

الجهود الدولية لمكافحة جريمة التزوير الإلكتروني في إطار التعاون الأمني والقضائي
**International Efforts to Combat Electronic Forgery
within the Framework of Security and Judicial
Cooperation**

تاريخ القبول: 20../..

تاريخ الإرسال: 20../..



Hocine Nesma	حسين نسمة*
جامعة قسنطينة 1 الاخوة منتوري	
University of Constantine 1 – Mentouri Brothers	
nesmahocine@gmail.com	

باحترافية وبوتيرة عالية هذا ما أدى بالدول للاعتماد على التعاون الدولي كضرورة أساسية لمكافحة هذه الجريمة عن طريق التعاون الأمني وكذا عن طريق المساعدة القضائية.

الكلمات الافتتاحية:

التزوير الإلكتروني، التعاون الدولي، التعاون الأمني، تسليم المجرمين.

Abstract:

International cooperation in combating the crime of electronic forgery is considered one of the most important mechanisms adopted by states to confront this crime, hold its perpetrators accountable, and ensure that they do not escape punishment. This is particularly due to the transnational nature of this crime on the one hand, and, on the other hand, its seriousness, as it

ملخص:

يعد التعاون الدولي في مكافحة جريمة التزوير الإلكتروني من أهم الآليات المعتمدة من قبل الدول لمحاربة هذه الجريمة ومساءلة مرتكبيها وضمان عدم افلاتهم من العقاب، خاصة وأن هذه الجريمة تتميز بأنها عابرة للحدود الوطنية هذا من ناحية، ومن ناحية أخرى تتميز بخطورتها لكونها تعتمد في ارتكابها على التطور التكنولوجي والذي يجعلها ترتكب

relies on technological advancement in its commission, which allows it to be carried out professionally and at a rapid pace. This has led states to adopt international cooperation as an essential necessity to combat this crime through security cooperation as well as judicial assistance.

Keywords:

Electronic forgery, international cooperation, security cooperation, extradition of criminals.

مقدمة:

إن التطور التكنولوجي في مجال الاتصال الإلكتروني الذي فرض نفسه في جميع ميادين الحياة، والذي انجر عنه نشأت أنماط مستحدثة من الجرائم التي تسمى بالجريمة الإلكترونية أو الرقمية، يعد من أكبر التحديات التي تواجه العدالة الجنائية ولاسيما أجهزة إنفاذ القانون.

ويرجع السبب في ذلك للتطور المتسارع لشبكة الإنترنت التي ساعدت بشكل رهيب مرتكبي هذه الجرائم مستغلين التسهيلات التي تقدمها هذه الشبكة لارتكاب جرائمهم هذا من جهة، ومن جهة أخرى يتميز هؤلاء المجرمين بدكاء وفوذ وتحكم كبير في هذه الشبكة مما أدى لصعوبة إثبات هذا النوع من الجرائم وكذا صعوبة الكشف عن هويتهم والقبض عليهم.

وهذا تمثل الجرائم الإلكترونية ظاهرة إجرامية ذات طبيعة خاصة بها ترتكب ضمن نطاق المعالجة الإلكترونية للبيانات، فلا تكاد تخلو جريمة من جرائم النظم المعلومات من شكل من أشكال تزوير أو تقليد أو اصطناع توقيع أو كتابة إلكترونية أو استعمال البطاقة الإلكترونية المقلدة (المزورة) مع علمه بذلك أو اصطناع وثائق أو سجلات أو قيود إلكترونية عمدًا أو لإحداث تغيير أو تلاعب في سند واستخدامه للمصلحة الشخصية. وعليه تعتبر جريمة التزوير الإلكتروني من أنواع الغش المعلوماتي الذي نتج عن الثورة المعلوماتية التي أدت إلى ظهور وسائل قادرة على تخزين المعلومات بكميات هائلة أين حلت هذه الوسائل محل الوثائق التقليدية مثل الأوراق والدفاتر، وقد أثبت الواقع أن هذه الأخيرة لا تضاهي الوسائل المعلوماتية، من حيث سعة التخزين وسرعة استرجاع المعلومات وتنظيمها بشكل فعال. وعمليًا وكواجهة هذا النوع من الجرائم كان لابد من التعاون فيما بين الدول للحد من جريمة التزوير الإلكتروني خاصة الواقعة على بطاقات الائتمان وهذا في المجال الأمني الدولي وكذا المجال القضائي الدولي بهدف تسهيل إجراءات الكشف عن هذه الجريمة الخطيرة التي لا تهدد فقط مصلحة الأشخاص بل تتعداهل للمساس بمصلحة الدولة، وكذا في خلق واستحداث أجهزة وتكاثف جهود الدول على المستويين الإقليمي والدولي.

وعليه كيف يساهم التعاون الدولي في مكافحة جريمة التزوير الإلكتروني؟ وللإجابة على هذه الإشكالية تتم اعتماد المنهج الوصفي والتحليلي، كما تم تقسيم الموضوع لمحورين أساسيين هما:

- المبحث الأول: الإطار المفاهيمي لجريمة التزوير الإلكتروني.
- المبحث الثاني: التعاون الأمن والقضائي الدولي لمكافحة جريمة التزوير الإلكتروني.

المبحث الأول: الإطار المفاهيمي لجريمة التزوير الإلكتروني.

نظراً لاختلافها عن جريمة التزوير التقليدية وتميزها بخصائص مختلفة كان لابد من التعرض لتحديد مجموعة المفاهيم الخاصة بها انطلاقاً من تعريفها وتحديد أوقاتها في المطلب الأول ودراسة أنواعها أو صورها في المطلب الثاني وهذا ما نراه من خلال ما يلي:

المطلب الأول: تعريف جريمة التزوير الإلكتروني وأركانها.

حتى يتمكن من تمييز جريمة التزوير الإلكتروني عن الجريمة التقليدية، وجب التعرض لتعريفها في الفقه والقانون هذا من جهة ومن جهة أخرى التعرض لأركانها وهذا فيما يلي:

الفرع الأول: تعريف التزوير الإلكتروني.

سنحاول في هذا الفرع إعطاء التعريف الفقهي والقانوني لجريمة التزوير الإلكتروني وهذا من خلال ما

يلي:

أولاً- التعريف الفقهي لجريمة التزوير الإلكتروني:

تتمثل هذه الجريمة أساساً في المساس العمدي بأنظمة الحاسب الآلي ومكوناته وبرامجه باستخدام أي تقنية حديثة من تقنيات الحوسبة والاتصال حيث يكون الفاعل فيها ملماً بهذه التقنية، ومن شأن هذا السلوك المساس بمصلحة محمية قانوناً والتي تتمثل في الحق في سرية وتكاملية ووفرة وإتاحة المعلوماتية¹. ويعرف التزوير الإلكتروني بأنه تغيير حقيقة في المستندات المعالجة آلياً والمستندات المعلوماتية وذلك بنية استعمالها².

كما عرف التزوير الإلكتروني كذلك بأنه: "التزوير الإلكتروني يختلف عن التزوير التقليدي، حيث يتضمن التزوير المعلوماتي إتلاف المعلومات أو تشويهها أو تحريفها بالتعديل سواء بالحذف أو الإضافة، إضافة إلى أنه قد يتعلق بالكيان المادي للحاسب الآلي أو البرامج ذاتها، وهو يندرج بصفة عامة تحت نطاق التزوير الإلكتروني كسلوك غير مشروع يتعلق بمعالجة المعلومات ونقلها، فهو سلوك غير قانوني وغير مسموح به يتعلق بالتعامل الفوري مع المعلومات والبيانات أو نقلها"³.

وعرف كذلك بأنه: "ارتكاب جريمة التزوير الإلكتروني سواء بالدخول المشروع أو غير المشروع على النظام المعلوماتي أو التعامل مع بياناته تزويراً بطرق التزوير المادية أو المعنوية باستخدام الحاسب الآلي وملحقاته للحصول على محرر أو وثيقة إلكترونية مزورة"⁴.

