

القانون والتطور التكنولوجي الحديث

The Law and Modern Technological Development

مصطفى عمراني*

أستاذ متعاقد- جامعة التكوين المتواصل- مركز بشار-
الجزائر

تاريخ الإرسال: اليوم / الشهر / السنة -- تاريخ المراجعة: اليوم / الشهر / السنة -- تاريخ القبول: اليوم / الشهر / السنة

الملخص:

تعالج هذه الورقة البحثية إشكالية عجز القواعد القانونية السارية في استيعاب وتنظيم المراكز القانونية التي تنتج عن التطور السريع للتكنولوجيا المعلوماتية. لاسيما البطاقات البنكية وإنترنت الأشياء، باعتبار سرعة نمو وانتشار هذه الأخيرة، وارتباطها بقطاعات حساسة كمحطات توليد الطاقة ومرافق مختلفة. بالإضافة إلى مخاطر استخدام هذه التكنولوجيا الحديثة من طرف عصابات إجرامية، واستثمارها لصالحهم وارتباطها ببعض الجرائم الخطيرة والحديثة. مما دفع بالدول المتقدمة وعلى وجه السرعة التعامل معها والتأطير القانوني لها سواء في المجال الإقتصادي أو التكنولوجي، أو التشريعي، أو حتى في مجال العلوم الجنائية...إلخ.

الكلمات المفتاحية: الجريمة السيبرانية، إنترنت الأشياء، البطاقة البنكية، التكنولوجيا الحديثة.

Abstract:

This article addresses the problem of the inability of the applicable legal rules to absorb and regulate legal centers resulting from the rapid development of information technologies, in particular bank cards and the Internet of things, given the speed of growth and spread of the latter and its connection to sensitive sectors such as power plants and various facilities, in addition to the risks associated with the use of this modern technology by criminal gangs and their investment in their profit and association to certain serious and modern crimes, which incites the developed

*مصطفى عمراني

countries to face them and the legal frameworks at their disposal, whether in the economic, technological or legislative fields, even in the field of criminal sciences ... etc.

Keywords: Cybercriminality; Internet of Things; Bank card; Modern Technology.

مقدمة:

لم يكن يتوقع أحد منا في الزمن القريب أن يصل العلم إلى هذا الحد من التطور المذهل، حتى أصبح لكل منا عالمان عالم واقعي وآخر افتراضي مبني على تقنيات الاتصال والمعلومات، وهذا بفضل انتشار الأجهزة الذكية وشبكات التواصل الاجتماعي، حتى أصبحنا نتساءل عن مستقبل عالمنا الافتراضي أكثر من العالم الواقعي. فيجبنا العلم حول تساؤلنا إنها "إنترنت الأشياء، البطاقات البنكية، البيوت الذكية..."

ولا كن هي أيضا فناء عالمنا الواقعي، وتبخر عالمنا الافتراضي، وهي مصدر قلق المستخدم، وكل الدلائل تشير أن الوضع لن يزداد إلا سوءاً. إذ يرتفع عدد الأجهزة غير المراقبة التي تدخل إلى الشبكات كل يوم بشكل كبير، وعندها لن تنجح الحلول الأمنية التقليدية في التعامل مع هذا العدد الهائل من الأجهزة، أو حمايتها من الاختراق وهو ما ينذر بخطر كبير، إذ ارتفع عدد الهجمات على الأجهزة التي تستخدم إنترنت الأشياء بنسبة 280% في النصف الأول من عام 2017. (Hope, 2017)

ولهذه الأسباب، تعمل الدول المتقدمة جاهدة في الاستثمار في الجانب الإيجابي لإنترنت الأشياء والبطاقات البنكية بهدف خلق فرصاً جديدة، وقيمة أكبر، وتأثيراً أوسع للحياة اليومية، وللأعمال التجارية، والتطرق لموضوع الأمن والخصوصية في مجال تكنولوجيا الإعلام، وتنمية الأمن السيبراني فيما يتعلق بإنترنت الأشياء، وأثر أحدث التطورات في مجال معايير حماية البيانات الشخصية، والخصوصية على المستوى الأوروبي وفي مناطق أخرى. هذا ما خلص إليه مؤتمر أسبوع إنترنت الأشياء لعام 2017 والذي أقيم في جنيف، سويسرا، 6-9 يونيو 2017، والذي توصل لعدة نقاط نذكر منها كما وردة في المؤتمر:

1. سيكون هناك قريباً المزيد من أجهزة إنترنت الأشياء في العالم أكثر من الناس، وتكثر المخاطر الأمنية
2. لحظة الحقيقة في إنترنت الأشياء – من يستطيع تأمين تدفق البيانات؟
3. لا يمكن ترك معايير إنترنت الأشياء للسوق.

ومن خلال ما سبق، يمثل هذا البحث غاية في الأهمية من حيث دراسة العلاقة بين القانون والتطور التكنولوجي لاسيما في مجال النظام المعلوماتي والاتصال. ولتوضيح هذه العلاقة وإلقاء نظرة في مستقبل ما سوف تؤول إليه التكنولوجيا الحديثة ارتأينا تسليط الضوء على دراسة البطاقات البنكية وإنترنت الأشياء للبحث في مدى مواكبة القواعد القانونية المعمول بها مقارنة بالتطور السريع للتكنولوجيا الحديثة.

وعليه، نصوغ إشكالية بحثنا حول مدى مساهمة التشريعات القانونية للتطور التكنولوجي السريع وظبط آثاره؟ لننطلق من خلالها للبحث عن هذه المشروعية على مستوى التشريعات المقارنة والتشريع الجزائري، ونعتمد في ذلك على المنهج المقارن الأنسب لمثل هذه الدراسات، بالإضافة إلى المنهج التحليلي الأقرب لاستخلاص النتائج وطرح التساؤلات.

وعلى هذا الأساس سيتم تغطية هذه الدراسة من خلال المحاور التالية:

المحور الأول: مظاهر التطور التكنولوجي السريع

المحور الثاني: تحديات القاعدة القانونية لاستيعاب ومسايرة التطور التكنولوجي

المحور الأول: مظاهر التطور التكنولوجي السريع

نتطرق في هذا المحور من الدراسة إلى إبراز التطور التكنولوجي المذهل لاسيما في مجال المعلوماتية، ولإبراز هذا الجانب من الدراسة نتطرق أولا إلى سرد الأسباب والدوافع وراء هذا التطور. بالإضافة للتطرق لمخاطر التطور التكنولوجي للنظام المعلوماتي من خلال حصر مجال الدراسة في كل من الثورة المعلوماتية لكل من البطاقات البنكية وإنترنت الأشياء.

