التعاون الدولي ومدى فعاليته في مكافحة جرائم تزوير بطاقات الدفع الإلكتروني

International cooperation and its effectiveness in combating the crimes of fraud in electronic payment cards

طالبة الدكتوراه/ نوال حاج مخناش *
جامعة يحيى فارس المدية، الجزائر
hadjmokhnachenawel@gmail.com
الدكتور/ رشيد شميشم
جامعة يحيى فارس المدية، الجزائر
rachidchemichem@gmail.com

تاريخ الاستلام: 2018/11/08 تاريخ القبول للنشر: 2019/01/28

❖❖❖❖❖❖❖

الملخّص:

تعتبر جرائم تزوير بطاقات الدفع الالكتروني باختلاف صورها وأساليبها من الجرائم المستحدثة في العصر الحالي، والتي أصبحت تمس كيان الدول والمجتمعات، لاعتبارها جرائم اقتصادية ذات مخاطر كبيرة على الاقتصاد العالمي، في ظل متطلبات التجارة الالكترونية، والتوجه الحديث لتعميم التعامل الالكتروني في المعاملات المصرفية، فأصبح التعاون الدولي لمكافحتها أمرا محتما. ولقد حاولنا من خلال هذه الورقة البحثية التطرق للمساعي الدولية للتصدي لها، والتي تجسدت غالبيتها في عقد المؤتمرات والمعاهدات من قبل المنظمات الدولية والإقليمية من جهة، والاعتماد على عدة وسائل قانونية وشرطية وإدارية، رغم وجود العديد من الصعوبات والمعوقات التي تحول دون تحقيق النتائج المرجوة من ذلك.

الكلمات المفتاحية: بطاقات الدفع الالكتروني، التعاون الدولي، التزوير، المنظمات الدولية، المعاملات المصرفية.

Abstract:

The crimes of forgery of electronic payment cards, with all its different forms and methods is considered a frequent crime in this current era, it has affected the entity of nations and societies, it is considered an economic crime that poses great risks to the global economy. In the light of the requirements of the electronic trade and the international cooperation, combating this issue has become inevitable. We have tried through this paper to address the international efforts that address this issue, most of which were embodied in the holding of conferences and treaties by international and regional organizations on the one hand, and relying on a number of legal, policing and administrative means on the other hand. This is in

despite of the many difficulties and obstacles they face to achieve the desired result.

Keywords: *Electronic Payment Cards, International Cooperation, Counterfeiting, regional organizations, Banking transactions.*

* المؤلف المراسل.

مقدّمة:

تعد بطاقات الدفع الإلكتروني وسيلة حديثة من وسائل الدفع، ظهرت نتيجة استخدامات الحاسبات الآلية وانتشارها على نحو واسع، في جميع مجالات الحياة، خاصة في القطاع المصرفي، وباتت شائعة بين كل أفراد المجتمع على الرغم من اختلاف مصادر دخلهم، وبدأت التوجهات المالية الجديدة لاعتبارها بديلا عن النقود التقليدية في الوفاء بقيمة السلع والخدمات. وتتميز هذه الوسيلة المستحدثة بأنها أداة دفع إلكترونية تقوم بتسوية المعاملات التجارية والبنكية بين الأفراد والتجار والبنوك طبقا لنظام التحويل الآلي للنقود أو بما يعرف بالنقود القيدية.

ونظرا لما تؤديه هذه البطاقات من خدمات ومزايا لجميع المتعاملين بها، انتشرت بطاقات الدفع الإلكتروني على المستويين المحلي والدولي، وأصبحت تحتل مساحة كبيرة في تعاملات الأفراد على حساب باقي وسائل الدفع الأخرى، وأدى هذا الانتشار إلى ظهور أساليب مختلفة ومتعددة للتلاعب والتحايل باستخدامها، مما يمثل تهديدا مباشرا للاقتصاد محليا ودوليا، وخلق هذا الانتشار نموا مطردا للجرائم المصاحبة لاستخدامها، حتى أن بعض المجرمين اتخذ من تزوير هذه البطاقات حرفة للاستيلاء على أموال الغير بدون وجه حق، وخاصة أن هذه النوعية من وسائل الدفع تعتمد في التعامل بها على النظام المعلوماتي، الذي تتدفق فيه المعلومات والبيانات، والذي تكون فيه النقود عبارة عن رموز وبيانات مشفرة إلكترونيا، الأمر الذي يسهل على محترفي الحاسب الآلي فك هذه البيانات والبيانات المشفرة وتغييرها، بهدف الحصول على الأموال بطرق غير شرعية.

ولم يقف الأثر السلبي لجرائم تزوير بطاقات الدفع الالكتروني عند الحدود الوطنية للدول، بل تعداها لتباشر أنشطتها على المستوى الدولي، مما أدى بالبعض إلى تصنيفها من بين الجرائم المنظمة العابرة للقارات، لارتباطها بنشاط العصابات المنظمة، التي تقوم بتجميع المعلومات الصحيحة في دولة، وإعداد البطاقة المزورة في دولة أخرى، وترويجها واستخدامها في دولة ثالثة، والتي تمكنت من تجميع ثروات طائلة تسمح لها بمنافسة سلطات الدول وزعزعة أنظمتها الاقتصادية. وأمام كل ذلك وجدت القوانين العقابية التقليدية نفسها عاجزة أمام احتواء هذه الظاهرة الإجرامية المستحدثة، مما أدى إلى تفطن الدول إلى ضرورة تكثيف جهود التعاون الدولي لمكافحة جرائم تزوير بطاقات الدفع الإلكتروني بمختلف صورها، وخاصة الدول النامية لما يؤثر هذا النوع الحديث من الإجرام على مصالحها القومية والاقتصادية والاجتماعية.

بناء على ما سبق سنحاول طرح الإشكالية التالية: **هل التعاون بين الدول في مجال مكافحة جرائم تزوير بطاقات الدفع الالكتروني حقق النجاح أم مازال دون المستوى المطلوب؟** و للإجابة على الإشكالية المطروحة فإن الدراسة ستناقش أربع محاور، **المحور الأول** بعنوان صور تزوير بطاقات الدفع الالكتروني، و**المحور الثاني** بعنوان أشكال التعاون الدولي لمكافحة جرائم تزوير بطاقات الدفع الإلكتروني، أما **المحور الثالث** فسنتطرق من خلاله لوسائل التعاون الدولي لمكافحة جرائم تزوير بطاقات الدفع الإلكتروني، وأخيرا نخصص **المحور الرابع** لدراسة صعوبات التعاون الدولي في مجال مكافحة جرائم بطاقات الدفع الالكتروني.

المحور الأول

صور تزوير بطاقات الدفع الالكتروني

لقد كان لكثرة بطاقات الدفع الالكتروني، واختلاف أنواع المشتريات والخدمات التي يمكن الحصول عليها بواسطتها، دافع لانكباب المزيفين والمزورين وعصابات الجريمة على إنتاج بطاقات مزورة ومقلدة لاستخدامها في التحايل والتلاعب والسرقة، فأصبح يطلق عليها جريمة العصر القادم، ويترتب على وقوعها خسارة كبيرة للعملاء والمصارف، وتهديد للاقتصاد المحلي والعالمي.

وقد ظهرت أساليب وأنماط مختلفة في تزوير هذه البطاقات سواء من قبل أطراف نظام التعامل ببطاقات الدفع الالكتروني-الحامل والتاجر وموظف البنك المصدر-أو من قبل الغير. ومن أجل الايضاح للقارئ الكريم حول صور تزوير بطاقات الدفع الالكتروني سنتناول التزوير الواقع على تلك البطاقات بحد ذاتها أولا، ثم نتطرق بالبحث لحالات تزوير الإشعارات والمستندات الخاصة ببطاقات الدفع الالكتروني.

