موقف التشريع المقارن والمنظمات الدولية من جرائم الإعلام الألي والعمل على كيفية مكافحتها والوقاية منها

الدكتور:أسود ياسين *أستاذ محاضر أ*عين تموشنت
Toufik.khadidja82@gmail.com

ط.د:سي عبد القادر حنان *جامعة سوسة *تونس
asswadhanane@gmail.com

لقد بات من المحتم على شعوب العالم الانصهار التدريجي في بوتقة المعلوماتية كنتيجة حتمية لمواكبة التطور التقني والتكنولوجي في ظل التحول الإلكتروني لمختلف نواحي الحياة لتحقيق المجتمع الافتراضي ، في ظل عالم مفتوح تتسيده المعلومات ، والتي أضحت وبحق مصدر القوة والتسلط والمعرفة ، ولهذا وجب علينا أن نسلم بما صاحب الثورة المعلوماتية من تحطيم الحدود الجغرافية والسياسية بميلاد ونمو شبكة الأنترنت.

لذلك ينبغي على جميع الدول وضع إستراتجية تعمل على تحقيق التوازن مابين الاستخدام الحر والكامل للمعلوماتية من ناحية وبين حماية المواطن وحريته من ناحية أخرى وهو ما يمكن تصوره والتخطيط له بالتحضير التشريعي والقانوني في إطار دولة واحدة تتولى بنفسها عمل الأنترنت وما يترتب عنه من جرائم قد تمس الشخص وممتلكاته المادية والمعنوية والتي تعجز النصوص العقابية في مواجهة أغلب صورها المستحدثة فالقوانين الجنائية التقليدية الموضوعية منها والإجرائية باتت قاصرة عن مواجهة الجرائم المرتكبة عبر الأنترنت .

ومادامت هذه الجرائم موجودة وهي تغزو جميع أنحاء العالم فلا بدا أن تكملها إستراتيجيات مختلفة على المستوى التقني والفني والقضائي ولذلك لمراقبة الأمن في مجال تقنية المعلومات أو في مجال التدريب والتكوين التخصصي لمختلف الأجهزة الأمنية المعنية والمكلفة بالمراقبة ، أو حتى في مجال التعاون والتنسيق الدولي لمواجهة هذا النوع المعقد من الإجرام المستحدث والذي هو في تزايد مستمر متماشيا والتطور التكنولوجي.

المبحث الأول: موقف التشريع المقارن من جرائم الإعلام الألي

المطلب الأول : موقف بعض الدول من جرائم الإعلام الألي

تختلف القوانين من بلد إلى أخر وذالك حسب طبيعة كل بلد ، سواء من ناحية دينية أو نظامية أو حتى مدى تحضره وتطوره ، وهذا ما جعل التشريعات المقارنة تختلف إزاء هذه الظاهرة الإجرامية المستحدثة

، فمنها من تطرق وعالج الموضوع وهذا بتحديث وتعديل القوانين ومنها مازال قيد الدراسة والانتظار ومن هذا المنطلق نذكر مواقف بعض الدول.

أولا: موقف المشّرع المصري: كان لظهور الحاسبات الإلكترونية في مصر وغزوها مختلف مجالات أنشطة الحياة أخطارا تهدد الأفراد والمجتمع ككل ، خاصة بعد ظهور فكرة

البنك القومي للمعلومات وقد أضحت حقيقة واقعية بعد صدور قرار رئيس الجمهورية رقم 35 من سنة 1960 بخصوص البيانات التي تجمع بشأن التعداد والإحصاء القومي للأفراد من قبل أجهزة الدولة ، والذي عدل بقانون رقم 28 لسنة 1982 الذي أعتبر البيانات الفردية التي تتعلق بأي إحصاء أو تعداد يعد بسرية ، حيث لا يجوز الإطلاع من أي فرد أو هيئة عامة أو خاصة ، أو الإبلاغ أي شيء منها ، كما لا يجوز استخدامها لغير الأغراض الإحصائية أو نشر ما يتعلق منها بالأفراد إلا بمقتضى إذن مكتوب من ذوي الإختصاص حسب المادة الثالثة من القرار [1] وقد نصت المادة الرابعة من القرار على أن يعاقب بالحبس بمدة لا تقل عن شهر ولا تزيد عن ستة أشهر وغرامة مالية لا تقل عن 100 جنيه مصري ولا تتجاوز 500 جنيه أو إحدى هاتين العقوبتين [2]وهي:

1- كل من أخل بسر البيانات الإحصائية أو أفشى بيانا من البيانات الفردية أو سر من أسرار الصناعة أو التجارة أو غير ذلك من أساليب العمل التي يكون قد أطلع عليها بصفة عامة في الإحصاء والتعداد.
2- كل من حصل بطريق الغش أو التهديد أو الإيهام بأي وسيلة أخرى على البيانات أو معلومات سرية بشأن الإحصاءات أو التعدادات أو حتى الشروع في ذلك[3].

ثانيا:موقف المشّرع الفرنسي: لقد عالج القانون الفرنسي[4] موضوع الجريمة المعلوماتية أولا في مجال القانون الصادر بتاريخ 06جانفي 1978 ، حيث اقتصر على ضمان احترام الحياة الخاصة للإنسان في مجال المعلوماتية فقط ، وذلك على ألا تستخدم المعلومات المسجلة في الحاسب الألي لغير الأغراض التي سجلت من أجلها وعدم إفشائها إلى أشخاص آخرين غير المرسلة إليهم هذه المعلومات من خلال الحاسب الألي ولتحقيق هذا الغرض فقد ذكر هذا القانون ثلاثة أنواع من الجرائم وهي:
1- الانحراف بالمعلومات لغير الأغراض التي حددت عند وضعها في الحاسب الألي وذلك بالإطلاع غير القضاة على سوابق المتهم و الأطباء على معلومات الطبية عن المرضى أو استعمال هذه المعلومات للأغراض قضائية حسب المادة الرابعة من نص القانون .

---

[1] الأستاد طارق أحمد فتحي سرور- الحماية لأسرار الأفراد في مواجهة النشر- كلية الحقوق جامعة القاهرة – ص 196.
[2] د:زكي أمين حسونة – جرائم الكمبيوتر والجرائم الأخرى في مجال التقنين- القاهرة – 1993 ص 27.
[3] الأستاذ: محمد قنديل- هل توفر الدولة الكومبيوتر والأنترنت لكل أسرة- مقال بمجلة أدم اليوم – مصر العدد 45 الصادرة في 20أوت 2002.
[4] الأستاذ :طارق أحمد فتحي سرور- نفس المرجع السابق ص ص 204و205.

2- إفشاء المعلومات المودعة في الحاسب الألي بسبب إهمال حسب المادة43 الفقرة 2 وبعدها في حملة لمكافحة هذه الجرائم بادر المشّرع الفرنسي في مشروع تعديل قانون العقوبات الفرنسي لعام 1986 بصياغة نص المادة 307 الفقرة 3 والتي تنص على أنه إذا ارتكب شخص عمديا وبدون مراعاة حقوق الغير تدميرا أو إتلافا لكل أو لجزء من نظام المعالجة الآلية للبيانات أو تعطيل أو إفساد التشغيل ، فإنه يعاقب بالسجن لمدة خمس سنوات وغرامة مالية تقدر بمقدار 250.000 فرنك فرنسي.

