تــنازع الاخــتصاص في الجرائم الالكــترونية

الدكــتور: لموســـــخ محـــــمد

أســـــتاذ مـــــــــحاضـــر ب

قســـم الحـــقوق

جامعـــة قاصدي مرباح ورقلة

الملخـــــص:

نظرا لطبيعة الجريمة الالكترونية فقد أفرزت تحديات واضحة للقوانين الوضعية التي وضعت لمكافحة، ذلك أنها غيرت من صورتها التقليدية المتمثلة في صورتها المادية إلى أخرى معنوية وما ينتج عن ذلك من مشكلة في تفسير النصوص القانونية وحضر القياس في المواد الجنائية واصطدامها بمبدأ الشرعية الجنائية وهذه القيود من شأنها أن تساهم في إفلات الكثير من المجرمين من العقاب من جهة، ومن جهة أخرى تطرح إشكاليات عند تطبيق النصوص خصوصا في مسائل الاختصاص .

Because of the nature of electroic crime in which it gives many clear challenges to the old laws which they put to struggle against crimes . these laws which changes their pictures from traditional (material) to its sense picture and this leads to a big problem in the explanation of laws texts . the measure is forbidden in the crimes articles.

The later is faced by the principal of crimes legality. These restrictions may halp many criminals to escape of peuamy .thes form one side tom the otger side.it proposes many problems in the application of artecles especially in the case of speciality.

الكلمات المفتاحية:

– الجريمة الالكترونية – مبدأ الشرعية– الجريمة العابرة للحدود – الجريمة الدولية– الجريمة العالمية– قواعد الاختصاص – مبدأ الإقليمية– مبدأ الشخصية– مبدأ العينية– التعاون القضائي الدولي– المساعدة القضائية الدولية في المواد الجنائية.

مقدمة:

مع زيادة انتشار شبكة الانترنت وتوسع استخدامها في مجال المعاملات التجارية ودخول جميع فئات المجتمع إلى قائمة المستخدمين بدأت تظهر جرائم ذات طبيعة خاصة على هذه الشبكة وازداد عددها وتعددت صورها وأشكالها وتسمى هذه الجرائم بالجرائم الالكترونية أو الجرائم المعلوماتية.

ولعل التطور المستمر للانترنت وما تتميز به من سرعة في إعداد ونقل وتحزين المعلومات وما تتوفر عليه من السرية التامة جعلها بيئة ملائمة للإجرام بعيد عن أعين الجهات الأمنية، وما زاد الأمر سهولة وجود فراغ تشريعي على المستوى الداخلي والدولي .

وعلى هذا الأساس أفرزت الجريمة الالكترونية تحديات واضحة للقوانين الوضعية التي وضعت لمكافحة، ذلك أنها غيرت من صورتها التقليدية المتمثلة في صورتها المادية إلى أخرى معنوية وما ينتج عن ذلك من مشكلة في تفسير النصوص القانونية وحضر القياس في المواد الجنائية واصطدامها بمبدأ الشرعية الجنائية وهذه القيود من شأنها أن تساهم في إفلات الكثير من المجرمين من العقاب .

وما زاد الأمر تعقيدا أن هذه الجرائم المستحدثة سريعة الحدوث وفي عديد من الدول (الجريمة العابرة للحدود)، وما تطرحه هذه الجرائم من مشاكل قانونية خصوصا في مجال الاختصاص من حيث الجهات المخول لها متابعة المجرم، أو من خلال المحكمة المختصة فقد ترتكب الجريمة في دولة و تكون آثارها في دولة أخرى، وقد يكون الجاني يحمل جنسية دولة أخرى وتكون أدلة الجريمة موجودة في دولة أخرى وخارج النطاق الإقليمي لجهة التحقيق، فكيف يتم جمع الأدلة وضبطها وما هو القانون الواجب التطبيق، و هذا ما يحتم علينا ضرورة البحث عن الاختصاص في جرائم المعلوماتية العابرة للحدود على المستوى الداخلي، وكذا على المستوى الدولي من خلال التعاون الاتفاقي والقضائي للحد من هذه الظاهرة الإجرامية الخطيرة .

وعلى هذا الأساس سنحاول في هذه الورقة أن نبين أحكام الاختصاص في جرائم المعلوماتية وهذا وفق للعناصر التالية:

أولا: خصائص الجريمة المعلوماتية

تتميز الجريمة المعلوماتية بجملة من الخصائص التي تميزها عن الجريمة التقليدية ومن أهمها:

1- الجريمة المعلوماتية عابرة للحدود:

ذلك انه غالبا ما يكون لهذه الجرائم طابع عالمي، لأن كل الدول مرتبطة وفي حالة اتصال دائم (ON LINE)، وعليه فالجريمة المعلوماتية لا تعرف حدود وبذلك أصبح مسرح الجريمة المعلوماتية عالميا[1].

وهذا ما يطرح العديد من الإشكاليات القانونية خصوصا أثناء عدم تواجد الجاني في مسرح الجريمة وكذا التباعد الزماني والمكاني بين السلوك الإجرامي والمتمثل في جهاز الكمبيوتر والنتيجة الإجرامية التي تمثل قاعدة البيانات والمعطيات محل الاعتداء بالنسبة اليها، وهذا الأمر يثير إشكالية التعارض مع السيادة الوطنية مما يزيد

من تعقيد الموضوع، وذلك من خلال صعوبة اللجؤ إلى عمل دولي مشترك للحد من هذه الجرائم، مما يستوجب الاعتماد على التشريعات الوطنية لكل دولة .

والحقيقة أن هذه الجرائم صورة صادقة من صور العولمة وذلك باعتبار العالم قرية مصغرة، حيث يمكن ارتكاب الجرائم عن بعد، وقد يتعدد المكان إلى أكثر من دولة بل أكثر من قارة وهذا من شأنه أن يطرح إشكالية القانون الواجب التطبيق .

2- صعوبة إثبات الجريمة المعلوماتية:

ما يميز هذه الجريمة أنها تتصف بالخفاء وعدم وجود أثار مادية يمكن متابعتها مما يجعلها صعبة الاكتشاف، وعليه فمن الصعب تحديد مكان وقوعها وترجع أسباب ذلك إلى :

* إنها جريمة لا تترك أثار مادية بعد ارتكابها، وغالبا ما يتم اكتشافها بالمصادفة وبعد وقت طويل من حدوثها.