أولا: الدوافع والأسباب

أ: بالنسبة للبطاقات البنكية

1. نبذة تاريخية

ظهرت أول شركة متخصصة في إصدار البطاقات البنكية في سنة 1949 م، وهي شركة داينرز كلوب Diners Club وقد اقتصر في البداية على إصدار بطاقة خاصة برواد المطاعم، ثم ظهرت أمريكان اكسبرس Express American و كارتبلانش Carte . Blanch وفي سنة 1951 انتقلت عملية إصدار البطاقات إلى البنوك حيث بدأ بنك فرانكلين في نيويورك Bank National Franklin بإصدار البطاقة، وفي نحو سنتين زاد عدد البنوك المصدرة للبطاقات في الولايات المتحدة عن 100 بنك، وكانت القفزة الكبرى في عالم بطاقات الائتمان عندما سمح بنك أمريكان Bank American للمصارف الأخرى ورخص لها بإصدار البطاقة الائتمانية مما جعل هذه البطاقة تتحرر من إقليميها لتنتشر عبر العالم وصار أكثرها انتشارا بطاقة Visa وبطاقة Card Master. وفي عام 1970 ظهرت فكرة بطاقة الائتمان بمفهومها الربوي، إذ تؤدي هذه البطاقة قرضا بفائدة ثابتة على رصيد البطاقة، وانتشرت هذه البطاقة حتى تسابق الناس للحصول عليها وتضخمت أرباح الشركات المصدرة لها (إبراهيم، أسامة، 2011)

2. التطور التكنولوجي للبطاقات البنكية

تعتبر البطاقة الذكية آخر ما توصلت له حاليا التكنولوجيا، فهي تعمل كجهاز تحكم حيث أنها تجعل المعلومات العملية والشخصية متاحة فقط لمستخدمين محددين. خدمة أخرى تقدمها البطاقة الذكية وهي تمكين الأشخاص من الشراء، وكذلك توفر البطاقة الذكية إمكانية نقل المعلومات الآمنة (محمد، علوان، جليل، 2013). البطاقة الذكية مشابهة للبطاقة البلاستيكية الممغنطة المعروفة ولكنها أكثر قوة وأمان. بالإضافة إلى الميزة العلمية المضافة لها، بحيث تمكن شريحتها التواصل مع القارئ بواسطة تلامس محسوس أو بواسطة موجات الراديو بالاعتماد على التصميم المستقبلي للنظام (عبد الجبار، 2008).

3. الآفاق المستقبلية للبطاقات البنكية

إن التقنيات والوسائل الحديثة المستخدمة في المجال المصرفي والأنشطة الاقتصادية، والمالية قد تطورت بشكل عام وكان من نتيجة ذلك تراجع التعامل بالنقود السائلة بصورة ملحوظة، وإحلال نظم استخدام البطاقات الائتمانية بأشكالها وأنواعها المختلفة بدلا منها، حتى أن هذه البطاقات أصبحت تقوم بدور أساسي في تعامل الناس مع البنوك والمؤسسات المالية، واتسع نطاق التعامل بها ليشمل المؤسسات العامة والخاصة والمجالات التجارية وأنشطة الخدمات (مصطفى، 2017).

وربما في المستقبل القريب تحل بطاقات الائتمان محل النقود، وهو تطور اقتصادي واجتماعي ملموس، واتجاه سريع نحو هذه الغاية. أما على المستوى الاقتصادي فهي تساعد على إدخال النقود المتداولة في السوق الموازية، إلى دائرة السوق المصرفية. وبالتالي المساهمة في التخفيف من حدة الاقتصاد غير الرسمي، والسوق الموازية وبالأخص في ظل توفير بيئة مناسبة لذلك.

ب: بالنسبة لإنترنت الأشياء

1. نبذة تاريخية

أول من استخدم لفظ إنترنت الأشياء هو العالم كيفن أشتون في عام 1999، ويُعد "أشتون" من الروّاد في مجال التقنية، فهو مؤسس أول مركز بحثي في معهد "ماسا تشوستس" للتقنية، وهو متخصص في مجال المعايرة الآلية والترددات اللاسلكية المتصلة بالشبكة. وما ساعد على انتشار فكرة إنترنت الأشياء هو تقنيات الاتصال الحديثة مثل شبكات تحديد الهوية بموجات الراديو، وشبكات الاتصالات في المجال القريب، حيث بات دمجها بكل شيء وتوصيلها مع الإنترنت أمراً عملياً ومتاحاً. فتخيل أن يطلب البراد من المتجر ما ينقصه من أصناف عن طريق البريد الإلكتروني أو ينبه صاحب المحل إن كان أحد محتوياته قد انتهت صلاحيته، أو أن تكون هناك سيارات تخاطب نفسها لاسلكياً أو أجهزة ذكية نرتديها وتخبّرنا كثيراً عن حياتنا وصحة أجسامنا، كلها أمثلة عمّا قد توفره هذه التقنية لنا في المستقبل القريب (رائد، 2015).

وتشير توقعات المتخصصين في صناعة الأجهزة الجوّالة، إلى أن معدلات الأجهزة المتصلة بالإنترنت زادت من 500 مليون جهاز في عام 2003 إلى 12.5 مليار جهاز في عام 2010، وإلى أكثر من 25 ملياراً سنة 2015 وأن تتضاعف بحلول عام 2020 إلى 50 مليار جهاز، أي إن معدل نموها يفوق النمو المحتمل لعدد سكان العالم بأكثر من سبعة أضعاف.

2. تعريف إنترنت الأشياء

بالإنجليزية Internet of Things-IoT، مصطلح برز حديثاً، يُقصد به الجيل الجديد من الإنترنت (الشبكة) الذي يتيح التفاهم بين الأجهزة المترابطة مع بعضها عبر بروتوكول الإنترنت. وتشمل هذه الأجهزة أدوات الذكاء الاصطناعي والمستشعرات والحساسات والمختلفة وغيرها. ويتخطى هذا التعريف المفهوم التقليدي

وهو تواصل الأشخاص مع الحواسيب والهواتف الذكية عبر شبكة عالمية واحدة ومن خلال بروتوكول الإنترنت التقليدي المعروف (شبكة نواف، 2018).

وما يميز إنترنت الأشياء أنها تتيح للإنسان التحرر من المكان، أي أن الشخص يستطيع التحكم في الأدوات من دون الحاجة إلى التواجد في مكان محدد للتعامل مع جهاز معين.

3. مجالات استخدام إنترنت الأشياء

حسب ما صرح به الباحثون فإن مجالات استخدام إنترنت الأشياء سوف يكون في جميع المجالات ويستخدم في قطاع الطاقة، والمرافق المختلفة، وصناعة السيارات، وعمليات النقل، والأمن والاستطلاع، وفي هذا الشأن قام قسم الأبحاث في شركة «Business Insider» بدراسة حول إنترنت الأشياء ومدى سرعة نموها وانتشارها بين قطاعات الأعمال، وأظهرت الدراسة أن أكبر المستثمرين في هذا المفهوم الجديد هو قطاع الصناعة، حيث من المتوقع أن تصل أحجام استثماراته إلى أكثر من 100 مليار دولار بحلول العام 2018، بينما يحتل قطاع المواصلات والتخزين المركز الثاني يليه قطاع المعلومات. وأظهرت الدراسة أن قطاع التشييد يعد من القطاعات المهمة بتقنية «إنترنت الأشياء» وقد يضخ ما يقارب 30 مليار دولار كاستثمار بحلول العام 2019 (<http://www.ericsson.com>, 2014).

