الاتحاد الدولي للاتصالات

ITU-T تقرير تقني

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

(11 ديسمبر 2015)

معدات تكنولوجيا المعلومات والاتصالات المزيَّفة

ملخص

يُعرف التزييف على نطاق واسع باعتباره مشكلة اجتماعية واقتصادية كبيرة ومتفاقمة. ويوفر هذا التقرير التقني معلومات أساسية عن طبيعة القضايا المتعلقة بتزييف معدات تكنولوجيا المعلومات والاتصالات (ICT)، ويوفر استعراضاً للاتفاقيات الدولية التي تغطي هذا النوع من التعدي على حقوق الملكية الفكرية وأنشطة المنظمات في إنفاذ هذه الحقوق، ووصفاً لمجموعة من الوسائل لمكافحة التجارة في المنتجات المزيَّفة. وبالإضافة إلى ذلك، يرد في الملحق A عدد من المبادرات الوطنية والإقليمية لمكافحة تزييف الأجهزة المتنقلة.

كلمات أساسية

مزيَّف، دون المستوى المطلوب.

الرقم المرجعي

.QSTR-COUNTERFEIT

سجل التغيير

هذا هو الإصدار 2 من التقرير التقني لقطاع تقييس الاتصالات بشأن *"معدات تكنولوجيا المعلومات والاتصالات المزيَّفة"*، وقد تمت الموافقة عليه في اجتماع للجنة الدراسات 11 بقطاع تقييس الاتصالات، الذي عُقد في جنيف، في 2-11 ديسمبر 2015.

المحرر: كيث مينوارينغ — رقم الهاتف: +46 76 107 6877

UNIS — البريد الإلكتروني: keith.mainwaring@ukrainesystems.com

المحتويات

قائمة الأشكال

الصفحة

تقرير تقني لقطاع تقييس الاتصالات

معدات تكنولوجيا المعلومات والاتصالات المزيَّفة

ملخص

يُعرف التزييف على نطاق واسع باعتباره مشكلة اجتماعية واقتصادية كبيرة ومتفاقمة. ويوفر هذا التقرير التقني معلومات أساسية عن طبيعة القضايا المتعلقة بتزييف معدات تكنولوجيا المعلومات والاتصالات (ICT)، ويوفر استعراضاً للاتفاقيات الدولية التي تغطي هذا النوع من التعدي على حقوق الملكية الفكرية وأنشطة المنظمات في إنفاذ هذه الحقوق، ووصفاً لمجموعة من الوسائل لمكافحة التجارة في المنتجات المزيَّفة. وبالإضافة إلى ذلك، يرد في الملحق A عدد من المبادرات الوطنية والإقليمية لمكافحة تزييف الأجهزة المتنقلة.

1 مقدمة: تزييف المنتجات – مشكلة متفاقمة

رغم الصعوبة البالغة التي ينطوي عليها القياس، هناك أدلة متراكمة على أن توزيع المنتجات المزيَّفة يشكل مشكلة متنامية من حيث كمية المنتجات المتضررة ونطاقها على السواء. وفي عام 2008، نشرت منظمة التعاون والتنمية في الميدان الاقتصادي (OECD) [1] تقريراً يقدِّر، على أساس المضبوطات الجمركية، أن قيمة التجارة الدولية الإجمالية في السلع المزيَّفة والمقرصنة (دون احتساب المنتجات الرقمية أو تلك التي تُنتج وتستهلك محلياً) فاقت 200 مليار دولار أمريكي في عام 2005. وجرى تحديث هذا التقدير على أساس النمو في التجارة الدولية وتكوينها المتغير، من ما يزيد قليلاً عن 100 مليار دولار أمريكي في عام 2000 إلى 250 مليار دولار أمريكي في عام 2007، وهو ما يمثل 1,95% من التجارة العالمية [2]. وتشير بعض التقديرات إلى نسب أعلى من ذلك، إذ يقدر مكتب استخبارات التزييف بغرفة التجارة الدولية (ICC) أن التزييف يشكل 5-7% من التجارة العالمية بقيمة 600 مليار دولار أمريكي سنوياً [3].

وكان فريق مبادرة الأعمال لوقف التزييف والقرصنة بغرفة التجارة الدولية (BASCAP) كُلف بإجراء دراسة [4] قدمها إلى منظمة التعاون والتنمية في الميدان الاقتصادي (OECD) من أجل استكمال صورة الآثار الاقتصادية والاجتماعية للتزييف والقرصنة. ويقدر هذا التقرير إجمالي القيمة الاقتصادية العالمية للمنتجات المزيَّفة والمقرصنة بواقع 650 مليار دولار أمريكي سنوياً، تشكل منها التجارة الدولية أكثر من النصف (285 مليار دولار أمريكي إلى 360 مليار دولار أمريكي)، والإنتاج والاستهلاك المحلي بين 140 مليار دولار أمريكي و215 مليار دولار أمريكي، والمحتوى الرقمي (الموسيقى والأفلام والبرمجيات) ما بين 30 مليار دولار أمريكي و75 مليار دولار أمريكي. وبالإضافة إلى ذلك، تشير التقديرات إلى أن تكلفة التزييف والقرصنة على حكومات ومستهلكي بلدان مجموعة العشرين (G20) تزيد عن 125 مليار دولار أمريكي كل عام (بسبب عوامل مثل انخفاض عائدات الضرائب وزيادة الإنفاق على إنفاذ التدابير المضادة والرعاية الصحية) وتنطوي على خسارة ما يقرب من 2,5 مليون فرصة عمل محتملة.

وقد سجلت السلطات الجمركية الوطنية للاتحاد الأوروبي (EU) أن السلع المزيَّفة التي تدخل الاتحاد الأوروبي قد تضاعفت ثلاث مرات بين عامي 2005 و2010. وتظهر الإحصاءات التي نشرتها المفوضية الأوروبية في يوليو 2011 اتجاهاً تصاعدياً هائلاً في عدد الشحنات المشتبه في انتهاكها حقوق الملكية الفكرية (IPR). وسجلت سلطات الجمارك نحو 80 000 حالة في عام 2010، وهو رقم تضاعف تقريباً منذ عام 2009. وصودر أكثر من 103 ملايين من المنتجات المزيَّفة في الحدود الخارجية للاتحاد الأوروبي. http://trade.ec.europa.eu/doclib/docs/2012/january/tradoc_149003.pdf.

وتزيَّف مجموعة واسعة جداً من المنتجات تشمل المواد الغذائية والمشروبات والمنتجات الصيدلانية، والمكونات الكهربائية وقطع غيار السيارات وجميع أنماط المنتجات الاستهلاكية وحتى متجراً بكامله. ومكونات الحاسوب (الشاشات والغلاف والأقراص الصلبة)، ومعدات الحاسوب، والمسيّرات، وكاميرات شبكة الإنترنت، وأجهزة التحكم عن بُعد، والهواتف المتنقلة، وأجهزة التلفزيون (TV)، ومشغلات الأقراص المدمجة (CD) والقرص الرقمي متعدد الاستخدامات (DVD)، ومكبرات الصوت، والكاميرات، والمجموعات الرأسية، ومكيفات المنفذ التسلسلي العام (USB)، والبرمجيات، والشهادات، وعلامات وبيانات المصادقة (مثل بيانات الاستدلال الأحيائي)، كلها تزيَّف.

وبالإضافة إلى ذلك، استُخدمت شبكة الإنترنت على نحو متزايد للقرصنة الرقمية وكذلك كسوق للبضائع المزيَّفة. وتبدو شبكة الإنترنت جذابة لمن يبيع السلع المزيَّفة بفضل جميع العوامل التي تجعل من الإنترنت مورداً جذاباً لتجار التجزئة، وخاصةً لأولئك منهم الذين يستهدفون الأسواق التي يصغر فيها حجم التداول (الوصول إلى السوق العالمية، وسهولة إنشاء ونقل وإغلاق المواقع الإلكترونية التي يمكن جعلها تبدو جذابة ومقنعة جداً، ورخص إرسال البريد الإلكتروني) إلى جانب إمكانية إغفال هوية التاجر. ويصعِّب العدد الضخم للمواقع الإلكترونية كثيراً على أصحاب حقوق الملكية الفكرية ووكالات الإنفاذ، تحديد العمليات غير القانونية. وتُستخدم العروض المرسَلة عبر البريد الإلكتروني والتجارة الإلكترونية ومواقع المزادات كلها في مساعٍ لبيع السلع المزيَّفة.

وفيما يتعلق بصناعة تكنولوجيا المعلومات والاتصالات، قدر تقرير KPMG وAGMA أن 8% إلى 10% من جميع سلع صناعة تكنولوجيا المعلومات (IT) التي بيعت في جميع أنحاء العالم كانت مزيَّفة، وأدى التزييف إلى خسارة في الإيرادات بقيمة 100 مليار دولار أمريكي لصناعة تكنولوجيا المعلومات في عام 2007. وأجرت شركة هيوليت باكارد (Hewlett-Packard) وحدها أكثر من 4,620 تحقيقاً في 55 بلداً بين عامي 2005 و2009 أدت إلى مصادرة مواد طباعة مزيَّفة تبلغ قيمتها أكثر من 795 مليون أمريكي [6]. وشكلت الإلكترونيات الاستهلاكية 22% من مضبوطات الجمارك في الولايات المتحدة في عام 2011 حيث زادت قيمة السلع بنسبة 16% عن عام 2010. وحوالي ثلث البضائع في هذه الفئة كانت هواتف متنقلة [5].

وفي عام 2011، كانت هناك سوق عالمية مقدرة بواقع 250,4 مليون من الهواتف المتنقلة المزيَّفة. http://press.ihs.com/press-release/design-supply-chain/cellphone-gray-market-goes-legit-sales-continue-decline. وهذا يعادل حوالي 16% من 1,546 مليون جهاز بيع في عام 2011 [8]. وهذا التقدير لمدى تغلغل المنتجات المزيَّفة في سوق الهاتف المتنقل يماثل ما جاء في دراسة، عن التدويل وتجزئة سلاسل القيمة وأمن التوريد، أعدت في عام 2011 للمفوضية الأوروبية. وتفيد الدراسة بأن الهواتف المتنقلة المزيَّفة تشكل 15%-20% من السوق العالمية من حيث عدد الوحدات المبيعة وحوالي 9 مليارات دولار أمريكي من الإيرادات.

وبالإضافة إلى إنتاج الأجهزة المزيَّفة، يجري إدخال المكونات الإلكترونية المزيَّفة في سلاسل توريد المنتج الشرعية. واحتل استخدام المكونات الإلكترونية المزيَّفة في المعدات العسكرية الأمريكية عناوين الصحف في خريف عام 2011 عندما عُقدت جلسة استماع للجنة القوات المسلحة في مجلس الشيوخ بشأن المكونات الإلكترونية المزيَّفة في سلاسل التوريد لوزارة الدفاع [9]. وقدرت دراسة أجراها مكتب الصناعة والأمن بوزارة التجارة [10] أن هناك نحو 1 800 حالة من حالات إدخال المكونات الإلكترونية المزيَّفة في سلاسل التوريد في عقود وزارة الدفاع، بما يشمل أكثر من مليون مكون. وتبيَّن أيضاً أن عدد هذه الحوادث ارتفع من 3 868 في عام 2005 إلى 9 356 في عام 2008. ونتيجة لجلسة الاستماع هذه، صار قانون تخويل الدفاع الوطني لعام 2012 (NDAA) يتضمن إرشادات بشأن التعامل مع المكونات المزيَّفة، بما في ذلك إخضاع المكونات الإلكترونية المستوردة لعمليات تفتيش إضافية، ويحمِّل هذا القانون المقاولين المسؤولية الكاملة عن كشف المكونات المزوَّرة وتصحيح أي حالة تجد فيها مكونات مزوَّرة طريقها إلى داخل منتجات [11].

ووجدت دراسة لمنظمة التعاون والتنمية في الميدان الاقتصادي في عام 2008 أن معظم المنتجات المزيَّفة تنبع من بلد واحد في آسيا (بما يشكل نسبة 69,7% من مضبوطات المنتجات المزيَّفة).

ويسعى هذا التقرير التقني لتقديم معلومات أساسية عن مشكلة التزييف وكيف تجري معالجتها مع التركيز على تزييف معدات تكنولوجيا المعلومات والاتصالات، وعلى أدوات تكنولوجيا المعلومات والاتصالات التي يمكن استخدامها للتخفيف من هذه المشكلة.

وبالإضافة إلى الأجهزة المزيَّفة، هناك أيضاً مشكلة معدات وملحقات انتشار تكنولوجيا المعلومات والاتصالات التي توصف عادةً بأنها "دون المستوى المطلوب" أو "غير مخوَّلة". ورغم عدم وجود تعريف معياري عالمي لهذين المصطلحين، غالباً ما تَستخدم هذه الأجهزة مكونات رديئة، ولا تلتزم، في معظم الحالات، بالمتطلبات القانونية المرعية على الصعيد الوطني بشأن منح الشهادات للأجهزة المتنقلة والموافقة عليها وتوزيعها وبيعها. ولا تنطوي هذه الأجهزة، في كل حالة، على انتهاك لحقوق الملكية الفكرية للشركات المصنعة للأجهزة، وبالتالي فهي لا تندرج ضمن التعريف المقبول للأجهزة "المزيَّفة"؛ ومن ثم، فهي لا تندرج في نطاق هذا التقرير التقني، الذي يركز على الأجهزة المزيَّفة. أما الأجهزة "دون المستوى المطلوب" فهي تشكل وتستدعي مجموعة متميزة من المشاكل والعلاجات التي يتعين النظر فيها على حدة.

2 ما هو التزييف؟

يعرِّف اتفاق منظمة التجارة العالمية بشأن الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية (اتفاق تريبس (TRIPS)) السلع ذات العلامة التجارية المزيَّفة بأنها "أي سلع، بما في ذلك مواد التعبئة والتغليف، التي تحمل دون تخويل علامة تجارية تطابق علامة تجارية مسجلة حسب الأصول فيما يتعلق بتلك السلع، أو التي لا يمكن تمييزها في جوانبها الأساسية عن تلك العلامة التجارية، والتي تعتدي بذلك على حقوق صاحب العلامة التجارية المعنية وفقاً لقانون البلد المستورد"(الحاشية 14 من المادة 51). لذا لا يُستخدم مصطلح "المزيَّفة" في اتفاق TRIPS إلا في مجال العلامات التجارية. وهو يشير إلى السلع المتعدية المعرَّفة بعبارة أدق من الانتهاكات العادية للعلامات التجارية على أساس أن العلامة التجارية مطابقة للأصل أو يتعذر تمييزها أساساً عن الأصل. ولا يتطرق هذا النص إلى القصد من وراء استخدام العلامة التجارية المزيَّفة. بل إنه يعرِّف المنتج المزيَّف من حيث قربه من علامة تُستخدم لمنتج مسجَّل وينطبق على الحالات التي تتطابق فيها السلع مع تلك التي سُجلت لها العلامة التجارية. وفي الممارسة العملية، عادةً ما تشمل مثل هذه السلع المخالفة الحالات التي تُنسخ فيها علامة ما بحذافيرها، عمداً لإعطاء الانطباع بأنها تحدد هوية منتج حقيقي. ومن شأن ذلك عادةً أن يحمل في ثناياه نية الاحتيال لأن الخلط بين المنتج الأصلي والمنتج المقلَّد خلط متعمد.

وتعرِّف الحاشية نفسها في اتفاق TRIPS السلع المقرصنة ذات حقوق النسخ المسجلة بأنها "أي سلع تُصنع منها نسخ دون موافقة صاحب الحق أو الشخص المخول حسب الأصول من صاحب الحق في بلد الإنتاج، والتي تُصنع بشكل مباشر أو غير مباشر من سلعة قد يشكل صنع تلك النُسَخة منها انتهاكاً لحقوق النسخ أو لحق ذي صلة وفقاً لقانون البلد المستورد". وبالتالي يتصل مصطلح "القرصنة" بالتعدي على حق النسخ والحقوق المتعلقة به في اتفاق TRIPS.

3 تأثيرات معدات ومكونات تكنولوجيا المعلومات والاتصالات المزيَّفة

تنفرد معدات تكنولوجيا المعلومات والاتصالات المزيَّفة في تأثيراتها على المجتمع، بما قد يختلف عن أنواع أخرى من انتهاكات حقوق الملكية الفكرية. فالمنتجات المزيَّفة، على سبيل المثال، لا تُختبر رسمياً عادة، ولا تنال الموافقة أيضاً وفقاً لأي متطلبات تنظيمية مرعية. ويمكن أن يكون استخدام المنتجات المزيَّفة خطراً للغاية. فمثلاً، هناك تقارير عن وفيات بسبب انفجار البطاريات المزيَّفة، وحالات صعق كهربائي وحرائق ناجمة عن أجهزة شحن، وحالات موثقة لهذه الأجهزة التي تحتوي على مستويات عالية من المواد الخطرة مثل الرصاص والكادميوم.

وقد تضمن تقرير منظمة التعاون والتنمية في الميدان الاقتصادي لعام 2008 تقييمات للآثار الاجتماعية والاقتصادية والآثار المترتبة على أصحاب الحقوق والمستهلكين والحكومات:

- وبالنظر إلى الآثار الاجتماعية والاقتصادية، لعل للتزييف أثراً سلبياً على الابتكار، ومستويات الاستثمار الأجنبي المباشر والنمو في الاقتصاد ومستويات العمالة، ناهيك عن أنه قد يحول الموارد أيضاً إلى جيوب شبكات إجرامية منظمة.
- ويرجح أن يؤثر التزييف تأثيراً اقتصادياً على أصحاب الحقوق نظراً لإمكانية تضرر حجوم المبيعات والربع والأسعار، وقيمة العلامة التجارية وسمعتها، وتكاليف العمليات ونطاقها.
- وقد يجد المستهلكون أن جودة المنتجات المزيَّفة أدنى من المستوى المطلوب وقد يتعرضون أيضاً لمخاطر جسيمة تهدد الصحة والسلامة.
- ولن تجبي الحكومات القدر نفسه من الضرائب، وربما تواجه قضايا فساد وتحتاج أيضاً إلى إنفاق موارد إضافية في مكافحة أنشطة التزييف.

1.3 أمثلة معدات تكنولوجيا المعلومات والاتصالات المزيَّفة

فيما يلي أمثلة رئيسية على تأثير معدات تكنولوجيا المعلومات والاتصالات المزيَّفة:

1.1.3 الهواتف المتنقلة

تؤثر الهواتف المتنقلة وملحقاتها المزيَّفة سلباً على المجتمع بأمور عدة منها:[1]

- تخفيض جودة خدمات الاتصالات المتنقلة، مما يؤثر على الواقع الملموس لدى المستهلكين والشركات؛
- التسبب بمخاطر تهدد سلامة المستهلكين نتيجة لاستخدام مكونات أو مواد فاسدة أو غير ملائمة؛
- إثارة تهديدات متعلقة بالأمن السيبراني؛
- تعريض خصوصيات المستهلك لخطر الانتهاك؛
- إضعاف سلامة التداولات الرقمية؛
- التهرب من الضرائب والرسوم المعمول بها، وبالتالي التأثير سلباً على خزائن الضرائب الحكومية؛
- إلحاق الضرر بأكثر المستهلكين هشاشةً مالياً جراء التقصير عن توفير أي ضمانات للمستهلك، ناهيك عن انتهاك متطلبات قانون المستهلك؛
- التسبب بمخاطر تهدد البيئة وصحة المستهلك نتيجة لاستخدام المواد الخطرة في تصنيع هذه الأجهزة؛
- تسهيل تجارة المخدرات والإرهاب، وغيرها من الأنشطة الإجرامية المحلية والدولية؛
- التسبب في ضرر اقتصادي نظراً لتشوه السوق الناجم عن المنافسة غير المشروعة والممارسات الخادعة؛
- الإضرار بالعلامات التجارية للشركات التي تصنع المنتجات الأصلية.

وأكدت دراسة أجراها معهد نوكيا للتكنولوجيا (INdT)، وهو هيئة بحث وتطوير مستقلة مقرها في البرازيل، رداءة نوعية الهواتف المزيَّفة وأثرها السلبي المحتمل على المستهلكين وشركات الاتصالات والاقتصادات المحلية. وتناولت الدراسة 44 هاتفاً متنقلاً مزيَّفاً ودون المستوى المطلوب، وقارنتها مع المعدات الحقيقية المعترَف بها. وتظهر الدراسة أن الهواتف المزيَّفة فشلت في 26% من محاولات النداء وانقطعت 24% من المكالمات التي أجريت. وبالإضافة إلى ذلك، في الأماكن التي يمكن أن يعمل فيها هاتف أصلي تماماً، لا تصلح الهواتف المزيَّفة للاستعمال بسبب جودة إرسالها المتدنية بالمقارنةً مع الهواتف الأصلية. وكانت هناك أيضاً إشكالات في تسليم الخلية (القدرة على الحفاظ على المكالمة أثناء الانتقال بين الخلايا) حيث كان الوقت المستغرَق في التسليم أطول بنسبة 41% منه في الهواتف الأصلية وانقطعت 34% من المكالمات خلال التسليم. انظر الأشكال في الملحق 1 بنشرة منتدى مصنعي الأجهزة المتنقلة (MMF) المعنونة: المزيَّف/دون المستوى المطلوب - دليل موارد للحكومات. http://spotafakephone.com//docs/eng/MMF_CounterfeitPhones_EN.pdf.

وتشكل الهواتف المتنقلة المزيَّفة كذلك مخاطر لا يستهان بها على الصحة والسلامة. فقد تحتوي هذه الأجهزة على مستويات من المواد الكيميائية تتجاوز معايير السلامة وتكون لملمتها أصعب من خلال برامج إدارة النفايات الإلكترونية. ولذلك تأثير ملموس وخاصةً في البلدان النامية ذات القدرات المحدودة أو المعدومة بيئياً لإعادةً التدوير السليمة وذات الكميات الكبيرة من الأجهزة المتنقلة المزيَّفة. ومن شأن معالجة قضية الأجهزة المزيَّفة بتعطيلها أن يفاقم هذه المشكلة في البلدان النامية.

وتحتوي المنتجات المزيَّفة، بسبب سوء تجميعها واستخدامها مكونات رديئة النوعية، على مواد خطرة محظورة في العديد من البلدان في إطار تقييد المواد الخطرة (RoHS) أو ما يعادله من تشريعات وطنية.

[1] يستند التالي إلى نشرة منتدى مصنعي الأجهزة المتنقلة (MMF) بعنوان المزيَّف/دون المستوى المطلوب – دليل موارد للحكومات http://spotafakephone.com//docs/eng/MMF%5FCounterfeitPhones%5FEN%2Epdf.

وتوضح دراسة أخرى حديثة أجراها معهد نوكيا للتكنولوجيا في البرازيل (INdT) عن المواد الخطرة، الأخطار المحتملة المتأتية من الهواتف المزيَّفة. وعلى وجه التحديد، تمثَّل الهدف في تقييم ما إذا كانت الهواتف المزيَّفة ملتزمة بتقييد المواد الخطرة وتوجيه الاتحاد الأوروبي بشأن تقييد استخدام مواد خطرة معينة في المعدات الكهربائية والإلكترونية. ويقيد هذا التوجيه استخدام ست مواد خطرة في أنواع مختلفة من المعدات الكهربائية والإلكترونية.

وقد استخدمت الدراسة أسلوب الاختبار المعياري IEC 62321 [75] وشملت اختبار خمسة هواتف مزيَّفة و158 قطعة بما في ذلك أغطية وشاشات عرض ودارات متكاملة (IC) ولوحة مفاتيح وغيرها من مكونات الدارات المركَّبة على السطح (SMD). وكشفت دراسة INdT وجود اثنتين من المواد الخطرة (الرصاص والكادميوم) في كل من المكونات الداخلية والخارجية بتركيزات أعلى بكثير من الحد الأقصى للقيم التي يَسمح بها تقييد المواد الخطرة (RoHS). الشكل A: يوضح تحليل للمواد الكيميائية الخطرة، في نشرة منتدى مصنعي الأجهزة المتنقلة (MMF) بعنوان المزيَّف/دون المستوى المطلوب – دليل موارد للحكومات، http://spotafakephone.com//docs/eng/MMF_CounterfeitPhones_EN.pdf، المستوى المفرط للرصاص والكادميوم الذي وُجد في المكونات الداخلية والخارجية للهواتف المتنقلة التي اختُبرت. وقد أكدت دراسات أخرى أجريت في بلدان أخرى وجود مواد خطرة في الهواتف المتنقلة المزيَّفة. وأجرى مركز مواد تكنولوجيا الإلكترونيات (C-MET)، في حيدر أباد، الهند، دراسة لاختبار امتثال الهواتف المتنقلة المطروحة في السوق الهندية لتقييد المواد الخطرة. وفي هذه الدراسة، اختار المركز 15 طرازاً من الهواتف المتنقلة المتاحة على نطاق واسع للاختبار. واختيرت الهواتف بناءً على رواجها وتوفرها في السوق الهندية وأجريت الاختبارات أيضاً باستخدام إجراءات أسلوب IEC 62321 (2008).

وبيَّنت النتائج أن جميع الهواتف المتنقلة المزيَّفة تحتوي على نسب عالية ومقلقة من المواد الخطرة، وخصوصاً الرصاص (Pb). وفي بعض الحالات، كانت القيم أعلى بواقع 35-40 مرة من الحدود المقبولة عالمياً للرصاص. وكان العديد من المكونات الهامة مثل فتحة بطاقة الذاكرة وفتحة وحدة هوية المشترك (SIM) والكاميرا، وغيرها الواقعة على تماس مباشر مع المستهلكين، الأسوأ من حيث محتوى المواد الخطرة، مما يزيد بوضوح من المخاطر التي تهدد المستهلكين مقارنةً بما إذا كانت المكونات داخل الجهاز. وفي المقابل، تبين أن الهواتف المتنقلة المختبَرة ذات العلامات التجارية العالمية والأخرى المعروفة تقع ضمن حدود تقييد المواد الخطرة (RoHS) وأنها بالتالي آمنة لاستخدام المستهلك. ويلخص الشكل B في نشرة منتدى مصنعي الأجهزة المتنقلة (MMF) بعنوان المزيَّف/دون المستوى المطلوب - دليل موارد للحكومات، http://spotafakephone.com//docs/eng/MMF_CounterfeitPhones_EN.pdf، هذه الدراسة، في حين أن الشكل C في نشرة منتدى مصنعي الأجهزة المتنقلة (MMF) بعنوان المزيَّف/دون المستوى المطلوب - دليل موارد للحكومات http://spotafakephone.com//docs/eng/MMF_CounterfeitPhones_EN.pdf، يبين بصرياً المجالات التي عُثر فيها على تركيزات عالية من الرصاص.

وبالإضافة إلى ذلك، يمكن لاستخدام الهواتف ذات الأرقام الدولية لهوية المعدات المتنقلة (IMEI) المنسوخة/الوهمية/المفقودة أن تشكل تهديداً للأمن القومي والشخصي نظراً لصعوبة تتبعها على الشبكة.

وأخيراً، وكمثال على الإيرادات التي يمكن أن تُفقَد بسبب التجارة في الأجهزة المتنقلة المزيَّفة، تفيد هيئة مكافحة التزييف الكينية أن البلاد فقدت زهاء 38,5 مليون دولار أمريكي نتيجة لهذا الاتجار بالهواتف المتنقلة المزيَّفة [39]. وأسفر تركيب نظام المعلومات المؤتمت لتسجيل المطاريف المتنقلة في أوكرانيا (AISMTRU) في عام 2009 عن مبلغ إضافي قدره 500 مليون دولار أمريكي في الإيرادات بين عامي 2010 و2012 حُصِّل من دفع رسوم الاستيراد الجمركية على المطاريف المتنقلة. وقبل تنفيذ هذا النظام في عام 2009، لم تكن سوى 5%-7% من الأجهزة المتنقلة المستخدمة في أوكرانيا مستوردة قانونياً، في حين أن 92%–95% منها تُستورد قانونياً اليوم [40].

2.1.3 ملحقات ومكونات منتجات تكنولوجيا المعلومات والاتصالات

في كثير من الأحيان، تكون ملحقات منتجات تكنولوجيا المعلومات والاتصالات المبيعة هي المزيَّفة. وفي حالة الهواتف المتنقلة، فضلاً عن غيرها من منتجات تكنولوجيا المعلومات والاتصالات، الملحقات هي البطاريات وأجهزة الشحن وسماعات الرأس. أما في حالة الطابعات، فغالباً ما تكون خراطيش الحبر هي المزيَّفة. وفي حالة الكاميرات الرقمية، تتوفر العدسات المقلدة التي تركَّب بشكل صحيح في جسم الكاميرا بين ملحقات مقلدة أخرى مثل الكابلات وبطاقات الذاكرة. وتتوغل هذه المكونات المقلدة حتى

إلى مستوى شرائح الدارات المتكاملة. ويمكن للتبديل العرضي أو المتعمد بمكونات إلكترونية مقلدة أن يسبب مشاكل جمة للمستخدمين عند استخدامها في المعدات الطبية أو غيرها من منتجات تكنولوجيا المعلومات والاتصالات الحرجة من ناحية السلامة. وفي عام 2013، ضُبطت مستنسخات غير مخوَّلة عن قارئة بطاقات MIFARE دون تماس في مؤتمر CarteS في باريس http://www.mifare.net/files/6114/2295/3702/NXP_Whitepaper_Protect_your_reputation_with_genuine_MIFARE_products_2015.pdf.

ويثير انتشار البطاريات المزيَّفة على نطاق واسع في جميع أنحاء العالم، القلق بشكل خاص. فالبطاريات المزيَّفة هي المسؤولة عن عدد من الحرائق. وتتراوح أنواع البطاريات المزيَّفة بين بطاريات AA القلوية وبطاريات أيونات ليثيوم القابلة للشحن التي تُدمج في العديد من أنواع مختلفة من المنتجات، وأبرزها الهواتف المتنقلة.

وأُبلغ عن بطاريات مزيَّفة تسببت بوفيات. http://www.bloomberg.com/apps/news?pid=newsarchive&sid= aLWvmmrHx9F0. وفيما يتعلق بهذا التقرير، ذُكر أن البطاريات المزيَّفة تنتشر على نطاق واسع في المناطق الأكثر فقراً لأن نسبة استخدام الأجهزة اليدوية أعلى هناك؛ ومن ثم تدعو الحاجة لتبديل البطاريات بتواتر أعلى.

وقد وقعت حوادث مماثلة في مختلف بلدان العالم. وهناك قلق متزايد بشأن تسبب هذه البطاريات لإشكالات على متن الطائرات بعد وقوع عدد من الحوادث المبلغ عنها. ففي فبراير عام 2014، أعرب جيف ليتش من هيئة الطيران المدني في المملكة المتحدة عن القلق بشأن "البطاريات المقلدة الرخيصة المشتراة من مصادر مشبوهة على شبكة الإنترنت، لأنها بطاريات معرضة للخلل وما يرافقه من عواقب وخيمة" http://www.bbc.co.uk/news/business-25733346.

وفي عام 2004، في شهادته أمام لجنة السلطة القضائية في مجلس الشيوخ الأمريكي، أوضح ممثل شركة جيليت (Gillette) أنهم صادروا، خلال عملية امتدت لأسبوع واحد، مليون بطارية دوراسيل (Duracell) مقلدة بين العديد من المنتجات المزيَّفة الأخرى http://www.judiciary.senate.gov/meetings/counterfeiting-and-theft-of-tangible-intellectual-property-challenges-and-solutions و http://www.judiciary.senate.gov/imo/media/doc/Willard%20Testimony%20032304.pdf.

وتستدعي سماعات الرأس القلق لأن النوعية الرديئة لسماعات الرأس المزيَّفة لا تقتصر إمكانية ضررها على الأذنين فقط، بل إنها تنطوي على خطر اندلاع حريق أيضاً. وفي عام 2013، أفيد أن المسؤولين صادروا ما قيمته 15 مليون جنيه إسترليني من سماعات الرأس المقلدة http://www.express.co.uk/news/uk/387869/Designer-headphones-top-16m-deluge-of-fake-goods.

3.1.3 أجهزة اللاسلكي ذات الاتجاهين

حذرت شركة حلول موتورولا (Motorola Solutions Inc.) العملاء من شراء أجهزة اللاسلكي المزيَّفة ذات الاتجاهين التي عُثر عليها في فيتنام في عام 2013. فهي قد تشكل خطراً على المستخدمين. وهي ليست مجرد نسخ من تصاميم اللاسلكي ذي الاتجاهين لشركة موتورولا، بل إنها تستخدم أيضاً شعار وأرقام نماذج موتورولا دون تخويل مما يصعِّب على العملاء تمييزها http://uk.reuters.com/article/2013/07/09/motorola-solutions-idUSnBw085384a+100+BSW20130709.

4.1.3 الكاميرات الرقمية

الكاميرات الرقمية هي جزء من قائمة طويلة من منتجات تكنولوجيا المعلومات والاتصالات المعرضة للتزييف. وحالها حال المنتجات الأخرى، يصعب جداً تحديد هويتها. وفي بعض الأحيان، يوفر الباعة وتجار التجزئة والمستخدمون المتعاونون إرشادات لمساعدة المستهلكين في التعرف على المنتجات المزيَّفة http://www.ebay.co.uk/gds/How-to-Identify-a-Fake-Nikon-Camera-/10000000177984982/g.html. ويمكن أن تشتد المخاطر التي تهدد أمن وخصوصيات المستخدمين من الأجهزة المزيَّفة مثل كاميرات الويب. وليست برمجيات هذه المنتجات ذات نوعية رديئة أو فاسدة منذ البداية فحسب، بل إن المستخدم لن يحصل على أي تحديثات أمنية أو دعم فيما بعد، مما يجعلها عرضة للمخاطر السيبرانية.

5.1.3 الحواسيب الشخصية واللوحية

أدت شعبية أنواع معينة من الحواسيب الشخصية واللوحية إلى التزييف على نطاق واسع. وفي بعض الحالات، كانت هذه المنتجات في الواقع "شراك خُلَّبية" تخلو حتى من لوحة دارة إلكترونية. http://www.cnn.com/2013/03/22/tech/mobile/fake-ipads-walmart/. أما تلك المنتجات التي تتضمن إلكترونيات، فقد سبق أن ثُبتت فيها، في بعض الحالات، برمجيات خبيثة مدرَجة في إصدارات مزيَّفة من أنظمة التشغيل http://www.computerworld.com/s/article/9231277/Microsoft_finds_new_computers_in_China_preinstalled_with_malware.

6.1.3 ألعاب الأطفال الإلكترونية

في عام 2014، كانت معظم ألعاب الأطفال تحتوي على إلكترونيات من نوع ما. ومن وحدات تشغيل الألعاب وأجهزة الألعاب المحمولة باليد المقلدة، مروراً بألعاب صغار الأطفال المقلدة، فإنها جميعها تنطوي على إمكانية التسبب في الأذى الجسدي للأطفال. ومن أمثلة المخاطر التي تهدد السلامة وحدات التغذية الكهربائية غير المؤرَضة التي تشكل مخاطر الصعق بالكهرباء http://www.theguardian.com/money/2011/dec/07/christmas-shopping-counterfeit-toys.

4 اتفاقيات حقوق الملكية الفكرية (IPR)

هناك عدد من الاتفاقات والاتفاقيات الدولية التي تضع معايير جوهرية لحماية حقوق الملكية الفكرية بموجب القوانين الوطنية، وكذلك استثناءات وحدوداً يُسمح بها، وهي تحدد الإجراءات اللازمة التي تتعهد الحكومات الوطنية أن تتيحها لتمكين صاحب الحق من اتخاذ إجراءات فعالة ضد أي ارتكابات منتهِكة.

1.4 اتفاقية باريس لحماية الملكية الصناعية واتفاقية برن لحماية الأعمال الأدبية والفنية

تدير المنظمة العالمية للملكية الفكرية (WIPO) المعاهدات المتعددة الأطراف المتعلقة بالملكية الفكرية. والمعاهدات الأساسية في هذا المضمار هي اتفاقية باريس لحماية الملكية الصناعية واتفاقية برن لحماية الأعمال الأدبية والفنية.

وقد اختُتمت اتفاقية باريس في عام 1883 وروجعت لاحقاً في عدد من المناسبات. وهدفها هو حماية "براءات الاختراع ونماذج المنفعة والنماذج الصناعية والعلامات التجارية وعلامات الخدمة والأسماء التجارية وبيانات المصدر أو تسميات المنشأ، وقمع المنافسة غير المشروعة" [18]. وفيما يتعلق بالتزييف، تلزم هذه الاتفاقية الدول المتعاقدة على اتخاذ تدابير ضد "الاستعمال المباشر أو غير المباشر لبيان مخالف للحقيقة عن مصدر المنتجات أو عن شخصية المنتج أو الصانع أو التاجر".

2.4 الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية (TRIPS) لدى منظمة التجارة العالمية (WTO)

تدير منظمة التجارة العالمية (WTO) الاتفاق المتعلق بالجوانب المتصلة بالتجارة من حقوق الملكية الفكرية (TRIPS)، وهو الاتفاق الذي يحدد المعايير الدنيا التي يتعين على جميع أعضاء منظمة التجارة العالمية تطبيقها فيما يتعلق بحماية وإنفاذ حقوق الملكية الفكرية على نحو جوهري. وهكذا يُدخِل اتفاق TRIPS لأول مرة مجموعة شاملة من أحكام الإنفاذ في اتفاق متعدد الأطراف. وتتعين تسوية أي خلافات بين أعضاء منظمة التجارة العالمية في هذا الصدد في إطار التفاهم بشأن تسوية المنازعات في منظمة التجارة العالمية.