* صعوبة الاحتفاظ بالدليل الفني على ارتكاب الجريمة[2]، وذلك لان الجاني يستطيع في ظرف وجيز جدا أن يمحوا أو يحرف أو يغير أو يتلف البيانات والمعلومات وجميع المعطيات الموجودة في قاعدة البيانات وعلى هذا الأساس كان للمصادفة دور كبير في اكتشافها.

* تحتاج هذه الجرائم إلى خبرة فنية وتقنية عالية، وذلك من خلال معرفة تقنيات الكمبيوتر ونظم المعلومات سواءا في مجال جمع الأدلة والتحقيق أو المتابعة القضائية .

لذلك فإن رجال الضبطية القضائية غير قادرين على التعامل مع هذه الفئة من الجرائم بالطرق التقليدية، بالإضافة إلى صعوبة تتبع مسار العمليات الكترونيا خصوصا إذا كانت عابرة للقارات.

* إن هذه الجرائم تعتمد على الخداع في ارتكابها والتضليل مما يساعد على عدم التعرف على الفاعل الحقيقي، والشيء الملاحظ هو أن المؤسسات والبنوك خصوصا تحجم عن الإبلاغ وهذا تجنبا للإساءة إلى السمعة والخوف من هز الثقة العملاء فيها، بالإضافة إلى إخفاء أسلوب ارتكاب الجريمة خوفا من تكرارها مما يزيد في فرص إفلات الجاني من العقاب[3].

* تعتمد جل جرائم المعلوماتية على الذكاء ولهذا تسمى (جرائم الذكاء) وهي ليست جريمة منظمة فغالبا ما ترتكب بصفة فردية، واهم دوافعها الطمع والجشع والانتقام وأحيانا بدافع إثبات الذات.

وعلى هذا الأساس نقول أن الإجرام المعلوماتي هو إجرام الأذكياء الذي يعتمد على مهارات فنية وتقنية وإلمام بنظم المعلوماتية بالمقارنة مع الإجرام التقليدي الذي يعتمد على العنف[4] .

3- عدم وجود مفهوم محدد ومشترك للجريمة المعلوماتية:

يرجع ذلك بالأساس إلى اختلاف النظم القانونية في دول العالم، و يظهر هذا جليا من خلال اختلاف الفكر القانوني حول حماية المعلومات، فهناك من يرى بأن المعلومات ذات طبيعة خاصة ولا يطبق عليها الشرط

المادي الضروري لتعريف الجريمة، و يرى البعض الآخر أن المعلومات تأخذ قيمة مالية ومادية بصفتها حقا خاصا ينسب لشخص محدد .

وما زاد الأمر تعقيدا هو مبدأ الشرعية الجنائية باعتباره أمرا نسبيا من دولة إلى أخرى، وأحيانا في نفس الدولة الواحدة ومثال ذلك ألعاب القمار عبر الانترنت مسموح بها في ولاية لاس فيجاس ومحرمة في ولاية نيويورك .

ولهذا يجب أن تتحرك الدول على محورين من أجل مكافحة الجريمة المعلوماتية :

- **أولا** :على المستوى الداخلي وهذا من خلال وضع قوانين تتماشى وطبيعة هذه الجرائم المستحدثة و إقامة هيئات وطنية مستقلة تشرف على المراقبة والعمل على الوقاية من هذه الجرائم

-**ثانيا:** على المستوى الدولي وهذا من حلال وضع اتفاقيات دولية وإقليمية وتفعيل دور المنظمات غير الحكومية من أجل مكافحة هذه الجرائم المستحدثة،والعمل على سد الفراغات التشريعية حتى لا يستفيد المجرمون من عجز التشريعات الداخلية وغياب النصوص الدولية[5].

4- وقوع الجريمة أثناء المعالجة الآلية للبيانات:

تعتبر هذه الخاصية ضرورية يجب توافرها لقيام الجريمة المعلوماتية وفي أي مرحلة من المراحل سواء أكانت في مرحلة إدخال البيانات أو أثناء معالجتها أو أثناء خروج المعلومات والمعطيات أو حتى بعد تخزينها وهذه الصور أخذ بها المشرع الفرنسي في قانون العقوبات المعدل لسنة 1994 ولا مانع في الاسترشاد بها عند وضع قانون خاص بالجريمة المعلوماتية[6].

5- الجريمة المعلوماتية جريمة مستحدثة :

إن التقدم العلمي والتكنولوجي في ظل العولمة تجاوز قدرات الدولة الرقابية وإمكانياتها بل وأضعف قدرتها على تطبيق قوانينها بالشكل الذي أصبح يهدد أمنها وسلامتها[7].

وعلى هذا الأساس سارعت الدول إلى وضع تشريعات خاصة تعمل على الوقاية ومكافحة هذه الجريمة المستحدثة و سعت إلى عقد اتفاقيات دولية في هذا المجال .

غير أنه بالنظر لطبيعة وخصائص هذه الجرائم نجدها تثير العديد من الإشكاليات القانونية خصوصا في مجال الاختصاص القضائي والقانون الواجب التطبيق، لذلك سنحاول في هذه الورقة إيجاد رؤية توافقية تعمل على الحد من هذه الجرائم من خلال ملاحقة ومتابعة الجنات وعدم تهربهم من العقاب من جهة، ومن وجهة أخرى حماية الحقوق الشخصية للأفراد و ضمان حرياتهم الأساسية من سرية المعلومات و حرية الاتصال ..... الخ

ثانيا- مبدأ الشرعية الجنائية في جرائم المعلوماتية

بالرجوع إلى قانون العقوبات الجزائري الحالي فإنه لا يكفي لمواجهة هذه الجرائم الجديدة والمستحدثة فهل هذا يعني أن نقف مكتوفي الأيدي أمام الفراغ والنقص التشريعي، مما يعني ترك أفعال إجرامية دون عقاب وملاحقة رغم خطورتها، أم نخالف مبدأ الشرعية الجنائية الذي نصت عليه المادة الأولى في قانون العقوبات (لا جريمة ولا عقوبة أو تدابير أمن بغير قانون) والحقيقة أن مصادر التجريم والعقاب تنحصر في القانون الجنائي، وعليه يجب على المشرع أن يتدخل كلما دعت إليه الحاجة ليجرم ويعاقب على الأفعال المستجدة وهذا عملا بمبدأ الشرعية والذي ينقسم إلى شقين :

الشق الأول : شرعية الجرائم وبمعنى أخر أنه كل واقعة لا يمكن أن تعد جريمة ما لم يقرر القانون ذلك صراحة

الشق الثاني : شرعية العقوبات ويعني أن المتهم لا يخضع لأي عقوبة تختلف عن ما يقرره المشرع .

