

تاريخ القبول: 2021/09/18

تاريخ الإرسال: 2021/05/01

إجراءات جمع الأدلة الرقمية طبقا للاتفاقية العربية لمكافحة جرائم تقنية المعلومات

The procedures of the collection of digital evidences in Arab Convention on Combating Information Technology Offences

ط.د.خيدل أحمد*¹، أ.د/ كيسي زهيرة²¹جامعة تامنغست، مخبر الموروث العلمي والثقافي لمنطقة تامنغست، (الجزائر)،

khid11med@gmail.com

¹جامعة تامنغست، مخبر الموروث العلمي والثقافي لمنطقة تامنغست، (الجزائر)،

zahkis@gmail.com

المخلص:

يهدف هذا المقال إلى دراسة الأحكام الواردة في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات والمتعلقة بتدابير جمع الأدلة الرقمية بشأن جرائم تقنية المعلومات والجرائم المرتبطة بهذه التقنية، وذلك من خلال تحليل المواد التي تضمنتها ومقارنتها بالمواد ذات الصلة التي تضمنتها اتفاقية بودابست لمكافحة جرائم الانترنت.

ومن أجل ذلك قسمت هذه الدراسة إلى شقين، تناول الشق الأول الإجراءات الخاصة بالمعلومات المخزنة، وفي حين تناول الشق الثاني، الإجراءات الخاصة بالمعلومات غير المخزنة، وفي الأخير اختتمت هذه الدراسة بمجموعة من النتائج التي تم التوصل إليها، وأيضاً بعض التوصيات التي من شأنها أن تساهم، على الأقل من الناحية الإجرائية، في مجهودات مكافحة جرائم تقنية المعلومات .

الكلمات المفتاحية: إجراءات جمع الأدلة الرقمية، جرائم تقنية المعلومات، المعلومات المخزنة، بيانات الحركة، اعتراض معلومات المحتوى.

*المؤلف المرسل

Abstract:

This article deals with the provisions in arab convention on combating information technology offences, and pertaining to measures for the collection of digital evidences of offences committed by means of information technology. Through analyzing the related convention articles, and comparing with the similar articles in Budabest convention on cybercrime.

Therefore, the study is divided un two parts, the first part discourse about the procedures of stored information, the second talk about the procedures of non-stored information. Finally, it concluded with several conclusions and recommendations.

Keywords: The procedures of collection a digital evidences, Information technology offences, Stored information, Traffic data, Interception of content data.

مقدمة

شكل تعقيد جرائم تقنية المعلومات وإمكانية تخطيها حدود الدول نتيجة ارتباط تقنية المعلومات بتقنية الاتصالات، والحاجة المتزايدة لاستعمال هذه التقنية من قبل الأفراد والمؤسسات وأيضا الحكومات، عاملا محفزا لتزايد ارتكاب هذا النوع من الجرائم. ولما كانت الدول ملزمة بالحفاظ على المصالح المشروعة للأشخاص ومنع الاعتداء عليها، فقد تصدت من خلال تشريعاتها الجزائية لجرائم تقنية المعلومات، غير أنها اصطدمت بواقع أن تشريعها الجزائي لا يسري سوى على رقعتها الجغرافية، وأن جرائم تقنية المعلومات لم تعد تعترف بالحدود الجغرافية للدول، وأن سبل التحقيق وجمع الأدلة بشأنها تختلف من دولة إلى أخرى، مما يزيد من إمكانية ضياع هذه الأدلة التي تمتاز أصلا بتقلبها وسهولة التلاعب بها بالحذف والتعديل.

لمواجهة هذه المعضلة خصوصا أدركت الدول أنه لا بد من تقريب أحكام القوانين الجزائية من بعضها البعض، والتمكين من استخدام وسائل وتدابير فعالة للتحقيق في جرائم من هذا القبيل وجمع الأدلة المتصلة بها، فقامت كل من دول الاتحاد الأوروبي والولايات المتحدة الأمريكية واليابان وجنوب إفريقيا ببذل مجهودات مضيئة تكلفت بإبرام اتفاقية عام 2001 عرفت باسم اتفاقية بودابست أو اتفاقية مكافحة الجرائم الإلكترونية.

إن الدول العربية هي الأخرى أدركت مكانم الخطورة في جرائم تقنية المعلومات، فبادرت إلى عقد اتفاقية فيما بينها تم التوقيع عليها سنة 2010، وسميت بالاتفاقية العربية لمكافحة جرائم تقنية المعلومات، وتضمنت هي الأخرى مجموعة من الالتزامات التي تهدف إلى توحيد إجراءات جمع الأدلة بشأن جرائم تقنية المعلومات والجرائم المرتبطة بهذه التقنية، والتي هي مدار الدراسة في هذا المقال، ونبحت فيه عن مدى فعالية الاتفاقية العربية في معالجة مشكلة جمع الأدلة بشأن جرائم تقنية المعلومات والجرائم المرتبطة بهذه التقنية.

من أجل ذلك، تنتهج هذه الدراسة منهجا تحليليا استقرائيا لمختلف البنود والأحكام التي تضمنتها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، والمتعلقة بجمع الأدلة بشأنها، مع مقارنتها بتلك التي تضمنتها اتفاقية بودبست باعتبارها أول اتفاقية تتعرض لمكافحة هذا النوع من الجرائم، وذلك من خلال نقطتين أساسيتين هما:

1. إجراءات جمع الأدلة المتعلقة بالمعلومات المخزنة.
2. إجراءات جمع الأدلة المتعلقة بالمعلومات غير المخزنة.
1. إجراءات جمع الأدلة المتعلقة بالمعلومات المخزنة.

دعت كل من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات¹ وكذلك الاتفاقية الأوروبية للجريمة الالكترونية (اتفاقية بودابست) الدول الأطراف إلى إقرار مجموعة من التدابير أو الإجراءات التي لا تطبق إلا على المعلومات المخزنة داخل تقنية المعلومات، ولتعتبر المعلومات مخزنة يجب أن تكون موجودة بالفعل ويجري تخزينها آنيا².

لأجل ذلك جاءت التدابير أولا من أجل فرض حفظ المعلومات المخزنة في يد من كانت عنده، ثم إلزامه، ثانيا، بتسليمها للسلطات المختصة في التحقيقات الجنائية، وأخيرا من أجل تمكين سلطات التحقيق من مباشرة مهامها المنوطة بها والمتعلقة بالبحث عن الأدلة وضبطها.

