمن دولة ما، وعليه يَنبغي أن تَندرِج سرقة هذه المعلومات أو إفشاؤها أو تخريبها ضمن جناية السرقة أو التخريب.

### 3.1.4 أمان المعلومات على مستوى الدولة

تُعدّ بعض المعلومات التي تَحتفِظ بها الدولة أهم بكثير وبكل المقاييس من المعلومات التي تَحتفِظ بها المنظَّمة أو الفرد، والسبب هو أنَّ الدولة تُمثِّل المجتمع الذي تَحكُمه، ومن ثم، فبعض المعلومات التيَ تحتفِظ بها الدولة وتَحميها مهمَّة بالنسبة إلى المجتمع ومرتَبِطة بأمنه، وهذا بلا شك بافتراض أنَّ الدولة التي نَتحدَّث عنها شرعيَّة. إذًا، يَجب أن تَحمي الدولة معلوماتها بشكل مناسب؛ لأنَّ الحفاظ على هذه المعلومات هو حفاظ على مصالح المجتمع ككل، وأنَّ سرقتها أو إفشاءها أو تخريبها هو تخريب لمصالح المجتمع ككل وتهديد لأمنه، ويَدلُّ هذا على أنَّ بعض المعلومات التي تَحميها الدولة حسَّاسة بطبيعتها.

والمعلومات التي تَحميها الدولة هي **المعلومات المصنَّفة سريَّة بكل مستويات هذه السرية**، فمثلًا من المعلومات التي تَحميها الحكومة الأمريكيَّة تحت بند المصنَّفة سريَّة الخطط العسكريَّة، والتصاميم الرئيسة للأسلحة، والأنشطة الاستخباراتيَّة، والمعلومات الاستخباراتيَّة عن دول أجنبيَّة، والمواد العلميَّة أو التكنولوجيَّة أو الاقتصاديَّة التي تَرتبِط بالأمن القومي، والمواد التي تَتعلَّق بإنتاج أسلحة الدمار الشامل واستخدامها. وفي

المملكة المتَّحدة تَعدّ الحكومة المعلومات التي تُهدِّد الاستقرار الداخلي لها أو للدول الصديقة، أو التي تُسبِّب تخريبًا للعلاقات مع الدول الصديقة، أو التي تُسبِّب تخريبًا طويل الأمد لاقتصادها الوطني، أو التي تُهدِّد بشكلٍ مباشر أمنها القومي، جميعها تحت بند المصنَّفة سريَّة. وأمّا في الصين، فالمعلومات التي تَحميها الحكومة تحت بند المصنَّفة سريَّة هي تِلْك المواد التي تَتعلَّق بالقرارات السياسيَّة الرئيسة، أو أنشطة القوات المسلَّحة، أو الأنشطة الدبلوماسيَّة، أو المرتبِطة بالاقتصاد الوطني، أو التي تَتعلَّق بالتكنولوجيا والعلوم.

من الطبيعي جدًّا أن تَحمي الدولة المعلومات التي تَمتلِكها، بل من غير الطبيعي ألا تَقوم بواجبها تجاه حماية المعلومات الحكوميَّة.

### 4.1.4 أمان المعلومات على المستوى الدولي

عندما يجري الحديث عن أمان المعلومات على المستوى الدولي، يُقصَد بذلك معلومات يَتجاوَز الاهتمام بها والاحتفاظ بسريَّتها حدود الدولة الواحدة، والمعلومات المطلوب حمايتها على المستوى الدولي لها شكلٌ واحد فقط هو معلومات خاصَّة تَتشارَك فيها أطراف دولية عدة، وتُدعَى **المعلومات الدوليَّة المصنَّفة سريَّة**. إنَّ أكبر تَجسيد لهذه المعلومات هو المعلومات الاستخباراتيَّة التي تَتضمَّن مصالح قوميَّة للدول التي تَمتلِكها، أو المعلومات العسكريَّة التي تَتعلَّق بخطَط دفاعيَّة فيما بينها، وأيضًا من المعلومات الدوليَّة المصنَّفة سريَّة تِلْك المتعلقة بمنظَّمات أو اتفاقيات دوليَّة خاصة، ومثال ذلك، المعلومات المصنَّفة سريَّة (بجميع مستويات تصنيفها السرِّي) المتبادَلة بين دول منظَّمة حلف شمال الأطلسي.

يَنطلِق الدافع لحماية المعلومات الدوليَّة المصنَّفة سريَّة من رَغْبة الدول التي تَمتلِكها في الحفاظ على مصالحها القوميَّة، وأوَّل هذه المصالح القوميَّة هو الأمان العام الذي يَتجسَّد في استقرار الدول المشارِكة وسلامتها، ومن ثم، فإنَّ سرقة هذه المعلومات

أو إفشاءها أو تخريبها سيُؤدِّي حتمًا إلى زعزعة استقرار الدول المشارِكة في استعمالها، وعليه، يَجب أن تَبذُل جميع الدول المشارِكة في هذه المعلومات أقصى ما لديها للحفاظ على سريَّتها وسلامتها وتَوافرها.

### 5.1.4 العلاقة بين مستويات أمان المعلومات

إنَّ مستوى أمان المعلومات المقصود بالتعاريف المذكورة أعلاه هو الحدُّ الأعلى المطلوب أن تَكون المعلومات فيه مَحميَّة، ومن المألوف أن تُحدَّد العلاقة بين مستويات أمان المعلومات بقانون **العلاقة التَراتُبيَّة** Hierarchical relationship الذي يَنصُّ عمليًّا على أن كل مستوى من مستويات أمان المعلومات المذكورة سهل الاختراق من قِبَل المستوى الذي يَعلوه، وصعب الاختراق من قِبَل المستوى الذي يَدنوه، فمثلًا، أمان المعلومات على مستوى المنظَّمة يَعني أنه يُمكِن للمعلومات المَحميَّة التي تَمتلِكها المنظَّمة أن تُختَرَق من قِبَل المستوى الأعلى (وهو الدولة أو دول أخرى متقدمة في هذا الحقل)، وفي الوقت نفسه لا يُمكِن اختراقها من قِبَل المستوى الأدنى (وهو الفرد أو شركات أصغر من المنظَّمة). أيضًا، أمان المعلومات على مستوى الدولة يَعني أنه قد يُمكِن للمعلومات المَحميَّة التي تَمتلِكها الدولة أن تُختَرَق من قِبَل المستوى الأعلى (وهو دول أخرى متقدمة في هذا الحقل)، وفي الوقت نفسه يَصعُب اختراقها من قِبَل المستوى الأدنى (وهو المنظَّمة أو الفرد).

