الحماية الإجرائية للمستهلك من جريمة الاستخدام غير المشروع لأدوات الدفع الإلكترونية
وفقا للاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010

الدكتورة : شرف الدين وردة
أستاذ محاضر قسم "ب"
جامعة محمد خيضر بسكرة

الدكتورة : احميدة هنية،
أستاذ محاضر قسم "أ"
جامعة محمد خيضر بسكرة.

الملخص:

أدى التطور التكنولوجي إلى ما يشار إليه عادة باسم التجارة الإلكترونية، وهي عملية ساعدت المستهلكين على الوصول إلى السلع والخدمات في أي مكان في العالم تقريبًا من خلال أدوات الدفع الإلكترونية، هذه السهولة لا تخلو من المخاطر بالنسبة للمستهلكين، وبالفعل، فإن استخدامهم لأدوات الدفع الإلكترونية وما يمكن أن يحتويه ذلك من بيانات شخصية خلال القيام بمختلف المعاملات مهددة بالإمكانيات المتاحة لاستغلال هذه البيانات بطريقة غير مشروعة.

ولقد عملت الاتفاقيات الخاصة بمكافحة جرائم تقنية المعلومات كالاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر سنة 2010 واتفاقية بودابيست بتاريخ 30 نوفمبر 2001 لمكافحة جرائم المعلوماتية، على تجريم الاستخدام غير المشروع لأدوات الدفع الإلكترونية، وعلى تقرير أحكام إجرائية خاصة وفعالة للتحري والتحقيق في هذا النوع من الإجرام تتناسب مع طبيعتها التي تميزها عن الجرائم التقليدية.

الكلمات المفتاحية: المستهلك، أدوات الدفع الإلكترونية، الاستخدام غير المشرع لأدوات الدفع الإلكترونية.

Résumé :

Le développement technologique a conduit à ce que l'on a appelé communément le commerce électronique. Un procédé qui a facilité aux consommateurs l'accès aux biens et services presque partout dans le monde grâce à des outils de paiement électronique. Cette facilité n'est cependant pas sans risque pour les consommateurs. En effet, l'utilisation par eux d'outils de paiement électroniques et de ce que ceux-ci peuvent contenir comme données personnelles lors des différentes transactions est menacée par les possibilités offertes que ces données soient exploitées de manière illicite.

Pour lutter contre les infractions touchant les technologies de l'information, la Convention arabe pour la lute contre la cybercriminalité du 21 décembre 2010 et la Convention de Budapest sur la Cybercriminalité du 23 novembre 2001 ont érigé en infraction toute utilisation illégale des outils de paiement électronique. Elles ont en outre prescrit des dispositions de procédures spéciales et efficaces d'investigation et d'instruction idoines à ce type de criminalité qui se distingue des crimes traditionnels.

Mots clé : consommateurs, outils de paiement électronique, Utilisation illégale d'outils de paiement électroniques.

مقدمة:

إن ظهور الحاسوب والإنترنت وما صاحبه من تقدم ورقي الشعوب إلا أنه من جهة أخرى ساعد في تطور الفكر الإجرامي لارتكاب الجرائم التقليدية وفي بروز جرائم جديدة وذلك عن طريق استخدام المجرمين لتكنولوجيات المعلومات لاقترف جريمة التزوير أو الإرهاب أو السرقة أو السب والقذف أو الجرائم الإباحية وجرائم الترويج بالمخدرات والاتجار بها، جريمة الإتجار بالأشخاص، جريمة الإتجار بالأعضاء، جريمة الاستخدام غير المشروع لأدوات الدفع الإلكتروني... مما أعطى لهذه الجرائم خصوصية وميزات جديدة، الأمر الذي استدعى بالسياسة الجنائية للدول إلى ضرورة مواكبة النصوص التشريعية بها لهذا التطور السريع في الإجرام بالتطوير من أساليب التحري والتحقيق في هذا النوع الجديد من الإجرام والمتصل بالجرائم المعلوماتية.

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 بتاريخ 21 ديسمبر سنة 2010 وهذا ما أكدته المادة الأولى من الإتفاقية 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، وقد تحدثت في المادة 18 منها على جريمة الاستخدام غير المشروع لأدوات الدفع الإلكترونية، كنوع من جرائم تقنية المعلومات. بينما تكلمت في الفصل الثالث على الأحكام الإجرائية المتبعة في مكافحة هذا النوع من الإجرام.

