الأحكام الإجرائية لمكافحة جريمة الاتجار بالأشخاص المرتكبة بواسطة تقنية المعلومات

- دراسة ضمن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010-

تاريخ استلام المقال: 19 جانفي 2018 تاريخ القبول النهائي: 23 مارس 2018

الدكتورة وردة شرف الدين

أستاذة محاضرة ب

كلية الحقوق والعلوم السياسية

جامعة محمد خيضر – بسكرة (الجزائر)

cherfeddinewarda@gmail.com

الملخص:

تعتبر جريمة الاتجار بالبشر من أخطر الجرائم المنظمة التي يعاني منها العالم اليوم، فهي تؤدي إلى استغلال البشر من قبل عصابات إجرامية بكل أشكال الاستغلال. وقد ازدادت هذه الجريمة خطورة في عصر العولمة لإمكانية ارتكابها بواسطة تقنية المعلومات التي سهلت الاتصال بين عصابات تهريب البشر والاتجار بهم.

لذا دعت الحاجة إلى ضرورة تعاون الدول فيما بينها لمكافحة جريمة الاتجار بالبشر، عن طريق إبرام العديد من الاتفاقيات الدولية، كبروتوكول الخاص بمنع وحظر ومعاقبة الاتجار بالأشخاص، بخاصة النساء والأطفال المكمل لاتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لعام 2000، بالإضافة إلى اتفاقيات دولية خاصة بمكافحة الجريمة المعلوماتية كاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة في القاهرة بتاريخ 21 ديسمبر سنة 2010.

الكلمات المفتاحية: الاتجار بالأشخاص، تقنية المعلومات، التحفظ على البيانات المخزنة، أمر تسليم المعلومات، تفتيش وضبط المعلومات.

Résumé:

Le crime de traite des êtres humains est l'un des plus graves crimes organisés dans le monde d'aujourd'hui. Il conduit à l'exploitation des êtres humains par les gangs criminels dans toutes les formes d'exploitation. À l'ère de la mondialisation, ce crime est devenu de plus en plus dangereux par la possibilité de l'utilisation à travers la technologie de l'information, ce qui a facilité la communication entre les gangs de la traite et le trafic.

Il est donc nécessaire une coopération internationale pour lutter contre le crime de traite des êtres humains en concluant plusieurs conventions telles que le Protocole visant à prévenir, réprimer et punir la traite des personnes, en particulier des femmes et des enfants, additionnel à la Convention des Nations Unies contre la criminalité transnationale organisée du l'année 2000, ainsi des conventions privées sur la lutte contre la criminalité de l'information, telle que la Convention arabe pour la lutte contre la cybercriminalité, faite au Caire, l e 21 décembre 2010.

Mots clés : Traite d'êtres humains, le système informatique, Conservation de Données Stockées, Injonction de produire les informations, Perquisition et Saisie de données.

مقدمة:

إن ظهور الحاسوب والإنترنت غير من الفكر الإجرامي لارتكاب الجرائم التقليدية وذلك عن طريق استخدام المجرمين لتقنية المعلومات من أجل اقترف جريمة التزوير أو الإرهاب أو السرقة أو السب والقذف أو الجرائم الإباحية أو جرائم الترويج بالمخدرات والاتجار بها أو جريمة الاتجار بالأشخاص أو جريمة تهريب المهاجرين ...إلخ مما أعطى لهذه الجرائم التقليدية خصوصية وميزات جديدة تختلف كل الاختلاف عما كانت عليه سابقا، الأمر الذي وضع أمام رجال التحري والتحقيق عقبات إجرائية كبيرة تتمثل في عدم كفاية إجراءات التحقيق والتحري التقليدية في تعقب الأدلة الجنائية الإلكترونية الناتجة عن ارتكاب هذا النوع المستحدث من الإجرام، لذا سعت الدول جاهدة إلى ضرورة التطوير من أساليب التحري والتحقيق بها.

ومن أجل إتباع سياسة جنائية فعالة لمكافحة جرائم تقنية المعلومات أدركت الدول العربية ضرورة التعاون الدولي فيما بينها من خلال إبرام الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر سنة 2010 وهذا ما أكدته المادة الأولى من الاتفاقية بأن الهدف من الاتفاقية هو" تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، لدرء أخطار هذه الجرائم حفاظا على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها"، وما كان على الجزائر إلا المصادقة بموجب المرسوم الرئاسي رقم 14-252 المؤرخ في 8 سبتمبر سنة 2014، على هذه الاتفاقية.

ولقد نصت الاتفاقية في الفصل الثاني بعنوان التجريم على جملة الجرائم التي تعتبر جرائم تقنية المعلومات، حيث تحدثت في المادة 16 منها على الجرائم المتعلقة بالجرائم المنظمة والمرتكبة بواسطة تقنية المعلومات مثل جريمة الاتجار بالأشخاص، كنوع من جرائم تقنية المعلومات، بينما خصصت الاتفاقية الفصل الثالث للحديث على الأحكام الإجرائية

إشكالية الدراسة: ما مدى كفاية الأحكام الإجرائية التقليدية للتحري والتحقيق في مكافحة جريمة الاتجار بالأشخاص والمرتكبة بواسطة تقنية المعلومات؟ وما موقف الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة سنة 2010؟

المبحث الأول: ضبط المفاهيم التي لها علاقة بالموضوع:

من أجل فهم أكثر للموضوع، لا بد أولا وقبل الخوض في مناقشة وتحليل مختلف جوانبه القانونية، ضبط وتحديد بعض المفاهيم الهامة، مثل مفهوم جريمة الاتجار بالأشخاص، ومفهوم جريمة الاتجار بالأشخاص والمرتكبة بواسطة تقنية المعلومات وذلك من خلال ما يلي:

المطلب الأول: مفهوم جريمة الاتجار بالأشخاص

سنستعرض في هذا المطلب تعريف جريمة الاتجار بالأشخاص، ثم تمييز هذه الجريمة

عن الجرائم المشابهة لها وذلك وفقا لما يلي:

الفرع الأول: التعريف بجريمة الاتجار بالأشخاص:

يعرف بعض الفقهاء الاتجار بالبشر بأنه "كافة التصرفات المشروعة وغير المشروعة التي تحول الإنسان إلى مجرد سلعة أو ضحية يتم التصرف فيه بواسطة وسطاء محترفين عبر الحدود الوطنية بقصد استغلاله في أعمال ذات أجر متدني أو في أعمال جنسية أو ما شابه ذلك، سواء تم التصوف بإرادة الضحية أو قسرا عنه أو بأية صورة أخرى من صور العبودية"[1]

ويعرف البعض الاتجار بالبشر بأنه: "تجنيد أشخاص أو نقلهم بالقوة، أو الإكراه أو الخداع لغرض الاستغلال بشتى صوره، ومن ذلك الاستغلال الجنسي، العمل الجبري، الخدمة القسرية، التسول، الاسترقاق، تجارة الأعضاء البشرية وغير ذلك".[2].

ووفق ما ورد في المادة 3 من بروتوكول الأمم المتحدة بشأن منع وقمع ومعاقبة الاتجار بالأشخاص لعام 2000 يعني الاتجار بالبشر " تجنيد أشخاص أو نقلهم أو إيواؤهم أو استقبالهم بواسطة التهديد بالقوة أو استعمالها أو غير ذلك من أشكال القسر أو الاختطاف أو الاحتيال أو الخداع أو إساءة استعمال السلطة أو اساءة استغلال حالة استضعاف، أو بإعطاء أو تلقي مبالغ مالية أو مزايا لنيل موافقة شخص له سيطرة على شخص آخر لغرض الاستغلال. ويشمل الاستغلال كحد أدنى، استغلال دعارة الغير، أو سائر أشكال الاستغلال الجنسي، أو السخرة أو الخدمة قسرا أو الاسترقاق أو الممارسات الشبيهة بالرق، أو الاستعباد أو نزع الأعضاء..."[3]

الفرع الثاني: تمييز جريمة الاتجار بالبشر عن الجرائم المشابهة لها

هناك العديد من الجرائم التي تتشابه مع جريمة الاتجار بالأشخاص كجريمة الهجرة غير المشروعة وجريمة تهريب المهاجرين، وسنبين نقاط الاختلاف والتشابه من خلال التالي:

---

[1]- سوزي عدلي ناشد، الإتجار بالبشر بين الإقتصاد الخفي والإقتصاد الرسمي، دار الجامعة الجديدة للنشر والتوزيع، الإسكندرية، 2005، ص 17.

[2]- محمد علي العريان، عمليات الإتجار بالبشر وآليات مكافحتها، دار الجامعة الجديدة، الإسكندرية، 2011، ص 30.

[3]- مرسوم رئاسي رقم 03-417، مؤرخ في 9 نوفمبر سنة 2003، يتضمن التصديق بتحفظ على بروتوكول منع وقمع الاتجار بالأشخاص بخاصة النساء والأطفال، المكمل لاتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، المعتمد من طرف الجمعية العامة لمنظمة الأمم المتحدة يوم 15 نوفمبر سنة 2000، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 69، الصادرة في 12 نوفمبر سنة 2003، ص 5، أنظر كذلك: عادل عبد الجواد محمد، الاتجار بالبشر، مقال منشور ضمن: مجلة الأمن والحياة، جامعة نايف العربية للعلوم الأمنية، العدد 354، 1432، ص 51-52.

