United Arab Emirates University
Scholarworks@UAEU

Public Law Theses | Public Law

11-2018

جرائم الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات الإلكترونية (وفقا للمرسوم بقانون اتحادي رقم (5) لسنة 2102 في شأن مكافحة جرائم تقنية المعلومات وتعديلاته)

إبراهيم محمد القاسمي

Follow this and additional works at: https://scholarworks.uaeu.ac.ae/public_law_theses

Part of the Law Commons

Recommended Citation

محمد القاسمي, إبراهيم, "جرائم الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات الإلكترونية (وفقا للمرسوم بقانون اتحادي رقم (5) لسنة 2102 في شأن مكافحة جرائم تقنية المعلومات وتعديلاته)" (2018). *Public Law Theses*. 12.
https://scholarworks.uaeu.ac.ae/public_law_theses/12

This Thesis is brought to you for free and open access by the Public Law at Scholarworks@UAEU. It has been accepted for inclusion in Public Law Theses by an authorized administrator of Scholarworks@UAEU. For more information, please contact fadl.musa@uaeu.ac.ae.

جامعة الإمارات العربية المتحدة
United Arab Emirates University

UAEU

جامعة الإمارات العربية المتحدة

كلية القانون

قسم القانون العام

جرائم الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات الإلكترونية (وفقاً للمرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات وتعديلاته)

إبراهيم محمد القاسمي

أطروحة مقدمة لاستكمال متطلبات الحصول على درجة الماجستير في القانون العام

إشراف د. جهاد محمد عبدالعزيز

نوفمبر 2018

إقرار أصالة الأطروحة

أنا **إبراهيم محمد القاسمي** الموقع أدناه، طالب دراسات عليا في جامعة الإمارات العربية المتحدة ومقدم الأطروحة بعنوان **" *جرائم الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات الإلكترونية (وفقاً للمرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات وتعديلاته)* "**، أقر رسمياً بأن هذه الأطروحة هي العمل البحثي الأصلي الذي قمت بإعداده تحت إشراف **الدكتور جهاد محمد عبدالعزيز، أستاذ مشارك في كلية القانون**. وأقر أيضاً بأن هذه الأطروحة لم تقدم من قبل لنيل درجة علمية مماثلة من أي جامعة أخرى، علماً بأن كل المصادر العلمية التي استعنت بها في هذا البحث قد تم توثيقها والاستشهاد بها بالطريقة المتفق عليها. وأقر أيضاً بعدم وجود أي تعارض محتمل مع مصالح المؤسسة التي أعمل بها فيما يتعلق بإجراء البحث وجمع البيانات والتأليف وعرض نتائج و/أو نشر هذه الأطروحة.

توقيع الطالب: _____ التاريخ: 2018-12-12

حقوق النشر© 2018 إبراهيم محمد القاسمي
حقوق النشر محفوظة

إجازة أطروحة الماجستير

أجيزت أطروحة الماجستير من قبل أعضاء لجنة المناقشة المشار إليهم أدناه:

1) المشرف (رئيس اللجنة) : د/ جهاد محمد عبد العزيز

الدرجة : أستاذ مشارك

قسم القانون العام

كلية القانون – جامعة الإمارات العربية المتحدة

التوقيع: _____ التاريخ: ٢٠١٨/١١/٢٦

2) عضو داخلي : أ.د/ فتيحه محمد قواراي

الدرجة : أستاذ

قسم : القانون العام

كلية : القانون – جامعة الإمارات العربية المتحدة

التوقيع: _____ التاريخ : 2018/11/26

3) عضو خارجي : أ.د / علي محمود محمد حمودة

الدرجة : أستاذ

أكاديمية كلية شرطة دبي

التوقيع: _____ التاريخ: 2018/11/26

الملخص

يعالج هذا البحث جرائم الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات الإلكترونية وشروطها وعقوباتها وظروفها المشددة والتدابير التي تطبق على مرتكبيها، وتناول ذلك بالفكر والشرح القانوني والمراجع التي تم بذل جهداً كبيراً في جمعها وتصفحها والموائمة بين أفكار مؤلفيها، والاسترشاد بمنهجية البحث التي وضعت حتى لا تحيد عن المسار لتحقيق أهداف الدراسة والبحث

وفي هذه الدراسة تم توضيح البنيان القانوني لجرائم الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات الإلكترونية وذلك في الفصل الأول من البحث والذي تناول مبحثين، أولهما أركان جريمة الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات الإلكترونية في صورتها المجردة والتعريف بالموقع الإلكتروني ونظام المعلومات الإلكتروني وشبكة المعلومات ووسائل تقنية المعلومات، ثم جرائم الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات الإلكترونية في صورتها المجردة وأركانها المادية والمعنوية

وفي المبحث الثاني تناول البحث جريمة الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات الإلكترونية بقصد الحصول على بيانات حكومية أو معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية، ودراسة محل الجريمة وبيان معنى ومفهوم البيانات الحكومية، والمعلومات السرية الخاصة بمنشأة مالية أو تجارية أو اقتصادية، ثم استطرق الركن المادي للجريمة، والركن المعنوي للجريمة من خلال دراسة القصد الجنائي العام والقصد الجنائي الخاص الذي تتطلّبه الجريمة

أما الفصل الثاني من البحث فقد اشتمل على ثلاثة مباحث تناول فيها العقوبات والتدابير المقررة لجرائم الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات الإلكترونية، حيث بدأ المبحث الأول بالعقوبات البسيطة والظروف المشددة لجريمة الدخول غير المشروع إلى

النظام المعلوماتي، وقد استعرض من خلاله جريمة الإضرار بالبيانات أو المعلومات الشخصية والغير شخصية، وجريمة الدخول أو الإضرار بالبيانات بمناسبة أو بسبب تأدية العمل

وتناول المبحث الثاني العقوبات المقررة لجرائم الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات الإلكترونية بقصد الحصول على بيانات حكومية أو معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية، وتم شرح العقوبات البسيطة والظروف المشددة للعقوبة، ومن ثم التدرج في تشديد العقوبة على هذه الجريمة

وتناول المبحث الثالث التدابير المقررة لجرائم الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات الإلكترونية، وذلك من خلال دراسة التدابير المقيدة للحرية والتدابير السالبة للحقوق والتدابير المادية، التي أوردها المشرع في المرسوم اتحادي بقانون رقم (5) لسنة 2012 وتعديلاتها، مستهدياً ومسترشداً بنصوص قانون العقوبات الاتحادي رقم (3) لسنة 1987 وتعديلاته.

كلمات البحث الرئيسية: النظام المعلوماتي، جريمة، العقوبات.

العنوان والملخص باللغة الإنجليزية

Crimes of Illegal Access to Information System (According to the Federal Law No. (5) for the year 2012 regarding the combating of information technology crimes and its amendments)

Abstract

This research handles illegal access and illegal stay in electronic data processing system; its conditions, sanctions, intensive circumstances and actions taken against violators. The legal information found in many books and references was enlightened with huge effort to gather, read and comply the different information given. The research also has a certain identified study methodology to achieve its goals.

In this study, the legal basis of the crime of unauthorized access and illegal stay in electronic data processing system have been explained; (first chapter made of 2 sections) the first section contains: Basis of the crime of unauthorized access and illegal stay in electronic data processing system in its abstract image/ electronic website definition/ electronic information system/ information network/ information technology methods/ the crime of unauthorized access and illegal stay in electronic data processing system in its abstract image, moral and material basis

The second section includes the following: the crime of unauthorized access and illegal stay in electronic data processing system to get any official government data or private confidential information related to financial, commercial or economic state/ the study of crime location and government data clarification/ financial, commercial and economic related data clarification/ the crime moral and material basis through the study of general criminal aim together with personal criminal aim.

While the second chapter handles 3 sections related to sanction, action taken against violators of unauthorized access and illegal stay in electronic data processing system. The first section includes: simple sanctions and intensive circumstances related to information system illegal access/ the crime of data, personal-impersonal information violation at work environment.

The second section includes: sanction and penalties taken against unauthorized information system access and illegal stay in electronic data processing system to get official government data or private confidential information related to a financial, commercial or economic state/ simple sanctions and intensive circumstances for penalties/ grading of penalty severity.

The third section include: actions planned to be taken against unauthorized access to information system and illegal stay in electronic data processing system through the study of restricted freedom actions, rights deprived action and financial action stated legally in the (emirates federal decree number 5 for 2012 with its modifications). The emirates sanction federal decree number 3 for 1987 is enlightened with its modifications.

Keywords: Information system, Crime, Punishments.

شكر وتقدير

الحمد والشكر لله سبحانه وتعالى عدد خلقه ورضى نفسه وزنة عرشه ومداد كلماته على نعمائه التي لا تعد ولا تحصى، والحمد لله الذي أعانني على إتمام هذه الدراسة.

والشكر والعرفان للدكتور جهاد محمد عبدالعزيز على جهودة في الإشراف على هذه الدراسة.

والشكر أيضاً موصول إلى أساتذتي الكرام أعضاء هيئة التدريس في كلية القانون في جامعة الإمارات العربية المتحدة، الذين لن أنسى فضلهم على كل ما بذلوه وقدموه لي من معرفة ودعم.

وجزيل شكري لكل من كان له الفضل في تعليمي ومن ساهم وساعد بأي صورة في إتمام هذه الدراسة.

الإهداء

إلى والدتي جنتي فوق الأرض

إلى والدي مصدر فخري وإعتزازي

إلى زوجتي وأبنائي سر بهجتي وسعادتي

إلى إخواني وأخواتي سندي وعزوتي

قائمة المحتويات

العنوان i
إقرار أصالة الأطروحة ii
حقوق الملكية والنشر iii
إجازة أطروحة الماجستير iv
الملخص vi
العنوان والملخص باللغة الإنجليزية viii
شكر وتقدير x
الإهداء xi
قائمة المحتويات xii
المقدمة 1
الفصل الأول: البنيان القانوني لجرائم الدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات الإلكترونية 6
المبحث الأول: أركان جريمة الدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات الإلكترونية في صورتها المجردة 7
المطلب الأول: ركن المحل (الموقع الالكتروني، نظام معلومات الكتروني، شبكة معلومات أو وسيلة تقنية معلومات) 8
الفرع الأول: الموقع الالكتروني 13
الفرع الثاني: نظام المعلومات الإلكتروني 16
الفرع الثالث: الشبكة المعلوماتية 18
الفرع الرابع: وسائل تقنية المعلومات 20
المطلب الثاني: صور الركن المادي 21
الفرع الأول: الدخول إلى نظام المعالجة الآلية للمعطيات الإلكترونية بدون تصريح 23
الفرع الثاني: تجاوز حدود التصريح 29
الفرع الثالث: البقاء بصورة غير مشروعة 31
المطلب الثالث: الركن المعنوي 33

الفرع الأول: القصد الجنائي 35
الفرع الثاني: الخطأ غير العمدي 39

المبحث الثاني: جريمة الدخول بدون تصريح إلى نظام المعالجة الآلية للمعطيات الإلكترونية بقصد الحصول على بيانات حكومية أو معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية 40

المطلب الأول: محل الجريمة 42

الفرع الأول: البيانات الحكومية 43
الفرع الثاني: المعلومات السرية الخاصة بمنشأة مالية أو تجارية أو اقتصادية 45

المطلب الثاني: الركن المادي 49

الفرع الأول: فعل الدخول 50
الفرع الثاني: عدم وجود تصريح 54

المطلب الثالث: الركن المعنوي 56

الفرع الأول: القصد الجنائي العام 56
الفرع الثاني: القصد الجنائي الخاص 60

الفصل الثاني: العقوبات والتدابير المقررة لجرائم الدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات الإلكترونية 62

المبحث الأول: العقوبات المقررة لجريمة الدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات الإلكترونية 63

المطلب الأول: العقوبات البسيطة 65

الفرع الأول: العقوبات الأصلية 67
الفرع الثاني: العقوبات الفرعية 70
الفرع الثالث: عقوبة الشخص المعنوي 72

المطلب الثاني: الظروف المشددة للعقوبة 73

الفرع الأول: الإضرار بالبيانات أو المعلومات غير الشخصية 76
الفرع الثاني: الإضرار بالبيانات أو المعلومات الشخصية 81
الفرع الثالث: ارتكاب جريمة الدخول أو الإضرار بالبيانات بمناسبة أو بسبب تأدية العمل 85

المبحث الثاني: العقوبات المقررة لجريمة الدخول بدون تصريح إلى نظام المعالجة الآلية للمعطيات الإلكترونية بقصد الحصول على بيانات حكومية أو معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية 89

المطلب الأول: العقوبات البسيطة 92

الفرع الأول: عقوبة السجن المؤقت 93
الفرع الثاني: عقوبة الغرامة 94
الفرع الثالث: العقوبات الفرعية 95

المطلب الثاني: الظروف المشددة 97

الفرع الأول: أن يترتب على الدخول غير المشروع قصد الحصول على بيانات حكومية أو معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية 97
الفرع الثاني: العقوبة المشددة 99

المبحث الثالث: التدابير المقررة لجرائم الدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات الإلكترونية 103

المطلب الأول: التدابير المقيدة للحرية 105

الفرع الأول: وضع المحكوم عليه تحت الإشراف أو المراقبة 105
الفرع الثاني: إبعاد المحكوم عليه الأجنبي عن الدولة 107
الفرع الثالث: محو وإعدام المعلومات أو البيانات 109

المطلب الثاني: التدابير السالبة للحقوق والتدابير المادية 110

الفرع الأول: حرمان المحكوم عليه من استخدام أي شبكة معلوماتية أو نظام المعلومات الإلكتروني أو أي وسيلة تقنية معلومات أخرى 111
الفرع الثاني: وضع المحكوم عليه في مأوى علاجي أو مركز تأهيل..... 112
الفرع الثالث: إغلاق المحل أو الموقع 114

الخاتمة 116

المراجع 121

المقدمة

في إطار ما يشهده العالم من تطور سريع في مجال تكنولوجيا المعلومات والتحول إلى المجتمعات المعلوماتية تظهر على القمة جرائم مستحدثة عديدة منها جرائم تقنية المعلومات وقد واكب هذا التباين والتطور التقني ظهور العديد من صور ارتكاب هذه الجرائم ومن ضمنها موضوع هذه الدراسة والتي تتناول جرائم الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات الإلكترونية.

وقد أحدثت التقنيات الحديثة إيجابيات غيرت من أنماط الحياة في جميع المجتمعات وساهمت في نشر المعرفة والتواصل بين الأمم وشكلت سيل متدفق من المعلومات، الأمر الذي أدى إلى تطور المجتمع الإنساني ورقيه وازدهاره، إلاّ أن هناك وجه آخر لهذه التقنية الحديثة كان له أثراً سلبياً على حياة الناس ومصالح المجتمع وعلى الدول أيضاً وقد تمثل ذلك في الاستخدام الضار لهذه التقنية كما انها استخدمت في ارتكاب الجرائم.

ففي هذه البيئة الضخمة المزدحمة تضيق قبضة الأمن وتعجز أساليب المراقبة والتحكم التقليدية عن التعامل مع التحديات التي تترتب على هذه الجرائم، فضلاً عما تشكله من تهديد بالغ لسائر المنظمات الحكومية والخاصة والتي تعتمد أعمالها على الحاسبات وشبكات الاتصال إلى جانب صعوبة السيطرة على هذه الجرائم فإنه يصعب أيضاً اكتشاف هوية مرتكبيها.

وما زالت عمليات تطوير المواقع الالكترونية أو شبكة المعلومات أو وسيلة تقنية المعلومات متواصلة وأصبحت تتقدم من جيل إلى آخر وأصبح لا يخلو منزل أو مؤسسة من التكنولوجيا الحديثة وهو ما زاد من ارتكاب الجرائم ذات الصلة بتقنية المعلومات والانترنت ومنها جرائم الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات الإلكترونية بصورتها المجردة، أو المصحوبة بقصد خاص مثل الدخول بقصد الحصول على بيانات حكومية أو

معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية، وهذا النوع من الجرائم هو الموضوع الذي يتناوله هذا البحث.

وفي دولة الإمارات العربية المتحدة صدر القانون الاتحادي رقم (2) لسنة 2006م بشأن مكافحة جرائم تقنية المعلومات ، ومن ثم تبعه المرسوم اتحادي بقانون رقم (5) لسنة 2012م بشأن مكافحة جرائم تقنية المعلومات، الذي ألغى القانون السابق، وسعى من خلال نصوصه لمعالجة القصور وسد الثغرات في القانون السابق بتعديل عدد من المصطلحات، وملاحقة التطور الذي حدث في مجال استخدام تقنية المعلومات بإضافة عدد من جرائم المعلوماتية إلى القانون.

بالإضافة إلى ذلك وعقب دخول المرسوم اتحادي بقانون رقم (5) لسنة 2012 إلى حيز التنفيذ، ظهرت الحاجة لإجراء بعض التعديلات عليه، كان أولها في 23 مايو 2016 عندما صدر القانون اتحادي رقم (12) لسنة 2016 الذي عدّل المادة رقم (9) الخاصة بجريمة التحايل على العنوان البروتوكولي للإنترنت بقصد ارتكاب جريمة أو الحيلولة دون اكتشافها.

ثم تلى ذلك المرسوم بقانون رقم (2) لسنة 2018 الصادر في 24 يوليو 2018 والذي عدّل المادة رقم (26) الخاصة بجريمة تسهيل نشاطات الجماعات الإرهابية والجمعيات غير المشروعة والمادة رقم (28) الخاصة بجريمة تعريض أمن الدولة للخطر والمساس بالنظام العام، والمادة رقم (42) الخاصة بتدبير إبعاد الأجنبي عن الدولة عند الإدانة بجرائم تقنية المعلومات.

تتخذ جرائم الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات الإلكترونية صورتين، الصورة الأولى مجردة تتمثل في حالتين هي بسيطة ومشددة ويكون التشديد في الحالات التالية:

- إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أية بيانات أو معلومات.

- أن تكون هذه البيانات أو المعلومات شخصية.
- ارتكاب الجاني جرائم الاعتداء في صورتيها بمناسبة أو بسبب تأدية عمله.

أما الصورة الثانية من جرائم الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات الإلكترونية فتكون مصحوبة بقصد البقاء والحصول على معلومات وبيانات حكومية أو معلومات سرية خاصة بمنشأة مالية أو اقتصادية أو تجارية.

أهمية الموضوع:

تكمن أهمية هذا الموضوع في أنه يسعى للإحاطة بجرائم الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات الإلكترونية بكافة أنواعها، المجردة منها والمصحوبة بقصد خاص، ذلك في ظل انتشار وتعدد وتنوع وسائل تقنية المعلومات والاعتماد عليها من قبل الافراد والمؤسسات والحكومات في تسيير أعمالهم اليومية، ورواج استخدام وسائل التواصل الاجتماعي، وما ترتب على ذلك من اتساع وزيادة جرائم انتهاك الخصوصية والدخول غير المشروع إلى المواقع الالكترونية ووسائل تقنية المعلومات، والمخاطر التي تهدد البيانات الحكومية والمعلومات السرية للمؤسسات المالية والتجارية والاقتصادية.

الدراسات السابقة:

1- د. هدى حامد قشقوش - الاتلاف غير العمدي لبرامج وبيانات الحاسب الآلي - بحث مقدم لمؤتمر القانون والانترنت في الفترة من 1 – 3 مايو 2000 - الطبعة الثالثة 2004 - المجلد الثالث.

2- د. زكي زكي أمين حسونة - جرائم الكمبيوتر والجرائم الأخرى في مجال التكنيك المعلوماتي (القاهرة - دار النهضة العربية - سنة 1993).

3- د. راشد بشير أحمد - التحقيق الجنائي في جرائم تقنية المعلومات - دراسة تطبيقية على إمارة أبوظبي - مركز الإمارات للدراسات والبحوث الاستراتيجية – الطبعة الأولى أبوظبي.

