

## الطابع العابر للحدود للجرائم الإلكترونية وأثره على عمليات التحقيق الجنائي

## The cross-border nature of cybercrime and its impact on criminal investigation processes

عبد القادر عمري

جامعة يحيى فارس - المدينة - الجزائر

Avocat.amri@yahoo.fr

نور الدين بن فرحات \*

جامعة يحيى فارس - المدينة - الجزائر

benferhat.noureddine@univ-medea.dz

تاريخ النشر: 2024/06/30

تاريخ القبول: 2024 /03/ 14

تاريخ الإرسال: 2023 /9/18

## ملخص:

تواجه الجرائم الإلكترونية تحديات عالمية بسبب طبيعتها العابرة للحدود، مما يسفر عن ظهور مشكلة تنازع الاختصاص وضرورة احترام سيادة الدول. تتمثل أهداف هذه الدراسة في تحسين كفاءة التحقيق الإلكتروني وتعزيز التعاون الدولي، وتطوير السياسات والقوانين لتحقيق العدالة، ويعتبر المنهج الوصفي هو الأداة المناسبة لفهم هذه الجرائم وتأثيرها عبر الحدود. توضح النتائج مشاكل متعددة تتعلق بقلة التعاون الدولي وتأخر في وضع القوانين، ونقص في النوعية وتكلفة التطوير التكنولوجي، وعدم وضوح مبدأ الاختصاص القضائي. تتجلى أهمية هذه النتائج في تسليط الضوء على معوقات التحقيق في الجرائم الإلكترونية في العصر الرقمي، ومحاول إيجاد حلول لها بدءاً بالعمل بمبدأ الإقليمية في تحديد الاختصاص القضائي، ثم الموازنة بين ضرورة احترام سيادة الدول وضرورة التحقيق الإلكتروني.

**كلمات مفتاحية:** الجرائم الإلكترونية. سيادة الدول. تنازع الاختصاص. الطبيعة العابرة للحدود. التحقيق الإلكتروني.

**Abstract:**

Cybercrimes pose global challenges due to their transboundary nature, leading to jurisdictional conflicts and the imperative of respecting state sovereignty. This necessitates multiple objectives, including enhancing electronic investigation efficiency, administering justice, fortifying international cooperation, and refining policies and legal frameworks. Employing a descriptive methodology facilitated comprehending the impact of cybercrimes and their cross-border ramifications

The results underscored deficiencies in international cooperation, delays in legislative development, inadequacies in public awareness, the financial burdens of technological advancement, and ambiguity surrounding jurisdictional principles. The significance of these findings lies in comprehending the challenges in cybercrime investigations and the critical need for bolstering international collaboration, improving public awareness, and advancing cybersecurity measures on both national and global scales.

**Keywords:** Conflict of jurisdiction-Cross border nature-Cyber crimes- Cybersecurity-Electronic investigation -State sovereignty.

## مقدمة

بعد أن كانت الجرائم تعالج بوسائل التحقيق التقليدية والبحث العادي، شهدت هذه الجرائم تطورًا كبيرًا نتيجة تقدم التكنولوجيا وتطور العقليات الإجرامية. أصبح المجرمون يستخدمون التكنولوجيا في ارتكاب جرائمهم، مما أدى إلى عدم ملائمة التحقيقات التقليدية لمثل هذه الجرائم الإلكترونية وزيادة صعوبة التحقيق فيها بشكل كبير بسبب طبيعتها العابرة للحدود، حيث إنها جرائم غير مادية وغير ملموسة تنتقل بسهولة عبر الفضاء الرقمي من دولة إلى أخرى. هذه الطبيعة العابرة للحدود خلقت تحديين رئيسيين أمام جهات التحقيق. يتمثل الأول في تحديد الاختصاص القضائي للتحقيق في الجرائم الإلكترونية، حيث أصبحت الدول تدعي اختصاصها في التحقيق بسبب تأثرها بالجريمة وطبيعتها العابرة للحدود. والثاني يتعلق بتجاوز سيادة الدول الأخرى التي تحمل آثار تلك الجريمة.

بالنسبة لتنازع الاختصاص بالتحقيق في الجرائم الإلكترونية فقد كان مبدأ الإقليمية الفاصل الوحيد لهذه المسألة باعتماد مفهومه الواسع في تحديد الجهة المختصة مكان وقوع الجريمة الإلكترونية، وعلى هذا الأساس يقوم المحققون بتنفيذ عمليات التحقيق والتفتيش داخل هذه الدولة المختصة، لكن في حالات معينة تتطلب حالات التفتيش الإلكتروني استخدام أجهزة التحقيق التابعة لدولة أخرى تحمل آثار هذه الجريمة، لغرض الوصول إلى معلومات أو بيانات مخزنة في أجهزة كمبيوتر تقع ضمن نطاق سيطرتها. دون الحصول على موافقتها أو تعاونها، هذا السلوك قد يؤدي إلى تصاعد التوترات الدبلوماسية و تجاوز سيادة الدول الأخرى التي تحمل آثار تلك الجريمة. مما يستند إلى الحاجة الملحة للتوازن بين التحقيق في الجريمة واحترام سيادة الدول.

تتجلى أهمية هذه الدراسة في تسليط الضوء على المعوقات التي تواجه التحقيق في الجرائم الإلكترونية في العصر الرقمي، حيث تعكس التطورات التكنولوجية تأثيرها على طرق التحقيق الجنائي. بالإضافة إلى ذلك، تكشف الطبيعة العابرة للحدود للجرائم الإلكترونية عن تحديات إضافية تواجه عمليات التحقيق، وتؤثر على العمليات الجنائية الشرعية. وتقوم أيضًا بحماية المجتمع من التهديدات الرقمية من خلال التعامل الفعال مع الجرائم الإلكترونية، مما يعزز الأمان والسلامة العامة. وتدعم تطوير التشريعات والسياسات الفعالة في مكافحة الجرائم الإلكترونية من خلال تحليل التحديات التي تواجه عمليات التحقيق وضمان فعالية الإجراءات القانونية.