وهناك هدفان أساسيان لأحكام اتفاق TRIPS بشأن الإنفاذ، أي وضع وسائل فعّالة للإنفاذ في متناول أصحاب الحقوق، وضمان كون إجراءات الإنفاذ متوازنة ومتناسبة وغير معرقلة للتجارة المشروعة. وهي تنقسم إلى خمسة أقسام. فينص القسم الأول منها على الالتزامات العامة التي يتعين على جميع إجراءات الإنفاذ أن تفي بها. وهو يهدف بوضوح لضمان فعاليتها ومراعاة بعض المبادئ الأساسية للأصول القانونية. وتتناول الأقسام التالية الإجراءات المدنية والإدارية وسبل الانتصاف، والتدابير المؤقتة، ومتطلبات خاصةً تتعلق بالتدابير الحدودية والإجراءات الجنائية.

ويفرق الاتفاق بين أنشطة التعدي بوجه عام، والتي يجب أن تتاح حيالها الإجراءات المدنية أو الإدارية وسبل الانتصاف، وبين التزييف والقرصنة – وهي أكثر أشكال أنشطة التعدي سفوراً وفحشاً – والتي تُتخذ حيالها بعض الإجراءات وسبل الانتصاف الإضافية الإلزامية، وهي التدابير الحدودية والإجراءات الجنائية. ولهذا الغرض، تعرَّف السلع المزيَّفة باختصار على أنها السلع التي تنطوي على نسخ العلامات التجارية بحذافيرها، وتعرَّف السلع المقرصنة على أنها السلع التي تنتهك حق الاستنساخ بموجب حق النسخ أو حق ذي صلة.

وبالتفاصيل، تتمثل التزامات أعضاء منظمة التجارة العالمية في ما يلي:

(أ) الإجراءات المدنية والإدارية: يجب أن يكون صاحب الحق قادراً على بدء إجراءات مدنية أو قضائية أو، على أساس اختياري، إدارية ضد الجهة المتعدية على حقوق الملكية الفكرية. ويجب أن تكون تلك الإجراءات عادلة ومنصفة. وهناك قواعد معينة راسخة بشأن الأدلة. وعلاوةً على ذلك، يُطلب من الأعضاء تخويل السلطات القضائية بمنح ثلاثة أنواع من سبل الانتصاف وهي: الأوامر القضائية والتعويضات عن الأضرار وسبل الانتصاف الأخرى. وكجزء من الضمانات ضد الإساءة، تشمل الالتزامات أيضاً تعويض المدعى عليه حيثما يسيء صاحب الحق استخدام إجراءات الإنفاذ.

(ب) التدابير المؤقتة: تشكل الأوامر المؤقتة أداةً هامة لحين حل النزاع في محاكمة. لذلك، يجب أن تمتلك السلطات القضائية صلاحية الأمر بتنفيذ تدابير مؤقتة فورية وفعّالة لاتخاذ إجراءات ضد تعديات مزعومة. وتهدف هذه التدابير إلى منع وقوع تعدٍ على حقوق الملكية الفكرية والحفاظ على الأدلة ذات الصلة بشأن التعدي المزعوم. وكما هو الحال في أقسام أخرى بشأن الإنفاذ، ترد بعض المتطلبات الإجرائية والضمانات ضد إساءة استخدام إجراءات الإنفاذ.

(ج) التدابير الحدودية: تمكِّن صاحب الحق في الحصول على تعاون إدارات الجمارك لاعتراض السلع المخالفة على الحدود ومنع إطلاق هذه السلع في حيز التداول. وهي تدابير إلزامية فيما يتعلق بالعلامات التجارية المزيَّفة والسلع المقرصنة ذات حقوق النسخ؛ في حين يمكن للأعضاء أن يطبقوا هذه التدابير أيضاً في حالات التعدي الأخرى على حقوق الملكية الفكرية وحالات السلع المتعدية المعدة للتصدير والسلع العابرة والواردات قليلة الشأن والواردات الموازية. وتخضع التدابير الحدودية لمتطلبات إجرائية معينة وضمانات ضد الإساءة، على غرار تلك التي تطبَّق على التدابير المؤقتة. وفيما يتعلق بسبل الانتصاف، لا بد من تمكين السلطات المختصة من الأمر بإتلاف السلع المخالفة أو التخلص منها خارج القنوات التجارية.

(د) الإجراءات الجنائية: أن تكون هذه الإجراءات متاحة لمعالجة حالات تعمد تزييف علامة تجارية أو قرصنة حقوق نسخ على نطاق تجاري. أما تطبيقها على حالات أخرى من انتهاك حقوق الملكية الفكرية فهو اختياري. ومن حيث سبل الانتصاف، ينص الاتفاق على أن العقوبات يجب أن تتضمن السجن و/أو غرامات مالية، وأن تتضمن في الحالات المناسبة أيضاً ضبط السلع المخالفة والمواد والمعدات المستخدمة لإنتاجها، ومصادرتها وإتلافها.

وأما أقل البلدان نمواً الأعضاء في منظمة التجارة العالمية فهي تستفيد حالياً من ترتيبات انتقالية تعفيها من الالتزام بتطبيق معايير الحماية والإنفاذ التي وضعها اتفاق TRIPS بوجه عام حتى يوليو 2021، وكذلك من الامتثال لأحكام حماية وإنفاذ براءات الاختراع والبيانات غير المعلنة في القطاع الصيدلاني حتى يناير 2016. والهدف من ذلك، من بين أمور أخرى، هو تمكينها من إنشاء قاعدة تكنولوجية قادرة على البقاء.

5 إنفاذ حقوق الملكية الفكرية

على الرغم من قيام المعاهدات الدولية المتعلقة بحماية حقوق الملكية الفكرية منذ أكثر من قرن من الزمان، فإن المحافل الدولية لم تتطرق إلى الإنفاذ إلا في الآونة الأخيرة. ويعود ذلك إلى الأسس التي يقدمها اتفاق TRIPS وأيضاً إلى تزايد الآثار الاجتماعية والاقتصادية للتعديات على حقوق الملكية الفكرية. ويرد إنفاذ حقوق الملكية الفكرية الآن في جداول أعمال العديد من المنظمات الدولية، مثل المنظمة العالمية للملكية الفكرية (WIPO) ومنظمة الجمارك العالمية (WCO) والإنتربول، في الاتحاد الأوروبي والعديد من الدول.

1.5 المنظمة العالمية للملكية الفكرية (WIPO)

أنشأت المنظمة العالمية للملكية الفكرية (WIPO) لجنة استشارية بشأن الإنفاذ (ACE) في عام 2002 تهدف للتنسيق مع المنظمات الدولية الأخرى والقطاع الخاص لمكافحة التزييف والقرصنة. وهي توفر برامج تدريب ومساعدة تقنية.

وتتعاون المنظمة العالمية للملكية الفكرية أيضاً مع برنامج الأمم المتحدة للبيئة (UNEP) ومنظمات أخرى مثل لجنة الأمم المتحدة الاقتصادية والاجتماعية لآسيا والمحيط الهادئ (UNESCAP) من أجل التوعية بالتحدي المتمثل في إعادةً تدوير الكميات المتزايدة من المنتجات المزيَّفة والتخلص منها http://www.wipo.int/wipo_magazine/en/2012/06/article_0007.html
http://www.unep.org/ozonaction/News/Features/2012/SoutheastAsiaexploressynergies/tabid/104354/Default.aspx
.http://www.unescap.org/events/wipoescapunep-workshop-environmentally-safe-disposal-ip-infringing-goods

2.5 منظمة التجارة العالمية – المجلس المعني باتفاق TRIPS

إن المجلس المعني باتفاق TRIPS هو واحد من ثلاثة مجالس قطاعية تعمل في إطار المجلس العام لمنظمة التجارة العالمية. وهو مسؤول عن إدارة اتفاق TRIPS، وعلى وجه الخصوص، عن مراقبة عمل الاتفاق ووفاء الأعضاء بالتزاماتهم بموجب اتفاق TRIPS. ويعقد المجلس اجتماعات رسمية في جنيف ثلاث مرات في السنة، فضلاً عن اجتماعات غير رسمية حسب اللزوم. وتشكل هذه الاجتماعات منتدى للنقاش والتشاور بشأن أي مسألة تتعلق باتفاق TRIPS، وكذلك لتوضيح أحكام الاتفاق أو تفسيرها. وقد أُفردت جلسات مخصصة لمناقشة إنفاذ حقوق الملكية الفكرية في مجلس TRIPS في عدة مناسبات، كان آخرها في عام 2012.

3.5 مكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC)

إن مكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC) هو القيِّم على اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية التي تشكل منصة عالمية للتعاون في التصدي لجميع أشكال الجريمة المنظمة. وفي الوقت الراهن، تضم أطراف الاتفاقية 167 بلداً التزمت بمكافحة الجريمة المنظمة من خلال التعاون وضمان الهيكلة المناسبة للقوانين المحلية.

ويعقد المكتب اجتماعات نصف سنوية للأطراف في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية. وتجمع هذه الاجتماعات بين الحكومات من مختلف أنحاء العالم لتعزيز واستعراض تنفيذ الاتفاقية من أجل ضمان أفضل نُهُج معالجة الجريمة المنظمة عبر الوطنية. وعُقد الاجتماع الأخير في أكتوبر 2012.

وقد ركز مكتب الأمم المتحدة المعني بالمخدرات والجريمة على الربط بين التجارة في السلع المزيَّفة والجريمة المنظمة عبر الوطنية http://www.unodc.org/counterfeit/. وأطلق المكتب حملةً شعارها "مزيَّف: لا تشتري ما يدعم الجريمة المنظمة" في يناير 2014 لزيادة وعي المستهلكين بما قيمته 250 مليار دولار أمريكي في السنة من الاتجار غير المشروع في السلع المزيَّفة. وتقوم هذه الحملة بإعلام المستهلكين بأن شراء السلع المزيَّفة يمكن أن يموِّل الجماعات الإجرامية المنظمة، ويعرِّض صحة المستهلك وسلامته للخطر، ويذكي المخاوف الأخلاقية والبيئية الأخرى.

ويعمل المكتب أيضاً على التصدي لتدفق السلع غير المشروعة مثل المنتجات المزيَّفة والمخدرات عن طريق برامج المساعدة التقنية. وقد أطلق المكتب ومنظمة الجمارك العالمية برنامج مراقبة الحاويات (CCP) في عام 2006. وأدى هذا البرنامج إلى ضبط 487 حاوية من البضائع المزورة والمهربة إلى جانب 195 حاوية أخرى من المخدرات.

https://www.unodc.org/unodc/en/frontpage/2014/January/counterfeit-dont-buy-into-organized-crime---unodc-launches-new-outreach-campaign-on-250-billion-a-year-counterfeit-business.html.

https://www.unodc.org/unodc/en/frontpage/2012/July/criminals-rake-in-250-billion-per-year-in-counterfeit-goods-that-pose-health-security-risks-to-unsuspecting-public.html.

4.5 منظمة الجمارك العالمية (WCO)

إن منظمة الجمارك العالمية هي منظمة حكومية دولية تتألف من 179 إدارة جمركية توفر القيادة والتوجيه والدعم لأعضائها لتأمين وتسهيل التجارة المشروعة، وتحقيق الإيرادات، وحماية المجتمع وبناء القدرات. وبما أن إدارات الجمارك مسؤولة عن حماية الحدود الوطنية من التدفق غير المشروع للسلع المزيَّفة والمقرصنة تتولى منظمة الجمارك العالمية قيادة المباحثات بشأن الجهود العالمية لمكافحة هذه الجرائم. ويستلزم ذلك دعم الجهود المبذولة لمكافحة التزييف والقرصنة من خلال تحسين أساليب الإنفاذ وتعزيز تبادل المعلومات بين دوائر الجمارك وكذلك بين الجمارك والقطاع الخاص.

والاستحواذ على انتباه ضباط الجمارك ودوائر الصناعات في جميع أنحاء العالم وضمان يقظتها فيما يتعلق بالمنتجات المزيَّفة، يقع في صلب برنامج حقوق الملكية الفكرية والصحة والسلامة لدى منظمة الجمارك العالمية. وإذ تُعتبر حماية صحة المستهلك وسلامته أولوية رئيسية، تسعى منظمة الجمارك العالمية بهمة عالية في القيام بأنشطة واسعة لبناء القدرات وفي تطوير أدوات الإنفاذ المختلفة.

وإدراكاً منها لأهمية التعاون مع القطاع الخاص، تعمل منظمة الجمارك العالمية عن كثب مع أعضاء وجمعيات الأوساط الصناعية من أجل تقييم احتياجاتها والصعوبات التي تعترضها في التصدي لهذه الظاهرة. ودأبت منظمة الجمارك العالمية على دعوة أصحاب الحقوق للمشاركة في مختلف أنشطة مكافحة التزييف، مثل العمليات الميدانية والندوات الإقليمية أو الوطنية، وقد أعدت أداة على شبكة الإنترنت كصلة وصل إلكترونية مع عامة الناس (IPM)، بغية تسليح ضباط الجمارك بوسائل كشف المنتجات المزيَّفة والمقرصنة وللتواصل الآني مع الجهات الفاعلة الاقتصادية.

وتشكل العمليات واسعة النطاق جزءاً حيوياً من مبادرات مكافحة التزييف بمنظمة الجمارك العالمية حيث يرتفع مستوى الإنفاذ لدى العديد من إدارات الجمارك في وقت واحد بشأن السلع المزيَّفة، وذلك للوقوف على تأثير أنشطة التزييف العالمية كماً ونوعاً. ففي عام 2013 وحده، اعترضت إدارات الجمارك في عملية في المنطقة الإفريقية وعملية في منطقة أمريكا اللاتينية 1,1 مليار سلعة مزيَّفة.

وقد أعدت منظمة الجمارك العالمية أيضاً أداة كشف عالمية على شبكة الإنترنت، IPM، موجَّهة إلى ضباط الجمارك في الخطوط الأمامية لتسهيل التمييز بين المنتجات الأصلية والنسخ المقلَّدة. ومنذ إطلاقها في عام 2010، أصبحت أداة الكشف IPM مركز تواصل حقيقي بين ضباط الجمارك على أرض الواقع وبين القطاع الخاص من خلال السماح لهم بتبادل المعلومات الحاسمة آنياً من أجل اعتراض السلع المزيَّفة.

وبإطلاق أداة الكشف IPM المتنقلة مؤخراً، يمكن لضباط الجمارك الميدانيين الآن النفاذ إلى أداة الكشف IPM عبر أجهزتهم المتنقلة واستخراج جميع المعلومات ذات الصلة الواردة في قاعدة البيانات. ويوفر هذا الإصدار الجديد إمكانية استخدام الأجهزة المتنقلة لمسح شفرات الخطوط العمودية GS1 المعيارية في دوائر الصناعة والموجودة على الملايين من المنتجات، مما يسرِّع البحث في قاعدة بيانات المنتجات. وعلاوة على ذلك، فإن مسح شفرات الخطوط العمودية سيمكِّن التوصيل التلقائي بأي خدمات استيقان مرتبطة بالمنتج قيد التفتيش. وتدعى هذه الميزة الجديدة بأداة IPM الموصولة – وهي شبكة عالمية من مقدمي ميزات الأمان (SFP) مربوطة بينياً مع أداة IPM. وباتساع هذه الشبكة من مقدمي ميزات الأمان، يتنامى أيضاً عدد أصحاب الحقوق المنضمين إلى أداة IPM التي تحوي أكثر من 700 علامة تجارية حالياً في نظامها، وتغطي مجموعة واسعة من القطاعات الصناعية، من الأدوية والمواد الغذائية والمبيدات الحشرية، إلى السلع ذات المبيعات السريعة والسلع الكمالية [16].

5.5 الاتحاد الأوروبي

على مستوى الاتحاد الأوروبي، أجريت سلسلة من المشاورات العمومية منذ عام 2011 بخصوص التوجيه 2004/48/EC بشأن إنفاذ حقوق الملكية الفكرية. وقد اختتمت المشاورة العمومية الأخيرة بشأن كفاءة أنظمة الإنفاذ المدنية للملكية الفكرية للدول الأعضاء في الاتحاد الأوروبي في مارس 2013. وقد نشرت المفوضية الأوروبية ملخصاً للردود في يوليو 2013.

واعتمدت المفوضية في الأول من يوليو بياناً بعنوان "نحو توافق متجدد بشأن إنفاذ حقوق الملكية الفكرية: خطة عمل للاتحاد الأوروبي."

وتركز الإجراءات العشرة المدرجة في خطة العمل على انتهاكات النطاق التجاري (ما يعرف بنهج "تتبع الأموال") وتهدف إلى تحسين الوقاية وزيادة التعاون عبر الحدود بين الدول الأعضاء وتحديد أولويات سياسات إنفاذ الملكية الفكرية على أساس بيانات موضوعية.

وأنشئ المرصد الأوروبي الخاص بالتزييف والقرصنة في 2009 ككيان تابع للمفوضية الأوروبية. وقد أعادت اللائحة رقم 386/2012 للبرلمان الأوروبي الخاص بانتهاكات حقوق الملكية الفكرية، وأسندت ولايته بالكامل إلى مكتب تنسيق السوق الداخلية في 5 يونيو 2012. ويعمل المرصد كمنصة لأطراف من القطاعين العام والخاص تتيح لهم تبادل أفضل الممارسات والخبرات بشأن إنفاذ حقوق الملكية الفكرية وزيادة الوعي والتعاون في جمع ومراقبة البيانات.

وشجعت المفوضية الأوروبية مذكرة تفاهم على مستوى الاتحاد الأوروبي بشأن بيع السلع المزيفة عن طريق الإنترنت (MoU). وقد وقعت في مايو 2011 بين منصات الإنترنت ومالكي العلامات التجارية والرابطات التجارية. وقد وضعت المذكرة مدونة ممارسات بشأن مكافحة بيع السلع المزيفة عبر الإنترنت وعززت التعاون بين الموقعين.

الجمارك

لائحة المجلس رقم 1383/2003 بتاريخ 22 يوليو 2003 بشأن الإجراءات الجمركية حيال السلع المشتبه في انتهاكها بعض حقوق الملكية الفكرية، تمت الاستعاضة عنها باللائحة 608/2013.

6.5 الإنتربول

بادر الإنتربول، وهو منظمة الشرطة الدولية، مع 190 بلداً عضواً، إلى إنشاء فريق عمل يعنى بالجريمة ضد الملكية الفكرية في عام 2002. ويدعم هذا الفريق العمليات الإقليمية والعالمية لضبط السلع المزيَّفة، وتنظيم دورات تدريبية من خلال كلية المحققين الجنائيين (IIPCIC) وقد أعد قاعدة بيانات عن الجريمة الدولية ضد الملكية الفكرية.

7.5 لجنة الأمم المتحدة الاقتصادية لأوروبا (UNECE)

أنشأت فرقة عمل اللجنة الاقتصادية لأوروبا المعنية بالتعاون التنظيمي وسياسات التقييس (WP.6) فريقاً استشارياً بشأن مراقبة السوق (فريق MARS) يهدف إلى تشجيع الدول الأعضاء على تنسيق جهودها لاحتواء مشكلة السلع المزيَّفة. فأنتج التوصية M بشأن "استخدام البنية التحتية لمراقبة السوق كوسيلة مكملة لحماية المستهلكين والمستخدمين ضد تزييف السلع" [18].

8.5 المبادرات الوطنية (بعض الأمثلة)

1.8.5 فرنسا

CNAC (*Comité National Anti Contrefaçon*) هي اللجنة الوطنية الفرنسية لمكافحة التزييف http://www.industrie.gouv.fr/enjeux/pi/cnac.php، وINPI (*Institut National pour la Propriété Industrielle*) هو المعهد الوطني للملكية الصناعية http://www.inpi.fr/fr/accueil.html. وتشارك وزارة المالية (*Ministère de l'économie et des finances*) أيضاً في أنشطة مكافحة التزييف http://www.economie.gouv.fr/signature-deux-nouvelles-chartes-lutte-contre-contrefacon-sur-internet.

2.8.5 مكتب الملكية الفكرية في المملكة المتحدة

أنشأ مكتب الملكية الفكرية التابع للحكومة البريطانية فريق الجرائم ضد الملكية الفكرية في عام 2004. وهو يعد تقريراً سنوياً عن الجرائم ضد الملكية الفكرية وقد نشر أيضاً مجموعة أدوات عن سلسلة التوريد [19]. ويوجد لدى المملكة المتحدة أيضاً وزير للملكية الفكرية.

3.8.5 وكالة مكافحة التزييف في كينيا

أقر برلمان كينيا قانون مكافحة التزييف (رقم 13) في عام 2008. ويحظر هذا القانون التجارة في السلع المزيَّفة، وقد أنشأ أيضاً وكالة مكافحة التزييف [20].

4.8.5 اللجنة الأمريكية الصينية المشتركة للتجارة والتبادل التجاري

أنشأت الولايات المتحدة والصين لجنة مشتركة بشأن التجارة والتبادل التجاري. وفي جلسته الرابعة والعشرين في ديسمبر 2013، التزم الفريق الوطني الرائد في الصين، المعني بمكافحة التعدي على حقوق الملكية الفكرية وتصنيع وبيع السلع المزيَّفة ودون المستوى المطلوب، باعتماد خطة عمل في عام 2014 تتضمن رفع مستوى الوعي العام بهذا الصدد، ومتطلبات الامتثال لجميع القوانين واللوائح المتعلقة بإجراءات حماية وإنفاذ حقوق الملكية الفكرية www.commerce.gov/news/fact-sheets/2013/12/20/fact-sheet-24th-us-china-joint-commission-commerce-and-trade-fact-sheet.

6 منتديات مكافحة التزييف في دوائر الصناعة

ردت مؤسسات الأعمال على مشكلة التزييف بإنشاء منتديات لتمثل مصالحها. وتوفر هذه المنتديات معلومات عن حجم المشكلة، وتقترح سبلاً للتخفيف من آثار التزييف وللسعي لدى الحكومات والمنظمات الدولية كي تتخذ إجراءات لمكافحة التزييف.

1.6 غرفة التجارة الدولية (ICC)

تمثل غرفة التجارة الدولية منظمات الأعمال في العالم. وتضم عضويتها آلاف الشركات والجمعيات في حوالي 120 بلداً. وهي تنوب عن مؤسسات الأعمال في عرض الأمور أمام الحكومات والمنظمات الحكومية الدولية. وكانت غرفة التجارة الدولية تأسست في عام 1919 وأنشأت بنفسها محكمة التحكيم الدولية في عام 1923.

وأنشأت غرفة التجارة الدولية مكتب استخبارات التزييف في عام 1985، وأنشأت، في الآونة الأخيرة، فريق مبادرة الأعمال لوقف التزييف والقرصنة (BASCAP).

ويدير مكتب استخبارات التزييف بغرفة التجارة الدولية قاعدة بيانات دراسات الحالة، ويقدم أيضاً خدمات التحقيق.

وتابعت مبادرة الأعمال لوقف التزييف والقرصنة (BASCAP) دراسة الآثار الاقتصادية والاجتماعية للتزييف والقرصنة التي بدأتها منظمة التعاون والتنمية في الميدان الاقتصادي [4] وأعدت مركزاً لتبادل المعلومات يقدم معلومات حسب البلد [21] والقطاع [22]، وأيضاً معلومات عن حماية العلامة التجارية [23] ودلائل الاتصال في جميع أنحاء العالم [24].

وتنشر غرفة التجارة الدولية أيضاً خارطة طريق للملكية الفكرية [25].

2.6 التحالف الدولي لمكافحة التزييف (IACC)

تأسس التحالف الدولي لمكافحة التزييف [26] في عام 1979 وهو يضم أعضاء من جميع فروع الصناعات، ويسعى إلى مكافحة التزييف والقرصنة من خلال تعزيز لوائح مكافحة التزييف.

3.6 منتدى مصنعي أجهزة الاتصالات المتنقلة (MMF)

يدير منتدى مصنعي أجهزة الاتصالات المتنقلة موقعاً على شبكة الإنترنت (spotafakephone.com) يقدم معلومات عن المزيَّف من أجهزة الاتصالات المتنقلة والبطاريات.

4.6 الجمعية الدولية لتجار الخدمات والحاسوب وجمعية أمريكا الشمالية لتجار الاتصالات (AscdiNatd)

أعدت الجمعية الدولية لتجار الخدمات والحاسوب وجمعية أمريكا الشمالية لتجار الاتصالات برنامجاً لمكافحة التزييف يتضمن سياسة لمكافحة التزييف كي تعتمدها الشركات الأعضاء، وأعدت موارد معلومات عن المنتجات المزيَّفة، بما في ذلك معلومات من شركتي HP وCisco [27].

5.6 تحالف الحد من السوق الرمادية والسلع المزيَّفة (AGMA)

شكلت شركات 3Com وCisco Systems وHewlett-Packard وNortel وXerox تحالف الحد من السوق الرمادية والسلع المزيَّفة، بهدف مكافحة الاتجار في منتجات التكنولوجيا الراقية المزيَّفة.

6.6 فريق عمل مكافحة التزييف التابع للجمعية البريطانية لمصنعي المنتجات الكهربائية التقنية وما يتعلق بها (BEAMA)

إن الجمعية البريطانية لمصنعي المنتجات الكهربائية التقنية وما يتعلق بها (BEAMA) هي قاعدة معارف خبراء مستقلة ومنتدى للصناعة الكهربائية التقنية في المملكة المتحدة وسائر أوروبا. وهي تمثل أكثر من 300 شركة صناعية في القطاع الكهربائي التقني، وتتمتع بنفوذ كبير على الصعيد الدولي؛ وكذلك ضمن المملكة المتحدة في المجالات السياسية، ومجال التقييس والسياسة التجارية.

وقد شُكل فريق عمل مكافحة التزييف التابع للجمعية (ACWG) في عام 2000. وهو يهدف إلى اتخاذ إجراءات ضد الجهات المزوِّرة التي تصنِّع منتجات المنشآت الكهربائية المزيَّفة، والتجار الذين يقومون بتوزيعها في العديد من الأسواق العالمية، بما فيها تلك الموجودة في أوروبا والشرق الأوسط وإفريقيا. وفضلاً عن أعضاء في الجمعية، يضم فريق العمل في صفوفه العديد من الجمعيات الرائدة في الصناعة من قطاعات تقوم بأعمال التركيب والتوزيع والاختبار ومنح الشهادات وإنفاذ القانون. وقد حاز اعترافاً عالمياً بأعماله الاستباقية وهو يحظى بتعاون الجمعيات التجارية وهيئات إنفاذ القانون في جميع أنحاء العالم.

وقد أنشئت قاعدة بيانات المزورين للاستخدام في أوساط صناعة التركيبات الكهربائية، ويجري تمريرها إلى السلطات في جميع أنحاء العالم كي تتولى ملاحقتهم في الأسواق المحلية.

ويُعلَن عن أنشطة فريق العمل من خلال مقالات المجلات التجارية، والعروض، والمشاركات في المؤتمرات، وإنتاج الأدلة والملصقات، للتوعية بالنمو السريع لهذا التهديد الذي يُحتمل أن تطال أضراره سلامة المستهلك وسلامة الأعمال.

ويتولى فريق العمل مسؤولية إدارة مشاريع أعمال مكافحة التزييف، وجمع المعلومات عن قضايا حقوق الملكية الفكرية ونشرها، والاستجابة للجهات الحكومية وغيرها نيابة عن الجمعية. وهو يقدم المشورة والمعلومات أيضاً لأي شركة أو جمعية تعترضها مشكلة في قضايا حقوق الملكية الفكرية.

وتشمل الأنشطة الحالية مشاريع في الصين والإمارات العربية المتحدة والمملكة المتحدة ونيجيريا والعراق، بالإضافة إلى برامج رقابة شاملة عبر الإنترنت والموانئ.

وفي المملكة المتحدة، تعمل جمعية BEAMA مع العديد من الهيئات الرائدة في الصناعة لرفع مستوى الوعي ومحاربة المنتجات المزيَّفة وغير الملتزمة – وقد أُطلقت البوابة الإلكترونية للصناعة www.counterfeit-kills.co.uk خصيصاً لهذا الغرض.

7.6 تحالف إلكترونيات المملكة المتحدة (UKEA)

إن تحالف إلكترونيات المملكة المتحدة هو اتحاد الجمعيات التجارية في المملكة المتحدة التي تمثل قطاع الإلكترونيات. وهو يهدف إلى تنسيق مناقشة القضايا داخل القطاع والتواصل مع الحكومة. وقد أنشأ تحالف UKEA منتدى لمكافحة التزييف [28] ينشر معلومات عن مشكلة المكونات الإلكترونية المزيَّفة ومقدمي الحلول المحتملين والممارسات الفضلى في هذا الصدد.

8.6 فريق مكافحة التزييف (ACG)

فريق مكافحة التزييف هو جمعية تجارية بريطانية أنشئت في عام 1980 بأعضاء ينتمون بسوادهم الأعظم إلى صناعة السيارات، ولكنه يمثل الآن معظم قطاعات الصناعة.

9.6 اتحاد المصنعين *(Union des Fabricants)* – UNIFAB

اتحاد المصنعين هو منظمة فرنسية مخصصة لمكافحة التزييف عن طريق زيادة الوعي العام (من خلال افتتاح متحف التزييف بالإضافة إلى أنشطة أخرى)، وتقديم المعلومات للشركات وجماعات الضغط المناهضة للتزييف http://www.unifab.com/en/.

10.6 مبادرة تصنيع الإلكترونيات الدولية (iNEMI)

حددت مبادرة تصنيع الإلكترونيات الدولية مشروعاً بشأن "المكونات المزيَّفة – منهجية التقييم وإعداد المقاييس" http://thor.inemi.org/webdownload/projects/Miniaturization/Counterfeit_WhitePaper_110513.pdf.

7 تدابير مكافحة المعدات المزيَّفة

1.7 مقدمة

تمكن مكافحة معدات التزييف بوسم المنتجات بطريقة ما بحيث يتسنى الاستيقان منها من خلال التحكم بدقة في دورة حياة المنتَج. فيمكن إرفاق المنتجات بعلامات يصعب تزويرها وتخصيص المنتجات بأرقام تسلسلية يمكن استخدامها للاستيقان من أصالة منتَج (عن طريق النفاذ إلى قاعدة بيانات، على سبيل المثال).

ويمكن أن تخصَّص معرفات تنفرد بها فرادى المنتجات. ومن أمثلة الأنظمة المستخدَمة لمكافحة التزييف نظام mPedigree الذي يُستخدم لمواجهة التزييف الصيدلاني في إفريقيا. إذ يسمح هذا النظام للمستهلكين من التحقق ما إذا كانت الأدوية أصلية أو مزيَّفة وربما خطرة عن طريق إرسال رسالة (مجانية) عبر خدمة الرسائل القصيرة (SMS) إلى سجل المنتجات الصيدلانية.

وتلزم رقابة صارمة على سلاسل التوريد، وربما على كامل دورات حياة المنتَج، مع الاختبار والتقييم ومنح الشهادات حسب الضرورة لضمان أمن المنتج والمحافظة على الجودة المناسبة. وبالإضافة إلى ذلك، يحتاج مسؤولو الجمارك للتزود بالأدوات اللازمة لتحديد المنتجات المزيَّفة، ويجوز استخدام آليات مراقبة السوق.

ويمكن وضع معرفات على منتَج في نص واضح أو يمكن تشفيرها على "وسم التعرف (ID)" مثل شفرة الخطوط العمودية أو وسم التعرف بواسطة الترددات الراديوية (RFID) أو البطاقة الذكية أو وسم بالأشعة تحت الحمراء، بحيث تمكن قراءتها تلقائياً. ويمكن تمييز ثلاثة مستويات في التعرف على منتَج. فهناك أولاً مستوى المعرِّف البحت الذي يُخص فيه كل منتَج بالتعريف، عن طريق شفرة المنتج الإلكترونية (EPC) على سبيل المثال. أما المستوى الثاني فهو مستوى التشفير حيث يمكن تشفير المعرِّفات البحتة في أنساق مختلفة، وأخيراً هناك التنفيذ المادي، عند كتابة الهوية المشفَّرة على وسم RFID، على سبيل المثال.

ولضمان أن يُخَّص كل منتج بمعرف ينفرد به على مستوى العالم في تطبيقات محددة، يجب أن تدار المعرفات بطريقة منظمة، وبشكل ما من إجراء التوزيع. فعلى سبيل المثال، تدير جمعية النظام العالمي للاتصالات المتنقلة (GSMA) هويات المعدات المتنقلة الدولية (IMEI) لأجهزة النظام العالمي للاتصالات المتنقلة (GSM) ونظام الاتصالات المتنقلة العالمي (UMTS) والتطور الطويل الأمد (LTE)؛ وتوزع جمعية صناعة الاتصالات معرفات المعدات المتنقلة (MEID) على أجهزة النفاذ المتعدد بتقسيم شفري (CDMA)، وتدير منظمة المعايير الدولية، GS1، معرفات شفرة الخطوط العمودية. فيما تدير المنظمة الدولية لتوحيد المقاييس (ISO) عدداً من ميادين المعرفات وتعمل أيضاً بمثابة سلطة رفيعة المستوى تضم مخططات معرفات منظمات أخرى مثل GS1.

وثمة مثال آخر في وسم المعدات لبيان الموافقة على تسويقها داخل بلد ما. على سبيل المثال، تتطلب الوكالة الوطنية البرازيلية للاتصالات (ANATEL) أن تحمل أجهزة شحن الهاتف المتنقل وبطارياته وسماً مُحْكَماً يحدده قرارها 2007/481[2]. انظر الشكل 1.

الشكل 1 – مثال الوسم المُحْكَم الذي تتطلبه الوكالة الوطنية البرازيلية للاتصالات (ANATEL) والمحدد بقرارها 2007/481

استُخدم هذا النهج في صناعة معدات الاتصالات لسنوات عديدة ونفذته بعض البلدان/المناطق بنجاح[3] (مثل اللجنة الفيدرالية للاتصالات (FCC)[4]، والوكالة الوطنية البرازيلية للاتصالات (ANATEL)[5]، والاتحاد الأوروبي (EU)[6]).

ويتعين على مسؤولي الجمارك أن يتمكنوا من التعرف على المنتجات المزيَّفة ومراقبة السوق وإعمال تدابير الإنفاذ الأخرى التي قد تُستخدم. وبالإضافة إلى ذلك، يمكن تحديد المستوردين ذوي السوابق في تجاهل ضوابط الاستيراد ووضعهم على قائمة خاصةً. وعندما يستورد المستوردون المتسيِّبون شحنات معدات تكنولوجيا المعلومات والاتصالات، يمكن إخطار السلطات التنظيمية بحيث يتسنى اتخاذ قرار للقيام بعمليات تفتيش، وينبغي بعد ذلك أن يكون الإنفاذ مسوَّغاً. انظر الشكل 2.

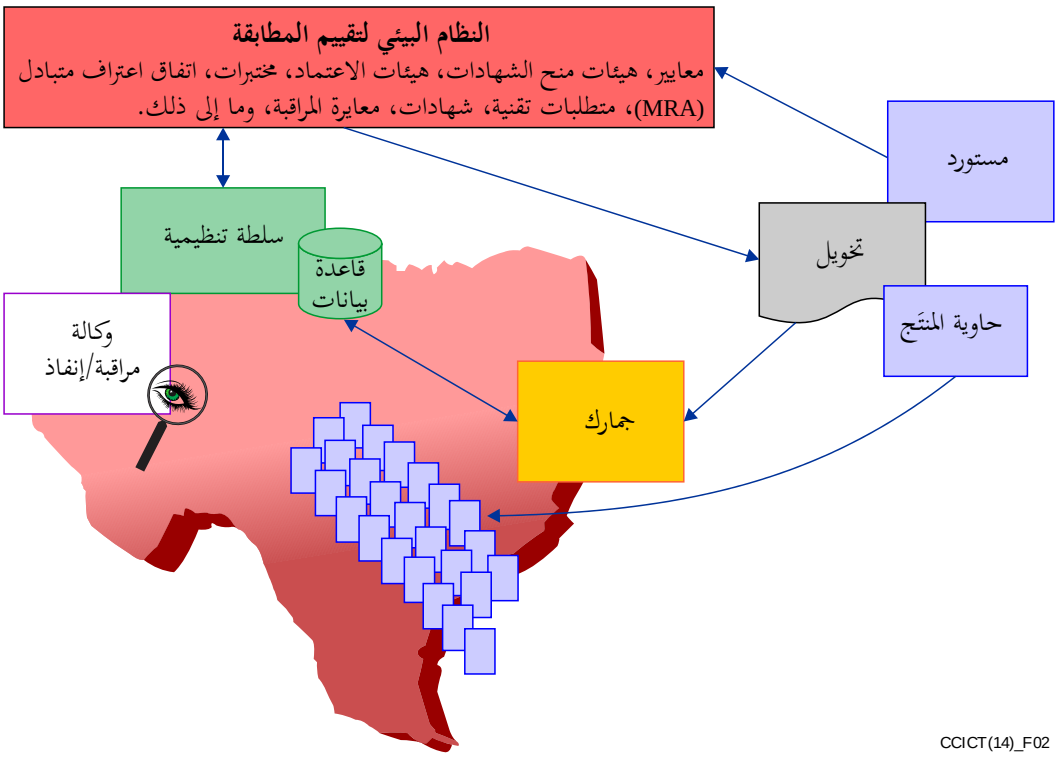
2 https://translate.google.com/translate?sl=pt&tl=en&js=y&prev=_t&hl=fr&ie=UTF-8&u=legislacao.anatel.gov.br%2Fresolu%C3%A7%C3%B5es%2F2007%2F192-resolu%C3%A7%C3%A3o-481&edit-text=.