إشكالية المداخلة: ما مدى كفاية الأحكام الإجرائية التقليدية للتحري والتحقيق في مكافحة جريمة الاستخدام غير المشروع لأدوات الدفع الإلكترونية ؟ وما موقف الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر سنة 2010,

المبحث الأول:إطار مفاهيمي لحماية المستهلك الإلكتروني وجريمة الاستخدام غير المشروع لأدوات الدفع الإلكترونية

سنتطرق من خلال هذا المبحث إلى تعريف المستهلك، مفهوم جريمة الاستخدام غير المشروع لأدوات الدفع الإلكترونية، مفهوم أدوات الدفع الإلكترونية وأخيرا مبررات حماية المستهلك من الاستخدام غير المشروع لأدوات الدفع الإلكترونية وذلك من خلال ما يلي:

أولا– التعريف بالمستهلك:

يمكن تعريف المستهلك بأنه كل شخص يقوم بتصرف قانوني، بغية استعمال السلع أو الخدمات لاستخدامه الشخصي أو المزود، أي أن المزود يمكن أن يكون شخصا طبيعيا، أو شركة أو منتجا، وبذلك يشمل المعاملات التجارية بين المنتجين أنفسهم.[1]

ويمكن تعريف المستهلك الإلكتروني بأنه ذلك الشخص الذي يقوم بإبرام العقود الإلكترونية المتنوعة من شراء وإيجار وقرض وانتفاع وغيرها لكي يوفر كل ما يحتاجه من سلع وخدمات لإشباع حاجاته الشخصية أو العائلية ودون أن يقصد من ذلك إعادة تسويقها ودون أن تتوافر له الخبرة الفنية لمعالجة هذه الأشياء وإصلاحها.[2]

ثانيا– مفهوم جريمة الاستخدام غير المشروع لأدوات الدفع الإلكترونية:

ويعد الحق في الخصوصية واحدا من بين حقوق الإنسان المعترف بها منذ القدم، وقد أثرت تقنية المعلومات على هذا الحق على نحو أظهر إمكان المساس به إذا لم تنظم أنشطة جمع ومعالجة وتبادل البيانات الشخصية الجارية في نطاق نظم معالجة البيانات وبنوك المعلومات، وأظهر الواقع العملي ضرورة التدخل التشريعي لتنظيم أنشطة معالجة البيانات المتصلة بالشخص وتنظيم عمليات تخزينها في بنوك وقواعد المعلومات وعمليات تبادلها، وهذا التنظيم التشريعي ليس مجرد إقرار قواعد ذات محتوى تنظيمي وإنما إقرار قواعد تتصل بالمسؤولية المدنية والجزائية على أنشطة مخالفة قواعد التعامل مع البيانات الشخصية سواء ما يرتكب من قبل القائمين على هذه الأنشطة أم من قبل الغير[3].

أما فيما يخص احترام خصوصية المستهلك فقد تتضمن المعاملات الإلكترونية بيانات شخصية يتم إرسالها من المستهلك إلى التاجر في إطار التأكيد على عملية البيع، وقد تكون هذه المعلومات عبارة عن بيانات اسمية، أو عدة صور في شكل إلكتروني، أو مقر إقامته، وطبيعة العمل الذي يقوم به، وغير ذلك من البيانات التي لا يرغب في الكشف عنها للغير، لولا ضرورات المعاملة الإلكترونية لما قام المستهلك بالكشف عنها، فقد يسيء التاجر الإلكتروني استخدام هذه البيانات ويتعامل معها في غير الحدود المخصصة له، كأن يقوم بإرسالها إلى متعاملين آخرين دون الحصول على اذن مسبق من صاحبها، أو يعرضها للعامة[4].

كما أن البنوك قبل منح أية تسهيلات لعملائها، تجري تحريات وثيقة ومفصلة عن مسلك الشخص ومركزه المالي ومن هنا يتحتم حماية البيانات الشخصية للمستهلك في التجارة الإلكترونية، إذ على البنوك احترام سرية البيانات المتعلقة بعملائها باعتبارهم مستهلكين، واحترام حقهم في الخصوصية[5].

ولقد جرمت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 في المادة 18 جريمة الاستخدام غير المشروع للأدوات الدفع الإلكترونية حيث تعد من قبيل هذه الجريمة الأفعال التالية [6]:

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

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

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

4- كل من قبل أداة من أدوات الدفع المزورة مع العلم بذلك).