إنَّ العلاقة السابقة بين مستويات أمان المعلومات ليسَت موضوعة أو مرسومة سابقًا (أو حتَّى موصَّى بها)، إنَّما هي علاقة طبيعيَّة عملية نابِعة من مقدار إمكانات وقدرات واهتمام كل مستوى (أي الفرد أو المنظَّمة أو الدولة أو العالَم)، فمثلًا لو كان الحديث عن أمان المعلومات على مستوى المنظَّمة يَتبيَّن أنَّ الدولة ببعض أو كل إمكاناتها تَستطيع أن تَخترِق أمان المعلومات التي تَمتلِكها منظَّمة إذا وجدَت الدولة ضرورة لذلك، وفي الوقت نفسه يصعب على الفرد أن يَخترِق أمان المعلومات التي تَمتلِكها منظَّمة. في

الواقع، يُفترض منطقيًّا أنَّ الفرد لن يُنفِق (أو يُضحِّي) بأموال طائلة لسرقة معلومات تَمتلِكها منظَّمة ما، فالقيمة الماديَّة لهذه المعلومات أقل من الأموال التي من المُمكِن أن يُنفِقها الفرد من أجل القيام بذلك، فلو كان الأمر كذلك، وأَنفَقَ الفرد أموالًا طائلة للاستحواذ على معلومات مَحميَّة للمنظَّمة قيمتها الماديَّة تَقلُّ عن الأموال التي أَنفَقَها ذلك الفرد، فهذا حتمًا ليس فردًا، وإنَّما منظَّمة لها أهداف وراء ذلك (أو فردًا يُمثِّل منظَّمة ما)، أو قد تكون هذه المعلومات ذات أهميَّة كبيرة بالنسبة إلى الفرد وأهميَّة أقل بالنسبة إلى المنظَّمة، ولنعطِ مثالًا آخر، وليَكُن عن أمان المعلومات على مستوى الدولة، فمن الممكن أن يُختَرَق أمان المعلومات التي تَمتلِكها دولة ما من قِبَل طرف دولي (دولة متقدمة في هذا الحقل)، أو من تعاون وكالتَي استخبارات أو أكثر؛ لأنَّ الدول المعنيَّة بعمليَّة التجسُّس والاختراق، التي تُمثِّلها وكالات الاستخبارات، ستَضَع إمكانات وموارد ضخمة للقيام بذلك، تَفوق ما تَمتلِكه الدولة المراد اختراق أمان معلوماتها من موارِد وإمكانات، وفي الوقت نفسه، سوف يَكون من الصعب على أي منظَّمة أن تَخترِق أمان المعلومات التي تَمتلِكها الدولة (إلا إذا كانت هذه المنظَّمة مَدعومة مثلًا من قِبَل وكالات استخبارات دول أخرى).

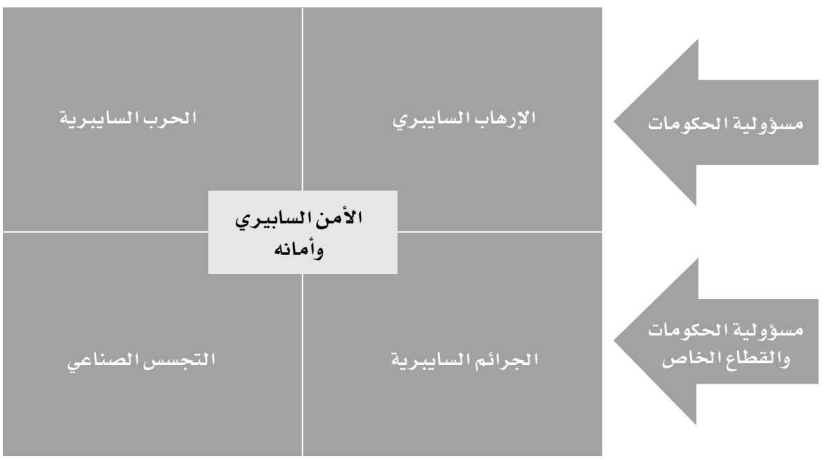
تُدعَى العلاقة بين الأطراف من مستوى الأمان نفسه **العلاقة التنافسيَّة** Competitive relationship، وقد يُحاوِل طرفٌ ما اختراق أمان معلومات طرف آخر من المستوى نفسه، ويَعتمِد نجاح محاولته على الإمكانات والموارِد المتاحة له للقيام بمحاولة الاختراق، ومن أمثلة هذه العلاقة التنافسيَّة قيام منظَّمة ما بسرقة معلومات ذات قيمة من منظَّمة أخرى، أو تَجسُّس دولة ما على دولة أخرى.

من المُمكِن تغيير مستوى أمان معلوماتٍ ما من خلال رفع هذا المستوى أو تخفيضه، فمثلًا يُمكِن أن يقوم فردٌ ما برفع مستوى أمان معلوماته ليَصِل إلى نفس مستوى أمان معلومات منظَّمة ما، ولكن مع هذا الإجراء ستَزداد تكلفة عمله، بمعنى آخر، سيَقوم الفرد الراغِب في رفع مستوى أمان معلوماته إلى نفس مستوى أمان معلومات منظَّمة

ما بدفع تكاليف إضافية قد تَصِل إلى التكاليف نفسها التي تَدفعُها المنظَّمة لحماية معلوماتها السريَّة، وقد يَبدو ذلك غباءً من الفرد إلا إذا كانت هذه المعلومات التي يُريد حمايتها ذات قيمة ماديَّة أكبر من تِلْك التكاليف الجاهِزة لدفعها، أو أنَّ هذا الفرد مدفوع للقيام بذلك، وهو مكلَّف بحمايتها، ومثال آخر على تغيير مستوى أمان المعلومات هو أن تَقوم منظَّمة ما بتخفيض مستوى أمان معلوماتها - إلى مستوى أمان معلومات الفرد - بعد أن تَرى أنَّها ليست ذات أهميَّة بالغة، ولا تَستحِق التكاليف المدفوعة لحمايتها.