أولاً- أساليب تزوير بطاقات الدفع الالكتروني:

يتم تزوير بطاقات الدفع الإلكتروني في محتوياتها بطرق مختلفة، وقد يقع التزوير على المعلومات المقروءة الموجودة عليها، أو على المعلومات المشفرة الموجودة على الشريط المغناطيسي، إذ قد يكون هذا التزوير كليا أو جزئيا وسنفصل في ذلك فيما يلي:

أ- التزوير الكلي لبطاقات الدفع الإلكتروني:

هناك رأيان حول إمكانية تزوير بطاقة الدفع الالكتروني من الناحية العملية[1]:

الرأي الأول: يرى بعدم إمكانية تقليد بطاقة الدفع الالكتروني، لأن لكل بطاقة رقما يعرفه صاحب البطاقة، وتمت برمجته على حساب صاحبها، ولكل بطاقة رقم سري لا يمكن استعمالها إلا به، ولتحقيق تقليد مثل هذا النوع من البطاقات يجب صنع البطاقة من نفس المادة التي تصنع منها البطاقة الأصلية، وأن تأخذ نفس رقمها وكذلك نفس رقمها السري، وأن يتم مغنطتها، وهذا ما يستحيل القيام به، إلا إذا كان المزور على صلة بموظف البنك المصدر لبطاقة الدفع، حيث يقوم هذا الأخير بتزويده بنفس البطاقة المراد تزويرها.

الرأي الثاني: يرى هذا الرأي إمكانية تزوير بطاقة الدفع الالكتروني، إذ يتصور أن يتم تزويرها بعدة طرق. وهذا هو الرأي الراجح، فمن الناحية العملية فإن تزوير بطاقة الدفع الالكتروني وإن كان

صعبا إلا أنه ليس بمستحيل، حيث يمكن استخدام مثل هذا النوع من البطاقات المزورة في الوفاء أو سحب النقود من الأجهزة الآلية أو الصراف الآلي، وذلك باستخدام أرقام بدلا من الرقم السري للبطاقة.

فيمكن القول بأن التزوير الكلي يتم بصنع بطاقة دفع إلكتروني مقلدة بكامل عناصرها التأمينية، وذلك بعد حصول الجاني على البيانات والمعلومات الخاصة ببطاقات العملاء، عن طريق تقديم الرشاوى للعاملين في الجهات التي تصدر تلك البطاقات و بوجه خاص الأقسام ذات الصلة بإصدار البطاقة[2]، أو الجهات التي تتعامل مع هذه البطاقات كأمناء صناديق المحلات التجارية الكبرى الفنادق والمطاعم ومحطات تزويد الوقود، حيث يقوم بإقناع الموظف التابع لهذه الأماكن أن يسجل له أو يبيعه أرقام بطاقات دفع الزبائن خاصة البطاقة الذهبية منها أو الكلاسيكية كونها تتمتع بسقف مدفوعات مرتفع[3]، أو الحصول على تلك المعلومات من منافذ استعمالها كقوائم الحجز في الفنادق أو وكالات السفر أو في قوائم الحساب المدفوع، والتي يتم التخلص منها لانتفاء الحاجة منها، ويمكن الحصول عليها أيضا عن طريق اختراق قواعد البيانات من خلال الدخول غير المشروع للمواقع أو لأجهزة الحاسب الآلي والتي توفرها تقنية العمل بشبكة المعلومات العالمية "الأنترنت".

ويتحقق التزوير من قبل الجاني من خلال خلق أو صناعة بطاقة مشابهة لنوع من أنواع البطاقات المتداولة بحيث يبدأ أولا بصناعة الجسم المادي للبطاقة، أي بصناعة البطاقة البلاستيكية ثم تقليد البيانات والرسوم والعلامات الخاصة والتي تتميز بها عن غيرها من البطاقات، ثم يتم تثبيت الشريط الممغنط، وشريط التوقيع كل حسب موضعه الأصلي من جسم البطاقة، ثم يتم أخيرا تزويد الشريط الممغنط بالبيانات والمعلومات الخاصة لكي يجعلها سارية المفعول[4]، وتجدر الإشارة أن المعلومات الموجودة على الشريط الممغنط يتم تزويرها إما بالنسخ أو التشفير[5].

فتتم عملية النسخ بوضع شريط تسجيل الكتروني على البطاقة الأصلية ثم يتم تمرير تيار حراري، من أجل إتمام عملية نسخ البيانات من البطاقة الأصلية إلى الشريط الممغنط، ثم بعد ذلك تأتي مرحلة التزوير، حيث يوضع الشريط الممغنط الذي تم نسخ المعلومات عليه على الشريط الممغنط الفارغ، ومن ثم العمل بنفس خطوات العملية الأولى، وذلك بتمرير التيار الحراري، حيث تنسخ البيانات على الشريط الممغنط الفارغ، وتسمى هذه العملية "بالإدخال"[6].

أما عملية التشفير، فتعتمد على مبدأ العملية التي تقوم بها البنوك أو المؤسسات المالية لترقيم البطاقات ، التي تتمثل في المعادلات الرياضية المعقدة التي يحكمها شفرة خاصة بكل بنك، وأصبح الحصول على هذه الأرقام المشفرة ممكنا من خلال برامج حاسوبية يتم تسويقها عبر الانترنيت، إذ أنه يكفي للحصول على تلك البرامج بالدخول إلى أحد تلك المواقع و تنزيل البرنامج، ثم يتم تشغيله وإدخال رقم بطاقة الدفع الإلكترونية صحيحة ليتولى البرنامج خلق أرقام بطاقات دفع صحيحة ثم يتم استخدامها في أي عملية يدمجها مع بطاقات مقلدة أو تلقينها بأشرطة ممغنطة لبعض البطاقات منتهية الصلاحية[7].

أما بالنسبة للبطاقات الذكية[8] التي تحمل وحدات إلكترونية، فيمكن كذلك نسخ المفاتيح التشفيرية، وكذا الأرصدة المخزنة في البطاقة والمعلومات والبيانات الخاصة بها، حيث تتطلب عملية نسخ البطاقة الذكية المرور بعدة خطوات ومراحل، الأمر الذي يقتضي وجود موارد مالية ضخمة، بالإضافة إلى الاعتماد على أشخاص ذوي الخبرة والكفاءة في هذا المجال. ومن يقوم بعملية نسخ البطاقة الذكية، فعليه الحصول على بطاقة دفع تتمتع بنفس مواصفات البطاقة الأصلية من حيث نوع الرقاقة المغروسة فيها، النظام التشغيلي والبرمجيات التطبيقية من خلال إعادة استخدام بطاقات منتهية الصلاحية أو ملغاة[9].

ب- التزوير الجزئي لبطاقات الدفع الالكتروني:

يقوم التزوير الجزئي على مبدأ وجود بطاقة صحيحة في يد المزور، حيث يستثمر هذا الأخير الجسم الحقيقي للبطاقة وما عليه من هولوغرام ونقوش وطباعة وكتابة أمنية، ثم يقوم بتزوير البطاقة عن طريق صهر ما عليها من أرقام بارزة لبطاقة مسروقة أو منتهية الصلاحية، ومن ثم إعادة قولبتها بأرقام حساب جرى سرقة المعلومات الخاصة بها بطريقة غير مشروعة، أو تقليد الشريط الممغنط عن طريق محو ما عليه من بيانات وإعادة تشفيره ببيانات جديدة وصحيحة تم سرقتها، أو إجراء العمليتين معا. كما يمكن أيضا أن يقوم المزور بعملية محو توقيع الحامل الشرعي المثبت على الشريط بصورة آلية أو كيميائية ويضع توقيعه مكانه. أما إذا كانت البطاقة المسروقة مزودة بصورة العميل قد يلجأ المزور إلى التخلص من الصورة أو تغطيتها ووضع صورته أو صورة شخص آخر مكانها إما بالحفر أو اللصق أو الاثنان معا[10].

ثانياً- تزوير الإشعارات والمستندات الخاصة ببطاقات الدفع الالكتروني:

سنتناول فيما يلي حالات تزوير الإشعارات والمستندات الخاصة ببطاقات الدفع الالكتروني من طرف موظف البنك، ثم من طرف التاجر، وأخيرا من قبل العميل حامل بطاقة الدفع.