3- إتلاف المال المعلوماتي المادي منه والمعنوي ، حيث نجد المشّرع الفرنسي أهتم كثيرا بهذا النوع من الإجرام وهذا من خلال نصوص القانون رقم 19 لعام 1988 والتي عالجت بعض الجرائم المعلوماتية وقد خصص لها بابا مستقلا في قانون العقوبات ، وقد احتلت جريمة الإتلاف العمدي للأموال المعلوماتية نصيب الأسد في هذا القانون ولقد أورد المشّرع الفرنسي في القانون السابق الذكر نصين مستقلين لمعالجة مشاكل إتلاف برامج وأدوات الحاسب الألي بالإضافة إلى نص مستقل يعالج جريمة التوصل بطرق التحايل لنظام المعالجة الآلية للبيانات وهذا التوصل يعتبر لصيق الصلة لجريمة الإتلاف العمدي للأموال المعلوماتية المادية منها والمعنوية.

فالمال المعلوماتي المادي يقصد به أجهزة وملحقات الحاسب الألي ، فتجد نصا جديدا يجرم المشّرع فيه إتلاف المال المعلوماتي المادي وينص على أن كل شخص يسبب عمدا أو بدون مراعاة حقوق الغير تعطيل أو إفساد تشغيل نظام المعالجة الألية للبيانات سيعاقب بالحبس لمدة تتراوح بين 03 أشهر وثلاثة سنوات وغرامة مالية تتراوح بين 10.000 و100.000 فرنك فرنسي أو إحدى هاتين العقوبتين وهو نص المادة 462 الفقر 3 ① .

أما المال المعلوماتي المعنوي يقصد به البرامج والبيانات ، فنجد أيضا أن المشّرع الفرنسي قد إستحدث نصا جديدا لذلك وهو نص المادة 462 الفقرة 4 ،وذلك لمنع الخلافات الفقهية التي لا تعتبر المال المعلوماتي المعنوي على قدم المساواة مع المال المعلوماتي المادي وصعوبة التطبيق الذي يصدم بمبدأ الشرعية حيث بين المشّرع في هذا النص صور الإتلاف والمتمثلة في :

* محو البيانات.
* إدخال البيانات في نظام المعالجة الألية .
* تعديل البيانات وطرق معالجتها أو وسائل انتقالها.

وعليه نجد أن المشّرع الفرنسي تفطن مبكرا لخطورة الظاهرة الإجرامية وقلم بتقديم عدة ضمانات للحد و مكافحة هذا النوع من الجرائم ②.

---

① د:زكي زكي أمين حسونة –- جرائم الكمبيوتر والجرائم الأخرى في مجال التقنين-ص 23.
② دكتورة : هدى حامد قشوش –-نفس المرجع السابق ص ص ص 3 و 10و11.

ثالثا: موقف المشّرع الأمريكي: في الولايات المتحدة الأمريكية نص القانون الصادر في سنة 1974 بشأن الخصوصية على بعض أنواع الجرائم المعلوماتية والتي تمس فقط الإعتداء على الحياة الخاصة للإنسان حيث كان الهدف الأساسي من هذا القانون هو تقرير الحماية لكل فرد ضد الإعتداء على حياته الخاصة ووضع قواعد لحماية الفرد من الإطلاع على المعلومات الخاصة به والمحفوظة في ذاكرة الحاسب الألي .

وبعدها اهتم المشّرع الأمريكي أكثر بالإجرام المعلوماتي ، حيث أصدر في 10أكتوبر 1984 قانونا مستقلا للمعلوماتية حلل فيه كل ما يتعلق بالإجرام المعلوماتي والذي أعتبر

كمرجع للمشرع الفرنسي عند صياغته للقانون لرقم 19 من سنة 1988 علما أن القانون الأمريكي يجد صعوبة في تطبيق المعايير القانونية على بنوك المعلومات ،خاصة المعلومات الشخصية ، حيث أنه لم يحدد بصورة ثابتة المعلومات الشخصية أو المعلومات الأخرى وكانت قد خرجت دعارة الأطفال على الأنترنت في الولايات المتحدة 1995 والتي بذل في شأنها جهد من طرف الكونغرس الأمريكي لتنظيم أوجه الإباحية عبر الأنترنت في عام 1996 بإصدار قانون آداب الإتصالات والذي جرم نقل المواد الفاحشة للأطفال في أي مكان على الأنترنت حيث كانت قد أصدرت المحكمة العليا بنيويورك في 1982 قرارا تستطيع به حضر تصوير أو رسم القاصرين الممارسين للسلوك الجنسي[①].

رابعا: موقف المشّرع الإنجليزي: عنى المشّرع الإنجليزي في التصدي للمواد الإباحية باختلاف أنواعها ، منذ أصدره لقانون الفحش لعام 1959و1964 وقد عمل المشّرع الإنجليزي على سد أوجه القصور في هذين القانونين بإصدار قانون حماية الأطفال لعام 1978 والذي يسمى ب: CHILD (CPA) PROTECTION ACT حيث فرض المشّرع حماية أوسع للأطفال بتوسيع صور الحماية ضد الاستغلال الجنسي لهم تحت قانون العدالة الجنائية لعام 1988 وقد عدلت هذه التشريعات حديثا بموجب قانون العدالة الجنائية والنظام العام لعام 1994 (CJPOA) CRIMINAL JUSTICE AND PUBLIC .ORDER والذي سد الثغرات التشريعية السابقة لصدوره [②] ولذالك يعد القضاء الإنجليزي من أفضل التشريعات في فرض الحماية للأطفال ولاسيما في مواجهة الاستغلال الجنسي لهم عبر شبكة الأنترنت[③].

خامسا: موقف المشّرع الأردني:قد نص المشّرع الأردني فيما يخص جرائم الإعلام الألي وأعطى الأهمية لمختلف الجرائم ضمن قانون الإتصالات رقم 13 من سنة 1995 وقد نصت المادة 76 منه على أن كل من أعترض أو أعاق أو حول أو شطب رسالة بواسطة شبكات الإتصالات أو شجع غيره على القيام بهذا

---

①martin forst – low – appellet court casesabout information technology by montilair-entreprise san francissco 1996 p 160

②HTTP:// WWW.EPIC.ORG/FREE-SPEECH/CONSORCHIP/COPA.HTML-

③LILIAN EDWARD ET CHARLOTTE WAELDE.OP.CIT. P-122.

العمل ، يعاقب بالحبس بمدة لا تزيد عن ستة أشهر أو بغرامة مالية لا تزيد عن 200 دينار أو بكلتا العقوبتين كما أنة قد تطرق قانون العقوبات الأردني إلى معالجة الاحتيال المعلوماتي بصورة مباشرة إلى أن جاء قانون المعاملات الإلكترونية رقم 85 من سنة 2001 حيث جرمت نصوص مواده أي إستخدام للمعلوماتية بغرض القيام بأفعال احتيالية كما نصت مختلف باقي المواد على جرائم الإعلام الألي التي سبق ذكرها④ .

سادسا:موقف المشّرع الكندي: إن التشريع الكندي في مجال الحقوق والحريات يشبه القانون الأمريكي غير أن إعلان الحقوق غير عازل للحق في الخصوصية وبالتحديد بشكل

غير مباشر في الاحتياطات مثل حمايتها من البحث غير المرخص والاستيلاء على البيانات الشخصية، حيث يعد تشريع كيوبك Quebec عام 1994 تشريعا شاملا للخصوصية.

سابعا: موقف المشّرع الصيني: أصدرت الصين مرسوما في فبراير 1996 بشأن تنظيم إستخدام الأنترنت ، حيث فرضت على كل مستخدم لبرامج بث المعلومات عبر الشبكة أن يحصل على موافقة مسبقة من قبل وزارة البريد والمواصلات وأنه يخطر عليه بث أي معلومة يكون من شأنها المساس بالنظام العام ، وكذلك هو الحال لكل من دولة النمسا بلجيكا ، ألمانيا ، السويد ، النرويج و الدانمارك حيث أصدرت عدة تشريعات فيما يخص إستخدام مجال الأنترنت ومختلف الجرائم المقترفة به①.