3 باستخدام نظام ما لتقييم المطابقة قد يتطلب إصدار شهادة و/أو إعلان المطابقة و/أو الاستفادة من استخدام اتفاقات الاعتراف المتبادل (MRA).

4 https://apps.fcc.gov/oetcf/kdb/forms/FTSSearchResultPage.cfm?id=30744&switch=P.

5 http://www.anatel.gov.br/grandeseventos/en/frequently-asked-questions-faqs.

6 http://exporthelp.europa.eu/thdapp/display.htm?page=rt%2frt_TechnicalRequirements.html&docType=main&languageId=en.



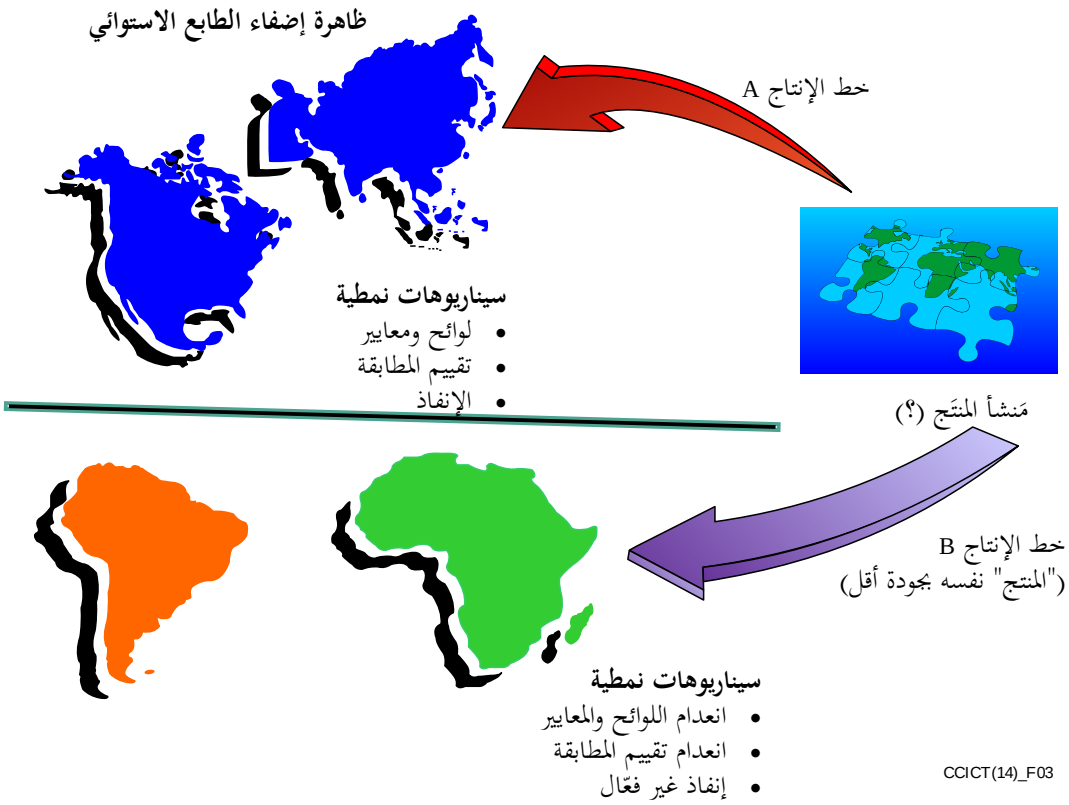
الشكل 2 – النظام البيئي لتقييم المطابقة

من الجدير بالذكر أن المنتجات المزيَّفة يمكن أن تلتزم في الواقع بمتطلبات محددة، وأن تعمل بينياً مع منتجات أصلية، وتجتاز بالتالي اختبار المطابقة وقابلية التشغيل البيني. وعلى هذا النحو، قد يلزم تقييم صاحب العلامة التجارية للمنتج لتحديد المنتجات المزيَّفة بدقة وتمييزها عن المنتجات الأصلية.

ويتميز قطاع تكنولوجيا المعلومات والاتصالات بحضور كبير للمتنافسين الدوليين الذين يعززون الابتكار المستمر. ورغم كون هذا الوضع مستحسناً، يَدخل إلى هذا السوق، في الوقت نفسه، مصنّعون/بائعون لا يلتزمون باتباع القواعد الدولية أو الإقليمية أو الوطنية.

وتكون مشكلة تفاوت الاطلاع على المعلومات أكثر وضوحاً في البلدان النامية، حيث يقل أو ينعدم أي تطوير للتكنولوجيات ولإجراءات تقييم المطابقة. وتتمثل المشاكل النمطية، التي تصادَف عادةً عند إدارة نظام تقييم المطابقة، في نقص المعلومات الموثوقة التي يمكن تقصيها، كما في الحالات التالية: '1' تحديد منشأ المنتجات أو الوكيل المسؤول عنها من الناحية القانونية؛ '2' مواقع منشآت التصنيع؛ '3' جهات منح الشهادات؛ '4' مختبرات مؤهلة حائزة شهادة اعتماد ذات صفة شرعية. وفي بعض الحالات، يمكن لمستوردين، دون أي معرفة وقدرة تقنية تؤهلهم لتقديم المساعدة، أن يمثلوا شركات أجنبية أوكلت وحدات الهندسة والتصنيع لديها إلى جهات خارجية مرتحلة إلى بلدان أخرى (ومثال ذلك مخططات الاستعانة بمصادر خارجية). وعلى الرغم من أن مثل هذه العمليات قد تمثل وفورات في عملية الإنتاج، فإنها تضعف الجودة والمساءلة في تصنيع معدات الاتصالات/تكنولوجيا المعلومات والاتصالات.

ويمكن القول كذلك إن المعدات منخفضة الجودة هي حصيلة المآرب الخاصةً و/أو الجشع و/أو الطلب الاستهلاكي و/أو انعدام المعايير و/أو هزالة الإنفاذ. وفي بعض الحالات، يؤدي غياب عملية المطابقة المناسبة في سوق مستهدف محدد إلى تركيب وبيع نفس العلامة التجارية أو الطراز بمكونات إلكترونية مختلفة، بعضها جيد وبعضها سيئ، ويُشحن هذا المنتج إلى مقاصد مختارة وفقاً لتهاونها النسبي بشأن الجودة. ويتبادر إلى الذهن إجراء يعرف باسم tropicalização (أي إضفاء الطابع الاستوائي، باللغة البرتغالية) كمثال على هذا العبث بالمعدات المخصصة للبيع جنوب خط الاستواء. انظر الشكل 3.



الشكل 3 – الإجراء المعروف باسم tropicalização (أي إضفاء الطابع الاستوائي، باللغة البرتغالية)

2.7 إساءة استخدام المعرفات وشعارات اعتماد النوع

إن جميع المعرفات التي تستحدثها الشركات المصنعة الأصلية للسلع يمكن أن يسيء المزورون استخدامها من أجل تحقيق أهدافهم في إيهام المستهلكين والسلطات بأن منتجهم أصلي. وهذه مشكلة تصادَف في العديد من الصناعات، وليست حكراً على تكنولوجيا المعلومات والاتصالات. وينبغي أن يضع القارئ في الاعتبار أن أي آلية تُعرف وما يحيط بها من إجراءات أمنية ستصبح هدفاً للمزورين والمجرمين. وكثيراً ما تخرَّب شعارات وأيقونات اعتماد النوع وكذلك معرفاته الإلكترونية على نحو متعمد للتهرب من تفتيش الجمارك وسلطات إنفاذ القانون عند الحدود. ويخلق ذلك إشكالات عملية للمصنعين والمستهلكين والجمارك وموظفي إنفاذ القانون الذين يصعب عليهم تمييز العلامات المعرِّفة المقلَّدة عن الأصلية، حتى قبل النظر في المنتج نفسه.

3.7 الهوية الدولية للمعدات المتنقلة (IMEI)

كما سبق الذكر، كانت الهواتف المتنقلة هدفاً جذاباً بشكل خاص للمزورين، ورداً على ذلك، أنشأ منتدى مصنعي الأجهزة المتنقلة (MMF) موقعاً على شبكة الإنترنت لتزويد المستهلكين بمعلومات عن كيفية اكتشاف الهواتف والبطاريات المزيَّفة. http://spotafakephone.com. ونصح بالتعرف على مظهر المواد الأصلية وقدراتها وتوفرها وأسعارها وأيضاً التحقق من رقم الهوية الدولية للمعدات المتنقلة (IMEI). فرقم IMEI هو معرف متفرِّد لكل هاتف متنقل وفي كثير من الأحيان لا تمتلك المنتجات المزيَّفة رقم IMEI أو تمتلك أرقاماً وهمية. ومن المشاكل التي تعترض المصنعين ومشغلي الشبكات والسلطات هي أن المزورين قد طوروا تصنيعهم بحيث يسرقون أحياناً مديات أرقام مشروعة من الشركات المصنعة القائمة كجزء من استراتيجيتهم للتزييف. ويمكن اللجوء إلى ذلك كأسلوب للتهرب من أنظمة فحص الهويات الدولية للمعدات المتنقلة.

وتدير جمعية النظام العالمي للاتصالات المتنقلة (GSMA) هويات المعدات المتنقلة الدولية (IMEI) لضمان تفرُّد هذه الهويات. ومخطط التوزيع تراتبي حيث تخصص جمعية النظام العالمي للاتصالات المتنقلة (GSMA) معرفات بخانتين رقميتين لهيئات الإبلاغ التي توزع بعدئذ الهوية الدولية للمعدات المتنقلة (IMEI) والرقم التسلسلي للمعدات. وفيما يلي هيئات الإبلاغ المخولة حالياً بتوزيع هويات المعدات المتنقلة الدولية: CTIA – الجمعية اللاسلكية، وBABT (مجلس الموافقات البريطاني للاتصالات)، وTAF (منتدى اختبار واعتماد مطراف الاتصالات اللاسلكية) (الصين)، وMSAI (تحالف معايير الأجهزة المتنقلة في الهند).

ويمكن الاطلاع في الشكل 4 على الهوية الدولية للمعدات المتنقلة (IMEI) سارية المفعول اعتباراً من 1 يناير 2003، على النحو التالي [37]:

شفرة توزيع النمط (TAC)	الرقم التسلسلي	الخانة الرقمية للتدقيق
NNXXXX YY	**ZZZZZZ**	**A**

TAC	شفرة توزيع النمط، المعروفة سابقاً باسم شفرة اعتماد النوع.
NN	معرف هيئة الإبلاغ.
XXXXYY	المعرِّف الذي تحدده هيئة الإبلاغ لنمط المعدات المتنقلة (ME).
ZZZZZZ	توزعها هيئة الإبلاغ ولكن الجهة المصنِّعة تخصصها لكل جهاز متنقل.
A	الخانة الرقمية للتدقيق المحدَدة كدالة لجميع الخانات الرقمية الأخرى للهوية الدولية للمعدات المتنقلة.

الشكل 4 – نسق الهوية الدولية للمعدات المتنقلة (IMEI)

تسجل جمعية النظام العالمي للاتصالات المتنقلة (GSMA) معلومات إضافية مثل اسم المصنِّع ورقم الطراز والقدرات التقنية، كالنطاقات الترددية المدعومة وفئة القدرة، لكل جهاز معرَّف بهويتها الدولية للمعدات المتنقلة.

وتدير جمعية النظام العالمي للاتصالات المتنقلة (GSMA) قاعدة بيانات الهوية الدولية للمعدات المتنقلة (IMEI DB) [38]، المعروفة سابقاً باسم السجل المركزي لهوية المعدات (CEIR). وتتضمن قاعدة بيانات الهوية الدولية للمعدات المتنقلة "قائمة بيضاء" بالمعدات التي تعتبر مناسبة للاستخدام في جميع أنحاء العالم، و"قائمة سوداء" بالهويات الدولية للمعدات المتنقلة المتعلقة بالأجهزة التي لا تعتبر مناسبة للاستخدام بسبب تعرضها للضياع أو السرقة أو الأعطال مما يشكل تهديداً لسلامة الشبكة. وتجدر الإشارة إلى أن هذه القائمة البيضاء هي قائمة بشفرات توزيع النمط (TAC) وليست بكامل الهويات الدولية للمعدات المتنقلة (IMEI)، وتتوفر البيانات مجاناً إلى الأطراف المؤهلة بما فيها الهيئات التنظيمية الوطنية ووكالات إنفاذ القانون ووكالات الجمارك. وبالإضافة إلى قاعدة بيانات الهوية الدولية للمعدات المتنقلة، يمكن لفرادى مشغلي الشبكات أن ينفذوا سجلاتهم الخاصةً بهوية المعدات (EIR)، وأن يحمِّلوا عليها "القائمة البيضاء"، بما يسمح للمشغلين بالسيطرة على ماهية الأجهزة التي يمكنها النفاذ إلى شبكاتهم http://www.gsma.com/managedservices/mobile-equipment-identity/the-imei-database/accessing-the-imei-database.

ويتمثل الاستخدام الرئيسي لقاعدة بيانات الهوية الدولية للمعدات المتنقلة (IMEI DB) في قدرة المشغلين على التعرف على ما يُستخدم عبر شبكاتهم من أجهزة وخصائصها، وعلى حجب الأجهزة اليدوية المسروقة. ويمكن أيضاً استخدام قاعدة بيانات الهوية الدولية للمعدات المتنقلة من أجل كشف الأجهزة المزيَّفة، مما يساعد في منع تصريف هذه الأجهزة وردع الجريمة ودعم الملاحقات القضائية.

ولكن كانت هناك مشاكل في تنفيذ الهوية الدولية للمعدات المتنقلة (IMEI). وقد أُبلغ عن حالات معدات بدون أي هوية IMEI، وأخرى ذات هوية IMEI بخانات رقمية صفرية بالكامل، وأخرى ذات هويات IMEI مكررة وأخرى ذات هويات IMEI وزعتها منظمات غير مخوَّلة. وكان بعض هذه الأجهزة ذات هويات IMEI غير الصالحة أو غير المتفرِّدة مزيَّفاً فيما كان البعض الآخر منها أصلياً ولكنه غير ملتزم بإجراءات توزيع هويات IMEI لدى جمعية النظام العالمي للاتصالات المتنقلة بسبب سوء الفهم من جانب الشركات المصنعة. فعلى سبيل المثال، أشارت تقديرات إلى وجود 30 مليون من أجهزة النظام العالمي للاتصالات المتنقلة (GSM)

في الهند بدون أي هوية IMEI، وقد خولت جمعية النظام العالمي للاتصالات المتنقلة (GSMA) تحالف معايير الأجهزة المتنقلة في الهند (MSAI) بتقديم برنامج عفو مؤقت ينطوي على غرس هويات IMEI أصلية (برنامج غرس هويات IMEI الأصلية (GII)) من أجل التمكن من التعرف على كل جهاز على حدة.

وكمثال على هويات IMEI المكررة، كُشف النقاب في أستراليا عن 6 500 جهاز يدوي يحمل رقم الهوية الدولية للمعدات المتنقلة (IMEI) 135790246811220. أما بالنسبة لهويات IMEI غير المسجلة، فقد أفاد مشغِّل شبكة في أوغندا أن عدداً ما يوجد على شبكته من شفرات توزيع النمط (TAC) غير المسجلة في قاعدة بيانات الهوية الدولية للمعدات المتنقلة (IMEI DB) يفوق العدد الذي وزعته جمعية النظام العالمي للاتصالات المتنقلة (GSMA) والمسجل في قاعدة البيانات تلك.

ولذلك هناك سبب وجيه يدعو لضمان التفويض باستخدام الهوية الدولية للمعدات المتنقلة (IMEI) وتوزيع هذه الهويات وفقاً لإجراءات جمعية النظام العالمي للاتصالات المتنقلة (GSMA). وقاعدة بيانات الهوية الدولية للمعدات المتنقلة (IMEI DB) هي إحدى أدوات كشف الهواتف المتنقلة المزيَّفة. وللاستشهاد بمثال واحد في هذا الصدد، حظرت كينيا النفاذ على الهواتف المتنقلة ذات هويات IMEI غير الصالحة اعتباراً من نهاية سبتمبر 2012 حيث كانت التقديرات تشير إلى أن 2,3 مليون مشترك يستخدمون أجهزة يدوية مقلدة هناك. وترد في الملحق A معلومات أوفى بشأن هذه الأمثلة والحالات الأخرى التي استخدمت هويات IMEI كأساس لتحديد الهواتف المتنقلة المزيَّفة. وبما أن العديد من الجهود الوطنية الرامية إلى معالجة قضية الأجهزة المتنقلة المزيَّفة تعتمد على استخدام الهوية الدولية للمعدات المتنقلة، تقتضي الضرورة أن تكون إجراءات وقاعدة بيانات الهوية الدولية للمعدات المتنقلة مؤمَّنة وموثوقة، وأن تكون هذه الهوية مشفرَّة على نحو آمن ضمن الأجهزة.

ومن الخيارات إلزام المشغلين بحجب الأجهزة ذات هويات IMEI المكررة وغير الصالحة لأن هذه الأجهزة يجب أن يُستيقن منها على الشبكة كي تعمل. ولعل حجب هذه الأجهزة عند أول توصيل لها هو الوسيلة الأكثر فعالية لمعالجة هذه المشكلة في هذا الوقت.

بيد أن حجب هويات IMEI دونه العديد من العوائق. فأولاً لا تحتفظ جمعية النظام العالمي للاتصالات المتنقلة (GSMA) بقائمة بيضاء كاملة بهويات IMEI بل بمجرد قائمة بيضاء بشفرات توزيع النمط (TAC). وثانياً، استُنسخت هويات IMEI من أجهزة مشروعة في أجهزة مزيَّفة وأخرى دون المستوى المطلوب مما يعقد عملية الحجب. وأخيراً، لا بد لأي حل حاجب أن يمنع أو يحظر نسخ هويات IMEI مستنسَخة أخرى إلى الأجهزة المعنية.

وفي حين أن الحجب تكتنفه تحديات، تتوفر حلول في السوق. وفي الوقت نفسه، من المهم تجنب خليط ترقيعي من حلول يُنفرَد بها على الصعيد الوطني فتدفع المشكلة ببساطة عبر الحدود الوطنية. وبالنظر إلى أن جمعية النظام العالمي للاتصالات المتنقلة (GSMA) توزع هويات IMEI وتدير قاعدة بيانات هذه الهويات، يبدو من المنطقي أنها ينبغي أن تشارك بطريقة ما في المبادرات الوطنية من أجل الاستفادة من كامل مجموعة القوائم المتاحة والتدابير التقنية الأخرى.

ولكن بالنظر إلى العدد الهائل المقدر للأجهزة المزيَّفة، فإن مجرد حجب المطاريف العاملة من شأنه أن يؤثر تأثيراً شديد الوطأة وغير متوقع على الشبكات والمستخدمين النهائيين. وهذه حقيقة لا يمكن تجاهلها.

وفي هذا الصدد، من المهم أن تؤخذ في الاعتبار حقيقة أن الهواتف المتنقلة، في البلدان النامية ذات الظروف الاجتماعية والاقتصادية المعسرة، هي البوابة الرئيسية للتواصل والمشاركة في مجتمع المعلومات[7]. وللأسف، يجري ذلك باستخدام عدد كبير من الأجهزة المزيَّفة الأرخص ثمناً.

ولهذا السبب، يتعين أن يكون المجتمع بأسره جاهزاً لمثل هذا التغيير. ويجب أن تُدرس النُهُج الفضلى، وأن تؤخذ بعين الاعتبار ويُخطَط لها. فعلى سبيل المثال، يجب أن توضَّح للمستهلكين دوافع عدم السماح بالأجهزة المزيَّفة (من المخاطر التي تهدد السلامة، إلى تدني جودة الخدمة وبالتالي زيادة الشكاوى، إلى مخاطر التداخل، والتعدي على حقوق الملكية الفكرية، وما إلى ذلك).

[7] مبادرة الاتحاد الدولي للاتصالات بشأن تمكين التنمية بواسطة الاتصالات المتنقلة: http://www.itu.int/en/ITU-D/Initiatives/m-Powering/Pages/default.aspx.

وبهذا المعنى، إذا اختارت الهيئات التنظيمية والحكومات أن تضع إجراءات حجب مطاريف في حيز النفاذ، من المهم اعتماد سياسات انتقالية، مثل البدء بحجب المطاريف الجديدة فقط، والسماح للأجهزة الموجودة بالفعل على الشبكة بمواصلة العمل، ولكن سيتعين على المستخدمين، في نهاية المطاف، الانتقال إلى مطاريف أصلية لأن دورة الحياة المقدرة لمطراف متنقل هي 18 شهراً.[8]

4.7 المعرفات المتفرِّدة

كان مركز الهويات التلقائية الذي أنشئ في عام 1999 في معهد ماساتشوستس للتكنولوجيا أول من أعد شفرات المنتج الإلكترونية (EPC) التي تديرها اليوم منظمة EPCglobal التابعة لمنظمة GS1 التي حددت المواصفات الأكثر استخداماً على نطاق واسع لأنظمة سلسلة التوريد العالمية. وكذلك حددت المنظمة الدولية لتوحيد المقاييس (ISO) ومركز الهويات في كل مكان (Ubiquitous ID Centre) (اليابان) معرفات لعدد من التطبيقات.

وتحدد منظمة GS1 تسعة "مفاتيح تحديد هوية" للتعرف على البنود والمواقع وحاويات الشحن والأصول والخدمات وأنماط الوثائق والشحنات والإرساليات، على النحو التالي:

- GTIN – رقم بند التجارة العالمي
- GLN – رقم موقع عالمي
- SSCC – الشفرة التسلسلية لحاوية الشحن
- GRAI – المعرف العالمي للأصل القابل للإرجاع
- GIAI – المعرف العالمي للأصل الفردي
- GSRN – الرقم العالمي للعلاقة الخدمية
- GDTI – المعرف العالمي لنمط الوثيقة
- GSIN – الرقم العالمي لهوية الشحنة
- GINC – الرقم العالمي لهوية الإرسالية

ويُستخدم المفتاح GTIN لتحديد فئات الأشياء في حين تحدد المفاتيح GLN وSSCC وGIAI وGSRN فرادى الأشياء؛ ويمكن استخدام المفتاحين GRAI وGDTI لتحديد إما فئات الأشياء أو فرادى البنود تبعاً لغياب أو وجود رقم تسلسلي. ويحدد المفتاحان GINC وGSIN التصنيفات المنطقية بدلاً من الأشياء المادية. وقد أُعدت مفاتيح تحديد الهوية هذه كي تنفَّذ باستخدام شفرات الخطوط العمودية. وتتوازى هذه الشفرات مع شفرات المنتج الإلكترونية (EPCs) التي حددتها منظمة EPCglobal للاستخدام مع التعرف بواسطة الترددات الراديوية (RFID). فيوسَّع مفتاح GTIN في مخطط شفرة EPC بإضافة رقم تسلسلي لتحديد شيء ما دوناً عن غيره. وتمتلك المفاتيح الأخرى التي تستخدم لتحديد فرادى الأشياء مكافئات مباشرة في شفرة EPC. وتعرَّف شفرات المنتج الإلكترونية (EPCs) التالية [41]:

- معرِّف عام (GID)
  - urn:epc:id:gid:*ManagerNumber.ObjectClass.SerialNumber*
- رقم بند التجارة العالمي المسلسل (SGTIN)
  - urn:epc:id:sgtin:*CompanyPrefix.ItemReference.SerialNumber*
- الشفرة التسلسلية لحاوية الشحن (SSCC)
  - urn:epc:id:sscc:*CompanyPrefix.SerialReference*
- رقم الموقع العالمي مع توسعة أو بدونها (SGLN)

8 http://www3.epa.gov/epawaste/education/quest/pdfs/unit1/chap2/u1-2_product-life.pdf: "تُستخدم الهواتف الخلوية لفترة وسطية مدتها 18 شهراً قبل تبديلها – حتى وإن كانت قادرة على العمل لفترة أطول بكثير".

- urn:epc:id:sgln:*CompanyPrefix.LocationReference.Extension*
- المعرف العالمي للأصل القابل للإرجاع (GRAI)
  - urn:epc:id:grai:*CompanyPrefix.AssetType.SerialNumber*
- المعرف العالمي للأصل الفردي (GIAI)
  - urn:epc:id:giai:*CompanyPrefix.IndividulAssetReference*
- المعرف العالمي لنمط الوثيقة (GDTI)
  - urn:epc:id:gdti:*CompanyPrefix.DocumentType.SerialNumber*
- الرقم العالمي للعلاقة الخدمية (GSRN)
  - urn:epc:id:gsrn:*CompanyPrefix.ServiceReference*
- وزارة الدفاع الأمريكية (DoD)
  - urn:epc:id:usdod:*CAGEOrDODAAC.SerialNumber*
- معرف الفضاء الجوي والدفاع (ADI)
  - urn:epc:id:adi:*CAGEOrDODAAC.OriginalPartNumber.Serial*

ويحدد المرجع ISO/IEC 15459 [42] معرفات متفرِّدة لتتبع سلسلة التوريد يمكن تمثيلها في وسائط التعرف التلقائي ونقل البيانات (AIDC) مثل شفرة الخطوط العمودية والتعرف بواسطة الترددات الراديوية (RFID).

وتحدد الأجزاء 1 و4 و5 و6 و8 من المرجع ISO/IEC 15459 سلسلةً متفرِّدة من الحروف للتعرف على وحدات النقل، وفرادى البنود، ووحدات النقل القابلة للإرجاع، وتصنيفات المنتجات ووحدات النقل، على التوالي. وفي كل حالة، يهيكَل المعرف المتفرِّد ضمن طبقات لتسهيل الإدارة الفعالة لمعرفات تلك الفئة من الأشياء.

ويحدد الجزء 2 المتطلبات الإجرائية لتوزيع معرفات متفرِّدة على تطبيقات إدارة البند ويصف التزامات سلطة التسجيل ووكالات الإصدار. ولا تنطبق هذه الإجراءات على البنود التي سبق للمنظمة الدولية لتوحيد المقاييس (ISO) أن عينت لها وكالات صيانة أو سلطات تسجيل لتوفر مخططات تعرف. وبالتالي فإنها لا تنطبق على:

- حاويات الشحن، لأن تشفيرها المتفرد موصَّف في المرجع ISO 6346 [43]؛
- المركبات، لأن تشفيرها المتفرد موصَّف في المرجع ISO 3779 [44]؛
- أجهزة لاسلكي السيارات، لأن تشفيرها المتفرد موصَّف في المرجع ISO 10486 [45]؛
- ومخططا ISBN [46] وISSN [47].

ويحدد الجزء 3 القواعد المشتركة التي تنطبق على معرفات متفرِّدة لإدارة البند والمطلوبة لضمان التوافق التام في جميع فئات المعرفات المتفرِّدة.

وكُلفت اللجنة التقنية 246 لدى المنظمة الدولية لتوحيد المقاييس (ISO) بإنتاج أدوات معيارية لمكافحة التزييف. وتقوم هذه اللجنة بإعداد معيار لمقاييس أداء حلول الاستيقان من أجل مكافحة إنتاج السلع المزيَّفة [48].

وبالإضافة إلى المنظمة الدولية لتوحيد المقاييس ومنظمة EPCglobal، حدد مركز الهويات في كل مكان الياباني معرفاً عاماً يسمى "ucode" [49]، لا يقتصر القصد منه على التعرف على الأشياء المادية بل يمكن أن يُستخدم أيضاً لتحديد الأماكن والمعلومات الرقمية، انظر الشكل 5. ويبلغ طول شفرات ucode الأساسية 128 بتة (ولكن تمكن توسعتها بمضاعفات 128 بتة)، ويمكن تضمينها معرفات أخرى مثل أرقام ISBN، أو عناوين بروتوكول الإنترنت (IP) أو أرقام الهاتف وفق التوصية ITU-T E.164 [76]. وشفرة ucode هي في الأساس رقم يتعين إسناد معنى له في قاعدة بيانات علائقية. ويمكن لأي فرد أو منظمة الحصول على شفرات ucode من مركز الهويات في كل مكان (Ubiquitous ID Centre) الذي يعمل كسلطة تسجيل لهذه الأرقام.

نسخة (4 بتات)	TLDc (16 بتة)	cc (4 بتات)	SLDc (متغيرة)	ic (متغيرة)
TLDc: شفرة الميدان ذات المستوى الأعلى (التي يخصصها مركز الهويات في كل مكان) cc: شفرة الصنف (مبينة الحدود بين SLDC وic) SLDc: شفرة الميدان ذات المستوى الثاني ic: شفرة التعرف لفرادى الأشياء				

الشكل 5 – نسق ucode

ويعمل قطاع تقييس الاتصالات على أنظمة للنفاذ إلى معلومات الوسائط المتعددة انطلاقاً من التعرف على الأشياء على أساس الوسم. وكجزء من هذا العمل، يجري إعداد وصف لمخططات الهوية المختلفة التي يمكن استخدامها لهذا التعرف. وقدم مركز الهويات في كل مكان (Ubiquitous ID Centre) مخطط ucode بحيث يخصَّص لشفرة ucode معرف كائن (OID) مسجل تحت الفرع {joint-iso-itu-t(2) tag-based(27)} امتثالاً للتوصية ITU-T X.668 [50]. ويخصَّص لما سبق وصفه من مخطط الهوية المتفرِّدة لدى المنظمة الدولية لتوحيد المقاييس (ISO)/اللجنة الكهرتقنية الدولية (IEC) معرف كائن تحت الفرع {iso(1)} في شجرة معرفات الكائن. ويؤدي ذلك إلى تخصيص معرفات كائن لمخططات المعرف في المنظمة الدولية لتوحيد المقاييس (ISO)/اللجنة الكهرتقنية الدولية (IEC) (بما في ذلك منظمة EPCglobal) وفي مركز الهويات في كل مكان، إما تحت فرع **{iso}** (ISO وEPCglobal) أو فرع **{joint-iso-itu-t}** (مركز الهويات في كل مكان) بما يسمح بتعايش مخططات تعرُّف مختلفة لها سلطات تسجيل مختلفة. وبالنسبة إلى وسوم التعرف بواسطة الترددات الراديوية (RFID)، يجري تشفير معرف الكائن (OID) والهوية على النحو المحدد في المرجع ISO/IEC 15962 [77].

ملاحظة – لا يُستخدم مصطلح "كائن" في "معرف كائن" هنا للإشارة إلى "شيء" بشكل عام، بل يُستخدم وفقاً للتعريف الوارد في المرجع ISO/IEC 15961 [78] على أنه: "معلومة أو تعريف أو توصيف معرَّف جيداً ويتطلب اسماً من أجل تحديد استخدامه في آلة اتصالات افتراضية". ومعرف الكائن يحدد مثل هذا الكائن بشكل لا لبس فيه. وتنظَّم معرفات الكائن تراتبياً حيث تبين جذور الشجرة أو "الأقواس" العليا، التنظيم المسؤول عن تعريف المعلومات. وتمثل الأقواس العليا قطاع تقييس الاتصالات (ITU-T) والمنظمة الدولية لتوحيد المقاييس (ISO)، وقطاع تقييس الاتصالات والمنظمة الدولية لتوحيد المقاييس مشتركين معاً. وتُسنَد إليها القيم الرقمية 0 و1 و2 على التوالي. وتُسنَد إلى القوس "القائم على الوسم" في الشجرة المشتركة لقطاع تقييس الاتصالات والمنظمة الدولية لتوحيد المقاييس، القيمة الرقمية 27.

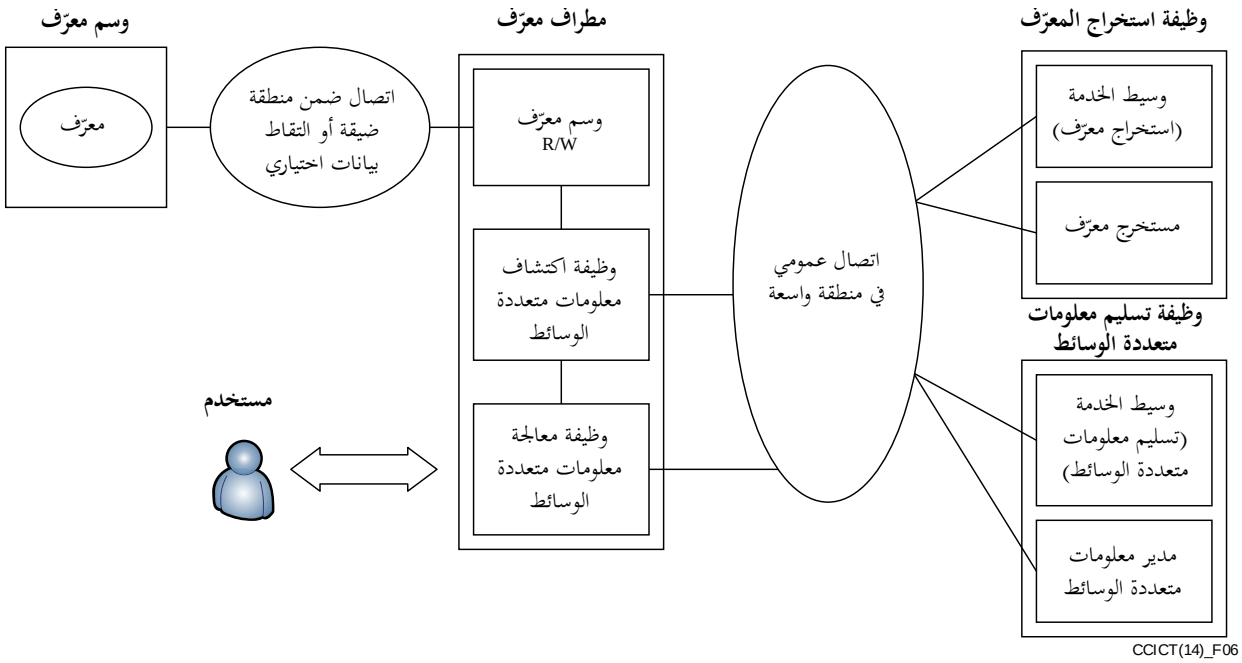
ويمكن تخزين البيانات المرتبطة بكائن في وسم إلى جانب المعرف، إذا امتلك الوسم ذاكرة كافية. غير أن هناك وسيلة أخرى ممكنة للعثور على المعلومات المرتبطة بمعرف تتمثل في استخدام آلية استخراج المعرف.

ويمكن تصور طائفة واسعة من الخدمات والتطبيقات للتعرف بواسطة الترددات الراديوية (RFID) حالما تتمكن من تقديم معلومات مرتبطة بمعرف وسمي في أشكال مختلفة (نص أو صوت أو صورة). ففي متحف، على سبيل المثال، يمكن استخدام معرف في وسم معلق على لوحة مرسومة للاطلاع على مزيد من المعلومات عن اللوحة والفنان. وفي محل للبقالة، يمكن استخدام معرف على رزمة غذائية للتأكد من أن الغذاء صالح للأكل وليس في عداد العينات التي تبين أنها ملوثة بطريقة ما. ومن المجالات الأخرى التي يستفاد فيها من المعلومات المستقاة من المعرف: الطب/الصيدلة والزراعة والمكتبات وتجارة التجزئة وإدارة سلسلة التوريد. ويمكن استخدام مثل هذه الآليات أيضاً لمكافحة التزييف. وتصف التوصية [ITU-T F.771] [55] عدداً من الخدمات التي يمكن أن تستند إلى استخدام المعلومات المرتبطة بالأشياء الموسومة ومتطلبات هذه الخدمات.

ويرد وفي التوصية [ITU-T H.621] [52] توصيف نموذج للنفاذ إلى المعلومات المرتبطة بشيء موسوم (انظر الشكل 6). وضمن هذا النموذج، يمكن لوظيفة اكتشاف معلومات متعددة الوسائط أن ترسل المعرف المحصَّل من قارئة وسم المعرف إلى وظيفة استخراج المعرف، وأن تحصل بالتالي على مؤشر (مثل URL) يشير إلى الإدارة المناسبة لمعلومات الوسائط المتعددة. ونتيجة لذلك، يصبح

من الممكن النفاذ إلى المعلومات ذات الصلة بمعرف الوسم. ونظراً للعدد الضخم المتوقع للمعرفات، يرجح أن توزَع وظيفة استخراج المعرف في هيكل شجرة.

وقد تستند هذه الوظيفة إلى استخدام نظام أسماء ميادين الإنترنت (DNS) الذي يستخدم لتوفير عنوان بروتوكول إنترنت (IP) المقابل للمحدد الموحد لموقع المورد (URL). وتستخدم خدمة تسمية الكائن (ONS) التي وصفتها منظمة EPCglobal آليات DNS للعثور على المعلومات المرتبطة بشفرات المنتج الإلكترونية.



