تحليل الآثار المترتبة عن أنظمة التعاملات والجرائم الإلكترونية في السعودية

د. إبراهيم سليمان عبدالله - جامعة الملك عبدالعزيز
Dr. Ibrahim S. Abdullah - King Abdulaziz University
iabdullah@kau. edu. sa

الملخص:

أقرّ مجلس الوزراء بالمملكة العربية السعودية في الجلسة الوزارية بتاريخ 1428/3/7 هـ نظامي التّعاملات الإلكترونيّة ومكافحة الجرائم الإلكترونيّة، ونظرا لما تمثّله هذه الأنظمة من تحوّل كبير في سبيل انتقال بيئة العمل السّعوديّة من البيئة التّقليديّة إلى بيئة العمل الإلكترونيّة في القطاع الحكومي والقطاع الخاص، وما يصاحب هذا الانتقال من تأثيرات اقتصادية واجتماعية كبيرة، فإنّ هذا التّحول بحاجة إلى دراسة ورصد للآثار المتوقّعة للأنظمة المشار إليها، سواء كانت إيجابيّة أو سلبيّة، من النّاحية الاجتماعيّة والاقتصاديّة والتّعليميّة والتّقنيّة، بهدف تنمية الجوانب الإيجابية والتّقليل من الجوانب السّلبيّة. وسيعتمد هذا البحث منهجيّة البحث المقارن التي تقوم على البعد المكانيّ والكيفيّ، لرصد الآثار المترتّبة على تطبيق هذه الأنظمة ومقارنة هذه الأنظمة ببعض التجارب المماثلة لبعض الدّول التي سبقت في هذا المجال، واستنباط الوسائل والسّياسات التي يمكن أن تساهم في تعزيز الآثار الإيجابية والتقليل من الآثار السّلبيّة. وقد توصّلت هذه الدراسة الى أنّ المملكة خطت خطوة مهمّة في تعزيز التّعاملات الإلكترونيّة بالمقارنة بما تمّ على المستوى العالميّ، حيث أنّ من أبرز متطلّبات نجاح التّعاملات الإلكترونيّة هو بناء الثّقة في البيئة القانونيّة التي تتمّ فيها هذه العمليّات. كما توصّلت الدّراسة الى ضرورة تدعيم هذه الخطوة من خلال الاتّفاقات الدّولية الثّنائية لملاحقة الجرائم الصّادرة من خارج المملكة، والحاجة الى ضوابط لإلزام الشّركات بالإفصاح عن الحوادث الإلكترونيّة، وآليّات لمتابعة مزودي خدمة الإنترنت لحفظ حركة المرور بطرق احترافيّة لأهمّيّتها الكبيرة في المساهمة في توفير الأدلّة الجنائيّة الإلكترونيّة. كما تشير النّتائج أيضاً الى أهمّيّة دمج التّدريب والتّوعية بهذه التشريعات ضمن جميع مسارات التّعليم سواء العاديّ أو التّقنيّ أو القضائيّ أو الأمنيّ.

الكلمات المفتاحية:

تجارة إلكترونيّة، تعاملات إلكترونيّة، جرائم إلكترونيّة، قوانين، أمن المعلومات.

تمهيد

صاحب ظهور الإنترنت والتّجارة الإلكترونيّة دعوات لتحرير البيئة الإلكترونيّة من الأنظمة وسيطرة الحكومات عليها بحجّة أنّها عالم جديد يتعدّى السّياسة والجغرافيا، ويؤسّس لعولمة تغطّي جوانب الحياة المختلفة خاصّة الاقتصاديّة والاجتماعيّة. لكنّ هذه الدّعوات ما لبثت أن خفتت وتضاءلت بحكم الواقع وبحكم أنّ الإنترنت بيئة ومجتمع حيّ انعكست فيه كلّ تصرّفات البشر الإيجابية والسّلبيّة، وهو لذلك بحاجة ماسّة للتّشريعات والنّظم من أجل أن تستقيم الحياة فيه، وتنتظم فيه شؤون المستخدمين والعاملين، وتُحفظ فيه حقوق كلّ الأطراف المتعاملة (Swire, 2003).

وقد أصبحت هذه التشريعات ضرورة ماسّة بسبب انتشار الاستخدام غير المشروع للوسائل الإلكترونيّة للإضرار بالآخرين، فقد جاء في دراسة مسحيّة أجراها معهد أمن الحاسب الآليّ بالتعاون مع وكالة الاستخبارات الفيدراليّة الأمريكية CSI/FBI أن متوسّط الخسارة للفرد الواحد في المسح الذي شاركت فيه 277 منظّمة من تسع دول بسبب قرصنة المعلومات زاد من 130 دولارا الى 136 دولارا للعام 2013 (Ponemon, 2013). وبالإضافة إلى ذلك فقد بلغت سرقة التّعاملات الإلكترونيّة عبر الإنترنت في العام 2012 نحو 5.3 بليون دولار في الولايات المتحدة الأمريكية (CyberSource, 2013). وفي تقرير مايو 2013 لمركز جرائم الإنترنت للحكومة الفدرالية الأمريكية IC3، وصل عدد بلاغات الجرائم للعام 2012 إلى 289,874 بزيادة قدرها 8% عن العام السابق (FBI, 2013). هذا في الجانب الاقتصادي. أمّا في الجانب الأخلاقيّ، فقد زادت عدد المواقع الإباحية المتاحة على الإنترنت من 88,000 موقع عام 2000 الى 1. 6 مليون موقع للعام 2008 ووصل عدد المحتويات الإباحية 2,8 بليون مادة في العام 2015 على الأجهزة الذكية المحمولة (CovenantEyes, 2013).

ومن مؤشّرات خطورة الانتشار الواسع للجرائم الإلكترونيّة حسب تقرير صحيفة الوول ستريت جورنال بلوغ معدل الجرائم الإلكترونيّة 53 % من إجمالي الجرائم التي تحدث لعامة العملاء. وقد أصبحت مكافحة الجرائم الإلكترونيّة تحتلّ المرتبة الثّالثة لدى مكتب التّحقيقات الفيدراليّ في الولايات المتّحدة الأمريكية بعد مكافحة الإرهاب ومكافحة التجسس (Kshetri, 2006). ومن أسباب صعوبة التّصدي لهذا النوع من الجرائم أنّها تحتاج إلى مهارات تقنيّة عالية، وأنّها عالميّة تتخطّى الحدود الجغرافيّة والسياسيّة، وأنّها جديدة وليس لدى الدّول حتّى المتقدمة منها الخبرة الكافية في تطوير تقاليد وأدوات كافية للتّعامل معها.

وعليه فإن ما صدر من أنظمة تشريعيّة لتنظيم البيئة الإلكترونيّة في السّعوديّة هو خطوة مهمّة في الاتّجاه الصحيح. وهذه الخطوة بحاجة إلى المزيد من الدّعم والتّعزيز نظراً لأنّ القضيّة ليست متعلّقة بمجرّد صدور قوانين بل هي بيئة متكاملة ودورة متسلسلة من الاحتياجات يكمّل بعضُها بعضاً، يدخل فيها التّشريعات والأجهزة الأمنيّة والتقنيّات والمستخدمين والتّعليم والاقتصاد. وفي هذا الإطار تأتي هذه الدّراسة لتلقي الضّوء على جانب من الآثار المتوقّعة نتيجة هذه التّشريعات، وكيف يمكن تحقيق أكبر قدر من الأهداف التي وُضعت من أجلها. وقد اعتمدت الدّراسة على تحليل بنود هذه الأنظمة ومقارنتها بتجارب الدّول المتقدّمة بحيث يتوصّل إلى مجموعة من التّوصيات تساهم في خدمة أهداف هذه الأنظمة.

