المواجهة الجنائية للجرائم الماسة بالسمعة

عبر الشبكة العنكبوتية

في المرسوم بقانون اتحادي رقم (5) لسنة 2012

الدكتــور

ممـدوح خليـل البحــر

أستاذ القانون الجنائي المشارك

كلية الشرطة / أبوظبي

مستخلص

مع تقدم البشرية تتقدم وتتطور معها الجريمة، وتعتبر الجريمة المعلوماتية أو جرائم تقنية المعلومات نوع جديد من الجرائم. هذا النوع من الجرائم المتمثل في الوصول إلى أجهزة الحاسب الآلي للضحايا نوع جديد من الجرائم، على يد هؤلاء المجرمين وتدمير واتلاف البيانات والمعلومات والشبكات وأنظمة التشغيل وسرقة البيانات والمعلومات المخزنة فيها.

كما إن الأشخاص الذين يرتكبون الجرائم الإلكترونية هم في الغالب على قدر كبير من المهنية حيث يقوموا بإنشاء واستخدام برامج شريرة ومعقدة يطلق عليها أسماء عديدة وكلها تندرج تحت مسمى عام هو الفيروسات ويطلق عليهم اللقب الأكثر انتشاراً (Hackers) أي القراصنة. وأن الجريمة المعلوماتية (الإلكترونية) لا تختلف عن الجريمة العادية من حيث أركانها وعقوباتها لأنها تعتبر تعدي على حقوق وملكيات الآخرين. تكلمنا في مقدمة عن أهمية الموضوع وخطورته، وتكلمنا في المبحث الأول: عن الأحكام الموضوعية لجريمتي القذف والسب (الركن المادي والركن المعنوي، وفي المبحث الثاني: عن أحكام العقاب على القذف والسب عبر مواقع التواصل الاجتماعي، وفي المبحث الثالث: عن وسائل الاثبات الجنائي لجرائم القذف والسب عبر الشبكة العنكبوتية. وفي ختام البحث توصلنا إلى عدد من التوصيات منها: ضرورة تعديل التشريعات وضرورة وضع نصوص خاصة بالجوانب الموضوعية والإجرائية خاصة فيما يتعلق (بالضبط والتحقيق)، وأكدنا على الجانب الوقائي

من خلال التوعية للأسرة والشباب ودور منظمات المجتمع المدني، وضرورة استحداث قضاء متخصص للنظر في هذا النوع من الجرائم مع تأهيل القائمين على إجراءات الضبط والتحقيق.

Abstract

Crime is considered as the most dangerous social disease facing humanity all through ages ever since creation of mankind. Therefore, heavenly legislations and positive laws were set forth to punish those who are driven away from the route of right and follow the route of crime. Thus, justice is achieved and the rights of individuals, groups and all categories are maintained.

Along with human progress and development, goes crime and develops. Electronic or IT crime , or computer crimes, are a new class of crime .This class of crime is represented in accessing victims computers via these criminals and destruction or corrupting data information ,networks, operating systems and stealing the stored data and information therein.

The criminals who commit such electronic or IT crimes are mostly highly professional where they manage to set up and use wicked and complicated programs under various names of one category – Viruses. These people are commonly named "Hackers" i.e. pirates. Among these criminals or intruders is a

group of young people and teenagers who are only after stressing their superiority and experiencing their capabilities in this field.

In the introductory chapter, the researcher will discuss the nature and concept of IT electronic crime and offender's behavior, on the other hand, the first chapter studies the subjective aspects of crimes on reputation as stipulated in the Federal penal code No (3) of the UAE of 1987 notably defaming, infringing privacy and disclosing secret and the Federal law No (5) of 2012 on combating IT crimes committed by IT devices with compare to Foreign and Arabs laws. Overall such acts fall on honor, freedom and privacy of person because such rights are secure and protected by law, religion, constitutions and resolutions for it represents the person morals and values. The second chapter touches the procedurals aspects of crimes on reputation by means of electronic IT devices.

مقدمة

من المعلوم أنه مع تطور البشرية تتقدم وتتطور معها الجريمة، وتعتبر الجريمة الالكترونية، وجرائم تقنية المعلومات نوع جديد من الجرائم، هذا النوع من الجرائم المتمثل في الوصول إلى حواسيب الضحايا من الناس وارتكاب الجرائم من خلالها، هؤلاء هم في الغالب على قدر كبير من المهنية، ويطلق على هؤلاء الاسم الشائع الـ(Hackers) أي القراصنة.

فالعالم يواجه خطراً داهماً مع تزايد انتشار هذا النوع من الجرائم[1]، والتي تقوم على الاعتداء على حرية الأشخاص وخصوصياتهم وعلى ممتلكاتهم وعلى عرضهم وشرفهم، فقد أصبحت تلك الجرائم تمثل تحدياً كبيراً لكافة المجتمعات، حيث يصعب اكتشاف الجريمة الإلكترونية بسبب سريتها، وسرعتها، وأنها مجهولة المصدر خاصة في حالة قيام شخص من خارج الدولة بارتكابها، فما زالت الأجهزة القضائية وفقهاء القانون عاجزين عن الخروج بتصور واضح عن الجريمة الإلكترونية، وهنا تأتي ضرورة وضع القوانين الرادعة لمثل هذه الأفعال المشينة لجعل كافة مستخدمي الشبكة على بينة من أمرهم لتحقيق الأمن الإلكتروني

[1]) د.محمود أحمد طه:المواجهة التشريعية لجرائم الكمبيوتر والإنترنت، دراسة مقارنة، دار الفكر والقانون، المنصورة، جمهورية مصر العربية، 2013، ص177 .

وحفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية ولحماية المصلحة العامة والأخلاق والآداب العامة [1].

وإزاء خطورة إساءة استخدام شبكة الإنترنت خاصة في جرائم السب والقذف والإساءة الموجهة لسمعة وشرف الأشخاص، والتي لم يتم التطرق إليها بشكل كبير من خلال الدراسات وما يسببه هذا النوع من الاخلال بالأمن الاجتماعي وارتفاع معدلات الجريمة داخل المجتمع الإماراتي والعربي، ولهذا فقد وقع اختياري لهذا الموضوع.

أولاً: إشكالية البحث:

كل ما يخل بنظام المجتمع ويحدث الاضطراب فيه محرم ومجرم شرعاً وقانوناً، ولما كانت الجريمة لا تقف عند عصر معين، بل تتطور بتطور العصور، وتعدد صورها بتعدد الوسائل والوسائط، ولما كان هذا العصر عصر الوسائل الحديثة من أجهزة اتصال وحاسب آلي وإلكترونيات عمت وغلبت في استعمالات الناس الخاصة والعامة؛ أصبحت بطبيعة الحال من الوسائل التي يمكن أن ترتكب بها الجريمة، وقد أدى ذلك إلى ظهور ما اصطلح على تسميته بالجرائم الإلكترونية؛ التي تمثل أحد معوقات التطور التقني والنمو الإلكتروني، والتي أدت

[1]) د. علي حسن الطوالبة: الحماية الجنائية لمواجهة الجرائم الأخلاقية المستحدثة في التشريع الأردني والإماراتي، مجلة الشريعة والقانون، جامعة الإمارات، دولة الإمارات العربية المتحدة، العدد 235، 2008، ص265 .

في كثير من الأحيان إلى إحجام كثير من الناس عن التعاملات الإلكترونية، وتخوفهم من تقديم أي بيانات خاصة بهم لأي موقع من المواقع على شبكة الإنترنت وعدم قناعتهم بأي ضمانات تقدم لهم وتتضمن حماية معلوماتهم الشخصية.

ومن أكثر الجرائم الإلكترونية انتشاراً وشيوعاً الجرائم الواقعة على الأشخاص عبر شبكة الإنترنت كالسب والقذف والجرائم الواقعة على السمعة عبر شبكة الإنترنت؛ فقد أصبحت تلك الجرائم تمثل تحدياً كبيراً لكافة المجتمعات لأنها تصيب الأشخاص في أعراضهم وسمعتهم وشرفهم حيث تعددت صورها من جرائم استخدام بيانات شخصية غير صحيحة، إلى جمع أو تخزين بيانات شخصية صحيحة ولكن على نحو غير مشروع جنائياً، مثل جرائم إفشاء الأسرار، جريمة التهديد والمضايقة والملاحقة، انتحال الشخصية والتغرير والاستدراج، الابتزاز الجنسي، وجرائم الاعتداء على السمعة عبر الإنترنت، وعليه تدور إشكالية الدراسة حول تساؤل، سيتم الإجابة عليه في إطار بحثنا للموضوع، وهو :هل نجح المشرع الإماراتي في وضع المعالجة الجنائية لمواجهة جرائم السب والقذف عبر شبكة الإنترنت بهدف حماية الأشخاص من الاعتداء عليهم؟.

وينبثق من هذا التساؤل الرئيسي عدد من التساؤلات الفرعية، منها ما يلي:

1- ما هو مفهوم جريمة السب والقذف؟.

2- ما العقوبة المقررة لجريمتي القذف والسب عبر شبكة الإنترنت؟.

3- ما هي وسائل الإثبات لجريمتي القذف والسب عبر شبكة الإنترنت؟.

ثانياً: أهمية الدراسة:

ترجع أهمية الدراسة إلى ما يلي:

إن جرائم السب والقذف عبر شبكة الإنترنت تشكل مشكلة يعاني منها مستخدمو الشبكة وذلك لصعوبة الحصول على أدلة رقمية للكشف عن مرتكب الجريمة الإلكترونية، مما يساعد على سرعة إنتشار هذه الظواهر السلبية بالإضافة لسهولة ارتكاب هذه الجرائم في الأماكن العامة وحتى أمام الملأ دون شعور الأخرين بحيث لا يترك المجرم أية بصمة عن جريمته.

ثالثاً: أهداف الدراسة:

هدفت الدراسة إلى تحقيق الأهداف التالية:

1- بيان مفهوم جريمة القذف والسب واركانهما.

2- توضيح العقوبة المقررة لجريمتي السب والقذف عبر شبكة الإنترنت في التشريعات العقابية لبعض الدول الأجنبية والعربية.

3- الوقوف على وسائل الإثبات الجنائي لجريمتي القذف والسب عبر شبكة الإنترنت.

رابعاً: منهج الدراسة:

استفاد الباحث من أكثر من منهج منها: المنهج الوصفي التحليلي لوصف الظاهرة موضوع الدراسة، والمنهج المقارن الذي يستدعي المقارنة مع بعض النظم القانونية، العربية والأجنبية، التي لها صلة مباشرة بموضوع المسؤولية الجنائية عن القذف والسب عبر شبكة الإنترنت، وضمنت تشريعاتها بنصوص قانونية تكفل حمايتها أمام تلك الجرائم، وهذه النصوص القانونية التي يمكن الاستفادة منها في تشريعاتنا القانونية والوطنية، والتوصل إلى توصيات ورؤى مفيدة لمواجهة جريمة السب والقذف عبر شبكة الإنترنت.

خامساً: الدراسات السابقة:

دراسة "ميثاء الشيباني، 2018" بعنوان (المسؤولية الجزائية عن جريمتي السب والقذف بالوسائل الإلكترونية طبقاً للمرسوم رقم (5) لسنة 2012 بشأن قانون مكافحة جرائم تقنية المعلومات) [1]، هدفت الدراسة إلى التعرف على المسؤولية الجزائية عن جريمتي السب والقذف عبر شبكة الإنترنت والوسائل الإلكترونية الأخرى في التشريع الإماراتي طبقاً للمرسوم أعلاه بشأن قانون مكافحة جرائم تقنية المعلومات، وقد أوصت الدراسة بأهمية التركيز على التوعية بهذا النوع من الجرائم

[1]) ميثاء الشيباني: المسؤولية الجزائية عن جريمتي السب والقذف بالوسائل الإلكترونية طبقاً للمرسوم رقم (5) لسنة 2012 بشأن قانون مكافحة جرائم تقنية المعلومات، رسالة ماجستير، جامعة الإمارات، 2018.

وضرورة تدريب وزيادة كفاءة العاملين في ضبط هذه الجرائم تماشياً مع التطور التكنولوجي في وسائل التقنيات الحديثة، وضرورة تشديد العقوبات على مرتكبي هذه الجريمة لما تشكله من خطر جسيم وأثر بالغ على شرف واعتبار المجني عليهم.

دراسة (محمد بن عبدالعزيز بن صالح المحمود، 2014) بعنون (المسؤولية الجنائية عن إساءة استخدام وسائل التواصل الاجتماعي الحديثة)[1]، هدفت الدراسة إلى التعرف على التكييف القانوني النظامي لاستخدام وسائل التواصل الاجتماعي الحديثة، والتعرف على تقرير مبدأ المسؤولية الجنائية لمستخدمي وسائل التواصل الاجتماعي الحديثة، وقد توصلت الدراسة إلى عدد من النتائج أهمها: وسائل التواصل الاجتماعي الحديثة اليوم هي بمثابة وسائل إعلامية من نوع خاص، عرفت بالإعلام الجديد، وتعامل من حيث المسؤولية الجزائية معاملة وسائل الإعلام الأخرى، وقد أوصت الدراسة المشرع السعودي بمراعاة إعادة النظر في المادة (6) من نظام مكافحة جرائم المعلوماتية بشأن وضع عقوبة مناسبة تفرق بين المنتج والمعد والمرسل وبين المخزن.

[1]) محمد بن عبدالعزيز صالح المحمود: المسؤولية الجنائية عن إساءة استخدام وسائل التواصل الاجتماعي الحديثة، دراسة تطبيقية تأصيلية، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، 2014.

دراسة إعداد (محمد سالم الزعابي، 2014) بعنوان (الجرائم الواقعة على السمعة عبر تقنية المعلومات الإلكترونية)[1]، هدفت الدراسة إلى التعريف بالجريمة الإلكترونية وأبعادها وخصائصها والطبيعة القانونية لها من حيث أركانها وأطرافها، والوقوف على الجرائم الواقعة على السمعة الناتجة عن استخدام تقنية المعلومات وشبكة الإنترنت وفئات الجناة في هذا النوع من الجرائم، كما هدفت الدراسة إلى التعرف على القوانين الوطنية والدولية والاتفاقيات الدولية الساعية لمكافحة جرائم تقنية المعلومات بالتركيز في المقارنة على القانون الاتحادي لدولة الإمارات العربية المتحدة رقم (5) لسنة 2012، في شأن مكافحة جرائم تقنية المعلومات بالإضافة إلى التعرف على أهم إجراءات التحقيق الابتدائي في الجرائم الواقعة عبر تقنية المعلومات الإلكترونية، وقد أوصت الدراسة بضرورة إدراج جوانب إجرائية منظمة لعمليات البحث والتحري والتحقيق في مجال الجرائم الإلكترونية عبر شبكة الإنترنت، وعدم الاعتماد على قانون الإجراءات الجزائية لدولة الإمارات.

أوجه الاستفادة من الدراسات السابقة:

لقد تمكن الباحث من خلال الدراسات السابقة أن يتعرف على بعض الأفكار والأدوات والإجراءات والمراجع الخاصة بالموضوع، والتي ساعدته على

[1]) محمد سالم الزعابي: بعنوان الجرائم الواقعة على السمعة عبر تقنية المعلومات الإلكترونية، دراسة مقارنة، رسالة ماجستير، كلية الشرطة، أبوظبي، دولة الإمارات العربية المتحدة، 2014.

تدعيم الدراسة، كما ساعدت الدراسات السابقة الباحث على التعرف للتوصيات والمقترحات التي توصل إليها الباحثين في نفس المجال.

تشابه الدراسة الحالية من الدراسات السابقة:

تتشابه الدراسة الحالية من الدراسات السابقة في الاهتمام بموضوع المسؤولية الجنائية عن جرائم السب والقذف عبر شبكة الإنترنت، كما اتفقت تلك الدراسات السابقة من الدراسة الحالية بمنهج الدراسة حيث استخدمت معظم تلك الدراسات المنهج الوصفي بمجالاته وأساليبه المختلفة.

اختلاف الدراسة الحالية عن الدراسات السابقة:

اختلفت الدراسة الحالية عن الدراسات السابقة في الأهداف التي سعت إليها كل دراسة من الدراسات السابقة عن الأهداف التي تسعى إليها الدراسة الحالة وذلك لاختلاف الموضوعات التي تناولت الدراسات السابقة عن الموضوع الذي تتناوله الدراسة الحالية، أما هذه الدراسة فقد ركزت من حيث الهدف على المسؤولية الجنائية لجريمة السب والقذف عبر شبكة الإنترنت بينما تنوعت أهداف الدراسات السابقة.

خطة البحث:

المبحث الأول: الأحكام الموضوعية لجريمتي القذف والسب عبر الشبكة العنكبوتية.

المطلب الأول: الركن المادي.

المطلب الثاني: الركن المعنوي.

المبحث الثاني: أحكام العقاب على السب والقذف عبر الشبكة العنكبوتية.

المبحث الثالث: وسائل الإثبات الجنائي لجرائم السب والقذف عبر الشبكة العنكبوتية.

المطلب الأول: التفتيش.

المطلب الثاني: شهادة الشهود والخبرة التقنية في جرائم السب والقذف.

الخاتمة

المبحث الأول

الأحكام الموضوعية لجريمتي القذف والسب

عبر الشبكة العنكبوتية في التشريع المقارن

تمهيد وتقسيم:

تعتبر جريمتي السب والقذف عبر الشبكة العنكبوتية، من الجرائم الواقعة على الشرف والاعتبار، وقد نص المشرع الإماراتي على هذه الجريمة في المادة (20) من القانون الاتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات وتعديلاته، والتي نصت على أنه: (مع عدم الإخلال بأحكام جريمة القذف المقررة في الشريعة الإسلامية، يعاقب بالحبس والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين، كل من سب الغير أو أسند إليه واقعة من شأنه أن تجعله محلاً للعقاب أو الازدراء من قبل الآخرين، وذلك باستخدام شبكة معلوماتية، أو وسيلة تقنية معلومات، فإذا وقع السب أو القذف في حق موظف عام أو مكلف بخدمة عامة بمناسبة أو بسبب تأدية عمله عُد ذلك ظرفاً مشدداً للجريمة).

ومن خلال نص هذه المادة يلاحظ أن المشرع الإماراتي قد جرم فعلي السب والقذف، لذا يقتضي تحديد البنيان القانوني لهذه الجريمة، وذلك على النحو التالي:

المطلب الأول: الركن المادي لجريمة القذف والسب عبر الشبكة العنكبوتية.

المطلب الثاني: الركن المعنوي لجريمة القذف والسب عبر الشبكة العنكبوتية.

المطلب الأول

الركن المادي لجريمة القذف والسب عبر الشبكة العنكبوتية

تمهيد وتقسيم:

يعرف السب بأنه: (خدش شرف واعتبار شخص عمداً دون أن يتضمن ذلك إسناد واقعة معينة له)[1]، أما القذف فهو: (اسناد واقعة محددة تستوجب عقاب من تنسب إليه أو احتقاره اسناداً علينا عمدياً)[2]، وتعتبر جريمتي السب والقذف عبر الشبكة العنكبوتية من الجرائم الواقعة على الشرف والاعتبار، وقد نص المشرع الإماراتي على هذه الجريمة في المادة (20) من المرسوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات.

تتميز جريمتي السب والقذف بالوسائل الإلكترونية بسمات خاصة تميزها عن جريمتي السب والقذف التقليدية، حيث تتمثل في أنها ترتكب بواسطة وسيلة إلكترونية قد لا تتوافر في الجريمة التقليدية، وتقع على المجني عليه مباشرة، كأن ينسب إليه في وسيلة إلكترونية مادة أو كلمة مشينة أو إسناد واقعة محددة تؤدي إلى احتقاره في المجتمع[3].

---

[1]) سالم روضان الموسوي: جرائم القذف والسب عبر القنوات القضائية، ص43.

[2]) عادل عزام: جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الإلكترونية، ص68.

[3]) حوراء موسى: الجرائم المرتكبة عبر وسائل التواصل الاجتماعي، ص341 .

الفرع الأول

عناصر الركن المادي لجريمتي القذف والسب عبر الشبكة العنكبوتية

يشترط لقيام الركن المادي في جريمتي القذف والسب عبر الشبكة العنكبوتية توافر عدة عناصر هي النشاط الإجرامي وهو (فعل الإسناد) أي الإفصاح عن الواقعة المستندة، (وموضوع الإسناد) وهو الواقعة المحددة محل الإسناد التي من شأنها أن تجعل من أسندت إليه محلاً للعقاب أو الازدراء[1]، و(وسيلة الإسناد) المستخدمة وهي وسيلة إلكترونية، وصفة لهذا النشاط وهي (العلانية)، وهو ما سنبحثه تفصيلاً على النحو التالي:

أولاً: الإسناد في جريمتي القذف والسب عبر الشبكة العنكبوتية:

الإسناد هو تعبير مضمونة رمي شخص، شخص آخر بما يخدش شرفه أو اعتباره[2]، ويعرف أيضاً بأنه نسبة أمر معين، أو بتعبير آخر هو اسناد واقعة معينة تمس سمعة المجني عليه بأي طريقة من طرق التعبير[3]، لذا فإن جريمتي القذف والسب عبر وسائل التواصل الاجتماعي تقوم على فعلين أولهما: الإفصاح

---

[1]) محكمة النقض – أبوظبي في الطعون (1182 ، 1167 ، 1110) لسنة 2015 جزئي، بتاريخ 2016/2/22.

[2]) محمد سعيد نمور: الجرائم الواقعة على الأشخاص، دار عمان للنشر، عمان، 2000، ص119.

[3]) عبدالرزاق الموافي: قانون العقوبات لدولة الإمارات، معهد دبي القضائي، دبي، 2010، ص178.

عن الواقعة، أي التعبير عنها، وثانيهما: إذاعة الواقعة، أي العلانية التي تتطلبها الجريمة.