أولا - الهجرة غير الشرعية:

هي خروج المواطن من إقليم الدولة من غير المنافذ الشرعية المخصصة لذلك أو من منفذ شرعي باستخدام وثائق سفر مزورة، أما الدولة المستقبلة للمهاجرين فينصب اهتمامها على الوجود على أراضيها بغير موافقتها، سواء كان ذلك الوافد قادما من بلده أو من دولة أخرى وسواء خرج من منفذ شرعي ووصل إلى منفذ شرعي أو أنه خرج من منفذ شرعي ووصل إلى منفذ غير شرعي، وسواء قصد الإقامة المستمرة أو المؤقتة، فمناط التأثير لديها هو الوجود على أراضيها بغير موافقتها.[1]

ومن ضمن التعريفات التي جاءت عن الهجرة غير الشرعية، أنها الانتقال من الوطن الأم إلى الوطن المهاجر إليه للإقامة فيه بصفة مستمرة، بطريق مخالف للقواعد المنظمة للهجرة بين الدول طبقا لأحكام القانون الداخلي والدولي. ويمكن أن تعرف الهجرة غير الشرعية أيضا بأنها تدبير الدخول غير المشروع من وإلى إقليم أية دولة من قبل أفراد أو مجموعات من غير المنافذ المحددة لذلك، دون التقيد بالضوابط والشروط المشروعة التي تفرضها الدولة في مجال تنقل الأفراد.[2]

ثانيا- تهريب المهاجرين (تهريب البشر):

يعرف بروتوكول مكافحة تهريب المهاجرين عن طريق البر والبحر والجو المكمل لاتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية في المادة 3: "يقصد بتعبير تهريب المهاجرين تدبير الدخول غير المشروع لأحد الأشخاص إلى دولة طرف ليس ذلك الشخص من مواطنيها أو من المقيمين الدائمين فيها، وذلك من اجل الحصول، بصورة مباشرة أو غير مباشرة، على منفعة مالية أو منفعة مادية أخرى".[3]

ثالثا- العلاقة بين الهجرة غير شرعية أو تهريب البشر والاتجار بالبشر:

والحقيقة أن الاتجار يختلف عن الاثنين وأحيانا يشتمل على الاثنين معا: التهريب والهجرة غير الشرعية، فالتهريب يشتمل على دخول الأشخاص لدولة ما بصورة غير قانونية وعبر الحدود الوطنية وبالمخالفة لقوانين الهجرة لتلك الدولة. وأحيانا يتحول التهريب إلى

---

[1] - ندوة علمية: مكافحة الهجرة غير المشروعة، مجلة الأمن والحياة، عدد 357، جامعة نايف العربية للعلوم الأمنية، 1433، 62-63.

[2] - المرجع نفسه، ص 63.

[3] - مرسوم رئاسي رقم 03-418، مؤرخ في 9 نوفمبر سنة 2003، يتضمن التصديق بتحفظ على بروتوكول مكافحة تهريب المهاجرين عن طريق البر والبحر والجو، المكمل لاتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، المعتمد من طرف الجمعية العامة لمنظمة الأمم المتحدة يوم 15 نوفمبر سنة 2000، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 69، الصادرة في 12 نوفمبر سنة 2003، ص 11.

اتجار بالأشخاص، وذلك يحدث عندما تدفع مجموعة أفراد أو حتى فرد واحد أموالا ليتم تهريبهم إلى دولة أخرى وعند وصولهم، يجدون أنفسهم واقعين تحت طائلة دين ضخم جدا جديد غير الذي دفعوه مسبقا وأنهم ليسوا أحرارا لمغادرة تلك الدولة حتى يسددوا هذا الدين.[1]

وهناك علاقة وطيدة بين الهجرة غير المشروعة وتهريب البشر والاتجار بهم، فغالبية المهاجرين غير الشرعيين يلجأون إلى أباطرة تهريب البشر لتنظيم هروبهم إلى الدول التي يرغبون في الانتقال والعيش بها مقابل مبالغ مالية، فتقوم عصابات تهريب البشر غالبا عن طريق البحر باستخدام السنابك القديمة والقوارب ذات المولدات الكبيرة في الإبحار من مناطق معينة بسواحل البحار متجهين إلى المناطق التي يقصدونها .[2]

المطلب الثاني: مفهوم جريمة الاتجار بالأشخاص والمرتكبة بواسطة تقنية المعلومات

سنتطرف في هذا المطلب إلى تعريف جريمة الاتجار بالأشخاص والمرتكبة بواسطة تقنية المعلومات في الفرع الأول، ثم العلة من ضرورة سن إجراءات حديثة وخاصة للتحري والتحقيق في هذا النوع من الإجرام في الفرع الثاني وذلك كالتالي:

الفرع الأول: تعريف جريمة الاتجار بالأشخاص والمرتكبة بواسطة تقنية المعلومات

نصت المادة 16 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة سنة 2010، على الجرائم المتعلقة بالجرائم المنظمة والمرتكبة بواسطة تقنية المعلومات، وهي:

"1- القيام بعمليات غسل أموال أو طلب المساعدة أو نشر طرق القيام بغسل الأموال.

2- الترويج للمخدرات والمؤثرات العقلية أو الاتجار بها.

3- الاتجار بالأشخاص.

4- الاتجار بالأعضاء البشرية.

5- الاتجار غير المشروع بالأسلحة" [3].

---

[1]- نهال فهمي، التجربة العربية في مكافحة الاتجار بالبشر، مقال مقدم في فعاليات المؤتمر: مكافحة الاتجار بالبشر، منشور بمجلة الأمن والحياة، العدد 332، جامعة نايف العربية للعلوم الأمنية، الرياض، 1431، ص 36.

[2]- أنظر في ذلك: عبد الله بن سعود السراني، العلاقة بين الهجرة غير المشروعة وجريمة تهريب البشر، بحث منشور ضمن فعاليات مؤتمر مكافحة الهجرة غير المشروعة، منشور ضمن: مجلة الأمن والحياة، العدد 357، جامعة نايف العربية للعلوم الأمنية، الرياض، 61-62.

[3]- مرسوم رئاسي رقم 14-252، المؤرخ في 8 سبتمبر سنة 2014، يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21 ديسمبر سنة 2010، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 57، الصادرة في 28 سبتمبر سنة 2014، ص 6.

وعليه اشترطت المادة 16 أن تكون الجرائم المنظمة السابقة الذكر مرتكبة بواسطة تقنية المعلومات -لكي تتخذ وصف الجرائم المعلوماتية أو جرائم تقنية المعلومات-، حتى يمكن تطبيق عليها الأحكام الموضوعية والإجرائية التي جاءت بها هذه الاتفاقية.

وتعرف المادة 2-1 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، مصطلح تقنية المعلومات بأنه: "أية وسيلة مادية أو معنوية أو مجموعة وسائل مترابطة أو غير مترابطة تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها وفقا للأوامر والتعليمات المخزنة بها ويشمل ذلك جميع المداخلات والمخرجات المرتبطة بها سلكيا ولا سلكيا في نظام أو شبكة"[1].

وعليه إذا ارتكبت جريمة الاتجار بالبشر بواسطة تقنية المعلومات فإنها تكيف على أنها جريمة معلوماتية أو جريمة تقنية معلومات، وهذا ما يقودنا بالتالي إلى تعريف الجريمة المعلوماتية من حيث معيار الوسيلة المستخدمة ولا نتطرق إلى تعريف الجريمة المعلوماتية من حيث معيار أنماط السلوك محل التجريم أو موضوع الجريمة أو من خلال المعيار الشخصي لأنها معايير لا ترتبط بموضوع بحثنا.

ينطلق أصحاب تعريف الجريمة المعلوماتية من خلال معيار الوسيلة المستخدمة من أن هذه الجريمة تتحقق باستخدام الكمبيوتر وسيلة لارتكاب الجريمة، حيث عرفها كلاوس تايدومان Tiedemaun بأنها " كافة أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب الآلي".[2]

وكذلك الأستاذ Leslie D .Ball أنها " فعل إجرامي يستخدم الحاسوب في ارتكابه كأداة رئيسية" [3]

وعرفها MERWE بأنها " الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي أو هي الفعل الإجرامي الذي يستخدم في اقترافه الحاسب الآلي كأداة رئيسية، أو هي مختلف صور السلوك الإجرامي التي ترتكب باستخدام المعالجة الآلية للبيانات ". [4]

---

[1]- مرسوم رئاسي رقم 14-252، المؤرخ في 8 سبتمبر سنة 2014، يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، السابق ذكره، ص 4.

[2]- تعريف مشار إليه لدى: طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2009، ص 154؛ قارة أمال، الجريمة المعلوماتية، رسالة لنيل درجة الماجستير في القانون الجنائي والعلوم الجنائية، جامعة الجزائر، 2001-2002، ص 18.

[3]- يونس خالد عرب مصطفى، جرائم الحاسوب، دراسة مقارنة، رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير في القانون، كلية الدراسات العليا، الجامعة الأردنية، عمان، 1994، ص 55.