تتمثل أهداف هذه الدراسة في تحسين كفاءة وفعالية عمليات التحقيق في الجرائم الإلكترونية العابرة للحدود، وذلك من خلال ضمان جمع الأدلة وملاحقة الجناة بنجاح، بالإضافة إلى تحقيق العدالة وضمان معاقبة المتورطين في الجرائم الإلكترونية دون المساس بحقوقهم. وتشمل الأهداف أيضًا تعزيز التعاون الدولي في مكافحة الجرائم الإلكترونية وتوجيه جهود مشتركة للحد من هذه الجرائم، بالإضافة إلى تطوير السياسات والقوانين من خلال تقديم توصيات لتحسين السياسات والإطار القانوني لتسهيل التحقيقات العابرة للحدود. وتهدف أيضًا إلى حماية سيادة الدول من خلال تطوير آليات للتحقيق تحترم سيادة الدول وتجنب التصاعد في التوترات الدبلوماسية، وتوجيه الأفراد والمؤسسات حول كيفية التعامل مع التحقيقات العابرة للحدود في حالات الجرائم

الإلكترونية، بالإضافة إلى زيادة التوعية بأهمية مكافحة الجرائم الإلكترونية وتأثيرها على المجتمعات والاقتصادات.

من خلال ما سبق يمكن طرح الإشكالية التالية:

كيف تؤثر الطبيعة العابرة للحدود الخاصة بالجرائم الإلكترونية على عمليات التحقيق الجنائي؟  
اتبعتنا في إجابتنا على هذه الإشكالية منهج من المناهج المعتمدة في الدراسات القانونية، هو المنهج الوصفي، لوصف الطبيعة العابرة للحدود للجرائم الإلكترونية، وتحديد الآثار الناتجة عنها المتمثلة في كل من تنازع الاختصاص بالتحقيق ومشكلة احترام سيادة الدول.

نقسم هذه الدراسة الى قسمين:

أولاً: تنازع الاختصاص بالتحقيق في الجرائم الإلكترونية

ثانياً: مشكلة احترام سيادة الدول

**أولاً: تنازع الاختصاص بالتحقيق في الجرائم الإلكترونية**

في عصر يمتد عبر الأفق الرقمي يتسع صدى الجرائم الإلكترونية<sup>1</sup> ليصبح واحداً من أبرز التحديات الجنائية الحديثة. إنها ليست مجرد أفعال إجرامية، بل هي حقيقة تجاوز الحدود والقوانين الوطنية. هذا التطور الملحوظ يجد دعماً في التفاعل الوثيق بين هذه الجرائم وعالم الشبكات الرقمية، حيث يعتمد وجودها على انسيابها داخل شبكات عالمية تمتد عبر القارات.

ينفذ المجرم الإلكتروني أفعاله باستخدام أدواته الإلكترونية، مثل الحواسيب والأجهزة الذكية، دون تقييدات جغرافية، يمكن للمنفذ أن ينشر برامج ملوثة من جهازه الإلكتروني إلى أرجاء العالم، تجاوزاً بذلك حدود البلد الذي بدأت فيه الجريمة الإلكترونية. هذا النهج، المعروف بالتجاوز الحدودي، يشكل تحديات قانونية معقدة وكذا ينشأ عنه صعوبات تعقب الدليل الرقمي، ويولد تنافساً قانونياً بين عدة جهات، مما يستدعي التنسيق الدولي والاستجابة المشتركة لمواجهتها بفعالية.<sup>2</sup>

### 1. مبدأ الإقليمية مبدأ معتمد لتحديد الاختصاص بالتحقيق في الجرائم الإلكترونية

تعقب الجرائم الإلكترونية عبر الحدود يشكل تحدياً كبيراً في عالم الأمان الرقمي. إذ يُشكّل العبور الإلكتروني الذي يعتر من أهم خصائص الجريمة الإلكترونية<sup>3</sup>، مشكلاً في تحديد الاختصاص القضائي وتطبيق القوانين، حيث يجد محققون<sup>4</sup> وسلطات قضائية أنفسهم في مواجهة تعقيدات جديدة في مجال مكافحة الجرائم الرقمية.

فمثلاً، يقوم المجرم المعلوماتي في دولة معينة بالاختراق وتحويل الأموال من حسابات أو مواقع بنوك في دولة أخرى إلى دولة ثالثة. وما يميز الجريمة المعلوماتية هنا هو أن المجرم يبقى مختبئاً في مكانه دون الحاجة للقيام بأي نشاط في الواقع، حيث يكفيه فقط جهاز كمبيوتر واتصال بالإنترنت للقيام بأعماله الإجرامية في أي مكان في العالم.<sup>5</sup>

فيما تسعى بعض الدول لمحاسبة المجرمين الذين يقتربون جرائمهم داخل حدود ترابها بموجب مبدأ الاختصاص الإقليمي، تسعى دول أخرى لمحاسبة المجرمين الذين يحملون جنسيتها بموجب مبدأ الشخصية. ولا تقتصر التحديات على ذلك، بل تتضمن أيضاً محاولات لحماية الأنظمة الإلكترونية المعرضة للتهديد من خلال تطبيق مبدأ العينية القانوني، وهذا يتطلب توازناً دقيقاً بين الحفاظ على الأمان الرقمي واحترام حقوق الأفراد.<sup>6</sup>

### 1.1. المفهوم التقليدي للركن المادي للجرائم وأثره على تحديد الاختصاص بالتحقيق

وبخلاف ذلك فمبدأ الإقليمية<sup>7</sup> يميز العديد من الجرائم الإلكترونية بتفرقتها المكانية وتوزعها عبر عدة إقليمية. حيث يمكن أن يبدأ المجرم بارتكاب جريمة في إقليم دولة معينة، وتنتشر تداعياتها الإجرامية في دولة أو دول أخرى، مثل إرسال برنامج ضار أو نشر صور إباحية من جهاز إلكتروني في إحدى البلدان إلى جهاز آخر في دولة أخرى عبر أجهزة متعددة تنتشر في دول مختلفة. هذا يثير تحديات في تحديد الاختصاص القضائي المناسب للتحقيق والتحديد القانوني الذي يجب تطبيقه. وقوانين تحديد موقع وقوع الجريمة تختلف من دولة إلى أخرى، مما يجعل الأمور أكثر تعقيداً.<sup>8</sup>

تُظهر بعض الدول أن الاعتبار الرئيسي لتحديد مكان وقوع الجريمة هو الموقع الذي وقع فيه النشاط الإجرامي، بغض النظر عن المكان الذي تحققت فيه نتائجه أو حتى المكان الذي كان من المفترض حدوثه.<sup>9</sup> بينما يعتبر البعض الآخر أن المكان ينبغي تحديده استناداً إلى المكان الذي تحققت فيه النتيجة الإجرامية أو كان مقرراً أن تحقق.<sup>10</sup> هناك أيضاً فريق ثالث من الدول يرون أن الأمور تتوقف على وجود أحد هذين الضابطين لتحديد مكان وقوع الجريمة<sup>11</sup>.<sup>12</sup>