ضف لذلك عرفه بعض الفقهاء بأنه: "الأفعال العمدية وغير الشرعية التي من شأنها إلحاق الضرر المادي بالغير، سواء بإتلاف المعطيات الإلكترونية أو فسخها أو تعديلها أو إدخالها أو صنعها أو بجميع أشكال الاعتداء على عمل النظام المعلوماتي، وذلك بهدف التزوير والحصول على مردود اقتصادي لفائدة الفاعل أو لفائدة الغير"⁵.

وعرف كذلك التزوير الإلكتروني بأنه تغيير الحقيقة يرد على مخرجات الحاسوب الآلي سواء تمثلت في مخرجات ورقية مكتوبة كذلك التي تتم عن طريق الطابعة أو كانت مرسومة عن طريق رسم.

ويمكن أن نستنتج من خلال مختلف هذه التعريفات الفقهية أنه لكي تعتبر الفعل جريمة إلكترونية يجب أن يقع التزوير على مستند إلكتروني وأن يتعارض هذا التزوير مع الحقيقة الموجودة في المستند، ويكون الهدف منه إثبات حق غير موجود في الأساس، وإحداث أثر قانوني معين مما يؤدي إلى إلحاق الضرر بالآخرين.

ثانياً - التعريف القانوني لجريمة التزوير الإلكتروني:

من بين الدول التي أولت اهتماماً بجريمة التزوير الإلكتروني هي فرنسا حيث عرفت هذه الجريمة في الفقرة الأولى من المادة 441 من قانون العقوبات الفرنسي على أن "التزوير هو تعديل مزلل للحقيقة باستخدام أي وسيلة أو وثيقة أو أي شكل آخر للتعبير عن الأفكار بهدف إثبات حق أو لها آثاراً قانونية، وتتميز هذا الفعل بقدرته على إحداث ضرر". ويلاحظ أن هذا التعريف جاء شامل لجميع أشكال التزوير، سواء كان تزويراً تقليدياً أو إلكترونياً⁶.

أما بالرجوع للمشرع الجزائري فنجد أنه قد نص على جريمة التزوير في المحررات في المواد من 214 إلى 229 من قانون العقوبات⁷. وهذا دون أن يعطى تعريف للتزوير ولا بيان أركانه، بل اكتفى بذكر وتحديد أنواع جرائم التزوير الواقعة على المحررات الرسمية والمصرفية وكذلك التزوير في بعض الوثائق الإدارية والشهادات. غير أنه يمكن استخلاص مفهوم التزوير الإلكتروني وفقاً للمادة 03 من القانون 02-24 على أنه تغيير للحقيقة في مخرجات أنظمة الحوسبة والاتصال والتي يمكن الاحتجاج بها لإثبات الحقوق بأي طريقة كانت من شأنها إلحاق الضرر بالغير.

أما المشرع المصري فقد أشارت في المادة 23 من قانون التوقيع الإلكتروني إلى أن التزوير الإلكتروني يتم عن طريق الاصطناع أو التعديل أو التحويل أو بأي طريق آخر وهي صنعة لم تكن موفقة في النص على طرق التزوير لتعديلها واختلافها لذلك أردفها بعبارة "أو بأي طريق آخر"⁸.

أما موقف المنظمات والهيئات الدولية، لقد تباينت في تعريف التزوير الإلكتروني حيث عرفت: "الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010 هذا النوع من الجرائم في المادة 10 على أنه: "استخدام وسائل تقنية المعلومات من أجل تغيير الحقيقة في البيانات تغييراً من شأنه إحداث ضرر وبنية استعمالها كبيانات صحيحة"⁹.

كما عرفت اتفاقية بودابست الموقعة في 2001/11/23 الاتفاقية الأوروبية لمكافحة الجرائم الإلكترونية "التزوير الإلكتروني" في المادة 07 على أن "التزوير المرتبط بالحاسب الآلي وهو يتكون من خلق أو تعديل غير مصرح به للبيانات المسجلة بطريقة من شأنها أن تجوز هذه البيانات المسجلة له قوة دافعة مختلفة عن سياق المعاملات القانونية، والتي تكون مؤسسة على صحة البيانات المستخرجة وبالتالي تكون موضوعاً لخداع المصالح القانونية المحمية"¹⁰.

وتتميز جريمة التزوير الإلكتروني بعدة خصائص التي تميزها عن باقي الجرائم أولها صعوبة الكشف عنها لأنها تنصف بالخفاء أي عدم وجود آثار مادية يمكن متابعتها وهي خطيرة وصعبة في تحديد مكان وقوعها ومكان التعامل معها بسبب اتساع نطاقها المكاني وضخامة البيانات.

بالإضافة لأنها عبارة للحدود أي ترتكب عبر عدة دول مما يعني أنها لا تتقيد بالحدود الجغرافية للدول في عصر الحواسيب وانتشار شبكة الإنترنت العالمية أصبح ربط عدد هائل من الحواسيب حول العالم بهذه الشبكة، مما يسهل عملية التنقل والتواصل بينها.

هذا بالإضافة لتفرد شخصية المجرم ودوافعه حيث ترتكب جريمة التزوير الإلكتروني بوسائل تقنية لذلك يحتاج مرتكبها إلى خبرة وتخصص في المجال الإلكتروني لأنه سيتعامل مع جهاز الكمبيوتر ونظام المعالجة الآلية للبيانات، فقد يكون هذا المجرم الإلكتروني من الموظفين المتخصصين في مجال الحاسب الآلي، وهم أشخاص يستغلون الحاسب الآلي ولكن بشكل غير قانوني، وهم فئتين الهاكرز القراصنة الهواة والكرakers وهم قراصنة المحترقون¹¹.

الفرع الثاني: أركان جريمة التزوير الإلكتروني:

تمثل أركان جريمة التزوير الإلكتروني في الركن المادي والركن المعنوي وهذا ما سيتم توضيحه من خلال ما يلي:

أولاً- الركن المادي لجريمة التزوير الإلكتروني:

إن مضمون الركن المادي في جريمة التزوير الإلكتروني تتمثل في تغيير الحقيقة محرر بإحدى الطرق التي حددها القانون من شأنه أن يسبب ضرراً ولقيام هذه الجريمة لابد من توفر ثلاثة عناصر أساسية هي وجود محرر وتغيير الحقيقة بالإضافة لوقوع ضرر.

فبالنسبة لوجود محرر لم تورد التشريعات العقابية تعريف للمحرر محل جريمة التزوير مكثفة بالنص على أن التزوير يقع على محرر، ويعد المحرر الإلكتروني أسلوب أو وسيلة حديثة تقوم بأداء وظائف المحررات الورقية فيما يتعلق بإثبات المعاملات، إلا أنها تختلف عنها في الاستخدام والبيئة التي تنتشر فيها وتعد من أحدث طرق الإثبات التي ظهرت مع الاستخدام الواسع لتكنولوجيا المعلومات والاتصالات. وقد اختلفت التشريعات الجنائية بشأن تسمية المحرر، وأطلقت عليه عدة مصطلحات مثل المستند الإلكتروني، الكتابة الإلكترونية، المحرر الإلكتروني، الوثيقة الإلكترونية إلا أن جميعها تحمل معنى واحد.

وتمثل الركن المادي في جريمة التزوير الإلكتروني تغيير الحقيقة في محرر بإحدى الطرق التي حددها القانون ومن شأنه أن يحدث ضرر بالغ، ويمكن تصور تغيير الحقيقة في النظام الآلي للمعالجة المعلوماتية بتغيير البيانات أو حذفها أو إضافتها أو التلاعب فيها بأي صورة سواء كانت هذه البيانات مخزنة في دائرة الآلة أو كانت تمثل جزء من برنامج التشغيل أو برنامج التطبيق¹².

ضف لذلك لا تكفي لقيام جريمة التزوير الإلكتروني تغيير الحقيقة في محرر وإنما يجب أن يكون من شأن ذلك إحداث ضرر للغير، فحصول الضرر شرط للعقاب على جرائم التزوير، فالضرر عنصر جوهري في هذه الجريمة.