ثمة تصور آخر للعلاقة بين مستويات الأمن والأمان المعلوماتي (السايبري) وهو بتصنيفه بحسب نوع التهديد والجهة المسؤولة عن الحماية ضده، ويبين الشكل توصيفًا مبسطًا لهذا التصور.

**نموذج في مسؤوليات الأمن السايبري (مسؤولية الفرد محدودة)**




### 2.4 درجات أمان المعلومات من حيث سريتها

لقد تَمَّ فيما سبق تَعَرُّفُ مستويات أمان المعلومات الأربعة التي ترسم الحدود الفاصلة بين حالات أمان المعلومات وفقًا لمتطلَّبات كل فئة من فئات المجتمع، ولقد حُدِّدت العلاقة التي تَربط بين هذه المستويات، ويُمكِن لمستويات أمان المعلومات أن

تُعطي فكرة عن أهميَّة المعلومات ومستوى حساسيَّتها بالنسبة إلى كل فئة من فئات المجتمع، ولكنَّ قياس أمان المعلومات من مَنظور أهميَّتها ومستوى حساسيَّتها من خلال درجات أمانها.

تقاس درجات أمان المعلومات من منطلَق قيمتها الماديَّة أو المعنويَّة أو المَجازيَّة، التي تَتطلَّب رَد فعل مناسِب يَتمثَّل في القيام بإجراءات لحمايتها، ويَتحدَّد مستوى هذه الإجراءات وفعاليتها اعتمادًا على القيمة الماديَّة أو المعنويَّة أو المَجازيَّة لتِلْك المعلومات. إذًا، فالقيمة تُحدِّد الدرجة المطلوبة من الأمان والكافية لكل طرف مَعني بتِلْك المعلومات، وهذا يَعني أن نَترُك مسألة إضفاء درجة أمان محدَّدة للمعلومات إلى المعلومات نفسها. أمّا الإجراء المقابِل والسليم للقيام فعليًّا بعمليَّة تحقيق هذه الدرجة من الأمان فهو من مهام الطرف الذي يَمتلِك تِلْك المعلومات.

يَندرِج أمان المعلومات مهما كانت قيمتها الماديَّة أو المعنويَّة أو المَجازيَّة في ثلاث درجات تُدعَى درجات أمان المعلومات، ودرجات أمان المعلومات هي:

1. الدرجة الأولى: **أمان المعلومات المطلَق.**
2. الدرجة الثانية: **أمان المعلومات العادي.**
3. الدرجة الثالثة: **أمان المعلومات المتكيِّف.**

### 1.2.4 الدرجة الأولى: أمان المعلومات المطلَق

الأمان المطلَق هو أقصى درجات الأمان الذي يُضفيه الطرف المالِك للمعلومات، فليسَ من السهل توفير الأمان المطلَق لأيّ معلومات مُراد حمايتها، فتكلفة وَضْع السياسات والخطط وتجهيز الأدوات اللازمة لإيجاد الأمان المطلَق باهظة جدًّا.

ومن صفات المعلومات المَحميَّة بدرجة الأمان المطلَق أنها ذات حساسيَّة عالية جدًّا، وتَحتوي على مواد يُمكِن، إذا تمَّ افتضاحها عَمْدًا أو عن غَير قَصْد، أن تُؤدِّي إلى

كوارث يُخيِّم تأثيرها السلبي على الأمن لدولة ما، أو قد تُسبِّب حربًا بين دولتين أو أكثر، فهي عادةً معلومات لا تَرتبِط بفرد أو منظَّمة، بل هي ذات أهميَّة كبرى على مستوى الدولة أو على المستوى الدولي، وأنَّ مستوى تصنيفها (بالنسبة إلى الدولة أو العالم) هو (سري للغايةUltra-Secret ) أو (**سرِّي جدًّا** Top Secret) فقط، وإنَّ أمثلة المعلومات المَحميَّة بدرجة الأمان المطلَق قليلة، ومن تِلْك الأمثلة الخطط العسكريَّة، ومواعيد إطلاق العمليات العسكريَّة، وتصاميم الأسلحة والمعدَّات الحربيَّة، والمواد المتعلِّقة بإنتاج أسلحة الدمار الشامل واستخدامها، والمَحميَّة جميعها تحت مستوى التصنيف (سرِّي جدًّا) كما في الولايات المتَّحدة الأمريكيَّة، أو المعلومات العسكريَّة التي تَتعلَّق بخطَط دفاعية متَّفَق عليها بين دولتين أو أكثر والمَحميَّة أيضًا تحت مستوى التصنيف (سري للغاية) أو (سرِّي جدًّا) كتِلْك المتبادَلة بين دول منظَّمة حلف شمال الأطلسي.

إنَّ أهم ما يُذكَر في درجة أمان المعلومات المطلَق أنَّ صفة الأمان فيها (ثابِتة ودائِمة) مهما تَغيَّرت الظروف المحيطة، وأنَّ الأمان نفسه يَمتدُّ لمدة زمنيَّة طويلة، ومن الضروري جدًّا أن نُولي اهتمامًا لموضوع (المدة الزمنيَّة) التي يَجب أن تَظل المعلومات في غضونها مَحميَّة، ويَجب عند اعتماد درجة الأمان المطلق لحماية معلوماتٍ ما أن يَتم أيضًا تحديد المدة الزمنيَّة التي يَنبغي أن تَبقى المعلومات في غضونها مَحميَّة، والأهم من ذلك أن يَتم الحفاظ على مستوى نوعيَّة الإجراءات المتَّخَذة نفسه مهما تَقادَم الزمن ضمن المدة المحدَّدة لذلك.