وتتكوّن الدّراسة من مقدّمة وخاتمة وثمانية فصول، الأوّل يعرض ملخّصا لنظام التّعاملات الإلكترونيّة، والثّاني يعرض أبرز محاور نظام الجرائم الإلكترونيّة، والثّالث يقدّم أبرز تجارب الدّول المتقدّمة في هذا المجال، والرّابع يناقش تحليل آثار هذه الأنظمة، والخامس يعالج المحور الاقتصاديّ، والسّادس يتناول المحور الاجتماعيّ والأخلاقيّ، والسّابع يدور حول المحور التّقنيّ، ثم في الفصل الثّامن يتم عرض ملخّص النتائج والتّوصيّات. كما أنّنا استخدمنا في هذا البحث كلمة تشريعات للإشارة إلى نظامي التّعاملات والجرائم الإلكترونيّة بالمعنى اللّغوي للكلمة وليس بالمعنى الشّرعي الدّينيّ، وذلك للتّفريق بينها وبين كلمة نظام التي تستخدم كمصطلح له معان كثيرة في بيئة تقنية المعلومات.

1. نظام المعاملات الإلكترونية

جاء في نظام التّعاملات الإلكترونيّة واحد وثلاثون مادّة، ففي الفصل الأول وردت أربع موادّ: عرضت المادّة الأولى تعريفاً بالمصطلحات المستخدمة في النّظام وأوردت المادّة الثّانية الأهداف التي يسعى النّظام إلى تحقيقها وحدّدت المادّة الثّالثة التّعاملات المستثناة من النّظام وحددت المادّة الرّابعة الجهات التي ينطبق عليها النّظام، ثم في الفصل الثاني من النّظام وردت الآثار النّظامية للتّعاملات والسّجلات والتّوقيعات الإلكترونيّة. أمّا الفصل الثّالث فجاءت فيه أربع موادّ أوردت كيفيّة إثبات التّعاقد في التّعاملات الإلكترونيّة. وعرض الفصل الرّابع مادّة تشرح أحكام وطريقة عمل التّوقيع الإلكترونيّ. وجاء في الفصول الأخيرة من الخامس إلى الفصل العاشر أحكام تتعلّق بجهات الاختصاص وواجبات مقدّم خدمة التّصديق الإلكترونيّ ومسئوليّة صاحب الشّهادة وأحكام مخالفة النّظام والعقوبات المترتّبة على تلك المخالفات.

ويهدف النّظام كما جاء في المادّة الثانية إلى رسم قواعد لاستخدام التّعاملات الإلكترونيّة وتسهيل تطبيقها والاعتراف بالسّجلات الإلكترونيّة والتّعويل عليها، سواء على الصّعيد المحلّيّ أو الدّوليّ في جميع المجالات الحكوميّة وغير الحكوميّة، الماليّة وغير الماليّة. كما يهدف النّظام إلى رفع العوائق والعقبات أمام التّعاملات الإلكترونيّة والتوقيعات الإلكترونيّة وكذلك منع إساءة الاستخدام والاحتيال فيها.

وبعبارة أخرى يمكن القول إنّ النّظام يدور حول محورين: الأوّل يتعلّق بالتعامل مع السّجلات الإلكترونيّة والثّاني يتعلّق بالتوقيع الإلكترونيّ. ففي جانب التّعامل مع السّجلات الإلكترونيّة، أقرّ واعترف النّظام بحجّيّتها وقابليّتها للتّنفيذ وحجّيّة انعقاد التّعامل بواسطتها متى كان الاطّلاع على تفاصيلها متاحاً ضمن المنظومة الإلكترونيّة. وحدّد النّظام طريقة حفظ السّجلات وصلاحيّتها واستلامها وتسليمها.

أمّا في المحور الثّاني، وهو محور التّوقيع الإلكترونيّ، فقد ساوى النّظام بين التّوقيع الخطّيّ والتّوقيع الإلكترونيّ في الحكم، وأنّ التّوقيع الإلكترونيّ بمثابة التّوقيع الخطّيّ وله نفس الآثار النّظاميّة. وربط النّظام بين التّوقيع الإلكترونيّ والشّهادة الرّقميّة، وحدّد شروط صحّة التّوقيع الإلكترونيّ وضرورة اعتماد الشّهادات الرّقميّة من قبل مقدّم خدمات تصديق إلكترونيّ معتمد. وأفرد النّظام فصلاً مستقلاً للتشريعات الخاصّة بالمركز الوطني للتّصديق الإلكترونيّ الذي يختصّ باعتماد شهادات التّصديق الرّقميّ الصّادرة من داخل المملكة وخارجها. ثمّ عرض النّظام واجبات ومسئوليات مقدّم خدمات التّصديق، وهي شركات خاصّة تحصل على ترخيص من هيئة

الاتّصالات وتتولّى تقديم خدمات إصدار الشّهادات الرّقميّة وتسليمها وحفظها. وأوضح النّظام المسؤوليّات المترتّبة على صاحب الشّهادة وضرورة التزامه بشروط استخدامها والالتزام بالآثار النّاشئة عن هذا الاستخدام وصحّة معلومات الشّهادة والإبلاغ عن فقدها أو تغيير المعلومات الواردة فيها.

2. نظام الجرائم الإلكترونية

حدّد النّظام مجموعة أهداف يسعى لتحقيقها تتلخّص في المساعدة في تحقيق أمن معلوماتيّ إلكترونيّ، وحفظ حقوق الأطراف المتعاملة عند الاستخدام المشروع للنّظم الإلكترونيّة والشّبكات، وحماية المصلحة العامة والأخلاق والآداب العامّة في البيئة الإلكترونيّة، وحماية الاقتصاد الوطنيّ في جانبه الإلكترونيّ والتّقليديّ نظراً للتّفاعل الكبير بين الجانبين. وقد غطت التّشريعات الجرائم الفعالة Active التي تتعلّق بالتّعدّي بالتعديل أو الحذف والإلغاء للرّسائل والمحتوى الرّقميّ أو تعطيل الأنظمة أو الأجهزة وإعاقة الوصول للخدمات الرّقميّة وكذلك الجرائم غير الفعّالة passive والتي تتعلق بالتعدّي بالتنصّت وسرقة المعلومات سواء خلال عمليّة الاتّصال وانتقال البيانات أو من مواقع تخزينها.

وشملت التّشريعات الاتّصال غير المشروع لتهديد شخص أو ابتزازه أو التّأثير عليه ليقوم بفعل معيّن ولو كان الفعل مشروعاً. وكذلك الاعتداء على تصاميم المواقع الإلكترونيّة بالتّغيير أو الإتلاف أو تعطيل العنوان. كما غطّت التّشريعات الأعمال التي تؤدّي إلى حماية المجتمع من خلال منع المواقع التي تعمل في الاتّجار في الجنس البشريّ أو تقديم الدعم والتسهيل لمثل هذا النشاط، وكذلك الأنشطة المخلّة بالآداب أو ترويجها وما يتعلّق بترويج المخدّرات والمؤثّرات العقليّة سواء ببيعها أو تسهيل التّعامل بها أو تعليم طرق التّعامل معها.

وتناول النّظام أيضا موضوع الأمن الوطنيّ من خلال تجريم كل ما يتعلّق بدعم الإرهاب عبر الوسائل الإلكترونيّة، واستخدام الشبكة العنكبوتيّة في الاتّصال مع أعضاء تلك المنظّمات أو ترويج أفكارها أو تمويلها أو نشر وسائل إعداد الخطط والأدوات التي تستخدم في الإرهاب، مثل طرق إعداد المتفجّرات والمواد الحارقة. وكذلك الاعتداء على مواقع تمس الأمن الوطني الداخليّ أو الخارجيّ للدّولة أو اقتصادها الوطنيّ عن طريق الشّبكة المعلوماتيّة وأجهزة الحاسب الآليّ.