ثامنا: موقف المشّرع التونسي: أقر المشّرع التونسي حماية خاصة للمعطيات الشخصية في مواجهة التطور التقني في المواد من 38 إلى غاية 42 من قانون التجارة الإلكترونية لعام 2000 وفرض عقوبات أصلية وعقوبات تكميلية على الأفعال التي تقع بالمخالفة لتلك المواد فنجد أن المادة 38 من القانون تنص على أنه لا يمكن لمزود خدمات المصادقة الإلكترونية معالجة المعطيات الشخصية ، إلا بعد موافقة صاحب شهادة المعني ويمكن اعتماد الإعلام الإلكتروني بالموافقة إذا ضمن المزود مايلي:

- إعلام صاحب الشهادة لحقه في سحب الموافقة في كل وقت.
- إمكانية تحديد هوية الأطراف المستعملة للمعطيات الشخصية.
- الاحتفاظ بحجة الموافقة التي يمكن تغيرها.

المطلب الثاني:موقف بعض المنظمات الدولية والإقليمية من جرائم الإعلام الألي

لم تكن الأخطار الناشئة عن الجرائم المعلوماتية موضوع اهتمام الدول فحسب ، بل كانت محل اهتمام المنظمات الدولية العالمية والإقليمية ، كما شغلت هذه الأخطار رجال القانون وأثارت مخاوفهم لما تنطوي

④د:نائل عبد الرحمان- واقع جرائم الحاسوب في التشريع الجزائي الأردني- الإمارات العربية المتحدة- 2000-ص 7.
①د: محمد سعيد رشدي-الأنترنت والجوانب القانونية لنظم المعلومات – ص ص51 و 52.

عليه من تهديدات خطيرة وهذا ما دفعهم إلى البحث في هذا الموضوع في مختلف المؤتمرات الدولية منها أو الإقليمية.

أولا: موقف الأمم المتحدة: أوصى المؤتمر الأول لحقوق الإنسان المنعقد بطهران في سنة 1968 والخاص بدراسة أثر التقّدم التكنولوجي على حقوق الإنسان على ضرورة احترام الحياة الخاصة في مواجهة هذا التقّدم وحماية حقوق الأفراد وحريتهم من خطر التعدي عليها ، وتبنت الجمعية العامة للأمم المتحدة في اجتماعها المنعقد في 19 ديسمبر 1968 توصيات مؤتمر طهران الخاصة باستخدام الإلكترونيات وأثرها على حقوق الإنسان ، ودعا السكرتير العام للأمم المتحدة إلى دراسة المشاكل التي يخلفها التقّدم التكنولوجي وبصفة خاصة فيما يتعلق باستخدام الإلكترونيات الذي يؤثر على حقوق الأفراد②.

كما ذكر السكرتير العام في تقريره أن الحاسبات الألية تمثل أكبر تهديدا للحياة الخاصة والحرية الشخصية ، إذ أنها تعد من أدوات المراقبة وأجهزة التطفل الحديثة خاصة إذا تم تخزين هذه البيانات في ذاكرة الحاسب الإلكتروني وتحليلها مما يكشف عن أنماط التعامل والعلاقات بين الأفراد ، حيث أنه في سنة 1975 قدم السكرتير العام للأمم المتحدة ① تقريرا أخر في هذا الشأن إلى لجنة حقوق الإنسان يوضح فيه الحالة التي وصل إليها ذات التقدم في مجال العلوم والتكنولوجيا وخطره على انتهاك حرمة الحياة الخاصة للإنسان ' هذا بالإضافة إلى العهد الدولي الخاص بالحقوق المدنية والسياسية للأفراد والذي وضعته في سنة 1966.

ثانيا: موقف منظمة اليونسكو: كانت أخطار الحاسبات الألية محور النقاش في اجتماع اليونسكو ② الذي أنعقد في باريس سنة 1970 في الفترة الممتدة من 19 إلى 23 جانفي وأتفق الرأي على أن إستخدام الحاسبات الألية يهدد الحياة الخاصة إذا ما أسئ استخدامها لما لها من قدرة فائقة على تخزين أكبر قدر من البيانات واسترجاعها في أقصر وقت ممكن ، ويفرض ضرورة وجود وسائل للرقابة على التخزين هذه البيانات وإقرار حق الأفراد في الوصول والإطلاع عليها وتصحيحها كلما أدعى الأمر إلى ذلك ③ ونظرا لإتهمام اليونسكو بهذا الموضوع تم مناقشته في بروكسل عندما عقدت الندوة الثالثة في نفس السنة 1970 حيث نقشت عدة تقارير عن الحياة الخاصة المعرضة للخطر بواسطة الحاسب الألي والمعلوماتية إضافة إلى إعداد وسائل رقابة على تخزين المعلومات④.

---

②د:زكي زكي أمين حسونة – مرجع سابق ص ص 29و30.
①الأستاذ :طارق فتحي سرور – مرجع سابق – ص 197.
②د:مبدر ألياس – أثر التطور التكنولوجي على الحريات العامة – مؤسسة المعارف – القاهرة – ص 154.
③د:زكي زكي أمين حسونة- مرجع سابق - ص 30.
④د: مبدر ألياس- مرجع سابق - ص 145.

ثالثا: موقف الإتحاد الأوروبي: كان للإتحاد الأوروبي دورا لا ينكر في مواجهة هذه ظاهرة الإجرام المعلوماتي وذلك من خلال التوصيات والاتفاقيات التي عقدت تحت مضلته والتي سنتطرق إلى البعض منها حسب تسلسلها الزمني.

- توصية البرلمان الأوروبي التي وضعها في 08ماي 1979 والمتعلقة بالحياة الخاصة والبيانات ذات الصبغة الشخصية من إساءة استخدامها بواسطة المعالجة الإلكترونية.
- أقر المجلس الأوروبي في 23 سبتمبر 1979 التوصية الخاصة بحماية التدفق ونقل المعلومات ذات الصبغة الشخصية بين الدول الأعضاء.
- في 28 جانفي1981 وافق المجلس الأوروبي على عقد اتفاقية لحماية الأشخاص في مواجهة الاستخدامات الآلية للمعلومات ذات الصبغة الشخصية وكان من الدول الموقعة الدانمارك ، النمسا، فرنسا ألمانيا، لوكسمبورغ،سويسرا وتركيا وبعد أنظم إليها كل من النرويج ،المملكة المتحدة والبرتغال وعدد أخر من الدول الأوروبية ومن مبادئ هذه الاتفاقية هو أنه يجب الحصول على المعلومات الشخصية من خلال وسائل مشروعة ولا يجوز استخدامها إلا لأغراض مشروعة والتزام كل دولة عضو

بأن لا تسمح بتدفق المعلومات التي تمس الحياة الخاصة للأفراد بين حدود الدول الأعضاء في الاتفاقية[1] .

- بتاريخ 23 نوفمبر 2001 في مدينة بودابست BUDAPEST عاصمة المجر أبرمت 26 دولة من أعضاء الإتحاد الأوروبي إضافة إلى كندا ، اليابان ، جنوب إفريقيا والولايات المتحدة الأمريكية أول معاهدة دولية بشأن الأفعال الإجرامية المعلوماتية وسميت المعاهدة الدولية لمقاومة جرائم المعلوماتية والاتصالات وأصبحت هذه المعاهدة التي كانت أوروبية النشأة ، فهي في الحقيقة دولية النزعة ومفتوحة للدول الأخرى التي تود الإنظمام إليها ، وهي تهدف إلى حماية الأفراد فيما يتعلق بالمعالجة الألية للبيانات الشخصية وقررت المعاهدة عدة توصيات أهمها[2]:

*التوصية رقم 87/15التي تنظم إستخدام البيانات الشخصية في المجال الشرطي.
*التوصية رقم 88/02 بشان القرصنة في مجال حقوق المؤلف والحقوق المجاورة.
*التوصية رقم 89/09 في مجال الجرائم المتصلة بالحاسب الألي والتي توفر توجيهات للمجالس التشريعية الوطنية بشأن تعريف جرائم الحاسب.
*التوصية رقم 90/04 بشأن حماية البيانات الشخصية في مجال خدمات الإتصال.
*التوصية رقم 95/13 المتعلقة بالمشاكل الإجرائية والجنائية المتصلة بتكنولوجيا المعلومات.

