إشكالية تحديد المسؤولية الجنائية للتحرش الإلكتروني كجريمة إلكترونية والجهود الدولية لمكافحته

دكتور / محمود سيد احمد عبد القادر عامر

دكتوراه في القانون الجنائي

كلية الحقوق جامعة المنصورة

مُدرس القانون الجنائي

بالجامعات المدنية والشُرطية والعسكرية

المقدمة

تتطور الجريمة بتطور الزمان والمكان فهي ظاهرة اجتماعية قديمة ومستمرة تنشأ بسبب الصراع على إشباع الحاجات اللامتناهي ومع التطور التقني المشهود تظهر في الوقت المعاصر الجريمة الإلكترونية؛ والتي تُعد ظاهرة إجرامية مُستجدة ومُستحدثة تستهدف المُعطيات بدلالاتها التقنية الواسعة (بيانات ومعلومات وبرامج) وقيم مادية ومعنوية بكافة أنواعها ولهذا ينبغي الالتفات بجدية لمعالجة هذه الظاهرة.

وتعددت ابعاد الجريمة الإلكترونية واكتسبت بُعداً جديداً بتطور أدواتها فيقوم المُجرمون بتطبيق أوجه التقدم العلمي والتكنولوجي في دعم أهدافهم غير المشروعة، ونتيجة للاستخدام المستمر لوسائل التكنولوجيا بأشكالها المتعددة كالهاتف والبريد الإلكتروني والمواقع الإلكترونية فضلاً عن البلوتوث ومواقع التواصل الاجتماعي وغيرها من المواقع والمنتديات التي تقصدها الفتيات والأطفال والشباب بوجهٍ عام وبحكم انهم الاكثر استخداما لها، انتشرت أفة الاستخدام الخاطئ لهذه التكنولوجيا وهي ظاهرة التحرش الإلكتروني باختلاف اشكاله؛ والذي يتم عن طريق استخدام المواقع الإلكترونية والرسائل العشوائية المحتوية على روابط جنسية كما تواجد في الآونة الأخيرة العديد من المنتديات الخاصة بنشر الثقافة الإلكترونية والمواقع الإباحية التي تُساعد على الانحراف.

ويُعتبر التحرش الإلكتروني امتدادًا للتحرش الجسدي، وكلّ ما يحتاجه المتحرش هو الوصول إلى جهاز كمبيوتر ومودم، حيث تكمن قوته في المعلومات الكثيرة التي يستطيع جمعها عن الضحية التي اختارها عن طريق الإنترنت طالما أن الأخير قد أصبح ملماً بالمعلومات والبيانات الشخصية، وبذلك يصبح جميع مستخدمي الإنترنت عرضةً للتحرش الإلكتروني. وعلى ما تقدم سنحاول التعرف على هذا النوع من الإجرام وذلك من خلال البحث في التحرش الإلكتروني كجريمة إلكترونية والمسئولية الجنائي لأطراف هذه الجريمة وأهم الجهود التشريعية المتخذة على المستويات المحلية والإقليمية والدولية في مجابهة الجريمة الإلكترونية.

خطة الدراسة:

المبحث الأول: صور وأركان جريمة التحرش الإلكتروني
المطلب الأول: صور التحرش الإلكتروني.
المطلب الثاني: أركان جريمة التحرش الإلكتروني في القوانين الوضعية.
المطلب الثالث: أركان جريمة التحرش الإلكتروني في الشريعة الإسلامية.
المبحث الثاني: المسئولية الجنائية عن جريمة التحرش الإلكتروني كجريمة إلكترونية
المطلب الأول: المسئولية الجنائية للجاني.
المطلب الثاني: المسئولية الجنائية لمزود الخدمة ومتعهد الإيواء (المستضيف).
المبحث الثالث: الجهود الدولية لمُكافحة الجرائم الإلكترونية
المطلب الأول: القوانين الدولية والعربية التي ساهمت في مُكافحة الجريمة الإلكترونية.
المطلب الثاني: أدلة اثبات الجرائم الإلكترونية في التشريعات العربية.
المطلب الثالث: التعاون الدولي للحد من الجريمة الإلكترونية.

المبحث الأول
صور وأركان جريمة التحرش الإلكتروني

تمهيد وتقسيم:

ساهم نظام مُكافحة الجرائم المعلوماتية في التصدي لانتشار التحرش الإلكتروني ولكنه لم يقض عليه ولقد عانى كثيرون من مستخدمي الأجهزة الإلكترونية الموصلة بشبكة الإنترنت من تعرضهم لأشكال مُختلفة من المُضايقات تبدأ بالإلحاح بالتعارف من اشخاص لا يعرفونهم وتستمر بتعرضهم للملاحقة والتعقب من جانب آخرين ممن لديهم خلافات شخصية معهم.

وقد يتعرض المرء للتحرش من أشخاص معروفين له او من مجهولي الهوية [1] ويُعرف التحرش الإلكتروني بأنه استخدام وسائل تكنولوجيا المعلومات والاتصالات من جانب فرد او مجموعة في إيذاء الآخرين في شكلٍ مُتعمد [2]. ولازالت الصورة حيال فرض عقوبة على المُتحرشين الكترونياً في عالمنا العربي مشوشه تنظيمياً [3] وفي ثلاثة مطالب متتابعة نُبين صور جريمة التحرش الإلكتروني وأركانها في القوانين الوضعية والشرعية الإسلامية وذلك على النحو التالي:

المطلب الأول: صور التحرش الإلكتروني.

المطلب الثاني: أركان جريمة التحرش الإلكتروني في القوانين الوضعية.

المطلب الثالث: أركان جريمة التحرش الإلكتروني في الشريعة الإسلامية.

---

[01] د/خالد الشرقاوي السموني، مكافحة الجرائم الإلكترونية على ضوء التشريعين الوطني والدولي ونشر في 2012/3/19م. www.startimes.com

[02] انظر: نورا جبران تعريف التحرش الإلكتروني في مجلة الحياة نُشر بتاريخ 2014/10/30م على الرابط www.alhayat.com

[03] حمدان محمود، التحرش الإلكتروني عبر الانترنت الأكاديمية العربية لخدمات الباحثين 2007م.

المطلب الأول

صور التحرش الإلكتروني

تمهيد:

التطور التقني والتكنولوجي الذي نشهده اليوم يسبق بكثير التشريعات التي من المفترض ان تواكبه ويستدعى ذلك اتخاذ مجموعة من الخطوات والإجراءات الاستراتيجية على كافة الأصعدة وبينها بالأخص خطوات وإجراءات تدخل ضمن النطاق التنظيمي لاسيما ان التطور التكنولوجي يمتاز بوتيرة مُتسارعة يجعل الكثير من النصوص والأحكام التنظيمية القائمة غير منطبقة وقد تجاوزها الزمن، وان بيئة بهذا القدر من التطور تواجه وظيفة التشريع تحدياً كبيراً ومتواصلاً ليس فقط على الدولة المعنية به بل امام المجتمع الدولي برمته.

ـ التحرش عبر البريد الإلكتروني [1]:

لم تُعد احتمالية تعرض الشخص للتحرش الجنسي مرتبطة بالمُقابلة المباشرة بين المُتحرش والضحية فمع انتشار وسائل التواصل الإلكتروني أصبح بإمكان المُتحرش الوصول إلى الشخص في أي مكان وفي أي وقت اذ يعاني الكثير من مستخدمي شبكات التواصل الاجتماعي والأجهزة الإلكترونية الموصولة بشبكة الإنترنت من استلامهم المتكرر للرسائل غير اللائقة التي قد تحتوي على عبارات او شتائم جنسية او صوراً او مشاهد جنسية [2]، او التهديد والابتزاز باستخدام صور الضحية او استخدامها فعلاً دون موافقة صاحبها او من دون عمله ومشاركتها في مواقع ذات طابع جنسي او مقرونه بعبارات غير لائقة.

وقد زادت إمكانية تعرض مستخدمي شبكة الإنترنت إلى هذا التحرش بسبب انتشار ثقافة الاستعراض من خلال نشر الصور والمعلومات الشخصية من جهة والفراغ النفسي والعاطفي الذي يدفع بعض الاشخاص لقضاء ساعات طويلة على شبكة الإنترنت قد تصل إلى إدمان الإنترنت والرغبة في إيذاء الاخرين من جهة اخرى ولا يقتصر التحرش فقط على الفتيات إذ يشكوا العديد من الرجال من تلقيهم لرسائل غير مناسبة تتضمن صور عبارات غير لائقة.

وقد بدأت ظاهرة التحرش باستخدام البريد الإلكتروني ومع انتشار الإنترنت أكثر شمل التحرش غرف الدردشة والمنتديات ومواقع التواصل الاجتماعي مثل الفيس بوك وتويتر والواتساب كما تحول التحرش عن طريق الإنترنت من مجرد التركيز على

---

01 د/ على محمد، شمول التكنولوجيا الحديثة الاتصال الدولي والانترنت ص 252.

02 نضال الشاعر الإطار التشريعي لجرائم المعلومات والانترنت داخله في ورشه عمل حول جرائم المعلومات والانترنت.

المواضيع الجنسية والسرقات المالية إلى مواضيع سياسية وتصفية حاسبات شخصية وتشمل اشكال هذا التحرش ملاحقة الاخرين او التشهير بهم [1].

وتعددت الأضرار النفسية لجريمة التحرش عبر الإنترنت فقد يُعانى من يتعرض للتحرش عن طريق الإنترنت من الاكتئاب وعدم الشعور بالأمان والراحة النفسية خاصة صغار السن اذ يُشكل الفتيان والفتيات الشريحة الاكثر عُرضة للتحرش فقلة خبرتهم وصغر سنهم واندفاعهم يجعلهم لا يدركون حجم الخطر الذي يُهددهم فعلى سبيل المثال يعتقد الكثير منهم من الممكن الوقوع في الحب عن طريق الإنترنت حيث يغلب الخداع فالمتحدث عن طريق الإنترنت غالباً مختبئ وراء شاشة يستطيع من خلالها قول أي كلام سواء كان صادق او كاذب ثم يتطور إلى طلب المحادثة بالصوت والصورة او اللقاء على أرض الواقع كعلاقة بريئة غالباً ما تنتهى بمأساة وقصص مُحزنة طبقاً لكثير من روايات من تعرضوا للخداع.

وهناك خطوات تساهم إلى حد كبير في الحد من التعرض للتحرش الإلكتروني وتضمن تحقيق اعلى مستوى من الخصوصية على شبكة الإنترنت او على الأجهزة الإلكترونية وتشمل الاتي [2]:

- عدم قبول طلبات الإضافة من أي شخص غير معروف.
- عدم نشر الصور الشخصية او ارقام الهواتف او المعلومات الشخصية في نطاق اوسع من نطاق الاصدقاء.
- وضع نظام للبريد الإلكتروني يضمن تحول الرسائل التي تحمل اسماء او كلمات غير مرغوبة إلى قائمة Spam.

المُضايقات الإلكترونية:

ومع تنامى الاعلام الإلكتروني فقد تزايدت اعداد الشكاوى من المُضايقات الإلكترونية او ما يسمى التخويف الإلكتروني إضافة إلى مُضايقات التحرش الجنسي وأنواع اخرى من حوادث الإيقاع بالضحايا.

وعلى الرغم من ان شتى الدراسات تعتمد على تعريفات مُختلفة وعلى طرق متنوعة للقياسات الخاصة في هذا المضمار الا انها تُشير إلى ان ما بين 9% و34% من المراهقين والمراهقات في الولايات المتحدة يقعون ضحية للمُضايقات الإلكترونية التي تعرف بانها نوع من التهديد او التخريف او القذف لأنها ليست مُضايقات جنسيه.

إلى ان ما بين 4% و21% من الاشخاص يقفون وراء هذه المُضايقات واظهر استطلاع أمريكي أجري عبر الهاتف للأطفال والمراهقين بين أعمار 10 و17 سنة ان

---

01 آية عامر، دراسة الانترنت يُسهل التحرش عبر مواقع التواصل الاجتماعي.
02 دُعاء عرابي، التحرش عن طريق الانترنت بحث منشور 2017/3/21م.

13% منهم قد تسلموا نوعاً ما من رسائل التحرش الجنسي الإلكتروني منهم 4% تسلموا رسائل مُحلة للالتقاء بهم في الخارج لذلك فإن مما لا يُسير الدهشة ان يتوجه اطباء الصحة النفسية والمدرسون والآباء إلى طلب النصائح والمشورة حول كيفية حماية الأطفال والمراهقين من هذا الأذى الإلكتروني.

وكان مركز مُكافحة الامراض ومرقبتها قد جمع عدداً من الخبراء عام 2006م لمناقشة سبل حماية المراهقين من التخويف والابتزاز الإلكتروني والمُضايقات الإلكترونية الأخرى وقد نشرت نتائج دراسة هذه المجموعة وتوصيتها في ديسمبر 2007م في عدد خاص من مجلة صحة المراهقين أما مجموعات البحث الأخرى فركزت دراستها حول كيفية حماية الفتيان والفتيات من التحرش الجنسي الإلكتروني.

لا يرغب مستخدمي الإنترنت في الغالب بوضع معلوماتهم الشخصية على الشبكة الإلكترونية ومع ذلك فإن الأبحاث التي أُجريت حتى الأن تُقدم دلائل على ان نشر هذه المعلومات ليس مماثلاً في خطره لخطر أنواع السلوك الأخرى على الإنترنت. وتزداد فُرص تعرض الفتيان والفتيات للمُضايقات او التحرش الجنسي الإلكتروني وتكون عندما يأخذون في التفاعل مع الآخرين الكترونياً مثل تبادل الرسائل الفورية او الدخول في حوار في غرف الدردشة الإلكترونية.

وليس من الواضح السبب الذي يقود فيه هذا السلوك إلى مثل هذه المشكلة إلى انه يبدو من المحتمل ان تكون غُرف الدردشة هذه التي تجرى فيها الأحداث مباشرة وفي الزمان الواقعي وفي أغلب الأحيان بعيداً عن اعين الكبار هي التي تشجع على حدوث سلوك تلقائي خطير [1].

الشبكات الاجتماعية:

وجد استطلاع اجراه موقع (بيو إنترنت اند أميركانا لايف) عام 2006 ان 55% من الاميركيين في اعمار 12إلى 17 سنة يستخدمون الشبكات الاجتماعية الإلكترونية فيسبوك وماي سبيس التي يمكنهم فيها وضع معلومات شخصية عنهم والاتصال الكترونياً بأشخاص اخرين مما يتيح الفرصة لبعض من الذئاب البشرية الإلكترونية لمراقبة ضحاياهم لاقتناصهم.

ومع ذلك فإن الباحثين الذين حللوا كلاً من مُضايقات التخويف الإلكترونية والتحرش الجنسي الإلكتروني توصلوا إلى استنتاج مفاده ان مواقع الشبكات الاجتماعية ليست خطيرة بمثل خطر النوافذ الإلكترونية الأخرى فقد وجد استطلاع وطني إلكتروني

[01] محمود عبدالعليم سليمان، إيذاء النساء، باثولوجيا التحرش الجنسي الإلكتروني بالمرأة، مجلة جيل العلوم الإنسانية والاجتماعية، العدد 42، مصر، مايو 2018، ص131.

للصغار من اعمار 10 إلى 15 سنة مثلاً ان 33% منهم قالوا انهم تعرضوا للتخويف الإلكتروني وقال 15% انهم تعرضوا للتحرش الجنسي الإلكتروني.

ومع هذا فإن غالبية مُضايقات التخويف الإلكتروني والتحرش الجنسي الإلكتروني حدثت في نافذة غرف الدردشة وعبر الرسائل الفورية وشكلت الشبكات الاجتماعية 9% فقط من التخويف الإلكتروني و4% من التحرش الجنسي الإلكتروني.

ووجد باحثوا مركز ابحاث الجرائم المواجهة ضد الاطفال في جامعة نيوهامشر الذين حللوا بيانات جمعت حول ضحايا الذئاب البشرية الجنسية على الإنترنت ان الصغار الذين وقعوا ضحايا كانوا على الاغلب من هؤلاء الذين تفاعلوا مع اشخاص غرباء من الذين وصلتهم رسائل منهم او شاركوا في حوار معهم [1].

الرسائل الفورية. [2]

تُسهل التقنيات الحالية في الإنترنت تبادل الرسائل المكتوبة جيئةً وذهاباً لأي شخص يستخدم الكمبيوتر والهاتف الجوال والأجهزة الإلكترونية الاخرى وهذه الوسيلة التي تزداد شعبيتها لدى الصغار والشباب يبدو انها تشكل خطراً عليهم يتمثل في التخويف والتحرش الجنسي الإلكتروني.