وفي هذا البحث، نعرض بعض النماذج لاستخدام إنترنت الأشياء على سبيل المثال لا الحصر حسب ما اطلعنا عليه في المجالات والجرائد والبرامج التي تعنى بالاختراعات التكنولوجية.

1.3 يمكن للثلاجة التراسل مع مركز التسوق وشراء المستلزمات وتوصيلها بلا تدخل بشري وإبداء رأيها حول إعادة ملئها بالمواد الغذائية بالإضافة إلى تفحص مدى صلاحية الأغذية فيها.

2.3 سيارات تتعقب الأمكنة التي تذهب إليها، وتقوم بالتنبؤ برحلاتها المقبلة، كما أنها تكون مستعدة للإجابة عن أقرب محطة تزويد بالوقود مستخدمة بيانات مستمدة من الإنترنت.

3.3 بالنسبة لشركات التأمين تستفيد من تقنية إنترنت الأشياء من خلال ما يشبه الصندوق الأسود والذي تم إبتكاره من طرف أحد الشركات، يقوم بإرسال معلومات إلى شركة التأمين وإخبارها إن كانت قيادة السائق آمنة وذلك لتخفيض رسوم التأمين.

4.3 في مجال الطب بعض المستشفيات بدأت في استخدام " الأسرة الذكية" والتي يمكن أن تحدد ما إذا كانت الأسرة شاغرة، كما يمكن أن تستخدم أيضا لمعرفة ما إذا كان المريض يحاول النهوض. ويمكن أن تقوم أيضا بضبط نفسها لضمان الضغط المناسب وتقديم الدعم للمريض. يمكن أيضا لأجهزة الإستشعار مراقبة الحالة الصحية لكبار السن في غرف المعيشة. كما يمكن للمستشفيات متابعة حالة المرضى، حيث يمكن للمريض

إرسال تقرير مباشر عن وضعه الصحي وقياس الضغط والسكر إلى المستشفى المركزي عبر الإنترنت، ويمكن للمستشفى متابعة حالته والتواصل معه مباشرة في حالة الخطر.

5.3 المدن الذكية في الصين قام رئيس وزرائها "وين جيا باوي" بجعل إنترنت الأشياء هدفا قوميا وأكد ذلك في قوله: "الصينيين يرون في ذلك جزءا أساسيا من المجتمع". وهذه المناسبة أعلنت السلطات البلدية في "ويوكسي" في ضواحي مدينة شنغهاي في الصين، عن نيتها تشييد حديقة تقوم على مبدأ إنترنت الأشياء، حيث من المتوقع أن تصبح مقصدا للسياح من جيل مستخدمي الإنترنت الجديد.

ثانيا: مخاطر التطور التكنولوجي للنظام المعلوماتي

أ. بالنسبة للأنار السلبية للبطاقات البنكية

انطلاقا من مقولة باسكال الشهيرة: "كل ما تأتي به النهضة تحطمه النهضة". أمام تسارع تطور العولمة والتطور التكنولوجي خاصة في مجال الإعلام الآلي ولواحقه، وتباين في قوانين التجريم بين الدول، قدمت العولمة الجانب السلبي لها في تعزيز روابط التشارك الإجرامي، وتعلم الأقران بعضهم من بعض بين الأفراد الذين ربما لم يكن ليتصل بعضهم بالآخر، فعلى سبيل المثال تتيح المنتديات الإلكترونية المسماة "قرصنة بطاقات الائتمان" أو "قرصنة بطاقات الائتمان" تبادل بيانات بطاقات الائتمان المسروقة. كذلك فإن مواقع الأسواق الإلكترونية المباشرة وغير المشروعة وما يرتبط بها من منتديات النقاش الإلكترونية المباشرة، لا تقتصر على توفير منابر لبيع السلع غير المشروعة فحسب، بل توفر أيضا منابر لتبادل المعلومات بشأن الحفاظ على إغفال هوية وتجنب لفت انتباه أجهزة إنفاذ القوانين (مؤتمر الأمم المتحدة، 2015).

ولقد أشارت مجلة Sécurité inform-atique وهي مجلة متخصصة في الأمن المعلوماتي أن 43% من حالات الغش المعلن عنها قد بوشرت من أجل:

- اختلاس أموال و سرقة المعلومات بنسبة 23%.

- أفعال إتلاف بنسبة 19%.

- سرقة وقت الآلة أي الاستعمال غير المشروع لأجل تحقيق منافع شخصية ما يعادل 15% (الرومي، 2003، ص 24).

1. صور الاستخدام غير المشروع للبطاقات البنكية

من الأفعال التي ينبغي تجريمها داخل إطار التجارة الإلكترونية، هو استخدام بطاقة الائتمان الإلكترونية التي قد يُساء استخدامها من قبل الحامل الشرعي لها، أو من قبل الغير، وعليه نعرض بعض صور العدوان على بطاقات البنكية كالتالي:

1.1 صور الاستخدام غير المشروع للبطاقات البنكية من قبل الحامل الشرعي لها:

1.1.1 جريمة إساءة استعمال البطاقة البنكية.

2.1.1 جريمة استخدام البطاقة البنكية منتهية الصلاحية.

3.1.1 جريمة استخدام بطاقة بنكية ملغاة.

4.1.1 جريمة إساءة استخدام بطاقة ضمان الشيكات.

5.1.1 إساءة استخدام بطاقة السحب الالكترونية من الصراف الآلي.

2.1 صور الاستخدام غير المشروع للبطاقات البنكية من قبل الغير:

1.2.1 جريمة استعمال بطاقة مسروقة أو مفقودة.

1.2.1 جريمة استعمال بطاقة بنكية مزورة.

3.2.1 جريمة تزوير البطاقات البنكية وهي الجريمة محل الدراسة.

ب. بالنسبة لمخاطر استخدام إنترنت الأشياء

تُعتبر مسألة الأمن السيبراني من مصادر القلق التي تؤرق المؤسسات، ففي عام 2016، خسرت الشركات حوالي 4 مليار دولار بسبب الخروقات الأمنية وتعرضت سجلاتها للاختراق الأمني بمعدل 24,000 سجل في كل مرة بالمتوسط. ومن المتوقع أن العدد ارتفع عام 2017 بنسبة 36%. وباتت التهديدات والهجمات الأمنية مستمرة ومتصاعدة ومن المتوقع استثمار الشركات أكثر من 93 مليون دولار لمواجهة التهديدات السيبرانية حتى عام 2018، وبدأ الكونغرس يتحرك بشكل أسرع لسن القوانين على أمل أن يساعد ذلك في تحسين الوضع. ونحن بدورنا سنعرض في هذا البحث بعض الجرائم والتي ارتكبت بواسطة إنترنت الأشياء، ثم التطرق إلى فرضية إمكانية استخدام بيانات إنترنت الأشياء كدليل جنائي رقمي.

1. بعض جرائم إنترنت الأشياء

1.1 التجسس على مستخدمي الإنترنت: بات من الصعب على المستخدمين التخلي عن المزايا الجمة التي توفرها خدمات شركات التقنية الكبرى، كما اعتاد المستخدمون مزايا المزامنة التي تسمح لهم بالدخول إلى حساباتهم عبر أجهزة متنوعة، وهو ما زاد من تعلقهم بخدمات شركات على غرار غوغل وأبل، لتصبح خدمات هذه الشركات هي مفتاح المستخدم أثناء ولوجه إلى شبكة الإنترنت.