أ- تزوير الاشعارات والمستندات الخاصة ببطاقات الدفع الالكتروني من طرف موظف البنك:

قد يتفق موظف البنك مع أفراد العصابات الإجرامية على مدهم بدون وجه حق ببيانات بطاقات الائتمان الصحيحة والمتداولة، وذلك لاستخدامها في تقليد أو اصطناع هذه البطاقات، ولا شك أن موظف البنك في هذه الحالة يكون دوره ا لإمداد بالمعلومات، أما دور العصابة فيتمثل في اصطناع البطاقة المزورة، فيشكل ذلك عدة جرائم متداخلة، من حيث الإمداد بمعلومات عن حسابات العملاء وتزوير البطاقات والاستيلاء على أموال بدون وجه حق.

وقد يعتمد أيضا موظف البنك إشعارات بيع صدرت استنادا إلى بطاقة وهمية أو مزورة أو منتهية الصلاحية أو ملغاة، وإذا ثبت علمه بوجود حالة من هذه الحالات فإن الأمر يشكل جريمة تزوير[11]. أضف إلى ذلك فإن موظف البنك قد يتلاعب شخصيا من خلال اختلاس مبالغ بنكية من البنك في حال تقدم حامل بطاقة الدفع الالكتروني إليه من أجل السحب أو الإيداع، فيقوم بتزوير قيمة المبلغ ويأخذ الفارق لنفسه[12].

وقد يتواطأ موظف البنك مع العميل لاستخراج بطاقة دفع بمستندات مزورة، حيث تبدو البطاقة سليمة، ولكن يتم استخراجها ببيانات ومستندات مزورة، ويستفيد صاحب البطاقة وموظف البنك بقيمة المبالغ الموجودة برصيد البطاقة، حيث يشمل هذا الاعتداء جريمة سلب أموال البنك والاستيلاء عليها دون وجه حق وتزوير البيانات والمستندات المقدمة[13].

ب- تزوير الإشعارات والمستندات الخاصة ببطاقات الدفع الالكتروني من طرف التاجر:

يقوم بعض التجار بالتلاعب باستخدام الماكينة اليدوية عن طريق شراء إشعارات شراء من تجار آخرين مطبوع عليها أرقام بطاقات مزورة لتحصيل الأموال من البنك دون وجه حق، أو طباعة أرقام بطاقات متعاملين معهم على فواتير خيالية بعد مغافلة العميل، وكذلك تقديم فواتير مطبوع عليها أرقام بطاقات عملاء وأرقام وتواريخ رغم إخطار التاجر بسرقتها[14]. وقد يقوم التاجر بإقناع العميل صاحب البطاقة بعد أن أخذ منه البطاقة ومررها بالماكينة الالكترونية بأن هذه الأخيرة بها عطل، ويجب تمرير البطاقة مرة أخرى في قارئة البطاقات حتى تتم العملية، وبذلك يكون التاجر قد أخذ موافقتين على البطاقة وبعمليتين مختلفتين، وبعد ذلك يقوم بتقليد توقيع حامل بطاقة الدفع الالكتروني على الإشعار الثاني الذي لم يوقع عليه العميل ويرسلها إلى البنك للتحصيل[15].

كما أنه قد يتواطأ التاجر مع حامل البطاقة، ويتم ذلك من خلال قيام حامل البطاقة بإجراء عمليات شراء وهمية بالاتفاق مع التاجر مقابل نسبة من قيمة الفاتورة يحصل عليها التاجر ويحصل ذلك في الغالب عند استيفاء الرصيد الشهري للبطاقة وبعدها يقوم التاجر بالحصول على قيمة الفاتورة من البنك مصدر البطاقة[16].

أضف لما سبق فإن التاجر قد يتواطأ مع الغير، بالسماح له باستخدام ماكينة البيع بالتجزئة المسلمة إليه من طرف البنك المصدر للتعامل بالبطاقات المزورة، وذلك مقابل نسبة من قيمة الصفقة التجارية، أو يقوم بتسليم صور لإشعارات البيع التي يدون بها أرقام بطاقة الدفع الالكتروني للعصابات الإجرامية حتى يتمكنو ا من استخدامها في تزوير البطاقات[17].

ج- الحصول على بطاقة الدفع الالكتروني بمستندات مزورة:

إن حصول الحامل على بطاقته يتم طبقا للقواعد المعمول بها والإجراءات التي ينص عليها مصدر البطاقة وحسب الأوراق والمستندات المطلوبة بشرط أن تكون كلها صحيحة وليست مخالفة للحقيقة، يفصح من خلالها عن اسمه ولقبه وعنوانه وموقفه المهني وحالته المادية وتوقيعه، لكن قد يقوم الحامل الذي سيحصل على البطاقة بتقديم مستندات هوية مزورة للمصدر ولا يكتشف هذا الأخير التزوير في حينه، وبذلك يحصل العميل على بطاقة دفع صحيحة ولكنها تحمل بيانات ومعلومات مزورة لا تخص مقدم الطلب إذ تسمى بالبطاقة المنتقصة، ويستخدم تلك البطاقة لإجراء عمليات سريعة ومتتالية ويمتنع عن الدفع فيرجع البنك المصدر عليه فلا يجده، فيضطر إلى دفع المستحقات الناتجة عن استعمال طالب البطاقة بمستندات مزورة، وهذا ما دفع مسؤولي مؤسسة الفيزا كارد إلى القول بأن المستندات المزورة للحصول على البطاقة الائتمانية هي الصداع الذي تعاني منه هذه الصناعة.

كما أن هناك نوعا آخر من الأساليب غير المشروعة التي يلجأ إليها بعض حاملي البطاقات الملغاة نتيجة لعدم الاستعمال الجيد للبطاقة في الولايات المتحدة الامريكية، إذ قد يرغب أحدهم في الحصول على بطاقة جديدة ولكن تاريخه الائتماني لدى جهات إصدار البطاقات يحول دون ذلك، فيلجأ إلى بعض العصابات الإجرامية والتي تطلق على نفسها "عيادات الإصلاح الائتماني"، والتي تحصل على مبالغ مالية تصل إلى 2000 دولار، حتى تمكن طالب البطاقة من استخراج بطاقة ائتمان دون اعتراض البنك المصدر، وذلك بعد تزوير المستندات التي تدل على سوء استخدامه للبطاقة من قبل[18].

المحور الثاني

أشكال التعاون الدولي لمكافحة جرائم تزوير بطاقات الدفع الإلكتروني

لقد أدى الانتشار الواسع لاستخدام بطاقات الدفع الإلكتروني إلى الاحتراف في إساءة استخدامها والتلاعب فيها، وصاحب ذلك جملة من التحولات على جرائم التزييف والتزوير سواء في الأساليب والطرق، أو في المحتوى والمضمون، الأمر الذي يشكل تهديدا مباشرا وفوريا وسريعا للاقتصاد العالمي و المحلي وحقوق الأفراد بغض النظر عن موقعهم في العالم، وقد نبه مؤتمر الأنتربول الثامن المنعقد في أتاوا بكندا عام 1992 إلى تفاقم مخاطر جريمة بطاقة الدفع الالكتروني وإلى عالميتها، حيث يتم إعداد وتصنيع البطاقات المزورة في دولة بينما تجمع المعلومات اللازمة عن البطاقة الصحيحة من دولة إلى دولة، ويجري ترويج البطاقات المزورة في مكان ثالث من العالم[19]، وفي المقابل أثبت الواقع العملي أن الدولة لا تستطيع بمجهودها المنفرد القضاء على هذا النوع الحديث من الجريمة، لذلك أصبحت الحاجة ماسة إلى وجود كيان دولي يأخذ على عاتقه القيام بهذه المهمة، وسنعرض فيما يلي دور المنظمات الدولية والاتفاقيات المنبثقة عنها في مكافحة جرائم تزوير بطاقات الدفع الإلكتروني.