وعليه فإن مبدأ الشرعية يقوم بالفصل بين سلطتي التنفيذ والقضاء، فالقاضي يقتصر دوره على تطبيق النصوص التي يضعها المشرع .

و إذا لم تكن هناك نصوص فلا يجوز اعتبار الفعل جريمة حتى لو تبين أن الفعل ضار أو مخالف لقواعد الأخلاق أو مجافيا للعدالة .

* و ما يميز القاضي الجنائي هو التفسير الضيق للنصوص وفي المقابل ضرورة تفسير الشك لصالح المتهم، وهذا من شأنه أن يدعم مبدأ الشرعية من خلال عدم المتابعة والمعاقبة على وقائع لم يتم تجريمها .

* كما يتميز مبدأ الشرعية بعدم اللجؤ للقياس أثناء تفسير النصوص، وعليه فلا يحوز للقاضي أن يقوم بقياس فعل لم يرد نص يجرمه على فعل ورد بشأنه نص يجرمه فيقررللأول عقوبة الثاني للتشابه بين الفعلين . وعليه ومن خلال ما تقدم يمكن القول:

إن الجريمة المعلوماتية باعتبارها جريمة مستحدثة ولم يتم تجريمها بنصوص قانونية في اغلب الدول خصوصا العربية منها باستثناء بعض التشريعات في الإمارات العربية المتحدة وسلطنة عمان وتونس زكذلك تم تجريمها في الجزائر في تعديل قانون العقوبات لسنة 2004 ، غير أن تلك السلوكيات والوقائع تبقي بعيدة عن المتابعة في اغلب الدول، مما يستوجب ضرورة الإسراع وتدارك هذا النقص التشريعي في القريب العاجل، رغم أن مرجعيتها تقوم على جرائم شائعة كالنصب والاحتيال والسرقة والتزوير إلا أنها تبقى بعيدة عن المتابعة لانعدام الشرعية القانونية.

ثالثا : نطاق الجريمة المعلوماتية

تتميز الجريمة المعلوماتية بأنها لا تقتصر على نظام المعلوماتي لدولة واحدة، وإنما تمتد إلى دول عديدة وفي قارات مختلفة، وعلى هذا الأساس ثار جدل فقهي حول نطاق الجريمة المعلوماتية فهل تعد جريمة دولية أم جريمة عالمية؟ وسنحاول شرح ذلك على النحو التالي:

1- الجريمة الدولية:

تعرف الجريمة في القانون الدولي (عدوان على مصلحة يحميها القانون الدولي الجنائي) أو هي كل تصرف غير مشروع يعاقب عليه القانون الدولي لانطوائه على اعتداء على العلاقات الإنسانية في الجماعة الدولية .

غير إن فقهاء القانون الجنائي الدولي إضافة طائفة أخرى من الجرائم بالنظر إلى وسيلتها وليس لطبيعتها ومن أمثلة ذلك جريمة خطف الطائرات والقرصنة ...الخ[8] .

2- الجريمة العالمية:

ويقصد بها مجموعة القوانين الجنائية الوطنية مجتمعة، وبمعنى أخر أن يطبق قانون العقوبات على كل مجرم يقبض عليه في إقليم الدولة، أيا كانت الدولة التي ارتكب فيها الفعل الإجرامي وأيا كانت جنسية الجاني وهذا ما يعبر عنه بعالمية القاعدة الجنائية.

ويرى جانب كبير من الفقه أن الجريمة المعلوماتية هي جريمة عالمية وهذا بالنظر لطبيعتها والوسائل المستعملة فيها والنتائج المترتبة عنها، مما يستوجب وضع تشريعات تعمل على تجريم جميع السلوكيات الإجرامية من جهة، والسعي لزيادة التعاون الدولي في المجالين الاتفاقي والقضائي وهذا في بسيل تطويق هذه الظاهرة الإجرامية الخطيرة[9].

رابعا: قواعد الاختصاص في الجريمة المعلوماتية:

الاختصاص هو السلطة التي يقرها القانون للقضاء في أن ينظر في دعاوى من نوع معين[10].

وبالنظر لطبيعة وخصائص الجريمة المعلوماتية فليس لها مقر ثابت أو دولة معينة بل تنتشر في كل دول العالم، وليست لها أية هيئة أو جهة تشرف عليها ومسؤولية عنها مما يترتب عن ذلك عدم وجود قانون جنائي محدد أو موحد يحكم الجريمة بل بالعكس هناك العديد من القوانين الجنائية بتعدد الدول و الأنظمة القانونية و ذلك يرجع أساسا لارتباط القانون الجنائي بالسيادة الوطنية .

ومن هنا تكمن الإشكالية في أن بعض السلوكيات والأفعال مجرمة في بعض الدول ومباحة في دول أخرى، وفي أغلب الدول لا توجد نصوص تنظم هذه السلوكيات، و السؤال المطروح إلى أي مدى يمكن تطبيق القانون الوطني على جرائم المعلوماتية العابرة للحدود ؟

أن القاعدة العامة المطبقة في أغلب الدول هي مبدأ الإقليمية، بمعنى أن القانون الجنائي يطيق على كافة الجرائم التي تقع في تراب الدولة بغض النظر عن جنسية فاعلها أو مرتكبها، ومع هذا فإن تطور الإجرام وتوسعه إلى دول العالم تطلب وجود اتفاقيات دولية لتسليم المجرمين، غير أن غالبية الدول لا تسلم رعاياها وفق لمبدأ السيادة من جهة، ومن جهة أخرى التعارض مع مبدأ أساسي في القانون الجنائي وهو عدم جواز محاكمة لشخص عن فعل واحد أكثر من مرة .