وغدا المستخدم مضطرا إلى الوثوق بشركات التقنية الكبرى التي تخزن بياناته الخاصة وتسجل تحركاته عبر شبكة الإنترنت، كون استثمار الخدمات المطورة من قبلها أصبح في كثير من الأحيان أمرا حتميا.

ورغم الفوائد التي تقدمها التقنيات المتصلة بالإنترنت لمستخدميها، فإن إحاطتها المتواصلة بالمستخدم تجعل منها أدوات لمراقبة تحركاته دون علمه، فمثلا، تواردت هذا العام أنباء متنوعة عن تجسس بعض التقنيات الحديثة على مستخدميها، على غرار تلفزيونات سامسونغ الذكية التي ذكرت تقارير أنها تسجل أصوات

المستخدمين وتنقلها لطرف ثالث، ودمى لعبة "باربي" التي تواردت أنباء عن قيامها بتسجيل أسئلة الأطفال وبيعها لطرف ثالث.

فكثيرا ما تطلب شركات الإنترنت من مستخدميها إدخال اسمه الحقيقي مثل غوغل وفيسبوك، كما يمكن للمواقع التعرف على هوية المستخدم لدى إدخاله بيانات بطاقته الائتمانية أو رقم هاتفه. ولا يخفى أن كثيرا من معلومات وبيانات مستخدمي التقنيات تقع تحت رحمة الشركات العملاقة، فعلى سبيل المثال تسيطر غوغل على ثلثي سوق البحث عبر الإنترنت في أميركا، كما يمتلك 75% من مستخدمي الإنترنت حسابات على شبكة التواصل الاجتماعي فيسبوك، في حين تتحكم أمازون بـ 70% من سوق الكتب الإلكترونية في السوق الأميركية، مما يجعل مثل هذه الشركات في موقع بارز يسمح لها بالتحكم بالبيانات الحساسة، حسب الخبير الأمني الأمريكي بروس شناير صاحب العديد من المؤلفات في مجال أمن المعلومات (الجزيرة نت، 2018).

2.1 قرصنة السيارات: أثار المقال الذي نشره موقع "وايرد" الشهر الماضي عن خبري أمن أميركيين سيطرا على سيارة جيب شيروكي قلق الكثيرين، خاصة أنهما تمكنوا من التحكم في السيارة عن بعد، بدءا من نظام التبريد ومساحات الزجاج والمكابح أيضاً، باستخدام الحاسوب.

وقد نشر الخبران -وهما تشارلي ميلر وكريس فالاسيك- التفاصيل التقنية لعملية الاختراق في مؤتمر "القبعة السوداء" الذي أقيم في مدينة لاس فيغاس الأميركية، لكنهما أبلغا شركة "فيات كريسler" الشركة الأم لشركة جيب المصنعة للسيارة عن اكتشافهما قبل عدة أشهر، مما دفعها لاستدعاء 1.4 مليون مركبة بغرض إجراء إصلاحات برمجية لحماية السيارة من أي اختراق محتمل.

ونظراً لاحتواء السيارات الحديثة على العديد من الخصائص التي يتحكم بها الحاسوب، وتتطلب وجود اتصال بالإنترنت -على غرار أنظمة تحديد الموقع والخرائط وتشخيص الأعطال عن بعد- فإن هذه السيارات تقع تحت خطر الاختراق من قبل المجرمين الإلكترونيين وقراصنة الإنترنت.

وتعتمد القرصنة على اعتراض إشارات الراديو لإغلاق وفتح السيارات، حيث يقوم القراصنة باعتراض الشفرة وإعادة إرسالها للسيارة بكل سهولة للاستيلاء على كل ما في داخلها من أشياء ثمينة، أو اختراق شبكتها اللاسلكية (واي-فاي) الخاصة بها ثم إعادة برمجة السيارة وتوجيهها حيث أرادوا، سواء كان ذلك بالتحكم في سرعتها أو حتى بتفجير إطاراتها.

وقد أصبحت قرصنة السيارات مشكلة متزايدة تعاني منها الدول المتطورة حيث شهدت المملكة المتحدة أكثر من ستة آلاف حادثة اختراق وقرصنة للسيارات من دون مفتاح في لندن وحدها (الجزيرة نت، 2018).

ويفتح اختراق السيارات المجال واسعا أمام سلسلة من العمليات التخريبية والإرهابية، فمن الممكن أن يتم استغلال الأمر للتجسس على أصحاب السيارات، أو شل حركة السيارات في الشوارع، أو استخدام قرصنة السيارات بغرض اغتيال شخصيات مهمة وارتكاب أعمال قد تتسبب في وفاة الكثيرين على الطرقات.

3.1 اختراق أنظمة محطات توليد الطاقة: عانت أوكرانيا من هجومين على شبكتها، كان الأول في مارس/آذار في عام 2015 والثاني في نهاية عام 2016. ووفقا لما نشره موقع TNW الهولندي، وقالت شركة iSIGHT Partners الأمنية في منشور لها على مدونتها الرسمية إنها تعتقد أن أول انقطاع للتيار الكهربائي في العالم الذي قام به هاكرز في أوكرانيا منذ أسبوعين مضيا ربما يكون من عمل مجموعة القرصنة الروسية Sandworm Team. وتسبب هذا الفيروس بقطع الكهرباء عن 230 ألف شخص لمدة ساعات بعدما أغلقت المحطات الفرعية جراء الفيروس. وشن القراصنة الإلكترونيين هجوما، على مراحل، باستخدام برامج خبيثة زرعت في أنظمة الكمبيوتر الرئيسية بشركات توليد الطاقة في أوكرانيا.

فيما أشار تقرير لرويترز أن إدارة جهاز أمن الدولة في أوكرانيا يعتقد أيضا أن روسيا هي المسؤولة عن هذا الانقطاع، لكن حتى الآن لم يتم العثور على دليل قاطع.

ويعتقد أن المجموعة استهدفت سابقا مسئولين أوكرانيين وأعضاء في حلف الناتو وحتى وزارة الأمن الداخلي الأمريكي وذلك من أجل التجسس عليهم.

4.1 تزوير الانتخابات الأمريكية: في مقال عرض في CNNArab.com.html بتاريخ 26/يناير/2017 تحت عنوان تزوير الانتخابات الرئاسية بأمريكا..من سيحقق وهل يمكن إيجاد دليل؟ والذي يشير إلى أن جهات روسية وراء تزوير الانتخابات الرئاسية الأمريكية الأخيرة إلا أن البيت الأبيض لم يقدم أي دليل حسي على وقوع التزوير المزعوم الذي قال إنه طال ما بين ثلاثة إلى خمسة ملايين صوت لناخبين شاركوا بشكل غير قانوني في الانتخابات الرئاسية.