المفهوم التقليدي للركن المادي للجرائم يُعتبر محدوداً وغير قادر على مواجهة التحديات الحديثة المتعلقة بالجرائم الإلكترونية والتي تتسم بتفرقتها المكانية وتوزعها عبر الإقليميات المختلفة. يجب أن يُفهم الركن المادي بشكل أوسع ليتناسب مع الواقع الرقمي الحديث، حيث يشمل ذلك تقدير الجهة المسؤولة للجريمة بناءً على موقع النشاط الإجرامي والنتائج المترتبة عنه، بغض النظر عن المواقع الفعلية للأطراف المعنية. يجب أن تتبنى الدول مفاهيم جديدة تسمح بتحديد الاختصاص القضائي بشكل فعال في عصر الجرائم الإلكترونية، مع تعزيز التعاون الدولي ووضع قوانين وآليات دولية لمواجهة هذه التحديات الجديدة بشكل شامل وفعال.

### 2.1. المفهوم الواسع للركن المادي للجرائم وأثره على تحديد الاختصاص بالتحقيق

لمبدأ الإقليمية مفهوم واسع للغاية عندما يتعلق الأمر بتحديد مكان ارتكاب الجريمة الإلكترونية. لم يعد هناك حاجة لوقوع فعل مادي أو وجود عناصر مادية محددة لتحقيق الجريمة، حيث تُزال النظرة التقليدية للجرائم تقتصر على العمليات الجسدية أو المادية. بدلاً من ذلك، تم استبدال هذه النظرة بواقعية العصر الحالي، حيث يمكن ارتكاب هذه الجرائم في العالم الرقمي دون أن تترك أثاراً ملموسة، وهذا ما جعل من تحديد موقع ومكان ارتكاب الجريمة في العالم الافتراضي تحدياً قانونياً أكبر وأكثر تعقيداً.<sup>13</sup>

المفهوم الواسع للركن المادي للجرائم يعكس التطورات في التكنولوجيا والعالم الرقمي، حيث لم يعد هناك حاجة لوجود عناصر مادية محددة لتحديد وجود الجريمة. يتيح هذا المفهوم الجديد فرصاً أوسع لتحديد الاختصاص بالتحقيق، مما يتطلب تكييف الأنظمة القانونية والقضائية لمواجهة هذا التطور. يجب أن يتخذ القضاء والفقه مواقف متقدمة ومرنة لمواجهة هذه التحديات القانونية الجديدة، وضمان توافق التشريعات مع الواقع الرقمي الحالي لتحقيق العدالة وحماية المجتمع من جرائم الإنترنت.

## 2. موقف القضاء والفقه من مبدأ الاقليمية المعتمد في تحديد الاختصاص بالتحقيق

في سياق تطور قضايا الجرائم الإلكترونية، يظهر تعقيد هذا المجال وأبعاده الدولية بوضوح. واحدة من القضايا المشهورة التي تسلط الضوء على هذا التحدي تعود إلى شركة ياهوو. هذه القضية أثارت تساؤلات حول الاختصاص القضائي والتشريعات القانونية التي تتعامل مع قضايا الجرائم الإلكترونية عبر الحدود. تتعلق هذه القضية بتجاوز المجرم الإلكتروني للحدود الجغرافية عن طريق نشر رسائل غير مشروعة على منصة ياهوو. وعلى الرغم من أن الموقع والخادم الذي يستضيفه يمكن أن يكونا خارج نطاق القوانين في بعض البلدان، إلا أن تأثير هذه الجريمة تجاوز الحدود ليصل مصالح وأفراداً في دول أخرى. وهذا أثار تساؤلات حول موقع وقوع الجريمة ومن يتحمل المسؤولية الجنائية.<sup>14</sup>

### 1.2. موقف القضاء الفرنسي

قرر القضاء الفرنسي أنه يمكنه النظر في هذه القضية وفقاً للقوانين الفرنسية. تأسس هذا القرار على استنتاج أن رسائل الجريمة تظهر في فرنسا ويمكن للجمهور الفرنسي الوصول إليها على الرغم من تواجد المركز والخادم خارج الإقليم الفرنسي. ونتيجة لذلك، تم اعتبار الجريمة مرتكبة في أي مكان يتم فيه عرض هذه الرسائل غير المشروعة، وفقاً للمادة 411 من القانون الفرنسي.<sup>15</sup>

### 2.2. موقف القضاء الأمريكي

النظام القضائي الأمريكي يظهر تفاعلاً استثنائياً تجاه التحديات الناشئة من جراء الجرائم الإلكترونية. حيث قرر التوسع في اختصاصه ليشمل الجرائم التي تنشأ خارج حدود البلاد وتلامس مصالح مواطنيها. على سبيل المثال، إذا تم نقل بيانات من دولة أخرى وأثرت سلباً على مصالح المواطنين الأمريكيين أو أضررتهم للمخاطر، سيتم معالجة هذه الجريمة بموجب القوانين الأمريكية.<sup>16</sup>

فلنأخذ مثلاً، إذا تم نشر محتوى إجرامي على خادم موجود في بريطانيا، وكان هذا المحتوى متاحاً للمواطنين الأمريكيين، سيقوم القضاء الأمريكي بالتحقيق واتخاذ الإجراءات اللازمة لمعالجة هذه القضية. هذا يعكس التزام الولايات المتحدة بالحفاظ على أمن مواطنيها ومكافحة الجرائم الإلكترونية على الساحة الدولية بأسلوب احترافي ومتميز.<sup>17</sup>

### 3.2. وقف الفقه

الفقه يسعى إلى تقديم حلاً متوازناً يعتمد على توافق بين مبادئ متعددة، مما يسمح للدول التي تجمع بين ثلاثة مبادئ رئيسية بمنحها الاختصاص. يتأكد هذا الاختصاص بناءً على مبدأ الإقليمية كأساس لتحديد الاختصاص الأنسب والأكثر تطبيقاً، خاصةً عندما يكون مكان الجريمة مركز اهتمام التحقيقات، حتى في حالة الجرائم الإلكترونية التي تتطلب تحقيقات معقدة. وفقاً لهذا النهج، يجب أن تكون الدول الرائدة في بدء التحقيقات ومتابعة الجناة هي التي تسهم في تقديم إجراءات تحقيقية فعّالة تستند إلى معايير علمية وتتجاوز مفهوم السيادة الوطنية.<sup>18</sup>