ويعرف عنصر الضرر في جريمة التزوير بأنه "كل إخلال أو احتمال الإخلال بمصلحة يحميها القانون، ويستوي في ذلك الضرر الجسيم واليسير، والضرر الفعلي والمحتمل، والضرر المادي والضرر الأدنى والضرر الخاص العام"¹³.

ثانياً- الركن المعنوي:

لا تكتمل جريمة التزوير التقليدية إلا بتوافر الركن المعنوي إلى جانب الركن المادي ولا بد من توافر القصد الجنائي العام والخاص، فالقصد الجنائي العام يقوم على انصراف إرادة الجاني إلى تغيير الحقيقة في المحرر بإحدى الطرق التي بينها القانون مع توقعه احتمال حدوث ضرر مادي، والإرادة اللازمة في جريمة التزوير الإلكتروني هي تلك التي تتجه لتحقيق الواقعة الإجرامية بسيطرتها على السلوك المادي وتوجيهه نحو تحقيق النتيجة¹⁴. مثالها تتجه إرادة الجاني في جريمة تزوير التوقيع الإلكتروني في بطاقات الائتمان إلى تغيير حقيقة الرقم السري لبطاقة الائتمان.

أما القصد الخاص فهو اتجاه نية الجاني إلى استعمال المحرر المزور فيما زور لأجله ويتوافر القصد الخاص حتى ولو لم يستعمل هذا المستند المزور فعلاً فلا يكفي لقيام الركن المعنوي توافر القصد العام فقط، بمعنى أنه لا يكفي توافر الإرادة والعلم بمكونات الجريمة، بل لا بد أن تكون نية الجاني قد اتجهت وقت ارتكاب هذا الفعل إلى استعمال المحرر المزور فيما زور من أجله أي الاحتجاج به على اعتبار أنه صحيح¹⁵.

المطلب الثاني: صور جريمة التزوير الإلكتروني:

اعتمدت الإدارة العامة كغيرها في القطاعات الأخرى التكنولوجية لتتحول معاملتها تدريجيًا من البيئة الورقية إلى البيئة الافتراضية بهدف تقليص النفقات والوقت وكذا الحد من التضخم الورقي وفي نفس الوقت تحسين أداء الخدمة. غير أنه في المقابل فتح الباب أمام ارتفاع نسبة الغش المعلوماتي وفي مقدمته التزوير في المحررات الإلكترونية وهذا ما نراه من خلال الفرعين التاليين فيما يلي:

الفرع الأول: التزوير في المحررات الإلكترونية الرسمية أو العمومية.

يقتضي التزوير في المحررات العمومية أو الرسمية المنصوص عليها في قانون العقوبات فضلاً عن الأركان المشتركة لكل صور التزوير، أن يقع التزوير على محرر عمومي أو رسمي وأن يتم التزوير بإحدى الطرق المادية أو المعنوية المبينة في نصوص القانون الجنائي¹⁶.

ويمكن تعريف المحرر الرسمي أو العمومي بأنه محرر يصدر أو من شأنه أن يصدر من موظف ومن شبهه مختص بمقتضى وظيفته بتحريره وإعطائه الصفة الرسمية أو يتدخل في تحريره أو التأشير عليه وفق ما تقتضيه القوانين، واللوائح التنظيمية التي تصدر إليه من جهته الرئيسية¹⁷.

وحسب الفقه والقضاء وتقسّم المحررات الرسمية إلى أربعة أنواع هي المحررات السياسية والمحررات القضائية بالإضافة للمحررات الصادرة عن الموتقين والمختصين وأخيرًا المحررات الإدارية.

ويكي نكون بصدد محرر رسمي يجب أن يتضمن شروط ثلاثة هي الصفة والاختصاص والشكل إلى جانب ذلك أن يصدر عن الدولة أو أحد الأشخاص المعنوية العامة وأن يتم تدوينه وفقاً للأوضاع والإجراءات التي يحددها القانون¹⁸.

وعلاوة على المحررات الرسمية أو العمومية، نص قانون العقوبات على صور أخرى للتزوير تتمثل في التزوير في بعض الوثائق الإدارية والشهادات مثالها تزوير الوثائق الإلكترونية.

في الواقع أن الوثائق الإلكترونية غير محصورة باعتبارها مرتبطة بالتطور التكنولوجي وتتخذ البطاقات الإلكترونية أشكالاً متعددة ووظائف مختلفة، كما أنها قد تصدر من جهات عمومية أو مؤسسات مالية خاصة نذكر منها، تزوير جواز السفر الإلكتروني.

حيث يعد هذا الأخير وثيقة تعريف وسفر عالية الأمان تحمل صورة وبصمات رقمية وخصائص بيومترية لصاحبها مخزنة ضمن شريحة إلكترونية، حيث تسمح هذه الشريحة بقراءة كل المعلومات الشخصية الخاصة بالشخص المسافر وقد عرفته المادة 02 من القانون 03/14 المتعلق بسندات ووثائق السفر بأنه "جواز السفر الذي يلزم بحمله كل مواطن يسافر إلى الخارج هو جواز سفر من نوع بيومتري إلكتروني أو قابل للقراءة بالآلة"¹⁹. وعليه نستنتج أن التزوير الواقع على جواز السفر البيومتري هو خاضع لقانون العقوبات الجزائري. أما الصورة الثانية فتتمثل في تزوير بطاقة الشفاء الإلكترونية والتي تسلم عادة من قبل هيئات الضان الاجتماعي للمواطنين المؤمنين اجتماعيًا وقد نظمها المشرع في القانون 01/08 الملمم للقانون 01/83 الخاص بالتأمينات الاجتماعية، وقد عالج مسألة تزوير بطاقات الشفاء الإلكترونية وهذا في نص المادة 93 مكرر بنصه على أنه كل من يقوم بطريق الغش بتعديل أو حذف كلي أو جزئي للمعطيات سواء التقنية أو الإدارية المدرجة في البطاقة الإلكترونية للمؤمن له اجتماعيًا، وأضافت المادة 93 مكرر 4 على التزوير كذلك يتم عن طريق النسخ أو الصنع أو الحيازة بطريقة غير مشروعة للبطاقات الإلكترونية للمؤمن له اجتماعيًا.

الفرع الثاني: تزوير التوقيع الإلكتروني وطاقات الائتمان نموذجًا.

وهذا ما نراه من خلال ما يلي:

أولاً- تزوير التوقيع الإلكتروني:

إن انتشار نظم المعالجة الإلكترونية للمعلومات في الشركات والإدارات والبنوك واعتمادها المباشر على هذه النظم أصبح لا يتفق مع فكرة التوقيع بمفهومها التقليدي، فقد أصبح التوقيع التقليدي عقبة في النظم الحديثة للإدارة وهذا ما فتح باب لارتكاب جريمة تزوير التوقيع الإلكتروني.

ومن بين التشريعات التي جرمت هذه الأفعال القانون النموذجي حول التجارة الإلكترونية الصادر عن لجنة القانون التجاري الدولي لدى الأمم المتحدة لعام 1996 الذي أقر بالقوة الشبوتية للسند والتوقيع الإلكترونيين. وكذلك قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية²⁰.

ويتم تزوير التوقيع الإلكتروني بطرق مختلفة حيث يكون التوقيع المزور مطابقًا تمامًا للتوقيع الأصلي، ويتم ذلك عن طريق سرقة نظام التوقيع الإلكتروني عبر التجسس الإلكتروني مما يتيح للجهة المهاجمة الحصول على التوقيع الإلكتروني واستخدامه في توقيع الوثائق والمحركات، وبالرغم من أن التوقيع يبدو صحيحًا إلا أنه لم يصدر عن مالك نظام التوقيع ولكن صدر عن شخص قام باختراق النظام وسرقة بيانات التوقيع²¹.