4- ممدوح عبد الحميد - جرائم استخدام شبكة المعلومات العالمية (الجريمة عبر الانترنت) - الشارقة: دار الفتح للطباعة والنشر - الطبعة الأولى 2000.

5- محمد عبدالرحيم العلماء - جرائم الانترنت والاحتساب عليها - بحث مقدم إلى مؤتمر القانون والانترنت - كلية الشريعة والقانون جامعة الإمارات العربية المتحدة سنة 2000 - المجلد الثالث.

منهج الدراسة:

تعتمد الدراسة على المنهج الوصفي التحليلي، وتفسير النصوص القانونية التي تجرم الدخول غير المشروع إلى النظام المعلوماتي، ودراسة وتحليل الأحكام والقوانين ذات الصلة، والاستفادة من السوابق القضائية في ترسيخ المعنى القانوني.

مشكلة الدراسة:

تعتبر الجرائم المرتكبة عبر الانترنت من الموضوعات الحديثة في عصرنا الحالي وذلك للتطور المتجدد والمستمر للمعلوماتية، وفي المقابل كان لابد من مواكبة التطور التشريعي أيضاً، وتكمن مشكلة البحث في التعرف على مدى الحماية الجنائية التي يوفرها المرسوم اتحادي بقانون رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات للنظام المعلوماتي، وحماية محتويات النظام المعلوماتي من البيانات والمعلومات، لا سيما المعلومات والبيانات الحكومية، والمعلومات والبيانات السرية الخاصة بالمنشآت المالية والتجارية والاقتصادية، وذلك من خلال تقييم النصوص القانونية الواردة في شأن هذه الجرائم، والعقوبات والتدابير المقررة لهذه الجرائم، وما تشتمل عليه من عنصر الردع وتشديد العقوبة والتدرج في تشديدها.

لذا نسعى في هذه الدراسة إلى الإحاطة بجوانب هذا الموضوع الهام من خلال التعريف بالجريمة وجوانبها، وموقف المشرع الوطني منها تجريماً وعقاباً لها في كافة أشكالها، مع دراسة التدابير التي يتم توقيعها على مرتكب الجريمة، وذلك في فصلين.

نخصص الأول منهما لدراسة البنيان القانوني لجرائم الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات الإلكترونية، أما الفصل الثاني فنعالج فيه بالدراسة والتحليل العقوبات والتدابير التي توقع على مرتكبي هذه الجرائم وذلك على النحو الآتي:

الفصل الأول: البنيان القانوني لجرائم الدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات الإلكترونية

لما لهذه الجريمة من خطورة، جاءت أهمية النص على تجريمها والعقاب على ارتكابها، فنص عليها المشرع الوطني الإماراتي في المواد (2،3،4،5) من قانون مكافحة جرائم تقنية المعلومات لسنة 2012م[1]، كما نص عليها أيضاً قانون سنة 2006 الملغي.

مما سبق ولأهمية ما تحميه النصوص المجرمة للدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات الإلكترونية، فإننا سنتعرض لهذه الجريمة بالدراسة في مبحثين نخصص الأول لدراسة أركان جريمة الدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات الإلكترونية في صورتها المجردة، وذلك في ثلاثة مطالب نخصص الأول لدراسة ركن المحل والمطلب الثاني لدراسة صور الركن المادي للجريمة، والمطلب الثالث لدراسة الركن المعنوي للجريمة.

أما المبحث الثاني فنخصصه لجريمة الدخول بدون تصريح إلى نظام المعالجة الآلية للمعطيات الإلكترونية بقصد الحصول على بيانات حكومية أو معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية وذلك في ثلاث مطالب نتعرض في الأول بالدراسة لركن المحل ثم نخصص الثاني للركن المادي للجريمة، ثم نتناول في المطلب الثالث الركن المعنوي للجريمة وذلك على النحو الآتي:

المبحث الأول: أركان جريمة الدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات الإلكترونية في صورتها البسيطة والمشددة

المبحث الثاني: جريمة الدخول بدون تصريح إلى نظام المعالجة الآلية للمعطيات الإلكترونية بقصد الحصول على بيانات حكومية أو معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية

---

[1]- نص المشرع الفرنسي على هذه الجريمة في المادة (1/323) من القانون الفرنسي الحالي، والتي تقرر معاقبة كل من يصل أو يبقى بطريقة مخادعة في كل أو جزء من نظام المعالجة الآلية للمعطيات بالحبس لمدة سنتين والغرامة 30 ألف يورو، وتكون العقوبة الحبس ثلاث سنوات والغرامة 45 ألف يورو إذا ترتب على نشاط الجاني إلغاء أو تعديل البيانات الموجودة بالنظام أو تعديل تشغيل النظام.

المبحث الأول: أركان جريمة الدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات الإلكترونية في صورتها المجردة

لا يعتبر السلوك الإنساني سلوكاً غير مشروعاً، أو جريمة بالمعنى القانوني، إلاّ إذا توافرت فيه العناصر اللازمة لتحقق الجريمة، وهي أركان الجريمة، وهذه الأركان هي التي تحدد نطاق التجريم والعقاب، وأركان الجريمة قد تكون عامة تندرج تحت نطاقها جميع الجرائم دون استثناء، أو قد تكون هذه الأركان خاصة بجريمة معينة بذاتها تلازمها دون غيرها لتميزها عن بقية الجرائم[1].

الأصل أن كل جريمة تتكون من ركنين هما الركن المادي والركن المعنوي، والركن المادي للجريمة هو مظهرها الخارجي المتمثل بنشاط الفاعل الايجابي أو امتناعه عن النشاط أي الموقف السلبي وما يترتب على ذلك من نتيجة، وقيام علاقة السببية بين النشاط الإجرامي والنتيجة[2].

ويقصد بالركن المادي للجريمة وفقاً لما جاء في المادة (31) من قانون العقوبات الاتحادي رقم (3) لسنة 1987 لدولة الإمارات العربية المتحدة وتعديلاته (أي نشاط إجرامي بارتكاب فعل أو الامتناع عن فعل متى كان هذا الارتكاب أو الامتناع مجرم قانوناً)[3].

على ذلك المقتضى سار القانون الاتحادي رقم (5) لسنة 2012م بشأن مكافحة جرائم تقنية المعلومات، فنجد أن المادة (2) منه نصت على أن: (يعاقب بالحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تزيد على ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين كل من دخل موقع

---

[1]- د.أمير فرج يوسف – جرائم تقنية المعلومات بدول الخليج العربي – دار الكتب والدراسات العربية 2016 – ص 235.

[2]- د.رضا محمد عيسى – محاضرات في قانون العقوبات القسم العام 2015- منشورة في الرابط earch.Ksu.edu.sa/ar/search، راجع بنفس هذا المعنى د. هدى حامد قشقوش – شرح قانون العقوبات القسم العام – دار النهضة العربية 2010- ص114 حيث تشير إلى أن الركن المادي للجريمة يتكون من ثلاثة عناصر هي السلوك الإجرامي، النتيجة الإجرامية، ورابطة السببية.

[3]- تنص المادة (31) من قانون العقوبات الاتحادي رقم (3) لسنة 1987 لدولة الإمارات العربة المتحدة على: (يتكون الركن المادي للجريمة من نشاط إجرامي بارتكاب فعل أو الامتناع عن فعل متى كان هذا الارتكاب أو الامتناع مجرما قانوناً)

إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات، أو وسيلة تقنية معلومات، بدون تصريح أو بتجاوز حدود التصريح، أو بالبقاء فيه بصورة غير مشروعة)[1].

لذلك يعتبر عنصر الدخول هو الفعل المادي لهذه الجريمة، ويتحقق عنصر الدخول غير المشروع إلى النظام المعلوماتي، متى ما كان هذا الدخول بدون تصريح أو بتجاوز حدود التصريح، أو أن الشخص بقي في الموقع أو النظام أو الشبكة أو الوسيلة المعلوماتية بصورة غير مشروعة.

مما تقدم نلاحظ أن جريمة الدخول غير المشروع إلى النظام المعلوماتي جريمة ذات طبيعة خاصة، حدد لها المشرع محلاً لابد من توافره قبل تحقق أي من أركان الجريمة، وهو توافر النظام المعلوماتي، فجريمة الدخول غير المشروع لا يكون لها وجود مالم يتوافر لدينا نظام معلوماتي، لذا كان لابد لنا من دراسة ركن المحل قبل الولوج إلى أركان الجريمة المادية والمعنوية.

المطلب الأول: ركن المحل (الموقع الالكتروني، نظام معلومات الكتروني، شبكة معلومات أو وسيلة تقنية معلومات)

تنص المادة (2) من القانون الاتحادي رقم (5) لسنة 2012م بشأن مكافحة جرائم تقنية المعلومات على: يعاقب بالحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تزيد على ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين كل من دخل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات، أو وسيلة تقنية معلومات، بدون تصريح أو بتجاوز حدود التصريح، أو بالبقاء فيه بصورة غير مشروعة.

---

[1]- تنص المادة الثانية من القسم الأول من الفصل الثاني من معاهدة بودابست لسنة 2001 بشأن مكافحة جرائم الفضاء المعلوماتي وعنوانها جريمة النفاذ أو الولوج أو الدخول غير المشروع لمكافحة جرائم الفضاء المعلوماتي على أن " سوف يتبنى كل طرف تدابير تشريعية وغيرها من التدابير حيثما كان ذلك لازمًا لاعتبار الولوج إلى كل أو جزء من نظام حاسب دون وجه حق جريمة مؤثمة طبقًا لقانونه الداخلي إذا ما ارتكبت عمدًا وقد يتطلب الطرف الموقع أن تكون الفعلة المقترفة قد تمت بمخالفة تدابير الأمن وذلك بنية الحصول على بيانات حاسب أو لغاية أخرى غير شرعية أو تكون قد اقترفت نظرًا لصلة نظام الحاسب بنظام حاسب آخر.

وهذا النص مهم جداً في تحديد محل الجريمة، وهو وفقاً لما جاء في النص القانوني إما أن يكون موقعاً إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية معلومات يتطلب الدخول إليها تصريحاً أو إذناً من صاحبه.

إن جريمة الدخول غير المشروع إلى النظام المعلوماتي جريمة ذات طبيعة خاصة، حدد لها المشرع شرطاً مفترضاً أو محلاً لابد من توافره ليقع عليه السلوك الإجرامي[1] المكون لأركان الجريمة، هذا الشرط المفترض أو المحل هو أنه لابد من توافر نظام معلوماتي، سواءً كان هذا النظام المعلوماتي موقعاً الكترونياً أو أنظمة معلومات الكترونية أو شبكة معلومات أو أي وسيلة تقنية معلومات[2].

لذا فإن جريمة الدخول غير المشروع إلى النظام المعلوماتي تثير ما يعرف في المصطلح القانوني بالشرط المفترض، وهو شرط سابق لتحقق الركن المادي للجريمة، يفترض القانون توافره حتى يتحقق قيام الجريمة، على الرغم من أنه ليس من الأركان العامة للجريمة، إلاّ أنه ضروري لقيام الجريمة وهو بمثابة ركن خاص للجريمة[3]، قد يتعلق بمحل الجريمة مثل المال المنقول في جريمة السرقة[4]، وكما هو الحال في جريمة الدخول غير المشروع إلى النظام المعلوماتي موضوع دراستنا هذه.

---

[1]- يعرف السلوك الإجرامي بأنه هو ما يتخذه الجاني من نشاط إنساني إرادي له مظهر خارجي مادي لا بد من توفره لوقوع الجريمة سواء كان سلوكاً ايجابياً أم سلبياً، كما عرفته د.هدى حامد قشقوش– شرح قانون العقوبات القسم العام – مرجع سابق – ص 114 بأنه: (نشاط إنساني صدر عن إرادة تم التعبير عنها في المجال الخارجي سواء عن طريق فعل ايجابي أو مجرد الامتناع وهذا السلوك بمعناه السابق يتحقق سواء في الجرائم العمدية أو غير العمدية، وبالنظر إلى هذا السلوك يمكن تكييف الواقعة الإجرامية).

[2]- د.عبد الرازق الموافي عبد اللطيف – شرح قانون مكافحة جرائم تقنية المعلومات لدولة الامارات العربية المتحدة المرسوم اتحادي بقانون رقم 5 لسنة 2012 – الكتاب الاول – اصدارات معهد دبي القضائي– ص 17.

[3]- د.شيماء عطا الله – الشرط المفترض في الجريمة - محاضرات منشورة على موقع الدكتورة شيما - http://www.shaimaaatalla.com/

[4]- د. غنام محمد غنام - شرح قانون العقوبات الاتحادي لدولة الامارات العربية المتحدة – مطبوعات جامعة الامارات- 2003 – ص 94.

عرّف الفقه المصري الشرط المفترض بأنه[1]: (العنصرالذي يفترض قيامه وقت مباشرة الفاعل لنشاطه)[2]، أو هو (عنصر سابق على السلوك يلزم وجوده كي يثبت لهذا السلوك صفته الجرمية)[3]، أو هو: (حالة واقعية أو قانونية يحميها القانون)[4]، كما عرف آخرون الشرط المفترض بأنه: (نسيج من شروط أو عناصر قانونية أو أوضاع ايجابية أو سلبية تتعلق بموضوع الجريمة أو بالجاني بالمجني عليه)[5].

أما الفقه الايطالي فقد ذهب إلى تعريف الشرط المفترض للجريمة بأنه: عنصر أو ظرف ايجابي أو سلبي يسبق بالضرورة وجود الجريمة أو الواقعة، أو أنه عنصر أو مركز يسبق في وجوده قيام الجريمة – منطقياً وقانونياً – ويعد بمثابة الوسط الضروري لتوافر السلوك غير المشروع[6].

على ذلك فإن جريمة الدخول غير المشروع إلى النظام المعلوماتي، تعتبر جريمة ذات طبيعة خاصة، بسبب أنها لا تتحقق إلاّ بتوافر شرط خاص أو مفترض، هو محل الجريمة المتمثل في وجود الكيان المادي للنظام الآلي لمعالجة المعلومات، والمكونات المادية له من أجهزة وآلات ومعدات أو نظام معلوماتي أو موقع الكتروني أو غيره من وسائل تقنية المعلومات.

بالتالي فإن هذه الجريمة تقوم عندما ينصب السلوك الإجرامي على المحل المذكور وهو إما المواقع الالكترونية أو أنظمة المعلومات الالكترونية أو شبكة المعلومات أو وسيلة تقنية

---

[1]- أورد د.عبد العظيم مرسي وزير في صفحة 44 من مؤلفه الشروط المفترضة في الجريمة – أن الفقه الفرنسي اعتمد على أفكار الأستاذ (ڤوان) الذي يعد أول من أطلق ما يعرف بتعبير: (الشرط السابق الأولي)، وقد عرّف هذا الفقيه الشروط المفترضة بقوله أنها: (العناصر التي تحدد المجال الذي يمكن للجريمة أن ترتكب فيه)، وبالجملة يعرّف الفقه الفرنسي هذه الشروط بأنها: مراكز قانونية، أو واقعية سابقة على النشاط الإجرامي، فهي بمثابة نسيج خارج عن الجريمة نفسها، يُنظم الجاني فوقها نشاطه الإجرامي من دون أن ينفك عنه، أو هي مراكز محايدة في ذاتها تمثل نقطة البدء لارتكاب بعض الجرائم وتكون لازمة لوقوع الجريمة.

[2]- د. محمود محمد مصطفى - شرح قانون العقوبات القسم العام - دار النهضة العربية ط1 1983 - ص39.

[3]- د. مأمون سلامة– شرح قانون العقوبات القسم العام- ص101.

[4]- د. أحمد فتحي سرور- الوسيط في قانون العقوبات القسم العام ط6 - دار النهضة العربية القاهرة 1996 – ص 256 وما بعدها

[5]- د. عبد المهيمن بكر – شرح القسم الخاص في قانون العقوبات جرائم الاعتداء على الأشخاص والأموال ط7 – دار النهضة العربية القاهرة 1977 – ص 13. وفيه يصف الشرط المفترض بأنه وعاء النشاط الإجرامي، ويشبهه بالوعاء الذي يحيط الجنين كالجريمة من حيث تهيئة الشروط اللازمة لوجوده ومن حيث انه يوجد في زمن سابق على النشاط ويظل قائماً حتى تكتمل الجريمة.

[6]- د.عبد العظيم مرسي وزير- الشروط المفترضة في الجريمة - دار الجليل للطباعة مصر 1983 – ص 43.

معلومات، ولا يلزم أن يقع السلوك على كل صور المحل التي نص عليها المشرع، وإنما يكفي أن ينصب على إحداها فقط لقيام الجريمة[1].

مما سبق يجد الباحث أن جرائم الدخول غير المشروع إلى النظام المعلوماتي تثير ما يعرف فقهاً بالشرط المفترض للجريمة، إذ أن هذه الجريمة لا تتحقق ما لم يتوافر لدينا شرطاً خاصاً أو محلاً، حدد القانون توافره وقت مباشرة الفاعل لنشاطه الإجرامي، فإذا لم يتوافر هذا المحل فإن الجريمة لا تقع ولا يتحقق وقوعها.

يلاحظ أن هذا المحل أو الكيان المادي حددته المادة الثانية من القانون المذكور بأنه النظام الآلي لمعالجة المعلومات والمكونات المادية له من أجهزة وآلات ومعدات، أو هو المواقع الالكترونية أو أنظمة المعلومات الالكترونية أو شبكة المعلومات أو وسيلة تقنية معلومات، ولعل المشرع أراد بذلك فرض الحماية لوسائل التقنية الحديثة من اقتحامها والتطفل عليها، وعلى ما تضمنته من بيانات ومعلومات.

حدد المشرع الوطني محل جريمة الدخول غير المشروع إلى النظام المعلوماتي، عندما نص في المادة (2) من القانون الاتحادي رقم (5) لسنة 2012م بشأن مكافحة جرائم تقنية المعلومات على معاقبة كل من يدخل أو يبقى بصورة غير مشروعة أو بدون تصريح أو بتجاوز حدود التصريح في أي موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية معلومات.

وقد عرف المشرع الوطني في المادة (1) من المرسوم اتحادي بقانون رقم (5) لسنة 2012 معنى كلمة إلكتروني بأنها كل: ما يتصل بالتكنولوجيا الكهرومغناطيسية أو الكهروضوئية أو الرقمية أو مؤتمتة أو ضوئية أو ما شابه ذلك ، وكان القانون الملغي قد أغفل تعريف كلمة الكتروني، على الرغم من أن القانون رقم (1) لسنة 2006 في شأن التجارة والمعاملات

[1]- د.عبد الرازق الموافي عبد اللطيف – مرجع سابق – ص 18.

الالكترونية كان قد نص على تعريف معنى الكتروني بأنه كل: (ما يتصل بالتكنولوجيا الحديثة ويكون ذا قدرات كهربائية أو رقمية أو مغناطيسية أو لاسلكية أو بصرية أو كهرومغناطيسية أو مؤتمتة أو ضوئية أو ما شابه ذلك).

ويلاحظ أن تعريف قانون التجارة والمعاملات الالكترونية جاء أوسع من التعريف الذي أورده المرسوم اتحادي بقانون رقم (5) لسنة 2012 على الرغم من أنه صدر بعده بأكثر من سبع سنوات ويستشف من هذا التعريف أن المشرع أراد أن يخرج ما يتصل بالتكنولوجية اللاسلكية والبصرية من دائرة التجريم في هذا القانون.

فيما عرف قانون التجارة والمعاملات الالكترونية في المادة الأولى منه المعاملات الإلكترونية المؤتمتة الواردة ضمن التعريف الالكتروني بأنها المعاملات التي يتم إبرامها أو تنفيذها بشكل كلي أو جزئي بواسطة وسائل أو سجلات إلكترونية، والتي لا تكون فيها هذه الأعمال أو السجلات خاضعة لأية متابعة أو مراجعة من قبل شخص طبيعي.