3. التجارب السابقة

بدأ صدور التّشريعات لتنظيم التّعامل في البيئة الرّقميّة مبكّراً في الولايات المتّحدة الأمريكيّة. فقد صدر نظام حماية الخصوصيّة للاتّصالات الإلكترونيّة المسمى Electronic Communication Privacy Act (ECPA) عام 1984، حيث جاء هذا القانون بمنع التنصّت غير المشروع على الاتّصالات الإلكترونيّة ومنع الدخول على المواقع التي تقدم خدمات إلكترونيّة عبر الاتّصالات مثل سيرفرات البريد الالكتروني وسيرفرات مزودي الخدمات. لكنّه لم يتناول حماية البيانات الشّخصيّة التي توجد على الحاسبات المنزليّة.

ونظراً لعدم شمول قانون حماية الخصوصيّة للاتّصالات الإلكترونيّة السابق الذكر، صدر نظام الاحتيال وسوء استخدام الحاسب الآلي في العام 1986 Computer Fraud and Abuse Act (CFAA). ويهدف هذا النّظام إلى منع

كلّ أشكال الوصول المتعمّد إلى ملفّات الحاسب الآلي وأنظمته بشكل غير مشروع أو التّسبّب بأيّ ضرر لهذه الأنظمة. وجاء في هذه التشريعات ثمانية بنود ملخّصها منع الوصول غير المشروع للمعلومات الحكوميّة المصنّفة كمعلومات سرية، وكذلك معلومات المؤسسات الماليّة وغير الماليّة المحصّنة وغير المصرّح بها للعامّة، والاحتيال عبر الوسائل الإلكترونيّة للحصول على أيّ شيء تزيد قيمته عن خمسة آلاف دولار خلال عام واحد. وجاء في هذا النّظام أيضاً منع إرسال برامج أو معلومات أو أوامر إلكترونيّة تتسبب في تعطيل أجهزة محصّنة وإحداث خسائر تتجاوز خمسة آلاف دولار، ثم جاء قانون باتريوت عام 2001 ليلغي حد الخمسة آلاف دولار.

أمّا من ناحية تطبيق القانون، ومع التّطور التّقنيّ الهائل للولايات المتّحدة الأمريكيّة، فقد ذكرت الواشنطن بوست في 17 مايو عام2000 أنّ الأجهزة الأمنيّة الأمريكيّة تضم ما يقارب 2% فقط من المتخصّصين المؤهّلين في تحقيق الجرائم الإلكترونيّة، وأنّ هذه الإدارات الأمنيّة ليس لديها الموارد الماليّة والتقنيّة الكافيّة لمواجهة الاحتياجات، وغير قادرة على ملاحقة التّطوّر السّريع الحاصل في هذا المجال (Kshetri, 2006, Chang, 2004) . وبسبب المهارة العالية التي تحتاج إليها تحقيقات الجرائم الإلكترونيّة، فإن كثيراً من الدّول لا تتمكّن من التّحقيق في كثير من البلاغات والتقارير التي تصل إليها، فعلى سبيل المثال تقدّر نسبة المخالفات الإلكترونيّة التي يتم اكتشافها في الولايات المتّحدة بحوالي عشرة في المائة من التي تحدث فعلاً، وتقدّر النّسبة التي يتمّ الإبلاغ عنها بـ 30%. ومن هذه النسبة التي يتمّ الإبلاغ عنها، يتمّ التّحقيق في نسبة ضئيلة منها لا تزيد عن عشرين في المائة (Chang, 2004). وفي مثال آخر في اندونيسيا تم التحقيق في 15% فقط من الجرائم الإلكترونيّة التي وردت بلاغات عنها (Kshetri, 2006).

ولو تمعّنّا في مشكلة توفّر الإمكانات للتّحقيق في الجرائم الإلكترونيّة، لوجدنا أنّ ما تمّ نشره ممّا تم التحقيق فيه من الجرائم ضئيل جداً مقارنة بعدد الجرائم التي تحدث، وذلك لعدة أسباب منها صعوبة اكتشاف هذه الجرائم وعدم الإبلاغ عن عدد كبير ممّا تمّ اكتشافه وقلة المتخصصين المؤهلين للتّحقيق فيما تم اكتشافه والتبليغ عنه. وفي دراسة أجريت على قضايا الجرائم الإلكترونيّة للعام 1999، تمّ التّحقيق في 419 قضيّة، رفضت المحكمة 339 قضيّة منها لعدم كفاية الأدلّة، وكان من أسباب عدم كفاية الأدلة ضعف وعي المجني عليهم بكيفية حفظ الأدلة الإلكترونيّة واستمرارهم على سبيل المثال في استخدام الأجهزة مما يؤدّي إلى مسح أثار الجرائم بسبب إعادة الكتابة أو امتلاء نظام المراجعة log files (Chang, 2004).

وتتلخّص أسباب عدم لجوء الشّركات للإبلاغ عن الحوادث الإلكترونيّة في الخوف من استغلال المنافسين لمثل هذه المعلومات في الدّعاية السّلبيّة، وكذلك بسبب بطء التّحقيقات وبالتّالي ارتفاع تكاليفها على الشّركة المجنيّ عليها من حيث عدد لقاءات التّحقيقات وما تستهلكه من وقت العمل. فعلى سبيل المثال أفلست شركة Egghead.Com المتخصّصة في التّسويق والتّقنية بسبب إبلاغها عن حادث اختراق الكترونيّ حدث لها عام 2000 بسبب أنّها سارعت بالإبلاغ واستخدمت مجموعة من أفضل المحقّقين الخاصّين لتحديد المشكلة واعتقدت أنّ الأمر سينتهي خلال خمسة أيام، لكن التّحقيقات استمرّت عشرين يوماً وانتشر الخبر وانهارت مبيعات الشّركة انهياراً حاداً أدى بها إلى إشهار إفلاسها ومن ثم اشترتها شركة أمازون عام 2001 (Chang, 2004).

وعلى الرّغم من مرور قرابة ثلاثين عاماً على صدور قانون CFAA، فإنّ معدّل الجرائم الإلكترونيّة لم يتراجع بل زاد. ففي المسح الذي أجرته شركة كاسبرسكاي المتخصصة في مكافحة الهجمات الإلكترونيّة أنّ اجماليّ الهجمات الإلكترونيّة بلغ عام 2013 أكثر من خمسة بلايين محاولة على أجهزة الحاسب الشخصية والهواتف الذكية المحمولة، منها 45% صادرة من أجهزة في الولايات المتحدة الأمريكية وروسيا (Kaspersky, 2013).

ومن أكبر عوائق مكافحة الجرائم الإلكترونيّة أنّ كثيراً من هذه الجرائم عابرة للحدود السياسيّة والجغرافيّة، مع ضعف في عدد من الدّول أو عدم وجود تعاون دوليّ في هذا المجال. فالاتفاقيّة الموقّعة على سبيل المثال بين الولايات المتحدة وروسيا للتّعاون في التّحقيق في كثير من الجرائم لا تشمل الجرائم الإلكترونيّة، وعندما احتاج المحقّقون في الولايات المتحدة تحميل بعض البيانات المتعلّقة بجريمة إلكترونيّة من أجهزة حاسب آلي في روسيا اعترضت روسيا ورفعت شكوى ضد مكتب التحقيقات الفيدرالي عام 2002. وبشكل عام فإن روسيا والصّين حتّى الآن لا تكترث كثيراً للجرائم الإلكترونيّة ما لم تمسّ أمنها الدّاخليّ. والوضع داخل الاتحاد الأوربي قريب من ذلك: فقد شاركت 34 دولة في أوربا بالتوقيع المبدئي على اتفاقية مكافحة الجرائم الإلكترونيّة، لكن حتى منتصف عام 2004 لم تعتمد الاتفاقية وتطبقّ إلا في 6 دول فقط (Kshetri, 2006).