إنَّ عددًا من حكومات الدول يَقوم بتمديد المدة الزمنيَّة لإبقاء المعلومات ذات مستوى التصنيف (سري للغاية) أو (سرِّي جدًّا) مصنَّفة سريَّة، وتَقوم أحيانًا بتعديل مستوى تصنيفها السرِّي، بل وحتَّى إلغاء تصنيفها سريَّة، وتَتَّبِع تِلْك الحكومات معايير محدَّدة لإلغاء تصنيف المعلومات سريَّة، ومن بين هذه المعايير مرور زمن معيَّن أو وقوع حدثٍ ما كما هو الحال في الولايات المتحدة الأمريكية، فقد يَفترِض الأمر التنفيذي ذو الرقم 13526 الذي أَصدَره الرئيس الأمريكي Barack Obama عام 2009 أن يَتم إلغاء

تصنيف المعلومات سريَّة تلقائيًّا عند مرور مدة زمنيَّة معيَّنة أو وقوع حدثٍ ما، والأمر التنفيذي نفسه يَنصُّ على عدم إبقاء المعلومات مصنَّفة سريَّة إلى أجل غير مسمَّى، ويَعتقِد Arvin Quist [1] أنَّ عملية إلغاء تصنيف المعلومات سريَّة بعد مرور زمن معيَّن أو وقوع حدثٍ ما، ضروريَّة من أجل تَفادي التكاليف الإضافيَّة غير الضروريَّة لإبقاء المعلومات مصنَّفة سريَّة، ولكنَّ ذلك الاعتقاد غير صحيح في بعض الحالات؛ لأنَّه من المُمكِن أن يُعَاد استخدام المعلومات المصنَّفة سريَّة ذات المستوى (سري للغاية) أو (سرِّي جدًّا) في أوقات لاحقة ولو بصيغةٍ أخرى، فمثلًا لو كانت هذه المعلومات تَتعلَّق بتصاميم أسلحة، يُمكِن أن يُعاد استخدامها لتطوير تِلْك الأسلحة وإضافة التحسينات عليها، وأيضًا لو تَمَّ رفع الحماية عن المعلومات ذات المستوى (سرِّي جدًّا) التي تَشرَح خطَّة العمل العسكري لدولة ما في حربٍ ما بعد نشوبها وانتهائها (استنادًا إلى مبدأ إلغاء تصنيف المعلومات سريَّة بعد وقوع حدثٍ ما)، فقد يَستفيد أعداء الدولة المَعنيَّة من تفاصيل خطَّة العمل العسكري، ويَستثمِرونها لاحقًا في حروب أخرى، ولكن ثَمَّة معلومات، وإنْ كانت ذات حساسيَّة عالية، وتَتطلَّب حماية مطلَقة يَمكِن بسبب طبيعتها قَبول المعايير التي تَقتضي إلغاء تصنيفها سريَّة عند مرور زمن معيَّن أو وقوع حدثٍ ما، مثل موعد إطلاق عمل عسكري ضد دولةٍ ما، كما سَنرى لاحقًا في درجة أمان المعلومات المتكيِّف.

والسؤال الذي يَجب أن يُطرَح الآن هو: (ما **الإجراءات** التي يَنبغي أن تُتَّخَذ لحماية المعلومات في درجة الأمان المطلَق؟)، فلا يُمكِن الإجابة بدقَّة وبالتفصيل عن هذا السؤال بسبب اختلاف الظروف بين طرف وآخر (أي بين دولة أو منظَّمة دوليَّة وأخرى)، ولكن يُمكِن تحديد صفة هذه الإجراءات ونوعيَّتها على نحوٍ عام، وفي البداية يَجب أن يَتم وَضْعُ الخطَط لحماية المعلومات في درجة الأمان المطلَق من قِبَل خبراء متخصِّصين وبالتنسيق مع الجهات العليا المالِكة للمعلومات، بعدها يَنبغي تخصيص

(1) Arvin S. Quist: هو موظَّف متخصِّص في أمن المعلومات وفي تصنيفها، يَعمَل لدى مختبر Oak Ridge الوطني التابع لوزارة الطاقة الأمريكيَّة.

الأدوات والبرامج اللازمة لحماية المعلومات، على أن تكون على مستوى عالٍ من القوَّة والاحترافيَّة، والأهم من ذلك ألا يَتم توظيف و(استعارة) الأدوات والبرامج المطروحة تجاريًّا، وبمعنى آخر، يجب أن يَتم استخدام أدوات وبرامج خاصَّة ومختلفة كليًّا (سواء من ناحية التصميم أو من ناحية القوة والكفاءة) عن جميع ما هو معروف لدى العامَّة سواء أكانوا أفرادًا أم منظَّمات (أو حتَّى عن تِلْك الأدوات والبرامج المستخدَمة في بعض المؤسسات الرسميَّة الحكوميَّة المتوسطة أو الصغيرة التي لا يَمُتّ عملها بأي صلة بالأمن القومي)، فمثلًا عندما أَقرَّ المعهد القومي للمقاييس والتكنولوجيا في الولايات المتَّحدة الأمريكيَّة خوارزميَّة التعمية DES بوصفها مقياسًا فيدراليًّا، أجازَها للاستعمال في حماية الاتصالات الحكوميَّة غير المصنَّفة سريَّة فقط (إضافة إلى الاتصالات التجاريَّة للأفراد والمنظَّمات)، وحَيَّد عنها جميع المعلومات المصنَّفة سريَّة، الذي صَرَّح بأنَّ لها أدوات تعمويَّة خاصَّة لحمايتها، وسوف يَقتضي ذلك دون شك أن تَكون تكاليف تصميم الخطَط وتجهيز الأدوات والبرامج ووَضْعُها باهظة جدًّا، وعليه فسوف يَتم استخدام أموال من ميزانيَّة الدولة (أو ميزانيَّات دول عدَّة متحالِفة ومعنيَّة بالأمر) لتغطية تِلْك التكاليف الباهظة، وذلك مبرَّر جدًّا؛ كون المنفعة النهائيَّة من كل ذلك ستَصُبُّ في مصلحة الأمن الوطني للدولة أو الدول المتحالِفة.

### 2.2.4 الدرجة الثانية: أمان المعلومات العادي

النموذج الشائع من الأمان الذي يُضفَى إلى المعلومات الخاصَّة على نحوٍ واسع هو أمان المعلومات العادي، ولا تَعني كلمة (العادي) أنَّ الإجراءات المستخدَمة لحماية المعلومات في هذه الدرجة عاديَّة، أو أنَّ المعلومات نفسها من مستوى عادي، بل هي اصطلاح يُميِّز هذا الأمان العادي عن ذلك الأمان المطلَق الذي نُضفيه إلى المعلومات الفائقة الأهميَّة، ولكلمة (عادي) في اصطلاح (أمان المعلومات العادي) دلالة مهمة هنا، وهي أنَّ إجراءات الحماية المستخدَمة وعلى مستويات عدَّة (الفرد – المنظَّمة – الدولة

- العالَم) متعارَفة من ناحية التخطيط والتطبيق والنتائج المتوقَّعة من تنفيذها (وإنْ اختلَفَتْ شدَّة تِلْك الإجراءات بين الفرد أو المنظَّمة أو الدولة أو حتَّى الطرف الدولي).