أولاً- المنظمة الدولية للشرطة الجنائية (الإنتربول)[20]:

تعود نشأة المنظمة الدولية للشرطة الجنائية إلى المؤتمر الدولي الثاني الذي عقده الدكتور "جوهانو سويرا" مدير شرطة فيينا، وذلك في الفترة 3-1923/09/7م، الذي ضمن مندوبي تسعة عشر دولة، وتمخض عنه ولادة اللجنة الدولية للشرطة الجنائية، ومقرها فيينا، للتعاون بين أجهزة الشرطة من أجل التعاون في مكافحة الجريمة[21].

وفي بروكسل ببلجيكا عقد مؤتمر في الفترة من 6-1946/06/9م، ولقد دعا إليه المفتش العام للشرطة البلجيكية "لوفاج"، وبموجبه تم إحياء اللجنة الدولية للشرطة الجنائية، ونقل مقرها إلى باريس بفرنسا، وتم تشكيل لجنة تنفيذية من خمسة أعضاء برئاسة المفتش العام للشرطة البلجيكية "لوفاج"، وغير اسمها ليصبح المنظمة الدولية للشرطة الجنائية، ثم انتقلت المنظمة لمقرها السابق في (سان كلود)، ليصبح مقرها الجديد رسميا في مدينة (ليون) الفرنسية عام 1989.

وتعد من بين أهم المنظمات الدولية الناشطة في مجال مكافحة الجريمة، نظرًا لما تقدمه من إمكانيات وضبط مرتكبي الجرائم على اختلاف أنواعها أينما وجدوا وتسليمهم إلى الهيئات المختصة بغية محاكمتهم، ويعتبر الإجرام المالي والمرتبط بالتكنولوجيا المتقدمة من أهم الجرائم التي يجري التركيز عليها

حاليًا من طرف هذه المنظمة. أما بالنسبة لدور المنظمة الدولية للشرطة الجنائية في مواجهة جرائم تزوير بطاقات الدفع الإلكتروني، فنجد أن السكرتارية العامة الخاصة بها، نظمت أول مؤتمراتها الدولية بخصوص الاحتيال والغش الذين يهددان نظام بطاقات الدفع الإلكتروني في أكتوبر 1994 والذي نتج عنه توصيتان هامتان هما[22]:

التوصية الأولى: على الدول الأعضاء مراجعة تشريعاتها وقوانينها الخاصة ببطاقات الدفع الإلكتروني، بما يضمن تجريم تصنيع أو امتلاك البطاقات المزورة، أو امتلاك معلومات غير قانونية أو تم الحصول عليها بطريقة غير مشروعة واستخدامها في إدخالها في نظام بطاقات الدفع الإلكتروني.

التوصية الثانية: إنشاء مجموعات عمل بوليسية من خبراء الاحتيالات الدولية التابعين لبوليس هونج كونج والشرطة الكندية والخدمة السرية الأمريكية وخدمة الاستخبارات القومية الجنائية لنيوزيلاند أو مندوبين من منظمات بطاقات الدفع الإلكتروني، لمكافحة هذه النوعية من الجرائم، والتقوا جميعًا في شهر فبراير 1995، وتم وضع الأسس الخاصة بتبادل المعلومات للحد من هذا الجرائم.

وفي الإطار ذاته قام الإنتربول بتوقيع خمس اتفاقيات مع المنظمات الراعية للبطاقات، وهي أمريكان إكسبريس وديسكفري، إيروباي أنترناشيونال، وماستر كارد الدولية، والفيزا الدولية، وذلك بهدف التعاون الوثيق في مجال جرائم بطاقات الدفع الإلكتروني عام 1999[23].

ثانياً- المنظمة الدولية لضباط الجرائم المالية[24]:

تعتبر هذه المنظمة منظمة دولية غير ربحية تسعى لتوفير الخدمات وتوفير البيئة التي من خلالها يتم جمع المعلومات حول الاحتيال المالي وطرق التحقيق والحماية المالية، وقد تم إنشاء هذه المنظمة عام 1986، عن طريق التعاون بين 68 محققًا دوليا مختصين في جرائم الأموال التي تم من خلالها إنشاء منظمة دولية لضباط جرائم بطاقات الائتمان.

ومن عام 1996 وهذه المنظمة تمنح عضويتها العادية لضباط الشرطة ومحققي مؤسسات إصدار البطاقات، وخبراء مكافحة الاحتيال بشتى أنواعه، وتتيح عضوية هذه المنظمة لأعضائها الحصول على المعلومات السرية الخاصة بالجرائم المالية الدولية والمجرمين الدوليين، وترسل إنذارات لأعضائها بالأماكن المعرضة لهذه الجرائم، كما تتيح للعضو الدخول على شبكات الحاسب الآلي التي تخص الجرائم المالية[25].

وتعمل هذه المنظمة على تبادل المعلومات بين أعضائها، بهدف الإنذار المبكر لأحدث أساليب ارتكاب الجريمة المالية، والتعرف على العصابات المتخصصة في النشاط الإجرامي المتخصص في جرائم الأموال بشتى صوره، ورصد عناصرها، ووضعهم تحت المراقبة في حالة دخولهم لبلادهم وضبط مرتكبيها طبقًا لتشريع كل دولة[26].

ثالثاً- المجلس الاقتصادي والاجتماعي للأمم المتحدة:

المجلس الاقتصادي والاجتماعي هو أحد مجالس الأمم المتحدة، وقد أنشأه ميثاق الأمم المتحدة في عام 1945، كجهاز رئيسي لتنسيق الأنشطة الاقتصادية والاجتماعية للأمم المتحدة والوكالات المتخصصة،

حيث يتألف من 54 عضوًا من أعضاء الأمم المتحدة، ينتخب 18 عضوًا منهم كل عام من قبل الجمعية العامة لمدة ثلاث سنوات وليس لأي دولة عضوية مستمرة في المجلس.

ومن بين أهم القرارات الصادرة عنه نذكر القرار رقم 39/2013 المعنون "التعاون الدولي على منع الاحتيال الاقتصادي والجرائم المتصلة بالهوية والتحقيق فيها وملاحقة مرتكبيها قضائيًا ومعاقبتهم"، ولقد شجع المجلس الاقتصادي والاجتماعي من خلاله الدول الأعضاء على النظر في اعتماد استراتيجيات وطنية لمنح الجرائم المتصلة بالهوية والتحقيق فيها وملاحقة مرتكبيها قضائيًا ومعاقبتهم وتنفيذها، بما يشمل إقامة شراكات بين القطاعين العام والخاص والاستفادة منها في التصدي للجرائم المتصلة بالهوية.

كما طلب المجلس في قراره من مكتب الأمم المتحدة المعني بالمخدرات والجريمة مواصلة جهوده، بالتشاور مع لجنة الأمم المتحدة للقانون التجاري الدولي، لتعزيز التفاهم وتبادل الآراء والخبرات بين مختلف أصحاب المصلحة، وخاصة كيانات القطاعين العام والخاص، بشأن الجرائم المتصلة بالهوية، وطلب منه أيضا مواصلة التعاون مع سائر المنظمات الدولية والمنظمات الحكومية الدولية والمؤسسات الأكاديمية الأخرى العاملة في هذا المجال عن طريق تمكينها من المشاركة والمساهمة بنشاط في العمل الذي سيضطلع به فريق الخبراء الأساسي المعني بالجرائم المتصلة بالهوية.