1.1.1. حفظ المعلومات المخزنة.

في البداية يجب الإشارة إلى أن مصطلح التحفظ الذي جاءت به الاتفاقية العربية في عنوان المادتين 23 و 24 ذات الصلة بحفظ المعلومات المخزنة يعتبر تعبيراً خاطئاً من الناحية القانونية، إذ له مفهوم قانوني يتعلق بالمعاهدات والاتفاقيات، ولما كان الأمر يخص أحكاماً تضمنتها اتفاقية فقد يؤدي ذلك إلى ارتباك المتلقي (المخاطب بأحكامها) في تحديد أي المفهومين تقصده الاتفاقية، هل هو التحفظ بمعناه القانوني³، أو هو المعنى اللغوي الذي يقابله الحفظ، كما ذهبت إلى ذلك بشكل سليم اتفاقية بودابست.

ومن أجل إقرار تدابير تتعلق بحفظ المعلومات، نصت الاتفاقية العربية في مادتها 23 و 24، على إجراءين هما: التحفظ (الحفظ) العاجل على البيانات المخزنة في تقنية المعلومات، والتحفظ (الحفظ) العاجل والكشف الجزئي لمعلومات تتبع المستخدمين، ويقابلها من اتفاقية بودابست - على التوالي - المادة 16 المتعلقة بالتسجيل في حفظ بيانات الكمبيوتر المخزنة و المادة 17 المتعلقة بالتسجيل في حفظ بيانات الكمبيوتر والكشف الجزئي عن بيانات الحركة.

1.1.1.1. الحفظ العاجل للبيانات المخزنة في تقنية المعلومات.

بينت المادة 23 في فقرتها الأولى أن على كل دولة طرف أن تلتزم بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأمر أو الحصول على الحفظ العاجل للمعلومات المخزنة بما في ذلك معلومات تتبع المستخدمين والتي خزنت على تقنية معلومات، خصوصاً إذا كان هناك اعتقاد أن تلك المعلومات عرضة للفقان أو التعديل.

بهذا فإن هذه المادة تستهدف ضمان قدرة السلطات الوطنية المختصة على أن توجه أمراً إلى الشخص الذي يحوز المعلومات أو يسيطر عليها بتسجيل حفظ بيانات تقنية معلومات مخزنة محددة ومتعلقة بتحقيق جنائي أو دعوى جنائية محددة، أو على أن تحصل بطريقة مماثلة على هذا الحفظ⁴.

ولما كانت بيانات الكمبيوتر تمتاز بتقلبها وسهولة تغييرها أو التلاعب بها، كانت السرعة ضرورية في تأمين سلامة هذه البيانات من خلال الأمر بحفظها، غير أن المادة لم تحدد كيفية الحفظ، وبالتالي يترك لكل دولة تحديد الطريقة المناسبة لحفظ البيانات، وما إذا كان ينبغي أن ينطوي أمر الحفظ العاجل للبيانات المخزنة على تجميد لهذه البيانات في بعض الحالات الخاصة والمناسبة⁵.

هذا ويرمي مصطلح "الحصول بطريقة مماثلة" الوارد في اتفاقية بودابست إلى إضفاء مرونة مقصودة تتمكن بها بعض الدول التي لا تعرف في قانونها الإجرائي أوامر الحفظ، سواء القضائية أو الإدارية، من تنفيذ أحكام هذه المادة باستخدام الوسائل القانونية الوطنية المتاحة⁶، بينما في الاتفاقية العربية استعملت مصطلح "الحصول"، وبالتالي فإن المعنى السابق لا يتحقق معه.

غير أن البيانات المخزنة، في الواقع، قد تكون في حوزة شخص أو تكون مخزنة في مكان آخر ولكن تخضع لسيطرة هذا الشخص، ولهذا جاءت المادة 02/23 من الاتفاقية العربية، ويقابلها المادة 02/16 من اتفاقية بودابست، لتحث الدول الأطراف فيها أن تتبنى في تشريعاتها ما يجعل أمر الحفظ يوجه إلى الشخص سواء كانت البيانات المخزنة بحوزته أو كانت في غير حوزته ولكن تحت سلطته، وذلك لمدة زمنية محددة تسمح للسلطات المختصة باتخاذ التدابير القانونية اللازمة مثل التفتيش أو المصادرة أو النفاذ والتأمين بطريقة أخرى، أو إصدار أمر تسليم المعلومات⁷.

ولما كانت البيانات المخزنة التي هي محل أمر الحفظ العاجل قد تنطوي على معلومات شخصية أو معلومات ينبغي إخفاؤها لغرض التحقيق عن المشتبه فيه، أو لغرض صرف الغير عن التلاعب بها أو حذفها، فقد ألزمت المادة 03/23 من الاتفاقية العربية، ويقابلها المادة 03/16 من اتفاقية بودابست، الدولة الطرف أن تتبنى الإجراءات الضرورية لإلزام الشخص الذي يوجه له أمر الحفظ العاجل للبيانات المخزنة على تقنية المعلومات بالإبقاء على سرية الإجراءات طوال المدة القانونية المحددة في القانون الداخلي.

2.1.1. الحفظ العاجل والكشف الجزئي لمعلومات تتبع المستخدمين.

تنص المادة 24 من الاتفاقية العربية ومثلها المادة 17 من اتفاقية بودابست على التزامات محددة تتعلق بنوع واحد من المعلومات وهي معلومات تتبع المستخدمين، أو ما عبرت عنه اتفاقية بودابست ببيانات الحركة، وهنا يتبادر إلى الذهن التساؤل عن ما هو المقصود من معلومات تتبع المستخدمين؟

في الواقع، لن تجد لهذا السؤال جواباً في الاتفاقية العربية، فقد جاءت خالية من بيان المقصود من معلومات تتبع المستخدمين، بينما عرفت اتفاقية بودابست بأنها: "أي بيانات كمبيوتر متعلقة باتصال عن طريق نظام الكمبيوتر والتي تنشأ عن نظام الكمبيوتر يشكل جزءاً في سلسلة الاتصالات، توضح المنشأ، والوجهة، والمسار، والزمن، والتاريخ، والحجم، والمدة، أو نوع الخدمة الأساسية"⁸.