ثانيًا- تزوير بطاقات الائتمان إلكترونيًا:

يعتبر تزوير بطاقات الائتمان من أخطر صور التزوير الإلكتروني، فمنذ اندلاع العالم بقوة نحو المعلوماتية والبرمجيات الحديثة أصبحت بطاقات الائتمان وسيلة الدفع الأكثر استخدامًا وانتشارًا في العالم، وهكذا بدأت بطاقات الدفع الإلكتروني تحل محل النقود والشيكات نظرًا لما تتمتع به من سهولة في الدفع مع إمكانية التعامل بها محليًا وعالميًا.

قد يتم تزوير بطاقات الائتمان بالتلاعب في محتوياتها بطرق مختلفة سواء تعلق الأمر بالمعلومات المرئية الموجودة عليها أو المعلومات المشفرة الموجودة على الشريط المغنط.

فقد يكون التزوير كلياً لبطاقة الائتمان فيقع على جميع عناصرها بمعنى يتم تزوير جميع المادة المكونة للبطاقة وهذا بتقليد بطاقة ائتمان إلكترونية أخرى مشابهة لها، حيث يتم التلاعب بالمادة المكونة للبطاقة بالإضافة لتزوير المعلومات الموجودة عليها كما سبق ذكره.

كما يمكن الاحتيال على صاحب البطاقة عبر شبكة الإنترنت وذلك عن طريق اصطياذ البيانات المصرفية عن طريق البريد الإلكتروني حيث يتلقى المستفيد رسالة إلكترونية تبدو وكأنها من بنك أو مؤسسة حكومية تريد التأكد من بياناته يتم إرسالها إلى موقع آخر شبيه الموقع الأصلي²².

علاوة على هذا قد يتم الاحتيال من خلال البطاقات الائتمانية عن طريق تحميل العميل لفواتير مزيفة أو استخدام خدمات الصراف الآلي لايداع الشيكات التي لا يوجد عليها رصيد بحيث يتم إضافة قيمة الشيك إلى رصيد الحساب الأصلي ثم سحب المبالغ المضافة عبر الصراف الآلي قبل المقاصة بين البنوك وغيرها من أساليب الاحتيال²³.

ومن بين الظواهر الدالة على التزييف الكلي لبطاقة الائتمان هو عدم دقة لصق وعدم ثبات تموضع الشريط المغنط وشريط التوقيع بظهر البطاقة الأمر الذي يترتب عليه إمكانية نزعها بسهولة بواسطة أضاف الأصابع. كذلك اختلاف شكل وحجم البيانات المطبوعة وإمكانية عدم التطابق بين البيانات المشفرة على الشريط المغنط وبين البيانات المقروءة بصرياً والمطبوعة.

أما الصورة الثانية لتزوير بطاقة الائتمان فهو التزوير الجزئي لها والذي يتم عن طريق التلاعب في المكونات المرئية وغير المرئية للبطاقة الصحيحة بالأساليب المناسبة حيث يستثمر المزور في هذه الحالة الجسم الحقيقي للبطاقة وما عليه من نقوش وطباعة وكتابة أمنية.

ويتخذ التزوير الجزئي لبطاقة الائتمان ثلاثة صور نذكرها هي سرقة المعلومات الخاصة بالبطاقة أو تزوير التوقيع على بطاقات ائتمان مسروقة أو عن طريق تزوير الشريط المغنط.

وإن أهم الظواهر الدالة على تزوير البطاقة في هذه الصورة هو انهيار بعض مواضع التوقيع وإمكانية ظهور سطح البطاقة أسفل مواضع الانهيار نتيجة للمحور الآلي، مع ظهور بقع قاتمة أو بنية أو مصفرة اللون نتيجة للمحور الكيميائي.

المبحث الثاني: التعاون الأمني والقضائي الدولي لمكافحة جريمة التزوير الإلكتروني.

في إطار محاربة الجريمة الإلكترونية ولاسيما جريمة التزوير الإلكتروني لا يمكن للدولة بمفردها الوصول لتحقيق ذلك إلا عن طريق التعاون الأمني والقضائي الدولي وهذا بسبب خصوصية هذه الجرائم التي تختلف عن الجرائم التقليدية الأخرى وهذا ما سنراه من خلال هذا المبحث فيما يلي:

المطلب الأول: التعاون الأمني لمواجهة جريمة التزوير الإلكتروني.

يعتبر التعاون الأمني من أهم الوسائل التي تحارب بها الجريمة الإلكترونية ولاسيما جريمة التزوير الإلكتروني وتمكن الدول من تتبع المجرمين خارج الحدود الوطنية من خلال أجهزته التي تعمل بمساعدة الدول

على الحد من هذه الجرائم وعليه تم التعرض في الفرع الأول للتعاون الأمني في إطار الأجهزة الدولية وخصص الفرع الثاني للتجربة الأمنية للدول العربية وهذا ما سنراه من خلال ما يلي:

الفرع الأول: التعاون الأمني في إطار الأجهزة الدولية.

في الواقع تلعب الاتفاقيات الشرطية بين الدول دورًا هامًا في ضبط الجرائم التزوير الإلكتروني ولا سيما بطاقات الائتمان، بحيث إذا ما اكتشفت الشرطة الوطنية لدولة وقوع جريمة تزوير إلكتروني واقعة على التوقيع الإلكتروني من خلال موقع موجود في الخارج، فإنها تقوم بالإبلاغ عن هذه الجريمة إلى سلطات البوليس بالدولة التي يقع فعل الاعتداء على إقليمها للقيام بالإجراءات اللازمة لوقف هذا الاعتداء فورًا، علاوة على الاستفادة من تبادل الخبرات الأمنية بين الدول في مجال العمليات الشرطية والتدريب ووسائل الاتصال وكمودج لذلك عملية "أود سيسوس" التي تمت في 26 فيفري 2004 بمبادرة من يوروبول، وقامت قوات الشرطة خلالها بعمليات شملت 10 دول وهي أستراليا، بلجيكا، كندا، ألمانيا، هولندا، النرويج، بيو، إسبانيا، السويد، وبريطانيا²⁴.

ونذكر كذلك بهذا الخصوص مؤتمر واشنطن لعام 1997 والذي اعتمد فيه وزراء العدل والشؤون الداخلية لدول مجموعة الثمانية المبادئ التي تشكل الأساس لشبكة نقاط اتصال وطنية، علاوة على اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية.

المطلب الثاني: التعاون القضائي كآلية لمكافحة جريمة التزوير الإلكتروني.

حتى تتمكن الدول من مكافحة جريمة التزوير الإلكتروني لابد لها من التضامن والتعاون القضائي الدولي في المجال الجزائي والمتمثلة أساسًا في المساعدة القضائية وكذا عن طريق تسليم المجرمين وهذا ما سنراه من خلال ما يلي:

الفرع الأول: المساعدة القضائية:

ويقصد بالمساعدة القضائية كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم²⁵، وتتخذ المساعدة القضائية في المجال الجنائي صور متعددة منها تبادل المعلومات، نقل الإجراءات الإنابية القضائية، وهذا ما سنتناوله فيما يلي:

[كما يقصد بها كذلك تقديم الدول الأطراف مساعدة قانونية فيما بينها فيما يخص التحقيقات والإجراءات القضائية المتصلة بجرائم تحددها الاتفاقيات الدولية].

أولاً_ تبادل المعلومات:

ويشتمل هذا الإجراء تبادل المعلومات، تقديم البيانات والوثائق والمواد الاستدلالية التي تطلبها سلطة قضائية أجنبية وهي بصدد النظر في جريمة ما من الاتجاهات التي وجهت إلى رعاياها في الخارج والإجراءات التي اتخذت ضدهم، كما يشمل تبادل السوابق القضائية للجنة ومن خلالها تتعرف الجهات القضائية على الأحكام الخاصة بالعود، وعدم الأهلية ووقف تنفيذ العقوبة²⁶.