ويلاحـظ من خلال نص المادة (20) من المرسـوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات[1]، تنوع صور الإسناد[2]، في جريمتي القذف والسب التقليدية، ويمكن تقسيمها إلى عدة صور على النحو التالي:

---

[1]) تنص المادة (20) من المرسوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات على أنه: (مع عدم الإخلال بأحكام جريمة القذف المقرر في الشريعة الإسلامية، يعاقب بالحبس والغرامة التي لا نقل عن مائتين وخمسين ألف درهم ولا تجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من سب الغير أو أسند إليه واقعة من شأنها أن تجعله محلاً للعقاب أو الازدراء من قبل الآخرين، وذلك باستخدام شبكة معلوماتية، أو وسيلة من وسائل تقنية معلومات. إذا وقع القذف أو السب في حق موظف عام أو مكلف بخدمة عامة بمناسبة أو بسبب تأدية عمله عُد ذلك ظرفاً مشدداً للجريمة.

[2]) لم يفرق المشرع بين الإسناد والإخبار والمقصود بهذا الأخير أن يروي عن غيره خبراً يحتمل الصدق أو الكذب، فالجريمة تتحقق سواء كان المجني عليه شخص طبيعي او معنوي في حضوره أو في غيابه، علم بها أو لم يعلم بها، وسواء كانت الصيغة المستعملة تأكيدية أو تشكيكية، صريحة أو ضمنية، ويستوي كذلك وسيلة القذف بأي لغة كانت بشرط أن تكون مفهومة، وتتحقق وسيلة الكتابة سواء بخط اليد أو الآلة الكاتبة أو بالحاسب الآلي او بغيرها من وسائل الكتابة التي تشمل الرموز والرسوم وغيرها، كما أن الإسناد يتحقق بالإشارة في هذه الجريمة إذا قصد به نسبة واقعة لآخر. أنظر: شريف سيد كامل: قانون العقوبات الاتحادي – القسم العام، مكتبة الجامعة، الشارقة، 2009م؛ ص 132.

1- الإسناد الصريح والإسناد الضمني: وتتحقق هذه الصور إذا كانت العبارات المستخدمة في جريمتي السب والقذف عبر وسائل التواصل الاجتماعي صريحة وواضحة ومباشرة، اي تعبر عن المعنى المراد توصيله إلى الجمهور، فالقاعدة هنا أنه لا عبرة بالأسلوب الذي صاغ فيه الجاني عباراته سواء كان صريحاً— أي لا يحتاج الشخص المستخدم لوسيلة التواصل الاجتماعي إلى مجهود ذهني لاستخلاص المعنى المقصود به، أم كان ضمنيا – أي يتطلب مجهود من المجني عليه لفهمه واكتشاف المعنى الحقيقي المراد منه، وعليه فإنه يستوي أن تكون العبارات المشينة المستخدمة في الجريمة دالة دلالة واضحة وصريحة على المعنى أو كانت على سبيل التلميح أو التعرض أو التورية، ففي جميع هذه الأحول تقوم الجريمة[1].

2- الإسناد على سبيل القطع أو على سبيل الظن: قد يسند المتهم للمجني واقعة ما على سبيل الجزم واليقين، وقد يسندها إليه على سبيل الشك والاحتمال، وتتحقق الصورة الأولى من الإسناد بكل صيغة كلامية أو كتابية توكيدية تجزم حقيقة الواقعة المراد نسبتها من المتهم إلى المجني عليه، فيؤدي هذا الإسناد الذي قام به الجاني عبر وسيلة من وسائل التواصل الاجتماعي إلى المساس بشرف واعتبار المجني عليه وجعله محط ازدراء الناس، أي أن يقع الإسناد من المتهم إلى المجني عليه في هذه الجريمة على سبيل القطع واليقين. أما الصورة الثانية فتتحقق

[1]) محمد سالم الزعابي: الجرائم الواقعة على السمعة عبر تقنية المعلومات، دار النهضة العربية، القاهر، 2014م، ص57.

بصيغة كلامية أو كتابية تشكيكيه شأنها أن تلقي في أذهان مستخدم الوسيلة الالكترونية الحديثة حقيقة وقتية أو ظناً أو احتمالاً للعبارات المسندة إلى المجني عليه[1]. وتطبيقاً لذلك فقد قضت محكمة تمييز دبي بأنه: (من المقرر في قضاء هذه المحكمة أن إسناد شخص لآخر واقعة من شأنها أن تجعله محلاً للعقاب أو الازدراء بإحدى طرق العلانية تقوم سواء كان هذا الإسناد على سبيل القطع أو على سبيل الظن آو الاحتمال ذلك أنهما متساويان في نظر القانون وترتكب بأيهما الجريمة – ولم يتطلب القانون في هذه الجريمة إسناد واقعة معينة إنما تقوم على ما يخدش شرف المجني عليه واعتباره[2]

3- الإسناد على سبيل الاستفهام: تتحقق هذه الصورة عندما يفرغ المتهم عباراته في صيغة استفهامية، كمن يطرح سؤالاً يسأل فيه عن صحة إسناد واقعة مشينة إلى المجني عليه دون تقديم إجابة، كأن يقول: هل صحيح إن فلان لص وزنديق؟، أو أن يجيب على سؤال يحتوي على عبارات مشينة بلفظ نعم أو لا، إذا كانت هذه الإجابة بهدف إسناد واقعة مشينة بحق المجني عليه. ويتحقق كذلك ولو كانت الإجابة في صيغة نفي متى كانت هذه العبارات دالة على أن الجاني هدف

[1]) حوراء موسى: الجرائم المرتكبة عبر وسائل التواصل الاجتماعي، مرجع سابق، ص342.

[2]) محكمة تمييز دبي، الطعن رقم 214، لسنة 2013 جزاء، جلسة 2013/3/18م.

إلى إسناد الوقائع المحددة إلى المجني عليه وتأكيدها، ولم يكن النفي في حقيقته إلا من باب سب وقذف[1].

4- الإسناد عن طريق الرواية عن الغير: تتحقق هذه الصورة عندما يروي الجاني عن الغير خبر ما، إما بسرد معلوماته الخاصة أو بسرد إشاعة تمس سمعته وشرفه واعتباره عبر وسائل التواصل الاجتماعي دون التحقق من صحتها، ففي الحالتين يتحقق المساس بشرف واعتبار المجني عليه، خاصة أن من يروي عن الغير إنما يعطي معلومات غير علنية لم تكن موجودة من قبل للعلن، أو أنه يوسع من نطاق العلانية لهذه العبارات، وقد يكون نشاطه من هذه الوجهة أشد خطورة على شرف المجني عليه ممن أدلى للغير بهذه المعلومات ويأخذ هنا نفس حكم من يقوم بنشرها ولو كانت منقولة عن الغير[2].

ثانياً: موضوع الإسناد في جريمتي القذف والسب عبر الشبكة العنكبوتية:

موضوع الإسناد هو "الواقعة التي يسندها المتهم إلى المجني عليه ويكون من شأنها المساس بشرفه واعتباره"[3]، وهو (كل ما يتضمن خدشاً لشرف المجني

---

[1]) عادل إبراهيم إسماعيل: جرائم السب والقذف عبر الإنترنت، مرجع سابق، ص39.

[2]) خالد حسين عبدالتواب: جرائم القذف والسب العلني عبر الإنترنت، أطروحة دكتوراه، كلية ا لحقوق جامعة عين شمس، 2016، ص82.

[3]) حسن محمد ربيع: شرح قانون العقوبات الاتحادي- المبادئ العامة للجريمة، دار النهضة العربية، القاهرة، 1993، ص133.

عليه أو اعتباره بأي وجه من الوجوه[1]، وقد يكون ذلك بإسناد عيب معين أو نقيصة، كأن يكون عيباً أخلاقياً.

ولم يقتصر المشرع الإماراتي في اعتبار جريمة القذف على حالة ما إذا كانت الواقعة المسندة توجب عقاب من أسندت إليه فقط، وإنما أضاف إلى ذلك حالة ما إذا كانت الواقعة المسندة توجب احتقار المسند إليه أمام الناس؛ كأن تكون قد تسببت في هبوط قدر المجني عليه وكرامته في نظر الناس[2]. والحقيقة أن الوقائع التي يترتب عليها هذا الأثر كثيرة جداً ويصعب حصرها، وقد تكون منافية للقيم الأخلاقية أو التعاليم الدينية أو التقاليد الاجتماعية.

ويستوي أن تنسب الواقعة إلى الشخص باعتباره فاعلاً لها أو باعتباره معتدى عليه فيها، ولا يشترط أن يؤدي ذلك إلى احتقار المجني عليه عند أهل وطنه، بل بكفي لقيام الجريمة أن يكون الإسناد من شأنه تحقير المسند إليه عند من يخالطهم أو يعاشرهم[3].

---

[1]) مؤيد محمد علي القضاة: شرح قانون العقوبات الاتحادي الإماراتي، القسم العام، مكتبة الجامعة، الشارقة، 2012، ص96.

[2]) عبدالرازق الموافي: شرح قانون مكافحة جرائم تقنية المعلومات الإماراتي، معهد دبي القضائي، دبي 2016، ص102.

[3]) حكم المحكمة الاتحادي العليا – الاحكام الجزائية – الطعن رقم 79 لسنة 2011 ، قضائية – في 2011/6/21.

ويشترط توافر ثلاثة شروط في الواقعة المسندة للمجني عليه هي:

1- أن تكون الواقعة التي يسندها الجاني للمجني عليه في جريمة القذف محددة: الواضح هن النصوص التشريعية التي تنظم الجرائم الواقعة على السمعة، أن الصفة المميزة لجريمة القذف هي المساس بالشرف والاعتبار، وقد تطلب المشرع الإماراتي أن تكون محددة ومعينة، وذلك بخلاف جريمة السب التي لا تتطلب ذلك، فالإسناد الغامض وغير المحدد يصلح أن يكون سباً وليس قذفاً، كما لو نسب الجاني إلى المجني عليه باستخدام تطبيق (الفيس بوك) أنه سرق ألف درهم من المجني عليه مثلاً، أو أنه استغل منصبه ووظيفته وتقاضى الرشوة؛ فإن جريمة القذف تقوم بسبب أن الواقعة محددة ومعينة. فالإسناد المحدد لا الغامض هو المنشئ لجريمة القذف، ولكن مع الأخذ بالاعتبار أن تحديد ما إذا كانت هذه الواقعة المسندة من الجاني إلى المجني عليه تشكل جريمة القذف هو من الأمور الموضوعية المتروكة لقاضي الموضوع يقدرها حسب ظروف الواقعة[1]، ويشترط في الأمر المسند بوسائل التواصل الاجتماعي إلى المجني عليه أن يكون معيناً ومحدداً على نحو يمكن إقامة الدليل عليه، لا أن يكون في صورة مرسلة مطلقة غير منضبطة، بل يكون صريحاً أو ضمنياً يمكن استخلاصه من سياق الكلام الذي في مجموعة يتضمن المعنى الحقيقي الذي ابتغاه الجاني عن طريق الكناية أو الاستعارة أو التلميح، والواقعة محل الإسناد هي تعبير عن حقيقة يمكن إدراكها

[1]) عمار عباس الحسيني: جرائم الحاسوب والإنترنت، منشورات زين الحقوقية، بيروت، 2017، ص176.

وإثباتها، ولا يشترط في تحديد الواقعة أن تكون مفصلة تفصيلاً يتضمن جميع عناصرها، أما بالنسبة للفظ الذي لا ينطوي على نسبة وقائع معينة فلا يتوفر فيه السب والقذف[1]. ويرى البعض – ويتفق معه الباحث – أنه يجب أن يوكل لقاضي الموضوع هذا التحديد، والصلة مع ذلك وثيقة بين هذا الضابط والضابط الذي يجعل العبرة في تحديد الواقعة بقابليتها للإثبات، فقبول الواقعة للإثبات يفترض أنه قد أمكن تحديد الظروف التي أحاطت بها والتي يرد عليها الإثبات ويستخلص منها ثبوت الواقعة، وفي حالة قبول ترك الفصل في تحديد الواقعة إلى قاضي الموضوع فإن قابلية الواقعة هي أهم اعتبار يمكن أن يسترشد به للقول بأن الواقعة محددة.

2- أن تكون الواقعة من شأنها أن تجعل من أسندت إليه محلاً للعقاب أو الازدراء: لم يحتم قانون مكافحة جرائم تقنية المعلومات الإماراتي لقيام جريمة القذف بوسائل التواصل الاجتماعي أن تكون الواقعة المسندة جريمة معاقباً عليها، بل يكفى أن يكون من شأنها أن تجعل من أسندت إليه محلاً للعقاب أو الازدراء، ويتحقق ذلك في كل ما من شأنه الحط من قدر المجني عليه وكرامته في نظر الناس. وتطبيقاً لذلك قضت محكمة تمييز دبي بأن: (إذ نص القانون في جريمة القذف على أن تكون الواقعة المسندة بما يوجب عقاب من أسندت إليه أو احتقاره عند أهل وطنه فإنه لم يحتم أن تكون الواقعة جريمة معاقب عليها قانوناً بل اكتفى بأن يكون من شأنها احتقار المسند إليه عند أهل وطنه)[1]. ويتضح من ذلك أن

---

[1]) سالم الموسوي: جرائم القذف والسب عبر القنوات الفضائية، مرجع سابق، ص81.

[1]) محكمة تمييز دبي، الطعن رقم 112 لسنة 2016، جزائي، جلسة 2016/3/19.

الوقائع التي يترتب عليها احتقار المجني عليه في جريمتي السب والقذف بوسائل التواصل الاجتماعي تختلف عن الوقائع التي تؤدي إلى عقاب المجني عليه، لأن هذه الوقائع إن صحت فإنها تعرض الذي أسندت إليه إلى عقوبة جنائية، عدا عن تعرضه للاحتقار أو الازدراء. ولا يشترط في جريمة القذف أن تكون الواقعة المسندة للمجني عليه كاذبة، فالجريمة تعد قائمة حتى لو كانت الوقائع صحيحة، ولذا لا يسمح للقاذف أن يثبت صحة إسناده للدفاع عن نفسه إلا إذا كانت هذه الوقائع مسندة إلى موظف عام وتتعلق بأمور وظيفته[1].

ثالثاً: تحديد الواقعة والشخص المسند إليه في الواقعة:

لا تقوم جريمة القذف إلا بإسناد الواقعة إلى شخص معين، أما في حالة لم بكن الإسناد موجهاً إلى شخص محدد أو معين، أو كان التعيين غير كافي لتحديد الواقعة المسندة إليه، فلا تتحقق جريمة القذف، لذلك يجب أن يكون المجني عليه في جريمة القذف معيناً، ولا يهم أن يكون الشخص المقذوف محدداً بالاسم، إنما يكفي أن يكون معيناً بشكل ولو نسبي بحيث يعرف من الشخص المقصود ولو كانت هذه المعرفة تقتصر على عدد قليل من الأشخاص[1].

---

[1]) حوراء موسى: الجرائم المرتكبة عبر وسائل التواصل الاجتماعي، مرجع سابق، ص347.

[1]) خليفة راشد الشعالي: شرح قانون العقوبات الإماراتي، النظرية العامة للجريمة، ط3، دار وائل للنشر، عمان، 2010، ص192.

وفي هذا الشأن قضت محكمة تمييز دبي بأنه: (من المقرر أنه بكفي لوجود جريمة السب أو القذف أن تكون عباراته موجهة على صورة يسهل معها فهم المقصود منها ومعرفة الشخص الذي يعنيه الساب أو القاذف، فإذا أمكن للمحكمة أن تدرك من فحوى عبارات السب أو القذف من هو المعني به استنتاجاً من غير تكليف ولا كبير عناء من جماع الأدلة المطروحة عليها، وهي ليست مطالبة بالأخذ بالأدلة المباشرة، بل لها أن تستخلص الحقائق من كل ما يقدم إليها من أدلة ولو كانت غير مباشرة متى كان ما حصل عليه الحكم من هذه الأدلة لا يخرج عن الاقتضاء العقلي والمنطقي وكانت الأركان الأخرى متوفرة حق العقاب على الجريمة ولو كان المقال خلواً من ذكر اسم الشخص المقصود[1]. ويتضح من هذا الحكم أنه بكفي لقيام جريمة القذف أن تكون عبارات القذف المسندة والموجهة إلى المجني عليه يسهل معها فهم المقصود منها وأيضاً معرفة الشخص الذي يعنيه القاذف، لأن القول بغير ذلك يؤدي إلى التضييق من نطاق القذف إلى الحد الذي يخل بالهدف من التجريم، ويرى الباحث وفقاً لذلك أنه لا يشترط لقيام جريمة القذف عبر وسائل التواصل الاجتماعي التحديد الدقيق للمجني عليه بذكر اسمه بالكامل عبر الوسيلة الإلكترونية، بل يكفي ذكر الأحرف الأولى من اسمه أو وضع صورته أو تحديد مهنته أو وظيفته أو صفة قديمة يستطيع أن يستدل بسهولة على شخصيته منها.

[1]) محكمة تمييز دبي، الطعن رقم 404 لسنة 2013 جزائي، جلسة 2013/4/10.

رابعاً: وسيلة الإسناد في جريمتي القذف والسب عبر الشبكة العنكبوتية:

القاعدة العامة أن المشرع الإماراتي لم يهتم بالوسيلة المستخدمة في ارتكاب الجرائم، إلا أنه أعطى أهمية بالغة وشدد من عقوبة بعض الجرائم نظراً للوسيلة التي استخدمت في ارتكابها، ومنها جريمتي السب والقذف عبر الشبكة العنكبوتية، فمن خلال الرجوع إلى نص المادة (20) من المرسوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات، يتضح وجود وسيلتين من وسائل الإسناد في جريمتي السب والقذف عبر وسائل تقنية المعلومات هما: استخدام شبكة معلوماتية، أو وسيلة تقنية معلومات. وهو ما سيتم توضيحه كالتالي:

(أ) الشبكة المعلوماتية:

عرفت المادة (1) من المرسوم بقانون اتحادي رقم (5) لسنة 2012 الشبكة المعلوماتية بأنها: (ارتباط بين مجموعتين أو أكثر من البرامج المعلوماتية ووسائل تقنية المعلومات التي تتيح للمستخدمين الدخول وتبادل المعلومات). **وتقسيم الشبكات المعلوماتية إلى ما يلي:**

1. **الشبكات العامة:** وهي التي تقدم خدمات تكون متاحة للأفراد بشكل عام، لأنها شبه مفتوحة بطبيعتها، حيث يتمكن الأفراد من الاتصال مع غيرهم بحرية وسهولة، ولا تستلزم التسجيل المسبق بها، كما أنه لا توجد قيود أو عوائق تمنع الأفراد من الاستفادة من إمكانياتها المتاحة، فمثلاً يستطيع أي شخص أو مستخدم لهذه الشبكة الإلكترونية أن يشئ موقعاً على الشبكة العالمية تتضمن معلومات

وبيانات وصوراً وغيرها، ويمكن الاطلاع عليها من قبل أي شخص في جميع أنحاء العالم، وتكون هذه المعلومات مفيدة في حال استخدمت بشكل صحيح، وقد تكون ضارة إذا هدف الشخص من ورائها الإساءة إلى الآخرين والمساس بشرفهم واعتبارهم، ومن أمثلتها مواقع التواصل الاجتماعي: فيس بوك، تويتر، انستجرام ... وغيرها.

2. **الشبكات الخاصة:** هي التي تقتصر خدماتها على شخص معين بذاته، ولا يستطيع أحد الاطلاع على محتواها إلا صاحبها أو من يملك إمكانية الدخول إليها عن طريق كلمة سر خاصة، مثل البريد الإلكتروني أو تطبيق الواتساب، التي تحظى المراسلات من خلالها بالخصوصية والحماية القانونية لسريتها[1].

(ب) وسيلة تقنية المعلومات:

عرف المشرع الإماراتي وسيلة تقنية المعلومات في المادة (1) من المرسوم بقانون اتحادي رقم (5) لسنة 2012 (تقنية المعلومات) بأنها: (أي أداة الكترونية مغناطيسية، بصرية كهروكيميائية، أو أي أداة أخرى تستخدم لمعالجة البيانات الإلكترونية وأداء العمليات المنطقية والحسابية أو الوظائف التخزينية، ويشمل أي وسيلة موصلة أو مرتبطة بشكل مباشر، تتيح لهذه الوسيلة تخزين المعلومات الالكترونية أو إيصالها للآخرين.

[1]) دينا عبدالعزيز: الحماية الجنائية من إساءة استخدام مواقع التواصل الاجتماعي، مرجع سابق، ص103.

وتطبيقاً لذلك قضت محكمة تمييز دبي بأنه: (.. وكان تقدير المحكمة بأن هذا القول يجعل المجني عليه محلاً للازدراء من قبل الآخرين فإن ذلك يعد سائغاً وصحيحاً ومتفقاً مع صحيح القانون ذلك أن كل فعل أو قول ثبت بحكم العرف بأنه فيه ازدراء وحطاً من الكرامة في أعين الناس تتوفر به أركان جريمة السب كما هي معرف بها في القانون فإن ما يثيره الطاعن بأن المبلغ ليس المقصود بالرسالة والحكم لم يبين من أرسل الرسالة وكيفية إرسالها لا يكون له محل، لما كان ذلك وكانت وسيلة تقنية المعلومات أداة الكترونية مغناطيسية، بصرية، كهروكيميائية أو أية أداة أخرى تستخدم لمعالجة البيانات الالكترونية وإدارة عمليات المنطق والحساب أو الوظائف التخزينية وتشمل أي وسيلة موصولة أو مرتبطة بشكل مباشر تتيح لهذه الوسيلة تخزين المعلومات الالكترونية أو إيصالها للآخرين من خلال تخزين بيانات أو اتصالات تتعلق أو تعمل بالاقتران مع مثل هذه الأداة بارتباط بين أكثر من وسيلة للحصول على معلومات وتبادلها لأن المشرع لم يحدد تقنية المعلومات بوسيلة معينة فقد تشمل الحاسب الآلي والشبكة المعلوماتية وأجهزة الموبايل والبلوتوث وجهاز الكتروني ثابت أو منقول سلكي أو لاسلكي يحتوي على نظام معالجة البيانات أو تخزينها أو استرجاعها أو إرسالها أو استقبالها أو تصفحها- كموقع التواصل الاجتماعي الواتساب والفيس بوك والرسائل القصيرة - يؤدي وظائف محددة حسب البرامج والأوامر المعطاة له- يمكن أن يكون من خلال كتابة وصور وصوت وأرقام وحروف ورموز واشارات وغيرها- وأية وسيلة تنشأ في المستقبل تحت ذات المعطيات باعتبارها ذات طابع مادي تتحقق بكل فعل أو

سلوك غير مشروع مرتبط بأي وجه او بأي شكل من الأشكال بالشبكة المعلوماتية الموصولة سلكياً أو لاسلكياً بالحاسب الآلي أو مشتقاته والهواتف النقالة والذكية[1].