وللاتحاد الأوربي تجربة تجدر الاستفادة منها وهي تجربة تطبيق قانون حماية الخصوصيّة الشّخصيّة عام 1998. فعلى سبيل المثال مما يؤخذ على هذا القانون أنّه يمنع بشكل قاطع ودون استثناءات نقل المعلومات الشّخصيّة لمواطني الاتحاد الأوربي إلى الدول التي ليس فيها نفس مستوى الحماية لهؤلاء المواطنين. وقد أثار هذا القانون العديد من الاشكالات من أبرزها أن الشّركات الأمريكيّة لا تستطيع جمع معلومات عن مواطني الاتحاد الأوربيّ ونقلها إلى الولايات المتّحدة لأنّ الولايات المتّحدة ليس لديها نفس المستوى من القوانين. وهناك مشكلة أخرى تتمثّل في منع رجال الأعمال في أوربا من نقل أجهزة الحاسب الآلي المحمولة (لاب توب) إلى خارج أوربا إذا كانت تحتوي على معلومات عن مواطنين أوربيين، وهو أمر يبدو غير واقعيّ، مما استدعى رجال تطبيق القانون إلى التهاون في تطبيقه (Shaffer, 2000). وبناء عليه فإنّ مواقع التّجارة الإلكترونيّة في السّعوديّة لن يسمح لها بالتّعامل مع مواطنين من الاتحاد الأوربي إذا نتج عن هذا التعامل انتقال بيانات هؤلاء المواطنين إلى السعودية لعدم وجود نفس مستوى التنظيم القانونيّ للخصوصيّة في السّعوديّة، وكذلك الأمر بالنّسبة إلى رجال الأعمال السعوديين الذين يحملون جهاز لاب توب، حيث لا يحقّ لهم نقل بيانات عن مواطنين في الاتحاد الأوربي أثناء مغادرتهم أوربا.

4. تحليل أنظمة التعاملات والجرائم الإلكترونية

من خلال دراسة التّشريعات في مجال التّعاملات الإلكترونيّة والجرائم الإلكترونيّة التي أقرّتها بعض الدّول مثل الولايات المتّحدة الأمريكيّة وهولندا، والنّظام النّموذجيّ للتّجارة الإلكترونيّة الذي تبنّته هيئة الأمم المتّحدة (UNCITR،1996) نجد أنّها تسعى إلى تغطية أكبر قدر من مجالات المخالفات التي يقع فيها المستخدمون لهذه التقنيات، والتي يمكن حصرها في: التّعاملات الإلكترونيّة، الاحتيال الإلكترونيّ، الاعتداء الإلكترونيّ والقرصنة الإلكترونيّة بنوعيها الفاعل وغير الفاعل Active and Passive والنّشر الإلكتروني (الشكل 1).

ولتأثير هذه المخالفات والجرائم مستويان: المستوى الأول هو مستوى التّأثير على الأجهزة والبيانات والمستوى الثاني وهو مستوى التّأثير على المستخدمين والمتعاملين مع تلك الأجهزة والشّبكات. فعلى مستوى الأجهزة والمعدّات والبيانات والمعلومات، يمكننا ضرب الكثير من الأمثلة: فالبيانات النّاتجة عن التّعاملات الإلكترونيّة تشمل كلّ عمليّات البيع والشّراء وتعاملات التّجارة الإلكترونيّة من حيث إعداد الطّلب والموافقة والتّوقيع الإلكترونيّ والتّوريد والتّوظيف وطرق التّسديد والتّعاملات الماليّة وتعاملات الحكومة الإلكترونيّة. كما يدخل فيه أيضاً الاعتداء الإلكترونيّ ويشمل صور تخريب أو تعطيل أجهزة ومعدّات حاسب آليّ أو شبكة الإنترنت أو مسح البيانات من الحاسبات الشخصية أو السيرفرات أو أجهزة الشّبكة. كما أنّ مستوى التّأثير على المستخدمين يشمل جوانب مثل وسائل الاحتيال التي تتمّ بواسطة الأنشطة الإلكترونيّة مثل استخدام البريد الإلكترونيّ للخداع والسّرقة ومثل الحصول على كلمات السرّ وهويّات المستخدمين وتزوير بطاقات الائتمان والحسابات المالية.

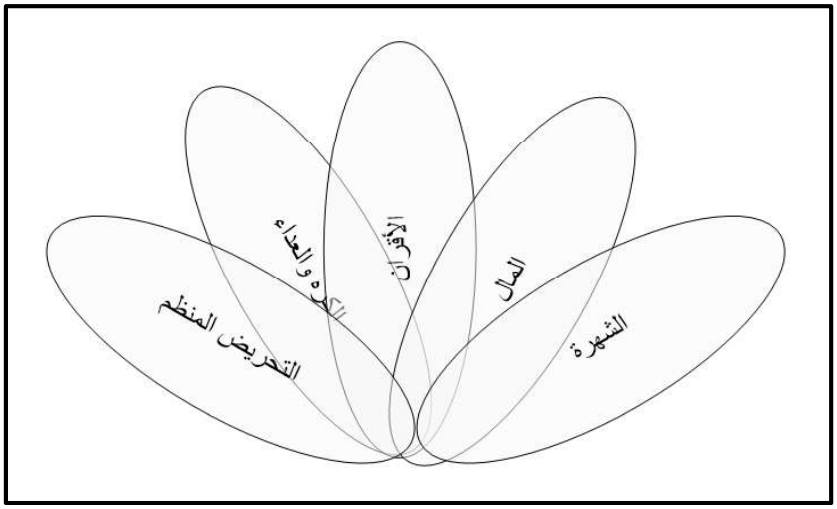
شكل رقم 1: تصنيف مجالات التّشريع الإلكترونيّ

أمّا بالنّسبة إلى نشاط القرصنة Hacking، فهو أيضاً من أنواع الاعتداء ولكن تمّ إفراده بمجال خاصّ لأنه أصبح مصطلحاً يُطلق على أفراد متخصصين ذوي مهارات تقنيّة اعتادوا هذا النشاط الذي يدور في الغالب حول التنصّت أو سرقة المعلومات، كما يمكن ألاّ يكون بهدف التخريب أو التعطيل لكن لأهداف كثيرة أخرى منها على سبيل المثال طلب الشّهرة، أو دوافع نفسية مرضية، أو بسبب الأقران والأصدقاء، أو العداء والكره، أو التحريض الحكومي بواسطة أجهزة الاستخبارات وأحياناً كثيرة بدافع المال. ويشير الشكل رقم 2 إلى أنّ هذه العوامل متداخلة أو قد ينفرد بعضها في التأثير على بعض الأشخاص. وقد حاولت دراسة تحديد تأثير التشريعات على دوافع القراصنة المختلفة (Lesson, 2005) واستنتجت أنّ التشريعات لا تؤثّر كثيراً في القراصنة الذين يحرّكهم طلب الشهرة، لكنّها تؤثّر في حالة ما إذا كان الدّافع ماليّاً وكانت العقوبات أكبر من المكتسبات المالية التي يسعى القرصان إلى تحقيقها.

أما بالنسبة إلى جرائم النشر الإلكتروني، فتدخل فيها كلّ أنواع النشر المخالف لحقوق الإنسان أو لكرامته أو ما يؤدي إلى الإضرار به صحياً أو عقلياً أو عقائدياً، كما يدخل في ذلك نشر الموادّ غير الأخلاقية والصّور والأفلام الإباحية، ونشر ما يثير الكراهيّة والعداء الطائفيّ والعنصريّة، وكذلك نشر المعلومات التي تمسّ الأمن الوطنيّ

والشّائعات الخطيرة على المجتمعات، ونشر معلومات تروّج للمخدّرات أو كيفيّة تعاطيها أو وسائل إعدادها، ونشر ما فيه ضرر بصحة عقل الإنسان وتمنع القوانين تعاطيه، وكذلك المعلومات المساندة للإرهاب وطرق تصنيع المتفجّرات والخطط الأمنيّة العسكريّة ومعلومات المواقع الأمنيّة وما شابهها.