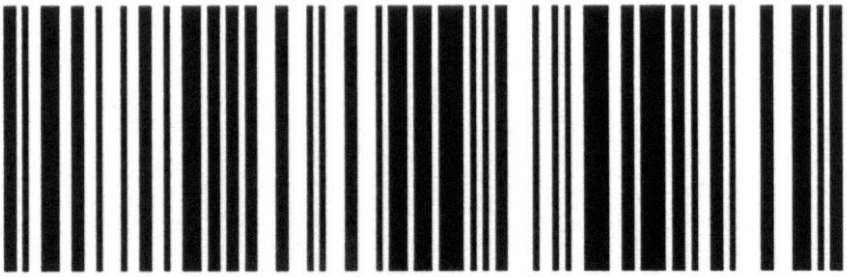
الشكل 6 – المعمارية الوظيفية للنفاذ إلى المعلومات متعددة الوسائط على أساس التعرف القائم على الوسم (التوصية ITU-T H.621)

وبالإضافة إلى ذلك، توفر التوصية ITU-T X.1255 [79] https://www.itu.int/rec/T-REC-X.1255-201309-I/en إطاراً لاكتشاف معلومات إدارة الهوية وهو إطار أقره القرار الصادر عن مؤتمر المندوبين المفوضين للاتحاد بشأن مكافحة تزييف أجهزة الاتصالات/تكنولوجيا المعلومات والاتصالات.

5.7 التعرف التلقائي ونقل البيانات (AIDC)

1.5.7 شفرات الخطوط العمودية

كثيراً ما تُستخدم شفرات الخطوط العمودية للتعرف على المنتجات. وهي تأخذ أشكالاً متنوعة تتراوح بين شفرات الخطوط العمودية لرمز المنتج العالمي (UPC) المألوفة في المتاجر الكبيرة ومصفوفة شفرات الخطوط العمودية (ثنائية الأبعاد). ويسهل على المزورين تقليدها ونسخها.



الشكل 7 – أمثلة من شفرات الخطوط العمودية الخطية

للاطلاع على أمثلة من شفرة الخطوط العمودية الخطية، انظر الشكل 7:

[80] UPC ISO/IEC 15420

شفرة الخطوط العمودية 16388 ISO/IEC 39 [81]

شفرة الخطوط العمودية 15417 ISO/IEC 128 [82]

الشكل 8 – أمثلة من مصفوفة شفرات الخطوط العمودية (ثنائية الأبعاد)

للاطلاع على أمثلة من مصفوفة شفرات الخطوط العمودية (ثنائية الأبعاد)، انظر الشكل 8:

Codablock F ISO/IEC 15417+

[83] PDF 417 ISO/IEC 15438

[84] Maxicode ISO/IEC 16023

[85] QR code ISO/IEC 18004

مصفوفة بيانات 16022 ISO/IEC [86]

يمكن استخدام شفرات الخطوط العمودية لتشفير رقم تسلسلي. فعلى سبيل المثال، يعرّف المرجع 66401 DIN [87] علامة تعرُّف متفرِّدة (UIM) تتألف من رمز مصفوفة (16022 ISO/IEC أو 18004 ISO/IEC) ومعرف بيانات متفرِّد (وفقاً للمرجع MH10.8.2 ANSI [88] والرمز "+"وفقاً للمرجع 2.3 ANSI/HIBC [89]). وهذا معيار تطبيق لوسم البنود الصغيرة في مجالات الإلكترونيات والرعاية الصحية على سبيل المثال. وهذه الشفرات مناسبة خاصةً للوسم المباشر باستخدام الوسم النافث للحبر أو الوسم الليزري وأيضاً لطباعة ملصقات الوسم.

وتحدَد المتطلبات اللازمة لوضع ملصقات الوسم على البند والوسم المباشر للمنتج بشفرات الخطوط العمودية الخطية وثنائية الأبعاد في المرجع 28219 ISO [53]. وتحدَد المتطلبات اللازمة لتصميم ملصقات شفرات الخطوط العمودية الخطية وثنائية الأبعاد لعبوات المنتجات في المعيار 22742 ISO [54] وتلك الخاصة بملصقات الشحن والنقل والاستلام في المرجع 15394 ISO [55].

2.5.7 التعرف بواسطة الترددات الراديوية (RFID)

يمكِّن التعرف بواسطة الترددات الراديوية (RFID) من وسم الأشياء وقراءة المعلومات المخزنة في هذه الوسوم باستخدام التكنولوجيا اللاسلكية قصيرة المدى. وتغطي مواصفات التعرف بواسطة الترددات الراديوية (RFID) التعرف على الأشياء، وخصائص السطح البيني الهوائي وبروتوكولات اتصالات البيانات.

ويوصِّف المرجع ISO/IEC 15963 [56] كيفية تخصيص وسوم الترددات الراديوية (RF) بمعرفات متفرِّدة. ويوجد في هذه الوسوم معرف موزع من مصنِّع دارات متكاملة – وهو معرِّف الوسم. ويمكن أن يُستخدم معرِّف الوسم (TID) كمعرف بند متفرِّد (UII) عند إلصاق الوسم على بند ما أو يمكن تخزين معرف البند المتفرِّد في جزء منفصل من الذاكرة على الوسم. وفي هذه الحالة يمكن أن يكون معرف البند المتفرِّد شفرة المنتج الإلكترونية (EPC) على النحو الذي توصِّفه منظمة EPCglobal.

ويبين الشكل 9 نسق معرف وسم ISO/IEC 15963.

صنف التوزيع (AC)	رقم تسجيل جهة إصدار TID	الرقم التسلسلي
8 بتات	المقاس المحدد بقيمة AC	المقاس المحدد بقيمة AC وقيمة جهة إصدار TID

الشكل 9 – نسق معرف وسم ISO/IEC 15963

يبين صنف التوزيع السلطة المخصصة للأرقام – أي جهة إصدار معرِّف الوسم (TID). ويمكن تسجيل مصنوعات بطاقة الدارات المتكاملة لتخصيص معرفات متفرِّدة في إطار مخطط المرجع ISO/IEC 7816-6 [90] أو مخطط اللجنة الدولية لمعايير تكنولوجيا المعلومات (INCITS) في المعهد الأمريكي للمعايير الوطنية، أسوةً بمصنعي الوسوم لتطبيقات حاويات الشحن والنقل الذين يتبعون إجراءات المرجع ISO 14816 [91]. وتُستوعب معرفات EPCglobal ضمن مخطط ISO/IEC 15963 كصنف GS1.

وتظهر في الشكل 10 الأصناف الخمسة من جهة إصدار معرِّف الوسم (TID):

قيمة AC	الصنف	مقاس معرف جهة إصدار TID	مقاس الرقم التسلسلي	سلطة تسجيل (رقم تسجيل جهة إصدار TID)
000xxxxx	INCITS 256	انظر ANSI INCITS 256 [92] و371.1 [93]	انظر ANSI INCITS 256 و371.1	autoid.org
11100000	ISO/IEC 7816-6	8 بتات	48 بتة	APACS (إدارة مدفوعات المملكة المتحدة)
11100001	ISO 14816	انظر NEN	انظر NEN	NEN (معهد التقييس الهولندي)
11100010	GS1	انظر ISO/IEC 18000-6 وType C [94] وISO/IEC 18000-3 وMode 3 [95]	انظر ISO/IEC 18000-6 وType C و18000-3 وMode 3	GS1
11100011	ISO/IEC 7816-6	8 بتات	48 بتة	APACS (بما في ذلك مقاس الذاكرة ورأسية TID الموسعة)
جميع القيم الأخرى	محجوز			محجوزة

الشكل 10 – أصناف جهات إصدار معرِّف الوسم (TID) المتفرِّد

كان التعرف على الحيوانات من التطبيقات المبكرة للتعرف بواسطة الترددات الراديوية (RFID). وأكملت المنظمة الدولية لتوحيد المقاييس (ISO) معياراً في عام 1994 يحدد بنية شفرة التعرف بواسطة الترددات الراديوية (RFID) للحيوانات (ISO 11784 [96]). ويصف المرجع المتمِم ISO 11785 [97] كيفية قراءة معلومات الوسم هذه.

وقد مضت المنظمة الدولية لتوحيد المقاييس في تحديد مجموعة كاملة من المواصفات لإدارة البند: فتصف معايير ISO/IEC ذات الأرقام من 15961 حتى 15963 بروتوكول البيانات المشتركة وأنساق المعرف التي تنطبق على سلسلة المعايير ISO/IEC 18000 [98] والتي تصف السطوح البينية الهوائية على ترددات مختلفة. وتلزم مواصفات منفصلة لنطاقات ترددية مختلفة لأن تردد التشغيل يحدد خصائص قدرات الاتصالات، فعلى سبيل المثال، يتأثر مدى التشغيل أو الإرسال بوجود الماء.

ويحدد المرجع ISO/IEC 29167-1 [57] معمارية الأمن وإدارة الملفات لمعايير السطح البيني الهوائي ISO/IEC 18000. وتعرِّف آليات الأمن التي تعتمد على التطبيق، ويمكن لوسم أن يدعمها كلها أو يدعم مجموعة فرعية منها. ويمكن لمستجوب وسم التعرف بواسطة الترددات الراديوية (RFID) النفاذ إلى معلومات بشأن آليات الأمن بدعم من وسم وكذلك إلى مزيد من المعلومات مثل خوارزمية التشفير وطول المفتاح المستخدَم.

وترد في المرجع ISO/IEC TR 24729-4 [58] مبادئ التنفيذ التوجيهية لمصممي النظام كي يقيِّموا التهديدات المحتملة لأمن البيانات الموجودة في الوسم وأمن الاتصالات من الوسم إلى الجهاز القارئ، إلى جانب وصف للتدابير المضادة المناسبة لضمان أمن بيانات الوسم.

ويرد في مراجع المنظمة الدولية لتوحيد المقاييس (ISO)، ذات الأرقام من 17363 إلى 17367 و[99] إلى [103]، توصيف تطبيقات التعرف بواسطة الترددات الراديوية (RFID) في سلسلة التوريد (حيث تنطبق أجزاء منها على حاويات الشحن وبنود النقل القابلة للإرجاع، ووحدات النقل وتعبئة وتغليف المنتجات ووسم المنتجات)؛ فيما يصف المرجع ISO 18185 [104] كيف يمكن استخدام التعرف بواسطة الترددات الراديوية لتعقب تحركات حاويات الشحن. وقد وضعت المنظمة الدولية لتوحيد المقاييس أيضاً مواصفات لاختبار الأداء والمطابقة.

ويمكن استخدام شعار التعرف بواسطة الترددات الراديوية (RFID) المحدد في المرجع ISO/IEC 29160 [105] كملصق على المنتجات يشير إلى احتوائها على وسم التعرف بواسطة الترددات الراديوية (RFID). انظر الشكل 11.

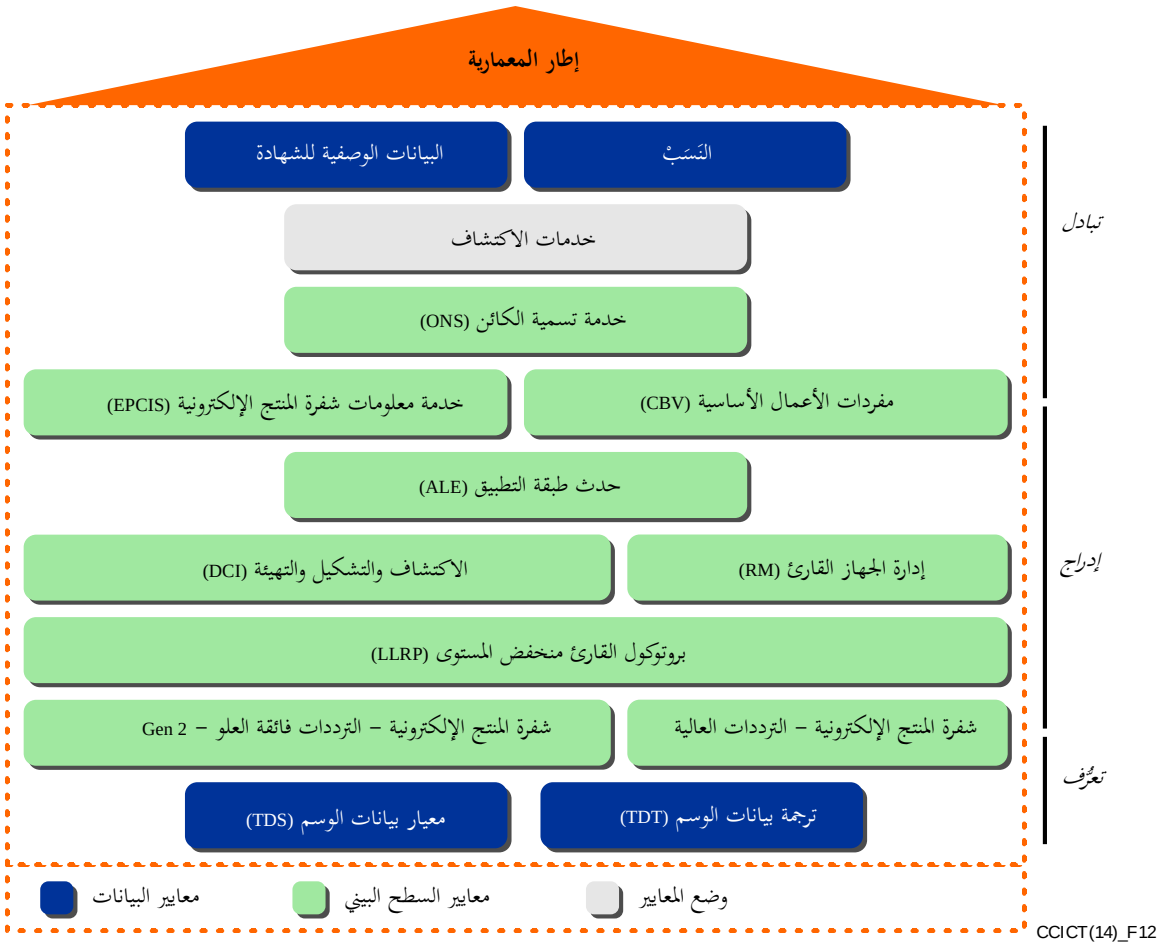
الشكل 11 – مثال التعرف بواسطة الترددات الراديوية (RFID) المحدد في المرجع ISO/IEC 29160

إن منظمة EPCglobal هي فرع من منظمة GS1 تضع مواصفات لاستخدام شفرات المنتج الإلكترونية من خلال التعرف بواسطة الترددات الراديوية (RFID). وقد أنتجت منظمة EPCglobal مجموعة من المعايير تتضمن مواصفات لتشفير بيانات الوسم وبروتوكولات السطح البيني الهوائي وبروتوكولات الجهاز القارئ وخدمات المعلومات واسم الكائن. وترد في الشكل 12 لمحة عامة عن مجموعة معايير EPCglobal.

وفيما يلي العناصر الرئيسية لمجموعة معايير EPCglobal:

- يعرِّف معيار وسم شفرة المنتج الإلكترونية (TDS) عدداً من مخططات التعرف ويصف كيف تشفَّر هذه البيانات في الوسوم وأيضاً كيف تشفَّر في شكل مناسب للاستخدام داخل شبكة أنظمة شفرة المنتج الإلكترونية (EPC).

- وترد في معيار ترجمة بيانات وسم (TDT) شفرة المنتج الإلكترونية نسخة مقروءة آلياً من أنساق بيانات شفرة المنتج الإلكترونية (EPC). ويمكن استخدام ذلك للتحقق من صحة معرفات EPC والترجمة بين تمثيلات مختلفة للبيانات.
- بروتوكولات الوسم هي سطوح بينية هوائية للتعرف بواسطة الترددات الراديوية (RFID). وعلى السطح البيني "Gen 2"، يرسل الجهاز القارئ معلومات إلى وسم بتشكيل إشارة ترددات راديوية في المدى 860-960 MHz. والوسوم منفعلة بمعنى أنها تستقبل الطاقة من الإشارة المرسلة من الجهاز القارئ. وقد أُدرج بروتوكول السطح البيني الهوائي هذا في سلسلة مواصفات ISO/IEC 18000 كالنمط C في الجزء 6. ويعمل السطح البيني الهوائي عالي التردد عند 13,65 MHz. وتتوافق هذه المواصفة مع المعيار ISO/IEC 15693 [106] الأقدم منها.
- يستخدم العميل بروتوكول القارئ منخفض المستوى (LLRP) للتحكم في جهاز القارئ على مستوى تشغيل البروتوكول الهوائي ويوفر سطح تماس بين برمجيات التطبيق وأجهزة القارئ (بروتوكول القارئ (RP)).
- تكتشف أجهزة القارئ عملاء باستخدام الإجراءات المحددة في معيار الاكتشاف والتشكيل والتهيئة (DCI).
- يُستخدم معيار إدارة جهاز القارئ (RM) لمراقبة حالة تشغيل أجهزة قارئ التعرف بواسطة الترددات الراديوية (RFID). وهو يقوم على استخدام بروتوكول إدارة الشبكات البسيط (SNMP) الذي عرَّفه فريق مهام هندسة الإنترنت (IETF).
- معيار أحداث طبقة التطبيق (ALE) يزود العملاء بوسيلة للحصول على بيانات شفرة المنتج الإلكترونية (EPC) المصطفاة. ويوفر هذا السطح البيني الاستقلال بين مكونات البنية التحتية التي تحصل على بيانات شفرة المنتج الإلكترونية الخام وبين المكونات التي تعالج تلك البيانات وبين التطبيقات التي تستفيد من البيانات.
- يسمح معيار خدمات معلومات شفرة المنتج الإلكترونية (EPCIS) بتبادل بيانات شفرة المنتج الإلكترونية (EPC) داخل المؤسسات وفيما بينها:
- تهدف مفردات الأعمال الأساسية (CBV) إلى التأكد من قيام فهم مشترك لمعنى البيانات بين جميع الأطراف التي تتبادل بيانات خدمات معلومات شفرة المنتج الإلكترونية (EPCIS).
- يصف معيار خدمة تسمية الكائن (ONS) كيف يمكن استخدام نظام أسماء ميادين الإنترنت (DNS) للحصول على ما يرتبط به من معلومات ذات شفرة EPC محددة.
- يصف معيار البيانات الوصفية لشهادة EPCglobal كيف يمكن الاستيقان من الكيانات داخل شبكة شفرة المنتج الإلكترونية (EPC) العالمية. ويُستخدم لذلك إطار الاستيقان الوارد في التوصية ITU-T X.509 [60] والبيانات الوصفية للبنية التحتية للمفتاح العمومي على شبكة الإنترنت على النحو المحدد في المرجعين IETF RFC 3280 [61] وIETF RFC 3279 [62].
- يوصِّف معيار النَسَب وسائل التعامل مع وثائق "النَسَب" الإلكترونية لاستخدامها في تطبيقات سلسلة توريد الأدوية.



الشكل 12 – نظرة عامة على معايير منظمة EPCglobal [59]

6.7 الطباعة المُحكمة والملصقات ثلاثية الأبعاد

يمكن استخدام تقنيات الطباعة المُحكمة لإنشاء ملصقات يتضح العبث بها، ويمكن أيضاً أن تُستكمل الملصقات بصور ثلاثية الأبعاد يصعب تزييفها. وتجدر الإشارة، مع ذلك، إلى أن هذه الآليات تتعرض للإساءة على نطاق واسع وينسخها المزورون.

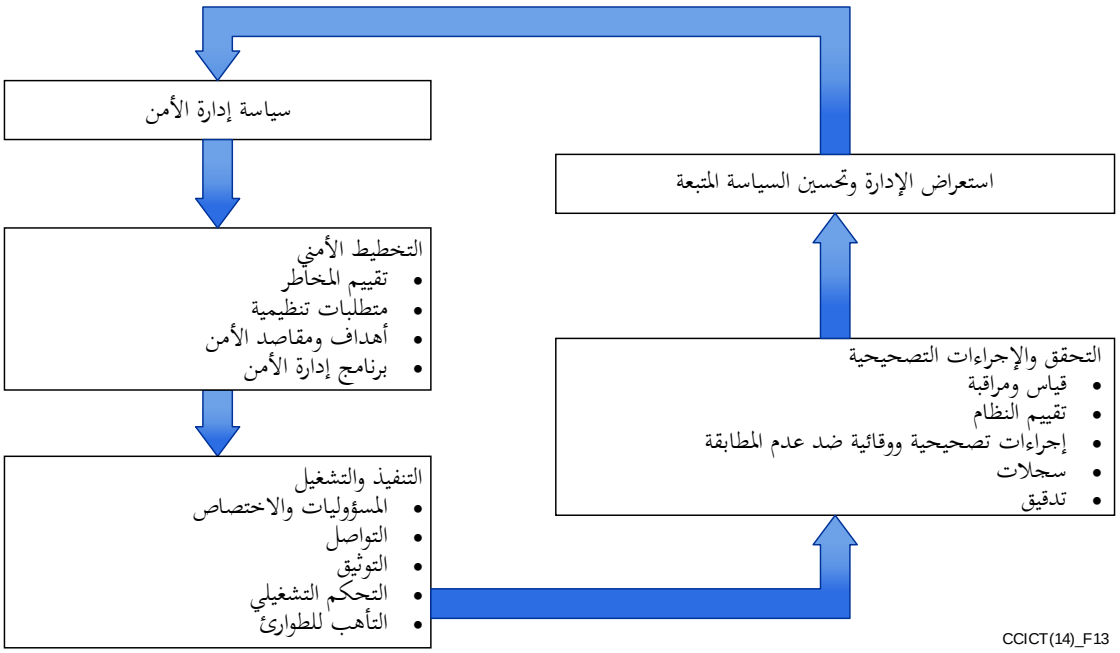
7.7 إدارة سلسلة التوريد

من الأهمية بمكان الحفاظ على أمن سلاسل التوريد لمكافحة أنشطة التزييف. وتحدد سلسلة المعايير الدولية ISO 28000 المتطلبات اللازمة للإدارة الآمنة لسلاسل التوريد. وتنطبق هذه المعايير على منظمات من أي حجم تشارك في التصنيع أو الخدمات أو التخزين أو النقل عن طريق الجو والسكك الحديدية والطرق البرية والبحر في أي مرحلة من مراحل عملية الإنتاج أو التوريد. وتتوفر المعايير التالية:

- ISO 28000: 2007، *توصيف لأنظمة إدارة الأمن في سلسلة التوريد*. [107]
- ISO 28001: 2007، *أنظمة إدارة الأمن لسلسلة التوريد – الممارسات الفضلى في تنفيذ تقييمات وخطط أمن سلسلة التوريد – متطلبات وإرشادات*. [108]
- ISO 28003: 2007، *أنظمة إدارة الأمن لسلسلة التوريد – متطلبات للهيئات القائمة بالتدقيق ومنح الشهادات لأنظمة إدارة أمن سلسلة التوريد*. [109]
- ISO 28004-1: 2007، *أنظمة إدارة الأمن لسلسلة التوريد – المبادئ التوجيهية لتنفيذ المعيار ISO 28000 - الجزء 1: المبادئ العامة*. [110]

- ISO 28005-2: 2011، *أنظمة إدارة الأمن لسلسلة التوريد – التخليص الجمركي الإلكتروني في الميناء (EPC) - الجزء 2: عناصر البيانات الأساسية*. [111]

ويتطلب المعيار ISO 28000 من المنظمات تقييم البيئة الأمنية التي تعمل فيها والوقوف على كفاية التدابير الأمنية المنفَّذة. وتظهر في الشكل 13 عناصر نظام إدارة الأمن.



الشكل 13 – عناصر نظام إدارة الأمن بمعيار ISO 28000

يهدف إطار المعايير SAFE [63] بمنظمة الجمارك العالمية (WCO) إلى ضمان أمن سلاسل التوريد العالمية، وهو يتضمن كتيباً يصف العوامل المبينة لشحنات تنطوي على درجة مرتفعة من مخاطر احتوائها سلعاً مزيَّفة. ويستند إطار SAFE إلى اتفاقات فيما بين هيئات الجمارك وإلى شراكات بين هيئات الجمارك ومصالح الأعمال بحيث تعطى الفوائد للشركات التي تلبي المعايير الأمنية لسلسلة التوريد.

وقد قامت اللجنة التقنية 107 باللجنة الكهرتقنية الدولية (IEC TC 107)، التي يقع مجال نشاطها في إدارة العملية لصناعة إلكترونيات الطيران، بإنتاج مواصفة تعنى بتجنب استخدام المكونات الإلكترونية المزيَّفة والمغشوشة والمعاد تدويرها [64]. وحالياً تعمل هذه اللجنة أيضاً على مواصفة لإدارة المكونات الإلكترونية من مصادر لا امتياز لديها لمنع دخول المكونات المزيَّفة سلسلة التوريد [65].

وقد وضعت جمعية مهندسي السيارات (SAE) الدولية (اسمها الأصلي جمعية مهندسي السيارات) عدداً من المواصفات تهدف على وجه التحديد لتجنب دخول المكونات الإلكترونية المزيَّفة في سلاسل توريد صناعتي الفضاء الجوي والسيارات التي يحال إليها على نطاق واسع في صناعة الإلكترونيات. وقد أنتجت جمعية مهندسي السيارات وثيقتين معدتين للاستخدام لدى الجهات التي تتخذ القرارات الشرائية:

الوثيقة SAE AS5553 [112]: "تجنب القطع الإلكترونية المزيَّفة وكشفها والتخفيف من حدتها".

والوثيقة SAE ARP6178 [113]: "القطع الإلكترونية المزيَّفة؛ أداة لتقييم المخاطر من الموزعين"؛ ومواصفة معدة كي يستخدمها الموزعون: SAE AS6081 [114]: "القطع الإلكترونية المزيَّفة؛ بروتوكول التجنب، الموزعون". وقد وضعت جمعية مهندسي السيارات أيضاً مواصفة بشأن الاختبار: SAE AS6171 [115]: "معيار أساليب الاختبار، القطع الإلكترونية المزيَّفة".

وتعمل لجنة IEC TC 107 بشكل وثيق مع جمعية مهندسي السيارات الدولية على الوثيقة SAE AS5553 من خلال ترتيب اتصال.

ومعظم المحافل المعنية بمشكلة السلع المزيَّفة سالفة الذكر تقدم المشورة أو مبادئ توجيهية بشأن إدارة سلسلة التوريد. وبوجه عام، هناك متطلبات تستلزم إمكانية تتبع المنتج، وإخضاعه للتفتيش واختباره (على أن يقوم بذلك الطرف الأول أو الثاني أو الثالث). وقد أنتج الفريق البريطاني المعني بالتصدي للجرائم ضد الملكية الفكرية (UK IP Crime Group) مجموعة أدوات سلسلة التوريد في عام 2011.

8.7 الاختبار

تشغِّل اللجنة الكهرتقنية الدولية (IEC) مخططات تقييم المطابقة التالية http://www.iec.ch/about/activities/conformity.htm:

- نظام IECEE – IEC لمخططات تقييم المطابقة للمعدات والمكونات الكهرتقنية؛
- نظام IECEx – IEC لمنح شهادات للمعايير المتعلقة بالمعدات المهيأة للاستخدام في الأجواء الانفجارية؛
- نظام IECQ – IEC سلتقييم جودة المكونات الإلكترونية.

وتستند مخططات IEC CA هذه إلى نيل شهادات من طرف ثالث، وهي تستخدم أنظمة عبر شبكة الإنترنت لتقدم معلومات عن الشهادات التي يمكن استخدامها في الجهود الرامية إلى تحديد المنتجات المزيَّفة.

ويشغِّل نظام IECEE مخطط هيئة منح الشهادات (CB) القائم على مبدأ الاعتراف المتبادل بين أعضائها بنتائج الاختبار للحصول على شهادة أو موافقة على المستوى الوطني. ونشرة هيئة منح الشهادات http://members.iecee.org/iecee/ieceemembers. nsf/cb_bulletin?OpenForm هي قاعدة بيانات لمستخدمي مخطط هيئة منح الشهادات، وهي تقدم معلومات عن:

- المعايير المقبولة للاستخدام في المخطط؛
- الهيئات الوطنية لمنح الشهادات، بما في ذلك فئات المنتجات والمعايير التي من أجلها اعتُرف بهذه المنتجات؛
- الاختلافات الوطنية لكل معيار في كل بلد عضو.

ونظام IECEE CBTC هو نظام تسجيل شهادة اختبار عبر الإنترنت لهيئات منح الشهادات الوطنية التي تسمح أيضاً بنفاذ العموم إليه.

وقد أنشأت لجنة IECEE فريق مهام لدراسة تدابير لمكافحة التزييف (CMC-WG 23 "التزييف").

ويتكون نظام منح الشهادات الدولي IECEx من المكونات التالية:

- مخطط IECEx للمعدات المعتمدة؛
- مخطط IECEx للمرافق الخدمية المعتمدة؛
- نظام IECEx لترخيص علامة المطابقة؛
- منح شهادة IECEx لكفاءات الموظفين (CoPC).

ويقدم نظام IECEx CoC Online معلومات عن الشهادات والتراخيص الصادرة وفقاً لهذه المخططات.

ويشغِّل نظام IECQ خطة إدارة المكونات الإلكترونية (ECMP) لأنظمة إلكترونيات الطيران ومخطط إدارة إجراءات المواد الخطرة (HSPM). وتتوفر الشهادات بهذا الصدد على شبكة الإنترنت.

9.7 قواعد البيانات

تقدَّم قواعد بيانات السلع المزيَّفة المعروفة كي تستخدمها وكالات الإنفاذ مثل تلك التي تشغِّلها منظمة الجمارك العالمية والانتربول، وكذلك كي يستخدمها المستهلكون. ويدير مكتب استخبارات التزييف بغرفة التجارة الدولية (ICC) قاعدة بيانات دراسات الحالة.

10.7 مراقبة السوق

تتكون مراقبة السوق من "الأنشطة التي نفذتها السلطات المعيَّنة والتدابير التي اتخذتها لضمان توافق المنتجات مع متطلبات المنصوص عليها في التشريعات ذات الصلة، وعدم تهديدها للصحة أو للسلامة أو لأي جانب آخر من جوانب حماية المصلحة العامة" [66].

ويمكن التعرف على السلع المزيَّفة من خلال أنشطة مراقبة السوق، ويمكن أن تشارك سلطات مراقبة السوق في الجهود المبذولة لمكافحة الاتجار في السلع المزيَّفة. وتوصي لجنة الأمم المتحدة الاقتصادية لأوروبا (UNECE) بتنسيق مراقبة السوق الوطنية مع أنشطة جمارك وبتمكين أصحاب الحقوق من إبلاغ سلطات مراقبة السوق عن المنتجات المزيَّفة [67].

وتتطلب بعض البلدان تسجيل المنتجات كي يجري تسويقها. فعلى سبيل المثال، طبقت منظمة المعايير في نيجيريا مؤخراً مخطط تسجيل للمنتج الإلكتروني في محاولة للحد من بيع المنتجات المزيَّفة.

8 منظمات وضع المعايير

إن منظمتي التقييس الدوليتين الرئيسيتين اللتين تتناولان مواضيع ذات صلة بمكافحة التزييف هما المنظمة الدولية لتوحيد المقاييس (ISO) واللجنة الكهرتقنية الدولية (IEC).

وأنشأت المنظمة الدولية لتوحيد المقاييس لجنة تقنية لإنتاج مواصفات أدوات مكافحة التزييف (ISO TC 246) في عام 2009. ووضعت هذه اللجنة توصيفاً لمعايير أداء حلول الاستيقان المستخدمة لمكافحة تزييف السلع المادية (ISO 12931) [48]. ويسعى هذا التوصيف إلى زيادة ثقة المستهلك، وجعل سلاسل التوريد أكثر أمناً، ومساعدة السلطات العامة في استحداث سياسات وقائية ورادعة وعقابية. وقد توقف نشاط اللجنة ISO TC 246، **ولكن العمل في هذا المجال يتواصل في إطار اللجنة ISO TC 247**.

ويشمل اختصاص اللجنة ISO TC 247 التقييس في مجال الكشف والوقاية والسيطرة إزاء الاحتيال الذي يطال الهوية والشؤون المالية والمنتجات وغير ذلك من أشكال الاحتيال الاجتماعي والاقتصادي: "التدابير المضادة للاحتيال وضوابطه". وقد وضعت هذه اللجنة معياراً توجيهياً من المنظمة الدولية لتوحيد المقاييس (ISO) بشأن قابلية التشغيل البيني لمعرفات الأشياء في مكافحة التزييف - ISO 16678 [116]: "مبادئ توجيهية للتعرف على الأشياء القابل للتشغيل البيني وأنظمة الاستيقان ذات الصلة لردع التزييف والاتجار غير المشروع". ويتعلق هذا المشروع الجديد باستخدام تسلسل شامل للتعرف على منتجات بالتحقق منها في قاعدة بيانات للتأكد من مستوى أصالتها. ويرمي هذا المعيار الدولي لتمكين التعرف الموثوق والآمن على الأشياء لردع إدخال الأشياء غير المشروعة إلى السوق. ويمكن الاستيقان من المنتجات ذات الأرقام التسلسلية على امتداد سلسلة التصنيع والتوزيع بما فيها المستهلك.

وأدركت المنظمة الدولية لتوحيد المقاييس (ISO) أن التزييف والقرصنة يؤثران على تشكيلة كبيرة من السلع الاستهلاكية بما في ذلك الملابس والأحذية والأدوية والسيارات وقطع غيار السيارات والمواد الغذائية والمشروبات ومستحضرات التجميل والأفلام والموسيقى والمنتجات الكهربائية وأجهزة السلامة وقطع غيار الطائرات. وتشمل مخاوف المستهلكين بوجه خاص المخاطر التي تهدد السلامة والصحة، وجوانب الأداء، وسهولة الاستخدام/الملاءمة للغرض المنشود، وإمكانية النفاذ، وحماية البيانات، وفقدان الوظائف، والضرر الاقتصادي، والصلات بالجريمة المنظمة http://www.iso.org/iso/copolco_priority-programme_annual-report_2012.pdf.

وتعمل اللجنة التقنية المشتركة لدى المنظمة الدولية لتوحيد المقاييس/اللجنة الكهرتقنية الدولية (ISO/IEC JTC 1/ SC 31) على تقنيات التعرف التلقائي والتقاط البيانات. ولهذه اللجنة سبعة أفرقة عمل بشأن المواضيع التالية:

- فريق العمل 1 (WG1) المعني بالوسائط الحاملة للبيانات؛
- فريق العمل 2 (WG2) المعني بهيكل البيانات؛

- فريق العمل 4 (WG4) المعني بالتعرف بواسطة الترددات الراديوية لإدارة البند؛
- فريق العمل 5 (WG5) المعني بأنظمة تحديد الموقع في الوقت الفعلي؛
- فريق العمل 6 (WG6) المعني بالتعرف على البند المتنقل وإدارته؛
- فريق العمل 7 (WG7) المعني بأمن إدارة البند.

وتعمل اللجنة الأوروبية للتقييس (CEN) أيضاً على تكنولوجيات التعرف التلقائي والتقاط البيانات (AIDC) في اللجنة التقنية TC 225.

وقد أنشأت العديد من منظمات التقييس الوطنية لجاناً تعادل تلك الموجودة في المنظمة الدولية لتوحيد المقاييس/اللجنة الكهرتقنية الدولية (ISO/IEC). وحسبنا مثال واحد في معهد التقييس الألماني (DIN) الذي أنشأ اللجنة DIN NA 043-01-31 للعمل على تقنيات التعرف التلقائي والتقاط البيانات [68] واللجنة DIN NA 043-01-31-04 UA للعمل على التعرف بواسطة الترددات الراديوية لإدارة البند.

وتعمل اللجنة IEC TC 107 المعنية بإدارة العمليات لإلكترونيات الطيران على منع التزييف.

وبالإضافة إلى ذلك، تنتج جمعية مهندسي السيارات (SAE) الدولية مواصفات لتجنب استخدام المكونات الإلكترونية المزيَّفة في صناعات التكنولوجيا الراقية، وقد أنتجت منظمة GS1 مجموعة من المواصفات بشأن التعرف على البنود وإدارة سلسلة التوريد.

9 المبادئ التوجيهية لمكافحة التزييف

عرض عدد من المنظمات مبادئ توجيهية لمكافحة التزييف من وجهات نظر مختلفة – من وجهات نظر المصنعين والموزعين، والحكومات ووكالاتها المعنية بالإنفاذ، والمستهلكين.

ويقترح منتدى مكافحة التزييف ممارسات فضلى لمصنعي المعدات الأصلية (OEM) والموزعين ومصنعي المكونات [69]. وتشمل هذه المبادئ التوجيهية ما يلي:

- التزود مباشرةً من المصنِّع أو الموزع المعتمد أو، إن لم يكن ذلك ممكناً، من مصدر سوق رمادية مُنشأ محلياً؛
- الإصرار على أدلة وثائقية على أصالة المنتجات في حالة استخدام مصادر السوق الرمادية؛
- تنسيق أكبر لإدارة دورة الحياة للمنتجات والمكونات؛
- التأكد من التخلص من الخردة والمنتجات المعيبة على نحو يمنع استخدامها؛
- تحسين إمكانية تتبع المنتج عن طريق استخدام المعرفات المتفرِّدة ومراقبة الوثائق.

وقد أعدت شركة معهد تكنولوجيا المكونات (CTI) برنامج تجنب المكونات المزيَّفة (CCAP-101) [70] لمنح شهادات لموزعي المكونات الإلكترونية المستقلين. فتحدَد متطلبات من الموزعين لكشف المكونات المزيَّفة وتجنب تسليمها لعملائهم. ويمكن إجراء اختبار كهربائي. ويهدف برنامج منح الشهادات هذا إلى تلبية أهداف المواصفة SAE AS5553.