ومفاد هذا الحكم أن جريمة السب أو القذف يمكن أن تقع وتثبت بأي وسيلة من الوسائل الإلكترونية سواء عن طريق رسالة نصية أو برنامج الواتساب أو فيس بوك أو تويتر أو سناب شات أو انستجرام أو غيرها من وسائل التواصل الاجتماعي، وبذلك يكون المشرع قد حدد وسيلتين لارتكاب جريمتي السب والقذف إلكترونياً، سواء بصدوره علنية أم غير علنية، وترك أمر الوسيلة بحسب الواقعة سواء كانت علنية عن طريق شبكة معلوماتية أي شبكة عامة ومتاحة لجميع الأفراد أو غير علنية باستخدام أجهزة الهاتف المتحرك من خلال شبكات التواصل

---

[1]) محكمة تمييز دبي، الطعن رقم 895 لسنة 2015؛ جلسة 23/2/2015م. كما قضت المحكمة الاتحادية العليا، الطعن رقم 191 لسنة 2017 جزاء شرعي، جلسة 13/6/2017 بأنه: ((حيث أن الوقائع– على ما يبين من مطالعة الحكم المطعون فيه وسائر أوراق الطعن– تتحصل في أن النيابة العامة أحالت المطعون ضده إلى المحاكمة الجرائية بوصف أنه بتاريخ 2017/1/23 بدائرة أم القوين استخدم إحدى وسائل تقنية المعلومات "برنامج الواتساب" بأن قام بسب المجني عليه بعبارة السب الواردة في الأوراق وارسال صور مخلة بالآداب يحمل معناها عزماً على السب على النحو المبين بالأوراق... ولوسيلة تقنية المعلومات من خطورة أفرد لها المشرع قانون خاص يحكم ضوابط الفعل المربوط باستخدام تلك الوسيلة في جرائم السب والقذف التي تختلف من حيث الشكل والوسيلة المستخدمة في تطبيقها لشموله الأشخاص الطبيعيين والمعنويين وما دام أنه وجد قانون خاص يعالج ما قام به الجاني من سب وقذف باستخدامه وسيلة تقنية المعلومات فإنه لا بصح بعد ذلك الاحتجاج بما افرد إليه قانون العقوبات الاتحادي في المادة 374.

الاجتماعي الحديثة في بعض الأحيان، وغيرها من البرامج وتكون في هذه الحالة بصورة غير علنية.

وعليه، يتضح مما سبق أنه يمكن أن يتحقق الإسناد بالقول في جريمتي السب والقذف بالوسائل الإلكترونية بالاعتداء بالقول على الآخرين عن طريق تسجيل صوتي أو مرئي، أو عبر الوسائل الإلكترونية الحديثة الأخرى، والقول هنا نعنى به الصوت، ولا عبرة بحجم القول سواء كان جملة واحدة أو جملاً عديدة أو جزء من جملة أو لفظ يعاقب عليه قانوناً، ونجد أن المشرع الإماراتي عندما نص على جريمتي السب والقذف بوسائل تقنية المعلومات قد حدد وسيلتين ترتكب من خلالهما هذه الجريمة، وذلك سعياً منه إلى محاربة هذه الجريمة على اختلاف وسائل ارتكابها.

الفرع الثاني

العلانية في جريمتي القذف والسب عبر الشبكة العنكبوتية

تعتبر العلانية من أهم عناصر الإسناد في جريمتي السب والقذف عبر وسائل التواصل الاجتماعي، لأنها الوسيلة لعلم أفراد المجتمع بعبارات القذف أو السب التي وجهت للمجني عليه[1]، وقد نص المشرع الإماراتي في قانون العقوبات الاتحادي على جريمتي القذف والسب التي تتم علانية ووضع لها عقوبة تختلف عن تلك التي تتم بصورة غير علنية، في حين أنه وضع عقوبة واحدة لجريمتي السب والقذف سواء وقعتا بصورة علنية آو غير علنية[2].

ويلزم لقيام جريمتي السب والقذف في التشريع الإماراتي أن تقع بصورة علنية، وشرط العلانية[3] شرط أساس لأن الخطورة هنا تكمن في علانية هذه

---

[1]) علي حمودة: شرح الأحكام العامة لقانون العقوبات الاتحادي، أكاديمية شرطة دبي، 2008، ص172.

[2]) مؤيد محمد علي القضاة: شرح قانون العقوبات الاتحادي الإماراتي، مرجع سابق، ص103.

[3]) نصت المادة (373) من قانون العقوبات الاتحادي على شرط العلانية بأنه: (يعاقب بالحبس مدة لا تزيد عن سنة أو بالغرامة التي لا تجاوز عشر آلاف درهم من رمى غيره بإحدى طرق العلانية بما يخدش شرفه أو اعتباره دون أن يتضمن ذلك إسناد واقعة معينة. وتكون العقوبة الحبس مدة لا تزيد عن سنتين والغرامة التي لا تجاوز عشرن ألف درهم في الحالتين، أو إحدى هاتين العقوبتين إذا وقع السب في حق موظف عام أو مكلف بخدمة عامة أثناء أو بسبب أو بمناسبة تأدية الوظيفة أو الخدمة العامة، أو كان ماساً بالعرض أو خادشاً لسمعة العائلات أو كان ملحوظاً فيه تحقيق غرض غير مشروع، وإذا وقع السب بطرق النشر في إحدى الصحف أو المطبوعات عد نلك ظرفاً مشدداً.

الجريمة، ولأن إعلانها للغير سواء عن طريق العبارات أو الكلمات التي تمس بشرف أو اعتبار المجنى عليه يعنى ان يحيط علم الكثير من الناس بالواقعة المشينة المسندة إلى المجني عليه[1].

والعلانية هي خلاف السرية، وهي الجهر بالشيء أو إظهاره وتعميمه، أي إحاطة الجمهور علماً به، لذلك يشترط لقيام جريمة القذف أن يكون إسناد الواقعة التي من شأنها أن نؤدي إلى المساس بشرف أو اعتبار المجني عليه هو إسناد علني، فالعلانية هي الركن المميز في هذه الجريمة[2].

ولقد أوضح المشرع الإماراتي في قانون العقوبات الاتحادي طرق وأساليب تحقق العلانية، وذلك في المادة (9) منه، والتي نصت على أن: (تعد طرقاً للعلانية في حكم هذا القانون: 1- القول أو الصياح إذا حصل الجهر به أو ترديده بإحدى الوسائل الآلية في جمع عام أو في طريق عام أو في مكان مباح أو مطروق أو إذا أذيع بأية وسيلة أخرى. 2- الأعمال أو الإشارات أو الحركات إذا وقعت في مكان مما ذكر أو نقلت إلى مكان من هذه الأماكن بطريقة من الطرق الآلية أو بأية طريقة أخرى. 3- الكتابة والرسوم والصور والأفلام والرموز وغيرها من طرق التعبير إذا عرضت في مكان مما ذكر أو وزعت بغير تمييز أو بيعت

---

[1]) محمد شلال العاني: أحكام القسم العام في قانون العقوبات الاتحادي الإماراتي، النظرية العامة للجريمة، الآفاق المشرقة للنشر، ط1، عمان، 2010م، ص215.

[2]) حسن محمد ربيع: شرح قانون العقوبات الاتحادي، المبادئ العامة للجريمة، مرجع سابق، ص136.

إلى الناس أو عرضت عليهم للبيع في أي مكان). كما نصت المادة (373) من قانون العقوبات الاتحادي على العقوبة المقررة لمن يخدش شرف أو اعتبار أحد الأشخاص بإحدى طرق العلانية السابقة، حيث نصت على أن: (يعاقب بالحبس مدة لا تزيد على سنة أو بالغرامة التي لا تجاوز عشر آلاف درهم من رمى غيره بإحدى طرق العلانية بما يخدش شرفه أو اعتباره دون أن يتضمن ذلك إسناد واقعة معينة). ونصت المادة (378) من نفس القانون على معاقبة كل من يقوم بنشر – بإحدى طرق العلانية المنصوص عليها في المادة (9) عقوبات – أخبار أو صوراً أو تعليقات تتصل بأسرار الحياة الخاصة أو العائلية للأفراد، ولو كانت صحيحة، حيث نصت على أن: (يعاقب بالحبس والغرامة كل من اعتدى على حرمة الحياة الخاصة أو العائلية للأفراد، وذلك بأن ارتكب أحد الأفعال الآتية في غير الأحول المصرح بها قانوناً أو بغير رضاء المجني عليه: .... كما يعاقب بذات العفوية من نشر بإحدى طرق العلانية أخبار أو صوراً أو تعليقات نتصل بأسرار الحياة الخاصة أو العائلية للأفراد ولو كانت صحيحة).

يتضح من ذلك أن علانية الإسناد هنا تتم باستخدام وسيلة من وسائل التواصل الاجتماعي، وهكذا فإن العلانية في الإسناد تتحقق عندما يقوم الجاني بالتعبير عن المعنى المقصود منه المسند للمجني عليه ويكون بطريقة تسمح لكافة الناس بالاطلاع عليه.

والجدير بالذكـر أن هنـاك العديـد من الخدمـات التي تقدمـها وسائل التقنية الحديثـة؛ منها الهـاتف المتحـرك، والبريد الإلكتروني وغيرها من وسـائل تقنيـة المعلومات التي تكفـل سرية الاتصالات والمرسلات، كالرسائل الخاصة التي تتمتع بالحماية القانونية المقررة لسرية الاتصالات عن بعد، الأمر الذي كفل عدم قدرة الآخرين على كشف مضمونها أو الاطلاع عليهـا إلا في حـال سمـح بذلك أحد الأطـراف المعنيين بهـذه الرسـالة. إلا أنه يمكـن أن تتوفر العلانية في الكتابات التي تحتوي على السب والقذف المرسلة عبر وسيلة إلكترونية في حال تم إرسالها إلى العديد من الأفراد الذين لا يجمع بينهم أي روابط بما يتوفر معه وصف التوزيع[1].

وتطبيقاً لذلك فقد قررت محكمة تمييز دبي بأن: (العلانية في جريمة القذف بطريق المطبوعات المنصوص عليها في قانون العقوبات الاتحادي يشترط لتوافرها عنصران هما: توزيع الكتابة المتعلقة بعبارات القذف على عدد من الناس بغير تمييز، وانتواء إذاعة ما هو مكتوب. ولا يشترط أن يكون التوزيع قد وصل إلى عامة الناس، بل بكفى أن يكون المكتوب قد وصل إلى عدد من الناس، ولو كان

[1]) المقصود بالتوزيع هو تسليم نسخ متعددة من المكتوب أو الرسم أو الرموز أو الأفلام او غيرها من طرق التعبير بحيث يمكن للجمهور رؤيتها أثناء وجودهم كما ذكرناه سابقاً في الطريق العام أو المكان المطروق، او في مكان خاص، ويمكن أن تكون الرؤية محتملة لتحقق العلانية. أنظر: خالد حسين عبد التواب: جرائم القذف والسب العلني عبر الإنترنت، مرجع سابق، ص 93.

قليلاً، سواء كان عن طريق تداول نسخة واحدة أو تداول عدة نسخ، ما دام ذلك لم يكن بفعل المتهم أو كان نتيجة حتمية لفعله ولا يتصور أنه يجهلها)[1].

وعليه فإن العلانية تتوافر في التعبيرات التي تتضمن كتابات أو صور أو في حال قيام المتهم بإرسالها عبر وسيلة من وسائل التواصل الاجتماعي أو عبر رسائل البريد الإلكتروني إلى العديد من الأشخاص سواء تربطهم أو لا تربطهم أية رابطة، رغبة منه في خدش شرف واعتبار المجني عليه حيث تؤدي إلى احتقاره وازدراءه من قبل الناس، سواء كان شخص طبيعي أو معنوي، ونستنتج من ذلك أن العلانية هنا تتوفر للكتابات والصور والرسوم التي تتضمن عبارات مسيئة موجهه للمجني عليه تمس بشرفه واعتباره وتحط من كرامته أمام الناس، في حال تم عرضها بوسائل تقنية المعلومات.

ولكن في الوقت ذاته يمكن أن تقع الجريمة بالرغم من عدم تحقق العلانية فيها، كما لو قام شخص بسب آخر عن طريق برنامج الواتساب، ففي هذه الحالة تعتبر غير علانية لأن الجريمة وقعت بين شخصين وعن طريق محادثة خاصة بينهما، دون السماح للأفراد برؤيتها، لذلك فإنه يقع على قاضي الموضوع استخلاص العلانية من وقائع الدعوي المعروضة أمامه بحسب الظروف والمكان والوسيلة الإلكترونية المستخدمة في وقوع الجريمة. وفي هذا الشأن قضت محكمة نقض أبوظبي بأنه: (لما كان من المقرر أن القانون لم يرسم شكلاً خاصاً يصوغ

[1]) محكمة تمييز دبي، الطعن رقم (59) لسنة 2011، جلسة 2011/1/24.

فيه الحكم ببيان الواقعة المستوجبة للعقوبة والظروف التي وقعت فيها فمتى كان مجموع ما أورده الحكم كافياً في تفهم الواقعة بأركانها وظروفها حسبما استخلصتها المحكمة كان ذلك محققاً لحكم القانون، ولما كان الحكم المطعون فيه قد بين في مدوناته عبارات السب العلني التي وجهها الطاعن إلى المجني عليه وكان ذلك بقسم العملاء بشركة الاتصالات وأثناء مواعيد العمل وفي حضور زملائه وهو مكان عام يتردد عليه الكثير من العملاء الأمر الذي يستفاد منه علانية الإسناد التي استظهرها الحكم ويتحقق به القصد الجنائي. وكان القصد الجنائي في جرائم السب يتحقق متى كانت الالفاظ الموجهة إلى المجني عليه شائنة بذاتها كما هو الحال في الدعوى المطروحة، فلا حاجة في هذه الحالة إلى الاستدلال عليه ولا على المحكمة إن هي لم تبحدث عن قصد الإذاعة على استقلال طالما أن هذا القصد يستفاد من علانية الإسناد، فإن الحكم يكون قد بين واقعة الدعوي بما تتوافر به كافة العناصر القانونية لجريمة السب التي أدان الطاعن بها وأورد على ثبوتها في حقه أدلة مستمدة من أقوال الشهود والقرينة المستمدة من أقوال المجني عليه وهي أدلة سائغة ومن شأنها أن نؤدي إلى ما رتبه الحكم عليها فإن ما ينعاه الطاعن على الحكم المطعون فيه من قصور في بيان أركان الجريمة يكون في غير محله)[1].

وخلاصة لما تقدم يتضح عدم اشتراط عنصر العلانية بمفهومها الوارد في قانون العقوبات الإماراتي بالنسبة لجريمة السب والقذف عبر وسائل تقنية

[1]) محكمة نقض أبوظبي، الدائرة الجزائية، حكم رقم 522، لسنة 2012 .

المعلومات التي نص فيها المشرع بتحقق الجريمة بالوسائل التي حددها في المادة (20) من المرسوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات، وهما: الشبكة المعلوماتية أو وسيلة تقنية المعلومات.

المطلب الثاني

الركن المعنوي لجريمة القذف والسب عبر الشبكة العنكبوتية

تعتبر جريمة القذف والسب جريمة عمدية، حيث يشترط توافر القصد الجنائي فيها[1]، وهو القصد العام الذي يتطلبه وجود علم بعناصر الجريمة وإرادة تتجه إلى السلوك المكون لهذه الجريمة وتتحقق بتحقق النتيجة وهي النيل من شرف المجني عليه وكرامته.

فالقصد الجنائي في جريمتي السب والقذف بالوسائل الإلكترونية يتحقق بانصراف إرادة الجاني إلى الفعل باستخدام الشبكة المعلوماتية وتقنية المعلومات كوسيلة لإيصال القذف والسب للمجنى عليه، ولا عبـرة بعد ذلك بما يكـون قد دفع الجاني إلى ارتكاب فعلتـه أو الغـرض الذي توخاه منها[2]، فجريمتـي السب

---

[1]) وتطبيقاً لذلك فقد قضت محكمة تمييز دبي بأن (القصد الجنائي في جريمة القذف ليس إلا علم القاذف بأن ما اسنده المقذوف من شأنه لو صح أن يلحق بهذا الأخير ضرراً مادياً وأدبياً وهذا الركن يتوافر إذا كانت عبارات القذف ذاتها من الصراحة والوضوح بحيث يكون من المفروض علم القاذف بمدلولها وأنها تمس المجني عليه في سمعته أو تستلزم عقابه عندئذ يكون مضمون العبارات حاملاً بنفسه الدليل الكافي على توافر القصد الجنائي، تمييز دبي– الدائرة الجزائية (القذف) الطعن رقم (491) لسنة 2006، جلسة 2006/5/13.

[2]) قضت محكمة تمييز دبي بأنه: (من المقرر أن القانون لا يتطلب في جريمة القذف قصداً خاصاً بل يكفي توافر القصد العام الذي يتحقق متى أذاع القاذف الأمور المتضمنة للقذف وهو عالم أنها لو كانت صادقة لأوجبت عقاب المقذوف في حقه أو احتقاره عند الناس ولا يؤثر في توافر هذا القصد أن يكون القاذف حسن النية أي معتقداً صحة ما رمي به المجني عليه من

والقـذف بالوسائل الالكترونية تعتبر من الجرائم العمدية، حيث يتحقق ركنها المعنوي في صورة القصد الجنائي فالركن الغير عمدي لا يمكن أن يتحقق في هذه الجريمة مهما بلغت جسامة الخطأ[1].

وعليه سنتناول هذا المطلب من خلال الآتي:

وقائع القذف، والمرجع في تعريف حقيقة القذف وبما يطمئن إليه القاضي في تحصيله لفهم الوقائع في الدعوى. الطعن رقم 81 لسنة 2016 جزاء، جلسة 2016/2/22.

[1]) جلال الزعبي، أسامة المناعسة: جرائم تقنية نظم المعلومات الإلكترونية، مرجع سابق، ص 203.

الفرع الأول

العلم في جريمتي القذف والسب عبر الشبكة العنكبوتية

تفترض جريمتي القذف والسب عبر وسائل التواصل الاجتماعي أن تكون الواقعة المسندة إلى المجني عليه على تكييفين، أنها تستوجب عقابه أو أنها تستوجب احتقاره عند أهل وطنه، أو عند الوسط الذي يعيش فيه، حيث يعتبر التكييف في ذاته أحد أركان الجريمة[1].

ومن ثم تقضي القواعد العامة في القصد الجنائي أن يحيط العلم به، والعلم المقصود هنا هو العلم الفعلي، فلا يكفي أن يكون مفترض، ولا يكفي استطاعة العلم[2].

وهذا يقتضي تناول العلم بواقعة جريمتي القذف والسب عبر الشبكة العنكبوتية والعلم بعلانية الإسناد، وذلك على النحو التالي:

1. علم الجاني بمعنى العبارات المسندة إلى المجني عليه: يجب أن يكون الجاني على علم بمعنى العبارات المتضمنة للسب والقذف التي تؤدي إلى خدش شرف أو اعتبار المجني عليه، ويكون هذا العلم مفترض طالما أن العبارات تخدش

---

[1]) د إمام حسنين خليل عطا الله: الحماية الجنائية لوسائل تقنية المعلومات في التشريعات العربية – الإمارات نموذجا، مركز الدراسات والاستطلاعات، وزارة الداخلية، أبوظبي، 2016م، ص 98..

[2]) غانم مرضي الشمري، الجرائم المعلوماتية، دار الثقافة للنشر، عمان، 2016م، ص 182..

شرف المجني عليه، ويجب هنا على المتهم أن يثبت عكس ذلك، إذ يستطيع المتهم أن ينفي القصد الجنائي إذا أثبت أنه كان يجهل معنى الكلمات التي وجهها إلى المجني عليه متضمنة عبارات السب، أما في حالة أن العبارات كانت لا تخدش شرف أو اعتبار المجني عليه، فيجب على المجني عليه أن يثبت أن المتهم كان يقصد بهذه العبارات النيل من شرفه واعتباره[1].

2. علم الجاني بالعلانية: لا يكفي علم الجاني بجريمتي السب والقذف بوسائل التواصل الاجتماعي، بل يجب أن يمتد إلى علم الجاني بأن إسناده لهذه الواقعة يتم بطريق العلانية، فعلانية الإسناد هي إرادة الفعل الإجرامي وهي وفقاً للقواعد العامة أحد عناصر القصد الجنائي، فيفترض هذا العنصر أن إرادة المتهم قد اتجهت إلى إسناد واقعة أو إلصاق وصف قذف أو سب بوسيلة من وسائل التواصل الاجتماعي. ومثال على ذلك: لو قام شخص بإرسال رسالة إلى آخر عبر وسيلة من وسائل التواصل الاجتماعي مثل: فيسبوك، وكان ضمن مجموعة من الأفراد أو ما يسمى بالمجموعات، وكان هذا الشخص من ضمن هذه المجموعة، ففي هذه الحالة يسأل الشخص المرسل عن جريمة سب وقذف بوسيلة تقنية معلومات، لأنها وقعت بوسيلة إلكترونية هدفها التشهير بالغير والمساس بسمعة واعتبار الشخص الآخر أمام الغير، ويقع على سلطة الاتهام عبء إثبات العلانية كما يقع عليها عبء إثبات القصد الجنائي، وللقاضي حرية قدير وجود هذا القصد او انتفائه بناء

[1]) محمد علي العريان: الجرائم المعلوماتية، دار الجامعة للنشر، الاسكندرية، 2013، ص117 .

على ما يطرح عليه من وقائع ظروف الدعوى، ويجب أن يبين وجود القصد الجنائي أو انتفائه وتوضيحه في حكمه.