[4]- تعريف مشار إليه لدى: طارق إبراهيم عطية، المرجع السابق، ص 153.

الفرع الثاني: العلة من سن اجراءت خاصة للتحري والتحقيق في جريمة الاتجار بالأشخاص المرتكبة بواسطة تقنية المعلومات

أبرزت عملية مكافحة جرائم الكمبيوتر والانترنت، تحديات ومشكلات كبيرة تغاير في كثيرا التحديات والمشكلات التي ترتبط بالجرائم التقليدية الأخرى حيث[1]:

هذه الجرائم لا تترك أثرا ماديا في مسرح الجريمة كغيرها من الجرائم ذات الطبيعة المادية كما أن مرتكبيها يمتلكون القدرة على إتلاف أو تشويه أو ضياع الدليل الرقمي في فترة قصيرة.

والتفتيش في هذا النوع من الجرائم يتم غالبا على نظم الكمبيوتر وقواعد البيانات وشبكات المعلومات، وقد يتجاوز أحيانا النظام المشتبه به إلى أنظمة أخرى مرتبطة به داخل الوطن أو خارجه، لشيوع التشبيك بين الحواسيب وانتشار الشبكة الداخلية على مستوى المنشآت والشبكات المحلية والإقليمية والدولية على مستوى الدول، وامتداد التفتيش إلى نظم غير النظام محل الاشتباه يثير تحديات كبيرة أولها مدى قانونية هذا الإجراء ومدى مساسه بحقوق الخصوصية المعلوماتية لأصحاب النظم التي يمتد إليها التفتيش.

كما أن الضبط لا يتوقف على تحريز جهاز الكمبيوتر ومكوناته المادية فقد يمتد الضبط إلى أشياء معنوية تتمثل في المعطيات والبيانات والبرامج المخزنة في النظام أو النظم المرتبطة بالنظام محل الاشتباه، والتي قد تتعرض بسهولة للتغيير والإتلاف، وهذه الحقائق تثير مشكلات متعددة، منها المعايير المقبولة للضبط المعلوماتي والمعايير المتبعة في التحريز إضافة إلى مدى مساس إجراءات الضبط بخصوصية صاحبه –وان كان المشتبه به– عندما تتجاوز أنشطة الضبط إلى كل محتويات النظام التي تضم عادة معلومات وبيانات قد يحرص على سريتها أو أن تكون محل حماية بحكم القانون أو لطبيعتها أو تعلقها بجهات أخرى.

وأدلة الإدانة في الجرائم المعلوماتية ذات نوعية مختلفة، فهي معنوية الطبيعة كسجلات الكمبيوتر ومعلومات الدخول والاشتراك والنفاذ والبرمجيات، وقد أثارت هذه الأدلة الرقمية وتثير أمام القضاء مشكلات كبيرة من حيث مدى قبولها وحجيتها والمعايير المتطلبة لتكون كذلك خاصة في ظل قواعد الإثبات التقليدية.

كما أن اختصاص القضاء بالنظر في الجرائم المعلوماتية والقانون الواجب تطبيقه على الفعل لا يتمتع دائما بالوضوح أو القبول لأن غالبية هذه الأفعال ترتكب من قبل أشخاص خارج الحدود أو أنها تمر عبر شبكات معلوماتية وأنظمة معلومات خارج الحدود حتى عندما

---

[1]– يونس عرب، جرائم الكمبيوتر والإنترنت، موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، الجزء الأول، منشورات اتحاد المصارف العربية، دون بلد نشر، 2002، ص 483-484.

يرتكبها شخص من داخل الدولة على نظام في الدولة نفسها، وهو ما يبرز أهمية معرفة ما إذا كانت النظريات والقواعد المعتمدة في مجال تحديد الاختصاص القضائي والقانون الواجب التطبيق يمكن تطبيقها على هذه الجرائم أم يتعين إفراد قواعد خاصة بها في ضوء خصوصيتها وما تثيره من مشكلات في حقل الاختصاص القضائي، ويرتبط بمشكلات الاختصاص وتطبيق القانون مشكلات امتداد أنشطة الملاحقة والتحري والضبط والتفتيش خارج الحدود وما يتطلبه ذلك من تعاون دولي للموازنة بين موجبات المكافحة ووجوب حماية السيادة الوطنية.

إن خصوصية الجرائم المعلوماتية والمشاكل الإجرائية التي تثيرها أمام القائمين على التحري والتحقيق والذي اثر على مستوى مكافحة هذا النوع من الإجرام، استدعى الدول إلى التطوير في سياستها الجنائية بتطوير إجراءات التحقيق والتحري، بصورة تتلائم مع هذه الخصوصية وتمكن رجال الشرطة القضائية، والمحقق من كشف الجريمة والتوصل إلى مرتكبيها والتحقيق معهم وجمع الأدلة بالسرعة والدقة اللازمين، وتقديمهم للمحكمة، ولتحقيق ذلك وجب: تطوير الإجراءات الجنائية التقليدية من جهة، ومن جهة أخرى، خلق إجراءات جزائية جديدة وحديثة، للتحقيق والتحري في هذا النوع المستحدث من الإجرام، كما سنتطرق إليه في المبحث الثاني من هذا البحث من خلال التكلم عن الإجراءات التي قررتها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، منها جريمة الإتجار بالأشخاص والمرتكبة بواسطة تقنية المعلومات..

المبحث الثاني: الإجراءات المتبعة في مكافحة جريمة الاتجار بالأشخاص المرتكبة بواسطة تقنية المعلومات من خلال الاتفاقية

نصت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة سنة 2010، في الفصل الثالث بعنوان الأحكام الإجرائية، على جملة من الإجراءات الجزائية التي تكفل مكافحة فعالة لجرائم تقنية المعلومات، وتتمثل هذه الإجراءات في إجراءات تتعلق بالبيانات الساكنة، إجراءات تتعلق بالبيانات المتحركة، وتفتيش وضبط المعلومات المخزنة، وسنستعرض كل إجراء من هذه الإجراءات من خلال ما يلي:

المطلب الأول: الإجراءات المتعلقة بالبيانات الساكنة

وتتمثل هذه الإجراءات في إجراء التحفظ العاجل على البيانات المخزنة في تقنية المعلومات وأمر تسليم المعلومات، وسنتطرق لهذين الإجراءين من خلال الآتي:

الفرع الأول: إجراء التحفظ العاجل على البيانات المخزنة في تقنية المعلومات

سنتناول هذا الإجراء من خلال تحديد مفهومه، ثم بيان أحكامه من خلال الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، وذلك كالآتي:

أولا- مفهوم الإجراء:

يحتوي هذا الإجراء على التحفظ العاجل على البيانات المخزنة في تقنية المعلومات والتحفظ العاجل والكشف الجزئي لمعلومات تتبع المستخدمين.

1- مفهوم التحفظ العاجل على البيانات المخزنة في تقنية المعلومات[1]:

ينطبق هذا الإجراء على البيانات المخزنة au données stockées **التي سبق تجميعها** collectées **والاحتفاظ بها** archivées **عن طريق حائزي البيانات** Les détenteurs de données، **مثال ذلك مقدمي الخدمات (مزودي الخدمات)، بيد أنها لا تنطبق على التجميع في الوقت الفعلي (الجمع الفوري)** en temps réel **والتحفظ المستقبلي على البيانات المتعلقة بالمرور (على معلومات تتبع المستخدمين) أو الولوج في الوقت الفعلي إلى محتوى الاتصالات (اعتراض معلومات المحتوى). إذ أن هذه المسائل تمت معالجتها.**

وبالنسبة لغالبية الدول، فإن التحفظ على البيانات يعد سلطة أو إجراء قانونيا جديدا كليا في القانون الداخلي. فهو أداة جديدة للتنقيب الهام في مجال الكفاح ضد الإجرام المعلوماتي والجرائم المتصلة به، وبالأخص ضد الجرائم المرتكبة بواسطة شبكة الانترنت وذلك للمبررات التالية:

– بسبب قابلية البيانات المعلوماتية للتلاشي، فإن هذه البيانات من السهل أن تخضع للتلاعب، أو التغيير وهكذا يسهل فقدان عناصر إثبات الجريمة، من خلال الإهمال وممارسات التخزين غير الدقيقة، أو التغيير العمدي لها أو محوها من أجل تدمير كل عنصر للإثبات، أو محوه في إطار العمليات العادية أو الروتينية لمحو البيانات التي لم تعد حاجة إليها، وإحدى وسائل المحافظة على سلامة البيانات تتمثل في قيام السلطات المختصة بعمل تفتيشات أو الولوج بطريقة أخرى للبيانات لضبطها أو الحصول عليها بطريقة أخرى.

ومع ذلك إذا كان حارس البيانات جدير بالثقة، كما في حالة شركة تجارية ذات سمعة طيبة، فإن سلامة البيانات يمكن ضمانها بطريقة أسرع عن طريق إصدار أمر بالتحفظ على البيانات لديه. وبهذا يمكن أن يكون الأمر بالتحفظ على البيانات أقل قلقا أو إخلالا بالنظام بالنسبة للأنشطة، وأقل ضررا على سمعة الشركة الأمينة، من عملية تفتيش الأماكن بغرض الضبط.