ثم إنه عادة ما يشارك في نقل الاتصال أكثر من مقدم خدمة واحد، ويحتفظ كل واحد منهم بجزء من معلومات تتبع المستخدمين أي ببعض أجزاء اللغز، فثمة حاجة لفحص كل جزء وتجميعها معاً حتى تكتمل الصورة من أجل تحديد مصدر ووجهة الاتصال⁹. فمن أجل ذلك جاءت المادة 24 من الاتفاقية العربية، وشبهتها المادة 17 من اتفاقية بودابست، لتعجيل حفظ معلومات تتبع المستخدمين في حالة اشتراك أكثر من مقدم خدمة واحد في إرسال الاتصال، ولكن دون تحديد الوسائل التي يمكن من خلالها تحقيق ذلك، تاركة هذا الأمر للقانون الوطني.

ولتحديد مقدمي الخدمة الذين شاركوا في إرسال الاتصال، جاءت المادة 02/24 من الاتفاقية العربية، والمادة 02/17 من اتفاقية بودابست التي تقابلها، لتلزم الدولة الطرف بتبني الإجراءات الضرورية التي من شأنها أن تفرض على مقدم الخدمة الذي توصل بأمر الحفظ أو بتدبير آخر مماثلاً، الكشف العاجل للسلطات المختصة أو لشخص تعينه هذه السلطات لمقدار كاف من معلومات تتبع المستخدمين، وذلك من أجل أن تتمكن تلك السلطات، وليس "الدولة" كما ورد في الاتفاقية العربية، من البدء فوراً في تتبع نقل البيانات وتحديد مزودي (مقدمي) الخدمة المشاركين في بث الاتصالات، والمسار الذي تم من خلاله بث هذه الاتصالات¹⁰.

2.1. أمر تسليم المعلومات

إذا كان أمر الحفظ العاجل لبيانات تقنية المعلومات كإجراء يُتصور اتخاذه لما تكون المعلومات في حوزة مقدم الخدمة، فإن الواقع يبرز أن هناك من مقدمي الخدمات من لا يبدي طوعية في مساعدة السلطات المختصة بإنفاذ القانون، بل إن هذه البيانات قد تكون على تقنية معلومات يحوزها شخص آخر، سواء طبيعي أو معنوي، وهو ليس من مقدمي الخدمات.

هذا من جهة، ومن جهة أخرى فإنه حتى بالنسبة لمقدمي الخدمات الذين يكونون مستعدين للتعاون مع السلطات المختصة لإنفاذ القانون فهم يفضلون أن يكون لهم سند قانوني من أجل تقديم البيانات التي بحوزتهم، والتي تخص عملاءهم أو زبائنهم، إلى هذه السلطات¹¹.

فأمر تسليم المعلومات، والذي نصت المادة 25 من الاتفاقية العربية والمادة 18 من الاتفاقية الأوروبية على ضرورة أن تتبناه الدولة الطرف من خلال تشريعها الداخلي، هو تدبير يمكن السلطات المختصة من إرغام شخص في إقليمها على تقديم معلومات معينة أو محددة مخزنة، أو مقدم خدمة يقدم خدماته في إقليمها على تقديم معلومات بشأن المنخرطين (معلومات عن المشترك)¹².

ويقصد بالمعلومات عن المشترك حسب المادة 03/18 من اتفاقية بودابست: "أي معلومات مدرجة في شكل بيانات الكمبيوتر أو في أي شكل آخر يحفظها مزود الخدمة والتي تتعلق بالمشتركين في الخدمة التي يزودها بخلاف بيانات الحركة أو المضمون والتي بموجبها يمكن تحديد:

- أ. نوع خدمة الاتصال المستخدمة والشروط الفنية المرتبطة بها ومدة الخدمة،
- ب. هوية المشترك، وعنوانه البريدي أو الجغرافي، ورقم هاتفه وغيره من أرقام الولوج، والبيانات الخاصة بالفواتير والدفع المتاحة بموجب اتفاق أو ترتيبات الخدمة،
- ج. أي معلومات أخرى عن موقع تركيب أجهزة ومعدات الاتصال المتاحة بموجب اتفاق أو ترتيبات الخدمة".

في المقابل نجد الاتفاقية العربية عرفت معلومات المشترك بموجب المادة 02/03، وحسنا فعلت، فما دامت خصصت مادة للتعريفات فكان لزاما أن تتضمن جميع التعريفات الخاصة بالاتفاقية، وهذا على خلاف ما ذهبت إليه اتفاقية بودابست، وقد أساءت فعلا، حينما عرفت من خلال المادة 18 رغم أنها قد خصصت المادة 01 للتعريفات.

غير أن التعريف الذي جاءت به الاتفاقية العربية جاء خاطئا، بل يمكن القول أن صياغته أفرغته من محتواه تماما، حيث أن معلومات المشترك حسب الاتفاقية العربية هي "أية معلومات موجودة لدى مزود الخدمة المتعلقة بمشتركي الخدمة عدا المعلومات التي يمكن بواسطتها معرفة:...", ثم عدت الثلاث نقاط التي ذكرتها المادة 03/18 من اتفاقية بودابست.

فطبقا لهذا التعريف الأخير تكون معلومات المشترك لا تفيد لا في تحديد نوع خدمة الاتصال المستعملة ولا الشروط الفنية ولا فترة الخدمة، ولا هوية المشترك ولا عنوانه البريدي... الخ، وبالتالي فأى معلومات تتعلق بالمشارك يمكن الاستفادة منها في التحقيقات الجنائية إذا ما تم طرح كل ما سبق.

على هذا فإن الصياغة الصحيحة لتعريف معلومات المشترك يمكن أن تكون كالتالي: " أية معلومات موجودة لدى مزود الخدمة المتعلقة بمشتركي الخدمة ما عدا معلومات تتبع المستخدمين ومعلومات المحتوى، والتي يمكن بواسطتها معرفة: ... (الباقى بدون تغيير)".

في الأخير يجدر التأكيد أن المعلومات المستهدفة بأمر التسليم هي المعلومات المحددة المخزنة أو الموجودة بالفعل، ولا تتضمن المعلومات التي لم تخرج بعد إلى حيز الوجود، أي المعلومات المستقبلية، كما لا يلزم مقدم الخدمة بضمان صحة هذه المعلومات، وعليه فهذا الأخير غير ملزم بتسجيل معلومات هوية المستخدمين، ولا بالتحقق من هوياتهم أو حتى مقاومة استعمالهم لأسماء مستعارة¹³.