نخلص من كل ذلك إلى أن المشرع الوطني حدد في المادة (2) من القانون الاتحادي رقم (5) لسنة 2012م بشأن مكافحة جرائم تقنية المعلومات ركن المحل لجريمة الدخول غير المشروع إلى النظام المعلوماتي وحصره في أي من العناصر الآتية:

1- الموقع الإلكتروني.
2- نظام المعلومات الإلكتروني.
3- شبكة المعلومات.
4- وسائل تقنية المعلومات.

وحتى تتضح معالم محل جريمة الدخول غير المشروع في النظام المعلوماتي في صورتها المجردة، كان لابد من معرفة المفهوم التقني لهذه العناصر، علماً بأن المادة (1) من القانون الاتحادي رقم (5) لسنة 2012م بشأن جرائم تقنية المعلومات تضمنت شرحاً لمعاني هذه العناصر

والكلمات والعبارات والمصطلحات التي اشتمل عليها القانون، وبناءً عليها نتناولها بالدراسة تباعاً على النحو الآتي:

الفرع الأول: الموقع الالكتروني

جاء تعريف الموقع الالكتروني في المادة (1) من القانون الاتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات، وذلك بأنه: مكان إتاحة المعلومات الالكترونية على الشبكة المعلوماتية ومنها مواقع التواصل الاجتماعي والصفحات الشخصية والمدونات[1].

وبذلك فإن جريمة الدخول غير المشروع تتوافر متى توافرت أركانها، وكان محل الجريمة موقعاً الكترونياً، بالمعنى الذي شرحه القانون، حيث يشتمل معنى الموقع الالكتروني على مواقع التواصل الاجتماعي[2] بمسمياتها المتعددة مثل: تويتر (Twitter) والفيسبوك (Facebook) والانستغرام (Instagram) والكيك (KeeK) والاسكايب (Skype) أو سناب شات (Snapchat) وغيرها من وسائل التواصل[3].

بالإضافة إلى الصفحات الشخصية والمدونات، يوجد على شبكة الانترنت عدد كبير من المواقع التي تقدم خدمات مجانية أو مدفوعة القيمة، مثل موقع (Google) الذي يقدم خدمة البحث على شبكة الإنترنت، أو موقع (Yahoo) الذي يقدم خدمة البريد المجاني وموقع (فور شير) الذي يقدم خدمة رفع الملفات على الإنترنت[4].

---

[1]- عرف المشرع السعودي في الفقرة التاسعة من المادة الأولى من نظام جرائم المعلوماتية لسنة 1428هـ الموقع الالكتروني بأنه مكان إتاحة البيانات على الشبكة المعلوماتية من خلال عنوان محدد، ويلاحظ الاختلاف في التعبير الذي استخدمه المشرع السعودي عن نظيره الإماراتي، حيث استخدم مشرعنا الوطني عبارة (إتاحة المعلومات)، بينما استخدم نظيره السعودي عبارة: (إتاحة البيانات).

[2]- لم يخص المشرع السعودي مواقع التواصل الاجتماعي بنص خاص يدخلها ضمن تعريف الموقع الالكتروني، إلاّ أنه وعلى الرغم من ذلك نلاحظ أنه خص جريمة الدخول غير المشروع باهتمام خاص، وذلك عندما قام بتعريف محل الجريمة وركنها المادي ضمن شرحه للمعاني والألفاظ التي يشتمل عليها القانون في الفقرة (7) من المادة الأولى، حيث عرف الدخول غير المشروع بأنه دخول شخص بطريقة متعمدة إلى حاسب آلي، أو موقع إلكتروني أو نظام معلوماتي، أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها.

[3]- كانت المادة الأولى من القانون الاتحادي (الملغي) تعرف الموقع الالكتروني بأنه (مكان إتاحة المعلومات على الشبكة المعلوماتية، دون أن يتضمن التعريف السابق مواقع التواصل الاجتماعي والصفحات الشخصية والمدونات).

[4]- مقال عن دور وسائل تقنية المعلومات منشور على https://support.google.com/adwords/answer/

ولقد عرف القانون الاتحادي رقم (5) لسنة 2012م الخاص بمكافحة جرائم تقنية المعلومات، قد عرف المعلومات في المادة الأولى منه بأنها: (أي معلومات يمكن تخزينها ومعالجتها وتوليدها ونقلها بوسائل تقنية المعلومات ، وبوجه خاص الكتابة والصور والصوت والأرقام والحروف والرموز والإشارات وغيرها)، وبالتالي فإن كل مكان داخل الشبكة الالكترونية، يكون متاحاً لحفظ البيانات يدخل ضمن المحل الذي تنطبق عليه أوصاف جريمة الدخول غير المشروع للنظام المعلوماتي.

من الناحية التقنية فإن تعريف الموقع الالكتروني يختلف على شبكة الإنترنت باختلاف الهدف منه[1]، فقد يكون الموقع مجموعة من الصفحات الثابتة التي تحتوى على معلومات عن المؤسسة أو الشركة ومقرها ونطاق نشاطها، والخدمات والمنتجات التي تقدمها، ومدى جودتها ووسائل الاتصال بالشركة.

فيكون الموقع بمثابة وسيلة إعلانية عن الشركة، وبشكل مستمر ودون انقطاع، كما يشكل الموقع الالكتروني الوسيلة الأفضل على الإطلاق لخدمة العملاء، والإجابة على استفساراتهم، ومن السهل أن يتم عبر الموقع الالكتروني بيع المنتجات والخدمات بشكل مباشر[2].

يلاحظ أن برنامج الواتساب (WhatsApp) وعلى الرغم من أنه يعتبر من وسائل التواصل الاجتماعي، إلاّ انه لا يدخل ضمن المعنى الذي يقصده القانون، وهو أن وسائل التواصل الاجتماعي هي وسائل تقنية المعلومات التي يتاح فيها للمستخدمين الآخرين الدخول على الشبكة وتبادل المعلومات.

وفي هذا السياق فقد قضت المحكمة الاتحادية العليا[3] بأن: (لما كان من المقرر قانونا أن جرائم السب الواردة في المادة 20 من المرسوم اتحادي بقانون رقم 5 لسنة 2012 بشأن مكافحة

---

[1]- منشور على موقع كنانة أونلاين على الرابط http://kenanaonline.com/users/MST/posts/
[2]- المرجع السابق.
[3]- الطعن رقم 248 لسنة 2018 جزائي.

جرائم تقنية المعلومات قد اشترط المشرع لقيامها وانطباق النص عليها أن يتم السب بواسطة شبكة المعلومات أو أيه وسيلة تقنية معلومات، وأن يتاح للمستخدمين الآخرين الدخول على الشبكة وتبادل المعلومات، إذ عرفت المادة الأولى من ذات القانون شبكة المعلومات بأنها ارتباط مجموعتين أو أكثر من البرامج المعلوماتية يتيح للمستخدمين الدخول وتبادل المعلومات، وعرفت وسيلة تقنية المعلومات بأنها " أية أداة مغناطيسية...).

يفهم من ذلك أن المشرع جعل من انتشار الجريمة عبر الفضاء الإلكتروني علة التجريم لخطورتها على المجتمع في حين أن جريمة السب الواردة في المادة 1/374 من قانون العقوبات هي جريمة تتم بواسطة الهاتف بين شخصين أو أكثر يحددهم المتصل ولا تخرج عن نطاق المتصلين ولا تسمح للآخرين الدخول وتبادل المعلومات.

ولما كان برنامج الواتساب من البرامج التي تستخدم بواسطة الهاتف حصرا وهو ارتباط بين شخصين أو أكثر يحدد المرسل، المرسل إليه دون أن يتاح للآخرين غير المعنيين بالإرسال الدخول على البرامج وتبادل المعلومات الواردة فيه شأنه في ذلك شأن الرسائل النصية ومن ثم فإن استخدام برنامج الواتساب في السب يندرج ضمن الجرائم الواردة بالمادة 1/374 من قانون العقوبات وتخرج من نطاق التجريم الوارد بالمادة 20 من المرسوم اتحادي بقانون سالفة الذكر[1].

لما كان ذلك وكان الحكم المطعون فيه إذ عدل وصف الواقعة المنسوبة إلى المطعون ضدها من تهمة السب باستخدام وسيلة تقنية المعلومات المنصوص عليها بالمادة 20 من المرسوم اتحادي بقانون رقم 5 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات إلى تهمة السب باستخدام الهاتف المعاقب عليها بالمادة 1/374 من قانون العقوبات فإنه يكون قد صادف صحيح الواقع والقانون ويغدو النعي الوارد بوجه هذا النعي على غير أساس خليقا برفض الطعن).

---

[1]- المرجع السابق

الفرع الثاني: نظام المعلومات الإلكتروني

نظام المعلومات عبارة عن آلية وإجراءات منظمة تسمح بتجميع وتصنيف وفرز البيانات (Data) ومعالجتها، ومن ثم تحويلها إلى معلومات يسترجعها الانسان عند الحاجة إليها، ليتمكن من إنجاز عمل أو اتخاذ قرار أو القيام بأية وظيفة، وقد يتم استرجاع المعلومات في نظام المعلومات يدوياً أو ميكانيكياً أو الكترونياً، وهذا هو الغالب في نظم المعلومات المعاصرة[1].

يقصد بنظام المعلوماتي الالكتروني كما عرفته المادة الأولى من القانون رقم (2) لسنة 2012 بشأن جرائم تقنية المعلومات، مجموعة برامج معلوماتية ووسائل تقنية المعلومات المعدة لمعالجة وإدارة وتخزين المعلومات الإلكترونية أو ما شابه ذلك[2].

ويلاحظ أن هذا التعريف اشتمل على مصطلحات تقنية تجعل فهمه في مجال التطبيقي العملي القانوني ليس بالأمر السهل، إذ لابد من فهم معنى المصطلحات التي اشتمل عليها مثل (مجموعة برامج معلوماتية) ومعرفة ماهية (وسائل تقنية المعلومات المعدة لمعالجة إدارة وتخزين المعلومات الالكترونية)[3].

نجد أن المشرع الوطني عرف في المادة الأولى من المرسوم بقانون رقم (5) لسنة 2012 البرنامج المعلوماتي بأنه: (مجموعة من البيانات والتعليمات والأوامر، القابلة للتنفيذ بوسائل تقنية المعلومات والمعدة لإنجاز مهمة معينة)، كما عرف المشرع في نفس المادة وسيلة تقنية المعلومات بأنها: (أي أداة إلكترونية مغناطيسية، بصرية، كهروكيميائية، أو أي أداة أخرى تستخدم لمعالجة البيانات الإلكترونية وأداء العمليات المنطقية والحسابية، أو الوظائف التخزينية،

---

[1]- د. خالد ممدوح ابراهيم – الجرائم المعلوماتية – دار الفكر الجامعي الاسكندرية 2009- ص 23.

[2]- جاء تعريف نظام المعلومات الالكترونية في المادة (1) من القانون رقم (1) لسنة 2006 في شأن التجارة والمعاملات الالكترونية بأنه: (مجموعة برامج وأجهزة معدة لمعالجة وإدارة البيانات والمعلومات لإنشاء أو استخراج أو إرسال أو استلام أو تخزين أو عرض الرسائل إلكترونيًا أو غير ذلك.)

[3]- عرفت معاهدة بودابست الدولية لسنة 2001 بشأن مكافحة جرائم الفضاء المعلوماتي النظام المعلوماتي بأنه (كل جهاز بمفرده أو مع غيره من الأجهزة من الآلات المتواصلة بينياً أو المتصلة، والتي يمكن أن يقوم واحد منها أو أكثر تنفيذاً لبرنامج معين بأداء المعالجة الالية للبيانات).

ويشمل أي وسيلة موصلة أو مرتبطة بشكل مباشر، تتيح لهذه الوسيلة تخزين المعلومات الإلكترونية أو إيصالها للآخرين).

وتعد المعلومات نتاجاً لمعالجة البيانات، وهي تختلف عن البيانات ذلك أن المعلومات عبارة عن نتاج معالجة البيانات داخل الحاسب الآلي، بينما البيانات عبارة عن مجموعة من الحقائق أو القياسات أو المعطيات التي تتمثل في شكل أرقام أو حروف أو رموز، تتعلق بفكرة أو بموضوع معين[1].

نلاحظ أن المشرع الوطني عرف في المادة الأولى من نفس القانون المعلومات الالكترونية بأنها أي معلومات[2]، يمكن تخزينها ومعالجتها وتوليدها ونقلها بوسائل تقنية المعلومات وبوجه خاص الكتابة والصور والصوت والأرقام والحروف والرموز والإشارات وغيرها[3].

ويعرف البعض المعلومات بأنها تعني البيانات المعالجة منطقياً ومنهجياً، باعتبارها سند للمعرفة الإنسانية[4]ويدخل ضمن هذه المعلومات المستندات الالكترونية[5]، والتي تعرض المشرع الوطني في المادة الأولى من المرسوم بقانون اتحادي رقم (5) لتعريفها بأنها: (سجل أو بيان

---

[1]- محمود أحمد عبابنة – جرائم الحاسوب وأبعادها الدولية – دار الثقافة للنشر والتوزيع – الاردن 2005 – ص 92.

[2]- كان قانون مكافحة جرائم تقنية المعلومات لسنة 2006 الملغي يعرف المعلومات بأنها: كل ما يمكن تخزينه ومعالجته وتوليده ونقله بوسائل تقنية المعلومات بوجه خاص الكتابة والصور والصوت والأرقام والحروف والرموز والإشارات وغيرها.

[3]- عرفت المادة (1) من القانون رقم (1) لسنة 2006 في شأن التجارة والمعاملات الالكترونية المعلومات بأنها: (بيانات ومعلومات ذات خصائص إلكترونية في شكل نصوص أو رموز أو أصوات أو رسوم أو صور أو برامج الحاسب الآلي أو غيرها)

[4]- د. على عادل إسماعيل – الجرائم الماسة بحقوق الملكية الفكرية الالكترونية – منشورات الحلبي 2017- ص 56.

[5]- تعرف المادة (1) من القانون الاتحادي رقم (1) لسنة 2006 في شأن المعاملات والتجارة الإلكترونية المستند الالكتروني بأنه: (سجل أو مستند يتم إنشاؤه أو تخزينه أو استخراجه أو نسخه أو إرساله أو إبلاغه أو استلامه بوسيلة إلكترونية، على وسيط ملموس أو على أي وسيط إلكتروني آخر، ويكون قابلاً للاسترجاع بشكل يمكن فهمه).

معلوماتي يتم إنشاؤه أو تخزينه أو استخراجه أو نسخه أو إرساله أو إبلاغه أو استلامه بوسيلة إلكترونية على وسيط)[1].

من التعريفات السابقة يمكن أن نعرف نظام المعلومات الالكتروني بأنه النظام الذي يستخدم لإنشاء رسائل بيانات أو إرسالها أو استلامها أو تخزينها أو لتجهيزها على أي وجه آخر، ويرتكز النظام المعلوماتي على ثلاثة أركان الأول هو: المدخلات (Input) وتتضمن البيانات المختلفة المرتكزة على قاعدتها بشكل غير منظم (Data).

الركن الثاني: المخرجات (Output) وهي نظم استدعاء هذه المعلومات في شكل منظم بحسب الحاجة إليها إذ تعطى ميزة الاخراج استدعاء معلومة محددة ومطلوبة فلا تظهر المعلومات كلها مرة واحدة.

الركن الثالث: فهو المعالجة الآلية للبيانات المدرجة في النظام بحيث تتقبل المعالجة الاستفهام أو الاستدعاء وتجيب عليه[2].

الفرع الثالث: الشبكة المعلوماتية

عرفت المادة الأولى من القانون الاتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات الشبكة المعلوماتية بأنها: ارتباط بين مجموعتين أو أكثر من البرامج المعلوماتية[3] ووسائل تقنية المعلومات التي تتيح للمستخدمين الدخول وتبادل المعلومات[4].

---

[1]- يتطابق تعريف المستند الإلكتروني في قانون المعاملات والتجارة الإلكترونية السابق الإشارة إليه مع التعريف الوارد في قانون مكافحة جرائم تقنية المعلومات لسنة 2006م (الملغي) تطابقاً تاماً من حيث الصياغة والمعنى، فيما اختلف كلا النصين عن التعريف الوارد في القانون رقم (5) لسنة 2012 من أن الأخير اعتبر أن السجل بيان معلوماتي، وأن استلامه يتم على وسيط دون أن يُذهب في شرح هذا الوسيط ودون أن يصف هذا الوسيط بأنه قابل للاسترجاع من عدمه.

[2]- د. عمر محمد أبو بكر بن يونس - الجرائم الناشئة عن استخدام الإنترنت – دار النهضة العربية – ص 336.

[3]- تعرف المادة (1) من المرسوم اتحادي الاتحادي بقانون رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات البرنامج المعلوماتي بأنه: مجموعة من البيانات والتعليمات والأوامر، القابلة للتنفيذ بوسائل تقنية المعلومات والمعدة لإنجاز مهمة معينة) وهو لا يختلف في مضمونه ومعناه عن التعريف الذي كان قد وضعه المشرع للبرنامج المعلوماتي في قانون مكافحة جرائم تقنية المعلومات لسنة 2006 الملغي، والذي كان يطابق التعريف الوارد في المادة (1) من القانون الاتحادي رقم (1) لسنة 2006م في شأن المعاملات والتجارة الإلكترونية والذي ينص على (أن البرنامج المعلوماتي هو مجموعة من البيانات والتعليمات والأوامر قابلة للتنفيذ بوسائل تقنية المعلومات ومعدة لإنجاز مهمة ما).

[4]- كانت المادة الأولى من القانون الاتحادي (الملغي) تعرف الشبكة المعلوماتية بأنها: (ارتباط بين أكثر من وسيلة لتقنية المعلومات للحصول على المعلومات وتبادلها)، ويلاحظ أن التعريف في القانون الحالي أوسع وأشمل وأدق من التعريف السابق).

بذلك فإن الشبكة المعلوماتية تختلف عن شبكة الاتصالات، من حيث أن الأخيرة هي عبارة عن شبكات تعمل على الربط بين أجهزة ووسائل الاتصال بهدف نقل أو بث خدمات الاتصالات[1]، أو تحويل أو استقبال الاتصالات السلكية واللاسلكية من خلال شبكة الاتصالات، أو لتمكين مستخدمي شبكة الاتصالات[2] من الاستفادة من خدمات الاتصالات.

تختلف أنواع شبكات المعلومات باختلاف الحيز الجغرافي الذي تعمل فيه، والمقصود بالحيز الجغرافي هو المساحة التي تغطيها الشبكة[3]، وتصنف الشبكة المعلوماتية على أساس حجمها إلى ثلاثة أنواع هي[4]:

أولاً: الشبكات المحلية: وهي شبكات صغيرة في موقع جغرافي واحد، ترتبط الأجهزة الموجودة في مساحة جغرافية صغيرة قد تكون داخل بناية واحدة أو طابق واحد بواسطة أسلاك.

ثانياً: الشبكات الواسعة: وهي شبكات متوسطة الحجم تمتد لمساحة أوسع من الشبكات المحلية قد يصل حجمها ما بين (40 – 80) كيلو متر.

ثالثاً: الشبكات الدولية: وهي شبكات تتجاوز مساحتها الدول، وتربط بين عدة شبكات مناطق مختلفة منتشرة بواسطة الخطوط السلكية واللاسلكية، وتعتبر شبكة الانترنت المثال النموذجي لها.