– الجرائم المعلوماتية والجرائم المتصلة بالحاسب، غالبا ما يتم ارتكابها عن طريق نقل الاتصالات بواسطة نظام معلوماتي. هذه الاتصالات يمكن أن تحوي محتوى غير مشروع، مثال

---

[1] – هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية، معلقا عليها، دار النهضة العربية، القاهرة، 2007.ص 191 وما بعدها.

ذلك مواد إباحية طفولية، فيروسات معلوماتية، أو أي تعليمات أخرى، تحمل اعتداء على البيانات، أو تعيق حسن أداء النظام المعلوماتي، كما يمكن أيضا أن تحوي عناصر يمكن من خلالها إثبات ان جرائم أخرى قد تم ارتكابها، مثال ذلك حالات الاتجار بالمخدرات أو النصب وترتيبا على ذلك فإن التحقق من هوية مصدر أو منتهى هذه الاتصالات الخارجية يمكن أن يساعد على تحديد هوية مرتكب هذه الجرائم. ومن أجل تعيين مصدر ومنتهى هذه الاتصالات، ينبغي تجهيز أو تهيئة بيانات التجارة غير المشروعة المتعلقة بهذه الاتصالات الخارجية.

- عندما تكون هذه الاتصالات تقدم محتوى غير مشروع أو دليل أفعال جنائية فإن صورا من هذه الاتصالات يتم الاحتفاظ بها بواسطة مقدمي الخدمات، على سبيل المثال البريد الإلكتروني التحفظ على هذه الاتصالات يكون هاما من أجل عدم فقد عناصر الإثبات الجوهرية. فلا مراء في أن إعطاء صور من هذه الاتصالات الخارجية، على سبيل المثال البريد المخزن، يمكن أن يكشف عن الجرائم التي تم ارتكابها.

2- مفهوم التحفظ العاجل والكشف الجزئي لمعلومات تتبع المستخدمين[1]:

حينما يكون هناك مقدم خدمة (مزود الخدمة) واحد أو عدة مقدمين للخدمة (مزودي الخدمة) قد ساهموا في نقل اتصال معين، فإن التحفظ العاجل على بيانات المرور (الحفظ العاجل لمعلومات تتبع المستخدمين) يمكن أن يتم من خلالها جميعا. بيد أن هذه المادة لم تحدد الوسائل التي من خلالها يمكن تحقيق ذلك، تاركة هذا الأمر للقانون الداخلي ليحدد الطريقة التي تتلائم مع نظامه القانوني والاقتصادي.

وإحدى وسائل التحفظ العاجل على البيانات في مثل هذه الحالات تتمثل في قيام السلطات المختصة بإصدار أمر عاجل منفصل لكل مقدم من مقدمي الخدمة. لكن لوحظ على هذه الوسيلة أن الحصول على عدة أوامر منفصلة يمكن أن يستغرق وقتا طويلا للغاية.

لذلك فإن أحد الحلول المفضلة هو الحصول على أمر واحد ولكن سوف ينطبق على كل مقدمي الخدمات الذين ساهموا في نقل الاتصال. وهذا الأمر العام يتم إبلاغه بالتعاقب لكل مقدمي الخدمات المعينين أو أصحاب الشأن.

وهناك بديل آخر، يمكن أن يضم كل مقدمي الخدمات، ثم يطلب من كل مقدم خدمة يصله الأمر، أن يقوم بإخطار من يليه بوجود وفحوى هذا الأمر بالتحفظ وهكذا. وهذا النقل يتم وفقا لنصوص القانون الداخلي بحيث يكون له أثر يسمح لمقدم الخدمة التالي بـــأن يتحفظ

---

[1] - هلالي عبد اللاه أحمد، كيفية المواجهة التشريعية لجرائم المعلوماتية، في النظام البحريني على ضوء اتفاقية بودابيست، دار النهضة العربية، القاهرة، 2011، ص 190 وما بعدها.

إراديا على بيانات المرور الملائمة، أو أن ينص على التحفظ عليها إجباريا. ويمكن لمقدم الخدمة التالي أن يقوم من جانبه بإخطار من يليه في التسلسل.

وبهذه الطريقة يكون بمقدور السلطات المكلفة بالتنقيب والتحري أن تحدد منبع ومصب الاتصال، وكذلك تحديد هوية أي فاعل أو فاعلين للجريمة النوعية والذين سيكونون موضوعا للتنقيب والتحري.

وفي الأخير، نجد أن الإجراءات المشار إليها في هذه المادة يجب أيضا أن تكون خاضعة للقيود، والشروط، والضمانات المشار إليها في المادتين 14-15 من الاتفاقية.

ثانيا- التحفظ العاجل على البيانات المخزنة في تقنية المعلومات وفقا للاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010:

تناولت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المبرمة بالقاهرة سنة 2010 التحفظ العاجل على البيانات المخزنة والتحفظ العاجل والكشف الجزئي لمعلومات تتبع المستخدمين وفقا لما يلي:

1- التحفظ العاجل على البيانات المخزنة في تقنية المعلومات:

نصت المادة 23 من الاتفاقية على أنه[1]:

"1- تلتزم كل دولة طرف 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 وخصوصا إذا كان هناك اعتقاد أن تلك البيانات عرضة للفقدان أو التعديل.

2- تلتزم كل دولة طرف بتبني الإجراءات الضرورية فيما يتعلق بالفقرة (1) بواسطة إصدار أمر إلى شخص من أجل حفظ معلومات تقنية المعلومات المخزنة والموجودة بحيازته أو سيطرته ومن أجل إلزامه بحفظ وصيانة سلامة تلك المعلومات لمدة أقصاها 90 يوما قابلة للتجديد. من اجل تمكين السلطات المختصة من البحث والتقصي.

3- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لإلزام الشخص المسؤول عن حفظ تقنية المعلومات للإبقاء على سرية الإجراءات طوال الفترة القانونية المنصوص عليها في القانون الداخلي".

2- التحفظ العاجل والكشف الجزئي لمعلومات تتبع المستخدمين:

نصت عليه المادة 24 من الاتفاقية، بحيث[1]:

---

[1]- مرسوم رئاسي رقم 14-252، المؤرخ في 8 سبتمبر سنة 2014، يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، السابق ذكره، ص7.

"تلتزم كل دولة طرف بتبني الإجراءات الضرورية فيما يخص معلومات تتبع المستخدمين من أجل:

[1]- ضمان توفر الحفظ العاجل لمعلومات تتبع المستخدمين بغض النظر عن اشتراك واحد أو أكثر من مزودي الخدمة في بث تلك الاتصالات.

[2]- ضمان الكشف العاجل للسلطات المختصة لدى الدولة الطرف أو لشخص تعينه تلك السلطات لمقدار كاف من معلومات تتبع المستخدمين لتمكين الدولة الطرف من تحديد مزودي الخدمة ومسار بث الاتصالات".

الفرع الثاني: أمر تسليم المعلومات

سندرس هذا الإجراء من خلال أيضا الوقوف على مفهومه، ثم بيان أحكامه من خلال الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 وذلك من خلال التالي:

أولا- مفهوم الإجراء[2]:

ويقصد بهذا الإجراء مناشدة كل دولة سلطاتها المختصة بأن تلزم شخصا ما داخل أراضيها بتقديم (بتجهيز) بيانات معلوماتية معينة مخزنة، أو أن تلزم مقدم خدمات على أرض طرف بأن يرسل بيانات المشترك (معلومات تتبع المستخدم). والبيانات المشار إليها عبارة عن بيانات مخزنة أو موجودة لكنها لا تضم بيانات لم توجد بعد، مثال ذلك بيانات المرور (معلومات تتبع المستخدمين) أو المحتوى المرتبطة بالاتصالات المستقبلية. وبدلا من إلزام الدول بتطبيق إجراءات إجبارية بالنسبة للأغيار أو الطرف الثالث مثل التفتيش وضبط البيانات، فإنه من المهم أن تفرض هذه الدول من خلال قانونها الداخلي وسائل أخرى للتنقيب والتحري بطريقة أقل تطفلا أو تدخلا للحصول على معلومات ضرورية بالنسبة للتحقيقات أو التنقيبات الجنائية.

وتأسيس مثل هذا المكانيزم الإجرائي سيصبح أيضا مفيدا من أجل الأغيار حائزي البيانات مثل مقدمي الدخول للأنترنت. الذين يكونون غالبا على استعداد لمساعدة السلطات في الكفاح ضد الإجرام على أساس إرادي من خلال تقديم البيانات التي بحوزتهم، ولكن منهم من يفضل وجود أساس قانوني مناسب من أجل تقديم هذه المساعدة، لإعفائهم من كل مسئولية عقدية أو غير عقدية.

---

[1]- مرسوم رئاسي رقم 14-252، المؤرخ في 8 سبتمبر سنة 2014، يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، المصدر السابق، ص8.

[2]- هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية، المرجع السابق، ص 221 وما بعدها.