الفرع الثاني

الإرادة في جريمتي القذف والسب عبر الشبكة العنكبوتية

لا بكفي أن تتجه إرادة الجاني من فعل الإسناد إلى إسناده للجاني وإعلانه – أي علانية للناس– بل لابد أن يكون بكامل إرادته وحريته السليمة خاليه من أي عيب[1]، ولتوضيح ذلك يتطلب الأمر الحديث عن إرادة الجاني إسناد الواقعة، وإرادة الجاني لعلانية هذه الواقعة المسندة:

1- اتجاه إرادة الجاني لإسناد واقعة القذف والسب بوسيلة من وسائل التواصل الاجتماعي: حتى يتوافر القصد الجنائي لدى الجاني لابد أن تتجه إرادته إلى إسناد عبارات السب والقذف ونشرها عبر وسائل التواصل الاجتماعي على الكافة، والقصد الجنائي في هذه الجريمة يتحقق بانصراف إرادة الجاني إلى الفعل باستخدام الشبكة المعلوماتية وتقنية المعلومات كوسيلة لإيصال السب والقذف للمجني عليه، ولا عبرة بعد ذلك بما يكون قد دفع الجاني إلى ارتكاب فعلته أو الغرض الذي توخاه منها[2]. ويفترض في هذه الحالة أن يكون الجاني قد وجه عبارات السب والقذف عبر وسائل التواصل الاجتماعي بإرادته الحرة دون اكراه أو تهديد، واتجهت إرادته إلى المساس بسمعة وشرف المجني عليه وجعله محل ازدراء بين الناس، ففي حال

---

[1]) مؤيد محمد علي القضاة: شرح قانون العقوبات الاتحادي الإماراتي، مرجع سابق، ص139.

[2]) عادل عزام: جرائم الذم والقدح والتحقير المرتكبة عبر الوسائل الإلكترونية، مرجع سابق، ص74.

ثبت أن الجاني كان مكرهاً على قول وكتابة هـذه العبارات المشينة عبـر وسائل التواصل الاجتماعي ينتفي توافر القصد الجنائي لديـه[1].

2- اتجاه إرادة الجاني إلى علانية واقعة القذف والسب بوسيلة من وسائل التواصل الاجتماعي: أن تكون إرادة الجاني قد اتجهت إلى إذاعة عبارات السب والقذف ونشرها على الكافة عبر وسائل التواصل الاجتماعي، أي أن إرادة الجاني اتجهت إلى التعبير عن المعنى المنسوب إلى المجني عليه علانية، فإذا انتفت هذه الإرادة، كما لو كان المتهم مكرهاً أو مجبر على إذاعة هذه العبارات ونشرها فإن القصد الجنائي ينتفي في هذه الحالة، كما يجب أن تتجه إرادة الجاني إلى إذاعة ما صدر عنه ويخدش اعتبار أو شرف المجني عليه، فإذا انتفت هذه الإرادة فإن القصد الجنائي ينتفي في هذه الحالة[2]، فلا يكفي للإدانة من أجل جريمتي السب والقذف عبر وسائل التواصل الاجتماعي القذف بعلانية العبارات، بل تتطلب توافر (قصد العلانية)، وهذا القصد لا يكفي لثبوته العلم بالعلانية، بل يجب أن تتوافر إرادة العلانية، ولا ينقض هذا القول أن هذه الإدانة تفترض في حال ثبت العلم بالعلانية، بل أنها تفترض إذا ثبتت العلانية ذاتها، ذلك بأن هذا الافتراض مجرد قاعدة إجرائية[3]. ويري الباحث أن إرادة الجاني تتحقق في هذه الحالة اذا قام

---

[1]) سالم الموسوي: جرائم القذف والسب عبر القنوات الفضائية، مرجع سابق، ص86.

[2]) جلال الزعبي؛ أسامة المناعسة: جرائم تقنية نظم المعلومات الإلكترونية، مرجع سابق، ص213 .

[3]) محمد سالم الزعابي: الجرائم الواقعة على السمعة عبر تقنية المعلومات، مرجع سابق، ص81.

بإرسال رسالة تتضمن عبارات سب وقذف تمس شرف واعتبار الشخص الآخر (المجني عليه) عبر برنامج الواتساب الموجود في هاتف هذا الشخص على سبيل المثال، ولا يطلع عليها سوى المرسل إليه، فهنا لا يسأل عن جريمة سب وقذف، وذلك لانتفاء قصد العلانية، إلا في حال علم الشخص المرسل إليه أنه أراد إعلانه للناس، فعندها يتحقق القصد الجنائي في حق المرسل.

الموقف في قانون العقوبات المصري:

وبالرجوع إلى نصوص قانون العقوبات المصري نجد أن المشرع اضفى حمايته الجنائية على الحياة الخاصة من خلال مدونته العقابية فجرم استراق السمع وتسجيل ونقل الاحاديث التي تدور في الأماكن الخاصة أو عن طريق الهاتف، كما جرم التقاط الصور الشخصية من الأماكن الخاصة، المادة (309 مكرر من قانون العقوبات المصري)

وأن الحديث عن حماية الحياة الخاصة من التعدي بالوسائل المعلوماتية يقتضي البحث في النصوص العقابية التي تكفل هذه الحماية في ظل عدم وجود قانون عقابي متكامل لمواجهة جرائم الكمبيوتر والانترنت وفيما يتعلق بقانون العقوبات المصري فقد نصت المادة (309 مكرر و 309 مكرر –أ) في شأن حماية الحياة الخاصة، فالمادتان متعلقتان بحماية حرمة الحياة الخاصة وذلك فيما يتعلق بحظر تسجيل الصوت والصورة بطريق غير مشروع، وفي غير الأحوال

المصرح بها قانوناً، وتجرم كذلك فعل إفشاء هذه الأسرار واذاعتها بأي طريقة أو المساعدة في هذه الأفعال أو التهديد أو القيام بها[1].

ويعاقب بالسجن الموظف العام الذي يرتكب أحد الأفعال المبينة بهذه المادة اعتماداً على سلطة وظيفته [2].

كما تناول المشرع المصري –جريمتي السب والقذف بتعريفهما في المادتين (302 و 306) عقوبات، حيث نصت المادة (302) من قانون العقوبات المصري المعدل بالقانون 147 لسنة 2006م: يعد قاذفاً كل من اسند لغيره بواسطة احدى الطرق المبينة بالمادة (171) من هذا القانون أموراً لو كانت صادقة لأوجبت عقاب من أسندت إليه بالعقوبات المقررة لذلك قانوناً أو أوجبت احتقاره عند أهل وطنه، ومع ذلك فالطعن في أعمال موظف عام أو شخص ذي صفة نيابية عامة أو مكلف بخدمة عامة لا يدخل تحت حكم هذه الفقرة، إذا حصل بسلامة نية وكان لا يتعدى أعمال الوظيفة أو الخدمة العامة، ويشترط أن يثبت المتهم حقيقة كل فعل أسنده إلى المجني عليه، ولسلطة التحقيق أو المحكمة بحسب الأحوال، أن تأمر بالزام الجهات الإدارية بتقديم ما لديها من أوراق ومستندات معززة لما يقدمه المتهم من أدلة لإثبات حقيقة تلك الأفعال ولا يقبل من القاذف إقامة الدليل لإثبات ما قذف به إلا في الحالة المبينة في الفقرة السابقة.

---

[1]) د. عبدالفتاح بيومي حجازي: نحو صياغة عامة في علم الجريمة المعلوماتية، ص181..

[2]) د. مدحت رمضان: جرائم الاعتداء على الأشخاص عبر الانترنت، ص111–112..

وتنص المادة (303) من ذات القانون على أن يعاقب على القذف بغرامة لا تقل عن سبعة آلاف وخمسمائة جنيه ولا تزيد على اثنين وعشرين ألف وخمسمائة جنيه، فإذا وقع القذف في حق موظف عام أو شخص ذي صفة نيابية عامة أو مكلف بخدمة عامة، وكان ذلك بسبب أداء الوظيفة أو النيابة أو الخدمة العامة، كانت العقوبة الغرامة التي لا تقل عن خمسة عشر ألف جنيه ولا تزيد على ثلاثين ألف جنيه، وتنص المادة (306) من ذات القانون على أن: كل سب لا يشتمل على اسناد واقعة معينة بل يتضمن بأي وجه من الوجوه خدشاً للشرف أو الاعتبار يعاقب عليه في الأحوال المبينة بالمادة (171) بغرامة لا تقل عن ثلاثة آلاف جنيه ولا تزيد على خمسة عشرة ألف جنيه، وتنص المادة (308) من ذات القانون على أن: إذا تضمن العيب أو الإهانة أو القذف أو السب الذي ارتكب بإحدى الطرق المبينة في المادة (171) سالفة الذكر طعناً في عرض الأفراد أو خدشاً لسمعة العائلات تكون العقوبة الحبس والغرامة معاً، على أن لا تقل الغرامة في حالة النشر في احدى الجرائد أو المطبوعات عن نصف الحد الأقصى وألا يقل الحبس عن ستة أشهر.

القانون المصري رقم (175) لسنة 2018 الخاص بمكافحة جرائم تقنية المعلومات:

تنص المادة (25) من الفصل الثالث الخاص بالجرائم المتعلقة بالاعتداء على حرمة الحياة الخاصة من القانون رقم (175) لسنة 2018 الخاص بمكافحة

جرائم تقنية المعلومات على أن: (يعاقب بالحبس مدة لا تقل عن ستة أشهر وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين كل من اعتدى على أي من المبادئ أو القيم الأسرية في المجتمع المصري أو انتهك حرمة الحياة الخاصة، أو أرسل بكثافة العديد من الرسائل الالكترونية لشخص معين دون موافقته، أو منح بيانات شخصية إلى نظام أو موقع الكتروني لترويج السلع أو الخدمات دون موافقته أو نشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات، معلومات أو اخباراً أو صوراً وما في حكمها، تنتهك خصوصية أي شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحة أو غير صحيحة).

كما نصت المادة (26) من القانون رقم 175 لسنة 2018 الخاص بمكافحة جرائم تقنية المعلومات المصري على: (يعاقب بالحبس مدة لا تقل عن سنتين ولا تجاوز خمس سنوات، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز ثلاثمائة ألف جنيه، أو بإحدى هاتين العقوبتين كل من تعمد استعمال برنامج معلوماتي أو تقنية معلوماتية في معالجة معطيات شخصية للغير لربطها بمحتوى منافٍ للآداب العامة، أو لإظهارها بطريقة من شأنها المساس باعتباره أو شرفه).

من خلال قراءة نصوص المواد السابقة في القانون رقم 175 لسنة 2018 والخاص بمكافحة جرائم تقنية المعلومات المصري، نجد أن المشرع قد جعل العقوبة مشددة (لا تقل عن ستة أشهر) في المادة (25) من القانون أعلاه وعقوبة الحبس

التي (لا تقل عن سنتين ولا تزيد على خمس سنوات)، في المادة (26) من ذات القانون، وكذلك شدد عقوبة الغرامة حيث جعلها لا تقل عن 50.000 جنيه، ولا تزيد عن 100.000جنيه، هذا ما نصت عليه المادة (25) من القانون أعلاه. وكذلك في المادة (26) من ذات القانون جعل الغرامة لا تقل عن 100.000جنيه، ولا تزيد على 300.000جنيه مصري، يتضح لنا الفرق واضحاً بين القانون المصري رقم (175) لسنة 2018 الخاص بمكافحة جرائم تقنية المعلومات، حيث شدد العقوبات وخاصة عقوبة الغرامة.

الموقف في التشريع الفرنسي:

كرس المشرع الفرنسي حماية حق الإنسان في كرامته من القذف والسب حيث أورد عبارات عن قدسية كرامة الإنسان في ديباجة الدستور الفرنسي لعام 1946م، ومن ثم أقرها دستور عام 1958، واعتبرها جزءاً منه[1].

وتجدر الإشارة إلى أن جميع الدساتير الفرنسية منذ عام 1798 وإلى يومنا هذا تعرف بحق الإنسان في التمتع بالحريات العامة والحفاظ على كرامته من الإهانة والتعدي وطالما أن هذه الحريات تتعلق ببعض أوجه الحياة الخاصة، فإن

[1]) فقد فصل المجلس الدستوري الفرنسي بأن الحفاظ على الكرامة الإنسانية ضد كل اشكال الاستعباد والانتقاص هو مبدأ ذو قيمة دستورية، انظر، مشار إليه لدى، فايد عابد فايد عبدالفتاح: نشر صور ضحايا الجريمة المسؤولية المدنية الناجمة عن عرض مأساة الضحايا في وسائل الاعلام، دراسة مقارنة في القانون المصري والقانون الفرنسي، دار الكاتب القانوني، القاهرة، 2008، ص31.

هذه الدساتير تكرس حق احترام الحياة الخاصة[1]، أما فيما يتعلق بالجانب المعلوماتي فإنه بتاريخ 1978/1/6 صدر قانون خاص يتعلق بمعالجة المعلومات ذات الطابع الشخصي حول المعلوماتية والملفات والحريات، حيث بينت المادة الأولى من هذا القانون الهدف من وضعه، فنصت على أن: (المعلوماتية يجب أن تكون في خدمة كل مواطن وتطويرها يجب أن يحصل في اطار التعاون الدولي، فلا يجب أن تلحق الضرر لا بالهوية البشرية ولا بحقوق الإنسان ولا بالحياة الخاصة، ولا بالحياة الفردية العامة للإنسان)، ومن أجل تحقيق هذا الهدف أرسى هذا القانون سلطة إدارية مستقلة مهمتها السهر على حسن تطبيقه، وهي اللجنة الوطنية للمعلومات والحريات[2].

كما قرر القانون الصادر في (1881/07/29) والمتعلق بحرية الصحافة حماية الفرد من الاعتداء على كرامته وسمعته، ومنحه حق إقامة دعوى القذف إلى جانب الحق في نشر الرد والتصحيح[3]، حيث تعاقب الفقرة الرابعة من المادة (35) من القانون المذكور أعلاه، على نشر أو إعادة انتاج واقعة (أي جريمة)، وبأي

---

[1]) مشار إليه لدى نعيم مغيبب: مخاطر الجريمة المعلوماتية والانترنت، بدون ناشر، 1998، ص44.

[2]) Memento – Guid Alain Besousaan, Les fichiers de personnes et le droit ED Hermes 1991, p 16 ets. Bensoussan.

[3]) Commission Nationale Informatique et Libertes (cnil): www.cnil.fr.

Yssinet (j), la directive du 24 October 1995, chiers lamy Droit del,Informatiqe 1996,

وسيلة من وسائل النشر مهما كان السبب، فمتى كان هذا النشر يمس كرامة الضحية (المعتدى عليه) وكان بدون موافقته، وتصل هذه العقوبة إلى غرامة مقدارها (15) ألف يورو[1].

وتمتاز الحماية الممنوحة بموجب المادة (3/37) من قانون الصحافة الفرنسي، انها اخذت بعين الاعتبار التطور التكنولوجي لوسائل الاعلام الحديثة، وبذلك فهي تمتد لتشمل كل الوسائل التي يمكن من خلالها الاعتداء على السمعة والشرف والاعتبار، بما في ذلك نشر الصورة كما أمكن تطبيقها على النشر من خلال الانترنت[2]. فضلاً عن ذلك القانون الفرنسي الصادر في 1994/7/29 فقد أدخل مادة جديدة على القانون المدني وهي المادة (16) التي تقضي بأن: (القانون يؤكد سمو الإنسان ويمنع أي اعتداء على كرامته وخصوصيته ويضمن احترامه منذ بداية حياته)، وفي حالة الاعتداء على حق الإنسان في سمعته واعتباره فإنه يمكن اللجوء وفقاً لقواعد المسؤولية التقصيرية التي تستلزم لتحققها إثبات عناصرها الثلاثة (الخطأ والضرر وعلاقة السببية).

ولا شك أن في إثبات هذه العناصر صعوبة لأن معظم حالات المساس بالشرف والاعتبار يترتب عليها أضراراً أدبية ليس من السهل إثباتها، إضافة إلى أن هذه الحماية تقتصر على معالجة الأضرار التي تحدث عن المساس بهذا الحق ولا

---

[1]) jean seager. P.1718.

[2]) للحصول على نسخة من القانون المدني الفرنسي والانجليزي على الموقع الالكتروني:
http:// www legii'rance.gouv. Fr/html/codes_ traduits_civil_textA.HTMAL

تمنح المتضرر حماية وقائية، مثل وقف نشر المطبوعة المنطوية على مساس بالشرف والاعتبار، غير أن القضاء الفرنسي قد عالج هذا القصور من خلال منح المتضرر إمكانية اللجوء إلى وسائل وقائية لحماية شرفه واعتباره وفقاً لتقدير المحكمة المختصة[1].

كما أن القذف والسب في النظام الفرنسي يعتبر من قبل الانتهاكات التي ترد في قانون الصحافة لعام 1881 والمنصوص عليه في المادة (29) منه، ولا يشترط لتحقيق هذا الانتهاك من خلال هذا القدح أن يتم تحديد الشخص المتضرر باسمه صراحة، ولكن يكفي إمكانية التعرف عليه من خلال ما صدر من المشتكى عليه[2].

وفي ظل الحماية الجنائية للبيانات في القانون الفرنسي فقد نص المشرع على هذه الحماية الجنائية في قانون المعلوماتية الصادر في يناير عام 1978، وقد أعيد النص عليها ضمن نصوص قانون العقوبات الفرنسي الجديدالصادر عام 1994، تأكيداً لحماية الحقوق والحريات المتعلقة بالمواطنين في مواجهة تطور تكنولوجيا المعلومات، وطبقاً لقانون المعلوماتية الفرنسي، فقد كانت الحماية الجنائية للبيانات منصوصاً عليها في المواد (41-42) من القانون، وقد أعيد النص عليها

---

[1]) حسام الدين الاهواني: الحق في الحياة الخاصة، دار النهضة العربية 1978، ص83.

[2]) انظر تعريف القدح الوارد في المادة 29 من قانون الصحافة الفرنسي.

في قانون العقوبات الجديد ضمن المواد (266-16) و (226-31) مع اجراء بعض التعديلات في هذه الجرائم.

وقد أنشأت اللجنة القومية للمعلوماتية والحريات في فرنسا بموجب القانون 17/78 في 6 يناير 1978، حيث تختص هذه اللجنة بإجراء رقابة سابقة ولاحقة للتأكد من الحماية الكاملة للحقوق والحريات في مواجهة نظم المعلومات[1]، وتختص هذه اللجنة بالإشراف على تطبيق قانون المعلوماتية وإبلاغ ذوي الشأن بحقوقهم وواجباتهم، والتحقق من احترام نظم المعلوماتية لأحكام القانون المذكور، وكذلك اصدار الإذن للإدارة من أجل إنشاء نظم المعلومات، أو تلقي الاخطارات من الأشخاص المجني عليهم في هذا الخصوص[2].

---

1) - I, information drs libertes, R.D.P, 1980, P. 1043 etc.

2) La mauutrise d,une interpenednce, commentaire de la loi 5 janvier 1978 j.c.p.I.

موقف التشريع الفرنسي واتجهاهات القضاء فيما يتعلق بحماية المعلومات الشخصية – المجلة الدولية للقانون المقارن، 1978، ص562، وما بعدها.

المبحث الثاني

أحكام العقاب على القذف والسب عبر الشبكة العنكبوتية

تمهيد وتقسيم:

قبل الحديث عن العقوبات المقررة لجريمتي القذف والسب عبر وسائل التواصل الاجتماعي، لابد من الاشارة إلى أن المرسوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات لم يتطرق لأسباب الإباحة؛ وبالتالي فإنه تسري القواعد العامة للإباحة وموانع العقاب على جريمتي السب والقذف عبر وسائل التواصل الاجتماعي، إلا أن القانون قد نص على الظروف المشددة في المادة (20) منه حيث نص على أنه: (... فإذا وقع السب أو القذف في حق موظف عام أو مكلف بخدمة عامة بمناسبة أو بسبب تأدية عمله عد ذلك ظرفاً مشدداً للجريمة)، وكذلك الحال فقد نص على التدابير الجنائية في المواد (41[1]، 42[1]، 43[2]) من ذات القانون.

[1]) تنص المادة (41) على أنه: (مع عدم الإخلال بحقوق الغير حسني النية يحكم في جميع الأحول بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا المرسوم بقانون أو الأموال المتحصلة منها، أو بمحو المعلومات أو البيانات أو إعدامها، كما يحكم بإغلاق المحل أو الموقع الذي يرتكب فيه أي من هذه الجرائم، وذلك إما إغلاقاً كلياً أو للمدة التي تقدرها المحكمة)..

وعليه سنتناول في هذا المبحث أحكام العقاب في جريمتي القذف والسب عبر الشبكة العنكبوتية. وذلك على النحو التالي:

المطلب الأول: العقوبات الأصلية والظروف المشددة للقذف والسب عبر الشبكة العنكبوتية.

المطلب الثاني: التدابير المقررة للسب والقذف عبر الشبكة العنكبوتية.

---

[1]) تنص المادة (42) على أنه: (تقضي المحكمة بإبعاد الأجنبي الذي يحكم عليه بالإدانة لارتكاب أي جريمة من الجرائم المنصوص عليها في هذا المرسوم بقانون وذلك بعد تنفيذ العقوبة المحكوم بها)..

[2]) وتنص المادة (43) على أنه: (مع عدم الإخلال بالعقوبات المنصوص عليها في هذا المرسوم بقانون يجوز للمحكمة أن تأمر بوضع المحكوم عليه تحت الاشراف أو المرقبة أو حرمانه من استخدام أي شبكة معلوماتية، أو نظام المعلومات الإلكتروني، أو أي وسيلة تقنية معلومات أخرى، أو وضعه في مأوى علاجي أو مركز تأهيل للمدة التي تراها المحكمة مناسبة).