وبالاطلاع على تقرير الأمين العام[27] الذي قدمه إلى لجنة منع الجريمة والعدالة الجنائية في دورتها الثالثة والعشرين عن تنفيذ القرار 39/2013 ، نجده يتضمن معلومات عن، التي كانت الدول الأعضاء قد وافت المنظمة بمعلومات ومواد ذات صلة بتنفيذ قرار المجلس الاقتصادي والاجتماعي، ونذكر منها الصين التي أبدت أنها تعمل بهمة ونشاط في مجال التعاون الدولي من خلال تبادل المعلومات بهدف مكافحة الجرائم عبر الوطنية المتصلة باستخدام البطاقات المصرفية مع الدانمارك وكندا والمملكة المتحدة لبريطانيا العظمى، وإيرلندا الشمالية والولايات المتحدة، وقدمت الصين لنفس الجهة بعض من الخطط الرامية إلى توسيع نطاق التعاون على إنفاذ القوانين مع مزيد من البلدان والمناطق في بعض المجالات المتعلقة بالجرائم المتعلقة بالبطاقات المصرفية نذكر منها ما يلي:

- تعزيز تبادل المعلومات الاستخبارية، خاصة من خلال توثيق أواصر التعاون في التحقيق في الجرائم عبر الوطنية المتعلقة باستخدام البطاقات المصرفية وإبلاغ النظراء الأجانب بالقضايا المصرفية عبر الوطنية المشتركة ذات الصلة في الوقت المناسب، واطلاعهم على معلومات مفصلة عن التحقيقات الجارية بشأنها وتقديم تقارير سنوية تضم معلومات عن الجوانب الوطنية العامة للقضايا المصرفية عبر الوطنية.

- إقامة نظام لتبادل القوائم السوداء للمشتبه فيهم في الجرائم المتعلقة باستخدام البطاقات المصرفية، وقد وضعت مكاتب التحقيقات التابعة لوزارة الأمن بالفعل قائمة سوداء بالمشتبه فيهم في جرائم الاحتيال المصرفي واقتراح تبادل القوائم السوداء ذات الأهمية المشتركة التي تتضمن أسماء المشتبه فيهم من مرتكبي الجرائم المالية مع قوات الشرطة الأجنبية سنويًا من أجل تسهيل توفير المعلومات لسلطات إنفاذ القوانين.

- التوسع في تبادل الزيارات والمعلومات والخبرات والعمل بجد على توفير أنشطة تدريبية متعددة الجوانب، ويمكن أن تشمل هذه الأنشطة التدريبية تبادل المعلومات عن النظم القانونية وآخر أساليب ارتكاب الجرائم المتصلة باستخدام البطاقات المصرفية وتبادل الخبرات في مجال مكافحة الجرائم المتصلة بالهوية.

رابعاً- اتفاقية بودابست بشأن مكافحة الجريمة الإلكترونية:

لقد حرص مجلس أوربا على التصدي للاستخدام غير المشروع للحاسبات وشبكات المعلومات، وتجلى ذلك في توقيع أول اتفاقية دولية بشأن الأفعال الإجرامية التي تتم ضد نظم الحاسب الآلي ونظم الاتصالات في العاصمة المجرية بودابست في 23 نوفمبر 2001[28]، حيث وقعت عليها 26 دولة من أعضاء المجلس الأوروبي إضافة إلى كندا، واليابان، وجنوب إفريقيا، والولايات المتحدة الأمريكية[29]. لإدراك هذه الدول أن مثل هذه النوعية من الجرائم لا تستطيع أي دولة مواجهتها بمفردها، مهما سنت من القوانين وشددت من العقوبات، لاعتبارها من الجرائم العابرة للحدود.

واستنادًا إلى مواد الاتفاقية، فهي تلزم الدول الأعضاء فيها باتخاذ التدابير التشريعية والإجراءات الملائمة لمكافحة جرائم المعلوماتية وخطورتها على الدول خصوصا في ظل شيوع شبكة المعلومات و الأنترنت، وتضمنت هذه الاتفاقية عدة مواد تناولت أوجه الإجرام المعلوماتي، إذ عرفت المادة 07 منها التزوير بأنه: «إدخال أو إفساد أو تعطيل أو محو أو شطب عن قصد وبدون وجه حق»[30]، وترمي هذه المادة إلى إنشاء جريمة موازية لتزوير الوثائق الملموسة، وتهدف إلى سد الثغرات في القانون الجنائي المتعلقة بالتزوير التقليدي، والتي تتطلب قراءة بصرية للبيانات أو التصريحات الورقية، والتي لا تنطبق على البيانات المخزنة إلكترونيا. ويستشف من خلالها أن التزوير المعلوماتي يتم بالإدخال، أو التعطيل أو الإفساد أو المحو أو الشطب، إذا ارتكب بقصد وبدون وجه حق في المعطيات الالكترونية، وكذلك الحصول على معطيات غير صحيحة بهدف استعمالها بطريق غير مشروع كما لو كانت تلك الوسائط صحيحة وأصلية. ويلاحظ أن الاتفاقية بينت الأفعال التي تشكل تزويرا دون التطرق للتزوير بطريق التغيير، رغم ذلك فإنه يمكن تطبيقها على تزوير بطاقات الدفع.

خامساً- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2012:

لقد تم توقيع الاتفاقية العربية لمكافحة جرائم تقنية المعلومات من طرف الدول العربية، وذلك بعد اقتناعهم بضرورة تعزيز التعاون فيما بينها لمكافحة هذا النوع الحديث من الجرائم التي تهدد أمنها ومصالحها وسلامة مجتمعاتها، وأيضًا بضرورة الحاجة إلى تبني سياسة جنائية مشتركة تهدف إلى حماية المجتمع العربي ضد جرائم التقنية. حيث تهدف هذه الاتفاقية إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، لدرء أخطار هذه الجرائم حفاظًا على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها[31].

وبعد تحليل نصوص الاتفاقية العربية نجد أنها جرمت الاعتداءات الواقعة على البيانات والمعلومات بصفة عامة، وجرمت التزوير المعلوماتي بصفة خاصة، إذ نصت المادة 10 منها على تعريف

التزوير المعلوماتي على النحو الآتي: «استخدام وسائل تقنية المعلومات من أجل تغيير الحقيقة في البيانات تغييرًا من شأنه إحداث ضرر، وبنية استعمالها كبيانات صحيحة».

كما تضمنت المادة 18 من الاتفاقية مسألة الاستخدام غير المشروع لأدوات الدفع الإلكترونية التي تعتبر بطاقات الدفع الإلكتروني أحد صورها التي جاء نصّها كما يلي: «الاستخدام غير المشروع لأدوات الدفع الإلكتروني:

1- كل من زور أو اصطنع أو وضع أي أجهزة أو مواد تساعد على تزوير أو تقليد أي أداة من أدوات الدفع الإلكتروني بأي وسيلة كانت.

2- كل من استولى على بيانات أي أداة من أدوات الدفع واستعملها أو قدمها للغير أو سهل للغير الحصول عليها.

3- كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في الوصول بدون وجه حق إلى أرقام أو بيانات أي أداة من أدوات الدفع.

4- كل من قبل أداة من أدوات الدفع المزورة مع العلم بذلك»، إذ يلاحظ من هذا النص أن الاتفاقية تصدت لتجريم أوجه الإجرام المعلوماتي المعاصر الذي يستهدف الأمن الاقتصادي والمصرفي للدول العربية التي تستخدم وسائل الدفع الحديثة، ومن بينها بطاقات الدفع الإلكتروني، وأقر حمايتها ضد أي شكل من أشكال التزوير أو الاصطناع أو التقليد.

المحور الثالث

وسائل التعاون الدولي لمكافحة جرائم تزوير بطاقات الدفع الإلكتروني

إذا كان التعاون الدولي بحد ذاته يتمركز على المنظمة الدولية للشرطة الجنائية، والمنظمة الدولية لضباط الجرائم المالية، ومختلف الاتفاقيات والمعاهدات، فإن ذلك غير كاف لتحقيق مساعي الدول في مكافحة الجرائم المرتبطة بتزوير البطاقات الإلكترونية، بل الأمر يحتاج إلى استخدام عدة وسائل للنهوض بمستوى مكافحة الجرائم الإلكترونية بصفة عامة، وجرائم تزوير بطاقات الدفع الإلكتروني بصفة خاصة، حيث يشمل هذا التعاون الوسائل الإدارية والوسائل الشرطية، والوسائل القانونية في مجال الجريمة، ونخص بالذكر هذا النوع من الجرائم المستحدثة التي تمس الاقتصاد القومي للدول، حيث أن التعاون الدولي بوسائله المتعددة لا يقتصر على جرائم تزوير بطاقات الدفع بل يشمل الجرائم جميعها أيا كان نوعها وطريقة ارتكابها، وسوف نتناول هذه الوسائل على النحو التالي:

أولاً- الوسائل القانونية:

إن هذه الوسائل يحكمها قانون الإجراءات الجزائية في كل دولة، من حيث الاختصاص والتنفيذ، بما يتماشى مع مبدأ إقليمية القانون الجنائي، والذي يقضي بعدم جواز ممارسة أي دولة اختصاصها الجنائي خارج حدودها الإقليمية، لأن ذلك يعد مساسًا لسيادة الدولة الأخرى. وبالتالي فإن هذه الإجراءات القانونية لا يمكن أن تتم إلا بموافقة كل دولة عل إجراء الدولة الأخرى بناء على طلب أو اتفاق مسبق

بينهما، وتتم هذه الاتفاقيات بالطرق الدبلوماسية، وأي خروج عن قواعد الإجراءات الجنائية دون اتفاق أو إذن مسبق بين الدول المعنية يكون باطلاً وغير قابل للتنفيذ[32].