المحور الثاني: تحديات القاعدة القانونية لاستيعاب ومسايرة التطور التكنولوجي

بعد التطرق لمظاهر التطور التكنولوجي السريع وما خلفه من إيجابيات وسلبيات، نخصص هذا المحور للدراسة بالتحليل الأسباب التي أدت إلى عجز القواعد القانونية لاستيعاب ومسايرة هذا التطور السريع وتنظيم العلاقات الناشئة منه.

أولا: بالنسبة للبطاقات البنكية

1. الطبيعة القانونية لجرائم البطاقات البنكية

ذهب رأي إلى القول، إن السداد في بطاقات الدفع الإلكتروني يقترب من حوالة الحق أو وكالة. والواقع وإن كان نظام العمل في هذه البطاقات يشبه النظم القانونية التي تحكم حوالة الحق أو تلك التي تحكم الوكالة، فإنه لا

يدخل ضمن هذه الأنظمة القانونية، لأن لهذه البطاقات طبيعة قانونية خاصة بها، يقتضي البحث عنها وتكييفها في ضوء النصوص القانونية الحالية (مصطفى، المرجع السابق).

وذهب رأي آخر إلى أن بطاقات الدفع الإلكتروني تعد نوعاً من النقود، تضاف إلى النقود الورقية والمعدنية المتداولة. ولكن هذا الرأي منتقد، فهذه البطاقات لا تصلح لأن تكون نقوداً، لأن نظامها يفتقد إلى خاصية التداول التي تتصف بها النقود، وإنما هي وسيلة لدفع النقود. لذلك لا تطبق عليها النصوص الجزائية المتعلقة بتقليد النقود وتزييفها وكذلك لا تكون شيكات، لأن الشيك واجب السداد بمجرد الاطلاع ولا يجوز من حيث المبدأ الرجوع فيه، في حين بطاقات الدفع الإلكتروني وإن كانت محل الشيك في الوفاء، لكن يجوز فيها الرجوع (عبد الجبار، المرجع السابق).

من خلال ما تقدم تتضمن البطاقة البنكية بصفة عامة بيانات عادية، وأخرى ممغنطة. فبالنسبة للأولى لا شك أنها تحقق مقومات المحرر، لأنها تعبر عن مجموعة من الأفكار والمعاني الصادرة عن شخص أو جهة معينة، فبصدورها عن بنك أو مؤسسة مصرفية توفر لها مقومات المحرر، فإذا وقع تحريف في أي من البيانات العادية التي تتضمنها البطاقة، كاسم حاملها، أو الرقم الخاص بالبطاقة، أو تاريخ صلاحيتها. فإن ذلك يعد تزويراً في محرر رسمي أو عرفي، وذلك حسب ما تكون البطاقة صادرة عن إحدى المؤسسات المصرفية العائدة للدولة، أو عن مؤسسة مصرفية خاصة. أما البيانات الممغنطة فتندرج ضمن مدلول التزوير المعلوماتي، والذي عرفته اتفاقية بودابست بأنه: "هو التزوير المرتبط بالحاسب الآلي والذي يتكون عند خلق أو تعديل غير مصرح به للبيانات في سياق المعاملات القانونية، بتغيير صحة البيانات المستخرجة التي تكون موضوع الخداع المصالح القانونية المحمية..." (مصطفى، المرجع السابق).

2. أساس وعلة التجريم

إن الطفرة الكبيرة التي يشهدها نظام التعامل بالبطاقات البنكية، تطلب منا التطرق لأساس وعلة التجريم، وهذا بغرض البحث عن المصلحة المحمية لهذه البطاقات من أية محاولات قد تنال من سلامتها أو تخل بالثقة التي اكتسبتها في مجال المعاملات المالي، من خلال تجريم فعل تزوير البطاقات البنكية، ثم مبررات التجريم.

1.2 المصلحة المحمية: نذكر منها على سبيل المثال لا الحصر.

- أضحى غش المستهلك الإلكتروني، أمراً شائعاً وعابراً للحدود الوطنية بسبب استخدام بطاقات الائتمان والبطاقات المصرفية للمدفوعات الإلكترونية.
- استخدام هذه البطاقة فرصة ذهبية لغاسلي الأموال وأقطاب تجارة المخدرات والجرائم المنظمة، إذ أنهم يمكنهم ممارسة أنشطتهم وتحويلاتهم المالية في إطار شرعي.

- تطرح تكنولوجيات المعلومات والاتصالات مواضيع جديدة للفعل الإجرامي أي المستهدف بالجريمة سواء أكان الشخص أو الشيء أو القيمة، مثل البيانات أو النظم الحاسوبية.

2.2 مبررات التجريم: نظرا لخطورة فعل تزوير البطاقات البنكية، والأضرار التي تنجم عنه سواء على حامل البطاقة أو المؤسسة المصرفية، فقد أصبحت جرائم بطاقة الدفع الإلكترونية تمثل تهديدا يتأثر به حامل البطاقة وجميع أطراف العملية المصرفية في جميع أنحاء العالم. وأصبحت جرائم العبث ببطاقات الائتمان من الجرائم المنظمة، حيث يتم تجميع المعلومات اللازمة عن بطاقات الائتمان الصحيحة في دولة، ويتم إعداد البطاقات المزورة في دولة أخرى، ويجري ترويجها واستخدامها في دولة ثالثة. وفي هذا الإطار، تدخل المشرع بتجريم فعل تزوير البطاقات البنكية، وهذا بغرض ضمان وتعزيز الثقة المكتسبة في مجال المعاملات المالية بين الزبون والمؤسسة المصرفية، وردع كل من يعتدي على هذه الثقة أو على أحد أطرافها.

3. التدابير والإجراءات الوقائية المقررة لجرائم البطاقات البنكية

إنه ليس من الصواب الانتظار حتى تقع الجريمة، بل يجب مكافحة الأسباب والعوامل التي تساعد على وقوعها وذلك بانتهاج منهج وقائي لتفادي وقوع الجريمة، مما دفع ببعض الدول ومن بينها المشرع الجزائري إلى تشريع قانون خاص بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، (قانون رقم 04-09، 2009) وإلى تشكيل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها (مرسوم رئاسي رقم 15-261، 2015).

وذلك من خلال تبني المفهوم الواسع للجرائم المتصلة بتكنولوجيات الإعلام والاتصال في المادة 2 منه: "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية." وبهذا التعريف لم يدع المشرع مجالا للشك في إدراج جميع الجرائم السيبرانية سواء نص عليها في قانون العقوبات أو تلك الجرائم التي يمكن أن تقع مستقبلا بقوله: "أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية"، تبقى على الجهات القضائية المختصة تحديد الركن المادي لكل جريمة وإثبات الضرر أي العلاقة السببية، وربطه بالركن المعنوي لها.

وفي هذا الصدد، نتطرق لمهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها: في إطار الوقاية من الجرائم السيبرانية بصفة عامة، والتي من بينها جريمة تزوير البطاقات البنكية حسب ما هو وارد في المادة 14، والمتمثل في تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها

بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال، تبادل المعلومات مع نظيراتها في الخارج قصد التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم.