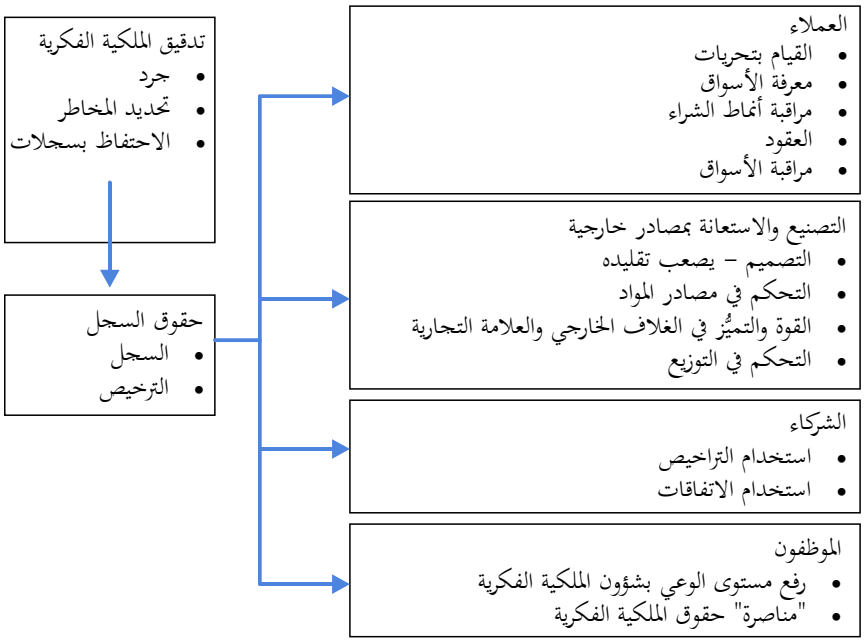
وبالمثل، فقد أنتجت جمعية موزعي الإلكترونيات المستقلة (IDEA) مواصفة للتخفيف من حدة التزييف وإخضاعه للتفتيش (IDEA-STD-1010A) [117] وأيضاً مواصفة لإدارة الجودة (IDEA-QMS-9090) [118].

وتضم خارطة طريق الملكية الفكرية بغرفة التجارة الدولية (ICC) توصيات بإجراءات تتخذها دوائر الأعمال والحكومة بشأن جميع جوانب حماية الملكية الفكرية، بما في ذلك مكافحة التزييف والقرصنة. وعلى وجه الخصوص، تحث غرفة التجارة الدولية الحكومات على بذل المزيد من الجهد لتطبيق لوائح حقوق الملكية الفكرية لأن "الموارد الحكومية المخصصة لمكافحة القرصنة والتزييف كثيراً ما تقصِّر على نحوٍ يرثى له عن الارتقاء إلى حجم المشكلة".

ولاحظت منظمة التعاون والتنمية في الميدان الاقتصادي (OECD) أن سوق المنتجات المزيَّفة والمقرصنة يمكن تقسيمه إلى "سوق رئيسي" يظن المستهلكون منتجاته أصلية، و"سوق ثانوي" يبتاع فيه المشترون المنتجات المزيَّفة أو المقرصنة عن علم في بحثهم عن صفقة جيدة. ولعل الشخص الذي لا يتورع عن شراء قميص مزيَّف أو حقيبة يد مزيَّفة، يُعرِض عن شراء الأدوية أو المعدات الكهربائية المزيَّفة. وتلزم استراتيجيات مختلفة لمكافحة التزييف في هذين السوقين، وبالتالي تدعو الضرورة إلى معرفة أي هو السوق الذي يُتداول فيه منتج معين.

فقد تتسنى مكافحة تزييف المنتجات في السوق الرئيسي على نحوٍ فعّال، على سبيل المثال، بحملات إعلامية تبرز أخطار شراء المنتجات المزيَّفة، فيما قد يلزم التشدد في فرض العقوبات حيال المنتجات في السوق الثانوي.

وتهدف مجموعة أدوات سلسلة التوريد لدى الفريق البريطاني المعني بالتصدي للجرائم ضد الملكية الفكرية (UK IP Crime Group) [71] إلى رفع مستوى الوعي بمشكلة السلع المزيَّفة التي تدخل سلاسل التوريد التجارية المشروعة، وهي تقدم إرشادات بشأن كيفية حماية أصول الملكية الفكرية. وترد في الشكل 14 الخطوط العريضة للعملية التي يمكن لشركة أن تقلل عبرها من مخاطر السلع المزيَّفة التي تدخل سلسلة التوريد.



الشكل 14 – حماية حقوق الملكية الفكرية (مقتبس من مجموعة أدوات الفريق البريطاني المعني بالتصدي للجرائم ضد الملكية الفكرية (UK IP Crime Group) [71])

وضع منتدى مصنعي الأجهزة المتنقلة (MMF) دليل موارد للحكومات يقترح مجموعة من التدابير تتضمن ما يلي:

- اعتماد تغييرات في الأطر القانونية والتنظيمية للحد من تفعيل الأجهزة المزيَّفة على شبكات الاتصالات؛
- فرض قيود على استيراد الأجهزة المتنقلة وملحقاتها التي لا تلتزم بمعايير الصناعة أو بالإطار التشريعي والتنظيمي لبلد ما؛
- إقامة التحالفات والحلول العالمية اللازمة بين دوائر الصناعة والسلطة كي تؤكد السلطات والمستهلكين وقنوات البيع صحة المنتجات الأصلية؛
- وضع حلول تكنولوجية مبتكرة ومواءَمة تحد من إمكانية تفعيل الأجهزة المتنقلة المزيَّفة على شبكات الاتصالات؛
- دعم المعايير التي تؤدي إلى تعزيز ميزات الأمن (كتمايز فرادى أرقام بطاقات الهوية فيما بينها) بما يردع تصنيع المنتجات المزيَّفة والأخرى غير القانونية.

ويمضي هذا النهج بالضرورة إلى أبعد من الاعتماد على إجراءات الإنفاذ التقليدية وحدها، وينحو بدلاً من ذلك نحو منع هذه الأجهزة من العمل على الشبكات. ومع ذلك يظل القيام بالإنفاذ وحملات التوعية ومراقبة السوق مهماً، وسيستمر مصنعو الهواتف المتنقلة في العمل مع السلطات الوطنية حيثما كان ذلك ممكناً.

10 الاستنتاجات

التزييف مشكلة مستفحلة تؤثر على منتجات ما برح نطاقها يتوسع. وفي قطاع تكنولوجيا المعلومات والاتصالات، تُستهدف الهواتف المتنقلة على وجه الخصوص، حيث يباع نحو 250 مليون جهاز مزيَّف منها سنوياً بما يشكل حوالي 15%-20% من السوق العالمي. وبصرف النظر عن الآثار الاقتصادية الواضحة على الشركات المصنعة للمنتجات الأصلية (من بَخس قيمة العلامة التجارية، وخسارة الإيرادات، والتعدي على حقوق النسخ والعلامات التجارية، والمنافسة غير الشريفة)، وعلى الوكلاء المعتمدين والحكومات (من حيث تجنب دفع الضرائب، والتكاليف الإضافية في ضمان الامتثال للتشريعات الوطنية المرعية، والحاجة للتصدي للأخطار المهددة للأمن العام، وفرص العمل الضائعة)، هناك أيضاً مخاطر مهددة لصحة المستهلكين وسلامتهم وخصوصياتهم، وجوانب السلامة العامة والآثار السلبية على مشغلي الشبكات (بسبب تدني جودة الخدمة (QoS) المقدمة، ومشاكل محتملة في التوافق الكهرمغنطيسي (EMC)، وتعطل شبكة). ويُنتج معظم هذه الهواتف المتنقلة المزورة في بلد واحد في آسيا. وهذا البلد هو مصدر غالبية المكونات الإلكترونية المزيَّفة الناتجة عن إعادةً التدوير في القطاع غير الرسمي للنفايات الإلكترونية من البلدان المتقدمة؛ كما تبيَّن في جلسة استماع للجنة القوات المسلحة بمجلس الشيوخ الأمريكي بشأن القطع الإلكترونية المزيَّفة في سلسلة توريد أنظمة الدفاع [9]. ومن الواضح أن هناك الكثير من العمل الذي يتعين القيام به لتحديد مصادر المعدات المزيَّفة والتعامل معها قبل تصديرها حول العالم.

والصكوك القانونية لمكافحة التزييف موجودة غالباً ولكن الإنفاذ لا يزال ضعيفاً. وقد خلص تقرير منظمة التعاون والتنمية في الميدان الاقتصادي (OECD) لعام 2008 إلى أن "جسامة وآثار التزييف والقرصنة بلغت من الخطورة مبلغاً يستلزم اتخاذ إجراءات قوية ومستدامة من الحكومات والشركات والمستهلكين. وتكتسي زيادة فعالية الإنفاذ أهميةً بالغة في هذا الصدد، وكذلك الحاجة إلى حشد الدعم الشعبي لمكافحة التزييف والقرصنة. وثمة فائدة ترجى من زيادة التعاون بين الحكومات، ومع دوائر الصناعة، وكذلك من تحسين جمع البيانات."

وأصبحت الحكومات أكثر انخراطاً في هذه المسألة، ويقوم كثير منها بحملات توعية، مقدمةً المشورة وملاحقةً الجناة بمزيد من الصرامة، كما يمكن أن يرى في الصين مؤخراً. ويتعين ألا تكتفي الحكومات بإنفاذ لوائح حقوق الملكية الفكرية بل عليها أيضاً أن تنفذ اتفاقية بازل (Basel) للتأكد من التعامل مع المعدات المستعملة وتلك التي بلغت نهاية عمرها بطريقة سليمة بيئياً، بدلاً من أن تساهم في اقتصاد التزييف غير الرسمي. وينبغي اعتماد ممارسات إعادةً التدوير الأخلاقية في جميع أنحاء العالم.

وقد ترغب الحكومات أيضاً بربط أنشطة مراقبة السوق بأنشطة السلطات الجمركية لتحسين قدرات كشف المنتجات المزيَّفة. وينبغي اعتبار معدات تكنولوجيا المعلومات والاتصالات المزورة المضبوطة بمثابة نفايات إلكترونية والتعامل معها وفقاً للمخططات السليمة بيئياً لإدارة النفايات.

وقد نظمت الشركات والصناعات المتضررة من التزييف حملات إعلامية وقامت بمساع دعماً لمصالحها. ولكن يبدو أن الحاجة تستدعي مزيداً من الوعي بقضايا التزييف. ففي الولايات المتحدة الأمريكية، ألقى قانون تخويل الدفاع الوطني لعام 2012 (NDAA) بالمسؤولية الكاملة على عاتق المقاولين لكشف المكونات المزورة وتصحيح أي حالة تتسلل فيها مكونات مزورة إلى المنتجات.

ويجب على المستهلكين أيضاً أن يكونوا على بينة من مخاطر شراء معدات مزيَّفة ومن أن مثل هذه المعدات قد لا تكون آمنة للاستخدام، وقد لا يجاري أداؤها أداء المواد الأصلية. ومن الواضح أن العديد من الهيئات الوطنية والدولية، وكذلك الشركات المصنِّعة، وتجار التجزئة ووسائل الإعلام، تسلط الضوء بانتظام على الإشكالات التي تسببها المنتجات المزيَّفة للمستهلكين. ويبقى الحال، مع ذلك، أن المستهلكين يعمدون في كثير من الأحيان إلى شراء السلع المزيَّفة، مهما كانت العواقب المحتملة، على أساس السعر فيما يبدو.

ولعل التزييف يمكن أن يكافَح أيضاً بإدارة دورة حياة المعدات، ليس في سلسلة التوريد فقط بل أيضاً في مراحل الإرجاع ومعاودة الاستخدام وإعادةً التدوير خلال دورة الحياة الكاملة للمعدات. وتتطلب إدارة دورة الحياة وسيلة للتعرف على البنود والاستيقان منها، وعمليات لتتبعها بنحو آمن. ولكن التتبع ينبغي أن يكون مناسباً وكافياً للغرض منه لأن تكنولوجيات التعرف التلقائي والتقاط البيانات (AIDC)، مثل التعرف بواسطة الترددات الراديوية (RFID)، تثير إشكالات كبيرة تطال الخصوصيات حيث يمكن أن تُربط الأشياء بأصحابها. وينبغي توخي الحذر في عملية المعايير لاحترام خصوصيات المستهلكين وعدم تسهيل قمع مستخدمي منتجات تكنولوجيا المعلومات والاتصالات من خلال آليات تسجيل المعرف. وتنبغي أيضاً حماية المستهلكين من الفصل التعسفي من الشبكات.

ويمكن تطبيق معايير تكنولوجيا التعرف التلقائي والتقاط البيانات (AIDC) وإدارة سلسلة التوريد، كما استُعرضت آنفاً، لمكافحة التزييف.

وتتطلب مكافحة التزييف التعاون عبر قطاعات الصناعة. ويمكن دعم جهات الإنفاذ مثل سلطات الجمارك ببعض الأدوات العامة (كتلك المعدة لكشف جوازات السفر والأوراق النقدية المزورة)، وكذلك بمجموعة من الآليات التي تخص قطاعات ومنتجات معينة وبإجراءات محدَّدة الأهداف من خلال التعاون بين القطاعين العام والخاص.

وفي قطاع الهاتف المتنقل اليوم، هناك عدد من الأنظمة القائمة على تسجيل الهوية الدولية للمعدات المتنقلة (IMEI)، التي تشغلها أو تخطط لها فرادى الإدارات والسلطات التنظيمية للتعرف على المطاريف المتنقلة الأصلية والمستوردة على نحو قانوني. وهناك أيضاً عدد من المبادرات الإقليمية لتبادل المعلومات بشأن المطاريف المتنقلة ذات المنشأ غير القانوني. ويمكن لهذه الآليات أن تسبب مشاكل للمستخدمين الشرعيين أيضاً. فعلى سبيل المثال، يمكن لمستخدم أجنبي، حين يسافر إلى بلد ما ثم يستخدم بطاقة SIM محلية في جهازه، أن يقع في فخ القائمة البيضاء حيث يعجز عن استخدام جهازه. ويمكن لهذه الآليات أن تسبب إشكالات لحرية حركة السلع. وفي قطاعات تكنولوجيا المعلومات والاتصالات الأخرى، لا وجود لهذه الآليات نظراً لطبيعة المنتجات وهيكل الصناعات.

وعلى الرغم من أن بعض البلدان قد نفذت حلولاً ناجحة تعتمد على الهوية الدولية للمعدات المتنقلة (IMEI) لردع انتشار الهواتف المتنقلة المزيَّفة؛ فإن الأخرى منها، وخاصةً البلدان النامية، لا تزال تواجه تحديات كبيرة في إيجاد حلول فعالة لمكافحة الأجهزة المزيَّفة. وفي الوقت الحاضر، تستند الحلول المتاحة في بعض البلدان إلى حجب الهواتف المتنقلة ذات أرقام الهوية الدولية للمعدات المتنقلة (IMEI) غير الصالحة عن شبكاتها، أو منع استخدام المعدات التي لم تقر الهيئة التنظيمية نمطها، أو منع الاستيراد غير المشروع لهذه الأجهزة، أو اتخاذ إجراءات أخرى بشأن توعية المستهلك وتدابير الإنفاذ وتغييرات مناسبة للتشريعات على المستوى الوطني.

وقد تناولت منظمات التقييس الدولية الرئيسية موضوعات ذات صلة بمكافحة التزييف. ولا توجد حالياً أي توصية متاحة من الاتحاد الدولي للاتصالات، على سبيل المثال، لمقارنةً الأنظمة الحالية المختلفة لمكافحة التزييف، ولوصف إطار ذي صلة، وللنظر في الأداء وقابلية التشغيل البيني على المستوى العالمي. وللاتحاد والجهات المعنية الأخرى أدوار رئيسية يؤدونها في تعزيز التنسيق بين الأطراف المعنية لتحديد سبل التعامل مع الأجهزة المزيَّفة دولياً وإقليمياً. وبالإضافة إلى ذلك، كُلف الاتحاد بمساعدة الأعضاء في اتخاذ الإجراءات اللازمة لمنع أو كشف العبث بمعرفات الأجهزة المتفرِّدة و/أو استنساخها.

ويتناول هذا التقرير التقني الموضوعات ذات الصلة بمكافحة التزييف حصراً، مثل ماهية التزييف، وأثره، واتفاقيات حقوق الملكية الفكرية وإنفاذها، ومنتديات مكافحة التزييف في دوائر الصناعة، وتدابير مكافحة التزييف والمنظمات المتورطة في التزييف. ولمساعدة السلطات التنظيمية في حماية المستهلكين والمشغلين والحكومات من الآثار السلبية للأجهزة المزيَّفة، ينبغي أن يتناول الاتحاد هذه المسألة بالدراسة.

11 مشاركة الاتحاد الدولي للاتصالات

إن القرار 177 الصادر عن مؤتمر المندوبين المفوضين للاتحاد عام 2010 (PP-10) "يدعو الدول الأعضاء وأعضاء القطاعات إلى أخذ الأُطُر القانونية والتنظيمية للبلدان الأخرى بعين الاعتبار فيما يتعلق بالتجهيزات التي تؤثر سلباً على نوعية البُنى التحتية للاتصالات والخدمات في هذه البلدان وخصوصاً الإقرار بشواغل البلدان النامية فيما يتعلق بالتجهيزات الزائفة" [72].

وإن القرار 79 الصادر عن المؤتمر العالمي لتنمية الاتصالات عام 2014 بشأن: "دور الاتصالات/تكنولوجيا المعلومات والاتصالات في مكافحة أجهزة الاتصالات/تكنولوجيا المعلومات والاتصالات المزيَّفة والتصدي لها" وقرار اللجنة COM5/4 177 الصادر عن مؤتمر المندوبين المفوضين عام 2014 بشأن "مكافحة أجهزة الاتصالات/تكنولوجيا المعلومات والاتصالات المزيَّفة" يفوضان الاتحاد الدولي للاتصالات بمعالجة قضية معدات تكنولوجيا المعلومات والاتصالات المزيَّفة.

ويعكف فريق المسألة 8 بلجنة الدراسات 11 (SG11) على دراسة هذه المسألة، وقد أقام الاتحاد ورشة عمل بشأن "مكافحة معدات تكنولوجيا المعلومات والاتصالات المزيَّفة وتلك دون المستوى المطلوب" في جنيف في نوفمبر 2014 http://www.itu.int/en/ITU-T/C-I/Pages/WSHP_counterfeit.aspx.

وقد أنتجت لجنتا الدراسات 16 و17 بقطاع تقييس الاتصالات، توصيات على صلة بالتعرف على الكائنات والاستيقان منها.

وتتولى لجنة الدراسات 5 (SG5) بقطاع تقييس الاتصالات مسؤولية دراسة منهجيات التصميم للحد من الآثار البيئية لاستخدام تكنولوجيا المعلومات والاتصالات من خلال وسائل مثل إعادةً التدوير.

وقد أنشأ مدير مكتب تقييس الاتصالات فريقاً مخصصاً (AHG) يعنى بحقوق الملكية الفكرية: http://www.itu.int/en/ITU-T/ipr/Pages/adhoc.aspx لدراسة سياسة براءات الاختراع وحقوق نسخ البرمجيات والمبادئ التوجيهية للعلامات، وغيرها من القضايا ذات الصلة. وقد دأب هذا الفريق على إقامة الاجتماعات منذ عام 1998. واشترك الاتحاد مع المنظمة العالمية للملكية الفكرية (WIPO) في ترتيب ندوات كتلك المعنية بأسماء الميادين متعددة اللغات في عام 2001 وبشأن "تسوية المنازعات في مفترق طرق المعلومات وتكنولوجيا الاتصالات والملكية الفكرية" في عام 2009: http://www.wipo.int/amc/en/events/workshops/2009/itu/index.html. ونظم الاتحاد أيضاً مائدة مستديرة بشأن براءات الاختراع في عام 2012 ليوفر منبراً محايداً لهيئات الصناعة والمعايير والتنظيم لمناقشة ما إذا كانت سياسات براءات الاختراع الحالية والممارسات الصناعية القائمة تستجيب استجابة كافية لاحتياجات مختلف أصحاب المصلحة. http://www.itu.int/en/ITU-T/Workshops-and-Seminars/patent/Pages/default.aspx وحتى الآن، لم يعالج هذا الفريق قضية التزييف.

وللاتحاد دور يؤديه في التصدي لمشكلة معدات تكنولوجيا المعلومات والاتصالات المزيَّفة.

وفي تقرير للجنة الدراسات 1 بقطاع تنمية الاتصالات في الاتحاد بشأن التنظيم وحماية المستهلك في بيئة متقاربة (مارس 2013)، وهو تقرير أعد في إطار القرار 64 للمؤتمر العالمي لتنمية الاتصالات للاتحاد الدولي للاتصالات (حيدر آباد، 2010)، ذُكر أن ثمة تحدياً للسلطات التنظيمية يتمثل في حماية المبتكرين والمبدعين والمستهلكين من أعمال التزييف والقرصنة المرتبطة بتوزيع السلع والخدمات بواسطة الإنترنت (عبر الحدود على نحو متزايد).

ووفقاً للمبادئ التوجيهية للبلدان النامية التي نشرها قطاع تنمية الاتصالات بالاتحاد في مايو 2012، بشأن إنشاء مختبرات لاختبار تقييم المطابقة في مختلف المناطق، أفادت الدول الأعضاء بأن المعدات المزيَّفة تفاقم مشاكل المطابقة وقابلية التشغيل البيني http://www.itu.int/ITU-D/tech/ConformanceInteroperability/ConformanceInterop/Guidelines/Test_lab_guidelines_EV8.pdf. وتجدر الإشارة إلى أن "شبهة إغراق السوق بالمنتجات دون المستوى المطلوب والتي أخفقت في اختبارات بلدان أخرى هي مدعاة أخرى للقلق كحال استيراد وتوزيع المنتجات المزيَّفة. ومن المقومات الرئيسية لطمأنة مثل هذه المخاوف، امتلاك نظام متين لاعتماد النوع ومختبر اختبار يعمل وفق مجموعة من المعايير التقنية، ونظام اختبار، وقدرة على اعتماد ومراقبة تكنولوجيات الاتصالات التي يجري طرحها في السوق مدعومة بالمراقبة والتدقيق والإنفاذ. وفي حال عدم وجود متطلبات تقنية قائمة، وعدم توفر نظام اعتماد نوع ومختبرات اختبار في بلد أو منطقة ما، لا تتوفر للسوق أسباب الحماية". ويمكن أن يتعرقل الاختبار والتشغيل البيني بشدة حيثما تنفَّذ معايير متعددة من هيئات مختلفة ضمن المنتج. وينبغي الاعتراف بأن نظام الاختبار وحده، رغم جاذبيته ظاهرياً، يُستبعد أن يُحدث أي تغيير حقيقي في الأوضاع لمعالجة المنتجات المزيَّفة.

وتجدر الإشارة إلى أنه بالتطور المتزايد في معارف المزورين، يمكن للمنتجات المزيَّفة أن تلبي المتطلبات التقنية الموصَّفة وأن تعمل بينياً مع منتجات أصلية. وعلى هذا النحو، يمكن أن تتوافق المنتجات المزيَّفة مع مجموعة المعايير التقنية ذات الصلة وأن تجتاز اختبار

المطابقة وقابلية التشغيل البيني. وفي هذه الحالة، لا يمكن إلا لصاحب العلامة التجارية يميز بدقة المنتجات المزيَّفة عن المنتجات الأصلية عن طريق إجراء تقييم للمنتج.

وقد تناولت ورشة العمل الإقليمية، التي نظمها الاتحاد بشأن سد الفجوة التقييسية من أجل المنطقتين العربية والإفريقية (في الجزائر 26–28 سبتمبر 2011)، مشكلة معدات تكنولوجيا المعلومات والاتصالات المزيفة، وصدر توجيه لتشجيع تبادل المعلومات على المستوى الإقليمي من خلال إنشاء قاعدة بيانات تحتوي على المنتجات المزيَّفة المدرجة في القائمة السوداء http://www.itu.int/ITU-T/newslog/ITU+Regional+Workshop+On+Bridging+The+Standardization+Gap+For+Arab+And+Africa+Regions+Interactive+Training+Session+And+Academia+Session.aspx.

وخلال الجلسة الإعلامية التي عقدها الفريق الاستشاري لتقييس الاتصالات (TSAG) بشأن تقييم المطابقة وقابلية التشغيل البيني (جنيف، في 13 يناير 2012) وكذلك منتدى الاتحاد بشأن المطابقة وقابلية التشغيل البيني للمنطقتين العربية والإفريقية (تونس، في 5-7 نوفمبر 2012)، سُلط الضوء على ما خلصت إليه المنطقة العربية من أن المعدات المزيَّفة مشكلة مرهقة، وخاصةً في سوق الهواتف المتنقلة، وكذلك على الحاجة إلى التعاون العالمي في هذا الصدد http://www.itu.int/ITU-D/tech/events/2012/CI_ARB_AFR_Tunis_November12/Presentations/Session5/CI%20Forum%202012_Tunis_AAlDin_S5_4.pdf، [http://www.itu.int/dms_pub/itu-t/oth/06/5B/T065B00000E0005PPTE.pptx].

وخلال اجتماع الجمعيات التنظيمية الذي نظمه قطاع تنمية الاتصالات بالاتحاد (سري لانكا، كولومبو، في 1 أكتوبر 2012) وفقاً للقرار 48 (المراجَع في حيدر آباد، 2010) بشأن "تعزيز التعاون بين هيئات تنظيم الاتصالات" والذي دعا الاتحاد لأن ينظم وينسق ويسهّل الأنشطة التي من شأنها تعزيز تبادل المعلومات بين الهيئات التنظيمية والجمعيات التنظيمية بصدد المسائل التنظيمية الرئيسية على المستوى الدولي والإقليمي، نُظر في قضية سرقة الأجهزة المتنقلة وفي السوق الرمادية والأجهزة المزيَّفة وتأثيرها على الصناعة وعلى المشغلين وعلى الحكومات وعلى المستخدمين. وأوضح ممثلو 10 جمعيات تنظيمية إقليمية، تشمل ARCTEL-CPLP وAREGNET وARTAC وEMERG وFRATEL وREGULATEL وOCCUR وFTRA وSATRC وAPT، أن الإجراءات الإقليمية يمكن أن تعود بفوائد جمة في هذا المجال، ومنها مثلاً:

- التشارك في قواعد بيانات القائمة السوداء لأجهزة النظام العالمي للاتصالات المتنقلة (GSM) وأجهزة النفاذ المتعدد بتقسيم شفري (CDMA) من خلال توقيع اتفاقات ثنائية أو متعددة الأطراف؛
- التزام دوائر الصناعة بتوصيات الأمن ضد إعادةً برمجة المكرر من الهويات الدولية للمعدات المتنقلة (IMEI) أو أرقام التعرف التسلسلية الإلكترونية للشركة المصنعة؛
- إنشاء آليات تنظيمية مالية و/أو جمركية تضمن تشديد المراقبة على الهواتف المستوردة، ومنع خروج أو إعادةً تصدير ما يُسرق من المطاريف المتنقلة و/أو قطعها؛
- شن حملات لرفع الوعي العام بأهمية الإبلاغ عن سرقة وفقدان المطاريف المتنقلة.

وأوضحت العديد من الجمعيات الإقليمية تجاربها في هذا الشأن وأقرت بحراجة المشكلة وبأنها تحتاج إلى معالجة بالتعاون مع دوائر الصناعة والمشغلين. واعتمد اجتماع الجمعيات التنظيمية توصية تدعو الاتحاد الدولي للاتصالات لإجراء دراسات، بالتعاون مع جمعية النظام العالمي للاتصالات المتنقلة (GSM)، بشأن قضية سرقة الأجهزة المتنقلة، والسوق الرمادية والأجهزة المزيَّفة، ولتقديم مبادئ توجيهية وتوصيات في هذا الصدد http://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR12/RA12/pdf/FinalReport_RA12.pdf.

12 المراجع

[1] *The Economic Impact of Counterfeiting and Piracy*, OECD, June 2008.

[2] http://www.oecd.org/sti/ind/44088872.pdf

[3] http://www.icc-ccs.org/icc/cib

[4] *Estimating the global economic and social impacts of counterfeiting and piracy*. http://www.iccwbo.org/uploadedFiles/BASCAP/Pages/Global%20Impacts%20-%20Final.pdf

[5] Intellectual Property Rights Fiscal Year 2100 Seizure Statistics U.S. Customs and Border Protection. http://www.ice.gov/doclib/iprcenter/pdf/ipr-fy-2011-seizure-report.pdf

[6] http://www.havocscope.com/counterfeit-hp-printing-supplies

[7] http://www.spotafakephone.com/

[8] IDC February 2012 http://www.idc.com/getdoc.jsp?containerId=prUS23297412

[9] http://www.gpo.gov/fdsys/pkg/CRPT-112srpt167/pdf/CRPT-112srpt167.pdf

[10] *Defence Industrial Base Assessment: Counterfeit Electronics*, January 2010 http://www.bis.doc.gov/index.php/forms-documents/doc_view/37-defense-industrial-base-assessment-of-count

[11] http://www.gpo.gov/fdsys/pkg/BILLS-112hr1540enr/pdf/BILLS-112hr1540enr.pdf HR 1540 SEC. 818

[12] In *WIPO Intellectual Property Handbook* http://www.wipo.int/edocs/pubdocs/en/intproperty/489/wipo_pub_489.pdf

[13] UK IP Toolkit 2009.

[14] http://www.wipo.int/treaties/en/ip/paris/trtdocs_wo020.html

[15] http://www.wipo.int/treaties/en/ip/washington

[16] www.wcoipm.org and http://ipmpromo.wcoomdpublications.org/

[17] void

[18] http://www.unece.org/trade/wp6/SectoralInitiatives/MARS/MARS.html

[19] https://www.gov.uk/government/publications/annual-ip-crime-report-2013-to-2014

[20] http://www.aca.go.ke

[21] http://www.iccwbo.org/advocacy-codes-and-rules/bascap/welcome-to-bascap/

[22] http://www.iccwbo.org/bascap/id7608/index.html

[23] http://www.pasdirectory.com

[24] http://www.iccwbo.org/bascap/id42204/index.html

[25] http://www.iccwbo.org/policy/ip/id2950/index.html

[26] http://www.iacc.org/

[27] http://www.ascdi.com/

[28] http://www.anticounterfeitingforum.org.uk

[29] http://archive.basel.int/convention/basics.html

[30] http://www.ier.org.tw/smm/6_PAS_141_2011_Reuse_Of_WEEE_And_UEEE.pdf

[31] http://www.bbc.co.uk/panorama/hi/front_page/newsid_9483000/9483148.stm

[32] http://www.bbc.co.uk/news/world-europe-10846395

[33] *Recycling – From E-Waste to Resources*, UNEP, 2009.

[34] Directive 2002/96/EC.

[35] BSI PAS141:2011, *Reuse of used and waste electrical and electronic equipment* (UEEE and WEEE). Process Management Specification (March 2011) http://shop.bsigroup.com/en/ProductDetail/?pid=000000000030245346

[36] http://www.numberingplans.com/?page=analysis&sub=imeinr

[37] IMEI Allocation and Approval Process, Version 7.0, GSMA, 31 October 2013.

[38] http://www.gsma.com/imei-database

[39] http://www.c4dlab.ac.ke/wp-content/uploads/2014/04/VAT-Report_TKO.pdf

[40] Annual Report of the National Commission for the State Regulation of Communications and Informatization for 2012. http://www.nkrzi.gov.ua/images/upload/142/3963/4b2c475b68c147860c36a6e1fc2a3e47.pdf

[41] GS1 EPC Tag Data Standard 1.6, 9 September 2011. http://www.gs1.org/sites/default/files/docs/epc/tds_1_6-RatifiedStd-20110922.pdf

[42] ISO/IEC 15459, *Unique identifiers*.

Part 1:2014, *Information technology – Automatic identification and data capture techniques – Unique identification – Part 1: Individual transport units*.

Part 2:2006, *Information technology – Unique identifiers – Registration procedures*.

Part 3:2014, *Information technology – Automatic identification and data capture techniques – Unique identification – Part 3: Common rules*.

Part 4:2014, *Information technology – Automatic identification and data capture techniques – Unique identification – Part 4: Individual products and product packages*.

Part 5:2014, *Information technology – Automatic identification and data capture techniques – Unique identification – Part 5: Individual returnable transport items (RTIs)*.

Part 6:2014, *Information technology – Automatic identification and data capture techniques – Unique identification – Part 6: Groupings*.

Part 8:2009, *Information technology – Part 8: Grouping of transport units*.

[43] ISO 6346:1995, *Freight containers – Coding, identification and marking*.

[44] ISO 3779:2009, *Road vehicles – Vehicle identification number (VIN) – Content and structure*.

[45] ISO 10486:1992, *Passenger cars – Car radio identification number (CRIN)*.

[46] ISO 2108:2005, *Information and documentation – International standard book number (ISBN)*.

[47] ISO 3297:2007, *Information and documentation – International standard serial number (ISSN)*.

[48] ISO 12931:2012, *Performance criteria for authentication solutions used to combat counterfeiting of material goods*.

[49] http://www.uidcenter.org/learning-about-ucode

[50] Recommendation ITU-T X.668 (2008) | ISO/IEC 9834-9:2008, *Information technology – Open Systems Interconnection – Procedures for the operation of OSI Registration Authorities: Registration of object identifier arcs for applications and services using tag-based identification*.

[51] Recommendation ITU-T F.771 (2008), *Service description and requirements for multimedia information access triggered by tag-based identification*.

[52] Recommendation ITU-T H.621 (2008), *Architecture of a system for multimedia information access triggered by tag-based identification*.

[53] ISO 28219:2009, *Packaging – Labelling and direct product marking with linear bar code and two-dimensional symbols*.

[54] ISO 22742:2010, *Packaging – Linear bar code and two-dimensional symbols for product packaging*.

[55] ISO 15394:2009, *Packaging – Bar code and two-dimensional symbols for shipping, transport and receiving labels*.

[56] ISO/IEC 15963:2009, *Information technology – Radio frequency identification for item management – Unique identification for RF tags*.

[57] ISO/IEC 29167-1:2014, *Information technology – Automatic identification and data capture techniques – Part 1: Security services for RFID air interfaces*.

[58] ISO/IEC TR 24729-4:2009, *Information technology – Radio frequency identification for item management – Implementation guidelines – Part 4: Tag data security*.

[59] http://www.gs1.org/gsmp/kc/epcglobal

[60] Recommendation ITU-T X.509 (2012) | ISO/IEC 9594-8:2014, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

[61] IETF RFC 3280 (2002), *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.

[62] IETF RFC 3279 (2002), *Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.

[63] http://www.wcoomd.org

[64] IEC/TS 62668-1 ed2.0 (2014), *Process management for avionics – Counterfeiting prevention – Part 1: Avoiding the use of counterfeit, fraudulent and recycled electronic components*.

[65] IEC/TS 62668-2 ed1.0 (2014), *Process management for avionics – Counterfeit prevention – Part 2: Managing electronic components from non-franchised sources*.

[66] Adapted from Market Surveillance Regulation EC no 765/2008, art 2 (17), http://www.unece.org/fileadmin/DAM/trade/wp6/documents/2009/WP6_2009_13e_final.pdf

[67] Recommendation M. on the: *Use of Market Surveillance Infrastructure as a Complementary Means to Protect Consumers and Users against Counterfeit Goods*. http://www.unece.org/fileadmin/DAM/trade/wp6/Recommendations/Rec_M.pdf

[68] http://www.nia.din.de/gremien/NA+043-01-31+AA/en/54773446.html

[69] http://www.anticounterfeitingforum.org.uk/best_practice.aspx

[70] http://www.cti-us.com/CCAP.htm]

[71] http://www.ipo.gov.uk/ipctoolkit.pdf

[72] http://www.itu.int/ITU-D/tech/NGN/ConformanceInterop/PP10_Resolution177.pdf

[73] Establishing Conformity and Interoperability Regimes – Basic Guidelines (ITU, 2014).

[74] *Guidelines for developing countries on establishing conformity assessment test labs in different regions*, ITU, 2012: www.itu.int/ITU-D/tech/ConformanceInteroperability/ConformanceInterop/ Guidelines/ Test_lab_guidelines_EV8.pdf

[75] IEC 62321:2008, *Electrotechnical products – Determination of levels of six regulated substances (lead, mercury, cadmium, hexavalent chromium, polybrominated biphenyls, polybrominated diphenyl ethers)*.

[76] Recommendation ITU-T E.164 (2010), *The international public telecommunication numbering plan*.

[77] ISO/IEC 15962:2013, *Information technology – Radio frequency identification (RFID) for item management – Data protocol: data encoding rules and logical memory functions*.

[78] ISO/IEC 15961:2004, *Information technology – Radio frequency identification (RFID) for item management – Data protocol: application interface*.

[79] Recommendation ITU-T X.1255 (2013), *Framework for discovery of identity management information*.

[80] ISO/IEC 15420:2009, *Information technology – Automatic identification and data capture techniques – EAN/UPC bar code symbology specification*.

[81] ISO/IEC 16388:2007, *Information technology – Automatic identification and data capture techniques – Code 39 bar code symbology specification*.

[82] ISO/IEC 15417:2007, *Information technology -- Automatic identification and data capture techniques – Code 128 bar code symbology specification*.

[83] ISO/IEC 15438:2006, *Information technology – Automatic identification and data capture techniques – PDF417 bar code symbology specification*.

[84] ISO/IEC 16023:2000, *Information technology – International symbology specification – MaxiCode*.

[85] ISO/IEC 18004:2006, *Information technology – Automatic identification and data capture techniques – QR Code 2005 bar code symbology specification*.

[86] ISO/IEC 16022:2006, *Information technology – Automatic identification and data capture techniques – Data Matrix bar code symbology specification*.