ونظرا للتطور السريع في مجال تكنولوجيا الكمبيوتر والإنترنت وشعور الدول الأوروبية بأهمية إعادة النظر في الإجراءات الجنائية في هذا المجال فقد أصدر المجلس الأوروبي التوصية رقم 13/95 في 11 سبتمبر 1995 في شأن مشاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات [33] لحث الدول الأعضاء على مراجعة قوانين الإجراءات الجنائية الوطنية لتلائم التطور في هذا المجال وأهم ما ورد فيها هو:

- أن توضح القوانين إجراءات تفتيش أجهزة الكمبيوتر وضبط المعلومات التي تحويها مراقبة المعلومات أثناء انتقالها.

- تطبق إجراءات المراقبة والتسجيل في مجال التحقيق الجنائي في حالة الضرورة في مجال تكنولوجيا المعلومات.

- يجب تعديل القوانين الإجرائية بإصدار أوامر لمن يحوز معلومات (برامج-قواعد-بيانات) تتعلق بأجهزة الكمبيوتر بتسليمها للكشف عن الحقيقة.

- يجب تطوير وتوحيد أنظمة التعامل مع الأدلة الإلكترونية، وحتى يتم الاعتراف بها بين الدول المختلفة، ويتعين أيضًا تطبيق النصوص الخاصة بالأدلة التقليدية على الأدلة الإلكترونية.

ولعل من أبرز المعاهدات الدولية المنظمة للمساعدة الجنائية على النطاق الدولي نذكر ما يلي:

- المعاهدة النموذجية للمساعدة المتبادلة في المسائل الجنائية:

وتشمل هذه المعاهدة الحصول على شهادات، أو بيانات، وعمل التحريات، وأعمال الضبط والتفتيش، وفحص الأشياء والأماكن ومعاينتها، وتوفير لمستندات والوثائق ونسخها، وكل ما يتطلب الحصول على البيانات، سواء كانت هذه البيانات مالية أو إدارية أو شخصية أو اجتماعية، وأيضًا عائدات أو متحصلات الجريمة من أموال.

- المعاهدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية:

وتشمل هذه المعاهدة تسهيل إجراءات إقامة الدعوى الجنائية، والحكم فيها إذا ما وقعت الجريمة طبقًا لقانون دولة ما، واقتضى الأمر أن ترفع الدعوى الجنائية في دولة أخرى عن هذا الفعل[34].

- معاهدة بودابست بشأن مكافحة جرائم نظم المعلومات والاتصالات:

وفي إطار المساعدة الجنائية نصت المعاهدة في المادة **24** على شروط تسليم المجرمين، كما نصت المادة منها**25** على المبادئ العامة المتعلقة بالمساعدة حيث ورد فيها أن تتفق الأطراف على أوسع نطاق للتعاون بهدف إجراء التحقيقات أو الإجراءات المتعلقة بالجرائم الجنائية للشبكات والبيانات المعلوماتية، وجمع الأدلة في الشكل الإلكتروني لهذه الجرائم.

ونصت **الفقرة الثالثة** من المادة **25** على أنه يمكن لأي طرف في الحالات الطارئة أن يوجه طلبًا للمعاونة أو للاتصالات المتعلقة بها عن طريق وسائل الاتصال السريعة مثل الفاكس أو البريد الإلكتروني، مع مراعاة استيفاء هذه الوسائل الشروط الكافية المتعلقة بالأمن والسرية، مع تأكيد رسمي

لاحق إذا اقتضت الدولة المطلوب منها المساعدة في ذلك، وتقوم الدولة المتلقية للطلب بالرد عن طريق إحدى وسائل الاتصال السريعة[35].

- المعاهدة الأوروبية لمكافحة جرائم الإنترنت:

لقد ألزمت هذه المعاهدة الدول المعنية بوضع الحد الأدنى من القوانين الضرورية للتعامل مع جرائم التقنية العالية [36].

ثانياً- الوسائل الشرطية:

تبرز هذه الوسائل من خلال التعاون بين الشرطة الوطنية والشرطة الدولية بخصوص الأمور التي تتعلق بكيفية اتصال الأجهزة بعضها ببعض، ولنفس الغرض قامت الشرطة الجنائية الدولية الأنتربول بإنشاء مكاتب مركزية وطنية في إقليم كل دولة عضو في الأنتربول، وتعد هذه المكاتب كجهاز من الأجهزة المكونة لها، تحقيقًا لفاعلية التعاون الدولي لمكافحة الجريمة، ويعد مكتب المنظمة هو حلقة الاتصال بين إدارات الشرطة في الدولة والمكاتب الدولية المماثلة في الدول الأخرى، والأمانة العامة للإنتربول[37]، وتتمثل المهمة الرئيسية لهذه المراكز في تسهيل مرور الرسائل من خلال نظامين هما: نظام الاتصال المركزي، ونظام الاتصال اللامركزي، حيث تجري من خلال النظام المركزي الاتصالات العالمية للشرطة من خلال الجمعية العامة واللجنة التنفيذية بواسطة السكرتارية العامة، أما النظام اللامركزي فيسمح بالاتصال المباشر بين أجهزة الشرطة، ويتيح إمكانية القيام بمختلف الاتصالات غير الرسمية عبر الحدود الدولية[38].

ثالثاً- الوسائل الإدارية:

تتجسد الوسائل الإدارية في تبادل الخبرات بين الدول في مجال جرائم تزوير بطاقات الدفع الإلكتروني، وكيفية ضبطها والوصول إلى مرتكبيها، فتتم الزيارات المنظمة والمتبادلة بين الدول، وتعقد الندوات والمناقشات مع الأجهزة المختصة بكل دولة، وكذلك تنظيم الدورات التدريبية، وتنظيم الندوات والملتقيات الدولية، التي تنبثق منها الاتفاقات والمعاهدات بين الأطراف[39]. حيث تشكل المؤتمرات الدولية عاملا مهمًا لمكافحة الجريمة والمجرمين، وقد تعقد المؤتمرات والاجتماعات لمكافحة جرائم تزوير بطاقات الدفع الإلكتروني، لتنظيم كيفية ضبطها، وتحديد العقوبات ضد مرتكبيها، وتعقد المؤتمرات عادة بصفة دورية، أو لمرة واحدة سنويًا أو أكثر من ذلك، فنجد مثلا منظمة الأمم المتحدة عقدت تسعة مؤتمرات حتى سنة 1995[40].

المحور الرابع

صعوبات التعاون الدولي في مجال مكافحة جرائم بطاقات الدفع الالكتروني

رغم المجهودات الفردية والثنائية ومساعي المنظمات الدولية التي تهدف إلى تحقيق التعاون الدولي لمكافحة الجريمة الإلكترونية بكل أنواعها، والحفاظ على أمن الدول الجنائي والاقتصادي، إلا أنه لازالت هناك مجموعة من المعوقات والصعوبات التي تعرقل وتقلص المجهودات الرامية إلى وضع حد لجرائم تزوير بطاقات الدفع الإلكتروني، ويمكن تلخيص هذه الصعوبات في العناصر التالية:

أولاً- عدم وجود نموذج موحد للنشاط الإجرامي:

يتضح من خلال الأنظمة القانونية للدول المتعلقة بمواجهة الجرائم المعلوماتية عدم وجود اتفاق عام مشترك بين الدول حول نماذج إساءة استخدام نظم المعلومات وشبكة الإنترنت الواجب تجريمها[41].