ثالثا- مفهوم أدوات الدفع الإلكترونية:

سنتناول في هذه المسألة تعريف أدوات الدفع الإلكتروني ثم بيان أنواعها المختلفة وذلك كالتالي:

1- التعريف بالدفع الإلكتروني:

يقصد بالوفاء الإلكتروني بالمعنى الواسع إلى كل عملية دفع لمبلغ من النقود التي تتم بأسلوب غير مادي لا يعتمد على دعامات ورقية بل بالرجوع إلى آليات إلكترونية، ويقصد بالوفاء الإلكتروني بالمعنى الضيق: عمليات الوفاء التي تتم دون وجود اتصال مباشر بين الأشخاص الطبيعيين(7).

2- أنواع أدوات الدفع الإلكترونية:

يمكن تصنيف أدوات الدفع الإلكتروني إلى ثلاث أصناف، وهي وسيلة الدفع المقدم كبطاقة الإئتمان، الدفع الفوري عند الاستلام، وأخيرا الدفع سلفا كالبطاقة الذكية.

أ- عملية الدفع المقدم: وتتمثل في:

أ/1- بطاقة الائتمان:

تستند هذه الوسيلة على أن إحدى المؤسسات المالية أو شركات الاستثمار تصدر بطاقات مصنعة ذات تصميم عالي التقنية، ويصعب العبث بها، حيث يسمح لحاملها تقديمها للبائع عند شراء بعض

السلع ليقوم البائع بتدوين بيانات البطاقة على فاتورة يصدرها ويوقعها حامل هذه البطاقة لترسل إلى البنك كمعتمد لتلك البطاقة ليتم الوفاء بالمشتريات. (8)

كما يمكن لمالك الموقع العنكبوتي، القيام بربط مباشر مع المصرف، مع التأكد مباشرة فيما إذا كان المستخدم يملك ائتمان كافي للدفع، كما قد يقوم العميل بإعطاء التاجر رقما سريا يسمح له بسحب الأموال النقدية أو تحويلها، وتتم الصفقة بهذه الطريقة مخلفة وراءها خيارات أوسع للمخاطر(9).

أ/2- الفواتير:

تعتبر الفواتير الطريقة الشائعة ما بين الشركات باعتبار أن حجم المبالغ المالية يكون كبيرا جدا ما بين الشركات بالنسبة للبطاقة. ولضمان أمان الفواتير تم استخدام نوع تعريف للمستخدم (10)

أ/3- صكوك الانترنت:

ومثال عن هذا النوع الصك الشبكيNet cheque ، فقد تم تطوير هذه الطريقة سنة 1995، إذ على البائع والمشترك أن يمتلكا لدى الصك الشبكي حساب، ولضمان الأمان تم استخدام كلمة سر وتعريف للمستخدم، ويتعين تنصيب برمجيات زبون خاصة تعمل مثل دفتر صكوك، إذ يمكن للزبون إرسال صك مشفر مع البرمجيات إلى التاجر، ومن ثم يستطيع التاجر الحصول على المال من المصرف، أو يمكن استخدام الصك كمعاملة، أو إجراء مع المجهز، فتقوم شبكة محاسبية خاصة بالتحقق من الصكوك وبإعطاء الموافقة للتاجر الذي يقوم بتسديد البضائع(11).

ب- الدفع الفوري (نقدا) عند الاستلام:

تسمح هذه الطريقة للزبائن من طلب بضائع أو خدمات على الشبكة، ويكون الدفع عند وصول البضائع أو الخدمات عند مقر سكناهم، وهناك نوعان من هذا الدفع.

ب/1- بطاقة المدين:

إن الفرق بين بطاقة الإئتمان وبطاقة المدين يكمن في أن بطاقة المدين يحتاج معرفة الرقم التعريفي للشخص، وجهاز يقرأ البيانات المخزونة في الخطوط المغناطيسية الموجودة بالجهة الخلفية للبطاقة، وذلك على غرار بطاقة الإئتمان أين يتم طبع كل البيانات على الجهة الأمامية للبطاقة، وبالتالي لا توجد هذه البطاقة على الإنترنت، حيث لا توجد حاسبة مرتبطة بطرف جهاز قادر على قراءة الخطوط المغناطيسية[12].