[87] DIN 66401 (2010), *Unique Identification Mark (UIM)***.**

[88] ANSI MH10.8.2-2010, *Data Identifier and Application Identifier Standard***.**

[89] ANSI/HIBC 2.3-2009, *The Health Industry Bar Code (HIBC) Supplier*.

[90] ISO/IEC 7816-6:2004, *Identification cards – Integrated circuit cards – Part 6: Interindustry data elements for interchange.*

[91] ISO 14816:2005, *Road transport and traffic telematics – Automatic vehicle and equipment identification – Numbering and data structure.*

[92] ANSI INCITS 256-2007, *Radio Frequency Identification (RFID)*.

[93] ANSI INCITS 371.1-2003, *Information technology - Real Time Locating Systems (RTLS) Part 1: 2.4 GHz Air Interface Protocol.*

[94] ISO/IEC 18000-6:2013, *Information technology – Radio frequency identification for item management – Part 6: Parameters for air interface communications at 860 MHz to 960 MHz General*.

[95] ISO/IEC 18000-3:2010, *Information technology – Radio frequency identification for item management – Part 3: Parameters for air interface communications at 13,56 MHz*.

[96] ISO 11784:1996, *Radio frequency identification of animals – Code structure*.

[97] ISO 11785:1996, *Radio frequency identification of animals – Technical concept*.

[98] ISO/IEC 18000 (All Parts), *Information technology – Radio frequency identification for item management*.

[99] ISO 17363:2013, *Supply chain applications of RFID – Freight containers*.

[100] ISO 17364:2013, *Supply chain applications of RFID – Returnable transport items (RTIs) and returnable packaging items (RPIs)*.

[101] ISO 17365:2013, *Supply chain applications of RFID – Transport units*.

[102] ISO 17366:20`3, *Supply chain applications of RFID – Product packaging*.

[103] ISO 17367:2013, *Supply chain applications of RFID – Product packaging*.

[104] ISO 18185 (All Parts), *Freight containers – Electronic seals*.

[105] ISO/IEC 29160:2012, *Information technology – Radio frequency identification for item management – RFID Emblem*.

[106] ISO/IEC 15693, *Identification cards – Contactless integrated circuit cards – Vicinity cards*.

[107] ISO 28000:2007, *Specification for security management systems for the supply chain*.

[108] ISO 28001:2007, *Security management systems for the supply chain – Best practices for implementing supply chain security assessments and plans – Requirements and guidance*.

[109] ISO 28003:2007, *Security management systems for the supply chain – Requirements for bodies providing audit and certification of supply chain security management systems*.

[110] ISO 28004-1:2007, *Security management systems for the supply chain – Guidelines for the implementation of ISO 28000 – Part 1: General principles*.

[111] ISO 28005-2:2011, *Security management systems for the supply chain – Electronic port clearance (EPC) – Part 2: Core data elements.*

[112] SAE AS5553 (2013), *Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition*.

[113] SAE ARP6178 (2011), *Fraudulent/Counterfeit Electronic Parts; Tool for Risk Assessment of Distributors*.

[114] SAE AS6081 (2012), *Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition – Distributors Counterfeit Electronic Parts; Avoidance Protocol, Distributors.*

[115] SAE AS6171 (2010), *Test Methods Standards; Counterfeit Electronic Parts*.

[116] ISO 16678:2014, *Guidelines for interoperable object identification and related authentication systems to deter counterfeiting and illicit trade*.

[117] IDEA-STD-1010A (2006), *Acceptability of Electronic Components Distributed in the Open Market*.

[118] IDEA-QMS-9090 (2013), *Quality Management System Standard*.

مسرد العبارات المختصرة

AC	صنف التوزيع *(Allocation Class)*
ADI	معرف الفضاء الجوي والدفاع *(Aerospace and Defence Identifier)*
AIDC	التعرف التلقائي ونقل البيانات *(Automatic Identification and Data Capture)*
ALE	حدث طبقة التطبيق *(Application Layer Event)*
AWP	مكان عمل مؤتمت *(Automated Working Place)*
CB	هيئة منح شهادات *(Certification Body)*
CBV	مفردات الأعمال الأساسية *(Core Business Vocabulary)*
cc	شفرة الصنف *(class code)*
CD	قرص مدمج *(Compact Disc)*
CDMA	النفاذ المتعدد بتقسيم شفري *(Code Division Multiple Access)*
CDR	سجل تفاصيل المكالمة *(Call Detail Record)*
CEIR	السجل المركزي لهوية المعدات *(Central Equipment Identity Register)*
CIPS	نظام حماية المعلومات الشامل *(Comprehensive Information Protection System)*
CoPC	شهادة كفاءات الموظفين *(Certification of Personnel Competencies)*
DB	قاعدة بيانات *(DataBase)*
DCI	الاكتشاف والتشكيل والتهيئة *(Discovery, Configuration and Initialisation)*
DNS	نظام أسماء ميادين الإنترنت *(Domain Name System)*
DVD	القرص الرقمي متعدد الاستخدامات *(Digital Versatile Disc)*
EIR	سجل هوية المعدات *(Equipment Identity Register)*
EMC	التوافق الكهرمغنطيسي *(Electromagnetic Compatibility)*
EPC	شفرة المنتج الإلكترونية *(Electronic Product Code)*
EPCIS	خدمة معلومات شفرة المنتج الإلكترونية *(EPC Information Service)*
GDTI	المعرف العالمي لنمط الوثيقة *(Global Document Type Identifier)*
GIAI	المعرف العالمي للأصل الفردي *(Global Individual Asset Identifier)*
GID	معرِّف عام *(General Identifier)*
GII	برنامج غرس هويات IMEI الأصلية *(Genuine IMEI Implant programme)*
GINC	الرقم العالمي لهوية الإرسالية *(Global Identification Number for Consignment)*
GLN	رقم موقع عالمي *(Global Location Number)*
GRAI	المعرف العالمي للأصل القابل للإرجاع *(Global Returnable Asset Identifier)*
GSIN	الرقم العالمي لهوية الشحنة *(Global Shipment Identification Number)*
GSM	النظام العالمي للاتصالات المتنقلة *(Global System for Mobile communications)*
GSRN	الرقم العالمي للعلاقة الخدمية *(Global Service Relation Number)*
GTIN	رقم بند التجارة العالمي *(Global Trade Item Number)*

HF	الترددات العالية *(High Frequency)*
ic	شفرة التعرف *(identification code)*
IC	دارة متكاملة *(Integrated Circuit)*
ICT	تكنولوجيا المعلومات والاتصالات *(Information and Communication Technology)*
ID	تعرف الهوية *(Identification)*
IMEI	الهوية الدولية للمعدات المتنقلة *(International Mobile Equipment Identity)*
IP	الملكية الفكرية *(Intellectual Property)*
IP	بروتوكول الإنترنت *(Internet Protocol)*
IPM	سطح التماس بين عامة الناس والأعضاء *(Interface Public-Members)*
IPR	حقوق الملكية الفكرية *(Intellectual Property Rights)*
ISBN	الرقم الدولي المعياري للكتاب *(International Standard Book Number)*
ISSN	الرقم التسلسلي الدولي الموحد *(International Standard Serial Number)*
IT	تكنولوجيا المعلومات *(Information Technology)*
LLRP	بروتوكول القارئ منخفض المستوى *(Low Level Reader Protocol)*
LTE	التطور الطويل الأمد *(Long-Term Evolution)*
ME	جهاز متنقل *(Mobile Equipment)*
MEID	هوية جهاز متنقل *(Mobile Equipment Identity)*
MIIM	التعرف على البند المتنقل وإدارته *(Mobile Item Identification and Management)*
MRA	اتفاق اعتراف متبادل *(Mutual Recognition Agreement)*
MSC	مركز تبديل الاتصالات المتنقلة *(Mobile Switching Centre)*
MSISDN	المشترك المتنقل في الشبكة الرقمية للخدمات المتكاملة *(Mobile Subscriber Integrated Services Digital Network)*
NIR	إشعاع غير مؤين *(Non-Ionizing Radiation)*
OID	معرف كائن *(Object Identifier)*
ONS	خدمة تسمية الكائن *(Object Naming Service)*
QoS	جودة الخدمة *(Quality of Service)*
RF	الترددات الراديوية *(Radio Frequency)*
RFID	التعرف بواسطة الترددات الراديوية *(Radio Frequency Identification)*
RM	إدارة الجهاز القارئ *(Reader Management)*
RoHS	تقييد المواد الخطرة *(Restriction of Hazardous Substances)*
RP	بروتوكول القارئ *(Reader Protocol)*
RUIM	وحدة هوية المستخدم القابلة للإزالة *(Removable User Identity Module)*
SFP	مقدم ميزات الأمن *(Security Features Provider)*
SGLN	رقم الموقع العالمي مع توسعة أو بدونها *(Global Location Number with or without Extension)*
SGTIN	رقم بند التجارة العالمي المسلسل *(Serialized Global Trade Item Number)*

SIM وحدة هوية المشترك *(Subscriber Identity Module)*

SLDc شفرة الميدان ذات المستوى الثاني *(Second Level Domain code)*

SMD الدارات المركَّبة على السطح *(Surface-Mounted Device)*

SMS خدمة الرسائل القصيرة *(Short Message Service)*

SNMP بروتوكول إدارة الشبكات البسيط *(Simple Network Management Protocol)*

SS7 نظام التشوير رقم 7 *(Signalling System No. 7)*

SSCC الشفرة التسلسلية لحاوية الشحن *(Serial Shipping Container Code)*

TAC شفرة توزيع النمط *(Type Allocation Code)*

TC لجنة تقنية *(Technical Committee)*

TDS معيار بيانات الوسم *(Tag Data Standard)*

TDT ترجمة بيانات الوسم *(Tag Data Translation)*

TID هوية الوسم *(Tag ID)*

TLDc شفرة الميدان ذات المستوى الأعلى *(Top Level Domain code)*

TV تلفزيون *(TeleVision)*

UHF الترددات فائقة العلو *(Ultra High Frequency)*

UII معرف البند المتفرِّد *(Unique Item Identifier)*

UIM علامة تعرُّف متفرِّدة *(Unique Identification Mark)*

UMTS نظام الاتصالات المتنقلة العالمي *(Universal Mobile Telecommunications System)*

UPC رمز المنتج العالمي *(Universal Product Code)*

URL المحدد الموحد لموقع المورد *(Uniform Resource Locator)*

USB المنفذ التسلسلي العام *(Universal Serial Bus)*

WG فريق عمل *(Working Group)*

الملحق A

أنظمة تعرف على الأجهزة المتنقلة المزيَّفة

كما أُوضح سابقاً في هذا التقرير التقني، كانت الأجهزة المتنقلة المزيَّفة ولا زالت تثير قلقاً خاصاً، وقد اتُّخذ عدد من المبادرات للحد من انتشار الأجهزة المتنقلة المزيَّفة. وكان القصد من بعض هذه المخططات في البداية التأكد من استيراد الأجهزة المتنقلة وفقاً للإجراءات القانونية (أي من عدم كونها مهربة) ثم تبينت فائدتها في وقت لاحق لمنح الثقة بكون الأجهزة غير مزيفة. وتشترك هذه المخططات في العديد من الخصائص مع المبادرات المصممة خصيصاً لمعالجة مشكلة التزييف، مثل كونها مبنية على الاستيقان من معرف متفرِّد (الهوية الدولية للمعدات المتنقلة (IMEI)).

وتعرض الفقرات التالية أمثلة عن التدابير التي تتخذها السلطات الوطنية وتلك المتخَذة على المستوى الإقليمي.

1.A أمثلة عن التدابير التي اتخذتها الإدارات والهيئات التنظيمية الوطنية

1.1.A أذربيجان

تأسس نظام تسجيل الأجهزة المتنقلة (MDRS) http://www.rabita.az/en/c-media/news/details/134 في مركز حاسوب المعلومات (ICC) بوزارة الاتصالات وتكنولوجيا المعلومات وفق "قواعد تسجيل الأجهزة المتنقلة" التي أُقرت بالقرار رقم 212، بتاريخ 28 ديسمبر 2011 الصادر عن مجلس وزراء جمهورية أذربيجان.

والغرض من تسجيل جهاز الهاتف المتنقل هو منع استيراد الأجهزة ذات الجودة المتدنية مجهولة المنشأ التي لا تستوفي المعايير التقنية المطلوبة، كتلك التي تحد من انبعاث الإشعاع الكهرمغنطيسي الضار، وزيادة الاعتراف بالقدرة التنافسية لشركات التصنيع. إذ يحول نظام التسجيل دون استخدام الأجهزة المتنقلة المفقودة/المسروقة وتلك المستوردة بطريقة غير قانونية إلى البلاد.

ومنذ 1 مارس 2013، صار مشغلو الاتصالات المتنقلة يُدخلون أرقام الهوية الدولية للمعدات المتنقلة (IMEI) للهواتف المتنقلة المستخدمة في أذربيجان إلى نظام قاعدة بيانات مركزي يومياً. وأفادت وزارة الاتصالات وتكنولوجيا المعلومات بتسجيل أكثر من 12 مليون جهاز GSM بعد إطلاق نظام تسجيل الأجهزة المتنقلة. وسُمح لنحو 300 000 من الأجهزة التي لا تستوفي المعايير بمواصلة العمل بأرقام هواتفها المتنقلة الحالية، ولكن أياً من الأجهزة الجديدة التي لا تستوفي المعايير لن تعمل في البلاد http://www.mincom.gov.az/media-en/news-2/details/1840.

واعتبرت أرقام الهوية الدولية للمعدات المتنقلة (IMEI) لجميع الأجهزة المتنقلة المستخدمة في الشبكة قبل 1 مايو 2013 مسجلةً، وبالتالي فهي تعمل بحرية في الشبكات. وبعد إطلاق نظام التسجيل، ينبغي تسجيل رقم الهوية الدولية للمعدات المتنقلة (IMEI) لكل جهاز متنقل مستورد إلى البلاد للاستخدام الخاص (مع بطاقة SIM صادرة عن أحد مشغلي الاتصالات المتنقلة في البلاد) في غضون 30 يوماً من تاريخ توصيله بالشبكة. ولا تسري هذه القاعدة على تجوال الأجهزة المتنقلة المستخدِمة لبطاقات SIM مقدَمة من مشغلين أجانب.

ويمكن للمشتركين تحديد شرعية أجهزتهم على أساس أرقام الهوية الدولية للمعدات المتنقلة (IMEI) لديهم باستخدام صفحة إلكترونية خاصةً على شبكة الإنترنت (imei.az) أو عن طريق استخدام رسائل SMS.

وأنشئ نظام قاعدة بيانات مركزية في مركز حاسوب المعلومات (ICC) بوزارة الاتصالات وتكنولوجيا المعلومات، وفي الوقت نفسه، ركَّب مشغلو الاتصالات المتنقلة المعدات المناسبة المتزامنة مع قاعدة البيانات المركزية. وأعد مختصون محليون برمجيات نظام تسجيل الأجهزة المتنقلة.

2.1.A البرازيل

SIGA – النظام المتكامل لإدارة الأجهزة

نصت لائحة الخدمة المتنقلة للوكالة الوطنية البرازيلية للاتصالات – ANATEL على أن ما يسمح به المشغلون من أجهزة تُستخدم على شبكاتهم، وما يستخدمه المستخدمون من أجهزة، ينبغي أن يقتصر على الأجهزة التي اعتمدتها وكالة ANATEL (الفقرة الرابعة من المادة 8 والفقرة الخامسة من المادة 10 في لائحة الخدمة المتنقلة التي أقرها القرار 2007/477[9]). وبناءً على ذلك، ألزمت وكالة ANATEL مشغلي الاتصالات المتنقلة البرازيليين بالتنفيذ المشترك لحل تكنولوجي للحد من استخدام الأجهزة المتنقلة غير المعتمدة أو التي جرى العبث بها أو ذات الهوية الدولية المستنسخة للمعدات المتنقلة.

وحددت خطة العمل، المرعية المقدمة من المشغلين للوفاء بهذا الالتزام، من بين أمور أخرى، الخطوط العريضة للحلول التكنولوجية التي سيجري تنفيذها، والمعايير الممكنة المستندة إلى مستخدمين حقيقيين من أجل تقليل الآثار على السكان إلى أدنى حد، والمعايير التي سيجري تنفيذها بالنسبة إلى المستخدمين الجدد بعد دخول الحل حيز التنفيذ حيث يقتصر النفاذ إلى الشبكة على الأجهزة الملتزمة بلائحة وكالة ANATEL، والمعايير التي سيجري تنفيذها بالنسبة لمستخدمي الهواتف المتنقلة من أجل تجنب إرباك المستخدمين أو المستخدمين الأجانب، وحملات التوعية بشأن مستخدمي شبكة الاتصالات المتنقلة.

ووافقت وكالة ANATEL على خطة العمل في عام 2012 آخذةً بعين الاعتبار الجوانب التقنية والتنظيمية. وكان الحل يسمى النظام المتكامل لإدارة الأجهزة أو SIGA اختصاراً، ويجري تطويره على أساس المنطلقات التقنية التالية:

- حل مركزي يضعه بشكل مشترك جميع مشغلي شبكات الاتصالات المتنقلة البرازيلية؛
- حل متكامل مع مشغلي المنصات المتنقلة؛
- حل مؤتمت يسمح بإدخال المعلومات بقدر يسير من التدخل البشري؛
- يتيح النمو والتعقيد على أساس إمكانية الاستيعاب التناسبي والتوسعة؛
- دينامي ومرن بقواعد يمكن تعديلها بمرور الزمن؛
- يتكون من مصادر متعددة للمعلومات مثل سجلات تفاصيل المكالمات (CDR) ومشغلي أنظمة الإدارة، بما في ذلك استخدام قواعد البيانات الدولية حسب الاقتضاء، من بين أمور أخرى؛
- كفء للسماح باتخاذ الإجراءات الكفيلة بالحد من استخدام الأجهزة غير المشروعة؛
- قادر على التقليل إلى أدنى حد من الآثار المحتملة على المستخدمين النهائيين العاديين؛
- موثوق وآمن.

واليوم تقوم جمعية ABR Telecom[10] بالتشغيل التقني لنظام SIGA، وهي جمعية تقنية أنشئت كمشروع مشترك بين معظم شركات الاتصالات البرازيلية لتطوير حلول تقنية مركزية لسوق الاتصالات البرازيلي ولنشرها وتشغيلها.

وفي هذا المشروع، هناك تفاعل قوي مع جميع الأطراف الأخرى المعنية بضمان نجاح نظام SIGA، مثل وكالة ANATEL وسلطات الجمارك ورابطة المشغلين (SindiTelebrasil) والمشغلين ومصنعي المعدات، واتحاد المصنعين (ABINEE) وجمعية ABR Telecom. أضف إلى ذلك أن المسألة معقدة لأنها تنطوي على جميع مجالات المشغِّل، والعديد من الجهات الفاعلة في السوق وكذلك المستخدم النهائي. ويتطلب الأمر مناقشةً مستفيضة لجميع الإجراءات.

9 http://legislacao.anatel.gov.br/resolucoes/2007/9-resolucao-477

10 http://www.abrtelecom.com.br

وينشط نظام SIGA على شبكة المشغلين منذ مارس 2014، فيجمع المعلومات المطلوبة لتشخيص حجم سوق الأجهزة غير الملتزمة باللائحة البرازيلية، حتى يتسنى لجميع الأطراف المعنية أن تحدد الإجراءات اللازمة لضمان إخلاء الشبكة من هذه الأجهزة المزيَّفة، وتلك دون المستوى المطلوب وغير المخوَّلة، بالحد الأدنى من التأثير على المستهلك.

وأحد الإجراءات التي يمكن اتخاذها في النقاش الدائر لتحقيق هذا المسعى يتمثل في إنشاء قاعدة بيانات للأجهزة القديمة تحتوي على جميع الحالات (حالات علاقة متفرِّدة بين مطراف ومستخدميه) التي يُسمح لها بالاستمرار في العمل على الشبكة مع حجب النفاذ إلى الشبكة لأي مطراف جديد غير نظامي. وإلى ذلك، يخف التأثير على المستخدم كثيراً، وينبغي أن تختفي قاعدة بيانات الأجهزة القديمة إذ تتجدد الأجهزة.

وبالإضافة إلى ذلك، من المهم إشراك جهات تمثل المستخدم في هذا النقاش وتنفيذ خطة تواصل قوية قبل اتخاذ أي إجراءات تؤثر بصورة مباشرة على المستخدم (مثل حجب أو تعليق استخدام الجهاز).

وإلى ذلك، يضع المشغلون ووكالة ANATEL واتحاد المصنعين معاً خطة تواصل لنظام SIGA، ينبغي أن تنفذها جميع هذه الجهات في جهد منسق عبر جميع قنوات التواصل مع المستهلك (مثل الإعلانات الدعائية، وفواتير المشغلين ومراكز النداء) لاطلاع المستخدمين على مزايا شراء مطاريف قانونية ومعتمدة وعلى المخاطر التي يقدمون عليها عند استخدام مطاريف مزيَّفة ودون المستوى المطلوب في السيناريو البرازيلي.

ويمكن الحصول على معلومات أوفى بتفاصيلها عن الجانب التقني لهذا المشروع مباشرة مع وكالة الوطنية للاتصالات - ANATEL لدى الإدارة البرازيلية.[11]

3.1.A كولومبيا

في عام 2011، أصدرت وزارة تكنولوجيا المعلومات والاتصالات المرسوم 1630 بغرض وضع آليات تهدف إلى السيطرة على تسويق وبيع أجهزة المطاريف الجديدة والمستعملة وإنشاء نوعين من قواعد البيانات المركزية: قاعدة بيانات فيها سجل بأرقام الهوية الدولية للمعدات المتنقلة (IMEI) لأجهزة المطاريف المبلَّغ عن سرقتها أو فقدانها حيث يُمنع استخدامها أو تفعيلها، وقاعدة بيانات أخرى فيها سجل بأرقام الهوية الدولية للمعدات المتنقلة (IMEI) المسجلة لأجهزة المطاريف المستوردة أو المصنعة قانونياً في البلاد والمشفوعة برقم هوية المالك أو المشترك لكل منها.

وينص القانون 1453 الصادر في 24 يونيو 2011 بشأن أمن المواطن على أحكام مدتها من 6 إلى 8 سنوات سجناً لمن يعبث بهوية IMEI لجهاز المتنقل أو يعيد برمجتها أو يغير تسميتها أو يعدلها، ولمن يفعِّل أجهزة جرى التبليغ عن سرقتها. وبالإضافة إلى ذلك، تصادَر المعدات التي جرى تغييرها http://www.gsma.com/latinamerica/wp-content/uploads/2012/05/Final-CITEL-Resolution-on-Handset-Theft.pdf.

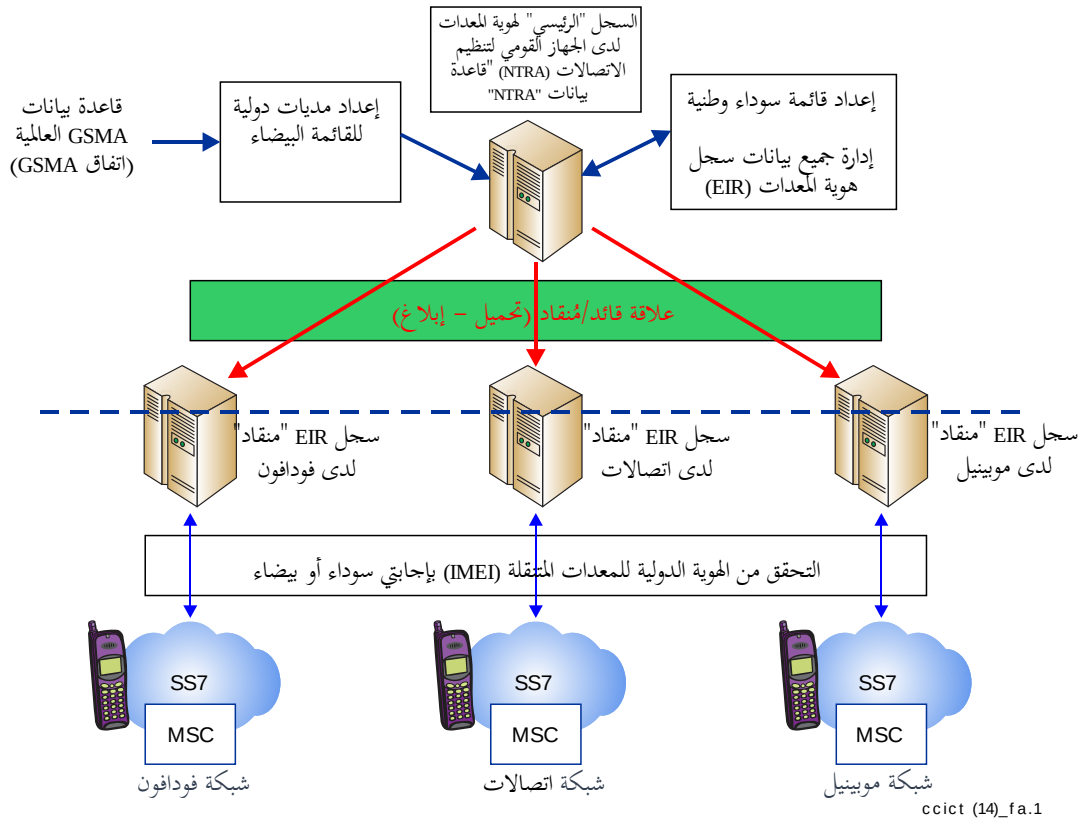
وقد اتخذت هذه المبادرات للسيطرة على بيع الأجهزة المتنقلة المسروقة واستخدامها، ولكن يرجَّح أيضاً أن يكون لها تأثير على استخدام المنتجات المزيَّفة.

4.1.A مصر

في عام 2008، أنشأ الجهاز القومي لتنظيم الاتصالات (NTRA) دائرة مراقبة السوق لدعم أنشطة اعتماد النوع. واعتُمد نظام في مصر في عام 2010 لمكافحة استخدام معدات المطاريف المتنقلة المزيَّفة. ويستفيد هذا النظام من قاعدة بيانات الهوية الدولية للمعدات المتنقلة في جمعية النظام العالمي للاتصالات المتنقلة (GSMA IMEI DB) ليقدم تحديثاً أسبوعياً للقائمة البيضاء لشفرة توزيع نمط (TAC) الهوية الدولية للمعدات المتنقلة (IMEI TAC) وللسجل المركزي لهوية المعدات (EIR) - قاعدة بيانات الهوية

11 prre@anatel.gov.br

الدولية للمعدات المتنقلة (IMEI). وسعى هذا الحل إلى الحد من استخدام أجهزة الهاتف اليدوية ذات هويات IMEI غير القانونية والوهمية واللاغية والمستنسخة، وإلى مكافحة سرقات أجهزة الهاتف اليدوية، وإلى معالجة المخاوف بشأن الصحة والسلامة.



الشكل 1.A – حل قاعدة بيانات السجل المركزي للهوية الدولية للمعدات المتنقلة (EIR IMEI) في مصر

ووفقاً للجهاز القومي لتنظيم الاتصالات، كان هناك 3,5 مليون من أجهزة الهاتف اليدوية المتنقلة ذات رقم هوية IMEI غير القانوني 13579024681122، و250 000 جهاز هاتف يدوي متنقل بهوياتIMEI مستنسخة، و500 000 جهاز هاتف يدوي متنقل بهويات IMEI وهمية، و350 000 برقم هوية IMEI كله أصفار، و100 000 دون أي رقم هوية IMEI .http://www.itu.int/ITU-D/tech/events/2012/CI_ARB_AFR_Tunis_November12/CI_Forum_Tunis_2012_Report.pdf

وفي فبراير 2010، أعلن الجهاز القومي لتنظيم الاتصالات أن مشغلي الاتصالات المتنقلة الثلاثة في البلاد سيحجبون الخدمات عن جميع المستخدمين المجهولي الهوية وعن الهواتف الخلوية دون الهوية الدولية للمعدات المتنقلة (IMEI) (http://www.cellular-news.com/tags/imei/) في السوق المصري http://www.cellular-news.com/story/42911.php.

5.1.A إندونيسيا

شُددت شروط استيراد الهواتف الخلوية إلى إندونيسيا في يناير 2013 من خلال فرض إجراءات تقنية ومتطلبات معايير، وقيود على التوزيع وعبر الموانئ، وضوابط ما قبل الشحن، والتزام بالتسجيل المسبق لأرقام الهوية الدولية للمعدات المتنقلة (IMEI) قبل الاستيراد. وترد حيثيات هذه المتطلبات في مرسوم وزير الصناعة رقم 2012/81 ومرسوم وزير التجارة رقم 2012/82 .http://trade.ec.europa.eu/doclib/docs/2013/september/tradoc_151703.pdf

6.1.A كينيا

1.6.1.A مقدمة

أفادت وكالة مكافحة التزييف (ACA) في كينيا بأن المنافسة غير الشريفة بين المنتجات المزيَّفة والأصلية تكلف مجتمع الأعمال (المصنعين المحليين والمستثمرين والمبتكرين) ما يقدَّر بمبلغ 50 مليار شلن (حوالي 596 مليون دولار أمريكي) من الإيرادات الضائعة سنوياً، مما يهدد بإغلاق و/أو نقل مواقع العديد من الصناعات. وتقدر الخسارة التي تلحق بالحكومة والاقتصاد من التزييف بما يربو على 19 مليار شلن (حوالي 227 مليون دولار أمريكي) سنوياً من خلال التهرب من دفع الضرائب. http://www.aca.go.ke/index.php?option=com_docman&task=doc_download&gid=20&Itemid=471. والبنود الأكثر تضرراً في هذا المضمار هي العقاقير الطبية والإلكترونيات والأقراص المدمجة والبرمجيات المقرصنة والمشروبات الكحولية، والهواتف المتنقلة والمدخلات الزراعية.

تأسست هيئة الاتصالات في كينيا بقانون المعلومات والاتصالات في كينيا، Cap 411A، لترخيص خدمات المعلومات والاتصالات وتنظيمها. وتفوض الفقرة 25 من القانون المذكور الهيئة بترخيص تشغيل أنظمة وخدمات الاتصالات وتقديمها، على التوالي، مع مراعاة الشروط المطلوبة. وأحد متطلبات الترخيص هو اعتماد نوع معدات الاتصالات للتأكد من توافقها مع شبكات الاتصالات العامة. وفي هذا السياق، تتطلب اللائحة 3 (استيراد معدات الاتصالات واعتماد نوعها وتوزيعها) من لوائح المعلومات والاتصالات في كينيا، لعام 2010، اعتماد نوع جميع أجهزة الهاتف المتنقل لدى الهيئة قبل التوصيل بالشبكات العامة http://www.cofek.co.ke/CCK%20Letter%20to%20Cofek%20-%20Counterfeit%20phone%20switch-off%20threat.pdf.

ويتمثل جوهر عملية اعتماد النوع أساساً في حماية عامة الناس من الآثار غير المرغوبة التي تحدثها أجهزة الهاتف المتنقل دون المستوى المطلوب و/أو المزيَّفة والتي تشمل المخاوف التقنية والاقتصادية والصحية والأمنية. وترد في الفقرة 2.6.1.A أدناه معلومات إضافية عن التحديات المرتبطة بالهاتف اليدوي المزيَّف في صناعة تكنولوجيا المعلومات والاتصالات. والهاتف اليدوي المتنقل الذي لا يملك الهوية الدولية للمعدات المتنقلة (IMEI) المناسبة لا يمكن اعتماد نوعه.

وللأسباب المذكورة أعلاه، كان لا بد من إنهاء استخدام أجهزة الهاتف المتنقل المزيَّفة على مراحل تدريجية. ولكن ذلك يُنفَّذ مع مراعاة مصالح جميع أصحاب الشأن، مما يفسر الأنشطة التي تجري على مراحل والمؤدية إلى موعد الإيقاف في 30 سبتمبر 2012.

وبغية ضمان أن تؤخذ مصالح واهتمامات أصحاب الشأن بعين الاعتبار، استضافت الهيئة اعتباراً من أكتوبر 2011 سلسلة من المشاورات المفتوحة بين جهات فاعلة في صناعة تكنولوجيا المعلومات والاتصالات والوكالات الحكومية المختلفة وغيرها من الجهات صاحبة المصلحة بشأن مسألة الهواتف المتنقلة المزيَّفة بهدف التصدي للتحديات التي تشكلها هذه الظاهرة للصناعة والاقتصاد ككل. ومن خلال هذه المشاورات، اتُفق على نقاط عمل محددة فيما يتعلق بهذا الموضوع.

وكان من بين الإجراءات المتفق عليها قيام الهيئة بشن حملة توعية للعامة لضمان اطلاع المشتركين على الآثار السلبية للأجهزة المزيَّفة؛ وإنشاء نظام تستخدمه عامة الناس لتحديد ما إذا كانت هواتفهم اليدوية أصلية؛ وإنشاء أنظمة لمنع استخدام الهواتف اليدوية المزيَّفة ضمن شبكات الاتصالات المتنقلة؛ وتقديم خدمات دعم العملاء ذات الصلة.

وتمثل إجراء آخر ذو شأن في تصعيد مراقبة الأجهزة المتنقلة المزيَّفة وقمعها من جانب جميع الجهات الحكومية ذات العلاقة. وأنشئ نظام تحقق من الهاتف اليدوي بالنفاذ إلى قاعدة بيانات جمعية النظام العالمي للاتصالات المتنقلة (GSMA) لتمكين المشتركين من التحقق من صلاحية هواتفهم من خلال هوية IMEI المقدَّمة. وعلاوة على ذلك، نُفذ نظام لمنع استخدام الهواتف اليدوية المزيَّفة ضمن شبكات الاتصالات المتنقلة.

ونتيجة للأنشطة المذكورة أعلاه، أوقف على مراحل تدريجية استخدام 1,89 مليون من الهواتف المتنقلة المزيَّفة في كينيا بعد 30 سبتمبر 2012.

2.6.1.A التخلص من أجهزة الهاتف المتنقل المزيَّفة على مراحل تدريجية

1 معلومات أساسية

أ) تنفيذ نظام سجل هوية المعدات (EIR)

إن استخدام الاتصالات المتنقلة في كينيا هو اليوم ضرورة وليس ترفاً. ويُرى ذلك في زيادة عدد المشتركين في البلاد المقدر حالياً بنحو 29,2 مليون مشترك. بيد أن أحد التحديات المرتبطة بإدخال خدمات الاتصالات المتنقلة هو سرقة الهاتف المتنقل فضلاً عن تزايد معدل الجرائم التي ارتكبت بمساعدة الهواتف المتنقلة، مما يشكل خطراً أمنياً كبيراً.

وفي أعقاب هذه التهديدات، شرعت الهيئة في عام 2001 في سلسلة من المشاورات مع مشغلي الاتصالات المتنقلة أصحاب التراخيص القائمين بهدف إيجاد حل دائم لهذه المشكلة. وفي الوقت نفسه، اعتمدت منظمة اتصالات شرق إفريقيا (EACO) قراراً يتطلب، في *جملة أمور*، من المنظمين والمشغلين في المنطقة التشاور بشأن أفضل سبيل للتحقق من سرقة الهواتف المتنقلة في المنطقة.

وخلال هذه المشاورات، لوحظ أن ثمة سمة متأصلة في شبكات الاتصالات المتنقلة، تدعى سجل هوية المعدات (EIR)، توفر آلية لمعالجة قضية سرقة الهاتف المتنقل. إذ يمكن لهذا السجل أن يتحقق من الهوية المتفرِّدة الدولية للمعدات المتنقلة لكل هاتف يَنفذ إلى شبكة الاتصالات المتنقلة، وأن يحتفظ بسجلاته. عندئذ تصبح هذه المعلومات متاحةً بالحد الممكن حينما تتطلب السلطات ذلك.

ولهذه الغاية، وقّع جميع مشغلي شبكات الاتصالات المتنقلة على مذكرة تفاهم (MoU) بشأن تنفيذ نظام سجل هوية المعدات (EIR) الذي سيمهد الطريق لتنفيذ النظام على المستوى الإقليمي. ولوحظ أيضاً أن وجود الهواتف اليدوية المتنقلة المزيَّفة، التي تكون فيها الهويات الدولية للمعدات المتنقلة (IMEI) في معظم الحالات مكررة و/أو وهمية، من شأنه أن يؤدي إلى حالة تُتعقب فيها هذه الهواتف المكتسبة بطرق غير قانونية ويلغى تفعيلها باستخدام نظام سجل هوية المعدات (EIR). ويرجَّح أيضاً إلغاء تفعيل عدة هواتف يدوية أخرى تحمل هويات دولية متماثلة للمعدات المتنقلة.

وفي هذا السياق، ظهر سبب يدعو لمعالجة وجود الهواتف اليدوية المزيَّفة في السوق قبل التنفيذ الكامل لنظام سجل هوية المعدات (EIR) لأن نجاحه سيعتمد على اجتثاث الهواتف اليدوية المزيَّفة على النحو المنشود دولياً.

ب) تنفيذ الإطار القانوني/التنظيمي فيما يتعلق بالهواتف اليدوية المتنقلة

'1' الإطار القانوني/التنظيمي

من وجهة نظر صناعة الاتصالات، توفر الفقرة 25، من قانون المعلومات والاتصالات في كينيا، Cap 4IIA، الإطار القانوني/التنظيمي ذا الصلة الذي يحكم الهواتف اليدوية. وتشترط التراخيص الممنوحة بموجب هذا القانون على الجهات المرخص لها عدم تقديم الخدمات إلا لمن يستخدم جهازاً معتَمَد النوع.