ثانياً- تنوع واختلاف النظم القانونية الإجرائية:

يلاحظ عدم وجود تنسيق فيما يتعلق بالإجراءات الجنائية المتبعة بخصوص الجريمة المعلوماتية بين الدول المختلفة خاصة ما تعلق بها بأعمال الاستدلال أو التحقيق، فنجد أن طرق التحري والتحقيق والمحاكمة التي تثبت فائدتها وفاعليتها في دولة ما قد تكون عديمة الفائدة في دولة أخرى، أو قد لا يسمح بإجرائها[42]. أضف إلى ذلك مشكلة البيانات المعلوماتية التي تقف عائقًا أمام إجراءات التحقيق الجنائي والبحث عن دليل الإدانة، في ظل قيام الجاني بتشتيت المعلومات والمستندات رغبة منه في عدم الإبقاء على أي دليل إثبات.

ثالثاً- مشكلة الاختصاص في جرائم تزوير بطاقات الدفع الإلكتروني[43]:

بما أن جرائم تزوير بطاقات الدفع الإلكتروني تعتبر من قبيل جرائم الإنترنت العابرة للحدود، فإنه تثار مشكلة الاختصاص على المستوى الدولي بسبب اختلاف التشريعات والنظم القانونية، فقد يحدث أن ترتكب الجريمة في إقليم دولة معينة من قبل أجنبي، فهنا تكون الجريمة خاضعة لاختصاص الدولة الثانية على أساس مبدأ الاختصاص الشخصي في جانبه، وقد تكون هذه الجريمة من الجرائم التي تهدد أمن وسلامة دولة أخرى فتدخل حينها في اختصاصها استنادًا لمبدأ العينية. كما قد تثار فكرة تنازع الاختصاص القضائي في حالة تأسيس الاختصاص على مبدأ الإقليمية، لذلك تعتبر مسألة الإقليمية من أهم الصعوبات التي تعترض ماهية التعاون الدولي في سبيل مكافحة الجريمة والإبرام خاصة في حال تمسك الدولة بهذا الإجراء واعتبرته مساسًا صارخًا بسيادتها الوطنية.

رابعًا- التجريم المزدوج:

يعتبر نظام تسليم المجرمين من أقدم صور التعاون القضائي الدولي في المواد الجنائية، وهو مشهود له بكونه واحدًا من أنجع وسائل هذا التعاون في مكافحة الجريمة، وبمقتضاه تقوم دولة بتسليم شخص موجود في إقليمها لسلطات دولة أخرى، تطالب بتسليمه إليها لمحاكمته أو لتنفيذ عقوبة صادرة في حقه، على أساس وجود اتفاقية ثنائية بين الدولتين أو اتفاقية إقليمية[44].

ومن بين المعوقات التي تعترض تطبيق نظام تسليم المجرمين هو إعمال قاعدة التجريم المزدوج، ومفاد هذه القاعدة أن يكون الفعل المطلوب التسليم من أجله خاضعًا للتجريم والعقاب في قوانين كلتا الدولتين، الطالبة والمطلوب منها التسليم[45]، وتجدر الإشارة إلى أن هذا الشرط يعتبر بديهيًا، لأنه من غير المعقول أن يكون الفعل المنسوب للشخص المطلوب تسليمه مجرمًا في تشريع الدولة الطالبة، إذ لا يتصور طلبها محاكمة هذا الشخص أو تنفيذ العقوبة عليه، إذا لم يكن الفعل مجرمًا في قانونها، استنادًا لمبدأ جزائي ثابت وهو "لا جريمة ولا عقوبة إلا بنص"[46]، ويجب أن يكون هذا التجريم ساريًا وقد ارتكب الفعل، ولا يجوز أن يكون القانون لاحقًا للفعل المجرم طبقًا لمبدأ عدم رجعية القانون الجنائي[47]، أما

بالنسبة للجرائم المعلوماتية وجرائم تزوير بطاقات الدفع خاصة، فنجد معظم الدول لا تجرم هذا النوع من الجرائم، بالإضافة إلى أنه من الصعوبة تحديد فيما إذا كانت النصوص التقليدية لدى الدولة المطلوب منها التسليم يمكن أن تنطبق على الجرائم المتعلقة بتزوير بطاقات الدفع أو لا، الأمر الذي يشكل عائقًا أمام تطبيق الاتفاقيات الدولية في مجال تسليم المجرمين، ويحول بالتالي دون جمع الأدلة ومكافحة مرتكبي هذا النوع من الجرائم.

الخاتمة:

في الختام نخلص إلى القول بأن المساعي الدولية المبذولة للتصدي لجريمة تزوير بطاقات الدفع الالكتروني على وجه العموم، مازالت دون المستوى المطلوب، مقارنة بتعاظم مخاطر هذه الجريمة وعالميتها، ولن يستقيم الأمر إلا بإيجاد أساس تشريعي موحد، وتصور شامل لمفهوم هذه الجريمة. ومن أجل ذلك ينبغي تكثيف جهود التعاون الدولي والإقليمي لمكافحة هذه الجرائم، ولتحقيق ذلك ارتأينا تقديم جملة من الاقتراحات المنبثقة عن التوصيات والمبادئ التي نصت عليها العديد من المنظمات والمعاهدات المتعلقة بالجرائم المعلوماتية بصفة عامة:

- تبادل المعلومات عن طريق إنشاء مكاتب دولية وإقليمية، وإنشاء قسم خاص داخل إدارات مكافحة التزييف والتزوير بوزارات الداخلية العربية، ويكون متخصصا في جرائم تزوير بطاقات الدفع الالكتروني، وتدريب العاملين به على أساليب التحري والضبطية في هذا النوع المميز من القضايا.

- العمل على تكوين فرق دولية من الضبطية القضائية وقضاة متخصصين في هذا النوع من الجرائم، ومدهم بكافة الوسائل المادية والتقنية اللازمة لأداء المهام المنوط بها.

- إنشاء قاعدة بيانات محلية ودولية، تتضمن المعلومات الكافية عن قضايا تزوير بطاقات الدفع، وأهم الخواص التي تتميز بها أنواع البطاقات التي جرى تزييفها أو تزويرها، وأماكنها وتاريخها، وأسماء المتهمين فيها للاستعانة بها في عمليات الربط وتحديد المصدر عالميا وإقليميا.

- تذليل الصعوبات والمعوقات التي تواجه التعاون الدولي في هذا المجال، عن طريق تحديث التشريعات المحلية المتعلقة بالجرائم المعلوماتية عامة، وجرائم تزوير بطاقات الدفع بصفة خاصة، وإبرام اتفاقيات خاصة يراعى فيها هذا النوع من الجرائم.

- ضرورة إبرام اتفاقيات ثنائية أو جماعية يتم فيها توحيد وجهات النظر فيما يتعلق بقواعد الاختصاص القضائي خاصة بالنسبة لجريمة تزوير بطاقة الدفع الالكتروني باعتبارها من قبيل الجرائم العابرة للحدود الوطنية، التي يسهل ارتكابها ويصعب إثباتها.

الهوامش:

(1) حوالف عبد الصمد، النظام القانوني لوسائل الدفع الالكتروني، رسالة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، الجزائر 2014-2015، ص 325.

(2) محمد حماد مرهج الهيتي، الحماية الجنائية لبطاقات الائتمان الممغنطة، دار الكتب القانونية ودار شتات للنشر والتوزيع، مصر، د.س.ن، ص 255.

(3) محمد عبد الرسول خياط، عمليات تزوير البطاقات الائتمانية، مقال مقدم في أعمال ندوة تزوير البطاقات الائتمانية، مركز الدراسات والبحوث، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2002، ص 39.