على الرغم من أنَّ أمان المعلومات في الدرجة الثانية عادي، إلا أنَّ أهميَّة المعلومات نفسها تَختلِف بحسب اختلاف الأطراف المَعنيَّة بها وبحسب مستويات هذه الأطراف، فقد تَكون أهمية المعلومات على مستوى المنظَّمة أكبر بكثير من أهمية المعلومات على مستوى الفرد، وأهمية المعلومات على مستوى الدولة أكبر بكثير من أهمية المعلومات على مستوَيَي الفرد والمنظَّمة، وهذا الأمر طبيعي بسبب اختلاف أهمِّيات مضامينها، فعلى سبيل المثال، المعلومات الاستخباراتيَّة التي تَمتلِكها دولةٌ ما أهم بكثير من أرقام الحسابات المصرفيَّة التي يَمتلِكها فردٌ ما، إذ إنَّ خصم دولةٍ ما يَستطيع دفع أموال بعشرات أضعاف المال الذي قد يَمتلِكه فرد للحصول على المعلومات الاستخباراتيَّة لتِلْك الدولة، ولكنَّ الصفة المشتَرَكة بين هذه المعلومات المتعدِّدة المستويات (الفرد - المنظَّمة - الدولة - العالَم) والمَحميَّة بدرجة الأمان العادي هي أنَّ هذه المعلومات ذات حساسيَّة عاديَّة، ومعظمها لا يُؤدِّي إلى كوارث تُؤثِّر سلبًا في الأمن القومي لدولة ما، أو تُسبِّب حربًا بين دولتين أو أكثر، إذا تمَّ افتضاحها عَمْدًا أو عن غَير قَصْد، ولكن يُمكِن القول: إنَّ جميع المعلومات المرتبِطة بالفرد أو بالمنظَّمة، ومهما كانت طبيعتها ومدى أهميَّتها وعواقب افتضاحها، مَحميَّة تلقائيًّا بدرجة الأمان العادي.

أمّا بالنسبة إلى مستوَيَي الدولة والعالم، فجميع المعلومات المرتبِطة بهما والمصنَّفة سريَّة ومن مستويات التصنيف (**سرِّي** Secret) وما دون؛ أي (**خاص** Confidential) و(**محدود** Restricted) كما في قوانين دول عدَّة، ومهما كانت طبيعتها ومدى أهميَّتها وعواقب افتضاحها، مَحميَّة تلقائيًّا بدرجة الأمان العادي، ومن المُلاحَظ أنَّه لم يُشمَل في تبويب المعلومات المصنَّفة سريَّة بالنسبة إلى الدولة والعالَم ومن مستوى التصنيف (سرِّي جدًّا) ضمن درجة الأمان العادي؛ لأنَّ المعلومات المصنَّفة سريَّة من مستوى التصنيف (سري للغاية) أو (سرِّي جدًّا) بالنسبة إلى الدولة والعالَم مَحميَّة عادةً بدرجة الأمان المطلَق.

إنَّ صفة الأمان في درجة أمان المعلومات العادي (ثابِت ومؤقت)؛ أي إنَّ مستوى الحماية المخصَّص للمعلومات في هذه الدرجة ثابِت مهما تَغيَّرت الظروف المحيطة، وإنَّ الحماية نفسها تَستمرُّ مدة زمنيَّة مؤقَّتة ومحدَّدة مسبقًا وقابِلة للتمديد تلقائيًّا لحين الانتهاء من استثمار المعلومات، و(قابِلة للتمديد) تَعني أنه يُمكِن أن تَمتدّ المدة الزمنيَّة لأطول مِمَّا خُطِّطَ لها إنْ احتاجَ الأمر، دونَ القيام بإعادة التخطيط مرةً أخرى، والنقطة الجوهريَّة هنا هي أنَّ المدة الزمنيَّة المخطَّط لها في درجة الأمان العادي، ستَنتَهي بمجرَّد أن يُحقِّق مالِك المعلومات الغرض من هذه المعلومات، ويَجب التمييز هنا بين حالة (تخفيض مستوى أو رفع الحماية كليًّا عن المعلومات) في درجة الأمان العادي، وحالتها في درجة الأمان المتكيِّف الذي سنأتي عليه لاحقًا.

تَختلِف إجراءات حماية المعلومات في درجة الأمان العادي بين كل طرف على المستوى نفسه (أي على مستوى الفرد أو المنظَّمة أو الدولة أو العالَم) وبين كل طرف من كل مستوى من المستويات، فقد تَكون الطُّرُق التي يَستخدِمها فردٌ ما لحماية معلوماته مختلفة كليًّا عن الطُّرُق التي يَستخدِمها فردٌ آخر لحماية معلوماته (وهذا على مستوى الفرد). وكذلك على المستويات الأخرى؛ أي إنَّ «إجراءات حماية المعلومات في درجة الأمان العادي تَختلِف باختلاف كل طرف عن الآخر على المستوى نفسه وباختلاف كل مستوى عن الآخر» أمّا بالنسبة إلى تفاصيل تِلْك الإجراءات، مثل تصميم الخطَط ووَضْعها والأدوات والبرامج، فالأمر عائدٌ لتقدير الطرف المالِك للمعلومات، ولكن مهما اختلَفَت تقديرات الأطراف في ذلك، إلا أنَّها ستَستخدِم آليات وَضْع الخطَط المتعارَفة والأدوات والبرامج المطروحة تجاريًّا لحماية معلوماتها.

### 3.2.4 الدرجة الثالثة: أمان المعلومات المتكيِّف

ثَمَّة شكل من المعلومات مستخدَم في الشؤون الحياتيَّة العامَّة التي تَحتاج إلى حماية واهتمام من أصحابها، تَفرِض طبيعتها عليهم فيما بعد إمّا رفع مستوى حمايتها أو

تخفيض مستوى حمايتها أو إهمال حمايتها، وإنَّ الأساس في هذه المعلومات أنَّها مَحميَّة بإحدى الدرجتين السابقتين (الأولى أو الثانية)، لكنَّ الظروف المحيطة بمالِكها تَفرِض تغيير مستوى الاهتمام بها، فإمّا أن يَقوم مالِكها برفع مستوى حمايتها أو تخفيضه أو حتَّى إلغاء الحماية كليًّا. إذًا، تَحتاج مثل هذه المعلومات إلى حماية يَتكيَّف مستواها مع مستوى أهميَّة تِلْك المعلومات بالنسبة إلى مالِكها في ذلك الزمن وفي ذلك الظرف، ومن ثم، فإنَّ أفضل حماية لمثل تِلْك المعلومات هي الحماية المتكيِّفة.

