جامعة سعد دحلب بالبليدة

كلية الحقوق

قسم القانون العام

مذكرة ماجستير

التخصص : القانون الجنائي الدولي

الإجرام الدولي الإلكتروني

من طرف علي بويوسفي

أمام اللجنة المشكلة من:

سعيد يوسف محمد يوسف	أستاذ التعليم العالي	جامعة سعد دحلب البليدة	رئيسا
شربال عبد القادر	أستاذ محاضر	جامعة سعد دحلب البليدة	مشرفا و مقررا
بوغزالة محمد ناصر	أستاذ التعليم العالي	جامعة الجزائر	عضوا مناقشا
سويرة عبد الكريم	مكلف بالدروس	جامعة البليدة	عضوا مناقشا

البليدة، سبتمبر 2008

شكر

بتمام هذا العمل المتواضع، أشكر الله و أحمده الذي أمدني بصواب العقل و كمال الصحة و على ما سخره لي من ظروف ساعدتني على ذلك.

أشكر أساتذتي الذين تعلمت منهم ألف باء الدراسة و منهم أستاذي المشرف و أساتذتي أعضاء اللجنة الذين وقفوا بجانبي من أجل تصويب ما غفلت عنه في بحثي هذا.

أشكر كل من ساعدوني من زملاء و أصدقاء.

الإهداء

أهدي هذا العمل،
إلى أهلي،
و من هم لي،
متمنيا التوفيق للجميع

ملخص

من خلال دراسة نشأة و تطور التقنينات و التشريعات الجنائية، يبدو لنا أن كل جريمة هي في أصلها اعتداء و سلوك منحرف، و أن كل اعتداء و سلوك منحرف مصيره لا محالة التجريم. و أن المجرم سواء كان فردا أو جماعة أو منظمة، و سواء مورس الإجرام من طرفهم بصفتهم الرسمية أو بصفتهم أشخاص طبيعيين، فإنهم في كل مرة يختارون لإجرامهم أفضل الطرق لما يمكنهم من تحقيق نتائجهم الإجرامية كاملة، و من الإفلات من العقاب. و إذا كان المشرع الوطني أو الدولي، في حالة الجريمة الدولية، يسعى دائما إلى ملاحقة هؤلاء المجرمين بسن قوانين تجرم أفعالهم و من ثم معاقبتهم، فإنهم يلجؤون دائما إلى تغيير طرق ارتكاب إجرامهم بما يحول دون ذلك. هذا يعني أنهم يجتهدون في إيجاد صور جديدة للإجرام.

و فيما يخص الإجرام الدولي، فإنه بعد ما بذلت الهيئات الدولية جهودا معتبرة طيلة قرن من الزمن و انتهت إلى حد ما إلى بلورة بعض الأفعال و وصفتها على أنها جرائم دولية، و كان ذلك في ميثاق روما الأساسي للمحكمة الجنائية الدولية، لاحت في الأفق صور جديدة للإجرام ضاربة هذه الجهود عرض الحائط. و من بين ما تتمثل فيه هذه الصور، هي الاعتداءات الالكترونية، حيث طغى فيها الوصف على الفعل في حد ذاته، إلى درجة لم تعد تفي عبارة "منع الجريمة بجميع صورها و أشكالها" التي احتوتها بعض النصوص الدولية بشأن ذلك.

و لذلك تقوم ضرورة التصدي لهذه الاعتداءات عن طريق احتوائها ضمن نصوص خاصة لما صار لها من إمكانية تشكيل جريمة دولية بنفس الخطورة أو أكثر و مع ما يتوفر من ظروف تسمح بهذا التجريم.

غير أنه تعترض ذلك صعوبات موضوعية ترجع إلى الخصوصية التقنية لهذا النوع من الإجرام، أسفرت عن صعوبات في المعالجة القانونية لها، لا سبيل إلى تجاوزها من غير إقامة تعاون دولي جدي، الشيء الذي ليس من السهل تحقيقه نظرا لما في هذه المسألة هذه المرة من جوانب حساسة و متميزة.

الفهرس

الصفحة

مقدمة

يعرف أن ظاهرة الإجرام بصفة عامة أخذت أشكالا عديدة و تطورت كما و نوعا في العقد الأخير و تعقدت مع تعقد و زيادة و تنوع وسائل ارتكابها خاصة العلمية و التكنولوجية منها. و كلما كان الإجرام منظما و محكوما و سريا، كلما تضاعفت خطورته و صعب التصدي له. مما جعل الإجرام يصنف إلى تقليدي، يمكن النجاح نسبيا في مكافحته و هو ينصب على العالم الواقعي، و حديث قد لا يمكن من ذلك بسهولة.

و من بين ما يتمثل فيه الإجرام الحديث؛ جرائم العالم الافتراضي الذي نشأ عن طريق الشبكات الإلكترونية و هي شبكات عالمية يعد الحاسب الآلي الجهاز الأساسي في إقامتها. فهي وليدة الولايات المتحدة الأمريكية منذ الخمسينات. و على رأس هذه الشبكات نجد شبكة الإنترنيت الممتدة عبر الكرة الأرضية بل قد تعبر ذلك و التي تسمى شبكة الشبكات.

فجريمة التعدي بواسطة الكمبيوتر أو ما تسمى بالجريمة الإلكترونية أو جرائم الإنترنيت تتم عن طريق أفراد يتمتعون بخبرة و دراية في التعامل مع هذه الأجهزة المتطورة و أن ارتكاب هذا النوع من الجرائم يتم في الغالب لأسباب شخصية أو سياسية أو اقتصادية للحصول على بعض المعلومات بقصد نشرها أو كشفها لجهات معينة أو للجمهور بغرض الابتزاز و طلب المال أو الشركات أو غيرهم.

و الأخطر أن هذه الجرائم ارتقت في بعض الحالات إلى مستوى عالمي من الإجرام الدولي تماما مثل الذي فصله نظام روما الأساسي للمحكمة الجنائية الدولية، الذي كان بمثابة إرساء محاولات مكافحة الجرائم الدولية الخطيرة التي أوقعت ملايين الأطفال و النساء و الرجال ضحايا لفظائع لا يمكن تصورها هزت ضمير الإنسانية بقوة مثل ما جاء في ديباجته.

و التقنية الإلكترونية و هي ترتقي لأن تكون وسيلة فعالة لتجسيد و ارتكاب أو لتسهيل ارتكاب بعض الجرائم لا سيما الجرائم ضد الأطفال و جرائم تبييض الأموال و غيرها، فهي من جهة أخرى ارتقت لأن تشكل خطورة أكثر اعتبارا و ذلك في عمليات التجسس التي تقوم بها الأجهزة الاستخبارية للحصول على أسرار و معلومات الدولة و من ثم إفشائها لدولة أخرى تكون عادة معادية أو استغلالها بما يضر المصلحة الوطنية للدولة. و هذا بلا شك يحيلنا إلى جريمة الإبادة خاصة إذا كان الإضرار بالمصلحة الوطنية للدولة يؤدي إلى إلحاق ضرر بشعبها كإخضاعه عمدا لأحوال معيشية يقصد بها إهلاكه كليا أو

جزئيا و ذلك عن طريق تحطيم معطيات اقتصادها بما يؤدي إلى تدهور المستوى المعيشي و تدني القدرة المعيشية و تعميم الفقر و إغراق أغلبية الشعب في الأمراض و المشاكل و هذه إبادة بعينها.

زيادة على ذلك، ارتقت الجريمة الإلكترونية في عصر الازدهار الإلكتروني لأن تبلور جرائم أكثر خطورة كجريمة الإرهاب الإلكتروني التي أخذت أشكالا حديثة تتماشى مع التطور التقني و أصبح الإرهاب الإلكتروني هو السائد في يومنا.

و أصبح اقتحام المواقع و تدميرها و انتحالها و تغيير محتوياتها و إزالتها أو تعطيلها عن العمل هو أسلوب الإرهاب حاليا في محاولة وصول الإرهابيين لتسديد ضرباتهم إلى غيرهم. و بذلك تحولت الإنترنيت إلى منفذ مهم يوظفه الإرهابيون خدمة لمخططاتهم الفكرية و العملياتية سواء من حيث الترويج أو الاتصال و التنسيق و تعلية الفكر العنيف و التحريض على الإرهاب و تحميل ملفات الفيديو المصورة لعمليات تركيب المتفجرات و نسف الجسور و اغتيال الشخصيات و غيرها و كلها لا تقل خطورة على الفعل المادي للإرهاب لأن التحريض على الجريمة هو جريمة.

و من هذا المنطلق فإن الإرهاب الإلكتروني هو في أغلبه حرب متبادلة بين الإرهابي و المقاوم.

بالإضافة إلى إمكانية استغلال وسيلة الإنترنيت لاستعمالها عن طريق الترويج لأدوية باعتبارها تستخدم لحل مشاكل صحية معينة مع إخفاء تأثيراته السلبية التي قد تكون هي المقصودة و التي قد لا يستبعد أن تكون محطمة للقدرات الجنسية و مانعة للإنجاب و كذلك استعمال الإنترنيت لتعزيز جريمة التمييز العنصري التي ترتكبها جماعة عرقية واحدة إزاء أية جماعة أو جماعات عرقية أخرى بنية الإبقاء على نظام تلك الجماعة و هذا ما ورد في ميثاق روما الأساسي للمحكمة الجنائية الدولية.

و نظرا لانعدام أي وجود للإجرام الدولي الإلكتروني كجريمة من الجرائم التي يتناولها القانون الجنائي الدولي، فإننا إن استعملنا هذا المصطلح كعنوان للدراسة فإننا نقصد به السلوك المنحرف أكثر مما نقصد به الفعل المعاقب عليه في القانون الجنائي الدولي. و هو في كل الحالات اعتداء مصيره التجريم لا محالة شأنه شأن جميع الجرائم التي سبقته. إلا أن في هذه المرة هو اعتداء إلكتروني مما جعله يتميز بخصوصيات لا بد من أخذها بعين الاعتبار في دراسته، بل هي الدافع لهذه الدراسة. كما أنه لا يقل شأنا عن الإجرام الدولي عموما من حيث خطورته و تهديده لسلم و أمن البشرية، و لا يعيبه نقص في توفر شروط تجريمه.

أهمية الموضوع :

إن استفحال ظاهرة الإجرام الإلكتروني وتزايد خطورته و توفر وسائل ارتكابه لدى العام و الخاص مع إمكانية الإفلات منه نظرا لتأخر فعالية التشريعات و عدم مواكبتها له، جعلت منه موضوعا مهما ينتظر دائما الإثراء و الدراسة. كما تتجسد هذه الأهمية في كون موضوع الإجرام الإلكتروني أصبح يعني الإجرام الدولي حيث صار مسألة رهيبة تهدد أمن و سلامة البشرية و هو بهذا يستدعي الإثارة أكثر.

و نظرا لاستعداد المخططين لسياسة العدوان على المستوى الدولي، لتبني طرق اعتداء جديدة تمكنهم من تنفيذ مخططاتهم الإجرامية خارج إطار القانون الدولي أي بما لا يعاقب عليه. و منها حالة الاعتداءات الإلكترونية التي لم يصل إلى حد الآن إلى منعها، جعل من موضوع الاعتداءات الإلكترونية ما يثير تساؤلات حول كيفية مكافحته هذا ما زاد من أهمية الموضوع و إفراده بالدراسة.

و باعتبار أن هذه الدراسات قليلة لم تفي إلى استهلاكه، بالمقارنة مع بعض المواضيع القانونية الأخرى، جعل منه موضوعا ذا أهمية كبيرة لمن يريد التطرق إليه. و ما زاد الموضوع أهمية، هو كونه موضوعا شيقا يخرج دارسيه إلى حقل تمتزج فيه اللهجة القانونية مع لهجة علمية تقنية لما يتضمنه من صيغ و عبارات و مصطلحات خاصة.

كل هذه القضايا كانت حافزا لي دفعتني لاختيار هذا الموضوع و أنا أبتغي أهدافا من وراء ذلك منها :

- تسليط الضوء على هذا النوع من الإجرام و ذلك عن طريق :
- التمهيد لطرحه كظاهرة جديدة للجريمة الدولية و التحسيس بخطورتها .
- التعرض لإمكانية تجريمه دوليا.
- محاولة التعرض لكيفية مكافحته و أساس هذه الكيفية.
- كشف خصائصه و الصور و الأشكال التي يأخذها، خاصة الخطيرة منها.
- و في الأخير أهدف إلى إثراء رف مذكرات التخرج في أجنحة المكتبات الجامعية.

الإشكالية :

إذا كانت الجرائم التقليدية ترتكب عادة في العالم الواقعي بمادياته و محدودياته و من ثم يسهل التحكم فيها و ضبطها و أيضا مكافحتها، فترى هل يختلف الأمر بالنسبة لجرائم الإنترنت التي أخذت منحى جد متطور و خاص بل خرجت من العالم الواقعي إلى عالم موازي يسمى العالم الافتراضي متمثل في الشبكات الإلكترونية و على رأسها شبكة الإنترنت، و ما يرتبط بها من تكنولوجيات في مجال الاتصال، التي هي شبكة مفتوحة و عالمية ترشحت لأن تكون وسيلة ترتكب من خلالها جرائم دولية من حيث خطورتها و آثارها فتولد بذلك إجراما دوليا إلكترونيا تخلف القانون الجنائي الدولي في وصفه.

إن كل هذا يثير تساؤلات حول ماهية هذا الإجرام الدولي الإلكتروني من جهة و في هذه الحالة، و إذا كان أصله هو اعتداءات إلكترونية، كيف يمكن تجريمها دوليا. و من جهة أخرى، هل أن خصوصيته تحول دون مكافحته.

و للإجابة على هذه التساؤلات، ارتأينا أن يكون ذلك في فصلين.

نعالج في الفصل الأول ماهية الإجرام الدولي الإلكتروني. و يضم مبحثين نتناول في الأول فكرة الجريمة الدولية و ظواهرها الجديدة، و نتناول في الثاني بعض صور الاعتداءات الإلكترونية التي يمكن أن تشكل جريمة دولية. و في مبحث ثالث، نتكلم عن إمكانية تجريم الاعتداءات الإلكترونية.

أما الفصل الثاني نخصصه لدراسة مكافحة الإجرام الدولي الإلكتروني و يضم مبحثين نتناول في الأول الصعوبات التي تواجه هذه المكافحة، و نخصص الثاني للآليات القائمة لمكافحة الإجرام الدولي الإلكتروني.

و هذا وفق الخطة التالية مستعملين في ذلك تارة المنهج الوصفي و تارة أخرى المنهج المقارن على حسب الضرورة التي تفرضها الدراسة.

الفصل 1
ماهية الإجرام الدولي الإلكتروني

الجريمة هي كل فعل ضار يأتيه الفرد و يكون لهذا الفعل أثر ضار على غيره من الأفراد. غير أن هذا الفعل ليس حكرا على الفرد وحده، و إنما يمكن أن تقترفه الدولة. لكن من الناحية القانونية لا يمكن أن نصف هذا الفعل على أنه جريمة إلا إذا وجد نص قانوني يجرمه، استنادا إلى مبدأ " لا جريمة و لا عقوبة إلا بنص". كما هو صحيح أيضا أن نقول أن كل جريمة هي في أصلها فعل ضار من غير نص قانوني. و عليه، لتفادي مشكلة النص نبدأ بما لا خلاف فيه، و هو أن كل الأفعال الضارة، هي في حقيقتها اعتداء. و نحن نقتصر في بحثنا على الجانب الجزائي، فإن كل فعل اعتداء ارتكبه الفرد أو الدولة، فمصيره التجريم في القانون الجنائي الداخلي أو القانون الجنائي الدولي الذي يشتغل دائما من أجل ذلك.

و من جملة أفعال الاعتداءات التي هي قائمة بشأنها مسألة مستقبلية التجريم خاصة على المستوى الدولي، نجد أفعال الاعتداءات الإلكترونية، التي بحكم طبيعتها، احتلت الصعيدين، الداخلي و الدولي. و لهذا يترقب مستقبلا ظهور ما يسمى بالإجرام الدولي الإلكتروني. فإذا كانت أفعال الاعتداء المعروف ترتكب بين الأفراد و بين الدول أو بين بعضهما مباشرة أو غير مباشرة في عالم واقعي مسموع و مرئي و محسوس في المجال البري و البحري و الجوي، فإن الأمر ليس كذلك بالنسبة للاعتداءات الإلكترونية التي اتخذت من عالم خاص لها لإضفاء بعد فني مثير عليها، لم يتأخر القانون الجنائي الداخلي في تجريمها. كما لم يتوانى القانون الدولي الجنائي هو الآخر في محاولات تجريمها لما اتخذته من بعد دولي لها يهدد مصالح الدول و الشعوب. و نحن نثير ظاهرة الاعتداءات الإلكترونية، ارتأينا أن نسبق بالإشارة إلى فكرة الجريمة الدولية باعتبارها منطلق بحثنا و ذلك بتبيان مفهومها و تناول القانون الجنائي الدولي لها ثم كيف صارت هذه الاعتداءات الإلكترونية يمكن أن تشكل جريمة دولية لننتهي إلى عرض بعض صور الاعتداءات الإلكترونية و الوقوف عند فرضية تجريمها دوليا مبرزين توفر الظروف و حيان ذلك، مقترحين ثلاثة مباحث خصصنا الأول للكلام عن فكرة الجريمة الدولية و عرضنا في الثاني بعض صور الاعتداءات الإلكترونية لنعبر في الأخير عن غاية التجريم الدولي لهذه الاعتداءات الإلكترونية.

1.1 : فكرة الجريمة الدولية و ظواهرها الجديدة

إن تطور العلاقات الدولية و اتساع حجمها، أدى إلى تطور تشكيلة الجماعة الدولية حيث أدى هذا بدوره إلى تطور في تركيبة أشخاص القانون الدولي. و بهذا نشأت علاقات دولية جديدة بمستوى أكثر تعقيدا تحكمها مصالح وقيم جديدة ومن ثم اتسم القانون الدولي الجنائي بالخاصية التطورية نحو فرض حمايته لهذه المصالح والقيم، وذلك من خلال الاتفاقيات الدولية المتتالية [1]. حيث أنه إذا كان الاعتداء على القيم والمصالح التي تهم الجماعة الوطنية، وانتهاكها توصف بأنها جرائم وطنية قرر لها القانون الجنائي الوطني جزاءات معينة كانتهاك حق الإنسان في الحياة والحرية وحق الملكية وغيرها، فإن الاعتداء على مصالح الجماعة الدولية وانتهاكها وصفت على أنها أفعال اعتداءات اهتم القانون الدولي الجنائي بتجريمها ومن ثم سميت جرائم دولية. و رغم قدم فكرة الجريمة الدولية التي ترجع إلى جريمة قانون الشعوب، إلا أنه لا يمكن إعطاء تحديد واضح لماهية الجريمة الدولية ولا حتى تعريف دقيق لها باستثناء محاولات الفقهاء. [2]

لكن هذا لم يكن مانعا أمام القانون الدولي الجنائي من محاولةِ ضبطٍ لبعض أفعال الاعتداءات والانتهاكات الخطيرة وبلورتها حاليا كجرائم دولية، رغم ما عرفه من إشكاليات في ذلك. لكن سرعان ما أصبحت أفعال الاعتداءات والانتهاكات هاته، تأخذ صورا جديدة متحدية القانون الدولي الجنائي ضاربة أبعادا فنية أكثر تدويلا منها ما اصطلح عليها بالاعتداءات الالكترونية وهذا بسبب التطور الهائل و المتسارع في المجال التكنولوجي الالكتروني، وهو لا يزال يتخبط في إرساء قواعده وضبط الجرائم الدولية بمدلولها التقليدي. فكيف حدد مفهوم الجريمة الدولية و كيف استقرت عليه حاليا وكيف صارت الاعتداءات الالكترونية مظهرا جديدا لها.

1.1.1 : مفهوم الجريمة الدولية و إشكالية التجريم

إن تطور القانون الدولي على النحو المتقدم وتغير بناء الجماعة الدولية كان له أثر كبير في تطور مفهوم الجريمة الدولية وتغير مدلولها.

فقد كانت الجريمة الدولية تفهم على أنها الخرق الخطير لقواعد القانون الدولي الذي ترتكبه الدولة عند انتهاكها للسلم والأمن الدوليين لتقع ضد أشخاص القانون الدولي الآخر من الدول فقط، وأبرز هذه الخروق جريمة حرب الاعتداء. فقد حصر عدد من الفقهاء الجرائم الدولية بالجرائم التي تتضمن عنصرا سياسيا فحسب، أي تلك الجرائم التي يرتكبها أفراد بوصفهم أعضاء دولة والتي تشكل أعمال دولة على حد تعبير الأستاذ (كلسن) [1] وتقع ضد السلم والأمن الدوليين أو ضد الاستقلال السياسي أو السلامة الإقليمية لدولة من الدول, و المشرع الجنائي الدولي قد جانب إلى حد ما هذا الطرح معتمدا في ذلك على

المعايير التي أجمعت عليها المجموعة الدولية. غير أن اتجاهها، على عكس ما سلكه الفقه، تضمن ما يشير إلى إمكانية وصف أفعال أخرى و إلحاقها بالجرائم الدولية المحددة.

فما هي إذا محاولات تعريف الجريمة الدولة التي لا يمكن إلا أن تكون فقهية، و كيف و لماذا اقتصر المشرع الدولي في تحديده للجرائم الدولية على أخطرها، ما هي المعايير التي اعتمدها في ذلك، و إلى أي مدى يمكن توسع تعداد الجرائم الدولية.

1.1.1.1 : تعريف الجريمة الدولية

تجدر الإشارة في البداية أنه في نطاق القانون الدولي الجنائي، لا يوجد تعريف للجريمة الدولية، الأمر الذي أعطى المجال للفقه ليسترسل في ذلك واصفا تعريفات متنوعة.

يعرف الفقيه Pella الجريمة الدولية بأنها "كل سلوك محظور يقع تحت طائلة الجزاء الجنائي، الذي ينفذ و يطبق باسم المجموعة الدولية[3] . وعلى ذلك فهو يرى أن الجريمة تكون دولية إذا كانت عقوبتها تطبق وتنفذ باسم الجماعة الدولية، وهذا التعريف يفترض وجود محكمة جنائية دولية تختص بمحاكمة مرتكبي الجرائم الدولية،

فضلا عن وجود قوات بوليس دولية تتولى تنفيذ الأحكام الصادرة عن هذه المحكمة، وهذا ما لم يتحقق حتى الآن. كما عرف الفقيه Saldana الجريمة الدولية بأنها "تلك الجريمة التي يترتب على وقوعها إلحاق الضرر بأكثر من دولة"، وضرب مثالا لذلك بجريمة تزييف العملة التي قد يعد ويدبر لها في دولة ما، وتنفذ في دولة أخرى، ويتم توزيع العملة في دولة ثالثة.

ويرى رمسيس بنهام أن الجريمة الدولية تمثل سلوكا بشريا عمديا يعتبره المجتمع الدولي –ممثلا في غالبية أعضائه- مخلا بركيزة أساسية لكيان هذا المجتمع – أي لقيام التعايش السلمي بين شعوب البشرية- أو بدعامة معززة لهذه الركيزة، ويكون منافيا للضمير البشري العالمي.

ويرى الأستاذ محمد عبد المنعم عبد الخالق أن الجريمة الدولية تتمثل في كونها سلوكا إراديا متعمدا –في الغالب- يصدر من شخص طبيعي أو مجموعة أشخاص، لحسابهم الخاص أو لحساب دولة، أو بمساعدة ورضاء وتشجيع منها، ويمثل اعتداء على مصلحة دولية يوليها القانون الدولي الجنائي عنايته، ويحرص على معاقبة مقترفيها.[2]

كما حصر الفقيه كلسن Kelsen الجرائم الدولية على التي تتضمن عنصرا سياسيا فحسب، أي تلك الجرائم التي يرتكبها افراد بوصفهم أعضاء دولة والتي تشكل أعمال دولة.[1]

وعرفها الاستاذ محي الدين عوض بأنها كل مخالفة للقانون الدولي، سواء كان يحظرها القانون الوطني أو لايحظرها، تقع بفعل أو ترك من فرد يحتفظ بحرية في الاختيار و مسؤول أخلاقيا، إضرارا بالأفراد

أو بالمجتمع الدولي بناء على طلب الدولة أو تشجيعها أو رضائها، ويكون من الممكن معاقبته جنائيا عنها طبقا لأحكام ذلك القانون. [4]

وعرفها الأستاذ حسنين عبيد بأنها سلوك إرادي غير مشروع يصدر عن فرد باسم الدولة أو بتشجيع أو رضاء منها، وبكون منطويا على مساس بمصلحة دولية محمية قانونا.

ويرى Plawski أن الجريمة الدولية تمثل سلوكا غير مشروع معاقبا عليه وفقا لقواعد القانون الدولي، نظرا لإضراره بالعلاقات الإنسانية في الجماعة الدولية.

بينما يرى Lombois ان الجريمة الدولية تتمثل في أفعال مخالفة لقواعد القانون الدولي العام، لانتهاكها المصالح التي تهم الجماعة الدولية، والتي قررت حمايتها بقواعد هذا القانون.[5]

وبذلك فالجريمة الدولية في نظر هؤلاء الفقهاء لا يمكن أن يرتكبها إلا أفراد بوصفهم أعضاء دولة ولا يمكن أن تقع إلا ضد الدول فقط. أما ما عداها من جرائم فقد رمزوا لها بأنها جرائم وطنية تارة أو جرائم عالمية تارة أخرى. غير أنه لا يعني إنكار الصفة الدولية لهذه الجرائم، فهي لا تنتهك بوقوعها مصالح وطنية يحميها القانون الوطني فحسب، بل تتعدى هذا النطاق إلى مصالح وقيم تهم المجموعة الدولية بأكملها.

ومن ناحية أخرى معروف أن القانون الدولي الجنائي هو قانون عرفي، بعد أن فشلت كل المحاولات حتى الآن في تقنينه, ولهذا، فالجرائم الدولية ليست دائما أفعالا منصوصا عليها في قانون مكتوب كما هو الحال في الجرائم الداخلية، بل أن للعرف سبق لتبيانها. ويبقى العرف الدولي مصدر التجريم في الجرائم الدولية حتى ولو نصت المعاهدات الدولية على تجريم بعض الأفعال، باعتبار أن هذه المعاهدات لا تنشئ الجرائم وأنما تكشف عن العرف الذي جرمها. وفي كل الأحوال يتبين لنا بوضوح صعوبة التوصل إلى معرفة الجريمة الدولية وتحديدها تحديدا دقيقا من خلال العرف الدولي أو المعاهدات الدولية أيضا.

2.1.1.1: اقتصار المشرع الجنائي الدولي على أخطر الجرائم الدولية

قد حظيت مسألة تعريف الجريمة الدولية كما سبق الإشارة إليه باهتمام بالغ في الدراسات الفقهية، خاصة الأولى منها، في سعيها إلى تمييز الجريمة الدولية عن بقية أنواع الجرائم، كنقطة ضرورية في كل دراسة يكون الهدف منها التأسيس للقانون الدولي الجنائي كفرع من فروع القانون الدولي.

حيث حاول تعريفها كما رأينا عدد من الأساتذة، مبتعدين في ذلك عن المعطيات الداخلية أو الوطنية التي تعرف بها الجرائم في القوانين الوطنية.

وعلى الرغم من إمكانية تعدد الجرائم الدولية التي يمكن التوصل إليها جراء تطبيق التعريفات السابقة، فإنه من غير الممكن التسليم بأن كل تلك الجرائم هي من الخطورة بمكان إلى درجة يترتب عنها عدم الاعتداد بالصفة الرسمية للمتهم إذ لا يخفى التباين الكبير بينها من حيث درجة هذه الخطورة.

و إلى جانب الاهتمام الفقهي، لم تكن لجنة القانون الدولي بعيدة عن إبراز خطورة بعض الجرائم الدولية، حيث ورد في تقريرها السنوي للدورة التاسعة والثلاثين (39)، أن "هناك إجماع حول معيار الخطورة، فالأمر يتعلق بجرائم تمس أساسا المجتمع البشري نفسه، ويمكن استخلاص الخطورة إما من طابع الفعل المجرم عندما يكون قاسيا، فضيحا و وحشيا، وإما من اتساع آثاره و ضخامتها عندما يكون الضحايا عبارة عن شعوب أو سكان أو إثنيات، وإما من الدافع لدى الفاعل كنية إبادة الأجناس مثلا، وإما من عدة عوامل كهذه. وأيا كان العنصر الذي يتيح تحديد خطورة الفعل، فهذه الخطورة هي التي تكون الركن الأساسي للجريمة المخلة بسلم الإنسانية وأمنها، هذه الجريمة هي التي تتميز بشدة بشاعتها ووحشيتها والتي تقوض أسس المجتمع البشري.[6]

خطورة هذا النوع من الجرائم، كانت الدافع الرئيسي لأغلب المبادرات الدولية التي اتخذت في سبيل إقامة المسؤولية الجنائية لمرتكبي الجرائم الدولية، انطلاقا من اتفاقية فرساي والأنظمة الأساسية للمحاكم العسكرية والمحاكم الجنائية الدولية الخاصة أو المؤقتة، وصولا إلى اتفاقية روما المنشئة للمحكمة الجنائية الدولية الموصوفة بالدائمة. [7]

لذلك إن تقنين الجرائم الدولية ظل حلما يراود البشرية بسبب تردد الجمعية العامة في اتخاذ موقف حاسم بشأنها حتى عام 1989 حيث قامت لجنة القانون الدولي في العام المذكور بفتح هذا الملف مرة أخرى بعد أن طلبت إليها الجمعية العامة إعداد تقرير حول الاختصاص الجنائي الدولي لمكافحة الاتجار بالمخدرات.

وناقشت اللجنة في هذا السياق طبيعة المحكمة الجنائية الدولية المقترحة الأحكام ذات الصلة باختصاصها والإجراءات التي يتعين إتباعها أمامها إلى غير ذلك من المسائل المتعلقة بعمل المحكمة كجهاز قضائي دولي.

وأسفرت مناقشات اللجنة إلى إعداد ثلاثة تقارير، الأول في عام 1992 والثاني في عام 1993 والثالث في عام 1994، والتقرير الأخير هو الذي تبنته الجمعية العامة في عام 1995 واعتمدته في إصدار قرارها المرقم (146/50) الخاص بتشكيل اللجنة التحضيرية المكلفة بإنشاء المحكمة.

كما صدر عن الجمعية العامة القرار (207/51) في 17 ديسمبر 1996 والذي دعت فيه اللجنة التحضيرية إلى الانعقاد خلال عامي 1997-1998 للانتهاء من الصياغة النهائية لمشروع إنشاء المحكمة الجنائية الدولية، توطئه لتقديمه على المؤتمر الدبلوماسي الذي تقرر عقده في العاصمة الإيطالية روما للفترة من 14 يونيه إلى 17 يوليو 1998. [8]

غير أنه قد سبقت ذلك محاولات لضبط الجرائم الدولية عن طريق إنشاء محاكم بالرغم من أنها كانت محاكم خاصة أو مؤقتة أي أنها تولت ولأوائل المرات في التاريخ عن طريق أنظمتها الأساسية مسألة معاقبة بعض المجرمين الذي ارتكبوا انتهاكات ضد الدول أو الأفراد أو الجماعات ووصفت هذه الانتهاكات بالجرائم الدولية.

وتجسد ذلك في محطات رئيسية هي [9]:

- إنشاء المحكمة العسكرية الدولية في نورمبارغ، حيث حددت المادة 06 من قانون إنشائها الجرائم الدولية في الجرائم ضد الإنسانية وجرائم ضد السلام وجرائم الحرب

- تأسيس المحكمة العسكرية الدولية في طوكيو في 1946 وبموجب المادة 05 من لائحة تأسيسها تم تحديد الجرائم الدولية التي تدخل في اختصاصها بأنها جرائم ضد السلام والجرائم ضد الإنسانية والجرائم المرتكبة ضد معاهدات الحرب.

- ثم في سنة 1993 أنشأت المحكمة الدولية الجنائية ليوغسلافيا السابقة، أين عددت م 05 من نظامها الأساسي الانتهاكات الجسيمة للقانون الدولي الإنساني المرتكبة في إقليم يوغسلافيا السابقة وهذه الانتهاكات هي:

- الانتهاكات الجسيمة لاتفاقية لاهاي 1949.
- انتهاك قوانين وأعراف الحرب.
- انتهاك اتفاقية منع والعقاب على جريمة إبادة الجنس البشري لعام 1948.
- الجرائم المناهضة للإنسانية

ونظرا لطبيعة النزاع في رواندا، فإن المادة 01 من النظام الأساسي للمحكمة الجنائية لرواندا تطرقت إلى جرائم الإبادة الجماعية والجرائم ضد الإنسانية كما أشارت المادة 03 منه إلى الانتهاكات المنصوص عليها في المادة 3 من اتفاقيات جينيف 1949 الخاصة بحماية الضحايا في وقت الحرب و البروتوكول الإضافي الملحق بها.

زيادة على هذا فإنه لم يكن الاهتمام بموضوع الجريمة الدولية محصورا في دراسات الفقهاء فقط، و إنما كان للمنظمات الدولية دورا و مساعي هامة في ذلك لما بذلته من محاولات للإلمام بالمبادئ التي يمكن أن تحكم هذه الجريمة من بين هذه المساعي تلك التي أسفر عنها مؤتمر لاهاي الثاني لسنة 1907 من محاولة وضع القواعد الخاصة بفض المنازعات الدولية بالطرق السلمية وقواعد الحرب البرية والبحرية، كما أبرمت في هذا المجال عدة اتفاقات من بينها اتفاقات جنيف الأربع لسنة 1949 والتي قننت قواعد حماية الأسرى والمرضى والجرحى والسكان المدنيين أثناء الحرب، والتي اعتبرت جميعها أن مخالفة أي حكم من أحكامها يعد جريمة حرب.[9]

وفي أول دورة لها سنة 1946، قررت الجمعية العامة تشكيل لجنة خاصة لبحث الوسائل الكفيلة بتشجيع تطوير القانون الدولي وتدوين قواعده، وتألفت هذه اللجنة من ممثلي سبع عشرة دولة، وبعد فترة وجيزة من ممارستها مهام عملها اقترحت إنشاء لجنة للقانون الدولي والتي شكلت فيما بعد من خمسة عشر عضوا من كبار فقهاء القانون الدولي.

وكان من أولويات عمل هذه اللجنة وضع هذه اللجنة وضع مشروع قانون للجرائم ضد أمن وسلامة البشرية، كما تولت بالدراسة موضوع مسئولية الدول عن الأفعال التي تعد دوليا عملا غير مشروع بمقتضى مواثيق دولية من ذلك مثلا مسئولية الدولة الناشئة عن عدم احترامها للحقوق السياسية للإنسان كما ورد النص عليها في الإعلان العالمي لحقوق الانسان.[8]

والملاحظ أن تقنين الجرائم الدولية ظل حلما يراود المجتمع الدولي منذ نهاية الحرب العالمية الثانية حتى صدور نظام روما الأساسي الذي واجه هذا الموضوع من خلال تحديد اختصاصات المحكمة الجنائية الدولية الدائمة[10]. إذ أن طريقة اللجوء إلى إنشاء محاكم جنائية دولية خاصة تحت سلطة مجلس الأمن، تختص بنظر جرائم معينة في مناطق وأوقات محددة، وإن حققت أهدافها من جهة في ملاحقة ومعاقبة المتهمين بارتكاب الجرائم الدولية، كما هو الشأن بالنسبة لمحاكم يوغسلافيا ورواندا وسيراليون. فقد يؤخذ عنها من جهة ثانية، خاصة في ظل الوضع الدولي الراهن –وجود محكمة جنائية دولية دائمة- إضعاف إرادة الدولة في الانضمام إلى النظام الأساسي للمحكمة بسبب تفضيل تلك الطريقة عن توسعة اختصاص المحكمة ليشمل جرائم أخرى. خاصة وأن المادة 13 فقرة ب من النظام الأساسي للمحكمة، تعطي مجلس الأمن صلاحية أن يحيل على المحكمة، وفقا لإجراءات الفصل السابع من الميثاق أية حالة يبدوا فيها أن جريمة واحدة أو أكثر من الجرائم التي تدخل في اختصاص المحكمة قد ارتكبت.

كما أن هذه الطريقة لا توفر الضمانات الكافية لتحقيق الاحترام الدائم للعدالة الدولية، باعتبارها ردة فعل عن ارتكاب جريمة معينة. إضافة إلى توقفها في الغالب على اعتبارات سياسية، ناشئة في الأصل عن كونها تتخذ مبادرة من جهاز سياسي –مجلس الأمن- وبالتالي انعدام الضمانات المسبقة حول إمكانية اللجوء إليها للمعاقبة على جرائم معينة. [7]

إن هذا الارتباط بين إنشاء قضاء جنائي دولي دائم وتقنين قواعد القانون الدولي الجنائي، يعد ارتباطا منطقيا إذ أن من مستلزمات عمل أي محكمة، قانون تقضي بموجبه في المنازعات المعروضة عليها. [8] وهي تتطرق إلى تحديد الجرائم الدولية الأكثر خطورة، أخذ ميثاق روما الأساسي لإنشاء المحكمة الجنائية الدولية في المادة الخامسة بمعيار المصلحة في تحديد الجرائم وهو المعيار المعمول به غالبا في تقسيم الجرائم الدولية والمجمع عليه في المواثيق الدول المختلفة أهمها لائحتي نورمبرغ وطوكيو.

على هذا الأساس فقد ورد في الفقرة الأولى من المادة 5 تحديد لهذه الجرائم على النحو التالي :

1- يقتصر اختصاص المحكمة على أشد الجرائم خطورة موضع اهتمام المجتمع الدولي بأسره، و للمحكمة بموجب هذا النظام الأساسي اختصاص النظر في الجرائم التالية :

(أ) جريمة الإبادة الجماعية.

(ب) الجرائم ضد الإنسانية.

(ج)جرائم الحرب.

(د) جريمة العدوان.

انتهى نص الفقرة.

حتى وإن كانت بعض الجرائم لا تقل خطورة عن تلك التي تضمنتها المادة 5 من اتفاقية روما، إلا أنها لم تدرج ضمن اختصاص المحكمة، بالنظر إلى اعتبارات مختلفة، منها، التقليل من نقاط الخلاف حتى يسهل دراسة بقية المسائل الجوهرية في إنشاء المحكمة، تشجيع أكبر عدد من الدول على قبول النظام الأساسي للمحكمة ومن ثم تعزيز مصداقيتها وفعاليتها، تفادي إثقال كاهل المحكمة بالنظر في جرائم يمكن الملاحقة عليها أمام المحاكم الوطنية و الاتفاق على إمكانية توسيع اختصاص المحكمة مستقبلا.

و خلاصة لما سبق، أنه إذا كان من جملة النتائج المباشرة لحداثة القانون الدولي الجنائي، صعوبة تحديد المفاهيم الأساسية التي يقوم عليها هذا النوع من فروع القانون الدولي العام، كمسألة تعريف الجريمة الدولية التي تكتسي بعض الخصائص الذاتية و القانونية، القانونية، تجعلها تتشابه في نقاط معينة و تتميز في نقاط أخرى عن بقية أنواع الجرائم، كالجريمة الداخلية و الجريمة السياسية. و مهما كانت نقاط التشابه أو الاختلاف التي يمكن حصرها، إلا أنه من جهة أخرى استطاع إلى حد ما، تكريس مبدأ الخطورة العالية التي ينبغي أن تتميز بها الجريمة الدولية[6]. إذ لا يقتصر معيار خطورة الجرائم الدولية على تمييزها عن بقية أنواع الجرائم الأخرى، و إنما ينصرف أيضا إلى ترتيب الجرائم الدولية نفسها من الأشد خطورة إلى الأقل خطورة، و ما قد يترتب عن ذلك من تركيز الجهود الدولية على البعض منها دون البعض الآخر، و من ثم تباين أثرها في تطور و تكريس المبادئ الأساسية للقانون الدولي الجنائي.