وبالإضافة إلى ذلك، فإن لوائح المعلومات والاتصالات في كينيا، لعام 2010، (بشأن استيراد معدات الاتصالات واعتماد نوعها وتوزيعها) تتطلب صراحةً اعتماد نوع جميع الهواتف اليدوية. وتجدر الإشارة إلى أن متطلبات اعتماد النوع لدى الهيئة تفيد بعدم إمكانية اعتماد نوع جهاز GSM يدوي إذا كانت الهوية الدولية للمعدات المتنقلة (IMEI) التي تخصه غير سليمة أو تعرضت للعبث. وبناءً على ذلك، فإن جميع الهواتف اليدوية الخالية من هوية IMEI سليمة أو المزودة بهوية IMEI مستنسخة هي باختصار غير قانونية، ولذلك يكون استخدامها مخالفاً للقانون المذكور أعلاه.

'2' التوجيه الصادر عن الهيئة مؤخراً وردّ المشغلين

في مايو 2011، وجهت الهيئة إخطاراً إلى جميع مشغلي شبكات الاتصالات المتنقلة للتخلص التدريجي من الهواتف المزيَّفة العاملة على شبكاتهم بحلول 30 سبتمبر 2011. وجاء هذا التوجيه متوافقاً روحاً ونصاً مع القوانين الناظمة لقطاع الاتصالات.

وعند استلام هذا التوجيه، عادت الجهات الفاعلة في صناعة الاتصالات المتنقلة بطلبات تدعو لإعادةً النظر في التوجيه مستشهدةً بكثرة أعداد المشتركين المستخدمين لهواتف ذات هويات IMEI المتماثلة أو المختلة. وبالإضافة إلى ذلك، تخوَّف المشغلون من أن فصل توصيل ما يقدَّر بأكثر من مليوني هاتف يدوي مزيَّف قيد الاستخدام سيؤثر سلباً على إيراداتهم.

ولضمان تنفيذ التوجيه بالحد الأدنى من انقطاع الخدمة، أنشأت الهيئة لجنة مفتوحة الأبواب تتكون أساساً من ممثلي شركات الاتصالات المتنقلة والوزارات والوكالات الحكومية ذات الصلة ومصنعي المعدات ومنافذ البيع والمجتمع المدني.

وتهدف سلسلة المشاورات بين الجهات الفاعلة في صناعة تكنولوجيا المعلومات والاتصالات ومختلف الوكالات الحكومية أيضاً إلى معالجة التحديات الناجمة عن الهواتف المتنقلة المزيَّفة في الصناعة والاقتصاد ككل. وأشارت جمعية النظام العالمي للاتصالات المتنقلة (GSMA) أن كينيا هي أحد البلدان التي توجد فيها سوق كبيرة لهواتف مسروقة في أوروبا أو محض مزيَّفة. وبالاستفادة من خبراتها في التعامل مع هذا الموضوع على المستوى الدولي، قدمت جمعية النظام العالمي للاتصالات المتنقلة كذلك مساهمات استشارية هامة لدعم العملية في كينيا من خلال مختلف التدخلات التقنية. وقد أسفرت المشاورات حتى الآن عن قرار باتخاذ إجراءات محددة لدعم هذه المبادرة.

ومن أهم هذه الإجراءات، قيام الهيئة بشن حملة توعية للعامة لضمان إدراك المشتركين للآثار السلبية للأجهزة المزيَّفة، وضمان التزام مصنعي الهواتف اليدوية المتنقلة بإنشاء نظام تستخدمه عامة الناس لتحديد ما إذا كانت هواتفهم اليدوية أصلية أم لا. وبالإضافة إلى ذلك، أنشأ مشغلو الشبكات أنظمة لمنع استخدام الأجهزة اليدوية المزيَّفة في شبكاتهم، ولتقديم خدمات الدعم ذات الصلة بالمشترك، ولتكثيف المراقبة وقمع استخدام الأجهزة اليدوية المزيَّفة من جانب الوكالات الحكومية.

ولدى إنشاء نظام تحقق من الهاتف اليدوي بالنفاذ إلى قاعدة بيانات جمعية النظام العالمي للاتصالات المتنقلة (GSMA) لتمكين المشتركين من التحقق من صلاحية هواتفهم من خلال هوية IMEI المقدَّمة، جرى تطوير هذا النظام ليسير يداً بيد مع حملة توعية المستهلكين http://www.cofek.co.ke/CCK%20Letter%20to%20Cofek%20-%20Counterfeit%20phone%20switch-off%20threat.pdf.

7.1.A رواندا

أعلنت وكالة تنظيم المرافق في رواندا (RURA) عن خطة لحظر استيراد الأجهزة المتنقلة المزيَّفة الى البلاد في عام 2013، في حين لم تمنع استعمال تلك التي سبق أن وُضعت قيد الاستخدام. http://www.newtimes.co.rw/news/views/article_print.php?i=15290&a=64650&icon=Print. وتواجه رواندا أيضاً تحدياً من الهواتف المزيَّفة التي تعيد تسيير المكالمات التي تجرى إلى رموز EACO القصيرة المواءَمة: 100 (خدمة العملاء) و101 (معاودة الشحن في تنزانيا) و102 (الاطلاع على الرصيد في تنزانيا) و112 (الطوارئ والشرطة). ولذلك اضطرت وكالة تنظيم المرافق في رواندا مؤقتاً لإعادةً تخصيص رمز قصير مختلف لخدمة معلومات العملاء http://www.eaco.int/docs/19_congress_report.pdf.

8.1.A سري لانكا

في مارس 2013، استدرجت هيئة تنظيم الاتصالات في سري لانكا (TRCSL) عروضاً من أجل "تصميم وتطوير وتركيب السجل المركزي لهوية معدات (CEIR) شبكات الاتصالات المتنقلة في سري لانكا" http://www.trc.gov.lk/images/pdf/eoi_ceir_07032013.pdf.

وللتضييق على سوق الهاتف المتنقل المزيَّف وردع سرقة الهاتف المتنقل وحماية مصالح المستهلكين، تعتزم هيئة تنظيم الاتصالات السريلانكية تنفيذ سجل مركزي لهوية المعدات (CEIR) يوصَّل بسجلات هوية المعدات (EIR) لدى جميع مشغلي الاتصالات المتنقلة. وسيعمل السجل المركزي لهوية المعدات (CEIR) بمثابة نظام مركزي لجميع مشغلي الشبكات كي يتبادلوا المعلومات عن المطاريف المتنقلة المدرجة في القوائم السوداء بحيث لا تعمل الأجهزة المدرجة في القائمة السوداء لشبكة ما على شبكات أخرى حتى لو جرى تغيير بطاقة وحدة هوية المشترك (SIM) في الجهاز.

ووفقاً لمتطلبات هيئة تنظيم الاتصالات السريلانكية (TRCSL)، يتعين أن يضمن السجل المركزي لهوية المعدات (CEIR) توفر الوظائف التالية:

'1' يتعين أن يمتلك السجل المركزي لهوية المعدات القدرة على إدارة قاعدة بيانات هويات IMEI لجميع الأجهزة المسجلة على شبكات الاتصالات المتنقلة.

'2' يتعين أن يتمكن السجل المركزي لهوية المعدات من التعرف على هويات دولية للمعدات المتنقلة (IMEI) مثل:

أ) هويات دولية للمعدات المتنقلة غير موزَّعة؛

ب) هويات دولية للمعدات المتنقلة لاغية أو مكررة أو كلها أصفار.

'3' يتعين أن تتضمن قاعدة بيانات السجل المركزي لهوية المعدات (CEIR) المعلومات التالية عن الأجهزة التي سُجلت لدى جميع شبكات الاتصالات المتنقلة في سري لانكا:

أ) الهويات الدولية للمعدات المتنقلة؛

ب) وضع الهوية الدولية للمعدات المتنقلة (IMEI) (أبيض، رمادي، أسود)؛

ج) تاريخ إنشاء السجل؛

د) تاريخ آخر تحديث للسجل؛

ه) رقم طراز الجهاز؛

و) سبب وضع الهوية الدولية للمعدات المتنقلة (IMEI) (غير صالحة، مسروقة، مستنسخة، صالحة).

'4' يتعين أن يتمكن السجل المركزي لهوية المعدات (CEIR) من حجب الخدمات عن المشتركين ذوي الأجهزة المسجلة بهويات IMEI غير صالحة أو مدرجة على القائمة السوداء.

'5' يتعين أن يتمكن السجل المركزي لهوية المعدات (CEIR) من تحديد طراز الجهاز وإصداره وغير ذلك من المعلومات.

'6' يتعين أن يسمح السجل المركزي لهوية المعدات بإنشاء سجل جديد في قاعدة البيانات التي تحتوي على الهويات الدولية للمعدات المتنقلة كلما فُعِّل حساب مشترك جديد.

'7' يتعين أن يتيح السجل المركزي لهوية المعدات (CEIR) أحدث معلومات قاعدة بيانات المشغلين المدرجة في القوائم المحلية السوداء/البيضاء/الرمادية، وذلك لمنع استنساخ الأجهزة عبر الشبكات ومواكبة أحدث معلومات قاعدة البيانات.

'8' يتعين أن يحدِّث السجل المركزي لهوية المعدات (CEIR) دورياً قاعدة بيانات الهوية الدولية للمعدات المتنقلة (IMEI) بأحدث المعلومات بشأن تخصيصات هوية IMEI الصالحة وذلك بأكثر الأساليب المتاحة كفاءةً.

'9' يتعين أن يتمكن السجل المركزي لهوية المعدات (CEIR) من التعرف على هويات IMEI المزيَّفة من خلال مقارنةً هويات IMEI التي تقدمها جمعية النظام العالمي للاتصالات المتنقلة (GSMA).

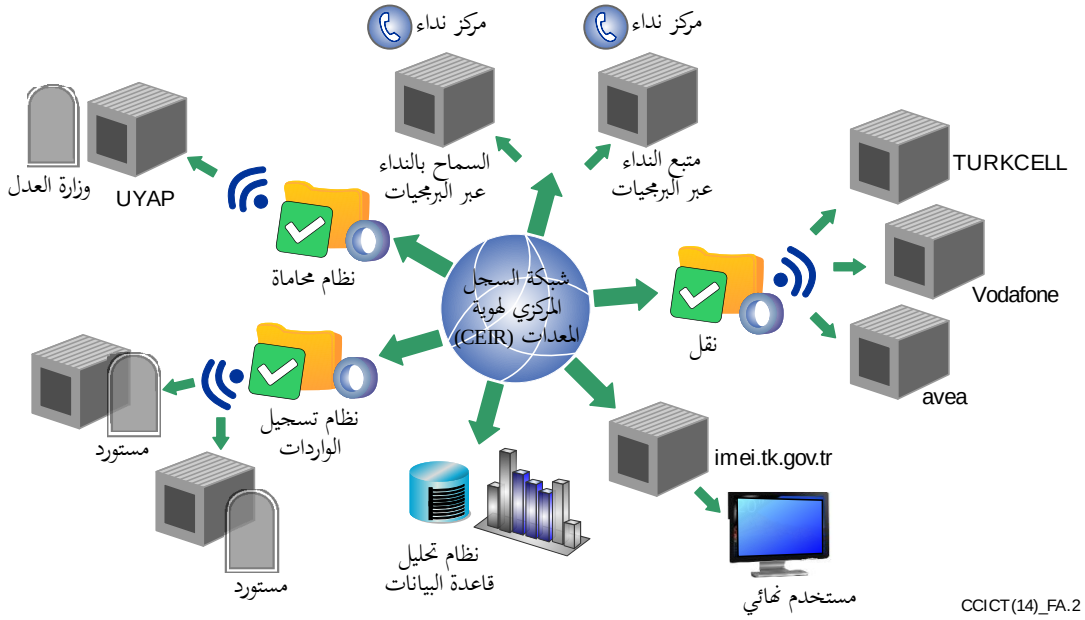
'10' يتعين أن يكون السجل المركزي لهوية المعدات (CEIR) قابلاً للتشغيل البيني مع جميع ما يناسب من عناصر الشبكة وسطوحها البينية لدى مشغلي الاتصالات المتنقلة.

'11' يتعين أن تدعم قاعدة بيانات السجل المركزي لهوية المعدات (CEIR) أسلوباً مرناً للمدخلات (عن طريق الإدخال اليدوي للبيانات والملفات المسطحة التي تحتوي على تحديثات لمديات الهويات الدولية للمعدات المتنقلة (IMEI)).

'12' يتعين أن يقوم السجل المركزي لهوية المعدات بفحص نسق الهوية الدولية للمعدات المتنقلة (IMEI) للتحقق من صلاحية نسقها ومداها.

9.1.A تركيا

في عام 2006، أنشأت سلطة تكنولوجيا المعلومات والاتصالات (ICTA) في تركيا سجلاً مركزياً لهوية المعدات (CEIR) من أجل قطع دابر استخدام الهواتف المتنقلة غير المسجلة، والخسارة الضريبية، والمنافسة غير الشريفة في القطاع، واختطاف عمليات الاستيراد؛ وكذلك من أجل أتمتة عمليات الاستيراد. وأنشئت البنية التحتية للحد من الأجهزة المستوردة بطريقة غير قانونية ولفصل الأجهزة، المهربة والمفقودة والمسروقة أو تلك ذات أرقام IMEI المستنسخة، عن الشبكة اللاسلكية.



الشكل 2.A – هيكل السجل المركزي لهوية المعدات

صنف قانون الاتصالات الراديوية أرقام الهوية الدولية للمعدات المتنقلة (IMEI) على النحو التالي:

- القائمة البيضاء: تتكون من أرقام الهوية الدولية للمعدات المتنقلة (IMEI) للأجهزة التي سُجلت ولم تتغير معلومات الهوية الإلكترونية الخاصةً بها.
- القائمة السوداء: تتكون من أرقام الهوية الدولية للمعدات المتنقلة (IMEI) التي تنتمي إلى فئة الأجهزة المفقودة والمسروقة والتي تغيرت معلومات الهوية الإلكترونية الخاصةً بها. ويفوَّض مشغلو الاتصالات بقطع الاتصالات اللاسلكية عن هذه الأجهزة.
- القائمة الرمادية: تتكون من أرقام الهوية الدولية للمعدات المتنقلة (IMEI) التي لا تنتمي إلى القائمة البيضاء ولا إلى القائمة السوداء، والتي يسمح لها بالاتصالات اللاسلكية. ويُلزم مشغلو الاتصالات بتحليل تفاصيل المكالمة من هذه الأجهزة، وإخطار سلطة تكنولوجيا المعلومات والاتصالات (ICTA) بها. ويُلزم مشغلو الاتصالات أيضاً بإخطار مستخدمي هذه الأجهزة من خلال رسالة نصية بأن أجهزتهم ليست مدرجة في القائمة البيضاء.
- القائمة البيضاء المتطابقة: تتكون من أرقام الهوية الدولية للمعدات المتنقلة (IMEI) المستنسخة عن أرقام أجهزة المشترك المتنقل في الشبكة الرقمية للخدمات المتكاملة (MSISDN) للمستخدمين الذين أودعوا رسوم التسجيل. وهي تتكون أيضاً من الأجهزة التي دخلت في عقد اشتراك لدى مشغِّل اتصالات، وأمضت فترة مؤقتة في تركيا برقم MSISDN.

ويفيد التقرير السنوي لسلطة تكنولوجيا المعلومات والاتصالات لعام 2010، أن 847 836 131 من أرقام الهوية الدولية للمعدات المتنقلة (IMEI) سُجلت قانونياً وأن 239 308 14 من أرقام الهوية الدولية للمعدات المتنقلة أدرجت في القائمة السوداء بسبب ضياعها أو تهريبها أو سرقتها أو استنساخها بنهاية عام 2010 https://www.icta.mu/mediaoffice/publi.htm.

10.1.A أوغندا

شرعت هيئة الاتصالات في أوغندا (UCC) بتنفيذ مشروع http://ucc.co.ug/data/mreports/18/0/ELIMINATION%20OF%20COUNTERFEIT%20MOBILE%20PHONES.html يهدف إلى إزالة الهواتف المتنقلة المزيَّفة تدريجياً من السوق الأوغندية. وتشير دراسة معتمدة من هيئة الاتصالات الأوغندية إلى أن حوالي 30% من الهواتف المتنقلة في السوق الأوغندي هي هواتف مزورة. ويشير الاستطلاع أيضاً أن المتاجرين بالهواتف المتنقلة المزورة أو المزيَّفة ضيَّعوا على الحكومة نحو 15 مليار شيلينغ (~400 5 مليون دولار أمريكي حتى نوفمبر 2014) من إيرادات ضريبية. http://www.monitor.co.ug/Business/Commodities/Survey+finds+30++of+Ugandan+phones+fake/-/688610/1527408/-/elvou8z/-/index.html وفي ديسمبر 2012، نشرت هيئة الاتصالات الأوغندية (UCC) وثيقة استشارية بعنوان "الجدول الزمني وتوزيع المهام لإزالة الهواتف المتنقلة المزيَّفة" http://www.ucc.co.ug/files/downloads/Counterfeit%20phones%20Consultative%20Document.pdf وهي تعرِّف المشروع ومراحل تنفيذه الأربع على النحو التالي:

المرحلة 1: التحقق من الهواتف المتنقلة:

خلال هذه المرحلة، سيتمكن المستهلكون من التحقق من حالة هواتفهم باستخدام أحد تطبيقي الإنترنت والرسائل النصية القصيرة أو كليهما.

ويُنصح المستهلكون بالتحقق على الفور من شرعية هواتفهم المتنقلة باستخدام الطريقين أعلاه.

المرحلة 2: حرمان الهواتف المزيَّفة الجديدة من الخدمة:

خلال هذه المرحلة، يتعين أن تُحرم الهواتف المتنقلة المزيَّفة الجديدة التي لم يسبق لها الاشتراك في أي شبكة من النفاذ إلى جميع الشبكات. وكان الموعد المقترح لتنفيذ هذه المرحلة، 31 يناير 2013.

المرحلة 3: قطع توصيل جميع الهواتف المتنقلة المزيَّفة:

خلال هذه المرحلة، يتعين قطع توصيل جميع الهواتف المتنقلة المزيَّفة، بما فيها تلك التي سبق أن اشتركت في الشبكة. وكان الموعد المقترح لتنفيذ هذه الخطوة، 1 يوليو 2013.

المرحلة 4: ترسيخ المشروع:

خلال هذه المرحلة، يتعين أن تقوم الهيئة باستعراض نتائج المشروع المتعلقة بتنفيذه والقضايا ذات الصلة بإدارة النفايات الإلكترونية، واستنساخ الهويات الدولية للمعدات المتنقلة. ولا تزال المقترحات بشأن معالجة مختلف القضايا في هذه المرحلة قيد النظر.

11.1.A أوكرانيا

1.11.1.A مقدمة

في عام 2008، كانت المشكلة الفورية والأكثر إلحاحاً التي تحتاج إلى معالجة هي استيراد مطاريف متنقلة مهرَّبة كانت تشكل 93%-95% من السوق. وكان جزء كبير من هذه الأجهزة اليدوية مجهول المصدر ولا يلبي المعايير الأوكرانية في خصائصه التقنية أو في خصائص السلامة. وكانت الهيئة الوطنية لتنظيم الدولة للاتصالات والمعلوماتية (NCCIR) خُوِّلت من خلال قانون أوكرانيا "بشأن موارد الترددات الراديوية في أوكرانيا" بفرض تدابير إضافية لحماية السوق الأوكرانية من المطاريف المتنقلة متدنية الجودة المستوردة دون ترخيص أو بطريقة غير قانونية.

وحددت الهيئة الوطنية لتنظيم الدولة للاتصالات والمعلوماتية إجراءً تنظيمياً لاستيراد المطاريف المتنقلة. وكتنفيذ تقني لإجراءات الاستيراد، أنشئ نظام المعلومات المؤقت لتسجيل مطراف متنقل في أوكرانيا (AISMTRU) ووضعه مركز الدولة الأوكرانية للترددات

الراديوية (UCRF) موضع التنفيذ عام 2009. ونتيجةً لذلك، انخفضت الواردات غير القانونية من المطاريف المتنقلة انخفاضاً هائلاً، حيث لم تشكل أكثر من 5%-7% من السوق في عام 2010، واستمر الانخفاض في السنوات التالية.

وتُستخدم الهويات الدولية للمعدات المتنقلة في أوكرانيا لإنشاء قاعدة بيانات للأجهزة التي استُوردت قانونياً إلى أوكرانيا. ويُحتفظ بالقوائم التالية: "قائمة بيضاء" بالأجهزة التي استُوردت قانونياً، و"قائمة رمادية" بالأجهزة ذات الوضع غير المؤكد و"قائمة سوداء" بالأجهزة التي ستُحرم من الخدمة. ويتاح النفاذ إلى هذه القوائم لسلطات التنظيم والجمارك ومشغلي الشبكات وعامة الناس بمستويات مناسبة من امتيازات النفاذ.

ويؤدي نظام المعلومات المؤتمت لتسجيل مطراف متنقل في أوكرانيا (AISMTRU) الوظائف التالية:

- أتمتة معالجة طلبات المستوردين لاستكمال الإجراءات التنظيمية للتسجيل واستخدام معدات المطاريف ضمن شبكات الاتصالات؛
- منع الاستيراد "الرمادي" غير القانوني للمطاريف المتنقلة إلى أراضي أوكرانيا؛
- مكافحة سرقة الأجهزة اليدوية؛
- أتمتة سير العمل في مركز الدولة الأوكرانية للترددات الراديوية (UCRF) وزيادة كفاءة العمل بين المركز والجهات الفاعلة في سوق المطاريف؛
- تحديد رموز الهوية الدولية للمعدات المتنقلة (IMEI) "المستنسخة" وحجب الخدمة عن المطاريف ذات رموز IMEI "المستنسخة".

وترد معلومات مفصلة عن نظام AISMTRU في الفقرة 2.11.1.A.

ويحظر التشريع الأوكراني بيع المطاريف المتنقلة ذات رموز IMEI غير المسجلة في نظام AISMTRU. والجزء الرئيسي من نظام AISMTRU هو قاعدة بيانات عامة تحتفظ بقوائم "بيضاء" و"رمادية" و"سوداء" لرموز IMEI للمطاريف المتنقلة. وعند أول توصيل وتسجيل لمطراف لدى أي مشغل شبكة، يُرسِل مشغل الاتصالات المتنقلة تلقائياً رمز IMEI العائد للمطراف إلى قاعدة البيانات العامة. ويكشف نظام AISMTRU رموز الهوية الدولية للمعدات المتنقلة (IMEI) غير الواردة في القائمة "البيضاء"، ويحدد الهواتف المتنقلة المزيَّفة ويسجل ما يقابلها من رموز الهوية الدولية للمعدات المتنقلة في القائمة "الرمادية". ويتلقى جميع مالكي تلك المطاريف إشعاراً عبر خدمة SMS بهذا الشأن، ويتعين عليهم تأكيد المصدر القانوني للمطراف في غضون 90 يوماً من تاريخ إدراجه في القائمة "الرمادية".

وتسجَّل رموز IMEI للمطاريف المسروقة في القائمة "السوداء" بناءً على طلب سلطة إنفاذ القانون، مما يجعل سرقة المطاريف عديمة الفائدة. ويطبَّق الإجراء نفسه على حظر نفاذ المطراف إلى الشبكات بناءً على طلب من أصحاب الهواتف المفقودة. فيمتنع مشغلو الشبكات عن تخديم المطاريف المدرجة في القائمة "السوداء".

ويتحقق هدف حماية المستهلك من خلال تنفيذ أداة للتحقق السهل من قانونية مطراف متنقل قبل شرائه. ويمكن لأي زبون أن يتحقق من وضع رمز IMEI للمطراف عن طريق إرسال رسالة SMS بذلك الرمز إلى الرقم الوطني "307" أو باستخدام بوابة الإنترنت لمركز الدولة الأوكرانية للترددات الراديوية (UCRF). ولا يتجاوز الوقت اللازم للتحقق 10 ثوان.

وإذ يضمن تنفيذ نظام المعلومات المؤتمت لتسجيل مطراف متنقل في أوكرانيا (AISMTRU) قانونية سوق المطاريف في أوكرانيا، فقد أحدث خفضاً حاداً في الاستيراد "الرمادي" (غير القانوني) للمطاريف المتنقلة في أوكرانيا. وقد انخفضت حصة المطاريف المتنقلة المستوردة بطريقة غير قانونية من 93%-95% في عام 2008 إلى 5%-7% في عام 2010 والسنوات التالية. وحُولت عائدات تربو على 500 مليون دولار إلى الموازنة العامة للدولة في أوكرانيا خلال الفترة 2010–2012 من الرسوم الجمركية على استيراد المطاريف المتنقلة، مقارنةً مع 30 مليون دولار على مدى السنوات الثلاث السابقة. ويتكون سوق المطراف المتنقل الأوكراني أساساً من المطاريف المتنقلة التي تلبي المتطلبات التقنية المميزة للاستخدام في أوكرانيا.

2.11.1.A نظام المعلومات المؤتمت لتسجيل مطراف متنقل في أوكرانيا (AISMTRU)

1.2.11.1.A معلومات أساسية

إن التطور السريع لخدمات الاتصالات (الخلوية) المتنقلة المقدمة من المشغلين وطغيان هذا النوع من خدمات الاتصالات في أوكرانيا أديا إلى النمو السريع لسوق المطاريف المتنقلة في أوكرانيا، وبالتالي إلى زيادة استيراد هذه المنتجات.

و"المطراف المتنقل" يعني جهازاً يدوياً متنقلاً أو أي من المعدات الأخرى، التي يستخدمها المستخدم النهائي لشبكة الاتصالات، ويمتلك كل منها معرفاً دولياً (رمز الهوية الدولية للمعدات المتنقلة (IMEI)) ويمكن التعرف عليها داخل الشبكة باستخدام هذا الرمز.

وفي عام 2008، كان وضع سوق المطاريف المتنقلة في أوكرانيا حرجاً: حيث كانت 93%-95% من المنتجات في السوق "واردات رمادية"، أو سلعاً مهربة بعبارة أبسط. وعلاوة على ذلك، كان جزء كبير من هذه المنتجات ممثلاً بنسخ من أجهزة يدوية ذات علامات تجارية مجهولة المصدر ولا تلبي المعايير الأوكرانية في خصائصها التقنية أو في خصائص السلامة. وكانت مختلف التدابير المتخذة لتنظيم السوق عاجزة عن تغيير هذا الوضع، ولم تُصنع هذه المطاريف في أوكرانيا.

وبعدئذ، خُوِّلت سلطة تنظيمية مستقلة هي الهيئة الوطنية لتنظيم الدولة للاتصالات والمعلوماتية (NCCIR) من خلال قانون أوكرانيا "بشأن موارد الترددات الراديوية في أوكرانيا" بفرض تدابير إضافية لحماية السوق الأوكرانية من المطاريف المتنقلة متدنية الجودة المستوردة دون إذن أو بطريقة غير قانونية.

2.2.11.1.A الأهداف

حددت الهيئة الوطنية لتنظيم الدولة للاتصالات والمعلوماتية (NCCIR) الأهداف التالية للسيطرة على الاستيراد وعلى إعداد المطاريف واستخدامها:

1 حماية السوق الأوكرانية من المطاريف المتنقلة متدنية الجودة التي يمكن أن تكون غير نظامية أو خطرة على صحة الإنسان.

2 ضمان الجودة الكافية لخدمات الاتصالات المتنقلة.

3 حل المشكلة الاجتماعية المتمثلة في سرقة الأجهزة اليدوية، وخاصةً من الأطفال.

4 مكافحة الاستيراد غير القانوني والإعداد غير القانوني للمطاريف المتنقلة في السوق الأوكرانية.

وقد وضعت إجراءات لاستيراد وإعداد المعدات المتنقلة مع إيلاء الاعتبار الواجب للأهداف المذكورة أعلاه. وقد نص قانونان رسميان على هذه الإجراءات – وهما قانون إجراءات استيراد المرافق الإلكترونية الراديوية والأجهزة المشعة وقانون إجراءات إعداد المرافق الإلكترونية وأجهزة البث في أوكرانيا.

3.2.11.1.A إجراءات الاستيراد

تتحكم السلطات الجمركية في استيراد المعدات الراديوية إلى أوكرانيا وفقاً للشروط التالية:

- توفر وثيقة التزام المعدات الراديوية باللوائح التقنية؛
- مطابقة المعدات لسجل المرافق الإلكترونية الراديوية والأجهزة المشعة التي يسمح باستخدامها في أوكرانيا في النطاقات الترددية شائعة الاستخدام؛
- عدم ورود المعدات في سجل المرافق الإلكترونية الراديوية والأجهزة المشعة التي يُحظر استخدامها في أوكرانيا في النطاقات الترددية شائعة الاستخدام.

وتعالَج رموز الهوية الدولية للمعدات المتنقلة (IMEI) المقدمة من المستورد إلى مركز الدولة الأوكرانية للترددات الراديوية (UCRF)، وتُدخل في "القائمة البيضاء" لقاعدة البيانات العامة للهوية الدولية للمعدات المتنقلة. ولتسجيل المعرفات الدولية لمعدات المطراف، المستوردة قانونياً إلى أوكرانيا، تقوم دائرة جمارك الدولة في أوكرانيا يومياً بتزويد مركز الدولة الأوكرانية للترددات الراديوية بمقتطف من البيان الجمركي (في شكل إلكتروني) لاستيراد مرافق إلكترونية راديوية.

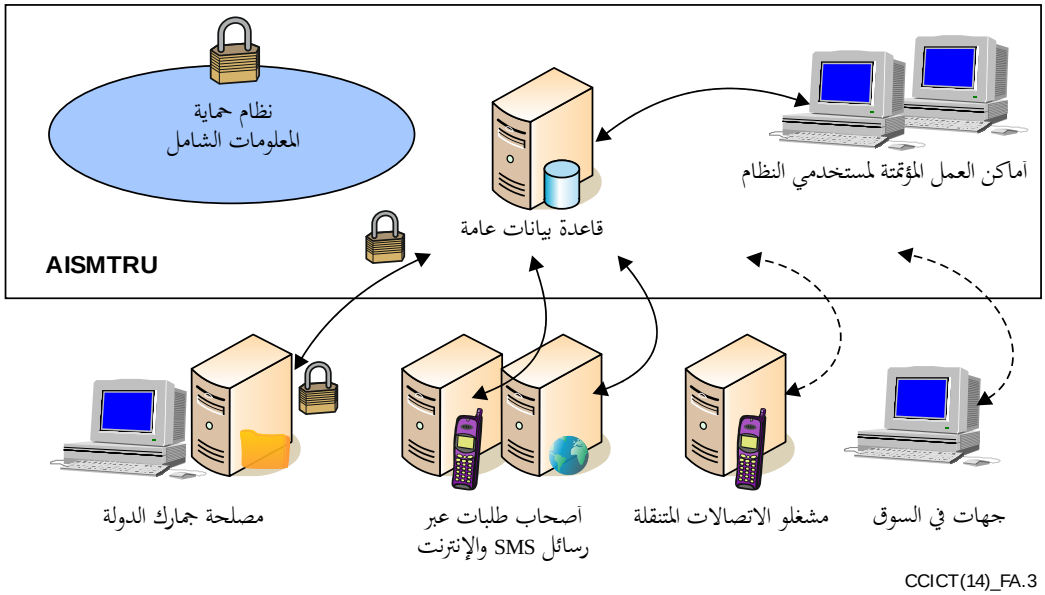
وتجلى التنفيذ التقني لإجراء الاستيراد التنظيمي المذكور أعلاه في إنشاء نظام المعلومات المؤتمت لتسجيل المطاريف المتنقلة في أوكرانيا (AISMTRU)، ووضعه مركز الدولة الأوكرانية للترددات الراديوية (UCRF) موضع التنفيذ في 1 يوليو 2009.

ووفقاً لقانون أوكرانيا "بشأن تأكيد المطابقة"، يتعين أن تقوم الجهات التي تقرها الهيئة التنظيمية (NCCIR) بمنح الشهادات لمعدات المطراف.

4.2.11.1.A وظائف نظام المعلومات المؤتمت لتسجيل المطاريف المتنقلة في أوكرانيا (AISMTRU)

ترد وظائف نظام المعلومات المؤتمت لتسجيل المطاريف المتنقلة في أوكرانيا (AISMTRU) في الفقرة 1.11.1.A، وهي على النحو التالي:

- أتمتة معالجة طلبات المستوردين؛
- منع الاستيراد "الرمادي" غير القانوني للمطاريف المتنقلة إلى أراضي أوكرانيا؛
- مكافحة سرقة الأجهزة اليدوية؛
- أتمتة سير العمل في مركز الدولة الأوكرانية للترددات الراديوية (UCRF) وزيادة كفاءة العمل بين المركز والجهات الفاعلة في سوق المطاريف؛
- تحديد رموز الهوية الدولية للمعدات المتنقلة (IMEI) "المستنسخة" وحجب الخدمة عن المطاريف ذات رموز IMEI "المستنسخة".



CCICT(14)_FA.3

الشكل 3.A – وظائف نظام المعلومات المؤتمت لتسجيل المطاريف المتنقلة في أوكرانيا (AISMTRU)

5.2.11.1.A التخويل

وفقاً للتشريعات الحالية، تخوَّل الجهات التالية باستخدام نظام المعلومات المؤتمت لتسجيل المطاريف المتنقلة في أوكرانيا (AISMTRU):

- مركز الدولة الأوكرانية للترددات الراديوية؛

- الهيئة الوطنية لتنظيم الدولة للاتصالات والمعلوماتية؛
- مشغلو الاتصالات المتنقلة؛
- دائرة جمارك الدولة؛
- وزارة الشؤون الداخلية؛
- مشترو ومستخدمو المطاريف المتنقلة؛
- المستوردون.

6.2.11.1.A قاعدة البيانات العامة للهوية الدولية للمعدات المتنقلة (IMEI)

يتألف الجزء الرئيسي في نظام AISMTRU من قاعدة البيانات العامة للهوية الدولية للمعدات المتنقلة (IMEI) التي تحتفظ بثلاث قوائم تسمى تقليدياً على النحو التالي:

- "القائمة البيضاء": سجل برموز هوية IMEI للمطاريف المستوردة قانونياً أو المصنعة في أوكرانيا.
- "القائمة الرمادية": سجل بقاعدة البيانات العامة لرموز هوية IMEI للمطاريف غير المدرَجة في "القائمة البيضاء" أو "القائمة السوداء" في لحظة أول تسجيل في شبكة الاتصالات.
- "القائمة السوداء": سجل برموز هوية IMEI للمطاريف التي تُحظَر عنها الخدمة في شبكات المشغل (أجهزة يدوية مسروقة أو مفقودة، أو مطاريف ذات منشأ قانوني غير مؤكد بعد 90 يوماً من تاريخ إدراجها في "القائمة الرمادية").

إن النظام الفرعي لإدارة قاعدة البيانات العامة للهوية الدولية للمعدات المتنقلة (IMEI) يعطي المستخدمين المخوَّل لهم من مركز الدولة الأوكرانية للترددات الراديوية (UCRF) أداة لإدراج البيانات في "القائمة البيضاء". ويتم توليد القائمتين "الرمادية" و"السوداء" أوتوماتياً. وللمستخدمين المخوَّل لهم من مركز الدولة الأوكرانية للترددات الراديوية (UCRF) حق محدود في تغيير وضع رموز محددة لهوية IMEI في القائمتين "السوداء" و"الرمادية".

ويؤكَد كل إجراء يتخذه مستخدم مخوَّل من مركز الدولة الأوكرانية للترددات الراديوية (UCRF) بالتوقيع الرقمي الإلكتروني الخاص بذلك المستخدم.

ويقوم النظام الفرعي بوظيفة استيراد البيانات لإعادةً تسيير البيانات من مستوردي المطاريف ومشغلي الاتصالات المتنقلة إلى سجل الهوية الدولية للمعدات المتنقلة (IMEI).

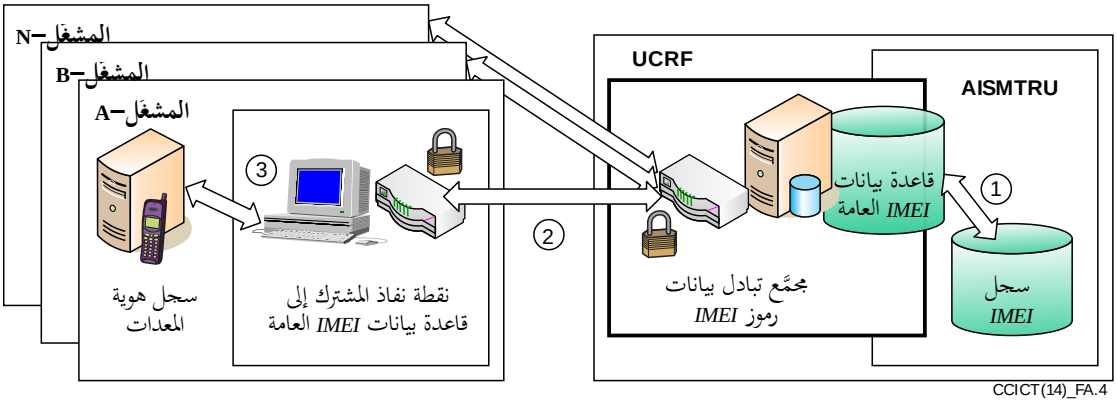
ومن خلال معالجة البيانات المستقاة من "القائمة البيضاء" والبيانات المستقاة من المشغلين ومن المستوردين ودائرة الجمارك، يمكن تشكيل وإدارة سجلات القائمتين "الرمادية" و"السوداء".