---

[1]- عرفت المادة (1) من المرسوم اتحادي بقانون اتحادي رقم (3) لسنة 2003 في شأن تنظيم قطاع الاتصالات المعدل بالمرسوم بقانون اتحادي رقم (5) لسنة 2008 شبكة الاتصالات بأنها: (منظومة تحتوي على جهاز أو وسيلة اتصال أو أكثر، بهدف نقل أو بث أو تحويل أو استقبال أي من خدمات الاتصالات، وذلك بواسطة أي طاقة كهربائية أو مغناطيسية أو إلكترومغناطيسية أو إلكتروكيميائية أو إلكتروميكانيكية وغير ذلك من وسائل الاتصال).

[2]- تعرف المادة (1) من قانون تنظيم قطاع الاتصالات المعدل أعلاه خدمات الاتصالات بأنها: (خدمة نقل أو بث أو تحويل أو استقبال من خلال شبكة الاتصالات لأي مما يأتي: 1- الاتصالات السلكية واللاسلكية. 2- الحديث والموسيقى وغيرها من الأصوات. 3- الصور المرئية. 4- الإشارات التي تستخدم في البث الإذاعي والتلفزيوني. 5- الإشارات المستخدمة في تشغيل والسيطرة على أية آلات أو أجهزة. 6- تركيب أو صيانة أو ضبط أو إصلاح أو تغيير أو نقل أو إزالة الأجهزة التي سيتم ربطها أو تكون مرتبطة بشبكة اتصالات عامة. 7- إنشاء وصيانة وتشغيل شبكات البرق والهاتف والتلكس والدوائر المؤجرة والمعطيات المحلية والدولية والإنترنت والإرسال اللاسلكي. 8- أية خدمات اتصالات أخرى يعتمدها مجلس الإدارة).

[3]- منشور على موقع موضوع كوم على الرابط http://mawdoo3.com/ .

[4]- د. محمد عزت فاضل ود. نوفل علي الصفو- جرائم تقنية المعلومات المخلة بالآداب العامة دراسة مقارنة – دار السنهوري بيروت 2017 – ص 22.

بذلك أصبحت الشبكات بنكاً زاخراً بالمعلومات من السهل أن يضعف مراقبتها والتحكم فيها، إذ تعد بيئة صالحة لعمليات التجسس على المعلومات الخاصة بالهيئات الحكومية والخاصة، وهذه المعلومات إذا ما تم الحصول عليها أو التجسس عليها، فقد يساء استخدامها سواءً من قوى داخلية أو خارجية معادية للدولة التي جمعت هذه المعلومات من شبكاتها[1].

الفرع الرابع: وسائل تقنية المعلومات

عرف المشرع الوطني في المادة الأولى من المرسوم اتحادي بقانون رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات وسيلة تقنية المعلومات بأنها أي أداة إلكترونية 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 الإلكترونية أو إيصالها للآخرين[2].

يدخل ضمن وسائل تقنية المعلومات كل ما يتصل بالتكنولوجيا الكهرومغناطيسية أو الكهروضوئية أو الرقمية أو مؤتمتة أو ضوئية أو ما شابه ذلك[3].

مما سبق نلاحظ أن المشرع الوطني قد أحاط بمعاني الكلمات والعبارات والمصطلحات التي تعرف النظام المعلوماتي بشكل واضح وجلي، وذلك من خلال المادة الأولى من المرسوم اتحادي بقانون رقم (5) لسنة 2012م، حيث اشتملت هذه المادة على التعريف بمعنى الموقع الالكتروني والشبكة المعلوماتية، ووسائل تقنية المعلومات.

---

[1]- عفيفي كامل عفيفي – جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون – منشورات الحلبي2007 – ص 325.

[2]- كان المشرع الوطني قد عرف وسيلة تقنية المعلومات في المادة (1) من القانون رقم (1) لسنة 2006 في شأن التجارة والمعاملات الالكترونية بأنها: (أداة الكترونية مغناطيسية، بصرية كهروكيميائية أو أية أداة أخرى تستخدم لمعالجة البيانات وأداء المنطق والحساب أو الوظائف التخزينية، ويشمل أية قدرة تخزين بيانات أو اتصالات تتعلق أو تعمل بالاقتران مع مثل هذه الأداة.

[3]- عرفت المادة (1) من المرسوم اتحادي بقانون رقم (5) لسنة 2012 النشاط الالكتروني بأنه: (ما يتصل بالتكنولوجيا الكهرومغناطيسية أو الكهروضوئية أو الرقمية أو مؤتمتة أو ضوئية أو ما شابه ذلك) .

وفي ذلك نشير إلى أن محكمة النقض بأبوظبي قضت بأنه " حيث أن الحكم المطعون فيه قد أدان المطعون ضده بجريمة الدخول إلى وسيلة تقنية المعلومات المملوكة لشركة.....بدون تصريح وأوقع عليه عقوبة الحبس لمدة شهرين وألغى تدبير الإبعاد المقضي به من محكمة أول درجة، لما كان ذلك وكانت المادة 42 من القانون رقم 5 لسنة 2012 مكافحة جرائم تقنية المعلومات قد أوجبت على المحكمة أن تقضي بإبعاد الأجنبي الذي يحكم عليه بالإدانه لارتكاب أي جريمة من الجرائم المنصوص عليها في هذا القانون بعد تنفيذ العقوبة المحكوم بها، لما كان ذلك وكان الحكم المطعون فيه قد أدان المطعون ضده وهو أجنبي باكستاني الجنسية بالحبس لمدة شهرين وألغى تدبير الابعاد فإنه يكون قد خالف القانون بما يوجب نقضه وتصحيحه بإضافة تدبير الابعاد"

المطلب الثاني: صور الركن المادي

تنص الفقرة الأولى من المادة الثانية من القانون الاتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات على: 1 - يعاقب بالحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تزيد على ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين كل من دخل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات، أو وسيلة تقنية معلومات، بدون تصريح أو بتجاوز حدود التصريح، أو بالبقاء فيه بصورة غير مشروعة .

باستقراء النص القانوني نجد أن الركن المادي لهذه الجريمة يتكون من نشاط إجرامي يتمثل في فعل الدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات، أي الدخول إلى موقع الكتروني أو نظام معلومات الكتروني أو شبكة معلومات أو وسيلة تقنية معلومات، إذ لا يجوز الدخول إلى النظام المعلوماتي إلاّ لمن كان مخولاً أو لديه تصريح بالدخول[1].

[1]-د. عبد الرازق الموافي عبد اللطيف – مرجع سابق – ص 16.

يتكون الركن المادي لجريمة الدخول غير المشروع إلى النظام المعلوماتي من عنصر واحد وهو السلوك الإجرامي، نظراً لكونها جريمة من جرائم الخطر لا الضرر وفقا لما انتهينا إليه سابقاً. والسلوك الإجرامي لهذه الجريمة والذي يتجسد في أحد أفعال ثلاثة هي[1]:

1- الدخول إلى النظام المعلوماتي بدون تصريح

2- تجاوز حدود التصريح

3- البقاء بصورة غير مشروعة في النظام المعلوماتي

تقوم هذه الجريمة بتحقق فعل الدخول إلى النظام المعلوماتي، ومدلول كلمة الدخول تشير إلى كل الأفعال التي تسمح بالولوج إلى نظام معلوماتي والإحاطة به أو السيطرة عليه وعلى المعطيات والمعلومات التي يتكون منها[2].

والجدير بالذكر أن فعل الدخول هنا لا يقصد به المعنى المادي للدخول، أي الدخول إلى مكان أو منزل أو حديقة، وفي نفس الاتجاه إلى جهاز الحاسب الآلي، وإنما ينظر إليه كظاهرة معنوية وهي ما تعرف بالدخول المعنوي الالكتروني[3]، أي الدخول إلى العمليات الذهنية التي يقوم بها نظام المعالجة الآلية للمعطيات[4]، أو أنه يعني الاتصال بالنظام المعلوماتي محل الحماية بالطرق الفنية اللازمة سواءً كان هذا الدخول باستخدام كارت ممغنط أو باستخدام أرقام سرية أو غيره[5].

---

[1]- المرجع السابق – ص 18.
[2]- نهلا عبد القادر المومني – الجرائم المعلوماتية – دار الثقافة 2008- ص 158.
[3]- المرجع السابق - ص 158.
[4]- د. عمر الفاروق- المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وابعادها الدولية – ط2-1995– ص 143
[5]- د.أيمن عبدالله فكري – جرائم نظم المعلومات دراسة مقارنة – دار الجامعة الجديدة الاسكندرية -2007 – ص 222

ويستوي أن يكون الدخول إلى النظام المعلوماتي باستخدام الوسائل الفنية أو التقنية، أو كان الدخول بصورة مباشرة إلى المعلومات أو تم عن طريق اعتراض غير مشروع لعمليات الاتصال من أجل الدخول إلى النظام المعلوماتي[1].

فعملية الدخول إلى النظام المعلوماتي قد لا تتطلب سوى تشغيل جهاز الحاسب الآلي، وفي بعض الأحيان يتطلب الدخول أموراً أكثر تعقيداً، كما هو الحال عندما يحاول الجاني الحصول على الرقم السري لدخول النظام المعلوماتي، كما قد يتم الدخول باستخدام برامج خبيثة يتم دمجها في أحد البرامج الأصلية لجهاز الحاسوب حيث تعمل كجزء منه وتقوم هذه البرامج بتسجيل الشفرات التي يستخدمها المستخدمون الشرعيون للدخول إلى النظام، واستعمالها بعد ذلك لاختراق النظام المعلوماتي[2].

بناء على ما تقدم نناقش الركن المادي لهذه الجريمة الدخول غير المشروع إلى النظام المعلوماتي في صورتها المجردة في ثلاث فروع وذلك على النحو الآتي:

الفرع الأول: الدخول إلى نظام المعالجة الآلية للمعطيات الإلكترونية بدون تصريح

جرّم المشرع الوطني مجرد الدخول إلى الموقع إلكتروني أو النظام المعلومات الإلكتروني أو شبكة المعلومات أو وسيلة تقنية معلومات، وهو ما سبق أن سميناه في المطلب السابق بمحل الجريمة، إلاّ أنه اشترط وحتى يكون الدخول مجرّماً أن يحدث دون تصريح.

---

[1]- نهلا عبد القادر المومني – مرجع سابق - ص 159.
[2]- المرجع السابق.

أولاً: مفهوم الدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات الإلكترونية

كما سبق وأن أشرنا فإن المشرع الوطني لم يعرف المقصود بفعل الدخول غير المشروع[1]، وإن كان يفهم من النص أن المقصود بفعل الدخول هو الوصول إلى المواقع الالكترونية أو أنظمة المعلومات الالكترونية أو شبكة المعلومات أو وسيلة تقنية المعلومات.

إذ أن مفهوم الدخول غير المشروع إلى النظام المعلوماتي يقوم على التواجد داخل أنظمة المعالجة الالية للمعطيات ضد ارادة من له حق السيطرة على النظام[2]، فالسيطرة على النظام قد تأخذ صورًا مختلفة منها اتيان الجاني أفعالاً من شأنها إخراج الحاسوب أو النظام المعلوماتي من حيازة مالكه وإدخاله في حيازته أو حيازة شخص آخر، واستخدامه دون موافقة مالكه أو حائزه القانوني[3].

إن مجرد الدخول إلى نظام الحاسب الآلي لا يشكل فعلاً غير مشروعاً، وإنما الذي يشكل الفعل غير المشروع هو عدم توافر المشروعية في دخول النظام الالكتروني وذلك لعدم الصلاحية[4]، بمعنى أن هذا الدخول يتم دون وجه حق، ويرتبط هذا المفهوم أساساً بمعرفة من له الحق أو السلطة في الدخول إلى النظام.

---

[1]- عرف نظام مكافحة الجرائم المعلوماتية السعودي الصادر بتاريخ 1428/3/8هـ بموجب المرسوم اتحادي الملكي رقم (17) في الفقرة (7) من المادة الأولى الدخول غير المشروع بأنه: دخول شخص بطريقة متعمدة إلى حاسب آلي، أو موقع إلكتروني أو نظام معلوماتي، أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول لها، كما عرف المشرع الكويتي الدخول غير المشروع في المادة الأولى من القانون رقم (63) لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات بأنه: (النفاذ المتعمد غير المشروع لأجهزة وأنظمة الحاسب الآلي أو لنظام معلوماتي أو شبكة معلوماتية أو موقع الكتروني من خلال اختراق وسائل وإجراءات الحماية لها بشكل جزئي أو كلي لأي غرض كان بدون تفويض في ذلك أو بالتجاوز للتفويض الممنوح).

[2]- د.علي عبد القادر القهوجي – الحماية الجنائية للبيانات المعالجة الكترونياً - بحث مقدم لمؤتمر القانون والكمبيوتر والانترنت الذي نظمته كلية الشريعة والقانون بجامعة الإمارات بالتعاون مع مركز الإمارات للدراسات والبحوث الاستراتيجية ومركز تقنية المعلومات بالجامعة – المجلد الأول – مايو 2000.

[3]- نهلا عبد القادر المومني – مرجع السابق – دار الثقافة 2008 - ص 97.

[4]- د.عمر محمد أبو بكر بن يونس – مرجع سابق – ص 331.

لذا فإن الدخول إلى نظام الحاسب الآلي يعد غير مصرح به في حالتين[1]، الأولى إذا كان هناك مسئول عن النظام، وكان الدخول إلى هذا النظام قد تم دون الحصول على تصريح منه إذ أن مجرد الدخول للشبكات أو الحاسبات أو النظام المعلوماتي بشكل عام بدون تصريح يشكل فعلاً غير مشروعاً يُعد جريمةً ولو لم يتحقق القيام بأي فعل آخر[2].

والثانية إذا كان دخول الفاعل إلى النظام قد تم في غير الحالات المرخص له فيها، بمعنى أن الفاعل لديه تصريح بالدخول إلاّ أنه تجاوز الصلاحيات الممنوحة له[3]، وهذا ما سنناقشه في الفرع الثاني والفرع الثالث.

ثانياً: المقصود بفعل الدخول إلى النظام

لم يحدد المشرع وسيلة الدخول أو الطريقة التي يتم الدخول بها إلى النظام، وإنما جاء النص في الفقرة الأولى من المادة الثانية من القانون الاتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات خالياً دون أن يحدد أي وسيلة أو شكل للفعل الإجرامي، لذلك تقع الجريمة بأي وسيلة أو طريقة.

يقصد بفعل الدخول الغير المشروع إلى النظام المعلوماتي، الاتصال بالنظام بأي طريقة كانت، دون تعليق ذلك على تطلب غرض ما من هذا الدخول، فقد يتم غالبا إما باستعمال أجهزة خاصة تمكنه من كسر شفرة قاعدة البيانات، أو بأن يستخدم الشفرة الصحيحة الخاصة بشخص آخر مأذون له بالدخول[4].

---

[1]- د. حسين بن سعيد الغافري – السياسة الجنائية في مواجهة جرائم الانترنت – دار النهضة العربية القاهرة 2009 – ص 348.

[2]- د.تركي بن محمد اليحيى - بحث مقدم للمؤتمر الدولي الرابع لمكافحة جرائم تقنية المعلومات المنعقد في أبو ظبي بدولة الإمارات العربية المتحدة بتاريخ 2011/12/14م

[3]- المرجع السابق – ص 349.

[4]- د. محمود أحمد طه - المواجهة التشريعية لجرائم الكمبيوتر والانترنت دراسة مقارنة - دار الفكر والقانون المنصورة – ص 26.

فقد يلجأ الجاني إلى التلاعب بعناصر النظام المادية لكي يصل إلى هدفه وهو الدخول أو يربطه بجهاز تنصت يستطيع من خلاله اختراق النظام أو استقبال المعلومات، كما قد يكون عن طريق برنامج فيروس مثل (فيروس حصان طروادة) أو عن طريق استخدام الرقم السري لشخص آخر أو الدخول من خلال شخص آخر مسموح له الدخول أو عن طريق الوصول إلى الرقم السري للدخول أو عن طريق تجاوز نظام الحماية الخاصة إذا كان ضعيفًا في حالة وجود مثل هذا النظام[1].

كما قد يكون الدخول غير مشروع إذا كان من له حق السيطرة على النظام قد وضع بعض القيود للدخول إلى النظام، إلاّ أن الجاني لم يحترم تلك القيود، وقام باستغلال خدمات البيانات استغلالاً غير صحيحاً ولأغراض غير مشروعة، ففي إحدى القضايا[2]، اتهمت النيابة العامة بدبي أحد الأشخاص بأنه استغل وأساء استخدام خدمات الإنترنت لأغراض غير مشروعة.

ذلك بأنه قام بتزويد حاسبه الآلي ببرنامج قرصنة تمكن من خلاله من كسر كلمات السر لموظفي مؤسسة الإمارات للاتصالات، والدخول إلى المواقع والأماكن الغير مصرح بها لمشتركي الشبكة، كما قام بنسخ بعض البيانات الخاصة بالكلمات السرية والمعلومات التي تحتويها رسائل البريد الإلكتروني لبعض موظفي المؤسسة.

يلاحظ أن هذه الواقعة حدثت قبل صدور قانون مكافحة جرائم تقنية المعلومات الاتحادي لسنة 2006 الملغي، لذا فإن محكمة أول درجة حكمت ببراءة المتهم لعدم وجود نص قانوني يجرم فض رسائل البريد الإلكتروني، وأن القاضي اعتبر مفهوم البريد الإلكتروني مغاير للرسائل العادية وأنه تحرز من القياس في مجال القانون الجنائي إعمالاً لمبدأ الشرعية الجنائية.

---

[1]- د. علي عبد القادر القهوجي – مرجع سابق - ص 11.

[2]- الطعن رقم 2001/230 جزاء محكمة تمييز دبي - نيابة دبي العامة، الندوة العلمية – مرجع سابق – ص 31.

إلاّ أن محكمة الاستئناف أدانت المتهم وأيدتها في ذلك محكمة تمييز دبي باستنادها للمادة رقم (380) من قانون العقوبات[1]، حيث اشتمل منطوق حكم محكمة تمييز دبي على أن: (المتهم اعترف باختراق شبكة الإنترنت الخاصة بمؤسسة الامارات للاتصالات مستخدماً برامج للبحث عن الثغرات تمكن من خلالها الحصول على كلمات السر الخاصة ببعض المواقع المحظورة على غير موظفي المؤسسة الدخول إليها، وقام بفك شفرة بعض الأجهزة ونسخ بعض الملفات وهو يعلم بحظر ذلك لغير موظفي المؤسسة المرخص لهم مما يشكل استغلالاً غير مشروعاً للشبكة يوقعه تحت طائلة العقاب)[2].

وبالإشارة أيضاً لحكم محكمة النقض بأبوظبي أنه "ولما كان ذلك وكان الثابت من مدونات الحكم المطعون فيه أن المطعون ضده.....هندي الجنسية فهو أجنبي عن الدولة وقد أدانته محكمة أول درجة بالحبس مدة أربعة أشهر والإبعاد وقد قضى الحكم المطعون فيه في استئنافه بتعديل الحكم المستأنف والاكتفاء بحبسه مدة شهر واحد ولم تتبعه الإبعاد، مما يفيد أنه أسقطه عنه وفق التعديل الذي أجراه على الحكم المستأنف. فيكون قد أخطأ في تطبيق القانون الواجب إعماله بما يوجب نقضه جزئياً وتصحيحه بإضافة عقوبة الإبعاد إلى العقوبة المقضي بها إذ العيب الذي شاب الحكم قاصر على الخطأ في تطبيق القانون[3].

ويلاحظ أنه يستوي أن يتم الدخول مباشرة أو بطريق غير مباشر، كما هو الحال في الدخول عن بعد عن طريق شبكات الاتصال سواءً كانت محلية أو عالمية، وتقع هذه الجريمة من كل إنسان أيًا كانت صفته، أي أنها ليست من الجرائم التي يطلق عليها جرائم ذوي الصفة مثل

---

[1] - تنص المادة (380) من قانون العقوبات على أنه " يعاقب بالغرامة التي لا تقل عن ثلاثة آلاف درهم من فض رسالة أو برقية بغير رضاء من أرسلت إليه أو استرق السمع في مكالمة هاتفية ويعاقب الجاني بالحبس مدة لا تقل عن ثلاثة أشهر أو بالغرامة التي لا تقل عن خمسة آلاف درهم إذا أفشى الرسالة أو البرقية أو المكالمة لغير من وجهت إليه ودون إذنه متى كان من شأن ذلك الضرر بالغير"

[2]- الطعن رقم 2001/230 جزاء محكمة تمييز دبي - نيابة دبي العامة، الندوة العلمية – مرجع سابق – ص 32.