و من ثم لم ينحصر التطور الذي ميز القانون الدولي الجنائي طيلة القرن الماضي فالعمل على إحداث تنظيم هيكلي خاص توج بإنشاء محكمة جنائية دولية دائمة، أو تكريس مجموعة من المبادئ العامة التي يرتكز عليها هذا القانون، كما وردت في الباب الثالث من نظام روما الأساسي. إذ ميزه أيضا التوسع الكبير في قائمة الجرائم الدولية، التي تضمنتها مختلف الوثائق الدولية ذات الصلة بالموضوع، على الرغم من الصعوبات التي حالت في البداية دون إمكانية استخدام مصطلح الجريمة لوصف بعض الانتهاكات الدولية، بالنظر إلى عدم تناسبه مع التركيبة الأفقية للمجتمع الدولي، الذي يعاني من غياب سلطة دولية كفيلة بفرض احترام قواعد القانون الدولي. مقارنة بالتنظيم الذي بلغته المجتمعات الوطنية،

في شكل عمودي أو هرمي، يضمن فرض احترام القانون عن طريق توقيع الجزاء على من يتجرأ على مخالفة أحكامه.[7]

3.1.1.1 : المعايير المعتمدة في تحديد أخطر الجرائم الدولية

نظرا لعدم كفاية الاعتبارات السابقة –تعريف الجريمة الدولية والمعايير المستخلصة من اتفاقيات الدولية- في وضع تعريف دقيق للجريمة الدولية، يحدد عناصرها بشكل يسهل معه إثبات ارتكاب شخص ما لجريمة معينة. أمام قناعة الدول بضرورة حصر الجهود الدولية في المتابعة على أخطر الجرائم الدولية. وضعت خلال الأشغال التحضيرية لمفاوضات روما معايير تسمح مراعاتها بتحديد الجرائم الأشد خطورة، ومن ثمة إيجاد المبرر الكافي لإدراجها ضمن اختصاص المحكمة، نوجزها فيما يلي :

- أن تلحق المعنية الضرر بمصالح البشرية كلها : إذا كانت الجرائم الدولية تتشابه في مجملها من حيث كونها عبارة عن سلوك مخالف لقواعد القانون الدولي، وفق ما هو مبين في التعريفات السابقة، فإن التباين فيما بينها يظهر بوضوح من خلال النتائج والآثار المترتبة عنها. وهي نظرة يصح الأخذ بها في مجال التمييز بين الجرائم الدولية، إذ تكشف عن نوع من التسلسل الهرمي بين الجرائم الدولية تبعا لخطورتها. وقد حاولت لجنة القانون الدولي أن تبرر الطابع الخطير لبعض الأفعال التي يمكن إدراجها ضمن فئة الجرائم الدولية، حينما قررت في دورة عام 185 أنه : "يبدو من المناسب أن نضيف أيضا أن الدول لا تعتبر انتهاكات الالتزامات المشار إليها داخلة في فئة الجرائم الدولية إلا إذا كانت تتضمن في ذاتها درجة معينة من الخطورة.

- أن تعتبر الأفعال المعنية جرائم بموجب مبادئ القانون الدولي الجنائي : على ضوء التجارب العملية التي أفرزتها محاكمات نورنبرغ وطوكيو، والتي شكلت مادة علمية حقيقية لم يتوان المجتمع الدولي في السعي نحو تقنينها في شكل مجموعة من المبادئ الأساسية، بعد إدراك أهميتها القانونية في إرساء دعائم القانون الدولي الجنائي. ورد من بين مجموعة المبادئ الأساسية التي فننها لجنة القانون الدولي وفق ما تم استخلاصه من محاكمات نرونبرغ، نص المادة 6 التي حددت الجرائم الدولية في الجرائم ضد السلام التي أصبحت تعرف لاحقا بجريمة العدوان، وجرائم الحرب، والجرائم ضد الإنسانية. إضافة إلى جريمة إبادة الجنس التي وردت الإشارة لها باعتبارها جريمة من جرائم القانون الدولي ضمن نفس قرار الجمعية العامة المحدد للمبادئ الأساسية للقانون الجنائي، ليتأكد الإجماع عليها مجددا بعد تبني اتفاقية الأمم المتحدة لمنع جريمة الإبادة والمعاقبة عليها في تاريخ 9 ديسمبر 1948 [6] . ومن هذا المنطلق انصرفت جميع جهود المجموعة الدولية إلى التركيز على الجرائم الأربع، باعتبارها تحظى بإجماع دولي كونها جرائم دولية بموجب مبادئ القانون الجنائي المعترف بها دوليا. حيث ورد النص عليها في المواد 16 (جريمة العدوان) و 17 (جريمة الإبادة) و18 (الجرائم ضد الإنسانية) و 20 (جرائم

الحرب) من مشروع الجرائم المخلة لسلم وأمن البشرية. كما ورد النص عليها في المواد من 2 إلى 5 من النظام الأساسي لمحكمة يوغسلافيا، والمواد من 2 إلى 4 من النظام الأساسي لمحكمة رواندا. إضافة إلى إدراجها في نص المادة 5 المحدد للجرائم الداخلة في اختصاص المحكمة.

- أن تنطوي مكافحة هذه الجرائم على التعاون فيما بين الدول : نظرا لتجاوز مهمة مكافحة الجرائم الدولية حدود إمكانيات الدولة الواحدة، لما تحتويه من خطورة بالغة أو تداخل عدة عناصر أجنبية فيها، كتعدد أو اختلاف جنسية الضحايا و الجناة أو ارتكابها على إقليم أكثر من دولة. تتخذ مسألة التعاون الدولي في تعقب ومكافحة مرتكبي أخطر الجرائم الدولية أهمية قصوى على صعيد العلاقات الدولية، غالبا ما تظهر في شكل تكريس التزام دولي بضرورة اتخاذ التدابير القانونية المناسبة على المستوى الوطني لمتابعة الجناة أو واجب تسليمهم إلى الجهات القضائية المختصة أو الإحالة على محكمة جنائية دولية. وأفضل دليل على قيمة التعاون الدولي في مجال مكافحة أخطر الجرائم الدولية، تخصيص الباب التاسع من النظام الأساسي للمحكمة الجنائية الدولية لواجب التعاون الدولي والمساعدة القضائية.

4.1.1.1 : التوسع المحتمل في تعداد الجرائم الدولية

تماشيا مع التوجه العام بقصر اختصاص المحكمة على جرائم معينة، ورد في المادة 1 من نظام روما الأساسي، تأكيد على أن المحكمة تمارس "...اختصاصها على الأشخاص إزاء أشد الجرائم خطورة موضع الاهتمام الدولي، وذلك على النحو المشار إليه في هذا النظام الأساسي[11]. حيث ورد في المادة 5 أن اختصاص المحكمة يقتصر على جريمة الإبادة الجماعية، الجرائم ضد الإنسانية، جرائم الحرب، وجريمة العدوان، باعتبارها من أخطر الجرائم وأنها تحظى بإجماع دولي. إلا أنه ينبغي الإشارة إلى أن هناك جرائم تستوفي معيار الخطورة ولم يتم إدراجها في اختصاص المحكمة، كجرائم الإرهاب والاتجار بالمخدرات، التي أشير لها في القرار هاء الملحق بالوثيقة الختامية للمؤتمر، على أن يتم بحثها لاحقا خلال المؤتمر الاستعراضي الذي عقده لبحث تعديل النظام الأساسي، بما في ذلك الجرائم الداخلة في اختصاص المحكمة وفقا للمادة 123 [11]

غير أن جهود الفقهاء لم تتوانى في النظر في إمكانية توسع تعداد الجرائم الدولية و من أهم المحاولات في هذا الصدد ما توصل إليه الأستاذ شريف بسيوني، من خلال دراسته لـ 128 وثيقة دولية تخص القانون الدولي الجنائي و تصل إلى غاية سنة 2002، استنتج من خلالها عشرة معايير أو خصائص تمكن من معرفة ما إذا كانت الوثيقة الدولية تعالج موضوعا من مواضيع القانون الدولي الجنائي. و من ثمة إمكانية تحديد الجريمة الدولية التي تنظمها الوثيقة المعنية،[12] هذه الأدلة هي :

أ- الاعتراف الصريح بأن الفعل المحظور يشكل جريمة طبقا للقانون الدولي، أو أنه جريمة دولية

ب- الاعتراف الضمني بالطابع الجنائي للفعل، عن طريق الدعوة إلى ضرورة تجريمه، والوقاية منه، بالمتابعة والقمع أو باتخاذ تدابير مماثلة .

ت- تجريم السلوك الممنوع.

ث- تكريس الالتزام أو الحق في المتابعة القضائية.

ج- تكريس الالتزام أو الحق في قمع السلوك الممنوع

ح- تكريس الالتزام أو الحق في مباشرة إجراءات تسليم المجرمين.

خ- وضع التزام أو واجب في متابعة ومعاقبة المجرمين، وكذلك آليات التعاون القضائي.

د- الاعتراف بالاختصاص الجنائي.

ذ- الإحالة على اختصاص محكمة جنائية دولية.

ر- استبعاد تلقي أوامر الرؤساء كسبب أو عذر مخفف للعقوبة

استنادا على هذه المعايير التي طبقها الأستاذ شريف بسيوني على مجموعة الوثائق الدولية ذات الصلة بالقانون الدولي الجنائي، تمكن من إحصاء 28 جريمة دولية، هي 1- جريمة العدوان. 2-جريمة الإبادة 3-الجرائم ضد الإنسانية \. 4-جرائم الحرب. 5-الاستعمال والإنتاج والتخزين غير المشروع لبعض الأسلحة 6-سرقة المواد النووية 7-المرتزقة 8-الأبرتايد 9-الرق والممارسات الشبيهة بالرق 10-التعذيب وكافة ضروب المعاملة القاسية أو المهينة أو اللاإنسانية 11-الاستغلال الإنساني الامشورع 12-القرصنة. 13-المساس بأمن الملاحة الجوية الدولية 14-المساس بأمن الملاحة البحرية والمنشآت القاعدية في البحار. 17-احتجاز الرهائن. 18-الاستعمال غير المشروع للوسائل البريدية 19-جرائم استعمال وتفجير المفرقعات. 20-تمويل الإرهاب. 21-جرائم زراعة وإنتاج والمتاجرة بالمخدرات 22-الجريمة المنظمة العابرة للقارات 23-سرقة وتدمير الكنوز الأثرية وممتلكات الثقافة الوطنية. 24-الجرائم المتعلقة بالبيئة 25-المتاجرة الدولية في المواد المخلة بالحياء. 26-تزييف العملة. 27-قطع الكوابل في أعماق البحار. 28-رشوة موظفين عموميين أجانب.

2.1.1 : الاعتداءات الإلكترونية كظاهرة يمكن أن تشكل جريمة دولية

تعد الاعتداءات الإلكترونية إحدى الأفعال التي تمس الأشخاص و الأموال و تلحق بها أضرارا كبيرة. وهي لم تتوقف عند هذا الحد، بل تعدته إلى المستوى الدولي، و هي تمارس شيئا فشيئا من خطير إلى أخطر وفقا لثلاثة عوامل أساسية و هي الأرضية الملائمة و المساعدة ثم أغراض و محفزات ممارسيها و أيضا ميل المجرمين و المنظمات الإجرامية إلى اعتمادها.

فمن حيث الأرضية المساعدة، نجد أن هذه الاعتداءات تتخذ من الفضاء الإلكتروني مسرحا مبيتا لها، هذا الفضاء يتمثل في وسائل الاتصالات السلكية و اللاسلكية الحديثة من طرق الاتصال التي تشتغل

مع الشبكة العالمية، الإنترنت و كل ما يلحق بها من تكنولوجيا حديثة. أما من حيث أغراض و محفزات ممارسيها، فنجد أن هؤلاء الأخيرين في بحث مستمر عن طرق ارتكاب أفعالهم بما يحقق أهدافهم أكثر و في مأمن مريح. و هم بتوجههم هذا، تمكنوا من إصباغ الكثير من هذه الأفعال الجنائية بصبغة فنية و إعطائها طابعا تقنيا حتى انتهوا إلى الأخطر منها الذي هو من قبيل الإجرام الدولي. فأدى هذا الطابع بالمجرمين و المنظمات الإجرامية إلى اعتماده لما فيه من مكاسب و مآمن هامة.

و نأتي لتفصيل هذه الجوانب في الفروع التالية :

1.2.1.1 : مسرح الاعتداءات الإلكترونية

إن صفة الإلكترونية تشير إلى البنية الأساسية العالمية للحاسبات و تكنولوجيات الاتصالات و الشبكات التي يجري عن طريقها معالجة و نقل البيانات الرقمية. و الإنترنت هي شبكة اتصالات عالمية مفتوحة و عامة واسعة النطاق تربط بين عدد ضخم من الشبكات الفرعية. و لذا يطلق عليه شبكة الشبكات. و لعل صفة مفتوحة و عامة هي أهم ما يميز الإنترنت عن غيرها من الشبكات و ذلك فضلا عن تعدد الوظائف التي يمكن أن تقوم بها. إذ أن العالم عرف من قبل، و لعدة عقود سابقة، الشبكات الخاصة المغلقة المملوكة لشركة أو مجموعة شركات، و التي تستخدم لأغراض محددة و تدار كلية لخدمة أصحابها دون غيرهم كالبنوك و شركات الطيران و ما إليها. و لذا يطلق عليها الشبكات المملوكة ملكية خاصة. و هي تستخدم بروتوكولات أي برامج أو نظم خاصة بها لنقل البيانات.

و الجديد في الإنترنت هي أن الاتصالات و المعاملات تتم عبر شبكة مفتوحة بين عدد يمكن أي يكون لا نهائيا من المشتركين الذين قد لا يكون قد سبق لهم إجراء أي اتصال أو تعامل من قبل. و المقصود بالشبكة المفتوحة هو شبكة تربط بين مجموعة كبيرة من الحاسبات و تنقل البيانات فيما بينها، باستخدام بروتوكولات عامة أي غير مخصصة لجهة بعينها، أو غير مسيطر عليها من جانب طرف بعينه و هو ما يطلق عليه TCP/IP كما تستخدم الإنترنت نظاما نمطيا لتكويد Codage البيانات أي لتحويلها إلى بيانات رقمية يطلق عليه HTML و يجري الاتصال فيما بين الحاسبات أو المواقع عبر الشبكة بطرق سلكية أو لا سلكية أشهرها حتى الآن خطوط التليفونات. و في بعض الأحيان يمكن استخدام خطوط نقل القوى الكهربائية كما سيمكن استخدام الألياف الضوئية في اتصال قطاع واسع من المستخدمين بالشبكات، و كذلك عن طريق نظم الاتصالات بالأقمار الصناعية. [13]

فيمثل هذا عالما افتراضيا موازيا للعالم الواقعي هو بمثابة مسرح مميز تمارس فيه، عن طريق ما يقدمه من فرص آمنة يستغلها المجرمون متجنبين ملاحقة سلطات التحقيق لتحقيق أغراضهم الإجرامية.

2.2.1.1 : الأبعاد الفنية للأفعال الجنائية و للجريمة الدولية

لقد صارت الأفعال الجنائية المرتكبة لها أبعاد فنية و طرق مستجدة و ذلك عن طريق استخدام التقنية. فمنها ما هي في أصلها تمثل جرائم تقليدية و منها ما يدخل في إطار ممارسات غير مشروعة من شأنها أن تلحق ضرر بالفرد أو الدولة و تهددهما في أمنهما و سلامتهما، بل أن منها ما يرقى إلى أن يكون جريمة دولية في صورة حديثة. و في كل الحالات فإن هذه الأفعال إما أنها مجرمة في صورتها التقليدية و إما أنها تجد ما يجرمها في العرق أو الديانات و غيرها. و في ما يلي بعض هذه الأفعال التي أخذت بعدا فنيا و طابعا تقنيا.

أ- الممارسات غير الأخلاقية : و تتعدد مجالاتها كما يلي :

1- الممارسات التي مسرحها المواقع الإباحية

و يدخل فيها ارتياد المواقع الإباحية، الشراء منها، الإشتراك فيها أو إنشائها و قد أصبح الإنتشار الواسع للصور و الأفلام الإباحية على شبكة الإنترنت يشكل قضية اهتمام عالمي في الوقت الراهن، و بسبب الإزدياد الهائل في أعداد مستخدمي الإنترنت حول العالم واستفادت هذه المواقع والقوائم من الانتشار الواسع للشبكة والمزايا الأخرى التي تقدمها حيث " تتيح شبكة الإنترنت أفضل الوسائل لتوزيع الصور الفاضحة والأفلام الخليعة بشكل علني فاضح يقتحم على الجميع بيوتهم ومكاتبهم، فهناك على الشبكة طوفان هائل من هذه الصور والمقالات والأفلام الفاضحة بشكل لم يسبق له مثيل في التاريخ"، فكل مستخدم للانترنت معرض للتأثر بما يتم عرضه على الإنترنت الذي لا يعترف بأي حدود دولية أو جغرافية فهو يشكل خطرا حقيقيا للأطفال فضلا عن الكبار نتيجة تأثيراته المؤذية وغير المرغوبة و هي بهذا يهدد كرامة الإنسان التي هي حق من حقوقه الأساسية اللاصقة فيه. كما تعرض الأطفال للخطر في سن ليسوا مسؤولين فيه عن أنفسهم خاصة لما اتضح أن أكثر مستخدمي المواد الإباحية تتراوح أعمارهم ما بين 12 و 15 سنة في حين تمثل الصفحات الإباحية أكثر صفحات الإنترنت بحثا و طلبا في على مختلف مواقعها التي يقدر عددها بحوالي 70.000 موقع. و مع تحايل و انحراف الكبار في استخدام و ارتياد هذه المواقع في بعض الحالات، صار ينال من كرامة هؤلاء الأطفال مما طرح في العالم مصيبة عظيمة و أمرا شنيعا و خطيرا سمي فيما بعد بجرائم الأحداث أو جرائم ضد الأطفال، أين قامت هيئات دولية و وطنية كثيرة و أبرمت اتفاقيات و معاهدات دولية من أجل حمايتهم.

2- أفعال القذف و تشويه سمعة الأشخاص :

تعمل هذه المواقع على إبراز سلبيات الشخص المستهدف ونشر أسراره، والتي قد يتم الحصول عليها بطريقة غير مشروعة بعد الدخول على جهازه، أو بتلفيق الأخبار عنه. وهناك حادثة مشهورة جرى تداولها بين مستخدمي الإنترنت في بداية دخول الخدمة للمنطقة حيث قام شخص في دولة خليجية

بإنشاء موقع ونشر صور إحدى الفتيات وهي عارية وفي أوضاع مخلة مع صديقها، وقد حصل علي تلك الصور بعد التسلل إلى حاسبها الشخصي وحاول ابتزازها جنسيا ورفضت فهددها بنشر تلك الصور على الإنترنت وفعلا قام بتنفيذ تهديده بإنشاء الموقع ومن ثم وزع الرابط لذلك الموقع على العديد من المنتديات والقوائم البريدية وأدى ذلك إلى انتحار الفتاة حيث فضحها بين ذويها ومعارفها.

وحوادث التشهير والقذف في شبكة الإنترنت كثيرة فقد وجد ضعفاء النفوس في شبكة الإنترنت، وفي ظل غياب الضوابط النظامية والجهات المسئولة عن متابعة السلبيات التي تحدث أثناء استخدام الإنترنت، متنفَسا لأحقادهم ومرتَعا لشهواتهم المريضة دون رادع أو خوف من المحاسبة وقد قيل قديما "من أمن العقوبة أساء الأدب".

والقذف في صورته التقليدية مُجَّرم شرعا و قانوناً، نظرا لشناعة الجرم ومدى تأثيره السلبي على المجنى عليه والمجتمع كونه يساعد على إشاعة الفاحشة بين الناس بكثرة الترامي به.

هذه بعض الممارسات غير الأخلاقية و في الحقيقة هي كثيرة و في اتساع و انتشار و ذلك لما 4تعرفه شبكة الإنترنت من تقدم و تطور في خدماتها.

3- زرع الفيروسات :

الفيروسات الحاسب الآلية هي إحدى أنواع البرامج الحاسب الآلية إلا أن الأوامر المكتوبة في هذه البرنامج تقتصر على أوامر تخريبية ضارة بالجهاز ومحتوياته، فيمكن عند كتابة كلمة أو أمر ما أو حتى مجرد فتح البرنامج الحامل لفيروس أو الرسالة البريدية المرسل معها الفيروس إصابة الجهاز به ومن ثم قيام الفيروس بمسح محتويات الجهاز أو العبث بالملفات الموجودة به. و الفيروسات عدة أنواع[14]:

الأول: فيروسات الجزء التشغيلي للاسطوانة كفيروس (Brain) و(Newzeland)

الثاني: الفيروسات المتطفلة كفيروس (Cascade) وفيروس (Vienna).

الثالث: الفيروسات المتعددة الانواع كفيروس (Spanish-Telecom) وفيروس (Flip)

الرابع: الفيروسات المصاحبة للبرامج التشغيلية (exe) سواء على نظام الدوسDOS أو الوندوز WINDOWS

الخامس: يعرف بحصان طروادة وهذا النوع يصنفه البعض كنوع مستقل بحد ذاته، وينسب هذا النوع إلى الحصان اليوناني الخشبي الذي استخدم في فتح طروادة حيث يختفي الفيروس تحت غطاء سلمي إلا أن أثره التدميري خطير.

وقد أصبحت الفيروسات سلاحا تهديديا فعالا يستعمله الأعداء لتلبية رغباتهم وتمكنوا من ذلك في عدة حالات منها على سبيل المثال ما تسبب فيه فيروس في إصابة شبكة كاملة من الحاسبات الشخصية لوزارة الدفاع البريطانية و ذلك في أحد قواعدها بمدينة بريستول في سنة 2003.[14]

كما أخذت كل من جريمة غسيل الأموال و تجارة المخدرات منحى متقدما لما صار الفضاء الإلكتروني أو العالم الافتراضي مسرحا لممارستهما و قد برز ذلك أساسا عبر شبكة الإنترنت لما تحتويه من مواقع مخصصة لذلك و التي لا تتعلق فقط بالدعوة إلى غسيل الأموال أو الترويج للمخدرات والتشويق لها و تناولها، بل تتعداه في حالة هذه الأخيرة إلى تعليم كيفية زراعة وصناعة المخدرات بكافة أصنافها وأنواعها و بأبسط الوسائل المتاحة.

بينما غسيل الأموال الذي هو مصطلح حديث نسبيا بدأ استخدامه في أمريكا نسبة إلى مؤسسات الغسيل التي تملكها المافيا. اتخذ هو الآخر مما توصلت إليه التقنية بعدا فنيا خدمة للمجرمين النشطين في هذا المجال فلجؤوا إلى الإنترنت لتوسعة وتسريع أعمالها في غسيل أموالهم غير المشروعة. ومن المميزات التي يعطيها الإنترنت لعملية غسيل الأموال السرعة، إغفال التوقيع و انعدام الحواجز الحدودية بين الدول، كما تساهم البطاقات الذكية، والتي تشبه في عملها بطاقات البنوك المستخدمة في مكائن الصرف الآلية، في تحويل الأموال بواسطة المودم أو الإنترنت مع ضمان تشفير وتأمين العملية.

ورغم اهتمام دول العالم قاطبة بمكافحة غسيل الأموال و المخدرات وعقدت المؤتمرات والاتفاقيات الدولية المختلفة على المستوى الدولي و الإقليمي، إلا أن التقنية حالت دون ذلك.

و حتى نصل عن طريق هذا التدرج إلى إبراز مدى خطورة الأبعاد الفنية للأفعال الجنائية التي تجعل هذه الأخيرة من مستوى جرائم دولية عصرية لا يستهان بها أبدا، نشير إلى أن الاتجاه بالكلام نحو الجريمة الدولية يضطرنا إلى أن نتحرر قليلا من قداسة النص القانوني المكتوب بما يسمح إلى حد ما بالجرأة على تجريم أفعال الاعتداءات الدولية بجميع صورها، باعتبار أن القانون الذي يحكمها هو القانون الدولي الجنائي ذي المصدر الأساسي المتمثل في العرف ثم المعاهدات و الاتفاقيات الدولية. لكن وصف الجريمة الدولية بأنها جريمة عرفية جعلها تتسم بالغموض و عدم التحديد. و إذا كان أشهر الفقهاء تناولوا مفهوم الجريمة الدولية واجتهدوا في وضع تعريف لها، و منهم الفقهاء، Pella و Glasser و Blaousski حيث أنها تعرف في نهاية المطاف بأنها " كل عمل أو امتناع عن عمل يصيب المصالح الدولية أو الإنسانية الكبرى بضرر يمنعه العرف الدولي و يدعو إلى المعاقبة عليه باسم المجموعة الدولية [6] ، فإن الاعتداءات الإلكترونية التي من أهم خصائصها تخطيها للحدود الجغرافية و من ثم اكتسابها طبيعة دولية أو كما يطلق عليها البعض أنها أفعال اعتداء ذات طبيعة متعدية الحدود بفضل ظهور التقنية الجديدة في الاتصالات المتمثلة في شبكة المعلومات العالمية الإنترنت بتكنولوجياتها الملحقة، و ما تشكله من مسرح إلكتروني ترتكب فيه هذه الجريمة كما رأينا، مما أدى إلى أن أماكن متعددة في دول مختلفة قد تتأثر بالعدوان الإلكتروني، الشيء الذي يمكن من تقابل المصالح الدولية و الإنسانية فوق هذا المسرح. و بعد هذه الإمكانية نستطيع تصور وقوع جميع الاعتداءات و الجرائم سواء التقليدية منها التي أخذت بعدا فنيا بسبب هذه التقنية، أو الحديثة التي مكنت منها.

و الأخطر أن الاعتداءات الإلكترونية ارتقت في بعض الحالات إلى مستوى عالمي من الإجرام الدولي تماما مثل الذي فصله نظام روما الأساسي للمحكمة الجنائية الدولية، الذي كان بمثابة إرساء محاولات مكافحة الجرائم الدولية الخطيرة التي أوقعت ملايين الأطفل و النساء و الرجال ضحايا لفظائع لا يمكن تصورها هزت ضمير الإنسانية بقوة مثل ما جاء في ديباجته.

و الاعتداءات الإلكترونية و هي ترتقي لأن تكون وسيلة فعالة لتجسيد و ارتكاب أو لتسهيل ارتكاب بعض الجرائم لا سيما الجرائم ضد الأطفال و جرائم تبييض الأموال و غيرها، فهي من جهة أخرى ارتقت لأن تشكل خطورة أكثر اعتبارا و ذلك في عمليات التجسس التي تقوم بها الأجهزة الاستخبارية للحصول على أسرار و معلومات الدولة و من ثم إفشائها لدولة أخرى تكون عادة معادية أو استغلالها بما يضر المصلحة الوطنية للدولة.

إن هذا بلا شك يحيلنا إلى جريمة الإبادة خاصة إذا كان الإضرار بالمصلحة الوطنية للدولة يؤدي إلى إلحاق ضرر بشعبها كإخضاعه عمدا لأحوال معيشة يقصد بها إهلاكه كليا أو جزئيا و ذلك عن طريق تحطيم معطيات اقتصادها بما يؤدي إلى تدهور المستوى المعيشي و تدني القدرة المعيشية و تعميم الفقر و إغراق أغلبية الشعب في الأمراض و المشاكل و هذه إبادة بعينها.

زيادة على ذلك، ارتقت الاعتداءات الإلكترونية لأن تبلور جرائم أكثر خطورة كجريمة الإرهاب الإلكتروني التي أخذت أشكالا حديثة تتماشى مع التطور التقني و أصبح الإرهاب الإلكتروني هو السائد في يومنا.

و أصبح اقتحام المواقع و تدميرها و انتحالها و تغيير محتوياتها و إزالتها أو تعطيلها عن العمل هو أسلوب الإرهاب حاليا في محاولة وصوا الإرهابيين لتسديد ضرباتهم إلى غيرهم. و بذلك تحولت الإنترنيت إلى منفذ مهم يوظفه الإرهابيون خدمة لمخططاتهم الفكرية و العملياتية سواء من حيث الترويج أو الاتصال و التنسيق و تعلية الفكر العنيف و التحريض على الإرهاب و تحميل ملفات الفيديو المصورة لعمليات تركيب المتفجرات و نسف الجسور و اغتيال الشخصيات و غيرها و كلها لا تقل خطورة على الفعل المادي للإرهاب لأن التحريض على الجريمة هو جريمة.

3.2.1.1 : الاعتداءات الإلكترونية و الجريمة المنظمة

تعتمد اليوم الكثير من المؤسسات سواء الرسمية منها كالحكومات و مختلف الأجهزة في الدولة، أو المؤسسات الموازية الأخرى كالمؤسسات التجارية و الصناعية على التقنية الحديثة في مجال الاتصالات، حيث بدأت حكومات ومؤسسات تجارية عديدة، كما بدأ الكثير من الناس حول العالم إدراك كيفية الاستخدام الأفضل لأحدث تكنولوجيات الاتصال. لكن جماعات الجريمة المنظمة اكتشفت أيضاً استخدام هذه التكنولوجيات بصفتها فرص للاستغلال وتحقيق أرباح غير مشروعة.

إن القدرات والفرص التي تؤمنها شبكة الإنترنت طورت العديد من النشاطات المشروعة. كما اكتشف المجرمون أيضاً أن شبكة الإنترنت تستطيع أن تؤمن فرصاً جديدة وفوائد متضاعفة للأعمال غير المشروعة. فالجانب المظلم من الإنترنت لا يشمل فقط الاحتيال والسرقة، ونشر المواد الإباحية، وشبكات المنحرفين جنسياً ممن يستهدفون الأحداث، بل أيضاً منظمات الاتجار بالمخدرات والمنظمات الإجرامية التي تُركز على استغلال ما توفره الشبكات الإلكترونية من تسهيلات وفرص.

فسواء في العالم الافتراضي أو في العالم الحقيقي، غالبا ما ترتكب الجرائم من قبل أفراد أو مجموعات صغيرة في إطار غبر منظم و من غير تخطيط، كما يمكن لهؤلاء الأفراد أو المجموعات استغلال ما يوفره العالم الافتراضي من فرص في مجال تقنيات الاتصال. لكن إذا تعلق الأمر بمجموعات الجريمة المنظمة، و إن ظلت تواصل ممارسة الإجرام في العالم الحقيقي، إلا أن درجة التداخل بين الفعل الإجرامي و الوسيلة، قد تصل إلى طغيان دور الوسيلة على الفعل في حد ذاته من حيث النتيجة الإجرامية. و في هذه الحالة قد يصبح الفعل يوصف بالوسيلة.

و كون أن المنظمات الإجرامية تتوفر على مهارة كبيرة في اكتشاف و استغلال فرص القيام بأعمال و مشاريع جديدة غير مشروعة، فإنها وجدت في ما يوفره العالم الافتراضي بصفة عامة و شبكة الإنترنت بصفة خاصة تلك الفرص لتحقيق أرباح غير مشروعة الشيء الذي انتشارها على نطاق واسع و كبير.

ففي البداية أخذت المنظمات الإجرامية تزيد من توظيف اختصاصيين ماليين كما استخدمت خبراء قانونيين وماليين عارفين بخفايا المعاملات المالية لتوفير ملاذات آمنة في أماكن ومؤسسات تعمل بطريقة الأوف شور. ثم انتهت إلى استخدام أشخاصاً من الخبراء في عمل الشبكة واستغلال مكامن الضعف فيها لتنفيذ المهمات الموكلة إليهم بفعالية وكفاءة.

ثم إن مجموعات الجريمة المنظمة تترصد ظروفا خاصة من أجل القيام بعملياتها الإجرامية العابرة للحدود بأقل قدر من المخاطر، حيث كانت لها في شبكة الإنترنت حظوظا كبيرة لأن في هذا العالم الافتراضي، أي عالم الشبكات الإلكترونية، لا توجد أي حدود، فيشكل ذلك مزية تجعل النشاط الإجرامي عملاً جذاباً للغاية. حيث عندما تحاول السلطات المختصة مراقبة هذا العالم الافتراضي تبدو أمامها حدود البلدان ومناطق الصلاحيات واسعة جداً، ما يجعل التحقيق في الجرم بطيئاً جداً في أحسن الأحوال، أو مستحيلاً في أسوأ الأحوال.

إن الترابط بين الجريمة المنظمة وشبكة الإنترنت ليس طبيعياً فقط، و إنما هو واقع تفرضه الممارسة أكثر فأكثر. فشبكة الإنترنت تؤمن الأقنية والأهداف في نفس الوقت للجريمة، وتُمكن من استغلال هذه الأقنية والأهداف لتحقيق أرباح كبيرة بأقل قدر ممكن من المخاطر. وجماعات الجريمة المنظمة لا تريد أكثر من ذلك. ولهذا السبب فمن الأهمية بمكان تحديد بعض الطرق التي تتداخل فيها الجريمة المنظمة حالياً مع الجريمة التي تُرتكب من خلال الشبكات الإلكترونية.

و إذا كعض الجرائم الدولية التي تناولها القانون الجنائي الدولي في أطار منع الجريمة الدولية و صدر بشأنها اتفاقيات دولية[15] و كان منها مثلا، جريمة الاتجار بالمخدرات و جريمة تبييض الأموال، فهل هناك من مجال لأن يتم ارتكاب هذين الجريمتين في إطار الإجرام الإلكتروني أو في العالم الافتراضي و على رأسه شبكة الإنترنت ؟.

إن جريمة غسيل الأموال هي جريمة لاحقة للجريمة التي تحصل منها الأموال غير المشروعة التي تكون محلا للغسيل، و هذا السلوك الإجرامي الأولي قد يكون الاتجار في المخدرات أو الاتجار في الأعضاء البشرية و النساء و الأطفال، و إدارة شبكات الدعارة، و كذالك عمليات تهريب الذهب و الأحجار الكريمة و تزييف و تزوير العملات و غيرها من صور الجريمة المنظمة العديدة.

فعُرف غسيل الأموال عبر الإنترنت، حيث كانت تمارس المقامرة و النشاطات المصرفية المقترنة بها، علاوة على العمليات المصرفية عبر الشبكة، كما أن استخدام الإنترنت يوفر آلية يمكن استخدامها في الحركة السريعة للنقود الإلكترونية بالمقارنة مع الاستخدام التقليدي للنقود الورقية[16] .

و يلاحظ أن هناك اتجاها متناميا لدى جهات غسل الأموال، للتحرك بعيدا عن البنوك نحو قطاع المؤسسات المالية غير المصرفية كسوق صرف العملات و سوق الحوالات المالية. و قد تم الالتفات نحو القطاعات غير المالية من تجارة البضائع الثمينة كالمجوهرات و السيارات الفخمة و غيرها.

و كل هذه الجهات يمكن عن طريقها غسل الأموال القذرة التي تهرب من خارج بلدان عديدة و يتم توظيفها في الهيكل الاقتصادي المالي في بلدان أخرى.

و الجريمة الاقتصادية المنظمة، بما فيها غسيل الأموال، يلجأ مرتكبوها إلى استخدام التقنية الحديثة، فيقيموا شركات مشروعة ليتستروا خلفها و يرتكبوا أنشطتهم غير المشروعة للتمويه حال ارتكاب الجرائم الاقتصادية [17] .

و نخلص من ذلك أن عمليات غسيل الأموال بطريق الإنترنت، هي أمر وارد في ظل نمو و ازدهار التجارة الإلكترونية، و ذلك عن طريق تحويل الأموال أو توظيفها و التعامل مع البنوك عبر الإنترنت أو إجراء عمليات معقدة من التحويلات النقدية من حساب لآخر و من بنك لآخر و ذلك لإخفاء الصفة غير المشروعة للأموال.

و بهذا يرى خبراء الحاسب الآلي، أن الإنترنت أحد أكبر الفرص لغسل الأموال خاصة مع النمو المتزايد للبرمجيات التي تزيد من سرية التعاملات، و ما تمكنه من نقل الأموال عبر الحدود نظرا لخصوصيتها.

و من مظاهر التداخل بين الجريمة المنظمة و الجريمة الإلكترونية أيضا، هو ما يمكن تسميته بتبديل مناطق الصلاحيات القانونية". لا شك أن الجرائم المتعلقة بالشبكات الإلكترونية، عندما ترتبط بالجريمة المنظمة، سوف تنطلق من مناطق لا يوجد فيها إلا القليل، إن وجد، من القوانين الموجهة

لمحاربة الجرائم التي ترتكب عبر الشبكات الإلكترونية أو المناطق التي لا تقدر على تطبيق القوانين المضادة للجرائم التي ترتكب عبر الشبكات الإلكترونية. و من بين الوقائع التي دفعت على الأقل إلى الانتباه إلى مثل هذا الترصد، هو استعمال أحد الطلبة في الفيليبين لفيروس بقة الحب. ومع أن الفيروس انتشر في العالم اجمع وكلف المؤسسات التجارية آلاف الملايين من الدولارات، فعندما تمكن مخبرو مكتب التحقيقات الفيدرالي من تحديد هوية مرتكب العمل، اكتشفوا أيضاً أنه ليس هناك من قانون يمكن من خلاله محاكمة المرتكب. بعد ذلك، عمدت دولة الفيليبين إلى إصدار قوانين تحرّم الجرائم التي تُرتكب عبر الشبكات الإلكترونية، وتبعتها في هذا السياق دول أخرى. مع ذلك، لا زالت توجد ثغرات تشريعية تسمح للمجرمين والمعتدين على الشبكات الإلكترونية بالعمل دون خوف من العقاب.

كما توفر مزادات السلع التي تتم بواسطة الإنترنت فرصا للمنظمات الإجرامية لنقل الأموال و من ثم تبييضها من خلال عمليات شراء قانونية ظاهريا.

لذلك يتعين تدريب رجال الشرطة و النيابة العامة و القضاة على كيفية مكافحة هذه الجرائم بالطرق المعلوماتية الحديثة و هذا يقتضي التدخل التشريعي لتطوير إجراءات التحقيق و المحاكمة و التوسع في سلطات التحري و تقنياته و مراقبة المحادثات التليفونية و جمع الاستدلالات و التحقيق و ما إلى ذلك[16] .

إن الانسجام ضروري بالنسبة إلى القوانين الأساسية كما بالنسبة إلى القوانين الإجرائية. على كافة الدول أن تُعيد تقييم ومراجعة قواعد الإثبات، والتفتيش، وإلقاء القبض، والتنصت الإلكتروني، وما شابه ذلك لتشمل المعلومات الرقمية، وأنظمة الكمبيوتر الحديثة، وأنظمة الاتصالات الحديثة، والطبيعة العالمية لشبكة الإنترنت.

2.1 : بعض صور الاعتداءات الإلكترونية

بعد ما رأينا كيف صار للاعتداء الالكتروني أبعادا فنية للأفعال الجنائية عموما و للجريمة الدولية خاصة شاملا بذلك جميع المجالات، نحاول التركيز على بعض صوره الخطيرة التي يمكن أن يكون فيها مساس بأمن و سلامة المجتمع الدولي مبرزين هذه الخطورة حاليا و فيما قد تؤول إليه في المستقبل.

كما أردنا أيضا أن نبين من خلال اختيارنا لأهم هذه الصور، كيف هذه الوسيلة الإجرامية احتوت جميع الصور الإجرامية في طابعها التقليدي. و لدراسة ذلك، رأينا أن نتطرق إلى الإرهاب الإلكتروني و العنصرية الإلكترونية، بحيث زيادة على أنها كما أشرنا، تعد من أخطر هذه الصور، فإنها تنسب إلى مراحل مختلفة من العصور من أقدمها مثل التجسس إلى أحدثها مثل الإرهاب.

1.2.1 : الإرهاب الدولي الإلكتروني.

يعد الإرهاب إحدى الظواهر الإجرامية الخطيرة التي تهدد سلام و أمن المجتمعين العربي و الدولي، و استقرار العلاقات الدولية، و تلحق الأذى بالمرافق الدولية كوسائل النقل الجوي و البري و البحري، و تشيع العنف و الرعب في نفوس الأبرياء من الناس، حيث أن هناك اجماع على أن خطر الجريمة الإرهابية لا يقتصر على دولة أو مجتمع و أنما يتعدي هذا الخطر كل الحدود ليشمل دول العالم بأسره.

و لعل من المسلم به أن الإرهاب ظاهرة صعبة و معقدة، تُسهم كثير من العوامل السياسية و الاقتصادية و الاجتماعية و الإنسانية و التاريخية في إفرازها و بلورتها، و في التمكين لها و انتشارها و مما لا شك فيه أن تكنولوجيا العصر ووسائل العلم الحديث قد أسهمت بنصيب وافر في سرعة و حرية و انتقال المجموعات الإرهابية، و في منح الحوادث الإرهابية فعالية أكبر و أخطر لذالك كان الإرهاب نوويا و بيولوجيا وكيماويا فلما نجحت المواجهة في استفراد وسائلهم كان الإرهاب صامتا. و الإرهاب الصامت هو أعتى صور الإرهاب المعاصر فهو لا يعتمد على الوسيلة بل يسعى دائما إلى الهدف و لو أعوزته الوسائل المستخدمة بل طور أساليبه و هجر الوسائل الدموية الأكثر وحشية واستبدلها بالوسائل المشروعة أو الأسلحة الناعمة واستخدم في هده الوسائل أو الأسلحة الناعمة الصوت و الضوء و الرائحة و الموسيقى و المصحف و القلم و المسبحة بدلا من القنبلة و الديناميت فتلك وسائل بالية[18] .