ب/2- الدين المباشر:

يستخدم هذا النوع في المعاملات عبر الشبكة، فيقوم أساسا عن السؤال عن رقم الحساب المصرفي للزبون، ورمز المصرف، بعدئذ يتم إدائة المال مباشرة من حساب المصرف، ولعل من البرمجيات المطلوبة لانجاز هذه التقنية، يحتاج الأمر إلى تصميم موقع عنكبوتي خاص يكفي لجمع كل المعلومات الخاصة من الزبون، ليتم طباعتها بعد ذلك وإرسالها بالفاكس إلى التاجر، أيضا يحتاج الأمر إلى برمجيات خاصة على خادم التاجر لتمرير المعاملة للمصرف حيث يتم تحويل المال[13].

ج-الدفع سلفا: من أهمها النقود الإلكترونية والبطاقات الذكية.

ج/1- النقود الإلكترونية:

وتسمى كذلك بالنقود الرقمية، وتتمثل في نقود غير ملموسة تأخذ صورة وحدات إلكترونية تخزن في مكان آمن على الوسائط الخزينة الثانوية (القرص الصلب)، لجهاز الحاسوب الخاص بالعميل يعرف باسم المحفظة الإلكترونية، إذ يمكن للعميل استخدام هذه المحفظة للقيام بعمليات البيع أو الشراء أو التحويل، بدون أية تكلفة مالية، وعليه يتم استبدال العملات والأوراق النقدية بملفات موقعة رقميا.[14]

ج/2- البطاقات الذكية:

هي عبارة عن بطاقة بلاستيكية تحتوي على شريحة تحفظ المعلومات الرقمية والأبجدية فيها تتوافق مع أجهزة حاسوبية، ويمكن قراءة البيانات داخل الشريحة وتحويلها إلى معلومات مقروءة تعتمد على طبيعة البرنامج والشيفرة الإلكترونية المحفوظة بها، تختلف أحجام التخزين بالبطاقة الذكية فتتنوع من 1 كيلوبايت إلى 1 ميجابايت، ومن ثم يمكن أن تستخدم كبطاقات الصراف الآلي وبطاقات الائتمان إلا أنها تحتوي على معالج صغير وذاكرة. كما تحتوي أيضا البطاقة الذكية على معلومات مهمة كالسجلات الطبية أو معلومات الحسابات المصرفية للمستخدم، ويتطلب استخدامها أن يتم إدخال رقم سري(15).

رابعا- مبررات حماية المستهلك من جريمة الاستخدام غير مشروع لأدوات الدفع الإلكترونية:

ويقصد **بحماية المستهلك**: الإجراءات اللازمة لحماية كل شخص يهدف للحصول على سلعة أو خدمة بغية إشباع حاجاته الشخصية أو العائلية.(16)

بعد توسع دائرة مستخدمي الإنترنت في العالم، تبلور مفهوم ضرورة الحماية الإلكترونية للمستهلك نظرا لوجود عدة مبررات:

1- أن التطور التقني الذي يشهده العالم من خلال شبكة الانترنت أدى إلى واقعا علميا يأتي كل لحظة بالجديد، مما ينبغي أن يقود إلى تحسين الروابط التجارية بين المزود والمستهلك بهدف الحصول على أفضل أداء للممارسات التجارية الإلكترونية.

2- إن حاجة المستهلك إلى السلع والخدمات الضرورية التي تقدم عبر شبكة الإنترنت (كالخدمة السياحية، والمصرفية والتأمين، وبيع تذاكر الطيران والحجز في الفنادق، وبرامج الحاسب الآلي وغيرها)، تدفعه إلى الإقبال على إبرام التصرفات من خلال شبكة الإنترنت، وغالبا ما يفتقد المستهلك إلى الخبرة والدراية والمعرفة في مجال تقنية تكنولوجيا المعلومات –لا سيما في مجال الشبكة العنكبوتية- الأمر الذي يدفعه إلى الدخول في علاقات من خلال مواقع إلكترونية وهمية وبالتالي تعرضه للاحتيال والخداع.

المبحث الثاني:الإجراءات المتبعة في مكافحة جريمة الاستخدام غير المشروع لأدوات الدفع الإلكترونية

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 للجريمة المعلوماتية، وتتمثل هذه الإجراءات في: التحفظ العاجل على البيانات المخزنة في تقنية المعلومات، أمر تسليم المعلومات، تفتيش وضبط المعلومات المخزنة، الجمع الفوري للمعلومات، وسنستعرض كل إجراء من هذه الإجراءات من خلال ما يلي:

أولا– 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:

1– مفهوم الإجراء:

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

أ– مفهوم التحفظ العاجل على البيانات المخزنة في تقنية المعلومات[17]:

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:

1- 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.