[3]- الطعن رقم 769 لسنة 2010 س4 ق.أ- جزائي

الرشوة أو الاختلاس أو الزنا، وإنما ترتكب من أي شخص سواء كان يعمل في مجال الأنظمة أو لا يعمل[1].

وسواءً كان يفهم أم لا يفهم أسلوب تشغيل النظام، وسواء كان يستطيع أن يستفيد من الدخول أم لا، فيكفي أن يكون الجاني ليس ممن يكون لهم الحق في الدخول إلى النظام أو من الذين ليس لهم الحق في الدخول بالطريقة التي دخلوا بها، فتتوافر الجريمة في كل حالة يكون فيها الدخول مخالفًا لشروط الدخول التي نص عليها القانون أو الاتفاق أو مخالفًا لإرادة من له حق السيطرة على النظام.

في ضوء ما سبق يمكن القول أن جريمة الدخول غير المشروع إلى النظام المعلوماتي تعتبر جريمة خطر وليست جريمة ضرر[2]، إذ لا يشترط أن يترتب على الدخول أي نتيجة، مثل حدوث ضرر للشبكة أو البيانات أو حدوث فائدة للجاني[3]، بمعنى أن جريمة الدخول غير المشروع إلى النظام المعلوماتي تُعد جريمةً تامةً بمجرد ارتكاب النشاط الإجرامي، وهو التداخل عمداً في النظام المعلوماتي دون موافقة صاحبه، حتى وإن لم يجد الجاني في الملفات ما يبحث عنه من معلومات أو بيانات[4]، إذ أن دخول الجاني للموقع أو النظام أو الشبكة أو وسيلة تقنية المعلومات دون أن يكون لديه تصريح بالدخول يُعد انتهاكاً أو اختراقاً لقواعد خصوصية وسائل تقنية المعلومات[5].

---

[1]- د.علي عبد القادر القهوجي – مرجع سابق ص 33.

[2]- أورد د. غنام محمد غنام في صفحة 119 من مؤلفه شرح قانون العقوبات الاتحادي – مرجع سابق – أنه يمكن تقسيم الجرائم من حيث الركن المادي إلى عدة أقسام، وأن أهم هذه التقسيمات هو تقسيمها إلى جرائم خطر وجرائم ضرر، وأن الجرائم التي تسمى بجرائم الخطر جرائم النشاط، وهي التي لا يلزم لوقوعها حدوث نتيجة معينة، وإنما تقع بمجرد حدوث النشاط الاجرامي الذي يتضمن اعتداءً على مصلحة قانونية لذا تعتبر من الجرائم الشكلية، أما جرائم الضرر فيقصد بها الجرائم التي يتطلب لوقوعها حدوث نتيجة مادية معينة، لذا فهي تسمى ايضاً بالجرائم المادية ومنها على سبيل المثال جريمة القتل التي لا تقع إلاّ إذا ترتب على الفعل الاجرامي نتيجة مادية وهي أُزهاق روح المجني عليه.

[3]- د. أحمد حسام طه تمام – جرائم الحاسب الآلي – دار النهضة العربية القاهرة ط1 سنة 2000 – ص 304.

[4]-د. عمر الفاروق- مرجع سابق – ص 123

[5]- المستشار علاء فكري اباظة – جرائم تقنية المعلومات دراسة تحليلية للمرسوم بقانون اتحادي رقم (5) لسنة 2012 – منشورات دائرة القضاء ابوظبي 2014 – ص40.

الفرع الثاني: تجاوز حدود التصريح

سبق وأن أوضحنا أن الفقرة الأولى من المادة الثانية من المرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات تنص على أن: 1- يعاقب بالحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تزيد على ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين كل من دخل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات، أو وسيلة تقنية معلومات، بدون تصريح أو بتجاوز حدود التصريح، أو بالبقاء فيه بصورة غير مشروعة .

وكما شكّل الدخول بدون تصريح أو إذن جريمةً يُعاقِب عليها القانون، فقد قررت الفقرة السابقة أيضاً مُعاقبة الشخص الذي تجاوز حدود هذا التصريح، بمعنى أن الجاني في هذه الحالة هو شخص يملك ترخيصاً أو إذناً مسبقاً للدخول إلى النظام المعلوماتي ولكنه تجاوز حدود هذا الإذن، وهذا الإذن أو التصريح قد يكون محدداً من حيث مدته أو زمانه أو نطاق المعلومات الجائز الاطلاع عليها[1].

فإذا تجاوز من صدر له التصريح نطاق المعلومات المصرح له بها أو قام الشخص بتجاوز الحدود الزمنية المحددة له بأن قام بالدخول في غير المواعيد المحددة في التصريح أو

[1]- على سبيل المثال ومن خلال عملي في القيادة العامة لشرطة أبو ظبي فقد لاحظت الأهمية العظيمة للنظام الإلكتروني الذي تعمل عليه وزارة الداخلية في دولة الإمارات العربية المتحدة والذي يعرف باسم (نظم المعلومات الجنائية)، والذي يشكل ثروة قومية وقوة معلوماتية متميزة حيث يجمع هذا النظام في معينه جميع مراكز الشرطة في الدولة والمنافذ الجوية والبرية والسجون والجوازات والجنسية، ويتم من خلال هذا النظام المعلوماتي فتح البلاغات وإجراء التحقيقات، كما يشتمل النظام على جميع الإجراءات التي يتم اتخاذها في إدارات الجوازات والإقامة المتعلقة بإصدار جوازات سفر المواطنين وإصدار تأشيرات وأذونات الدخول للوافدين إلى الدولة بغرض العمل والسياحة، وإدراج حركات الدخول والخروج في المنافذ الجوية والبرية والبحرية، وكذلك جميع الإجراءات الخاصة بالموقوفين والمحبوسين والسجناء لدى المراكز وإدارات المنشآت العقابية والإصلاحية منذ دخول النزيل وحتى الإفراج عنه وغيرها من الاجراءات والبيانات والمعلومات.
ويمنح العامل في وزارة الداخلية صلاحية للعمل في هذا النظام، وهي صلاحيات محددة بحسب العمل المناط بالشخص القيام به، فلا يسمح للموظف أن يتجاوزها، ويكون دخول الموظف للنظام بواسطة (كلمة السر) تسمح له بالدخول إلى النظام ليباشر مهامه حسب الصلاحية المحددة له، وهو دخول مباح وفقاً لتصريح يمنح للموظف بناء على طبيعة عمله، إلاّ أنه إذا تجاوز الموظف حدود التصريح الممنوح، بأن دخل إلى حقول غير مصرح له الدخول فيها، او دخل إلى الحقول التي لا تسمح حدود واجبات وظيفته بالاطلاع عليها أو العمل فيها، فإنه يكون قد ارتكب فعلاً مجرما وهو تجاوز حدود التصريح الممنوح له.

تجاوز المدة المحددة للدخول في التصريح فإنه يكون قد تجاوز الحدود المصرح له بها ويكون قد ارتكب الجريمة في صورتها الثانية[1].

ويلاحظ أنه يمكن التمييز بين طائفتين من الجناة يمكن أن تنطبق عليهما صفة تجاوز حدود إذن التصريح بالدخول إلى النظام المعلوماتي، الطائفة الأولى هم: الأشخاص من داخل المؤسسة المسئولة عن النظام المعلوماتي (The Insiders) وأشخاص من خارج المؤسسة التي يوجد بها النظام (The Outsiders)، وهؤلاء يدخلون إلى النظام إما مباشرةً أو عن طريق اعتراض هذا النظام[2].

بالنسبة إلى الدخول غير المشروع إلى النظام والذي يتم من قبل الفئة الثانية فلا يوجد ثمة مشكلة، وإنما المشكلة تثور في حالة لو تم الدخول من قبل الطائفة الأولى وهم العاملون بالمؤسسة التي يوجد بها النظام ففي هذه الحالة يتجاوز العامل السلطة الممنوحة له، ويصعب في كثير من الأحيان معرفة عما إذا كان التجاوز قد تم عمداً أو عن طريق الخطأ[3].

مما سبق نجد أن تجاوز حدود التصريح كما ينطبق على الأشخاص من خارج المؤسسة، فإنه أيضاً ينطبق على الأشخاص الذين يعملون داخل المؤسسة المسئولة عن النظام المعلوماتي، أي أن الجاني في هذه الجريمة قد يكون في الأصل أحد موظفي أو عمال الجهة صاحبه النظام المعلوماتي، وهو في الأصل لديه صلاحية أو تصريح في الدخول إلى النظام المعلوماتي، ولكنه تجاوز حدود التصريح.

ويختلف الفعل المكون لهذا الجريمة، أي أن تجاوز التصريح الممنوح للجاني يختلف بحسب طبيعة عمله، فقد يكون الفعل المادي في هذه الجريمة هو الاطِّلاع على البيانات أو المعلومات من غير إذن عام أو خاص، أو من دون مسوغ نظامي صحيح، سواءً كان هذا الاطلاع

---

[1]- أ.د. إمام حسنين خليل عطا الله – الحماية الجنائية لوسائل تقنية المعلومات في التشريعات العربية – مركز الدراسات والاستطلاعات وزارة الداخلية دولة الامارات العربية المتحدة – سنة 2016 – 58.

[2]- د. محمود أحمد طه – مرجع سابق – ص 27.

[3]- المرجع السابق – ص 27.

من خلال الدخول غير المشروع لقواعد البيانات أو الأجهزة الحاسوبية، أو من خلال اعتراض البيانات المرسلة أو الحصول عليها أو مشاهدتها بأي وسيلة أخرى[1].

ويخرج من وصف هذه الجريمة ما كان مأذوناً فيه للشخص بالاطلاع عليه من البيانات أو المعلومات، مثل الموظف الذي يعمل في حدود صلاحياته الوظيفية، أو من يعملون ضمن شبكة معلومات واحدة لا تمنع أصحابها من اطلاع بعضهم على بعض، وتثور الجريمة متى تعدى هذا الموظف حدود التصريح أو الصلاحية الممنوحة له[2].

الفرع الثالث: البقاء بصورة غير مشروعة

يقصد بالبقاء الغير مشروع التواجد داخل النظام المعلوماتي دون وجه حق أو تصريح ممن له الحق في السيطرة التامة على هذا النظام[3]، وضد إرادته وقد يتحقق البقاء المعاقب عليه مقترناً مع الدخول غير المشروع، وهذا يعني أن البقاء في الموقع يسبقه بالضرورة دخول إلى الموقع الالكتروني وهي الصورة الأولى من الجريمة، حيث تقوم بها الجريمة سواء استمر الدخول أو لم يستمر أي سواء بقي الجاني أم لم يبقى في النظام[4]، كما قد يتحقق البقاء مستقلاً عنه، ويكون البقاء في النظام معاقباً عليه استقلالاً حين يكون الدخول إلى النظام مشروعاً[5].

حرص المشرع الوطني على تجريم هذه الصورة من الفعل الإجرامي، وذلك بأن نصت الفقرة الأولى من المادة الثانية من المرسوم بقانون اتحادي رقم (5) لسنة 2012 على تجريم هذا الفعل بعبارة (.....، أو بالبقاء فيه بصورة غير مشروعة).

يتضح من خلال نص الفقرة السابق الإشارة إليها أن الصورة البسيطة للجريمة تتمثل في مجرد الدخول من غير تصريح أو تجاوز التصريح الممنوح للدخول، أما الصورة الثالثة لجريمة

---

[1]- د. تركي بن محمد اليحيى – مرجع سابق – ص 10.
[2]- المرجع السابق.
[3]- د. علي عبد القادر القهوجي – مرجع سابق ص 55.
[4]- أ.د. إمام حسنين خليل عطا الله – مرجع سابق - ص 59.
[5]- د. سعيدي سليمة، الأستاذ حجاز بلال – جرائم المعلومات والشبكات في العصر الرقمي – دار الفكر الجامعي الاسكندرية 2017 - ص 149.

الدخول غير المشروع في شقها المجرد فتتمثل في البقاء غير المشروع في النظام المعلوماتي، حيث تقع الجريمة سواءً تم البقاء في النظام كله أو في جزء منه فقط، أي أنه يكفي لتوافر جريمة الدخول غير المشروع في صورتها الثالثة أن يبقى الجاني في بعض عناصر النظام أو في عنصر واحد منه أو منطقة ضيقة منه.

ويلاحظ أنه قد يتحقق الركن المادي للجريمة في صورته الثالثة التي يعاقب عليها القانون، وهي البقاء داخل النظام بشكل مستقل عن الدخول إلى النظام، كما أنهما قد يجتمعان سوياً، علماً بأن البقاء في النظام بصورة غير مشروعة يعاقب عليه القانون بصورة مستقلة عن فعل الدخول خاصة عندما يكون الدخول إلى النظام مشروعاً، ويتحقق ذلك الأمر في حالتين[1]:

الأولى: إذا تم الدخول إلى النظام بمصادفة أو عن طريق الخطأ أو السهو، وفي هذه الحالة يجب على المتدخل أن يقطع وجوده وينسحب فوراً، فإذا بقى رغم ذلك فانه يعاقب على جريمة البقاء غير المشروع متى تبث في حقه تعمده البقاء.

الثانية: إذا تجاوز المتدخل المدة المسموح بها للبقاء بداخل النظام، أو حصل المتدخل بصورة مشروعة على الخدمة مدة أطول من المدة التي دفع مقابلتها نتيجة استخدام وسائل أو عمليات غير مشروعة.

وقد يجتمع الدخول غير المشروع والبقاء غير المشروع معاً، وذلك في الفرض الذي لا يكون فيه للجاني الحق في الدخول إلى النظام، ويدخل إليه فعلاً ضد إرادة من له حق السيطرة عليه، ثم يبقى بعد ذلك داخل النظام، وإن كانت جريمة البقاء غير المشروع في النظام – من الناحية العملية - لا تقع من الفاعل في جريمة الدخول غير المشروع إلى النظام المعلوماتي[2].

---

[1]- د. محمود أحمد طه – مرجع سابق - ص 31.
[2]- د.عمر الفاروق- مرجع سابق – ص 123

ذلك أن تجريم فعل البقاء يأتي من قبيل النص الاحتياطي بالنسبة لتجريم الدخول غير المشروع، فلا تنسب جريمة البقاء الغير المشروع في النظام إلى الشخص الذي قام بالدخول غير المشروع، شأنها في ذلك شأن جريمة إخفاء الأشياء المسروقة فهي لا تقع من مرتكب جريمة السرقة[1]، إذا ضبطت عنده المسروقات، بينما جريمة إخفاء الأشياء المسروقة تقع من شخص آخر لم يساهم في جريمة السرقة.

المطلب الثالث: الركن المعنوي

يعرف الركن المعنوي للجريمة بأنه إرادة إجرامية تستمد صفتها الإجرامية من اتجاهها إلى ماديات غير مشروعة تقوم عليها الجريمة ويحدد القانون صور هذا الاتجاه وكيفيته[2]، وتتكون الإرادة من عنصرين: الأول هو إرادة النشاط إذ يلزم أن يكون الجاني مريداً تحقيق النشاط الذي نسب إليه، أما العنصر الثاني فهو إرادة النتيجة أي أن إرادة الجاني اتجهت إلى تحقيق النتيجة، ويعتبر عنصر إرادة النتيجة عنصراً هاماً، فهو الذي يفرق به بين الجرائم العمدية والجرائم الغير عمدية[3].

كما يُعرف الركن المعنوي بأنه العزم ونية الفاعل لارتكاب الجريمة وتحقيق نتيجتها[4]، ويشترط توافره سواءً في الجريمة التامة أو الشروع، فإذا ثبت أن الفاعل لم يقصد تحقيق نتيجة الفعل، وإنما قصد الوقوف عند مرحله الشروع دون إتمام الجريمة فيسأل عن الشروع، وبالتالي لا يسأل عن جريمة تامة بل يسأل في حدود الأفعال التي صدرت منه إذا شكلت جريمة[5].

---

[1]- د. محمود أحمد طه – مرجع سابق - ص 32.

[2]- د. محمود نجيب حسني - شرح قانون العقوبات القسم العام النظرية العامة للجريمة والنظرية العامة للعقوبة والتدبير الاحترازي– دار النهضة العربية القاهرة 1977 – ص 599.

[3]- د.غنام محمد غنام - شرح قانون العقوبات الاتحادي لدولة الإمارات العربية المتحدة - الناشر جامعة الإمارات 2003 – ص 169.

[4]-د. رضا محمد عيسى – مرجع سابق – ص 53.

[5]-المرجع السابق - ص 54.

ووفقاً للمادة (38) من قانون العقوبات الاتحادي الإماراتي لسنة 1987 فإن الركن المعنوي للجريمة يتكون من العمد أو الخطأ، ويتوافر العمد بحسب اتجاه إرادة الجاني إلى ارتكاب الفعل أو الامتناع عنه بقصد إحداث نتيجة مباشرة أو أية نتيجةٍ أخرى مجرمةً قانوناً يكون الجاني قد توقعها، متى ما كان هذا الارتكاب أو الامتناع مجرماً قانوناً، أما الخطأ فهو يتوفر إذا وقعت النتيجة الإجرامية بسبب خطأ الفاعل سواءً كان هذا الخطأ إهمالاً أم عدم انتباه أم عدم احتياط أو طيشا أو رعونة أم عدم مراعاة القوانين أو اللوائح أو الأنظمة أو الأوامر.

نستنتج من هذا التعريف أن الركن المعنوي يتكون إما من قصد جنائي أو خطأ غير عمدي، وأن ما يحدد طبيعة الركن المعنوي هو نوعية خطأ الجاني وهل كان يقصد إتيان الفعل أم أن الفعل صدر عنه على سبيل الخطأ غير العمدي[1]، وبذلك فإن الجرائم تنقسم استناداً إلى ركنها المعنوي أي بحسب القصد الجنائي إلى قسمين[2].

الأول: هي الجرائم العمدية، وهي التي يتعمد الجاني فيها إتيان الفعل المحرّم وهو عالم بذلك، فلا يتحقق ركنها المعنوي إلاّ بتوفر القصد أي اتجاه إرادة الفاعل إلى القيام بالفعل المكون للجريمة بهدف تحقيق النتيجة الجرمية التي يريدها[3].

أما الثاني: فهي الجرائم غير العمدية أو ما يعرف بجرائم الخطأ غير العمدي[4]، وهي جرائم لا يتوافر فيها القصد الجنائي ويكفي لتحققها أن يرتكب الجاني فعلاً لا يبغي منه تحقيق نتيجة جُرمية ولكن النتيجة تتحقق رغم ذلك بسبب خطأ ارتكبه الجاني كونه لم يسلك سلوك الشخص العاقل المتزن، كالقتل الخطأ أو الإيذاء الخطأ الناجم عن الحوادث المرورية[5].

---

[1]- د.هدى حامد قشقوش - شرح قانون العقوبات القسم العام – مرجع سابق - ص 112
[2]- د. رضا محمد عيسى – مرجع السابق – ص 23.
[3]- المرجع السابق – ص 24
[4]- د.هدى حامد قشقوش - شرح قانون العقوبات القسم العام – مرجع سابق - ص 112.
[5]- د. رضا محمد عيسى – مرجع سابق – ص 53.

لذا ومن واقع هذا التقسيم كان لابد لنا أن نتعرض لدراسة القصد الجنائي والخطأ الغير عمدي ونبحث من خلال دراستنا لهما مدى انطباق أي منهما أو كليهما على جرائم الدخول الغير مشروع إلى النظام المعلوماتي.