إلى أن ظهر الإرهاب الإلكتروني حيث مورس الإرهاب كنظام قائم على الرعب مستخدما الشبكة الدولية، الإنترنيت ، في تنفيذ الكثير من الأعمال الإرهابية التي روعت أمن المواطن و أمن الدولة . واستعار الإرهابيون هذه الوسيلة الآمنة في نشر ما يعرف بالرعب الإلكتروني باعتباره أحد الأبعاد الجديدة للإرهاب التقليدي و صورة مطورة من الإرهاب الصامت.

ثم تصاعدت حدة الإرهاب باستخدامه للشبكة الدولية كوسيلة لتصدير الإرهاب الدولي العابر للحدود وتخصيص مواقع محددة له كنواة لشبكة عنكبوتية خاصة به[19] . و من ثمة كان الإرهاب الدولي الإلكتروني فما هي هذه الظاهرة و كيف أخذت بعدا دوليا وواقعا حقيقيا.

1.1.2.1: ماهية الإرهاب الدولي الإلكتروني

لقد استغلت المنظمات الإرهابية و الإرهابيون شبكة الإنترنيت مثلا، كمصدر ثري للمعلومات و البيانات وأعدت موسوعة إجرامية تظم كثيرا من الأعمال الإجرامية العنيفة أو الإرهابية التي قامت بها أو التي يمكنها الوفاء بتنفيذها عبر دول العالم المختلفة وتظم هده المعلومات أو البيانات المسجلة كثيرا من المواقع الرئيسية و الحساسة في الدولة مثل البنوك و السفارات و المنشآت المهمة و

المستشفيات و غيرها من المواقع المهمة التي تسجلها الدولة كمواقع يحتاج إليها المواطن لإنهاء خدماته او كمواقع تنشر المعرفة و توفر المعلومات للجماهير تجاه موضوعات مختلفة.

و بهذا الاستغلال السيئ استطاعت بعض المنظمات الإجرامية الاتصال بمواقع منشآت حيوية و مهمة وترصدت بها لتمارس الإرهاب[17] .

فإذا كانت تعريفات الإرهاب تركزت بشكل عام على استخدام العنف أو التهديد به في وصف الإرهاب و كان ذلك بمفهوم مادي في عالم مادي، فإنه بعد ما ظهر العالم الإفتراضي و صار إلى ما هو عليه، احتل العنف و التهديد به مكانة عالية فيه و أ صبح يمارس بالموازاة إلى العالم المادي الذي يشير إلى قضايا و ظواهر متعددة مثل الطاقة، الضوء و الظلام، و البرودة و الحرارة و جميع الأمور المادية و الحيز الذي نعيش فيه و نمارس الوظائف و الأدوار من خلاله.

ورغم تمتع كل من العالمين باستقلالية تامة فإن تقاطعهما و التقاءهما يمثل وسيلة أو أداة الإرهاب الإلكتروني، السلاح الجديد الذي يهدد العالم في الألفية الثالثة و ما أنتجه من تقانة تتصل بجميع مجالات الحياة.

فينطلق إذا تعريف الإرهاب الإلكتروني من هذين العالمين، فيُستعمل العالم المادي لملاقاة العالم الافتراضي الذي فيه تتم عملية الإرهاب و التدمير لتتحقق النتائج و الخسائر في العالم المادي من جديد، و إذا كان في بعض الحالات لا يتحقق العنف الإلكتروني بصورة مباشرة كما هو الحال في نتائج الإرهاب التقليدي، إلا أنه قد يحدث ذلك لما يشتمل على أفعال مادية يقوم بها مرتكب العملية أو ارهابي الارهاب الالكتروني[20] .

كما يشكل الاحتمال المتزايد للالتقاء بين العالمين تزايد محتمل في الاعتمادية على العالم الافتراضي في الاستخدامات اليومية العادية على جميع المستويات.

و هناك بعض النقاط الواضحة للالتقاء بين العالم المادي و الافتراضي و التي تمهد الطريق أمام شبكات الإرهاب الإلكتروني :

- فتح باب المرآب
- جهاز نبضات القلب
- شريحة جهاز الحاسوب توضع في آخر تصميم لنموذج سيارة فاخرة.
- جهاز الميكرويف[21].

إن هذه المجالات التي تلاقي بين العالم المادي و الافتراضي قضايا تمارس في حياتنا اليومية المعتادة و يستغلها إرهابي شبكة الإرهاب الإلكتروني و ذلك لسهولة الوصول إليها و إتاحتها كفرص تستغل و توظف في خدمة العملاء.

و لا يتوقف الأمر عند هذا المستوى، بل إن التقدم و التطور التكنولوجي المتسارع الذي يشهده عصرنا في مجال التسيير الآلي أو الالكتروني، ولد نقاطا جديدة أخرى يلتقي بها العالم المادي و الإفتراضي و أصبحت أكثر سهولة و يسرا في أيدي عملاء الشبكات الإرهابية الإلكترونية و ذلك باعتمادها على منتجات الحداثة و استغلالها في مصالحها الخاصة. لذلك فإن مجتمعات ما بعد الحداثة أفرزت قوى ووسائل تمنح الشبكات الإرهابية الإلكترونية البنى التحتية في تنفيذ ما تريد من تدمير و تهديد للحداثة و تقانتها.

و تتمثل نقاط الالتقاء الجديدة في الميادين الآتية :

- مصانع أنتاج الأطعمة.
- مصانع إنتاج الأدوية.
- منشآت الكهرباء و الغاز الطبيعي.
- نظم تقاطع القطارات و التحكم بالمرور.
- نظام التحكم بالملاحة الجوية للجيل القادم.
- معدات القوات المسلحة و خاصة الإلكترونية.
- أمن الإتصالات العامة.
- اتصالات المواطنين.

و لتحقيق نظام الالتقاء السالفة بين العالم المادي و العالم الافتراضي في القرن الحادي و العشرين، يسعى عملاء الإرهاب الإلكتروني و منظماته إلى السيطرة على قوى نقاط الالتقاء من خلال بعض الأهداف الأساسية:

- الوصول إلى المداخل.
- التحكم بآليات ووسائل العالمين المادي و الافتراضي.

التعدين و ذلك بمعرفة المداخل النظرية و التطبيقية للعالم المادي و آليات مداخلها من خلال العالم الافتراضي.

و لتفعيل الأهداف السالفة الذكر، (الوصول و التحكم و التعدين) هناك أربع أدوات تزود شبكات الإرهاب الإلكتروني بسرعة التحكم و السيطرة:

- الانتقال : سرعة الانتقال عبر الخطوط و الأراضي.
- الاتصال : سرعة الاتصال.
- التجميع : جمع المعلومات الكثيرة و فصلها.
- استرداد : استرداد المعلومات بالطرق المتنوعة[21].

إن عملاء الإرهاب الإلكتروني من خلال استغلال موارد العالم المادي و الافتراضي، يستطيعون تدمير نقاط الالتقاء الإيجابية و التي تمثل حالة لرفاه المجتمع، إضافة إلى عمل تغييرات أساسية في الأنظمة العاملة مساسا بمنشآت مدنية أو أمنية أو تدميرا للبنى التحتية و الفوقية لها عبر آلاف الأميال و في جو مريح و هادئ و بعيد عن الإزعاج و الفوضى على استرخاء في فندق فاخر في مدينة لندن أو باريس أو واشنطن، و بعيدا عن أعين الناظرين. و لذلك نستطيع القول أن الإرهابيين التقليديين يستخدمون الأسلحة المدمرة ومواد المتفجرات و يكونون أداة لإحداث حالات الفزع بين السكان في حين أن الإرهاب المستحدث يتم عن بعد ودون اللجوء إلى العنف المادي و الجسدي.

إن إخضاع العالم المادي بما يحتويه من بنى تقنية و معرفية و العلم الافتراضي إلى سيطرة و تحكم إرهابي الإرهاب الإلكتروني، يختلف تماما عن دور القراصنة و الهواة الذين يسعون إلى الاستيلاء على مكاسب مادية محدودة أو بغرض المتعة أو أحيانا للإزعاج فالقراصنة يسعون إلى خلق جو من الإشاعات مثل البلبلة الاقتصادية بتدهور العملة و الفساد و إجراء الاتصالات الدولية مجانا و الحصول على بطاقات الائتمان.

و من هنا فإن القراصنة لعبوا دورا في القرن الماضي من خلال خلق جو من الفوضى في بعض المراكز التجارية في حين يقوم دور إرهابيي الإرهاب الإلكتروني على مهمات معقدة و مدمرة و تعد منهجا للإرهاب الإلكتروني في هذا القرن[21] و إن كان لا يوجد إلى حد الآن تعريف محدد لمصطلح الإرهاب الالكتروني، إلا أنه من خلال المفاهيم السابقة برزت بعض المحاولات في ذلك. فعُرِّف بأنه " العمل الناتج عن تخريب أو إتلاف أو تبديل معطيات أو المعلومات أو لأنظمة الإعلام الآلي الأساسية الموضوعة لحسن سير أجهزة الدولة و مؤسساتها من أجل إلحاق ضرر بها لهدف سياسي أو ديني أو إيديولوجي، أو حتى اقتصادي أو اجتماعي و بيئي،و مساسا بحياة الأفراد"[22] .

كما عرف بأنه "التهديد والتخريب التقني لمحطات التحكم و قواعد المعلومات و أجهزة الحاسبات و شبكات الاتصالات و الذي ينتج عنه أضرارا بالغة و كبيرة[23] .

كما لجأ آخرون إلى تعريف الإرهاب الإلكتروني بأنه "العدوان أو التخويف أو التهديد ماديا أو معنويا باستخدام الوسائل ، و الصادر من الدول أو الجماعات أو الأفراد على الإنسان، دينع أو نفسه أو عرضه أو عقله أو ماله بغير حق بشتى صنوفه و صور الإفساد على الأرض"

2.1.2.1 : أهداف الإرهاب الإلكتروني و تطلعاته.

يهدف الإرهاب الإلكتروني للدخول إلى نظام التحكم الإنتاجي لمصنع إنتاج مثل حبوب الذرة و من ثم تغيير مستوى الحديد المزود في هذه الوجبة بهدف إيذاء و قتل الملايين من الأطفال المعتمدين على تلك الوجبة. و هذا لا يمثل هدفا جوهريا للقراصنة. كما يقوم الإرهاب الإلكتروني بوضع عدد من

المتفجرات الرقمية في أنحاء مدينة معينة، و في حالة توقف إحدى المتفجرات فإن جميع القنابل ستنفجر. و هذه العملية الإرهابية تختلف تماما عن صور الإرهاب التقليدي.

إن إرهابي الإرهاب الإلكتروني غير مجبر على أن تكون المتفجرات ملتصقة به، و لا يستلزم الأمر وجود شاحنة لحمل تلك القنابل من أجل خلق ترويع و إفزاع للأهداف المحددة. و الأخطر من ذلك أننا لو حاولنا توقيف قنبلة واحدة ستنفجر جميع القنابل مما يؤدي إلى خسائر مادية في المعدات و الأهداف المحددة بعيدا عن الترويع و الفزع و القتل. إنه إرهاب علمي و مُخطط له و هادف و يستند على أسس منهجية يقوم به أشخاص أذكياء و مؤهلون علميا و ذهنيا.

يهدف الإرهاب الإلكتروني إلى نشر الفوضى في البنوك و التحويلات المالية العالمية، و تدمير قيمة الأسهم. من هنا يسعى الإرهابيون إلى إفقاد الثقة في الاقتصاد العالمي المعاصر و إضعاف قدراته.

إن أهادف الإرهاب الإلكتروني عامة و ليست خاصة على عكس القراصنة و ذلك حتى يكونوا بعيدين عن أعين المراقبة الأمنية.

يهدف الإرهاب الإلكتروني إلى مهاجمة نظام التحكم الملاحي و ذلك من خلال توجيه حركة طائرتين مدنيتن على سبيل المثال لتتصادما كونه يمكن من الدخول إلى نظام التوجيه الإلكتروني للطائرتين و هذا نفسه يمكن أن يخص طائرة تقل رئيس دولة ما أو فرقة علمية مهمة خاصة كما ينطبق أيضا هذا الأسلوب على محطات القطارات الدولية خاصة التابعة لدول كبرى، مثل لندن و نيويورك و طوكيو.

و سيدخل الإرهاب الإلكتروني في المعدات الدوائية في مصانع الأدوية بهدف تحقيق أكبر قدر من الخسائر في الأرواح و الإساءة إلى كبرى الشركات الدوائية العالمية.

و عن طريق الإرهاب الإلكتروني يمكن رفع مستوى الضغط في أنابيب الغاز و هذا يؤدي إلى الضغط على الصمامات العاملة و من ثم يوقع إنفجارات ضخمة و هائلة تهلك مدينة بكاملها.

سيدخل الإرهاب الإلكتروني في محطات الطاقة النووية وهذا ما قد ينعكس سلبيا على البشرية.

كما يهدف الإرهاب الإلكتروني في هذا القرن الجديد إلى فرض الحصار على التجمعات البشرية و لمنعهم في النهاية من الحصول على الماء و الغذاء و الهواء. فالجميع مهدد بالإرهاب الإلكتروني ووحشيته.

و عموما فإن الإرهاب الإلكتروني يستهدف التقنية في القرن الحادي و العشرين و الذي يؤثر على قوة الإنتاجية و الثقة بالمجتمعات ما بعد صناعية. و يمكن إلحاق مجالات الإرهاب إلى الصناعة الخاصة و أمن الحاسوب حيث يرى الخبراء أن العديد من الشركات العالمية تخسر الملايين بسبب دخول الإرهابيين و اختراقهم أمن المؤسسات الكبرى، و قد يكون القرصان من منظمات خارجية أو منافسين لشركات أخرى من الشركة نفسها. ولا شك أن الكثير من العاملين في الشركات الكبرى حول مهددات الإرهاب الإلكتروني والمخاطر التي يجدونها في مجال أعمالهم من تخريب و تدمير للأنظمة العاملة.

و أشارت التقارير في مجال مكافحة الإرهاب الإلكتروني إلى أن الكثير من مديري الشركات لا يخصصون الميزانيات الكافية لتطوير البرامج المضادة و لتوفير الحماية اللازمة لأنظمة الشركات.

و يرى الباحثون في مجال الإرهاب الإلكتروني أن الرشاش الآلي لم يعد هو السلاح الفتاك و المتطور و الفعال في هذا القرن الجديد بل أصبحت التكنولوجيا و تطور المعلومات التكنولوجية و خاصة الكمبيوتر و ثورة المعلومات و الإنترنت و التي أصبحت توازي تطوير قنبلة نووية بالنسبة إلى حجم الدمار الذي يخلفه تدمير أنظمة الشركات متعددة الجنسيات و الآثار المادية الهائلة وراء تلك الاختراقات الإرهابية المدمرة. و يسعى إرهابي الإرهاب الإلكتروني من خلال تطور التكنولوجيا المذهل إلى تدمير البنى التحتية للأعداء و خاصة القوات المسلحة من حيث تدمير أنظمة الاتصال الجوية و البرية و البحرية[21].

و إن الإرهاب يهدف أيضا إلى تدمير البنية التحتية المعلوماتية للنظام الإنساني و تعريض حياتنا لمخاطر غير محتملة و متوقعة.

وفي النهاية يمكن القول أنه كما هو الحال في أية حرب، فإن الجيوش المتصارعة تستهدف دوما ثلاثة عناصر أساسية من أجل كسب المعركة؛ وهي العناصر العسكرية، والاقتصادية، والسياسية. فإنه يحدث ذلك أيضا في عالم حروب المعلوماتية أو الحروب الإلكترونية، و في هذه العناصر الثلاثة وعلى رأسها مراكز القيادة والتحكم العسكرية، والبنوك والمؤسسات المالية، ومؤسسات المنافع كمؤسسات المياه والكهرباء وذلك لإخضاع إرادة الشعوب.

3.1.2.1 :واقع الإرهاب الإلكتروني و بعده الدولي.

من خلال ما سبق الإشارة إليه، فيما يخص أهداف الإرهاب الإلكتروني، يلاحظ أن هذه الأهداف لم تعد تعني الأقاليم الداخلية للدول، بل أخذت بعدا وواقعا دوليين مستغلة في ذلك تزايد الصراعات الدولية في الكثير من مناطق العالم التي تسببها تضارب المصالح الاقتصادية و السياسية و الاجتماعية الشيء الذي أدى إلى وقوع الكثير من العمليات الإرهابية الإلكترونية على المستوى الدولي[24].

فتعد معسكرات الجيش التابعة لكل دولة و مصادر طاقتها و مراكز التحكم في ملاحتها الجوية و بنوكها و شبكة اتصالاتها أهدافا أساسية تزيد احتمالية تعرضها للإرهاب يوما بعد يوم، كما تشمل الأهداف الأخرى أجهزة الشرطة أو المنشآت و الوحدات الطبية و أنظمة الإنقاذ و مكافحة الحرائق و الإطفاء و التي من الممكن أن تتعرض للمخاطر الأهداف المحتملة للإرهاب الإلكتروني في هذا القرن[21] .

و تشير الإحصائيات إلى أن قراصنة الكمبيوتر (الهواة)، أكبر مصادر خطورة على الإنترنت إذ أنهم يمَثلون بنسبة 90% من حالات القرصنة و الدخول غير المشروع إلى عدة مواقع.

و تشير الإحصائيات إلى أن الإرهاب الإلكتروني لا يأتي من قراصنة الكمبيوتر وحدهم أو الإرهابيين العاديين، بل تقوم به الحكومات أحيانا بسلسلة من الهجمات على المواقع الخاصة لها بغرض اختبار درجة حمايتها ضد الهجمات و محاولات الدخول غير المشروع التي تظهر من خلال شبكة الإنترنت.

و وجدت إدارة حماية معلومات وزارة الدفاع الأمريكية من خلال بعض المسوحات التي قامت بها بأن 88 من إجمالي أنظمة الكمبيوتر المستخدمة في وزارة الدفاع و البالغ مجموعها 3000 نظام كمبيوتر تعرضت إلى الهجوم و كان اختراقها سهلا جدا و 97 من الاختراقات لم تكتشف و 4 تم اكتشافه و 5 فقط تم الإبلاغ عنها و التحقيق فيها.

و هذه النتيجة حول تفاقم خطورة الإنترنت كما أشارت النسب السابقة مع المنظور الأمني و الذي بين أهمية البعد الموضوعي و الذاتي في تفسير المهددات الأمنية.

و أظهرت الدراسة أن هناك مجموعة من الدوافع وراء الاختراق المعلوماتي. كما أظهرت دراسة مسحية قامت بها مؤسسة التطبيقات العلمية العالمية في عام 1996 حول تكاليف الإرهاب الإلكتروني بأن 40 مؤسسة من كبار المؤسسات تكبدت خسائر تفوق 800 مليون دولار بسبب حالات الدخول غير المشروع. و بينت دراسة قام بها مكتب التحقيقات الفيدرالية FBI بأن 40 % من مواقع الحكومة و المؤسسات الأمريكية و الجامعات و البالغ عددها 248 موقعا قد تم الدخول إليها بصورة غير شرعية مرة على الاقل. و قد أوضح ثلث أصحاب هذه المواقع بأن الدخول غير الشرعي قد تم عبر الإنترنت.

كما أظهرت دراسة أخرى أن أنظمة الدفاع و التي تحتوي على معلومات حساسة قد تعرضت لحوالي 25000 دخول غير شرعي عبر شبكات المعلومات المتعددة، و أن 150 حالة فقط من مجموع حالات الاختراق أو الدخول غير الشرعي قد تم الكشف عنها. و يقدر مكتب التحقيقات الفيدرالية خسائر النشاطات التجارية المترتبة على عمليات قراصنة الكمبيوتر حوالي 138 مليون دولار سنويا. وطبقا لمعلومات وكالة الاستخبارات الأمريكية فإن أنظمة الكمبيوتر الحكومية قد شهدت خلال الثلاث سنوات الماضية حالات اختراق و دخول بصورة غير شرعية بلغت 250000 حالة.

و ذكر أحد المصادر في بريطانيا بأن الإرهابيين قد حصلوا على 400 مليون إسترليني خلال الفترة 1993 إلى 1995 عبر تهديد المؤسسات التجارية. كما تلقت البنوك في بريطانيا و الولايات المتحدة من منظمات إرهابية تعمل في مجال الإرهاب الإلكتروني العديد من التهديدات.

و منطقة الشرق الأوسط ليست بمنأى عن الإرهاب الإلكتروني، فقد أظهر تقرير مجلة بي سي العدد 3 لعام 1997 أن هناك تباينا بين دول المنطقة في حجم جرائم الحاسب.

وورد أيضا في أحد تقارير جامعة ETSU لعام 1998 أن عدد المحاولات الناجمة التي تم فيها إختراق شبكة البنتاغون للمعلومات غير المصنفة تتجاوز 250 ألف محاولة و أن الخسائر السنوية من جراء هذه الإختراقات غير المشروعة تتجاوز 138 مليون دولار، و قد تضاعف هذا الرقم كثيرا في

عام 2003. هذه الأمثلة و غيرها تعطينا مؤشرات بأن الإرهاب الإلكتروني ليس نظرية أو ضربا من الخيال و إنما هو خطر حقيقي وواقع له بعد دولي يهدد المعلومة الإلكترونية و البنية التحتية للتكنولوجيا. بل أن أحد الأبحاث المعدة من قبل الأكادمية الوطنية للعلوم في الولايات المتحدة أوضح خوفا و قلقا شديدين من أن يأتي الوقت الذي يكون فيه التدمير عن طريق لوحة المفاتيح CLAVIER أكبر من تدمير القنبلة. [18]

هناك العديد من المواقع الإجرامية المعلنة عبر الشبكة الدولية مخصصة لمنظمات إجرامية محترفة في جميع أعمال العنف و الإرهاب يتم الاتصال معها و الاتفاق على تنفيذ الأعمال الإجرامية من قتل أو اغتيال أو نسف و تفجير أو خطف طائرات أو حتى تصدير مواد نووية أو أسلحة متقدمة. و تخصص مثل هذه المواقع بعضا منها للقيام بأعمال التدريب العملي على استخدام هذه الأدوات، و يمكنها تأمين نفسها ضد أية اختراقات أو أعمال تدمير بالفيروسات. و قد استطاعت بعض المنظمات الحصول على أرباح مالية من بعض الأفراد و المؤسسات تحت التهديد بكثير من أعمال العنف و الإرهاب و لكن الغريب في الأمر أن هؤلاء الضحايا سارعوا بالاستجابة إلى كل الطلبات تحت وطأة الإكراه و التهديدات، و على أساس قناعتهم بقدرة هذه المنظمات و افتراض عدم قدرة الجهات المسؤولة على ملاحقة هؤلاء المجرمين باعتبار أن وسيلة الإنترنت وسيلة آمنة و غير مراقبة، فكان ذلك سببا في اعتبار الإنترنت وسيلة إجرامية و الجدير بالذكر أن الولايات المتحدة الأمريكية قد أنشأت عقب أحداث 11 سبتمبر 2001 محطة رصد عملاقة يمكنها التنصت على كل الإتصالات الدولية عبر شبكة الإنترنت، عرفت بمحطة " إيشلون " و يوجد مركزها المتقدم في إنجلترا و يمكنها التلصص على كل المواقع و تفحصها و تنقيتها حماية للأمن الوطني[18].

إن دل هذا على شيء، فإنما يدل على **أن** الإرهاب الإلكتروني صار إرهابا ضد الدول لما لهذه الأخيرة من إمكانية النفاذ إلى شبكات التحكم في المرافق العامة مما يتسبب في الشلل التام للبنى التحتية الأساسية, بل واحتمال تدميرها بالكامل. إن الدول باتت معرضة لما يمكن أن نطلق عليه: أسلحة التدمير الشامل باستخدام الأسلحة البيولوجية المعلوماتية المتمثلة في جيوش الفيروسات التي تخترق حدود الدول لتشيع الخراب والفوضى في أرجاء البنية المعلوماتية,. ومن قبيل المفارقة, فإنه كلما ارتقت الدول في استخدام شبكات نظام المعلومات وزاد الترابط بين هذه الشبكات, زاد تعرضها بالتالي لمثل هذا النوع من التهديد, وهو الوضع الذي يثير أشد القلق لدى الدول المتقدمة التي يتزايد اعتمادها على شبكات المعلومات في إدارة معظم شئون حياتها.

علاوة على ما سبق, قد يقع الإرهاب إلكترونيا بغرض الإضرار بالمصالح الاقتصـــادية للدولة. وقد مارست إسرائيل هذا النوع من الإرهاب بهدف تشـــويه صورة السياحة المصرية. لا يمكن مواجهة هذا النوع من الإرهاب دون تشريعات دولية مستحدثة ,بجانب إشاعة خلق عالمي جديد

لن تقوم له قائمة ما لم تتخلص دول العالم المتقدم من نظرتها الضيقة لمفهوم السلام العالمي, وهي النظرة التي تتصدى لأطراف المشكلة وتنأى بشدة عن مواجهة أصولها التي يرجع قدمها إلى أعماق التاريخ الحديث, وتتعدد جوانبها السياسية والاقتصادية والثقافية والأمنية[25].

لقد أصبحت دول عديدة تشهد في السنوات الأخيرة حروبا متبادلة و ساحة العمليات الحربية هذه المرة هي شبكة الإنترنت بكل ما فيها من مواقع و عناوين إلكترونية.

أما الهدف من هذه الهجمات الإلكترونية كان في كثير من الحالات إغلاق المواقع الإلكترونية لفترات زمنية مختلفة أو تدمير حواسيب الخصم بغية إلحاق الأذى البالغ به. و لو أخذنا الحرب الإلكترونية الثانية التي حصلت بين الصين و الولايات المتحدة الأمريكية في 2002 و التي جاءت بعد الهبوط الاضطراري لطائرة الاستطلاع و التجسس الأمريكية فوق إحدى الجزر الصينية، هذه الحرب أدت في نهاية المطاف إلى إغلاق 2000 موقع إلكتروني في كل من الصين و الولايات المتحدة الأمريكية، بالإضافة إلى الحرب الإلكترونية التي شنتها أمريكا على تنظيم ما أسمته بالقاعدة منذ بدأ الحملة العسكرية في أفغانستان في نهاية عام 2001 و بعد أحداث 11 سبتمبر، عمدت أجهزة الإستخبارات الأمريكية إلى ضرب موقع مركز الدراسات و الأبحاث الإسلامية الناطق بإسم هذا التنظيم على الإنترنت[26].

2.2.1 : التجسس الدولي الإلكتروني

إن من بين المجالات أيضا التي برز فيها الاعتداء الإلكتروني بصفة فعالة،هو التجسس . حيث بهذا الأخير صار المتجسسون، لا سيما إذا كانوا دولا، و لا يمكن أن يكونوا أي دول إن لم تكن تلك التي تملك القدرة على انتهاج هذا الأسلوب في الاعتداء، بإمكانهم ارتكاب عدوان من شأنه أن يحبط خطة مجتمع بأكمله في جميع جوانبها و ذلك عن طريق الترصد و التنصت على سياسة الدولة و هي تعمل على وضع هذه الخطط و البرامج للنهوض بهذا المجتمع. هذا على خلاف دور الجاسوس بالمستوى التقليدي، أين يقتصر على العمل على إحباط و تتبع عملية معينة واحدة من أجل إفشالها عن طريق تحويل المعلومات المتجسس عليها للدولة العدوة. و ما نلاحظه أنه بالرغم من صغر حجم فعل الجوسسة هنا بالمقارنة مع حجم التجسس الإلكتروني، إلا أن التشريعات الدولية قد عنيت بهذا السلوك و جرمته في بعض حالاته،ما يجعلها بالأحرى أن تجرم هذه الصورة الجديدة له، لما أعادت ارتكابه بفعالية أكبر. فكيف كان ذلك، و إلى أي مستوى صارت إليه ممارسات التجسس الدولي الإلكتروني.

1.2.2.1 : الإلكترونية تحي جريمة التجسس

إن ظاهرة التجسس ليست ظاهرة حديثة، بل هي ظاهرة قديمة و موغلة في القدم، إذ نشأت مع نشأة أولى المجتمعات البشرية و أيا كانت صورة هذا المجتمع، أسرة، عشيرة، قبيلة، قرية، مدينة. فمتى ظهر أي تجمع بشري، و في أي زمن، فقد نشأ التجسس، فهو يعتبر من أقدم الأنشطة الاستخبارية التي مارسها الإنسان لأن كل تجمع يسعى جاهدا لمعرفة ما لدى غيره من التجمعات الأخرى من أسرار أو معلومات وخطط لمهاجمته. و قد ارتبطت هذه الظاهرة في الماضي البعيد بالقدرات الخارقة للآلهة، و الأساطير و كانت الوسيلة الأولى للحصول على المعلومات في ذلك الزمن تتمثل في اللجوء إلى العرافين و الكهان و السحرة باعتبارهم وسطاء بين البشر و الآلهة، مستعملين إمكانيات التنجيم و الأحلام و غيرها في ذلك.

ثم أخذ التجسس بعد ذلك طابعا أكثر واقعية، فلم يعد مرتبطا بإرادة الآلهة أو الأرواح و لكنه ارتبط بقوة و مشيئة الحكام و الغزاة، و إرادة المحافظة على الجماعة السيلسية تحت سلطان الملك. و لهذا وجد التجسس منذ القديم و قد عرفه كل من الفراعنة و البابليين و اليهود و الرومان و الإغريق و القرطاجيين و غيرهم من شعوب العصور القديمة و استمرت ظاهرة التجسس خلال العصور الوسطى إلى أن انتقلت إلى العصر الحديث، أين ازداد تشكل الدول و من ثم ظهور التجسس الدولي.[27]

و يمكن القول بأن قيام الدول بالمستوى المعاصر قد قلل إلى حد ما من حدة ذلك التجسس، غير أنه تطورت فكرة التجسس من حيث مضمونها و طريقة ممارستها عما كانت عليه في القديم طبقا لِما ساد المجتمع من تطورات علمية و تكنولوجية ابتداء من اختراع الإنسان للرادار ليتجسس على أعدائه و معرفة كافة تحركاتهم، ثم اختراع الأقمار الصناعية التي تقوم بتصوير الإنسان و الآلات الحربية و المباني و كل ما فوق الأرض يتم تصويره في كل فترة زمنية معينة لضبط كل التحركات الممكنة. و الآن في ظل التطور التقني، فقد أصبح ما يعرف بالتجسس الإلكتروني.[14]

حيث إن عصر المعلومات وبفعل وجود تقنيات عالية التقدم فإن حدود الدولة صارت مستباحة بأقمار التجسس والبث الفضائي و كما أن العالم العربي و الإسلامي كان ولا يزال مستهدفا امنيا وثقافيا وفكريا وعقديا، فإنه بتحول وسائل التجسس من الطرق التقليدية إلى الطرق الإلكترونية لم يسلم العالم الغربي و لا الدول الأخرى الأقوى منها ضد الأقل قوة. و بصفة عامة فالتجسس الإلكتروني هو الذي يعتمد على استخدام التقنيات الإلكترونية في الحصول على المعلومات ابتداء من التجسس على الأفراد عن طريق الإنترنت، و هو أبسط أنواع التجسس الإلكتروني و التجسس من خلال الشبكات السلكية واللاسلكية، و هو من أشهرها[28].

و يمثل اختراق الأنظمة و الشبكات و الوصل غير المخول للبيانات عن طريق اختراق أجهزة الكمبيوتر الشخصية و اختراق الشبكات و المواقع الإلكترونية و اختراق الخطوط الهاتفية و أجهزة الاتصال و اختراق أنظمة المعلومات الدولية الخاصة، طرقا للتجسس الإلكتروني على الأفراد و المؤسسات و الحكومات، سواء عن طريق الإنترنت و من خلال الشبكات الداخلية أو باستعمال الوسائل الكبيرة كالأقمار الصناعية و الأنظمة العالمية المتخصصة في مجال التجسس الإلكتروني الدولي و الخارجي[28]

فيتم استخدام نظام الكتروني لمراقبه واعتراض خطوط الاتصالات الإلكترونية التي تجري في جميع أنحاء العالم. وعملية مراقبة الاتصالات الإلكترونية تقوم حاليا باختبار أكثر من3 بلايين اتصال يومي. وتشمل هذه الاتصالات المكالمات التليفونية ورسائل البريد الالكتروني والفاكسات والإرسال المنبعث من أي قمر صناعي بالفضاء وعمليات إنزال الملفات من علي شبكه الانترنت سواء للاستخدام الشخصي أو استخدامات الشركات أو الاستخدامات العامة, ويتم هذا المشروع بالتعاون بين عده دول منها الولايات المتحدة وانجلترا واستراليا وكندا ونيوزلندا, والاسم الكودي القفل يطلق علي المنظمة التي تملك الأجهزة الإلكترونية التي تقوم باعتراض الاتصالات الإلكترونية التي ترسل من أي مكان بالعالم. وهذا النظام يقوم بجمع المعلومات من خلال أجهزه بالغه التطور مثل الهوائيات التي تلتقط موجات الراديو, وأقمار صناعية وظيفتها التجسس علي الأقمار الصناعية الأخرى المستخدمة في الاتصالات, كما زود هذا النظام بأجهزة إلكترونية أخري وظيفتها مراقبه ما يحدث علي شبكه الانترنت من خلال تتبع البيانات التي ترسل عبر خطوط اتصال الانترنت.

ويقول بعض الخبراء: أن هذا المشروع لا يقوم بمراقبه الاتصالات التي تتم عبر الأقمار الصناعية ولكن تم زرع أجهزة إلكترونية في أعماق المحيطات لمراقبه الكابل البحري المستخدم في الاتصالات. وهذا الكابل يربط قارات العالم كلها ويعمل علي التوازي من شبكه الأقمار الصناعية للاتصالات لتكوين منظومة الاتصالات العالمية, ونظرا للكم الهائل من المعلومات التي يقوم هذا النظام بالتقاطها يوميا فهي تستخدم تطبيقات حديثه تعتمد على نظم الذكاء الاصطناعي لفحص هذه البيانات والحصول علي المعلومات الهامة والمفيدة. ويستخدم هذا النظام تقنيات متقدمه في التعرف على الصوت.

ولا تكمن الخطورة في استخدام الإنترنت ولكن في ضعف الوسائل الأمنية المستخدمة في حماية الشبكات الخاصة بالمؤسسات والهيئات الحكومية من جهة و في عدم الاطمئنان إليها باعتبارها عادة ما تنتجها شركات تابعة للدول العدوة المحتكرة لهذه التكنولوجيا. ولا يقتصر الخطر على محاولة اختراق الشبكات والمواقع على العابثين من مخترقي الأنظمة أو ما يعرفون اصطلاحا (hackers) فمخاطر هؤلاء محدودة وتقتصر غالبا على العبث أو إتلاف المحتويات و التي يمكن التغلب عليها باستعادة نسخة أخرى مخزنة في موقع امن، اما الخطر الحقيقي فيكمن في عمليات التجسس التى تقوم بها الأجهزة

الاستخباراتية للحصول على أسرار ومعلومات الدولة ومن ثم إفشائها لدول أخرى تكون عادة معادية، أو استغلالها بما يضر بالمصلحة الوطنية لتلك الدولة، و هذا باستعمال الإمكانيات التي أشرنا إليها.

2.2.2.1 : ممارسات التجسس الدولي الإلكتروني

إن الجانب الأخطر في عمليات التجسس الإلكتروني كما رأينا، يكمن في محاولات التجسس الدولي، التي تنقل أسرار دول بأكملها إلى دول عدوة. فبعد ما تقلص دور الجواسيس الدوليين، الذي كان منتشراً أيام الحرب الباردة، واقتصر هذا الدور على حالات خاصة، وقلت لذلك، الحاجة لتجنيد وتدريب أشخاص ذوي كفاءات ذهنية وبدنية عالية، لسنوات عديدة، ومن ثم دسهم في قلب نظام دولة معادية، لسرقة أسرارها، وتسريبها إلى دولتهم الأصلية، تحولت طرق التجسس الدولي في عصر الإنترنت، إلى عمليات تجسس إلكترونية، واختراق لأنظمة وشبكات الدول بعضها بعضاً. [29]

يتفق معظم الخبراء أن إسرائيل تصنف في المرتبة الثانية، بعد الولايات المتحدة الأمريكية، بين الدول المنتجة للتقنيات المعلوماتية، وخاصة الأمنية منها. فتعتبر القوات المسلحة الإسرائيلية، منبعا لخبراء أمن المعلومات حيث تختلف سنوات الخدمة الإلزامية العسكرية، في الجيش الإسرائيلي، عنها في الكثير من دولة العالم، إذ تعتبر فترة تطوير لخبرات المختصين في مجال أمن المعلومات. و عليه يعتبر هذا الأمر من أهم العوامل المؤثرة في دفع تطوير الحلول الأمنية، والتطبيقات المتعلقة بأمن المعلومات في إسرائيل. كما تلقت إسرائيل حوالي 800 ألف مهاجر من الاتحاد السوفييتي السابق، وأدت هذه الهجرة إلى ارتفاع نسبة العلماء والمهندسين فيها، لتصل أواخر التسعينيات إلى رقم قياسي عالمي، هو 135 عالماً أو مهندساً لكل 10 آلاف نسمة.[30]

تعتمد الأجهزة الاستخبارية الإسرائيلية على مصدرين أساسيين لجمع المعلومات الاستخبارية اللازمة لحربها ضد حركات المقاومة الفلسطينية، وهما المصادر البشرية، القائمة على تجنيد العملاء، سواء كانوا عملاء غير مرتبطين بتنظيمات محددة، أو عملاء تستطيع زرعهم داخل هذه التنظيمات، والمصادر الالكترونية، والقائمة على الاستعانة بأحدث ما توصلت إليه التقنيات المتقدمة. وكما أن هناك أقسام داخل المؤسسات الاستخبارية الأساسية في الدولة العبرية تعنى بشكل خاص بتجنيد العملاء، فان هناك أقساما تعنى بالتجسس الالكتروني. لكن في ما يتعلق بالتجسس الالكتروني، فإنه من بين الأجهزة الاستخبارية الإسرائيلية الثلاث وهي جهاز المخابرات الداخلية " الشاباك"، وشعبة الاستخبارات العسكرية " آمان "، وجهاز " الموساد "، فيبرز جهاز " أمان "، بالدور الأساسي والحاسم في كل ما يتعلق بهذا المجال من عمليات التجسس الالكتروني.[31]

دشن جهاز " آمان "، الذي يعتبر أكبر الأجهزة الاستخبارية الإسرائيلية، قسما متخصصا في مجال التجسس الالكتروني، أطلق عليه " الوحدة 8200" حيث تكمن أهداف هذه الوحدة في المساهمة في تقديم

رؤية استخبارية متكاملة مع المعلومات التي توفرها المصادر البشرية القائمة على العملاء. وتعتمد الوحدة على ثلاث صور من صور العمل في المجال الاستخباري وهي :الرصد، والتصنت، والتصوير، والتشويش.[32]

و بحكم اعتماد الفلسطينيين بصفة واسعة على التكنولوجيا التقنية الإسرائيلية، مورس التجسس الإلكتروني و مورس التصنت و الرصد على قادة وعناصر المقاومة: من اجل رصد تحركات عناصر المقاومة من التنظيمات المختلفة، تعطي الوحدة "8200" أولوية قصوى للتنصت على هواتف عناصر المقاومة. بحيث تستخدم المادة التي يتم التنصت عليها في بناء ملف امني للذين يتم رصد مكالماتهم، هذا من ناحية، ومن ناحية ثانية يتم استخدام رصد هذه المكالمات في إحباط عمليات تخطط لها حركات المقاومة. فضلا عن استخدام محتوى هذه المكالمات في تحديد الإجراء المتخذ ضد عناصر المقاومة، إن كان اغتيالا أو اعتقالا.[33]

و تبدي المخابرات الإسرائيلية اهتماما بالغا بمعرفة ما يدور في أروقة السلطة و قادتها و مسؤوليها، من اجل مساعدة الحكومة على اتخاذ القرارات المناسبة في كل ما يتعلق بالعلاقة مع السلطة .وقد نقلت الصحف العبرية عن مصدر امني قوله أن " الوحدة 8200 " ، بناء على تعليمات من قيادة جهاز " آمان " لا تستثني أيا من قادة السلطة ومسؤولي وموظفي أجهزتها الأمنية من عمليات التنصت المنهجية. وقد كشفت القناة الثانية في التلفزيون الإسرائيلي النقاب عن أن شارون نجح في إقناع الرئيس بوش في التحول ضد عرفات بهذا الشكل الجارف عندما عرض شارون على مسامع بوش محادثات لعرفات يطلب فيها من مقاومين في حركة فتح مواصلة العمل المسلح ضد إسرائيل في مطلع انتفاضة الأقصى.[32]

وقد وجدت بعض حالات التجسس الدولي ومنها ما اكتشف أخيراً عن مفتاح وكالة الأمن القومي الأمريكي NSA والتي قامت براعته في نظام التشغيل الشهير ويندوز، كما كشف أخيراً النقاب عن شبكة دولية ضخمة للتجسس الإلكتروني تعمل تحت إشراف وكالة الأمن القومي الأمريكية بالتعاون مع أجهزة الاستخبارات والتجسس في كندا وبريطانيا واستراليا ونيوزيليذا. لرصد المكالمات الهاتفية والرسائل بكافة أنواعها ويطلق عليها اسم" ECHELON").