[1] أستاذ:طارق أحمد فتحي سرور- مرجع سابق - ص 206.
[2] د:عمرو زكي عبد المتعال- الأنترنت والقانون- مقال منشور على موقع الأنترنت www.islamonline.net

- في شهر جوان من سنة 2000 أنعقد اجتماع لوزراء العدل الأوروبيين للتشاور والتمكين أكبر عدد من الدول لتصبح أطرافا في هذه المعاهدة نظرا للحاجة إلى نظام سريع وفعال في التعامل الدولي لمحاربة الجريمة المعلوماتية .

وتتضمن هذه المعاهدة 48 مادة موزعة على أربعة فصول حيث يتناول الفصل الأول منها التعريفات الخاصة لبعض المصطلحات الفنية التي تتناولها المعاهدة ، أما الفصل الثاني به ترتيبات لابدا من اتخاذها على المستوى المحلي بالإضافة إلى النصوص الجنائية الموضوعة بشأن الجرائم ضد الخصوصية في سلامة وتواجد معلومات الحاسب و إلى أنواع متعددة من الجرائم أما الفصل الثالث فيتطرق إلى مسائل التعاون الدولي وتسليم الجناة أما الفصل الرابع تم التطرق فيه إلى التعاون الدولي بالنسبة للإجراءات الوقتية والتحفظية وكذا التعاون فيما يتعلق بجمع بيانات المرور والحركة الخاصة بالبيانات .

رابعا: جامعة الدول العربية: لقد عقد المؤتمر التاسع عشر للقادة الشرطة وأمن العرب بمدينة تونس خلال الفترة من 16 إلى 18 أكتوبر 1995 وقد ناقش عدة مواضيع شكلت جدول الأعمال هذا المؤتمر وكان من بينها:

* تعزيز سبل ووسائل الإتصال المباشر بين أجهزة الأمن والشرطة العربية .
* دعوة الدول الأعضاء التي تمتلك تقنيات المعلومات المتطورة إلى مساعدة باقية الدول التي تفتقر إلى مثل هذه التقنيات.
* مشروع إستراتجية إعلامية عربية للتوعية الأمنية والوقاية من الجريمة المعلوماتية.
* إستخدمات الحاسب الألي في المجال الأمني في البلدان العربية.
* التطرق إلى جرائم الحاسب الألي ، أشكالها وأساليب مواجهتها .
* أساليب العلمية في إدارة الأزمات العلمية .
* ضرورة إنشاء مركز خاص بنظم المعلومات والحاسب للدول الأعضاء.
* اقتراح على الدول الأعضاء تضمين تشريعاتها الوطنية ما يلزم من نصوص ومواد تساعد على الحد من جرائم الحاسب الألي [1].

المطلب الثالث: موقف التشريع الجزائري من جرائم الإعلام الألي

[1] مجلة الشرطة- العدد 63 الصادرة في شهر أكتوبر 1996 – ص 13.

إن التشريع الجزائري يعاني فراغا تشريعي في مجال المعلوماتية وجرائم الإعلام الألي بصفة عامة والتي عرفت انتشارا خلال السنوات الأخيرة ومست جميع المجالات وبعض المواقع الرسمية ، ناهيك عن جرائم القرصنة والنسخ الغير المشروع للبرامج وغيرها حيث أصبح من الضروري إحداث تعديلات وخلق نصوص جديدة للحد من هذه الظاهرة الإجرامية بجميع أنواعها وعدم ترك الباب مفتوح أمام مرتكبي هذه الأفعال بدون عقاب والذين أصبحت لهم صلة وطيدة بقراصنة العالم في مجال تبادل تقنيات الإجرام ، وخاصة ونحن على بوابة الألفية الثالثة والتي تعرف في مضمونها تطورا تكنولوجيا في جميع المجالات ، خاصة الإتصالات منها.

وتماشيا مع الوضع والإحساس به قام المشّرع الجزائري بإصدار الأمر رقم 97 – 10 المؤرخ في 06 مارس 1997 المتعلق بحقوق المؤلف والحقوق المجاورة حيث تتضمن على مصنفات وقواعد البيانات الخاصة بالحاسوب في مادته السادسة 06 الفقرة أ كما أعطت المادة 27 من نفس الأمر الحق للمؤلف دون سواه أو لمن سيسمح له أن يقوم باستنساخ المصنف بأية وسيلة وجعله في متناول الجمهور وكذا تأجير الاحترافي لبرامج الحاسب الألي والبيانات ، وكل هذا باستثناء استنساخ المصنف بهدف الاستعمال الشخصي الذي لا يشكل فعلا معاقب عليه .

أما المادة 149 من نفس الأمر نصت على جنحة التزوير والتقليد التي تتجسد في القيام بإستنساخ المصنف بأي أسلوب من الأساليب في شكل نسخة مقلدة ومزورة ، ويعاقب المرتكب لهذه الجريمة بالحبس من ستة أشهر إلى ثلاثة سنوات ، وغرامة مالية تقدر ب: 500.000 د ج إلى مليون د ج سواء تمت عملية النشر في الجزائر أو غيرها [1] .

إلا أنه في سنة 2004 تم تعديل قانون الإجراءات الجزائية وقانون العقوبات حيث صدر بالجريدة الرسمية الخاصة به وهذا بتاريخ10 نوفمبر 2004 حيث نص القسم السابع مكرر على المساس بأنظمة المعالجة الألية للمعطيات في مادته 394 مكرر إلى غاية 7 مكرر من نفس المادة [2] .

المبحث الثاني: الوقاية من جرائم الإعلام الألي

[1] الأمر رقم 97 – 10 المؤرخ في 06 مارس 1997 – م 27 و149.
[2] الجريدة الرسمية الصادرة بتاريخ 10نوفمبر 2004.

المطلب الأول: تقدير التهديدات والأخطار الناجمة عن جرائم الإعلام الألي

إذا كان الجدول والنقاش القائم على تقنين جرائم الإعلام الألي عبر العالم فهناك ثمة تهديدات هي الأخرى قائمة ، قد تنجر عنها عدة أخطار من مدى إمكانية تطابق النصوص والقوانين الجنائية التقليدية على الجرائم التي تستهدف الإعتداء على المعطيات الحاسوب أو المعلومات ، فإن هذا الجدل الذي سنبينه تفصيلا لدى تحليلنا لأنماط جرائم الحاسوب الذي أمتد إلى القضاء وحتى جهات التشريع ، لم يكن بمقدوره إضعاف القناعة السائدة لدى العموم بشأن الطبيعة الخاصة لموضوع جرائم الحاسوب بالطبيعة المعنوية للمعلومات والمعطيات التي لم تكن فيما سبق محلا للحماية الجنائية③.

حيث أن الهدف من هذه التهديدات هو توجيه التوصيات تخص وقاية هذه التكنولوجيات من الأخطار الناجمة عنها بهدف تمكين مركز المسؤولية من اتخاذ إجراءات وقائية مناسبة تدخل في جميع مجالات التعامل الإلكتروني ، هذه العملية ستسمح بتقدير مدى حماية المعلومات ويكون ذلك من طرف لجنة مؤهلة لها دراية بالأخطار والتهديدات الناجمة وتعمل على تحضير العمل حول الأنظمة المعلوماتية الواجب وقايتها وتقدير التهديد القائم على الشبكة العالمية والمحلية ، وما سيترتب عنها من أخطار لتمكنهم من تحديدها والوقاية منها وإعطاء توصيات ونصائح تحدد كيفيات تفادي الخطر وإستباعده نهائيا من أجل حماية وسلامة المعلومات .