وفيما يخص تبادل المعلومات في جريمة التزوير الإلكتروني وخاصة الواقعة على التوقيع الإلكتروني وقد حرصت المادة 26 من اتفاقية بودابست على التأكيد على واجب الدولة التي تملك معلومات هامة في مساعدة دولة أخرى، ومن جهة أخرى تلعب المنظمة الدولية للشرطة الجنائية (الأنتربول) دورًا مهمًا كذلك في الكشف

عن جرائم التزوير الإلكتروني، لقد جاءت هذه المنظمة نتيجة الإدراك الكامل من جميع الدول بأهمية التعاون في مجال مكافحة الجريمة خاصة التي تمتد تنفيذها وتأتجها إلى عدة دول مختلفة²⁷. وتعد من أهم المنظمات الدولية الناشطة في مجال مكافحة الجريمة بصفة عامة والإجرام المالي المرتبط بالتكنولوجيا المتقدمة من أهم الجرائم التي يجري التركيز عليها مؤخرًا من قبل منظمة الإنتربول أما بالنسبة لدورها في مواجهة جرائم التزوير الإلكتروني كالبطاقات الدفع الإلكترونية، فنجد أن السكرتارية العامة الخاصة بها نظمت أول مؤتمراتها الدولية بخصوص الاحتيال والغش الذين يهددان نظام بطاقات الدفع الإلكتروني عام 1994 والذي نتج عنه توصيات تتعلق الأولى بضرورة مراجعة تشريعاتها وقوانينها الخاصة ببطاقات الدفع الإلكتروني بما يتضمن تجريم تصنيع أو امتلاك البطاقات المزورة أو امتلاك معلومات غير قانونية واستخدامها في إدخالها في نظام الدفع الإلكتروني²⁸.

أما الوصية الثانية فنصت على ضرورة إنشاء مجموعات عمل بوليسية من خبراء الاحتيالات الدولية التابعين لبوليس هونج كونج والشرطة الكندية والخدمة السرية الأمريكية وخدمة الاستخبارات القومية الجنائية لنيوزيلاند ومندوبين من منظمات بطاقات الدفع الإلكتروني لمكافحة هذا النوع من الجرائم، وفي هذا الإطار ذاته قامت المنظمة الدولية للشرطة الجنائية بتوقيع خمس اتفاقيات مع المنظمات الراعية للبطاقات وذلك بهدف التعاون الوثيق في مجال جرائم بطاقات الدفع الإلكتروني لعام 1999²⁹.

وتجدر الإشارة أنه حصلت منظمة الإنتربول على الصفة الاستشارية الخاصة بالمنظمات غير الحكومية سنة 1949، وبعدها 1975 أصبحت تتمتع المنظمة الدولية للشرطة الجنائية الدولية بصفة عضو دائم مراقب، ولقد انضمت الجزائر إلى هذه المنظمة عام 1963 ممثلة بالمكتب المركزي الوطني حيث يعمل المكتب المركزي الوطني تحت الوصاية المباشرة لمديرية الشرطة القضائية المديرية العامة للأمن الوطني ويباشر مهامه وفقًا للنصوص والتشريعات الوطنية، ملتزمًا بالأطر القانونية المميّزة للمنظمة الدولية للشرطة الجنائية³⁰.

أفراد ينتقلون بين المجموعات ضد شركات يطلبون منها أموال عن طريق الابتزاز والتهديد بشن هجمات حجب الخدمة الموزعة وفعلاً قاموا بذلك باستخدام شبكة "البوت نت" أو ما يسمى "روبوت الأنترنت"³¹.

ثانيًا - نقل الإجراءات:

ويقصد به اتخاذ دولة ما بناءً على اتفاقية إجراءات جنائية وهي بصدد جريمة ارتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة متى توافرت شروط معينة أهمها ازدواجية التجريم وشرعية الإجراءات المطلوب اتخاذها بمعنى أن تكون الإجراءات المطلوب اتخاذها مقررّة في قانون الدولة المطلوب إليها عن الجريمة ذاتها، وقد أقر المجلس الأوروبي نقل الإجراءات الجنائية التي تعطى للأطراف المنظمة إمكانية محاكمة الجاني طبقًا لقوانينها، وبناءً على طلب دولة أخرى طرف في هذه الاتفاقية، يشترط أن يكون الفعل معاقبًا عليه في الدولتين³².

كما يجوز للدولة المطلوب إليها أن ترفض نقل الإجراءات في الحالات الآتية:

أ_ إذا كان طلب نقل الإجراءات ليس له ما يبرره كأن تكون الأسباب التي ذكرتها الدولة الطالبة لا تدعو لاتخاذ مثل هذه الإجراءات.

ب_ إذا ثبت أن الدافع وراء طلب نقل الإجراءات اعتبارات سياسية أو دينية عنصرية.

جـ_ إذا كانت الدولة المطلوب إليها قد طبقت قوانينها على الجريمة قبل استلامها من الدولة الطالبة، وكان الإجراء الذي سبق اتخاذه مطابقاً للقانون.

د_ إذا كانت الإجراءات التي تطلبها الدولة الطالبة مخالفة لواجبات تلزم بها الدولة المطلوب إليها.

هـ_ إذا كانت الإجراءات المطلوبة مخالفة لقوانين الدولة المطلوب إليها³³.

ثالثاً_ الإنابة القضائية:

ويقصد بها طلب اتخاذ إجراء قضائي من إجراءات الدعوى الجنائية وتقديمه الدولة الطالبة إلى الدولة المطلوب إليها، للفصل في مسألة معروضة على السلطة القضائية في الدولة الطالبة ويتعذر عليها القيام به بنفسها. فالإنابة القضائية تسهل إذن الإجراءات الجنائية بين الدول، بما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة. والتغلب على عقبة السيادة الإقليمية التي تتمتع الدولة الأجنبية من ممارسة بعض الأعمال القضائية داخل أقاليم الدولة الأخرى³⁴.

ويتم إرسال الإنابة القضائية عبر القنوات الدبلوماسية وهذا من شأن النياية العامة وذلك من خلال قيام المحكمة الوطنية بتوقيف الطلب في الدولة الطالبة لتقوم هذه الأخيرة بإرساله بعد ذلك إلى السلطات القضائية المختصة في الدولة متلقية الطلب وما أن يتم تلبية الطلب ينعكس الاتجاه الوارد في سلسلة العمليات³⁵. لكن تجدر الملاحظة أن مرور إجراءات التعاون القضائي بالطرق الدبلوماسية يجعلها تتسم بالبطء وكثرة التشكيلات وهو ما يتعارض في الواقع مع شبكة الإنترنت التي تتطلب السرعة والمرونة في تبادل المعلومات.

ونظراً لأن مثل هذه الإجراءات كما سبق ذكره تتميز بوقت طويل فقد أبرمت العديد من الاتفاقيات الجديدة التي ساهمت باختصار الإجراءات عن طريق الاتصال المباشر بين السلطات المعنية بالتحقيق مثال ذلك الاتفاقية الأمريكية الكندية، التي تنص على إمكانية تبادل المعلومات شفويًا في حالة الاستعجال³⁶.

الفرع الثاني: تسليم المجرمين:

لقد حرصت أغلب دول العالم على سن التشريعات الخاصة تسليم المجرمين بالإضافة لعقد العديد من الاتفاقيات الإقليمية والدولية التي تهتم بعملية التسليم إسناداً إلى فكرة التعاون الدولي القضائي لضمان عدم إفلات الجناة من العقاب، وعليه يمكن تعريف بأنه تخلي دولة عن شخص موجود على إقليمها إلى دولة أخرى بناءً على طلبها، لتحاكمه عن الجريمة التي يعاقب عليها القانون أو لتنفيذ فيه حكماً صادراً عليه من إحدى محاكمها³⁷.

وقد خلصت المحكمة الأمريكية العليا لتعريف التسليم بأنه الإجراء القانوني المؤسس على معاهدة أو المعاملة بالمثل أو قانون وطني تسلم بمقتضاه دولة ما من دولة أخرى شخص متهم أو مرتكب مخالفة جنائية ضد القوانين الخاصة بالدولة الطالبة، أو مخالفة القانون الجنائي الدولي، حيث يعاقب على ذلك في الدولة الطالبة³⁸. وحتى يمكن تطبيق إجراء تسليم المجرمين في الجريمة الإلكترونية ولا سيما جريمة التزوير الإلكتروني لا بد من توافر مجموعة من الشروط منها ما يتعلق بالشخص المطلوب تسليمه ومنها ما يتعلق بالواقعة الإجرامية محل التسليم.