وعلى سبيل المثال فإن الدراسة على تلاميذ المدارس المتوسطة في الجنوب الشرقي وفي الشمال العربي للولايات المتحدة وجدت ان الرسائل الفورية كانت المصدر الشائع الاكبر للتخويف الإلكتروني مقارنة برسائل البريد الإلكتروني او غرفة الدردشة او الشبكات الاجتماعية. وقال 67% من التلاميذ انهم وقعوا ضحية لمُضايقات التخويف الإلكتروني عبر هذه الرسائل كما وجد استطلاع وطني لمستخدمي الإنترنت ما بين 10 إلى 15 سنة ان المُضايقات الإلكترونية والتحرش الجنسي تظهر على الاغلب اثناء الرسائل الفورية.

غُرف الدردشة:

هذه المنتديات الإلكترونية المخصصة للحوار تتيح للناس تبادل الرسائل المكتوبة فيما بينهم والمحادثات كما تتيح بعض المواقع للمشاركة وتبادل الصور والأحاديث في نفس الوقت.

وفي استطلاع لتلاميذ المدارس المتوسطة قال واحد من اربعة من الذين تعرضوا لمُضايقات الإلكترونية انها وقعت عندما كانوا يشاركون في حوار في غُرف الدردشة

---

01 استطلاع أُجري عام 2006حول مخاطر الانترنت على الاطفال منشور بتاريخ 2016/3/28م.

02 د/ جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، أجهزة الرادارات والحاسبات الآلية والبصمة الوراثية الطبعة الأولى دار النهضة العربية 2001م /ص100.

وفي استطلاع وطني للفتيان بين 10 إلى 15 سنة قال واحد من كل خمسة تقريباً انه تعرض للمُضايقات في غرف الدردشة [1].

إلا ان غُرف الدردشة هذه تشكل خطراً أكبر من ناحية التحرش الجنسي الإلكتروني ويعتقد الباحثون ان غرف الدردشة خطره لكونها تتيح للمشاركين فيها الاتصال المباشر وبشكل شخصي ولأن بعضاً منها يُشجع على استخدام اللغة البذيئة والأحداث الجنسية والتلميحات الجنسية.

كما توجد ايضاً دلائل على ان الصغار الذين يزورون غرف الدردشة غالباً ما يشعرون بالوحدة او بالكأبة او بالاغتراب عن والديهم كذلك وعلى الاغلب يعانون من الانتهاك الجنسي او ان لديهم سلوكاً خطراً مقارنة بالأشخاص الذين لا يزورون غرف الدردشة.

المدونات الإلكترونية.

هذه المدونات التي يُسجل فيها الكاتب خواطره وآراءه او معلوماته الشخصية ويمكن لقارئ هذه المدونات ارسال تعليقاتهم ايضاً التي قد تقود إلى حوار إلكتروني بين القارئ واخرين او من كاتب المدونة وقد اسس 1 من كل 5 من الفتيات بين اعمار 12 إلى 17 سنة مدوناتهم الخاصة بهم.

وتزيد المدونات من المُضايقات الإلكترونية وقد تزيد من خطر التحرش الجنسي الإلكتروني حيث يكشف كُتاب المدونات عن خفايا ذاتهم الشخصية على الإنترنت ومن بينها مشاعر ضعفهم وبياناتهم الشخصية [2].

---

[01] محمد امين الشوابكة، جرائم الحاسوب والإنترنت الجريمة المعلوماتية، دار الثقافة والنشر والتوزيع، الأردن،2011م، ص 45 -46.

[02] محمد امين الشوابكة جرائم الحاسوب والإنترنت الجريمة المعلوماتية مرجع سابق ص 117-124.

المطلب الثاني

أركان جريمة التحرش الإلكتروني في القوانين الوضعية

تمهيد وتقسيم:

وعلى كل حال فإن جريمة التحرش الإلكتروني تخضع للقواعد العامة بوجهٍ عام ولا تختلف عن الجرائم الأخرى بهذا الخصوص فلابد من توافر الركن المادي والمعنوي وفقاً لما هو متعارف عليه من قانون العقوبات وهو ما سوف نُفصله في فرعين من النحو التالي:

الفرع الأول: الركن المادي في جريمة التحرش الإلكتروني.
الفرع الثاني: الركن المعنوي في جريمة التحرش الإلكتروني.

الفرع الأول
الركن المادي في جريمة التحرش الإلكتروني.

يتمثل الركن المادي في الجريمة بالسلوك الذي جعل الجريمة تحدُث حتى ولو لم تتوافر وجود لمعرفة بداية هذا النشاط والشروع فيه ونتيجته [1] فالركن المادي للجريمة هو سلوك إجرامي يتم فيه ارتكاب فعل جرمه القانون او امتناع عن فعل أمر به القانون [2]. وللركن المادي الدور الأساسي في البنيان القانوني للجريمة حيث أن وجودها يؤدى إلى وجود جريمة وفقاً للنموذج المحدد لها في نصوص التجريم، والعِقاب في التشريعات المُختلفة وحتى تقضى المحكمة بتقرير المسؤولية الجنائية للجاني فلابد ان يكون هذا الأخير قد ارتكب افعالاً يتحقق بها الركن المادي لجريمته ويترتب على ما ارتكابهم من أفعال نتيجة مادية مُحددة وسواء كانت بصورة مباشرة او غير مباشرة طالما توافرت علاقة السببية بين سلوكه الإجرامي نتيجة مُتحصلة من هذا السلوك او القيام بنشاط يُجرمه القانون حتى ولو لم تتحقق معه نتيجة معينة كما هو الحال في الجرائم الشكلية ومنها جريمة التحرش الإلكتروني [3].

فتتكون جريمة التحرش الإلكتروني مثلها مثل باقي الجرائم من نشاط إجرامي يقوم به الجاني ونتيجة إجرامية وما يترتب على ذلك النشاط وعلاقة سببية تربط بين النشاط والنتيجة. وعلى ذلك سنتناول هذا الموضوع بالشرح في ثلاث فقرات تُمثل في مجموعها العناصر التي يقوم عليها الرُكن المادي لجريمة التحرش الإلكتروني وهي

---

01 د. عبد الفتاح بيومي حجازي، مكافحه جرائم الكمبيوتر والانترنت في القانون العربي النموذجي. دار الكتب القانونية القاهرة 2007م ص347-397.

02 قانون العقوبات العراقي رقم 111 لسنة 1969م.

03 د. احمد فتحي سرور، الوسيط في قانون العقوبات القسم الخاص طبيعة نادى القضاء مصر القاهرة 1980م - ص 199.

السلوك او النشاط الإجرامي فقرة اولى والنتيجة الإجرامية فقرة ثانية وعلاقه السببية بين السلوك والنتيجة فقرة ثالثة وذلك على النحو التالي:

الفقرة الأولى: النشاط الإجرامي في جريمة التحرش الإلكتروني:

المُراد بالنشاط الإجرامي وهو ذلك النشاط المادي الملموس الذي يأتيه الجاني او يتقاعس فيه عن تنفيذ واجب قانوني مفروض عليه بما يوقعه تحت طائلة العقاب.

ويتنوع السلوك الإجرامي إلى نوعين إيجابي وسلبي فتكون جريمة التحرش الإلكتروني إما ان تُرتكب بسلوك إيجابي او سلوك سلبي. وسوف نبين هذه الافعال المحظورة وفقاً لنوع السلوك المرتكب فيما يلي:

أ. السلوك الإيجابي.

فهو حركة عُنصرية إرادية يقوم بها الجاني لتنفيذ الجريمة التي ينسب اليه ارتكابها [1].

ومن امثلة هذا في جريمة التحرش الإلكتروني قيام المُتحرش بإرسال رسالة تحتوي على كلمات إباحية والفاظ جنسية على الصفحات الخاصة بضحايا التحرش الإلكتروني او عبر إيميل الخاص.

ب. السلوك السلبي.

ويقصد به الإحجام او التقاعس عن إتيان سلوك إيجابي مُحدد كإن من الواجب فعله والوفاء به حال توافر ظرفٍ ما [2].

والعلة من التجريم والعقاب على سلوك الامتناع تكمن في ان هذا السلوك من شأنه الإفصاح عن الإرادة الإجرامية التي اتجهت إلى الامتناع عن الفعل الإيجابي الذي اوجب القانون القيام به.

وفي التطور التقني الحالي يعتبر السلوك السلبي ركن له أهميته في جرائم التحرش الجنسي بوجهٍ عام والتحرش الإلكتروني بوجهٍ خاص فهو يجد انتشاراً واسعاً في مثل هذه الجرائم فإن الامتناع عن اداء الواجب الذي يُفرضه القانون او التقاعس المُتمثل في الامتناع عن اتخاذ الاحتياطات اللازمة يؤدى إلى وقوع حالات تحرش إلكتروني قد تصل إلى حد الزنا.

---

[01] احمد عوض بلال، مبادئ قانون العقوبات المصرية القسم العام. دار النهضة القاهرة ص 255.

[02] محمود نجيب حُسنى، قانون العقوبات القسم العام، دار النهضة، مصر، 1998 ص 375.

الفترة الثانية: النتيجة الإجرامية في جريمة التحرش الإلكتروني.

تتمثل النتيجة الإجرامية في جريمة التحرش الإلكتروني في الأثر الذي يترتب على السلوك الإجرامي الذي يُحدد له القانون حماية جنائية [1] وتحدد التشريعات الجنائية النتيجة الإجرامية بالنظر إلى طبيعة المصلحة المراد حمايتها بنصوص خاصة بالتجريم والعقاب وعلى ذلك فإن ثمة مصالح تحتاج إلى حماية لمُجرد تهديدها بالخطر حتى ولو لم يترتب على ذلك آثار مادية كما ان هناك مصالح وحقوقاً لا يكفي لحمايتها مجرد تهديدها بالخطر وانما يلزم ان يترتب على ذلك أثار مادية مُحددة [2].

وعلى ضوء ما تقدم يمكن القول ان النتيجة الإجرامية لها مدلولان أحدهما مادي والاخر قانونيا.

والمدلول المادي يُمثل أثر ارتكاب النشاط الإجرامي في التغير الذي يحدث في العالم الخارجي والذي يوجب ارتباط السلوك بالنتيجة التي أدَّى اليها برابطة سببية مادية.

والمدلول القانوني يُمثل الاعتداء على المصلحة التي يحميها القانون سواء أدَّى هذا الاعتداء إلى إحداث ضرر بالمصلحة المعتدى عليها او كونه مُجرد تهديد بالخطر.

ويترتب على مدلول النتيجة القانونية ان جرائم الشروع لها نتيجة إجرامية تتمثل فيما تُحدثه من الضرر الذي تسبب فيه الفعل الإجرامي بالنسبة للمصلحة المراد حمايتها قانوناً.

ويُعتبر عنصر النتيجة بمدلوليه من المسائل الشائكة الدقيقة صعبة الإثبات في جريمة التحرش الإلكتروني ويرجع ذلك إلى الطبيعة الخاصة لهذه الجريمة وما يترتب عليها من نتائج فهذه النتيجة قد لا تتحقق في الحال ولكن قد يتراخى تحقيقها لفترة قد تطول او تقصُر كما انها قد تتحقق في مكان حدوث الفعل وقد تتحقق في مكان اخر وهو ما عليه الحال في جريمة التحرش الإلكتروني واخيراً قد لا يمكن السلوك الإجرامي مكوناً لنتيجة مادية معينة ولكن مجرد تعريض أحد العناصر المراد حمايته للخطر يؤدى إلى تحقق النتيجة [3].

جرائم الضرر وجرائم الخطر في التحرش الإلكتروني.

تنقسم الجرائم وفقاً للمفهوم القانوني للنتيجة إلى قسمين من حيث ما تُحدثه من ضرر وخطر إلى جرائم ذات ضرر مؤكد تتمثل فيها النتيجة القانونية المُترتبة على النشاط الإجرامي في إلحاق ضرر فعلى بالمصلحة محل الحماية الجنائية وإلى جرائم ذات

---

01 أحمد شوقي ابو خطوه، شرح الأحكام العامة لقانون العقوبات دار النهضة العربية مصر – القاهرة 2000م ص 226.

02 أحمد شوقي ابو خطوه، المرجع السابق ص 228.

03 د/احمد شوقي ابو خطوه، مرجع سابق ص 226 وما بعدها.

خطر او ضرر مُحتمل تتمثل فيها النتيجة القانونية المترتبة على النشاط الإجرامي في مجرد تهديد المصلحة المحمية بالخطر دون استلزام الإضرار الفعلي بها.

فهذا الخطر هو النتيجة في هذه الجرائم والتي يُعاقب عليها القانون ليتفادى حدوث الضرر والخطر حالة واقعية وهو مجموعة من الآثار المادية ينشأ بها احتمال حدوث اعتداء ينال الحق [1].

وفي جريمة التحرش الإلكتروني قد يتطلب المُشرع الجنائي حدوث نتيجة مادية معينة تتمثل في الضرر الذي أدَّى إليه النشاط الإجرامي المُرتكب ليقرر مُعاقبته وأحيانًا قد لا يتطلب المُشرع تحقيق نتيجة إجرامية معينة بحيث ينصب التجريم على ذات النشاط الإجرامي للجاني بغض النظر عن أية نتائج مُستقلة أخرى يؤدى إليها هذا السلوك الإجرامي فإن المسؤولية الجنائية كما انها تتوافر في حالة تحقق نتيجة معينة فأنها كذلك قد تنشأ في حالة ارتكاب النشاط المجرد بشرط ان يكون من شأنه تعريض المصلحة محل الحماية للخطر وهذا لا يمنع من ان ثمة أفعالاً يتطلب المُشرع الجنائي فيها تحقق نتيجة معينة حتى يمكن القول باكتمال أركانها القانونيه وهي السمة الغالبة في جرائم التحرش الإلكتروني. لذلك لا تختلف النتيجة الإجرامية في جرائم التحرش الإلكتروني عن النتيجة الإجرامية للجرائم الأخرى.

النطاق الزماني للنتيجة الإجرامية في جريمة التحرش الإلكتروني:

تُعتبر غالبية جرائم التحرش الإلكتروني من الجرائم الوقتيه لأن مناط ذلك هو السلوك الإجرامي ومدى استمرار او وقت ارتكابه، فالنتيجة في جريمة التحرش الإلكتروني قد تتراخى لتتحقق في زمان لاحق على ارتكاب النشاط الإجرامي.

النطاق المكاني للنتيجة الإجرامية في جريمة التحرش الإلكتروني:

ما يميز جريمة التحرش الإلكتروني عن غيرها من الجرائم أنه قد يرتكب السلوك الإجرامي في مكان معين وتتحقق النتيجة الإجرامية في مكان اخر.

الفقرة الثالثة: علاقة السببية في جريمة التحرش الإلكتروني.

الصلة التي تربط ما بين النشاط الإجرامي والنتيجة الجرمية المتحققة منه تكمن في العلاقة السببية وهي التي تثبت ان ارتكاب السلوك أدَّى إلى حدوث النتيجة وبعبارة أخرى فإن علاقة السببية هي الرابطة التي تصل ما بين النشاط والنتيجة الإجرامية المترتبة عليه وتثبت بأن هذه الأخيرة قد تحققت بسبب الأول وأنها قد ارتبطت به ارتباط المسبب بالسبب [2].

---

[01] محمود نجيب حسنى، المرجع السابق، ص 386.
[02] د/احمد عوض بلال مرجع سابق ص 301.

وتمكن الأهمية القانونية لعلاقه السببية في انها تربط ما بين عنصري الركن المادي السلوك والنتيجة فتقيم بذلك وحدته وكيانه وتجعل منه فكرة وظاهرة قانونية متمسكة العناصر والبنيان [1].

ومن الأمور التي تتصل ايضاً بإثبات علاقة سببية ان النتيجة بمفردها قد تساهم في تحقيقها أكثر من سبب ومن ثم يكون من الصعوبة إثبات السبب الذي افضى دون غيره إلى وقوع الجريمة. ويمكن القول بأنه يشترط لمُساءلة الفاعل جنائياً في جريمة التحرش الإلكتروني ان يكون سلوكه هو الذي أدَّى إلى إحداث النتيجة الإجرامية المعاقب عليها مع وجوب التمييز بين جرائم الضرر وجرائم الخطر.

ووفقاً لما ذهب إليه المُشرع المصري بأن جريمة التحرش الإلكتروني تُعد من الجرائم البسيطة حيث يكفي لقيامها ممارسة الأنشطة والوظائف المنصوص عليها قانوناً ولو لمرة واحدة لقيام الجريمة في حق مرتكبيها ولا يتطلب لتمامها اعتياد اتيان الفعل وتكراره وذلك على خلاف ما ذهب اليه المُشرع الفرنسي الذي اعتبر هذه الجريمة من الجرائم التي تلزم لتمامها اعتياد اتيان الفعل وتكراره والقيام بأكثر من عمل من الاعمال المماثلة او المشابهة.