المطلب الأول

العقوبات الأصلية والظروف المشددة للقذف والسب

عبر الشبكة العنكبوتية

سنتناول في هذا الفرع العقوبات الأصلية والظروف المشددة للعقاب على جريمتي القذف والسب عبر وسائل التواصل الاجتماعي، وذلك على النحو التالي:

الفرع الأول

العقوبات الأصلية لجريمتي القذف والسب عبر الشبكة العنكبوتية

العقـوبة الأصلية التي فرضها المشرع تكون مستقلة عن غيـرها وليست متعلقة بعقـوبة أخـرى ولا ترتبط بها، فهي الأصل في تقرير العقوبات، وبالرجوع إلى نص المادة (20) من المرسوم بقانون اتحـادي رقم (5) لسنة 2012 الإماراتي بشــأن مكافحة جرائم تقنية المعلــومات يتضح أن العقوبة التي حددها المشرع لهذه الجريمة هي: (الحبس والغرامة التي لا تقل عن مائتين وخمسـين ألف درهم ولا تجاوز خمسمائة ألف درهم). ويلاحظ هنا أن المشــرع شدد العقوبة عندما رفـع حـد الغرامة عما هو منصوص عليه في قانون العقوبات الاتحادي لنفس الجريمة التي جعل حدها الأدنى 20 ألف درهم، مما يؤكد على رغبة المشرع الإماراتي في مكافحة الجرائم التي تقع عبر وسائل التواصل الاجتماعي، خصوصاً بسبب انتشارها كثيراً. وعليه فسوف نعرض فيما يلي كلا من عقوبتي الحبس والغرامة:

(أ) الحبس:

عرف المشرع الإماراتي في المادة (69) هن قانون العقوبات الحبس بأنه: (وضع المحكوم عليه في إحدى المنشآت العقابية المخصصة قانوناً لهذا الغرض وذلك للمدة المحكوم بها. ولا يجوز أن يقل الحد الأدنى للحبس عن شهر ولا أن يزيد حده الأقصى على ثلاث سنوات ما لم ينص القانون على خلاف ذلك).

والجدير بالذكر أن عقوبة الحبس مقرة للجنح، فإذا نص القانون على عقوبة الحبس دون تحديد مدة معينة، فإن على المحكمة أن تنطق بالحكم بمدة تقدرها بحيث لا تقل عن شهر ولا تزيد على ثلاث سنوت[1]. وعقوبة الحبس هي عقوبة سالبة للحرية بصفة مؤقتة، للمدة المحددة في الحكم الجنائي الصادر بها، وهي عقوبة مقررة للجنح وفقاً لنص المادة (29) [2]، من قانون العقوبات الاتحادي.

ويعرف الحبس بأنه: (سلب حرية المحكوم عليه الذي يلتزم بالعمل أحياناً، ويعفى في أحيان أخرى من هذا الالتزام)[3]. إذن فالحبس عقوبة أصلية مقررة لجريمة الجنحة، وتفترض حجز حرية المحكوم عليه مدة معينة في إحدى المنشآت العقابية المخصصة لهذه الغاية. وبما أن عبارة الحبس جاءت مطلقة في نص المادة (20) من المرسوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات فهذا يعني أن المشرع الإماراتي قد ترك للقاضي سلطة تقدير العقوبة المناسبة بحسب ما يراه من ظروف للواقعة.

(ب) الغرامة:

---

[1]) لطيفة الجميلي: الوجيز في شرح قانون الإجراءات الجزائية الاتحادي، الآفاق المشرقة للنشر، الشارقة، 2013م، ص166.

[2]) نص المادة 29 من قانون العقوبات الاتحادي على أنه: (الجنحة هي الجريمة المعاقب عليها بعفوية أو أكثر من العفويات الآنية: 1-الحبس. 2- الغرامة التي تزيد على ألف درهم 3- الدية).

[3]) عبدالرازق الموافي: قانون العقوبات لدولة الإمارات، مرجع سابق، ص192.

عرفت المادة (71) من قانون العقوبات الاتحادي الغرامة على أنها: (إلزام المحكوم عليه أن يدفع للخزينة المبلغ المحكوم به، ولا يجوز أن تقل الغرامة عن ألف درهم ولا أن يزيد حدها الأقصى عن مليون درهم في الجنايات وثلاثمائة ألف درهم في الجنح وذلك كله ما لم ينص القانون على خلافه). وعرفها جانب من الفقه بأنها: (ايلام المحكوم عليه بطريق الاقتطاع من ماله)[1]، وتعرف أبضاً بأنها: (عقوبة توقعها الدولة بما لها سلطة العقاب على الأفراد وتذهب حصيلتها إلى الدولة) [2].

والغرامة يمكن أن تكون عقوبة أصلية يقضي بها بمفردها، أو عقوبة تكميلية يحكم بها بالإضافة إلى عقوبة أصلية سالبة للحرية، فهي جزاء توقعه الدولة بما لها من سلطة العقاب على الأفراد نتيجة لانتهاك قواعد القانون، وهي لا تنتج عن اتفاق بين الأفراد أو عن الإخلال بالتزام تعاقدي، وبالتالي فإن حصيلة الغرامات تذهب إلى خزينة الدولة، ولا تكون من نصيب الطرف المضرور لأن الدولة هي التي توقع هذا الجزاء بما لها من سلطة العقاب[3].

وبالنسبة للأشخاص الطبيعيين تفضل الغرامة على العقوبات المقيدة للحرية قصيرة المدة، لأنها تحقق الغاية من العقاب بصفة عامة دون أن يكون هناك وجه

---

[1]) محمد شلال العاني: أحكام القسم العام في قانون العقوبات الاتحادي الإماراتي، مرجع سابق، ص219.

[2]) شريف سيد كامل: قانون العقوبات الاتحادي، مرجع سابق، ص213.

[3]) خليفة راشد الشعالي: شرح قانون العقوبات الإماراتي، مرجع سابق، ص198.

للتخوف من خطر عدوي الإجرام الذي تكون نتيجته في أغلب الأحيان من اختلاط المحكوم عليه مع المسجونين داخل السجن، فضلاً عن اعتبارها مورداً مالياً، وهي في الغالب عقوبة أصلية، وقد تكون تكميلية في بعض الأحيان على حسب وقائع الجريمة وحكم القاضي ونص القانون. أما بالنسبة للأشخاص المعنويين فتعتبر عقوبة الغرامة من أهم وأبرز العقوبات التي تطبق عليه ولا يجد القاضي حرجاً من الحكم بها[1].

وسواء كانت الغرامة عقوبة للأشخاص الطبيعيين أو المعنويين فإنها لا تفرض إلا إذا نص عليها القانون تطبيقاً لمبدأ الشرعية، كما يجب أن يصدر بها حكماً قضائياً من محكمة مختصة، ولا يحكم بها إلا على من تثبت مسؤوليته عن الجريمة احتراماً لمبدأ شخصية العقوبة. لذلك فإن الغرامة كسائر العقوبات، تخضع لقاعدة لا عقوبة إلا بنص، وهذه القاعدة هي الأساس التي يقوم عليها نظام العقوبات في التشريعات الحديثة، أي أن الأفعال التي تصدر من الإنسان وتشكل جريمة يكون لها عقابها القانوني، وبذلك يقتصر دور القاضي على تطبيق الغرامة المنصوص عليها في القانون، ويجب عليه أن لا يتجاوز الحد الأقصى المنصوص عليه، ولا أن ينزل عن الحد الأدنى إلا بنص[2].

---

[1]) علي حمودة: شرح الأحكام العامة لقانون العقوبات الاتحادي، مرجع سابق، ص182.

[2]) حوراء موسى: الجرائم المرتكبة عبر وسائل التواصل الاجتماعي، مرجع سابق، ص346.

وخلاصة ما سبق، فإن عقوبة هذه الجريمة قد تكون الحبس والغرامة معاً أو تكون إحداهما، وقد ترك أمر تحديد مدة عقوبة الحبس للقاضي بينما قيد المشرع مقدار عقوبة الغرامة بحد أدنى هو مائتين وخمسين ألف درهم وحد أعلى هو خمسمائة ألف درهم.

الفرع الثاني

الظروف المشددة لعقوبة جريمتي القذف والسب عبر الشبكة العنكبوتية

نصت المادة (20) من المرسوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات في الفقرة الثانية على أنه: (إذا وقع السب والقذف في حق موظف عام أو مكلف بخدمة عامة بمناسبة أو بسبب تأدية عمله عد ذلك ظرفاً مشدداً)، أي أن المشرع شدد العقاب في حال ارتكاب الجريمة بحق طائفة معينة من الأفراد نظراً لخطورتها على المصلحة العامة، ومن هؤلاء الأفراد الموظف العام أو المكلف بخدمة عامة، وذلك إذا وجهت إليه عبارات القذف بصفته لا بشخصه وهو ما يتطلب ارتباط القذف بأعمال الوظيفة لا بالحياة الخاصة للموظف، وقد نصت المادة (5) من قانون العقوبات الاتحادي أيضاً على هذه الطائفة المعينة من الناس[1].

وعلة تشديد العقوبة في هذه الحالة هي رغبة المشرع الإماراتي في توفير حماية خاصة للوظيفة أو الخدمة العامة حتى يمكن القيام بها على أكمل وجه، وحتى يتمتع الموظف العام أو المكلف بخدمة عامة بقدر من الطمأنينة يمكنه من

[1]) عبدالرازق الموافي: شرح قانون مكافحة جرائم تقنية المعلومات الإماراتي، مرجع سابق، ص127.

أداء واجبات وظيفته، إذ تتطلب المصلحة العامة أن يكون هذا الموظف آمناً من أن يمس أحد سمعته أو ينال من شرفه وكرامته واعتباره[1].

ويرى الباحث أن القذف في حق الموظف العام أو المكلف بخدمة عامة يلحق الضرر بالمصلحة العامة بصورة أكبر من الضرر الذي ينجم عن القذف في حق فرد عادي.

وبناء على ذلك يتضح أنه لإعمال هذا الظرف المشدد لابد من توافر شرطان همان:

أن يكون الشخص المقذوف موظفاً عاماً ومكلفاً بخدمة عامة.

أن يكون القاذف قد وجه إلى المجني عليه أثناء أو بسبب أو بمناسبة تأدية الوظيفة أو الخدمة العامة.

وجدير بالإشارة أن هذين الشرطين بكملان بعضهما البعض، لأن محل الاعتداء هي صفة المجني عليه لا شخصه، ففي حال لم يكن متمتعاً بهذه الصفة فلا تقوم جريمتي السب والقذف عبر وسائل التواصل الاجتماعي بصورتها المشددة[2].

---

[1]) محمد سالم الزعابي: الجرائم الواقعة على السمعة عبر تقنية المعلومات، مرجع سابق، ص81.

[2]) حوراء موسى: الجرائم المرتكبة عبر وسائل التواصل الاجتماعي، مرجع سابق، ص347.

المطلب الثاني

التدابير المقررة كعقوبة للقذف والسب عبر الشبكة العنكبوتية

تعرف التدابير الجنائية بأنها: (مجموعة من الإجراءات القانونية التي تتخذ في مواجهة بعض الجناة ممن تثبت خطورتهم الإجرامية لمنعهم من ارتكاب جرائم في المستقبل)[1]. ويتضح من خلال هذا التحديد لمفهوم التدابير الجنائية أنها ذات طابع تأهيلي وقائي، فهي من ناحية تفرض على الجاني لاعتبارات تتعلق بمصلحته ومصلحة المجتمع، بالإضافة إلى أنها تهدف إلى حماية الجاني وتأهيله وإصلاحه، مع ملاحظة أن بعض هذه التدابير– مثل الإبعاد والإلزام بالعمل وحظر ممارسة عمل معين– يجوز للمحكمة أن تأمر بأحدها بدلاً من الحكم بالعقوبة السالبة للحرية.

وقد نص المشرع الإماراتي في المواد (41، 42، 43) من المرسوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات على هذه التدابير، وهي تنقسم إلى نوعين من التدابير: تدابير وجوبية وتدابير جوازيه. وهذا ما سنتناوله على النحو التالي:

[1]) حسن محمد ربيع: شرح قانون العقوبات الاتحادي– المبادئ العامة للجريمة، مرجع سابق، ص149.

الفرع الأول

التدابير الوجوبية

ورد النص في المرسوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات على التدابير الوجوبية التي يجب تطبيقها على الجاني الذي يرتكب جريمتي السب والقذف عبر وسائل التواصل الاجتماعي تحديداً في المادة (42) المعدلة بالقانون الاتحادي رقم 2 لسنة 2018 والتي تنص على ما يلي: (مع مراعاة حكم الفقرة الثانية من المادة (121) من قانون العقوبات الاماراتي تقضي المحكمة بإبعاد الأجنبي الذي يحكم عليه في أي من الجرائم الواقعة على العرض، أو يحكم عليه بعقوبة الجناية في أي من الجرائم المنصوص عليها في هذا المرسوم بقانون وذلك بعد تنفيذ العقوبة المحكوم بها). كما ونصت المادة (43) من ذات القانون على أنه: (مع عدم الإخلال بحقوق الغير حسني النية يحكم في جميع الأحوال بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا المرسوم بقانون أو الأموال المتحصلة منها، أو بمحو المعلومات أو البيانات أو إعدامها، كما يحكم بإغلاق المحل أو الموقع الذي يرتكب فيه أي من هذه الجرائم، وذلك إما إغلاقاً كلياً أو للمدة التي تقدرها المحكمة).

ويتضح من النصين المذكورين أعلاه أن التدابير الوجوبية التي يتصور أن يحكم بها القاضي عند الحكم بالإدانة في جريمتي القذف والسب عبر الشبكة العنكبوتية تنقسم إلى التالي:

1- **الإبعاد:** نصت المادة 42 من الموسوم بقانون اتحادي على أنه: (تقضي المحكمة بإبعاد الأجنبي الذي يحكم عليه بالإدانة لارتكاب أي جويمة من الجرائم المنصوص عليها في هذا المرسوم بقانون وذلك بعد تنفيذ العقوبة المحكوم بها). وقد استقرت أحكام الفقه والقضاء على وصف إبعاد الأجنبي بأنه أحد التدابير الجزائية، كما أن الحكم بتدبير الإبعاد جوازي لمحكمة الموضوع دون معقب عليها[1]، فالإبعاد من البلاد تدبير لا يقع إلا على الأجانب[2]، والإبعاد المقرر بموجب قانون العقوبات الاتحادي هو إبعاد قضائي[3] يصدر من المحكمة الجزائية التي أصدرت الحكم الجزائي ضد المحكوم عليه، وفي الحالات التي لا يكون فيها

---

[1]) حكم المحكمة الاتحادية العليا، الطعن رقم (139) لسنة 2005، جلسة 2005/6/1.

[2]) نصت المادة (121) من قانون العقوبات الاتحادي رقم (3) لسنة 1987 على أنه: (إذا حكم على أجنبي في جناية بعقوبة مقيدة للحرية أو في الجرائم الواقعة على العرض تقرر الحكم بإبعاده عن الدولة. ويجوز للمحكمة في مواد الجنح الأخرى أن تأمر في حكمها بإبعاده عن الدولة، أو الحكم بالإبعاد بدلاً من الحكم عليه بالعقوبة المقيدة للحرية).

[3]) لإبعاد القضائي هو الذي يتخذ بناء على حكم أو أمر قضائي يصدر من المحكمة المختصة، عند ارتكاب بعض الجرائم، وهذا النوع من الإبعاد قد يكون وجوبياً تلتزم المحكمة بالحكم به، وقد يكون جوزياً بحيث تملك المحكمة السلطة التقديرية في تحديد المدة من عدمها.

الحكم بالإبعاد قد صدر كبديل للعقوبة المقيدة للحرية المقررة للجنحة يتم تنفيذ حكم الإبعاد بعد انتهاء المحكوم عليه من تنفيذ العقوبة المحكوم بها عليه[1].

2- مصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في الجريمة:

والمصادرة هي نزع مال- تم ضبطه- جبراً عن صاحبه لكي يؤول إلى الدولة بغير مقابل، فهي إجراء الفرض منه تمليك الدولة أشياء مضبوطة ذات صلة بالجريمة، قهراً عن صاحبها وبغير مقابل، فهي إذاً عقوبة مالية، تتمثل في نزع المال قسراً عن صاحبه، وإدخاله في ملك الدولة بلا مقابل[2]، والأصل في قانون العقوبات الإماراتي أن المصادرة عقوبة تكميلية، وهو ما أكدته المادة (82) من قانون العقوبات الإماراتي، حيث نصت على أنه: (تحكم المحكمة عند الحكم بالإدانة بمصادرة الأشياء والأموال المضبوطة التي استعملت فيها أو كان من شأنها أن تستعمل فيها أو كانت محلاً لها أو التي تحصلت من الجريمة، فإذا تعذر ضبط أياً من تلك الأشياء أو الأموال حكمت المحكمة بغرامة تعادل قيمتها، وذلك كله دون الإخلال بحقوق الغير حسن النية). وقد أكدت على ذلك أيضاً المادة (41) من المرسوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات حيث نصت على أنه: (مع عدم الإخلال بحقوق الغير حسني النية يحكم في جميع الأحول بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من

---

[1]) محكمة تمييز دبي، الطعن رقم 180 لسنة 2013 جزاء جلسة 2013/7/12.

[2]) حسن محمد ربيع: شرح قانون العقوبات الاتحادي – المبادئ العامة للجريمة، مرجع سابق، ص157.

الجرائم المنصوص عليها في هذا المرسوم بقانون أو الأموال المتحصلة منها، أو بمحو المعلومات أو البيانات أو إعدامها، كما يحكم بإغلاق المحل أو الموقع الذي يرتكب فيه أي من هذه الجرائم، وذلك إما إغلاقاً كلياً أو للمدة التي تقدرها المحكمة).

3- **محو المعلومات أو البيانات أو إعدامها:** يقصد بالمحو المسح الذي ينصب على البرامج أو البيانات أو المعلومات بما يجعلها غير صالحة للغرض الذي أعدت من أجله، ويشمل أفعال الإدخال والإتلاف والمحو والطمس لبيانات أو برامج معلوماتية[1]، ومثال ذلك: إذا قام شخص بسب آخر عبر الهاتف المتحرك من خلال استخدام أحد وسائل التواصل الاجتماعي، فعندما يصدر القاضي الحكم بهذا التدبير فسوف تقوم الجهة المختصة بطلب الهاتف المتحرك محل الجريمة من الجاني ومحو كافة المعلومات والبيانات التي أرسلت إلى المجني عليه.

4- **إغلاق المحل أو الموقع المرتكب فيه الجريمة:** لقد ورد تدبير إغلاق المحل في القوانين العقابية كعلاج للجريمة، وهنا يختلف الإغلاق بحسبانه جزاءً جنائياً – وهو ما نحن بصدده– عن الإغلاق الإداري– وهو ما يخرج عن نطاق هذه الدراسة، فالإغلاق يقصد به إيقاف نشاط المنشأة أو المؤسسة أو المحل المرتكب فيه الجريمة الإلكترونية المقضي بإغلاقه أو منع ممارسته لنشاطه

[1]) عمار عباس الحسيني: جرائم الحاسوب والإنترنت، مرجع سابق، ص181.

المرخص له به[1]، وهو يعادل عند تطبيقه على الشخص المعنوي لفترة معينة عقوبة الحبس بالنسبة للشخص الطبيعي[2]، ويعرف أيضاً بأنه حظر مزاولة العمل الذي كان يمارس فيه قبل إنزال هذا التدبير، وينصرف الإقفال إلى المحل كمؤسسة تجارية، لا ككيان مادي[3]، وقد يكون المحل أو المكان أو الموقع الذي ارتكبت فيه جريمتي السب والقذف بالوسائل الإلكترونية وسيلة تسهل للجاني ارتكابها فيه، ولذلك يحكم بإغلاق المحل أو الموقع الذي ترتكب فيه هذه الجريمة– إذا كانت قد ارتكبت بعلم مالكها– إغلاقاً كلياً أو لمدة معينة تحددها المحكمة[4]؛ وهو ما جاء في نص المادة (41) من المرسوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات التي نصت على أنه: (كما يحكم بإغلاق المحل أو الموقع الذي يرتكب فيه أي من هذه الجرائم، وذلك إما إغلاقاً كلياً أو للمدة التي

---

[1]) أشارت المادة (128) من قانون العقوبات الاتحادي على أنه: (فيما عدا الحالات الخاصة التي ينص عليها القانون على الإغلاق يجوز للمحكمة عند الحكم بمنع شخص من ممارسة عمله وفقاً للمادة 126 أن تأمر بإغلاق المحل الذي يمارس فيه هذا العمل وذلك لمدة لا تقل عن شهرين ولا تزيد عن سنة، و يستتبع الإغلاق حظر مباشرة العمل أو التجارة أو الصناعة نفسها في المحل ذاته سواء أكان نلك بواسطة المحكوم عليه أم أحد أفراد أسرته أم أي شخص آخر يكون المحكوم عليه قد أجر له المحل أو تنازل له عنه بعد وقوع الجريمة ولا يتناول الحظر مالك المحل او أي شخص يكون له حق عيني عليه إذا لم تكن له صلة بالجريمة).

[2]) عبدالرزاق الموافي: شرح قانون مكافحة جرائم تقنية المعلومات الإماراتي، مرجع سابق، ص112.

[3]) إمام حسنين خليل عطا الله: الحماية الجنائية لوسائل تقنية المعلومات في التشريعات العربية، مرجع سابق، ص138.

[4]) حوراء موسى: الجرائم المرتكبة عبر وسائل التواصل الاجتماعي، مرجع سابق، ص352 .

تقدرها المحكمة). ويلاحظ أن المشرع الإماراتي في المادة (41) من المرسوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات لم يحدد مدة الإغلاق، فقد تركها مطلقة غير مقيدة أي تخضع لتقدير القاضي، فله أن يجعل الغلق كلياً أو جزئياً لمدة تحددها المحكمة الصادر منها الحكم بإغلاق هذا المحل. **ويرى الباحث**، أن المشرع منح للجهة الإدارية المختصة بعض السلطات التي من خلالها تقوم بتسيير واستغلال وإدارة هذا المحل بتوافر الاشتراطات فيها، وجعلت الغلق هو جزاء مخالفة ذلك، حيث تقوم هذه الجهة بغلق بعض المحلات أو المنشآت التي تخالف القانون غلقاً إدارياً دون انتظار حكم قضائي من المحكمة، وبصدر قرار إداري بغلق هذا المحل أو المنشأة محل الجريمة.

الفرع الثاني

التدابير الجوازية

نصت المادة (43) من المرسوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات على أنه: (مع عدم الإخلال بالعقوبات المنصوص عليها في هذا المرسوم بقانون يجوز للمحكمة أن تأمر بوضع المحكوم عليه تحت الإشراف أو المراقبة أو حرمانه من استخدام أي شبكة معلوماتية، أو نظام المعلومات الإلكتروني، أو أي وسيلة تقنية معلومات أخرى، أو وضعه في مأوى علاجي أو مركز تأهيل للمدة التي تراها المحكمة مناسبة.