ويهدف تفعيل دور الهيئة و تعزيز مهامها، أصدر المشرع المرسوم الرئاسي رقم 15-261، بحيث تنص المادة 06 منه: "تضم الهيئة، لجنة مديرة، مديرية عامة، مديرية للتنسيق التقني، مركز للعمليات التقنية، ملحقات جهوية، مديرية للمراقبة الوقائية واليقظة الإلكترونية". هذه الأخيرة التي يلقى على عاتقها تنفيذ عمليات المراقبة الوقائية للاتصالات الإلكترونية من أجل الكشف على الجرائم المتصلة بالإعلام الآلي، بالإضافة إلى جمع ومركزة واستغلال كل المعلومات التي تسمح بالكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مساعدة مصالح الشرطة القضائية المختصة والسلطات القضائية.

4. أساليب المكافحة المقررة لجريمة تزوير البطاقات البنكية

تجد الجهات القضائية ذات الاختصاص الموسع أساسها القانوني في نص المواد 37 و 40 و 329 من قانون الإجراءات الجزائية، حيث تم إدخال هذا النظام بموجب التعديل الذي أدخل على ق.إ.ج في سنة 2004 بموجب القانون رقم 04-14 المؤرخ 10-11-2004 الذي عدل وتمم القانون رقم 66-155 المؤرخ في 08-06-1966 المتضمن قانون الإجراءات الجزائية. ولقد تم تجسيد هذا التوجه في الواقع العملي بعد صدور المرسوم التنفيذي رقم 06-348، المؤرخ في 05-10-2006 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق.

وعلى ضوء المواد 37، 40، 329 من ق.إ.ج المعدل والمتمم ينحصر الاختصاص النوعي للمحاكم ذات الاختصاص الموسع (الأقطاب الجزائية) في متابعة أو بمعنى أدق القيام بإجراءات البحث والتحري عن الجرائم وكشف مرتكبها وضبطهم والتحقيق معهم ومحاكمتهم، بخصوص الجرائم التالية: جرائم المخدرات، الجريمة المنظمة عبر الحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، جرائم تبييض الأموال، جرائم الإرهاب، الجرائم المتعلقة بالتشريع الخاص بالصرف، وجرائم الصفقات العمومية. فهي سبعة (07) جرائم، تجمع بينهم درجة الخطورة، ونطاق انتشارها الواسع، وأثرها المدمر على الاقتصاد الوطني والأمن والاستقرار، وكذلك خطورة واحترافية مقترفها.

أساليب التحري الخاصة: المقصود بأساليب التحري هي تلك الإجراءات التي بواسطتها يتم جمع التحريات من مصادرها، ويعبر عنها بالحدود الشكلية لها، وهي تلك الحدود التي يجب مراعاتها عند إجراء التحريات حتى تحقق آثارها إزاء تفاعلها مع الحدود الموضوعية وتنأى عن كل بطلان، أما أساليب التحري الخاصة فلا نجد لها تعريفا محددا، فالاتفاقيات الدولية نصت على استخدامها كاتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة واتفاقية الأمم المتحدة لمحاربة الفساد تضمنت دعوة الدول الأعضاء في الاتفاقية إلى اتخاذ مايلزم من تدابير على ضوء

نظامها الداخلي لاستخدام ما تراه مناسباً من أساليب تحري خاصة واكتفت بتعريف أسلوب التسليم المراقب بالنظر إلى طابعها لدولي، وتركت مسألة تقدير وتعريف بقية الأساليب إلى كل دولة وفقاً للتشريع الجنائي والمبادئ الأساسية لنظامها الداخلي (مصطفى، 2016، ص 349).

ونحن بصدد دراسة جريمة تزوير البطاقات البنكية، نرى بأن أساليب التحري الخاصة أنجع طريقة لكشف أوكار المجرمين عن طريق التسريب والتسليم المراقب، وفي سبيل رصد مخططاتهم الداخلية والخارجية عن طريق ما يسمى الجريمة المنظمة، فأسلوب اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، والترصد الإلكتروني، كفيل بإيقاع المجرمين في حالة تلبس، وهو ما أكد عليه المشرع في المادة 3 من قانون 04-09.

أما بالنسبة للأدلة المتوصل إليها عن طريق إتباع أساليب التحري الخاصة وفقاً للإجراءات القانونية وبإذن من السلطة القضائية، كوكيل الجمهورية في مرحلة البحث والتحري وجمع الاستدلالات والجريمة المتلبس بها. وقاضي التحقيق في مرحلة التحقيق الابتدائي أو الإنابة القضائية، تكتسي هذه الأدلة بطابع الشرعية والحجية القانونية أمام الجهات القضائية.

ثانياً: بالنسبة لإنترنت الأشياء

أ. إشكالية استخدام بيانات إنترنت الأشياء كدليل جنائي رقمي

بعد جهد كبير للبحث عن قضايا استعملت فيه أدلة جنائية رقمية ناشئة من إنترنت الأشياء، صادفنا مقال بعنوان (Aurélien, 2017) *OBJETS CONNECTÉS, NOUVEAUX TÉMOINS-CLÉS?* أين وجدنا قضايا عرض أصحابها أدلة جنائية رقمية ناشئة من إنترنت الأشياء كدليل جنائي وقد تعاملت معه الجهات القضائية. يعرض صاحب المقال أنه يمكن للأجسام المتصلة أن تصبح أدلة مهمة من خلال المعلومات المتعلقة بمكان ونشاط صاحبها.

القضية الأولى: مارس/آذار 2015 -ولاية بنسلفانيا- استخدمت المعلومات التي جمعها سوار "فيتبيت" المتصل كجزء من شكوى الاغتصاب. وأشار نشاط صاحب الشكوى الذي سجلته السوار إلى أنها كانت تتحرك طوال الليل بينما قالت إن سوار تعقب النشاط كان قد وقع على الأرض أثناء كفاحها على فراشها ضد المعتدي. إلا أنه تم رفض التحقيق في النهاية بسبب أن الأدلة المقدمة من طرف الضحية كانت غير متناسقة.

القضية الثانية: نوفمبر/تشرين الثاني 2015-أركنساس- طلبت الشرطة الأمريكية الاستعانة بتسجيلات المتحدث الذكي "أمازون إكو" كشاهد أصلي للتحقيق في جريمة قتل. بعد أمر تفتيش، طلبت السلطات القضائية الوصول إلى التسجيلات بتسجيلات المتحدث الذكي "أمازون إكو" في المتصل في مسرح الجريمة وذلك باستخدام تقنية التعرف على الصوت. وقد سجل الأخير جميع الأحداث التي وقعت في الليلة التي تم فيها غرق رجل في ممتلكات أحد أقاربه.

بشكل عام، كل الكائنات الذكية تقدم الآن بيانات يمكن استخدامها في المسائل القضائية. تكشف دراسة قام بها مركز "بيركمان كلاين" في جامعة هارفارد عن قائمة طويلة جدًا من الأجهزة المتصلة: أجهزة التلفزيون والمحامص وصانعي القهوة وفرشاة الأسنان وأقفال الأبواب والمقاييس والحرارة وحتى المصابيح المتصلة. قد يكون لأحدهم يومًا ما عنصرًا حاسمًا في البراءة أو إدانة أي فرد.