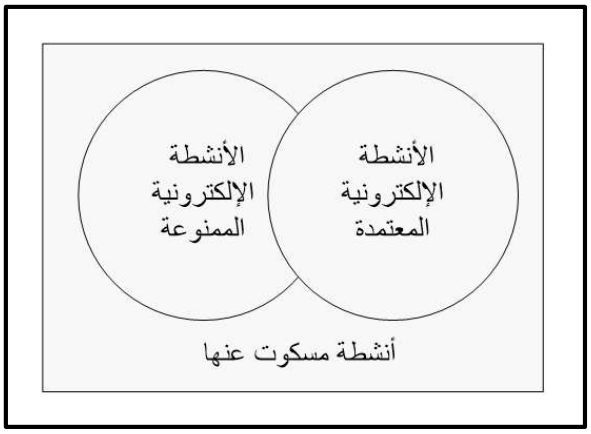
شكل رقم 2: العوامل التي تدفع إلى القرصنة الإلكترونيّة



أمّا بالنّسبة إلى مستوى المستخدمين والمتعاملين الذي ورد في الشكل 1، فيُقصد به استخدام أيّة وسيلة من تلك الوسائل في أيّ مجال من تلك المجالات للتّأثير لا على البيانات والأجهزة فحسب، ولكن على ذات المستخدمين أنفسهم لخداعهم أو التأثير عليهم أو الضّغط عليهم أو إكراههم على شيء ممنوع أو ترك شيء واجب فعله. ويدخل في هذا النوع جميع الحيل التي تؤذي صغار السن وتؤدي على سبيل المثال إلى اختطافهم أو استغلالهم جنسياً أو الاستيلاء على الأموال أو الممتلكات. وهذا النوع من الجرائم في الغالب تحكمه التّشريعات التّقليديّة، لكن أحياناً يحدث إشكال في الاعتراف بالوسائل التّقنيّة كأدلّة إدانة في المحاكم إن لم يكن هناك تقنين واعتماد لتلك الوسائل أو على الأقلّ وعي وعناية بها، ولو على مستوى القرائن أثناء التّحقيقات.

كما أنّ هذه التّشريعات والأنظمة تدور من حيث مضمونها إما على منع أنشطة وتعاملات معينة أو على اعتماد أنشطة وتعاملات معيّنة أخرى والاعتراف بها. وعليه فإن تلك التّشريعات عندما تعلن عن منع مجموعة من الأنشطة فإنّها بذلك تكون قد أتاحت باقي الأنشطة التي لم تصرّح بها، غير أنّ عدم اعتمادها الأنشطة الإلكترونيّة صراحة يترك الباب مفتوحاً للأطراف المتعاملة للاعتراف بها أو عدم الاعتراف بها بموجب عقود بينيّة بين المتعاملين. ويوضح الشكل رقم 3 تصنيف التشريعات من حيث الاعتماد والمنع. فعلى سبيل المثال عندما لا تذكر أنظمة التّعاملات والجرائم الإلكترونيّة مسألة جمع عناوين البريد الإلكترونيّ واستخدامها في إرسال بريد دعائيّ غير مرغوب، فإنّها بذلك تكون قد أجازت هذا النوع من العمل، إلاّ أن يكون هناك تعاقد مباشر وصريح بين صاحب العنوان والشّخص الذي جمع العناوين، يحدّد طبيعة استخدام العنوان. وعندها فقط يتمّ اعتماد بنود هذا العقد بناء على قاعدة العقد شريعة المتعاقدين.

شكل رقم 3: تصنيف التشريعات من حيث الاعتماد والمنع



5. المحور الاقتصادي

أتاحت الوسائل الإلكترونيّة والاتّصالات سهولة فائقة لسرقة الأسرار التّجارية مثل برامج الحاسب المصدريّة وأسرار تركيب المنتجات وأسرار عمليّات التّصنيع التي تعتبر ذات قيمة ماليّة كبيرة للشّركات قد لا يمكن تعويضها بل يمكن أن تؤدي إلى خسارة الشركة بالكامل وإفلاسها بسبب موظف استطاع أن يقوم بنسخ هذه الأسرار من جهاز الشركة في ثوان معدودة وتحميلها على الإنترنت ونقلها في دقائق قليلة إلى أجزاء بعيدة من العالم (Carr,2000). ونذكر هنا على سبيل المثال الحادث الشهير الذي تم فيه سرقة أرقام كروت ائتمان لعدد 300,000 من عملاء شركة CDUniverse.com في العام 2000، وهو ما أدّى إلى تراجع التّعامل مع الشّركة لخوف العملاء من تسرّب أرقام كروت الائتمان التي يستخدمونها إلى القراصنة (Chang, 2004). ومما يؤكد شكوك العملاء وخوفهم ما جاء في دراسة لمؤسسة الأبحاث IDC حيث تبيّن أنّ 60 % من عمليّات الاختراق الإلكترونيّ تركّز على المؤسّسات الماليّة (Kshetri, 2006).

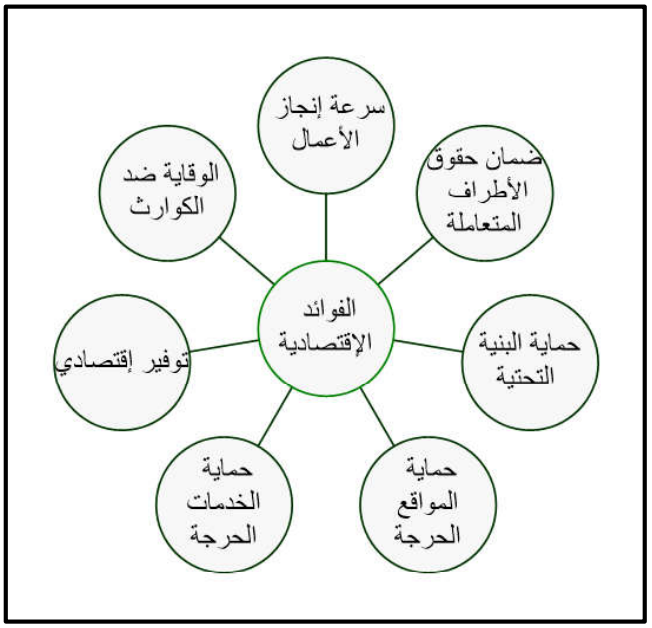
وكمثال آخر، نذكر ما قام به أحد مواطني الفلبين الذي كتب الفيروس الشهير Love letter عام 2000: فقد تكبّد الاقتصاد الأمريكي ما بين 4 و15 بليون دولار خسائر شركات، ومع ذلك لم تستطع الولايات المتحدة ملاحقة ذلك الشخص لعدم وجود قوانين في الفلبين لتجريم كتابة الفيروسات (Chang, 2004, Lesson, 2005).

وبناء على هذه المعطيات فإن نظامي التعاملات والجرائم الإلكترونيّة يحقّقان مجموعة من الفوائد الاقتصاديّة يمكن تلخيصها في الشّكل رقم 4. ومن أبرز هذه الفوائد سرعة إنجاز المعاملات بحكم طبيعة التّعامل الإلكترونيّ وبحكم كونه معتمداً ومعترفاً به في الواقع، وتوفير كميّة الورق المستخدمة في المعاملات وتكاليف نقل تلك المعاملات من جهة إلى أخرى، وضمان حقوق الأطراف المتعاملة عند استخدام الشهادات الإلكترونيّة ونظام الشهادات الإلكترونيّة العامة. كما أنّ اعتماد الشّهادات الإلكترونيّة يحمي أيضاً الخدمات والمواقع الحرجة بحيث لا يسمح بدخول هذه الخدمات والمواقع إلا للمستخدمين المصرح لهم بذلك.