ويتضح من هذا النص أن التدابير الجوازية لجريمتي القذف والسب عبر الشبكة العنكبوتية تنقسم إلى التالي:

(أ) وضع المحكوم تحت الإشراف أو المراقبة:

تعرف المراقبة بأنها: (تدبير احترازي مقيد للحرية يبتغي توفير معاملة خاصة لمن ينزل به تستهدف تحقيق إصلاحه وضمان ائتلافه مع المجتمع) [1]، وقد عرفت المادة(115) من قانون العقوبات المراقبة بأنها: (المراقبة هي إلزام المحكوم عليه بالقيود التالية كلها أو بعضها وفقاً لما يقرره الحكم:

[1]) حسين سعيد الغافري: السياسة الجنائية في مواجهة جرائم الإنترنت، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2013، ص185 .

1) أن لا يغير محل إقامته إلا بعد موافقة الجهة الإدارية المختصة فإذا لم بكن له محل إقامة عينت له هذه الجهة محلاً.

2) أن يقدم نفسه إلى الجهة الإدارية المختصة في الفترات الدورية التي تحددها.

3) ان لا يرتاد الأماكن التي حددها الحكم.

4) أن لا يبرح مسكنه ليلاً إلا بإذن من الجهة الإدارية المختصة.

فالمراقبة كما يتضح من النص أعلاه هي تدبير جنائي يقوم على مجموعة من الواجبات التي تفرض على المحكوم عليه وتمثل تقييداً لحريته من حيث إلزامه بعدم تغيير محل إقامته إلا بعد الحصول على إذن من السلطة المختصة، وعدم ارتياد الأماكن التي حددتها المحكمة في الحكم، وعدم مغادرة المسكن ليلاً إلا بناء على موافقه من الجهات المختصة بذلك.

وقد نصت المادة (139) من قانون العقوبات على أنه: (تسري على المراقبة المنصوص عليها في هذا الباب أحكام المادة (115) ولا يجوز أن تزيد مدة المراقبة على ثلاثة سنوات). أي بمعنى أن المشرع حدد مدة تدبير المراقبة ولم يتركها مطلقة وأشترط أن لا تزيد على ثلاث سنوت.

ويقوم مركز الإشراف أو المراقبة بدراسة الحالات المحولة إليه سوء اجتماعياً وطبياً ونفسياً، للوقوف على العوامل التي أدت إلى وقوع الجريمة، ورسم خطة للعلاج،

وتقديم التقارير المطلوبة إلى المحكمة والإشراف على تنفيذ التدابير المنصوص عليها في هذا القانون[1].

كما يختص مكتب المراقبة بتنفيذ برنامج الرعاية اللاحقة لخريجي هذه المراكز والمؤسسات، أما بالنسبة لسلطة المراقبة فهنا تتجه جهود المراقب الاجتماعي في هذه المرحلة نحو شخصية الحدث وحاجاته ومطالبه المالية والاجتماعية والنفسية محاولاً بأقصى جهد تعديل شخصيته وإعادة تنشئته بما يجعله يعيش حياة طبيعية في هذا المجتمع[2].

(ب) الحرمان من استخدام شبكة معلوماتية:

يقصد بهذا التدبير الجوازي منع الشخص من استخدام أي وسيلة تقنية معلومات تؤدي إلى ارتكاب جريمتي السب والقذف. ولم يحدد المشرع الإماراتي مدة معينة للحرمان فقد تركها تقديرية للقاضي وله أن يحكم بالمدة التي تتناسب مع الجريمة المرتكبة.

---

[1]) عبدالرازق الموافي: شرح قانون مكافحة جرائم تقنية المعلومات الإماراتي، مرجع سابق، ص136.

[2]) محمد سالم الزعابي: الجرائم الواقعة على السمعة عبر تقنية المعلومات، مرجع سابق، ص97.

(ج) الوضع في مأوى علاجي أو مركز تأهيل:

بالرجوع إلى نص المادة (137) من قانون العقوبات الاتحادي بخصوص الإجراءات الواجب إتباعها لتنفيذ تدبير الإيداع في مأوى علاجي، وما يلزم اتخاذه لمتابعة حالة الجاني نجدها تنص على أن: (يرسل المحكوم بإيداعه مأوى علاجياً إلى منشأة صحية مخصصة لهذا الغرض حيث يلقي العناية التي تدعو إليها حالته). ويصدر بتحديد المنشأة الصحية قرار من وزير الصحة بالاتفاق مع وزير العدل. وإذا حكم بالإيداع في مأوى علاجي وجب أن تعرض على المحكمة المختصة تقارير الأطباء عن حالة المحكوم عليه في فترات دورية لا يجوز أن تزيد أي فترة منها على ستة أشهر وللمحكمة بعد أخذ رأي النيابة العامة أن تأمر بإخلاء سبيله إذا تبين أن حالته تسمح بذلك[1].

ويقصد بإعادة التأهيل: (مجموعة العمليات أو الأساليب التي يقصد بها تقديم أو إعادة توجيه الأشخاص المنحرفين أو المجرمين نحو الحياة السوية)[2]، ويقصد به أيضاً: (إعادة تزويد الشخص بما يجعله يثق في نفسه بتصحيح شخصيته معنوياً وفكرياً واقتصادياً واجتماعيا وجسمانياً لكي يعيش حياته بشكل طبيعي كبقية الأفراد دون الرجوع مرة أخرى لارتكاب مثل هذه الجريمة) [3]، كما يعرف التأهيل بأنه:

---

[1]) حوراء موسى: الجرائم المرتكبة عبر وسائل التواصل الاجتماعي، مرجع سابق، ص358 .

[2]) مؤيد محمد علي القضاة: شرح قانون العقوبات الاتحادي الإماراتي، مرجع سابق، ص134.

[3]) علي حمودة: شرح الأحكام العامة لقانون العقوبات الاتحادي، مرجع سابق، ص197.

(عمل إداري اجتماعي متخصص يمتزج فيه الفن القانوني مع الفن والخبرة التي يقوم بها المؤهل بإعادة تأهيل المُؤهَل لتحقيق غرض محدد) [1].

ويضمن معنى التأهيل إثارة الحوافز الإيجابية عند الشخص بحيث يؤمن بالقيم والمواقف الجديدة التي سوف تغرس فيه، فبذلك يحترم القوانين بعد ما كان يخالفها، ويندمج في الحياة الاجتماعية بعدما كان بعيداً ومنعزلاً عنها. ويلاحظ هنا أن المشرع الإماراتي في نص المادة (43) سالفة الذكر ترك أمر تحديد مدة العلاج مطلقة وحسب تقدير القاضي وما يراه، فلم يقيدها بمدة معينة أو محددة.

[1]) محمد شلال العاني: أحكام القسم العام في قانون العقوبات الاتحادي الإماراتي، مرجع سابق، ص236.

المبحث الثالث

وسائل الإثبات الجنائي لجرائم السب والقذف

عبر الشبكة العنكبوتية

تمهيد وتقسيم:

من المعلوم أن الجريمة عبارة عن واقعة مادية وقانونية يرتب عليها القانون أثراً جنائياً هو توقيع العقوبة، وللوصول إلى إثبات الجريمة ينبغي قيام الدليل على ارتكابها، وثبوت نسبتها إلى متهم معين سواء أكان هذا الأخير معروفاً أم مجهولاً، والدليل هو الوسيلة التي يستعين بها القاضي للوصول إلى حقيقة الواقعة المعروضة أمامه، وترجع أهمية الدليل إلى أنه يشير إلى وقوع الجريمة ونسبته إلى المتهم[1]، ومن المعلوم أن الإثبات الجنائي يعتبر من أهم موضوعات الإجراءات الجنائية، وإن جميع الإجراءات هدفها الأساسي هو كيفية إثبات الحقيقة التي وقعت، حيث بموجب الإثبات الجنائي يتحقق براءة المتهم أو معاقبته، لأن هدفه إقامة الدليل لأجل كشف الحقيقة بغية تحقيق العدالة.

مفهوم الإثبات في المواد الجنائية هو: (إقامة الدليل لدى السلطات المختصة بالإجراءات الجنائية على حقيقة واقعة ذات أهمية قانونية، وذلك بالطرق التي

---

[1]) د. محمد مصطفى الدغيدي: التحريات والإثبات الجنائي، مطبعة المنيا، القاهرة، مصر، 2002، ص211.

حددها القانون، ووفق القواعد التي أخضعها لها)[1]، ويعرفه آخرون بأنه: (إقامة الدليل على وقوع الجريمة أو عدم وقوعها وعلى اسنادها إلى المتهم أو براءته منها[2].

كما أن الثورة العلمية في مجال نظم المعلومات الإلكترونية لم تؤثر فقط في نوعية الجرائم التي ترتبت عليها وفي نوعية الجناة الذين يرتكبون هذه الجرائم، وإنما أثرت تأثيراً كبيراً على الإثبات الجنائي، خاصة على طرق هذا الإثبات، حيث يمكن القول أن الطرق التقليدية أصبحت عقيمة بالنسبة لإثبات هذا النوع من الجرائم المستحدثة، لذلك ظهر نوع خاص من الأدلة يمكن الاعتماد عليه في إثبات الجرائم، ومن ثم نسبتها إلى فاعليها، وهو ما يعرف بالدليل السيبراني أو الرقمي[3].

وقسمنا هذا المبحث إلى مطلبين كالآتي:

المطلب الأول: في التفتيش.

المطلب الثاني: في شهادة الشهود والخبرة التقنية.

---

[1]) د. محمود نجيب حسني: شرح قانون الإجراءات الجنائية، رقم 866، ص797.

[2]) د. شعبان محمود محمد الهواري: افتراض البراءة في المتهم كأساس للمحاكمة العادلة، رسالة دكتوراه، دار الفكر والقانون، المنصورة، 2013، ص40 .

[3]) د. عائشة بن قارة مصطفى: حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة، الإسكندرية، 2010، ص27 .

المطلب الأول

إجراءات التفتيش على مواقع الشبكة العنكبوتية

من المعلوم أن التقنية بطبيعتها غير قادرة على تمييزها ما هو مباح وما هو مجرم، وحتى في ظل تزويدها، مثلاً، بنظام مراقبة وفلترة على مواقع الشبكة العنكبوتية، فهي تنفذ أوامر صماء تصلها عبر مخاطبة المبرمج لها، وعبر ترجمة اللغة البرمجية إلى لغة الديجيتال التي تفهمها الأنظمة الحاسوبية، وقد عمد المبرمجين إلى ابتكار مصائد تقنية كثيرة ضمنوها برمجيات الحواسيب الشخصية، وبرمجيات حواسيب المزودين، ليسهل على المحققين الجزائيين اقتفاء أثر المجرم الإلكتروني، فيكون في مقدورهم معرفة المواقع الإلكترونية التي ولجها المعتدي وربطها بموضوع جريمته، أو ليكون في مقدورهم أيضاً تتبع حركة مسار الرسالة الإلكترونية التي أسند فيها تحقيراً إلى المعتدى عليه[1].

وطبقاً للمادة (1/19) من اتفاقية بودابست[2]، تلتزم الدول الأطراف بتخويل السلطات المختصة، صلاحية التفتيش والولوج إلى البيانات المعلوماتية التي تم احتواؤها، سوءا في داخل النظام المعلوماتي أو على دعامة مستقلة، وكذلك تفتيش المكونات المتصلة بالنظام، كما في حالة الحاسب الآلي المحمول والطابعة وأجهزة

---

[1]) د. نبيلة هبة هروال: الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، دراسة مقارنة، دار الفكر، الإسكندرية، 2013، ص199 .

[2]) انظر اتفاقية بودابست المتعلقة بالإجرام المعلوماتي

Convention sur la Cyber Criminalite "BUDAPEST"

التخزين المتصلة، وإذا كانت البيانات مخزنة مادياً في نظام آخر أو في جهاز تخزين آخر، فإنه يمكن الوصول إليها وضبطها من خلال النظام المعلوماتي مع النظم المعلوماتية الأخرى، وطبقاً للفقرة الثانية من المادة (19) من هذه الاتفاقية، فإن للجهات المختصة صلاحية توسيع نطاق التفتيش ليشمل نطاقاً معلوماتياً آخر أو جزءاً منه، بناءاً على أسباب معقولة تدعو للاعتقاد بأن البيانات المطلوب ضبطها مخزنة في هذا النظام المعلوماتي.

كما تنص المادة (4/19) من نفس الاتفاقية أعلاه على أن: لكل دولة طرف الحق في أن تسن من القوانين ما هو ضروري لتمكين السلطات المختصة أن تقوم بالتفيش أو الدخول إلى:

1- نظام الكمبيوتر، أو جزء منه، أو المعلومات المخزنة به.

2- الوسائط التي يتم تخزين معلومات الكمبيوتر بها، مادامت مخزنة في إقليمها.

يبدأ التفتيش الرقمي في جرائم السب والقذف المرتكبة عبر الشبكة العنكبوتية في القطع الصلبة للجهاز، فالمواد التي أسندها المعتدي إلى المعتدى عليه قد تكون محفوظة في القرص الصلب، وتمر الإجراءات من خلال فحص نظام ذاكرة التخزين لمعرفة كل المواقع التي زارها المعتدي في تواريخ معينة، وقد يصل التفتيش إلى الملقمات لدى مزود خدمة الإنترنت، وهي التي استقبلت ملفات بروتوكول الإنترنت الخاص بالمعتدي، وحفظت مسارات ولوجه إلى غرف التداول

وتواريخها، أو حفظت رسائله الإلكترونية أو مكالماته الدولية أو غير ذلك، هذا ويحتاج التفتيش إلى غطاء من المشروعية يتمثل في إذن تفتيش صادر من الجهات المختصة[1].

غير أن برتوكول الشبكة العنكبوتية لا يكفي في إسناد العمل الإجرامي إلى مالك الحاسوب، أو إلى مالك عنوان البرتوكول المتحصل عليه، فقد يكون وقت الجهاز مختلساً، وقد يرتكب المجرم جريمته من جهاز مؤسسة لا تعرف شيئاً عن نشاطه الإجرامي، وقد يرتكبها من مقهى انترنت، أو أن المجرم انتحل عنوان برتوكول لجهاز شخص آخر. لذلك يجب أن تتحصل جهات الاستدلال والتحقيق على أدلة مادية أو على اعترافات قانونية تدعم الدليل الرقمي المتحصل عليه اعتماداً على مسار حركة الشبكة لتتمكن بذلك كله من إدانة المتهم[2].

ولابد من وجوب توفر شرطين في الدليل الإلكتروني حتى يعتد به لدى القضاء، أولهما: الحصول على الدليل بصورة مشروعة توافق أحكام الدستور

---

[1]) د. أبو الوفا محمد أبو الوفا: المواجهة الإجرائية للجرائم المعلوماتية، بحث مقدم الى كلية القانون، جامعة الإمارات، 2009، ص83 .

د. خالد ممدوح إبراهيم: فن التحقيق الجنائي في الجرائم الإلكترونية، ص229

[2]) د. سعيد عبداللطيف حسن: إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، دار النهضة العربية، القاهرة، 2015، ص23-34 .

H.L.CAPRON- J.A.Johnson computer tools for information age 8th Ed, PEARSON Education, Inc., UpperSaddle River, New Jersey 2004, p.p290.

وقانون العقوبات وأصول المحاكمات الجزائية، والآخر: أن تكون الأدلة يقينية غير قابلة للشك[1].

[1]) د. خالد ممدوح إبراهيم: فن التحقيق الجنائي في الجرائم الإلكترونية، ص306.

الفرع الأول

طريقة الحصول على الدليل الرقمي من خلال الشبكة العنكبوتية

من الممكن أن يكون مرتكب الجريمة الإلكترونية أكثر مكراً ودهاءاً مما تتصوره سلطات التحري أو سلطات التحقيق، فيقوم حال احساسه بالمداهمة بمسح البيانات، أو بإتلاف الأقراص الإلكترونية أو بإطلاق فيروسات أو برامج تدميرية لطمس الدليل الرقمي الذي تحصل عليه من جريمته، لذلك يجب على مأمور الضبط القضائي في مرحلة التحريات، وعلى وكلاء النيابة العامة في مرحلة التحقيق الابتدائي أن يتوخوا الحيطة والحذر[1].

ومرحلة التحري هي مرحلة جمع المعلومات المتعلقة بوقوع الجريمة، وهي أيضاً مرحلة الكشف على مكان وقوعها، وضبط الآثار الناتجة عنها، وتحريزها، وملاحقة الجناة والقبض عليهم[2]، ويتولى العمل في هذه المرحلة رجال الضبط القضائي تحت إشراف النيابة العامة، وقد تمتد هذه المرحلة إلى المراحل التي تليها، إلى حين صدور الحكم النهائي في الدعوى، لاستجلاء بعض أوجه الغموض التي تكتنفها. وقد أوجب المادة (40) من قانون الإجراءات الجزائية الإماراتي استعانة السلطة المختصة بالتفتيش بالخبراء، ونصها هو: (لمأموري الضبط القضائي أثناء

---

[1]) د. محمد أمين الشوابكة: جرائم الحاسوب والإنترنت، الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2011، ص98.

[2]) د. عبدالفتاح بيومي حجازي: الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، ص23.

جمع الأدلة أن يسمعوا أقوال من تكون لديهم معلومات عن الوقائع الجنائية ومرتكبيها وأن يسألوا المتهم عن ذلك ولهم أن يستعينوا بالأطباء وغيرهم من أهل الخبرة...).

معاينة المسرح الافتراضي:

1- تحديد نوع نظام المعالجة الآلية للمعلومات، فعملية البحث والتحري أكثر تعقيداً في حال ارتباط الجهاز بمحطات طرفية أخرى.

2- وضع خطة إجمالية للمنشأة وإعداد كشف بأسماء المسؤولين عنها وبعمل كل منهم[1].

3- إذا كان الأمر يتعلق بشبكة، فيجب إحصاء الطرفيات وتحديد طبيعة الروابط القائمة بينها، لمعرفة الطريقة التي يتم بها نقل المعلومات من موقع إلى آخر[2].

4- إن الدليل في مجال معالجة البيانات يمكن أن يختفي في وقت قصير إذا كان الجاني قد أعد فخاً برمجياً، كالقنبلة المنطقية، يعمل في ظروف تشغيلية معينة[1].

---

[1]) د. علي حسن الطوالبة: التفتيش الجنائي على نظم الحاسوب والإنترنت، دراسة مقارنة، عالم الكتب الحديث، القاهرة، 2010، ص179. .

[2]) د. علي حسن الطوالبة: التفتيش الجنائي على نظم الحاسوب والإنترنت، المرجع السابق، ص179 .

5- إن الجاني يمكن أن يتدخل من خلال وحدة طرفية لإتلاف المعلومات المخزنة[2].

6- فصل التيار الكهربائي عن المكان قبل دخوله، فهذا الإجراء يمنع المستخدم من التلاعب بالمعلومات أو محوها، وإن كان لذلك أثره في فقد المعلومات المخزنة في الذاكرة العشوائية لأجهزة الحاسبات الآلية.

7- فصل خطوط الهاتف، خشية استعمال مودم في جهاز المعالجة الآلية للمعلومات المراد ضبطها.

8- التأكد من عدم استخدام خاصية تحويل المكالمات، والتأكد أيضاً من أن رقم الهاتف يخص جهاز الحاسوب المستهدف.

9- إبعاد جميع الموظفين عن أجهزة الحواسيب، مع محاولة الحصول منهم على معلومات حول كلمات السر أو شيفرات الدخول وعن الأماكن الأخرى التي فيها أجهزة حواسيب مرتبطة بهم[3].

---

[1]) د. محمد بن نصير محمد السرحاني: مهارات التحقيق الجنائي الفني في جرائم الحاسب والإنترنت، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2004، ص63.

[2]) د. محمد بن نصير محمد السرحاني: المرجع السابق، ص63.

[3]) د. سامي جلال فقي حسين: الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي، ص61 .

10- تصوير الأجهزة المستهدفة من الأمام والخلف لإثبات أنها كانت تعمل، والمساعدة في إعادة تركيبها لأغراض التحقيق.

ويجب على مأمور الضبط القضائي إعداد نسخة احتياطية من وسائط تخزين المعلومات الموجودة في مسرح الجريمة، وتوثيق جميع نشاطات التحقيق، وهذا أمر مهم للإجراءات الجنائية، فمنذ لحظة فتح القضية إلى لحظة اغلاقها يجب توثيق كل ما يفعله المحقق بالوقت والتاريخ.

كما يتعين تخزين أدلة الأجهزة والبرامج في بيئة مناسبة، ويجب الحذر من المجالات الكهرومغناطيسية والكهرباء الساكنة والغبار، ويجب استخدام ملصقات أو أوراق طرفية لتمييز أجهزة الحاسوب والوسائط والكوابل والأدوات[1].

وفي مرحلة فحص الكيانات المادية والمعنوية وشبكات الحاسوب لاستخراج الدليل الرقمي فإن هناك جانب من الفقه يرى ضرورة اتباع الإجراءات التالية:

1 – فحص الحاسوب والكيانات المادية والمعنوية المتصلة به:

قد تضطر جهة التحقيق إلى ضبط الحاسوب وحجزه وإلى ضبط القطع الصلبة المتصلة به والبرمجيات المخزنة فيها، ويقوم الخبير المختص بالقضايا الشرطية بفحص الحاسوب من خلال تسخير نظم الحاسوب ذاته لتفقد برامجه

[1]) د. عبدالفتاح بيومي حجازي: نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، منشأة المعارف، الإسكندرية، 2009، ص329.

واستدعاء معلوماته، أو قد يتم الفحص بواسطة جهاز حاسوب آخر وبأجهـزة تقنية عالية التخصص، وتقديم تقرير بذلك إلـى طالب الفحص[1].

(أ) فحص القرص الصلب[2]:

يضم القرص الصلب داخله مجموعة البيانات الرقمية ذات الطابع الثنائي، ويمكن إجراء الفحص الكلي أو الجزئي على القرص الصلب، وذلك لهدف التعرف على محتوى البيانات ثنائية الرقم التي يؤدي التعامل معها إلى الكشف عن القيمة الاستردادية للبيانات المخزنة في القرص، سواء أكانت مكتوبة أم على هيئة صور أم أصوات.