### 3. موقف الإتفاقيات الدولية والمشرع الجزائري من مبدأ الإقليمية المعتمد في تحديد الإختصاص بالتحقيق

لحل مشكلة تنازع الاختصاص في التحقيقات بشأن الجرائم الإلكترونية، قامت الدول باتخاذ إجراءات تنظيمية تهدف إلى تجنب هذا التنازع. تمثل هذه الإجراءات في تأسيس اتفاقيات دولية ثنائية ومتعددة الأطراف تحتوي على تفصيلات وضوابط واضحة تحدد توزيع الولاية القضائية بين الدول المتعاقدة، كما قام المشرع الجزائري بمحاولة حل هذا النزاع من خلال نصوص قانونية.

#### 1.3. موقف الإتفاقيات الدولية

المادة (15) في اتفاقية منظمة الأمم المتحدة لمكافحة الجريمة المنظمة تنص على هذه الشروط وهي:<sup>19</sup>

عندما يتم ارتكاب الجريمة داخل إقليم دولة معينة.

عندما تكون الجريمة موجهة ضد أحد مواطني تلك الدولة.

عندما يتم ارتكاب الجريمة بواسطة مواطني تلك الدولة أو بواسطة شخص ليس لديه جنسية ويعيش في إقليمها.

وتشير هذه المادة أيضاً إلى أنه في حالة وجود معلومات عن تحقيقات جارية في إحدى الدول بشأن نفس

الجريمة أو إذا علمت بأن دولة واحدة أو أكثر قامت باتخاذ إجراءات تحقيقية بالفعل، يجب على السلطات

المعنية في هذه الدول التشاور والتنسيق لضمان تنفيذ تدابير منسقة للتحقيق ومتابعة الجريمة.

مع اتفاقية مجلس أوروبا لمكافحة الجريمة الإلكترونية<sup>20</sup>، تم تنظيم قضية الاختصاص بطريقة مختلفة.

المادة (22) في هذه الاتفاقية تنص على التزام كل طرف باتخاذ التدابير التشريعية اللازمة لتحديد الاختصاص

بشأن الجرائم الإلكترونية. وهذا التحديد يشمل:

تنفيذ الاختصاص عندما تحدث الجريمة داخل إقليم الدولة.

تفعيل الاختصاص إذا ارتكبها مواطنو الدولة وكانت هذه الجريمة معاقباً عليها وفقاً للقوانين الجنائية للدولة التي

وقعت فيها الجريمة.

معالجة الاختصاص في حالة وقوع الجريمة خارج الاختصاص القضائي الإقليمي لأي دولة.

من وجهة نظرنا، المواد (15) و (22) في اتفاقية منظمة الأمم المتحدة لمكافحة الجريمة المنظمة واتفاقية

مجلس أوروبا لمكافحة الجريمة الإلكترونية تبرز أهمية التعاون الدولي في مجال مكافحة الجرائم، بما في ذلك

الجرائم الإلكترونية. تحدد هذه المواد معايير وإجراءات لتحديد الاختصاص القضائي للتحقيق في الجرائم، مما

يسهم في توجيه الجهود المشتركة لمكافحة الجريمة عبر الحدود. يُعزز هذا النهج الدولي التنسيق والتعاون بين الدول لضمان تنفيذ التدابير المنسقة والفعالة في التحقيق ومتابعة الجرائم، مما يساهم في تحقيق العدالة وتعزيز الأمان الإلكتروني على الصعيدين الوطني والدولي.

### 2.3. موقف الشرع الجزائري

بناءً على الأسس القانونية المطبقة في الجزائر، تم التركيز بشكل كبير على التصدي لتحديات الصراع فيما يتعلق بالاختصاص في الجرائم ذات الصلة بتكنولوجيا المعلومات والاتصالات. هذا التوجه تم تعزيزه من خلال المادة 15 في القانون رقم 04-09<sup>21</sup>، الخاص بالوقاية من الجرائم المرتبطة بتكنولوجيا المعلومات والاتصالات. تنص المادة على أن: "بالإضافة إلى قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية، فإن المحاكم الجزائرية تكون مختصة أيضاً بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الوطن عندما يكون مرتكبها أجنبياً وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني".

بالنظر الدقيق إلى هذا النص، نجد أنه يُعد تكراراً للمادة (588) من قانون الإجراءات الجزائية، حيث يُعيد مبدأ الاختصاص العيني بدون إدخال أي تعديلات جديدة أو تحسينات.

بالمقارنة مع المادة (15) من القانون رقم 04-09، يُظهر هذا النص نقاط تشابه واضحة بين النصين. لا يُلمح النص إلى أي تغيير كبير في قواعد الاختصاص، ويُمكن القول إنه يتبنى نفس المفهوم الموجود في المادة (15) من القانون 09/04، دون إضافة جديدة تُذكر.

### ثانياً: مشكلة إحترام سيادة الدول

في عالم متصل دائماً ومتقدم تكنولوجياً، تنشأ مسألة تجاوز الحدود واحترام سيادة الدول كمسألة معقدة. عندما نتحدث عن التفتيش الإلكتروني العابر للحدود، نتحدث عن التحديات الجديدة التي تواجهنا. يعني التفتيش عن بعد البحث عن معلومات وبيانات تخزن في أجهزة إلكترونية تقع خارج نطاق سيادة الدول. هذه المعلومات قد تكون مفيدة للكشف عن الجرائم الإلكترونية. تطرح هذه الحالات تحديات تتعلق بكيفية التعامل مع البيانات الحساسة دون انتهاك سيادة الدول الأخرى.