وبمأن المشكلة أصبحت عالمية ، بحيث أن جرائم الكمبيوتر ترتكب عن طريق الحاسب الألي في دولة ما في حين يتحقق الفعل الإجرامي في دولة أخرى ، إذن فهي لا يحدها حدود ، فلذا يتطلب إجراءات التعاون الوطني والدولي لتصدي لهذه الظاهرة وهذا

بالعمل على الوعي الوطني لظاهرة الإجرام المعلوماتي وما يترتب عنه من عقوبات ومن هذا المنطلق فإن التكنولوجيات بصفة عامة وشبكة الأنترنت بصفة خاصة ، أصبحت وسيلة جديدة التي ينجم عنها الإجرام المعلوماتي وجرت المجتمع أمام تحدي جديد لبدا من التكيف معه ، ولذا فإن مختلف المؤسسات القائمة يجب عليها حماية أنظمتها المعلوماتية الخاصة بهدف ضمان بقائها ونجاحها في عملها وبالمقابل هذا لا يمنع القوات الأمنية المعنية بالعمل على تطوير أجهزتها الخاصة في إطار مكافحة الجرائم المعلوماتية.

المطلب الثاني : إستراتيجية الجزائر في الوقاية من جرائم الإعلام الألي

③د:عبد العظيم وزير – جرائم الإعتداء على الأموال – الطبعة الأولى – دار النهضة العربية – القاهرة – 1993- ص 42.

إذا كانت مجتمعاتنا العربية لم تتأثر بعد بشكل ملموس بمخاطر الجرائم المستحدثة فإن جرائم الكمبيوتر والانترنت المحتملة في البيئة العربية يمكن أن تكون كبيرة وقد تكون الجزائر من ضمن الدول العربية التي ترى في جاهزيتها التقنية والتشريعية والأدائية إستراتيجية لمواجهة حماية المعلومات فهي حاليا ليست في المستوى المطلوب ، إن لم تكن غائبة تماما ، وبالمقابل فقد أمست جرائم الإعلام الألي والانترنت من أخطر الجرائم التي تقترف في الدول المتقدمة وتحديدا الأمريكية والأوروبية منها ، ولهذا ازدادت خطط مكافحة هذه الجرائم وانصبت الجهود على دراستها المتعمقة بهدف خلق آليات قانونية للحماية من أخطارها والمتمثلة في ثلاث قطاعات مستقلة وهي:

- حماية إستخدام الكمبيوتر أو مايعرف بجرائم الكمبيوتر ذات المحتوى الاقتصادي.
- حماية البيانات المتصلة بالحياة الخاصة (الخصوصية المعلوماتية).
- حماية حق المؤلف على البرامج وقواعد لبيانات الملكية الفكرية والمصنفات الرقمية.

ويكون ذلك من أبرز المشاكل التي تواجه سياسات مكافحة جرائم الحاسوب و المعلوماتية لا على الصعيد الدولي بل حتى في نطاق التشريعات الوطنية ، مما يجعل الجزائر تعمل جادة لمواكبة العصر للتصدي لهذه الظاهرة ، وخاصة أن مستعملي الأنترنت في تزايد مستمر وهذا بإستعمال الشبكات العالمية والمحلية لبعض المؤسسات الوطنية.

ففي هذا الصدد تم تعديل قانون العقوبات والإجراءات الجزائية لبعض المواد وتم إصدارها بالجريدة الرسمية الصادرة بتاريخ 10 نوفمبر 2004 والتي تتضمن المساس بأنظمة المعالجة الألية للمعطيات حيث تناولتها كل من المواد التالية 394 مكرر 1 ومكرر 2 إلى غاية مكرر 7 من نفس المادة والتي أظهر فيها المشّرع الجزائري بعض العقوبات لكل فعل على حدى ، وهذا في انتظار صدور مشروع القانون الجديد والذي سيتطرق إلى معظم جرائم الإعلام الألي التي تقترن عبر مختلف الشبكات المحلية منها والعالمية ، هذا المشروع المقترح سيتم مناقشته وتقديمه أما البرلمان بغرفتيه [1].

وأمام هذا الوضع فأن إستراتيجية الدولة الجزائرية هادفة إلى حماية كل مؤسستها من الخطر الداهم وهذا بالتطلع إلى إستراتيجية وقائية من التهديدات القائمة في مجال الجريمة المعلوماتية وهذا بالتنسيق الدولي بغية جلب الخبرات والتكنولوجيات الحديثة لمواكبة العصرنة والتحضير للدخول إلى التجارة العالمية وهذا لا يتأتى إلا بالتكوين المتواصل والعمل الدؤوب و التطلع حول ما يجري في العالم الخارجي ومختلف التحولات القائمة.

[1] الجريدة الرسمية الصادرة بتاريخ 10نوفمبر2004- مرجع سابق.

وعليه يتطلب من المؤسسات الأمنية بصفة عامة مواكبة العصر والإحساس بالخطر القائم والتهديدات المتوالية من هنا وهناك في مجال المعلوماتية وشبكات الأنترنت والتصدي له حيث تعد مؤسسة الدرك الوطني السباقة في هذا المجال وهذا بإخطار الهيئات العليا بخطورة الوضع القائم وما يترتب عنه من خسائر ، وهذا مما يدفع بمؤسسة الدرك الوطني إلى تكوين إطاراتها في مختلف التخصصات لا سيما الجرائم المستحدثة والتي تقترف عبر الشبكة في الداخل والخارج فهذا التكوين والتحضير تم ولا يزال في بعض الدول الأجنبية المتطورة والتي تعرف شتى أنواع الإجرام المستحدث هذا ناهيك عن إنشاء معهد الوطني لأدلة الجنائية وعلم الإجرام لمؤسسة الدرك الوطني يعمل في هذا الاتجاه.

إضافة إلى ذلك فالجزائر تشارك في مختلف اللقاءات والمؤتمرات التي تصب في هذا الاتجاه وإبرام اتفاقيات في مجال البحث العلمي والتكنولوجي وهي تطمح أن تبدأ عصر الحكومة الإلكترونية حيث في هذا الشأن أعلنت شركة سيسكو سيستمز ووزارة البريد وتكنولوجيات الإعلام أن مبادرة الحكومة الإلكترونية في الجزائر قد تم تطبيقها والانتهاء منها وسيمكن هذا المشروع الوزارات الجزائرية من تقديم خدامات عامة ذات مستوى محسن عبر شبكة برتوكول انترنت متقاربة ، توفر خدمات مركزية للصوت ، فيديو البيانات IP TELEPHONY البريد الإلكتروني والاجتماع .

وفي هذا المجال قال نائب رئيس شركة سيسكوسيستمز CISCO SYSTEMESE مارك دي سيموني في الشرق الأوسط وإفريقيا أن مبادرة الحكومة الإلكترونية الجزائرية هي خطوة مهمة اتجاه تحسين الفاعلية وقدرات الخدمة لكل الوزارات مشيرا إلى أن الشركة أشركت شريكة قنوات سيسكو سيستمز الفرنسية FRANCE PARTNER CISCO ALBUM CFAO CHANNEL على عملية تطبيق الحلول غي الوزارة التي ستصبح محورا يصل بين مختلف مشاريع الحكومة الإلكترونية عبر الوزارات المختلفة[1].

المطلب الثالث : الوقاية بالوسائل التقنية لجرائم الإعلام الألي.