وبعد الاعتداءات الأخيرة علي الولايات المتحدة الأمريكية صدرت تعليمات جديدة لأقمار التجسس الاصطناعية الأمريكية بالتركيز علي أفغانستان والبحث عن الجماعات المعادية لها ، وقررت السلطات الأمريكية للاستعانة في عمليات التجسس علي أفغانستان بقمرين اصطناعيين عسكريين مصممان خصيصاً لالتقاط الاتصالات التي تجري عبر أجهزة اللاسلكي والهاتف المحمولة بالإضافة لقمرين اصطناعيين أخريين يلتقطان صوراً فائقة الدقة، وفي نفس الوقت طلب الجيش الأمريكي من شركتين

تجاريتين الاستعانة بقمرين تابعين لهما لرصد الاتصالات ومن ثم تحول بعد ذلك إلي الولايات المتحدة حيث تدخل في أجهزة كمبيوتر متطورة لتحليلها .

و من بين ما يكون عن طريقه التنصت على الاتصالات من طرف الاستخبارات الأمريكية، هو الأقمار الصناعية. حيث أرسلت الولايات المتحدة أول قمر صناعي للتنصت في نهاية عام 1976م زادت قدرة وإمكانات وكالة (NSA) في عمليات التنصت على جميع الأجهزة السلكية واللاسلكية للاتحاد السوفييتي، وبلدان أوروبا الشرقية، أما في التسعينيات فقد بلغ عدد الأقمار عدة مئات. وهذه الزيادة في عدد الأقمار التجسسية كان ضرورياً لمواكبة الزيادة الكبيرة، و الانفجار في عدد الهواتف ووسائل الاتصال الحديثة، ففي عام 1987م كان عدد الهواتف الموجودة في العالم كله يبلغ 447 مليون هاتف، ولكن هذا العدد طفر في تسع سنوات فقط إلى 741 مليون هاتف، هذا عدا وسائل الاتصالات الأخرى، وبلغ مجموع المكالمات الهاتفية بين الولايات المتحدة وكندا وحدها في عام 1996م رقماً خيالياً وهو خمس مليارات ومائة وسبعة ملايين دقيقة، والخط الثاني من ناحية كثافة الاتصالات الهاتفية هو خط (الصين ـ وهونج كونج)، إذ بلغ مليارين وسبعمائة وستةً وخمسين مليون دقيقة.[34]

تمثل الأقمار الصناعية ربما أهم طرق التجسس في الوقت الحالي، ويمثل التواجد الأمريكي في الفضاء الخارجي حوالي 90 %من المواصلات الفضائية. و أنواع الأقمار الصناعية عديدة ؛ فهناك مثلا الأقمار الخاصة بالتقاط الصور والتي تمر فوق أية نقطة على الكرة الأرضية مرتين يوميا .تتراوح قدرة التبيين لهذه الأقمار ما بين 10 سنتيمترات إلى حوالي متر واحد.

و من جهة أخرى، فإن ممارسات التجسس الدولي ضد هيئة الأمم المتحدة، أو كما تسمى، رمز الشرعية الأممية، باتت مؤكدة من خلال ما كانت تقوم به الولايات المتحدة الأمريكية و بريطانيا، سواء تلك التي صرح بها المتضررون أنفسهم أو الذين كانوا وراء هذه الممارسات.

و الحقيقة التي صارت تثبتها الاعترافات والتصريحات المتلاحقة أن عمليات التجسس على الأمم المتحدة ورموزها كانت على الدوام أمراً طبيعياً. في الحياة الأميركية, إلى درجة أن كافة الأمناء العامين السابقين لكوفي عنان كانوا تحت المراقبة. وتحديداً طوال الخمسين سنة الماضية, مشيرة إلى أن يوثانت وكورت فالدهايم وخافيير دي كويلار كانوا من أشهر الذين جرى التجسس عليهم.

فلقد صرحت مصادر مخابراتية إسترالية بالاعتراف أن الهاتف الجوّال لهانز بليكس كان تحت المراقبة من قبلهم كما اعترف بليكس نفسه في هذه الأثناء أنه كان يشعر بوضعه تحت السمع والبصر, لكن ذلك كان بالنسبة إليه أهون بكثير مما فاجأه ذات يوم, حين زاره قبل أسبوعين فقط من بدء الحرب أحد كبار موظفي البيت الأبيض وعرضَ عليه صوراً سرّية من أرشيف الأمم المتحدة وهيئة المراقبة على أسلحة الدمار, تضمنت إحداها صورة لطائرة عراقية بدون طيار, وأخرى لقنبلة انشطارية, أي أن لدى أجهزة الاستخبارات الأميركية صوراً ليست ملكها, بل ملك الأمم المتحدة, فكيف حصلت عليها وعن طريق من؟[35] إن لم تكن قد وجدت في

التجسس الإلكتروني ما يمكنها من ذلك أخذا بعين الاعتبار المستوى الضعيف في مجال تكنولوجيا الاتصال آنذاك، بالمقارنة مع ما توصلت إليه الولايات المتحدة الأمريكية من تقدم في هذا المجال كونها المالكة الأولى و الأصلية لهذه التكنولوجيا، أين أصبحت شبكة الاتصال تربط بن جميع وسائل الاتصال من أقمار صناعية و هواتف ثابتة و جوالة و شبكة الإنترنت، التي صارت هي بدورها تمكن من هذا التداخل بين كل هذه الوسائل.

3.2.1 : العنصرية و التمييز العنصري الإلكترونيين.

ففي الوقت الذي كان يعمل فيه مناهضو العنصرية على مدى سنوات لرفع الوعي بهذه القضية والتحذير من خطورتها، كانت الجماعات التي تحض على الكراهية العنصرية تحتمي بالإنترنت لنشر رسالة الكراهية التي تحملها.[36]

فمنذ السنوات الأخيرة، أخذت إذا جريمة التمييز العنصري طابعا تقنيا و صارت ترتكب ارتكابا إلكترونيا و ذلك عبر شبكة العنكبوت العالمية (الإنترنت) بحجم يفوق صورتها التقليدية و بخطورة أكبر نظرا لفعالية هذه الوسيلة، مما شغل المجتمع الدولي من دول و منظمات دولية و جعله يولي اهتماما كبيرا بها.

1.3.2.1 : مفهوم العنصرية الإلكترونية و اهتمام المجتمع الدولي بها.

إن استعمال جهاز الحاسوب و غيره الموصول بشبكة الإنترنت من طرف الأفراد و المنظمات لأهداف التمييز و العنصرية ظهر منذ إخراج تكنولوجيا الإنترنت إلى العالم الصناعي و الجامعات في أمريكا ثم في الدول الأخرى و بالذات منذ بداية إمكانية الاتصال عن طريق النوادي و البريد الإلكتروني. إن وضع هذه الشبكة كان سبيلا فعالا لتفشي هذه الظاهرة و الشيء الذي يجعلها أكثر تفشيا فأكثر، هو استعداد هذه التكنولوجية لإنشاء مواقع خاصة بذلك و فهرستها في دلائل و محركات بحث موصولة بروابط تحيل إلى بعضها البعض و هذا ما يجعل أي موقع موجود على الشبكة معرض لتلقي الخطاب العنصري عبرها.[37]

إن مستعملي الإنترنت الذين يرغبون في نشر الكراهية، يمكنهم استخدام هذه الوسيلة بحيث هناك العديد من نوادي الدردشة تجلب الكثير من مستخدمي الشبكة إلى تبادل الآراء و الأفكار بخصوص موضوع معين و بذلك يمكن إما الاكتفاء أو الكف عند قراءة محتوى الموقع أو الذهاب إلى حد المشاركة في الدردشة و إرسال كتابات. و النتيجة هي أن رسالات الحاملين للخطاب الكراهي تؤذي من دون شك القراء الآخرين لمحتوى هذه المواقع في مشاعرهم و أحاسيسهم سواء كانوا زوارا اعتياديين أو عارضين.

وطبعا هناك نوادي أنشئت خصيصا لتبادل و نشر الأفكار العنصرية و رسائل الكراهية، و في هذه الحالة، على الأقل، يمكن لزوار هذه المواقع معرفة مسبقا ما ينتظرهم. لكن في حالات أخرى ، عادة ما

تلوح الكراهية و الخطاب التمييزي و العنصرية من نوادي ليست لها أية علاقة بهذا الموضوع و ذلك في إطار إستراتيجية تمكن من إخفاء رسائل لا تخلوا من طابعها الكراهي و العنصري.

كما أن هناك وسيلة تستخدم كثيرا من طرف ناشري الكراهية و العنصرية و هي البريد الإلكتروني، الوسيلة الجيدة للوصول بهوية مجهولة و بتكلفة أقل إلى جمهور أوسع و ضحايا لهذا الاعتداء أكثر. و في هذه الحالة يتم التطرق لأحداث مصحوبة بتعليقات خاصة أو رواية وقائع غير حقيقية بهدف إلحاق ضرر بسمعة شخص ما مثلا، أو مجتمعا بكامله.

إن هذه الوضعية أدت بالكثير من الدارسين لهذا السلوك المنحرف إلى القول بأن الجريمة الإلكترونية أو عبر الإنترنت، هي مجال جديد في القانون الجنائي و الإجراءات الجزائية و تشمل فئتين رئيسيتين:

الفئة الأولى تلك التي تتعلق مباشرة بتكنولوجيا الإعلام و الاتصال و على رأسها شبكة الإنترنت، و ذلك بالاعتداء على أجهزتها و أنظمتها الإعلامية و من ثم تحقيق النتائج الإجرامية المتمثلة في الركن المادي لها مثل ما فصلناه في الكلام عن الإرهاب الإلكتروني و التجسس الإلكتروني.

و الفئة الثانية تشمل الجرائم التي يكون استعمال هذه التكنولوجيا في نشر المحتويات الممنوعة و أهمها تلك التي تحمل الخطاب العنصري و الكراهي و من ثم ارتكاب أفعال التمييز العنصري و نشر الكراهية في عالم و بطابع مميزين تاركة جهود الهيئات الدولية في مجال منع جريمة التمييز العنصري من غير جدوى، ما ضاعف من اهتمام المجتمع الدولي من دول و هيئات دولية، و أدى إلى حد ما إلى إجماع على وجوب التصدي لها. و في هذا الإطار نظم المجلس الأعلى لحقوق الإنسان و منظمة اليونسكو unisco، التابعين لمنظمة الأمم المتحدة أشغال ورشات في 19 و 20 فيفري 2003 في باريس، أبدوا فيها تأسفهم على لجوء بعض التنظيمات الإعلامية، باستعمالها للتكنولوجيات الجديدة في مجال الاتصال و منها الإنترنت، إلى نشر مواد تمرر من خلالها خطابات عنصرية و أخرى محرضة على الكراهية [38] . مخالفة احترام القيم الإنسانية و مبدأ المساواة و عدم التفرقة و احترام الغير و التسامح، بمنأى عن أي متابعة عقابية خاصة في بعض الدول تخلوا تشريعاتها من أي عقاب على ذلك..

و من جهة أخرى فإن الاهتمام بتجريم أفعال التمييز العنصري و نشر الكراهية عبر الإنترنت، كان قد شغل أوروبا ككل بتبنيها للاتفاقية الأوروبية حول الجرائم المعلوماتية و البروتوكول الإضافي الخاص بتجريم ممارسة العنصرية عبر الإنترنت إلى درجة أنه حسب ما جاء في نص البروتوكول أنه إذا كان للدولة الحق في عدم تطبيق بعض أحكام هذا البروتوكول، فإنه لا يحق لها ذلك بالنسبة للأحكام الخاصة بتجريم ممارسة العنصرية و الكراهية [39] باعتبار أن هذه الأخيرة تعتبر مجرمة لدى الكثير من الدول منها الولايات المتحدة الأمريكية و أنها مجرمة في صورتها التقليدية إن شئنا أن نعتبرها صورة من صورها، و هنا يمكن الرجوع إلى الاتفاقية الدولية لمناهضة العنصرية بجميع اشكالها [40] .

بالإضافة إلى ذلك فإن كل من كندا و فرنسا و سويسرا و السويد و اليابان و ألمانيا و غيرها من الدول التي نجدها إما قد انتهت إلى سن تشريعات بشأن ذلك أو سبق لها أن أصدرت أحكاما قضائية تدين هذه الأفعال العنصرية، و إما نجد ذلك يتمخض على مستوى الهيئات الرسمية و غير الرسمية التابعة لها.
بالإضافة إلى الكثير من الجمعيات و المنظمات التي لا يمكن حصرها التي قد اهتمت بمخاطر العنصرية الإلكترونية أو عبر الإنترنت.

2.3.2.1 : ممارسات العنصرية الإلكترونية.

تُعتبر العنصرية الإلكترونية أو عبر الإنترنت بصفة عامة، سلوكا متداولا لدى الكثير من المهتمين و الناشطين في هذا المجال من أفراد و جماعات ممن يحملون منطق نبذ الغير. و هو متداول بصفة أساسية لد ى الأوساط و في الظروف أين تكون الصراعات الدولية قائمة سواء على شكل عدوان أو هيمنة. و في هذه الحالة الأخيرة، تأخذ هذه الممارسات إتجاها أكثر خطورة و تصبح ترتكب هذه الأفعال برضا هذه الدول إن لم تكن من تخطيطها. ولذلك نجد يتصدر الممارسون لهذا السلوك الولايات المتحدة الأمريكية و إسرائيل و بعض الدول ممن يُعرفون بهذا السلوك كألمانيا و هولندا و غيرهما.
فأوضح تقرير مقدم إلى مؤتمر تعقده الأمم المتحدة لمناهضة العنصرية، بأن الولايات المتحدة الأمريكية تعتبر مكانا آمنا لذوي الدعوات العنصرية عبر الإنترنت فيستغل هؤلاء الأخيرين الحرية التي يكفلها القانون الأمريكي من أجل ممارسة نشاطهم الداعي إلى الكره و النازية و نبذ الأجانب، خاصة إذا علمنا أن الولايات المتحدة الأمريكية ترفض دائما المشاركة في أي آلية لفرض نوع من الرقابة على الإنترنت، ما جعلها تشهد في السنوات الأخيرة تدفق عدد من الجماعات العنصرية خوفا من التعرض للملاحقة القانونية في بلدانها. بحيث قبل هذه الفترة لم يكن هناك سوى موقع واحد للعنصرين على الإنترنت يدعى ستورم فرونت الذي يدعو إلى تفوق الجنس الأبيض، ثم بعدها ارتفع عدد المواقع ليصل إلى ألفي موقع تروج كلها للعنصرية و النازية الجديدة و معاداة السامية و من أشكال ذلك ، الأعمال العنصرية التي تحض على الكراهية [41]
وكانت قضية الترويج للكراهية العنصرية عبر موقع ستروم قد أثيرت في الولايات المتحدة خلال سنة 1995 لما أقدمت جماعة عنصرية بيضاء على إنشاء هذا الموقع بمعرفة دون بلاك و هو خبير في الكمبيوتر و عضو سابق في جماعة كوكلوكس كلان العنصرية البيضاء. و هذا الكلام يوحي أن مجرمو العنصرية التقليدية، هم نفسهم مرتكبو أفعال العنصرية الإلكترونية أو عبر الإنترنت من خلال هذا الموقع، بدليل ما صرح به هذا الخبير بأن لتجربة أثبتت أن الإنترنت وسيلة لا يمكن تعويضها لتجنيد مزيد من الأعضاء لصالح قضية البيض التي يزعم الدفاع عنها. و من هنا، فُكر في توسعة هذا العالم ليشمل تلك المواقع الأخرى و ما تضمنه من بريد إلكتروني ومساحات للحوار التي يؤكد الناشطون على أنها أصبحت وسائل لتجنيد أنصار جماعات الكراهية العنصرية وجمع التبرعات لها.

ويقدر مركز سيمون وسينثال ذلك في أحدث تقرير له، وجود ثلاثة آلاف موقع تنشط في هذا المجال من أجل ترويج العنف العرقي ومعاداة السامية والإرهاب وموسيقى الكراهية..

و بالرغم أن المركز يضغط على الشركات التي تقدم خدمات الإنترنت لحظر الوصول إلى هذه المواقع وفي مقدمتها موقع ستورم فرونت، لكن الحملة التي يقودها المركز ضد المواقع العنصرية قوبلت بانتقاد في بعض الأحيان من الجماعات المدافعة عن الحريات المدنية حيث في عام 1996 صرح الاتحاد الأمريكي للحريات المدنية، إن المركز محق في سعيه للتعريف بخطورة أنشطة المواقع العنصرية لكنه انتقد دعوته شركات الإنترنت لإغلاق هذه المواقع و أكد أنه إذا اعتبرنا المركز مؤسسة تدعو إلى التسامح فإنه لا يقبل أن يدعو للهجوم على الحرية المدنية الضرورية لمجتمع حر و متسامح، و هي حرية التعبير. إن هذا يبين مركز قوة هذه الجماعات العنصرية كونها، تستغل مبادئ القانون الدولي و مواثيقه، لتخترق مبادئ القانون الدولي و مواثيقه.[42]

إن ممارسة العنصرية في هذه الظروف جعلت مناهضوها، زيادة على تصديهم للخصوصية التقنية للوسيلة ذاتها بحيث أنه حتى أذا أصبح من الممكن فنيا إعاقة الوصول إلى المواقع العنصرية، فإن الطبيعة العالمية لهذه الوسيلة - الإنترنت- تجعل من المستحيل صدور تشريع يسمح بذلك، بل و حتى إن وجد هذا التشريع فإن تطبيقه سيكون مستحيلا في بلد يضمن حرية التعبير مثل الولايات المتحدة [36]، فإنهم من جهة أخرى، في صراع دائم من أجل إيجاد مخرج لهذه المشكلة القانونية المتمثلة في تداخل الاعتداء و مبرر الاعتداء.

و فيما يخص الولايات المتحدة دائما، ينبغي الإشارة إلى أن احتكارها لعملية إدارة الإنترنت صار يشكل إشكالية هامة عند مكافحة استخدام شبكة الإنترنت في ممارسة العنصرية بصفة عامة و في بث الكراهية الدينية بصفة خاصة. [43]

وذكرت الباحثة بياتريس متيرو في معهد القوانين المقارنة في لوزان بسويسرا أن شركة "اونلي سوليوشنز" (حلول فقط) الألمانية أحصت خمسين ألف صليب معقوف على الإنترنت ألفان منها في ألمانيا من أصل مليار موقع تم التحقق منها، مضيفة أن 85 في المائة من الرموز الفاشية كانت موجودة في مواقع أميركية. وتابعت أن هذه الظاهرة العنصرية تنتشر في السويد وفنلندا والنمسا كما في ألمانيا، وذلك خلال جلسة استماع نيابية لمشروع معاهدة أعدها مجلس أوروبا من أجل محاربة الجريمة على الإنترنت. و قالت أن الخطير في الأمر هو أن السرية والشعور بالإفلات من العقوبة يحثان أنصار العنصرية على التجمع وارتكاب أعمال عنف مثل إعداد لوائح سوداء بأسماء شخصيات يعتبرونها معادية أو تبرير هجمات عنيفة لليمين المتطرف. وختمت بالقول أن تلك المواقع مجانية ومن السهل الوصول إليها.[44]

إن ظاهرة التعبير التمييزي أو العنصري عند news groups و نوادي الدردشة و جلسات الحديث، عرفت في بلجيكا هي الأخرى لما قام شخص بنشر رسائل إلكترونية ذات محتوى عنصري في أحد نوادي الدردشة، أين حكم عليه من قبل محكمة في بلجيكا.

كما كشف التقرير السنوي 2004 للمركز الهولندي لرصد مظاهر التفرقة العنصرية عبر شبكة الإنترنت أن تلك المظاهر تزايدت بالمواقع الهولندية بنسب كبيرة للغاية، وأن المسلمين هم أكثر الفئات تضررا من التفرقة العنصرية على تلك المواقع، وهو ما اعتبره أحد الضحايا المسلمين لهذا النشاط الإجرامي "نتيجة حتمية للسياسة المتبعة من قبل الحكومة والسياسيين الهولنديين تجاه المسلمين". الشيء الذي يؤكد إمكانية ارتكاب و ممارسة العنصرية الإلكترونية أو عبر الإنترنت، بعلم الدولة و برضاها و بتخطيط منها.

وزادت حالات التفرقة العنصرية على الإنترنت في هولندا من 1300 في العام 2003 إلى 1800 حالة في العام 2004 وفقا للرصد الذي أجراه المركز الهولندي وضمنه تقريرا نشر في 25-4-2005. وأكد التقرير كون المسلمين هم الفئة الأكثر تعرضا للتفرقة العنصرية بهولندا، حيث تضاعف تقريبا عدد المواقع التي احتوت على دعوات صريحة مناهضة للإسلام والمسلمين لترتفع من 231 واقعة عام 2003 إلى 409 عام 2004. وبالتوازي مع تزايد العنصرية ضد المسلمين ارتفعت كذلك الدعوات العنصرية ضد الجاليات من البلاد التي يكثر مجيء المسلمين منها، خاصة القادمين من سورينام (بلد في شمال أمريكا الجنوبية) والأفارقة واللاجئين بصفة عامة، خاصة ذوي الشعور و البشرات السوداء.

من جهة أخرى أشار التقرير إلى أن حادث مقتل المخرج الهولندي ثيو فان جوخ على يد مغربي مسلم في نوفمبر 2004 ساهم بدرجة كبيرة في تزايد حوادث التفرقة العنصرية ضد المسلمين.

وأشار المركز الهولندي إلى أنه تقدم بـ 530 طلبا رسميا إلى مواقع إنترنت لإزالة فقرات أو مقالات أو تصريحات احتوتها تحمل دعوات للتفرقة، وتجاوب 457 منها للطلب بالإيجاب، بينما استدعى الأمر تدخل الأجهزة القضائية في حالات أخرى، ولا تزال بعض القضايا معلقة في أروقة المحاكم انتظارا للحسم بشأنها.[45]

3.1 : من أجل التجريم الدولي للاعتداءات الإلكترونية

إن الاعتداءات الإلكترونية وهي تتخذ هذه الصور المستجدة من الإجرام الدولي التقليدي، دفعت إلى التفكير في إلحاقها إلى قائمة الجرائم الدولية و هذا يعني تطويع القانون الجنائي الدولي ليشملها ما دام أنه لم يعد يوجد أي مبرر لتأخر تجريمها. و هي إذا أخذت وصف الإجرام الدولي الإلكتروني قانونا، ينتظر ألا يطرح هناك إشكال ليشملها هو الآخر القضاء الجنائي الدولي.

1.3.1 : غياب مبرر تأخر التجريم

لقد بات التجريم الدولي للاعتداءات الإلكترونية أمرا واقعا و لم يعد يقبل أي مبرر من شأنه أن يؤخر هذا التجريم لا من حيث خطورتها و لا من حيث قيام عناصر تجريمها و لا من حيث الصعوبات التي كانت تحول دون تجريم الأفعال التي كانت ترتكب باسم الدولة في ظل قانون دولي لم يكن يقر آنذاك إلا المسؤولية الجنائية الدولية.

1.1.3.1 : من حيث جسامة الخطورة و الضرر

لقد أدى انتشار وسائل الاتصال الحديثة الموصولة بالشبكات العالمية و بشبكة الشبكات المعروفة بالإنترنت إلى فرض عالم جديد و نمط آخر من الحياة و أصبح الاعتماد على هذه الوسائل يزداد يوما بعد يوم إلا أنه و إن كان لهذه الأخيرة فوائد كثيرة، فإن الوجه الآخر لها و المتمثل في استخداماتها السيئة و الضارة و منها ما سبق الإشارة إليه في هذا البحث من صور الاعتداءات الإلكترونية و ما سيأتي ذكره، أصبح خطرا يهدد العالم بأسره.

ثم أنه لا يمكن حصر مخاطر الاعتداءات الإلكترونية بصفة دقيقة لسبب بسيط هو أن انتشار الإنترنت، الوسيلة الأساسية لارتكابها، يعتبر حديثا نسبيا كما انه و لخصوصية هذه الوسيلة فان المخاطر دائما مستجدة [46]. و على هذا، فإن مخاوف الدول صارت تتعدى مسألة تدمير المواقع الإلكترونية و الحواسيب على المستوى البسيط إلى أمور مرعبة حقا و منها احتمال قيام إرهابيين إلكترونيين بإدخال فيروسات إلى شبكة الحواسيب الخاصة بالمنشآت الحساسة.[26]

فالتقدم الحاصل في مجال التكنولوجيا و أنظمة المعلومات و شيوع استخدام الإنترنت، جعل بعض المجتمعات تعتمد في تسيير أوجه مختلفة من حياتها من مرافق صناعية، البورصات و عمليات المصارف وسائل الإتصال و المواصلات و غيرها، على برامج معلوماتية تقوم بتشغيلها بشكل آلي و تلقائي و منظم. فعلى سبيل المثال يتم التحكم بحركة الملاحة الجوية و أنظمة السلامة في المطارات و تسيير القطارات و مواعيدها و خطوطها، إدارة و تشغيل مرافق توليد الطاقة و السدود و مصافي النفط، التحكم بأنظمة إطلاق الصواريخ و توجيهها و الأسلحة النووية و البيولوجية و الكيميائية و محطات إنتاجها، إدارة صناعة الأدوية و ما إلى ذلك بواسطة برامج معلوماتية متصلة معظمها ببعضها بواسطة شبكات كشبكة المعلومات العالمية شبكة الشبكات.

و عليه فإن العبث بأي من هذه الأنظمة عبر الدخول غير المشروع أو غير ذلك من الوسائل قد يتسبب بأضرار وخيمة و كارثية، من الأمثلة على ذلك :

- التسبب بسقوط الطائرات أو تصادمها عبر تزويدها بمعلومات ملاحية خاطئة أو تعطيل وسائل التحكم الإلكترونية فيها.
- التلاعب بالبرامج التي تتحكم بأجهزة تصنيع الدواء ينتج عنه فوضى في المقادير المستخدمة و بالتالي التسبب بأضرار صحية جسيمة لا يتم اكتشاف سببها إلا متأخرا و بعد فوات الأوان.
- تعطيل عمل محطات الكهرباء و المياه و شبكات الاتصال و الأنظمة المصرفية و البورصة.
- التلاعب بأنظمة تشغيل و إطلاق أو توجيه الصواريخ الإستراتيجية و أسلحة الدمار الشامل الذي قد يتسبب بإطلاقها عشوائيا مما ينتج عنه من دمار و ردود محتملة قد تقود إلى حرب كونية.
- التسبب بتعطيل عمل المحطات النووية و الكيميائية و البيولوجية أو عملها على نحو غير صحيح و ما قد ينتج عن ذلك من تسرب للإشعاعات و المواد الخطرة.

إن هذه الأخطار هي حقيقة و ليست أبدا من قبيل الخيال العلمي و إذا كانت نسبة تحققها صعبة و أنها ليست شائعة حتى اليوم إلا أنها تبقى ممكنة.

و بالنظر إلى ما قد يترتب من خسائر هائلة من الأرواح و الممتلكات فإنها تعتبر من قبيل " القوة التي حظرت المادة 02 فقرة 04 من ميثاق الأمم المتحدة على الدول اللجوء إلها أو مجرد التهديد بذلك. فمعنى "القوة" لا يجب أن يقتصر على الأسلحة التقليدية أو غير التقليدية التي عرفتها البشرية حتى اليوم، و إنما كل ما يترتب على استخدامه من خسائر في الأرواح و الممتلكات. هذا و قد أشارت الأمم المتحدة مرارا إلى " خطر استخدام الجماعات الإرهابية لتكنولوجيا الاتصالات "، و دعت إلى " النظر في المخاطر المتمثلة في استعمال الإرهابيين للنظم و الشبكات الإلكترونية.[47]

و ما يزيد من شدة خطورة الاعتداءات الإلكترونية و الجريمة عبر الإنترنت عامة و جسامة الضرر اللاحق من جرائها، هو ما طرأ عليها من تطورات حيث لم تعد تنحصر في تلك الصورة البسيطة التي يرسمها البعض لأنماط الجريمة الإلكترونية وأشكالها و إنما أبدع مخططوها في ابتكار أساليب يصعب اكتشافها و ملاحقة مرتكبيها.

ويقول خبراء مكافحة الجرائم الدولية و الإنتربول، أن هناك تطورا ملحوظا طرأ على أساليب جرائم الإنترنت البسيطة والتي تشمل صناعة ونشر الفيروسات، الاختراقات، تعطيل الأجهزة، انتحال الشخصية، المضايقة والملاحقة، التغرير والاستدراج، التشهير وتشويه السمعة، ،وجرائم النصب والاحتيال و غير ذلك مما سبق الإشارة إليه. حيث أن هذه الأنماط لم تعد هي الأشكال الوحيدة للجريمة عبر الإنترنت، نظرا للدور الأكثر خطورة الذي لعبته هذه الوسيلة، أي الإنترنت، عن طريق مثلا، التشجيع على الانتحار، فصارت جرائم القتل و

الاغتصاب ترتكب ارتكابا إلكترونيا لاستخدام عصابات دولية لمواقع أنشأتها لهذا الغرض تعرض من خلالها خدماتها لمن يريد تصفية الخصوم أو إذلالهم و إهانتهم عن طريق اغتصاب زوجاتهم أو بناتهم.

وتؤكد إحدى منظمات مكافحة جرائم الشبكة الإلكترونية أن إحدى هذه العصابات حققت أرباحا هائلة من وراء أنشطتها الإجرامية، ويقدر التقرير أرباح هذا الموقع بـ 3.6مليون يورو خلال سنتين فقط، مقابل 58% من الجرائم التي تم اكتشافها!

وفي مصر ، اكتشفت الشرطة أن إحدى هذه العصابات وراء لغز اختفاء طفل كان قد حير أجهزة البحث طويلا، حيث قامت أمه الأمريكية بتأجير محترفين عبر الإنترنت لاختطاف ابنها من مصر وإحضاره بجواز سفر مزور إلى أمريكا انتقاما من والده الذي طلقها وحصل على حكم قضائي بحضانة الطفل. وتشير المعلومات إلى أن هذه الأنشطة لم تعد تمارس من وراء الستار كما كان الحال سابقا، حيث كانت العصابات تضطر إلى التخفي وتمارس نشاطها عبر مواقع الزواج أو غرف الدردشة، فقد أصبحت الآن تعرض خدماتها عيانا وتحصل على المقابل عن طريق الدفع بالفيزا كارد، وإن تعذر ذلك بسبب كثافة الملاحقة الأمنية، فيمكنها الاتفاق على وسائل أخرى، وقد سجل العام الماضي نشاطا تجاريا من هذا النوع حجمه 500 مليون يورو. ويعرض أحد هذه المواقع "في جنوب أفريقيا" خدمات القتل والاغتيال للزبائن من رواده، ويؤكد أن لديه أعضاء مدربين جيدا على القيام بعمليات التصفية الجسدية دون ترك أي آثار تدل فرق البحث إلى مرتكب الجريمة، ويؤكد الموقع أن خطط تنفيذ الجرائم لا يضعها أشخاص عاديون، بل هم خبراء في هذا النوع من التخطيط، ومعظمهم من رجال الشرطة والمخابرات السابقين.[48]

كما يمكن النظر للانترنت كمهدد للأمن الاجتماعي وخاصة في المجتمعات المغلقة والشرقية، حيث أن تعّرض مثل هذه المجتمعات لقيم وسلوكيات المجتمعات الأخرى قد تسبب تلوثا ثقافيا يؤدي إلى تفسخ اجتماعي و انهيار في النظام الاجتماعي العام لهذه المجتمعات. إن الاستخدام غير الأخلاقي و اللاقانوني للشبكة قد يصل إلى شرائح واسعة من المراهقين والهواة عبر دول العالم مما يؤثر سلبا على نمو شخصياتهم النمو السليم ويوقعهم في أزمات نمو، وأزمات قيمية لا تتماشى مع النظام الاجتماعي السائد، وبخاصة عند التعامل مع المواضيع الجنسية وتقديم الصور والمواد الاباحية".[46]

إن الاعتداءات الإلكترونية كظاهرة جديدة التي رأينا كيف يمكن أن تشكل جريمة دولية، تهدد بمخاطر متفاوتة الدرجة تتفاقم بمرور كل يوم ملحقة أضرارا جسيمة على الأفراد و المنظمات و الدول، الشيء الذي يبطل أي مبرر يدعي تأخر تجريمها دوليا.

2.1.3.1 : من حيث توفر الأركان

الجريمة بصفة عامة لابد لقيامها من توافر ثلاثة أركان و هي الركن الشرعي و الركن المادي و الركن المعنوي. أما الجريمة الدولية فيشترط فيها، إضافة إلى الأركان السابقة، الركن الدولي الذي يميزها عن الجريمة الداخلية. و إذا كنا في هذا البحث بصدد دراسة الجرائم الدولية الإلكترونية، فإننا نحاول إبراز مدى توفر كل هذه الأركان في بعض أفعال الاعتداءات الإلكترونية من عدمه. و إذا كان من الأصح إثبات هذه الأركان لكل فعل على حده، فإنه لكثرة عدد هذه الأفعال و ترشحها لتكون أكثر، نتناول هذه العناصر بصفة مجملة، مرجئين الكلام عن الركن الشرعي إلى المطلب الثاني من هذا المبحث.

أولا : الركن المادي

يعرف الركن المادي للجريمة بأنه المظهر الخارجي للجريمة و يتمثل في سلوك إجرامي معين يتطلبه القانون كمناط للعقاب على هذه الجريمة. على أن تتحقق عن هذا السلوك الإجرامي نتيجة ضارة تربطه بها علاقة سببية و هو ما يطلق عليه " الإسناد المادي". [49] [06]

فيقصد به إذا، السلوك أو العمل أو الفعل المحظور الذي يصيب المصالح الدولية بضرر أو يعرضها للخطر و هو غير النوايا التي لا عقاب عليها و ذلك أن القانون لا يعتد بالنوايا و لو كانت خبيثة قبل أن تتجسد في أفعال مادية موجهة لارتكاب الجرائم. [50]

و في الجريمة الإلكترونية التي سميت بالجريمة المعلوماتية، طبيعة الركن المادي فيها يطرح إشكالا عمليا، فهذه الجريمة تظهر سلوكا غير مشروع أو غير أخلاقي أو غير مصرح به، و يتعلق بالمعالجة الآلية أو الإلكترونية للبيانات كنقلها وسرقتها أو إساءة استخدامها عن تعمد حيث يتسبب ذلك في خسارة تصيب المجني عليه. و نستخلص كيفيات توافر الركن المادي في الجريمة الإلكترونية من عدة حالات نشير إلى بعضها فيما يلي :

فيقوم الركن المادي للجريمة الإلكترونية مثلا في حالة الدخول غير المصرح به إلى نظام الحاسب الآلي و المعلومات التي يحتوي عليها، بفعل الدخول ذاته و ما يترتب عليه من خسائر و إضرار بمحل الدخول الذي يتعدد إلى ثلاث صور، وهي المعلومات و النظام الآلي و الشبكة.[51]

كما يقوم الركن المادي للجريمة الإلكترونية ببعدها الدولي في جريمة نشر الفيروسات، حيث أسفرت تطبيقات برامج شركات مكافحة الفيروسات الشهيرة مثل McAfee وشركة Norton أن عدد الفيروسات يتراوح ما بين 50 إلى 60 ألف فيروس تتحرك عبر شبكة

الإنترنت. و يسبب إنتشار الفيروسات خسائر اقتصادية هائلة و يعطل حركة الشبكة العالمية و يساهم في إضعاف ثقة المستخدمين بها. و تختلف قوة ضعف هذه الفيروسات بحسب آلية عملها و برمجتها و هدف مصممها منها.

أو في ما تناولناه بالتفصيل في هذه الدراسة في صور الإجرام الدولي الإلكتروني و الذات في ظاهرة الإرهاب الإلكتروني أو الإرهاب التقني حيث يتحلى هذا النوع من الجرائم قيام الركن المادي لها بعنصريه الفعل و الضرر حيث يعد اقتحام المواقع و تدميرها و تغيير محتوياتها و الدخول على الشبكات و العبث بمحتوياتها بإزالتها أو بالإستلاء عليها أو الدخول على شبكة الطاقة أو شبكات الاتصالات بهدف تعطيلها عن العمل أطول فترة ممكنة أو تدميرها نهائيا،[14] أفعالا غير مشروعة يقوم بها الجناة بل يعتبر أفعالا غير مشروعة أيضا ما يقوم به الإرهابيون اليوم من عدوان عن طريق شبكة المعلومات العالمية الذي يتمثل في جعل هذه الشبكة منفذا مهما يوظفه الإرهابيون خدمة لمخططاتهم الفكرية و العملياتية سواء من حيث الترويج أو الاتصال و التنسيق و تعلية الفكر العنيف و التحريض على الإرهاب و تحميل ملفات الفيديو المصورة لعمليات تركيب المتفجرات و نسف الجسور و اغتيال الشخصيات و غيرها و كلها لا تقل خطورة على الفعل المادي للإرهاب لأن التحريض على الجريمة هو جريمة. [46]

فنلاحظ من خلال كل ما سبق كيف لبعض الجرائم الإلكترونية أن تأخذ مستوى الجريمة الدولية مثل جريمة الإرهاب الدولي من جهة و من جهة أخرى كيف للركن المادي يمكن أن يتوافر بعنصريه الفعل و الضرر.

ثانيا : الركن المعنوي

يقصد بالركن المعنوي الجانب الشخصي أو النفسي في الجريمة، فلا تقوم الجريمة بمجرد قيام الواقعة المادية. إذ لا بد من أن تصدر هذه الواقعة عن إرادة فاعلها و أن ترتبط به ارتباطا معنويا أو أدبيا. فالركن المعنوي للجريمة يتمثل في قيام هذه الرابطة المعنوية أو الصلة النفسية أو العلاقة الأدبية التي تربط ماديات الجريمة بنفسية الفاعل بحيث يمكن أن يقال بأن الفعل المقترف هو نتيجة إرادة الفاعل [06]. إن ضرورة وجوب توافر الركن المعنوي أمر لا جدال فيه لقيام الجريمة الدولية و لكن الإرادة و العقل و التمييز هي صفات طبيعية لا تثبت في حقيقة الحال إلا للأفراد [06]، ويقصد بالأفراد هم الأشخاص بغض النظر عن مركزهم فيما إذا كانوا أشخاصا طبيعيين أو أفراد عاديين أو كانوا كبار مسؤولين في دولة معينة فأينما كانوا يتم مساءلتهم في حالة ارتكابهم جرائم دولية و قد رأينا في تعرضنا للركن المادي كيف تأرجح من يكون مقترف الجرائم الدولية الإلكترونية بين فرد عادي و مسؤول

كبير في الدولة و لذلك لما نثير مسألة الركن المعنوي للجريمة فإننا عن هؤلاء نتكلم، و هل هناك رابطة نفسية بينهم كجناة و بين أفعالهم. هذه الرابطة النفسية التي يعبر عنها بالقصد الجنائي الذي يعكس الإرادة المضادة للمجتمع و هو، أي القصد، نية ارتكاب الجريمة أو اتجاه الإرادة إلى ارتكاب الجريمة مع ضرورة أن يكون المجرم على علم بارتكابها.

فيقصد بالإرادة و العلم في الجريمة الإلكترونية، أن تتجه إرادة الجاني إلى إتيان الفعل مع علمه بأنه يقوم بعمل يعاقب عليه القانون و ذلك بغض النظر عن الباعث و الدافع لاقترافها. كمن يقوم بالتزوير و التقليد و السرقة في البيانات المعالجة إلكترونيا و برامج النظم المعلوماتية و شبكة الإنترنت و بيئة الاتصالات التكنولوجية الرقمية الحديثة.