وفي إطار التنقيب الجنائي، فإن المعلومات المتعلقة بالمشتركين (معلومات تتبع المستخدمين) يمكن أن تكون ضرورية في حالتين خاصتين:

الأولى: إن هذه المعلومات ضرورية من أجل تحديد الخدمات والإجراءات الفنية المرتبطة التي استخدمت أو التي تستخدم بواسطة المشترك، مثل نوع الخدمة التليفونية المستخدمة كأن يكون تليفونا محمولا مثلا.

نوع الخدمات المرتبطة المستخدمة: مثل النداء الآلي والبريد الصوتي رقم التليفون أو أي عنوان إليكتروني، مثل عنوان البريد الإليكتروني.

الثانية: عندما يكون العنوان التقني معروفا، فإن المعلومات المتعلقة بالمشتركين تتم حيازتها من أجل المساعدة في تحديد هوية الشخص المطلوب، وهناك المعلومات الأخرى المتعلقة بالمشتركين، مثال ذلك المعلومات التجارية التي تتمثل في دوسيهات الفواتير، ودفع الاشتراك، يمكن أن تكون مفيدة للتنقيبات والتحقيقات والتحريات الجنائية، وبالأخص عندما تكون الجريمة موضوع التنقيب والتحري متعلقة بحالة غش معلوماتي أو جريمة أخرى اقتصادية.

وتأسيسا على ما تقدم، فإن المعلومات المتعلقة بالمشتركين تشمل على أنواع مختلفة من المعلومات بالنسبة لاستخدام الخدمة ومستخدم الخدمة.

ثانيا- أمر تسليم المعلومات وفقا للاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010:

نصت المادة 25 من الاتفاقية على[1]:

"تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى:

1- أي شخص في إقليمها لتسليم معلومات معينة في حيازة ذلك الشخص والمخزنة على تقنية معلومات أو وسيط تخزين معلومات.

2- أي مزود خدمة يقدم خدماته في إقليم الدولة الطرف لتسليم معلومات المشترك المتعلقة بتلك الخدمات في حوزة مزود الخدمة أو تحت سيطرته".

المطلب الثاني: الإجراءات المتعلقة بالبيانات المتحركة (الجمع الفوري للمعلومات)

سنتكلم عن إجراء الجمع الفوري للمعلومات، من خلال تحديد مفهومه وبيان قواعده وفقا للاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 وذلك من خلال:

---

[1]- مرسوم رئاسي رقم 14-252، المؤرخ في 8 سبتمبر سنة 2014، يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، السابق ذكره، ص8.

الفرع الأول: مفهوم الإجراء[1]:

عبارة "في الوقت الفعلي" أو "الجمع الفوري" تعني أن هذا العنوان يطبق على تجميع أدلة المحتويات المتعلقة بالاتصالات في فترة الإنتاج وتجميعها لحظة النقل عبر الاتصال.

البيانات التي يتم تجميعها تنقسم إلى نوعين: البيانات المتعلقة بالمرور (معلومات تتبع المستخدمين) والبيانات المتعلقة بالمحتوى (اعتراض معلومات المحتوى). وبالنسبة للنوع الأول فتعرف بأنها كل البيانات التي تعالج الاتصالات التي تمر عن طريق نظام معلوماتي، والتي يتم إنتاجها بواسطة هذا النظام المعلوماتي بوصفه عنصرا في سلسلة الاتصال، مع تعيين المعلومات التالية: أصل الاتصال، مقصد أو الجهة المقصودة بالاتصال، خط السير، ساعة الاتصال، تاريخ الاتصال، حجم الاتصال، وفترة الاتصال أو نوع الخدمة. أما بالنسبة للنوع الثاني: فتشير إلى المحتوى الإخباري للاتصال، بمعنى مضمون الاتصال أو الرسالة أو المعلومات المنقولة عن طريق الاتصال، فيما عدا البيانات المتعلقة بالمرور.

الفرع الثاني: الجمع الفوري للمعلومات في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010

نصت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، ضمن الفصل الثالث الخاص بالأحكام الإجرائية، على التزام الدول الأطراف بتبني في قانونها الداخلي التشريعات والإجراءات الضرورية لجمع الأدلة عن الجرائم بشكل إلكتروني، حيث نصت الاتفاقية في المادتين 28 و29 على: الجمع الفوري لمعلومات تتبع المستخدمين، واعتراض معلومات المحتوى ونظمتهما وفقا لما يلي:

أولا- الجمع الفوري لمعلومات تتبع المستخدمين

نصت عليه المادة (المادة 28) بحيث:

"1- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من[2]:

أ) جمع أو تسجيل بواسطة الوسائل الفنية على إقليم تلك الدولة الطرف،

ب) إلزام مزود الخدمة ضمن اختصاصه الفني بأن:

- يجمع أو يسجل بواسطة الوسائل الفنية على إقليم الدولة الطرف، أو

- يتعاون أو يساعد السلطات المختصة في جمع وتسجيل معلومات تتبع المستخدمين بشكل فوري مع الاتصالات المعنية في إقليمها والتي تبث بواسطة تقنية المعلومات.

---

[1]- هلالي عبد اللاه أحمد، كيفية المواجهة التشريعية لجرائم المعلوماتية، المرجع السابق، ص213 وما بعدها.

[2]- مرسوم رئاسي رقم 14-252، مؤرخ في 8 سبتمبر سنة 2014، يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، السابق ذكره، ص 8-9.

2- إذا لم تستطع الدولة الطرف بسبب النظام القانوني الداخلي تبني الإجراءات المنصوص عليها في الفقرة (1-أ) فيمكنها تبني إجراءات أخرى بالشكل الضروري لضمان الجمع أو التسجيل الفوري لمعلومات تتبع المستخدمين المرافقة للاتصالات المعنية في إقليمها باستخدام الوسائل الفنية في ذلك الإقليم".

ثانيا- اعتراض معلومات المحتوى:

تكلمت عليه الاتفاقية بالمادة 29 حيث:

"1- تلتزم كل دولة طرف بتبني الإجراءات التشريعية والضرورية فيما يخص بسلسلة من الجرائم المنصوص عليها في القانون الداخلي، لتمكين السلطات المختصة من[1]:

أ) الجمع أو التسجيل من خلال الوسائل الفنية على إقليم الدولة الطرف، أو

ب) التعاون ومساعدة السلطات المختصة في جمع أو تسجيل معلومات المحتوى بشكل فوري للاتصالات المعنية في إقليمها والتي تبث بواسطة تقنية المعلومات.

2- إذا لم تستطع الدولة الطرف بسبب النظام القانوني الداخلي تبني الإجراءات المنصوص عليها في الفقرة (1-أ) فيمكنها تبني إجراءات أخرى بالشكل الضروري لضمان الجمع والتسجيل الفوري لمعلومات المحتوى المرافقة للاتصالات المعنية في إقليمها باستخدام الوسائل الفنية في ذلك الإقليم.

3-تلتزم كل دولة طرف باتخاذ الإجراءات الضرورية لإلزام مزود خدمة بالاحتفاظ بسرية أية معلومات عند تنفيذ الصلاحيات المنصوص عليها في هذه المادة".

المطلب الثالث: تفتيش وضبط المعلومات المخزنة

سنتطرق لمفهوم كل من إجراء التفتيش والضبط ثم بيان أحكام كل إجراء من خلال الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 وذلك كالتالي:

الفرع الأول: مفهوم إجراء التفتيش والضبط:

سنتطرق أولا إلى التعريف بإجراء التفتيش والضبط، ثم بيان أحكام تفتيش وضبط المعلومات المخزنة وفقا للاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.

أولا- التعريف بالتفتيش:

لم تتضمن التشريعات العربية تعريفا للتفتيش واكتفت بالنص على أنه من إجراءات التحقيق. ولكن الفقه العربي أورد تعريفات متعدد للتفتيش كإجراء تحقيقي، وعلى الرغم من

---

[1]- مرسوم رئاسي رقم 14-252، مؤرخ في 8 سبتمبر سنة 2014، يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، السابق ذكره، ص 9.

اختلافها من حيث الشكل إلا أنها تتحد في الموضوع. فيعرف جانب من الفقه التفتيش بأنه: (إجراء من إجراءات التحقيق التي تهدف إلى ضبط أدلة الجريمة وكل ما يفيد في كشف الحقيقة من أجل إثبات ارتكاب الجريمة أو نسبتها إلى المتهم وينصب على شخص المتهم أو المكان الذي يقيم فيه، ويجوز أن يمتد إلى أشخاص غير المتهمين ومساكنهم وذلك وفقا للشروط والأوضاع المحددة في القانون)[1].

والمقصود بالتفتيش كذلك (هو البحث في مستودع سر المتهم عن أشياء تفيد في كشف الحقيقة ونسبتها إليه، أو هو الاطلاع على محل منحه القانون حماية خاصة، باعتباره مستودع سر صاحبه، ويستوي في ذلك أن يكون المحل مسكنا أو ما هو في حكمه أو أن يكون شخصا)[2].