تستعمل مختلف المؤسسات والشركات الكبرى في العالم أحدث التقنيات للتصدي لظاهرة الإجرام المعلوماتي ، وهي تعمل جادة على تطوير أحدث البرمجيات لتأمين التعامل الإلكتروني بشتى أنواعه ومن أهم تقنيات الوقاية الأكثر استعمالا في العالم هناك

الجدران النارية FIREWALL ، والشيفرة ENCRYPTION وكذا استعمال كلمة المرور PASSWORD حيث سنتطرق إلى كل منهم على حدى.

[1] جريدة السفير – العدد 247 الصادر بتاريخ 25 فيفري 2005 – ص 14.

أولا: الجدران النارية :FIREWALL هي إحدى وسائل الأمن المعلوماتي ، وهي عبارة عن برنامج يستعمل كبوابة للتحكم بنقاط الدخول مابين الشبكة والمستخدمين ، وأعتمدت للحماية بهذا النوع من البرامج إستراتيجيات متباينة ، كإستراتيجية السماح للكافة بالدخول إلى الموقع مع منع من لا تريد الشبكة إدخالهم ، أو إستراتيجية منع الكافة من الدخول والسماح فقط لمن تريد الشبكة إدخالهم ، وقد تطورت وسائل الجدران النارية وإستراتيجيتها بشكل مذهل وحاليا تستعمل مختلف المؤسسات الجدران النارية لتأمين أنظمتها المعلوماتية خاصة منها البنوك والمؤسسات الأمنية ، لكن هذا لا يقف حاجزا أمام القراصنة الذين بدورهم يسعون إلى ضعف هذا النوع من البرامج وإظهار نقاط ضعفها.

ثانيا: التشفير: ENCRYPTION يمكن تعريف التشفير بأنه وسيلة لإستبدال رسالة أو أي مستند بالترميز بحيث لايمكن معرفة محتوياتها ، وهي عملية تحويل النص المبسط أو المستند الواضح إلى رموز ، وترميز المحتويات هو نظام إظهار البيانات بواسطة سلسلة محددة سابقا من الحروف ،الأرقام ، الرموز ، الكلمات والإشارات والهدف من ذلك هو منع فهم واستخدام البيانات من قبل الأشخاص الذين لا يملكون وسائل فك الترميز ، حيث أن الأشخاص المزودين فقط بوسائل تشفير الملف يمكنهم الإطلاع عليه باستخدام برامج لها القدرة على تحويل وترجمة تلك المعلومات إلى رموز .

- التشفير المتناظر أي SYMMETRIC ALGORITHEMS : ويتم هذا الأخير باستخدام الرقم العام مع إجراء فك الشفرة DECRYPTION وترجمة المعلومات إلى وضعها الأصلي في نفس الوقت باستخدام نفس الرقم العام .
- التشفير الغير متناظر ASYMMETRIC ALGORITHEMS : هو تشفير المعلومات بإستخدام الرقم العام مع عدم القدرة على فك الشيفرة والوصول إليها يكون إلا بالمفتاح الخاص لصاحب ذلك المفتاح العام الذي تمت على أساسه عملية التشفير .

وتعتمد قوة التشفير على عدد الخانات المكونة لكل رقم وتقاس بالبت BIT ، فإذا كان الرقم المكون من أربعين 40 خانة فإن القوة ستكون أربعين 40 بث وإذا كان الرقم عبارة عن ستة وخمسون 56 خانة فإنه تكون قوة التشفير ستة وخمسين 56 بث ، لذا فعملية التبادل والتسوق تتم بأمان بشرط التأكد من قوة التشفير المستخدمة [1].

ثالثا: كلمة المرور: PASSWORD تعتبر كلمات المرور مفاتيح هامة لأي شخص يمتلكها لأن بواسطتها نستطيع تأمين جميع الخدمات على الشبكة وغيرها وهي تساعد في

[1] المهندس حسام شوقي – حماية وأمن المعلومات على الأنترنت –دار الكتب العلمية للنشر والتوزيع- القاهرة -2003 ص 61و63.

عملها على تأمين كل الحسابات التي تدخل ضمن المعاملات التجارية التي تستعمل فيها مختلف البطاقات الأكثر استعمالا حيث تكون هذه الكلمات صعبة الحفظ والتكهن ، لذا يجب تفادي عند استعمالها تواريخ هامة مثل تواريخ الميلاد ، أرقام الهواتف ، ألقاب الأبناء والأقارب والمناسبات الهامة ، إلا أن هذا الخيار أحينا أصبح غير فعال ومجدي أمام الاختراقات التي يقومون بها القراصنة.

المطلب الرابع : أسباب وأثار الاختراقات وكيفية الوقاية منها

عرف الاختراق HAKING بأنه الوصول لهدف ما بطريقة غير مشروعة وهذا عن طريق ثغرات في نظام الحماية الخاصة بالجهاز وهي سمة سيئة بالطبع يتسم بها المخترق لقدرته على الوصول إلى أجهزة الآخرين عمدا ودون رغبة الضحية ومن أسباب الاختراق ودوافعه نجد مايلي:

أولا: الدافع التجاري: يعد الدافع التجاري من أهم وأبرز دوافع الاختراق الحالية ، حيث بينت إحدى الدراسات أن عددا من أكبر الشركات التجارية يجري عليها أكثر من خمسين 50 محاولة اختراق لشبكتها كل يوم .

ثانيا: الدافع السياسي والعسكري: مع بروز مناطق جديدة للصراع في العالم والتغير طبيعة الدول التكنولوجيا أصبح اعتماد كليا على الكمبيوتر وعن طريقه أصبح الاختراق من أجل الحصول على المعلومات السياسية والعسكري والاقتصادية كما نرى الدافع الفردي يظهر جليا عندما بدأت محاولة الإختراق بين طلاب الجامعات الأمريكية كنوع من التباهي بالنجاح في اختراق أجهزة شخصية لأصدقائهم ومعارفهم .

1_ أنواع الاختراق: للاختراق هناك ثلاثة أنواع وهم [1]:

- اختراق أجهزة الشركات والمؤسسات الرئيسية أو الجهات الحكومية باختراق الجدران النارية التي عادة توضع لحمايتها.
- اختراق الأجهزة الشخصية والعبث بما تحتويه من معلومات .
- التعرض للبيانات أثناء انتقالها والتعرف على شيفرتها إذا كانت مشفرة والتي تستخدم في الكشف على أرقام بطاقات الإئتمان وكشف الأرقام السرية للبطاقات البنكية .

2_ أثار الإختراق: من أثار الاختراقات هناك مايلي:

[1] مهندس حسام شوقي – مرجع سابق – ص 37و41.

- تغير واجهة المواقع الرئيسية وتتمثل هذه العملية في تغير صفحة الموقع ولا تكون هذه الأخيرة إلا عملية تشويه بحتة يعلن فيها المخترق قدرته في التغلب على الإجراءات الأمنية للأجهزة والشبكات ، حيث تختلف هذه العملية من موقع إلى أخر بناءا على نوع التشغيل المستعمل .

- حجب دخول الموقع وفيها تظهر رسالة عند فتح موقع ما ويكون نصها الوصول إلى هذا الموقع غير ممكن ، ومعناه أن الموقع الذي تحاول فتحه قد تعرض لهجمات.

- حجب خاصة ، وتوجد عدة أهداف قد تدفع جهة معينة ، أو شخص معين إلى القيام بمثل هذه الهجمات وأهمها :

* الانتقام والأخذ بالثأر	* عوامل سياسية دولية أو شخصية
* التسلل إلى النظام	* عوامل اقتصادية

3_ طرق الحماية من الإختراق: جميع المواقع والأجهزة معرضة للاختراق أثناء تواجدك على الشبكة وهذا إما عن طريق ملفات أحصنة طروادة أو عن طريق معرفة IP ADRESS الخاص بالجهاز وخلالها تكون عرضة لكشف الكثير من المعلومات والسيطرة على المعلومات المتواجدة بالجهاز خلال فترة الإتصال .