3.1. تفتيش وضبط المعلومات المخزنة

تشتمل قوانين الإجراءات الجزائية على تدابير تمكن من التفتيش عن الأدلة وضبطها، غير أن هذه الصلاحيات قد لا تصلح إذا تعلق الأمر بمعلومات أو بيانات تشكل أدلة رقمية تخص جرائم تقنية المعلومات، ولذا كان لزاماً أن يتم تكيفها بما يتناسب مع الطبيعة غير الملموسة للمعلومات المخزنة في تقنية المعلومات.

1.3.1. تفتيش المعلومات المخزنة

التفتيش هو البحث والاستقصاء وهو إجراء من إجراءات التحقيق التي تسمح بالاطلاع على محل منح له القانون حرمة خاصة باعتباره من خصوصيات الشخص¹⁴.

ولذلك ينص المشرع على ضمانات معينة يجب مراعاتها عند اتباع إجراء التفتيش حتى يمكن التوفيق بين اتجاه الدستور نحو حماية الحقوق التي يكفلها وبين مقتضيات تطبيق العدالة الجنائية¹⁵، ومن أهم هذه الضمانات أن لا تفتيش إلا إذا قامت دلائل قوية ضد شخص معين بأن له يد في ارتكاب الجريمة، فلا يصح مباشرته لجريمة مستقبلية ولو قامت التحريات والدلائل الجدية على أنها ستقع بالفعل¹⁶.

فتحت ضرورة قيام العديد من الضمانات الخاصة بالتفتيش التقليدي، يأتي تفتيش المعلومات المخزنة كإجراء من إجراءات التحقيق هدفه البحث عن أدلة رقمية ضد متهم في جريمة معينة من جرائم تقنية المعلومات وقعت بالفعل، وذلك من أجل كشف الحقيقة المتعلقة بهذه الجريمة¹⁷.

بيد أن محل التفتيش في جرائم تقنية المعلومات يختلف عنه في الجرائم التقليدية، ولذا جاءت المادة 26 من الاتفاقية العربية والتي يقابلها المادة 01/19 من اتفاقية بودابست لبيان محل هذا التفتيش، وهو أولاً تقنية المعلومات أو جزء منها مثل جهاز متصل لتخزين المعلومات، مع ملاحظة أن التفتيش يشمل كل العناصر المكونة لتقنية المعلومات، كما ورد في تعريفها بالمادة 01/02 من الاتفاقية العربية أو المادة 01/أ من اتفاقية بودابست، مثل جهاز الكمبيوتر وآلة الطباعة وأجهزة التخزين ذات الصلة وشبكة المنطقة المحلية¹⁸، وعلى ذلك فالنفتيش يشمل كل مكونات تقنية المعلومات سواء كانت مادية أو معنوية أو شبكات الاتصال الخاصة بها¹⁹.

ثاني محل للتفتيش هو بيئة أو وسيط تخزين معلومات أو كما عبرت عنه اتفاقية بودابست بدعامة تخزين بيانات الكمبيوتر (مثل الأقراص المرنة، بطاقات الذاكرة) والتي يمكن أن تكون بيانات الكمبيوتر مخزنة داخلها على أراضي تلك الدولة الطرف. أما محل التفتيش الأخير فهو المشار إليه في الاتفاقيتين العربية والأوروبية، من خلال المادتين 02/26 و 02/19 تباعا، ويتعلق بتقنية معلومات معينة أخرى أو جزء منها موجودة على إقليم الدولة وتم فعليا تخزين بيانات أو معلومات يعتقد بأنها البيانات المطلوب التفتيش عنها أو فيها، وأنه يمكن النفاذ إليها عن طريق تقنية المعلومات الأولى أو أنها متاحة قانونيا على هذه الأخيرة، وعليه يفترض في هذه الحالة أن تكون هناك تقنية معلومات أصلية، وهي المذكورة في المادة 01/26/أ من الاتفاقية العربية والمادة 01/19/أ من اتفاقية بودابست، لديها روابط مع تقنية معلومات أخرى عن طريق شبكات الاتصالات داخل إقليم الدولة الطرف، فيمتد إجراء التفتيش من التقنية الأصلية إلى تقنية المعلومات الأخرى²⁰.

من أجل ذلك جاءت كلتا الاتفاقيتان لتلزم الدول الأطراف فيها باتخاذ الإجراءات الضرورية لتمكين سلطاتها المختصة من القيام بالتفتيش أو الوصول إلى محلات التفتيش المذكورة سابقا، وإن كانت اتفاقية بودابست في نسختها العربية عبرت عن ذلك باستعمال مصطلحين مختلفين وهما "البحث" و"النفاذ".

فإن كان كل من مصطلحي البحث (أو التفتيش) عن البيانات أو فيها يشير إلى أن هذه الصلاحية مشابهة لصلاحية التفتيش (أو البحث) التقليدي بما تنطوي عليه من فكرة ممارسة الدولة للقوة القسرية، وهو يعني إيجاد بيانات أو معلومات أو قراءتها أو فحصها أو مراجعتها، فإن مصطلح الوصول (أو النفاذ) يحمل معنى محايدا، وهو يعكس بمزيد من الدقة المصطلحات الحاسوبية، ويستخدم كلا المصطلحين من أجل جمع المصطلحات التقليدية بالمصطلحات الحديثة²¹.

ولما كان إجراء التفتيش التقليدي عادة ما يقتضي ضبط الأشياء والوثائق من أجل البحث فيها والحصول على الأدلة ومن ثم تأمينها، فإنه يتعين بحث كيف عالجت الاتفاقية محل الدراسة هذا الإجراء عندما يتعلق الأمر بمعلومات مخزنة في تقنية

المعلومات، باعتبار أن هذه المعلومات تتصف بأنها شيء غير ملموس خلافا للأشياء والوثائق التي تعتبر شيئا ماديا ملموسا.

2.3.1. ضبط المعلومات المخزنة.