أمان المعلومات في هذا النوع من الحماية يَتكيَّف مع الزمن والأحداث المحيطة بمالِك تِلْك المعلومات، فمن المُمكِن أن تَزداد أهميَّة المعلومات (التي قد تَكون في ذلك الوقت مَحميَّة بالدرجة الثانية، وهي الحماية العاديَّة) لتَصِل إلى مستوى ذي حساسيَّة عاليَّة جدًّا، ومن ثم، سيَتطلَّب أن تُصبِح المعلومات مَحميَّة بالدرجة الأولى، وهي الحماية المطلَقَة، أو أن تَقل أهميَّتها (التي قد تَكون في ذلك الوقت مَحميَّة بالدرجة الأولى) لتَصِل إلى مستوى عادي، وذلك لا يَتطلَّب إلا أن تُصبِح المعلومات مَحميَّة بالدرجة الثانية، وقد تَقلُّ أهميَّة المعلومات لتَصِل إلى مستوى يُمكِن من خلاله أن تُرفَع الحماية كليًّا عنها.

يَتكيَّف أمان المعلومات في هذه الدرجة مع عامِلَين اثنين هما: الزمن، والأحداث المحيطة، ويَعني التكيف مع الزمن أنَّ المعلومات قد تُصبِح مع مرور الزمن إمّا ذات أهميَّة كبيرة، أو قد تَفقد أهميَّتها لتُصبِح عديمة القيمة، أمّا أن يَكون أمان المعلومات متكيِّفًا مع الأحداث المحيطة فيَعني أنَّها قد تُصبِح عند حدوث أمرٍ ما إمّا ذات أهميَّة كبيرة، أو قد تَفقد أهميَّتها لتُصبِح عديمة القيمة. إذًا، نَستطيع القول ممَّا سَبَق: إنَّ صفة الأمان في درجة أمان المعلومات المتكيِّف (متغيِّرة).

ومن الأمثلة الواقعيَّة على رَفْع مستوى حماية معلوماتٍ ما من الدرجة الثانية إلى الدرجة الأولى القيام برَفْع مستوى حماية معلومات عسكريَّة عند نشوب حرب، فيَجب التذكير هنا بأنَّ بعض المعلومات العسكريَّة عادةً مصنَّفة سريَّة لدى كثير من حكومات

الدول، وليس بالضرورة أن يَكون مستوى تصنيفها (سري للغاية) أو (سرِّي جدًّا) إلا عند نشوب حرب.

من البدهي ملاحظة أنَّ رَفْع مستوى حماية معلوماتٍ ما من الدرجة الثانية إلى الدرجة الأولى لا يُمكِن أن يَتم إلا من خلال أطراف كبرى تَستطيع تَحمُّل التكاليف الباهظة لإجراءات الحماية المطلَقة ذات الدرجة الأولى كحكومة ما.

من أمثلة تخفيض مستوى حماية معلوماتٍ ما من الدرجة الأولى إلى الدرجة الثانية خطَّة عسكريَّة لحرب متوقَّعة تَكون من الأساس مَحميَّة بالدرجة الأولى قبل نُشوب الحرب، يُمكِن بعد انتهاء الحرب تخفيض مستوى حمايتها إلى الدرجة الثانية، أو حتَّى رفع الحماية عنها، وذلك من أجل تَفادي التكاليف الباهظة في إبقائها مَحميَّة بالدرجة الأولى، وفي هذا المثال تَكيَّف أمان المعلومات (والمعلومات هي هنا الخطَّة العسكريَّة) مع عامِل الأحداث المحيطة، حيث أجازَ حَدَث وقوع الحرب أن تُصبِح تِلْك المعلومات مَحميَّة بالدرجة الثانية.

تُماثِل عبارة (تخفيض مستوى حماية معلوماتٍ ما من الدرجة الثانية) معنى (رَفْع الحماية كليًّا عن المعلومات)، وذُكِرَ في 2,2,3 أنَّ المعلومات المَحميَّة بالدرجة الثانية، وهي الحماية العاديَّة قد تَكون إمّا لأفراد أو منظَّمات (أو حتَّى مؤسَّسات رسميَّة حكوميَّة لا يَمتُّ عملها بأي صلة بالأمن القومي)، وإنَّ الأمثلة على تخفيض مستوى حماية معلوماتٍ ما من الدرجة الثانية كثيرة جدًّا، ومنها رَفْع الحماية كليًّا عن كلمات السرّ الخاصَّة بصناديق البريد الإلكتروني بعد إغلاقها، وأرقام الحسابات المصرفيَّة بعد إقفالها، وهذا بلا شك بالنسبة إلى الأفراد، فمن المُلاحَظ أنَّ أمان المعلومات السابقة يَتكيَّف مع عامل الأحداث المحيطة، كإغلاق صناديق البريد الإلكتروني أو إقفال الحسابات المصرفيَّة، وأمّا بالنسبة إلى المنظَّمات، فمن أمثلة تخفيض مستوى حماية معلوماتٍ ما من الدرجة الثانية قيام مكتب حوالات ماليَّة برَفْع الحماية كليًّا عن المعلومات التي