أ- الإرادة : و هي تلك القوة النفسية التي تتحكم في سلوك الإنسان، فهي نشاط نفسي يصدر عن وعي و إرادة لبلوغ هدف معين فإذا توجهت هذه الإرادة المدركة و المميزة عن علم و حرية لتحقيق الواقعة الإجرامية بسيطرتها على السلوك المادي للجريمة و توجهت نحو تحقيق نتيجة. و للإرادة دور بالغ في تحديد المسؤولية عن الفعل فإن قام بأفعال مجرمة قانونا بإكراه أو أي عيب في إرادته ووجود موانع المسؤولية فلا يمكن مساءلته و معاقبته عليها.

ب- العلم : إن إرادة الجاني تتجه لتحقيق الفعل الإجرامي و يقصد بالعلم، إدراك الأمور على نحو صحيح مطابق للواقع، و من ثم ينبغي أن يعلم الجاني بأن أركان الجريمة متوافرة و أن القانون يعاقب عليها. و العلم بالقانون هو علم مفترض لدى العامة و بالتالي لا يجوز الدفع بالجهل بالقانون

فمن يقوم بجريمة معينة تتمثل في اعتداء إلكتروني على بيانات أو برامج أو مواقع أو إساءة استعمالها على نحو غير مشروع يكون قد ارتكب جريمة عمدية إذا كان يعلم أن فعله سيؤدي بالإضرار إلى الغير. إذ يكفي توقعه للنتيجة لقيام القصد الجنائي لديه. فليس للجاني في هذه الحالة أن ينفي قصده الجنائي اعتمادا على أنه لم يكن يريد النتيجة [52].

إن الممارسات المستجدة للجرائم الإلكترونية جسدت في كثير من الأحيان قيام الركن المعنوي فيها. حيث أنه زيادة على كون بعض الجرائم الدولية التقليدية التي ضبطها القانون الدولي الجنائي أو نظام روما الأساسي للمحكمة الجنائية الدولية مثل جريمة الفصل و التمييز العنصري، نجد أن مثل هذه الجريمة صار بالإمكان أن ترتكب إلكترونيا عن طريق استعمال شبكة الإنترنت العالمية، المسرح الملبي لرغبات العنصريين الإجرامية لما يمكنهم من تفعيل تصرفاتهم الإجرامية أكثر و من تحقيق نتائج أكبر. هذه الجريمة التي هي من أخطر الجرائم الدولية حيث تناولتها العديد من المواثيق و القرارات و الاتفاقيات الدولية، أين أكدت المادة

الأولى من الاتفاقية الدولية لقمع جريمة الفصل العنصري و المعاقبة عليها الصادرة عن الجمعية العامة للأمم المتحدة في 30 نوفمبر 1973 على أن الفصل العنصري جريمة ضد الإنسانية و أنها انتهاك لمبادئ القانون الدولي و تشكل تهديدا للسلم و الأمن الدوليين ، كما اعتبرت الاتفاقية الدولية للقضاء على جميع أشكال التمييز العنصري و التي اعتمدتها الجمعية العامة بقرارها الصادر في 21 ديسمبر 1965، و التي جاء في مادتها الأولى أنه يقصد بتعبير التمييز العنصري في هذه الاتفاقية أي تمييز أو استثناء أو تقييد أو تفضيل يقوم على أساس العرق أو اللون أو النسب أو الأصل القومي أو الإثني و يستهدف أو يستتبع تعطيل أو عرقلة الاعتراف بحقوق الإنسان و الحريات الأساسية أو التمتع بها أو ممارستها على قدم المساواة في الميدان السياسي أو الاقتصادي أو الاجتماعي أو الثقافي أو في أي ميدان آخر من ميادين الحياة العامة، و قد اعتبرت هذه الاتفاقية جميع الأعمال العنصرية و التحريض عليها أو النشاطات الدعائية لها بمثابة جريمة يعاقب عليها القانون (المادة 5) [53].

إن ما يثير الاهتمام أن الإجرام التقني أو الإلكتروني جعل من الركن المعنوي في هذه الجريمة الدولية، التمييز العنصري، يأخذ منحى متميزا إذ صار القصد الجنائي بصورتيه العام و الخاص أعم و أشمل و أوضح و من ثم أخطر حيث إذا كان النازيون قد مارسوا تصرفاتهم العنصرية الداعية إلى تفوق العنصر الجرماني على غيرهم من الأجناس المقيمين في أرض الدولة الألمانية، فإنهم اليوم يستعملون التقنية الحديثة المتمثلة في شبكة الإنترنت العالمية ليمارسوا تصرفاتهم العنصرية التي يحرمها القانون الدولي ضد غيرهم من الأجناس ليس فقد المقيمين على أرض دولة ألمانيا بل في العالم أجمع حيث ما كانوا و حيث ما وجدوا و من هذا المثل يتبن لنا كيف أن فئة المجنى عليهم إلكترونيا أصبحوا مستهدفين ليس فقط في ناحية أو منطقة معينة تقرب إقليميا من الفئة الجانية كما كان في السابق و أنما حيث ما وجد لهم أثر في العالم كله و بهذا أصبح القصد الخاص يأخذ مفهوما عالميا و كأن أصابه مس من العولمة بل الأمر كذلك فنحن في عصر عُولم فيه العدوان و عولمت فيه ماهية العدو و المعتدى عليه فكلاهما صار له مفهوما عالميا و أن هذه المدلولات تأخذ شكلا أوضح و أبلغ في العالم الافتراضي عنه في العالم الواقعي و لا يقصد بالعالم الافتراضي غير عالم الاتصالات الإلكترونية بشتى أنواعها.

و الجريمة الدولية الإلكترونية جريمة قصدية يتخذ الركن المعنوي فيها صورة القصد الجنائي المتمثل في العلم و الإرادة بحيث يجب أن تتجه نية و إرادة الجاني إلى ارتكاب فعل الإدخال أو الدخول أو المحو أو التعديل للمعطيات أو التجسس عليها أو نشرها لغاية يجرمها القانون الدولي الجنائي مع علم الجاني بنشاطه الإجرامي.

ثالثا : الركن الدولي

إن الركن الدولي، هو أحد أركان الجريمة الدولية التي تطرق إليها الفقه أو اعتادت المواثيق و الهيئات الدولية تعدادها. إذ أن تخلف هذا الركن يسقط عن الجريمة صفتها الدولية و هي تتميز به عن الجرائم الداخلية [06]. و في كل الحالات لاحظنا كيف أن هذا الركن تتعدد زوايا قيامه بين وجوب ارتكاب الجرائم بناء على تخطيط من جانب إحدى الدول المتحاربة و تنفيذ من أحد مواطنيها أو التابعين لها أو مرتزقة، باسم الدولة أو برضاها، ضد مؤسسات أو آثار دولة أخرى و هذا في جريمة الحرب مثلا، حيث يجب أن يكون كل من المعتدي و المعتدى عليه منتميا إلى دولة في حالة نزاع مسلح (حرب) مع الأخرى.

و بين أن يكفي لقيام هذا الركن كون الجريمة قد وقعت تنفيذا لخطة مرسومة من جانب الدولة ضد جماعة بشرية يجمعها عقيدة معينة أو رباط معين و لا يشترط انتماءها إلى دولة أخرى و هذا في الجرائم ضد الإنسانية.

و بين أن يقوم الركن الدولي بأن ترتكب الجريمة بناء على خطة مرسومة من الدولة ينفذها المسؤولون الكبار فيها أو تشجع على تنفيذها من قبل الموظفين أو ترضى بتنفيذها من قبل الأفراد العاديين ضد مجموعة أو جماعة من الأفراد تربطهم روابط خاصة و هذا في جرائم الإبادة.

كما لاحظنا كيف لهذا الركن أن يتوافر في حالة ما إذا كان الجاني تابعا لدولة و المجني عليه تابعا دولة أخرى أم تابعين لدولة واحدة في ممارسة التفرقة العنصرية من طرف فئات من الأفراد و هذا في جريمة الفصل أو التمييز العنصري.

أما و نحن في معرض الكلام عن الجريمة الدولية الحديثة أو العصرية و بالذات عن الجريمة الدولية الإلكترونية، التي بحكم طبيعتها هي جريمة لها بعد و امتداد دوليين [52]. ما يرشحها لأن تتقابل فيها الدول ممثلة في مجموعة أفراد عاديين أو كبار مسؤولين سياسيين أو عسكريين بل و حتى في رؤسائها؛ فسوف نلاحظ أن منها ما ترقى لأن يتوافر فيها الركن الدولي بالمفهوم الذي ورد في الجرائم التقليدية من دون أن ينتقص من قيمته شيء خاصة في بعض الجرائم الإلكترونية ذات الجسامة و الخطورة الكبيرتين التي تمس بأمن و سلامة الدول و الأنظمة و شعوبها. فلقد انتشرت الجريمة الدولية الإلكترونية و تعممت و أفرزت صورا حديثة للإجرام.

إن ظاهرة الاختراقات الإلكترونية مثلا، لم تعد تقتصر على ما يقوم به الهواة العابثين HACKERS حيث هدفهم في ذلك هو العبث بالمحتويات أو إلغاء بعضها أو كلها، و إنما تعدت ذلك ليصبح القائم بتلك الاختراقات هي أجهزة المخابرات في بعض الدول للتجسس على

دولة أخرى. حيث بدأت محاولات اختراق شبكات الكمبيوتر منذ سنوات عديدة و استهدفت شركات الكمبيوتر و الهاتف و الجامعات و مكتب التحقيقات الأمريكي، و البنتاجون و وكالة الفضاء الأمريكية و غيرها، لكن معظم هذه المحاولات كانت فردية، أبطالها شباب صغار يحاولون إثبات إمكانياتهم، و الحصول على أسرار تقنية تساعد في تعميق مواهبهم، ثم تكونت في الولايات المتحدة و بعض البلدان الغربية منظمات أطلقت على نفسها تسمية – الهاكرز – تتخصص في اختراق شبكة الكمبيوتر. و تعمل معظم هذه المنظمات بشكل شرعي و يتعاون بعضها مع مكتب التحقيقات الفيدرالية الأمريكي لتتبع و اكتشاف الثغرات الموجودة ضمن برامج الشبكات المستخدمة بالفعل. و لهذه المنظمات دورا تلعبه برعاية أمريكية تتمثل في تنظيم حملات لاختراق شبكات بعض البلدان التي تتعارض سياستها مع السياسة الأمريكية تحت شعار الدفاع عن حقوق الإنسان أو التصدي للدكتاتورية [16].

و الحقيقة أن عمليات اختراق الشبكات و التي تهدد الأمن القومي ليست قاصرة على دولة بعينها، فكما وقعت في الولايات المتحدة الأمريكية، فقد وقعت أيضا في دولة الإمارات العربية المتحدة و جمهورية الصين و استهدف العراق بها رغم تدمير بنيته التحتية بما فيها شبكة الاتصالات، و امتدت كذلك إلى اليابان و إلى كند و إلى بلدان أوربية أخرى عديدة.

لكن المشكلة الكبرى تكمن في محاولات التجسس الدولي التي تنقل أسرار دولة بأكملها إلى دولة معادية لها، ذلك أن الجاسوسية التقليدية تحولت في العصر الحديث إلى عمليات تجسس إلكترونية و اختراق لأنظمة و شبكات الدول بعضها بعضا [16].

و إن كان هذا جانب من جوانب الإجرام الإلكتروني الدولي، ففيه ما يدل على توافر الركن الدولي الذي يتمثل في تدخل الدول عن طريق أفراد عاديين أو مسؤولين أو منظمات خاصة لتقوم بهذه الجرائم.

3.1.3.1 : من حيث إقرار مسؤولية الفرد الجنائية عن الجريمة الدولية

إذا كانت الجرائم الدولية التي استقر عليها القانون الجنائي الدولي انتهاء بميثاق روما الأساسي مقتصرا على الأخطر منها، قد لزمها قرن من الزمن من أجل الاتفاق على تجريمها، فإن ذلك يرجع إلى أن القواعد العامة للقانون الدولي لم تكن تقر آن ذاك مسؤولية الفرد الجنائية عن أعمال الدولة بل كانت المسؤولية الجماعية هي الأثر الوحيد الذي يرتبه القانون الدولي عن خرق الدولة لالتزاماتها الدولية ويأتي هذا المبدأ تطبيقا لمبدأ آخر من مبادئ القانون الدولي العام

يقضي بعدم خضوع أعمال الدولة لولاية دولة أخرى، وبعبارة أخرى عدم خضوع أعمال الدولة للاختصاص الجنائي أو المدني لدولة أخرى.

والمبدأ الأخير ينبع من مبدأ المساواة التامة بين الدول وعدم خضوع أية دولة لسلطان دولة أخرى، و نظرا لكون الدولة شخصا معنويا لا يمكنها القيام بأعمال، فإن خضوع الأفراد الموكلين بتنفيذ تلك الأعمال للقضاء الأجنبي لغرض مساءلتهم هذا يعني خضوع الدولة نفسها لسلطان دولة أخرى وهذا ما يخالف القواعد العامة للقانون الدولي،[01] فلم يكن يقبل أن يحاكم قادة ورؤساء الدول الذين عادة هم من اقترفوا تلك الجرائم ولا أن يتم تنفيذ الأحكام ضدهم.

وبالرغم أن هناك من يقول أن أول سند تضمن أحكاما تتعلق بمسؤولية الفرد الجنائية يرجع إلى المادة 227 من معاهدة فرساي الدولية لـ 28 جوان 1919 باعتبارها كرست مبدأ المسؤولية الجنائية الفردية لما أدانت الدول المنتصرة في الحرب العالمية الأولى امبراطور ألمانيا "غليوم" لإرتكابه الجريمة العظمى ضد الأخلاق الدولية وقدسية المعاهدات، حيث أن نفس المعاهدة أخذت بالحسبان إنشاء محكمة خاصة من أجل ذلك التي بقيت مجرد محاولة [09].

إلا أن هناك من يرى أن قواعد القانون الدولي لم تكن تقرر مسؤولية الفرد الجنائية عن الجرائم الدولية قبل نفاذ معاهدة لندن 1945 حيث لما جاءت المادة 227 من معاهدة فرساي بالمسؤولية الجنائية الشخصية لإمبراطور ألمانيا عن الجريمة التي اقترفها، لم تُجرَ تلك المحاولة بدون موافقة ألمانيا، حيث صادقت الأخيرة على معاهدة فرساي ومنحت موافقتها على محاكمته أمام محكمة دولية. ذلك لأن هذه الموافقة تعتبر ضرورية ومنسجمة مع القواعد العامة للقانون الدولي السائد آنذاك والتي تقضي بأن أية دولة لا يمكنها أن تُخضع لولاية محاكمها الجنائية أو المدنية أعمال دولة أخرى دون موافقة الأخيرة [01].

فجاءت **إذاً** معاهدة لندن لأول مرة في تاريخ القانون الدولي حينما نصت على المسؤولية الجنائية الفردية عن الجرائم ضد السلام والجرائم ضد الإنسانية التي ترتكبها أجهزة الدولة وذلك دون الاعتداد بالصفة الرسمية لمتركبيها كمانع يحول معاقبتهم. وهذا ما عبرت عنه المواد 7 ، 8 من ميثاق محكمة نورنبرغ الملحق باتفاقية لندن، فنصت المادة 7 بأن (الوضع الرسمي للمتهمين سواء كانوا رؤساء دول أو موضفين مسؤولين في أقسام الحكومة سوف لا يكون عذرا يعتد به لإعفائهم من المسؤولية أو تخفيف العقاب). كما نصت المادة 8 من الميثاق المذكور على أن (حقيقة كون المتهم قد تصرف طبقا لأوامر حكومته أو رئيسه الأعلى أمر لا يعفيه من المسؤولية) ونصت المادة 6 من ميثاق المحكمة العسكرية الدولية في الشرق الأقصى على ما

يلي (لا الوضع الرسمي للمتهم ولا حقيقة كونه قد تصرف بناء على أوامر صادرة من حكومته أو رئيسه الأعلى، تكون بوحدها كافية لإعفائه من المسؤولية عن أية جريمة متهم بها.

فتم صياغة المادة 7 تجسيدا للمبادئ المسماة، "مبادئ نورنبرغ" التي تم فيما بعد تعديلها من طرف لجنة القانون الدولي وعرضت على الجمعية العامة للأمم المتحدة لعام 1950 في إطار أولى الأشغال تتعلق بسلطة قضائية دولية.

وعلية كان لمعاهدة لندن أثر كبير في تطوير القانون الدولي في هذا المجال إذ كانت بمثابة الأساس في تثبيت وتطوير مبدأ المسؤولية الجنائية الفردية عن أعمال الدولة في القانون الدولي، هذا الأمر فان إليه الأمين العام للأمم المتحدة في تقريره الذي رفعه إلى الجمعية العامة للأمم المتحدة في 24 أكتوبر سنة 1946، و الذي أشار فيه إلى أن (من الأمور المهمة جدا جعل المبادئ التي طبقت في محاكمات نورنبرغ جزءا من القانون الدولي بالسرعة الممكنة) فهي جاءت تعبيرا عن رغبة المجتمع الدولي في إخضاع الأفراد الذين روعوا أمنه وطمأنينته إلى دائرة العدالة الجنائية وذلك عن طريق إنشاء محكمة جنائية دولية أخذت على عاتقها مهمة إنزال العقوبات بهم.[01]

وبعد ظهور العدوان الإلكتروني الذي رأينا كيف يمكن أن يشكل جريمة دولية تترامى خطورتها في اتجاه غير متوقف بفعالية أكبر وتكلفة أقل، فإنه بفضل تطور القانون الجنائي الدولي بإقراره مسؤولية الفرد الجنائية عن الجريمة الدولية من جهة وانتفاء ضرورة أن يكون مرتكبوا الجريمة هم القادة من الدول أو من يخضعون لأوامرهم، نظرا للإمكانيات التي يتطلبها ارتكاب الجريمة الدولية والتي لم تكن مملوكة إلا لدى الدولة على عكس إمكانيات ووسائل ارتكاب العدوان الالكتروني التي هي في متناول أي فرد يفكر في ارتكاب جريمة دولية، فإنه لم يعد يُبَرَر أي تأخر في تجريم أفعال الاعتداءات الالكترونية هذه وتدارك خطورتها عن طريق إدراج الأخطر منها على الأقل في اختصاص القضاء الجنائي الدولي.

2.3.1: إمكانية طرح الإجرام الدولي الإلكتروني أمام القضاء الدولي الجنائي

إذا كان التجريم الدولي للاعتداءات الإلكترونية يعني وضع الإطار القانوني الذي يعالج هذا السلوك و يضع له نصوصا، تصفه و تجرمه، فإن من وراء ذلك غاية لا شك أنها تتمثل في تهييئه للقضاء الجنائي الدولي من أجل ملاحقته و من ثم منع الإفلات من العقاب.

و أمام الوضعية التي أثرناها فيما يخص تأخر التجريم التشريعي الدولي له، و إلى حين ذلك، هل من إطار قانوني يمكن من جهة من طرح هذه الظاهرة أمام القضاء الجنائي الدولي، و من جهة أخرى، هل يمكن أن يكون للمحكمة الجنائية الدولية الآلية الوحيدة، دورا في ذلك.

1.2.3.1 : من حيث الإطار القانوني

لا شك أن تحديد الإطار القانوني للإجرام الدولي الإلكتروني ضمن مبادئ و قواعد القانون الدولي سيسهم في بيان المركز القانوني له ، و لن يتأتى ذلك إلا باستقراء القواعد القانونية الدولية ذات الصلة ، و نعتقد أن ذلك يكون و بالضرورة بالرجوع إلى المصادر الأساسية للقانون الدولي المنصوص عليها في المادة 38 من النظام الأساسي لمحكمة العدل الدولية ، و التي تتمثل في المعاهدات الدولية و العرف الدولي ، و مبادئ القانون العامة المعترف بها من قبل الأمم المتمدنة. [54]

هذا من جهة ومن جهة أخرى لا يمكن لفعل ما أن يشكل جريمة دولية ما لم تكن هناك قاعدة قانونية دولية تقرر ذلك و هذا ما أشار إليه النظام الأساسي للمحكمة الجنائية الدولية [53]، في الباب الثالث تحت عنوان " المبادئ العامة للقانون الجنائي " ، حيث تنص المادة 22 في فقرتها الأولى تحت عنوان " لا جريمة إلا بنص " على أنه : (لا يسأل الشخص جنائيا بموجب هذا النظام الأساسي ما لم يشكل السلوك المعني وقت وقوعه جريمة تدخل في اختصاص المحكمة).

و لدراسة هذه المسائل، ينبغي أن نتعرض لدراسة و تحديد القواعد القانونية الدولية القاضية بتجريم الأفعال التي تقع بواسطة المعلوماتية و في العالم الافتراضي عموما حينما تكون بطريقة مخالفة للقوانين التي تنظم استعمال التكنولوجية و التقنية الحديثة و هذا يقتضي التعرض إلى القواعد الإتفاقية و المبادئ العامة للقانون المعترف بها من قبل الأمم المتمدنة .

لقد تعذر على المجتمع الدولي أن يتوصل إلى إبرام اتفاقية دولية تكون بمثابة الإطار الذي من خلاله يتم العمل على مكافحة الإجرام الإلكتروني ، و لكن يمكن أن نلاحظ الجهود المبذولة و المتلاحقة التي باتت تأخذ شكل اتفاقيات جماعية تعنى بتجريم أفعال محددة تعتبرها مظهرا للإجرام الدولي و تحمل في طياتها التزامات معينة على الدول الموقعة عليها لمكافحة هذه الجرائم و تقديم مرتكبيها إلى المحاكمة.

لا شك أن أعمال القرصنة التي تتم بواسطة المعلوماتية تنطوي على مخالفة جسيمة لمبادئ و أحكام القانون الدولي ، فهي تعرض حقوق الإنسان إلى الإنتهاك خاصة في جانب الحياة الخاصة للإنسان، بجعله هدفا مباشرا من أهداف نشاط ذي طبيعة غير شرعية، و بالتالي فإنها تشكل خطرا جديا على حق من الحقوق الجوهرية للإنسان بما يجعلها ضارة بالمصالح الأساسية للمجتمع الدولي و لذلك يجب مكافحتها و على هذا الأساس [55]. و لكن هل يعني هذا بالضرورة، أن تكون أعمال الاعتداءات الإلكترونية ، دائما و أبدا من قبيل الأعمال المجرمة

دوليا ؟ أم أنه يلزم لذلك أن يكون الاعتداء على سلامة المعلومات منطويا على تخريبها أو سرقتها أو استعمالها للدعاية المغرضة من أجل التشهير بأشخاص معينين لتدمير حياتهم الأسرية أو الفكرية أو العقدية [56] ؟

لقد عملت الأمم المتحدة في إطار جهودها لمكافحة الجريمة على دعوة جميع الدول للإنضمام و التصديق على الإتفاقيات ذات الصلة بالموضوع ، و قد أثير عند مناقشة هذه الإتفاقيات عدة تساؤلات حول العلاقة بين الأعمال غير المشروعة الموجهة ضد أمن المعلومات الإلكترونية و ظاهرة تزايد و استفحال هذه الأخيرة .

و لعل الإختلاف بشأن تدويل الجريمة الإلكترونية يرجع أساسا إلى الإختلاف في اعتبارها جريمة دولية . ففي حين يرى جانب من الفقه الدولي أنها جريمة دولية استجمعت كل الشروط و العناصر الواجب توافرها في الجريمة الدولية، يصر جانب آخر على رفض اعتبارها كذلك ، و هذا لعدم كفاية النصوص القانونية الدولية التي تجرم هذه الأفعال بالإضافة إلى غياب مفهوم محدد و متفق عليه لهذه الأفعال .

و أمام هذا الإنقسام في وجهات النظر ينبغي أن نشير إلى مسألة هامة ، إذ أن قواعد القانون الدولي الجنائي و على خلاف قواعد القانون الجنائي الوطني ، ليست مقننة في معاهدات متفق عليها بشكل عام و كلي ، و في هذا الإطار يقول الأستاذ " Zappala " أن القانون المطلوب للتجريم على المستوى الدولي في ظل المبدأ العام الذي يقضي بأن " لا جريمة إلا بقانون " لا يقتصر فقط على القواعد المقررة اتفاقا ، و لكن يجب الأخذ في الإعتبار تلك القواعد التي لها صفة القانون العرفي و القواعد التي لها صفة المبادئ العامة ، فإهمال هذه المصادر لغرض تقرير التجريم أو نفيه على فعل ما يعتبر أمرا مضللا. [57]

لذلك لا ينبغي إهمال القواعد الإتفاقية و المبادئ العامة ذات الصلة بالموضوع و التي تجرم أفعالا محددة تعتبرها مظهرا من مظاهر الإجرام الدولي الإلكتروني ، و هذا التجريم فرضته المصلحة العامة للدول ، لهذا دأبت المنظمات الدولية على الإهتمام بالموضوع لاسيما منظمة الأمم المتحدة و المنظمة العالمية للملكية الفكرية .

كما أن المعاهدات الشارعة ، ضمن شروط و ظروف معينة يمكن أن تشكل أساسا صالحا لتكوين القواعد الدولية العرفية ، و هذا ما يفهم من المادة 38 من اتفاقية فيينا لقانون المعاهدات لعام 1969 ، حيث تشترط أن تكون هذه المعاهدات واسعة الإنتشار على مستوى الدول المعنية بموضوع المعاهدة ، مع ضرورة تواجد تعامل دولي موحد اتجاه هذه القواعد ، الأمر الذي يؤكد صفتها الإلزامية للجميع .

و عليه فإن القواعد الموضوعية في معظم الإتفاقيات التي تعنى بمكافحة جرائم الحاسب الآلي ، تعتبر الأفعال غير المشروعة الموجهة ضد المعلوماتية من صميم الإجرام الدولي ، مع الإشارة إلى أن هذه الإتفاقيات أصبحت ذات طبيعة عرفية ملزمة لجميع الدول ، و هو ما جعل غالبية الفقه الدولي يصنفها ضمن المعاهدات الدولية الشارعة نظرا لتعلقها بمصالح أساسية و حيوية للمجتمع الدولي، كونها تحظى بانتشار واسع على المستوى العالمي نتيجة لاستقرار العمل بمقتضى أحكامها.

أما على مستوى المبادئ العامة فإن غالبية الدول إن لم نقل كلها قد اعتمدت في تشريعاتها قواعد قانونية تحظر الجرائم الإلكترونية و تجرمها و ذلك بتعريفها و ذكر الأفعال المعتبرة كذلك على سبيل المثال أو الحصر و صارت جرائم موصوفة .

نستخلص مما سبق أن الدول تصدت للإجرام الإلكتروني و جرت على تحديد الجرائم التي تقع على الحاسب الآلي و الشبكات الوصول بها، و لم تحصر النشاط الإجرامي في جريمة واحدة أو في عدد محدود من الجرائم ، و إنما أشارت إلى العديد من الجرائم المنصوص عليها في قانون العقوبات ، بحيث تعد هذه الجرائم أفعالا إجرامية في حالة ارتكابها من خلال تنظيم غرضه سرقة المعلومات أو كان ارتكابها بقصد الإرهاب أو بقصد القرصنة .

و بهذا يتضح جليا أن معظم الأفعال التي توردها القوانين الجنائية الوطنية تعدادا لها تحت مسمى " جرائم الحاسب الآلي " أو " المعلوماتية" و تجرمها ، تكاد تكون مشتركة بين هذه القوانين جميعها .

و بهذا يمكننا القول بوجود مبدأ قانوني عام يجرم هذه الأفعال في القانون الدولي ، حيث أن وجهة التجريم بالإستناد إلى المبادئ العامة للقانون سبق و أن اعتمدت في العهد الدولي الخاص بالحقوق المدنية و السياسية لعام 1966 ، إذ تنص المادة 15 الفقرة الثانية منه على (ليس في هذه المادة ما يحول دون محاكمة أو معاقبة أي شخص من أي فعل أو امتناع عن فعل إذا كان ذلك يعتبر وقت ارتكابه جريمة طبقا للمبادئ العامة للقانون المقررة في المجتمع الدولي) [58].

و أيضا في المادة 21 الفقرة (ج) من النظام الأساسي للمحكمة الجنائية الدولية تحت عنوان " القانون الواجب التطبيق " تطبق المحكمة المبادئ العامة للقانون التي تستخلصها من القوانين الوطنية للنظم القانونية في العالم ، بما في ذلك ، حسبما يكون مناسبا ، القوانين الوطنية للدول التي من عادتها أن تمارس ولايتها على الجريمة ، شريطة ألا تتعارض هذه المبادئ مع هذا النظام الأساسي و لا مع القانون الدولي و لا مع القواعد و المعايير المعترف بها دوليا.

و بناء على ما تقدم فإن الأعمال التي قد تقع تنفيذا لمشروع إجرامي إلكتروني بالمعنى المشار إليه سابقا تعتبر جرائم بطبيعتها بمقتضى المبادئ العامة للقانون ، و أحكام القانون الدولي الاتفاقية و العرفية، الأمر الذي يؤكد ذاتية و خصوصية الجريمة الإلكترونية ، بمقتضى قواعد القانون الدولي العام. و هذا ما يراه الأستاذ " عبد العزيز سرحان "[59] حينما يقول : إن الإجرام الدولي يقع بالمخالفة لأحكام القانون الدولي بمصادره المختلفة بما في ذلك المبادئ العامة للقانون بالمعنى الذي تحدده المادة 38 من النظام الأساسي لمحكمة العدل الدولية ، و بذلك يمكن النظر إلى الإجرام الإلكتروني على أساس أنه جريمة دولية أساسها مخالفة القانون الدولي ، ومن هنا تقع تحت طائلة العقاب طبقا لقوانين سائر الدول.

و يعد الفعل إجراما إلكترونيا و بالتالي جريمة دولية ، سواء قام به فرد أو جماعة أو دولة، و بهذا المنطق فإن الإجرام الإلكتروني لا يخرج عن هذا الوصف الذي يجرمه القانون الدولي

2.2.3.1 : دور المحكمة الجنائية الدولية في تناول الظاهرة

إن أي تقنين لقواعد القانون الجنائي الدولي فيما يخص تجريم أفعال جنائية معينة وإدراجها ضمن الجرائم الدولية ما لم يكن قد تم تخصيص قضاء جنائي دولي من جهة يشمل في اختصاصه هذه الجرائم ومن جهة أخرى ينزل العقاب على مرتكبيها، يصير كل منهما، أي التقنين والقضاء، دون جدوى ومن ثم لا يمكن تفعيلهما.

وإذا كانت بعض الأفعال الجنائية قد حظيت بإقرار تجريمها دوليا مثل تبييض الأموال وجرائم المخدرات وغيرها، وإن لم تدرج لحد الآن ضمن اختصاص القضاء الجنائي الدولي المتمثل أساسا في المحكمة الجنائية الدولية، فإن الأمر يختلف بالنسبة لأفعال الاعتداءات الإلكترونية التي رأينا كيف يمكن لها كظاهرة جديدة أن تشكل جريمة دولية، هذه الأفعال التي ليس فقط أنها لم تدرج ضمن هذا الاختصاص، وإنما لا تزال لم تجرم بعد دوليا رغم غياب مبرر تأخر هذا التجريم كما سبق توضيحه ما عدى بعض المحاولات العربية أو الأوروبية التي لا تخرج عن كونها إقليمية. وإن كانت تعمل على التحسيس ضمنيا بتجريمها دوليا، إلا أنها إلى يومنا ليست كذلك. ومن جهة أخرى لم يتم إقرار إحالة مرتكبي هذه الأفعال أو الجرائم إلا على القضاء الوطني أو المحاكم الوطنية للدول المتفقة وهنا يبقى يتسنى للمجرمين التسلل أو الإفلات من العقاب. ويكفي أن يقع ذلك بسبب تأخر دولة في تجريم الفعل المرتكب أو توانيها في مباشرة الدعوة القضائية لأسباب سيادية أو مصلحية أو عجزها و عدم قدرتها على ذلك نظرا لضغوطات داخلية أو خارجية معينة، أو بسبب إرتكاب الفعل من طرف فرد ينتمي إلى دولة ليست طرفا في الاتفاقية.

من أهم هذه المحاولات نجد اتفاقية بودبست، التي سنسهل في الكلام عنها في الفصل الثاني من هذه الدراسة و مع غيرها من التشريعات، إذ نحن نصفها بالإقليمية، زيادة على أنها تفتقر إلى جهاز قضائي دولي يختص بالنظر في الأفعال التي جرمتها، فإنها لحد الآن لم تجرؤ إلا على تجريم الأفعال الأقل خطورة ساكتة على الأخطر مثل الإرهاب الإلكتروني الذي يعتبر جريمة العصر، أين نجد الدول الأكثر تضررا منه، الدول المهيمنة مثل الولايات المتحدة الأمريكية التي تنفق مرارا ملايين الدولارات من أجل إصلاح ما تم تدميره و رغم ذلك التزمت هذا التردد. ربما حتى لا تجرها الدعوة إلى تجريمه دوليا بهذه الصورة، إلى تجريمه بصورته التقليدية.

غير أنه على حسب المعطيات الحالية لا يمكن تفادي هذا الوضع إلا من خلال ما أفسحه نظام روما الأساسي من مجال لإضافة أية جريمة لقائمة الجرائم التي أوردتها المادة 5 منه، بحيث وإن كان بموجب هذه المادة للمحكمة صلاحية النظر في أربعة جرائم هي (الإبادة الجماعية – الجرائم ضد الإنسانية – جرائم الحرب – جريمة العدوان) وهي أشد الجرائم الدولية خطورة، أين يكون واضعوا النظام الأساسي قد ارتأوا تحديد اختصاص المحكمة النوعي من خلال وضع هذه القائمة من الجرائم التي للمحكمة الجنائية الدولية صلاحية النظر فيها تطبيقا لمبدأ لا جريمة ولا عقوبة إلا بنص[08]، (لا يسال الشخص جنائيا بموجب هذا النظام الأساسي ما لم يشكل السلوك المعني وقت وقوعه جريمة لا تدخل في اختصاص المحكمة)، إلا أنه تطبيقا لنص المادة 121 وأيضا ما جاء بالملحق E/1 للوثيقة الختامية لمؤتمر روما أن (مؤتمر الأمم المتحدة الدبلوماسي للمفوضين بشأن إنشاء محكمة جنائية دولية وقد اعتمد النظام الأساسي للمحكمة، يعترف أن أعمال الإرهاب والتداول غير المشروع للمخدرات هي من الجرائم شديدة الخطورة موضع الاهتمام الدولي ولذلك يوصي عند مراجعة نظام المحكمة وفقا المادة 121 من النظام إدراج جرائم الإرهاب وجرائم المخدرات وفق للتعريف المتفق عليه في قائمة الجرائم التي تدخل في اختصاص المحكمة)[08].

فعلى الأقل كما تم الاقتصار في تحديد الجرائم الدولية على الأخطر منها في صورتها التقليدية، ينتظر أن يتم إدراج ضمن الاختصاص الجنائي الدولي الأخطر من الجرائم الإلكترونية التي وإن تناولناها في بحثنا في ثلاث صور وهي الإرهاب الإلكتروني ، التجسس الإلكتروني والعنصرية الإلكترونية ، فإننا نرشح كبداية أفعال الإرهاب الإلكتروني لتجريمها دوليا وإدراجها ضمن اختصاص القضاء الجنائي الدولي وذلك للاعتبارات التالية :

- اغتنام فرصة تصنيفها احتياطيا ضمن الأفعال التي يمكن إضافتها إلى اختصاص المحكمة الجنائية الدولية وفق المادة 121 من نظام روما والملحق E/1 السابق الذكر باعتبار أن

الإرهاب في صورته الإلكترونية يكاد يكون أخطر من الإرهاب التقليدي من حيث التكلفة والنتيجة.

- يمكن مؤقتا وإلى حد ما إذابة أفعال التجسس الإلكتروني في جانب من الإرهاب الإلكتروني.
- ترك تجريم العنصرية الإلكترونية يستمر في هدوء حتى لا يتم إثارة تماشي بعض الدول إلى حد ما مع توجه القانون الجنائي الدولي.

الفصل 2
مكافحة الإجرام الدولي الإلكتروني

إن مكافحة الجريمة بشكل عام ينحصر أساسا في إصدار تشريع عقابي يجرم أي فعل جنائي تتوفر فيه أركان الجريمة المعروفة. لكن في حالة الجريمة الدولية، زيادة على وجوب توفر الركن الدولي، فإنه لا يكفي كل ذلك في منع الجريمة ما لم تتفق و تتحد الدول و تتعاون جميع الدول من أجل ذلك و هذا يعني على الأقل التزامها بسن تشريعات داخلية، ناهيك عن ضرورة استعدادها للدخول في اتفاقيات دولية تسعى إلى التعاون من أجل تفعيل تلك المكافحة. و في هذه الحالة لا يطرح فقط مشكل الظروف الخاصة لكل دولة و مدى إمكانية تجريمها لتلك الأفعال من حيث رغبتها أو قدرتها على ذلك، و إنما نجد مشكل المصالح المختلفة لكل دولة و صيغ التعاون يطرح بقوة.

بالإضافة إلى ذلك، إن تطور الإجرام الدولي في صوره الجديدة يحتم على المجتمع الدولي تطوير وسائل المكافحة لتتلاءم مع طبيعة الأفعال الجنائية. و هذا ما يصعب أكثر من هذه المهمة بخصوص بعض الجرائم التي صارت ترتكب ارتكابا تقنيا، بل أخذت طابعا جديدا لا تكون بالضرورة التشريعات الدولية أو الداخلية القائمة قد تناولته.

و هنا يأتي دور الجناة ليغتنموا فرصة غياب التشريع ليبقوا في إفلات من العقاب. إلى حين ذلك، فحتى لو عملت الدول على تدارك هذا الجانب عن طريق الإسراع في تجريم الصور الجديدة، فبغض النظر عن ما يكلفها ذلك من إحداث شبه تجديد كلي إن على مستوى نظامها التشريعي، أو على هياكلها العقابية و حتى لو ظفرت بذلك، من دون أن ننسى أننا نتكلم عن المكافحة الدولية التي تستدعي الامتثال لما توصل إليه القانون الدولي الجنائي، فإنه تبقى إشكالية مدى تحكمها في خصوصية الجريمة و طبيعتها المستحدثة. و نحن بصدد دراسة الإجرام الدولي الإلكتروني كحالة لذلك، فسوف نرى أنه ليس من السهل التحكم في جانبه التقني مع ضرورة ذلك لأنه قد لا يُرد على التقنية إلا بالتقنية. هذا يعني اعتماد آليات من نفس طبيعة الفعل في مكافحته و من ثم يجد المشرع و القاضي نفسهما هذه المرة على غير العادة في حاجة إلى الطرح التقني و من ثم الاعتماد على الدليل العلمي التقني لإقامة الاتهام. و بحكم طبيعة الإجرام الدولي الإلكتروني و ارتكابه في عالم افتراضي أين يغيب الدليل المادي و يحل محله الدليل

العلمي التقني، فمن دون شك لا تسلم الآليات التقنية هنا من إشكاليات عملية تماما كما لا تسلم منها هي الأخرى الآليات القانونية في مكافحة هذا النوع من الإجرام، مما يُصَعب أكثر من التصدي لهذا الإجرام. و لتوضيح هذه الرؤية، نجمل في مبحث أولٍ النقاط التي تتعلق بالصعوبات التي تواجه مكافحة الإجرام الدولي الإلكتروني بجانبيها، التقني و القانوني، و في مبحث ثانٍ، نحاول إثارة أهم الآليات القائمة لمكافحة الإجرام الدولي الإلكتروني.

1.2: الصعوبات التي تواجه مكافحة الإجرام الدولي الإلكتروني

لا شك أن هذه الصعوبة ناتجة عن خصائص الجريمة في صورتها المستجدة و المتمثلة في العامل التقني و أيضا في الخصائص المستجدة للمجرم، من حيث مؤهلاته. فهي هنا صعوبة تقنية. كما هي ناتجة بصفة رئيسية عن قصور في التشريع و في أهلية السلطات المخول لها متابعة مراحل ارتكاب الجرائم و التخلص منها و في هذه الحالة هي صعوبة قانونية و هذا ما جعل الكثير من المختصين بدراسة هذا النوع من الإجرام يبرزون هذه الصعوبة على هذا الشكل [60].