### 1. علاقة التفتيش الإلكتروني بمسكلة إحترام سيادة الدولة

بناءً على التصورات القانونية المتبنات، تتطلب حالات التفتيش الإلكتروني العابرة للحدود امتناعاً عن استخدام أجهزة التحقيق التابعة لدولة ما لغرض الوصول إلى معلومات أو بيانات وأدلة إلكترونية<sup>22</sup> مخزنة في أجهزة كمبيوتر تقع ضمن نطاق سيطرة دولة أخرى. هذا الأمر يُعتبر انتهاكاً لسيادة الدولة الأخرى وتجاوزاً للمبادئ القانونية المخصصة لتحديد الاختصاص القضائي. يؤكد خبراء القانون الدولي أن احترام سيادة الدول يعد أمراً بالغ الأهمية وأنه يجب تجنب التدخل في شؤونها الداخلية أثناء تنفيذ عمليات التفتيش الإلكتروني خارج حدودها.<sup>23</sup>

### 1.1. موقف منظمة الأمم المتحدة من تطبيق التفتيش الإلكتروني على الدول

تتناول تقرير منظمة الأمم المتحدة المتعلق بالجرائم المعلوماتية يظهر أهمية احترام سيادة الوطنية في مجال التحقيقات الإلكترونية. يُشدد التقرير على أن أي محاولة مباشرة لاختراق قاعدة بيانات جهاز كمبيوتر موجود في إقليم دولة أجنبية دون الحصول على موافقتها أو إعلامها يُعتبر انتهاكاً لسيادتها ويتعارض مع مبدأ عدم التدخل في شؤونها الداخلية. هذا التقرير يسلط الضوء على أهمية إيجاد توازن بين حقوق الدول وسيادتها وبين الضرورة الحقيقية لمكافحة الجرائم التكنولوجية على الصعيدين الوطني والدولي. يعكس هذا التوازن الحساسية القائمة بين الحاجة إلى الأمان السيبراني والالتزام بالقوانين والأعراف الدولية.<sup>24</sup>

ان موقف منظمة الأمم المتحدة يعكس الحاجة الملحة لتحقيق توازن بين الحقوق السيادية للدول والضرورة الواقعية لمكافحة الجرائم المعلوماتية. يتناول التقرير بشكل دقيق أهمية احترام سيادة الدول وعدم التدخل في شؤونها الداخلية، مع التأكيد على ضرورة التعاون الدولي في مجال مكافحة الجرائم التكنولوجية. يجسد هذا الموقف الحساسية للتحديات الأمنية الحديثة وضرورة التعاون الدولي المشترك لمواجهةها، ويبرز أهمية وضع قواعد وآليات دولية لتحقيق التوازن بين الأمن السيبراني واحترام سيادة الوطنية.

### 2.1. موقف اللجنة الأوروبية من تطبيق التفتيش الإلكتروني على الدول

بناءً على هذا السياق، أصدرت اللجنة الأوروبية المختصة في معالجة مسائل الجرائم الإلكترونية توصية تشدد على أن أي اختراق مباشر لأغراض التفتيش أو التحكم أو أي إجراء تحقيق آخر داخل إقليم دولة أجنبية يُعتبر تداخلاً في اختصاص السلطات التحقيقية الوطنية لتلك الدولة. هذا ينتج عنه إلغاء صحة هذا الإجراء وعدم قانونية الأدلة المحصلة من خلاله.<sup>25</sup>

أكدت القضاء هذا الموقف في العديد من القضايا، بما في ذلك قضية الاحتيال الإلكتروني المعروضة أمام المحكمة الألمانية، حيث رفضت محكمة التحقيق الألمانية بشدة منح إذن بالوصول عن بُعد إلى البيانات المخزنة في حاسوب موجود في سويسرا دون موافقة أو تعاون السلطات القضائية السويسرية، معتبرة ذلك انتهاكاً واضحاً لسيادة الدولة المعنية.<sup>26</sup>

موقف اللجنة الأوروبية يعكس التزامها بمبادئ الاحترام المتبادل لسيادة الدول وعدم التدخل في شؤونها الداخلية. توصية اللجنة تؤكد على أهمية احترام الاختصاص الوطني للسلطات التحقيقية في كل دولة، وتعزز مبدأ التعاون الدولي والحصول على الموافقة المسبقة قبل أي عملية تفتيش أو تحقيق إلكتروني داخل إقليم دولة أخرى. يعكس هذا الموقف التزام اللجنة بضمان حماية حقوق الأفراد وتطبيق القانون بطريقة شفافة وقانونية، مما يعزز الثقة في العدالة ويحد من انتهاكات الخصوصية وسيادة الدول.

### 3.1. موقف المجلس الأوروبي من تطبيق التفتيش الإلكتروني على الدول

في سياق مماثل، صدرت توصية من قبل اللجنة الأوروبية المعنية بقضايا الجرائم الإلكترونية في عام 1995، والتي تتعلق بقضايا قانون الإجراءات الجزائية المرتبطة بتكنولوجيا المعلومات. هذه التوصية، المعروفة

برقم (13)، أكدت على ضرورة تجنب التدخل الإلكتروني عبر الحدود أو التفتيش عن بعد دون وجود اتفاقيات تعاون قضائي متفق عليها بين الدول المعنية. تعبر هذه التوصية عن مفهوم أساسي يتعلق بالاحترام المتبادل للسيادة الوطنية، حيث يجب أن يتم التفتيش الإلكتروني العابر للحدود وفقاً لإتفاق مسبق بين الدول، وإلا فإنه سيتم اعتباره غير قانوني ويتسبب في بطلان المزامنة المرتبطة به. هذا الموقف يعكس أهمية تعزيز التعاون والتنسيق الدولي في مكافحة الجرائم الإلكترونية والحفاظ على سيادة الدول واحترام القوانين الوطنية والدولية.<sup>27</sup>

## 2. الموازنة بين ضرورة التفتيش الإلكتروني في الجرائم المعلوماتية وضرورة احترام سيادة الدولة:

مسألة توازن حرية البحث والحصول على المعلومات مع الحفاظ على الأمان الإلكتروني وحقوق الأفراد في العصر الرقمي. غالباً ما تُثير الجرائم المعلوماتية تحديات قانونية تتعلق بالتحقيق والتفتيش عبر الحدود، وهو ما يتطلب معالجة دقيقة.