وعليه فإن هناك ثمة قاعدة أساسية تقول أن وجود برنامج حماية من الاختراقات لا يعني عدم قدرة المخترقين على إختراقه ، كما أن عدة برامج حماية تعمل في آنٍ واحد لا يعني أن جهازك مؤمن لأن ذلك يضعف من إمكانية شالحماية ومن هنا يجب عليك إتباع مايلي:

- لا تستقبل الملفات أو البرامج أو الصور إلا من الأشخاص الموثوقي بهم فقط ولا تفتحها إلا بعد خروجك من الأنترنت OFFLINE .
- يفضل أن يكون مفتاحك السري مكون من حروف وأرقام وأكثر من ثمان وحدات.
- تأكد من عدم وجود تروجان TROJAN عن طريق مسح القرص الصلب ثم إلغائه على الفور إذا تم العثور عليه.
- حاول تغير رقمك السري دوريا على الأقل كل شهر .
- لا تستقبل الملفات المرسلة إليك في البريد الإلكتروني من شخص لا تثق به وخاصة الملفات ت من نوع.DLL أو .EXE.
- تجنب فتح الملفات المرفقة بالرسائل الإلكترونية والغير المعروفة خاصة إذا كانت من نوع EXE. أي EXECUTABLE FILE الذي يلغي وجود ملف تقيّدي وهي تنفذ الأمر دون إذن منك وتعتبر

أكثر خطورة على نظامك ، ونوع COM. أي COMMAND.FILE وهي تدل على وجود أمر معين موجه لأحد ملفات النظام في تشغيل الجهاز، أما نوع APP. أي APPLICATION.FILE وهذا يعني وجود ملف به برنامج تطبيقي قد يحتوي على إحدى برامج التجسس.

- استعمال برنامج البروكسي PROXY الخاص بالحماية وتخفيف حدة الحمل الزائد على الشبكة أثناء دخول عدد كبير من المستخدمين إلى الشبكة في نفس الوقت.

المبحث الثالث:عمل الدرك الوطني في مكافحة جرائم الإعلام الألي

المطلب الأول: المعاينة والتفتيش من طرف وحدات الدرك الوطني

إن المعاينة والتفتيش من طرف وحدات الدرك الوطني تتم نحو ما قررته التشريعات الوطنية المقارنة والتي لازالت غير كافية وملمة على مختلف جرائم الإعلام الألي وهذا مقارنة مع بعض الدول التي أعطت أهمية كبرى لجرائم المعلوماتية ، كونها عرفت خسارة كبيرة أمام هذه الظاهرة ، أما المشّرع الجزائري فلم يقنن كل الجرائم ماعدا ما نصت عليه بعض من مواد المقرر رقم 10/97 المؤرخ في 06مارس1997 والمتعلق بحقوق المؤلف والحقوق المجاورة وقواعد البيانات الخاصة بالحاسوب في مادته السادسة الفقرة أ وبقي هذا الأمر إلى غاية تعديل بعض من مواد قانون العقوبات والإجراءات الجزائية والصادر بالجريدة الرسمية بتاريخ 10نوفمبر2004 ، حيث تم التطرق فيه إلى المساس بأنظمة المعالجة الألية للمعطيات .

لكن يبقى قانون العقوبات الجزائري غير كافي وغير شامل لجرائم الإعلام الألي ويعرف تأخرا ملحوظا في هذا المجال ، رغم أن الجزائر تعرف تحسنا وتطورا مذهل في ميدان استعمال الإعلام الألي والانترنت والتي مست جميع المؤسسات من شبكات محلية وعالمية، ومن هنا فإن مؤسسة الدرك الوطني ، مؤسسة تعمل وفقا للقوانين والأنظمة وعملها هذا اتجاه جرائم المعلوماتية يجب أن يدخل ضمن الإطار القانوني الذي لا يزال يعرف فراغا في ذالك .

ومن خلال ذلك وإن وجد التفتيش والمعاينة يتطلب من المحقق أن يعلم قبل كل شيء عن ابتداء وجود الأدلة المتصلة بجريمة ما ضمن أحد أنظمة الكمبيوتر أو الشبكات هذا من جهة أما من جهة أخرى فإن التحري والتفتيش في بيئة جرائم الكمبيوتر والانترنت يتوقف على مدى دقة محضر أو مذكرة التفتيش ونطاقها المكاني ، ويتعين أن يحرص المحققون أو جهة الضبطية المكلفة بالتفتيش من قبل النيابة .

وأمام هذا الوضع وقصد الابتعاد عن كل تأويلات خاصة ونحن نواكب عصر التكنولوجيات ، فيستوجب على وحدات الدرك الوطني المعنية بالبحث والتفتيش اللجؤ إلى إذن بالتفتيش من طرف

السلطات القضائية ، كون العمل تقني ويتطلب معرفة جيدة في هذا المجال وهذا بهدف التفتيش والتوغل إلى أنظمة الحاسب وتفحص القرص الصلب والأقراص الأخرى من أجل ضبط كل ما من شأنه أن يكون دليل أو قرينة دالة.

المطلب الثاني : عمل مؤسسة الدرك الوطني لمجابهة جرائم الإعلام الألي

إن مؤسسة الدرك الوطني تعمل جادة على التطلع لمختلف الجرائم المرتكبة على شبكة الأنترنت بالإضافة إلى إحصاء ومعرفة مزودي خدمة الأنترنت ومستخدميها ، وهذا لتسهيل مهمة البحث والمعاينة والتفتيش في أنظمة الحواسب والعمل على مراقبة مختلف الشبكات

كما أن مؤسسة الدرك الوطني ترى كباقية المؤسسات الأمنية الأخرى أن خدمة التزويد بالانترنت ، تعتبر نشاط تجاري كما هو معمول به في باقية الدول الأخرى ، وقد ضبط هذا النشاط في الجزائر ضمن دفتر الشروط المنجز من قبل وزارة البريد وتكنولوجيات الإعلام والاتصال التي لها الحق في منح رخصة استغلال خدمة الأنترنت لمزوديها أو بما يسمى ISP أي بمعنى INTERNET SERVICE PROVIDER وهذه الخدمة تعرف ثلاثة مستخدمين خواص وهم سيريست CERIST و إباد EBAD وكذلك جيكوس GECOS وهناك مستخدم البريد والموصلات جواب .

ومن هذه المعطيات وصل عدد مستخدمي الأنترنت في الجزائر إلى غاية سنة2004 إلى حوالي 180 ألف مستخدم [1] من مختلف الأعمار وأغلبهم شباب وهذا ما يعطي صورة واضحة على أنه هناك ثمة جرائم معلوماتية ترتكب داخل مختلف الشبكات وخاصة العالمية منها وهذه الجرائم إما أن يكون مرتكبيها داخل الوطن وتقترن جريمته في بلد أخر والعكس صحيح وخاصة ونحن في عالم الرقميات بشتى أنواعها .

كما لاحظت قيادة الدرك الوطني أن شبكة الأنترنت في الجزائر تتضخم ويزداد عدد مستخدميها بشكل غير مسبوق خاصة في السنوات الأخيرة ن وأصبح يعتمد أغلب مستعمليها على عمليات البحث في مختلف المجالات ، ليصبح مجال الإتصالات المتمثلة في خدمة البريد الإلكتروني تحتل المركز الأول في الجزائر أما في مجال تبادل المعلومات أصبحت مواقع الشبكة هي المصدر الرئيسي للحصول عليها[2] .

وأمام هذا الوضع قامت قيادة الدرك الوطني ب:

[1] جريدة السفير الأسبوعية – العدد 248- الصادرة من تاريخ 26فيفري إلى غاية 04 مارس 2005 م – ص 14.