1.1.2: الصعوبات التقنية

إن الطبيعة التقنية للإجرام الدولي الإلكتروني قد أفرزت صعوبة في مكافحته. و الإجراءات الخاصة التي يتوقف عليها إقامة الدليل لم تعد سلطات الإستدلال تتحكم فيها. و إن كون هذا الإجرام يرتكب في عالم غير واقعي جعل من بعض المصطلحات القانونية الواردة في مراحل التحقيق غير مجدية مثل معاينة مكان ارتكاب الجريمة. و لذلك سوف نتطرق فيما يلي إلى بعض هذه الصعوبات.

1.1.1.2: غياب الدليل المادي و إشكالية الدليل العلمي :

تتم الجريمة الإلكترونية في بيئة أو عالم افتراضي غير مرئي و غير ملموس لا علاقة له بالأوراق أو المستندات، فعن طريق الحاسب الآلي أو شبكة المعلومات العالمية - الإنترنت- أو مختلف أنظمة الاتصال السلكي و اللاسلكي الحديثة، فيمكن للجاني عن طريق نبضات إلكترونية لا ترى، أن يعبث في بيانات و معطيات في وقت قياسي قد يكون جزءا من الثانية، قبل أن تصل يد العدالة إليه، سيما و أن عملية الضبط لا تتم سوى بمعرفة خبير فني أو متخصص. ذلك أن رجل العدالة الحالي، سواء تمثل في سلطات الأمن أو أجهزة الإدعاء أو التحقيق أو الحكم، لا دراية له بالأمور الفنية أو التقنية في الجريمة الإلكترونية حتى يمكنه مجاراة الجاني في جرمه و القبض عليه، كرجل الشرطة الذي يقوم بجمع التحريات في واقعة

سرقة حتى يصل إلى المتهم و يستصدر أمرا بالقبض عليه، و تتولى النيابة العامة التحقيق معه ثم إحالته لقضاء الحكم، فكل هذه الحالات هي وقائع خاضعة لسيطرة أجهزة العدالة، و الدليل فيها مرئي و مقروء [61]، عكس الجريمة الإلكترونية التي ترتكب مع إمكانية محو كل أثر لأي دليل و في بعض الحالات يمكن برمجة محو الدليل قبل ارتكاب الجريمة و يكون ذلك هو الآخر بطريقة تقنية و من مكان ثالث غير مكان ارتكاب الجريمة أو مكان حصول نتائجها. و لذلك، فغالبية الجرائم الإلكترونية تكتشف مصادفة و ليس بطريق الإبلاغ عنها استنادا إلى ضبط دليل ما.

و صعوبة استخلاص الدليل في مثل هذه الجريمة يشكل تحديا هائلا لرجال الأمن، ذلك أن رجل الأمن غير المتخصص و الذي انحصر تكوينه في ملاحقة الجرائم التقليدية في عالمها الواقعي من قتل و ضرب و سرقة و غيرها، لن يكون في إمكانه التعامل مع الجريمة الإلكترونية و التي تقع بطريقة تقنية عالية.

و إذا كانت المصادفة من الأمور التي يعول عليها في كشف الجريمة الإلكترونية، فإن وجود أجهزة للرقابة و التدقيق داخل جهة الإدارة سواء كانت حكومية أو خاصة أو شركة من الشركات، سوف يؤدي إلى كشف وقوع هذه الجريمة و من ثم إظهار الدليل الخفي الذي تتسم به مثل هذه الجرائم شريطة أن يكون الجهاز الذي يتولى هذه الرقابة ذا تخصص و خبرة عالية في الجانب التقني من الجريمة و ذا علم بأحدثها و طرق التعامل معها، سيما و أن المجرم في هذه الجريمة لديه الخبرة الفنية و المعرفة الكافية التي تمكنه من اقتراف جريمته [61].

و لذلك نجد إن المتخصصين و جانبا من الفقه الجنائي، بسبب خفاء الدليل في الجريمة الإلكترونية، يطلق على الجناة فيها اسم القراصنة les pirates و هم نوعان، الهواة Hackers و هؤلاء هم الأشخاص الذين لهم القدرة الفائقة على اختراق الأجهزة و الشبكات أيا كانت إجراءات و برامج و تدابير الحماية التي تم اتخاذها، إلا أنهم لا يقومون بأي من الإجراءات التي تؤذي من تم اختراق جهازه أو شبكته. أما الكراكرز Crackers و هؤلاء يطلق عليهم المخربين و هم يتشابهون مع الهاكرز في قدراتهم الفائقة على الاختراق و تخطي إجراءات و برامج الحماية، إلا أنهم يقومون بالعبث بالبيانات و المعلومات المخزنة على تلك الحاسبات و الشبكات و تخريبها [14] و هم يرتكبون جرائمهم كمخادعون أو جواسيس.

- المخادعون Fraudreurs و هم يتمتعون بقدرات فنية عالية باعتبارهم أخصائيين في المعلوماتية و من أصحاب الكفاءات و لديهم مقدرة فائقة على إخفاء دليل الجريمة الإلكترونية.

- الجواسيس Espions و هؤلاء يسعون إلى جمع المعلومات لمصلحة دولهم أو لمصلحة بعض الجهات الأخرى. و لا شك أن هؤلاء قادرون كذلك على إخفاء جريمتهم نظرا لكونهم

مجرمين متخصصين، و ليدهم قدرة فائقة على طمس الأدلة المتعلقة بجرائمهم الإلكترونية.[61]

فتظل الجريمة التي ترتكب ارتكابا إلكترونيا مجهولة ما لم يبلغ عنها للجهات الخاصة بالاستدلالات أو التحقيق الجنائي، فهي جرائم لا تخلف آثارا مادية كتلك التي تخلفها الجريمة العادية مثل الكسر في جريمة السرقة و جثة المجني عليه في القتل أو الدمار و التشريد و التنكيل في الحروب. ذلك أن الجهات التي تمارس المعاملات الإلكترونية يوميا كالشركات التجارية الكبرى الدولية أو المؤسسات الاقتصادية أو العسكرية أو الأمنية، قد لا تكتشف الجريمة في حين ارتكابها إلا بعد تحقق نتائجها. و هذا ما يؤكد ن الجريمة الإلكترونية جريمة متخصصة، بمعنى أنه لا يقترفها سوى مجرم له طبيعة خاصة نظرا لأن المعلومات المعالجة إلكترونيا تكون مرمزة أو مشفرة، و التشفير يعني تحويل أو إرسال بيانات عبر وسط ناقل معين إلى جهة محددة بحيث لا يمكن لأي جهة غير الجهة المقصودة تفسير هذه البيانات المبهمة و استخلاص البيانات المفهومة منها. أما الترميز فهي عملية معقدة و سرية، بحيث أن من لا يملك مفتاحها لا يستطيع تفسيرها و الاستفادة منها و لو توصل إلى هذه البيانات و ذلك يدل على صعوبة استخلص الآثار المادية التقليدية للجريمة الإلكترونية.[61]

و من الأسباب التي تساهم في تعذر الحصول على آثار تقليدية للجريمة و التي يمكن أن نأخذها مبدئيا كدليل من أجل إثباتها، هي أن الجاني نفسه، يملك محو الأدلة التي تدينه أو تدميرها في زمن قصير جدا و حتى لو تم ضبطه فقد يمكنه التسلل من مسؤوليته مرجعا الجريمة إلى خطأ في نظام الشبكة أو الجهاز.[62] و الجريمة الإلكترونية بصفة عامة هي حرب ما بين المجني عليه و هو المؤسسة أو الشركة التي كانت هدفا للاعتداء على نظامها المعلوماتي و من ثم الإضرار بها ماليا و اقتصاديا، و ما بين المجرم الإلكتروني، و يمكن أن تكون الدولة في إحدى مؤسساتها جانية أو مجني عليها مباشرة أو غير مباشرة، أو يكون الأطفال ضحية لهذه الجريمة. لذلك فإن الهيئات و الجهات التي تتبني في نشاطها معالجة إلكترونية للمعلومات لتسيير شؤونها في جميع المجالات، تحاول دائم الحفاظ على معلوماتها و بياناتها عن طريق تخزين هذه البيانات و المعلومات بعيدا عن أيدي محترفي الجريمة الإلكترونية.

و إذا كان الترميز و التشفير أحد طرق الحماية الإلكترونية للأنظمة المعلوماتية المستعملة من طرف تلك الجهات، إلا أن ذلك لا يضمن سلامة هذه الأنظمة من الاختراقات، لما للقراصنة من تفوق في هذا المجال، و من ثم يجعلون طرق حمايتها في هذه الحالة عديمة الجدوى. بل إنهم، كما أشرنا، يسبقون إلى منع اكتشاف الدليل، . و ذلك كاستخدام كلمات سر حول مواقعهم تمنع الوصول إليها أو ترميزها أو تشفيرها لاستحالة الإطلاع على هذا الدليل الذي يخلفه

نشاطهم الإجرامي، الشيء الذي يحول دون الرقابة على المعطيات المخزنة أو المنقولة أو المتداولة إلكترونيا عبر حدود الدولة، خصوصا و أنه بعد التقدم المستجد على شبكة الإنترنت الدولية، لم تعد تشكل الحدود الجغرافية مانعا في الاختراق، بل على العكس، و مع انفتاح الشبكة على العالم،و بالتالي تصبح حرمة المجال المعلوماتي الإلكتروني للدولة مهددا، خاصة الحساس منه مثل الذي يخص تدابير الدفاع و الأمن و أسرار اقتصادها، ما يوحي بضرورة وجود إجراءات تمكن من المتطلبات الجديدة التي تفرضها هذه التكنولوجيا [63]

و الحقيقة إن مسألة استخلاص الدليل في الجريمة الإلكترونية، و بغير الطرق التقليدية، يثير ما يسمى بالدليل العلمي في مسألة الإثبات الجنائي. و الدليل العلمي يقصد به النتيجة التي تسفر عنها التجارب العلمية لتعزيز دليل إثبات أو نفي واقعة يثار حولها الشك. وبطبيعة الحال فإن إجراء هذه التجارب والوسائل لا تكون سوى من مختص فنيا وهو بهذه المثابة لا يعدو إلا أن يكون رأيا فنيا.

وهذا الدليل العلمي، يعد شكلا من أشكال الأدلة المقدمة في الدعوى الجنائية، ويكون طلبه بناءً على طلب القاضي أو أحد الخصوم في الدعوى.

وطلب القاضي للدليل العلمي، هو من المسائل الفنية التي لا يجوز للمحكمة أن تحل نفسها فيها محل الخبير، لأنها مسألة فنية في حاجة إلى خبير فني. ومع ذلك لو كان طلب ندب الخبير من جانب الخصوم فإن المحكمة غير ملزمة بإجابة طلبهم طالما أن الواقعة قد وضحت لديها، وفي مقدورها أن تشق طريقها في المسألة المطروحة عليها.

والقاعد العامة أن الدليل العلمي والمستفاد من الخبرة الفنية لابد وأن يكون مشروعا. ومع ذلك ورغم مشروعية الدليل العلمي والحاجة إليه، إلا أنه في حالة الشك يفسر لصالح المتهم. وهناك من أشار أن الوسائل العلمية في اغلب حالاتها ليست دليلا مستقلا في ذاته وإنما هي قرائن يتم دراستها واستخلاص دلالتها، وهي غير مستقلة عن القرائن هذا يعني أنها لا تكفي لوحدها كدليل يعتمد عليه المحقق القضائي من إقامة الإدانة.

بالإضافة إلى ذلك، و نحن بصدد الكلام عن الصعوبات التقنية التي تواجه مكافحة هذا النوع من الإجرام، هناك بعض الجوانب السلبية التي تزيد من تعذر إدراك الآثار و من ثم بلورة الدليل و هي [61] :

أولا : أن المستوى الثقافي المتواضع في الوقت الحالي لأجهزة العدالة سواء تمثلت في رجال الشرطة والأمن أو جهات التحقيق أو المحاكم، يجعل مسألة الاطلاع غير المسموح به، والمثارة في هذا الفرض مجرد تصور نظري، لأن مأمور الضبط أو رجل التحقيق ليست لديه المقدرة الفنية أو التقنيش على عملية الدخول إلى شبكة البيانات المعالجة آليا والاطلاع عليها، سيما لو

كان الأمر بالسرية ومن ثم سيكون هناك احتياطات أمنية متمثلة في المفاتيح LES CODES السرية وعمليات التشفير والترميز.

ثانيا : أن عمليات الاختراق أو القرصنة الإليكترونية لست قاصرة داخل المؤسسة أو داخل الدولة بل قد يكون المتدخل من خارج حدود الدولة، ذلك أن التكنولوجيا وثورة الاتصال، كما أشرنا، قد ألغت ما يسمى بالحدود الجغرافية وأصبحت عملية الاختراق الإلكتروني تتجه لخدمة المصالح السياسية والاقتصادية بين الدول. وذلك يتطلب ضرورة تفعيل التعاون الدولي من أجل اقتفاء آثار الإجرام الإلكتروني.

ومن أمثلة ممارسة الجريمة الإلكترونية بمعرفة الدولة ذاتها [64]، ما لجأت إليه الولايات المتحدة الأمريكية من تأسيس شبكة استخبارات عالمية من أجل التجسس على الشركات البريطانية لخدمة المصالح الأمريكية للفوز بعقود تقدر قيمتها بملايين الدولارات، وفي مثال آخر وفي مطلع عام 2000، طور الجيش في "تايوان" ترسانة من الفيروسات تحسبا للاختراقات التي قد شنها الصين عليها، حيث سبق أن تعرضت في السابق لهجمات متعمدة ذات طابع سياسي وقابل ذلك تخصيص الجيش التايواني ترسانة دفاعية لتطوير المقدرات الدفاعية والهجومية على صعيد الحرب التقنية.

2.1.1.2 : المعاينة في الجريمة المعلوماتية كوسيلة للحصول على الدليل.

يقصد بالمعاينة إثبات حالة الأماكن والأشياء والأشخاص، وكل ما يعتبر في كشف الحقيقة، والمعاينة بهذا المعنى تستلزم الانتقال إلى محل الواقعة أو إلى أي محل آخر توجد به أشياء أو آثار يرى المحقق أن لها صلة بالجريمة، غير أن انتقال المحقق قد يكون لغرض آخر غير المعاينة، كما في انتقال المحقق إلى مسكن المتهم أو غيره لتفتيش أو لسماع الشهود.

والمعاينة وإن كانت واردة في كل الجرائم، إلا أن أهميتها تتضاءل في بعض الجرائم دون غيرها مثل جريمة التزوير المعنوي وجريمة السب فإن المعاينة فيهما غير ذات جدوى هذا من ناحية، ومن ناحية أخرى فإن معاينة الجرائم التقليدية والاطلاع على مسرح الجريمة فيها يكون ذو أهمية متمثلة في تصور كيفية وقوع الجريمة وظروف وملابسات ارتكابها، وتوفير الأدلة المادية التي يمكن تجميعها عن طريق هذه المعاينة، لكن هذه المعاينة لا تؤدي ذات الدور في كشف غموض الجريمة المعلوماتية وضبط الأشياء التي قد تفيد في إثبات وقوعها ونسبتها إلى مرتكبها [61].

وإذ تظهر أهمية المعاينة عقب وقوع جريمة من الجرائم التقليدية، حيث يوجب مسرح فعلي للجريمة يحتوي على آثار مادية فعلية، يهدف القائم بالمعاينة إلى التحفظ عليها تمهيدا لفحصها،

لبيان مدى صحتها في الإثبات، فليس الحال كذلك بالنسبة للجرائم الإلكترونية، حيث يمكن أن يتخلف عن ارتكابها آثار مادية، وقد تطول الفترة الزمنية بين وقوع الجريمة واكتشافها، مما يعرض الآثار الناجمة عنها إلى المحو أو التلف أو العبث به [65] ا.

و إذا أمكن إلى حد ما القيام بالمعاينة في مستوى معين في حالة وقوع الجريمة في المجال الإلكتروني عن طريق :

- تصوير الحاسب والأجهزة الطرفية المتصلة به، على أن يتم تسجيل وقت وتاريخ ومكان التقاط كل صورة.
- العناية بملاحظة الطريقة التي تم بها إعداد النظام.
- ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عمليات المقارنة والتحليل حين عرض الامر فيما بعد على المحكمة.
- عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل إجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الحاسب من أي مجال لقوى مغناطيسية يمكن أن يتسبب في محو البيانات المسجلة.
- التحفظ على معلومات سلة المهملات من الاوراق الملقاة او الممزقة وأوراق الكربون المستعمله والشرائط والأقراص الممغنطة غير السليمة، وفحصها، ويرفع من عليها البصمات ذات الصلة بالجريمة.
- التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة، لرفع ومضاهاة ما قد يوجد عليها من بصمات.

فإنه في مستوى آخر، لا يمكن ذلك بالبساطة لما يتعلق الأمر بالمجال الافتراضي و العالم الرقمي أين يكون التعامل مع أجهزة الحاسوب و الملحقات المرتبطة بها أو بالشبكة بوجه عام، يجب أن يتم بمعرفة خبراء مختصين من أجل إجراء المعاينة، و إلا فإن أي تعامل خاطئ مع هذا العالم الافتراضي و الأنظمة الشاغلة فيه، قد يؤدي إلى فقدان أدلة مهمة إن لم تكن قد فقدت مسبقا على الشكل الذي تم توضيحه. و من ثم قد يتعذر نهائيا القيام بهذا الإجراء القضائي الضروري [66].

و على هذا الأساس ، تكمن الصعوبة في ما يجب أن يتوافر من ظروف و إمكانيات من أجل توثيق مسرح الجريمة و السيطرة عليه ووصفه بكامل محتوياته وذلك عن طريق تحديد مراحل التعامل مع هذا المسرح بدءا بوضع خطة لذلك و حمايته و تأمينه و الشروع في البحث عن الأدلة و من ثم وجودها و معالجتها. مع ضرورة الأخذ بعين الاعتبار أثناء التعامل مع الأدلة الرقمية ما يلي :

عدم القيام بأي عمل من شأنه إحداث تعديل أو تغيير في أي دليل.

عدم تنفيذ أية برامج على حواسيب في موقع الجريمة خصوصا البرامج ذات الصلة بأنظمة التشغيل.

ضرورة عمل نسخ مطابقة للأقراص الصلبة و يجب التأكيد على هذه النسخ حيث لا تكفي نسخة احتياطية من البيانات المراد فحصها، و إنما يجب عمل نسخة مطابقة تماما لكامل القرص الصلب و على مستوى وحدة الـ Bit و هي أصغر وحدة لقياس كم البيانات الرقمية، بل من الأفضل عمل نسخة احتياطية ثانية يتم إجراء الفحوصات عليها. و طريقة التعامل بالنسخ تستغرق من فريق التحقيق وقتا أطولا و تتطلب جهدا أكبرا و تستهلك موارد أكثرا و ثم هي معرضة للتلف في أي لحظة، الشيء الذي يعطل المعاينة.

كل هذا إذا توافرت حقيقة الأجهزة القضائية على هذه الإمكانيات البشرية و الخبرة التكنولوجية و على قدرة و جرأة على القيام بهذه المهام خاصة و نحن نثير حالة الجريمة الدولية و ما تطرحه من عوائق مردها خصوصية المجال الافتراضي لكل دولة [66].

2.1.2 : الصعوبات القانونية

فإذا خلصت الجريمة العادية أو التقليدية من صعوبة مكافحتها إلى حد ما ، فإن الأمر ليس كذلك في الجريمة الإلكترونية، حيث بغض النظر عن الصعوبات التقنية السابقة الذكر، فإن مكافحتها عرفت أيضا صعوبات في جانبها القانوني. و بالإضافة إلى عدم وجود تعريف قانوني للجريمة الدولية، بصفة عامة و للجريمة الإلكترونية بصفة خاصة، يُمَكن من انتقاء أفضل الآليات لمكافحة الإجرام الدولي الإلكتروني، تطرح في هذا المجال بعض الصعوبات التي مردها بصفة أساسية هو خصوصيته الدولية و تعدد من يكونوا مرتكبوه [63] هذه الصعوبات التي تحول دون تفعيل هذه المكافحة نوردها فيما يلي :

1.2.1.2 : صعوبات مصدرها الأحجام عن الإبلاغ

تظل الجريمة المعلوماتية مستترة ما لم يتم الإبلاغ عنها، ومن ثم عمل الاستدلالات أو تحريك الدعوى الجنائية حسب القانون السائد، والصعوبة التي تواجه أجهزة الأمن والمحققين هي أن هذه الجرائم لا تصل إلى علم السلطات المعنية بالصورة العادية –كما هو الحال في الجريمة التقليدية- وذلك لصعوبة اكتشافها من قبل الأشخاص العاديين أو حتى الشركات والمؤسسات التي وقعت مجنيا عليها في هذه الجرائم، أو لأن هذه الجهات تحاول درأ الأثر السلبي للابلاغ عما وقع لها وحرصا على ثقة العملاء فلا تبلغ عن تلك الجرائم التي ارتكبت ضدها [61].

في الغالب الأعم - الإبلاغ عن جرائم الانترنت إما لعدم اكتشاف الضحية لها وإما خشيته من التشهير. لذا نجد أن معظم جرائم الانترنت تم اكتشافها بالمصادفة ؛ بل وبعد وقت طويل من ارتكابها، زد على ذلك أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف الستار عنها . فالرقم المظلم بين حقيقة عدد هذه الجرائم المرتكبة ؛ والعدد الذي تم اكتشافه ؛ هو رقم خطير . وبعبارة أخرى ؛ الفجوة بين عدد هذه الجرائم الحقيقي ؛ وما تم اكتشافه : فجوة كبيرة.

ولذلك وطبقا للتقديرات فإن ما بين 20 و 25 % من جرائم الحسابات لا يتم الابلاغ عنه مطلقا خشية الإساءة للسمعة، إلا أن دراسة أخرى في الولايات المتحدة، أجريت على ألف شركة تنتج جهاز (Fortune 500) أظهرت نتائجها أن 2% فقط من كل جرائم الحاسب هي التي يتم الابلاغ عنها للشركة أو لمكاتب التحقيقات الفيدرالي، كما سجلت دراسة أخرى من أمن الحاسبات بالولايات المتحدة عام 1988 أن 6% من حوادث الأمن الخطيرة هي فقط التي يتم إبلاغها إلى السلطات المختصة، وفي دراسة أخرى تمت لهذا الغرض تبين أن الشركات والمؤسسات تدخل في حسابها الموازنة بين الوضع المترتب على الجريمة وعلاقة الجاني بالمنظمة والخسائر التي تكيدتها أو تكيدها الأفراد والمشاكل المحتملة المترتبة على الاتصال والتعامل مع أجهزة العدالة الجنائية وأعباء ومخاطر العلانية [61].

فإذا كانت الجريمة في صورتها التقليدية تصل إلى علم سلطات لضبط عن طريق الشكوى أو الإبلاغ والتي يجب على هذه الأخيرة أي السلطات، التأكد من محتوى الإبلاغ فيما إذا تم مشاهدة الجريمة حال ارتكابها أو مشاهدة الجريمة عقب ارتكابها ببرهة يسيرة، أو إذا تمكن المبلغ من تتبع الجاني أثر وقوع الجريمة، أو إذا تمت مشاهدة الجاني بعد وقوع الجريمة بوقت حاملا أشياء أو به آثار يستدل منها على أنه فاعل الجريمة أو شريك فيها، فإن البلاغ باعتباره هو الآخر الوسيلة التي يصل من خلالها إلى علم سلطات الضبط أخبار الجريمة و ذلك بـ :

- تلقى سلطات الضبط أو أجهزة التحقيق معلومات عن أشخاص معروفين يمارسون أنشطة تندرج تحت تعريف الجريمة المعلوماتية، وذلك في مكان معروف وعلى أجهزة محددة، ووفق لغات برمجية معلومة.

- ضبط شخص معين وبحوزته أموال مشبوهة أو بطاقات مزورة أو بطاقات تعريف مشبوهة "حالة تلبس".

- إفادة سلطات الضبط أو التحقيق ببلاغ من أحد المجني عليهم يفيد تلاعب أو ممارسات خاطئة في حقه أو حقوق الآخرين.

- توافر معلومات عم نشر فيروسات تخريبية عبر شبكة الانترنيت، سيما وأن تطبيق القانون في مجال الفيروسات المعلوماتية، تواجهه عدة صعوبات وموانع كثيرة هي :

أ- عدم معرفة المجني عليه بالمخرب الذي صمم الفيروس الذي هاجمه.

ب- عدم رغبة المجني عليه في الإبلاغ عن وجود فيروس بنظامه المعلوماتي، حفاظا على الثقة بينه وبين الذين يستخدمون هذا النظام.

ج- عدم دراية المجني عليه بإصابة نظامه بفيروس معلوماتي لفترة غير محدودة من الزمن، وبالتالي يصعب تحديد وقت الإصابة.

د- عدم القدرة عل قياس الخسائر التي يحدثها هذا الفيروس

- توافر معلومات عن وقوع عمليات اعتراض أو قرصنة فضائية للمعلومات، ذلك أن الظاهرة –الاختراقية- للمعلومات تتجاوز حدود الجغرافيا، وقد جعلت شبكة الانترنيت هذا النوع من الجرائم ساحة للمعارك بين الدول، وصارت الحركة التجارية والتعاملات المصرفية هدفا لهذه الاختراقات الاليكترونية

فإن هذه الكيفية، أول ما تطرحه هو مشكل التبليغ. حيث أن هناك بعض المشكلات التي تتعلق بعملية التبليغ عن جرائم الحاسوب و الإنترنت و الجرائم الإلكترونية بصفة عامة، و التي يجدر بالمحقق أخذها بعين الاعتبار و تكمن أساسا في الإحجام عن التبليغ، حيث يحجم البعض عن إبلاغ السلطات المختصة عن الجرائم التي ارتكبت بحقهم أو بحق غيرهم من أفراد و مؤسسات و شركات تجارية [66].

و يمكن أن يعود إحجام البعض عن الإبلاغ لعد أسباب من أهمها :

- قد يحجم بعض الأفراد و مدراء الأنظمة الحاسوبية و سؤولي الشركات عن الإبلاغ عن جرائم وقعت و تم اكتشافها، نتيجة عدم إدراكهم أن مثل هذه الأفعال و الهجمات تعتبر جرائم يمكن معاقبة مرتكبيها بموجب التشريعات و الأنظمة المطبقة على إقليم الدولة أو المطبقة دوليا.

- خوف الجهات التي وقعت عليها الجرائم، خاصة المؤسسات و الشركات المالية من أن يؤثر انتشار خبر الجريمة على سمعتها و ثقة السوق المتعاملة معها في قدرتها، الأمر الذي قد ينعكس سلبا على أرباحها و قيمة أسهمها.

- تخوف المؤسسات و الشركات التجارية من أن تؤدي أعمال التحقيق التي تقوم بها الشرطة إلى احتجاز حواسيبها أو تعطيل شبكاتها لفترة طويلة، مما قد يتسبب في زيادة خسائرها المالية جراء التحقيق، إضافة إلى ما قد تتسبب الجريمة في خسارته أصلا. و الواقع أنه في بعض الأحيان قد تتسبب إجراءات التحقيق الخاطئة في خسائر مادية تفوق تلك التي تسببت فيها الجريمة.

- بعض الضحايا قد تساورهم الشكوك حول قدرة الشرطة على التعامل مع الجرائم الإلكترونية من حيث توفر الخبرة الفنية لدى ضباطه، أو توفر المعدات و التجهيزات اللازمة للتحقيق في هذا النوع من الإجرام [66].

إضافة إلى ذلك، إذا كان يعرف الإبلاغ على أنه إخبار السلطات المختصة عن وقوع جريمة أو أنها على وشك الوقوع أو أن هناك اتفاقا جنائيا على ارتكابها، فإنه بحكم طبيعة الجريمة الإلكترونية، يطرح الإشكال أيضا على كل من المُبلغ و من يتلقى التبليغ إشكالا آخرا. إذ أن المُبلغ في جرائم الحاسوب و الإنترنت، يجب أن يتسم بدرجة مقبولة من الإلمام و المعرفة بالجوانب الفنية للحاسوب و لتكنولوجيا شبكات الاتصال عموما، حتى يتمكن من تقديم معلومات تصف الحادث بشكل جيد يمكن معه للمحقق الوقوف على طبيعة الجريمة بشكل مقبول مما يمكنه من مباشرة التحقيق فيها. و بالتالي يفترض أن يكون لدى من يتلقى الإبلاغ، المعرفة الكافية بالجوانب الفنية للحاسوب و الشبكات حتى يستطيع مناقشة المُبلغ في الجوانب المتعلقة بالجريمة محا الإبلاغ.

ثم أننا، إذا أثرنا الجريمة الإلكترونية الدولية، فإن من صعوبات الإبلاغ عن هذه الجرائم على نطاق دولي، عدم وجود شبكة دولية لتبادل المعلومات الأمنية كما هو الحال في شبكة (يورب بول) التي تعمل حاليا في إطار الشرطة الدولية، بمعزل عن الشبكة العامة المستخدمة حاليا كما هو الحال إنترنت (2) التي تمثل اتحاد شركات عالمية تعمل بمعزل عما تواجهه شبكة الانترنيت الحالية من مشاكل وثغرات [61].

2.2.1.2 : صعوبات مصدرها نقص خبرة سلطات الاستدلال و التحقيق

إضافة إلى مسألة الإبلاغ و ما يقع عليها من إشكالات تعوق استخلاص الدليل و من ثم إثبات الجريمة الإلكترونية على المستوى الوطني أو الدولي، نجد كذلك مشكلة نقص الخبرة لدى رجال الضبط القضائي أو أجهزة الأمن بصفة عامة، وكذلك لدى أجهزة العدالة الجنائية ممثلة في سلطات الاتهام و التحقيق الجنائي، وذلك فيما يتعلق بمدى درايتهم و علمهم بخبايا تكنولوجيا العالم الافتراضي، مسرح الجريمة الإلكترونية. و كذلك درجة إلمامهم بعناصر هذه الجريمة و كيفية التعامل معها، علما أن مشكلة نقص الخبرة لا تعني أكثر الدول مالكة هذه التكنولوجيا بقدر ما تعني غيرها باعتبار أن هذه الأخيرة اعتمدت متأخرة على تجربة الاعتماد على تقنيات الحاسب الآلي و يلحقه من أنظمة معلوماتية و شبكات اتصال عالمية بالمقارنة مع الأولى مثل دول أوربا و كندا و الولايات المتحدة.

و في كل الحالات، حتى لو افترضنا شروع أجهزة العدالة الدولية المقاومة للجرائم المرتبطة بهذه التقنية تبدأ في التكوين والتشكيل و اكتساب هذه الخبرة فلم يكن ذلك إلا عقب ظهور هذه الجرائم، وهو أمر يستغرق وقتا أبطأ من وقت انتشار الجريمة لان الجريمة الإلكترونية تتقدم بسرعة هائلة توازي سرعة تقدم التقنية ذاتها، وحتى الآن فان الحركة

التشريعية، أو الثقافة الأمنية أو القانونية بخصوص هذه الجرائم لا تسير بذات المعدل، وهذا الفارق في التقدم أو التطور ينعكس سلبا على فنية إجراء الاستدلالات والتحقيقات في الدعوى الجنائية عن الجريمة الإلكترونية، ومن هنا تأتي الدعوة إلى وجوب تأهيل سلطات الأمن وجهات التحقيق والإدعاء والحكم على النطاق الدولي في شأن هذه الجرائم لاستيعاب تقنيات الحاسب الآلي من حيث برامجه، أنظمته، طبيعة الجريمة الواقعة عليه ومفرداتها من احتيال إليكتروني وقرصنة واختراق وحماية وكيفية كسر جدار الحماية، وفيروسات الكمبيوتر، ونظم استعمال ومعلومات دولية وغيرها من مصطلحات يمكنه عن طريقها التعامل مع هذه الجريمة المتفردة في خصوصيتها وكذلك التعامل المجرم الإلكتروني وهو مجرم ذا طبيعة خاصة يتعين تفهم كيفية التعامل معه.

ثم أن الجناة في هذه الجرائم لهم المفردات والمصطلحات الخاصة بهم، لدرجة أنهم يطلقون على أنفسهم اسم ((النخبة) (Elites) بدعوى أنهم الأكثر معرفة بأسرار الحاسب الآلي ولغاته المتميزة، ويطلق على رجال الشرطة والنيابة والقضاء صفة الضعفاء أو القاصرين (Damers) [61].

إن مبرر هذه الضرورة ناتج أساسا عن طبيعة التعامل أو تداول المعلومات على هذه الشبكة، الأمر الذي يزيد من إرهاق سلطات الضبط و رجال القضاء و يكلفهم تدريبا أكثر من أجل معرفة متميزة بنظم الحاسبات، وكيفية تشغيلها، ووسائل إساءة استعمالها من قبل مستخدميها، و بالشبكات و طرق الدخول و التسلل إلى المواقع الشاغلة فيها و الأنظمة الموصولة بها. ولن تتحقق هذه المعرفة التقنية إلا بتدريب القائمين على أعمال التحري، والمباشرين للتحقيق في مجال الجرائم الإلكترونية، إلى الحد الذي دعا البعض إلى القول بضرورة وجود شرطة متخصصة، ونيابة متخصصة في هذا المجال من أجل ضمان مهارات ومعارف تمكن من السيطرة على هذه الوسيلة، وأساليب ارتكاب هذا النوع من الإجرام، مع دراسة حالات تطبيقه لجرائم وقعت سلفا، وكيف تم مواجهتها [65].

3.2.1.2 : مسألة الخبرة القضائية في الجريمة الإلكترونية

وفقا لقواعد قانون الإجراءات الجنائية فإن إثبات الحالة قد يتطلب استطلاع الرأي في مسألة يختص بها أهل الخبرة كالأطباء والمهندسين والمحاسبين وخبراء الخطوط، وللمحقق من تلقاء نفسه أو بناء على طلب الخصوم أن يندب خبيرا للاستعانة برأيه في هذه المسألة (وهذا ما هو معمول له في كثير من التشريعات) وتقدير ما إن كانت الدعوى تستلزم ندب خبير من عدمه هو أمر من شأن المحقق، لذلك فهو ليس ملزما بإجابة الخصوم لهذا الندب، كما أن للمحقق حرية اختيار الخبير الذي يندبه دون تقيد بالخبراء المقيدين بجدول الخبرة أمام المحاكم. [61]

وإذا كانت الاستعانة بخبير فني أمر جوازي للمحقق أو لجهة التحقيق والحكم في بعض حالات الجريمة التقليدية، إلا أنه في المسائل الفنية البحتة، لا يمكن للقاضي أن يقطع فيها برأي دون استطلاع رأي أهل الخبرة، في هذه الحالة يجب عليه أن يستعين بالخبير، فإذا تصدى للمسألة الفنية وفصل فيها دون تحقيقها بواسطة خبير، فبالنسبة لما استقر عليه القضاء يكون حكمه معيبا مستوجبا نقضه [65].

فأمام هذه الوضعية، بأي مستوى تقدر صعوبة الخبرة القضائية في الجرائم الإلكترونية بالمقارنة مع الجرائم التقليدية ؟ خاصة بعد ما علمنا أن لا حدود معلومة و لا كيفية ثابتة و لا مقترفين محددين لهذا الإجرام الذي لا ساحة و لا مسرح معروفين له أو واقعيين.

فإذا كانت الإجابة على هذا السؤال تبين من جهة، الحاجة إلى خبراء وفنيين عند وقوع الجريمة المعلوماتية ويمتد عملهم ليشمل المراجعة والتدقيق على العمليات الآلية للبيانات، وكذلك إعداد البرمجيات، وتشغيل الحاسب وعلومه، و التعامل مع الشبكات و المواقع فانه من جهة أخرى، إن نجاح الاستدلالات وأعمال التحقيق في هذه الجرائم يكون مرتهنا بكفاءة وتخصص هؤلاء الخبراء إن وجدوا.

ثم أنه إضافة إلى مسألة حجية الدليل العلمي من عدمها و كيف يفسر لصالح المتهم في حالة الغموض، يطرح ثانية كفاءة القاضي التي تسمح له بفهم الدليل التقني و من ثم إهماله، وهذا يعود بنا إلى ضرورة تأهيل رجال الضبط وسلطات التحقيق في الجرائم المعلوماتية لنجاح تحقيق مثل هذه الجرائم، ودرءا لما ينادي به البعض من أنه للخبير نفسه أن يحدد إطار مهمته، إذ أن ذلك سوف يقوض دور المحقق والقاضي في الدعوى الجنائية في مثل هذه الجرائم المعلوماتية.

ونظرا لأن الجريمة الإلكترونية لها خصوصيتها فإن الخبير القضائي في مثل هذه الجرائم قد يكون من أولئك الجناة الذين سبق لهم ارتكاب مثل هذه الجرائم وتم تذويبهم داخل المؤسسات الإلكترونية للاستفادة إيجابيا من قدراتهم، فضلا عن تأهيلهم كمواطنين صالحين. وإن كان ذلك يجوز أن يكون سببا برد الخبير المنتدب في الدعوى من قبل أصحاب المصلحة في ذلك.

فيتعين إذا في خبراء الحاسب الآلي و تقنية الإنترنت و العالم الافتراضي عموما، المنتدبين للتحقيق أن يتوافر لديهم المقدرة الفنية والإمكانيات العلمية والفنية في المسألة موضوع الخبرة. [61]

و إذا استرجعنا من خصائص الجريمة الإلكترونية كونها ترتكب بنوع بل بكثير من التمويه، فمن غير مقارنة و مطابقة خبرات جميع الخبراء بالتنسيق مع المحقق الجنائي أو سلطات الضبط أو التحقيق في تلقي البلاغ أو إجراءات الضبط والتفتيش أو فحص البرامج وجمع الأدلة

الجنائية و ذلك قبل محاكمة الجاني في الجريمة الإلكترونية، كما يجب على المحقق الجنائي قبل ذلك أن يكون قد شرح لهؤلاء الخبراء الجوانب القانونية لطبيعة المهمة الموكلة لهم مع التأكيد على وجود العلاقة بين الأدلة والخبرة العلمية و عناصر وأركان الجريمة المقام عنها الدعوى الجنائية ضد المتهم.

4.2.1.2 : صعوبة التعاون الدولي في مكافحة الجرائم الإلكترونية

إن الاستخدامات المختلفة التي تقدمها شبكات الاتصال و أساسا شبكة الشبكات العالمية، الإنترنت، في الكثير من المجالات إن لم تكن جميعا و نظرا لدقة استعمال هذه الوسيلة و تطورها المذهل، صارت تُنقل و تُشَغل المعلومات و البيانات عبر الحدود الكونية بكيفية مذهلة و في غير مأمن إذ صار التلاعب بسريتها و خصوصيتها بغض النظر عن الهدف الذي من وراء ذلك، يشكل خطرا على الدول باعتبارها إذا كانت قد تمكنت من السيطرة على إقليمها الولي البري و البحري و الجوي، فإنه بدرجات متفاوتة لم تتمكن لا الدول مالكة هذه التكنولوجيا و لا غيرها من تحصين اقليهما الافتراضي، الشيء الذي جعلها تجزم أنه لا سبيل إلى تجنب مخاطر هذه التقنية و ما يمكن أن تتسبب فيه من اعتداءات بل جرائم دولية كما رأينا، سوى التعاون الدولي بكافة صوره. لكن سرعان ما واجه هذا التعاون صعوبات تعمدتها الدول ذات مصالح في ذلك، أعاقت قيامه و جعلت منه أمرا شبه مستحيل و أن الضرورة إلى ذلك تصير تتحتم أكثر فأكثر لأن أهم المؤسسات في كل دولة من عسكرية و اقتصادية و أمنية و سياسية بل أهم من ذلك، المجتمع كله. من أهم هذه الصعوبات و المعوقات التي جعلت هذا التعاون صعبا ما يلي :

أولا : عدم وجود نموذج موحد للنشاط الإجرامي :

إننا إذا لاحظنا تشريعات الدول في مجال منع الجريمة الإلكترونية بمختلف مسمياتها يتبين لنا من خلال ما تصفه من أفعال، عدم وجود اتفاق عام و مشترك بين الدول حول نماذج إساءة استخدام نظم المعلومات و شبكة الإنترنت الواجب تجريمها. فما يكون غير مجرم في دولة ما، قد يكون مجرما في دولة أخرى و العكس. و يمكن إرجاع ذلك إلى عدة أسباب و عوامل كاختلاف البيئات و العادات و التقاليد و الديانات و الثقافات من مجتمع لآخر، و من ثم يكون اختلاف السياسة التشريعية من مجتمع لآخر.[67] إذ لا ننسى أن من أهم خصائص القاعدة القانونية أنها قاعدة اجتماعية. ثم أن عدم تمكن تشريعات الدول منفردة على تحديد تعريف دقيق للنشاط المجرم ناهيك عن توحدها مع بقية الدول الأخرى، زاد من حدة صعوبة هذا التعاون.