### 1.2. دور إتفاقية بودابست في خلق التوازن بين التفتيش الإلكتروني وضرورة احترام سيادة الدول

في هذا السياق، أُنيت إتفاقية بودابست الأوروبية لمكافحة الجرائم المعلوماتية عام 2001 كخطوة مهمة في تقديم إطار قانوني للتعامل مع هذه القضايا. تركز هذه الإتفاقية على تعزيز التعاون القضائي بين الدول الأعضاء، مما يساهم في تسهيل التحقيقات وجمع الأدلة الإلكترونية المتعلقة بالجرائم المعلوماتية. من ناحية أخرى، تنص الإتفاقية على حالتين استثنائيتين يمكن فيهما اللجوء إلى التفتيش الإلكتروني عبر الحدود دون الحاجة إلى إذن مسبق من الدولة المعنية. الحالة الأولى تتعلق بالمعلومات العامة أو البيانات المتاحة علناً، في حين تتطلب الحالة الثانية موافقة صاحب تلك المعلومات.<sup>28</sup>

إتفاقية بودابست الأوروبية تلعب دوراً مهماً في خلق التوازن بين التفتيش الإلكتروني واحترام سيادة الدول وحقوق الأفراد. توفر الإتفاقية إطاراً قانونياً للتعاون القضائي بين الدول الأعضاء، مما يسهل التحقيقات في جرائم المعلوماتية وجمع الأدلة الإلكترونية بطريقة قانونية وشفافة. بالإضافة إلى ذلك، تحدد الإتفاقية حالات استثنائية تسمح بالتفتيش الإلكتروني عبر الحدود، لكنها تتطلب موافقة أو موقع صاحب المعلومات. يعكس هذا التوازن الحساسية لضمان الأمن السيبراني ومكافحة الجرائم المعلوماتية دون المساس بحقوق الأفراد وسيادة الدول، مما يعكس التحديات والاحتياجات في عصر التكنولوجيا والمعلوماتية.

### 2.2. دور المشرع الجزائري في خلق التوازن بين التفتيش الإلكتروني وضرورة احترام سيادة الدول

في إطار ممارسة السلطات الجزائرية لسياستها القانونية، يظهر أن المشرع الجزائري قرر أن يتبع مقاربة متحفظة تجاه التفتيش عن بعد لأنظمة الحواسيب المتواجدة خارج الإقليم الوطني. وهذا بمعنى أنه لن يُسمح بالتفتيش الإلكتروني إلا إذا كان ذلك ضمن إطار التعاون المتبادل مع السلطات الأجنبية المختصة وتحت

اتفاقيات دولية ذات صلة. يتجلى هذا الموقف بوضوح من خلال نص المادة 5/2 في القانون رقم 09/04 بحيث تنص على: "إذا تبين مسبقاً بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقاً من المنظومة الأولى مخزنة في منظمة معلوماتية تقع خارج الإقليم الوطني، فالحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقاً للاتفاقيات الدولية ذات صلة ووفقاً لمبدأ المعاملة بالمثل".

تُظهر هذه السياسة التزاماً بمبدأ سيادة الوطنية وضرورة احترام القوانين الوطنية، وفي الوقت نفسه، تؤكد على أهمية التعاون الدولي في مكافحة الجرائم الإلكترونية. ولتحقيق هذا التوازن الرقمي، يتعين على الجهات المعنية الالتزام بالتعاون الدولي والالتزام بالاتفاقيات الدولية ذات الصلة، مما يساهم في حماية سيادة الوطنية ومكافحة الجريمة الإلكترونية على الساحة العالمية.

بالنظر إلى الواقع الراهن، نجد نقاشاً مستمراً حول مدى توافق التفتيش الإلكتروني العابر للحدود مع مبدأ احترام سيادة الدول. يُرى أن استخدام هذه التقنية يُعد تحدياً كبيراً أمام جهود مكافحة الجريمة الإلكترونية. هناك آراء مختلفة بشأن كيفية التعامل مع هذه القضية المعقدة. يُمكن للبعض أن يروجوا لاستخدام التفتيش الإلكتروني عن بُعد دون علم الدولة الأجنبية المعنية كوسيلة لمكافحة الجريمة الإلكترونية عبر الحدود. ومع ذلك، يُثير هذا النهج مشكلات متعلقة بحقوق الخصوصية وسيادة الوطنية.

من ناحية أخرى، يُمكن للآخرين أن يُفضلوا التعاون مع الدول الأخرى وطلب المساعدة من سلطات التحقيق الأجنبية بشكل قانوني. ومع ذلك، هذا النهج يعاني من التأخير وعدم الفعالية في الكثير من الحالات. بشكل عام، هناك حاجة إلى تطوير إطار قانوني ودولي يضمن استخدام التفتيش الإلكتروني العابر للحدود بشكل عادل وفعال مع احترام حقوق الأفراد وسيادة الدول. هذا سيساهم في تحقيق التوازن المطلوب بين مكافحة الجريمة الإلكترونية وحماية الحقوق والحريات الأساسية.

### الخاتمة

تتميز الجرائم الإلكترونية بطبيعتها العابرة للحدود والتي بدورها تخلق مشاكل متعلقة بتنازع الاختصاص بالتحقيق في الجرائم الإلكترونية، ومشكلة احترام سيادة الدول.

لهذا أردنا من خلال هذا البحث الوصول لحل لهذه المشاكل المتمثل في اعتماد كل من مبدأ الإقليمية بمفهومه الواسع لتحديد الاختصاص بالتحقيق، والموازنة بين ضرورة التفتيش واحترام سيادة الدول أثناء التحقيق في هذه الجرائم الإلكترونية.

من خلال دراسة هذا الموضوع توصلنا الى مجموعة من النتائج والتوصيات تتمثل فيما يلي:

### النتائج

قلة التعاون الدولي: عدم وجود تعاون كافٍ بين الدول قد ساهم في هروب مرتكبي الجرائم الإلكترونية من العدالة وصعوبة متابعتهم.

تأخر في وضع القوانين: يمكن أن يستغرق وضع قوانين دولية واضحة وشاملة وقتاً طويلاً، مما يعني أنه لا يمكن الاعتماد عليها فوراً.

نقص في التوعية: إذا لم تتم جهود كافية لتعزيز التوعية بمخاطر جرائم الإنترنت، قد يستمر التهديد دون تقليده. تكلفة التطوير التكنولوجي: يمكن أن يكون تطوير التكنولوجيا المخصصة لمكافحة الجريمة الإلكترونية مكلفاً، وهذا قد يكون تحدياً مالياً.

عدم وضوح مبدأ الاختصاص القضائي: سابقاً كان هناك تباين في تفسير مبدأ الاختصاص القضائي، مما أدى إلى تأخير في معالجة الجرائم الإلكترونية وزيادة التنازعات.