جاءت المادة 01/27 من الاتفاقية العربية ويقابلها المادة 03/19 من اتفاقية بودابست من أجل وضع إجراءات تمكن السلطات المختصة من ضبط (مصادرة حسب النسخة العربية لاتفاقية بودابست) أو تأمين معلومات تقنية المعلومات التي تم البحث فيها أو النفاذ إليها تطبيقاً لأحكام الفقرتين 01 و 02 من المادة 19 من اتفاقية بودابست، أو تطبيقاً لأحكام المادة 26 من الاتفاقية العربية وليس فقط الفقرة 01 منها، كما ذهبت إلى ذلك بالخطأ المادة 27 من نفس الاتفاقية، حيث بينا أنفاً أن الفقرة 02 من المادة 26 ما هي إلا تمديد اختصاص للإجراء الذي جاءت به الفقرة 01/01 من نفس المادة. وتشمل هذه الإجراءات الصلاحيات التالية:

- ضبط وتأمين تقنية المعلومات أو جزء منها أو وسيط تخزين المعلومات تقنية المعلومات.
- عمل نسخة من معلومات تقنية المعلومات والاحتفاظ بها.
- الحفاظ على سلامة معلومات تقنية المعلومات المخزنة.
- إزالة أو منع الوصول إلى تلك المعلومات في تقنية المعلومات التي يتم الوصول إليها.

هذا، ويقصد بمصطلح الضبط (المصادرة) التقليدي هنا حجز وإبعاد الدعامة المادية التي سجلت عليها المعلومات، أو إجراء نسخة من هذه المعلومات والاحتفاظ بها، وأيضاً استخدام وحجز البرامج اللازمة للنفاذ إلى المعلومات التي تتم مصادرتها، في المقابل يأتي مصطلح التأمين ليشمل الوسائل الأخرى التي يتم من خلالها إزالة معلومات غير ملموسة يجعلها غير قابلة للوصول (أو النفاذ) أو بالتحكم فيها بطريقة أخرى في البيئة المعلوماتية، أما الحفاظ على سلامة معلومات تقنية المعلومات المخزنة فيعني أن المعلومات التي تم نسخها أو إلتهها يجب أن يتم الاحتفاظ بها في الدولة التي وجدت فيها وقت مصادرتها وأن يتم حفظها من أي تغيير خلال فترة الدعوى الجزائية،

وذلك بهدف الحفاظ على سلسلة احتجاز هذه المعلومات، ويشمل هذا المصطلح أيضا التحكم في المعلومات أو إبعادها²².

بينما جاء مصطلح " إزالة " للتعبير على أنه لا يتم تدمير المعلومات التي تمت إزالتها أو منع الوصول إليها، ولكن تظل موجودة ويحرم منها المشتبه فيه مؤقتا، أما منع الوصول إلى المعلومات أو جعلها غير قابلة للنفاذ بحسب اتفاقية بودابست فيشمل تشفير المعلومات أو منع أي شخص من الوصول (النفاذ) إليها²³.

في الواقع، قد يكون من الصعب عمليا الوصول إلى المعلومات المطلوبة كدليل وتحديدها، نظرا لكمية المعلومات التي يمكن معالجتها وتخزينها، أو لاشتمالها على تدابير تأمينية (تشفير، كلمة سر...إلخ)، ونظرا لطبيعة العمليات الحاسوبية في حد ذاتها، مما قد يجعل سلطات التحقيق تبقى في أماكن البحث وتمنع الوصول إلى تقنية المعلومات لفترة طويلة من الزمن²⁴.

من أجل ذلك، جاءت المادة 02/27 من الاتفاقية العربية ومثلها المادة 04/19 من اتفاقية بودابست بحكم قسري، يتمثل في تمكين السلطات المختصة من أن تأمر أي شخص لديه معرفة بوظيفة تقنية المعلومات المستهدفة أو الإجراءات المطبقة لحمايتها بتقديم المعلومات الضرورية من أجل إتمام ما عبرت عنه الاتفاقية العربية بـ "تلك الإجراءات المذكورة في الفقرتين (1،2) من المادة 26 من هذه الاتفاقية"، أي ما هو مذكور في المادة 26 المعنونة بـ "تفتيش المعلومات المخزنة" فهي فعليا تتكون من فقرتين فقط.

نعم، يبدو من الغريب أن يدرج حكم يتعلق بالمادة 26 فقط ضمن أحكام المادة 27، وهذا ما يعطينا انطباعا قويا أن الاتفاقية العربية إنما هي ترجمة لاتفاقية بودابست مع بعض التعديلات التي لم تكن موفقة في بعض الأحيان، مثل هذه الحالة التي جمعت فيها اتفاقية بودابست التدابير المتعلقة بالتفتيش عن المعلومات المخزنة وضبطها في مادة واحدة هي المادة 19، بينما قامت الاتفاقية العربية بتقسيمها إلى تدابير تتعلق بالتفتيش تضمنتها المادة 26 وأخرى تتعلق بالضبط تضمنتها المادة 27، فكان نتيجة ذلك هذه الاختلافات في صياغة هذه الأخيرة.

2. الأحكام الإجرائية المتعلقة بالمعلومات غير المخزنة.

تعتبر جرائم تقنية المعلومات معقدة بطبيعتها أو بحسب وسائلها نظرا لاعتمادها على التزاوج الحاصل بين تقنية الكمبيوتر وتقنية الاتصالات، وهذا ما يجعل اكتشاف بعض هذه الجرائم يحتاج إلى استعمال تدابير استباقية باستعمال وسائل فنية تكون حاسمة في التحقيق، فمثلا في الجرائم إلي تنطوي على الوصول غير المشروع أو على توزيع المواد الإباحية، قد يتعذر تحديد مصدر التطفل أو التوزيع دون جمع بيانات الحركة في الوقت الفعلي، وقد يتعذر اكتشاف طبيعة الاتصال دون اعتراض بيانات المحتوى في الوقت الفعلي.

ويهدف كل من التدبيرين المتمثلين في الجمع الفوري لمعلومات تتبع واعتراض المحتوى إلى جمع الأدلة عن طريق جمع البيانات (المعلومات) الواردة في الاتصالات المولدة في الوقت الحاضر، أو التي تجمع في وقت إجراء الاتصال أي الوقت الحقيقي أو الفعلي، وتعتبر هذه البيانات غير ملموسة من حيث الشكل (مثلا في شكل ارسالات صوتية أو نبضات إلكترونية)، ولا يتأثر تدفقها بشكل هام بسبب عملية الجمع، حيث يصل الاتصال إلى المتلقي المقصود منها، فبدلا من المصادرة الفعلية للبيانات فإنه يتم تسجيل (أي استنساخ) البيانات التي يتم إرسالها عبر الاتصال خلال فترة معينة من الزمن²⁵.