بل وأكثر من ذلك، فمع الساعات أو المتبعتات المتصلة بالتقاط نبضات قلبها في الوقت الحقيقي، يصبح من الأسهل تحديد تاريخ وفاة الضحية حسب الوقت والمدة الدقيقة لاعتداء. بعد التحقق من صحة من قبل الأطباء الشرعيين. يمكن للمرء أن يتخيل، في نهاية الأمر، أن الأجسام المتصلة تشارك في تقييم معاناة مسبقة. يمكن قياس مشكلة الاستمتاع بالضحية من خلال مقارنة وضعه قبل وبعد العدوان.

ب. إشكالية مشروعية الدليل الجنائي لإنترنت الأشياء لدى القاضي الجزائري

1. تحديد الجهة المتحكمة في الكم الهائل للبيانات

لكي تكون لهذه البيانات الرقمية حجية أما القضاء أو أي جهة معنية تطرح إشكالية تحديد الجهة المتحكمة في الكم الهائل للبيانات، فيرى بعض الحقوقيين والخبراء إلى ضرورة وجود قوانين منظمة لضبط وتحديد ملكية الكميات الهائلة من البيانات التي تلتقطها الأجهزة المتصلة بالإنترنت، والتي قد تتعلق بنشاط المستخدم وصحته أو بنمط حياته داخل المنزل، حيث يتوقع "شايبرو" أن يثير هذا الأمر جدلا كبيرا في الأوساط التقنية قبل تحديد الجهة الأحق بامتلاك هذه البيانات وإدارتها.

وفي حين يرى البعض أن هذه الجهة يجب أن تكون الشركات المطورة للأجهزة المتصلة بالإنترنت، يرى آخرون ضرورة أن تكون هذه البيانات في أيدي جهات حكومية أو منظمات غير ربحية (الدقموني، 2018).

ولإيضاح مدى جدلية هذا الأمر، طرح "شايبرو" مثالا عن إحدى الشركات التابعة لشركة صناعة السيارات "جنرال موتورز" والمسماة "أون ستار"، حيث تهتم هذه الشركة بجلب بيانات عن السيارات المتصلة بالإنترنت المشتركة بخدماتها تسمح بتوفير تشخيص للأعطال وتزويد السائق بمعلومات تهمه، ومن ثم الاستفادة من البيانات الملتقطة لتحسين صناعة السيارات، في حين يرى البعض أنه يجب على جهات حكومية أن تصل إلى هذه البيانات لتستفيد منها بغرض توفير درجات أمان أعلى على الطرقات (الجزيرة نت، 2018).

وفي هذا البحث المتواضع نتفق مع الرأي القائل أنه يجب على جهات حكومية أن تصل إلى هذه البيانات لتستفيد منها بغرض توفير درجات أمان أعلى على الطرقات. ونجد هذا الرأي مجسد ضمن المادة الرابعة، من المرسوم الرئاسي رقم 15-261 المتعلق بتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها حين أسند للهيئة الوطنية مهام: "تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية".

2. الدليل الجنائي لإنترنت الأشياء ومدى مشروعيته مع القانون الجزائري الحالي

باستقراء مواد القانون رقم 04-09 والمرسوم الرئاسي رقم 15-261 نجد أن المشرع خاصة في المرسوم الأخير أنه عرّف الاتصالات الإلكترونية في المادة 05 بقوله: "كل تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات أيا كانت طبيعتها عن طريق أي وسيلة إلكترونية بما في ذلك وسائل الهاتف الثابت والنقال". إلا أننا ندعو المشرع وفي هذا البحث المتواضع تعديل المادة بحذف كلمة "إلكترونية" وتصبح المادة كالتالي: "كل تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات أيا كانت طبيعتها عن طريق أي وسيلة بما في ذلك وسائل الهاتف الثابت والنقال" وبهذا التعديل يكون مفهوم إنترنت الأشياء قد تم إدراجه ضمن التعريف الوارد في سياق المادة، كما أن كلمة أي وسيلة لها نفس المدلول لكلمة أي شيء، بالإضافة إلى مفهومها الجديد أي المادة 05 من نفس المرسوم الرئاسي السابق فهي تشمل كذلك الوسائل الإلكترونية والتي تم حذفها قبل التعديل.

وبمأن إنترنت الأشياء عابرة للحدود بحسب طبيعتها واتصالها بالشبكة العالمية وسع من المشرع من صلاحيات الهيئة الوطنية وأصبح على عاتقها:

السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها" بالإضافة إلى المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيات الإعلام والاتصال، وبمأن مجال الإختصاص يفوق قدرة القاضي والمشرع سمح للمشرع للهيئة الوطنية المساهمة في تحديث المعايير القانونية في مجال إختصاصها.

كما كلف مديرية التنسيق بما يتوافق مع مهامها خاصة فيما يخص إنجاز الخبرات القضائية في مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وهذه بادرة حسنة من المشرع، بالإضافة إلى تكوين قاعدة معطيات تحليلية للإجرام المتصل بتكنولوجيات الإعلام والاتصال واستغلالها ضمن المادة 12 من نفس المرسوم الرئاسي.

وقد أحسن المشرع في المادة 07 حين جعل تشكيلة اللجنة المديرية للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها تتضمن كل من وزير العدل رئيسا، -الوزير المكلف بالداخلية، -الوزير المكلف بالبريد وتكنولوجيات الإعلام والاتصال، -قائد الدرك الوطني، -المدير العام للأمن الوطني، -ممثل عن رئاسة الجمهورية، -ممثل عن وزارة الدفاع الوطني، -قاضيان من المحكمة العليا يعينهما المجلس الأعلى للقضاء لأن الجرائم السيبرانية بصفة عامة وإنترنت الأشياء مستقبلا تحتاج في حقيقة الأمر جهود كبيرة تقع مسؤوليتها على الجميع بما فيهم رجال الشرطة والنيابة والقضاة والخبراء. فالخبراء يفهمون كل شيء عن تقنية المعلومات وشبكات الاتصالات وطريقة عملها، ولا كن لا يدركون متطلبات الإجراءات القانونية

وقواعد وكيفية التعامل معها والمختصون في العلم الجنائي مختصون في التعرف على الآثار المادية وتحليلها ومضاهاتها ولكن يجهلون الدراية باستخدام البرامج الرقمية وتقنياتها في مجال عملهم، والمحامون ورجال النيابة والقضاة فإنهم يفهمون القانون شكلا ومضمونا وليس أكثر من ذلك.

وقد أحسن المشرع حين استدرك المرسوم الرئاسي رقم 15-261 بخصوص عملية مراقبة الاتصالات الإلكترونية حين أخضعها برخصة مسلمة من السلطة القضائية بدلا من الشرطة القضائية. بمناسبة إجراء عملية رقابة تنفذ من طرف مستخدمين تقنيين يعملون تحت إدارة ورقابة قاضي يساعده ضابط أو أكثر ينتمي للهيئة بالإضافة إلى كون المحاضر التي تحررها الهيئة الوطنية تكون طبقا لأحكام قانون الإجراءات الجزائية.