ويعرف الفقه الغربي التفتيش بتعاريف تشبه ما جاء به الفقه العربي-وقد يكون العكس صحيحا- بسبب أن مرجعية أغلب القوانين العربية وتأثر الفقهاء العرب بالفقه اللاتيني والانكلوسكسوني، فيعرف الفقه الفرنسي التفتيش بأنه البحث الدقيق لكل عناصر الأدلة التي يمكن استخدامها في الدعوى الجزائية والتي تجرى على مسكن المتهم. ويفرق الفقه الفرنسي بين تفتيش المساكن La Perquisition ويطلق عليه أيضا اسم الزيارة المنزلية visite domiciliaire، وتفتيش الأشخاص la fouilié corporlle والذي يكون محله جسم الإنسان وملابسه.

وهكذا فإن التفتيش التحقيقي وسيلة للحصول على الدليل وليس دليلا في حد ذاته[3].

والتفتيش كعمل تحقيقي ينطوي على هذه الدرجة من الأهمية، إن لم يكن الجسامة، فلا يجوز اتخاذه إلا من قبل سلطة التحقيق. ولا يكون لرجال الضبط العدلي حق مباشرته إلا في حالتين: الجرم المشهود من ناحية، والإذن الصادر عن سلطة التحقيق ذاتها من ناحية أخرى (حالة الندب). بل إن الضبطية العدلية إذ تقوم بالتفتيش في حالة الجرم المشهود، فإن هذا

---

[1] - عماد محمد ربيع، حقوق المتهم في مرحلة التحقيق الإبتدائي في قانون أصول المحاكمات الجزائية الأردني، مقال منشور ضمن مجلة البلقاء للبحوث والدراسات، مجلة علمية محكمة، تصدرها عمادة الدراسات العليا والبحث العلمي في جامعة عمان الأهلية، المجلد 12، العدد 1، آب 2007، ص 140.

[2] - علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، عالم الكتب الحديث، الأردن، ،ص 11، كذلك: محمد طارق عبد الرؤوف الحن، جريمة الاحتيال عبر الإنترنت، منشورات الحلبي الحقوقية، لبنان، 2011، ص 274.

[3] - علي حسن محمد الطوالبة، المرجع السابق، ص 12.

التفتيش الواقع لا يعتبر من إجراءات التحقيق، وإنما ينظر إليه بوصفه من قبيل إجراءات الاستدلال[1].

وفي الجرائم المعلوماتية نجد أن الدخول غير المشروع إلى الأنظمة المعلوماتية للبحث والتنقيب في البرامج المستخدمة أو في ملفات البيانات المخزنة عما قد يتصل بجريمة وقعت، إجراء يفيد في كشف الحقيقة عنها وعن مرتكبها. وتقتضيه مصلحة وظروف التحقيق في الجرائم المعلوماتية هو إجراء جائز قانونا ولو لم ينص عليه صراحة باعتباره يدخل في نطاق التفتيش بمعناه القانوني ويندرج تحت مفهومه[2].

ويمكن تعريف تفتيش نظم الحاسوب والانترنت بأنه: (البحث في مستودع سر المتهم عن أشياء مادية أو معنوية تفيد في كشف الحقيقة ونسبتها إليه). أو هو (الإطلاع على محل منحه القانون حماية خاصة باعتباره مستودع سر صاحبه يستوي في ذلك أن يكون هذا المحل جهاز الحاسوب أو نظمه أو الانترنت)[3]. وقد عرف المجلس الأوروبي هذا النوع من التفتيش بأنه إجراء يسمح بجمع الأدلة المخزنة أو المسجلة بشكل إلكتروني[4].

التفتيش في الجرائم الرقمية (المعلوماتية) يكون محله كل مكونات الحاسب الآلي سواء كانت مادية أو معنوية، وكذلك شبكات الاتصال الخاصة به، بالإضافة إلى الأشخاص الذين يستخدمون الحاسب الآلي محل التفتيش وتشمل جميع مكوناته المادية، والمكونات المعنوية التي تشمل برامج النظام وبرامج التطبيقات سابقة التجهيز طبقا لاحتياجات العميل، ويستلزم تفتيش الحاسب الآلي مجموعة من الأشخاص لديهم الخبرة ومهارة تقنية في نظم الحاسب الآلي كمشغلي الحاسب الآلي وخبراء البرامج ومديري النظم المعلوماتية[5].

ونحن بدورنا نرى أن تفتيش الحاسوب الآلي هي تلك الإجراءات المتبعة للبحث عن الأدلة المادية والرقمية الناجمة عن ارتكاب جريمة معلوماتية، بهدف الكشـــف عـن الحقيقة،

---

[1] – سليمان عبد المنعم، أصول الإجراءات الجزائية في التشريع والقضاء والفقه، المؤسسة الجامعية للدراسات، بيروت، الطبعة الثانية، 1999، ص 551-552.

[2] – علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، دراسة مقارنة، المكتب الجامعي الحديث، دون بلد نشر، 2012، ص 38.

[3] – علي حسن محمد الطوالبة، المرجع السابق، ص 12-13.

[4] – علي عدنان الفيل، المرجع السابق، ص 39

[5] – عبد الناصر محمد محمود فرغلي و محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية دراسة تطبيقية مقارنة، بحث مقدم إلى المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، الرياض، 2007، ص 20.

ويشمل التفتيش كل مكونات الحاسوب المادية والمعنوية وشبكات الاتصال الخاصة به وكذا الأشخاص المستخدمون للحاسب الآلي.

ثانيا- التعريف بإجراء الضبط:

يهدف التفتيش إلى ضبط الأدلة المادية التي تفيد في كشف الحقيقة، فالضبط هو غاية التفتيش القريبة أي الأثر المباشر الذي يسفر عنه الإجراء[1]، وهدف التفتيش-سواء في ذلك تفتيش الأشخاص أم المساكن- هو ضبط الأشياء التي تفيد في كشف الحقيقة، أي الأشياء التي تعد في ذاتها الدليل على الجريمة، أو يمكن أن يظهر منها هذا الدليل، وقد تكون هذه الأشياء هي ما استعمل في ارتكاب الجريمة، وقد تكون الأشياء السبب الذي ارتكب لأجله الجريمة[2]. ولما كان الضبط هو الأثر المباشر للتفتيش، وباعتباره أحد إجراءات التحقيق، فتنطبق عليه القواعد التي تنطبق على التفتيش، والعلاقة وثيقة بين التفتيش والضبط، فإذا ما بطل إجراء التفتيش بطل الضبط[3]. وقد يتم الضبط من غير تفتيش، فقد يقدم المتهم أو الشاهد باختياره الأشياء المتعلقة بالجريمة[4].

فالضبط هو الوسيلة القانونية التي تضع بواسطتها السلطة المختصة يدها على جميع الأشياء التي وقعت عليها الجريمة أو نتجت عنها أو استعملت لاقترافها، كالأسلحة والأشياء المسروقة، والثياب الملوثة بالدم، والأوراق...وغير ذلك[5].

الضبط بطبيعته وبحسب تنظيمه القانوني وغايته لا يرد إلا على الأشياء أما الأشخاص فلا يصلحون محلا للضبط بالمعنى الدقيق وإذا كان قانون الإجراءات يتحدث في بعض التصرف عن ضبط الأشخاص وإحضارهم فإنه يعني القبض عليهم وإحضارهم، والقبض نظام قانوني يختلف تماما عن ضبط الأشياء[6].

ولا يفرق القانون في مجال الضبط بين المنقول والعقار فكلاهما يمكن ضبطه كذلك فإنه يستوي أن يكون الشيء مملوكا للمتهم أو لغيره، والقاعدة أن الضبط لا يرد إلا على شيء مادي

---

[1]- فتوح الشاذلي، عفيفي كامل، جرائم الكمبيوتر وحقوق الملف والمصنفات الفنية ودور الشرطة والقانون، منشورات الحلبي الحقوقية، لبنان، 2003، 135.

[2]- محمود نجيب حسني، شرح قانون الإجراءات الجنائية، الطبعة الثالثة، دار النهضة العربية، القاهرة، 1996، ص 481.

[3]- فتوح الشاذلي، عفيفي كامل، المرجع السابق، ص 135.

[4]- محمد طارق عبد الرؤوف الحن، المرجع السابق، ص 290.

[5]- حسن الجوخدار، أصول المحاكمات الجزائية، الجزء الثاني، الطبعة الخامسة، منشورات جامعة دمشق، 1991، ص 162.

[6]- علي عدنان الفيل، المرجع السابق، ص 54.

أما الأشياء المعنوية فلا تصلح بطبيعتها محلا للضبط والشرط اللازم لصحته أن يكون الشيء مفيدا في كشف الحقيقة فكل ما يحقق هذه الغاية يصح ضبطه[1] .