كما وينطبق التدبيران على الاتصالات المحددة المرسله بواسطة تقنية المعلومات والتي يمكن أن تشمل نقل الاتصال من خلال شبكات الاتصالات قبل استلامها بواسطة تقنية المعلومات أخرى، وذلك دون تمييز بين نظام الاتصال السلكي واللاسلكي، أو تقنية المعلومات العامة أو الخاصة، أو بين استخدام الأنظمة وخدمات الاتصالات المعروضة من قبل الجمهور العام أو مجموعات مغلقة من المستخدمين أو أطراف خاصة²⁶.

ثم لما كانت العديد من الدول تميز بين اعتراض معلومات المحتوى في الوقت الحقيقي وبين الجمع الفوري لمعلومات تتبع المستخدمين من حيث الشروط القانونية المطلوبة للترخيص بإجراء أحد التدبيرين، بحيث يمكن فرض قيودا أكثر على التدبير الأول منها على التدبير الثاني، نظرا لأن مصالح الخصوصية المرتبطة بمعلومات المحتوى أكبر

من تلك المرتبطة بمعلومات تتبع المستخدمين، فإن الاتفاقية، سواء العربية أو الأوروبية، ومن أجل الاعتراف بهذا التمييز عبرت في عناوين المواد ذات الصلة بجمع معلومات تتبع المستخدمين باعتباره "جمع فوري" بالنسبة للاتفاقية العربية، أو "جمع في الوقت الحقيقي" بالنسبة للاتفاقية الأوروبية، بينما عبرت في تلك المتعلقة بمعلومات المحتوى باعتباره "اعتراض بشكل فوري" بالنسبة للاتفاقية العربية، أو "اعتراض في الوقت الحقيقي" بالنسبة للاتفاقية الأوروبية²⁷.

في المقابل، فإن بعض الدول لا تميز بين جمع معلومات تتبع المستخدمين واعتراض معلومات المحتوى، فتجعل الشروط القانونية المطلوبة لاتخاذ كلا التدبيرين هي نفسها، وقد اعترفت الاتفاقية الأوروبية، ومثلها الاتفاقية العربية، بهذا الوضع من خلال الاستخدام الوظيفي المشترك لمصطلح "جمع أو تسجيل" في النص الراهن للمواد ذات الصلة²⁸.

على كل، فيجب أن تتوفر الصلاحية القانونية التي ترخص بجمع بيانات أو معلومات في المستقبل، ولذا جاءت كلتا الاتفاقيتان، العربية والأوروبية، بأحكام تركز ذلك من خلال مادتين، تتعلق الأولى بالجمع الفوري لمعلومات تتبع المستخدمين، وتتعلق الثانية باعتراض معلومات المحتوى.

1.2. الجمع الفوري لمعلومات تتبع المستخدمين

أشارت المادة 28 من الاتفاقية العربية، ومثلها المادة 20 من اتفاقية بودابست، إلى ضرورة أن تتبنى كل دولة طرف الإجراءات الضرورية لتمكين السلطات المختصة من القيام بإجراء الجمع الفوري لمعلومات تتبع المستخدمين، أو كما عبرت عنه الاتفاقية الأوروبية في نسختها العربية بجمع بيانات الكمبيوتر في الوقت الحقيقي، غير أن الترجمة الصحيحة هي "جمع بيانات الحركة في الوقت الحقيقي".

إن كانت الاتفاقية العربية لم تعرف معلومات تتبع المستخدمين (بيانات الحركة)، بينما ورد تعريفها في المادة 01/د من اتفاقية بودابست، وهو ما وقفنا عليها سابقاً، سوى أن الأمر هنا يتعلق بهذه المعلومات أو البيانات لما تكون غير مخزنة أو بمعنى آخر أنها

لم يتم استلامها بعد من طرف تقنية المعلومات المرسل إليها عن طريق اتصالات محددة²⁹.

ونظرا لاعتبار المصلحة الخصوصية ذات الصلة بجمع معلومات تتبع المستخدمين، والتي تُطرح بشكل أقل عندما تتعلق بوقت الاتصال ومدته وحجمه بينما تُطرح بشكل أكبر لما تتعلق بالمعلومات المرتبطة بمصدر الاتصال ووجهته (مثلا المواقع الإلكترونية التي تم تصفحها)، فإنه يتعين تحديد الاتصالات التي يمكن جمع أو تسجيل معلومات تتبع المستخدمين بشأنها، فالاتفاقية، سواء العربية أو الأوروبية، لا تسمح بالمراقبة العامة أو العشوائية وجمع كميات كبيرة من معلومات تتبع المستخدمين، بالإضافة إلى أنها لا ترخص بحالة " تصيد المعلومات بنية مبيتة" من أجل اكتشاف أنشطة إجرامية بدلا من التحقيق في حالات محددة من الجرائم³⁰.

كما يتعين أن تكون الاتصالات مبنوثة من إقليم الدولة الطرف، وتكون كذلك إذا كان أحد المتصلين متواجدا على إقليمها، أو إذا كان الكيان المادي لتقنية المعلومات أو معدات الاتصال عن بعد التي يتم من خلالها الاتصال متواجدا على إقليمها³¹.

ورغم ما يكتسبه استعمال الوسائل التقنية في التحقيق في جرائم تقنية المعلومات عن طريق جمع معلومات تتبع المستخدمين، خاصة في الربط بين وقت وتاريخ ومصدر ووجهة اتصالات المشتبه فيه بوقت اقتحام أنظمة الضحايا أو تحديد الضحايا الآخرين أو إظهار روابط مع شركاء في الجريمة، إلا أن كلتا الاتفاقيتين لم تبينا كيفية إجراء عملية الجمع، ولم ترضا أي التزامات من الناحية التقنية³².

ألزمت المادة 28 من الاتفاقية العربية، والمادة 20 من اتفاقية بودابست، كل دولة طرف بأن تُمكن لسلطاتها المختصة بأن تباشر بنفسها، وباستعمال الوسائل التقنية، عملية جمع أو تسجيل معلومات تتبع المستخدمين في الوقت الحقيقي (بشكل فوري)، حسب الفقرة 1(أ) من كلا المادتين، وعليها في نفس الوقت أن تُمكن لسلطاتها المختصة من إجبار مزود الخدمة على جمع أو تسجيل تلك المعلومات، أو من إجباره على التعاون معها ومساعدتها في عملية جمع أو تسجيل هاته المعلومات، طبقا للفقرة 1(ب) من نفس المادتين.