2- 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 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.

3- 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.

ب- مفهوم التحفظ العاجل والكشف الجزئي لمعلومات تتبع المستخدمين[18]:

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.

ولذلك 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 بأن يتحفظ 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.

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

2- 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:

أ- التحفظ العاجل على البيانات المخزنة في تقنية المعلومات:

نصت المادة 23 من الاتفاقية على أنه[19]:

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 الأولى بواسطة إصدار أمر إلى شخص من أجل حفظ معلومات تقنية المخزنة والموجودة بحيازته، أو سيطرته ومن أجل إلزامه بحفظ وصيانة سلامة تلك المعلومات لمدة أقصاها 90 يوما قابلة للتجديد، من أجل 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.

ب- التحفظ العاجل والكشف الجزئي لمعلومات تتبع المستخدمين

نصت عليه المادة 24 من الاتفاقية، بحيث[20]:

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.

ثانيا- 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:

1- مفهوم الإجراء[21]:

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.

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.

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

نصت المادة 25 من الاتفاقية على[22]:

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).

ثالثا- 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:

1- مفهوم إجراء التفتيش والضبط:

أ- 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 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)[23].

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)[24].

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 المساكنLa 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[25].

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 التفتيش الواقع لا يعتبر من إجراءات التحقيق، وإنما ينظر إليه بوصفه من قبيل إجراءات الاستدلال[26].

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[27].

ويمكن تعريف تفتيش نظم الحاسوب والأنترنت 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)[28]. وقد عرف المجلس الأوروبي هذا النوع من التفتيش بأنه إجراء يسمح بجمع الأدلة المخزنة أو المسجلة بشكل إلكتروني[29].

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[30].

ونحن بدورنا نرى أن تفتيش الحاسوب الآلي هي تلك الإجراءات المتبعة للبحث عن الأدلة المادية والرقمية الناجمة عن ارتكاب جريمة معلوماتية، بهدف الكشف عن الحقيقة، ويشمل التفتيش كل مكونات الحاسوب المادية والمعنوية وشبكات الاتصال الخاصة به وكذا الأشخاص المستخدمون للحاسب الآلي.

ب– 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[31]، 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[32]، 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[33]، وقد يتم الضبط من غير تفتيش، فقد يقدم المتهم أو الشاهد باختياره الأشياء المتعلقة بالجريمة[34].

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[35].

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[36].

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 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[37] .

وعن قواعد التحريز والتأمين للمضبوطات المعلوماتية[38]: 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 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 الممغنطة 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.

2– 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:

أ- تفتيش المعلومات المخزنة:

نصت المادة 26 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على تفتيش المعلومات المخزنة حيث[39]:

(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:

(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.

ب- ضبط المعلومات المخزنة:

نصت المادة 27 من الاتفاقية على ضبط المعلومات المخزنة حيث[40]:

(1-تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من ضبط وتأمين معلومات تقنية المعلومات التي يتم الوصول إليها حسب الفقرة الأولى 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 الثانية 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 الضرورية لإتمام تلك الإجراءات المذكورة في الفقرتين (1،2) من المادة السادسة والعشرين من هذه الاتفاقية).

رابعا- 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- مفهوم الإجراء[41]:

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.

2- 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:

أ- الجمع الفوري لمعلومات تتبع المستخدمين (المادة 28):

1- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من[42]:

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.

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.

ب– اعتراض معلومات المحتوى (المادة 29):

1–تلتزم كل دولة طرف بتبني الإجراءات التشريعية والضرورية فيما يخص بسلسلة من الجرائم المنصوص عليها في القانون الداخلي، لتمكين السلطات المختصة من[43]:

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.

خاتمة:

أثبتت الجريمة المعلوماتية، بخاصيتها غير المادية للأدلة التي تخلفها، إلى عدم كفاية الآليات الإجرائية التقليدية لمكافحة جرائم المعلوماتية منها جريمة الاستخدام غير المشروع لأدوات الدفع الإلكترونية، 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 بتاريخ 30 نوفمبر سنة 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 الاستخدام غير المشروع لأدوات الدفع الإلكترونية، 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 الاستخدام غير المشروع لأدوات الدفع الإلكترونية 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.