وعلى هذا الأساس سنحاول وضع ملامح نظام قانوني يسمح بمتابعة وملاحقة مرتكبي الجرائم المعلوماتية دون المساس بحقوق وحريات الأفراد التي تقرها المواثيق الدولية، ووجوب احترام مبدأ الشرعية دون إعطاء

فرصة للجنات من الإفلات من المتابعة الجنائية وتوقيع العقوبة المناسبة عليهم مما يحقق الأمن والاستقرار للمجتمع، وعليه سنبحث على معيار يتلائم وطبيعة الجرائم الالكترونية.

1- مبدأ الاختصاص الإقليمي :

تأخذ أغلب التشريعات الوضعية بهذا المبدأ على غرار المشرع الجزائري في المادة 03 من قانون العقوبات التي تنص(يطبق قانون العقوبات على كافة الجرائم التي ترتكب في أراضي الجمهورية)

كما أخذ بهذا المبدأ المشرع الفرنسي في المادة 113 ف 02 من قانون العقوبات الجديد التي تنص (يطبق القانون الفرنسي على الجرائم المرتكبة على إقليم الجمهورية و تعتبر قد ارتكبت على إقليم الجمهورية إذا كان أحد عناصر الجريمة قد وقع على هذا الإقليم)[11]

و يعني هذا المبدأ أن قانون العقوبات يطبق على أي جريمة تقع داخل القطر الوطني بغض النظر عن جنسية مرتكبيها أو المجني عليه و ينعقد الاختصاص وفقا لهذا المبدأ بتحقق أحد العناصر المكونة للجريمة سلوكا أو نتيجة .

كما أن هذا المبدأ يسمح بمتابعة كل من ارتكب أحد العناصر المكونة للجريمة ولو كان الفعل غير معاقب عليه في بلد المنشأ الأصلي أي بداية السلوك الإجرامي، ومن ثم تنقل البيانات والمعلومات بين العديد من الدول وبمجرد اقتراف أحدى سلوكيات الجريمة في القطر الوطني ينعقد الاختصاص للقاضي الوطني، ومن ثم يجب تطبيق قانون العقوبات الوطني كما يمكن بناء على هذا المبدأ متابعة الجاني خارج القطر متى كان مساهما أو شريكا في الجريمة التي وقعت داخل القطر لأن العبرة بمكان وقوع الجريمة .

غير إن هذا المبدأ يجد صعوبة كبيرة في تطبيقه بالنسبة الجريمة المعلوماتية وهذا بالنظر لطبيعتها و خصائص التي تميزها عن الجريمة التقليدية وخصوصا صعوبة تحديد مكان وقوعها وارتكباها بدقة وكذا زمان حدوثها .

كما أن هذا المبدأ يجد صعوبة في تطبيقه في قانون العقوبات الفرنسي حيث تنص المادة 113 ف 05 (يطبق القانون الفرنسي على كل من ارتكب فعلا في إقليم الجمهورية يجعله شريكا في جناية أو جنحة وقعت بالخارج إذا كانت الجناية أو الجنحة معاقبا عليها في القانون الفرنسي والقانون الأجنبي و كانت ثابتة بمقتضى حكم نهائي من القضاء الأجنبي)

وعليه وبناء على نص المادة أعلاه فإنه لكي يسأل الشريك يجب توافر ما يلي :

- أن يكون الفعل مجرما في البلد المنشأ – الفعلي الأصلي –
- أن يصدر حكم الإدانة عن الفاعل الأصلي في البلد المنشأ

وعليه فإن تطبيق هذا النص يصطدم بعقبة مادية تتمثل في صعوبة تحديد مكان وقوع الفعل الأصلي، لأنه شرط أولي لعقد الاختصاص للقاضي الوطني، لأن ذلك يترتب عليه معرفة ما إذا كان الفعل مباحا أو مجرما في ذلك البلد.

وأخيرا نقول أن مبدأ الإقليمية يقوم على أساس مكان وقوع الجريمة أو أحد عناصرها المادية وهذا المبدأ يبدوأ أنه غير ملائما للجريمة المعلوماتية، وهذا بالنظر لطبيعتها غير المادية من جهة ومن جهة أخرى لصعوبة اكتشافها وتحديد مكان وزمان وقوعها بدقة

2-مبدأ الاختصاص الشخصي :

يأخذ هذا المبدأ وجهان وجه إيجابي ووجه سلبي وسنحاول توضيح ذلك كما يلي: .

الوجه الإيجابي: ويعني تطبيق القانون الجنائي على كل من يحمل جنسية الدولة ولو ارتكب الجريمة خارج إقليمها.

الوجه السلبي: ويعني تطبيق القانون الجنائي على كل جريمة يكون فيها المجني عليه ينتمي إلى جنسية الدولة ولو كان الجاني أجنبيا وارتكب الفعل خارج إقليم الدولة[12].

والمشرع الجزائري على غرار باقي التشريعات لا يعترف بمبدأ الشخصية في وجه السلبي لأن جنسية المجني عليه ليست محل اعتبار في تطبيق القانون الجنائي من حيث المكان .

وعلى العكس من ذلك يأخذ المشرع الجزائري بمبدأ الشخصية في شقه الإيجابي وهو ما نصت عليه المادتين 582- 583 من قانون الإجراءات الجزائية .

غير أن هذا المبدأ وردت عليه قيود بصفة عامة و بالتالي فإن الاختصاص لا ينعقد في المحاكم الوطنية بشكل تلقائي بالنسبة للجرائم التي تقع في الخارج بل يجب علم النيابة العامة بها، كما أنه لا يجوز محاكمة الشخص على نفس الفعل الواحد مرتين وهذه الإجراءات طويلة ومكلفة وتقيد تطبيق مبدأ الاختصاص الشخصي .

والملاحظ أن هذا المبدأ يعتمد بصفة أساسية على الجاني من حيث الكشف على هويته ومن ثم التعرف عن جنسيته، وهذه المعلومات تعد صعبة وعسيرة في جرائم الانترنت أين يستعمل التشفير والأسماء المستعارة بالإضافة إلى اللغة الصعبة والمعقدة في كشفها والتعامل معها .

كما أن محاكمة المجرم الذي يقيم في دولة أجنبية تحتاج إلى إجراءات طويلة وشاقة ومعقدة ومكلفة، وهذا ما يصدق كذلك بالنسبة لتنفيذ الأحكام الصادرة في الخارج .