فعلى الأقل بالنسبة للاتفاقية الأوروبية يبدو واضحا، من خلال استعمال حرف العطف "و" للربط بين الفقرة 1(أ) و(ب)، أنه يجب على كل طرف أن يضمن توافر كلتا الطريقتين الواردتين في هاتين الفقرتين، ولكن دون أن يستلزم ذلك استخدام كلتا الطريقتين في كل مرة، بينما قد لا يستشف هذا المعنى المتعلق بضرورة توافر الطريقتين معا من نص المادة 28 من الاتفاقية العربية، لانعدام وسيلة الربط بين الفقرتين 1(أ) و1(ب).

كذلك وطبقا للمادة 02/28 من الاتفاقية العربية والمادة 02/20 من اتفاقية بودابست إذا لم تتمكن الدولة الطرف من تبني الطريقة أو التدبير الوارد في الفقرة 1(أ)، بسبب المبادئ الثابتة في قانونها الوطني، كأن تكون سلطاتها المختصة غير قادرة على جمع معلومات تتبع المستخدمين إلا من خلال مساعدة مقدم الخدمة، أو على الأقل دون علمه، فيمكنها أن تعتمد بدلا من ذلك مقارنة مختلفة، من قبيل الاكتفاء بإلزام مقدم الخدمة من توفير المرافق التقنية الضرورية من أجل أن تتولى السلطات المختصة بنفسها، وفي الوقت الحقيقي، عملية جمع أو تسجيل معلومات تتبع المستخدمين³³.

وحيث أن الجمع الفوري لمعلومات تتبع المستخدمين لا يكون فعالا إلا إذا نفذ دون علم الأشخاص الذين يجري التحقيق بشأنهم³⁴، فقد وضعت الفقرة 03 من المادة 28 من الاتفاقية العربية، ويقابلها نفس الفقرة من المادة 20 من اتفاقية بودابست، على عاتق كل دولة طرف بأن تعتمد الإجراءات الضرورية لإجبار مقدم الخدمة على الحفاظ على سرية تنفيذ أي من التدابير المنصوص عليها في هذه المادة.

وعلى الرغم من أن الجمع الفوري لمعلومات تتبع المستخدمين يمثل تدبيرا مهما في ما يخص جمع المعلومات غير المخزنة على تقنية المعلومات، بيد أنه قد يكون قاصرا في بعض الحالات، لذا فقد عملت الاتفاقية العربية ومثلها الأوروبية على اعتماد إجراء آخر يتمثل في اعتراض معلومات المحتوى.

2.2. اعتراض معلومات المحتوى

تحوي العديد من جرائم تقنية المعلومات على إرسال أو نقل معلومات كجزء من ارتكابها، فمثلا الاتصالات المرسلة من أجل توزيع محتوى غير قانوني كالمواد

الإباحية أو توزيع فيروسات الكمبيوتر لا يمكن تحديدها طبيعتها غير القانونية، في الوقت الحقيقي، دون اعتراض مضمون الاتصال.

لذلك يكتسي الاعتراض الفوري لمعلومات محتوى الاتصالات عبر تقنية المعلومات، نفس القدر من الأهمية، إن لم يكن أكبر، من ذلك الذي يولى لاعتراض الاتصالات السلكية واللاسلكية في الوقت الحقيقي، مثل اعتراض المحادثات الهاتفية والرسائل النصية القصيرة، خاصة وأن تقنية المعلومات بإمكانها نقل كميات هائلة من البيانات أو المعلومات بما في ذلك الفيديوهات والنصوص المكتوبة والصور المرئية والصوت³⁵.

من أجل ذلك جاءت الاتفاقية العربية من خلال المادة 29 منها، واتفاقية بودابست من خلال المادة 21 لتلزم الدول الأطراف بضرورة تبني كافة التدابير التشريعية وغيرها من التدابير من أجل تمكين سلطاتها المختصة من مباشرة جمع أو تسجيل معلومات المحتوى في الوقت الحقيقي، عندما يتعلق الأمر بمجموعة من الجرائم الخطيرة التي يحددها القانون الداخلي، وهذه التدابير مشابهة تماما لتلك المتعلقة بالجمع الفوري لمعلومات تتبع المستخدمين، ولذا نحيل إليها تجنباً للتكرار.

بيد أنه جاءت كل من الاتفاقيتين العربية والأوروبية خالية من بيان المقصود من معلومات أو بيانات المحتوى، إلا أنها تشير إلى محتوى الاتصال أي معنى أو مضمون الاتصال أو الرسالة أو المعلومات التي يتم نقلها عبر الاتصال، بخلاف معلومات تتبع المستخدمين (أو بيانات الحركة)³⁶.

في الأخير نشير إلى أن جميع المواد ذات الصلة بجمع الأدلة الواردة في اتفاقية بودابست، والمذكورة سابقاً، تضمنت فقرة تبين أن التدابير والإجراءات التي تضمنتها المادة تخضع لأحكام المادتين 14 و15 من الاتفاقية، وما يهمننا هنا هو المادة 15، والتي تؤكد على أن كل دولة طرف عليها أن تسعى لضمان وضع وتنفيذ التدابير والإجراءات المنصوص عليها في القسم الخاص بالجانب الإجرائي إلى الضمانات والشروط التي توفق بين متطلبات إنفاذ القانون وحماية حقوق الإنسان والحريات، وهي مادة ليس لها مقابل في الاتفاقية العربية.