(ب) فحص البرمجيات[3]:

وتكون من خلال الفحص الداخلي والخارجي لتلك البرمجيات، ففي الفحص الداخلي يتم التأكد من البناء المنطقي للبرمجية، والبحث عن مصدر الملفات، فصور دعارة الأطفال المخزنة في القرص الصلب في جهاز المعتدي، هل جرى تنزيلها من المواقع الإلكترونية؟ أم أن المعتدي قـام بتنزيلها رقمياً إلى القـرص

---

[1]) د. محمد بن نصير: مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت، المرجع السابق، ص64 وما بعدها.

[2]) د. هلالي عبداللاه أحمد: نظم الحاسب الآلي وضمانات المتهم المعلوماتي، مرجع سابق، ص202.

[3]) د. هلالي عبداللاه أحمد: المرجع السابق، ص202 وما بعدها .

الصلب في جهـازه من كاميرا ديجيتال، ومن ثم قام بتحميلها على مواقع الإنترنت الخاصة بالدعارة؟ ومن ثم فقد يكون المعتدي عميلاً يلعب دوراً خطيراً في جريمة الاتجار بالأطفال، وغيرها أو ما شابه، أما الفحص الخارجي فيتم بموجبه فحص بناء البرمجية، مثلاً: فحص ما إذا كانت البرمجيات منسوخة عن أصل محمي، وحينئذ مطابقة عيوب النسختين للتأكد من كـون إحداهما منسوخة عن الأخـرى، مما يعني قيام جريمة تقليـد البرمجيات[1].

(ج) فحص النظام المعلوماتي[2]:

وهو ضبط كافة ما يحتويه الحاسوب من معلومات مخزنة في ملفات، ويمكن استردادها ما دام موضوعها يتصل بالجريمة، والنظام المعلوماتي في جوهره هو بيانات رقمية مخزنة في أنساق معينة للرقمين، وحين يتم استدعاؤها يظهرها النظام الحاسوبي في صورة معلومات محددة، يفهمها المستدعي مستخدم الجهاز.

(د) فحص نظام ذاكرة التخزين:

إن نظام ذاكرة التخزين كما يقول البعض[1]: (قدرة الحاسوب الآلية على الاحتفاظ في ذاكرته بنسخة كاملة مما اطلع عليه عضو الإنترنت، في أثناء ابحاره

---

[1]) د. علي محمود علي حمودة: الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، مرجع سابق، ص14.

[2]) د. خالد عياد الحلبي: إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2011، ص177-178.

عبر العالم الافتراضي)، حيث يمكن فحص نظام الحاسوب لمعرفة مواقع الإنترنت التي زارها المعتدي فترات طويلة من الزمن، تصل إلى ستة أشهر كاملة، حتى وإن قام المعتدي بحذف كافة الملفات التي قام نظام التشغيل بتخزينها، فيمكن باستخدام برمجيات معينة استعادة كل الملفات المحذوفة التي تبين على وجه الدقة رحلات المتصفح في ربوع المواقع الافتراضية[2].

2 – فحص نظام الاتصال بالإنترنت[3]:

على الرغم من اتساع قاعدة الدليل الرقمي إلا أنه لا يمكن أن يكون متواجداً في صيغة لا يمكن توقعها، فمثلاً: نجد أن التفتيش والتقصي في الحاسوب الشخصي، سعياً وراء البحث عن ملف ما، يرتبط بارتكاب جريمة موضوع هذا التقصي، قد لا يؤدي إلى نتيجة تذكر، إلا أن البحث في نظام البريد الإلكتروني قد يؤدي إلى العثور على ما يفيد في إثبات الجريمة الإلكترونية المرتكبة عبر الإنترنت، على أن يصل إلى الملف من أي مكان وفي أي وقت وذلك من خلال فحص ما يلي:

---

[1]) د. سامي جلال فقي حسين: التفتيش في الجرائم المعلوماتية، دار الكتب القانونية، القاهرة، 2015، ص201.

[2]) د. سامي جلال فقي حسين: التفتيش في الجرائم المعلوماتية، المرجع السابق، ص270.

[3]) د. سامي جلال فقي حسين: التفتيش في الجرائم المعلوماتية، المرجع السابق، ص270.

(أ) فحص مسار الإنترنت:

وهي الحركة التراسلية للنشاط الممارس عبر شبكة الإنترنت من خلال الحاسوب، بمجرد أن يتعرف على المسار، ويقوم تلقائياً باختيار البروتوكول التراسلي، ومن خلاله يقوم باستدعاء البيانات، ويستخدم نظام الفحص الإلكتروني في تتبع حركة مسار الإنترنت، الذي يطلق عليه علم البصمات المعاصر في القرن الواحد والعشرين، وهو عبارة عن منهج ينشط في تتبع الحركة العكسية لمسار الإنترنت[1].

(ب) فحس بروتوكول الإنترنت:

يعد هذا البروتوكول الطابع المميز لاستخدام الإنترنت، فأي شخص يحصل على بروتوكول الإنترنت يمكنه الإبحار في ربوع المواقع الافتراضية، فيباشر تصفح المواقع والانتفاع بخدماتها، وعملية البحث في قواعد البيانات لدى مسجلي بروتوكول الإنترنت عملية سهلة، تمكن سلطة التحقيق من تحديد حائز هذا البروتوكول أو ذلك، عن طريق البحث في قاعدة بيانات خاصة بالمسجلين[2].

---

[1]) د. علي محمود حمودة: الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، مرجع سابق، ص14.

[2]) د. سامي جلال فقي حسين: التفتيش في الجرائم المعلوماتية، المرجع السابق، ص202.

د. علي محمود حمودة: الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، المرجع السابق، ص15.

(ج) فحص الخادم:

الخادم هو حاسوب مهمته تحقيق حركة الاتصال بالمواقع والصفحات، وكذلك تحديد مسارات الاتصال المعقدة على هيئة بيانات رقمية على الشبكة العنكبوتية، ومن الخوادم ما لا تكون مهمته تحقيق اتصال مع المواقع والصفحات، وإنما القيام بتحقيق التواصل مع حلقات النقاش والأحاديث المباشرة أو تخزين البريد الإلكتروني لا غير، على أن يعمل هذا الخادم على ربط أعضاء الإنترنت بغرف التداول والحديث المتواصل، فيبرز عضو الإنترنت كما لو كان يستضيف من يتحدث معه[1].

[1]) د. نبيلة هبه هروال: الجوانب الإجرائية لجرائم الإنترنت، ص227 .

الفرع الثاني

التفتيش في مراسلات البريد الإلكتروني وتعقب المرسل

تم ابتكار نظام البريد الإلكتروني ليتمكن مستخدمو هذه التقنية من تبادل الرسائل والصور وغيرها من المواد القابلة للإدخال الرقمي في صندوق الرسالة، أو القابلة للتحميل الرقمي بصفتها ملحقات بالرسالة، وترسل الرسالة من بريد أحدهم إلى عنوان بريد إلكتروني ما، دون أي إبطاء ودون كلفة مالية سوى كلفة اشتراك خدمة التزود بوقت الإنترنت بشكل عام[1]، ويتمتع البريد الإلكتروني أيضاً بخدمة (قائمة التراسل)، وهو نظام تراسل جماعي يمنح صلاحيات بث رسالة إلى مجموعة من الأشخاص المسجلين في هذه القائمة، ولا شك أن هذا النظام تم تطويره لتشجيع العمل الجماعي وتبادل الأفكار والخبرات ويحتوي البريد الإلكتروني برامج متخصصة لكتابة الرسائل الإلكترونية وإرسالها واستعراضها وتخزينها، وكذلك للتوقيع الإلكتروني وقد ابتكرت نظم البريد الإلكتروني برامج تشفير خاصة لحماية خدمة البريد الإلكتروني من الاختراقات ولضمان خصوصية محتوياتها[2].

الأصول القانونية المتبعة في تفتيش البريد الإلكتروني:

---

[1]) د. أمير فرج يوسف، الإثبات الجنائي للجريمة الإلكترونية والاختصاص القضائي بها، مرجع سابق، ص85.

[2]) د. أبو الوفا محمد أبو الوفا: المواجهة الإجرائية للجرائم المعلوماتية، بحث مقدم الى كلية القانون جامعة الإمارات، المرجع السابق، ص81-82.

يتم ضبط البريد الإلكتروني الخاص بالضحية كالآتي: يطلب المحقق من الضحية الولوج إلى بريده باستخدام اسم المستخدم وكلمة السر، ثم يذهب إلى قائمة Inbox وينقر على الرسالة التي تتضمن الأسانيد الجارحة في جريمة القذف والسب، ويطبع الرسالة بصورة تظهر صندوق العرض وفيه اسم المرسل وعنوان بريده الإلكتروني وعنوان بريد الضحية، وكذلك مادة الرسالة وكما يلي[1]:

1- إذا اقتضت الحال البحث عن أوراق فللمدعي العام وحده أو مأمور الضبط القضائي المستناب وفقاً للأصول أن يطلع عليها قبل ضبطها.

2- لا تفض الاختام ولا تفرز الأوراق بعد ضبطها إلا في حضور المشتكى عليه أو وكيله أو في غيابهما إذا دعيا وفقاً للأصول ولم يحضرا ويدعى أيضاً من جرت المعاملة عنده لحضورها، يتبع هذا الأصول بقدر الإمكان ما لم يكن هنالك ضرورة دعت لخلاف ذلك.

3- يطلع المدعي العام وحده على الرسائل والبرقيات المضبوطة حال تسلمه الأوراق في غلافها المختوم فيحتفظ بالرسائل والبرقيات التي يراها لازمة لإظهار الحقيقة أو التي يكون أمر اتصالها بالغير مضراً بمصلحة التحقيق، ويسلم ما بقي منها إلى المشتكى عليه أو إلى الأشخاص الموجهة إليهم.

---

[1]) د. انظر المادة (89) من قانون أصول المحاكمات الجزائية الأردني وتعديلاته رقم (9) لسنة 1961، بعنوان (أحكام ضبط الأدلة الورقية).

4- ينبغي أن ترسل أصول الرسائل والبرقيات المضبوطة جميعها أو بعضها أو صور عنها إلى المشتكى عليه أو إلى الشخص الموجهة إليه في أقرب مهلة مستطاعة إلا إذا كان أمر اتصالها بهما مضراً بمصلحة التحقيق.

إجبار المتهم والشاهد على تقديم الدليل الرقمي:

يفترض القانون أن المتهم برئ حتى تثبت إدانته، لأن الأصل في الإنسان البراءة، لذلك يتطلب افتراض البراءة في المتهم عدم مطالبته بتقديم أي دليل على براءته، ويمكن للمتهم أن يتخذ موقفاً سلبياً تجاه الدعوى أو الشكوى المقدمة ضده، وعلى النيابة العامة تقديم الدليل على ثبوت التهمة المنسوبة إليه، ويتصل بهذا المبدأ عدم جواز إجبار الشخص على اتهام نفسه، سواء عن طريق الاعتراف أو عن طريق تقديم أدلة تدينه، وبناء على هذا فهل يجوز لسلطة الضبط أن تجبر المتهم على الكشف عن شيفرة الدخول إلى جهازه، أو ا لى أحد أقسام التخزين لتمكينها من الوصول إلى المعلومات المجرمة؟ وهل يجوز أن تجبر الشاهد على ذلك؟[1].

انطلاقاً من المبدأ السابق، يذهب الفقه إلى أنه لا يجوز قانوناً إجبار المتهم على طباعة ملفات بيانات خاصة مخزنة داخل نظام المعالجة الآلية للمعلومات أو إلزامه بالكشف عن الشفرات أو كلمات السر بالدخول إلى هذه المعلومات، أو

[1]) انظر المادة (89) من قانون أصول المحاكمات الجزائية الأردني رقم (9) لسنة 1961 المعدل.

إجباره على تقديم الأسم Command اللازم لوقف الفيروس، أو تفكيك القنبلة المنطقية، غير أن رفض المتهم التعاون قد يدفع سلطات التحقيق إلى حبسه احتياطياً بحجة عدم التأثير على سير التحقيق أو العبث بالأدلة. ويشترط لذلك أن تكون الجريمة موضوع المحاكمة مما يجيز فيها المشرع الحبس الاحتياطي، كما أن تصرف المتهم على هذا النحو قد يلعب دوراً في تكوين عقيدة القاضي ضده[1].

[1]) د. أبو الوفا محمد أبو الوفا: المرجع السابق، ص82.

المطلب الثاني

أقوال الشهـود والخبرة التقنية

الفرع الأول

أقوال الشهـود

الشهادة لها دور كبير كدليل إثبات، كما أنها المصدر المهم الذي يستطيع أن يقدم الأدلة في مراحل الجريمة الإعداد لها والشروع بعد ذلك في ارتكابها، ثم إتمام تنفيذها، والاختفاء بعدئذ، لذلك تبقى الشهادة عماد الإثبات في المسائل الجنائية بالنظر لما تمثله من دليل حي ملموس يسمعه المحقق الجنائي ويؤثر بشدة في تشكيل اقتناعه مما يجعلها تتميز عن غيرها من الأدلة[1].

والشهادة تعرف بأنها: (الأقوال التي يدلي بها غير الخصوم أمام سلطة التحقيق بشأن جريمة وقعت، سواء كانت تتعلق بثبوت الجريمة وظروف ارتكابها وإسنادها إلى متهم أو براءته منها)[2]، وعرفت الشهادة أيضاً بأنها: (كل ما يروى

---

[1]) رياد بن محمد بن فالح اللحيد: العزوف عن الشهادة في القضايا الجنائية–الأسباب والحلول، رسالة ماجستير، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2002، ص6.

[2]) د. هلالي عبداللاه أحمد: تفتيش نظم الحاسب وضمانات المتهم المعلوماتي، مرجع سابق، ص48.

من أي شخص متصلاً بموضوع أو واقعة معينة عن طريق الرؤية أو السماع المباشر)[1].

كما يعرف الشاهد على أنه: (هو الشخص الذي كان حاضراً وقت ارتكاب واقعة ما، أو من يمكن الحصول منه على إيضاحات بشأن الواقعة وفاعلها، أو من يرى المحقق فائدة من سماع شهادته، أو من يرى لزوم سماع شهادته على الوقائع التي تثبت ارتكاب الجريمة وأحوالها وإسنادها للمتهم، أو براءة ساحقة منها ويتوصل بها إلى ذلك)[2].

فقد نصت المادة (36) من قانون الإجراءات الجزائية الإماراتي على أنه: (يجب أن تثبت جميع الإجراءات التي يقوم بها مأمور الضبط القضائي في محاضر موقع عليها منهم يبين بها وقت اتخاذ الإجراءات ومكان حصولها، ويجب أن تشمل تلك المحاضر زيادة على ما تقدم تواقيع المتهمين والشهود والخبراء الذين سئلوا، وفي حالة الاستعانة بمترجم يتعين توقيعه على المحاضر المذكورة، وترسل المحاضر إلى النيابة العامة مع الأوراق والأشياء المضبوطة).

وكذلك نصت المادة (40) من قانون الإجراءات الجزائية الإماراتي على: (لمأموري الضبط القضائي أثناء جمع الأدلة أن يسمعوا أقوال من تكون لديهم معلومات عن الوقائع الجنائية ومرتكبيها وأن يسألوا المتهم عن ذلك، ولهم أن

---

[1]) د. نبيل عبدالمنعم جاد: التحريات الجنائية، مرجع سابق، ص65.

[2]) د. رياد بن محمد بن فالح: المرجع السابق، ص7.

يستعينوا بالأطباء وغيرهم من أهل الخبرة ولا يجوز لهم تحليف الشهود أو الخبراء اليمين إلا إذا خيف ألا يستطاع فيما بعد سماع الشهادة).

ومع ذلك هناك جانب من التشريعات يلزم الغير، ومنهم الشهود، بتقديم المساعدة للسلطة القضائية عن طريق تقديم الأدلة أو المساعدة في الوصول إليها، مثل قانون الإجراءات الجزائي الهولندي، الذي يجيز في المادة (1-125) منه قيام قاضي التحقيق بإلزام أي شخص بالكشف عن سبيل الدخول إلى المعلومات الجرمية المخزنة في الحاسوب المضبوط، والمادة (125-k) من نفس القانون تجيز لقاضي التحقيق أن يأمر أي شخص له دراية بتشغيل نظام المعالجة بفك شيفرة النظام لتمكين المفتش من الدخول إلى البيانات الجرمية، كما أن بعض التشريعات القانونية تمارس الضغط على الشهود لهدف حملهم على التعاون الإيجابي مع سلطات التحقيق، فمنها من يسأل الشاهد الذي يخفي الشيفرة أو كلمات السر عن جريمة شهادة الزور، لأنه في فهمها يعوق سير العدالة، ومنها من يسأل الشاهد غير المتعاون باعتباره شريكاً في الجريمة موضوع المحاكمة[1].

[1]) د. خالد ممدوح إبراهيم: فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص229، ص386.

د. مصطفى محمد موسى: التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص64.

والشهود في الجرائم المرتكبة عبر الإنترنت، عدة طوائف منهم ما يلي[1]:

1- **المبرمجون:** هم المتخصصون في كتابة البرامج ويقسمون إلى فئتين، الأولى: هم المتخصصون في برامج التطبيقات، وهؤلاء يحصلون على خصائص النظام المطلوب من محلل النظم ثم يقوم بتحويلها إلى برامج دقيقة، أما الفئة الثانية فهم: المتخصصون في برامج النظم ويقومون باختبار وتعديل وتصحيح برامج نظام الحاسوب الداخلية التي تتحكم في وحدات الإدخال والإخراج ووسائط التخزين بالإضافة إلى إدخال أي تعديل أو إضافة تعديلات لهذه البرامج[2].

2- **المحلل:** هو شخص متمكن بتحليل خطوات العمل والبيانات وتحليلها ويقوم بتتبع البيانات داخل النظام.

3- **مهندسو الصيانة والاتصالات:** وهم الأشخاص المسؤولون عن أعمال الصيانة الخاصة بتقنيات الحاسب بمكوناته وشبكات الاتصال المتعلقة به، وهؤلاء يمكن الاستعانة بهم عند إجراء تفتيش شبكات الحاسب لأن هؤلاء يكونون على دراية تامة بكيفية عمل الشبكات وكيف يمكن استخراج الأدلة منها.

---

[1]) د. عبدالله حسين علي: إجراءات جمع الأدلة في مجال جريمة السرقة، بحث مقدم الى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي، 2003، ص20.

د. أحمد يوسف الطحاوي: الأدلة الإلكترونية ودورها في الإثبات الجنائي، مرجع سابق، ص140-141.

[2]) د. هلالي عبداللاه أحمد: تفتيش نظم الحاسب الآلي، المرجع السابق، ص49 وما بعدها.

4- **مديرو النظم:** وهم الذين يوكل إليهم أعمال الإدارة في النظم المعلوماتية.

الفرع الثاني

الخبــرة التقنية

تكمن أهمية الخبرة في إنها تقدم مساعدة كبيرة للقضاء وللسطات المختصة بالدعوى الجزائية، وبدونها يتعذر الوصول إلى الحقيقة بشأن المسائل الفنية التي تحتاج إلى خبير مختص، خصوصاً تلك التي من شأنها أن تكشف الجوانب المبنية على الحقائق العلمية والفنية. فالعنصر المميز للخبرة عن غيرها من إجراءات الإثبات هو علم ودراية الخبير وإلمامه بهذا الفن وقدرته على التوصل للحقيقة من خلال كشف الدلائل أو الأدلة وتقديمها للعدالة[1].

وهو ما نص عليه المشرع في قانون الإجراءات الجزائية الإماراتي في المادة (93) حيث نصت على أنه: (إذا اقتضى التحقيق الاستعانة بطبيب أو غيره من الخبراء لإثبات حالة من الحالات كان لعضو النيابة العامة أن يصدرا أمراً بندبه ليقدم تقريراً عن المهمة التي يكلف بها. ولعضو النيابة العامة أن يحضر وقت مباشرة الخبير مهمته ويجوز للخبير أن يؤدي مهمته بغير حضور الخصوم)[2]، وللخبير التقني[3]، في سبيل تحري الحقيقة أن يقوم بكل ما يمكنه من التوصل

---

[1]) د. خالد حامد مصطفى: شرح قانون الإجراءات الجزائية لدولة الإمارات العربية المتحدة، مرجع سابق، ص506.

[2]) المادة (93) من قانون الإجراءات الجزائية لدولة الإمارات العربية المتحدة.

[3]) تطبيقاً لذلك: قضت المحكمة الاتحادية العليا بأنه إذا كان الحكم المطعون فيه قد استند في قضائه ببراءة المطعون ضده الأول إلى ما ثبت للمحكمة التي أصدرته بعد اطلاعها على

إليها، وعليه في إطار القيام بعمله أن يستخدم الأساليب العلمية التي يقوم عليها تخصصه، وليس للمحكمة أن ترفض تلك الأساليب، ما لم يكن رفضها لها مسبباً بشكل منطقي وإلا تعرض حكمها للطعن عليه بالنقض[1].

وهناك أسلوبان لعمل الخبير التقني:

الأول: القيام بتجميع وتحصيل لمجموعة المواقع التي تشكل جريمة في ذاتها، وذلك هو الشأن في التهديد، أو النصب أو السب أو جرائم النسخ وبث صور فاضحة بقصد الدعاية للتحريض على ارتكاب جرائم القذف والسب والدعارة والرق ودعارة الأطفال وغيرها، ثم القيام بعملية تحليل رقم لها لمعرفة كيفية إعدادها البرمجي ونسبتها إلى مسارها الذي اعدت فيه، وتحديد عناصر حركتها، وكيف تم التوصل

العلامتين التجاريتين، الأصلية والمقلدة، من عدم وجود تشابه بينهما دون الاستعانة بأهل الخبرة الفنية المتخصصة في هذا الشأن فإنه يكون مشوب بالقصور المبطل الموجب للنقض.

المحكمة الاتحادية العليا، نقض جزائي، 7/4/2008، مجموعة الأحكام الجزائية رقم 19، ص63.

ونخلص مما سبق بيانه أن تقرير الخبير يخضع في نهاية الأمر. لتقدير محكمة الموضوع صاحبة السلطة التامة في فهم وتقدير الادلة فيها، ومنها تقارير الخبرة ولا معقب عليها في ذلك طالما لم تعتمد على واقعة بغير سند وحسبها أن تبين الحقيقة التي اقتنعت بها.