الفرع الأول: القصد الجنائي

كما سبق وأن أسلفنا فإن القصد الجنائي هو أحد صورتي الركن المعنوي (القصد، الخطأ غير العمدي)، ويُعرّف القصد الجنائي بأنه: اتجاه إرادة الجاني إلى النشاط الإجرامي الذي باشره وإلى تحقيق النتيجة المترتبة عليه مع علمه[1] بجميع العناصر التي يشترطها النظام لقيام الجريمة.

إذ لا يكفي أن يكون الجاني عالماً بالركن المادي للجريمة، بل يلزم أن يكون مريداً[2] تحقيق تلك النتيجة[3]، أي يرتكب السلوك المادي الذي يكون من شأنه تحقيق هذه النتيجة فلا يتوافر القصد الجنائي إلاّ إذا كان المتهم يريد تحقيق النشاط، وكذلك تحقيق النتيجة، وهذا ما يفرق الجرائم العمدية عن الجرائم غير العمدية[4].

نخلص من ذلك إلى أن تحديد وصف الجريمة يتوقف على مدى توافر القصد الجنائي لدى الجاني[5]، وأن القصد الجنائي يتكون من عنصرين[6] أساسيين هما العلم والإرادة،وأن تعريف القصد

---

[1]- تعرف د. هدى حامد قشقوش في صفحة 191 من مؤلفها جرائم الحاسب الالكتروني في التشريع المقارن – سبق الإشارة إليه، العلم بأنه أحد عنصري القصد الجنائي وينصرف معناه إلى الواقعة الإجرامية وتكييف الفعل ذاته، فيجب أن يكون الجاني على علم تام بالجريمة التي يرتكبها بكل عناصرها التي يحددها النص القانوني وهذه العناصر إما أن تكون عناصر واقعية أو قانونية.

[2]- كما تعرف د. هدى حامد قشقوش الإرادة في صفحة 197 من المرجع السابق بأنها العنصر الثاني للقصد الجنائي وبدونها ينتفي القصد الجنائي، وهي أهم ما يميز الإنسان عن غيره من المخلوقات، والإرادة تعبر عن قوة داخلية نفسية ومعنوية يعبر عنها الإنسان في سلوكه الخارجي ولكي تكون الإرادة غير معيبة يجب أن تصدر عن وعي وإدراك وهي حين ذلك توجه أعضاء الجسم للسلوك وتسيطر عليه.

[3]- د. رضا محمد عيسى – مرجع سابق – ص 54.

[4]- د. غنام محمد غنام – مرجع سابق- ص 169.، وفي نفس المعنى راجع د. هدى حامد قشقوش - شرح قانون العقوبات القسم العام – مرجع سابق - ص 112.

[5]- د. رضا محمد عيسى – مرجع سابق – ص 39.

[6]- إن تحديد عناصر القصد الجنائي محل لخلاف فقهي ويرى د. محمود نجيب حسني في مؤلفه شرح قانون العقوبات القسم العام– النظرية العامة للجريمة والنظرية العامة للعقوبة والتدبير الاحترازي - الطبعة الرابعة – دار النهضة العربية القاهرة 1977 أن صياغة تعريف القصد الجنائي تتوقف على البت في هذا الخلاف بين ما يعرف بأنصار نظرية العلم وأنصار نظرية الإرادة.

الجنائي يجب أن يشتمل على عناصره الأساسية، بمعنى أن يكون الجاني على علم تام بماهية الواقعة الإجرامية ونتيجتها وأن تتجه إرادته إلى إحداثها[1].

إذ لابد من توافر عنصر الإرادة لقيام القصد الجنائي، وعلى سبيل المثال فإن ذلك يتحقق إذا كان الدخول إلى النظام يتطلب شفرة أو بطاقة معينة، فقام الجاني بسرقة هذه البطاقة أو بكسر هذه الشفرة، كما يُعد استخدام المتهم وسائل خداعية في تحقيق الدخول أو البقاء في النظام قرينة على توافر القصد الجنائي في حقه، وإذا توافر القصد الجنائي، فإنه لا عبرة بالبواعث التي تكون وراء قيامه بفعله[2].

لم يحدد المرسوم اتحادي بقانون رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات في دولة الإمارات العربية المتحدة صورة الركن المعنوي لجريمة الدخول أو البقاء غير المشروع في النظام المعلوماتي في صورتها المجردة المنصوص عليها في المادة الثانية منه، وذلك على عكس القانون الاتحادي رقم (2) لسنة 2006م الملغي، الذي كان ينص على صورة الركن المعنوي صراحةً، حيث ابتدر المشرع الفقرة الأولى من المادة (2) بعبارة: (كل فعل عمدي يتوصل فيه بغير وجه حق إلى موقع أو نظام معلوماتي سواء بدخول الموقع أو... إلخ).

وقد اختلف الفقه في محاولته لمعرفة حكم الركن المعنوي في الحالة التي يسكت فيها المشرع عن التصريح بصورة الركن المعنوي، فيرى البعض[3]، أنه إذا لم يصرح المشرع بصورة الركن المعنوي للجريمة، سواءً كانت ترتكب عمداً أو بغير عمد، فمعنى ذلك أنه يستوي في نظر المشرع أن يرتكب الفعل بطريق العمد أو الخطأ[4].

---

[1]- د. هدى حامد قشقوش - شرح قانون العقوبات القسم العام – مرجع سابق - ص 191.
[2]- د. محمود أحمد طه – مرجع السابق – ص 33.
[3]- د. رمسيس بهنام - النظرية العامة للقانون الجنائي – دار النهضة العربية 1971 – ص 490.
[4]- د.عبد الرازق الموافي عبد اللطيف – شرح قانون مكافحة جرائم تقنية المعلومات لدولة الإمارات العربية المتحدة المرسوم اتحادي بقانون الاتحادي رقم 5 لسنة 2012– الكتاب الأول – إصدارات معهد دبي القضائي – ص 24.

ذهب الرأي الراجح في الفقه إلى أن الأصل هو أنها جريمة عمدية، إذ لا عقاب على غير العمد إلاّ بنص خاص[1]، وهذا يعنى أنه إذا لم ينص المشرع على اعتبار الفعل جريمة إذا وقع بغير عمدٍ، وذلك يترجم رغبته في اشتراط أن يقع الفعل عمداً لإمكان اعتباره جريمة وبعكس ذلك تكون القاعدة في المخالفات فلا يكون القصد الجنائي ضروريا لتكوين الجريمة إلاّ عندما يستلزمه القانون وبنص خاص[2].

ويذهب جانب من الفقه[3] إلى أن جريمة الدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات الإلكترونية جريمة عمدية يتخذ الركن المعنوي فيها صورة القصد الجنائي العام بعنصريه العلم والإرادة[4]، وأنه وحتى يتحقق وقوع الجريمة فلا بد أن يعلم الجاني بأنه يدخل إلى موقع لا يجوز له الدخول فيه، وأن تتجه إرادته إلى ذلك[5]، فهي جريمة عمدية لا تقع بطريق الخطأ ويتكون الركن المعنوي فيها من القصد الجنائي[6].

وأن يعلم الجاني بكل العناصر التي تدخل في بناء الجريمة، وأن سلوكه بالدخول إلى الموقع الالكتروني أو النظام الالكتروني بصفة عامة، فالسلوك هو وسيلة الإنسان في التعبير عن إرادته، كما أن الإرادة هي المحرك لسلوك الإنسان[7]، ومتى ما توافر القصد الجنائي بعنصرية العلم والإرادة فإنه لا محل للسؤال عن الباعث على ارتكاب الجريمة، فالجريمة تقوم بحق الجاني حتى وإن كان دخوله إلى النظام بدافع سياسي أو عسكري أو تجاري أو كان لمجرد الفضول والتنزه واثبات القدرات في الانتصار على النظام[8].

---

[1]- د. محمود نجيب حسني - شرح قانون العقوبات - مرجع سابق – ص 645.
[2]- د.عبد الرؤوف مهدي - شرح القواعد العامة لقانون العقوبات – دار النهضة العربية – 2011 – ص 481.
[3]- يأتي من بين أنصار هذا الرأي د. علي عبد القادر القهوجي، ود. حسين بن سعيد الغافري وأ.د. إمام حسنين خليل عطا الله.
[4]- د. حسين بن سعيد الغافري – مرجع سابق – ص 356.
[5]- د. محمود أحمد طه – مرجع سابق – ص 32.
[6]- أ.د. إمام حسنين خليل عطا الله – مرجع سابق - ص 60.
[7]- د.هدى حامد قشقوش – مرجع سابق – ص 197.
[8]- د. حسين بن سعيد الغافري – مرجع سابق – ص 357.

وينتفي القصد الجنائي في حق المتهم إذا كان الدخول أو البقاء قد تم بطريق الخطأ، وتطبيقاً لذلك ينتفي القصد الجنائي إذا كان دخوله إلى النظام أو البقاء فيه أو استعماله كان مشروعاً، أو إذا ثبت أنه دخل على قواعد البيانات مصادفةً، وأن دخوله كان وليد خطأ، ولم يكن فعله كاشفاً عن توافر هذا القصد، أو إذا كان الدخول على النظام يتم بموجب اشتراك وأن الشخص دخل بوجه مشروع إلاّ أن مدة اشتراكه انتهت وكان يجهل ذلك[1].

بينما يرى جانب آخر من الفقه[2] أن الجاني يُسأل عن جريمة الدخول الغير المشروع إلى النظام المعلوماتي في صورتها المجردة سواءً وقعت عمداً أم بطريق الخطأ، ويستند أصحاب هذا الرأي إلى أن المشرع الوطني وعلى الرغم من أنه لم يحدد صورة الركن المعنوي عندما نص على هذه الجريمة في المرسوم بقانون رقم (5) لسنة 2012، إلاّ أنه كان قد وضع قاعدة عامة ثابتة لمعالجة هذه الحالة بنص صريح في المادة الثالثة والأربعون من قانون العقوبات التي تنص على أنه: (يُسأل الجاني عن الجريمة سواءً ارتكبها عمداً أم خطأً ما لم يشترط القانون العمد صراحةً)، وبالتالي يعاقب الجاني على جرائم الدخول الغير مشروع إلى النظام المعلوماتي في صورتها المجردة سواءً وقعت عمداً أم بطريق الخطأ[3].

بمعنى أنه يُسأل الجاني عن جريمة الدخول أو البقاء غير المشروع في النظام المعلوماتي في صورتها المجردة سواءً وقعت عمداً أم بطريق الخطأ، وذلك أن هذا الرأي يتفق مع صحيح المادة (43) من قانون العقوبات الاتحادي لدولة الإمارات العربية المتحدة لسنة 1987 المعدل، والتي تقرر معاقبة الجاني عن الجريمة سواءً ارتكبها عمداً أم خطأً ما لم يشترط القانون العمد صراحةً، كما يتفق هذا الرأي مع رغبة المشرع الوطني في تجريم هذه الأفعال، فقد كان المشرع في القانون الملغي يشترط صراحة عمدية الأفعال التي يتوصل بها إلى النظام المعلوماتي.

---

[1]- د.علي عبد القادر القهوجي - مرجع سابق.
[2]- من أنصار هذا الرأي د. عبد الرازق الموافي عبد اللطيف – مرجع سابق– ص 25.
[3]- د.عبد الرازق الموافي عبد اللطيف – مرجع سابق– ص 25.

ونرى أن ما كان يتطلبه القانون الملغي من عمدية فعل الدخول الغير مشروع إلى النظام المعلوماتي هو الأفضل والأوفق، وذلك بأن تكون جريمة الدخول غير مشروع إلى النظام المعلوماتي جريمة عمدية يعاقب فيها الجاني إذا دخل متعمداً إلى النظام المعلوماتي بشكل غير مشروع، حيث لم يقرر المشرع عقوبة للجريمة العمدية وعقوبة للجريمة غير العمدية في المادة (43) من قانون العقوبات الاتحادي.

الفرع الثاني: الخطأ غير العمدي

الخطأ غير العمدي هو الركن المعنوي للجريمة غير العمدية، وهو إخلال الجاني عند تصرفه بواجبات الحيطة والحذر التي يفرضها القانون، وعدم حيلولته تبعاً لذلك دون أن يفضي تصرفه إلى إحداث النتيجة الإجرامية في حين كان ذلك في استطاعته وكان واجباً عليه[1].

نخلص من هذا التعريف إلى أن جوهر الخطأ غير العمدي هو إخلال الجاني بالتزامٍ عام مستطاع وفي وسعه يفرُضه عليه القانون، هذا الالتزام هو مراعاة الحيطة والحذر والحرص على الحقوق والمصالح التي يحميها القانون، فإن كان منها ما يمس بالحقوق والمصالح التي يحميها القانون تعين عليه بذل الجهد للحيلولة دون هذا المساس[2]، وقد قررت محكمة النقض المصرية في حكم لها: (أن سلامة الحكم بالإدانة في الجرائم غير العمدية مشروط ببيان ركن الخطأ والتدليل عليه)[3].

تتمثل صور الخطأ غير العمدي في الإهمال أو الرعونة أو عدم الاحتياط أو عدم مراعاة اللوائح والقوانين فالجاني لا يقصد إتيان الفعل المجرم ولكن بسلوكه الخاطئ يؤدي إليه، وعلى ذلك نجد أن المادة (38) من القانون العقوبات الاتحادي لسنة 1987 المعدل تنص على (... ويتوفر

---

[1]- د. محمود نجيب حسني – شرح قانون العقوبات – القسم العام ط 4 – النظرية العامة للجريمة والنظرية العامة للعقوبة والتدبير الاحترازي – مرجع سابق – ص 644.

[2]-د. محمود نجيب حسني - مرجع سابق – ص 664.

[3]- نقض 2001/4/15 – الطعن رقم 10678 لسنة 67 قضائية – مجموعة أحكام النقض لعام 2001 – ص 418، راجع في ذلك د.هدى حامد قشقوش - شرح قانون العقوبات القسم العام – مرجع سابق - ص 113.

الخطأ إذا وقعت النتيجة الإجرامية بسبب خطأ الفاعل سواء أكان هذا الخطأ إهمالا أم عدم انتباه أم عدم احتياط أو طيشا أو رعونة أم عدم مراعاة القوانين أو اللوائح أو الأنظمة أو الأوامر).

المبحث الثاني: جريمة الدخول بدون تصريح إلى نظام المعالجة الآلية للمعطيات الإلكترونية بقصد الحصول على بيانات حكومية أو معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية

تمهيد:

إن تقنية المعلومات أصبحت مرتكزاً رئيسياً لإدارة العمليات الحكومية في ظل الحكومة الإلكترونية ومن بعدها الحكومة الذكية، كما أنها قطعت شوطاً كبيراً في إدارة النشاط التجاري والاستثماري المحلي والدولي، بل أنها أصبحت أهم متطلبات التنافس في هذا الحقل، وكان من أهم إفرازاتها في القطاع الخاص شبكات الأعمال الإلكترونية واعتماد تحقيق عناصر اساسية من معايير الجودة الشاملة في الإدارة والانتاج والخدمات القائمة على تقنية المعلومات[1].

وبلا شك أن الحاسبات الذكية ونظم تقنية المعلومات بما لديها من امكانيات وقدرة فائقة في التخزين والمعالجة الإلكترونية، أصبحت مخزناً لأهم المعلومات وأكثرها حساسية سواءً التي تتعلق بمصالح الدول والحكومات أو التي تتعلق بمصالح الأفراد أو المؤسسات الاقتصادية أو المالية أو التجارية، لذا كان لابد من بسط الحماية القانونية لهذه البيانات والمعلومات على المستويين الحكومي والمؤسسي[2].

وذلك أسوةً بالحماية الجنائية التي وضعها المشرع الوطني للبيانات والمعلومات بصفةً عامة في المرسوم اتحادي بقانون رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات، والتي سبق وأن تعرضنا اليها في هذه الدراسة، بدءً بتجريم الدخول الغير مشروع إلى النظام

---

[1]- د. أمير فرج يوسف – مرجع سابق– ص 397.

[2]- د. نائلة عادل محمد فريد قدورة – جرائم الحاسب الالي الاقتصادية – منشورات الحلبي الحقوقية بيروت – سنة 2005- ص 275.

المعلوماتي في شتى صوره وأشكاله، حيث لاحظنا كيف أنه شدد العقوبة عند الاضرار بهذه البيانات والمعلومات في الفقرة (2) من المادة الثانية، ثم تدرج في تشديد العقوبة تبعاً للأثر الجرمي، بأن زاد من العقوبة عندما تعلق الإضرار بمعلومات شخصية، وعند ارتكاب الجريمة بمناسبة أو بسبب تأدية العمل.

وسيراً على هدى الحماية الجنائية للنظام المعلوماتي والبيانات والمعلومات، فقد خص المشرع الوطني البيانات الحكومية، والمعلومات السرية الخاصة بالمؤسسات أو المنشآت المالية والتجارية والاقتصادية بحماية جنائية خاصة فرضها من خلال الفقرة الأولى من المادة (4) من المرسوم اتحادي بقانون رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

حيث تنص على أنه: (يعاقب بالسجن المؤقت والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون وخمسمائة ألف درهم كل من دخل بدون تصريح إلى موقع إلكتروني، أو نظام معلومات إلكتروني، أو شبكة معلوماتية، أو وسيلة تقنية معلومات، سواء كان الدخول، بقصد الحصول على بيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية، أو تجارية، أو اقتصادية).

هذه الفقرة تقابل نص الفقرة الأولى والثالثة من المادة (22) من القانون الملغي اللتان كانتا تنصان على: (يعاقب بالسجن كل من دخل وبغير وجه حق موقعا أو نظاما مباشرة أو عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات بقصد الحصول على بيانات أو معلومات حكومية سرية اما بطبيعتها أو بمقتضى تعليمات صادرة بذلك ويسري حكم هذه المادة على البيانات والمعلومات الخاصة بالمنشآت المالية والتجارية والاقتصادية.

وحتى نقف على معالم الحماية الجنائية التي رسمها المشرع في المرسوم اتحادي بقانون رقم (5) لسنة 2012 للبيانات الحكومية والمعلومات السرية الخاصة بالمؤسسات أو المنشآت المالية والتجارية والاقتصادية، كان لابد لنا من تقسيم هذا المبحث إلى ثلاثة مطالب، نخصص

الأول منها لدراسة محل الجريمة، والمطلب الثاني لدراسة الركن المادي، والمطلب الثالث للركن المعنوي للجريمة وذلك على النحو الآتي:

المطلب الأول: محـل الجريمـة

عرفنا أن المقصود بمحل الجريمة هو العناصر التي تحدد المجال الذي يمكن أن ترتكب فيه الجريمة، وهو بمثابة نسيج خارج عن الجريمة نفسها، يُنظم فوقه الجاني نشاطه الإجرامي من دون أن ينفك عنه، أو هو مركز محايد في حد ذاته يمثل نقطة البدء لارتكاب بعض الجرائم ويكون لازماً لوقوع الجريمة[1].

محل هذه الجريمة هو إما أن يكون البيانات الحكومية المعالجة الكترونياً[2]، أو المعلومات السرية الخاصة بمنشأة مالية أو تجارية أو اقتصادية[3]، إذ أن القانون يفرض سرية معينة بالنسبة لبعض الأنظمة مثل أسرار الدولة، لذا تشمل الحماية القانونية البيانات الحكومية المنشورة على الموقع الالكترونية الحكومية الاتحادية والحكومات المحلية للإمارات.

كما تشمل الحماية القانونية السرية المتعلقة بالمعلومات الذاتية أو الاسمية أو سر المهنة، أو أسرار الأشخاص مثل أسرار الحياة الخاصة المهنية، أو أي معلومات تجمعها المنشآت المالية أو التجارية أو الاقتصادية في النظام المعلوماتي ولا يسمح بالاطلاع عليها لأي إنسان من خارج المنشأة[4].