الهوامش:

[1]– الصرايرة منصور، **الإطار القانوني للعقد المبرم عبر وسائل الاتصال الإلكترونية**، دراسة في التشريع الأردني، مجلة جامعة دمشق للعلوم القانونية والإقتصادية، المجلد 25، العدد 2، 2009، ص 838.

[2]– أحمد السيد طه الكردي، **إطار مقترح لحماية حقوق المستهلك من مخاطر التجارة الإلكترونية**، جامعة بنها– كلية التجارة، 2011، ص 13

[3]– يونس عرب، **تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية**، ورشة عمل مقدمة من قبل هيئة تنظيم الإتصالات مسقط–سلطنة عمان 2، من 2–4 نيسان/ ابريل 2006، ص 15.

[4]– سليمة لدغش، **حماية المستهلك عبر شبكة الانترنت بين الواقع والضرورة**، مقال منشور ضمن مجلة الحقوق والحريات، تصدر عن مخبر الحقوق والحريات في الأنظمة المقارنة، جامعة محمد خيضر بسكرة، ص 368.

[5]– عبد الفتاح بيومي حجازي، **مقدمة في حقوق الملكية الفكرية وحماية المستهلك في عقود التجارة الإليكترونية**، دار الفكر الجامعي، مصر، الطبعة الأولى، 2005، ص 20.

[6]– 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، ص 6.

[7]– عدنان إبراهيم سرحان، **الوفاء (الدفع) الإلكتروني**، بحوث مؤتمر الأعمال المصرفية بين الشريعة والقانون المنعقد في 10–12 ماي 2003 بكلية الشريعة والقانون وغرفة التجارة وصناعة دبي، المجلد الأول، ص 286 وما بعدها.

[8]– محمد الكيلاني، **التشريعات التجارية والمعاملات الإلكترونية**، الطبعة الأولى، دار وائل، عمان–الأردن، 2004، ص 505.

[9]– نظال اسماعيل برهم، **أحكام عقود التجارة الإلكترونية**، دار الثقافة للنشر والتوزيع، عمان–الأردن، الطبعة الأولى، 2005، ص 92.

[10]– مصطفى بوادي، **الدفع الإلكتروني كآلية لحماية المستهلك ومظاهر تطبيقه في التشريع الجزائري**، مقال منشور بمجلة الإجتهاد القضائي، العدد الرابع عشر، مخبر الإجتهاد القضائي على حركة التشريع، جامعة محمد خيضر، بسكرة، أفريل 2017، ص 50.

[11]– المرجع نفسه، ص 50.

[12]– المرجع نفسه، ص 51.

[13]– المرجع نفسه، ص 51.

[14]– حسن على القفعي، **الإلكترونية وتاثيرها على دور البنوك المركزية في إدارة السياسة النقدية**، مؤتمر القانون بجامعة اليرموك، اربد، المملكة الردنية الهاشمية، في الفترة 12–14 تموز 2004ن ص 2 وما بعدها.

[15]– منير الجهنمي، **البنوك الإلكترونية**، دار الفكر الجامعي الإسكندرية، 2005، ص 52.

[16]– حسن عبد الباسط الجميعي، **حماية المستهلك**، الحماية الخاصة لرضا المستهلك في عقود الاستهلاك، القاهرة، دار النهضة العربية، 1996، ص 30.

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

[18]– 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.

[19]– 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، ص7.

[20]– 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.

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

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

[23]– 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.

[24]– 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**، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2011، ص 274.

[25]– علي حسن محمد الطوالبة، المرجع السابق، ص 12.

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

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

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

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

[30]– 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.

[31]– فتوح الشاذلي، عفيفي كامل، **جرائم الكمبيوتر وحقوق المِلف والمصنفات الفنية ودور الشرطة والقانون**، منشورات الحلبي الحقوقية، لبنان، 2003، 135.

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

[33]– فتوح الشاذلي، عفيفي كامل، المرجع السابق، ص 135.

[34]– محمد طارق عبد الرؤوف الحن، المرجع السابق، ص 290.

[35]– حسن الجوخدار، **أصول المحاكمات الجزائية**، الجزء الثاني، الطبعة الخامسة، منشورات جامعة دمشق، 1991، ص 162.

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

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

[38]– 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.

[39]– 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، المصدر السابق، ص 8.

[40]– 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، المصدر السابق، ص 8.

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

[42]– 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، المصدر السابق، ص 8-9.

[43]– 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، المصدر السابق، ص 9.