وعن قواعد التحريز والتأمين للمضبوطات المعلوماتية[2]: فإن الدليل في الجرائم المعلوماتية، يتمثل في ذبذبات أو نبضات إلكترونية، مسجلة على دعائم ممغنطة، أو مخزنة في ذاكرة الحواسيب الآلية وبنوك المعلومات. وعملية تحريز وتأمين مضبوطات الأنظمة والشبكات المعلوماتية، بحاجة بأن يكون المحقق، أو من ينتدبه مدركا لطبيعة الأنظمة المعلوماتية، ومؤهلا ودربا للتعامل معها، فكل إغفال، أو إهمال في التعامل مع هذه الأنظمة، قد يؤدي إلى إتلاف الدليل وإفساده، لذا لا بد من وجود إجراءات مقننة، تهدف للمحافظة على سلامة المضبوطات، ومن أبرز الإجراءات الموصى بإتباعها نذكر ما يلي:

– تحديد المادة المعلوماتية المراد ضبطها: نظرا لسهولة التلاعب، في بيانات الأنظمة المعلوماتية وشبكاتها، وبدون ترك أي آثار تذكر، فيتعين على المحقق عند تحديد البيانات المراد ضبطها، أن يقوم بوضع علامة مادية خاصة عليها وينقلها إلى أقراص، أو أشرطة ممغنطة، ومن ثم يقوم المحقق ومشغل النظام بتسجيل بياناته التعريفية على هذه الشرطة، ومن ثم توضع هذه الأشرطة، في علب مخصصة لحفظها والتوقيع عليها، وختمها، وأن تنظم هذه الإجراءات بمحضر، يوقع عليه حسب النصوص القانونية الخاصة بضبط الأشياء وحفظها.

– تأمين البرامج المضبوطة قبل تشغيلها: وفي حالة ضبط البرامج المعلوماتية، يجب على المحقق، أو مشغل الأنظمة المعلوماتية، العمل على تأمين هذه البرامج فنيا، وذلك بعمل نسخ كاملة وسليمة منها، قبل تشغيلها من قبل الخبراء وبواسطة أنظمة معلوماتية مأمونة من جانبه لأنه في كثير من الحالات، إذا تم تشغيل هذه البرامج بغير الطريقة التي صممت فيها، قد تتحول برنامج تدمير ذاتي، وبالتالي يفقد الدليل.

– الالتزام بإتباع القواعد الفنية الخاصة بكيفية نقل الأحراز المعلوماتية وحملها: في عالم الإجرام بشكل عام، يكون هناك مضبوطات، وهناك العديد من المضبوطات، بحاجة الى إتباع طرق خاصة لحفظها خشية عليها من التلف والضياع، والبيانات المعلوماتية المضبوطة والمفرغة على الأقراص، أو الأشرطة الممغنطة، بحاجة إلى عناية خاصة للمحافظة عليها من التلف والضياع، فيجب عند نقلها مراعاة عدم تعرضها للغبار والأتربة، وعدم تعريضها

---

[1] – علي عدنان الفيل، المرجع السابق، ص 54.

[2] – غازي عبد الرحمان هيان الرشيد، الحماية القانونية من الجرائم المعلوماتية (الحاسب والانترنت)، أطروحة دكتوراه في القانون، كلية الحقوق، الجامعة الإسلامية في لبنان، بيروت، 2004، ص 566-567.

للصدمات، أو لأشعة كهرومغناطيسية، حتى لا يتم إتلاف محتوياتها كليا أو جزئيا، وبالتالي تفقد الدليل على ارتكاب الجريمة.

- مراعاة ظروف الحرارة والرطوبة المناسبة لتخزين الأحراز المعلوماتية: يجب عند تخزين الأقراص، والأشرطة المغنطة المحرز، مراعاة ظروف التخزين من حيث الحرارة والرطوبة، ولذلك لا بد من معرفة دراجات الحرارة، والرطوبة المناسبة لحفظها، وإلا قد يؤدي إلى إتلاف البيانات أو إتلاف الأقراص، والأشرطة ذاتها، بما هو مخزن عليها من بيانات مطلوبة.

- ضبط الأقراص والأشرطة الأصلية، وعدم الاقتصار على ضبط نسخها: من المهم في الجرائم المعلوماتية، أن يرد الضبط على الأقراص والأشرطة الأصلية، مع تمكين الجهة التي تحوزها من نسخها، لاستخدامها كي لا يتوقف أو يعاق استمرارها في مباشرة أنشطتها، خاصة في حالة تأخر المحاكمة، أو ثبت فيما بعد عدم وجود دليل جرمي كافي للإدانة.

الفرع الثاني: إجراء تفتيش وضبط المعلومات المخزنة ضمن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010:

نصت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المبرمة بالقاهرة سنة 2010، على إمكانية تفتيش وضبط بيانات المعلومات المخزنة كالآتي:

أولا- تفتيش المعلومات المخزنة:

نصت المادة 26 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على تفتيش المعلومات المخزنة حيث[1]:

"1-تلتزم كل دولة بتبني الإجراءات الضرورية لتمكين سلطاتها المختصة من التفتيش أو الوصول إلى:

أ)-تقنية معلومات أو جزء منها والمعلومات المخزنة فيها أو المخزنة عليها،

ب)-بيئة أو وسيط تخزين معلومات تقنية معلومات والذي قد تكون معلومات التقنية مخزنة فيه أو عليه".

وعن التفتيش في حالة اتصال حاسبة المتهم بحاسبة أخرى أو نهاية طرفية موجودة في مكان آخر داخل: نصت المادة 2/26 على:

[1]- أنظر في هذه الاتفاقية، مرسوم رئاسي رقم 14-252 مؤرخ في 8 سبتمبر سنة 2014، يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، السابق ذكره، ص 8.

"2- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من التفتيش أو الوصول إلى تقنية معلومات معينة أو جزء منها بما يتوافق مع الفقرة (1-أ) إذا كان هناك اعتقاد بأن المعلومات المطلوبة مخزنة في تقنية معلومات أخرى أو جزء منها في إقليمها وكانت هذه المعلومات قابلة للوصول قانونا أو متوفرة في التقنية الأولى فيجوز توسيع نطاق التفتيش والوصول للتقنية الأخرى".

وعن التفتيش في حالة اتصال حاسبة المتهم بحاسبة أخرى أو نهاية طرفية موجودة في مكان آخر خارج الدولة: أجازت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات من إمكانية تفتيش حاسبة متصلة بأخرى خارج الوطن، هذه الفكرة تم حلها في الفصل الرابع من الاتفاقية الخاص بالتعاون القانوني والقضائي في المادة 39 التي تتناول التعاون والمساعدة الثنائية المتعلقة بالوصول إلى معلومات تقنية المعلومات المخزنة.

ثانيا- ضبط المعلومات المخزنة:

نصت المادة 27 من الاتفاقية على ضبط المعلومات المخزنة حيث[1]:

"1- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من ضبط وتأمين معلومات تقنية المعلومات التي يتم الوصول إليها حسب الفقرة (1) من المادة السادسة والعشرين من هذه الاتفاقية.

هذه الإجراءات تشمل صلاحيات:

أ) ضبط وتأمين تقنية المعلومات أو جزء منها أو وسيط تخزين معلومات تقنية المعلومات،

ب) عمل نسخة من معلومات تقنية المعلومات والاحتفاظ بها،

ج) الحفاظ على سلامة معلومات تقنية المعلومات المخزنة،

د) إزالة أو منع الوصول إلى تلك المعلومات في تقنية المعلومات التي يتم الوصول إليها.

وأضافت الفقرة 2 من المادة 27 من الاتفاقية على ضرورة لجوء السلطات المختصة بكل شخص لديه معرفة بنظام الحاسب الآلي، لمساعدتها على جمع الأدلة المخزنة بالنظام الكمبيوتر عند اتخاذ إجراء التفتيش والضبط حيث:"2- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى أي شخص لديه معرفة بوظيفة تقنية المعلومات أو الإجراءات المطبقة لحماية تقنية المعلومات من أجل تقديم المعلومات

[1]- أنظر في هذه الاتفاقية، مرسوم رئاسي رقم 14-252 مؤرخ في 8 سبتمبر سنة 2014، يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، السابق ذكره، ص 8.

الضرورية لإتمام تلك الإجراءات المذكورة في الفقرتين (1،2) من المادة السادسة والعشرين من هذه الاتفاقية).

خاتمة:

أثبتت الجريمة المعلوماتية، بخاصيتها غير المادية للأدلة التي تخلفها، إلى عدم كفاية الآليات الإجرائية التقليدية لمكافحة جرائم المعلوماتية منها جرائم الاتجار بالأشخاص المرتكبة بواسطة تقنية المعلومات، مما يقتضي على السياسة الجنائية، ومن أجل مكافحة فعالة لهذا النوع من الإجرام، ضرورة "تطوير أساليب التحري والتحقيق"، بصورة تتلائم مع هذه الخاصية، وذلك من خلال إتباع حركتين تكميليتين: أولا، تطوير الإجراءات الجنائية التقليدية لجمع الأدلة وثانيا، خلق إجراءات جنائية حديثة لجمع الأدلة تتأقلم مع العالم الافتراضي.

لذا عملت الدول من خلال الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر سنة 2010، على خلق أحكام موضوعية وإجرائية فعالة ومناسبة لمكافحة هذا النوع الحديث من الإجرام، وتدعيم سبل التعاون الدولي فيما بينها، ويمكن إبداء النتائج التالي:

- خصصت الاتفاقية الفصل الثالث للحديث على الأحكام الإجرائية لمكافحة جرائم تقنية المعلومات، والمتمثلة في إجراء التحفظ العاجل على البيانات المخزنة في تقنية المعلومات (المادة 23)، التحفظ العاجل والكشف الجزئي لمعلومات تتبع المستخدمين (المادة 24)، أمر تسليم المعلومات (المادة 25)، تفتيش المعلومات المخزنة (المادة 26)، ضبط المعلومات المخزنة (المادة 27)، الجمع الفوري لمعلومات تتبع المستخدمين (المادة 28)، اعتراض معلومات المحتوى (المادة 29).