الخاتمة:

وفي ختام هذا البحث يجب أن ننوه بأن موضوع القانون والتكنولوجيات الحديثة أثبت عجز المنظومة القانونية الحالية لمواكبة هذا التطور العلمي والتقني، وفرض حتمية تطوير هذه المنظومة القانونية بما يواكب هذه الدراسة التي قدمها على سبيل المثال لا الحصر بالنسبة للبطاقات البنكية وإنترنت الأشياء والذي يتوقف على فهم عميق للجانب التقني المعقد لهذه التكنولوجيا التي تتميز بالتطور السريع، لاسيما إنترنت الأشياء والتي تعتبر في حد ذاتها ثورة علمية خيالية سوف تجعل من الخيال حقيقة والعلم الواقعي سوف يصبح افتراضي. وعليه سوف تتغير عدة مفاهيم وخلق مراكز وعلاقات جديدة وآخرها حسب ما طلعنا عليه انعدام الشخصية الطبيعية للإنسان ليصبح هو الآخر "شيء" ضمن "الأشياء" المتصلة ضمن إنترنت الأشياء وهذا عن طريق غرس شريحة إلكترونية في جسم الإنسان تصبح وسيلة اتصال بالعالم الخارجي، فهذه الشريحة تذكرك بمواعيد الاجتماعات وتتصل بأصدقائك وتخبرهم عن مكانك، وترسل إشارات إلى الطبيب عن الحالة الصحية لقلبك وضغط الدم... وكذلك يتغير مفهوم البيوت لتصبح بيوت ذكية، والمدن كذلك والمفاهيم الاقتصادية تتغير وبالموازات تتغير معها مفهوم تحديد المسؤولية وتتغير بذلك الجريمة.

وإلى ذلك الحين نرى بأن الجدل الفقهي لن يتوقف، وإن كانت بوادر الإتفاق بين الدول العظمى حول القواعد والمعايير، والتي تقييد الحرب السيبرانية بقانون النزاعات المسلحة، الأمر الذي يستلزم التمييز بين الأهداف العسكرية والمدنية والتناسب من حيث النتائج. وقد أوصت مجموعة الأمم المتحدة من الخبراء الحكوميين باستبعاد الأهداف المدنية من الهجمات السيبرانية، كما أقرت مجموعة العشرين هذا المعيار، لاسيما بعد الهجوم الإلكتروني الذي شنته روسيا ضد إستونيا عام 2007، والذي تسبب في شلل تام للدولة ومرافقها العسكرية والحكومية الحيوية، حيث أعتبر آنذاك أول هجوم إلكتروني تشنه دولة ضد دولة أخرى (سعيد، بدون سنة نشر).

ونحن بدورنا نقول إفتراضا لا جوابا بأن الأدلة المستمدة من إنترنت الأشياء سوف تصبح لها مشروعية وحجة وقد تحل محل الأدلة الإقناعية لدى القاضي الجزائري بالنسبة التشريعات الأجنبية وخاصة الدول المتقدمة في هذا المجال. أما بالنسبة للقاضي وللمشرع الجزائري فمستقبلا حينما تفرض هذه التكنولوجيا نفسها على أرض الواقع سوف نعلم على تبني أي نظرية من بين النظريات السائدة حينها.

قائمة المراجع:

القوانين

1. قانون رقم 04-09، مؤرخ في 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرام المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية رقم 47، بتاريخ 16 غشت 2009.
2. مرسوم رئاسي رقم 15-261، مؤرخ في 8 أكتوبر 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية رقم 53، بتاريخ 8 أكتوبر 2015.

المراجع بالعربية

1. عمراني مصطفى. (2016). جريمة استغلال النفوذ في مجال الصفقات العمومية "دراسة مقارنة"، مركز الدراسات العربية للنشر والتوزيع، جمهورية مصر العربية، الطبعة الأولى.
2. محمد أمين الرومي. (2006). جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية.

المقالات

1. إبراهيم محمد شاشو، أسامة الحموي. (2011). بطاقة الانتماء حقيقتها وتكييفها الشرعي، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 27، العدد الثالث، كلية الشريعة، جامعة دمشق، سوريا.
2. رائد الشيخ. (2015). إنترنت الأشياء عندما تتولى التجارة التسوق بنفسها، مجلة القافلة، العدد 3، مجلد 64، الناشر، شركة الزيت العربية السعودية، أرامكو السعودية، الظهران، المملكة العربية السعودية.
3. سعيد درويش. (بدون سنة نشر). ماهية الحرب الإلكترونية في ضوء قواعد القانون الدولي، حوليات جامعة الجزائر 1، العدد 29، الجزء الثاني.
4. عبد الجبار الحنيص. (2008). الحماية الجزائية لبطاقات الائتمان الممغنطة من التزوير، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 24، العدد الثاني.
5. عمراني مصطفى. (بدون سنة نشر). جريمة تزوير البطاقات البنكية، مجلة الدراسات والبحوث القانونية، المسيلة، الجزائر، المجلد 02، العدد 07.
6. محمد ناصر إسماعيل، أمل حسن علوان، تغريد جليل. (2013). البطاقة الذكية وأثرها في التقليل من بعض المخاطر المصرفية، دراسة استطلاعية لعينة من زبائن مصرف الراجحي - فرع الخضراء، العدد 37، مجلة كلية بغداد للعلوم الاقتصادية الجامعة.
7. مهند فايز الدويكات، حسين محمد الشبلي. (بدون سنة نشر). صور الاحتيال والتزوير في بطاقات الائتمانية، المجلة العربية للدراسات الأمنية والتدريب، المجلد 29، العدد 57، الرياض، السعودية.

المراجع الفرنسية

1. Aurélie Lagoutte. (2017). **OBJETS CONNECTÉS, NOUVEAUX TÉMOINS-CLÉS?** Legimag, magazine du droit au Luxembourg, N°19.

المواقع الإلكترونية

1. شبكة ابو نواف. (2016). ما هو إنترنت الأشياء وكيف يعمل؟ وما هي أهم استخداماته؟، أطلع عليه بتاريخ 2020/03/29.
2. BBCArabic.html. (2017). تاريخ زيارة الموقع 2019/03/29.
3. الجزيرة نت. (2015). إنترنت الأشياء ومشاكل الخصوصية، تاريخ زيارة الموقع، 2020/03/28.
4. الجزيرة نت. (2015). هل يمكن الوثوق بتقنيات "إنترنت الأشياء"؟، تاريخ تصفح المقال، 2019/04/01.
5. الجزيرة نت. (2015). قرصنة السيارات.. المخاطر القادمة، تاريخ تصفح المقال، 2020/04/01.

⁶. رماح الدلقموني.(2017). إنترنت الأشياء بين تحسين الحياة وتهديدها، مقال منشور على موقع الجزيرة نت.(2017). تاريخ زيارة الموقع 2020/04/01.

¹. Hope Reese.(2017). **Report: IoT attacks exploded by 280% in the first half of 2017**, www.techrepublic.com/article/report-iot, 9August 2017, Date de visite, 30/03/2020.

². Report, <http://www.ericsson.com/res/docs/2014/ericsson-mobility-report-june-2014>.