المحكمة الاتحادية العليا – الأحكام الجزائية– الطعن رقم 79 لسنة 2011 قضائية بتزيخ 21/6/2011..

[1]) د. سامي جلال فقي حسين: التفتيش في الجرائم المعلوماتية، مرجع سابق، ص147.

إلى معرفتها، ومن ثم التوصل في النهاية إلى معرفة بروتوكول الإنترنت IP الذي ينسب إلى جهاز الكمبيوتر الذي صدر عنه هذه المواقع[1].

الثاني: القيام بتجميع وتحصيل لمجموعة المواقع التي لا يشكل موضوعها جريمة في ذاته، وإنما يؤدي حال تتبع موضوعها إلى قيام الأفراد بارتكاب جرائم، كما هو الحال في المواقع التي تساعد الغير على التعرف على جرعات المخدرات والمؤثرات العقلية ذلك حسب وزن الإنسان بادعاء انه إذا تم تتع التعليمات الواردة فيها فلن يطالب الشخص بحالة إدمان، وأيضاً كيفية زراعة المخدرات بعيداً عن أعين الغير، وأيضاً كيفية إعداد القنابل وتخزينها، وكيفية التعامل مع القنابل الزمنية وتركيبها والقيام بفكها وحفظها، وكذلك القيام بتحديد مسار الدخول على مواقع دعارة من أماكن متفرقة دون لزوم القيام بتحديد مسار الدخول من مكان ثابت، ومثل هذا الأمر جائز الحدوث كما لو كان مرتكب الجريمة مشتركاً لدى مزود في مدينة مختلفة عن تلك التي يقيم فيها معلوماتياً محدداً غير قابل للتحويل إلى مظهر آخر إلا بإجراء تعديلات رقمية في البيانات المذكورة[2].

---

[1]) د. عبدالفتاح بيومي حجازي: الدليل الجنائي والتزوير في الجرائم الإلكترونية، مرجع سابق، ص102.

د. خالد ممدوح إبراهيم: فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص292.

[2]) انظر في ذلك، د. أمير فرج يوسف: الإثبات الجنائي للجريمة الإلكترونية والاختصاص القضائي بها، مرجع سابق، ص98؛ د. مصطفى محمد موسى: التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص215.

أما بالنسبة لعملية حفظ الأدلة في العالم الرقمي فإنه يتطلب من الخبير التقني رصد موقع الإنترنت أو المعلومات التي تشير إلى الجريمة والتي تكون في مظاهر مختلفة الأشكال، كما لو كانت الجريمة من جرائم القذف والسب في غرف المناقشة، ففي مثل هذه الحالة الأخيرة يتم اللجوء إلى ذاكرة الخادم الذي يتولى ربط هذه الغرف عبر العالم الرقمي لكي يمكن التوصل إلى تحديد موضوع السب والقذف وتاريخه، وإذا كانت الجريمة من جرائم النشر عبر الإنترنت فقد يكتفي بمجرد اللجوء إلى ذاكرة الحاسب الآلي المستخدم هنا دون حاجة إلى تحديد الخادم ..الخ.

في مثل هذه الحالات يقوم الخبير باستخدام برمجيات مساعدة للتوصل إلى القيم بالحفظ في العالم الرقمي، كما هو الشأن في حجز وتشفير مثل هذه المواقع بعد تحديد جدليتها ودقتها ومسارها، وهذا أمر يترتب عليه عدم إمكانية حذفها من العالم الرقمي، فإذا قام أحدهم بالحذف اعتبر عمله قرينة على أنه هو من ارتكب الجريمة[1].

وتستدعي عملية حفظ الأدلة في العالم الرقمي لزوم قيام الخبير بعرض الأدلة في المحكمة أو على جهات التحقيق، ومثل هذا الأمر يجعل عمل الخبير يستمر لمرحلة المحاكمة، كما هو الشأن حال عرض الدليل المقدم إلى محكمة

[1]) د. أمير فرج يوسف: الإثبات الجنائي للجريمة الإلكترونية والاختصاص القضائي بها، مرجع سابق، ص98.

الموضوع أمام جهة قضائية أعلى كالاستئناف أو النقض (في حالة اختصاصها بالموضوع – الطعن مرتين)[1].

ويقوم بالولوج إلى الإنترنت من محل إقامته، وهذا الأخير من الدفوع التي تلتزم محكمة الموضوع بالرد عليها[2].

والخبرة في الجرائم الإلكترونية تساعد في المسائل الآتية:

- الكشف عن الدليل الإلكتروني.
- إجراء الاختبارات التكنولوجية والعلمية عليه لاختباره والتحقق من أصالته ومصدره كدليل يمكن تقديمه لأجهزة إنفاذ وتطبيق القانون.
- تحديد الخصائص الفريدة للدليل الإلكتروني[3].
- إصلاح الدليل وإعادة تجميعه من المكونات المادية للكمبيوتر.
- عمل نسخة أصلية من الدليل الرقمي للتأكد من عدم وجود معلومات مفقودة أثناء عملية استخلاص الدليل.

---

[1]) د. مصطفى محمد موسى: التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص215.

[2]) د. خالد ممدوح إبراهيم: فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص294.

[3]) د. عفيفي كامل عفيفي: جرائم الكمبيوتر، مرجع سابق، ص306.

راضية سلام عدنان: مشروعية الدليل الإلكتروني، مرجع سابق، ص101.

- استخدام الخوارزميات[1] للتأكد من أن الدليل الإلكتروني لم يتم العبث به أو تعديله.

- تحريز الدليل الرقمي لإثبات أنه أصيل وموثوق به ويقع ضمن سلسلة الأدلة المقدمة فى الدعوى.

- جمع الآثار المعلوماتية الإلكترونية التي قد تكون تبدلت خلال الشبكة المعلوماتية.

- تحديد الخصائص المميزة لكل جزء من الأدلة الإلكترونية، ومن ذلك المستند الرقمي، البرامج، التطبيقات، الاتصالات، الصور، الأصوات .... وغيرها[2].

[1]) الخوارزميات هي مجموعة هن التعليمات التي يمكن أن تتبع لإنجاز عمل ما بعدد محدد من الخطوات وذلك عبر تجزئة المسألة البرمجية المراد حلها إلى أجزاء صغيرة بسيطة وبتجميع هذه الأجهزة يمكن التوصل إلى حل صحيح. انظر في ذلك : د. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص303.

[2]) د. عفيفي كامل عفيفي: جرائم الكمبيوتر، مرجع سابق، ص306.

راضية سلام عدنان: مشروعية الدليل الإلكتروني، مرجع سابق، ص101.

وسائل الخبرة في اكتشاف الدليل الإلكتروني:

ثمة وسائل قد تساعد الخبير في الوصول إلى المجرم الإلكتروني ومعرفة كيفية وقوع الجريمة، وهي وسائل مادية، أو وسائل إجرائية، نتناولها على النحو التالي:

1- الوسائل المادية:

هي الأدوات الفنية التي غالباً ما تستخدم في بنية نظام المعلومات والتي يمكن باستخدامها تنفيذ إجراءات واساليب التحقيق المختلفة التي تثبت وقوع الجريمة، ومن أهمها:

- **عنوان بروتوكول الإنترنت IP والبريد الإلكتروني برامج المحادثة**[1]:

عنوان الإنترنت هو المسؤول عن تراسل حزم البيانات عبر شبكة الإنترنت وتوجيهها إلى أهدافها، وهو يشبه إلى حد كبير عنوان البريد العادي، حيث يتيح للموجهات والشبكات المعنية نقل الرسالة، وهو في كل جهاز مرتبط بالإنترنت. ويتكون من أربعة أجزاء وكل جزء يتكون من أربع خانات، حيث يشير الجزء الأول من اليسار إلى المنطقة الجغرافية، والجزء الثاني لمزود الخدمة، والثالث لمجموعة الحاسبات الآلية المرتبطة، والرابع يحدد الكمبيوتر الذي تم الإتصال منه.

وفي حالة وجود أي مشكلة أو أية أعمال تخريبية فإن أول ما يجب أن يقوم به المحقق هو البحث عن رقم الجهاز وتحديد موقعه لمعرفة الجاني الذي قام بتلك

[1]) د. خالد ممدوح إبراهيم: فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص360.

الأعمال غير القانونية، ويمكن لمزود خدمة الإنترنت أن يراقب المشترك، كما يمكن للشبكة التي تقدم خدمة الاتصال الهاتفي أن تراقبه أيضاً إذا ما توافرت لديها أجهزة وبرامج خاصة لذلك[1]، وهناك أكثر من طريقة يمكن من خلالها معرفة هذا العنوان الخاص بجهاز الكمبيوتر في حالة الاتصال المباشر، ومن ذلك على سبيل المثال ما يستخدم في حالة العمل على نظام التشغيل Windows حيث يتم كتابة wingpcfg في أمر التشغيل ليظهر مربع حوار يبين فيه عنوان IP، مع ملاحظة أن عنوان الإنترنت قد يتغير مع كل اتصال بشبكة الإنترنت. أما في حالة استخدام أحد البرامج التحادثية كأداة للجريمة فإنه يتطلب تحديد هوية المتصل، كما تحدد رسالة البريد الإلكتروني عنوان شخصية مرسلها ولو لم يدون معلوماته في خانة المرسل، شريطة آن تكون تلك المعلومات التي وضعت في مرحلة إعدادات البريد الإلكتروني معلومات صحيحة[2].

- **البروكسيPROXY**[3]: يعمل البروكسي كوسيط بين الشبكة ومستخدميها بحيث تضمن الشركات الكبرى المقدمة لخدمة الاتصال بالشبكات قدرتها لإدارة الشبكة، وضمان الأمن وتوفير خدمات الذاكرة الجاهرة. وتقوم فكرة البروكسي على تلقي مزود البروكسي طلباً من المستخدم للبحث عن صفحة ما ضمن ذاكرة المحلية

---

[1]) د. عفيفي كامل عفيفي: جرائم الكمبيوتر، مرجع سابق، ص308.

[2]) د. علي محمود علي حمودة: الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، مرجع سابق، ص921.

[3]) د. خالد ممدوح إبراهيم: فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص305.

المتوفرة، فيتحقق البروكسي فيما إذا كانت هذه الصفحة قد جرى تنزيلها من قبل، ليقوم بإرسالها إلى المستخدم بدون الحاجة إلى إرسال الطلب إلى الشبكة العالمية، فإذا لم يتم تنزيلها من قبل فسوف يتم إرسال الطلب إلى الشبكة العالمية، وفي هذه الأخيرة يعمل البروكسي كمزود عميل ويستخدم عنوان IP . ومن أهم مزايا مزود البروكسي أن ذاكرة Cache المتوفرة لديه يمكن أن تحتفظ بتلك العمليات[1]، التي تمت عليها مما يجعل دوره قوياً في الإثبات عن طريق فحص تلك العمليات المحفوظة بها والتي تخص المتهم والموجودة عند مزود الخدمة[2].

- **نظام كشف الاختراق:** يرمز له اختصاراً بالأحرف IDS ، وهذه الفئة من البرامج تتولى مراقبة بعض العمليات التي يجري حدوثها طي أجهزة البرامج، تتولى مراقبة بعض العمليات التي يجري حدوثها على أجهزة الحاسب الآلي أو الشبكة مع تحليلها بحثاً عن أية إشارة قد تدل على وجود مشكلة قد تهدد من الكمبيوتر أو الشبكة. ويتم ذلك من خلال تحليل رزم البيانات أثناء انتقالها عبر الشبكة ومن بعض ملفات نظام التشغيل الخاصة بتسجيل الأحداث فور وقوعها في جهاز الحاسب الآلي أو الشبكة، ومقارنة نتائج التحليل بمجموعة من الصفات المشتركة للاعتداءات على الأنظمة الحاسوبية، والتي يطلق عليها أهل الاختصاص مصطلح

---

[1]) د. خالد بن مرزوق بن سراج العتيبي: الجوانب الإجرائية في الشروع في جرائم المعلوماتية، مرجع سابق، ص68-69.

[2]) راضية سلام عدنان: مشروعية الدليل الإلكتروني، مرجع سابق، ص103.

د. خالد ممدوح إبراهيم: فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص305.

التوقيع، وفي حال اكتشاف النظام وجود أحد هذه التواقيع يقوم بإنذار مدير النظام بشكل فوري وبطرق عدة ويسجل البيانات الخاصة بهذا الاعتداء في سجلات كمبيوترية خاصة[1].

- **برامج التتبع:** تقوم هذه البرامج بالتعرف على محاولات الاختراق التي تتم، وتقديم بيان شامل بها إلى المستخدم الذي تم اختراق جهازه، ويحتوي هذا البيان على اسم الحدث وتاريخ حدوثه وعنوان IP الذي تمت من خلاله عملية الاختراق، واسم الشركة المزودة لخدمة الإنترنت المستضيفة للمخترق، وأرقام مداخلها ومخارجها على شبكة الإنترنت ومعلومات أخرى[2].

2 – الوسائل الإجرائية[3]:

يقصد بهذه الوسائل الإجراءات التي باستخدامها يتم تنفيذ طرق التحقيق الثابتة والمحددة والمتغيرة وغير المحددة التي تثبت وقوع الجريمة، وتحدد شخصية مرتكبها ومنها:

---

[1]) د. علي محمود علي حمودة: الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، مرجع سابق، ص91.

[2]) د. خالد بن مرزوق بن سراج العتيبي: الجوانب الإجرائية في الشروع في جرائم المعلوماتية، مرجع سابق، ص30.

[3]) انظر بصورة مفصلة، د. خالد ممدوح إبراهيم: فن التحقيق في الجرائم الإلكترونية، مرجع سابق، ص306

- **اقتفاء الأثر:** من أخطر ما يخشاه مجرم نظم المعلومات تقصي أثره أثناء ارتكابه للجريمة، فهناك الكثير من الوثائق التي يتم نشرها في المواقع الخاصة بالمخترقين تحمل بين جنباتها العديد من النصائح، وأهم نصيحة هي: قم بمسح الآثار فمؤكد أنه سوف يتم القبض عليه حتى وإن كانت عملية الاختراق قد تمت بشكل سليم، ويمكن تقصي الأثر بطرق عدة، سواء عن طريق بريد إلكتروني تم استقباله، أو عن طريق تتبع أثر الجهاز الذي تم استخدامه للقيام بعملية الاختراق.

- **الاطلاع على عمليات التنظيم المعلوماتي وأسلوب حمايته:** ينبغي على المحقق وهو بصدد التحقيق في إحدى الجرائم المعلوماتية كالجرائم المتعلقة بشبكات وتطبيقات وخدمات العملاء، كما ينبغي عليه الاطلاع على عمليات النظام المعلوماتي كقاعدة البيانات وإدارتها وخطة تأمينها، ومراقبة مواد النظام والمستفيدين، والملفات والإجراءات، وتصنيف الموارد العامة، ومدى مزامنة الأجهزة، ومدى تخصيص وقت معين في اليوم يسمح باستخدام كلمات المرور، ومدى توزيع الصلاحيات للمستفيدين، وإجراءات أمن العاملين، وأسلوب النسخ الاحتياطي والاستعانة ببرامج الحماية، كمراقبة المستفيدين والموارد والبرامج التي تعالج البيانات وتسجيل الوقائع وحالات فشل الدخول إلى النظام.

- **الاستعانة بالذكاء الاصطناعي:** أثبتت تقنيات الكمبيوتر نجاحها في جمع الأدلة الجنائية وتحليلها واستنتاج الحقائق منها، وهنا يمكن الاستعانة بالذكاء الصناعي في حصر الحقائق منها، كما يمكن الاستعانة بالذكاء الصناعي في

حصر الحقائق والاحتمالات والأسباب والفرضيات، ومن ثم استنتاج النتائج على ضوء معاملات حسابية يتم تحليلها بالكمبيوتر وفق برامج صممت خصيصاً لهذا الغرض[1].

دور الخبير التقني في حفظ أدلة الكمبيوتر:

في إطار جرائم الإنترنت يجب التمييز بين الأدلة التي يلزم التحفظ عليها داخل جهاز الحاسب الآلي وبين تلك التي يلزم بقاؤها في العالم الافتراضي، وبين تلك الأدلة النوعية التي تنتمي إلى العالم الرقمي؛ ومع ذلك يمكن اللجوء إلى إخراجها من إطار الحاسوب والعالم الرقمي إلى العالم المادي بحيث يتم التعامل معها كمخرجات يقبلها القضاء كأدلة كاملة في الجريمة تساعد في الإدانة وكذلك في البراءة[2].

إن التحفظ عر الأدلة داخل جهاز الكمبيوتر من العمليات المعقدة التي تحتاج بدايةً إلى رصد دقيق لمدى صحة البيانات التي يحتوي عليها الكمبيوتر، وهذا الأمر يستلزم بالضرورة قيام الخبير التقني بالكشف – بدايةً – على مدى صحة حركة الكمبيوتر، ولا سيما من حيث الخلل والعطب ويعطي العدوان الفيروسي مثالاً حيوياً

---

[1]) انظر في ذلك؛ د. خالد ممدوح إبراهيم: فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص310.

[2]) د. عبدالفتاح بيومي حجازي: الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، مرجع سابق، ص112.

هنا، إذ يكفي أن يكون هناك فيروس في الجهاز لكي يتم التشكيك في صحة الأدلة المستفادة من هذا الكمبيوتر، ومثل هذا الاتجاه في التشريع الإنجليزي[1].

وتتم عملية حفظ الأدلة داخل جهاز الكمبيوتر بأساليب متعددة تتمثل في أبسط مظاهرها باستخدام أسلوب الحفظ العادي، وأقوى مظاهرها في عمليات حجز الحاسوب على الدليل الموضوع فيه لذلك، والدليل الرقمي هو في العادة ملف يحتوي على بيانات رقمية تعطي مظهراً.

[1]) د. خالد ممدوح إبراهيم: فن التحقيق في الجرائم الإلكترونية، مرجع سابق، ص311

الخـاتمة

جريمة القذف والسب من الجرائم الماسة بالشرف والاعتبار، والتشريعات وضعت لها العقوبات الرادعة لحماية أعراض الناس ولحماية أمن واستقرار المجتمع، فقد جرمته وقررت عقوبات رادعة، وجريمة القذف والسب وفقاً لما استقر عليه القانون والفقه هي إسناد واقعة في مكان عام أو على مسمع أو مرأى من شخص آخر غير المجني عليه تستوجب عقاب من تنسب إليه أو تؤذي سمعته. وتقوم أركان جريمة القذف والسب قانوناً بتوافر ركنين أولهما: الركن المادي وهو يتكون من نشاط يتمثل في فعل أو قول يصدر من المتهم يسند فيه واقعة محددة وذلك بطريقة العلانية إلى المجني عليه، وثانيهما: الركن المعنوي أو القصد الجنائي والذي يتمثل في العلم والإرادة، وهو أن يعلم من تصدر منه الأقوال المؤثمة قانوناً شأنها أن تؤدي إلى إيذاء سمعة المجني عليه أو تعرضه للعقاب.

أولاً: النتـائج:

1- ظهور الفضـاء الإلكترونـي ووسـائل الاتصـالات الحديثـة كشـبكة الإنترنـت الذي استغله مرتكبو الجرائم الإلكترونية في تنفيذ جرائمهم، ومنها جرائم الاعتداء علـى الأشـخاص عبـر الشـبكة العنكبوتيـة، كانتهـاك حرمـة الحيـاة الخاصـة وجـرائم الاعتداء على العرض وجرائم السب والقذف.

2- أن الجرائم التي تمس السمعة (السب والقذف) بالوسائل الإلكترونية تقع من خلال نشر أو إرسال كتابات أو صور مسيئة من قبل شخص معين.

3- إن الهـدف مـن تجـريم السـب والقـذف هـي مساسـه بشـرف المجنـي عليـه واعتباره ويتخذ هذا المساس صورة سيئة فالإسناد موضوعه واقعة محددة مما يجعل تصديقها أقرب إلى الاحتمال، إذ يفترض تحديدها أن تكون لدى المتهم أدلة تثبتها.

4- إن الجرائم الماسة بالسمعة عبر شبكة الإنترنت لم تعد تقتصر على إقليم دولة واحدة، بل تجاوزت حدود الدول، وهي جرائم مبتكرة ومستحدثة، فالتقدم التقني وظهور تقنية المعلومات الحديثة والتطور الهائل والسريع في وسائطها وانتشارها بين أفراد المجتمع.

5- أهتم التشريع الإماراتي والتشريع المقارن بتجريم كافة صور الاعتداء على الأشـخاص عبـر الإنترنـت، وخاصـة جـرائم السـب والقـذف، حيـث أصـدر نصوصـاً قانونية عدة تكفل الحماية الجنائية للحاسب الآلي وشبكاته، وقد تباينت اتجاهات

الدول المختلفة في التعامل مع تلك الجرائم والعمل على خلق إطار قانوني لها يقوم على تصنيفها وضبطها ووضع العقوبات الرادعة اللازمة لحماية البشر من تأثيرها وحماية النشاطات بكافة أنواعها.

ثانياً: التوصيات:

1- ضرورة تعديل التشريعات الإماراتية ووضع نصوص خاصة بالجوانب الإجرائية (الضبط والتحقيق) للجرائم الإلكترونية.

2- ضرورة جعل قضاء متخصص للنظر في جرائم تقنية المعلومات وخاصةً الجرائم التي تتم عبر الشبكة العنكبوتية.

3- التأكيد على الجانب الوقائي من خلال تفعيل دور الأسرة والمدرسة ومنظمات المجتمع المدني لتوعية الشباب من عدم الانزلاق في بعض السلوكيات السيئة والتي تسيء للآخرين.

4- ضرورة تأهيل القائمين على إجراءات الضبط والتحقيق في الجرائم المعلوماتية وخاصةً تلك التي تتعلق بالشبكة العنكبوتية وذلك بإدخالهم دورات فنية متخصصة سواء داخل الدولة أو خارجها، وذلك لرفع كفاءتهم وقدراتهم في هذا المجال المهم.

5- ضرورة تشديد العقاب على مرتكبي هذه الجرائم لما تشكله من خطر جسيم وأثر ذلك على شرف واعتبار المجني عليهم.