- وكذلك من مخاطر تطبيق القانون الوطني على الجرائم التي تقع في الخارج والتي يختص بها القانون الأجنبي في ذات الوقت أنه قد يؤدي إلى المساس بمبدأ عدم جواز محاكمة الشخص عن الفعل الواحد أكثر من مرة وهو إحدى المبادئ الأساسية للقانون الجنائي

– و على العكس من ذلك إذا لم يكن القانون الوطني مختص بنظر للواقعة فتثار الإشكالية بالنسبة للمضرور من الجريمة الذي يجب عليه التنقل إلى الدولة حيث ارتكب الفعل لرفع دعواه المدنية[13]

والأخطر من ذلك أن يكون الفعل غير معاقب عليه في هذه الدولة ولذلك نري بأنه يجب أن يكون هناك قانون جنائي دولي على غرار القانون الدولي الخاص ليطبق على جرائم المعلوماتية.

3-مبدأ الاختصاص العيني:

طبقا لهذا المبدأ يطبق القانون الجنائي الوطني على الجرائم التي ترتكب بالخارج بصرف النظر عن جنسية مرتكبها، ويرجع هذا المبدأ إلى المساس بسيادة الدولة[14].

وحقها في الدفاع عن جميع صور الاعتداء على مصالحها الحيوية والأساسية ولو وقعت تلك الجرائم خارج إقليمها.

وعلى هذا الأساس يمكن أن يطبق هذا المبدأ على جرائم المعلوماتية إذا كانت تمس بالسيادة الوطنية ووحدة الدولة أو تعمل على المساس بالمصالح الحيوية ولو ارتكبت من قبل أجانب وخارج إقليم الدولة .

غير أن هذا المبدأ في الواقع يصادف العديد من الصعوبات ترجع بالأساس إلى طبيعة وخصائص الجريمة المعلوماتية حيث لا تظهر مادياتها بوضوح، كما أن الفاعل يبقى مجهولا بالإضافة إلى تعدد وتنوع الأنظمة القانونية في العالم واختلافها مما يترتب عليه البطء والتعقيد وطول مدة الإجراءات .

4- مبدأ الاختصاص العالمي:

يطبق وفقا لهذا المبدأ القانون الجنائي على كل جريمة يقبض على مرتكبها في إقليم الدولة أيا كان مكان ارتكابها وجنسية الفاعل أو الجاني[15].

وهذا المبدأ يعطي لقانون العقوبات مجال متسعا يشمل العالم كله، فلا يتقيد بمكان ارتكاب الجريمة أو احد سلوكياتها ولا بجنسية مرتكبها ولا بطبيعة الجريمة ومساسها بالسيادة والمصالح الوطنية .

وإنما يتطلب فقط القبض على الجاني في إقليم الدولة ليعطى للقانون الجنائي الوطني الاختصاص، وهذا المبدأ يتلائم كثيرا وطبيعة الجريمة المعلوماتية رغم ما يطرحه من تنازع حاد بين التشريعات الجنائية في الدول

وعليه فانه يمكننا القول:

بأن أهمية هذا المبدأ ومدى ملائمته للجريمة المعلوماتية مستمدة من خطورتها من جهة، ومن طبيعتها من جهة أخرى، كونها سهلة الوقوع من أشخاص يحملون جنسيات مختلفة وتمتد عناصرها المادية وسلوكياتها الإجرامية بين أكثر من دولة، وفي فترات زمنية قصيرة جدا، وهذا المبدأ – أي العالمية- يبقى عاجزا عن معالجة جميع القضايا في هذا الشأن ما لم يكن هناك تعاون دولي جاد وسريع ،وكذا وجوب إعداد تشريعات

وطنية لتجريم الظاهرة، ومنها إمكانية معاقبة كل من يتم القبض عليه على إقليم الدولة دون مراعاة لجنسيته أو مكان وقوع الفعل الإجرامي.

والملاحظ أن اغلب التشريعات الوضعية ومنها المشرع الجزائري لم ينص على هذا المبدأ بالرغم من أهميته خصوصا في مجال الجريمة المعلوماتية، ونرى وجوب النص عليه عند إعداد قانون خاص بمعالجة الجريمة المعلوماتية وجرائم الكمبيوتر والانترنت، وهذا بالرغم من أن الاتفاقيات الدولية تركز بل وتعول عليه كثيرا في هذا المجال خصوص اتفاقية بودابست 2001 لمكافحة الجريمة المعلوماتية وكذا القانون العربي النموذجي لمكافحة جرائم تقنية أنظمة المعلوماتية 2003 في المادة 26.

كما أن الفقه يرى بوجوب الأخذ به على غرار جريمة القرصنة في القانون الدولي الجنائي[16].

ونحن نعتقد أن الجريمة المعلوماتية لا تقل أهمية عن جريمة القرصنة كونها تهدد امن وسلامة المجتمع الدولي من خلال اهتزاز الثقة في التعامل بالبيانات والمعطيات على الشبكة العنكبوتية مما يهدد الاقتصاد العالمي الذي يشهد وتيرة متصاعدة خصوص في المجال المالي والبنكي، وعليه أصبح من الضروري الاخذا بهذا المبدأ ومعاقبة الجاني في أي إقليم يتم فيه القبض عليه دون مراعاة لجنسيته أو مكان ارتكاب جريمته لارتكابه جريمة عالمية.

خامسا : التحديات التي تواجه الجوانب الإجرائية في الجريمة المعلوماتية:

بالنظر لطبيعة هذه الجرائم فإنها لا تترك اثرا ماديا في مسرح الجريمة بالإضافة إلى قدرة الجاني على إتلاف وتشويه الدليل في وقت قصير وتظهر جملة من التحديات تتعلق أساسا بما يلي:

*بالنسبة لإجراءات التفتيش:إن هذه الجرائم تعتمد على نظم المعلومات وقد تتجاوزه إلى أنظمة أخرى غير نظام المشتبه به، وهذا الإجراء يعتمد على تمديد نطاق التفتيش على نظام غير نظام محل المشتبه به، وهذا من شانه أن يطرح جملة من الإشكاليات القانونية من خلال مدى احترام وعدم المساس بالحريات الشخصية ومبدأ سرية الاتصالات لأشخاص التي يمتد إليهم التفتيش[17].