وتمثل أول شرط في عدم جواز تسليم اللاجئ السياسي، فحسب المبدأ السائد في أغلب التشريعات وكذا الاتفاقيات الدولية المتعلقة بتسليم المجرمين يكون الفرض من المطالبة به هو اتخاذ إجراءات انتقامية ضده وهو عمل لا يليق بالدولة المطلوب منها التسليم أن تساهم في تنفيذه³⁹.

كما لا يجوز تسليم الشخص التي سبق وأن تمت محاكمته على الجريمة محل الطلب أو صدر في حقه حكم ببراءته أو إدانته أو كانت الجريمة قيد التحقيق وذلك لعقوبة مزدوجة.

بالإضافة لازدواجية التحريم فيجب أن يكون الاعتداء على التوقيع الإلكتروني مثله أو التزوير الواقع على بطاقة الائتمان المشوبة للمتهم تشكل جريمة في قانون الدولة طالبة التسليم وكذا في قانون الدولة المطلوب إليها التسليم، ويجب مراعاة كذلك التقادم في هذه الجرائم فإذا انقضت الدعوى بموجب قانون الدولة التي طلبت التسليم، فلا يكون هناك محل للتسليم⁴⁰.

علاوة على هذا أن يكون قانون الدولة طالبة التسليم مختصاً بمحاكمة الشخص المطلوب تسليمه، وعليه يجب أن ينعقد الاختصاص بنظر جريمة التزوير الإلكتروني كجريمة التوقيع الإلكتروني مثلاً لقانون الدولة طالبة التسليم وبالمقابل يتعين ألا يكون قانون الدولة المطلوب إليها التسليم مختصاً بمحاكمة الشخص المطلوب تسليمه عن ذات الفعل المنسوب إليه⁴¹.

أما بالرجوع للإجراءات الشيقة في تسليم المجرمين فيجب أن تتبع الدول الأطراف في عملية التسليم بهدف المحافظة على حقوق الإنسان وحرية وتأمين الصالح العام قواعد إجرائية مقيدة ببعض الالتزامات الدولية أو التعاهدية.

تقديم الطلب لإجراء التسليم كتابياً مع إرفاقه بالوثائق التي تسهل على الدولة المطلوب منها التسليم التعرف على هوية المطلوب تسليمه وعرض موجز للوقائع المتابع من أجلها، يرفق بنسخة مصادق عليها للنص القانوني المطبق على تلك الوقائع ونسخة من مستندات التحقيق إن وجدت.

أما إن كان الطلب الخاص بتنفيذ العقوبة فإن الوثائق الواجب إرفاقها مع طلب التسليم فهي نسخة أصلية من الحكم الذي يتضمن العقوبة وتشترط بعض الدول التوقيع على هذه الوثائق من الجهات الرسمية في حين تكتفي بعض الدول الأخرى باتباع الطريق الدبلوماسي الذي يعد ضمانة لرسميتها⁴².

في حال صدر أمر الموافقة على طلب التسليم من طرف الدولة المطلوب منها ذلك فيحق لها تسلمه في مدة زمنية تقدر بشهر وهذا وفق أغلب المعاهدات فإذا لم يتم خلالها جاز للدولة المطلوب منها التسليم إطلاق سراح الشخص المطلوب كما ذهبت قوانين أخرى إلى رفض التسليم لوجود الطلب مرة أخرى عن نفس الجريمة.

أما عن مكان تنفيذ طلب التسليم فقد جرى العمل أن يكون في إحدى الموانئ أو مطارات الدولة المطلوب منها التسليم أو أحد نقاط الحدود بالنسبة للتسليم الذي يتم بين دول متجاورة، وفي حال وجود دول أخرى تتوسط الدولة طالبة والمطلوب منها التسليم فيجب الحصول على موافقة جميع الدول.

أثناء التحقيقات أو تداول الدعوى الجنائية في الحالات التي تدرك فيها سلطات التحقيق في الدولة التي تجري التحقيقات أو الملاحقة وجود هذه المعلومات دون حاجة لتقديم طلب بالمساعدة المتبادلة في تلك الحالة⁴³.

كما يمكن كذلك للدولة في حالات أخرى تقديم طلب لنظريتها لمدها بالمعلومات والوثائق التي تطلبها سلطة قضائية أجنبية بصدد جريمة ما عن الاتهامات التي وجهت رعاياها في الخارج والإجراءات التي تتخذ ضدهم، كذلك الحال فيما يتعلق بالسوابق القضائية للجنة أو يطلب المثل الشخصي لشاهد أو خبير⁴⁴. وقد تم إيراد صور المساعدة القضائية الدولية في المادة الأولى من معاهدة الأمم المتحدة النموذجية لتبادل المساعدة القضائية في المسائل الجزائية والتي تقضي باتفاق أطرافها على أن يقدم كل طرف أكبر قدر ممكن من المساعدة المتبادلة في التحقيقات وإجراءات المحاكمة المتعلقة بجرائم يكون العقاب عليها وقت طلب المساعدة داخله في اختصاص السلطة القضائية في الدولة الطالبة للمساعدة⁴⁵.

أم بخصوص المشرع الجزائري فقد نص على أنه "في إطار التحريات أو التحقيقات القضائية الجارية لمعانة الجرائم المشمولة بهذا القانون وكشف مرتكبيها يمكن للسلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشعل الإلكتروني".

وتضيف المادة 16 من القانون 04/09 على أنه "إذا وردت عن طريق وسائل الاتصال السريعة بما في ذلك أجهزة الفاكس أو البريد الإلكتروني وذلك بقدر ما توفره هذه الوسائل من شروط تكن كافية للتأكد من صحتها"⁴⁶.

وكمؤج لهذه الحالة "عملية كاتريك" التي قامت به شركات القمار عبر الأنترنت في الفترة من ماي إلى أكتوبر 2004، وقام بها عدد من المجموعات الإجرامية مع أفراد يتنقلون بين المجموعات، وفي هذه العملية كان المجرمون يرسلون إلى إحدى الشركات يطلبون منها أموالاً مهددين إياها بأن يشنوا على موقعها هجمات حجب الخدمة الموزعة في حالة امتناعها عن الدفع، ونفذت فعلاً العصاة الهجمات وتعرضت حوالي 57 شركة في أنحاء العالم ومنها شركات بريطانيا تجاوزت خسائرها 30 مليون جنيه.

الفرع الثاني: التعاون الأمني العربي.

يعتبر التعاون الأمني العربي امتداداً للتعاون الدولي الإقليمي في مجال مواجهة الجرائم بصفة عامة والجرائم الإلكترونية، بما فيها التزوير الإلكتروني بصفة خاصة، حيث تعمل الدول العربية جاهدة من أجل مجابهة الإجرام المنظم.

وتتجلى مظاهر التعاون الأمني على المستوى العربي في عمل مجلس وزراء الداخلية العرب تحت مظلة جامعة الدول العربية إضافة إلى منظمة المكتب العربي لمكافحة التطرف والإرهاب بالإضافة للاتفاقية الأمنية لدول مجلس التعاون الخليجي.

أولاً - مجلس وزراء الداخلية العرب:

يعتبر مجلس وزراء الداخلية العرب أهم المنظمات الدولية الأمنية المتخصصة التابعة لجامعة الدول العربية، ويهدف إلى مكافحة الجريمة وتحقيق الأمن الداخلي والأمن الإقليمي فيما بين الدول العربية، وذلك عن طريق دعم التعاون وتحقيق التكامل الأمني العربي.

ويعد مجلس وزراء الداخلية العرب أعلى سلطة أمنية عربية مشتركة بعد مؤتمر القمة مؤتمر قادة رؤساء الدول العربية، ويهدف المجلس إلى تنسيق الجهود بين الدول العربية في مجال الأمن الداخلي ومكافحة الجريمة وتشمل اختصاصاته حسب المادة 04 من القانون الأساسي للمجلس في إنشاء الهيئات والأجهزة اللازمة لتنفيذ

أهدافها مع العمل على دعم الأجهزة الأمنية العربية ذات الإمكانيات المحدودة وتعزيز رسائل التعاون مع الهيئات الدولية المعنية باختصاصاته⁴⁷.