الشروع في الجريمة التحرش الإلكتروني:

يتجه التشريع المصري إلى إقرار العقاب على الشروع في الجريمة مع تحديد العقوبة ففرض للشروع عقوبة أخف ومن ناحية اخرى ميز المُشرع في تنظيم احكام العقاب على الشروع بين الجنايات والجنح فالشروع في الجنايات مُعاقب عليه دائماً مالم ينص على خلاف ذلك اما الجنح فيحددها القانون كقاعدة عامة ويحدد كذلك عقوبة الشروع.

وتُعد جريمة التحرش الإلكتروني من الجرائم التي لا شروع فيها بل تتم بمجرد القيام بقائمة اعمال تدخل في نطاق ما يرد من انشطة ولا تقوم هذه الجريمة بمجرد التحضير لهذه الأنشطة او التمهيد لها او محاولة الاتيان بها دون ان تقع بالفعل [2].

كما تعد جريمة التحرش الإلكتروني من الجرائم الشكلية التي يكفي لقيامها مجرد القيام بالنشاط المادي المُخالف وبمجرد ارتكاب السلوك الإجرامي ولم يشترط المُشرع تحقيق نتائج معينة او وقوع اضرار نتيجة ارتكاب هذا النشاط الإجرامي كما تُعد جريمة التحرش الإلكتروني من الجرائم الإيجابية وكذلك هي من الجرائم المستمرة.

---

[1] د/ محمود نجيب حسنى، علاقة السببية في قانون العقوبات طبعة نادى القضاة، مصر، 1984م ص5.

[2] Azy Barak, Sexual Harassment on the Internet, Social Science Computer Review, Vol. 23 No. 1, 2005, P 77

الفرع الثاني

الركن المعنوي في جريمة التحرش الإلكتروني

تمهيد:

يتشكل الركن المعنوي بالقصد الجنائي وهو الحالة النفسية للجاني والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني.

واساس الركن المعنوي يتمثل في العلاقة النفسية التي تربط بين شخصية الجاني وماديات ارتكاب الجريمة، وهو إدارة جريمة تستمد صفتها هذه من سيطرتها او اتجاهها إلى الماديات غير المشروعة التي تقوم عليها الجريمة [1].واصل هذه العلاقة هو الإرادة ولا يستطيع القانون تحديد المسؤليه عن الجرم المحظور إلا بعد قيام علاقة بين ذلك الفعل وشخص من الاشخاص وهي علاقة من نوع خاص كما يفترض الركن المعنوي توجه الإرادة نحو ماديات الجريمة وتتبلور ارادة الجاني في صورة القصد الجنائي وعلى اساسه تكون الجريمة عمدية والصورة الثانية الخطأ الغير العمدي وعلى اساسه تكون الجريمة غير عمدية [2].

ولقد خلت الكثير من جرائم التحرش الإلكتروني التي نص المُشرع على تجريمها من تحديد صورة الركن المعنوي الواجب توافرها فيها، وان هناك الكثير من الصعوبات التي تعترض اثبات هذا الركن لان افعال التحرش الإلكتروني قد تُرتكب في كثير من الصور بعيداً عن شخص الجاني وقد يصعب الوقوف عما إذا كان الجاني قد قصد بفعله الإضرار بالغير ام لا وقد تعجز النيابة العامة كسُلطة اتهام وتحقيق عن اثبات تسافر هذا القصد او الخطأ [3].

وسوف نوضح بالتفصيل الركن المعنوي بصورتيه في الفقرتين الآتيتين.

الفقرة الأولى: القصد الجنائي في جريمة التحرش الإلكتروني.

يُعد القصد الجنائي وهو الصورة الأكثر أهمية ويتوافر هذا القصد متى عُلِم الجاني بحقيقة الواقع المُجرمة التي يرتكبها وبعناصرها القانونية مع اتجاه إرادته إلى ارتكاب النشاط الإجرامي وتحقيق النتيجة من وراءه ويتحدد نطاقه على الجاني الواجب توافره في القصد باشتماله على أركان الجريمة وما يخرج عن هذه العناصر والأركان فلا يشترط علم الجاني به ويكون العلم بالقانون مفترضاً فلا يقبل الدفع من الجاني بأنه كان يجهل وجود نص يجرم فعله.

---

01 محمود نجيب حسنى، علاقة السببية في قانون العقوبات، مرجع سابق ص525.

02 المرجع السابق ص 526.

03 د. غنام محمد غنام، الوجيز في شرح قانون العقوبات مطبعة جامعة المنصورة والكتاب الجامعي مصر المنصورة 2008م ص 526.

ويتم مُعالجة القصد الجنائي في جريمة التحرش الإلكتروني على النحو الاتي:

1ـ العلم بالحق محل الحماية

يجب ان يحتاط الجاني المُتحرش الإلكتروني علماً بالحق محل الحماية القانونية فيجب ان يعلم الجاني كذلك بعناصر النشاط الإجرامي الذي يرتكبه عمداً أي ان من شأن جُرمه ان يُفضي إلى تحقيق النتيجة الإجرامية التي نص عليها القانون وتطبيقاً لذلك يجب ان يعلم الجاني ان من شأن فعله ان يؤدى إلى الخوض في اعراض المجني عليهم وانتهاك حُرماتهن المقدسة [1].

2ـ القصد الجنائي الخاص في جريمة التحرش الإلكتروني.

انصراف ارادة الجاني إلى تحقيق واقعة معينة لا علاقة لها بالركن المادي للجريمة وهو ما يسمى بالقصد الجنائي الخاص، وحين يستوجب المُشرع توافر قصد خاص في الجريمة فإن النتيجة التي تترتب على انتفاء هذا القصد تُعد انتقاء للجريمة نفسها إلا إذا كان المُشرع قد نص على تجريم الفعل المكون للجريمة تحت مُسمى اخر [2].

ولم يتطلب المُشرع في جريمة التحرش الإلكتروني توافر قصد خاص او نية خاصة فهي تقوم على اساس توافر القصد العام الذي يتكون من العلم والإرادة.

3ـ القصد المحدود والقصد الغير محدود

يكون القصد محدوداً إذا اتجهت إرادة الجاني إلى تحقيق النتيجة الإجرامية ويكون القصد الغير محدود إذا اتجهت إرادة الجاني إلى تحقيق النتيجة الإجرامية دون تحديد لنوعها، ولا يتمثل التفرقة بين نوعي القصد أهمية قانونية إذا يكفي توقع الجاني للنتيجة الإجرامية واتجاه إرادته إلى تحقيقها اما موضوع النتيجة واتجاه الإرادة إلى تحقيقها فيه فلا يُعتبر عُنصراً من عناصر القصد الجنائي [3].

وتتحقق اغلب جرائم التحرش الإلكتروني بتوافر القصد الغير محدود حيث تتجه إرادة الجاني إلى تحقيق خدش الحياة والدعوة إلى ارتكاب الفاحشة ولا يهم ما إذا كان هذا التعامل قد نال من الشرف والكرامة الإنسانية.

---

01 د/ غنام محمد غنام مرجع سابق ص 196.

02 محمود نجيب حسنى، علاقة السببية في قانون العقوبات، مرجع سابق ص 582.

03 د/ مأمون سلامة شرح قانون العقوبات "القسم العام والخاص"، دار سلامة للنشر والتوزيع، القاهرة، 2018، ص 313.

4ـ القصد المباشر والقصد الاحتمالي.

يكون القصد الجنائي مباشراً إذا اتجهت إرادة الجاني والمُتحرش الإلكتروني على نحو مؤكد إلى الاعتداء على الحق الذي يحميه القانون. ويكون القصد احتمالياً إذا توقع الجاني النتيجة الإجرامية كأثر محتمل للفعل المرتكب وعلى ذلك يرتكبها وإذا لم يتأكد الجاني من تحقق النتيجة كأثر لفعله الذي ارتكبه وانما مُجرد احتمال لديه بوقوعه مع توقعه ذلك ولكنه قبل ورغب في وقوع النتيجة [1]. لذلك يجب الاخذ بفكرة القصد الاحتمالي في جرائم التحرش الإلكتروني لِما يترتب على ارتكاب معظمها من اضرار معنويه محتملة بُحكم طبيعتها والتي يتعذر تفاديها او تداركها.

الفقرة الثانية: الخطأ الغير عمدي في جريمة التحرش الإلكتروني.

الصورة الثانية في جريمة التحرش الإلكتروني للركن المعنوي تتمثل في الخطأ غير العمدي ويقصد به إخلال الجاني عند تصرفه بواجبات اليقظة والحذر التي يُفرضها القانون ويترتب على ذلك عدم توقعه حدوث النتيجة وعدم حيلولته دون حدوثها في حين انه كان في استطاعته ومن واجبه ان يتوقها وان يحاول دون حدوثها.

ولتوافر الخطأ الغير عمدي يلزم تحقق عنصريين أولهم عنصر الإخلال بواجبات الحيطة والحذر التي يُفرضها القانون على الناس في تصرفاتهم والعنصر الثاني عنصر عدم التوقع لحدوث النتيجة التي يتمثل فيها الاعتداء على الحق محل الحماية او توقعها مع الاعتماد على قدراً غير كافياً للحيلولة دو حدوثها [2].

التمييز بين القصد الجنائي والخطأ الغير عمدي في جريمة التحرش الإلكتروني:

تبدو اهمية التمييز بين القصد الجنائي والخطأ الغير عمدي في جريمة التحرش الإلكتروني من أن التشريعات الجنائية لا تنص على مُعاقبة بعض الجرائم الا إذا كانت عمدية، ويختلف العقاب المُكرر على الجرائم اختلافاً كبيراً بحسب ما إذا كانت عمدية او غير عمديه. لذلك على المُشرع التدخل بالنص صراحة في جريمة التحرش الإلكتروني على صورة الركن المعنوي فيها سواء تمثل في العمد ام الخطأ.

---

[1] د/ محمود نجيب حسنى، قانون العقوبات – القسم العام – مرجع سابق ص 566.

[2] المرجع السابق ص 601.

المطلب الثالث

أركان جريمة التحرش الإلكتروني في الشريعة الإسلامية

تمهيد:

تُعرف الجريمة في الاصطلاح بأنها محظورات شرعية ونهي الله تعالى عنها بحد او تعزيز [1]. وجريمة التحرش الإلكتروني لا تتعدى كونها فعل عمدي يقع ضد إرادة المجني عليه وقد يستطيل إلى ما يُعد عورة، ولبيان جريمة التحرش الإلكتروني على نحوٍ يُسمح بتكوين صورة واضحة عنها فلابد من توافر أركان لهذه الجريمة.

اولاً: الركن الشرعي.

يتمثل الركن الشرعي في تجريم المُشرع لمجموعة من الأفعال وذلك بالنص عليها وتقرير عقوبة جنائية لمُقترفها فاذا لم تُجرم صراحة بالنص عليها من قِبل المُشرع أُعتبرت من الافعال المباحة التي لا مسئولية على مرتكبيها مهما كان استنكار المجتمع لها فالعبرة بموقف المُشرع وليس المجتمع او الراي العام وحيث ان التشريعات تتفاوت في تجريم التجاوزات الإلكترونية ما بين مضيق وموسع كما انها غير ثابتة في سياسة التجريم خلال الشريعة الإسلامية فأنه على ذلك اعتبار الجريمة الإلكترونية من قبيل الجرائم النسبية فهي تكتسب صفة التجريم داخل النطاق الزماني والمكاني.

وهذا يعنى ان ما يعد جريمة في ظل تشريع معين قد يكون فعلاً مباحاً في ظل تشريع اخر مهما كان ماساً بالأعراض او مُخدشاً لمشاعر الحياة ومهما اتصف بالشذوذ او الانحراف [2]. ويتضح لنا هذا الركن في جريمة التحرش الإلكتروني بالتحديد من خلال النص التشريعي الذي يحدد ما إذا كان الفعل داخلاً في دائرة العقاب ام لا جريمة ولا عقوبة إلا بنص شرعي وتكون على شقين هما على النحو الاتي:

1- شق التكليف: ما يعتبره المُشرع جريمة من افعال ايجابية كانت او سلبية والفعل السلبي هو الامتناع حيث يتضمن هذا الشق وصفاً دقيقاً لسلوك المُجرم بحيث لا يختلط بغيره ولا يتداخل مع غيره من الافعال ولهذا يشترط ان يتطابق الفعل المرتكب في أي جريمة مع الفعل المحدد في شق التكليف تطابقاً تاماً حتى تقوم الجريمة.

2- شق الجزاء: ويتحقق هذا في حالة مُخالفة المُكلف لِما ألقاه عليه المُشرع من تكليف إيجابي كان هذا التكليف ومِثاله عدم إيذاء الغير او الاعتداء على ماله وقد

---

[01] الماوردي، الأحكام السُلطانية والولايات الدينية. المكتب الإسلامي للطباعة والنشر 1996م ص258.
[02] د/ منصور رحماني، علم الإجرام والسياسة الجنائية، الجزائر ،2006م، ص 110.

يتمثل الجرائم على شكل عقوبة كما قد يتمثل كتدبير وقائي [1]. وقد نصت الشريعة الإسلامية على تحريم التحرش الإلكتروني وتجريمه فقد جاء في القران الكريم قوله تعالى: ((وَلَا تَقْرَبُوا الزِّنَا ۖ إِنَّهُ كَانَ فَاحِشَةً وَسَاءَ سَبِيلًا)) [2].

والنهى عن الزنا وعن كل ما يقرُب إليه هو ايضاً نهى عن التحرش الإلكتروني ويلزم ان يكون تحريم الشريعة الإسلامية بالفعل نافذاً وقت ارتكاب الجريمة وذلك بأن يكون النص على التحريم سابقاً على ارتكاب الجريمة وان يكون التحريم سارياً على شخص الجاني مُرتكب هذه الجريمة [3] وإذا بلُغت الجريمة مرحلة التنفيذ وجب عندها ان يتوافر لها رُكنان لوجوب العقاب عليها وهما الركن المادي والركن المعنوي.

ثانياً: الركن المادي.

وهو اقتراف الفعل المُكون للجريمة والركن المادي لجريمة التحرش الإلكتروني يتحقق بإتيان الجاني لفعل مُنافِ للشريعة الإسلامية سواء وقع على جسم المجني عليه ام مجرد اصابه الكرامة والعفة الذاتية، ويجب ان تكون هناك إرادة لفعل التحرش الإلكتروني والاعداد لها والسعي لتنفيذها والاقبال على ارتكابها وتنفيذها وهذا الفعل التحرش الإلكتروني لابد من تتوافر له شروط في التحرش والمُتحرش به.

ثالثاً: الركن المعنوي

وهي نية التحرش او القصد ويتكون من إرادة الفعل والعلم به ويُقصد بذلك ان يتوفر لدى مرتكب فعل التحرش الإلكتروني النية او العمد على اتيان الفعل مع العلم بانه قد تصل النية للزنا او اللواط.

ويجب ان يكون المُتحرش عالماً بما يفعل اثناء قيامه بالتحرش ويجب ان تتجه إرادة المُتحرش نحو ارتكاب فعل التحرش الإلكتروني وإذا أُكره على ذلك فلا حد عليه ولا تعزيز.

لقول الله تعالى: (فَمَنِ اضْطُرَّ غَيْرَ بَاغٍ وَلَا عَادٍ فَلَا إِثْمَ عَلَيْهِ ۚ إِنَّ اللَّهَ غَفُورٌ رَّحِيمٌ)

ولقول الرسول (ص) ان الله وضع عن امتى الخطأ والنسيان وما استكرهوا عليه [4].

---

01 عبد الفتاح مصطفي الصيفي، الاحكام العامة للنظام الجنائي في الشريعة الاسلامية والقانون الوضعي، دار النهضة العربية، القاهرة ، 2001.ص133

02 سورة الإسراء الآية 32.

03 إسماعيل محمد رشدي، الجنايات في الشريعة الإسلامية دار الأنصار القاهرة ط1 1403هـ1983 ص88.

04 الندي سُنن الإمام ابن ماجه بن رشف ابى الحسن الحنفي رقم الحديث 2555 ج2ص3333 /محمد ناصر الدين صحيح سُنن ابن ماجه باختصار و سند مكتبة التربية العربي لدول الخليج الرياض ط3 (1408هـ — 1988م).

وإذا أُكره الرجل فلا حد عليه وهو الرأي الراجح في مذهب الإمام أبى حنيفة ومالك الشافعي وعند الحنابلة عليه الحد لا الوطء لا يكون إلا بالانتشار والاكراه شبه فيمنع الحد كما لو كانت امرأة[1].