وقد تحقق هدفان خلال المرحلة الأولى من وضع النظام قيد التشغيل:

1 حماية السوق الأوكرانية من المطاريف المتنقلة غير المخوَّلة متدنية الجودة التي قد تشكل خطراً على صحة المستخدم.

2 منع الاستيراد غير القانوني للمطاريف المتنقلة وتفعيلها في السوق الأوكرانية.

وفيما بعد، أُعد نظام لضمان تحقيق جميع الأهداف، بما في ذلك إزالة حافز سرقة المطاريف المتنقلة، وخاصةً من الأطفال.



الشكل 4.A – سجل هوية المعدات (EIR) وقاعدة البيانات العامة للهوية الدولية للمعدات المتنقلة (IMEI)

وكمرحلة ثانية، نُفِّذ النظام الفرعي لتبادل رموز الهوية الدولية للمعدات المتنقلة (IMEI) من القوائم "البيضاء" و"الرمادية" و"السوداء" بين نظام المعلومات المؤتمت لتسجيل المطاريف المتنقلة في أوكرانيا (AISMTRU) ومشغلي الاتصالات المتنقلة على الصعيد الوطني. وفي هذه المرحلة، أجري تبادل رموز الهوية الدولية للمعدات المتنقلة (IMEI) بالأسلوب "اليدوي".

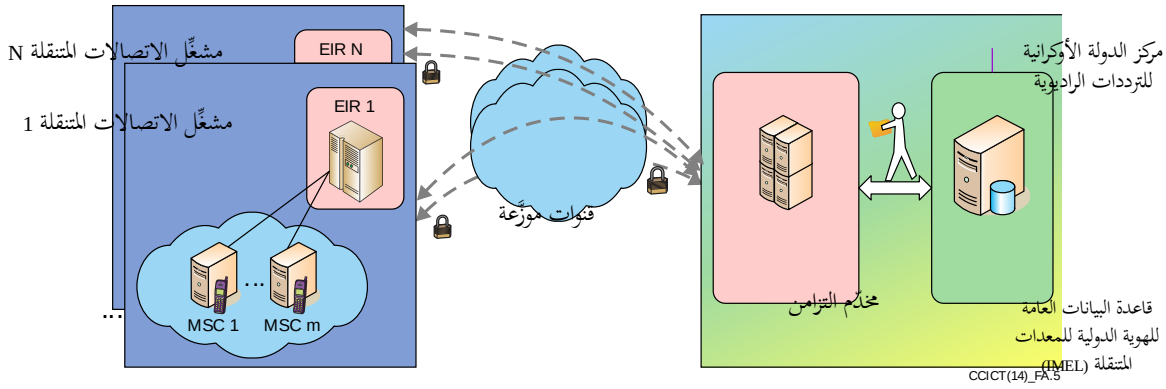
وبالإضافة إلى ذلك، نُفِّذ النظام الفرعي لتبادل البيانات لإبلاغ وزارة الشؤون الداخلية بشأن المطاريف المسروقة/المفقودة، وللتواصل مع دائرة الجمارك لاستقاء المعلومات عن المطاريف المستوردة.

ولضمان التفاعل النشط مع نظام AISMTRU، أتاح المشغلون ومركز الدولة الأوكرانية للترددات الراديوية (UCRF) ما يلي:

- إدارة سجل هوية المعدات (EIR)؛
- نقطة نفاذ المشتركين إلى قاعدة البيانات العامة للهوية الدولية للمعدات المتنقلة (IMEI)؛
- قناة للتفاعل بين نقطة المشتركين وسجل هوية المعدات؛
- تطبيق شهادات التوقيع الرقمي للمستخدمين المخوَّلين.

ويزامن النظام المدمج في نظام AISMTRU عمل سجل هوية المعدات (EIR) لدى مشغلي الاتصالات الخلوية (المتنقلة) وقاعدة البيانات العامة للهوية الدولية للمعدات المتنقلة (IMEI). ويمكِّن ذلك التبادل التلقائي لقوائم رموز الهوية الدولية للمعدات المتنقلة (IMEI) بين سجلات هوية المعدات في شبكات مشغلي الاتصالات المتنقلة وقاعدة البيانات العامة للهوية الدولية للمعدات المتنقلة (IMEI). وبذلك، يظهر في نظام AISMTRU رمز الهوية الدولية للمعدات المتنقلة (IMEI) لكل مطراف، بعد تسجيله في شبكة المشغل، ويجري التحقق منه في قاعدة البيانات العامة للهوية الدولية للمعدات المتنقلة (IMEI).

واليوم، يدعم مخدِّم التزامن الأسلوبين اليدوي والتلقائي للتوصيل بسجل هوية المعدات (EIR) لدى المشغلين.



الشكل 5.A – مخدِّم التزامن

7.2.11.1.A الميزات

تتضمن ميزات النظام ما يلي:

- استخدام معايير الصناعة لتخزين البيانات ونقل (تبادل البيانات)؛
- ضمان أمن البيانات والنظام بأكمله؛
- استخدام معيار وطني للتوقيع الرقمي لضمان النزاهة وعدم التنصل في جميع مراحل معالجة البيانات في النظام؛
- هيكل مؤلف من وحدات للنظام؛
- أسلوب التشغيل 24x7.

8.2.11.1.A أمن البيانات

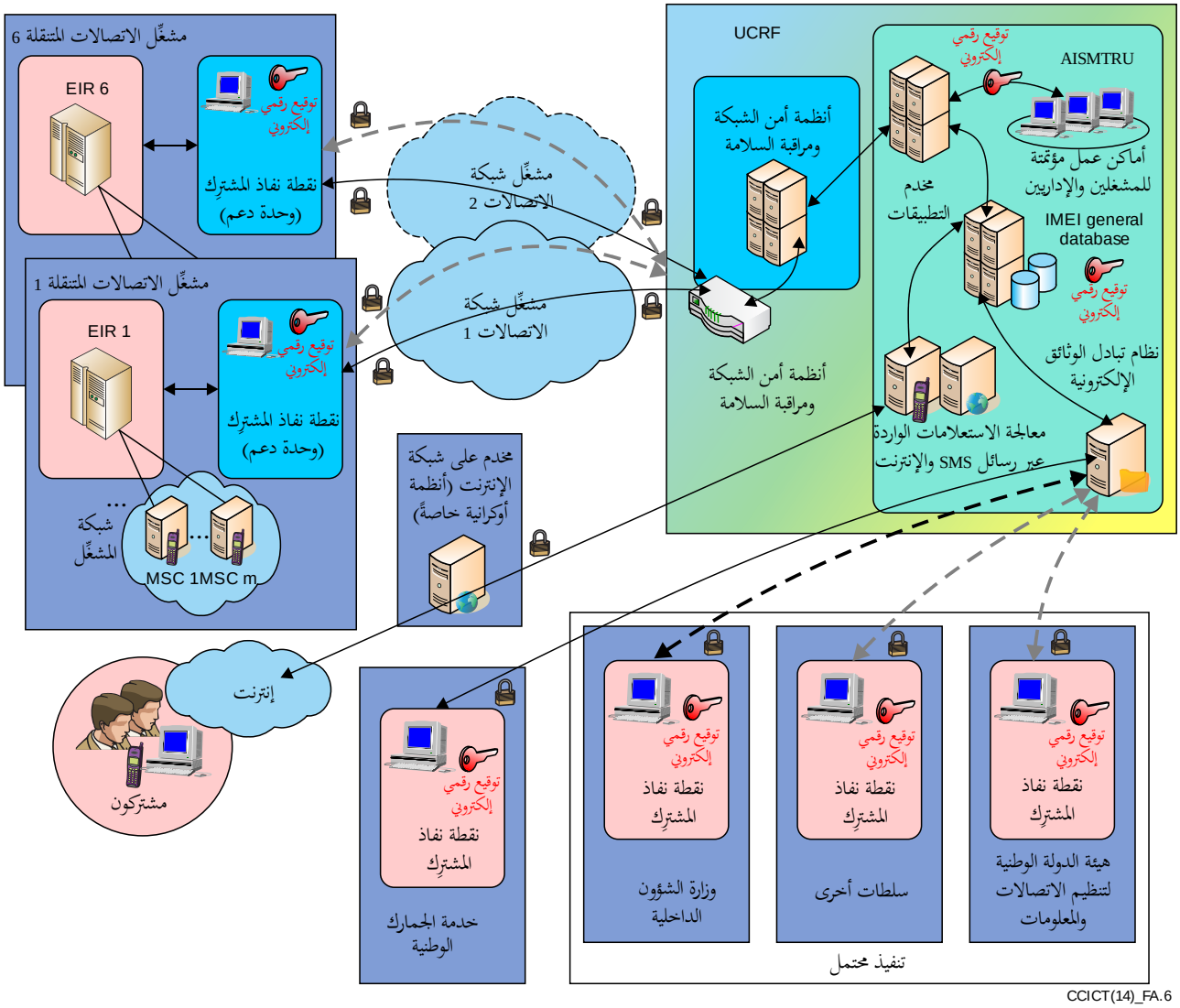
يلبي نظام حماية المعلومات الشامل (CIPS) في نظام المعلومات المؤتمت لتسجيل المطاريف المتنقلة في أوكرانيا (AISMTRU) متطلبات التشريع الحالي، وقد تأكد ذلك بنتيجة إيجابية صدرت على أساس نتائج فحص أجرته سلطة حكومية مختصة.

ويضمن نظام حماية المعلومات الشامل (CIPS) ما يلي:

- التحكم في محدودية النفاذ إلى المعلومات السرية؛
- تحديد التهديدات لسلامة النفاذ المحدود إلى المعلومات التي يجري نقلها ومعالجتها وتخزينها في النظام؛
- حماية سرية النفاذ المحدود إلى المعلومات وسلامته وتيسره من النفاذ غير المخوَّل به؛
- منع تسرب المعلومات خلال عبورها بيئة غير آمنة؛
- حماية المعلومات التكنولوجية من النفاذ غير المخوَّل به ومن التدمير أو التغيير أو الحجب.

ويُضمن الأمن والموثوقية من خلال التالي:

- استخدام وسائل التوقيع الرقمي الإلكتروني الموثوقة لضمان صحة وسلامة المعلومات، ولتخويل المستخدمين المخولين والاستيقان منهم؛
- تنفيذ التوقيع الرقمي الإلكتروني وفقاً لمعايير أوكرانيا الوطنية؛
- توفر نظام نسخ للاحتياط والاسترداد؛
- الحفاظ على سجل آمن (تسجيل أي فعل من المستخدم أو حدث في النظام).



الشكل 6.A – نظام حماية المعلومات الشامل (CIPS) في نظام المعلومات المؤتمت لتسجيل المطاريف المتنقلة في أوكرانيا (AISMTRU)

9.2.11.1.A مؤثرات التنفيذ

1 حماية المستهلك

يمكن لكل مشتري التحقق من قانونية مطراف متنقل قبل شرائه في أوكرانيا. ويمكن أن يتم ذلك عن طريق استخدام الموقع الرسمي لمركز الدولة الأوكرانية للترددات الراديوية (UCRF) أو عن طريق إرسال رسالة نصية قصيرة تحتوي على رمز هوية IMEI المتحقق منه للمطراف إلى الرقم "307"، المشترَك بين جميع مشغلي الاتصالات المتنقلة. وبعد بضع ثوان، يوضح الجواب وضع رمز هوية IMEI المطلوب في قاعدة البيانات العامة للهوية الدولية للمعدات المتنقلة (IMEI).

وهذا يحمي السوق الأوكرانية من المطاريف التي لا تلبي متطلبات الاستخدام المحددة في أوكرانيا.

ويحظر التشريع الأوكراني الحالي وجود المطاريف المتنقلة ذات رموز الهوية الدولية للمعدات المتنقلة (IMEI) التي لم تسجَّل في قاعدة البيانات العامة للهوية الدولية للمعدات المتنقلة (IMEI).

2 مكافحة سرقة المطاريف

تسجَّل رموز هوية IMEI للمطاريف المسروقة في "القائمة السوداء" بناءً على طلب سلطة إنفاذ القانون، مما يجعل سرقة المطاريف عبثية.

ويطبَّق الإجراء نفسه على حجب الخدمة عن مطراف، بناءً على طلب من أصحاب الهواتف المفقودة.

3 قمع الاستيراد غير القانوني

في أول توصيل مع أي مشغل شبكة، يسجَّل أي مطراف فوراً مع الشبكة ذات الصلة. أما رموز هوية IMEI للمطاريف التي تخدمها شبكة المشغل (باستثناء تلك الموجودة حالياً في خدمة التجوال الدولي)، فيعيد مشغلو الاتصالات المتنقلة تسييرها تلقائياً في الوقت المناسب (ليلاً) إلى قاعدة البيانات العامة للهوية الدولية للمعدات المتنقلة في نظام المعلومات المؤتمت لتسجيل المطاريف المتنقلة في أوكرانيا (AISMTRU).

ويكشف نظام AISMTRU عن رموز الهوية الدولية للمعدات المتنقلة (IMEI) التي لا ترد في "القائمة البيضاء" من قاعدة البيانات العامة للهوية الدولية للمعدات المتنقلة (IMEI). وتسجَّل رموز الهوية الدولية للمعدات المتنقلة (IMEI) هذه في "القائمة الرمادية". ويتلقى جميع أصحاب تلك المطاريف تحذيراً طي رسالة نصية قصيرة (SMS) بفصلها عن الشبكة بعد 90 يوماً.

وبعد فترة 90 يوماً، يُنقل رمز الهوية الدولية للمعدات المتنقلة (IMEI) من "القائمة الرمادية" إلى "القائمة السوداء". ولا يخدّم المشغلون مطاريف "القائمة السوداء" (برفض تسجيلها في الشبكة، باستثناء مكالمات الطوارئ إلى الرقم "112"). ولا يغير التوصيل بأي شبكة مشغل أخرى الوضع القائم للمطراف المدرج في القائمة "الرمادية" أو "السوداء".

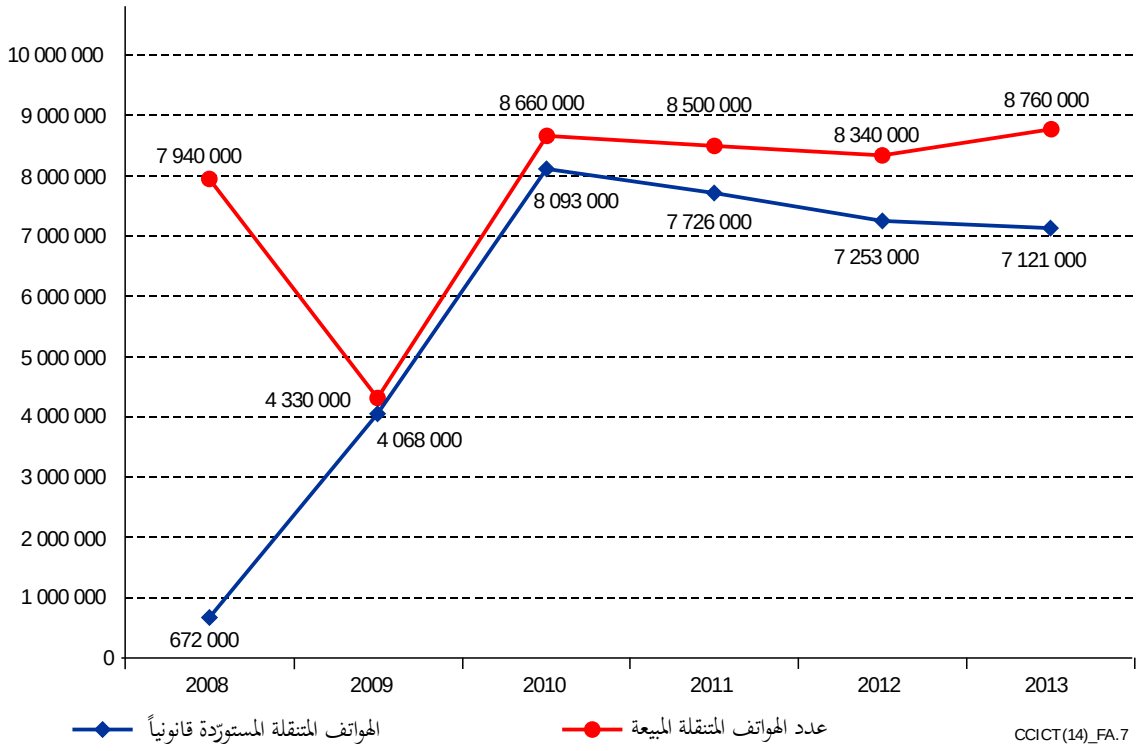
وبعد تلقي التحذير طي رسالة نصية قصيرة (SMS) بالإدراج في "القائمة الرمادية" وفترة الخدمة المحدودة بمدة 90 يوماً، يمكن لصاحب المطراف التقدم بطلب إلى مركز الدولة الأوكرانية للترددات الراديوية (UCRF) ليعرض تأكيداً للاستيراد القانوني للمطراف. ويستعرض موظف المركز طلب المالك، وفي حال تأكد قانونية الاستيراد، ينقل رمز الهوية الدولية للمعدات المتنقلة (IMEI) من "القائمة الرمادية" إلى "القائمة البيضاء". وبعد هذا الإجراء، يبدأ مشغلو الاتصالات المتنقلة بخدمة المطراف دون حد زمني.

بيد أن مطاريف "القائمة السوداء" لا تُفصَل، في الوقت الحاضر، جراء غياب الصك القانوني المطلوب.

ويدير مركز الدولة الأوكرانية للترددات الراديوية (UCRF) مركز المكالمات للتعامل مع المكالمات المتعلقة بطلبات من مستخدمي المطراف المتنقل بشأن وضع رمز الهوية الدولية للمعدات المتنقلة (IMEI) واستيراد المطاريف.

4 تقنين سوق المطاريف في أوكرانيا

- لقد انخفض بشدة الاستيراد "الرمادي" (غير القانوني) للمطاريف المتنقلة في أوكرانيا. وارتفعت حصة المطاريف المتنقلة المستوردة قانونياً إلى 93%-95% في عام 2010 (مقابل 7,5% في عام 2008).
- حُولت إيرادات تزيد عن 500 مليون دولار أمريكي إلى الموازنة العامة للدولة في أوكرانيا خلال الفترة 2010–2012 من الرسوم الجمركية على الواردات من المطاريف المتنقلة، مقارنةً مع 30 مليون دولار أمريكي خلال السنوات الثلاث السابقة.
- يتكون سوق المطاريف المتنقلة الأوكراني أساساً من المطاريف المتنقلة التي تلبي المتطلبات التقنية المميزة للاستخدام في أوكرانيا.
- كان هناك 140 865 260 من رموز هوية IMEI للمطاريف المتنقلة المسجلة في قاعدة البيانات العامة للهوية الدولية للمعدات المتنقلة في نظام AISMTRU في 30 أبريل 2013.
- استُردت تكاليف نظام المعلومات المؤتمت لتسجيل المطاريف المتنقلة في أوكرانيا (AISMTRU) خلال سبعة أشهر من مجرد الأموال الواردة إلى مركز الدولة الأوكرانية للترددات الراديوية (UCRF) عن مدفوعات المستوردين.



الشكل 7.A – مؤثرات تنفيذ نظام المعلومات المؤتمت لتسجيل المطاريف المتنقلة (AISMTRU) في أوكرانيا

12.1.A الإمارات العربية المتحدة (UAE)

تحظر قوانين الاتصالات في الإمارات العربية المتحدة استخدام الأجهزة المتنقلة المقلَّدة وبيعها وشراءها وتوزيعها والترويج لها. وتتخذ هيئة تنظيم الاتصالات (TRA) كل الخطوات اللازمة لضمان الوقف الكامل لبيع هذه الأجهزة واستخدامها في الإمارات العربية المتحدة. ويُنبَّه المتورطون في بيع الهواتف المتنقلة المقلَّدة ويغرَّمون، بينما يمكن في بعض الحالات حجب التراخيص نتيجة عدم تلبية اللوائح.

وفي عام 2011، أطلقت هيئة تنظيم الاتصالات حملة جديدة http://www.uaeinteract.com/docs/TRA_urges_against_use_of_fake_cell_phones/47437.htm لزيادة الوعي والثني عن استخدام الهواتف المتنقلة المقلَّدة في الإمارات العربية المتحدة، وأُعلن أن جميع الهواتف المتنقلة ذات أرقام الهوية الدولية للمعدات المتنقلة (IMEI) المزورة ستتوقف، اعتباراً من 1 يناير 2012، عن العمل ضمن شبكة الاتصالات المتنقلة في الإمارات العربية المتحدة. ونشرت هيئة تنظيم الاتصالات إعلانات في الصحف اليومية تحذر الناس بشأن الحظر الوشيك على الهواتف المزيَّفة.

وفي حين سعى هذا الإجراء إلى جعل أجهزة الهاتف المتنقل المزورة من مخلّفات الماضي، لم تتأثر الاشتراكات بالخدمة واستمرت في العمل بشكل طبيعي عند استخدام أجهزة الهاتف المتنقل الأصلية. ويمكن للمستخدمين الحصول على رد من مقدم خدمة يورد معلومات عن وضع الجهاز المتنقل عن طريق إرسال رسالة نصية قصيرة (SMS) مشفوعةً برقم هوية IMEI للجهاز المتنقل إلى رقم الهاتف "8877". ويبادر مقدمو الخدمة إلى الاتصال على الفور بمستخدمي الأجهزة المزورة، فيما يتعين فصل جميع الهواتف غير المعتَمدة من حيث النوع عن جميع خدمات الاتصالات، بما في ذلك المكالمات والنصوص والإنترنت.

وأعلنت الهيئة أن الأجهزة المتنقلة المزورة يمكن أن تكون ضارة لصحة المستخدم، وحثت جميع المستخدمين على اتخاذ الاحتياطات المناسبة عند شراء الأجهزة والمعدات المتنقلة. ووفقاً لهيئة تنظيم الاتصالات، تكون الهواتف المقلَّدة عرضة بشكل خاص لتسربات وانفجارات البطارية التي تطلق مواد كيميائية أكَّالة أو سامة. ويؤدي تدني جودة التجميع أيضاً إلى عدم ضبط مستويات الإشعاع مما يرجح سرعة استنزاف البطاريات ويضعف بشدة عادةً الإشارة المستقبَلة.

وتمثل الهدف النهائي لهيئة تنظيم الاتصالات في إزالة الأجهزة المتنقلة المقلدة من الإمارات العربية المتحدة وتثقيف الجمهور العام فضلاً عن تجار التجزئة بشأن المخاطر التي ينطوي عليها استخدامها. وأدركت هيئة تنظيم الاتصالات أن قضايا التزييف والقرصنة كان لها تأثير هائل على الاقتصاد وحقوق الملكية الفكرية، وأن الهواتف المتنقلة المقلدة كانت أيضاً أجهزة متدنية الجودة صُنعت دون الاختبارات والضوابط المناسبة.

2.A أمثلة عن تدابير مشتركة على المستويات الإقليمية

1.2.A لجنة البلدان الأمريكية للاتصالات (CITEL)

أسست الجمعية العامة لمنظمة الدول الأمريكية (OAS) لجنة البلدان الأمريكية للاتصالات (CITEL) في عام 1994 بهدف تعزيز تنمية الاتصالات/تكنولوجيا المعلومات والاتصالات في الأمريكتين. وتضم عضوية اللجنة كل الدول الخمس والثلاثين، فضلاً عن أكثر من 100 عضو منتسب من دوائر صناعة تكنولوجيا المعلومات والاتصالات.

وفي عام 2009، أوصت اللجنة الاستشارية الدائمة الأولى (الاتصالات) لدى لجنة البلدان الأمريكية للاتصالات (CITEL PCC.I) الدول الأعضاء بأن "تنظر في إنشاء قواعد بيانات كجزء من برنامج شامل لمكافحة التزييف والاحتيال" (التقرير النهائي للاجتماع الخامس عشر للجنة CITEL PCC.I في 2 أكتوبر 2009)، وفي ديسمبر 2011 بدأت اللجنة الاستشارية الدائمة الثانية (الاتصالات الراديوية بما في ذلك الإذاعة) لدى لجنة البلدان الأمريكية للاتصالات (CITEL PCC.II) بدراسة التدابير التي تتخذها إدارات الاتصالات بشأن استخدام الهواتف المتنقلة المزيَّفة.

وقررت اللجنة PCC.II أن تطلب إلى الإدارات تقديم معلومات "بشأن الإجراءات والتدابير التنظيمية والإدارية المتخذة أو المخطط لها فيما يتعلق بالهواتف الخلوية المقلَّدة أو المزيَّفة أو تلك دون المستوى المطلوب وآثارها السلبية على المستخدمين والمشغلين بما في ذلك التداخل ومستويات الإشعاع غير المؤين واستخدام المكونات الكيميائية الخطرة أو المحظورة"(القرار 121 الوارد في التقرير النهائي للاجتماع الثامن عشر للجنة CCITEL PCC.II في 22 ديسمبر 2011).

وقد نظرت البلدان الأمريكية للاتصالات أيضاً في قضية سرقة الهاتف المتنقل ووافقت كلتا اللجنتين الاستشاريتين الدائمتين على عدد من القرارات المتعلقة بهذا الموضوع.

ووافقت اللجنة PCC.II على القرار 73 في سبتمبر عام 2011 بشأن "إقامة شراكة إقليمية لمكافحة سرقة المعدات الطرفية المتنقلة". وطلب هذا القرار إلى اللجنة PCC.I النظر في "أن تروج لجنة البلدان الأمريكية للاتصالات (CITEL) لأن تضع الدول الأعضاء تدابير مشتركة من أجل تقييد تفعيل هذه المعدات الطرفية المتنقلة المسروقة، في أي بلد من بلدان المنطقة، وأن تعتمد توصيات محددة للمشغلين بحيث يستخدمون الموارد التي تُتيحها التكنولوجيا ولا يسمحون بتوصيل المعدات التي لم يُحدَد منشؤها تماماً بشبكاتهم، مقيمين شراكة إقليمية لمكافحة سرقة هذه المعدات" (القرار 73 الوارد في التقرير النهائي للاجتماع السابع عشر للجنة PCC. II، في 6 سبتمبر 2011).

واستجابت اللجنة PCC.I على الفور تقريباً من خلال الموافقة على قرار بشأن "التدابير الإقليمية لمكافحة سرقة المطاريف المتنقلة" (القرار 189 الوارد في التقرير النهائي للاجتماع التاسع عشر للجنة PCC. I، في 20 سبتمبر 2011). ويشير هذا القرار إلى الطبيعة الدولية لهذه المشكلة إذ تُرسَل الأجهزة المتنقلة إلى بلدان أخرى عندما يتخذ أي بلد إجراءات ضد سرقة الأجهزة، وبالتالي تقتضي الضرورة اتخاذ تدابير على المستوى الإقليمي. وبالإضافة إلى التدابير المتعلقة بالأجهزة اليدوية المسروقة/المفقودة، يدعو القرار 189 الدول الأعضاء أيضاً إلى "النظر في تضمين أطرها التنظيمية حظر تفعيل واستخدام الهويات الدولية للمعدات المتنقلة أو الأرقام التسلسلية الإلكترونية للمصنِّع العائدة للأجهزة التي أُبلغ عن سرقتها أو ضياعها أو تلك *ذات المنشأ غير القانوني* في قواعد البيانات الإقليمية أو الدولية"(الخط المائل بقلم المحرر).

ويتضمن الملحق بالقرار 189 عدداً من التدابير التكميلية مثل "دراسة جدوى تنفيذ ضوابط للتسويق المحلي لأجهزة المطاريف المتنقلة وتوصيلها بشبكات" و"تشجيع إنشاء آليات مالية تنظيمية و/أو جمركية تضمن استيراد أجهزة المطاريف المتنقلة و/أو قِطَعها من مصدر مشروع ومنحها الشهادات وفقاً للإطار التنظيمي لكل دولة عضو، وكذلك إنشاء ضوابط جمركية تمنع خروج أو إعادةً تصدير ما يُسرق من أجهزة المطاريف المتنقلة و/أو قِطَعها".

ووافقت اللجنة PCC.I على توصية بشأن "التدابير الإقليمية لتبادل المعلومات عن أجهزة المطاريف المتنقلة التي أُبلغ عن سرقتها أو ضياعها أو استردادها" في عام 2012 (التوصية 16 الواردة في التقرير النهائي للاجتماع العشرين للجنة CITEL PCC.I، في 10 يونيو 2012) والتي تضمنت أيضاً المطاريف ذات "المنشأ غير القانوني". ودعيت الدول الأعضاء "لتنفيذ الإجراءات والتدابير الوطنية والإقليمية والدولية بحيث يمكن لمقدمي خدمة الاتصالات المتنقلة تبادل المعلومات بشأن أجهزة المطاريف المتنقلة المفقودة أو غير القانونية من خلال مختلف المنصات القائمة والعاملة لمختلف تكنولوجيات النفاذ بغية مكافحة الأسواق غير الرسمية وتعزيز التعاون بين الدول والحفاظ على مبادئ أمن المواطن وحقوق المستخدمين النهائيين". وأوصيت الدول الأعضاء أيضاً "بالنظر في إنشاء منصة قاعدة بيانات لتبادل المعلومات عن المطاريف المتنقلة المسروقة أو المفقودة أو ذات المنشأ غير القانوني باستخدام أرقام معرف المعدات المتنقلة (MEID) المستخدمة في النفاذ المتعدد بتقسيم شفري (CDMA) وEV-DO والجيل الرابع من النفاذ المتعدد بتقسيم شفري (CDMA/4G) وفي العديد من الشبكات، وفي وحدة هوية المستخدم القابلة للإزالة (RUIM)".

وقد وافقت اللجنة PCC.I أيضاً على "الكراس التقني" بشأن " المطاريف المتنقلة المسروقة و/أو المفقودة" (القرار 217 الوارد في التقرير النهائي للاجتماع الثالث والعشرين للجنة CITEL PCC.I في 10 أكتوبر 2013).

وفي مايو 2014، وافقت لجنة البلدان الأمريكية للاتصالات (CITEL) على القرار 222 (XXIV-14) بشأن "*تعزيز التدابير الإقليمية لمكافحة انتشار الأجهزة المتنقلة المزيَّفة، ودون المستوى المطلوب وغير الموافَق عليها*".

ونتيجة لذلك، شُكل فريق مراسلة لمناقشة التدابير الإقليمية لمكافحة انتشار الأجهزة المتنقلة المزيَّفة، ودون المستوى المطلوب وغير الموافَق عليها، من أجل تبادل المعلومات والخبرات والممارسات الفضلى من الناحية التقنية والتنظيمية مع الدول الأعضاء المعنية بهذه القضية، وذلك بهدف وضع التوصيات والمبادئ التوجيهية التي يمكن إرساؤها ضمن منطقة الأمريكتين.

وفي أغسطس 2014، تمت الموافقة على خطة عمل فريق المراسلات هذا وأُدرجت في نطاق مهام المقرر المعني بضبط الغش والممارسات المخالفة للوائح في مجال الاتصالات، وفي التدابير الإقليمية ضد سرقة أجهزة المطاريف المتنقلة، على أساس التفويض التالي:

1 وضع تعريف لما هو مقصود بالأجهزة المتنقلة المزيَّفة، ودون المستوى المطلوب وغير الموافَق عليها.

2 تقييم نطاق وطبيعة مشكلة الأجهزة المتنقلة المزيَّفة، ودون المستوى المطلوب وغير الموافَق عليها.

3 تعزيز تبادل المعلومات والخبرات بين أعضاء لجنة البلدان الأمريكية للاتصالات بشأن التدابير المتخذة لمحاربة بيع واستخدام الأجهزة المتنقلة المزيَّفة، ودون المستوى المطلوب وغير الموافَق عليها.

4 توثيق الممارسات الفضلى من مختلف أنحاء العالم في مكافحة بيع واستخدام الأجهزة المتنقلة المزيَّفة، ودون المستوى المطلوب وغير الموافَق عليها.

5 اقتراح وضع كراسات و/أو توصيات و/أو قرارات تقنية من لجنة البلدان الأمريكية للاتصالات تتناول التدابير التقنية والتنظيمية لمكافحة بيع واستخدام الأجهزة المتنقلة المزيَّفة، ودون المستوى المطلوب وغير الموافَق عليها، في منطقة الأمريكتين.

6 إنهاء العمل وتقديم تقرير عن النتائج التي تحققت إلى مكتب المقرر المعني بضبط الغش والممارسات المخالفة للوائح في مجال الاتصالات.

2.2.A مجموعة شرق إفريقيا (EAC)

تفقد منطقة شرق إفريقيا أكثر من 500 مليون دولار أمريكي من العائدات سنوياً جراء تقليد المنتجات http://www.trademarkea.com/ea-loses-huge-sums-of-money-in-counterfeit-products. فيحمل تغليف المنتجات الرخيصة ودون المستوى المطلوب المورَّدة من خلال التجار والمصنعين الأجانب والمحليين نسخاً غير قانونية للأسماء والتصاميم التجارية المعروفة.

ووفقاً لبروتوكول السوق المشتركة، الذي اعتمدته مجموعة شرق إفريقيا (EAC) في عام 2010، لا يمكن أن تُحزم المنتجات المزيَّفة والتجارة فيها إلا من خلال التعاون.

ومنظمة اتصالات شرق إفريقيا (EACO) هي هيئة إقليمية تجمع المنظمات التنظيمية والبريدية ومنظمات الاتصالات والإذاعة من الدول الخمس الأعضاء في مجموعة شرق إفريقيا (كينيا وتنزانيا ورواندا وبوروندي وأوغندا). وقد نظرت منظمة اتصالات شرق إفريقيا في قضية إغراق المنطقة بالهواتف المتنقلة المزيَّفة ووافقت على مبادرة مشتركة تقابلها في عام 2012.

وأوصى فريق مهام الترقيم في منظمة اتصالات شرق إفريقيا (CCK–كينيا، وTCRA–تنزانيا، وRURA–رواندا، وARCT–بوروندي، وUCC–أوغندا) في مايو 2012 بإعداد قاعدة بيانات على الصعيد الوطني واعتماد إجراءات للتحقق من الأجهزة اليدوية لحماية المستهلكين والشركات والشبكات من مؤثرات المعدات المزيَّفة (تقرير فريق مهام الترقيم في منظمة اتصالات شرق إفريقيا للفترة 2011-2012).

وأُعلم المؤتمر التاسع عشر لمنظمة اتصالات شرق إفريقيا بحالة تنفيذ سجلات هوية المعدات (EIR) في المنطقة، وجاء وصف بعض التحديات التي تعترضه في الرابط http://www.eaco.int/docs/19_congress_report.pdf. وكانت هذه التحديات كالتالي:

- نسخ وغياب الهوية الدولية للمعدات المتنقلة (IMEI)؛
- قلة وعي المستهلكين بالمخاطر المرتبطة بالمعدات المزيَّفة ونقص المعرفة بكيفية التحقق من أن المعدات أصلية؛
- قلة وعي منافذ البيع المحلية/"البائعين" المحليين بالقضايا المرتبطة ببيع المعدات الرخيصة ذات المستوى دون المطلوب؛
- ارتفاع تكلفة التنفيذ.

ومن أجل التغلب على هذه التحديات، اقترحت الحلول التالية:

- تنفيذ حملات توعية للمستهلكين والبائعين المحليين؛
- ترخيص جميع منافذ البيع/البائعين؛
- تعزيز إجراءات اعتماد النوع؛
- إنشاء قواعد بيانات المعدات؛
- اشتراط تسجيل بطاقة وحدة هوية المشترك (SIM).

3.2.A رابطة منظمي وسائل التواصل والاتصالات لمجموعة البلدان الناطقة بالبرتغالية (ARCTEL-CPLP)

تضم رابطة منظمي وسائل التواصل والاتصالات لمجموعة البلدان الناطقة بالبرتغالية (ARCTEL-CPLP) أعضاء من أنغولا والبرازيل والرأس الأخضر وغينيا–بيساو وموزامبيق والبرتغال وسان تومي وبرينسيبي وتيمور الشرقية (http://www.arctel-cplp.org). وقدمت الرابطة عرضاً في الندوة العالمية لمنظمي الاتصالات التي نظمها الاتحاد الدولي للاتصالات في عام 2012 بشأن النهج الإقليمية لمكافحة سرقة الأجهزة المتنقلة والسوق الرمادية والأجهزة المزيَّفة https://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR12/RA12/pdf/Batista3_ARCTEL_Session3_mobilerobbery.pdf.

واقترحت رابطة منظمي وسائل التواصل والاتصالات لمجموعة البلدان الناطقة بالبرتغالية (ARCTEL-CPLP) توسعة الحل التقليدي (أي أنظمة قواعد بيانات القائمة السوداء الوطنية) لتشمل المستوى الإقليمي من خلال التالي:

- التشارك في قواعد بيانات القائمة السوداء لأجهزة النظام العالمي للاتصالات المتنقلة (GSM) وأجهزة النفاذ المتعدد بتقسيم شفري (CDMA) من خلال اتفاقات ثنائية أو متعددة الأطراف؛
- إنشاء آليات تنظيمية مالية و/أو جمركية تضمن قدراً أكبر من السيطرة على استيراد الأجهزة اليدوية ومنع إعادةً التصدير؛
- التزام دوائر الصناعة بالتوصيات الأمنية ضد إعادةً برمجة أو نسخ الهويات الدولية للمعدات المتنقلة أو أرقام التعرف التسلسلية الإلكترونية للمصنِّع؛
- تنفيذ حملات لرفع الوعي العام بأهمية الإبلاغ عن سرقة وفقدان أجهزة المطاريف المتنقلة.