الخاتمة

جاءت الأحكام الإجرائية في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بعدة تدابير تخص جمع الأدلة الرقمية، وذلك من أجل تطوير وتوحيد بنيتها التشريعية ذات الصلة بالتحقيق في هذه الجرائم بما يتناسب مع الطبيعة الخاصة لتقنيات المعلومات والاتصالات، ومن خلال دراستنا لهذه التدابير خلصنا إلى النتائج والتوصيات التالية :

النتائج :

- فرقت الاتفاقية العربية بين التدابير التي تستهدف المعلومات المخزنة على تقنية المعلومات وهي الحفظ العاجل للبيانات المخزنة، الحفظ العاجل والكشف الجزئي لمعلومات تتبع المستخدمين، أمر تسليم المعلومات وأخيرا تفتيش وضبط المعلومات المخزنة، وبين تلك التي تستهدف المعلومات غير المخزنة على تقنية المعلومات وهي الجمع الفوري لمعلومات تتبع المستخدمين، واعتراض معلومات المحتوى.
 - راعت الاتفاقية العربية في طرحها للالتزامات الملقاة على الدول الأطراف، سيادة هذه الدول وحققها في تبني ما تراه مناسباً مع قوانينها الداخلية خاصة مع نظامها الإجرائية.
 - التطابق الكبير جداً - إن لم نقل التام - بين التدابير والإجراءات الواردة في الاتفاقية العربية مع تلك الواردة في اتفاقية بودابست
 - الغموض في بعض نصوص الاتفاقية العربية نتيجة الغلط في بعض التعريفات مثل ما وقع في تعريف معلومات المشترك أو عدم ورود التعريف أصلاً مثل غياب المقصود من معلومات تتبع المستخدمين ومن معلومات المحتوى.
 - وقوع الاتفاقية العربية في الغلط في صياغتها للمادة 27 بإدراجها في هذه المادة للفقرة 03 والتي جاءت بحكم يتعلق فقط بالمادة 26.
 - ضعف إخضاع الاتفاقية العربية للصلاحيات والإجراءات التي جاءت بها، والمتعلقة بجمع الأدلة، إلى الشروط والضمانات التي توفق بين متطلبات إنفاذ القانون وحماية حقوق الإنسان والحريات.
- التوصيات :

- العمل على تصحيح تعريف مصطلح معلومات المشترك الواردة في المادة 02 من الاتفاقية.
 - إضافة تعريف خاص بمعلومات المستخدمين وآخر خاص بمعلومات المحتوى في نص المادة 02 الخاصة بالتعريفات.
 - إعادة صياغة المادة 27، بحذف الفقرة 03 منها وإضافتها كفقرة جديدة للمادة 26.
 - العمل على إنتاج تقرير تفسيري للاتفاقية العربية من أجل إيضاح أكبر لمواد وبنود الاتفاقية وذلك أسوة بالمشروع الأوروبي.
 - إخضاع الصلاحيات والإجراءات الواردة في الاتفاقية لمزيد من الشروط وضمانات حماية حقوق الإنسان والحريات مع مراعاة متطلبات إنفاذ القانون.
 - حث الدول العربية من خلال جامعتها على الانضمام لاتفاقية بودابست، خاصة وأن هذه الأخيرة دعت مختلف دول العالم للانضمام إليها.
- المراجع والهوامش**

- 1- مرسوم رئاسي رقم 14-252 المؤرخ في 8 سبتمبر 2014 المتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، ج ر، عدد57، الصادرة بتاريخ 28 سبتمبر 2014، ص04 ومايليها.
- 2- مجلس أوروبا، التقرير التفسيري لاتفاقية الجريمة الإلكترونية، نوفمبر 2001، متوفر على الرابط: <https://rm.coe.int/explanatory-report-budabest-convention-in-arabic/1680739174>، فقرة 150.
- 3- نصت المادة 1/2 د من اتفاقية فيينا لقانون المعاهدات لعام 1969 والتي دخلت حيز النفاذ في 27 يناير 1980 على: " يقصد بالتحفظ إعلان من جانب واحد...".
- 4- التقرير التفسيري، مرجع سابق، فقرة 158.
- 5- نفس المرجع، فقرة 155 و159.
- 6- نفس المرجع، فقرة 160.

- 7- نفس المرجع، فقرة 162.
- 8- المادة 01/ د من اتفاقية بودابست.
- 9- فايز محمد راجح غلاب، الجرائم المعلوماتية في القانون الجزائري واليمني، رسالة لنيل درجة الدكتوراه في القانون، فرع القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر (1)، 2011، ص427.
- 10- Rayan M.F.Baron, *A Critique Of The International Cybercrime Treaty*, Commlaw conspectus, vol10, 2002, p275.
- 11- التقرير التفسيري، مرجع سابق، فقرة 171.
- 12- Peter Csonka, *the concil of europe's convention on cyber-crime and other auropean initiatives*, International review of penal law, vol.77, 2006/3, p492-493.
- 13- Ahmad Kamal, *The Law Of Cyber-Space (An invitation to the table of negotiations)*, UNITAR, Edition01, Octobre2005,p237.
- 14- مروك نصر الدين، محاضرات في الإثبات الجنائي (النظرية العامة للإثبات الجنائي)، ج01، دار هومه، الجزائر، 2013، ص337.
- 15- آمال عبد الرحيم عثمان، شرح قانون الإجراءات الجنائية، الهيئة المصرية العامة للكتاب، القاهرة، 1991، ص449.
- 16- حسن صادق المرصفاوي، المرصفاوي في أصول الإجراءات الجنائية، ج01، ط أخيرة، منشأة المعارف، الإسكندرية، 1996، ص390.
- 17- فهد عبد الله عبيد العازمي، الإجراءات الجنائية المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2016، ص250.
- 18- التقرير التفسيري، مرجع سابق، فقرة 188.
- 19- فهد عبد الله عبيد العزمي، مرجع سابق، ص264.
- 20- علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الإبتدائي في الجريمة المعلوماتية (دراسة مقارنة)، المكتب الجامعي الحديث، 2012، ص45-46.
- 21- التقرير التفسيري، مرجع سابق، فقرة 191.
- 22- Peter Csonka, *Opcit*, PP493-494.

- 23- التقرير التفسيري، مرجع سابق، فقرة 198.
- 24- نفس المرجع، فقرة 200-201.
- 25- نفس المرجع، فقرة 208.
- 26- نفس المرجع، فقرة 206-207.
- 27- نفس المرجع، فقرة 210.
- 28- نفس المرجع، فقرة 211.
- 29- نفس المرجع، فقرة 206.
- 30- نفس المرجع، فقرة 219، 227.
- 31- براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة لنيل شهادة الدكتوراه في العلوم، تخصص القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2018، ص115.
- 32- التقرير التفسيري، مرجع سابق، فقرة 220.
- 33- نفس المرجع، فقرة 224.
- 34- براهيمي جمال، مرجع سابق، نفس الصفحة.
- 35- التقرير التفسيري، مرجع سابق، فقرة 228.
- 36- Peter Csonka, Opcit, P494.