والرأي الراجح في المذاهب جميعها انه لا عقوبة على الرجل إذا أكره لان الإكراه يتساوى امام الرجل والمرأة [2]. إذن فأركان جريمة التحرش الإلكترونية الخاصة للشريعة الإسلامية هي (المُتحرش -المُتحرش به -الفعل الجنائي)

أركان جريمة التحرش الإلكترونية في القانون الوضعي:

جريمة التحرش الإلكتروني تتكون من عدة اجزاء تتفاوت في اهميتها وتتحلل إلى أركان والأركان تتحلل إلى عناصر ثم إلى شروط، ويستلزم النموذج القانوني لكل عنصر شروطاً مختلفة تختلف من عنصر إلى اخر فالنموذج القانوني هو الشكل القانوني للجريمة الذي يضم كل الأركان اللازمة لقيام الجريمة التي لو تخلف أحدها لامتنع قيامها [3].

اولاً: الركن المادي لجرائم الإنترنت.

والركن المادي في جرائم التحرش الإلكترونية هو قيام الجاني بارتكاب الأفعال التي يؤثمها المُشرع كونها جريمة جنسية ماسة بالعرض او مشاعر الحياة سواء اكان فاعلاً أصلياً فيها وذلك بقيام الافعال التنفيذية او بوصفه شريكاً سواء بالتحريض او الاتفاق او المساعدة [4].

ان النشاط او السلوك المادي في جرائم الإنترنت يتطلب وجوده بيئة رقمية واتصال بالإنترنت ويتطلب ايضاً معرفة بداية هذا النشاط والشروع فيه ونتيجته، وليس كل جريمة تستلزم وجود اعمال تحضيريه وفي الحقيقة يصعب الفصل بين العمل التحضيري والبدء في النشاط الإجرامي في جرائم الكمبيوتر والإنترنت – حتى ولو كان القانون لا يعاقب على الاعمال التحضرية إلا انه في مجال تكنولوجيا المعلومات الامر يختلف الشيء فشراء برامج اختراق ومعدات لفك الشفرات وكلمات المرور وحيازة صورة دعارة للأطفال فمثل هذه الاشياء تمثل جريمة في حد ذاتها [5].

---

01 ابا قُدامه عبد الله بن احمد المغنى، الشرح الكبير دار الحديثي القاهرة ط 1425هـ 2004م ج12 ص138.

02 عبد القادر عوده التشريع الجنائي الإسلامي مرجع سابق ص365.

03 وزير عبد العظيم مُرسى، الشروط المُفترضة في الجريمة دراسة تحليلية تأصيلية دار النهضة القاهرة ط1983م ص 46.

04 انظر: محمد امين الرومي، جرائم الكمبيوتر والانترنت دار المطبوعات الجامعية 2003م ص182. وكذلك انظر: د/أحسن بوسقيه، الوجيز في القانون الجنائي الخاص، الجرائم ضد الاشخاص ولجرائم ضد الاموال دار هومه الجزائر 2005م ص 141.

05 اللواء الدكتور فؤاد جمال، الجرائم المعلوماتية، دار النشر ، مصر، 2011، ص13، بحث منشور على الرابط: www.wata.cc/forums/uploaded/72 وكذلك انظر د/ محمد على قطب الجرائم المعلوماتية وطرق مواجهتها الجزء الثاني مارس 2010 ص2.

ثانياً: الركن المعنوي في جرائم الإنترنت [1].

الركن المعنوي هو الحالة النفسية للجاني والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني وقد تنقل المُشرع الأمريكي في تحديد الركن المعنوي للجريمة بين مبدا الإرادة ومبدأ العلم فهو تارة يستخدم الإرادة كما هو الشأن واحياناً اخرى يأخذ بالعلم وبرزت تلك المشكلة في قضية موريس الذي كان متهماً في قضية دخول غير مصرح به على جهاز حاسب فيدرالي وقد دفع محامى موريس على انتقاء الركن المعنوي الامر الذي جعل المحكمة تقول هل يلزم ان يقوم الادعاء بإثبات القصد الجنائي وجُرمية الدخول غير المصرح به بحيث تثبيت نية المتهم في الولوج إلى حاسب فيدرالي ثم يلزم اثبات نية المتهم في تحدى الحظر الوارد على استخدام نظم المعلومات في الحاسب وتحقيق خسائر ومثل هذا إلى تحديد أركان جريمة الدخول دون تصريح وبذلك ذهبت المحكمة إلى تبنى معيارين هنا هما الإرادة بالدخول غير المصرح به وكذا معيار العلم بالحظر الوارد على استخدام نظم المعلومات الفيدرالية دون تصريح.

اما بالنسبة للقضاء الفرنسي فإن منطق سوء النية هو الأعم في شأن جرائم الإنترنت حيث يشترط المُشرع الفرنسي وجود سوء نية في الاعتداء على بريد إلكتروني خاص بأحد الاشخاص [2].

---

[01] د/ عبد الفتاح بيومي حجازي مكافحة جرائم الكمبيوتر والإنترنت مرجع سابق ص394/391. وانظر د/ محمود محمود مصطفي شرح قانون العقوبات القسم الخاص دار النهضة العربية القاهرة 1999م -ص419.

[02] اللواء الدكتور فؤاد جمال، الجرائم المعلوماتية مرجع سابق 14ص.

المبحث الثاني:

المسئولية الجنائية عن جريمة التحرش الإلكتروني كجريمة إلكترونية

مع تطور وسائل الاتصالات وانفتاح العالم في تدفق المعلومات باستخدام الإنترنت وتوافر لحُرية انتقال هذه المعلومات، انتشرت معها بعض الانحرافات نتيجة لهذا التطور التكنولوجي الهائل. كإمداد مستخدمي الشبكة بالمعلومات المؤذية والضارة وغير المشروعة والممارسات والصور الغير أخلاقية كـأحد صور التحرش الإلكتروني.

يُعرف البعض الجريمة الإلكترونية بأنها تلك الجريمة التي تكون معرفة بالحاسب أو استخدامه شرطاً ضرورياً لارتكابها أو هي فعل غير مشروع تكون المعرفة بتقنية المعلومات إساءة لمرتكبه بينما ذهب البعض إلى أن تعريف الجريمة الإلكترونية إنما يرجع إلى محل هذه الجريمة كما أنه غير مُتعلق بالوسيلة التي تُنفذ به حيث يرى هؤلاء بأن الجريمة الإلكترونية هي الجريمة التي موضوعها أو محلها المعلومات دون اعتبار لِما إذا كان الحاسب الآلي والوسيلة المستخدمة في ارتكاب الجريمة من عدمه على ذلك فقد عرف البعض الجريمة الإلكترونية بأنها كل فِعل غير مشروع موجه لنسخ أو تغيير أو حذف أو وصول المعلومات المُخزنة داخل الحاسب أو التي تحول عن طريقه، بينما عرفها البعض الأخر بأنها: كل غش معلوماتي ينصرف إلى كل سلوك غير مشروع يتعلق بالمعلومات المعالجة ونقلها.

وهي كل عمل يأتيه الأنسان ويُحدث إضراراً بمكونات الحاسب المادية والمعنوية وشبكات الاتصال الخاصة به يمكن اعتبارها من المصالح والقيم المتطورة التي تمتد لحمايتها مظلة قانون العقوبات وثمة تعريف آخر: هي كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع للتقنية المعلوماتية بهدف الاعتداء على الأموال المادية والمعنوية. وتتعدد أوجه التشابه بين الجريمة الإلكترونية والجريمة التقليدية في أطراف الجريمة من مُجرم ذي دافع لارتكاب الجريمة وضحية قد يكون شخص طبيعي أو شخص اعتباري وأداة ومكان الجريمة وهنا يكمن الاختلاف الحقيقي بين نوعي الجريمة ففي الجريمة الإلكترونية الأداة ذات تقنية عالية وايضاً مكان الجريمة الذي لا يتطلب انتقال الجاني إليه انتقالاً فيزيقياً ولكن في الكثير من تلك الجرائم أن الجريمة تتم عن بعد باستخدام خطوط وشبكات الاتصال بين الجاني ومكان الجريمة[1].

ولأجل إزالة اللبس سنتناول في هذا المبحث المسئولية الجنائية عن جريمة التحرش الإلكتروني كجريمة إلكترونية من خلال المطلبين التاليين على نحو الاتي:

المطلب الأول: المسئولية الجنائية للجاني.
المطلب الثاني: المسئولية الجنائية لمزود الخدمة ومتعهد الإيواء (المستضيف).

---

[01] اللواء الدكتور فؤاد جمال، الجرائم المعلوماتية مرجع سابق ص4.

المطلب الأول

المسئولية الجنائية للجاني

أولاً: سمات المُجرم الإلكتروني:

لقد تنازعت الدراسات التي تُحدد المُجرم وشخصيته ومدى جسامة جُرمه كأساس لتبرير وتقدير العقوبة ويكمن السؤال في حالتنا تلك كيف يمكن تبرير وتقدير العقوبة في حالة مُجرم الكمبيوتر والإنترنت وهل هناك نموذج مُحدد للمُجرم المعلوماتي بالتأكيد لا يمكن أن يكون هناك نموذج مُحدد للمُجرم المعلوماتي وأن هناك سمات مُشتركة بين هؤلاء المُجرمون ويمكن اجمال تلك السمات فيما يلي [1]:

1 - مُجرم متخصص: له قدرة فائقة في المهارة التقنية ويستغل مداركه ومهاراته في اختراق الشبكات وكسر كلمة المرور أو الشفرات ويسبح في عالم الشبكات ليحصل على كل غالى وثمين من البيانات والمعلومات الموجودة على اجهزة الحواسب وخلال الشبكات.

2- مُجرم عائد للإجرام: يتميز المُجرم المعلوماتي بأنه عائد للجريمة دائماً فهو يوظف مهاراته في كيفية عمل الحواسيب وكيف تخزين البيانات والمعلومات والتحكم في أنظمة الشبكات في الدخول غير المُصرح به مرات ومرات فهو قد لا يحقق جريمة الاختراق بهدف الايذاء وإنما نتيجة شعوره بقدراته ومهارته في الاختراق.

3- **مُجرم محترف:** له من القدرات والمهارات التقنية ما يؤهله ليوظف مهاراته في الاختراق والشر والنصب والاعتداء على حقوق الملكية الفكرية وغيرها من الجرائم مقابل المال.

4- مُجرم ذكي: حيث يمتلك هذا المُجرم من المهارات ما يؤهله أن يقوم بتعديل وتطوير في الأنظمة الأمنية حتى لا تستطيع أن تلاحقه وتتبع اعماله الإجرامية من خلال الشبكات أو داخل اجهزة الحواسيب.

ثانياً: المسئولية الجنائية عن المجرم الإلكتروني:

ويتمثل أساس المسئولية الجنائية سواء كانت الجريمة تقليدية او إلكترونية في الالتزام القانوني بتحمل التبعية فهي تنشأ تابعة لالتزام أخر وهو في حقيقته واجب اصلى فللمسئولية الجنائية رُكنان اساسيان الأول هو الرابطة المادية بين الواقعة والنشاط المادي أي الإسناد المادي من جهة والثاني هو الرابطة المعنوية بين الشخص والسلوك فإن كانت أساس المسئولية الجنائية والقاعدة العامة فيها شخصية، كان كل إنسان لا

[01] اللواء الدكتور فؤاد جمال، الجرائم المعلوماتية مرجع سابق ص12.

يُسأل إلا عن أعماله وسلوكه، فالمسؤولية الجنائية عن الغير تأخذ بالمسؤولية الجنائية المُفترضة على أساس تضامني؛ فمثلاً يعتبر رئيس التحرير الفاعل الأصلي في الجرائم المرتكبة بواسطة النشر وهى المسؤولية الجنائية المفترضة على أساس تضامني استناداً إلى علم رئيس التحرير بالمضمون المنشور في الصحيفة واعتباره الفاعل الأصلي وكل من يساهم فيها يُعد فاعلاً أو شريكاً حسب القواعد العامة بحيث لا يُسأل شخص بينهم ما دام يوجد من قَّدمه عليه القانون في ترتيب المسؤولية الجنائية وهى ما تسمى بالمسؤولية المتتابعة [1].

والقصد الجنائي أو قصد العيان هو تعَّمُد إتيان العمل المُحرم أو تركه مع العلم بأن المُشرع يُحرم الفعل أو يؤُجبه وينبغي أن لا يفوتنا إدراك الفرق بين العُصيان وبين قصد العُصيان فالعُصيان عنصر ضروري يجب توفره في كل جريمة سواء كانت الجريمة بسيطة ام جسيمه ومن جرائم العمد أو من جرائم الخطأ فإن لم يتوفر عنصر العُصيان في الفعل فهو ليس جريمة اما قصد العُصيان فلا يجب توفره إلا في الجرائم العمدية من دون غيرها والعُصيان هو فعل المعصية أي إتيان الفعل المحرم والامتناع عن الفعل الواجب دون أن يقصد الفاعل العُصيان كمن يلقى حجراً من نافذة ليتخلص منه فيصيب به ماراً في الشارع فأنه يأتي معصيه بإصابة غيره ولكنه لم يقصد بأي حال أن يُصيب غيره ولم يقصد فعل المعصية اما قصد العُصيان فهو أتجاه نية الفاعل إلى الفعل أو الترك مع علمه بأن الفعل أو الترك مُحرم أن هو فعل المعصية بقصد العُصيان كمن يلقى حجراً من نافذة قاصداً إصابة شخصاً ماراً في الشارع فيُصيبه فأنه يرتكب معصية لم يأتها إلا وهو قاصد فعلها ويتفق هذا المثل مع المثل السابق في أن كل من الجانيين أتى معصية حرمها الشارع ويختلف المثلان في أن الجاني في المثل الثاني قصد إتيان المعصية بينما الجاني في المثل الأول لم يقصد إتيان المعصية [2].

---

[1] د/ هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة أسيوط 1992م ص5.

[2] عبد القادر عوده، المسئولية الجنائية في الشريعة الإسلامية والقوانين الوضعية مرجع سابق ص 409.

المطلب الثاني

المسئولية الجنائية لمزود الخدمة ومتعهد الإيواء (المستضيف).

تمهيد:

تتعدد طرق الوصول إلى الإنترنت إلا أنه في كافة الأحوال يجب وجود مُقدِم خدمة ولقد أثارت الكثير من الجدل مسألة اعتبار مُقدِم الخدمة فاعل أصلى في الجريمة فيرى بعض الفقهاء أنه على أُسس المسئولية التوجيهية فأنه يتعين على مُقدِم الخدمة منع نشر محتوى صفحات الشبكة المتعارضة مع القوانين والنظم واللوائح والمصلحة العامة [1].

ولكن انتُقِد هذا الرأي فلا يُعد مُقدِم الخدمة مسئولاً عن محتوى المعلومة فمسئولية مُقدِم هذه الخدمة مسئولية تعاقدية فقط وذلك في حالة عدم تنفيذ التزامه بتمكين العميل من الدخول للشبكة ولأنه لا يملك الوسائل الفنية التي تُمكنه من الرقابة على صحة هذه المعلومات ومشروعيتها وقد يضع مُقدِم الخدمة شروط تعفيه من المسئولية أو تُحد منها ومن أمثلة الشروط المُحددة للمسئولية، الاتفاق على حد اقصى للتعويض وفي جميع الأحوال فأنه يُلزم في حالة عدم تنفيذ العقد برد قيمة اشتراك الخدمة.

وتقوم مسئولية مُقدِم خدمة الإنترنت فضلاً عن القواعد العامة من المسئولية إذا وقع خطأ في إبلاغ الرسالة الإلكترونية إلى المُرسل إليه ناتج عن سبب راجع إلي مُقدِم الخدمة أو أحد العاملين لديه كما تقوم مسئوليته إذا انتُهكت سرية المُراسلات والمُكاتبات والاتصالات الإلكترونية ما لم يكن تدخله يبرره الضرورة الفنية لتشغيل الشبكة وليس سبب أخر وفي حال تعسفه في معالجة البيانات المعلوماتية الاسمية يمكن أن يُسال جنائياً فضلاً عن مسئوليته المدنية له بسبب معالجته الخاطئة تسبب في ضرر للغير.

ويُعتبر الوصول للمُجرم المعلوماتي أو الإلكتروني يُشكل عبء فني وتقني بالغ على القائمين بأعمال التتبع والتحليل لملابسات الوقائع الإجرامية المُختلفة وقد نصت المادة 12 من معاهدة بودابست لمُكافحة جرائم الفضاء المعلوماتية والتي لم تكن الولايات المتحدة طرفاً فيها وسارعت بالانضمام اليه بعد احداث الحادي عشر من سبتمبر تنص على [2].

البند 1: سوف يتبنى كل طرف تدابير تشريعية وأي تدابير أخرى لضمان قيام مسئولية الأشخاص المعنوية عن أي جريمة موثَّقة في هذه المعاهدة إذا ما ارتُكِبت لصالح الشخص المعنوي بواسطة شخص طبيعي اقترافه بشكل مُنفرد أو بصفة جزء

---

[1] د/ محمد حسين منصور، المسئولية الإلكترونية الناشر دار الجامعة الجديدة الإسكندرية 2003م ص20.