وبالنّظر إلى واقع التّطوّر التّقنيّ السّريع في المملكة، نجد أنّ عدداً متزايداً من الخدمات الحرجة يتمّ تقديمها إلكترونياً عبر الإنترنت منذ صدور الأمر السامي الكريم رقم 7/ب/33181 بتاريخ 1424/7/10هـ، والمتضمن وضع

خطّة التّحوّل إلى الخدمات الإلكترونيّة وإنشاء برنامج "يسر" الذي يقوم بدور الممكّن والمحفّز والمنسّق لتطبيق التّعاملات الإلكترونيّة الحكوميّة.

شكل رقم 4: الفوائد الاقتصادية



ولتقريب تصوّر التّوفير الذي يتحقّق نتيجة تطبيق نظام التعاملات الإلكترونيّة، لنفترض أنّ كلّ ساكن في المملكة يحتاج على الأقلّ إلى ثلاث معاملات في السّنة يتمّ تنفيذها إلكترونياً مثل تجديد رخصة سير أو شهادة ميلاد أو تجديد إقامة وما شابهها. وحيث أنّ تعداد سكّان المملكة بحسب الإحصاء الأخير لعام 2013 يبلغ تقريباً 30 مليون نسمة، وبحذف 50 % من هذا العدد على أساس أنهم صغار السن، يبقى 15 مليون نسمة. وعلى فرض أن كلّ فرد من هؤلاء سينفذ معاملة واحدة في السنة فيصبح عدد المعاملات 15 مليون معاملة. وعلى فرض أنّ كل معاملة بحاجة إلى ثلاث عمليات وكل عملية تستغرق خمس دقائق شاملاً وقت مراجعة بيانات المعاملة فإنّ الوقت اللازم لكل هذه التوقيعات سوف يبلغ 75 مليون دقيقة أي ما يعادل 1. 25 مليون ساعة عمل وبالقسمة على 8 ساعات دوام يوم العمل الرّسميّ، يصبح الناتج 156,250 يوم عمل. ناهيك عن الوقت المستهلك لنقل هذه المعاملات واستهلاك الورق. فالتوفير الاقتصادي هائل بكل المقاييس، وما كان هذا ليتحقّق لولا الضّمانات التي توفّرها التّشريعات النّظاميّة التي اعتمدتها الحكومة.

ومن الآثار الإيجابيّة الكبيرة لهذه الأنظمة تعزيز الثّقة في بيئة التّعاملات الإلكترونيّة وبالتّالي تنشيط الحركة الاقتصاديّة وزيادة تسهيل تعاملات الأفراد في المجتمع. ويدلّ على ذلك التّطور الحاصل في المجال البنكيّ والماليّ ومنها انتشار أجهزة الصّراف الإلكترونيّ وتزايد الخدمات البنكيّة عبر الإنترنت مثل خدمات التّحويل وتسديد الفواتير ومتابعة كشوف الحسابات ومؤخراً نظام سداد الإلكتروني الذي يتيح للأفراد تسديد المشتريات بطريقة إلكترونيّة عبر الإنترنت ومكائن الصّراف ونقاط البيع الإلكترونيّة. ويعتبر نظام تداول لبيع وشراء الأسهم من أبرز الخدمات الماليّة في السّعودية من حيث عدد المستخدمين وحجم المبالغ التي تدور فيه يومياً بواسطة الأفراد والتي تصل إلى عشرات المليارات من الريالات. لكن قد يقال إنّ ما دفع النّاس لاستخدام تداول هو الطّفرة التي

حصلت في الأرباح لكنّ الواقع يدلّ على أنّ الأمر مستمرّ وأنّ فعاليّة النّظام الإلكترونيّ والثّقة فيه تزداد بمرور الوقت، وأنّ التعاملات في نموّ وإن كانت عودة عامة الناس بطيئة بسبب النكسة التي عرفتها سوق الأسهم.

6. المحور الاجتماعي والأخلاقي

إنّ وجود الأنظمة القانونيّة لدعم بيئة التّعاملات الإلكترونيّة ضرورة على المستوى الاجتماعيّ والأخلاقيّ إذ لها عدّة وجوه من أهمّها خلق الشّعور بالذنب خصوصاً أن قراصنة الإنترنت يغيب عنهم في الغالب الشعور بأنّ ما يقومون به غير أخلاقي وغير قانوني (Lesson, 2005). ومن أبرز دواعي وجود هذه الأنظمة حماية حقوق الإنسان وكرامته وحماية صغار السّنّ وحماية العقيدة وصيانة الأبدان والعقول وحماية الأعراض. وعليه فقد جاء في نظام الجرائم الإلكترونيّة مجموعة من الفقرات لتحقيق الحماية الاجتماعيّة والأخلاقيّة، منها الفقرة الخامسة في المادّة الثالثة والتي تنصّ على تجريم التشهير وإلحاق الضرر بالآخرين عبر الوسائل التّقنيّة، ثم جاءت في المادّة السادسة أربعة بنود تهدف إلى منع إنشاء مواقع الاتّجار في الجنس البشريّ أو تسهيله، ومنع نشر الموادّ الإباحيّة أو نشر أنشطة القمار والميسر أو ترويجها، وكذلك منع الاتّجار في المخدرات والمؤثّرات العقليّة أو ترويجها أو نشر طرق تعاطيها وتسهيل التّعامل معها. وكذلك الفقرة الثّالثة من المادّة الثامنة التي تنصّ على تجريم التغرير بالقصّر ومن في حكمهم واستغلالهم.

وقد أحسنت صنعاً مدينة الملك عبدالعزيز للعلوم والتقنية على مدى السّنوات الماضية بحجبها لمواقع الإنترنت الضّارّة بالمجتمع مثل المواقع الإباحيّة ومواقع العقاقير الممنوعة ومواقع الميسر، وانتقلت مؤخراً مسؤوليات حجب المواقع إلى هيئة الاتصالات وهي مستمرة على نفس المستوى.

وممّا يزيد من أهمّيّة هذه التّشريعات انتشار تقنيات التصوير الحديثة المحمولة مثل كاميرات الهاتف الجوّال. هذه الكاميرات تجعل التّصوير الرّقميّ وتحميل الصّور على الإنترنت في غاية السّهولة ولا يمكن إيقاف انتشار الصّور بعد ذلك إلاّ من خلال قوانين رادعة وتطبيق حازم يؤثّر في النّفوس الضّعيفة وبالتّالي يخفّف من مخاطرها على المجتمع. وتظهر أبرز آثار التّشريعات بعد المحافظة على صحّة الأبدان والعقول في المحافظة على الخصوصيّة. والخصوصيّة تدخل في جانب حفظ الأعراض في المصطلح الشّرعي الإسلاميّ. وحماية الخصوصيّة حقّ من حقوق الإنسان تسعى الدّول المتقدّمة إلى حمايته من خلال التّشريعات التي تطوّرت على مدى سنوات طويلة قبل انتشار الإنترنت، لكن ازدادت أهمّيتها مع ازدهار الفضاء الإلكترونيّ.

وخلاصة ما تدور حوله التشريعات في العالم ما يلي:

1- قانونية قنوات الحصول وتجميع المعلومات،
2- استخدام البيانات للأغراض التي جمعت لها وعدم تجاوز ذلك،
3- تحديث البيانات والمحافظة على صحتها،
4- توفير حقّ وصول الأفراد للبيانات المتعلقة بهم،
5- المحافظة على سرّيّة البيانات،
6- إتلاف البيانات والتخلّص منها بعد انتهاء الغرض من استخدامها.