تَتضمَّن قيمة مبلغ حوالة ماليَّة مرسَلة بعد تسلّمها من قِبَل صاحِبها، وهنا أمان معلومات القيمة الماليَّة للحوالة يَتكيَّف مع عامِلَي الزمن والأحداث المحيطة معًا (فإمّا أن تَمُر مدة زمنيَّة معيَّنة دون أن يَقوم صاحب الحوالة الماليَّة بتسلّمها، وعندئذٍ يَتم إرجاع قيمتها إلى الفرع الخاص بالبلد المرسِل، أو أن يَقَع حَدَث تسلّم الحوالة الماليَّة من قِبَل صاحِبها، وفي كلتا الحالتين تُصبِح معرفة قيمة الحوالة الماليَّة من قِبَل آخرين غير صاحِبها عديمة الفائدة)، ويَقوم كثير من مكاتب الحوالات الماليَّة بإخفاء تفاصيل قيمة الحوالة الماليَّة ومرسِلها عن جميع الأشخاص باستثناء صاحِبها، والسبب كما يُعتَقَد، هو من أجل حماية صاحبها من قيام لصٍّ ما بالترصُّد له لسرقة حوالته الماليَّة بعد معرفته بقيمتها التي قد تَكون كبيرة بالنسبة إلى اللِّصّ (التي قيمتها بالنسبة إلى اللِّصّ تستحِق عناء التَّرصُّد لصاحِب الحوالة الماليَّة وسرقتها منه)، ومثال آخر عن تخفيض مستوى حماية معلوماتٍ ما من الدرجة الثانية بالنسبة إلى المنظَّمات هو رَفْع الحماية كليًّا عن جميع معلومات العمليات التجاريَّة أو الصناعيَّة لشركة ما بعد انتهاء عملها.

أمّا بالنسبة إلى رَفْع الحماية كليًّا عن معلومات مَحميَّة بالدرجة الأولى فمثاله المعلومات التي تَتضمَّن موعد بدء العمليات العسكريَّة لدولة ما ضد دولة أخرى، المصنَّفة من مستوى التصنيف (سري للغاية) أو (سرِّي جدًّا) تَكون في الأساس مَحميَّة بالدرجة الأولى؛ أي الحماية المطلَقة، ولكن في أثناء نُشوب الحرب وبعده تَفقد هذه المعلومات قيمتها المعنويَّة بشكل كامل، وعليه ليسَ بالضرورة إبقاؤها مصنَّفة سريَّة، ويُمكِن تَداولها.

يَعتمِد اختيار **إجراءات** حماية المعلومات في درجة الأمان المتكيِّف على مستوى الحماية الجديد المقرَّر للمعلومات بعد تغيير درجة أمانها، فإذا كانت المعلومات مَحميَّة بدرجة الأمان المطلَق، وتَمَّ تخفيض مستوى حمايتها لتُصبِح مَحميَّة بدرجة الأمان العادي، يَنبغي اعتماد إجراءات الحماية المتعارَفة في درجة الأمان العادي، وأمّا إذا كانت المعلومات مَحميَّة بدرجة الأمان العادي، وتمَّ رَفْع مستوى حمايتها لتُصبِح مَحميَّة

بدرجة الأمان المطلَق، يَنبغي عندها اعتماد إجراءات الحماية المخصَّصة للمعلومات ذات الحساسيَّة العالية جدًّا، أو المعلومات المصنَّفة سريَّة، ومن مستوى التصنيف (سرِّي جدًّا). وعند رَفْع الحماية كليًّا عن المعلومات (مهما كانت درجة أمانها السابق)، فيُمكِن عندها إلغاء إجراءات الحماية عنها.

### 3.4 الأمان وعلاقته بالتكلفة أو بالزمن

عَرَّف Bruce Schneier قاعدة عامَّة لقياس أمان المعلومات المعمَّاة بخوارزميَّة تعمية، تَستنِد إلى تكلفة كسر الخوارزميَّة والمدة الزمنيَّة المطلوبة لذلك، ويُمكِن تطبيق تِلْك القاعدة لقياس أمان المعلومات المَحميَّة مهما كانت قيمتها الماديَّة أو المعنويَّة أو المَجازيِّة، ومن هنا يُمكِن طَرْح مبدأ قياس أمان المعلومات استنادًا إلى عامِلَين اثنين هما: التكلفة الماليَّة والمدة الزمنيَّة، وهذا المبدأ هو (مبدأ الأمان بالتكلفة أو بالزمن).

يَنصُّ (مبدأ الأمان بالتكلفة أو بالزمن) على ما يأتي: إذا كانت التكلفة الماليَّة المطلوبة لاختراق أمان معلوماتٍ ما أكبر من القيمة الماليَّة الفعلية[1] لتِلْك المعلومات، فالمعلومات آمنة، وإذا كانت المدة الزمنيَّة المطلوبة لاختراق أمان معلوماتٍ ما أطول من المدة الزمنيَّة التي يَنبغي أن تَظل المعلومات في غضونها مَحميَّة، فالمعلومات آمنة، ويُرادِف مَعنى أن تَكون المعلومات آمنة في المبدأ السابق معنى أنَّ النظام الذي يَحتوي على تِلْك المعلومات آمن وحصين من جميع الهجمات التي يُمكِن أن تُشَنّ عليه، خاصةً إذا كان نظامًا حاسوبيًّا، وإنَّ الأساس في (مبدأ الأمان بالتكلفة أو بالزمن) هو المقارَنة بين طرفين في كل من الحالتين (**الأمان بالتكلفة**) و(**الأمان بالزمن**)، ففي حالة (الأمان بالتكلفة) عنصر المقارَنة هو المال، أمّا في حالة (الأمان بالزمن) فعنصر المقارَنة هو الزمن، وأمّا طَرفَا المقارَنة في الحالة الأولى فهما التكلفة الماليَّة لاختراق

(1) القيمة الماليَّة الفعليَّة للمعلومات هي القيمة الماليَّة الحقيقيَّة الآنيَّة لتِلْك المعلومات (أي قيمتها الماليَّة في وقتها).

أمان المعلومات والقيمة الماليَّة للمعلومات المَحميَّة، وطَرفَا المقارَنة في الحالة الثانية هما المدة الزمنيَّة لاختراق أمان المعلومات والمدَّة الزمنيَّة لإبقاء المعلومات مَحميَّة، وسوف نَتحدَّث عن كِلتا الحالتين (الأمان بالتكلفة) و(الأمان بالزمن) من المبدأ السابق بالتفصيل.