[2] اللواء الدكتور فؤاد جمال، الجرائم المعلوماتية مرجع سابق ص13 /14.

من عضو في الشخص المعنوي على أساس من تفويض من الشخص المعنوي سُلطة اتخاذ قرارات لصالح الشخص المعنوي سُلطة لممارسة رقابة أو سيطرة داخل الشخص المعنوي.

البند 2: إلى جانب الحالات الواردة في البند 1 سوف يتخذ كل طرف التدابير اللازمة لضمان قيام مسئولية الشخص المعنوي إذا ما أدَّى نقص الإشراف أو السيطرة من قِبل الشخص الطبيعي المُشار اليه في الفقرة 1 إلى إمكانية ارتكاب جريمة قائمة طبقاً لهذه المُعاهدة لصالح الشخص المعنوي بواسطة شخص طبيعي اقترافها تحت سيطرته.

البند 3: هذه المسئولية لن تُأثر على قيام المسئولية الجنائية للأشخاص الطبيعيين الذين اقترفوا الجريمة.

الإطار القانوني لجرائم تقنية المعلومات.

- قانون الأحوال المدنية رقم 143لسنة 1994م.
- قانون الطفل رقم 12 لسنة 1996 والمعدل برقم 126 لسنة 2008م.
- قانون حماية الملكية الفكرية رقم 82 لسنة 2002م.
- قانون الاتصالات رقم 10 لسنة 2003م.
- قانون التوقيع الإلكتروني رقم 15 لسنة 2004م.

1. قانون الأحوال المدنية رقم 143لسنة 1994م.

تنص المادة 72 من قانون الأحوال المدنية على عقوبة الحبس مدة لا تتجاوز ستة أشهر وبغرامة لا تزيد عن خمسمائة جُنيهاً أو بإحدى هاتين العقوبتين لكل من اطلع أو شَرع في الاطلاع أو حصل أو شَرع في الحصول على البيانات أو المعلومات التي تحتويها السجلات أو الحاسبات الألية أو وسائط التخزين المُلحقة بها أو قام بتغيرها بالإضافة أو الحذف أو بالإلغاء أو التدمير أو بالمساس بها بأي صورمن الصور أو إذاعتها أو افشائها في غير الأحوال التي نص عليها القانون ووفقاً للإجراءات المنصوص عليها فيه. فإذا وقعت الجريمة على البيانات أو المعلومات أو الاحصاءات المجمعة تكون العقوبة السجن.

2. قانون الطفل رقم 12 لسنة 1996 والمعدل برقم 126 لسنة 2008.

المادة 116 مُكرر يُعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن عشرة الأف جنيه ولا تجاوز خمسين ألف جنيه كل من استورد أصدر أو أنتج أو اعد أو عرض أو طبع أو روج أو أنحاز أو بث أي اعمال إباحية يشارك فيها اطفال أو تتعلق بالاستغلال الجنسي للأطفال ويحكم بمصادرة الادوات والآلات المستخدمة في ارتكاب الجريمة والأموال المُتحصلة منها وغلق الاماكن محل ارتكابها مدة لا تقل عن ستة أشهر وذلك كله مع عدم الاخلال بحقوق الغير الحسن النية.

ومع عدم الاخلال بأي عقوبة اشُيد بنص عليها في قانون أخر يُعاقب بذات العقوبة كل من استخدم الحاسب الآلي أو الإنترنت أو شبكات المعلومات أو الرسوم المتحركة لإعداد أو لحفظ أو لمعالجة أو لعرض أو لطباعة أو لنشر أو لترويج أنشطة أو اعمال إباحية تتعلق بتحريض الأطفال أو استغلالهم في الدعارة والاعمال الإباحية أو التشهير بهم أو بيعهم.

واستخدام الحاسب الآلي أو الإنترنت أو شبكات المعلومات أو الرسوم المتحركة لتحرض الأطفال على الانحراف أو لتسخيرهم في ارتكاب جريمة أو على القيام بأنشطة أو اعمال غير مشروعة أو مُنافية للآداب ولو لم تقع الجريمة فعلاً.

3. قانون حماية الملكية الفكرية رقم 82 لسنة 2002.

جُرم المُشرع في المادة 181 من ذلك القانون نشر مُصنف أو تسجيل صوتي أو برنامج إذاعي أو اداء محمى عبر اجهزة الحاسب الآلي أو شبكات الإنترنت أو شبكات الاتصالات أو غيرها من الوسائل بدون إذن كتابي مُسبق من المؤلف أو صاحب الحق المجاور وعاقب المُشرع على مُخالفة هذه المادة بالحبس مدة لا تقل عن شهر وبغرامة لا تقل عن خمسة الأف جُنيهاً ولا تجاوز عشرة ألاف جنيه أو احدى هاتين العقوبتين.

وفي حالة العودة تكون العقوبة الحبس مدة لا تقل عن ثلاثة أشهر والغرامة لا تقل عن عشرة الأف جنيه ولا تجاوز خميسنا ألف جُنيهاً. وفي جميع الأحوال تقضى المحكمة بمصادرة النسخ محل الجريمة أو المتحصلة منها وكذلك المُعدات والادوات المستخدمة في ارتكابها. ويجوز للمحكمة عند الحكم بالإدانة أن تقضى بغلق المنشأة التي استغلها المحكوم عليه في ارتكاب الجريمة مدة لا تزيد على ستة أشهر. وتقضى المحكمة بنشر ملخص الحكم الصادر بالإدانة في جُرمه يومياً أو أكثر على نفقة المحكوم عليه.

4. قانون الاتصالات رقم 10 لسنة 2003.

جَّرم المُشرع في المواد من 70 وحتى 86 من القانون: إنشاء الشبكات والبث وتقديم خدمات الاتصالات بدون ترخيص وتمرير المكالمات والتعدي على البنية الأساسية للاتصالات كما جَّرم الازعاج والمضايقة بإساءة استخدام الاتصالات ومن امثلتها السب والتهديد والتشهير ونشر الصور عبر الإنترنت.

جُرم كذلك نشر وإذاعة معلومات عن العمل تؤدى لقيام منافسة غير مشروعة والعقوبات تبدأ بالحبس وغرامة لا تقل عن خمسة الأف وخمسمائة جُنيهاً حالة الإهمال وحتى السجن وغرامة مائة ألف جُنيهاً. وتتمثل العقوبات التكميلية في الإزالة والمصادرة ووقف الترخيص مؤقتا أو إلغائه.

مادة 86 يُعاقب المسئول عن الإدارة الفعلية للشخص الاعتباري بذات العقوبات المقررة عن الأفعال التي تُرتكب بالمخالفة لأحكام هذا القانون إذا ثُبت علمه بها وكان إخلاله بالواجبات التي تفرضها عليه تلك الإدارة قد أسهم في وقوع الجريمة. ويكون الشخص الاعتباري مسئولاً بالتضامن عن الوفاء بما يحكم به من عقوبات مالية وتعويضات.

5. قانون التوقيع الإلكتروني رقم 15 لسنة 2004.

تضمن قانون التوقيع الإلكتروني مواد قانونية تُجَّرم الاعتداء على اجهزة الحاسب الآلي سواء باستخدام الإنترنت أو بغير ذلك من الوسائل.

وعاقب قانون التوقيع الإلكتروني بالمادة 23 فقرة 1(أ-ب-ج-هـ) بالحبس من اربعة وعشرون ساعة إلى ثلاث سنوات وغرامة من عشرة الأف جُنيهاً إلى مائة ألف جُنيهاً على كل من أصدر شهادة تصديق بدون ترخيص وكل من اتلف أو استعمل أو حصل بغير حق على توقيع أو وسيط أو محرراً إلكترونياً معيباً أو مزوراً مع علمه بذلك.

كما أن القانون شدد العقوبة في حالة العودة بالإضافة للنشر في جريدتين يوميتين واسعتي الانتشار وعلى شبكة المعلومات الإلكترونية المفتوحة على نفقة المحكوم عليه. كما عاقب المسئول عن الإدارة الفعلية للشخص الاعتباري بذات العقوبة إذا أسهم اخلاله في وقوع الجريمة مع علمه بذلك بالإضافة لتضامنه في أداء الغرامات والتعويضات متيتمة باسم ولصالح الشخص الاعتباري مادة 24 بالإضافة لوقوف أو الغاء الترخيص مادة 26.

مسئولية مُقدِمي خدمة الوصول للإنترنت [1].

تتعدد طرق الوصول إلى الإنترنت سواء على طريق Dial up leased line IDSL IDsالا أنه في كل الأحوال يجب وجود مُقدِم خدمة Internet service provider ولقد اثارت مسألة مُقدِم الخدمة باعتباره فاعل الخدمة أصل في الجريمة الكثير من الجدل ويرى اتجاه من الفقهاء عدم مسئوليته تأسيساً على أن عمله فني وليس في مقدوره مراقبة المحتوى المُقدَم ولا متابعة تصرفات مستخدم الإنترنت.

ويرى الاتجاه الثاني مُسائلته تأسيساً على أساس المسئولية التوجيهية فأنه يتعين على مُقدِم الخدمة منع نشر محتوى صفحات الشبكة المتعارضة مع القوانين والنُظم واللوائح أو المصلحة العامة [2].

ويذهب القضاء الفرنسي أن مجرد قيام مُستخدم الشبكة ببث رسالة غير مشروعة لا يكفي لقيام مسئولية مُقدِم خدمة الإنترنت وذلك أُخذ في الاعتبار العدد اللانهائي للمشتركين وحجم الرسائل الرهيب المتداول يومياً.

مسئولية مُقدِم مُتعهد الاستضافة [3].

مُقدِم خدمة الاستضافة هو الشركة التي تستضيف موقع على الإنترنت على خوادمها ويكون مُقدِم الخدمة مؤجر وصاحب الموقع مُستأجر لمساحة معينة على الجهاز الخادم الخاص بالشركة والمستخلص من احكام القضاء والفقه المقارن قيام مسئولية مُتعهد أو مُقدِم خدمة الاستضافة إذا كان يعلم أو كان عليه أن يعلم بالجريمة ولم يأخذ الإجراءات اللازمة لوقفها.

والسؤال المطروح في هذا الصدد هو عن نوع المسؤولية الجنائية لوسطاء تقديم خدمات شبكة الإنترنت فإذا كانت شبكة الإنترنت وسيلة من وسائل النشر والعلانية مما لا تُثار معه صعوبة في إمكانية تطبيق الاحكام القانونية لجرائم السب والتشهير فإن الجدل القانوني يُثار بالنسبة لتحديد المسؤولين جنائياً عن سلوك المرتكب في الفضاء الإلكتروني وحصر المساهمين فيه فمنهم الاشخاص القائمين على تشغيل الشبكة وخدماتها المعتمدة.

ولقد أصبحت الشبكة العالمية اليوم تضم مجموعة من الأنشطة والخدمات المختلفة فهي بنية تحتية للاتصالات اهم خدماتها البريد الإلكتروني E-mailوالمنتديات والناقل TransForce Protocol FTBلنقل الملفات بين ارجاء الشبكة ووسيلة

---

[1] 0 اللواء الدكتور فؤاد جمال، الجرائم المعلوماتية مرجع سابق ص15 للمزيد حول مسئولية مقدمي الخدمة.

[2] 0 احمد قاسم فرح، النظام القانوني لمقدمي خدمات الأنترنت بحث منشور على مجلة المنارة الإلكترونية المجلد 13 ال عدد9 تاريخ النشر 2005/5/27م ص358.

[3] 0 اللواء الدكتور فؤاد جمال الجرائم المعلوماتية مرجع سابق ص 15.

المتصل TELNET وهو برنامج الذي يتيح لأي شخص استخدام ومميزات حاسوبية موجودة في جهاز أخر بعيد ولا توجد في جهاز المستخدم اما شبكة المعلومات WWW فهي إحدى خدمات الشبكة من صفحات مصححة بلغة HTML التي تتيح إمكانية ربط الصفحات بالوسائط Links وهو سر تسميتها بالشبكة العنكبوتية [1].

فمن هم هؤلاء الوسطاء ما الدور الذي يلعبه كل وسيط من علاقته بالمضمون المنشور على الشبكة؟

فمزود الخدمة I.S.P هو شخص يمد المستخدمين بالقدرة على الاتصال بواسطة أنظمة الحاسب الآلي أو يقوم بمعالجة البيانات وتخزينها بالنيابة عن هؤلاء المستخدمين وهو ما نصت عليه المادة واحد من اتفاقية بودابست 2001 بشأن جرائم الإنترنت فمزود الخدمة هو من يُمكِن المشتركين من ووصول إلى شبكة الإنترنت عن طريق مدهم بالوسائل الفنية اللازمة الوصول إلى الشبكة بمقتضى عقد توصيل الخدمة فهو لا يقوم بتوريد المعلومة أو تأليفها ولا يملك أي وسائل فنية لمُراجعة مضمونها. فدوره فني فقط يتمثل في نقل المعلومات على شكل حزم إلكترونية عن طريق حساباته الخادمة فهل يجوز اعتباره أحد المسئولين على الجريمة المعلوماتية هنا ظهر اتجاهان نعرضهما تباعاً.

اولاً: الاتجاه القائل بعدم مسئوليه المزود

قد استند هذا الاتجاه إلى أن مزود الخدمة لا يملك القدرة على التحكم في أي مضمون يُبث على الشبكة والقول بتقرير مسئوليته هنا يُناظر القول بمُساءلة مدير مكتب البريد والهواتف على مدى مشروعية الخطابات والمكلمات التي تجرى عبر هذا الخط. بل أن المسالة قد تنتهي بنا إلى تقرير مسؤولية الجهات العامة وعلى توفير محطات التقوية لبث القنوات الفضائية المرئية ولتقرير مسؤولية مزود الخدمة يتطلب أن يكون دوره أكثر ايجابية في بث المادة المُجرمة فضلاً عن أنه لا يملك وسائل الفنية التي تُمكنه من مراقبة تلك المعلومات المتدفقة بأعداد تتجاوز الملايين [2].

ثانياً: الاتجاه القائل بتقرير مسؤولية مزود الخدمة.

أنقسم أنصار هذا الاتجاه إلى فريقين الأول يُنادى بتقرير المسؤولية الجنائية طبقاً لأحكام المسؤولية المتتابعة والثاني يذهب إلى تقرير المسؤولية طبقاً لأحكام العامة للمسؤولية الجنائية.

---

[01] فهد بن عبد الله الحيدان، الأنترنت شبكة المعلومات العالمية الطبعة الأولى الناشر مكتبة الملك فهد الوطنية الرياض 1996 ص 32 وما بعدها.

[02] مدحت رمضان جرائم الاعتداء على شخص الأنترنت دار النهضة العربية القاهرة 2000 ص 69/57

1. مُساءلة مزود الخدمة طبقاً لأحكام المسؤولية المتتابعة [1].

يبدو لأول وهلة استجابة الدور الذي يقوم به مزود الخدمة لهذا النظام استناداً إلى مساهمته في عملية النشر وتحقيق العلانية ووضعها في متناول المستخدمين إلا أن المسؤولية المتتابعة في مجال النشر بالنسبة للمؤلف والناشر تقوم على أساس العلم المُسبق بما تم إعلانه ونشره وهو ما يوجب التزام الناشر أو رئيس التحرير لمراقبة ما يُنشر والتزامه بالمسئولية المتتابعة.

مما لا يتوفر بالنسبة لمزود الخدمة خاصة عند قيام بالربط اثناء المنتديات المختلفة حيث يقوم بتثبيت تلك المنتديات على جهازه الخادم وكل ما يصل لمزود الخدمة في هذه الحالات هي حزم من البيانات المشفرة وهو ما نصل معه إلى عدم قبول التطبيق احكام المسؤولية المتتابعة فمزود الخدمة لا يملك الوسائل الفنية والقانونية التي تمكنه من مراقبة المضمون الذي يُنشر ويتحرك على الشبكة.

2. مُساءلة مزود الخدمة طبقاً للأحكام العامة للمسؤولية الجنائية.

يستند اصحاب هذا الرأي إلى أن مُزود الخدمة لا يملك الوسائل الفنية اللازمة لمراقبة الصورة أو الكتاب الا أنه يملك الوسائل الفنية اللازمة لمنع الدخول إلى هذه المواقع مما يؤدى إلى تقديم المساعدة لأصحاب تلك المواقع عن طريق مدَّهم بالزائرين وهو ما تتحقق به المساهمة الجنائية التبعية بالمساعدة.

لكن يُعد هذا الرأي ايضاً محل النظر فالمساهمة الجنائية لا تقوم إلى بالأعمال السابقة أو المعاصرة للسلوك الإجرامي ولا تكون بالأعمال اللاحقة [2] اما مزود الخدمة فدوره يأتي لاحقاً لارتكاب الجريمة التي تحققت بكامل عناصرها على الشبكة قبل أن يبدأ دور مزود الخدمة [3].