*بالنسبة لإجراءات الضبط : لا تتوقف إجراءات الضبط على جهاز الكمبيوتر بل تمتد من ضبط المكونات المادية إلى مختلف أجزاء النظام، وعليه فتمتد إلى المعلومات والمعطيات والبيانات والبرامج المخزنة في النظام أو إلى النظم المرتبطة بالنظام محل الاشتباه وكل الأشياء ذات الطبيعة المعنوية لأنها معرضة بسهولة للتلف والضياع وهذا ما يثير إشكالية من الجهة القانونية خصوصا ما تعلق بالحقوق المحمية قانونا وكذا الحق في سرية البيانات واحترام سرية الاتصالات[18].

*بالنسبة لأدلة الإثبات والإدانة : وهي كلها بيانات معنوية كسجلات الكمبيوتر ومعلومات الدخول والاشتراك والنفاذ وهي تثير جملة من الإشكاليات أمام القضاء من حيث مدى قبولها وحجيتها مع وسائل الإثبات التقليدية

و خلاصة القول أن أهم التحديات التي تواجه الجريمة المعلوماتية تتمثل في[19] :

– الحاجة إلى سرعة الكشف عن الجريمة و تعقبها و خشية ضياع الدليل بالإضافة إلى خصوصية قواعد التفتيش والضبط الملائمة لهذه الجرائم .

مدى قانونية وحجة الأدلة في الجرائم المعلوماتية التي تقع عن الانترنت .

– الحاجة إلى المزيد من التعاون الدولي في مجال التحقيق وتسليم المجرمين وتنفيذ الأحكام القضائية

سادسا : التعاون الدولي في مجال مكافحة الجرائم المعلوماتية:

يتجلى التعاون الدولي من خلال التعاون الاتفاقي بإبرام جملة من المعاهدات الدولية من أجل الوقاية و الحد من جرائم الانترنت وكذا التعاون القضائي من خلال المساعدة القضائية وتسليم المجرمين .....الخ

1– التعاون الاتفاقي الدولي في مجال مكافحة الجرائم المعلوماتية

تعتبر الاتفاقات الدولية أهم وسيلة في هذا المجال و تعمل على توحيد الجهود الدولية لمكافحة هذه الجرائم و تعمل الأمم المتحدة باعتبارها مركز لتنسيق الجهود بين الدول على ذلك ويظهر ذلك جليا من خلال جملة من القرارات و التوصيات و الاتفاقيات الدولية و منها نذكر :

أ– **قرار هافانا 1991** الناتج عن مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة السجناء حيث وضع إطار دوليا لمكافحة لجرائم الكمبيوتر وجاء في هذا القرار بما يلي[20]:

– التأكيد على وضع إطار قانوني دولي ملائم مما يتطلب جهدا جماعيا بين الدول

– الطلب من الدول الأعضاء القيام بالإجراءات التالية :

* تحديث القوانين لمواكبة المرحلة خصوصا في مجال التحقيق وقبول الأدلة والإجراءات القضائية

* تحسين تدابير الأمن و الوقاية المتعلقة بالحاسوب مع مراعاة الخصوصية وحقوق الإنسان .

* زيادة الوعي لدى الجماهير من خلال إبراز أهمية مكافحة جرائم ذات صلة بالحاسوب .

* اعتماد تدابير خاصة لتدريب القضاة و الضبطية القضائية لمواكبة متطلبات المرحلة .

* زيادة التعاون بين المنظمات ذات العلاقة ووضع قواعد للأخلاق للتعامل بها .

ب– **انعقاد المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات** في البرازيل 1984 ووقع جملة من الأسس الواجب احترامها ومراعاتها في مكافحة الجرائم المتعلقة بالكمبيوتر ومنها نذكر[21]:

* وجوب تحديد السلطات التي تقوم بالتفتيش والضبط في بيئة تكنولوجيا المعلومات

* السماح للسلطات العامة باعتراض الاتصالات داخل نظام الحاسوب ذاته مع استخدام الأدلة المحصل عليها أمام المحاكم

*يجب مراعاة المسائل المرتبطة ببنية المعلومات وما يمثله ضياع الفرص الاقتصادية وانتهاك الحرمة والحياة الخاصة وكذا كلفة إعادة بناء قاعدة البيانات وهذا قبل كل تفتيش أو تحقيق .

*إعادة النظر في قواعد الإثبات الكتروني ومصداقية الأدلة مع مراعاة القواعد التشريعية

ج-اتفاقية بودا باست 2001 لمكافحة الجرائم المعلوماتية : وتتلخص أهداف هذه الاتفاقية في ما يلي [22]:

* السعي لتوحيد التدابير التشريعية بين الدول للوقاية من هذه الجرائم

* ضرورة تفعيل خطة العمل على الجانب الموضوعي و الإجرائي للحد من هذه الظاهرة

* التأكيد على أهمية التعاون الإقليمي والدولي للوقاية من هذه الجرائم

* العمل على تحقيق التوازن بين حقوق الإنسان الأساسية و حرية الرأي وحرية الوصول للمعلومة وحرية البحث والحق في الخصوصية ....الخ غيرها من الحقوق الأساسية الثابتة في العلاقات الدولية.

د/ **أما على المستوى الإقليمي العربي فنجد القانون العربي** النموذجي لمكافحة جرائم تقنية أنظمة المعلوماتية و الذي صادق عليه مجلس وزراء العدل العرب في2003/10/08 في دورته التاسع عشر [23]:

وقد جاء هذا القانون بجملة من الأحكام الموضوعية والإجرائية تعمل على الحد من الجريمة المعلوماتية .

واعتمد القانون في مجال الاختصاص –موضوع دراستنا – على مبدأ العينية وفقا للمادة 26 التي تنص على أنه (تسري أحكام هذا القانون على أيا من جرائم المنصوص عليها فيه ولو ارتكبت كليا أو جزئيا خارج إقليم الدولة متى أضرت بإحدى مصالحها ويختص القضاء الوطني بنظر الدعاوى المترتبة عليه) .

ومن خلال النص نلاحظ أن القانون أخذ بمبدأ العينية باعتماده على المصلحة الوطنية كمعيار أساسي لثبوت الاختصاص و بالتالي تطبيق القانون الجنائي الوطني .