وعقد المجلس عدة مؤتمرات في معالجة الظواهر الإجرامية المستحدثة مع التركيز على الجرائم الإلكترونية في المجال الأمني وهذا على غرار الدورة 17 للمجلس التي احتضنتها الجزائر في 2000، والتي من خلالها أنشأت في كل دولة من الدول الأعضاء شعبة اتصال بهدف التنسيق بين هذه الدول، وذلك بوضع نظام اتصالات عصري يربط الدول العربية وأجهزة المجلس، كما أنشأ كذلك المكتب عدة مكاتب متخصصة في مكافحة الجريمة المنظمة العابرة للحدود، كالمكتب العربي لمكافحة الجريمة ببغداد والمكتب العربي للإعلام الأمني بالقاهرة وغيرها من المكاتب⁴⁸، كما شكل مجلس وزراء الداخلية العرب فريق خبراء معني بمواجهة الجريمة الإلكترونية خلال دورته الـ 35 وهذا نظراً لطبيعة هذه الجريمة وأبعادها المتعددة، كما اتخذ مجموعة من الإجراءات من بينها اعتماد الإستراتيجية العربية لمواجهة جرائم تقنية المعلومات في دورته الـ 37 المنعقدة عام 2020⁴⁹.

ثانياً: المكتب العربي لمكافحة التطرف والإرهاب وجرائم تقنية المعلومات:

لقد نشأ هذا المكتب انطلاقاً من مقولة "الفكر لا يواجه إلا بفكر" لصاحب السمو الملكي السعودي، وصدر القرار رقم 691 في عام 2014 القاضي بالموافقة على إنشاء مكتب عربي للأمن الفكري، ثم صدر بعده القرار رقم 728 في 2016 من قبل السمو ومعالي وزراء الداخلية العرب بتعديل تسميته ليصبح المكتب العربي لمكافحة التطرف والإرهاب وفي 2017/10/16 تم توقيع اتفاقية المقر بين حكومة المملكة العربية السعودية والمكتب العربي لمكافحة التطرف والإرهاب.

وبعد ذلك أصدر وزراء الداخلية العرب في 2025/02/16 قرار رقم 948 لعام 2025 يقضي بتعديل تسمية المكتب العربي لمكافحة الإرهاب وجرائم تقنية المعلومات ليصبح المكتب العربي لمكافحة التطرف والإرهاب وجرائم تقنية المعلومات⁵⁰، ويعد جزء من مجلس وزراء الداخلية العرب.

وتمثل مهامه في تعزيز التعاون بين الدول الأعضاء في مكافحة التطرف والإرهاب ودعم "الأمن الفكري" أي الجوانب الفكرية أو العقائدية المرتبطة بالتطرف بالإضافة لمكافحة الجرائم المعلوماتية للدول الأعضاء عند الطلب في هذه المجالات وقد قام المكتب مؤخراً فيما يخص الجرائم المستحدثة بعرض ورقة عمل حول التداعيات الأمنية للذكاء الاصطناعي وسبل مواجهتها على الاجتماع الـ 32 للنخبة المتخصصة بالجرائم المستجدة، بالإضافة لعرضه لحظة عربية لمواجهة الجرائم المرتكبة بواسطة الذكاء الاصطناعي وهذا في المؤتمر الأول للمسؤولين عن مواجهة جرائم تقنية المعلومات في وزارات الداخلية العربية⁵¹.

ثالثاً: الاتفاقية الأمنية لدول مجلس التعاون الخليجي:

من بين الآليات على المستوى الأمني العربي، نجد هذه الاتفاقية والتي تم التوقيع عليها في الرياض بتاريخ 2012/10/13 وهذا رغبة من الدول الأعضاء في المحافظة على أمن واستقرار دول مجلس التعاون الخليجي وتحقيق أكبر قدر من التعاون من أجل مكافحة الجرائم بصفة عامة والجرائم الإلكترونية بصفة خاصة والعمل قد استطاع على رفع كفاءة الأجهزة الأمنية⁵².

وتمثل أهدافها في تبادل المعلومات والخبرات التي تساهم في تطوير سبل منع مكافحة الجريمة على اختلافها وأنواعها، لاسيما المنظمة المستجدة وتقديم الدعم الفني في جميع الشؤون الأمنية بما يحقق التكامل المنشود.

ومن جهة أخرى توحيد القوانين والأنظمة والإجراءات بما يكفل مكافحة الجريمة وهذا تحقيقاً لأمن الدول الأطراف مع تبادل القوانين واللوائح المتعلقة بعمل بعض الوزارات الداخلية وأجهزة الأمن الأخرى ذات الصلة وكذلك الأبحاث والكتب والمطبوعات والنشرات التي تصدرها الوزارات والأجهزة الماثلة ووسائل الإيضاح. كذلك دعم الأجهزة الأمنية بأحدث التقنيات وتدريب العاملين من خلال دورات تدريبية مشتركة مع عقد اللقاءات الدورية وتبادل الزيارات الميدانية بين العاملين في وزارات الداخلية وأجهزة الأمن⁵³.

أما في مجال التحقيقات والمباحث الجنائية توصلت دول مجلس التعاون الخليجي إعداد دراسة قاعدة معلومات أمنية تحق الربط الآلي بين دول المجلس في مجال التحقيقات والمباحث الجنائية، ويجري العمل على تمكين دول المجلس من استخدام المنظومة (I24-7) المعمول بها في المنظمة الدولية للشرطة الجنائية (الأنتربول) فيما بين دول المجلس فقط، كما يجري العمل إيجاد قانون استرشادي لدول المجلس لمكافحة الجرائم الإلكترونية⁵⁴.

الخاتمة:

جريمة التزوير الإلكتروني من الأنماط الإجرامية الحديثة التي تتطلب المواجهة سواء على المستوى الداخلي أو الدولي وهذا بسبب سرعة تناميها وتزايد درجة ارتقائها، مستفيدة من التطورات الحاصلة في مجال تقنيات المعلومات.

ويتضح من خلال دراسة موضوع التزوير الإلكتروني أنها تتميز بطبيعة خاصة تميزها عن جريمة التزوير التقليدية لأن ارتكابها يتطلب معرفة جديّة بتقنية الحاسب الآلي، وعليه يتزايد التزوير الإلكتروني بوتيرة سريعة في الفترة الأخيرة في الوقت الذي حلت فيه المحررات الإلكترونية والبطاقات الإلكترونية محل الوثائق والمحررات الورقية.

إن جريمة التزوير الإلكتروني تؤدي حتماً إلى فقدان الثقة بالتعاملات الإلكترونية في مختلف المجالات. لقد وسع المشرع من خلال القانون رقم 02-24 من نطاق التجريم ليشمل التزوير الإلكتروني، مما يواكب التطورات الحديثة في مجال الجرائم المالية والإدارة، كما غرز دور الخبرة الجنائية والرقابة الإدارية والقضائية في التصدي لهذه الجريمة، ومن جهة أخرى تكريس البعد الدولي للقانون 02-24 بامتداد تطبيقه للجرائم حتى إذا وقعت في الخارج.

ولضمان عدم إفلات الجناة من المساءلة الجنائية وجب العمل قدر المستطاع بين الدول في مجال مكافحة جريمة التزوير الإلكتروني والذي تتجسد في التعاون الأمني الدولي سواء الإقليمي أو الدولي وكذا التعاون القضائي الدولي والذي ساهم بشكل كبير في مواجهة هذه الجريمة العابرة للحدود. وقبل اختتام هذه الدراسة نتقدم بمجموعة التوصيات التالية:

— على المستوى الوطني يجب تطوير الرقابة التكنولوجية الإلكترونية لكشف عمليات التزوير الحديثة بفعالية أكبر من خلال اعتماد تقنيات الذكاء الاصطناعي للكشف عن عمليات التزوير في الوثائق الرسمية والبطاقات الإلكترونية.