هكذا نصل إلى صعوبة تطبيق فكرة العِلم المُسبق لأسباب فنية وقانونية فالأسباب الفنية تتمثل في عدم وجود الإمكانية لمراقبة المضمون المنشور قبل نشره اما الأسباب القانونية فترجع إلى عدم اختصاص مزود الخدمة بممارسة أي نوع من أنواع الرقابة التوجيه على ما يتم نشره لما في ذلك من تعارض والعديد من الضمانات الخاصة بحق المؤلف وحق الحياة الخاصة ولا يمكن قبول قيامها بأي دور وقائي على الأخرين.

---

[01] د/ شيماء عبد الغنى محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية دار الجامعة الجديدة الإسكندرية 2007 ص 178.

[02] د/ جميل عبد الباقي الصغير، الأنترنت والقانون الجنائي دار النهضة العربية 2001م ص 129. وكذلك احمد السيد عفيفي، الأحكام العامة للعلانية في قانون العقوبات دراسة مقارنة دار النهضة العربية القاهرة 2001 و2002 ص551/552.

[03] د/ جميل عبد الباقي الصغير، الأنترنت والقانون الجنائي دار النهضة العربية 2001م ص 132/134.

المبحث الثالث

الجهود الدولية لمُكافحة الجرائم الإلكترونية

تمهيد وتقسيم:

لوقوف الزحف الخطير لانتشار الجرائم الإلكترونية كظاهرة عالمية كان من الضروري البحث في كيفية ايجاد حلول فعالة واتخاذ تدابير وقائية منها وردعية لهذه الكوارث التقنية التي باتت تهدد اقتصاديات أمن واستقرار الدولة بعد تطور الجريمة الإلكترونية من اطارها الكلاسيكي المعروف إلى التقنية العلمية الحديثة لتصبح تجارة الكترونية رائجة وهوما اصطلح عليه بالاقتصاد الرقمي وهو ما تُفسره نسبة الشكاوى الرسمية التي اعتمدها المركز العالمي لشكاوى الإنترنت والتي كلفت سنة 2000 خسارة مادية فادحة قدرت بـ12 بليون دولار جراء النتائج التدميرية التي تسببت فيها فيروسات اتلاف البرامج المعلوماتية وقد قُدرت مُجمل الشكاوى الرسمية التي قدمها الضحايا للمركز ب 275.284 ألف شكوى.

وفي مصر خصص وزير الداخلية رقم 108 للتبليغ عن جرائم الإنترنت ولهذا ومن اجل حماية فعالة لبرامج المعلوماتية وقاعدة للبيانات يجب اعتماد السبل القانونية الوقائية من خلال الدخول اليها عن طريق كلمات مرور سرية يجتنب فيها استخدام كلمات سر مكونة من كلمات عادية مع الحرص على تغيرها دورياً كل شهر إن تطلب الأمر ذلك مع تكثيف برامج الرقابة على نوادي ومقاهي الإنترنت والعمل على ترصد وحجب المواقع الإباحية كما هو الحال بالمملكة العربية السعودية وتونس مع الاعتماد علي برامج خاصة مضادة للفيروسات التدميرية واستعمالها بشكل مستمر [1].

لأجل إزالة اللبس سنقسم هذا المبحث إلى ثلاث مطالب نخصص المطلب الأول القوانين الدولية والعربية التي ساهمت في مُكافحة الجريمة الإلكترونية وفي المطلب الثاني أدلة الإثبات الجرائم الإلكترونية في التشريعات العربية ونخصص مطلب الثالث والأخير التعاون الدولي للحد من الجريمة الإلكترونية. على نحو الاتي:

المطلب الأول: القوانين الدولية والعربية التي ساهمت في مُكافحة الجريمة الإلكترونية.

المطلب الثاني: أدلة اثبات الجرائم الإلكترونية في التشريعات العربية.

المطلب الثالث: التعاون الدولي للحد من الجريمة الإلكترونية.

---

1 0 أنظر: عبد الصبور عبد القوى، على الجريمة الإلكترونية والجهود الدولية للحد بحث منشور على الرابط

http://www.droitarab.com/2013/11/blog -27.html

المطلب الأول

القوانين الدولية والعربية التي ساهمت في مُكافحة الجريمة الإلكترونية

1. قانون البيانات السويدي عام 1973م:

تُعد السويد أول دول تسن تشريعات تضم جرائم الإنترنت أو جرائم المعلوماتية ولا سيما التزوير المعلوماتي اذ صدر قانون البيانات السويدي عام 1973م الذي عالج قضايا الدخول غير المشروع للبيانات الحاسوبية أو تزويرها أو تحويلها أو الحصول غير المشروع عليها.

2. قانون مُكافحة جرائم الحاسب الآلي والإنترنت الدنماركي 1985م.

وفي عام 1985 سنت الدنمارك أول قوانينها الخاصة بجرائم الحاسب الآلي والإنترنت التي شملت في فقراتها العقوبات المحددة بجرائم الحاسب الآلي كالتزوير المعلوماتي.

3. قانون مُكافحة التزوير والتزييف البريطاني 1986م.

اصدرت بريطانيا قانون مُكافحة التزوير والتزييف عام 1986م الذي شمل في تعاريفه الخاصة تعريف اداة التزوير وهي وسائط التخزين الحاسوبية المتنوعة أو أي اداة أخرى يتم التسجيل عليها سواء بالطرق التقليدية أو الإلكترونية أو باي طريقة أخرى.

4. قانون مُكافحة التزوير المعلوماتي الألماني 1986م.

سن المُشرع الألماني قانون مُكافحة التزوير المعلوماتي سنة 1986م.

5. القانون الفرنسي الخاص بالتزوير المعلوماتي 1988م.

اصدرت فرنسا في عام 1988م قانون رقم 19 الخاص بالتصدي للتزوير المعلوماتي.

6. اتفاقية الإجرام السيبيري الإجرام عبر الإنترنت عام 2001م.

صدرت هذه الاتفاقية عن المجلس الأوروبي ووقعت في العاصمة المجرية بودابست في 23 نوفمبر 2001م حيث وقعت عليها 30 دولة ولأهمية هذه الاتفاقية أنضم اليها العديد من الدولة من خارج المجلس الأوروبي وأبرز هذه الدول الولايات المتحدة الأمريكية التي صادقت عليها في 22 سبتمبر 2006م ودخلت حيز النفاذ في الأول من يناير 2007م واشتملت على عدة جوانب من جرائم الإنترنت بينها الإرهاب وعمليات تزوير بطاقات الائتمان ودعارة الأطفال.

7. قانون مُكافحة الجرائم الإلكترونية مواده مستحدثة ضمن احكام قانون الجزاء العماني بسلطنة عمان 2001م.

اصدرت سلطنة عمان جملة من التشريعات لمُكافحة الجريمة المعلوماتية تحت مسمى:

قانون سلطنة عمان لمُكافحة جرائم الحاسب الآلي فقد صدرت المرسوم السلطاني رقم 72 لسنة 2001م بشأن تعديل بعض احكام قانون الجزاء العماني ليشمل معالجة جرائم الحاسب الآلي وذلك بإضافة فصل في الباب السابع من قانون الجزاء العماني تحت عنوان جرائم الحاسب الآلي وكذلك أُضيفت مواد إلى قانون الاتصالات العماني تجرم تبادل وسائل تخدش الحياء العام وتُجرم استخدام اجهزة الاتصالات للإهانة والحصول على معلومات سرية أو إفشاء الأسرار أو إرسال رسائل تهديد، وسنت السلطنة قانونا ينظم المعاملات الحكومية الإلكترونية والتوقيع الإلكتروني وحوادث اختراق الأنظمة.

8. المعالجة القانونية للجريمة المعلوماتية في التشريع المغربي.

ادخل المُشرع المغربي الفصول التي تُعاقب على الأفعال التي تُشكل جرائم بعنوان المس بنظام المعالجة الألية للمُعطيات وذلك بموجب القانون رقم 7.003 الصادر بتاريخ 16 رمضان 1424هـ الموافق 11 نوفمبر 2003م.

9. قانون الامارات العربي الاسترشاد لمُكافحة جرائم تقنية المعلومات وما في حكمها.

اعتمده مجلس وزراء العدل العرب في دورته التاسعة عشرة بالقرار رقم 495-د19-2003/10/8م ومجلس وزراء الداخلية العرب في دورته الحادية والعشرين بالقرار رقم 417 – د 2004/21م.

10.قانون مُكافحة الجرائم المعلوماتية الإماراتي 2006م.

تُعد دولة الإمارات العربية أول دولة عربية تُسن قانوناً مُستقلاً لمُكافحة الجرائم المعلوماتية رقم 2 لسنة 2006م.

11.نظام مُكافحة الجرائم المعلوماتية السعودي 2007م.

سنت المملكة العربية السعودية نظام مُكافحة الجرائم المعلوماتية الذي أقره مجلس الوزراء الموقر برئاسة خادم الحرمين الشريفين الملك عبد الله بن عبد العزيز – نظام مُكافحة الجرائم المعلوماتية الصادر بالرسوم الملكي رقم م/17. وبتاريخ 1428/3/8هـ

بناء على قرار مجلس الوزراء رقم 79 وتاريخ 1428/3/7هـ الذي يهدف إلى الحد من نشوء الجرائم المعلوماتية وذلك بتحديد تلك الجرائم والعقوبات المقرر لها [1].

12.القانون العربي الاسترشاد للأثبات بالتقنيات الحديثة 2008 م.

اعتمده مجلس وزراء العدل العرب ب قرار 771/د24-2008/11/27

13.مشروع مُكافحة الجرائم المعلوماتية المصري.

كان حرص المُشرع المصري عظيماً في مواكبة النهضة التكنولوجية والمعلوماتية التي يعيشها العصر فأصدر قانون خاص للاتصالات [2].

رقم2003/10م لتأمين نقل وتبادل المعلومات وقانون أخر للتوقيع الإلكتروني رقم 2004/15م لتأمين معاملات الأفراد عبر شبكة المعلومات الدولية الإنترنت فضلاً عن أن هناك جهود تُبذل لإصدار قانون خاص بالمُعاملات الإلكترونية لسلامة وتامين المعلومات المختلفة من كافة جوانبها القانونية والجنائية وهناك دراسات جادة لأعداد مشروع قانون مُكافحة الجريمة المعلوماتية

المطلب الثاني

أدلة إثبات الجرائم الإلكترونية في التشريعات العربية

أولاً: تاريخ تشريعات الجرائم الإلكترونية وأدلة اثباتها.

الهدف من الإثبات الجنائي هو بيان مدى التطابق بين النموذج القانوني للجريمة وبين الواقعة والمعروضة فأنه في سبيل ذلك يستخدم وسائل معينة هي وسائل الإثبات ووسيلة الإثبات هي: كل ما يستخدم في إثبات الحقيقة فهي نشاط يُبذل في سبيل

[1] وجاء في المادة الثانية من هذا النظام بأنه يهدف هذا النظام إلى الحد من وقوع الجرائم المعلوماتية وذلك بتحديد هذه الجرائم والعقوبات المُقررة لكل منها وبما يؤدى إلى: المساعدة على تحقيق الامن المعلوماتي، وحماية الاقتصاد الوطني، وحماية المصلحة العامة والاخلاق والآداب العامة.

[2] وعُرفت الاتصالات في هذا القانون في م1/ف3 بأنها اية وسيلة لإرسال أو استقبال الرموز أو الإشارات أو الرسائل أو الكتابات أو الصور أو الاصوات وذلك أياً كأنت طبيعتها وسواء كأن الاتصال سلكياً أو لاسلكياً. المزيد من مشاريع القوانين أنظر: العادلي محمود صالح، الجرائم المعلوماتية ماهيتها وصورها. ورقة عمل مقدمة لورشة العمل الإقليمية حول تطوير التشريعات في مجال مكافحة الجرائم المعلوماتية عمان مسقط 3-4/ابريل ص13 وما بعدها

اكتشاف حالة أو مسألة أو شخص أو شيء ما أو ما يفيد في إظهار عُنصر الإثبات المختلف أي الأدلة ونقلها إلى مجال الواقعي الملموس [1].

وقد شهد مطلع السبعينات الانطلاقة الحقيقية لموجة تشريعات الخصوصية وعلى امتداد العقدين بعدهما شهد انطلاقة الموجة الثانية المُتمثلة بقوانين جرائم الكمبيوتر في حين شهدت السبعينات البحث الجَّدى لحماية برامج الكمبيوتر. فضم نظام الملكية الفكية وتحديد حق المؤلف وانطلاقة التدابير التشريعية الأولى في هذا الحقل؛ ليشهد انطلاقة موجة ثالثة من التشريعات المُتصلة بالكمبيوتر هي موجة تشريعات حماية البرمجيات التي تمثل المُصنف الأهم من بين عناصر تكنولوجيا المعلومات التي ستفتح الباب امام مفهوم المُصنفات الرقمية واتساع دائرة الحماية القانونية في نطاقها.

ومنذ نهاية السبعينيات ومطلع الثمانينات كانت تُثار في الاطار القانوني التساؤلات بشأن حجية مُستخرجات الكمبيوتر ومشكلات الإثبات بواسطة ملفات الكمبيوتر والبيانات المخزنة فيه أياً كانت صورة هذه البيانات وقد شهدت أوروبا تحديداً نشاطاً محموداً في هذا الحقل أنطلق مع منتصف الثمانينات وأنصب على البحث في تطوير قواعد الإثبات والوصول للمحاكمات في المواد المدنية والتجارية لاستيعاب التوظيف المُتنامي لأنظمة الكمبيوتر والاعتمادية المتزايدة عليها وما ينشأ عن ذلك من كثرة اللجوء لسجلات الكمبيوتر وملفات البيانات المُخزنة للاحتجاج بها ليس فقط تلك المُخزنة في نظام المعلومات بل سجلات وبيانات شبكات الاتصالات الخاصة كبيانات شبكة سويفت وغيرها الخاصة بالعمل المصرفي وبيانات أنظمة الشحن البحري الإلكتروني التي اخذت في الاتساع والنماء وبيانات سجلات الشبكات الاتصالية.

لكن هذه البدايات ما لبثت أن أخذت منحنى مُختلفاً تماماً مع دخول الإنترنت في مطلع التسعينيات الاستخدام التجاري الواسع إذا مع الاتجاه إلى التشبيك أو بناء شبكات المعلومات على النحو الواسع والتحول من أنماط العمل المادي إلى العمل الإلكتروني أصبح الأمر أكثر من مُجرد حجية مستخرجات نُظُم الكمبيوتر وشبكات الاتصال بل أصبح وسائل التعاقدات ووسائل اثبات في بيئة الشبكات والنظم الإلكترونية [2].

ثانياً: طرق الإثبات الجنائي في قوانين الدول العربية.

لم تشهد قوانين الإثبات العربية تعديلات خاصة بتشريعات مُستخرجات الكمبيوتر والمواد الإلكترونية في النزاعات الحقوقية والتجارية ولكن تتجه العديد من الدول العربية إلى الاعتراف بالحجية القانونية لملفات الكمبيوتر ومستخرجاته والرسائل

---

1 0 أنظر: د/ علي حسن الطوالبة، مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي دراسة مقارنة مركز الاعلام الأمني 2009 ص93

2 0 د/ يونس عرب، حجية الإثبات بالاستخراجات الإلكترونية، في القضايا المصرفية مجلة البنوك –الأردن ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية هيئة تنظيم الاتصالات مسقط سلطنة عمان 2-4/ابريل 2006م ورقة قانون تكنولوجيا المعلومات ص 8.

الإلكترونية ذات المحتوى المعلوماتي ليس بصورتها الموضوعة ضمن وعاء مادي ولكن بطبيعتها الإلكترونية المحضة.

والقواعد في الدعاوى الجزائية أو الجنائية جواز الإثبات بكافة طُرق الإثبات القانونية فيحق للمدعى أن يُثبت دعواه بكافة هذه الطرق ويحق القاضي أن يكون قناعته من أي دليل أو امارة أو اجراء يُقدم اليه أو يطلع عليه بنفسه ثم اقتضت الضرورة تفقد الوسائل بعدد من الطرق والقيد على هذه القاعدة أن الدليل يتعين أن يكون من الأدلة التي يقبلها القانون وبالتالي تظهر اهمية اعتراف قانون الأدلة ذات الطبيعة الإلكترونية والمعلومات وأن كانت قيمتها تتجاوز شيئاً فشيئاً الموجودات والطاقة فانها ليست ماديات لتقبل كبينة في الإثبات ووسائط تخزينها غير الورق كمخرجات لا تحظى من حيث محتواها بقبولها دليلاً مادياً من هنا كان البحث القانوني يسعي لإيجاد إثبات جنائي للجرائم الإلكترونية.