كما نلاحظ أن هذا القانون لم يعين أي جهة تتولى عملية الضبط القضائي في جرائم المعلوماتية مما يعني ترك المجال مفتوحا للدول العربية من خلال إعطاء تلك السلطة لأي هيئة أو جهة تراها قادرة على اكتشاف ومتابعة تلك الجرائم .

2 –التعاون القضائي الدولي في مجال مكافحة الجرائم المعلوماتية

يعتمد التعاون القضائي الدولي أساسا على دعم جهود الشرطة الدولية في ملاحقة والقبض وتسليم المجرمين وكذا وجوب المساعد القضائية في المواد الجنائية خصوصا، وقد قطع الاتحاد الأوربي شوطا كبيرا في تنمية وتفعيل

سياسة مشتركة من خلال توسيع خطة(فينا) بتاريخ1998/12/03 والتي تدعوا إلى ضرورة تعزيز التعاون القضائي الإداري والمعلوماتي في الشق الجنائي في مجالات حماية البيئة بكل عناصرها[24].

وعلى هذا الأساس سنبين الجهود الدولية من خلال تبادل والمعلومات والمساعد القضائية كما يلي:

أ- تبادل المعلومات

أن مكافحة الجرائم الالكترونية لا تتحقق إلا من خلال تعاون دولي حقيقي، ولا يتأتي ذلك إلا من خلال التعاون على المستوى الإجرائي، والمتمثل في تبادل المعلومات عن طريق تسهيل الاتصال بين الأجهزة القضائية بين الدول، وخصوصا دور الشرطة في الكشف عن الجرائم والمجرمين وفتح مكاتب متخصص في كل الدول لذلك الغرض .

وقد تبلور هذا النوع من التعاون منذ إنشاء المنظمة الدولية للشرطة الجنائية (الانتربول)[25].

وتقوم هذه المنظمة بتشجيع التعاون الدولي بين أجهزة الشرطة في الدول الأطراف على نحو فعال يحقق مكافحة الجريمة، وهذا من خلال تجميع المعلومات والبيانات المتعلقة بالمجرم والجريمة عبر كل المكاتب الوطنية للشرطة الدولية الموجودة في أقاليم الدول الأعضاء.

وعلى خط الانتربول أنشاء المجلس الأوربي عام1991 الشرطة الأوربية تكون حلقة وصل بين الشرطة المحلية لدول الاتحاد الأوربي فيما بينها من جهة ومن جهة أخرى تعمل على كشف الجريمة عبر الحدود والدولية[26] .

ب: المساعدة القضائية الدولية في المواد الجنائية

بالنظر لطبيعة جرائم المعلوماتية ذات الطابع العالمي فإن الإجراءات الجنائية التي تبدأ بملاحقة الجناة وتقديمهم للمحاكمة وسماع الشهود أو اللجوء للإنابة القضائية لجمع المزيد من المعلومات التي يمكن أن تساهم في التحقيق والكشف عن هذه الجرائم وتساعد في توقيع العقوبة عليهم، لا تتحقق إلا من خلال المساعدة القضائية في إطار التعاون الدولي، ولهذا فقد نصت أغلب الاتفاقيات الدولية على ضرورة المساعدة القضائية وهذا من خلال:

* **تبادل المعلومات:** وهي تشمل تقديم كل البيانات والوثائق التي تطلبها سلطة قضائية أجنبية بصدد متابعة جريمة ما والرد على الاتهامات التي وجهت إلى رعاياه في الخارج وتبيان الإجراءات التي اتخذت ضدهم.

ومن مظاهر تبادل المعلومات ما ستعلق بالمساعدة في الكشف عن السوابق القضائي للجناة من خلال التعريف بالماضي الجنائي لهم ، وهذا من شأنه تكوين فكرة على طريقة عمل والتخطيط للمجرم مما يساعد في القبض عليه أثناء التحقيق، أو التخفيف والتشديد العقوبة عند محاكمته.

***نقل الإجراءات:** ويقصد بها قيام دولة بناء على اتفاقية باتخاذ إجراءات جنائية بصدد جريمة ارتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة وهذا إذا ما توافرت شروط معينة وهي[27]:

- أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والدولة المطلوب منها.

– أن يكون الإجراء المطلوب اتخاذه مقرر في قانون الدولة المطلوب إليها عن ذات الجريمة

– أن يكون الإجراء المطلوب اتخاذه يؤدي إلى الوصول للحقيقة كان تكون أدلة للجريمة موجودة بالدولة المطلوب إليها.

وعليه فانه يجب على الدول المعنية أن تتعاون فيما بينها حتى يمكنها معالجة جرائم المعلوماتية، وعلى هذا الأساس فقد شددت مسودة الاتفاقية الأوربية لجرائم المعلوماتية من خلال القانون الجنائي على ضرورة تدويل هذه الجرائم وخاصة تلك العابرة للحدود، وضرورة قيام الدول الأطراف بتبني قوانين جنائية وطنية في هذا المجال.

كما أوصت الاتفاقية على المستوى الدولي بضرورة قيام الدول بالتعاون فيما بينها من أجل التصدي لهذه الجرائم على ضوء المبادئ التالية:

– تقديم المساعدة في التحقيق الجاري في أي دولة بالنسبة لهذه الجرائم المنصوص عليها في المادة 04 من هذه الاتفاقية

– التزام بالتعاون مع سلطات التحقيق

– تقديم المساعدة الفنية والتقنية اللازمة في التحقيق الجنائي

– تسهيل الإجراءات الإدارية والتقنية من اجل حل مشاكل الإثبات في جرائم المعلوماتية.

ج: تبادل الإنابة القضائية الدولية:يقصد بالإنابة القضائية طلب اتخاذ إجراء قضائي من إجراءات الدعوى الجنائية، تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها لضرورة ذلك الفصل في مسألة معروضة على السلطة القضائية في الدولة الطالبة، ويتعذر عليها القيام بها بنفسها، وأن تنفيذ طلب الإنابة غير ملزم للدول المنابة لان أساسها اعتبارات المجاملة الدولية[28].

وهذا الإجراء من شانه تسهيل الإجراءات الجنائية بين الدول بما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة، والتغلب على عقبة السيادة الإقليمية التي تمنع الدول الأجنبية من ممارسة بعض الأعمال القضائية داخل أقاليم الدول الأخرى، مثل ما جرى به العمل من سماع الشاهد المقيم بالخارج عن طريق الإنابة القضائية.