وإن كانت بعض الدول الأوربية كفرنسا و بلجيكا، وكذلك الولايات المتحدة الأمريكية، وكندا أصدرت تشريعات تخص مكافحة الجريمة الإلكترونية عبر الحاسب الآلي والانترنت، إلا أن هذه التشريعات ليست جريئة، ولا يمكن اعتبارها كافية [62]، بدليل أن المؤسسات المحلية لديها تطالب في كل عام بإضافة نماذج من السلوك الإجرامي المعلوماتي لتكون محلا للتجريم، ولم تكن متضمنة في التشريعات العقابية المعمول بها.

إن هذه الوضعية المتمثلة في عدم توحد التشريعات الجنائية فيما بين الدول على نموذج متقارب في وصف الاعتداءات الإلكترونية على أنها جرائم، أعطت لمجرمي الإجرام الإلكتروني فرصة لتنظيم أنفسهم و إيجاد الوقت الكافي لاختيار المكان الذي ينفذون منه عملياتهم الإجرامية متسللين حدود هذه الدول.

ثانيا : عدم وجود تنسيق فيما يتعلق بالإجراءات الجنائية المتبعة في شأن الجريمة المعلوماتية بين الدول المختلفة، خاصة ما تعلق منها بأعمال الاستدلال أو التحقيق، سيما وأن عملية الحصول على دليل في مثل هذه الجرائم خارج نطاق حدود الدولة، عن طريق الضبط أو التفتيش في نظام معلوماتي معين هو أمر غاية في الصعوبة، فضلا عن الصعوبة الفنية في الحصول على الدليل ذاته [61].

ثالثا : عدم وجود معاهدات دولية تفرض هذا التعاون بين الدول بما يهون من حدة الصعوبات التي يواجهها في مجال مكافحة هذه الجرائم، وحتى في حال وجود لهذه المعاهدات فإنها من جهة بقيت جهوية أو إقليمية، و من جهة أخرى هي تقتصر في تكريسها لمبدأ التعاون على صيغة الدعوة أو الإيصاء بعيدا عن أي معنى يحمل الإلزامية بمدلولها الحقيقي، ومن ثم تطورت الجريمة الإلكترونية بسرعة على نحو يؤدي إلى إرباك مشرع التعاون وسلطات الأمن في الدول، ومن ثم يظهر الأثر السلبي في عدم التعاون الدولي، الشيء الذي حصر إلى حد كبير توجه جهود الدول في تركيزها على إيجاد صيغ لهذا التعاون.

رابعا: مشكلة الاختصاص في الجرائم المتعلقة بالإنترنت:

بحكم طبيعة الجرائم الإلكترونية من حيث إمكانية اقترافها دوليا، جعلها تكون من أكبر الجرائم التي تثير مسألة الاختصاص على المستوى الدولي. حيث أن اختلاف التشريعات والنظم القانونية والتي قد ينجم عنها تنازع في الاختصاص بين الدول بالنسبة للجرائم المتعلقة بالإنترنت التي تتميز بكونها عابرة للحدود. فقد يحدث أن ترتكب الجريمة في إقليم دولة معينة من قبل أجنبي، فهنا تكون الجريمة خاضعة للاختصاص الجنائي للدولة الأولى استنادا إلى مبدأ الإقليمية ، وتخضع كذلك لاختصاص الدولة الثانية على أساس مبدأ الاختصاص الشخصي في جانبيه ، وقد تكون هذه الجريمة من الجرائم التي تهدد أمن وسلامة دولة أخرى فتدخل عندئذ في اختصاصها

استنادا إلى مبدأ العينية. كما تثار فكرة تنازع الاختصاص القضائي في حالة تأسيس الاختصاص على مبدأ الإقليمية. كل هذا في ظل غياب تشريعات دولية تتناول هذا الاختصاص. [67]

2.2 : الآليات القائمة لمكافحة الإجرام الدولي الإلكتروني

بعد ما غدا الإجرام الدولي الإلكتروني واقعا مفروضا على الأقل كسلوك منحرف يشكل اعتداء و خطرا على حقوق الأفراد التي أقرتها المواثيق الدولية و كذلك على المصالح الدولية التي طال ما بذلت الهيئات الدولية جهودا للحفاظ عليها و إيجاد صيغ اتفاقية لاحترامها و الالتزام بعهود أبرمتها فيما بينها في الكثير من المجالات، فإن هذه الهيئات لم تتوان في وضع آليات لمكافحة هذا النوع من الإجرام متحدية بمساعيها تلك الصعوبات التي تواجه هذه المكافحة و متخذة التكنولوجية و التقنية كوسيلة تَرُد بها على التقنية حتى تكون من نفس طبيعة وسيلة ارتكاب هذا الإجرام. فوضعت لذلك أنظمة إلكترونية خاصة. ثم أن الضرورة لهذه المكافحة جعلت هذه الجهود تتكرس دوليا و إقليميا أو جهويا (عربيا و غربيا) منتهية بالتمسك بالتعاون الدولي باعتباره أساس مكافحة هذا الإجرام.

1.2.2 : التكنولوجية (التقنية) كأداة لمكافحة الإجرام الدولي الإلكتروني

وجدت تقنية المراقبة الالكترونية قبل وجود الإجرام الالكتروني و كان ذلك مع بداية الحرب الباردة، أين تحالفت الولايات المتحدة الأمريكية مع بريطانيا مرتبطتين إلى شبكة استعلامات مهمتها اعتراض الاتصالات تدعى COMINT [68] و بتطور تكنولوجيات الاتصال ظهور شبكة الإنترنت العالمية بالمستوى المتقدم، تبعها تطور أنظمة المراقبة الإلكترونية و صارت تشتغل في هذا العالم الافتراضي الذي يربط بين كل وسائل الاتصال الحديثة. و بالرغم من تمكنها إلى حد كبير من الحد من الإجرام فإنه نظرا لحداثة هذه التقنية و عدم التحكم في توجيه خدماتها من جهة و بقائها ملكا و حكرا على الدول المهيمنة، جعل منها آلية بوجهين و وسيلة يساء استخدامها بما يمس بسيادة الدول الأخرى.

1.1.2.2 : نظام المراقبة الإلكترونية

سواء سميت أنظمة المراقبة الإلكترونية، أو الدخول المشروع أو الاعتراض، فهي أنظمة ووسائل إلكترونية تشتغل في العالم الافتراضي المتجسد أساسا في شبكة الشبكات العالمية (الإنترنيت) بمستواها المتطور ، حيث اجتهدت الدول في وضعها من أجل تقصي وتتبع وتقفي أثار الجريمة الإلكترونية ومجرمي الإجرام الإلكتروني وإقامة الدليل الجنائي بشأن ذلك ولعل

هذه الأنظمة اعتُمدت لأنها من نفس طبيعة الجريمة. هذه الأخيرة تفاقمت بفضل استخدام الوسائل الإلكترونية ولم يعد ممكنا مكافحتها إلا بنفس السلاح الذي صار آلية لمكافحتها.

وباعتبار هذه الآلية هي من قبيل التطور التكنولوجي في مجال الاتصال، عرفت تطورا وتفعيلا من أجل تأدية دورها في منع الجريمة الإلكترونية أو الاعتداء الإلكتروني. وظلت بطبيعة الحال حكرا على ممالكي التكنولوجية من الدول القوية والمتقدمة وعلى رأسها الولايات المتحدة الأمريكية ولذلك سوف نلاحظ أن هذه الأنظمة عموما هي من وضع أمريكي. [34] [69]

فإذا كانت الاعتداءات الإلكترونية تتخذ من العالم الافتراضي (الأنترنيت) مسرحا ووكرا لارتكاب الاعتداءات الإلكترونية، فحتما يكون ذلك بلهجة خاصة، هذه الأخيرة بعدما صارت مدركة له صارت تعترض وتراقب إلكترونيا وتمكن من اكتشاف مسرح الجريمة أو الاعتداء ومن ثم الدخول و الولوج إليه، لكن لأجل هذا كان بالإضافة إلى التحكم التقني، من محاولة وضع إطار قانوني يصادق على هذه الاستخدامات، التي و إن بدأت منذ حوالي 1948 كأنظمة الاعتراض إشارات الاتصالات الإلكترونية ثم تطورت بتطور هذه الأخيرة التي صارت تعرف بكل هذا التضاد الإلكتروني الذي تشهده اليوم،إلا أنه إلى غاية 1995 لم تكن أية دولة تعترف بوجود مثل هذه الأنظمة التي كانت في قمة تطورها باسم إيشلون Echelon لأن هذا الأخير لم يظهر كنظام للمراقبة الإلكترونية إلا في سنة 1998 أثناء قيام وكالة الأمن الوطنية NSA في الولايات المتحدة الأمريكية بتغيير تصنيف الوثائق السرية بحيث في هذه السنة تم للمرة الأولى إبداء الحكومات الأوروبية لاندهاشها المزعوم بوجود مثل هذا النظام الرقابي الإلكتروني المعمم على كل الكوكب وبدأت تظهر قلقها لظهور أنظمة المراقبة الإلكترونية الذي كان في بادئ الأمر يقتصر على مراقبة الولايات المتحدة الأمريكية لإقليمها باعتبارها صاحبة هذه التكنولوجيا وبتحقيق نتائج عالية واتضاح إمكانية تمديدها خارج إقليمها فهي لم تتوان في ذلك وبالتعاون مع دول العهد انتهت إلى إقامة عدة أنظمة أشهرها نظام carnivore كنظام للمراقبة الإلكترونية داخل الإقليم ونظام إيشلون الخاص بالمراقبة الإلكترونية خارج الإقليم أي على المستوى العالمي.

إن أول نظام وضع سمي بنظام omnivore كان يشتغل على نظام Solaris x86 وفي 1999 تم وضع قالب جديد له سمي بـ Carnivore ثبتته FBI وكان الهدف منه مراقبة شخص واحد، لكن بعد التحقق من اشتغال النظام اتضح أنه بإمكانه مراقبة جميع المشتركين في الخادم الذي تم فيه تثبيت النظام. وكان هذا السبب في إثارة اهتمام FBI بهذا النظام و الإلحاح على تثبيته فأدشئ إذا هذا النظام من طرف NSA وهو يأخذ شكل برنامج يشتغل بنظام windows يسمح بمراقبة جميع الاتصالات الإلكترونية المارة من FAI ويمكنه عمل نسخة

من المعلومات الرقمية التي يتم طبعها إلى FBI سواء كانت رسائل إلكترونية ، CHAT، FTP غرق دردشة وغيرها، وأكثر من ذلك يمكنه رسم مسار تسلل مستعمل شبكة الإنترنيت، سالكا هيئة أحد sniffer، المستعملة من طرف القراصنة من أجل الحصول على مفتاح الدخول إلى الخادم مثلا Serveur[68] .

الاتصالات التي يقوم بها الشخص المشتبه به، وإنما يراقب أيضا العناوين البريدية لجميع المشتركين مع FAI لكن مبدئيا لا يسحب سوى ما يتعلق بالشخص المقصود، وإن كان ما يجب تصفيته يتم تحديده بأمر من الشرطة الأمريكية يبقى من الممكن الإنحراف في القيام بهذه المهمة من دون علم .FAI.

تكمن نجاعة نظام carnivire في أن المعلومات المهمة لا يمكنها أن تضيع في الزخم. يشتغل بواسطة كلمات دالة بحيث يعزل المعطيات التي تحتوي مثل هذه الكلمات ويحولها إلى مصالح الاستعلامات المكلفة بترجمتها، كما يمكن لنظام إيشلون أيضا فحص بحجم Go15 من الوسائل الإلكترونية والمتبادلة عبر غرف الدردشة المرسلة يوميا عبر الإنترنيت.

تعالج وكالة الأمن الوطنية للولايات المتحدة الأمريكية في وقت قياسي 1000 مليار بيت (bits) يتمتع النظام بقدرة تخزين لـ 90 يوم ما يمثل 1 تيرا أوكتي octet

تتقاسم الخمس دول العهد هذه المهمة-

تتجسس NSA على الأمريكيين، أنكلترا، وأوربا وإفرايقيا، كندا، الأعالي القطبية الشمالية، أستراليا، نيوزيلاندا، آسيا و المحيط الأطلسي.

هذه التقنية التي تطلبت أكثر من 120 قمر صناعي صعب حجبها بقدرتها إلتقاط جميع الاتصالات مهما كانت طبيعتها ثم تحليلها إلى "الآذان العملاقة" ذات هوائيات مقعرة بقطر 30 متر والمنتشرة في الفضاء منذ سنة1971 .

بهذا قد صارت الولايات المتحدة الأمريكية قادرة إلى حد ما على مراقبة جميع الإتصالات داخل وخارج إقليمها.

وصار نظام Echelon يوحي إلى إرادتها ورغبتها في إقامة رقابة عالمية. مما جعله نظام بوجهين

2.1.2.2 : نظام المراقبة الإلكترونية آلية ذات وجهين :

إن مكافحة الجرائم الإلكترونية عن طريق اعتماد أنظمة للمراقبة الإلكترونية كآلية أساسية كونها من نفس الطبيعة التقنية للجريمة في حد ذاتها، صار ينجر عنه الكثير من السلبيات، بل صار يساء استخدامها من طرف الدول المالكة لهذه التكنولوجيا.

فإذا كان مما لا شك فيه أن أنظمة المراقبة الإلكترونية التي أشرنا إليها في الفرع السابق، قد حققت نتائج كبيرة في منع الإجرام الإلكتروني أة ملاحقته و أنها اعتمدت من طرف الكثير من الدول و بدأت ترسم شيئا فشيئا في قوانينها الوطنية ، فإنه في نفس الوقت ساعدت على انتهاك حقوق أساسية للدول و الأفراد على السواء و على خرق مبادئ مقدسة سواء في القانون الدولي أو في القوانين الداخلية للدول. و بهذا صارت تعتبر هذه الآلية كسلاح ذو حدين و كوسيلة بوجهين في يد الدول المحتكرة لها مستعملة إياها لتحقيق أغراض أخرى. و صار الاعتداء و رده خاصيتين متلازمتين لآلية واحدة صارت تشبه القواعد العسكرية التي تنصبها الدول المهيمنة و على رأسها الولايات المتحدة الأمريكية بقرار أو لا من مجلس الأمن ضاربة الدول و الشعوب تحت شعار فرض السلم و الأمن الدوليين، أو في اطار ما أصبح يسمى بالحروب الاستباقية.

لقد وجدت مراقبة التدفق المعلوماتي منذ مدة و كان استعمالها على الإقليم الوطني أكثر منه خارج الإقليم أو ما يسمى بالعابر للحدود، و حقا يمكن تبرير هذه المراقبة من زاوية الخطورة التي يشهدها تطور ممارسة الإرهاب، تهريب المخدرات، غسيل الاموال و أيضا إمكانية نشوب الحروب الإلكترونية. و أن حماية النظام العمومي الداخلي و الامن الوطني يفرض على الدولة التأقلم مع التطور التكنولوجي و من ثم اعتماد أنظمة الاعتراضات. [70]
كل هذا من أجل مكافحة الاجرام الذي صار يرتكب عبر الفضاء الالكتروني ابتداء من شبكة الانترنت و ما ترتبط به من وسائل اتصال ككل انواع الهاتف و الاقمار الصناعية التي هي بدجورها مجهزة بتكنولوجيات حديثة و موصولة بانظمة متنوعة في مجال التصنت و المراقبة، و صار بالإمكان قيام مراقبة شاملة من حيث القدرة و المجال المطبقة عليه. و هنا لم يعد يَفرق ممارسة هذه المراقبة داخل الإقليم أو خارجه من حيث يسرة المساس بتلك الحقوق المقدسة.
فمن حيث المساس حقوق الدول الاخرى، نقول أن تطبيق نظام ايشلون Echelon أو نظام كارنيفور Carnivore أو غيرهما من أنظمة المراقبة الالكترونية يثير التسلاؤل حول مدى امكانية التوفيق بين قضايا، سيادة الدول، اختصاصها بل القانون الدولي في حد ذاته مع خاصيات المراقبة الالكترونية كونها عابرة للحدود، متواصلة و آنية، أي لحظية و فورية.[68]
في الواقع ان استخدام انظمة المراقبة الالكترونية قد جعل الدول و القانون الدولي على السواء يواجهان ظاهرة محو الحدود، رمز الاختصاص و السيادة كحقوق صارت تنتهك عن طريق التجسس المتجدد بفضل خاصية التواصل و الديمومة في نظام ايشلون، أين صارت الدولة فريسة لاعتراضات ليس فقط لا يمكنها تحديد موقعها، و إنما من دون أن يكون لها الحق حتى في مراقبة التدفق المار من إقليمها. و حتى نرجئ الحديث عن هذا الجانب إلى الفرع الموالي

نظرا لأهميته، نأتي إلى تبيان كيف يكون المساس بحقوق الأشخاص الخاصة و منها الحريات الأساسية للأفراد و حقوق المؤسسات.

رغم كثرة التشريعات الحامية للحياة الخاصة للافراد لاسيما الإعلان العالمي لحقوق الإنسان المرجع الأساسي الذي يدعو إلى احترام هذا الحق في مادته 12 التي تنص " لا يعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه وسمعته، ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات."

و كذلك المادة 17 من العهد الدولي للحقوق المدنية و السياسية التي تكرس حرمة هذا الحق

" 1. لا يجوز تعريض أي شخص، على نحو تعسفي أو غير قانوني، لتدخل في خصوصياته أو شؤون أسرته أو بيته أو مراسلاته، ولا لأي حملات غير قانونية تمس شرفه أو سمعته.

2. من حق كل شخص أن يحميه القانون من مثل هذا التدخل أو المساس." [68]

لقد سبقت الإشارة إلى أن أنظمة المراقبة الالكترونية تشتغل من خلال كلمات دالة تعترض كل اتصالات الأفراد في العالم الافتراضي و التي تحويها و ليس عن طريق إدخال أرقام هاتف أو فاكس أو عناوين إلكترونية في شبكة الإنترنت لأشخاص معينين لتتم مراقبتهم. إن المراقبة بهذه الكيفية جعلت كل فرد معرض للاستماع

هذا ما أدى بشرائح و فئات مختلفة من المجتمع الكندي باعتباره دوله متقدمة في مجال مكافحة الجرائم الإلكترونية و إرساء أنظمة المراقبة في ذلك، إلى معارضة مشروع الحكومة " الدخول المشروع" Accès légal و التجند من أجل الضغط عليها للعدول عنه.

مبدئيا، يخص هذا المشروع مكافحة الإجرام الإلكتروني، لكنه بالمناسبة يضع إجراءات من شأنها تشديد وسائل المراقبة و التحقيق على كل المواطنين المستعملين للتكنولوجيات الجديدة في جميع مجالات حياتهم، رامية إلأى تعلية قدرة مراقبة أنظمة المعلوماتية من إنترنت و ملحقاتها، و الاتصالات الهاتفية التي صارت جزءا لا يتجزأ من الشبكة العالمية. و من جة أخرى يرمي هذا المشروع إلى إجبار مزودي الاتصالات المعلوماتية كالخوادم les serveurs الخاصة أو العمومية على تخزين و حفظ المعطيات من أجل إعطائها إن لزم ذلك إلى الجهات المكلفة بفحصها، كما أن كل الإرسالات الالكترونية أصبحت تحت المنظار من بريد إلكتروني و مبادلات بنكية و وصفات صيدلانية و معلومات طبية و غيرها. و بهذا يصير جانب كبير لا يستهان به من الحياة الخاصة للأفراد و التي تعتمد أساسا خاصة في المجتمعات المتقدمة مثل المجتمع الكندي على العالم الإفتراضي، عرضة للفضح باعتبار أن مثل هذا المشروع من شأنه أن يرصد أبسط حركة يقدم الفرد على القيام بها و بقدرة فائقة، حتى صار المجتمع كالمكروب تحت المجهر في المخبر.

فهل يمكن بعد هذا أن يكون لحياة الأفراد الخاصة حماية في ظل تلك المبادئ و المواثيق التي كلفت المجتمع الدولي عناء كبيرا من أجل تكريسها إن لم تكن قد أكل الدهر عليها و شرب.
ثم هناك المساس بحقوق المؤسسات العسكرية و الإقتصادية عن طريق التجسس عليها و خرق المبادئ الدولية لتنظيم التجارة. بحيث صارت إمكانية استعمال نظام ايشلون لمع المعلومات ذات الطبيعة الإقتصادية سهلة من الناحية التقنية، خاصة لدي الدول مالكة التكنولوجيا. فلا الولايات المتحدة الأمريكية و لا المملكة المتحدة ترددتا في ذلك . فنجد هذه الأخيرة، تحت شعار حفظ المصالح الاقتصادية للبلد، تجرأ على جمع هذه المعلومات بطريقة غير شرعية. كما تستعمل الولايات المتحدة الأمريكية التجسس الصناعي عن بفضل خدمات و قدرات أنظمة المراقبة.
و على سبيل المثال عرفت اتفاقية GATT و منظمة التجارة العالمية OMC انتهاكات من طرف نفس الدولتين رغم أنهما عضوين فيها، و أيضا رغم أن المادة 14 من اتفاقية منظمة التجارة العالمية ل 15 أفريل 1994 تشترط على الدول ألا تقوم بأي ترتيبات لا تتماشى مع احترام الحياة الخاصة للأفراد، إلا أننا نجد مثلا انجلترا تتصرف بدور غامض و تلجأ إلى المنافسة غير المشروعة بمساعدة تقنيات التجسس .
فإذا كان الاتحاد الأوروبي يضمن بالدرجة الأولى التعاون الاقتصادي بين الدول، كيف يمكن الكلام عن هذا التعاون إذا كانت انجلترا تساعد الولايات المتحدة الأمريكية على سرقة أسواق من الدول الأوروبية
و بعد ما عرفنا كيف تلعب أنظمة المراقبة الإلكترونية، كآلية لمكافحة الإجرام الإلكتروني دورا ازدواجيا بل كيف صارت تستخدم لأغراض أخرى أكثر من استخدامها في منع الجريمة، أصبح من الضروري تأطيرها في إطار القانون الدولي و تحديد عملها من طرف القضاء الجنائي الدولي قبل أن تصير وسيلة إجرام و اعتداء حقيقين.

3.1.2.2 : نظام المراقبة الإلكترونية و مسألة السيادة :

إن اكتشاف نظام إيشلون جعل وضع الدول الأنجلوسكسونية تواجه المجموعة الدولية تماما مثل اكتشاف نظام carnivore الذي وضع الحكومة الأمريكية في واجهة موقف مواطنيها.

مع ذلك يمكننا القول أن المراقبة الإلكترونية أو بالأحرى التي تكون عن بعد، تعتبر ضرورية للأمن الوطني. لكن إذا كانت هذه المراقبة من طرف الدولة على إقليمها تبرر من زاوية النظام العمومي الداخلي، إلا أنه لا بد لها إلى جانب ذلك احترام الحقوق الأساسية للأفراد. بينما القيام بالمراقبة على المستوى العالمي من طرف دولة أو مجموعة من الدول يمس من دون شك

بسيادة الدول الأخرى وبحقوق رعاياها، كما سوف نرى، اعتماد أنظمة المراقبة الشاملة بمعنى تلك التي تخص كل من المرسل والمستقبل من دول تمييز، مثل نظام أيشلون أو carnivore قد يخلق خصومات حول الكوكبة، مما يطرح بجدية أكثر بعض المسائل بخصوص مصير حدود اختصاص وسيادة كل دولة، ومدى استساغة كون الدولة تتمتع باختصاصٍ يُمَكنها من المراقبة الشاملة على إقليمها، وهي من جهة أخرى تُمَس سيادتها وتُشارك في اختصاصها ما دام هناك مراقبة شاملة على كل ما يصدر عنها يمكن أن تكون من طرف الغير ومن دون أن تَقْدر عمل شيء بل قد لا تدرك ذلك.

و الأعقد من ذلك، كيف يمكننا أن نتكلم عن نظام عمومي دولي وفي نفس الوقت يضمن سيادة الدول وحقوق الأفراد؟

في القرن 19 كانت تعرف السيادة بصفة عامة بأنها سلطة عليا وغير محدودة. أين نجد الفيلسوف هيجل ربط مفهوم السيادة بالقوة المطلقة للدولة. لكن لم يكن لهذا المفهوم واقعا، لا لشيء إلا لأنه في المجتمع الدولي المعاصر الذي كله علاقات دولية تصطدم سيادة كل دولة بسيادة الدول الأخرى التي تتمتع بالشرعية. وبهذا صارت السيادة تظهر كمصدر الاختصاصات التي تأخذها من القانون الدولي. [68]

لكن المشكلة أن نظاما كنظام أيشلون قد ينحرف عن الإطار الشرعي بحيث كل ما يمكنه القيام به يخرق القانون الدولي، لما يمس مباشرة بتساوي الدول في السيادة مثل ما جاء في ميثاق الأمم المتحدة وكذلك استقلاليتها في ذلك [71] وعلى حد ما جاء في التقرير الذي أعده خبراء مكلفون بالأبحاث في مجال الإعلام الآلي والمرفوع إلى اللجنة الدائمة لمراقبة مصالح الاستعلامات في بلجيكا، أن الالتقاط المبالغ فيه للرسائل من طرف شخص أجنبي يمس بسيادة الجولة بمعناها الدال على مبدأ استقلالية كل دولة و ظل النظام الدولي. وهنا ، كيف تصبح استقلالية أي دولة إذا كانت أسرار أجهزتها من إدارة وحكومة وشركات وحتى أسرار رعاياها، يمكن أن تلتقط لخدمة قوى أجنبية بمجرد اقتحامها الفضاء.

إن هذه التكنولوجيا كونها حكرا على بعض الدول العظمى فقط، وعلى رأسها الولايات المتحدة الأمريكية سوف ينال من مبدأ المساواة في السيادة بين الدول. وبهذا يصبح الكلام عن مبدأ السيادة المقرر في ميثاق الأمم المتحدة عبارة عن أسطورة وخرافة ليأتي نظام أيشلون ليبطلها وهنا يكون هذا النظام قد جسد مقولة Marcel Merle "لا بد أولا من تحطيم الخرافات التي صنعها رجال القانون من حديد". فصارت السيادة خرافة لها مفعول يغطي عدم المساواة بجميع جوانبه من حيث الطبيعة والأدوار الموجودة بين الدول. [72]

إن الواقع الذي يفرض نفسه، هو أن تمتع الدول من حيث الحقوق والامتيازات في ظل تطبيق مبدأ المساواة في السيادة، ليس مضمونا في مجال القضاء الإلكتروني، وعليه صارت الدول الضحية بسبب عدم المساواة، أكثر تضررا بمجيء أو قيام المجتمع المعلوماتي أو الإلكتروني خاصة إذا لم ننس أنه مسرح مرشح لاحتواء جرائم خطيرة، وهكذا أصبح يساء استخدام الآلية الأساسية لصد ومكافحة الاعتداءات الإلكترونية، التي رأينا كيف يمكن أن تشكل جريمة دولية وبالتالي بصبح الإجرام الدولي إلكترونيا، وأساسية هذه الآلية تكمن في كونها لا يستغنى عنها مهما توفرت الآليات الأخرى إلى أن يثبت العكس، تبذل المجموعة الدولية جهودا كبيرة وتنفق أموال كثيرة من أجل تفعيل هذه الآلية لتعود في الأخير سلبا و تُمَس عن طريقها في أقدس مبادئ المجتمع الدولي وهو مبدأ السيادة.

وليتها كانت هذه الآلية ملكا للمجموعة الدولية ككل. لكن للأسف هي ملك وحكر على الولايات المتحدة الأمريكية وبالذات في يد NSA، المنظمة المكلفة باعتراض الاتصالات بجميع أشكالها، وهي أي هذه الوكالة أغنى بكثير من CIA، بحيث يقدر أنها تشكل على الأقل 100.000 شخص عبر العالم وتتوفر على ميزانية حقيقية يقدرها البعض بأكثر من 16 مليار دولار.

فعلى حسب الأخصائي جون بيك John Pike في مسائل الاستعلامات لدى فدرالية العلميين الأمريكيين "تلتقط الوكالة العظمى للأمن الوطني كل أو 95% من الاتصالات المارة من كمبيوترات عملاقة. أجل كل المكالمات الهاتفية والفاكسات والبريد الإلكتروني وجميع المعطيات المعالجة آليا يتم اعتراضها وبعبارة أخرى اعتراض جميع أمواج الراديو والهاتف والاتصالات عبر الانترنيت.[68]

وإن كان ليس القصد هو تكرار قدرات هذه التقنية أو التعجب والاستغراب من عظمتها، لأنها هي أصلا وضعت لتكون على هذه الفعالية، وأننا إذا أضفنا أنه عن طريق القواعد السرية التي تملكها أمريكا بعدد 50 قاعدة الموضوعة للتنصت على الأقمار الصناعية الخاصة بالاتصالات وهي منتشرة عبر 20 دولة يوجد أهمها في انجلترا، نيوزيلندا، اليابان، ألمانيا وأستراليا، يبدوا أن أمر المساس بالسيادة ليس أمرا مزعوما خاصة وأن مثل هذه الدول لم يُثبت واقع المجتمع الدولي أو العلاقات الدولية براءتها.

فهل نحن أمام ضرورة إعطاء مفهوم جديد للسيادة ؟.

قبل كل شيء، إننا إذا واجهنا الاختصاص الإقليمي للدول، الذي يمارس في إطار السيادة الإقليمية، كأول تصور لمفهوم السيادة مثل الذي طرح في قرار لوتيس LOTUS لمحكمة العدل الدولية مع كون الاعتراضات التي يتم القيام بها من خلال نظام ايشلون و التي تعتبر من قبيل النشاطات الفضائية غير القابلة للتحديد مكانيا.

و إذا عرفنا أن كل من نظام اعتراض الاتصالات COMINT و نظام اعتراض الإشارات SIGINT ، لا يقتصران بالضرورة على خرق المجال الإقليمي للدول المقصودة فقط، مادام أن جزءا كبيرا من هذه الاعتراضات يتم بتلقي رسائل مارة عبر الأقمار الصناعية و أن 40% من الاتصالات العالمية لغير الولايات المتحدة الأمريكية تمر عبر شبكات الولايات المتحدة. إن هذه التبعية التكنولوجية قد سهلت من سيطرة الدول المالكة لها.

كما أن غالبا ما تتم الاعتراضات من غير أن تخرق اقليم الدولة المقصودة.

فإن اللجوء الى فكرة الإقليم من اجل ضمان سيادة الدولة و اختصاصها غير صالح لما يتعلق الأمر بمعلومات سابحة في فضاء افتراضي غير محسوس.

فهنا تتحقق مقولة مارسل مارل Marcel Merle " يتراجع الإقليم شيئا فشيئا كرمز لسيادة الدولة".

و هذا في سياق كلامه عن فرضية وجود نظام أو مجموعة دولية من غير إقليم. [72]

ففي حالة وقوع الاعتراضات داخل الإقليم الوطني للدولة، فتجد هذه الأخيرة نفسها أمام تطبيق قوانينها الخاصة بأفعال الخيانة و التجسس و لا يطرح أي مشكل بخصوص إدانة مرتكب هذه الأفعال سواء كان شخصا معنويا او طبيعيا بما في ذلك مؤسسات الاتصالات. و عليه، مشكل اختصاص الدولة على إقليمها فيما يخص الاعتراضات، لا يطرح في حالة ارتكابها من طرف شخص يتواجد على إقليمها.

لكن كيف يكون الحل بالنسبة للدولة التي تريد أن تتمسك باختصاصها بعد ما رأينا أن جل الاعتراضات تتم خارج المجال الإقليمي و أنها تشكل نشاطا فضائيا غير قابل للتحديد بحيث لا مجال للكلام عن السيادة الإقليمية. إن هذا يستدعي ضرورة تطوير القانون الدولي ليرسم مجال المشروع لقبول الاعتراضات.

غير أنه تماما مثل ضبط استعمال وسيلة الإنترنت، لا يصير هذا ممكنا إلا عن طريق تكثيف التعاون الدولي خاصة مع الولايات المتحدة الأمريكية، و هو الأمر الذي ليس بالسهل مما يبقي كل شيء مغلق على إرادة الدول و بذلك يجب تحديد فيما إذا كانت المجموعة الدولية ككل، لها من الوزن ما يلزم لإخضاع الولايات المتحدة الأمريكية، دون إغفال أمل كل دولة في الاستفادة خفية من خدمة نظام كايشلون، بل إن لم تكن تسعى لاقتنائه و وضعه تحت تصرفها.

2.2.2 : التعاون الدولي كضرورة لمكافحة الإجرام الدولي الإلكتروني

لقد بات مسلما به أنه لا سبيل إلى مكافحة الإجرام الدولي عموما دون أن تتحد الدول ساعية إلى التعاون فيما بينها من أجل ذلك. و هذا يعني على الأقل التزامها بسن تشريعات

داخلية، ناهيك عن ضرورة استعدادها للدخول في اتفاقيات دولية تسعى إلى التعاون من أجل تفعيل تلك المكافحة.

وخصوصية أهمية التعاون الدولي في التعامل مع الجرائم الإلكترونية, تكمن في تطويره لأساليب متشابهة لتحقيق قانون جنائي وإجرائي لحماية شبكات المعلومات الدولية, خاصة أن هذه الجرائم هي عابرة للقارات ولا حدود لها, و أن انتشارها عالميا أمام عجز الدول فرادى عن مكافحتها، زاد من حدة ضرورة هذا التعاون. [73]

و لتحقيق هذا التعاون، قد عملت منظمات و هيئات دولية على بذل جهود معتبرة تدخل في إطار مكافحة الإجرام الإلكتروني. و قد تفاوتت هذه الجهود من حيث أهمية و دور هذه الهيئات في إرساء و تطوير قواعد القانون الدولي في هذا المجال، و أيضا من حيث درجة خطورة الجرائم التي اهتمت بتجريمها و مكافحتها. و سوف نتعرض في الفروع التالية إلى أهم هذه الجهود التي، إما أنها تدعوا إلى التعاون الدولي و إما أنها جاءت تفعيلا لما دعا إليه التعاون الدولي.

1.2.2.2 : جهود الأمم المتحدة في مواجهة جرائم الحاسب الآلي على النطاق الدولي.

عملت الأمم المتحدة من خلال جهود مضنية منذ إنشائها، على التصدي للجريمة الدولية بوجه عام، و للجريمة الإلكترونية في مراحل متلاحقة، حيث أكدت على ضرورة تعزيز العمل المشترك بين أعضائها للتعاون من أجل الحد من انتشار و تعاظم آثار الجريمة الإلكترونية.

و هذا ما يظهر من خلال المؤتمرات الدولية التي دعت إليها الأمم المتحدة، و التي كانت كلها تقريبا تحت عنوان : مكافحة الجريمة بكل صورها ، ناهيك عن المؤتمرات التي ترعاها الجمعية الدولية لقانون العقوبات. و في خضم هذه الحركة المتسارعة للتصدي للجريمة الدولية، قد حظيت الجريمة الإلكترونية باهتمام متزايد خاصة في إطار الوكالات و المنظمات التي تعمل تحت رايتها المنظمة العالمية للملكية الفكرية (وايبو) التي وقعت في استكهولم في 14 يوليو / تموز 1967 وعدلت بتاريخ 28 سبتمبر/ أيلول 1979، وهي إحدى الوكالات الستة عشر المتخصصة في منظومة الأمم المتحدة، وتدير 23 معاهدة دولية معنية بمختلف جوانب حماية الملكية الفكرية، وتضم في عضويتها 181 دولة. وقد اعتمد المؤتمر الدبلوماسي المنعقد في 20 ديسمبر / كانون الأول من عام 1996 بعض التعديلات على حق المؤلف، في معاهدة الويبو، لتواكب التطور العلمي وخاصة فيما يتعلق ببرامج الحساب الآلي. [44]

و أمام الظروف الدولية التي تطورت كانت الحاجة إلى إيجاد سبل و آليات قانونية لمواجهة الجريمة المرتكبة على البرمجيات التي تستعمل في الحاسبات الآلية ، ضرورية و ملحة ما أدى

بالمنظمة العالمية للملكية الفكرية إلى إنشاء مجموعة عمل مكونة من الخبراء و التقنيين المتخصصين بغرض حماية برامج الحاسب الآلي و بالتالي التصدي للجريمة التي ترتكب بواسطة هذه الأخيرة ، مع الإشارة إلى التطور القانوني الحاصل آن ذاك لم يكن يعتبر برامج الحاسب الآلي من ضمن الابتكارات الفكرية ، و هو ما نجده مؤكدا في الاتفاقية الأوروبية لبراءات الاختراع المنشأة بتاريخ: 1973/10/05 ، و لكن نظرا للاستمرارية التي تبنتها لجان الخبراء في دراسة الأساليب المناسبة لحماية برامج الحاسب الآلي و ما يعلق بجانبها التقني ، و من خلال اجتماعاتها الدورية ، حيث تم في آخر هذه الاجتماعات عام 1985 و بالتعاون بين الويبو و اليونيسكو في مدينة جنيف، تبني الاتجاه السائد لدى أغلب الدول الصناعية و دول العالم الثالث القاضي بإخضاع برامج الحاسب الآلي للقوانين المنظمة و الحامية لحق المؤلف ، و منذ ذلك الحين و حتى وقتنا الحاضر لا زالت الدول تعمل جاهدة على تعديل تشريعاتها الوطنية بما يوافق توصيات تلك اللجان ، حيث تم إضافة أو إدراج برامج الحاسب الآلي إلى المصنفات الأدبية المحمية بما يتناسب و القوانين الوطنية .

إضافة إلى ذلك، عقدت الأمم المتحدة عدة مؤتمرات خاصة بمنع الجريمة و معاملة المجرمين المتهمين بالجرائم التقنية أو الجرائم الإلكترونية بوجه خاص.

حيث تشير في هذا الإطار إلى المؤتمر الدولي الذي تم عقده تحت رعايتها بمدينة [ميلانو] الإيطالية عام 1985 ، حيث تمخضت عنه مجموعة من القواعد التوجيهية لمكافحة الجريمة الإلكترونية ، و التي اكتملت صياغتها بشكل نهائي في الاجتماعات الإقليمية التحضيرية للمؤتمر الثامن الذي انعقد بمدينة [هافانا] الكوبية عام 1990 و الذي كان الغرض منه هو تبنى هذه المبادئ ، و قد تم ذلك فعلا.

و كان هذا المؤتمر قد كلف لجنة الخبراء العشرين بدراسة موضوع حماية نظم المعلومات و الإعتداء على الحاسب الآلي ، و إعداد تقرير عنه لعرضه على المؤتمر الثامن للأمم المتحدة للوقاية من الجريمة، و بعد أن قامت اللجنة المذكورة بدراستها عقدت اجتماعا في كندا و أقرت مجموعة من المقترحات و التوصيات لمكافحة الظواهر الإجرامية المتعلقة بالحاسب الآلي، و تبنى مؤتمر [هافانا] السابق الإشارة إليه هذه التوصيات بعد أن أدخل عليها بعض التعديلات مع تضمينها بعضا من المقترحات ، و ذلك بأن أوجب تطبيق التطورات الجديدة في مجال العلم و التكنولوجيا في كل مكان لصالح الجمهور، و هذا للحيلولة دون استشراء الجريمة و انتشارها، كما أكد على أن التكنولوجيا بما أنها قد تولد أشكالا جديدة من الجريمة فإنه ينبغي اتخاذ تدابير ملائمة ضد حالات إساءة الاستعمال الممثلة لهذه التكنولوجيا، و أشار إلى مسألة الخصوصية التي يمكن أن تخترق عن طريق الإطلاع على البيانات

الشخصية المخزنة داخل نظم الحاسب الآلي، و التي تشكل انتهاكا لحقوق الإنسان و اعتداء على حرمة الحياة الخاصة، و أكد المؤتمر على وجوب اعتماد ضمانات ملائمة لصون السرية و إقرار نظم تكفل وصول الأفراد إلى هذه البيانات لتصحيح الأخطاء فيها، كما أكد المؤتمر من خلال قواعد التوجيهية على ضرورة تشجيع التشريعات الحديثة التي تجرم و تتناول جرائم الحاسب الآلي باعتبارها نمطا من أنماط الجريمة المنظمة كجريمة غسيل الأموال و الإحتيال المنظم، و فتح حسابات و تشغيلها بأسماء وهمية ...و غيرها.