ومن أبرز الاتّفاقيّات في هذا المجال وأحدثها الاتفاقيّة التي صوت عليها برلمان الاتّحاد الأوربّيّ لحماية البيانات الشّخصيّة في الفضاء الالكترونيّ. وقد تأثّرت بها العديد من مشاريع القوانين الوطنيّة خارج إطار الدّول الموقّعة عليها (EU, 2014, Levin, 2005 , Younos, 2002). وفي هذا الصّدد فقد غطّى نظام الحكومة السّعوديّة للجرائم الإلكترونيّة جانبا من متطلّبات حماية الخصوصيّة من خلال البنود المتعلّقة بمنع التّنصّت والتّجسّس وسرقة البيانات أو إساءة استخدامها بواسطة الاحتيال وسرقة الهويّة. لكنّ النّظام لم يتناول جوانب جمع البيانات أو تجاوز استخدامها في الأغراض التي لم تجمع لها، كما أنّه لا يوفّر حقّ الوصول إليها والمحافظة على تحديثها والمحافظة على سريتها وإتلافها بعد انتهاء الغرض منها. وجميع هذه الجوانب مهمة، والحاجة إلى تشريعات تحدّد الممنوع والمعتمد منها ضرورة تحتاجها المجتمعات الحديثة. وللدلالة على أهمّيّة هذا الموضوع نذكر الانتشار الواسع لعمليّات تجميع معلومات الأفراد في قواعد بيانات تسمى بنوك المعلومات لأغراض مختلفة واستخدامات ضارة بالمجتمعات، مما جعل المجتمع الدولي يسعى جاهداً لإيجاد مبادئ وقواعد من شأنها مراعاة حماية الحق في الحياة الخاصة والبحث عن توازن بين حاجات المجتمع وكفالة حماية البيانات الخاصة من الاستخدام غير المشروع. ومن أكثر معالم خطورة هذه البنوك مشكلة البيانات الخاطئة أو الناقصة عن الإفراد، فعلى سبيل المثال قام الدكتور لوردن هو عالم في مجال الجريمة بفحص قواعد بيانات وكالة التحقيقات الفيدرالية FBI وإدارة الشرطة بمدينة نيويورك واكتشف أنّ نسبة عالية من البيانات غير صحيحة وغير مكتملة أو أنّها متعلّقة بجنح بسيطة قديمة لكن مع ذلك تسبّبت في فقدان الكثير من المواطنين فرصا وظيفيّة كان يمكنهم الحصول عليها لولا اطّلاع أصحاب الأعمال على تلك السّجلات وبالتّالي تكوينهم فكرة خاطئة عن المتقدّمين ثم رفضهم بناء على ذلك (Younos, 2002).

7. المحور التقني

إحدى الجوانب السّلبيّة للتّشريعات في المجال الإلكترونيّ أنّها أحيانا تتسبّب في نوع من الأمان الزائف للشّركات والأفراد فيحدث تفريط في اتخاذ الإجراءات الوقائيّة الضروريّة اعتماداً على وجود التّشريعات. لهذا يجب أن يرافق هذه التّشريعات نشاط إعلاميّ تثقيفيّ وتدريبيّ لتجنّب مثل هذه السلوكيّات. فعلى سبيل المثال كلّ شركة وكلّ منزل يستخدم الإنترنت بحاجة إلى نظام جدران الحماية Firewall، وهو نظام يتمّ تشغيله على نقاط الاتّصال بالإنترنت لحماية الشّبكة الدّاخليّة من الدّخلاء، وكذلك لمنع المستخدمين في الشبكة الداخلية للشركة أو المنزل من الوصول إلى المواقع غير المرغوب فيها. ومثل هذا النّظام ضرورة وقائيّة لكلّ من يتّصل بالإنترنت حتّى وإن كانت هناك تشريعات تمنع دخول القراصنة على شبكات الآخرين. فمن غير المنطقي أن يترك الإنسان باب بيته مفتوحاً ثم يتوقع أن تحميه القوانين من الدخول غير المشروع.

ومن جهة أخرى فإنه من الواضح أنّ نظامي التّعاملات والجرائم الإلكترونيّة لن يكون لهما تأثير في جانب صناعة التّقنية لأنّنا جزء من العالم المستهلك لهذه التقنيات ولسنا جزءًا من العالم المصنّع لها. لكنّ هذه الأنظمة ستكون مؤثّرة في جانبين آخرين وهما جانب استخدام تقنيات أمن التعاملات إلكترونيّة المتقدمة مثل التشفير والتوقيع الإلكتروني، وجانب التحقيقات الإلكترونيّة. والتأثير في الجانب الأول أقوى، وهو متوقّع بشكل مؤكّد

لأنّ فيه مصالح اقتصاديّة على مستوى القطاع الحكوميّ والخاص سبقت الإشارة إليها في المحور الاقتصاديّ. أمّا بالنّسبة إلى الجانب الثّاني، وهو جانب التّحقيقات في الجرائم الإلكترونيّة، فهو مسؤولية الأجهزة الأمنية. والمؤمل أن تكون هذه الأجهزة على مستوى التوقّعات لأنّ آثار هذه التّشريعات لن تظهر إلاّ من خلال تطبيقها، والتّطبيق بحاجة إلى موارد وخبرات ينبغي أن تكون متوفّرة لدى الجهات الأمنية حتى تتمكن من القيام بدورها على الوجه الصّحيح.

ومن الآثار الواضحة لنظام التّعاملات الإلكترونيّة في جانب استخدام التقنيات، تطوّر استخدام مجموعة من التّطبيقات الحديثة منها تقنيات حفظ ومعالجة السّجلات، وتقنيات تبادل السّجلاّت، وتقنيات التّعاقد الإلكترونيّ، وتقنيات التّوقيع والشّهادات الإلكترونيّة. فبالنّسبة إلى حفظ السّجلات وطريقة تبادلها، يشير نظام التّعاملات الإلكترونيّة في الفقرات الثلاثة للمادّة السّادسة إلى ضرورة حفظ السّجلات بالشّكل الذي أنشئت أو أرسلت به بحيث يمكن إثبات مطابقة المحتوى المرسل مع المحتوى المستلم، وكذلك الاحتفاظ بالسجل على نحو يتيح الرجوع إليه لاحقاً مع حفظ المعلومات المتعلقة بالسجل والتي تمكن من معرفة المنشئ والمرسل والمستلم وتاريخ ووقت الإرسال والاستلام. وهذه العمليات تحتاج إلى عناية وخبرات متقدمة ليست متوفرة بسهولة بحسب ما نراه من حولنا في الواقع في الوقت الراهن لدى العديد من الجهات الحكوميّة والخاصّة، وسوف تتطور وتتحقق مع الوقت بفضل مراعاة تطبيق هذه الأنظمة الجديدة.

ومن الآثار التّقنيّة تطوّر تقنيات التّوقيع الرّقميّ بعد أن ساوى النّظام بين التّوقيع الخّطيّ والتّوقيع الرّقميّ. ومن أبرز الإنجازات في هذه الأنظمة أيضاً إقرار لائحة المركز الوطني للتّصديق الإلكترونيّ ولائحة واجبات مقدّم خدمات التّصديق الإلكترونيّ ومسؤوليّاته ومسؤوليّات صاحب الشّهادة الرّقميّة. وبهذا تمّ توفير الأرضيّة والقاعدة التّشريعيّة لبناء ما يُطلَق عليه مصطلح البنية التّحتيّة للمفاتيح العمومية PKI، وهي عبارة عن مجموعة من الآليات والسّياسات التي توفّر بيئة متكاملة لاستخدام التّوقيعات الإلكترونيّة ابتداء من مصادر الحصول على الشّهادة الإلكترونيّة التي تحتوي على مفتاح التّشفير العامّ للمستخدم والتّصديق عليها من قبل مزوّدي خدمة الشّهادات، واعتماد الشّهادات الصّادرة من الدّول الأخرى، ثمّ استخدام المفتاح الخاصّ في التّوقيع ومسؤولية صاحب التّوقيع على التّوقيع الصّادر منه، وأحكام فقدان المفتاح الخاصّ وصلاحيّة الشّهادة والتّحقّق من صحّتها، والأحكام المتعلّقة بمخالفات استخدامها.