التشريعات وطنية غير كافية: القوانين الوطنية القديمة لم تكن كافية لمواجهة تطورات الجرائم الإلكترونية الحديثة.

انتهاكات لحقوق الإنسان: بعض الدول سبق أن انتهكت حقوق الإنسان في مساعيها لمكافحة الجرائم الإلكترونية.

استعمال التقنيات القديمة في التحقيق الجنائي: استخدام التكنولوجيا القديمة قد أدى إلى فشل في تحديد وتتبع مرتكبي الجرائم بشكل فعال.

اتفاقيات دولية محدودة: الاتفاقيات الدولية السابقة لم تكن شاملة بما يكفي لمعالجة جميع جوانب مكافحة جرائم الإنترنت.

نقص في دعم البحث والتطوير: عدم دعم كافٍ للأبحاث والتطوير في مجال التكنولوجيا والقانون أثر على القدرة على التعامل مع تحديات التفتيش الإلكتروني بفعالية.

نقص في التحقيقات القانونية: كان هناك تركيز سابق على التدخلات غير القانونية، مما أثر على القدرة على تحقيق العدالة والمحافظة على السيادة الوطنية.

نقص في الشفافية: كانت السياسات والإجراءات غير واضحة وغير مفهومة بشكل كافي للجمهور، مما أدى إلى عدم الثقة والتوترات في العلاقات الدولية.

### التوصيات

تعزيز التعاون الدولي: من المهم أن تعمل الدول على تعزيز التعاون الدولي في مكافحة جرائم الإنترنت، بما في ذلك تبادل المعلومات والتعاون في التحقيقات.

تطوير قوانين دولية: يجب أن تسعى الدول إلى وضع قوانين دولية تنظم تحقيق الجرائم الإلكترونية وتحديد الاختصاص القضائي بشكل أوسع وأكثر وضوحاً.

تعزيز التوعية: يجب على الحكومات والمنظمات التعاون في توعية المواطنين بمخاطر جرائم الإنترنت وكيفية الوقاية منها.

تطوير تكنولوجيا مكافحة الجريمة: يجب الاستثمار في تطوير تكنولوجيا مكافحة الجريمة الإلكترونية لتعزيز قدرة التحقيق والتتبع.

تحديد مبدأ الاختصاص القضائي بدقة: يجب على القوانين الوطنية والدولية تحديد مبدأ الاختصاص القضائي بشكل واضح ودقيق لتجنب التنازعات والتأخير في التحقيقات.

تطوير التشريعات الوطنية: يجب على الدول تحسين وتطوير قوانينها الوطنية لتكون متناسبة مع التحديات الناشئة من جرائم الإنترنت ومبادئ تحديد الاختصاص القضائي.

الالتزام بحماية المصالح الوطنية: يجب أن تلتزم الدول بحماية مصالحها الوطنية ومواطنيها من التهديدات الإلكترونية والتعاون في مكافحتها.

الالتزام بمبادئ حقوق الإنسان: يجب أن تتخذ الدول إجراءات لضمان أن مكافحة جرائم الإنترنت لا تنتهك حقوق الإنسان والخصوصية الشخصية.

توسيع الاتفاقيات الدولية: يجب أن تعمل الدول على توسيع وتعزيز الاتفاقيات الدولية لتشمل مزيداً من الجوانب المتعلقة بمكافحة جرائم الإنترنت.

التأكيد على أهمية التوازن: يجب أن يتم التأكيد دائماً على أهمية إيجاد توازن بين مكافحة الجرائم المعلوماتية واحترام سيادة الدول للحفاظ على التوازن والعدالة.

دعم الأبحاث والتطوير: يجب دعم الأبحاث والتطوير في مجال التكنولوجيا والقانون لمواجهة تحديات التفتيش الإلكتروني بفعالية واحترام سيادة الدول.

توجيه الشفافية: يجب أن تكون السياسات والإجراءات المتعلقة بالتفتيش الإلكتروني مفهومة بوضوح ومتاحة للجمهور للمساهمة في تعزيز الشفافية وبناء الثقة.

### الهوامش:

<sup>1</sup> الجريمة المعلوماتية على أي سلوك غير مشروع تكون تقنية المعلومات وسيلة لارتكاب الجريمة، أو تكون موضوعاً لها، وعليه فإننا نقترح التعريف التالي: تعد جريمة معلوماتية كل سلوك غير مشروع يرتكب على أنظمة المعالجة الآلية للمعطيات وكذلك كل جريمة تقليدية يمكن ارتكابها أو يسهل ارتكابها بواسطة وسائل تقنية المعلومات. أنظر: حبيباتي بثينة، الطبيعة الخاصة للجريمة المعلوماتية، مجلة دراسات وأبحاث، جامعة الجزائر 1، المجلد 12، العدد 3، 2020، ص 607.

<sup>2</sup> CHAWKI Mohamed, combattre la cybercriminalité, Edition de saint-amans, Paris, 2008, p318.

Voir aussi Rapport explicatif sur la convention du conseil de l'Europe 2023/9/12 : www.Coe.int.

<sup>3</sup> صغير يوسف، الجريمة المرتكبة عبر الإنترنت، مذكرة مقدمة لنيل شهادة الماجستير في القانون، كلية الحقوق والعلوم السياسية جامعة مولود معمري-تيزي وزو، 2013، ص 16.

<sup>4</sup> المحقق الجنائي هو الشخص القائم بأعمال إجراءات التحقيق الجنائي ولا يختلف تعريف المحقق في الجرائم التقليدية عن تعريفه في الجرائم الإلكترونية، فالفرق هنا في نوعية الجريمة وليس في المحقق ويتضح من التعريفات السابقة ان الاختلاف راجع إلى الاختلاف في نطاق النظر إلى عمل المحقق أو تحديده من حيث ما يقوم به المحقق من إجراءات ووسائل، في حين اتجهت

تعريفات من حيث مهام عمله والأعمال المنوطة القيام بها، انظر: خالد علي نزال الشعار، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة مقدمة لنيل شهادة الدكتوراه، كلية الحقوق والعلوم السياسية جامعة المنصورة، 2020، ص25.

<sup>5</sup> بن بادة عبد الحليم، إجراءات البحث والتحري عن الجريمة -المعلوماتية- الخصوصية والإشكالات، مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشور الجلفة، المجلد2، العدد23، 2015، ص89.