ثالثاً: طريقة اعتماد وسائل الإثبات الإلكتروني:

جاء في القانون العربي الاسترشاد لإثبات بالتقنيات الحديثة 771/د24 – 2008/11/27م حجية الكتابة والمحررات التواقيع الإلكتروني ثم ذكر لهذه الحجية شروطاً وهي:

- ارتباط التوقيع الإلكتروني بالموقع وحده دون غيره.
- سيطرة الموقع وحده دون غيره على أداة إنشاء التوقيع الإلكتروني.
- إمكانية كشف أي تغيير في بيانات المُحرر الإلكتروني أو التوقيع الإلكتروني بعد وضعه على أي محرر.

وجاء في المادة العاشرة من هذا الفصل انه يمكن توافر صفة النسخ الأصلية للمحرر الإلكتروني إذا توفرت فيه الشروط الأتية:

- أن تكون المعلومات الواردة به قابلة للحفظ والتخزين بحيث يمكن في أي وقت الرجوع اليها.
- أن يكون محفوظاً بالشكل الذي تم أنشاؤه أو إرساله أو تسليمه أو بأي شكل يسهل دقة المعلومات التي وردت به عند أنشائه أو تسليمه.
- أن تدل المعلومات الواردة به على من أنشأه أو تسليمه وتاريخ ووقت إرساله وتسليمه
- إمكانية الاعتداد بمصدر المعلومات إذا كان معروفا.

وهكذا يكون القانون العربي الاسترشاد لإثبات التقنيات الحديثة قد اعتبر صراحة حجية الكتابة والمحررات والتوقيع الإلكتروني وعليه فانه يؤخذ من ذلك اعتبار هذه المحررات الإلكترونية أدلة اثبات يمكن الاحتجاج بها عند التنازع. ويتعين مساواة الأدلة ذات الطبيعة المادية القائمة على الكتابة والورق من حيث المقبولية والحجية وكلما كان التصرف المادي في البيئة الواقعية محل اعتبار يتعين الاعتراف بما يُقابله من تصغر معنوي في البيئة الرقمية والتوقيع الإلكتروني يقتضي مساواته بالتوقيع المادي والتصديق الإلكتروني يتعين بمساواته بالتصديق المادي وهكذا شريطة أن تحقق البيئة الرقمية من حيث المعايير والإجراءات المتصلة بالسلوكيات المعنوية أو سلوكيات البيئة الافتراضية ما يوفر الثقة التي تحلت بها السلوكيات المادية [1].

ثم أنه ينبغي على القاضي أن يكون مُتفهماً لفحوى التقدم التقني وما ينتج عنه من وسائل إجرامية يغلب عليها هذا الطبع التقني الحديث.

وعلى هذا الأساس ينبغي أن يقبل الأدلة المُستمدة من الكمبيوتر لاثبات وقائع الدعاوى التي تتناول الجرائم المعلوماتية ويساعده في هذا الأمر طُرق وقواعد ومبادئ الإثبات العامة والقناعة الشخصية للقاضي في المجال الجنائي.

ومن ناحية أخرى فأنه ينبغي على القاضي أن يتحلى بمقدره على التكيف القانوني للأفعال الاجرامية المستحدثة مع التشريعات القائمة [2].

رابعاً: صعوبة اثبات الجريمة الإلكترونية.

بخلاف ما يتصوره كثير من الباحثين والمختصين في مجال مُكافحة الجريمة المعلوماتية فإن ظاهره انتشار التشريعات والقوانين للحد من هذه الأفة اخذت في الازدياد في كثير من دول العالم واغلب هذه القوانين لم تأخذ في الاعتبار عند أنشائها أن الجريمة المعلوماتية تنشأ في بلد ويحدث أثرها في بلد أخرى.

ومن امثلة الواقعية على ما تقدم ما حصل في دولة الامارات العربية المتحدة حيث قام مشغل حاسوب بتهديد المؤسسة التي يعمل لديها بتنفيذ مجموعة من مطالبه وذلك بعد أن حذف كافة البيانات الموجودة على الجهاز الرئيسي للمؤسسة وقد رفضت المؤسسة الاستجابة لمطالبه فأقدم على الانتحار ووجد المؤسسة صعوبة في استرجاع البيانات النت التي حُذفت. [3]

---

[1] د/ يونس عرب التدابير التشريعية العربية لحماية المعلومات الرقمية، العربية 3000، س4،ع1،ص155-219.

[2] القاضي وليد عكوم، التحقيق في جرائم الحاسوب الدليل الإلكتروني للقانون العربي، لبنان، ص8.

[3] د يونس عرب، مرجع سابق، ص213..

وتتعقد المشكلة عندما يتعلق الأمر بمعلومات أو بيانات تم تخزينها في الخارج بواسطة شبكة الاتصال عن بعد، فالقواعد التقليدية بالإثبات لا تكفي لضبط مثل هذه المعلومات بحثاً عن الأدلة ، فمن الصعوبة اجراء التفتيش للحصول على الأدلة في هذه الحالة في داخل دولة اجنبية حيث أن هذا الاجراء يتعارض مع سيادة هذه الدولة الأخيرة ولِما كانت أدلة الإثبات المتحصلة من التفتيش على نظم الحاسوب والإنترنت تحتاج إلى خبرة فنية وادارية فائقة في هذا المجال فإن نقص خبرة سلطات جمع الاستدلالات والتحقيق والمحاكمة قد يؤدى إلى ضياع الدليل بل تدميره أحياناً وفضلاً عن ذلك أن كل المعطيات ليس لها تجسيد دائم على اية دعامة بمعنى أنها لا توجد مسجلة على أسطوانة صلبة أو مرنة ولا على اية دعامة مادية منقولة أياً كانت فقد توجد هذه المعطيات في الذاكرة الحية للحاسوب ويتم محوها في حالة عدم حفظها أو تسجيلها على اية أسطوانة وحتى لو كانت المعطيات قد تم تخزينها على دعامة مادية الا أنه قد يكون من الصعب الدخول اليها بسبب وجود نظام معلوماتي للحماية وعلاوة على ذلك قد يتقاعس المجني عليه عن التبليغ عن جرائم المعلوماتية إلى السلطات المختصة بالإضافة لما تقدم من صعوبات ومشكلات [1].

وتدعي الجرائم الإلكترونية بالجرائم النظيفة وذلك لصعوبة اكتشاف دليل ثبوتها فلا أثر فيها لا أية عنف أو دماء وإنما مُجرد ارقام وبيانات يتم تغيرها أو محوها من السجلات المخزنة في ذاكرة الحاسبات الألية وليس لها أثر خارجي مادي [2]. ومن هنا نقف على حقيقة الصعوبات التي تواجه كافة أطراف المنظومة الأمنية والقضائية في هذا الاصدار التي تتجلى عندما تكون الجريمة واقعة على برامج الكمبيوتر وبياناتها أو بواسطتها وذلك بالنظر إلى عدم توافر الآثار المادية التي قد تنتج عن هذا النوع من الجرائم واكثره عدد الاشخاص الذين قد يترددون على مسرح الجريمة خلال المادة الفاصلة بين وقوع الجريمة والكشف عنها. لذا لابد للحفاظ على مسرح الجريمة فيما يأتي:

- ملاحظة طريق اعداد نظام الكمبيوتر بعناية بالغة.
- اثبات الحالة التي تكون عليها تفصيلات وكابلات الكمبيوتر المتصلة بمكونات النظام.
- عدم التسرع في نقل أي مادة معلوماتية من مكان وقوع الجريمة خشية اتلاف البيانات المخزنة [3].

---

[1] د/ علي حسين الطوالبة، مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي مرجع سابق، ص97.

[2] أنظر: عبد الرحمن بحر، معوقات التحقيق في جرائم الأنترنت. دارسة مسحية على ضباط الشرطة في دولة البحرين أكاديمية نايف العربية للعلوم الأمنية 1420هـ 1999. م/ رامي على وشاح، الصعوبات المادية التي تعترض الإثبات بالمحررات الإلكترونية. وأكاديمية للدراسات الاجتماعية والإنسانية 2010/3 ص44-52.

[3] وليد عَكوم التحقيق في جرائم الحاسوب مرجع سابق ص 6.

ومما تقدم نخلص إلى أبرز الصعوبات التي تعترض اثبات الجريمة الإلكترونية:

1- تقع الجريمة في عدة دول وتحكمها عدة قوانين وقواعد معينة بذلك مما يشكل تحديداً اما الجهات القضائية في تطبيق القانون ويزيد من صعوبة التحقيق فيها [1].
2- مهارات التخزين الإلكتروني من معطيات الذي يجعلها غير مرئية وغير مدركة بالعين المجرد.
3- تشفير البيانات المخزنة الإلكترونيات أو المنقولة عبر شبكات الاتصال.
4- سهولة محو الأدلة في زمن قصير.

المطلب الثالث

التعاون الدولي للحد من الجريمة الإلكترونية

تمهيد:

بات من الضروري ايجاد اطار فعال يضمن استحداث اليات التعاون الدولي في مجال مُكافحة هذا النوع من الجرائم من خلال التشجيع على تبادل الخبرات من اجل الضبط الجنائي لها باعتبارها جرائم افتراضية مع تكوين مُختصين في المجال سواء الضبطية القضائية أو القضاء بوجه عام وايجاد تشريع دولي خاص لمواجهة هذا الخطر وتبنى منظومة معلوماتية موحدة تعتمد على إنشاء مكتب عالمي أو إقليمي للتوثيق الإلكتروني مع تسجيل البرامج المعلوماتية كافة وحفظها واعتماد الدلائل أو القرائن الرقمية كدلائل اثبات الجريمة ومن ثمة إدانة مُقترفيها والحرص على إدراج مثل هذه الجرائم ضمن اختصاصات المحكمة الجنائية الدولية نظراً لطابعها العالمي فالتشريع الدولي المنشود يجب أن يبنى على اطر قانونية موحده يتم فيها عولمة القوانين وصلاحيات الاختصاص المفتوحة والشركات بين جميع دول العالم [2].

ومن أوائل الدول العربية التي سنت قوانين خاصة لمُكافحة الجريمة الإلكترونية هي السعودية وتلتها الامارات العربية المتحدة ثم عمان ولكنها قوانين غير فعالة نظراً لطابعها المحلى من جهة والثغرات القانونية الموجودة بها لِذا اصبح من الضروري الدعوة للعمل على سن القانون الدولي فعال شامل يكون مبنى على قاعدة معلومات ومعطيات بيانية معلوماتية موثقة شاملة تخص هذا الجانب مع تكثيف التعاون العربي الدولي من خلال عقد مؤتمر عالمي موحد لاحتواء هذا الخطر الزاحف وتدعيم اجهزة

---

[1] الاجراءات الوقائية والتعاون الدولي لمحاربة الجريمة الإلكترونية ضمن اعمال ندوة الإقليم حول الجرائم المتصلة بالكمبيوتر 20-19 نيسان / يونيو 2007م المملكة الغربية ص119.
[2] د / يوسف حسن يوسف الجرائم الدولية للأنترنت مرجع سابق ص 173/141.

الأمن بما فيها الشرطة الجنائية الدولية الإنتربول المُعطيات اللازمة كافة بتكوين خبراء متخصصين في التقنية الإلكترونية إلى جانب تكريس وتشجيع البحث العلمي العربي وتكثيف حجم التبادل في الخبرات وسن القوانين ذات الشمولية الدولية ضمن الاستراتيجية الأمنية العربية، حيث لازالت مُعظم القوانين الموجودة لا تتماشى مع حجم الكوارث المُرتكبة يومياً لذا من الواجب من الأن إعادة النظر في المنظومة القانونية الخاصة وادراج قوانين جديدة للتصدي لظاهرة تنمية الجريمة الإلكترونية في ابعادها المختلفة.

وفي خطوة اعتبارها البعض بداية صحيحة لطريق طويل ملئ بالعقبات يعتزم الاتحاد الأوروبي وضع خطة جديدة يقوم بموجبها تفتيش اجهزة الكمبيوتر عن بعد وذلك لمُكافحة جرائم الإنترنت وستشمل خطة العمل الخمسية لاتحاد الخطوات للقضاء على الزيادة المُطردة في السرقة الإلكترونية وفي عدد الأجهزة المستخدمة في نشر الرسائل غير المرغوب فيها وغير ذلك من البرامج الخبيثة.

كما ستشجع الخطة تبادل المعلومات بين قوات الشرطة الإلكترونية لمُلاحقة ومقاضاة المُجرمين وستنسق هذه القوات المعروفة باسم يوروبول عملها الاستقصائي كما ستوجه تحذيرات حول موجات الجريمة الإلكترونية [1].

وقد حظيت الخطة الخمسية بدعم وزراء الاتحاد الأوربي في اجتماع تقرر فيه ايضاً منح يوروبول مبلغ 300 ألف يورو لتُنشئ جهازاً لتجميع تقارير الإجرام واصدار تحذيرات حول الاخطار المُحدقة.

ودعم الاجتماع الوزاري استراتيجية مُكافحة الجريمة الإلكترونية التي ستنشئ فرق تحقيق تعمل عبر الحدود وترخص استخدام دوريات افتراضية لضبط بعض النواحي الإنترنت. ومن الإجراءات العملية الأخرى للخطة تشجيع تبادل أفضل للمعلومات بين قوات الشرطة في الدول الأعضاء حول طرق التحقيق واتجاهاته.

وتهدف الاستراتيجية بشكل خاص إلى مُكافحة التجارة في صور الأطفال الثاء تعرضهم للإيذاء الجنسي [2]. وقال الاتحاد في بيان يضع الخطوط العامة لاستراتيجية أن نصف جرائم الإنترنت تشمل أنتاج وتوزيع وبيع صور إباحية للأطفال.

كما ستشارك هذه القوات في تفتيش اجهزة الكمبيوتر عن بعد وتسفير دوريات على الإنترنت لملاحقة المُجرمين واكد الاتحاد الأوروبي أن الضوابط موجودة لضمان احترام قوانين حماية المعلومات اثناء جمعها وتبادلها.

---

1 0 موقع البوابة القانونيةwww.tashreaat.com.

2 0 د/ مدحت عبد الحليم، جرائم الاعتداء على الأشخاص والأنترنت، دار النهضة القاهرة 2000 ص23 وما بعدها.

وكان الاتحاد الدولي للاتصالات قد استحدث دليلاً الكترونياً لتتبع المعايير الأمنية الخاصة بتكنولوجيا المعلومات والاتصالات لمُكافحة الجريمة على الإنترنت ويعتمد على المفهوم أن تنهض جهة مفردة بذلك التتبع ما يمكن المستخدمين من الرجوع اليها ومتابعتها بسهولة.

ووصف الدليل بأنها خريطة طريق فيما يتعلق بمعايير الأمن الخاصة بتكنولوجيا المعلومات والاتصالات حيث يستطيع أن يُلاحق المعلومات عن أحدث المعايير الأمنية المُتجددة باستمرار ثم يخزنها في قاعدة بيانات تفتح امام المعنيين ما يُسهل مهمة البحث عن المعلومات المطلوبة وتم وضع الدليل بالتعاون المشترك بين الاتحاد الدولي للاتصالات والوكالة الأوربية المختصة بأمن الشبكات والمعلومات وأطراف دولية أخرى مهتمة بشئون الأمن المعلوماتي على شبكة الإنترنت.

ويعرض الدليل اسماء المنظمات المعنية بتطوير المعايير وما تنشرها من صيغ خاصة بأمن الإنترنت ما يُجنب تكرار الجهود كما يُسهل مُهمة مهندسي أمن الشبكات الإلكترونية في كشف الثغرات التي تُمكن العابثين من تهديد أمنهم.

ويضم الدليل خمس اقسام تحدث بصفة مستمرة وتناول منظمات تطوير المعايير الخاصة بالتكنولوجيا المعلومات والاتصالات واعمالها والصيغ المعتمدة لتلك المعايير وطرق اقرار الاتفاق على تلك المعايير والحاجات المستقبلية

محاولات للحد من تلك الجرائم.

وفي نفس السياق وللحد من الخطر القادم عبر الشبكات تُسارع الدول إلى وضع ضوابط وحماية وإنشاء أمن خاص للشبكات حيث شَكلت وزارة الداخلية المصرية دوريات أمنية من خلال الشبكة ومهامها منع الجريمة قبل وقوعها. واستطاعت هذه الدوريات من ضبط تنظيم للشواذ يمارس جرائم عبر الإنترنت [1] وكذلك ضبط العديد مما يحاول استخدام بطاقات ائتمان مسروقه.

والحكومة البريطانية ايضاً شكلت وحدة من قوات الشرطة وكلفت بمتابعة المُجرمين الذين يستخدمون أجهزة الكمبيوتر وبعد اقتناع تام بالخطر القادم ومداولاًت استمرت أربع سنوات قامت ثلاثون دولة أوروبية لتوقيع مُعاهدة لتوحيد الجهود في محاربة جرائم الإنترنت [2]. ومطلوب من اجهزة الأمن العربية أن تواجه هذا التحدي وتطور قدراتها وتحث برامجها للقضاء أو للحد من مثل هذه الجرائم.