(4) محمد حماد مرهج الهيتي، مرجع سابق، ص 255-256.

(5) مهند فايز الدويكات، حسين محمد الشبلي، سلسلة الجرائم المالية والمستحدثة "التزوير والاحتيال بالبطاقات الائتمانية"، دار مجدلاوي للنشر والتوزيع، الأردن، 2009، ص 65.

(6) محمد حماد مرهج الهيتي، مرجع سابق، ص 255.

(7) براهمي حنان، جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية، أطروحة دكتوراه، تخصص قانون جنائي، جامعة بسكرة، كلية الحقوق والعلوم السياسية، الجزائر، السنة الجامعية 2014-2015، ص. 273-275.

(8) لقد ظهر جيل جديد من البطاقات تسمى البطاقة الذكية، وهي عبارة عن رقيقة إلكترونية فائقة القدرة على تخزين جميع البيانات والمعلومات الخاصة بحاملها مثل الاسم والعنوان والمصدر لها وأسلوب الصرف والمبلغ المتصرف وتاريخه، وتاريخ حياة العميل المصرفية. لمزيد من التفاصيل راجع: لزعر فتيحة، تنفيذ العقد الإلكتروني، مذكرة ماجستير، فرع العقود والمسؤولية، كلية الحقوق بن عكنون، الجزائر 1، 2010-2011، ص 185-186.

(9) حوالف عبد الصمد مرجع سابق، ص 326.

(10) مهند فايز الدويكات وحسين محمد الشبلي، مرجع سابق، ص 66-67. -محمد حماد مرهج الهيتي، مرجع سابق، ص 254و255و257. - براهمي حنان، مرجع سابق، ص 276-278.

(11) إيهاب فوزي السقا، الحماية الجنائية والأمنية لبطاقات الائتمان، دار الجامعة الجديدة للنشر، د.ب.ن،2007، ص 201.

(12) مهند فايز الدويكات وحسين محمد الشبلي، مرجع سابق، ص 68-69.

(13) إيهاب فوزي السقا، مرجع سابق، ص 201.

(14) معادي أسعد صوالحة، بطاقات الائتمان "النظام القانون وآليات الحماية الجنائية والأمنية –دراسة مقارنة"، المؤسسة الحديثة للكتاب، لبنان، 2011، ص 338.

(15) أيمن عبد الحفيظ، حماية بطاقات الدفع الالكتروني، د.دن، د.ب.ن، 2007، ص 67. – أمجد حمدان الجهني، المسؤولية المدنية عن الاستخدام غير المشروع لبطاقات الدفع الالكتروني، دار المسيرة للنشر والتوزيع والطباعة، الأردن، 2010، ص 346.

(16) مهند فايز الدويكات وحسين محمد الشبلي، مرجع سابق، ص 69.

(17) إيهاب فوزي السقا، مرجع سابق، ص 186.

(18) إيهاب فوزي السقا، مرجع سابق، ص164 وما بعدها. - مهند فايز الدويكات وحسين محمد الشبلي، مرجع سابق، ص 70.

(19) مشار إليه في: رياض فتح الله بصلة، جرائم الاحتيال بالبطاقات الائتمانية وأساليب مكافحتها، مقال مقدم في أعمال ندوة تزوير البطاقات الائتمانية، مركز الدراسات والبحوث، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2002، ص 73-74.

(20) International Criminal Police Organisation (Interpol)

(21) محمد أحمد سليمان عيسى، التعاون الدولي لمواجهة الجرائم الإلكترونية، المجلة الأكاديمية للبحث القانوني، المجلد 14، العدد 02، 2016، الجزائر، ص 53. وانظر: منتصرة سعيد حمودة، المنظمة الدولية للشرطة الدولية الانتربول، دار الفكر الجامعي، مصر، 2008، ص 11.

(22) هاتان التوصيتان مشار إليهما لدى: إيهاب فوزي السقا، المرجع نفسه، ص 508، ومحمد علي سليمان، عباس طالب زروقي، الأساس القانوني لحماية بطاقة الائتمان من التزوير، مقال منشور في مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد 02، 2015، ص 127-128.

(23) معادي أسعد صوالحة، مرجع سابق، ص 507.

(24) International Association of Financial crimes.

[25] معادي أسعد صوالحة، مرجع سابق، ص 507.

[26] إيهاب فوزي السقا، مرجع سابق، ص 515.

[27] تقرير الأمين العام عن الجهود التي تبذلها الدول الأعضاء لتنفيذ قرار المجلس الاقتصادي والاجتماعي 39/2013 والسياسات والتدابير الوطنية في مجالات منع جرائم الاحتيال الاقتصادي والجرائم المتصلة بالهوية والتحقيق فيها وملاحقة مرتكبيها قضائيًا ومعاقبتهم، مقدم للجنة منع الجريمة والعدالة الجنائية، في دورتها الثالثة والعشرون، البند 7، فيينا 12-16أيار/مايو 2014.

[28] تتضمن هذه المعاهدة 48 مادة موزعة على أربعة فصول

1- استخدام المصطلحات، 2- التدابير الواجب اتخاذها على الصعيد المحلي، القانون الموضوعي والقانوني الإجرائي، 3- التعاون الدولي، 4- الأحكام الختامية.

راجع في ذلك: التقرير التفسيري لاتفاقية بودابست بشأن الجريمة الالكترونية الصادرة بتاريخ 22 نوفمبر 2001.

[29] إيهاب فوزي السقا، مرجع سابق، ص 521-522.

[30] محمد علي سليمان، عباس طالب زروتي، مرجع سابق، ص 128.

[31] المادة الأولى من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[32] معادي أسعد صوالحة، مرجع سابق، ص 512.

[33] محمد أحمد سليمان عيسى، مرجع سابق، ص 58 وما بعدها.

[34] إيهاب فوزي السقا، مرجع سابق، ص 520-521.

[35] محمد أحمد سليمان عيسى، مرجع سابق، ص 57-58.

[36] إيهاب فوزي السقا، مرجع سابق، ص 522.

[37] علاء الدين شحاتة، التعاون الدولي لمكافحة الجريمة، إيتراك للنشر والتوزيع، مصر، 2000، ص 173.

[38] علاء الدين شحاتة، المرجع نفسه، ص 112.

[39] عبد المنعم سعيد، أسلوب تحليل الأحداث في العلاقات الدولية، بحث مقدم إلى ندوة البحث الإفريقي في الدراسات السياسية، مركز البحوث والدراسات السياسية، كلية الاقتصاد والعلوم السياسية، جامعة القاهرة، من 17 و1987/12/18، ص 1 وما بعدها.

[40] محمد بدر الدين مصطفى، المفاوضات الدولية، الهيئة العامة للكتاب، مصر، 1991، ص 09 وما بعدها.

[41] عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، 2006، ص 142-143.

[42] محمد أحمد سليمان عيسى، مرجع سابق، ص 60.

[43] معادي أسعد صوالحة، مرجع سابق، ص 514 وما بعدها. أنظر أيضًا: إيهاب فوزي السقا، مرجع سابق، ص 522 وما بعدها.

[44] محمد عبد الله حسين العاقل، النظام القانوني الدولي للجريمة المنظمة عبر الدول، دار النهضة العربية، مصر، 2010، ص 639.

[45] شريف سيد كامل، مكافحة جرائم غسل الأموال في التشريع المصري، دار النهضة العربية، مصر، 2002، ص 183.

[46] لقد نص المشرع الجزائري على هذا المبدأ من خلال نص المادة الأولى من قانون العقوبات كما يلي: «لا جريمة ولا عقوبة أو تدابير أمن بغير قانون» أمر رقم 66-156 مؤرخ في 08 جوان 1966، يتضمن قانون العقوبات، ج. ر. ج. ج، عدد 49، صادرة بتاريخ 11 جوان 1966، معدل ومتمم.

[47] حسن أدربيلة، مكافحة غسل الأموال بين التشريع والتطبيق، دراسة مقارنة في ضوء الاتفاقيات والتقارير الدولية، دار الامان، المغرب، 2014، ص 365.