ولدراسة محل هذه الجريمة رأينا أن نقسم هذا المطلب إلى فرعين نخصص الأول منهما لدراسة البيانات الحكومية أما الفرع الثاني فنتناول فيه بالدراسة المعلومات السرية الخاصة بالمنشآت المالية والتجارية والاقتصادية وذلك على النحو التالي:

---

[1]- راجع في ذلك محل الجريمة – ص (10).
[2]- د. عبد الرازق الموافي عبد اللطيف – مرجع سابق – ص 39.
[3]- المرجع السابق – ص 43.
[4]- د. علي عبد القادر القهوجي – مرجع سابق.

الفرع الأول: البيانات الحكومية

بالاطلاع على نص الفقرة (1) من المادة (4) نجد أنها تقرر حالة الدخول بدون تصريح إلى موقع إلكتروني، أو نظام معلوماتي إلكتروني، أو شبكة معلوماتية، أو وسيلة تقنية معلومات، إما بقصد الحصول على بيانات حكومية، أو بقصد الحصول على معلومات سرية خاصة بمنشاة مالية أو تجارية، أو اقتصادية.

أولاً: مفهوم البيانات الحكومية

يقصد بالبيانات الحكومية البيانات أو المعلومات الإلكترونية الخاصة أو العائدة إلى الحكومة الاتحادية أو الحكومات المحلية لإمارات الدولة أو الهيئات العامة أو المؤسسات العامة الاتحادية أو المحلية[1]، إذ أن للبيانات الحكومية المعالجة الكترونياً خصوصيتها وأهميتها التي توجب المحافظة عليها وتأمينها حتى تتمكن أجهزة الدولة من القيام بمهامها على أكمل وجه خاصة في ظل التطور النوعي لنظم المعلومات الحكومية المتمثل في الحكومة الإلكترونية والحكومة الذكية التي باتت تطبيقاتها تحل محل العمل التقليدي.

أما الجهات الحكومية التي تملك البيانات محل الحماية الجنائية فهي الوزارات الاتحادية والدوائر المحلية والسلطات والهيئات والمؤسسات العامة التابعة لها، بما في ذلك القوات المسلحة، والشرطة وأجهزة أمن الدولة، ويستثنى من ذلك أية شركة أو مؤسسة تجارية ولو كانت مملوكة من قبل هذه الجهات أو تملك مصالح فيها[2].

---

[1]- أنظر تعريف البيانات الحكومية في المادة (1) من القانون رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

[2]- تنص المادة الأولى من المرسوم اتحادي بقانون رقم (3) لسنة 2003 في شأن تنظيم قطاع الاتصالات المعدل بالمرسوم بقانون اتحادي رقم (5) لسنة 2008على أنه: (في تطبيق أحكام هذا المرسوم بقانون يقصد بالكلمات والعبارات التالية المعاني المبينة قرين كل منها ما لم يقض سياق النص بغير ذلك: الدولة: دولة الإمارات العربية المتحدة. الحكومة: حكومة دولة الإمارات العربية المتحدة. الجهات الحكومية: الوزارات الاتحادية والدوائر المحلية والسلطات والهيئات والمؤسسات العامة التابعة لها بما في ذلك القوات المسلحة والشرطة وأجهزة أمن الدولة، ويستثنى من ذلك أية شركة أو مؤسسة تجارية ولو كانت مملوكة من قبل هذه الجهات أو تملك مصالح فيها. الجهات الحكومية: الوزارات الاتحادية والدوائر المحلية والسلطات والهيئات والمؤسسات العامة التابعة لها بما في ذلك القوات المسلحة

بالتالي فإن محل الجريمة هو البيانات الحكومية لجميع هذه الجهات الاتحادية والمحلية التي فصلتها المادة الأولى من المرسوم اتحادي بقانون رقم (3) لسنة 2003 في شأن تنظيم قطاع الاتصالات المعدل بالمرسوم بقانون اتحادي رقم (5) لسنة 2008، بينما لا تكون البيانات الخاصة بالشركات والمؤسسات التجارية المملوكة لهذه الجهات أو التي تملك هذه الجهات مصالح فيها محلاً للجريمة.

ثانياً: طبيعة البيانات الحكومية

باستقراء نص الفقرة الأولى من المادة (4) من المرسوم اتحادي بقانون رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات، نجد أن المشرع أسبغ الحماية على البيانات الحكومية أياً كانت طبيعتها، سواءً كانت هذه البيانات الحكومية سرية أو غير سرية، مخالفاً بذلك القانون (الملغي) الذي كان يشترط أن تكون البيانات الحكومية محل الانتهاك سرية إما بطبيعتها أو بناءً على تعليمات[1]، أي بمعنى أن الحماية الجنائية وفقاً للمرسوم الحالي تشمل البيانات الحكومية المعالجة الكترونياً بشكل مطلق.

ويستوي أن تتعلق هذه البيانات بأمور مالية او تجارية او اقتصادية، ما دام محل هذه الصورة من التجريم هو بيانات حكومية، فإن ذلك يعني أن الامر يتعلق بمستندات أو وثائق تتضمن بيانات على قدر كبير من الأهمية لمصالح الدولة[2].

يلاحظ أنه وكما سبق وأن أشرنا إلى أن شبكات المعلومات تعد بيئة صالحة لعمليات التجسس على المعلومات الخاصة بالهيئات الحكومية والخاصة، وهذه المعلومات إذا ما تم

والشرطة وأجهزة أمن الدولة، ويستثنى من ذلك أية شركة أو مؤسسة تجارية ولو كانت مملوكة من قبل هذه الجهات أو تملك مصالح فيها..... إلخ)

[1]- المستشار علاء فكري اباظة – مرجع سابق – ص 53.

[2]- د.عبد الرازق الموافي عبد اللطيف – مرجع سابق – ص 40.

الحصول عليها أو التجسس عليها، فقد يساء استخدامها سواءً من قوى داخلية أو خارجية معادية للدولة التي جمعت هذه المعلومات من شبكاتها[1].

الفرع الثاني: المعلومات السرية الخاصة بمنشأة مالية أو تجارية أو اقتصادية

يقصد بالمعلومات السرية، تلك المعلومات التي لا يكون مصرحاً للغير الاطلاع عليها أو إفشائها إلا بإذنٍ مسبقٍ ممن يملُك هذا الإذن[2]، أما المنشآت المالية أو التجارية أو الاقتصادية فيقصد بها أي منشأة تكتسب وصفها المالي أو التجاري أو الاقتصادي بموجب الترخيص الصادر لها من جهة الاختصاص في الدولة[3].

بناءً على ذلك فإنه يجب النظر دائماً للترخيص الصادر من الجهة الإدارية المختصة الممنوح للمنشأة بمزاولة نشاطها، فإن كانت تلك المنشأة قد اكتسبت صفتها المالية أو التجارية أو الاقتصادية بموجب ذلك الترخيص فإن الجريمة تقع متى ما توافرت باقي أركانها.

أولاً: مفهوم المعلومات السرية

بالإضافة إلى الترخيص الصادر من جهة الاختصاص فإن محل هذه الجريمة يشتمل على عنصر السرية بالنسبة للمعلومات الخاصة بالمنشآت المالية أو التجارية أو الاقتصادية، إذ أن المشرع استلزم لقيام الجريمة بشأن هذا النوع من المعلومات أن تكون سرية، فإذا لم تكن هذه المعلومات سرية فلا تقع هذه الجريمة، وإنما يمكن أن تتحقق جريمة أخرى، وهي الجريمة الواردة في المادة الثانية من المرسوم اتحادي بقانون رقم (5) لسنة 2012[4].

من المعلوم أن أكبر المخاطر التي تتعرض لها شبكة الانترنت في تداول المعلومات هي عدم وجود الأمان (Security) الكافي بالنسبة للعميل، حيث يأتي هذا السبب على رأس الأسباب

---

[1]- عفيفي كامل عفيفي – مرجع سابق – ص 325.
[2]- أنظر تعريف السرية في المادة (1) من المرسوم اتحادي بقانون رقم (5) لسنة 2012.
[3]- أنظر تعريف المنشآت المالية أو التجارية أو الاقتصادية في المادة (1) من المرسوم اتحادي بقانون رقم (5) لسنة 2012.
[4]- المستشار علاء فكري اباظة – مرجع سابق – ص54.

التي يتخوف منها العميل وتجعله يتردد عند استخدام الشبكة، ومن أجل تلافي هذا الخطر نجد أن البنوك والمؤسسات العالمية تتجه إلى وضع حماية أمنية عالية التقنية لحماية المستهلك في إجراء عمليات الشراء والبيع، وكذلك لحماية التاجر الذي يقوم بعرض السلعة أو الخدمة[1].

البيانات المعالجة الكترونياً والمعلومات التي يتم التعامل به في نطاق التجارة، لا سيما التجارة الالكترونية يجب الحفاظ على سريتها وخصوصيتها، وذلك تأميناً لممارسة العمليات التجارية في أمان، وتختلف أنظمة الأمان وحماية البيانات في مدى السرية التي توفرها للبيانات، من حيث سهولة أو عدم سهولة اختراق نظام عن آخر، حيث أن حماية نظام المعلومات يعتمد على عدة عوامل أهمها السرية[2].

وهذه المعلومات قد تكون سرية بطبيعتها وبمقتضى أوامر صادرة بذلك، كما أن إضفاء السرية على تلك المعلومات يعني حظر الاطلاع عليها من الغير، وهذه المعلومات قد تتعلق بمنشأة مالية كالبنوك أو منشأة تجارية كإحدى الشركات أو منشأة اقتصادية كالمطارات والموانئ[3].

لا ينظر في شأن تحديد معنى السرية الواجب توافره في المعلومات الخاصة بتلك المنشآت إلى طبيعة المعلومات ذاتها، إذ المعيار في معنى السرية أن تكون تلك المعلومات مما لا يجوز للغير الاطلاع عليها أو إفشائها إلاّ بإذن مسبق ممن يملك هذا الإذن[4].

معنى ذلك أن البحث في مدى سرية المعلومات لا يكون من خلال ذاتيتها، وإنما من خلال عامل خارجي، يتمثل في صدور قرار من شخص مختص يملك الصلاحيات في المنشأة، يحظر فيه الاطلاع أو إفشاء المعلومات إلاّ بإذن مسبق منه، فالسرية تعني أن المعلومات في النظام

---

[1]- د.هدى حامد قشقوش – الحماية الجنائية للتجارة الالكترونية عبر الإنترنت – دار النهضة العربية 2000- ص 21
[2]- المرجع السابق - ص 41
[3]- د.عبد الرازق الموافي عبد اللطيف – مرجع سابق – ص 43.
[4]- المستشار علاء فكري اباظة – مرجع سابق – ص54.

مسموح بمعالجتها من قبل الأشخاص المصرح لهم فقط، وذلك من أجل منع وإعاقة إفشاء المعلومات[1].

يلاحظ أننا كنا قد أشرنا في مكان سابق من هذه الدراسة عند تناولنا لموضوع تشديد المشرع للعقوبة على الاعتداء على البيانات والمعلومات ذات الطابع الشخصي، أنه يشترط في المعلومة الإلكترونية كي تعتبر سراً يستحق الحماية أن تكون هذه الأسرار ذات صلة بالشخص، وأن تحظى بحرص صاحبها في إبقائها سرية بعيدة عن علم الغير، وأن يكون من شأن الاعتداء على سريتها هذه احتمال الإضرار المادي أو المعنوي بصاحبها[2].

مع ملاحظة أن مفهوم الشخص الطبيعي لا يختلف عن الشخص المعنوي أو ما يعرف اصطلاحاً بالشخص الاعتباري[3]، من حيث الحقوق والالتزامات، فكلاهما يتمتع بجميع الحقوق، إلا ما كان منها ملازماً لصفة الإنسان الطبيعية، وذلك وفقاً للحدود التي يقررها القانون[4].

نخلص من ذلك أن الحماية الجنائية في نص الفقرة الأولى من المادة الرابعة من المرسوم اتحادي بقانون رقم (5) لسنة 2012 تنصرف إلى السر كعنصر مرتبط بنشاطات القطاع الخاص وعلاقته بالمجتمع والأفراد، والعلاقات الخاصة الناشئة عن ذلك كله، سواءً كان السر ذو طبيعة اقتصادية أو مالية أو تجارية معلوماتية بحتة[5].

---

[1]- د. صالح سليمان عبد العظيم - الندوة العلمية – بحث بعنوان الأبعاد والتأثيرات الاجتماعية المرتبطة باستخدام الانترنت على الأسرة العربية – ص 217.

[2]- د. محمود أحمد طه – مرجع سابق – ص 60، وفي نفس المعنى راجع د. أسامة العبيدي – حماية الحق في الحياة الخاصة في مواجهة جرائم الحاسب الآلي والانترنت – المجلة العربية للعلوم الأمنية – مجلد 23 – العدد 46.

[3]- عرفت المادة (92) من القانون الاتحادي رقم (5) لسنة 1985 في شأن المعاملات المدنية وتعديلاته الأشخاص الاعتباريون أو المعنويون بأنهم: (أ/ الدولة والإمارات والبلديات وغيرها من الوحدات الإدارية بالشروط التي يحددها القانون. ب/ الإدارات والمصالح والهيئات العامة والمنشآت والمؤسسات العامة التي يمنحها القانون الشخصية الاعتبارية. ج/ الهيئات الإسلامية التي تعترف لها الدولة بالشخصية الاعتبارية. د/ الأوقاف. هـ/ الشركات المدنية والتجارية إلا ما استثني منها بنص خاص. و/ الجمعيات والمؤسسات الخاصة المنشأة وفقاً للقانون. ز/ كل مجموعة من الأشخاص أو من الأموال تثبت لها الشخصية الاعتبارية بمقتضى نص القانون)

[4]- نشير في ذلك إلى ما تقرره المادة (93) من القانون الاتحادي رقم (5) لسنة 1985 في شأن المعاملات المدنية وتعديلاته عن تمتُّع الشخص الاعتباري بجميع الحقوق إلا ما كان منها ملازماً لصفة الإنسان الطبيعية مثل الأهلية والذمة المالية المستقلة وحق التقاضي وغيره من الحقوق في الحدود التي يعينها التي يقررها القانون.

[5]- القاضي جلال محمد الزعبي والقاضي أسامة أحمد المناعسة – جرائم تقنية نظم المعلومات الإلكترونية – دراسة مقارنة – دار الثقافة للنشر والتوزيع الأردن – سنة 2010 – ص 265.

وأن البحث في مدى سرية المعلومات لا يكون من خلال ذاتيتها، وإنما يكون من خلال عامل خارجي عنها هو ما إذا كان قد صدر قرار من مختص في المنشأة يحظر فيه الاطلاع أو إفشاء المعلومات إلاّ بإذن مسبق منه، فإذا لم يكن قد صدر مثل ذلك القرار فلا تكتسب المعلومات وصف السرية حتى لو كانت بطبيعتها سرية[1].

ثانياً: تعريف المنشآت المالية والتجارية والاقتصادية

عرفنا من خلال التعريف الوارد في المادة الأولى من المرسوم اتحادي بقانون رقم (5) لسنة 2012 أن المقصود بالمنشآت المالية والتجارية والاقتصادية أي منشأة تكتسب وصفها المالي أو التجاري أو الاقتصادي بموجب الترخيص الصادر لها من جهة الاختصاص في الدولة ، وتعرف المادة الأولى من القانون رقم (8) لسنة 1980 في شأن تنظيم علاقات العمل وتعديلاته المنشأة بأنها هي كل وحدة اقتصادية فنية أو صناعية أو تجارية يعمل فيها عمال تهدف إلى إنتاج سلع أو تسويقها أو تقديم خدمات من أي نوع.

فالمنشأة وفقاً للتعريف الوارد في قانون تنظيم علاقات العمل تشمل النشاط الاقتصادي والفني والصناعي والتجاري وهذه المنشأة قد تكون مالية مثل البنوك والمصارف والصرافات ومؤسسات التمويل أو المنشآت التجارية العاملة في الدولة وفقاً لأحكام القانون رقم (8) لسنة 1984 في شأن الشركات التجارية، أو أي منشأة اقتصادية مثل الشركات العاملة في مجال النفط والتنقيب والغاز وإنتاج الكهرباء وغيرها من المنشآت الاقتصادية التي تعمل وفقاً لقوانين خاصة، أو قوانين مستثناه صادرة عن مجلس الوزراء[2].

---

[1]- المستشار علاء فكري اباظة – مرجع سابق – ص 55.

[2]- راجع في ذلك نص الفقرة (3) من المادة (2) من القانون رقم (8) لسنة 1984 في شأن الشركات التجارية وتعديلاته.

المطلب الثانـي: الركن المادي

لكي تتكون الجريمة فلابد من ارتكاب الجاني لفعل مادي محسوس (أو الامتناع عن اتيان فعل) يعاقب عليه القانون، فالجريمة ليست مجرد وجود نية جرمية، إذ لابد لهذه النية أن تتجسد في كيان مادي محسوس، هذا السلوك المادي المحسوس الذي ينص عليه القانون يعرف بالركن المادي للجريمة، والذي يشكل شرطاً أساسياً للبدء في عملية البحث عن توافر الجريمة من عدمه، لذا لإكمال الركن المادي لابد من توافر ثلاثة عناصر هي السلوك الإجرامي، والنتيجة الجرمية، وعلاقة السببية بينهما[1].

يقوم الركن المادي، لهذه الجريمة حسب نص الفقرة الأولى من المرسوم اتحادي بقانون رقم (5) لسنة 2012 على توافر عدة شروط أولها أن يرتكب الجاني السلوك الإجرامي الذي يتجسد في الدخول إلى النظام المعلوماتي المتمثل في (موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلوماتية أو وسيلة تقنية معلومات)، ويشترط في هذا السلوك أن يكون دخولاً بدون تصريح، وأن يكون القصد من الدخول هو الحصول على بيانات، وان تكون هذه البيانات تخص الحكومة[2]، أو بقصد الحصول على معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية.

بناءً على ما تقدم سنتناول الركن المادي بالدراسة في فرعين نخصص الأول منهما لفعل الدخول، أما الفرع الثاني فنتناول فيه بالدراسة الشرط الثاني المكون للركن المادي وهو عدم وجود التصريح اللازم لدخول النظام المعلوماتي وذلك على النحو التالي:

---

[1]- القاضي جلال محمد الزعبي والقاضي أسامة أحمد المناعسة – مرجع سابق – ص 49.
[2]- د.عبد الرزاق الموافي عبد اللطيف – مرجع سابق – ص 40.

الفرع الأول: فعل الدخول

يُعد الدخول فعلاً غير مشروعاً متى ثبت أنه تم بعدم رضا صاحب الحق في الدخول إلى النظام[1]، إذ أن مجرد الدخول إلى النظام المعلوماتي بدون تصريح يمثل جريمة في حد ذاته، وكنا قد أشرنا إلى ذلك سابقاً في هذه الدراسة، وأوضحنا أن هذه الجريمة تدخل تحت وصف الجريمة الشكلية.

ذلك أن القانون لا يتطلب فيها حدوث نتيجة معينة، وإنما كل ما يتطلبه القانون هو مجرد القيام بالسلوك أو النشاط التقني الإجرامي، وأن المشرع في مثل هذه الجرائم يكتفي بمجرد حدوث الحدث الإجرامي المتمثل في السلوك لتوقيع العقاب، ومثال ذلك الجرائم التقليدية بجريمة انتهاك المسكن أو جرائم السب والقذف[2]، والتي سأتطرق لها لاحقاً.

باستقراء نص الفقرة الأولى من المادة الرابعة من المرسوم اتحادي بقانون رقم (5) لسنة 2012 نلاحظ أن المشرع لم يحدد الوسيلة أو الطريقة الإجرامية، التي يتم بها الدخول إلى النظام، لذلك فإن الجريمة تقع بأي وسيلة أو طريقة يتم بها الدخول الغير مشروع إلى نظام المعلومات، ويستوي أن يتم الدخول بصورة مباشرة أو عن طريق غير مباشر[3].