8. النتائج والتوصيات

إنّ هذه الدّراسة والدّراسات المشابهة لها وتجارب الدّول المتقدّمة تؤكّد أنّ المملكة خطت خطوة مهمّة في الاتّجاه الصّحيح، وأنّ هذه الخطوة بحاجة إلى دعم محلّيّ بتوفير باقي متطلّبات النّجاح من دعم تدريبيّ وفنّيّ وتقنيّ للأطراف المعنيّة بهذا النّظام حتّى يحقّق الأهداف المرجوّة منه. وفيما يلي مجموعة من التّوصيات التي تمّ التوصّل إليها لتوفير بيئة النّجاح المطلوبة لهذه الأنظمة:

- ابرام اتّفاقات دوليّة، على غرار الاتّفاقات الأمنيّة التّقليديّة التي تُعقد بين المملكة والدّول الأخرى، تحدّد ضوابط للنشاطات الإلكترونيّة وتمكّن من ملاحقة الجرائم الصادرة من خارج المملكة والعكس،
- إلزام الشركات بالإفصاح عن الحوادث الإلكترونيّة إلى الجهات المختصة،
- وضع ضوابط تحدّد كيفيّة حفظ الأدلّة الإلكترونيّة بوساطة الشّركات والمتخصّصين في تقنية المعلومات بحيث لا تفقد مع التّشغيل اليوميّ للأنظمة الإلكترونيّة،
- دعم توفير وتدريب كوادر في الجهات الأمنيّة ذات العلاقة متخصّصة في وملاحقة الجرائم الإلكترونيّة وتوفير ما تحتاج إليه من أجهزة ومعدّات متقدّمة،
- وضع تنظيم وآلية لمتابعة أساليب مزودي خدمة الإنترنت في حفظ ملفّات المراجعة لحركة مرور البيانات والتعاملات عبر أجهزة التوجيه والتمرير المركزية (Log files)،
- تنفيذ دورات وورش عمل حول طرق تطوير أدوات وبرامج أمن المعلومات وطرق عمل التّحقيقات في الجرائم الإلكترونيّة،
- وضع تنظيم خاص بحفظ خصوصيّة المستخدمين للإنترنت لحمايتهم من استغلال الشّركات وغيرها لبياناتهم دون إذن منهم،
- تشجيع الدّراسات والأبحاث المتعلقة بحفظ الأمن الإلكترونيّ وتطوير الأنظمة التّشريعيّة لها،
- تشجيع جمعيّات حماية المستهلكين الإلكترونيّة لعمل برامج تثقيفيّة حول أفضل أساليب العمل والاستخدام التي تحميهم من الجرائم والاحتيال الإلكترونيّ،
- إدراج مبادئ الوقاية الإلكترونيّة ضمن مناهج التّعليم العامّة لزيادة وعي صغار السّن بمخاطر البيئة الإلكترونيّة.

خاتمة

إنّ أبرز آثار نظامي التّعاملات والجرائم الإلكتروني في السعودية هو توفير الثّقة في البيئة الإلكترونيّة. فالتّعامل الإلكترونيّ عبر الإنترنت يقوم على فرضيّتان الأولى أنّ المعاملات تتمّ بين المتعاملين عن بعد بإلغاء عوامل المكان والزمان، والفرضيّة الثّانية أنّ الثّقة مفقودة بين الأطراف لأنّ الوسائل الإلكترونيّة المجرّدة لا تستطيع توفير الثّقة لعدة عوامل منها أنّ العامل النّفسيّ والعاطفيّ الذي يتولّد عند التّعامل وجهاً لوجه

مفقود في البيئة الإلكترونيّة، وكذلك لسهولة سرقة الهويّة وانتحال الشّخصيّة في البيئة الإلكترونيّة. بناء على ذلك فإنّ النّظم والتّشريعات تصبح ضرورة لتوفير الثّقة التي يحتاج إليها المتعاملون، ولا يوجد بديل واقعيّ يمكن الاعتماد عليه سوى الدّعم التّشريعيّ والقانونيّ. أمّا الآثار الأخرى التي يمكن أن تتحقّق بتطبيق هذه الأنظمة فهي عديدة وتشمل الجوانب التي سعت هذه الدّراسة إلى إلقاء الضّوء عليها، سواء كانت اقتصاديّة أو اجتماعيّة أو أخلاقيّة أو تقنيّة. وفي الختام نؤكّد أنّ هدف هذه الدّراسة لم يكن استقصاء جميع الآثار، ولكن سعينا إلى إبراز أهمّ تلك الآثار في الوقت والإمكانات المتاحة، بهدف المساهمة في إنضاج هذه التجربة حتى تحقّق أكبر قدر ممكن من أهدافها ومنافعها. وفي مقابل إيجابيّات التّشريعات التي أشرنا إليها في هذه الدّراسة، فإنّنا لا ندعو إلى التّوسع في التّشريعات للبيئة الإلكترونيّة، ذلك أنّ كثيراً من الخبراء في الدّول المتقدّمة يحذّرون من سلبيّة الإفراط في فرض التّشريعات لأنّها قد تتسبّب في إعاقة تطوّر التّعاملات الإلكترونيّة.

قائمة المصادر والمراجع:

- Carr, A. , Morton, J. and Funiss, J. 2000. *The Economic Espionage Act: Bear Trap or Mousetrap?* Texas Intellectual Property Law Journal, 8: 159-209.
- Chang, J. 2004. *Computer Hacking: Making the Case for a National Reporting Requirement*. Berkman Center for Internet & Society at Harvard Law School Research Publication. Retrieved from http://cyber. law. harvard. edu/publications. Retrieval date: August 11, 2014.
- CovenantEyes. 2014. *Pornography Statistics 2013*. Retrieved from www. covenanteyes. com. Retrieval date: August 2, 2014.
- CyberSource Corporation. 2013. *Online Fraud Report, Online Payment Fraud Trends,*
- *Merchant Practices and Benchmarks 14th Annual Edition*. Retrieved from www. cybersource. Retrieval date: August 2, 2014.
- EU commission. 2014, *Progress on EU data protection reform now irreversible following*
- *European Parliament vote*, European Commission - MEMO/14/186. Retrieval date: August 2, 2014.
- FBI. 2013. *Kaspersky Security Bulletin 2013 Overall statistics for 2013. IC3 2013 Internet Crime Report*. Retrieved from http://report. kaspersky. com/. Retrieval date: August 16, 2014.
- Kshetri, N. 2006. *The simple economics of cybercrimes*, IEEE Security & Privacy Magazine. V. 4, 1: 33-39.
- Lesson, P. T. , 2005. *The economics of Computer Hacking, Journal of Law, Economics and Policy*. Retrieved from http://papers. ssrn. com/sol3/papers. cfm?abstract_id=868335. Retrieval date: August 11, 2014.
- Levin, Avner and Nicholson, Mary Jo. 2005. *Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground*. University of Ottawa Law & Technology Journal. V. 2, 2: 357-395.
- Ponemon Institute. 2013. *Cost of Data Breach Study: Global Analysis, Research Report*. Retrieved from http://www. ponemon. org/library/2013-cost-of-data-breach-global-analysis. Retrieval date: August 11, 2014.
- Shaffer, Gregory C. 2000. *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting up of U. S. Data Privacy Standards*. Yale Journal of International Law. 25: 1-88
- UNCITRAL. 1996. *Model Law on Electronic Commerce*. Retrieved from http://www. uncitral. org. Retrieval date: August 11, 2014.
- Younos, A. 2002. *Privacy and Protecting Data in the Electronic Age*. Arabic e-book.