— تعزيز التبادل الدولي للمعلومات والخبرات من الجهات الشرطية في مختلف الدول مع تأهيل الكوادر المحلية من أجل مجابهة هذه الجريمة.

— العمل على تعزيز التدريب وبناء القدرات الفنية والتكنولوجية لدى الجهات الأمنية لمكافحة جريمة التزوير الإلكتروني.

الهوامش والمراجع:

- ¹ وفاء صدراي، آليات مكافحة جريمة التزوير الإلكتروني، رسالة دكتوراه جامعة تبسة، الجزائر، 2021، ص 31.
- ² علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، منشأة المعارف، مصر، 1997، ص 63.
- ³ محمد حماد مرهج الهيبي جرائم الحاسوب، دار المناهج للنشر والتوزيع، عمان، 2005، ص 76.
- ⁴ حفص عباس، جرائم التزوير الإلكترونية (دراسة مقارنة)، رسالة دكتوراه، جامعة وهران، 2014، ص 20.
- ⁵ علي كحلون، الجريمة المعلوماتية وتوجيهات محكمة التعقيب، مجلة الأخبار القانونية، تونس، العدد 127/126، 2012، ص 16.
- ⁶ أحمد محمد محروس عبد العال، التزوير الإلكتروني بين التشريع التقليدي وآليات المواجهة الحديثة، المجلة الأكاديمية للأبحاث والنشر العلمي، الإصدار السابعون، 2025، ص 53.
- ⁷ أنظر المواد من 214 إلى 229 من قانون العقوبات القرار رقم 04-23 المؤرخ في 7 ماي 2023.
- ⁸ وفاء صدراي، المرجع السابق، ص 35.
- ⁹ أحمد محمد محروس عبد العال، المرجع السابق، ص 49.
- ¹⁰ أحمد محمد محروس عبد العال، المرجع السابق، ص 50.
- ¹¹ أسامة سمير حسين، الاحتيال الإلكتروني الوجه القبيح للتكنولوجيا، الجندرية للتوزيع، ط 1، الأردن، 2011، ص 96.
- ¹² العبودي عباس، تحديات الإثبات بالمستندات الإلكترونية، منشورات حلبي الحقوقية، ط 1، لبنان، 2011، ص 33.
- ¹³ وفاء صدراي، المرجع السابق، ص 67.
- ¹⁴ فوزية عبد الستار، شرح قانون العقوبات، القسم الخاص، وفقاً لأحداث التعديلات، دار النهضة العربية، ط 3، مصر، 2012، ص 305.
- ¹⁵ فارس خطالي، دليلة ماري، تزوير التوقيع الإلكتروني في بطاقات الائتمان دراسة على ضوء القانون 04-15 المتعلق بالتوقيع والتصديق الإلكترونيين، المجلة الجزائرية للأمن الإنساني، المجلد 5، العدد 02، 2020، ص 664.
- ¹⁶ أنظر المواد من 214 إلى 2016 من قانون العقوبات الجزائري رقم 04-23 المؤرخ في 4 ماي 2023.
- ¹⁷ وفاء صدراي، المرجع السابق، ص 96.
- ¹⁸ وفاء صدراي، المرجع نفسه، ص 99.
- ¹⁹ راجع المادة 02 من القانون 03/14 المتعلق بسندات ووثائق السفر، الجريدة الرسمية، العدد 16 الصادر في 23 مارس 2014.
- ²⁰ منى عصر حمد، المرجع السابق، ص 518.
- ²¹ أحمد محمد محروس عبد العال، المرجع السابق، ص 54.
- ²² نجاح محمد فوزي، وعي المواطن العربي اتجاه جرائم بطاقات الدفع الإلكتروني، ط 1، السعودية، 2007، ص 103.
- ²³ أحمد محمد محروس عبد العال، المرجع السابق، ص 55.

الجهود الدولية لمكافحة جريمة التزوير الإلكتروني في إطار التعاون الأمني والقضائي حسين نسمة

- 24 بن ترعي ليلي، المرجع السابق، ص 82.
- 25 طارق إبراهيم الدسوقي، الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، ص 597.
- 26 وفاء صدراقي، آليات مكافحة جريمة التزوير الإلكتروني، رسالة دكتوراه، جامعة تبسة، الجزائر، 2021، ص 270.
- 27 بن تركي ليلي، المرجع السابق، ص 83.
- 28 نوال حاج مخناش، رشيد شمشيم، التعاون الدولي ومدى فعاليته في مكافحة جرائم تزوير بطاقات الدفع الإلكتروني، مجلة العلوم القانونية والسياسية، المجلد 10، العدد 01، 2019، ص 1124.
- 29 نوال حاج مخناش، رشيد شمشيم، المرجع نفسه، ص 1125.
- 30 بن تركي ليلي، المرجع السابق، ص 85، 86.
- 31 بن تركي ليلي، المرجع نفسه، ص 100.
- 32 طارق إبراهيم الدسوقي، الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2009، ص 599.
- 33 وفاء صدراقي، المرجع السابق، ص 271.
- 34 جمال محمد خلفان محمد النقي، سلطان محمد سالم عوض هيسان المصعبي، التعاون الوطني والدولي في الجرائم الإلكترونية المشكلات والحلول، مجلة المعهد العالي للدراسات النوعية، مجلد 3، العدد 16، 2023، ص 5485.
- 35 وفاء صدراقي، المرجع نفسه، ص 272.
- 36 ترجان نسمة، مداح حاج علي، التعاون الدولي في مجال مكافحة جرائم التوقيع الإلكتروني، مجلة صوت القانون، المجلد 7، العدد 1، 2020، ص 63.
- 37 مفيد نايف الديلمي، غسيل الأموال في القانون الجزائري، ط 1، دار الثقافة للنشر والتوزيع، الأردن، 2006، ص 184.
- 38 وفاء صدراقي، المرجع السابق، ص 276.
- 39 ترجان نسمة، مداح حاج علي، المرجع السابق، ص 64.
- 40 ترجان نسمة، مداح حاج علي، المرجع نفسه، ص 64.
- 41 أيمن رمضان محمد أحمد، الحماية الجنائية للتوقيع الإلكتروني، رسالة دكتوراه، جامعة عين شمس، مصر، 2010، ص 410.
- 42 وفاء صدراقي، المرجع السابق، ص 280.
- 43 بن تركي ليلي، التعاون القضائي الدولي لمكافحة جرائم الاعتداء على التوقيع الإلكتروني (بطاقات الائتمان نموذجاً)، كلية الحقوق، جامعة قسنطينة، العدد 10، الجزء الأول، ص 98.
- 44 بن تركي ليلي، المرجع نفسه، ص 99.
- 45 أسامة بن غانم العبيدي، الجهود الدولية في مكافحة الجرائم المعلوماتية، مجلة الحقوق، العدد 4، 2015، ص 128، 129.
- 46 راجع المادة 16 من القانون 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام ومكافحتها.
- 47 وفاء صدراقي، المرجع السابق، ص 257، 258.
- 48 وفاء صدراقي، المرجع نفسه، ص 258.
- 49 اجتماع المكتب العربي لمكافحة التطرف والإرهاب، اجتماع خبراء عرب لبحث الأمن السيبراني والجرائم الإلكترونية، 2022/10/05، متوفر موقع: <https://nauss.edu.sa/ar-sa/news/pages/5-10-2022.aspx>.
- 50 مجلس وزراء الداخلية العرب، المكتب العربي لمكافحة التطرف والإرهاب، د.ت، متوفر على موقع: aim-council.org.
- 51 مجلس وزراء الداخلية العرب، المرجع نفسه.
- 52 وفاء صدراقي، المرجع السابق، ص 259.
- 53 وفاء صدراقي، المرجع السابق، ص 260.
- 54 الأمانة العامة لمجلس الخليجي، التعاون الأمني، متوفر على موقع: gcc-sg.org.