[2] www.c-i-a.com/methodology.htm#internetuser.

1- بإنشاء مكتب خاص بمكافحة جرائم الإعلام الألي على مستوى قيادة الدرك الوطني والذي بدوره يضم أربع مصالح منها مصلحة المكونات المادية ، مصلحة الشبكات و مصلحة الوقاية والاستشارة و مصلحة الإعلام الألي للوقاية والاستشارة.

2- أسبوع دراسي حول جرائم الإعلام الألي من طرف خبراء فرنسيين أقيم بالمدرسة العليا للدرك الوطني بيسر وحضره بعض من صف الضباط الذين يملكون خبرة في ميدان الإعلام الألي والتابعين لمختلف الوحدات والقيادات الجهوية.

3- إنشاء المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني ببوشاوي الجزائر العاصمة والذي سيعمل بأحدث الوسائل والتقنيات لمحاربة مختلف الجرائم المستحدثة.

4- إرسال البعض من إطارات الدرك الوطني إلى بعض الدول الأجنبية كدولة فرنسا وكندا،بلجيكا وسويسرا من أجل تكوينهم في مختلف تقنيات جرائم المعلوماتية .

5- تحرير لائحة عمل إلى مختلف وحدات الدرك الوطني بما فيها مختلف المدارس التكوينية تحمل رقم 4/360/2001 ق إ ب/ق د وتحت موضوع الإجرام عبر الإعلام الألي في الجزائر بغية تحسيس الأفراد بهذه الظاهرة وتقديم بعض الإقتراحات الممكنة.

6- لفت انتباه مختلف السلطات المعنية وعلى رأسهم وزارة العدل حول التهديدات القائمة لهذه الظاهرة ، وضرورة تشريع قانوني يتماشى وتطور الإجرام المعلوماتي.

7- إحصاء مختلف مزودي خدمة الأنترنت ومقاهي الأنترنت ونسبة مستخدمي الشبكة والجهات العاملة عليها بالإضافة إلى المواقع الحساسة في الجزائر.

8- إعطاء فرص إنجاز بحوث علمية حول جرائم الإعلام الألي من طرف الضباط المتربصين لمختلف التشكيلات على مستوى المدرسة العليا للدرك الوطني بيسر.

9- المشاركة بمواضيع تدخل ضمن الإجرام المعلوماتي وتقنيات التكنولوجيا الجديدة في مجلات الدرك الوطني.

المطلب الثالث: التكوين التخصصي لإطارات الدرك الوطني في مكافحة الجريمة المعلوماتية

لقد أصبح من الضروري ، إذا أردنا مواجهة هذا النوع من الإجرام المعلوماتي القيام بتكوين مكونين قادرين على التحكم ومعرفة تقنيات مكافحة الجرائم المستحدثة ، ولاسيما جرائم الإعلام الألي وهذا يهدف للوصول إلى ركب العصرنة والبلوغ إلى مختلف ميادين العمل في تلك القطاعات بصفة مستمرة وواسعة ويشمل هذا التكوين الخاص كل الضباط وضباط صف الذين تتوفر فيهم الشروط المطلوبة ويتم ذلك من طرف المكونين الذين لهم قدرة التحكم في مختلف التقنيات بعدما أجرو تكوينا في الدول الأجنبية كفرنسا ، كندا و بلجيكا وسويسرا ثم التحقوا بالجزائر، على أن يتم هذا التكوين لصالح الفئة المذكورة أعلاه بالجزائر وبالضبط بمدارس الدرك والوطني وخلال مختلف الملتقيات .

ويكون الهدف من هذا التكوين التخصصي للأفراد المؤهلين هو:

* إعطاء للدركيين تقنيات كافية تساعدهم على مواجهة الأوجه الرئيسية لهذه الظاهرة.
* تحضيرهم للتقنيات الجديدة في التحقيق والتحري حول التكنولوجيات الجديدة.
* تحضيرهم للمسؤوليات المتعلقة بإنشاء خلايا تعمل لمكافحة الإجرام المعلوماتي .
* تدعيم ثقافتهم المهنية والتقنية لتحسين تحليل المواقف المقدمة وأخذ القرارات المفروضة.
* الأخذ بعين الاعتبار التقدم التكنولوجي و استعمال التكنولوجيات للأغراض إجرامية.
* تحضيرهم للقيام بعمليات تقنية دقيقة متعلقة بالجرائم المعقدة و هذا لاكتشافها.

_ تحسين نوعية العمل ب:

- التسيير الجيد للمعلومات، الفهم الواسع للملفات، إنشاء توجهات البحث.
- ممارسة الوسائل التقنية للتحريات بالطرق العملية و تدريس منهجية العمل و المعرفة الجيدة للتقنيات العصرية.

المواد اللازمة دراستها:

- المعلومة، الشبكات، الأنترنت، التشكيلة الرقمية(الصورة و الصوت الرقمي).
- وسائل الاتصال(الهاتف، الهاتف الخطي و بواسطة الأمواج، السمعية البصرية).

- التجارة الإلكترونية.
- التشفير وطرق الحماية بالوسائل التقنية.
- بطاقات و ذاكرات.
- الاستقبال الساتيليتي.
- الفيروسات و أحصنة الطروادة.
- الغش و القرصنة.

الخاتمة

من خلال بحثنا هذا ،تم دراسة موقف التشريع المقارن والمنظمات الدولية والإقليمية من جرائم الإعلام الألي ، والعمل على كيفية مكافحتها والوقاية منها من طرف الدولة الجزائرية، وهذا بإستراتجية عامة يفرضها التطور التكنولوجي المعاش حيث تجعل من الجهات الأمنية الجزائرية ومن بينها مؤسسة الدرك الوطني تقوم بعمل فعال في عصرنة الجهاز وجلب أحدث التقنيات والتكنولوجيات الحديثة لمواجهة هذا النوع من الإجرام المعلوماتي وصعوبة الكشف والمعاينة عنه في ظل غياب التشريعات المقننة.

إن هذه الصعوبات الناجمة عن عدم كفاية القوانين التشريعية الموضوعية والإجرائية أثرت على نحو حقيقي في اتجاه عدد كبير من الدول ، ولِسن هذه التشريعات في الجزائر التي لا تزال لحد الآن تعاني من فراغ قانوني يدخل في نطاق قوانين الموضوعية ، بات من المؤكد وضع قانون يشمل مختلف الجرائم المقترفة عبر الشبكة والتي تدخل في إطار المعلوماتية حيث يتطلب على الجزائر وضع إستراتيجية تتماشى والتطور التكنولوجي وهذا بالتنسيق مع مختلف الدول التي لها خبرة في هذا المجال وكانت قد عرفت هذا النوع من الجرائم وذلك بالإسراع في انجاز مشروع قانون العقوبات الذي يلم بمختلف الجرائم المستحدثة للمعالجة الألية للبيانات .

وفي الأخير تم التطرق إلى الوسائل التقنية المستعملة في الوقاية من الجرائم المعلوماتية وحماية الأجهزة العاملة على الشبكة من مختلف الاختراقات ، وهذا بالإضافة إلى أهم الأعمال التي قامت بها قيادة الدرك الوطني انطلاقا من أنشاء المعهد الوطني للأدلة الجنائية وعلم الإجرام الذي يتوفر على أحدث التكنولوجيات والتقنيات ووصولا إلى التكوين التخصصي للإطارات الدرك الوطني في بعض البلدان الأجنبية التي تعرف تطورا في هذا المجال ونقل أحدث التقنيات التكنولوجيا لوحدات الدرك الوطني للعمل بها مستقبلا في المعاينة والكشف عن هذا النوع من الإجرام ومكافحته بالوسائل التقنية.