- استنبطت معظم نصوص الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 من اتفاقية بودابيست لمكافحة جرائم المعلوماتية لسنة 2001، حيث تعتبر هذه الأخيرة الاتفاقية النموذجية لمكافحة هذا النوع المستحدث من الإجرام.

- يعتبر المشرع الجزائري المشرع العربي الوحيد الذي نص على أحكام إجرائية خاصة بمكافحة الجريمة المعلوماتية والتي تندرج ضمنها جريمة الاتجار بالأشخاص والمرتكبة بواسطة تقنية المعلومات حتى قبل المصادقة على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 وذلك من خلال إصدار قانون رقم: 06-22، المؤرخ في 20 ديسمبر سنة 2006، يعدل ويتمم الأمر رقم 66-155 المؤرخ في 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، وقانون رقم 09-04، المؤرخ في 5 أوت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. في حين تعتمد التشريعات العربية المصادقة على الاتفاقية العربية لمكافحة جرائم تقنيات المعلومات لسنة 2010 وبالتالي لمكافحة جريمة

الاتجار بالأشخاص والمرتكبة بواسطة تقنية المعلومات على الإجراءات التقليدية كالتفتيش والضبط والمعاينة والاستجواب والخبرة والشهادة وتسجيل المكالمات الهاتفية، ما عدا المشرع الأردني الذي نص من خلال قانون الجرائم المعلوماتية رقم (27) لسنة 2015، على إجراء تفتيش وضبط النظم المعلوماتية المخزنة لكن دون التفصيل في أحكام هذا الإجراء.

وفيما يتعلق بالتوصيات والمقترحات: فإننا نقترح ما يلي

– على الرغم من مصادقة معظم الدول العربية على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 إلا أنها لم تدرج نصوص هذه الاتفاقية بالقوانين الداخلية لهذه الدول على الرغم من إلزام هذه الاتفاقية الدول المنظمة إليها من القيام بذلك وهذا ما نصت عليه الاتفاقية العربية بالفصل الثالث بعنوان الأحكام الإجرائية بالمادة 22 المعنونة ب: (نطاق تطبيق الأحكام الإجرائية) بقولها (1- تلتزم كل دولة بأن تتبنى في قانونها الداخلي التشريعات والإجراءات الواردة في الفصل الثالث من هذه الاتفاقية)، لذا نقترح على الدول العربية المصادقة على هذه الاتفاقية إدراج نصوص هذه الاتفاقية وأحكامها ضمن قوانينها الإجرائية الداخلية تنفيذا لالتزاماتها الدولية من جهة ومن أجل ضمان مكافحة فعالة لهذا النوع من الإجرام الذي يستدعي إجراءات تحري وتحقيق خاصة تختلف عن الإجراءات التقليدية المتبعة في مكافحة الجرائم العادية من جهة ثانية.

– لا يكفي انضمام وتصديق الدول العربية على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 لمكافحة فعالة لهذا النوع من الإجرام، لذا نقترح على الدول العربية منها الجزائر توسيع سبل التعاون الدولي من خلال الانضمام إلى الاتفاقيات العالمية والإقليمية المتنوعة والخاصة بمكافحة هذه الجريمة وخاصة منها اتفاقية بودابيست لمكافحة جرائم المعلوماتية لسنة 2001.

قائمة المصادر والمراجع:

أولا- قائمة المصادر:

[1]– مرسوم رئاسي رقم 03-417، مؤرخ في 9 نوفمبر سنة 2003، يتضمن التصديق بتحفظ على بروتوكول منع وقمع الإتجار بالأشخاص بخاصة النساء والأطفال، المكمل لاتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، المعتمد من طرف الجمعية العامة لمنظمة الأمم المتحدة يوم 15 نوفمبر سنة 2000، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 69، الصادرة في 12 نوفمبر سنة 2003.

2– مرسوم رئاسي رقم 03-418، مؤرخ في 9 نوفمبر سنة 2003، يتضمن التصديق بتحفظ على بروتوكول مكافحة تهريب المهاجرين عن طريق البر والبحر والجو، المكمل لاتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، المعتمد من طرف الجمعية العامة لمنظمة الأمم المتحدة يوم 15 نوفمبر سنة 2000، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 69، الصادرة في 12 نوفمبر سنة 2003

3– مرسوم رئاسي رقم 14-252، المؤرخ في 8 سبتمبر سنة 2014، يتضمن التصديق على الاتفاقية العربية

لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21 ديسمبر سنة 2010، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 57، الصادرة في 28 سبتمبر سنة 2014.

ثانيا- قائمة المراجع

[1]- سوزي عدلي ناشد، الإتجار بالبشر بين الإقتصاد الخفي والإقتصاد الرسمي، دار الجامعة الجديدة للنشر والتوزيع، الإسكندرية، 2005.

[2]- محمد علي العريان، عمليات الإتجار بالبشر وآليات مكافحتها، دار الجامعة الجديدة، الإسكندرية، 2011.

3- عادل عبد الجواد محمد، الاتجار بالبشر، مقال منشور ضمن: مجلة الأمن والحياة، جامعة نايف العربية للعلوم الأمنية، العدد 354، 1432.

4- ندوة علمية مكافحة الهجرة غير المشروعة، مجلة الأمن والحياة، عدد 357، جامعة نايف العربية للعلوم الأمنية، 1433ه.

[5]- نهال فهمي، التجربة العربية في مكافحة الاتجار بالبشر، مقال مقدم في فعاليات المؤتمر: مكافحة الاتجار بالبشر، منشور بمجلة الأمن والحياة، العدد 332، جامعة نايف العربية للعلوم الأمنية، الرياض، 1431.

6- عبد الله بن سعود السراني، العلاقة بين الهجرة غير المشروعة وجريمة تهريب البشر، بحث منشور ضمن فعاليات مؤتمر مكافحة الهجرة غير المشروعة، منشور ضمن: مجلة الأمن والحياة، العدد 357، جامعة نايف العربية للعلوم الأمنية، الرياض.

[7]- طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2009.

8- قارة أمال، الجريمة المعلوماتية، رسالة لنيل درجة الماجستير في القانون الجنائي والعلوم الجنائية، جامعة الجزائر، 2001-2002.

9- يونس خالد عرب مصطفى، جرائم الحاسوب، دراسة مقارنة، رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير في القانون، كلية الدراسات العليا، الجامعة الأردنية، عمان، 1994.

10- هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية، معلقا عليها، دار النهضة العربية، القاهرة، 2007.

11- هلالي عبد اللاه أحمد، كيفية المواجهة التشريعية لجرائم المعلوماتية، في النظام البحريني على ضوء اتفاقية بودابيست، دار النهضة العربية، القاهرة، 2011.

12- عماد محمد ربيع، حقوق المتهم في مرحلة التحقيق الإبتدائي في قانون أصول المحاكمات الجزائية الأردني، مقال منشور ضمن مجلة البلقاء للبحوث والدراسات، مجلة علمية محكمة، تصدرها عمادة الدراسات العليا والبحث العلمي في جامعة عمان الأهلية، المجلد 12، العدد 1، آب 2007.

13- علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، عالم الكتب الحديث، الأردن.

14- محمد طارق عبد الرؤوف الحن، جريمة الاحتيال عبر الإنترنت، منشورات الحلبي الحقوقية، لبنان، 2011.

15- سليمان عبد المنعم، أصول الإجراءات الجزائية في التشريع والقضاء والفقه، المؤسسة الجامعية للدراسات، بيروت، الطبعة الثانية، 1999.

16- علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، دراسة مقارنة، المكتب الجامعي الحديث، دون بلد نشر، 2012.

17- عبد الناصر محمد محمود فرغلي و محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من

الناحيتين القانونية والفنية دراسة تطبيقية مقارنة، بحث مقدم إلى المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، الرياض، 2007.

18- فتوح الشاذلي، عفيفي كامل، جرائم الكمبيوتر وحقوق المِلف والمصنفات الفنية ودور الشرطة والقانون، منشورات الحلبي الحقوقية، لبنان، 2003.

19- محمود نجيب حسني، شرح قانون الإجراءات الجنائية، الطبعة الثالثة، دار النهضة العربية، القاهرة، 1996.

20- حسن الجوخدار، أصول المحاكمات الجزائية، الجزء الثاني، الطبعة الخامسة، منشورات جامعة دمشق، 1991، ص 162.

21- غازي عبد الرحمان هيان الرشيد، الحماية القانونية من الجرائم المعلوماتية (الحاسب والانترنت)، أطروحة دكتوراه في القانون، كلية الحقوق، الجامعة الإسلامية في لبنان، بيروت، 2004.

22- يونس عرب، جرائم الكمبيوتر والإنترنت، موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، الجزء الأول، منشورات اتحاد المصارف العربية، دون بلد نشر، 2002.