وفي السعودية تفرض الحكومة عقوبات بالحبس لمدة عام واحد وغرامات لا تزيد عن 500 ألف ريال فيما يعادل 133 ألف دولار لجرائم القرصنة المرتبطة بالإنترنت

---

[1] 0 من موقع www.websy.net موضوعات بعنوان الدوريات الأمنية المنظمة لمنع الجرائم الإلكترونية.

[2] 0 د/ محمد منير التهبتن، جرائم الحاسبات ووسائل مكافحتها، دار الفكر الجامعي الطبعة الثانية الإسكندرية 2000م ص 43 وما بعدها.

واساءة استخدام كاميرات الهواتف المحمولة مثل التقاط صورة دون تصريح. وأكدت النيابة العامة السعودية أن أي رسائل أو صور أو مقاطع مرئية تنطوي على مدلول جنسي تجاه شخص آخر تمس عرضه أو تخدش حياءه باستخدام وسائل التواصل الاجتماعي أو أي وسيلة تقنية في هذا الشأن، تُعد جريمة تحرش، وأن مُرتكِب تلك الجريمة يعاقب بالسجن مدة تصل إلى سنتين وغرامة مالية تصل إلى 100 ألف ريال، أو بإحدى هاتين العقوبتين.

وفي بيان صادر من الحكومة السعودية تعلن موافقتها على مشروع قانون بخصوص جرائم تكنولوجيا المعلومات، وبموجب مشروع القانون توقيع العقوبة على الدخول المحظور إلى موقع إلكتروني أو لتغير تصميم هذه الموقع أو إلغائه أو اتلافه أو تعديله كما يجُرم مشروع القانون المساس بالحياة الخاصة عن طريق إساءة استخدام هواتف المحمول المزودة بكاميرا أو ما في حكمها بقصد التشهير بالأخرين وإلحاق الضرر بهم عبر وسائل تقنيات المعلومات المختلفة.

بروتوكول مصري لمُكافحة جرائم الإنترنت.

وقعت الجمعية المصرية لمُكافحة جرائم الإنترنت [1] بروتوكول تعاون مع كلية الحقوق جامعة عين شمس بهدف تثقيف وتدريب طلبة وخريجة كلية الحقوق والآداب والاعلام والسياحة والاثار والتجارة والحاسبات والمتخصصين والسادة القضاة واعضاء النيابة العامة والسادة المحامين والعاملين في القطاعات القانونية بالمؤسسات وتأهيل وإكساب المتدربين المهارات القانونية والعلمية والعملية والفنية الخاصة بارتباط وسائل المعلومات والاتصالات بتخصصاتهم ومدى تأثير استخدام تكنولوجيا المعلومات في إنجاز مهام اعمالهم والتعريف بماهية التعامل مع الإشكاليات القانونية في حقل المعاملات الإلكترونية حول موضوعات تشمل كيفية اثبات الشخصية وكيفية التوقيع الإلكتروني وأنظمة الدفع النقدي الرقمي والمال الرقمي أو الإلكتروني وسرية وأمن المعلومات من مخاطر جرائم التقنية العالمية وخصوصية العميل والمسؤولية عن الأخطاء والمخاطر حجية المراسلات الإلكترونية والتعاقدات المصرفية الإلكترونية ومسائل الملكية الفكرية للبرمجيات وقواعد معلومات البنوك أو المستخدمة من موقع البنك أو المرتبطة بها علاقات وتعاقدات البنك مع الجهات المزودة للتقنية أو الموردة لخدماتها.

وماهية التنظيم القانوني للعالم الافتراضي بأقسامه من المعاملات القانونية الرقمية وعقود التجارة الإلكترونية وحماية الملكية الفكرية عبر الإنترنت والتعريف بأنماط واشكال الجرائم عبر الإنترنت، وماهية الدليل الرقمي وحجيته في الإثبات وعرض احداث التقنيات الفنية العالمية للتعامل مع مثل هذه النظم إن كان ما أوردته عبارة عن

[1] موقع الجمعية المصرية لمكافحة جرائم الأنترنت والمعلوماتية www.eapiic.net

دراسة بحثية صغيرة لكن لابد أن نعرف أن الجريمة الإلكترونية جريمة ذات ابعاد دولية تخضع لمبدأ تنازع القوانين هذا فضلا عن القصور التشريعي لدي الكثير من الدول للحد من تلك الجرائم.

الخاتمة:

إن تحديد المسؤولية الجنائية على شبكة الإنترنت يُعد بلا شك من أدق الموضوعات التي يُمكن مواجهتها حيث يُعتمد تشغيل شبكة الإنترنت على آلات قام بعض مُتخصصين ببرمجتها ببرامج يجب أن يتحملوه مسئولياتها ونظراً لشبكة الإنترنت ليست خدمة يُديرها شخص ما يتعاقد معه من ناحية ومع مُقدِمي المعلومات والمستخدمين من ناحية أخرى فالإنترنت قوة كامنة في توفير الخدمة بعدد غير محدود للحسابات على مستوى العالم تلبية لرغبة مستخدميها عن طريق الاتصال بها ونظراً لتفاعل ادوار القائمين على تنظيم شبكة الإنترنت فهذا يقودنا إلى مواجهة مستويات مُختلفة من المسئولية القانونية بالنسبة للمتداخلين الذين يتنوع ادوارهم في تقديم خدمة الإنترنت.

ويعاني كثيرون من مستخدمي الأجهزة الإلكترونية الموصولة بشبكة الإنترنت من الجرائم الإلكترونية بشكلٍ عام وجرائم التحرش الإلكتروني بشكلٍ خاص من خلال تعرضهم لأشكال مختلفة من المُضايقات بدءاً من الإلحاح بالتعارف من أشخاص لا يعرفونهم أو تعرضهم للمُلاحقة والتعقب من أخرين ممن لديهم خلافات شخصية معهم أو من خصومهم السابقين أو التعقب من الجهات الأمنية وقد يتعرض المرء للتحرش من اشخاص معروفين له أو من مجهولي الهوية.

وتشمل أشكال هذا التحرش مُلاحقة الأخرين أو التشهير بهم كتوجيه الرسائل التي تحتوي على مواد تسبب الانزعاج للمتلقي سواء كانت تلميحاً إلى الرغبة بالتعرف الي المُتلقي لأهداف جنسية أو كانت تحتوي على عبارات أو شتائم أو نشر صور الشخص من دون علمه أو التهديد أو الابتزاز أو الملاحقة والتجسس أو التتبع بالتعليقات المُسيئة أو التشهير بالشخص عبر وسائل إلكترونية مختلفة أو انتحال شخصية بتزوير البريد الالكتروني أو انتحال الحسابات على مواقع التواصل الاجتماعي.

وتسعي حالياً الجهات الحكومية من توفير الحماية لمستخدمي الإنترنت من الجرائم الإلكترونية، فيمكن للأشخاص الذين يتعرضون للتحرش الإلكتروني بالتقدم بشكوى رسمية لمباحث الإنترنت فهناك عقوبات على الجرائم الإلكترونية وإزعاج الاخرين والتعرف على هويتهم الحقيقية وبالآتي تعرضهم للملاحقة القانونية لذا من الضروري الاحتفاظ بأدلة تتضمن المُضايقات والتعليقات والرسائل التي يتم التعرض لها لأنها ستساعد في اثبات هذه الوقائع ويُسهل الوصول إلى مجرمي الفضاء الإلكتروني.

التوصيات:

1. نوصي بضرورة نشر الوعي بين الأفراد– ولا سيما الشباب – بمخاطر التعامل مع المواقع السيئة على شبكة الإنترنت ودعم الوعي المجتمعي بالمخاطر النفسية والاجتماعية وغيرها الناجمة عن الاستخدامات غير الآمنة للإنترنت.
2. نوصي بإدخال مادة " أخلاقيات استخدام الإنترنت " ضمن المناهج الدراسية في تعليم ما قبل الجامعي.
3. نوصي بإنشاء قسماً جديداً بكليات الحقوق بالجامعات العربية لدراسة الحماية القانونية للمعلومات.
4. نوصي بتدريب رجال الضبط الجنائي والمحققين والقضاة المتخصصين بجرائم تقنية المعلومات على الأساليب الفنية المستخدمة في ارتكاب الجرائم وفيما يتعلق بالكشف عنها والدلائل المستحدثة في مجال اثباتها.
5. نوصي بتفعيل دور المجتمع المدني ولا سيما الجمعيات الأهلية للقيام بدورها في وقاية الشباب من الوقوع في الممارسات الخاطئة للسلوكيات والممارسات الضارة أخلاقياً عبر شبكة الإنترنت.
6. نوصي بتعزيز التعاون والتنسيق مع المؤسسات الدولية المعنية بمُكافحة الجرائم الالكترونية من خلال الاتفاقيات الدولية الخاصة بمُكافحة جرائم الإنترنت وخاصة المعاهدة الدولية لمُكافحة الجرائم الالكترونية والإنترنت مع متابعة المستجدات على الساحة العالمية.
7. نأمل أن تسعي الدول العربية إلى انشاء مُنظمة عربية تهتم بالتنسيق في مجال مُكافحة الجرائم الإلكترونية عبر الإنترنت وتشجيع قيام اتحادات عربية تهتم بالتصدي لجرائم الإنترنت وتفعيل دور المنظمات والادارات والحكومات العربية في موجهة هذه الجرائم.
8. نوصي بتفعيل دور المؤسسات التوعية (المسجد – الاسرة – دور التعليم – أجهزة الاعلام) وذلك بالتوعية بخطورة الجرائم الالكترونية على الاسرة والمجتمع والسعي في تقوية الوازع الديني.
9. نوصي بإنشاء مدارس ومعاهد واقسام في الجامعات ومراكز بحثية خاصة تعني بالأمن المعلوماتي والتدريب فيه ومواكبة كل ما هو حديث في هذا المجال.
10. نوصي بسن القوانين والأنظمة الخاصة التي تسد كافة ثغرت الجريمة الالكترونية مثل القوانين المُتعلقة بكيفية اكتشاف الأدلة الالكترونية وحفظها والنص على طرق ثبوتها.

قائمة المراجع

الكتب القانونية:

1. أحمد شوقي عمر أبو خطوة، شرح الأحكام العامة لقانون العقوبات دار النهضة العربية – مصر – القاهرة 2000م.
2. أحمد عوض بلال، مبادئ قانون العقوبات المصري " القسم العام " دار النهضة – القاهرة.
3. أحمد فتحي سرور، الوسيط في قانون العقوبات – القسم الخاص طبعة نادي القضاة – مصر – القاهرة 1980م.
4. بكاي يحي، جريمة التحرش الالكتروني دراسة مقارنة مجلة المناظرة – هيئة المحامين بوجده – المغرب 2010م.
5. جميل عبد الباقي، القانون الجنائي والتكنولوجيا الحديثة دار النهضة العربية 1992م.
6. عزمي، الجرائم الالكترونية وإثباتها مبادئ أوصل عزلة الجنائية في مجال إثباتها دون مكان النشر دون سنة النشر.
7. على عبد القادر القهوجي، الحماية الجنائية المعالجة إلكترونياً – بحث مُقدِم الي مؤتمر " القانون والكمبيوتر والإنترنت " جامعة الامارات العربية المتحدة في الفترة من 1-3 مايو لعام 2000م.
8. محمود حمدان، التحرش الإلكتروني عبر الإنترنت الاكاديمية العربية لخدمات الباحثين 2007م.
9. محمود نجيب حسنى، علاقة السببية في قانون العقوبات طبعة نادى القضاة، مصر، 1984م
10. محمود نجيب حُسنى، قانون العقوبات القسم العام، دار النهضة، مصر، 1998.

الرسائل والمطاريح العلمية:

1- ذياب موسي البدانة، الجرائم الالكترونية: المفهوم والأسباب ورقة عمل مُقدِمة الي الملتقي العلمي الجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية والدولية خلال الفترة من: 11/1435 والمقام بكلية العلوم الاستراتيجية عمان – المملكة الأردنية الهاشمية.
2- على أحمد فرجاني، جريمة القرصنة المعلوماتية – دراسة مقارنة من الجانبين الموضوعي والاجرائي بحث مُقدِم في الدورة التدريبة في موضوع الاحكام الموضوعية والاجرائية في الجرائم الناشئة عن الشبكات الإلكتروني في الفترة من الخميس 15 مارس الي الاثنين 12 مارس 2012م والمقاومة بمركز أ.م. عبد الروف مهدي للدارسات والبحوث الجنائية كلية الحقوق – جامعة المنصورة

3- غنام محمد غنام، دور قانون العقوبات في مُكافحة جرائم الكومبيوتر والإنترنت بحث مُقدِم في الدورة التدريبية في موضوع الاحكام الموضوعية والاجرائية في الجرائم الناشئة 2012 م
4- مهند بن حمد بن منصور الشعيبي، تجريم التحرش الجنسي وعقوبته رسالة مُقدِمة لاستكمال متطلبات درجة الدكتوراه في العدالة الجنائية تخصص ساسة جنائية المملكة العربية السعودية – الرياض 2009/1430م.
5- محمود عبدالعليم سليمان، إيذاء النساء، باثولوجيا التحرش الجنسي الإلكتروني بالمرأة، مجلة جيل العلوم الإنسانية والاجتماعية، العدد 42، مصر، مايو 2018.

القوانين:

1- قانون البيانات السويدي عام (1973م)
2- القانون الفرنسي الخاص بالتزوير المعلوماتي (1988م)
3- قانون مُكافحة التزوير المعلوماتي الألماني (1986م)
4- قانون مُكافحة الجرائم الإلكترونية (مواده مستحدثة ضمن أحكام قانون الجزاء العماني).
5- قانون مُكافحة جرائم الحاسب الآلي والإنترنت الدنماركي (1985م)
6- نظام مُكافحة الجرائم المعلوماتية السعودي (2007م)

المواقع الالكترونية:

1- أمنية حماشي ماهية الجريمة المعلوماتية بحث منشور على الرابط: www.asjp.cerist.dz
2- أية عامر دراسة الإنترنت يسهل التحرش عبر المواقع التواصل الاجتماعي بحث منشور على الرابط: www.shorouknews.comتاريخ الزيارة 9/22
3- استطلاع ع أجارة (بيو إنترنت أند أميركانا بريكة) عام 2006 حول مناظرة الإنترنت على الأطفال ومنشور عيل رابط: www.ror21.d19.com
4- حمد عبد العزيز سليم الجرائم الالكترونية مقال منشور على موقع منتديات ستار تايمز الالكترونية 2012 عنوان الرابط الالكتروني: www.startimes.com
5- حمدان محمود التحرش الالكتروني عبر الإنترنت الأكاديمية العربية لخدمات الباحثين: ar.scribd.com/document/111993270
6- خالد الشرقاوي السموني مُكافحة الجرائم الالكترونية على ضوء التسرعين الوطني والدولي نشر في 2012/3 الرابط: www.startimes.com
7- دعاء عرابي التحرش عن طريق الإنترنت بحث منشور على الرابط: www.m3looma.net
8- عبد الصبور عبد القوي على الجريمة الالكترونية والجهود الدولية للحد منها بحث منشور على الرابط: www.droitarab.com/201311/blog-post-27.htm
9- نهلة عبد القادر الموفي الجرائم المعلوماتية بحث منشور على موقع طريق التفوق والنجاح: www.kenanaonline.com/users/ahmedkordg/pst/409914

ثانياً: المراجع الأجنبية.

1. Chriss reed internet law-2004 camp ridge university press.
2. Daniele Borolo Daniele local la liberate sexually presses universities de France praise 2005.
3. Denis harcelement au travel de quell droid ?Edition L'harmattan hanot paris 2002.
4. Franciose. Jedeffossez Le Harcelements aux droids Francis discriminations our attainted a la liber? Apropos de lattices 222-33 du nouveau code penalty de la loin n92 09-1178 du 2 novmbre1992.
5. J.deveze les qualifications penalesaux frauds information in le droid criminal face au techniques de communication lies an l'inftmaiqe.
6. Jean pride Michel data Juan droid penal special 2eme edition
7. k.tiedemnn' fraud ET actor delist dairies commas a laid d'ordinateure electroniques rev droid penal cram 1984.
8. Lilianed ward& charlotte wailed law and the internet (regulations) hart publishing oxford 1997
9. Michele laurel Passat droid penal special dales 1997.
10. Publication Sous le titer de Lobos de boudoir sexual – le harcelement sexual au travel end la deceiver le boreal 1990.
11. Schiolberg Computers and penal leg is lotion as tidy of the legal politics of a new technology 1983.