و يمكن إجمال التوصيات السابق الإشارة إليها و التي أوردها مؤتمر [هافانا] لعام 1990 في العناصر التالية [74]: مع الدعوة إلى التعاون الدولي في مجال مكافحة الجريمة الإلكترونية

- ضرورة تحديث و عصرنة القوانين الوطنية الجنائية بما يتوافق و طبيعة الجريمة الإلكترونية
- تحسين و تطوير أمن الحاسب الآلي ، مع اتخاذ التدابير الفعالة لمنع الجريمة .
- العمل على اتخاذ إجراءات تدريب متطورة بالنسبة للموظفين و الوكالات المسؤولة عن منع الجريمة الاقتصادية و الجرائم المتعلقة بالحاسب الآلي ، و التحري و الإدعاء فيها .
- إدراج آداب الحاسب الآلي ضمن مفردات مقررات الاتصالات و المعلومات .
- العمل على وضع منهجيات لحل المشكلات المتعلقة بالمجني عليهم في تلك الجرائم.

و في إطار المؤتمر التاسع لمنع الجريمة و معاملة المجرمين الذي رعته الأمم المتحدة بالقاهرة عام 1995، حيث تم التأكيد على وجوب حماية خصوصية حياة الإنسان، و كذا ملكيته الفكرية من تزايد مخاطر التكنولوجيا ، مع ضرورة التنسيق و التعاون بين أشخاص المجتمع الدولي .

و في 2000 عقدت الأمم المتحدة مؤتمرها العاشر تحت نفس العنوان بمدينة [بودابيست] بالمجر [52]، حيث أكدت من خلاله الأمم المتحدة على وجوب العمل الجاد للحد من انتشار الجرائم الإلكترونية التي تتزايد كل يوم ، باعتبارها نمطا جديدا و حديثا من الجرائم التي أفرزتها التطورات الهائلة في مجال التكنولوجيا و المعلوماتية ، لذلك وجبت المبادرة باتخاذ التدابير و الإجراءات المناسبة للتصدي و الوقوف في وجه القرصنة التي تستعمل بأساليب تختلف عن تلك المألوفة.

2.2.2.2 : دور المجلس الأوروبي في مكافحة الإجرام الدولي الإلكتروني .

لعب المجلس الأوروبي دورا بارزا في تنظيم و محاولة الحد من جرائم الحاسب الآلي من خلال إقراره للعديد من التوصيات الخاصة بحماية البيانات ذات الصبغة الشخصية من سوء

الاستخدام و حماية تدفق المعلومات و في 1981/01/28 وقعت اتفاقية تحت مظلة المجلس الأوروبي تتعلق بحماية الأشخاص في مواجهة المعالجة الإلكترونية للبيانات ذات الصبغة الشخصية .

بالإضافة إلى ما سبق فقد صدر عن المجلس الأوروبي العديد من القواعد التوجيهية في مجال جرائم الحاسب الآلي ، تضمنت وجوب تجريم العديد من السلوكيات التي تعد من الجرائم كالغش المعلوماتي و تزوير المعلومات و سرقة الأسرار المخزنة و التوصل غير المصرح به و سرقة منفعة الحاسب ، كما أن هذه الإجراءات تضمنت عددا من الإجراءات الفنية التي يتوجب اتخاذها بهدف الحيلولة دون الوصول غير المرخص به إلى المعلومات المختزنة كحماية كلمة السر المستخدمة في النهايات الطرفية و حماية الأوامر الخاصة بالتشغيل، و ترميز المعلومات الشخصية و أسماء من تتعلق بهم. [73]

غير أن أهم النشاطات الهامة و الرئيسية للمجلس الأوروبي يتمثل أساسا في الاتفاقية الأوروبية بشأن جرائم الحاسب الآلي ، المنشأة بتاريخ 2000/04/25 الذي توج بها اجتماع المجلس في مدينة ستراسبورغ، حيث تصدرت الاتفاقية مقدمة فحواها أن الدول الأعضاء و حرصا منها على حماية مجتمعاتها من جرائم الحاسب الآلي و إقرارا بحاجتها إلى التعاون بين الدول الأعضاء و العمل على تطوير التعاون الدولي، و حتمية انتهاج سياسة جنائية مشتركة تضمن من خلالها حماية مجتمعاتها من الجرائم المرتكبة عبر الفضاء الإلكتروني يجب عليها أن تعمل على سن تشريعات ملائمة مع ضرورة تعزيز التعاون الدولي في ظل تزايد معدلات الجرائم المرتبطة بالتقنية من جرائم شبكات الحاسب الآلي ، و الاعتداء على المعلومات الإلكترونية [39] و التي تتطلب القيام بجهود كبيرة للبحث عن الأدلة و الإثبات نظرا لما تتميز به هذه الجرائم لأن الأدلة في هذه فيها تخزن و تنقل بواسطة الشبكات في عالم افتراضي.

فجاءت هذه الاتفاقية في أربعة فصول، حيث خصص الفصل الأول لضبط المصطلحات إذ ورد في نص المادة الأولى من الاتفاقية عدة تعاريف ، كتعريف نظام الحاسب الآلي بأنه : أي جزء من الأجزاء المترابطة التي تعالج البيانات و تشغل البرامج ، و عُرفت معطيات الحاسب بأنها تمثيل للحقائق و المعلومات بشكل ملائم للمعالجة في أي نظام حاسب آلي ، كما عرف مقدم الخدمة بأنه أي هيئة عامة أو خاصة تزود مستخدميها بإمكانية تبادل الاتصالات الإلكترونية.

و في الفصل الثاني تناولت الاتفاقية الإجراءات الواجب اتخاذها على المستوى الوطني، و في القسم الأول من هذا الفصل الذي يتعلق بوجودية القانون الجنائي ، خُصص العنوان الأول منه للاعتداءات ضد السرية و الوفرة التي يجب أن تتمتع بها معطيات الاتفاقية إلى وجوب أن

يعمل كل طرف مشترك في هذا الميثاق لبناء تشريعات أو إجراءات رادعة لمنع الاعتداءات على الصعيد الوطني.

كما توجب الاتفاقية على الدول الأعضاء إضافة نصوص قانونية خاصة بالاعتراض غير الشرعي الذي تم من خلال نفس نظام الحاسب أو من خلال اعتراض البث الكهرومغناطيسي للمعطيات ، و إضافة أيضا نصوص قانونية أخرى تتعلق بإتلاف المعطيات و إتلاف الأنظمة ، و وجوب تبني نصوص تجرم التعطيل الكبير لوظيفة الحاسب الآلي سواء بإدخال أو بث أو تخريب أو حذف أو تغيير للمعطيات و المعلومات الشاغلة فيه وفقا لما جاء في المادة الخامسة من الاتفاقية.

بينما فيما يخص الجرائم المتصلة بالحاسب الآلي ، فجاء في المادة السابعة من العنوان الثاني : تسمية الجرائم المعالجة آليا، ما يتعلق بالتزوير المرتبط بالحاسب الآلي على وجوب إدراج الدول لتشريعاتها بما يضمن العقاب عليه مع ترك المجال مفتوحا فيما يخص تنظيم مسألة القصد الجرمي.

و في المادة الثامنة الخاصة بالاحتيال المتصل بالحاسب الآلي ، أوجبت الاتفاقية على الدول الأعضاء وجوب إدراج الاحتيال الذي يتم إما بإدخال أو تغيير أو حذف أية معطيات و التدخل في وظائف الحاسب الآلي يقصد تحقيق منفعة اقتصادية للشخص أو للغير .

أما العنوان الثالث، تناول الاعتداءات المتعلقة بالمحتويات ، و جاء في المادة التاسعة من الاتفاقية تحريم تداول الصور الإباحية للأطفال ، و كل ما يشمل ذلك من ممارسات جنسية مع الأحداث سواء في حالة أي شخص يتظاهر بأنه طفل أو أي صور حقيقية تمثل طفلا يباشر العملية الجنسية ، و أشارت الاتفاقية إلى أن تعريف الحدث يرجع في تعريفه الأول للدول الأعضاء ، و لكن في جميع الأحوال يجب ألا يتجاوز في سنه 18 عاما .

و تطرق العنوان الرابع إلى الاعتداءات المتصلة بحقوق النسخ، حيث ورد في الفقرة الأولى من المادة العاشرة، وجوب تبني الدول بقوة في تشريعاتها نصوصا قانونية تحرم إعادة إنتاج أو توزيع أي مواد محمية بقوانين حماية الملكية أو أي اعتداء عليها عن طرق الحاسب الآلي ، بالشكل المخالف لاتفاقية برن بشأن المصنفات الأدبية و الفنية ، و في فقرتها الثانية أشارت إلى حقوق التأليف المحمية في الدول المجاورة كما جاء في اتفاقية الويبو .

و تناول العنوان الخامس مسألة المسؤولية و العقوبات حيث نصت المادة الحادية عشر على وجوب معاقبة الشروع في هذه الجرائم و عقاب المساهم على ارتكابها ، و المادة الثانية عشر تخص المسؤولية عن المساهمة بحيث يتوجب معاقبة [لأشخاص أو المؤسسات التي

ترتكب الجريمة لمصلحتهم شريطة أن يكون مرتكب الجريمة ممثلا قانونيا للمؤسسة و يملك سلطة اتخاذ القرار إذا تم ارتكاب الجريمة بتكليف منهم.

و تشديدا للعقوبة الموقعة على مرتكبي هذه الجرائم، أوجبت المادة الثالثة عشر الخاصة بالعقوبات على أن تكون من السالبة للحرية مع فرض الغرامات.

أما بخصوص القسم الثاني من هذه الاتفاقية فلقد خصص للقانون الإجرائي ، حيث تم التطرق إلى أحكام التفتيش و مصادرة معلومات الحاسب الآلي المخزنة التي تفيد في التحقيق، كما تناول تنظيم الأحكام الخاصة للتعاون ما بين الدول الأعضاء في مجال التحقيق و تبادل المعلومات و تقديم المساعدة .

و اهتم الفصل الثالث من الاتفاقية بمسألة التعاون الدولي حيث تضمن عدة مبادئ عامة تلزم الدول الأعضاء بوجوب التعاون لاتخاذ الإجراءات و التشريعات الكفيلة بتحقيق التعاون و تطبيق التشريعات الدولية في مجالات التحقيق و سرقة المعلومات . و جمع الأدلة الإلكترونية وفقا لما جاء بنص المادة العشرين من الاتفاقية. و تناولت المادة الواحدة و العشرون أحكاما خاصة تتعلق بتسليم المتهمين كما تضمنت عدة مواد قانونية تتعلق بالتعاون المتبادل، و منه ما يخص المعلومات إذا كانت تحت سلطة دولة أخرى مخزنة في مجالها، و من ثم تسليم هذه المعلومات، و وجوب التزام كل طرف بتعيين مركز اتصال دائم و على مدار الساعة و في أيام العطل لاستقبال طلبات التحقيق في الاعتداءات التي تقع على معطيات الحاسب الآلي و المعلومات كما يشتغل هذا المركز لجمع الأدلة الإلكترونية.

و تعد هذه الإتفاقية بمثابة القانون بين الدول الأعضاء و التي بموجبها تلتزم الدول الأعضاء في المجلس و الموقعون عليها بضرورة العمل على تنفيذ أحكامها و الخضوع لها و احترام تنفيذها و تطويع النصوص القانونية بالشكل الذي يضمن عدم التعارض مع أحكامها .[75]

إضافة إلى ما سبق الإشارة إليه، من الجهود الدولية التي بذلتها منظمة الأمم المتحدة ووكالاتها المتخصصة و المجلس الأوربي في إطار التعاون الدولي من أجل مكافحة الجرائم الإلكترونية، هناك جهودا بُذلت تبعا لذلك من طرف الكثير من الدول تفعيلا و تعزيزا لهذا التعاون الذي لا نجد أي معاهدة أو اتفاقية دولية إلا و تنادي و تدعو إليه. إذ اتجهت غالبية الدول خاصة المتقدمة تكنولوجيا إلى سن تشريعات و نصوص قانونية جديدة تجرم الاعتداءات الإلكترونية و ذلك إما - كما سبق الإشارة إليه – باستحداث قوانين جديدة خاصة تصف جرائم إلكترونية، و إما على الأقل بإدراج بعض الأفعال و تجريمها إلى جانب الجرائم التقليدية في تشريعاتها القائمة بالرغم أن دولا أخرى فضلت عدم تقييد هذه التكنولوجيا. [63] [14]

3.2.2.2 : التعاون العربي

من أبرز الجهود العربية التي بذلت في إطار مواجهة الجرائم الإلكترونية، و المسماة جرائم الحاسب الآلي أو الكمبيوتر و غيرها، ما تجسد بموجب القرار رقم 229 عام 1996 الصادر عن مجلس وزراء العدل العرب للقانون الجزائي العربي الموحد ، ، حيث وردت في الباب السابع الخاص بالجرائم ضد الأشخاص مواد خاصة بالاعتداء على حقوق الأشخاص الناتج عن الجذاذات و المعالجات المعلوماتية ، خاصة المواد من 461 إلى 464 ، و التي أكدت على وجوب حماية الحياة الخاصة و أسرار الأفراد من خطر المعالجة الآلية و كيفية جمع المعلومات الاسمية و المحافظة عليها ، وعلى ضرورة عقاب من يقوم بفعل الدخول عن طريق الغش إلى كل أو جزء من نظام المعالجة الآلية للمعلومات ، أو عرقلة أو إفساد نظام التشغيل عن أداء وظائفه المعتادة ، وتغيير المعلومات داخل النظام ، وتزوير وثائق المعالجة الآلية ، والسطو على المعلومات و البيانات المخزنة .

أما في إطار حماية الملكية الفكرية وحق المؤلف ، فقد تم عقد إتفاقية عربية في هذا الإطار ، حيث أوصى المؤتمرون عام 1981 ببغداد الدول العربية بالمصادقة عليها ، وقد ورد في ديباجة الاتفاقية، إن الدول العربية قد تحذوها الرغبة على حد سواء في حماية حقوق المؤلفين على المصنفات الأدبية و الفنية بطريقة فعالة و موحدة ، استنادا للمادة الحادية و العشرين من ميثاق الوحدة الثقافية العربية الصادرة عام 1964 ، التي أهابت بالدول العربية ضرورة وضع تشريعات محلية لحماية الملكية الأدبية و الفنية و العلمية ، وهذا من أجل وضع نظام عربي موحد لحماية حقوق المؤلف .كما أبرمت المنظمة العربية للتربية و الثقافة و الفنون اتفاقية عربية خاصة بتيسير انتقال الإنتاج الثقافي العربي عام 1987 .وقد انعقد مؤتمر عربي دولي لحماية الملكية الفكرية و الإجراءات المطلوبة من الدول العربية في عمان عام 1995 ، وهذا من أجل تنفيذ اتفاقية تريبس (TRIPS) . [73]

وقد عقدت الجمعية المصرية للقانون الجنائي مؤتمرها السادس عام 1993 ، حول جرائم الكمبيوتر و الجرائم الأخرى في مجال تكنولوجيا المعلومات ، حيث أكد المؤتمرون على عالمية جرائم المعلوماتية ووجوب تكاتف الجهود لمكافحتها لأنها تمثل وجها سلبيا للتقدم الحضاري، وضرورة تعديل نصوص قانون العقوبات التقليدية ، أو إضافة نصوص جديدة، للإحاطة بمعظم الأنشطة المراد تجريمها. كما أوصى المؤتمرون بضرورة التعاون الدولي في مجال مكافحة جرائم المعلوماتية خاصة فيما يتعلق بالإنابة القضائية و تسليم المجرمين و تنفيذ الأحكام وتدريب رجال الضبطية القضائية و النيابة العامة و القضاة على طرق التحقيق و جمع الأدلة الخاصة بمثل هذا النوع من الجرائم.

وفي مؤتر بيروت عام 1997 طالب المؤتمرون بضرورة إنشاء محاكم متخصصة للبت في النزاعات المتعلقة بالحماية الفكرية و تشجيع التعاون بين الدول العربية . وفي المؤتمر الثاني للدول العربية المتعلق بحماية الملكية الفكرية عام 1998 ، طالب المؤتمرون بضرورة تسهيل نقل التكنولوجيا من الدول الصناعية إلى المنطقة العربية وحماية الاختراعات ومكافحة القرصنة و تسهيل نقل اختراعات العلماء العرب إلى أوطانهم . تضاف هذه الجهود إلى الجهود التي تبذلها المؤسسات المعنية بالموضوع ، من نقابات محامين و جامعات وغيرها من المؤسسات المتخصصة. [73]

4.2.2.2 : التعاون من خلال الجمعيات و المنظمات العالمية

إن للجهود الجماعية في مجال مكافحة جرائم المعلوماتية دور لايستهان به ، ففي عام 1992 عقدت الجمعية الدويلة لقانون العقوبات مؤتمرا تناولت فيه بالبحث مدى التحديات التي تنطوي على إساءة استخدام الحاسب الآلي ، ومدى الضرر الناجم عن الاعتداء على نظم المعلومات وأكدت على ضرورة تجريم مثل هذه الأفعال المستحدثة التي نجمت عن التقنية العالية في مجال المعلوماتية . أما في مؤتمر العاصمة البرازيلية (ريو دي جانيرو) عام 1994 الذي نظمته الجمعية الدولية لقانون العقوبات ، فقد تم مناقشة موضوع جرائم المعلومات ضمن موضوعات المؤتمر ، حيث أوصى المؤتمر بضرورة التكاتف الدولي لمحاربة مثل هذا النوع من الجرائم.

وللإتحاد الدولي للملكية الفكرية الكائن مقره بالعاصمة الأمريكية (واشنطن دي سي) دور هام في مجال نشر الدراسات و الإحصائيات المنتظمة المتعلقة بحجم خسائر الدول من جراء أعمال القرصنة و خاصة المتعلقة منها بالبرامج ، ومناقشة الأحكام المتصلة بحماية حقوق الملكية الفكرية وفقا لاتفاقية (تريبس) و بيان نقاط الضعف فيها ، كعدم إمكانية التفتيش في غياب الخصم ، و انخفاض قيمة التعويضات التي يقررها القانون ، وعدم إمكانية إلقاء الحجز على الآلات المستخدمة في القرصنة ...، ويرى الإتحاد إمكانية مواجهة القرصنة من خلال اتخاذ الإجراءات الفورية ضد القطاع الأكبر من القراصنة التجاريين ، وفرض عقوبات رادعة وتطبيق الالتزامات المفروضة وفقا لاتفاقية تريبس ، ووضع أسس متكاملة من خلال إتاحة الإجراءات المدنية و الإدارية و الجنائية لتنفيذ القانون بصورة فعالة ضد أشكال القرصنة في مجال حق المؤلف و القرصنة على خط الشبكة (On Line) في مجال استخدام الحواسيب .

وتعتبر جامعة " ستانفورد – كاليفورنيا " في الولايات المتحدة الأمريكية من المؤسسات العلمية الرائدة على المستوى العالمي، حيث تزايد اهتمام في الآونة الأخيرة بجرائم التقنية العالية، ونشر العديد من الدراسات و الإحصائيات حول جرائم الكمبيوتر و أصنافها . وقامت بعقد العديد من

المؤتمرات أبرزها مؤتمر عام 1999 بمشاركة العديد من المنظمات و الهيئات الدولية ، والذي قدمت فيه اقتراحات لاتفاقية دولية لتعزيز الحماية من الإرهاب و جرائم المعلوماتية ، تكون خاصة بالولايات المتحدة الأمريكية . حيث أشار المؤتمرون إلى وجوب رد فعل عالمي لمواجهة جرائم المعلومات ، لأنها هذه الجريمة لها صفة دولية ، ومرتكبي مثل هذه الجرائم استغلوا ضعف القوانين ، ونقص التعاون فيما بين الولايات الأمريكية .

عرفت الاتفاقية المقترحة جريمة الحاسب الآلي بأنها كل سلوك متصل بأنظمة التحكم و الاتصالات في الحاسب الآلي و التي تصنف على أنها جريمة معاقب عليها وفق هذه الاتفاقية ، وعرفت المعطيات (DATA) بأنها معلومات أو محتوى اتصالات تتضمن الخطب ، النصوص ، الأصوات ، التلفزيون . وقد حددت المادة الثالثة من الاتفاقية المقترحة ، الجرائم التي تشملها ، و التي تكون عن طريق التوصل غير المصرح به ، والتعديل ، وحذف البيانات بهدف الإضرار بالمؤسسة التي تملك الجهاز أو يعمل في خدمتها ، أو حذف البيانات و تغييرها لإعطاء معلومات كاذبة بهدف إيقاع أضرار مادية ، إضافة إلى الصور الشائعة من جرائم الحاسب الآلي و الانترنت . و نظمت المادة الرابعة أحكام التآمر و التحريض و المساعدة و المحاولة فيها ، أما المادة الخامسة فنظمت اختصاصات الولايات على الجرائم التي تقع في إقليمها وفقا لمبادئ القانون الدولي .

تضاف إلى هذه الجهود المؤتمرات التي عقدت عام 2000 لمواجهة الهجمات التي تتعرض لها العديد من المواقع الإلكترونية مثل (CNN) (YAHOO) ، وظهور فيروسات عديدة ألحقت أضرارا بالغة في شتى أنحاء العالم بأجهزة الحاسب الآلي و برامجه ، من بين هذه المؤتمرات مؤتمر جرائم الحاسب الآلي الدولي الذي عقد في " أسلو " شهر ماي عام 2000 ، بمشاركة العديد من الدول و الهيئات و المنظمات الدولية ، حيث بحث هذا المؤتمر أنواع جرائم المعلوماتية و التحديات الفنية و القانونية و التشغيلية التي تعيق مواجهة هذه الجرائم ، ودور القطاع الخاص و المستهلكين ، وضرورة نشر أخلاقيات المعلوماتية. وأكد المؤتمر على الجهود الدولية ، وخاصة جهود المجلس الأوربي التي تمثلت بمسودة الاتفاقية الخاصة بجرائم الحاسب الآلي ، التي خلقت أرضية جديدة في المنطقة باعتبارها اتفاقية جديدة لمواجهة جرائم الحاسب الآلي و الانترنت و اختراق الشبكات.

الخاتمة

بعدما توصل المجتمع الدولي و الهيئات الدولية و لأول مرة إلى بلورة مجموعة من الأفعال التي كانت تشكل اعتداءات ووصفها على أنها جريمة دولية ووضع لها آليات قانونية لمواجهتها تتمثل في إحداث اتفاقيات دولية و أجهزة قضائية كانت بمثابة تطويرا مهما لقواعد القانون الدولي.

حيث يتمثل هذا أساسا في إنشاء المحكمة الجنائية الدولية الموصوفة بالدائمة التي أقيمت من أجل إيقاف ووضع حد للاعتداءات التي كانت تمارس ضد أمن وسلامة البشرية و أوقعتها ضحية لفضائح خطيرة. و بعدما عرفناه من خلال دراستنا عن الجهود التي بذلت طيلة قرن من الزمن (من 1899-1998) من أجل الوصول إلى هذه النتيجة و أسباب ذلك، يكفي هذا لفهم خلفية الإجرام إذ أن وراءه دائما جهات تسعى بكل ما تملك إلى صد الناس عن الكلام عنه و هذا هو سبب انقضاء مدة القرن هاته.

و إذا لم تتمكن هذه الجهات من ذلك فإنها تلجأ إلى أساليب أخرى لتغذية الإجرام و ممارسته بأنفسهم أو بغيرهم و التمتع بنتائجه

ولعل هذا ما يفسر تجدد الإجرام، و ظهوره بصور مستحدثة.

حيث أن أساس اللجوء إلى استحداث أساليب جديدة لممارسة الإجرام، هو التخطيط للإفلات من العقاب، وفي هده الحالة يكو ن من التضليل لو تمسكنا بقبول أفعال اعتداءات أو انتهاكات معينة جديدة و السكوت عنها بحجة عدم احتواء النصوص و المواثيق القائمة إياها.

لان بهذا رأينا كيف طفح الإجرام الدولي في صورته التقنية تاركا وراءه الجهود الدولية التي تصدت للإجرام التقليدي دون جدوى و انه لا يمكننا بالبساطة الاستهانة بمخاطره إن لم تكن كما رأينا في بعض حالاته اخطر بكثير و اشمل و اعم و أوسع و اكبر نتيجة من الأول.

ثم أنه و إن لم نكن بصدد مقارنة مدة تأخر تجريم هذه الصورة الجديدة للإجرام مع مدة التأخر التي عرفتها الصور التقليدية، لا يمكن للأطراف الضعيفة أن يكون لها دور في هذا التأخر، بل من دون شك ليس غير الأطراف المهيمنة من يكون وراء ذلك. بل أقل ما يتسبب في ذلك هو وقوعها برضاها.

و إذا استقر رأينا من جهة، مدى ترشح بعض الاعتداءات الالكترونية أو الإجرام الالكتروني ليشكل جريمة دولية من حيث خطورتها مثل الإرهاب الالكتروني و التجسس الالكتروني و العنصرية الالكترونية.

و من جهة أخرى، من يكون مرتكبو هذه الاعتداءات و ليسوا غير الأطراف المهيمنة باعتبارها نفسها مالكة هذه التكنولوجيا، الوسيلة التي ترتكب بها هذه الأفعال، الشيء الذي يحصن كيانها و لا يجعلها تتحمس إلى تجريم هذه الاعتداءات أو التعاون من أجل ذلك في حالة ممارسة

غيرها لها، يمكننا القول بأننا نعيش نفس الوضعية لأنه و إ، كانت الجهود و المساعي التي بذلت إلى حد الآن في مجال التصدي للإجرام الدولي الإلكتروني هي في بدايتها بالمقارنة مع ما وصلت إليه مثيلتها في التصدي للإجرام الدولي بمفهومه التقليدي، إلا أنه تلوح في الأفق نفس الظاهرة. و هذا ما يتبين من ما آلت إليه هذه المساعي من وضع صعب يتمثل في عدم تماشي جميع الأطراف و خاصة المهيمنة مع هذه المساعي و بقاء هذه الأخيرة منحصرة و بصعوبة في تجريم أخف الاعتداءات الإلكترونية خطورة. و مثال ذلك ما يحدث من امتناع عن انضمام أو مصادقة أو تردد و تحفظ على ما أسفرت عنه بعض هذه الجهود مثل الاتفاقية الأوروبية الخاصة بالجرائم السيبيرنيتية - ترجمة عن Cybercriminalité باعتبار عدم وجود تسمية رسمية باللغة العربية لها- ربما يرجع ذلك إلى عدم قبول وقوع هذه الأطراف في حتمية تجريم تلك الأفعال في صورتها التقليدية التي طالما هي تتهرب من ذلك.

و مثال ذلك، جريمة الإرهاب التي رغم جسامتها، لم تجرم دوليا بعد في صورتها التقليدية، و أن قبول تجريمها في صورتها الإلكترونية يدعو إلى البدء بتجريمها تقليديا، الشيء الذي لم ترد أن تقع في بعض الدول المهيمنة مثل الولايات المتحدة الأمريكية بالرغم أنها تعد من ضحايا الإرهاب الالكتروني، و كونها الأثر مقدرة على مكافحته، لا يدفعها إلى السعي و التعاون على تجريمه دوليا حتى لا يجرها إلى قبول تجريم صورته التقليدية دوليا لأنها في هذه الحالة هي بطلته.

ثم أن الخصوصية التقنية للإجرام الإلكتروني عامة و للإجرام الدولي الإلكتروني خاصة، باعتباره عابر للحدود و إشراق على الإجرام المنظم و ما أسفر عن ذلك من صعوبات تعوق دون تجريمه دوليا، لا شك أنها تديم لمرتكبيه فرصة الإفلات من العقاب، مما يبطل فعالية القضاء الجنائي الدولي المتمثل أساسا في المحكمة الجنائية الدولية و يجعله من غير جدوى.

و بظهور بعض الجرائم و ما تحمله من طابع دولي و عبور للحدود مثل جرائم تبييض الأموال و الاتجار بالمخدرات و الإجرام الإلكتروني الذي زيادة على أنه أعطى تلك الجرائم دفعا ملموسا كما رأينا، استحدث جرائم أخرى لم تكن من قبل و صارت تهدد أكثر أمن و سلامة المجتمع الدولي و البشرية كلها، مما صعب على أية دولة التصدي له بمفردها من غير يكون بالتعاون الدولي سبيل إلى ذلك.

غير أنه، ليس من السهل أن يحصل التعاون الدولي في مجال مكافحة الإجرام الإلكتروني، نظرا لما يتطلبه في هذه الحالة و لما ينعكس سلبيا على سرية و خصوصية المجال الافتراضي للدول المتعاونة.

إذ أن أقل ما يعنيه التعاون هنا، هو قبول الأطراف المتعاونة للأطراف الضحية أو من يتأسس في حقهم، اقتفاء آثار الجريمة إذا ما تبن أنها ارتكبت ضدها في مجالها الافتراضي بالشيء الذي ألحق ضررا بمصالحها أو شكل اعتداء على شعبها و مس بأمنهما و سلامتهما اقتصاديا أو سياسيا أو عسكريا أو ثقافيا أو غير ذلك.

هذا يعني السماح للأطراف الضحية الدخول إن لزم الأمر إلى مواقع الدول الأخرى لإجراء المعاينة و التحقيق و جمع الأدلة و من ثم الشروع في إجراءات التسليم و المحاكمة و غيرها الشيء الذي زيادة على رفض الدول له مثل في حالة الجرائم الدولية التقليدية لما فيه من مساس بسيادة الدول، فإنه لا يمكن التأكد من حسن نية الدول الضحية أو من يتأسس في حقهم في عدم لجوئها إلى التسلل إلى مواقع ومعلومات أخرى من أجل التجسس عليها أو تعطيلها و إعاقتها و من ثم التسبب في ارتكاب جرائم أخرى و في هذه الحالة يكون رفضها لهذا التعاون أشد. و هذا ما يجعل الوسيلة الوحيدة لمكافحة الإجرام الدولي الإلكتروني، إلى حد ما، غير قابلة للتحقيق، و عليه يبقى مجرمو الإجرام الدولي الإلكتروني في إفلات من العقاب ما دام هذا الوضع قائما.

قائمة المراجع

01. عباس هاشم السعدي، مسؤولية الفرد الجنائية عن الجريمة الدولية، الطبعة الأولى ، دار المطبوعات الجامعية الإسكندرية، 2002.
02. سامي جاد عبد الرحمن واصل، إرهاب الدولة في إطار القانون الدولي العام، منشأة المعارف بالإسكندرية، 2003.

03. بن عامر التونسي، المسؤولية الدولية، منشورات دحلب، 1995.
04. محي الدين عوض، دراسات في القانون الدولي الجنائي،مجلة القانون و الاقتصاد، العدد الأول، 1965.
05. محمود صالح العادلي، الجريمة الدولية، دار الفكر الجامعي، 2004.
06. عبد الله سليمان، المقدمات الأساسية في القانون الجنائي الدولي، الطبعة الأولى، ديوان المطبوعات الجامعية، 1992.
07. نصر الدين بوسماحة، مسؤولية رؤساء الدول عن ارتكاب جرائم دولية، أطروحة دكتوراه، جامعة وهران 2007
08. علي يوسف الشكري، القانون الجنائي الدولي في عالم متغير، الطبعة الأولى، مصر، 2005.
09. William Bourdon - Immanuel Duverger, La Cour Pénal Internationale, Edition du Seuil, 2000
10. Annuaire français Dehaussy, de Droit international, 1992, p 747
11. نظام روما الأساسي للمحكمة الجنائية الدولية.
12. Cherif BASSIOUNI, introduction au droit pénal international, Bruylant, , .Bruxelles,2002, p 61
13. إبراهيم العيسيوي، التجارة الإلكترونية، المكتبة الأكاديمية،مصر، 2003.
14. منير محمد الجنبهي-ممدوح محمد الجنبهي، جرائم الإنترنت و الحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي الإسكندرية، 2005.
15. اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية
16. عبد الفتاح بيومى حجازي، الأحداث و الإنترنت دراسة متعمقة عن أثر الإنترنت في انحراف الأحداث، الإسكندرية، الطبعة الأثلى 2002.
17. ممدوح عبد الجميد عبد المطلب، جرائم الكمبيوتر و شبكة المعلومات العالمية.
18. محمد مؤنس محب الدين، تحديث أجهزة مكافحة الإرهاب و تطوير أساليبها، مجلة نايف العربية للعلوم الأمنية- الرياض، عدد 408، سنة 2006.
19. حسني الجنيدي، جرائم المساس بأمن الدولة و الإنترنت، أكادمية الشرطة، 15 ماي 2003.
20. محمد الملفي، قنابل موقوتة عبر الانترنت، http://www.alwatan.com.sa/daily/2005-07-10/local/local16.htm، 10 /2005/09، ص 02.
21. أحمد فلاح العموش، مستقبل الإرهاب في هذا القرن، ، مجلة نايف العربية للعلوم الأمنية- الرياض، عدد 395، سنة 2006.
22. Patrick CHAMBET, Le Cyber –terrorisme, http://www.chambet.com, 20/10/2005, p01.
23. سامي بن حامد الحربي، الإرهاب الإلكتروني، مجلة الأمن و الحياة، العدد 275، 2005.
24. عماد حسين عبد الله، التصدي للإرهاب بأبعاده المعاصرة، مجلة الأمن و الحياة، العدد 176، 2000
25. نبيل على، عنف المعلومات وارهابها، http://www.alarabimag.com/arabi/data/2002/9/1/، بدون ذكر الصفحة.
26. ريش- ن. لحياني، الحرب الالكترونية بين الماضي و الحاضر، مجلة الأمن و الحياة، عدد 744، سنة 2003.
27. محمود سليمان موسى، التجسس الدولي و الحماية الجنائية للدفاع الوطني و أمن الدولة، منشأة المعارف الإسكندرية،2001.
28. جمعان عبد الله البريكي، جرائم الكمبيوتر و التجسس الإلكتروني الدولي والشخصي للمعلومات.
29. التجسس الالكتروني واختراق الأنظمة الحكومية العربية ، http://www.kaadesign.com/vb/archive/index.php?t-421.html
30. آيشلون".. أضخم نظام رقمي دولي للجاسوسية بقيادة واشنطن ،http://www.sharesgate.com/vb/t5856.html 05/05/2006
31. صالح النعامي، ذراع التجسس الإلكتروني لإسرائيل، ،http://www.voltairenet.org/article146534.html 05/03/2007
32. عامر خليل، الاستخبارات العسكرية الإسرائيلية"أمان" النشأة والتطور وعلاقتها بالجيش الإسرائيلي،

.2007/05/30 ، id=922&http://www.alasra.ps/news.php?maa=View
33. إبراهيم السعيد، جهاز استخبارات إسرائيلي يتجسس إلكترونياً،
01/10/2004 ،http://www.alarabnews.com/alshaab/-2004/q8.htm
34. محمد عبد الله منشاوي، جرائم الإنترنت، http://www.minshawi.com/old/internet-crime.htm ، 2004 .
35. كلير شورت ، كل أسرار الأمم المتحدة في جيب "السي.آي.إيه، مجلة البيادر عدد 850 .
36. مكافحة عنصرية الإنترنت،
http://news.bbc.co.uk/hi/arabic/news/newsid_1518000/1518212.stm
37. eric mugneret-echelon, la nsa pose un lapin à l'europe . instruments juridiques pour lutter contre le racisme sur internet,
38. Kevin Boyle, les dimensions du racisme
www.ohchr.org/Documents/Publications/**Dimensions**Racismfr.pdf 20/06/2006.,
39. العهدين الدوليين الخاصين بحقوق الإنسان
40. الاتفاقية الدولية للقضاء على التمييز العنصري بجميع أشكاله لـ 1965
41. العنصرية على الإنترنت
http://news.bbc.co.uk/hi/arabic/news/newsid_646000/646702.stm
42. الإعلان العالمى لحقوق الإنسان
43. عادل عبد الصادق، مكافحة الإرهاب عبر الإنترنت.. التحديات والفرص ،
http://acpss.ahram.org.eg/ahram/2001/1/1/ANAL734.HTM
44. أحمد فاضل شبلول، الملكية الفكرية وحقوق المؤلف على شبكة الإنترنت،
.2007/02/08 ، http://www.alyaseer.net/vb/showthread.php?t=7818
45. عنصرية هولندية ضد المسلمين عبر http://www.almotamar.net/news/21152.htm الإنترنت
46. محمد عبد الله منشاوي، المخاطر الأمنية للأنترنت، www.minshawi.com 23 ماي 2006 ، بدون ترقيم الصفحات.
47. حسين السويدان، الإرهاب الدولي في ظل المتغيرات الدولية، الطبعة 1. العربية، الرياض 2004.
48. 13- عبد القادر الفنتوخ، الجريمة الإلكترونية، www.fantoukh.com ، 19 محرم 1425 هـ
49. رؤوف عبيد، مبادئ القسم العام من التشريع العقابى، الطبعة الثالثة 1966، دار الفكر العربي.
50. فايز بن عبد الله الشهري، التحديات الأمنية المصاحبة لوسائل الاتصال الجديدة، المجلة العربية للدراسات الأمنية و التدريب، المجلد 20 العدد 39 سنة 1319.

51. نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، الطبعة الأولى، 2005، ص 322.
52. مناصرة يوسف، الجريمة المعلوماتية، مذكرة تخرج، المعهد الوطني للقضاء، 2004.
53. عبد القادر القهوجي، القانون الدولي الجنائي أهم الجرائم الدولية و المحاكم الجنائية، الطبعة الأولى منشورات الحلبي الحقوقية بيروت، 2001.
54. أحمد بلقاسم ، القانون الدولي العام المفهوم و - رشاد السيد – القانون الدولي العام في ثوبه الجديد – دار النشر ، الأردن ، الطبعة الثانية 2005 .
55. تركى ضاهر – الإرهاب العالمي – دار الحسام ، لبنان ، الطبعة الأولى 1994 .
56. حسنين ابراهيم صالح عبيد – الجريمة الدولية دراسة تحليلية و تطبيقية.
58. قادري عبد العزيز – حقوق الإنسان في القانون الدولي و العلاقات الدولية، دار هومة، الجزائر، 2003.
59. حسنين المحمدي بوادي ، الإرهاب الدولي بين التجريم و المكافحة، دار الفكر الجامعي، الاسكندرية،

الطبعة الأولى، 2004.
60. Mohammed BOUZOUBAR la criminalité informatique sur internet; Journal of law, N° 7, Mars 2003
61. عبد الفتاح بيومي حجازي، الدليل الجنائي و التزوير في جرائم الكمبيوتر و الإنترنت، الطبعة الأولى، 2004.
62. غنام محمد غنام، عدم ملاءمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر و الإنترنت، بحث مقدم لمؤتمر – القانون و الكمبيوتر و الإنترنت، 2000، ص 09.
63. Mohammed BOUZOUBAR la criminalité informatique sur internet; Journal of law, N° 1, vol. 26, Mars ,2002, P¨77
64. موزة المزروعي، الاختراقات الإلكترونية خطر كيف نواجهه، مجلة آفاق الاقتصادية، عدد 9 سنة2000 ص 56 و ما بعدها.
65. التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، http://3dpolice.maktoobblog.com موقع ثقافي مهني و غير رسمي لرجال الأمن بالمملكة المغربية، بدون ذكر صاحب المقال.
66. محمد بن نصير محمد السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب و الإنترنت، مجلة العلوم الأمنية، أكاديمية نايف للعلوم الأمنية، الرياض، 1997.
67. حسن بن سعيد الغافري، الجهود الدولية في مواجهة جرائم الإنترنت، http://www.eastlaws.com/iglc/résearch/research-show.php?id 29 /08/2007، .
68. Sebastien BERNARD- Laititia CHEVALIER- Marc JULIE?- Mathias MOULIN- Judicael PHAN ,www.droitetinternet.com, p 04
69. Rapport préparé par l'Institut suisse de droit comparé (Lausanne), Strasbourg, Août 2000 , .115 Système Echelon et programme Carnivore ,
70. Philippe COUVE, Réseau Echelon: la justice Française ouvre une enquête ,http://www.fas.org/irp/program/process/echelon.html
71. ميثاق الأمم المتحدة
72. Marcel Merle, un système international sans territoire www.conflits.org/Numéros/20merle.html.
73. محمود أحمد عبابنة، جرائم الحاسوب و أبعادها الدولية، دار الثقافة للنشر و التوزيع عمان، 2004.
74. عبود السراج، مكافحة الجرائم الإقتصادية و الظواهر الإنحرافية، مجلة العلوم الأمنية، أكاديمية نايف للعلوم الأمنية، الرياض، 1998.
75. Direction des affaires criminelles et des grâces, Le traitement juridique de la cybercriminalité, guide méthodologique, république française, Mai 2002, p 34