### 1.3.4 قياس الأمان بالتكلفة

تَعني هذه الحالة أنَّه إذا تَجاوزَت التكلفة الماليَّة لاختراق أمان معلوماتٍ ما القيمة الماليَّة الفعليَّة التي تَحمِلها تِلْك المعلومات، عندها يُمكِننا اعتبار تِلْك المعلومات آمنة من الناحية الاقتصادية، فكلَّما ازدادَت التكلفة الماليَّة المطلوبة لاختراق أمان المعلومات، ازدادَ أمان المعلومات، ومن المُمكِن أن يُوجَد أطراف قادرون على دفع تكاليف ماليَّة أكثر للوصول إلى المعلومات المَحميَّة، وتَعود مَهمَّة زيادة التكلفة الماليَّة لاختراق أمان معلوماتٍ ما إلى الطرف المالِك لتِلْك المعلومات، وتَتمثَّل مَهمَّته في تمديد مجال الأمان من خلال تعزيز إجراءات أمن المعلومات ورَفْع كفاءة أدوات حماية تِلْك المعلومات.

لا يَنطبِق قياس أمان المعلومات بالتكلفة إلا على المعلومات ذات القيمة الماديَّة، فالشركة التجاريَّة المتنافِسة مع شركة تجاريَّة أخرى تَستطيع أن تَدفَع أموالًا لقاء الوصول إلى معلومات ذات قيمة ماليَّة عالية بالنسبة إليها، إذا ارتَأتْ أنَّ مقدار الأموال المستعِدَّة لدَفْعها أقل من القيمة الماليَّة لتِلْك المعلومات، أمّا المعلومات ذات القيمة المعنويَّة، كالمعلومات المصنَّفة (سريَّة للغاية) أو (سرية جدًّا) لدى حكومات الدول (التي تَحمِل على سبيل المثال أهميَّة كبيرة على مستوى الدولة أو على المستوى الدولي)، فلا تَنطبِق عليها هذه الحالة، فمن المُمكِن أن تَقوم دولة ما (أو دول عدَّة مشارِكة) بدَفْع أموال كثيرة لقاء الحصول على معلومات مصنَّفة سريَّة لدولة أخرى، إلا إذا كانت هذه المعلومات

المصنَّفة سريَّة ذات طابع اقتصادي (كمشروعات تجاريَّة مستقبليَّة حكوميَّة) ومن غير المعقول إنفاق أموال لاختراق أمانها أكثر من قيمة تِلْك المعلومات[1].

### 2.3.4 قياس الأمان بالزمن

خلافًا للحالة السابقة المرتَبِطة بالمال، تَرتبِط هذه الحالة بالزمن، وتَعني أنَّه إذا كانت المدَّة الزمنيَّة المطلوبة لاختراق أمان معلوماتٍ ما أطول من المدة الزمنيَّة المطلوب أن تَبقى تِلْك المعلومات في غضونها مَحميَّة، عندها يُمكِننا اعتبار تِلْك المعلومات آمنة أمانًا كافيًا، فكلَّما طَالَت المدة الزمنيَّة المطلوبة لاختراق أمان المعلومات، ازدادَ أمان المعلومات.

يَنبغي أن يَتم تقدير المدة الزمنيَّة المطلوبة لاختراق أمان معلوماتٍ ما على نحوٍ مختلف من الجهتين: جهة الطرف المالِك للمعلومات، وجهة الطرف المخترِق، ويَجب على الطرف المالِك للمعلومات المَحميَّة أن يَضَع تَصوُّرًا يرى فيه أنَّ المدة الزمنيَّة التي ستَأْخُذ من وقت الطرف المخترِق للوصول إلى تِلْك المعلومات قصيرة، ويَنبغي للطرف المخترِق أن يَضَع تَصوُّرًا يرى فيه أنَّ المدة الزمنيَّة التي ستَأْخُذ من وقته لاختراق أمان تِلْك المعلومات طويلة؛ أي إن تقديرات المدة الزمنيَّة لاختراق أمان المعلومات لدى الجهتين هي التي تحدد أمان المعلومات في حالة (الأمان بالزمن).

يَنطبِق قياس أمان المعلومات بالزمن على المعلومات ذات القيمة الماديَّة والقيمة المعنويَّة والقيمة المَجازيَّة، وبالنسبة إلى المعلومات ذات القيمة الماديَّة، فمثلًا إذا كان الوقت الذي ستَستغرِقه شركة تجاريَّة ما لاختراق أمان معلومات ذات قيمة ماليَّة معتَبَرة من شركة تجاريَّة أخرى أطول من المدَّة الزمنيَّة المخطَّط أن تَظل المعلومات

---

(1) قد تَقوم دولة ما بدفع تكاليف ماليَّة ضخمة يَتجاوَز مقدارها قيمة المعلومات المصنَّفة سريَّة ذات الطابع الاقتصادي لدولة أخرى إذا كان هَدَف الأولى استثمار تِلْك المعلومات لتدمير اقتصاد الثانية.

في غضونها مَحميَّة، عندها ستَكون معلومات الشركة التجاريَّة الأخرى آمنة، أمّا إذا استطاعَت الشركة التجاريَّة الأولى الوصول إلى معلومات الشركة التجاريَّة الثانية في الوقت الذي تَكون فيه هذه المعلومات مَحميَّة، فعندها تَكون الشركة التجاريَّة الثانية قد تَكبَّدَت خسائر ماليَّة من جَرَّاء ذلك، وتَحصَل هذه المحاولات كثيرًا في عالَم الأعمال، وبالنسبة إلى المعلومات ذات القيمة المعنويَّة (كالمعلومات المصنَّفة سريَّة لدى كثير من الدول والمنظَّمات الدولية)، فيَنبغي للأطراف المالِكة لهذه المعلومات أن تَحميها لحين مرور زمن معيَّن أو وقوع حدثٍ ما، وأكبر مثال على هذا هو العبارة التي تَنصُّ على أن يَتم إلغاء تصنيف المعلومات على أنها سريَّة تلقائيًّا بعد مرور زمن معيَّن أو وقوع حدثٍ ما في الأمر التنفيذي ذي الرقم 13526 الذي أصدَرَه الرئيس الأمريكي عام 2009م، وأمّا بالنسبة إلى المعلومات ذات القيمة المَجازيَّة (مثل كلمات السرّ الخاصَّة بصناديق البريد الإلكتروني أو المذكِّرات الشخصيَّة)، فإذا كان مثلًا الوقت الذي سَيستَغرِقه طرفٌ ما محاولًا اختراق أمان كلمات السرّ الخاصَّة بصناديق البريد الإلكتروني لطرفٍ آخر أكبر من المدَّة الزمنيَّة المخطَّط أن تَبقى كلمات السرِّ مَحميَّة ودون تغيير، فعندها كلمات السرّ تِلْك آمنة.