ولم نجد في القانون الجزائري ما يشير إلى تنظيم مسالة الإنابة القضائية مما يتطلب الرجوع للأحكام التي تنظمها في الاتفاقية الدولية التي انضمت إليها الجزائر .

ومن بين الاتفاقيات التي أبرمت في مجال الإنابة تلك التي عقدت بين الجزائر ومصر في 1964/07/15 وكذا التوقيع على اتفاقية جامعة الدول العربية المتعلقة بالتعاون القضائي في المواد الجنائية بتاريخ 1953/07/09.

وما يلاحظ انه غالبا ما يتم استبعاد تنفيذ أحكام الإنابة القضائية في المجال السياسي والضريبي والعسكري، لأنها مجالات من شانها المساس بالسيادة والنظام العام والمصالح الأساسية للدول، غير أن هذا النظام يبقى معيب لارتباطه بالطرق الدبلوماسية والتي تتسم بالبطء وكثرة الشكليات والبرتوكولات وهو ما يتعارض وطبيعة جرائم البيئة التي تتميز بالسرعة والتغير وتأخر ظهور نتيجتها الإجرامية أحيانا، وهذا من شانه ضياع أدلة وبيانات أو اختفاءها والتي قد تشكل دليل مهما لإدانة المتهم.

الـــــخاتمـــة :

في ختام دراستنا يتضح أن جريمة المعلوماتية جريمة مستحدثة ومتطورة وغير تقليدية مما يستوجب ضرورة الإسراع في وضع تشريع جنائي يكفل حمايتها من خلال إيجاد آليات جديدة تتلائم و طبيعتها خصوص في الجانب الإجرائي و هذا من خلال :

– ضرورة العمل على توحيد الجهود من اجل عقد مؤتمر دولي لصياغة قانون موحد لمعالجة جرائم المعلوماتية يكون تحت رعاية الأمم المتحدة

– الاعتماد على مبدأ العالمية بالنظر لطبيعة الجرائم المعلوماتية العابرة للحدود ونرى أنه أكثر ملائمة من مبدأ الإقليمية المطبق في أغلب التشريعات الجنائية الحالية

– كما يتوجب إعطاء الضبطية القضائية المزيد من الوسائل التقنية المتطورة مع ضرورة التكوين والتأهيل المتواصل و إمكانية الاستعانة بأهل الخبرة والاختصاص

– إقامة هيئة وطنية وإقليمية وعالمية تتولى تنسيق الجهود والعمل على الوقاية من هاته الجرائم

– ضرورة تأهيل و تكوين قضاة متخصصين في هذا النوع من الجرائم وإقامة محاكم مختصة في هذا المجال
– ضرورة تفعيل التعاون الدولي من خلال إبرام المزيد من الاتفاقيات الدولية على المستوى الإقليمي والعالمي.

– أهمية تفعيل دور الأسرة في متابعة الأبناء ووقايتهم من إخطار شبكة الانترنت بالإضافة إلى توعية المجتمع المدني والجمعيات وكذا وسائل الإعلام في الحد من هذه الجرائم .

الهـــوامش:

1– عبد الله حسين على محمود: **سرقة المعلومات المخزنة في الحاسب الآلي** ، دار النهضة العربية، الإسكندرية، 2002، ص351

2- John Eaton & jermy smithers, A managers Guide to information Technology, London, Philip Allan,1982,p263

3– خالد ممدوح ابراهيم : **امن الجريمة الالكترونية**، الدار الجامعية، الإسكندرية، 2008 ، ص47

4–جعفر حسن جاسم الطائي: **جرائم تكنولوجيا المعلومات** ، دار البداية، ليبيا، 2007، ص144.

5–خالد محمد كدفور المهيري: **جرائم الكمبيوتر والانترنت والتجارة الالكترونية**،دار العزيز للطباعة والنشر، دبي ،2005،ص135.

6–نائلة عادل محمد فريد:**جرائم الحاسوب والجريمة الاقتصادية**،منشورات الحلبي الحقوقية، لبنان،2005،ص55

7–نبيلة هروال :**الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات**، دار الفكر الجامعي ، الإسكندرية،2006،ص35

8–حسنين عبيد: **الجريمة الدولية دراسة تحليلية وتطبيقية** ،دار النهضة العربية، الإسكندرية، 1989، ص10.

9– انظر:–جلال ثروت، **شرح قانون العقوبات القسم العام**، منشاة المعارف، الإسكندرية،1989،ص104.

– مأمون محمد سلامة، **شرح قانون العقوبات القسم العام**ط03 دار النهضة العربية، الإسكندرية2002ص80

10– محمود نجيب حسني، **شرح قانون الإجراءات الجزائية**، دار النهضة العربية، 2002، ص723.

11- VIDAL (G) , Cours de droit criminal et de science penitenterntniaire 8eme ed,mis a jour par Magnol , libraie Arthur Rousseau, paris,1935,N 0 1,p1071.

12– جميل عبد الباقي الصغير: الجوانب الإجرائية للجرائم المتعلقة بالانترانت ، دار النهضة العربية، الإسكندرية،2002،ص55.

13–جمال محمود الكردي:**المحكمة المختصة والقانون الواجب التطبيق بشان دعاوى المسؤولية والتعويض عن مضار التلوث البيئة العابرة للحدود**،ط01، دار النهضة العربية، الإسكندرية، 2003،ص132.

14–مأمون محمد سلامة: مرجع سابق،ص75.

15– محمود نجيب حسني ، المرجع السابق،ص140

16– المرجع نفسه،ص141.

17– عبد الفتاح حجازي: **مكافحة جرائم الكمبيوتر والانترنت،دراسة معمقة في القانون المعلوماتي، ط01، دار الفكر الجامعي**،الإسكندرية،2006،ص14.

18– عبد الله عبد الكريم عبد الله:**جرائم المعلوماتية والانترنت دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والانترانت مع الإشارة إلى جهود مكافحتها محليا وعربيا ودوليا** ،ط01، منشورات الحلبي الحقوقية، لبنان ،2007،ص 47.

19–محمد الشكوابة :**جرائم الحاسوب والانترنت** ،دار الثقافة للنشر، الأردن، 2004، ص13.