<sup>6</sup> عبد محمد بحر، معوقات التحقيق في جرائم الانترنت، مذكرة لنيل شهادة الماجستير في العلوم الشرطية، معهد الدراسات العليا جامعة نايف العربية للعلوم الأمنية، دبي، 1999، ص26.

<sup>7</sup> في مفهوم النظام الاقليمي يتم تنظيم الجرائم في نطاق معين بقوانين الدولة الخاصة بهذا الإقليم. المحاكم في هذا الإقليم تكون المسؤولة الأساسية لمعالجة القضايا التي تنشأ فيه، وقوانين الدول الأخرى لا تلزمها إلا في حالات استثنائية تتعلق بالأمن الوطني أو التعاون الدولي في مكافحة الجريمة أنظر: على احمد راشد، المدخل وأصول النظرية العامة، 1974 ص 185، نقلا عن موسى مسعود ارحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، 2009، ص 12.

<sup>8</sup> DIOP. Abdoulaye, Cour procédure Pénale et TIC article publier sur le site suivant:  
<http://196.1.99.9/moodle/mod/book/print.php?id=106>, 2011. P 14+ 2023/9/9.

<sup>9</sup> أقر بهذا الرأي كل من المشرع الفرنسي والمشرع المصري.

<sup>10</sup> تبني هذا الرأي من طرف المشرع الألماني في عام 1975 و المشرع البلجيكي في عام 1982.

<sup>11</sup> أخذ بهذا الرأي المشرع الدانمركي، المشرع الايطالي والمشرع الترويجي.

<sup>12</sup> ناني لحسن، التحقيق في الجرائم المتصلة بتكنولوجيا المعلوماتية بين النصوص التشريعية والخصوصية التقنية، ط1، النشر الجامعي الجديد، الجزائر، 2018، ص59.

<sup>13</sup> VERGUCHT Pascal, la répression des délits informatiques dans une perspective internationale, thèse de doctoral soutenue a L'université Montpellier 1. le 11 avril 1996, pp. 347-348.

<sup>14</sup> براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة مقدمة لنيل شهادة الدكتوراه، كلية الحقوق والعلوم السياسية جامعة مولود معمري- تيزي وزو، 2018، ص188.

<sup>15</sup> DIOP Abdoulaye, op.cit. p15, voir aussi MIGNARD Jean-Pierre, cybercriminalité et cyber- répression entre désordre et harmonisation mondiale, thèse de doctorat, université paris I panthéon- Sorbonne, 2004, pp 603-604.

<sup>16</sup> من خلال تصدر المحكمة العليا لنيويورك قرارات قاطعة، يظهر بوضوح أن جرائم التجاوز على حقوق المستهلك والدعاية الخادعة تأخذ مكانة كبيرة في النظام القانوني الأمريكي. لا يقتصر الأمر هنا، بل تمتد تلك الأحكام المهمة إلى المحكمة في مينيسوتا، حيث تمت معالجة قضية "جرانتي جات ريسورت"، تُظهر أهميتها فيما يتعلق بنشر موقع لألعاب القمار عبر الإنترنت من ولاية لاس فيغاس في نيفادا. ما يثير الانتباه أكثر هو التجاوب القضائي القوي الذي يظهره القرار الصادر عن الدائرة الخامسة للاستئناف في قضايا القمار والرهان عبر الإنترنت. حيث تم تصنيف تطبيق برمجية فك التشفير (PGP) على الإنترنت على أنه تصدير، مما يظهر تغييراً جذرياً في موقف المحكمة الأمريكية تجاه هذه القضايا. ولاحظ أنها تُعالج هذه القضايا دون الالتفات إلى موقع تطوير البرمجية، مما يجسد التحول البارز في القضاء الأمريكي وتفهمه للأمر التكنولوجية المعاصرة. أنظر تفاصيل هذه القضايا في: عمر محمد بن يونس، الجرائم الناشئة عن استخدام الإنترنت، ط1، دار النهضة العربية، القاهرة- مصر، ص-ص910-908.

<sup>17</sup> CHAWKI Mohamed, op cit, pp 323-324.

<sup>18</sup> جمال براهيمي، مرجع سبق ذكره، ص190.

<sup>19</sup>اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية باليرمو عام 2000.

متوفرة في الموقع التالي:

[http://www.uncjin.org/documents/conventions/dcatoc/final\\_documents\\_2/convention\\_french](http://www.uncjin.org/documents/conventions/dcatoc/final_documents_2/convention_french). 2023/9/12

<sup>20</sup>اتفاقية مجلس أوروبا لمكافحة الجريمة الإلكترونية في الموقع التالي:

<http://convention.coe.int/Treaty/FR/Treaties/Htm/185.htm> 2023/9/12

<sup>21</sup>القانون: رقم 09/4، مؤرخ في 05 أوت سنة 2009، المتضمن القواعد الخاصة بالوقاية المتصلة بتكنولوجية الإعلام والاتصال ومكافحتها، ج.ر. عدد 47، صادرة في 16 أوت 2009، ص 8.

<sup>22</sup> يعرف الدليل المعلوماتي أو الإلكتروني بأنه "عبارة عن معلومات مستخلصة تكون مخزنة إما على جهاز الحاسوب نفسه أو ملحقاته كالأقراص الصلبة الخارجية أو المدمجة، أو بطاقات الذاكرة، أو ذاكرة الطابعة أو متنقلة عبر الشبكات الاتصال والتي يتم التقاطها وتجميعها من أجل تحليلها واسترجاعها بواسطة برامج خاصة"، ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة دكتوراه، كلية الحقوق جامعة باتنة 1، 2016، ص 262.

<sup>23</sup> VERGUCHT Pascal, op.cit, p 406

<sup>24</sup>O.N.U. Manuel des Nations Unies sur la prévention et la répression de la criminalité informatique, New York, Nations Unies. 1994

<sup>25</sup>COMITE EUROPEEN; la Recommandation N°(89)9 sur la criminalité en relation avec Tordinateur et le Rapport final du comité européen pour les problèmes criminels, Strasbourg, 1990,p98.

<sup>26</sup> جمال براهيم، مرجع سبق ذكره، ص 193.

<sup>27</sup> CONSEIL DE L'EUROPE; la Recommandation N°(95) 13 sur les problèmes de procédures pénales liées a la technologie de l'information et exposé des motifs, Strasbourg, 1996, p 188.

<sup>28</sup> CHAWKI Mohammed «< combattre la cybercriminalité >> op.cit., p 333.