ويتحقق الدخول غير المشروع إلى النظام المعلوماتي في هذه الجريمة بالوصول إلى البيانات أو المعلومات المخزنة داخل النظام دون وجه حق، سواءً دخل الشخص بناء على إذن ولكنه تعدى حدود الإذن والترخيص الممنوح له أو أنه دخل بطريقة متعمده إلى النظام المعلوماتي[4].

---

[1]- د.محمود أحمد طه - المواجهة التشريعية لجرائم الكمبيوتر والانترنت دراسة مقارنة - دار الفكر والقانون المنصورة – ص 26.

[2]- راجع المستشار د. ربيع محمود الصغير - مرجع سابق - ص 350.

[3]- د.سعيدي سليمة والأستاذ حجاز بلال – مرجع سابق – ص 149.

[4]- د.حسين بن سعيد الغافري – مرجع سابق - ص 346.

أي بمعنى آخر أنه عندما يتم خرق حرمة النظام والدخول إليه، فإن المتطفل يتمكن من الوصول إلى البيانات والمعلومات الموجودة والاطلاع عليها، أي الوصول لكل ما هو مسموح الوصول إليه بالنسبة لصاحب الحساب الأصلي، من البيانات أو الوثائق السرية الخاصة بالمنشأة[1].

لذا فإنه يفهم من ظاهر النص القانوني في الفقرة الأولى من المادة الرابعة أن مقصود الجاني من الدخول هو الوصول إلى المواقع الالكترونية أو أنظمة المعلومات الالكترونية أو شبكة المعلومات أو وسيلة تقنية المعلومات[2]، والاطلاع على ما تحويه من بيانات حكومية أو معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية، كل ذلك مع عدم توافر المشروعية أو الصلاحية[3]، التي تبيح للجاني دخول النظام المعلوماتي، بمعنى أن هذا الدخول يتم دون وجه حق.

لذلك تقع الجريمة عندما ينجح الجاني في الدخول للنظام المعلوماتي من خلال تجاوز الضوابط من غير وجه حق، ويكون دخوله الغير مشروع بقصد الحصول على البيانات الحكومية أو المعلومات السرية الخاصة بالمنشأة المالية أو التجارية أو الاقتصادية، فيكون دخوله معاقب عليه بموجب الفقرة الأولى من المادة الرابعة بغض النظر عن الوسيلة المستخدمة طالما كان لا يملك التصريح بالدخول.

بناءً عليه ولتوضيح المكنون القانوني والفني لفعل الدخول نقسم هذا المطلب إلى أولاً النشاط التقني المكون لفعل الدخول ومن ثم نتعرض لعلاقة السببية بين النشاط التقني والنتيجة الإجرامية وذلك على النحو التالي:

أولاً: دور النشاط التقني في الدخول للنظام المعلوماتي

سبق وأن أشرنا عند تناولنا لفعل الدخول في الفصل الأول أن المقصود بفعل الدخول الغير المشروع إلى النظام المعلوماتي، هو الاتصال بالنظام بأي طريقة كانت، دون تعليق ذلك

---

[1]- المرجع السابق - ص 346.
[2]- د.عبد الرزاق الموافي عبد اللطيف – مرجع سابق – ص 18.
[3]- د.عمر محمد أبو بكر بن يونس – مرجع سابق – ص 333.

على تطلب غرض ما من هذا الدخول، سواءً تم هذا الدخول باستعمال أجهزة خاصة تمكنه من كسر شفرة قاعدة البيانات، أو باستخدام الشفرة الصحيحة الخاصة بشخص آخر مأذون له بالدخول.

بالتالي فإن فعل الدخول في هذه الجريمة التقنية عبارة عن نشاط مختلط يجمع بين المادية والتقنية، التي تعتبر أمر ضروري في هذا النوع من الجرائم، والتي يعتمد عليها الهكر في كسر القيود التقنية والدخول إلى النظام المعلوماتي بشكل غير مشروع، وذلك باستخدام الحوسبة والرقمية بشكل مغاير لما هو دارج عليه عامة مستخدمي تقنية المعلومات[1].

من هنا تظهر أهمية بل ضرورة الحاجة إلى النشاط التقني في كل الأحوال للدخول إلى النظام المعلوماتي، سواءً كان القصد من الدخول ارتكاب جريمة أو مجرد التصفح[2].

لذلك لا تقوم هذه الجريمة مثل غيرها من جرائم الدخول إلى النظام المعلوماتي دون إتيان نشاط تقني، لذا فإن استخدام الحاسب الآلي جزءً من النشاط المادي، وهما لازمان لتكوين النشاط المادي المكون لجريمة الدخول غير المشروع بقصد الحصول على البيانات الحكومية، أو الحصول على المعلومات السرية الخاصة بالمنشأة المالية، أو التجارية، أو الاقتصادية .

وقد سبق وأن ذكرنا في هذه الدراسة بأن جريمة الدخول غير المشروع إلى النظام المعلوماتي تتحقق بمجرد الدخول غير المشروع إلى النظام، وكذلك في هذه الجريمة فإنها تتحقق بمجرد الدخول إلى النظام المعلوماتي بوجه غير مشروع، إذ لم يشترط القانون لقيامها الحصول الفعلي على البيانات الحكومية أو المعلومات السرية[3].

لذا فإن هذه الجريمة تعتبر جريمة تامة متى ما كان القصد من الدخول الغير مشروع هو الحصول على البيانات الحكومية أو المعلومات السرية، وهناك رأي قانوني ينتقد هذا الاتجاه

---

[1]- المستشار د. ربيع محمود الصغير - مرجع سابق – ص 342.
[2]- المرجع السابق – ص 343.
[3]- المستشار علاء فكري اباظة – مرجع سابق – ص 54.

التشريعي[1]، ويرى أن يتم تعديل صياغة نص هذه المادة، وأن يشترط النص الحصول الفعلي على هذه البيانات والمعلومات السرية كي تقوم الجريمة.

يُدَعِّم الرأي الفقهي وجهة نظره بقوله أنها تحقق فائدتين: الأولى فهي أن هذا التعديل يتفق مع المنطق القانوني العقابي الصحيح، أما الثانية أن الشروع في ارتكاب هذه الجريمة أمر قائم بحسبان أنها تعتبر جناية، وفي واقع الأمر فإن الشروع يستغرق الجريمة الحالية[2]، لذا لابد من تعديل صياغتها بأن يشترط فيها تحقيق نتيجة إجرامية وهي الحصول على البيانات الحكومية أو المعلومات السرية.

ثانياً: علاقة السببية

يقصد بعلاقة السببية أن النشاط الإجرامي هو الذي تسبب في حدوث النتيجة[3]، وهي أحد عناصر الركن المادي، وهي العنصر الثاني للركن المادي[4]، والمستقر عليه الفقه وكأصل عام أن علاقة السببية ذات طبيعة مادية، حيث أن المشرع لا يستطيع ان يحدد السببية وكذلك هي لا تقع ضمن الافتراضات القانونية، لأنها ليست علاقة قانونية وإنما هي علاقة مادية[5].

قرر المشرع في الفقرة الأولى من المادة الرابعة من المرسوم اتحادي بقانون رقم (5) لسنة 2012 أن يكون الدخول غير مصرح به بقصد ارتكاب جريمة أخرى، وهي إما الحصول على بيانات حكومية أو الحصول على معلومات سرية تخص منشأة مالية أو تجارية أو اقتصادية، ويبين من هذه الصورة أن تكون هناك جريمة أولى وهي الدخول غير المصرح به، وأن تلحق بهذه الجريمة جريمة أخرى.

---

[1]– المرجع السابق – ص56.
[2]– المرجع السابق – ص56.
[3]- المستشار د. ربيع محمود الصغير - مرجع سابق – ص 345.
[4]- د. غنام محمد غنام - شرح قانون العقوبات الاتحادي – مرجع سابق – ص 145.
[5]- المستشار د. ربيع محمود الصغير - مرجع سابق – ص 345.

مما يترتب عليه من الضرورة توافر علاقة السببية بين الجريمة الأولى والثانية، وتتصف علاقة السببية أنها ذات طبيعة مادية، وبالنظر إلى النشاط التقني الذي يمارسه الجاني على نحو تكون فيه الجريمة الثانية هي النتيجة للجريمة الأولى[1].

الفرع الثاني: عدم وجود تصريح

يتحقق في هذه الجريمة ما سبق وأن أشرنا إليه سابقاً من أن الفرض في هذه الجريمة أن الجاني ليس له الحق في الدخول إلى النظام المعلوماتي إلاّ بتصريح، ويترتب على هذا الفرض ضرورة تحديد من هو الشخص الذي له الحق في الدخول، ومن الذي يملك الحق في التصريح لدخول النظام، إذ أن عدم وجود التصريح يعني عدم مشروعية دخول الجاني للنظام المعلوماتي، لعدم تمتعه بسلطة تمكنه وتعطيه الحق في الدخول، كل ذلك مع علمه بأنه ليس لديه الحق في الدخول[2].

يلاحظ ان الدخول في النظام بدون تصريح المنصوص عليه في هذه المادة ليس دخولاً مجرداً كما هو في المادتين الثانية والثالثة السابقتين لهذه المادة، وإنما هو دخول بدون تصريح بهدف تحقيق غرض من الغرضين الواردين في النص القانوني، إذ أنه وحتى يتم تطبيق العقاب المقرر لهذه الجريمة يجب أن يقترن الدخول بقصد الحصول على البيانات الحكومية أو بقصد الحصول على المعلومات السرية الخاصة بالمنشأة المالية أو التجارية أو الاقتصادية[3].

كما يلاحظ أن المشرع في الفقرة الأولى من المادة الرابعة من المرسوم اتحادي بقانون رقم (5) لسنة 2012، قصر تجريم الدخول غير المشروع للنظام المعلوماتي على الصورة الأولى الواردة في المادة الثانية من المرسوم اتحادي بقانون رقم (5) وهي الدخول بدون تصريح، ولم

---

[1]- د.أشرف توفيق شمس الدين، مرجع سابق، ص 149.
[2]- د.عبد الرازق الموافي عبداللطيف – مرجع سابق – ص 19.
[3]- المستشار علاء فكري اباظة – مرجع سابق – ص 53.

يتطرق في المادة الرابعة إلى صور الركن المادي الأخرى المتمثلة في تجاوز حدود التصريح، أو البقاء في النظام من غير تصريح.

إذن صورة الركن المادي لهذه الجريمة هو صورة واحدة وهي الدخول للنظام المعلوماتي دون ترخيص بقصد الحصول على البيانات الحكومية أو الحصول على معلومات سرية تخص المنشأة المالية أو التجارية أو الإقتصادية، ولعل اقتصار فعل الدخول على صورة واحدة ذلك يرجع إلى الأسباب الآتية:

1- أن الحماية التي فرضتها الفقرة الأولى من المادة الرابعة من المرسوم اتحادي بقانون رقم (5) لسنة 2012 ليست للنظام المعلوماتي في حد ذاته، وإنما هي حماية للبيانات الحكومية والمعلومات السرية الخاصة بالمنشآت المالية والتجارية والاقتصادية.

2- أن البقاء في النظام المعلوماتي بدون ترخيص أو تجاوز حدود الترخيص، هما صورتان يسبقهما دخول صحيح للنظام أو غير صحيح، بمعنى أن الجاني قد لا يكون له الصلاحية في الدخول إلى النظام، أو قد يكون مصرحاً له الدخول إلى النظام ابتداءً، وبالتالي فإنه يكون مطلعاً على البيانات الحكومية أو الأسرار الخاصة بالمنشأة المالية أو التجارية أو الاقتصادية.

3- إن التشديد في عقوبة هذه الجريمة الذي جعل وصفها بالجناية يستلزم أن يرتقي السلوك الإجرامي للجاني إلى مرحلة الخطورة، وبالتالي لا يمكن أن نساوي الأشخاص الذين يملكون الحق في دخول النظام ولكنهم خالفوا حدود الرخصة، بالأشخاص الدخلاء الذين لا يملكون ترخيصاً بالدخول إلى النظام المعلوماتي وعلى الرغم من ذلك قاموا بانتهاك خصوصيته ودخلوا إليه بطريقة غير مشروعة قاصدين الحصول على البيانات الحكومية، أو المعلومات السرية الخاصة بالمنشأة المالية أو التجارية أو الاقتصادية.

المطلب الثالث: الركن المعنوي

يأخذ الركن المعنوي لهذه الجريمة صورة العمد وقوامه القصد الجنائي، حيث أن العمد ينطوي على خطورة إجرامية أكبر، وتستلزم هذه الجريمة بالإضافة الى القصد العام قصداً خاصاً، وهو قصد الحصول على بيانات حكومية، أو قصد الحصول على معلومات سرية خاصة بمنشأة مالية او تجارية او اقتصادية[1].

يلزم لقيام القصد العام توافر عنصرين هما العلم والإرادة، والعلم يعني أن الجاني يعلم بأنه يدخل موقع الكتروني أو نظام معلومات إلكتروني، أو شبكة معلوماتية، أو وسيلة تنقية معلومات، وكذلك يجب علمه بأن دخوله للنظام المعلوماتي يتم بدون تصريح، ويعد استخدام الجاني لوسائل خداعية لتحقيق الدخول غير المشروع أو استخدامه لأسلوب تقني لكسر الشفرة قرينة على توافر القصد الجنائي[2].

بناءً عليه نتناول القصد الجنائي لهذه الجريمة في فرعين نخصص الأول للقصد الجنائي العام، والفرع الثاني لدراسة القصد الجنائي الخاص وذلك على النحو التالي:

الفرع الأول: القصد الجنائي العام

سبق وأن أشرنا إلى أن القصد الجنائي هو اتجاه إرادة الجاني إلى النشاط الإجرامي الذي باشره وإلى تحقيق النتيجة المترتبة عليه مع علمه بجميع العناصر التي يشترطها النظام لقيام الجريمة[3]، وأنه لا يكفي أن يكون الجاني عالماً بالركن المادي للجريمة، بل يلزم أن يكون مريداً[4]

---

[1]- د.عبد الرازق الموافي عبداللطيف – مرجع سابق – ص 40.
[2]- د. محمود أحمد طه – مرجع سابق – ص 33.
[3]- د.هدى حامد قشقوش - جرائم الحاسب الالكتروني في التشريع المقارن – مرجع سابق – ص 191.
[4]- راجع المبحث الأول – المطلب الثالث من البحث - ص (31).

تحقيق تلك النتيجة[1]، فلا يتوافر القصد الجنائي إلاّ إذا كان المتهم يريد تحقيق النشاط، وكذلك تحقيق النتيجة، وهذا ما يفرق الجرائم العمدية عن الجرائم غير العمدية[2].

القصد الجنائي هو اتجاه إرادة الجاني إلى مخالفة القانون الجنائي، أي أنه هو الإرادة الإجرامية التي بدونها لا يتحقق الأذناب أو الاسناد المعنوي في الجرائم العمدية، ويتطلب القصد أن يكون الجاني عالماً بماهية الواقعة الإجرامية سواء من حيث الواقع أو من حيث القانون لها، وقد استقر الفقه والقضاء على أن القصد الجنائي يقوم على عنصرين هما العلم والإرادة[3].

يأخذ الركن المعنوي لهذه الجريمة صورة العمد وقوامه القصد الجنائي، بمعنى أن يأتي الجاني نشاطه التقني الإجرامي وهو عالماً بأنه يدخل إلى نظام معلوماتي غير مصرح له الدخول إليه، وأن تتجه إرادته إلى هذا الدخول[4]، وأن يقصد من هذا النشاط التقني الحصول على البيانات الحكومية أو المعلومات السرية الخاصة بالمنشأة المالية أو التجارية أو الاقتصادية.

لذا فإن هذه الجريمة تستلزم لقيامها القصد العام وتوافر عنصرين هما العلم والإرادة، فالعلم يعني أن ينصرف علم الجاني إلى كافة العناصر الأساسية التي يقوم عليها كيان الجريمة[5]، أما الإرادة فتعني أن تتجه إرادة الجاني إلى الدخول والحصول على المعلومات الحكومية أو المعلومات السرية الخاصة بالمنشآت المالية أو التجارية أو الاقتصادية، ويؤخذ كقرينة على توفر العمد أن يستخدم الجاني من الوسائل الاحتيالية ما يمكنه من الدخول غير المشروع إلى النظام المعلوماتي.

---

[1]- د.رضا محمد عيسى – مرجع سابق – ص 54.

[2]- د.غنام محمد غنام – مرجع سابق- ص 169، وفي نفس المعنى راجع د. هدى حامد قشقوش - شرح قانون العقوبات القسم العام – مرجع سابق - ص 112.

[3]- المستشار د. ربيع محمود الصغير - مرجع سابق – ص 380.

[4]- د.أشرف توفيق شمس الدين، مرجع سابق، ص 147.

[5]- د.محمود نجيب حسني، شرح قانون العقوبات - مرجع سابق – ص 583.

أولاً: العلم

يُعرّف العِلم بأنه أحد عنصري القصد الجنائي، وينصرف معناه إلى الواقعة الإجرامية، وإلى تكييف الفعل ذاته، فيجب أن يكون الجاني على علم تام بالجريمة التي يرتكبها، بكل عناصرها التي يحددها النص القانوني، وهذه العناصر إما أن تكون عناصر واقعية أو عناصر قانونية[1].

فالعلم يعني أن ينصرف علم الجاني إلى كافة العناصر الأساسية التي يقوم عليها كيان الجريمة[2]، أي ماديات الجريمة الواردة بالنص القانوني، وهو علم مفترض بأن هذه الأفعال تُعد جريمة، إذ لا يعتد بالجهل بالقاعدة القانونية[3]، بمعنى أن يأتي الجاني نشاطه التقني الإجرامي وهو عالماً بأنه يدخل إلى النظام المعلوماتي الغير مصرح له الدخول إليه[4]، أي أن الجاني يعلم بأنه يدخل موقع الكتروني، أو نظام معلومات إلكتروني، أو شبكة معلوماتية، أو وسيلة تنقية معلومات، وكذلك يجب علمه بأن دخوله للنظام المعلوماتي يتم بدون تصريح[5].

كما يجب أن يعلم الجاني بالوقائع التي تُعد عنصراً في الجريمة، ومن ذلك العلم بمحل الجريمة، فلا تقوم الجريمة في حالة اعتقاد الجاني أنه يقوم بعمليات حسابية من خلال الحاسب الآلي، ولا يعلم انه يدخل في موقع إلكتروني، أو نظام معلومات إلكتروني، أو شبكة معلوماتية، أو وسيلة تقنية معلومات بما تحويه من بيانات ومعلومات، وذلك متى كان اعتقاده مبنياً على مبررات معقولة[6].

ويلزم ان يعلم الجاني بخطورة سلوكه على المحل الذي يقع عليه الاعتداء فلا يتوافر القصد الجنائي إذا انتفى هذا العلم، وأن يعلم أن دخوله يعد اعتداء، كأن يأتي فعل الدخول وهو

---

[1]- د.هدى حامد قشقوش - جرائم الحاسب الالكتروني في التشريع المقارن – مرجع سابق – ص 192.
[2] د.محمود نجيب حسني، شرح قانون العقوبات - مرجع سابق – ص 583.
[3]- القاضي جلال محمد الزعبي والقاضي أسامة أحمد المناعسة – مرجع سابق – ص 56.
[4]- د.أشرف توفيق شمس الدين – الحماية الجنائية للمستند الالكتروني – دراسة مقارنة ط1 – دار النهضة العربية – سنة 2006 – ص 147.
[5]- د.عبد الرازق الموافي عبداللطيف – مرجع سابق – ص 39.
[6]– المرجع السابق – ص 40.

يعتقد أنه لا يمس الحق او المصلحة محل الحماية الجنائية[1]، بالإضافة إلى ذلك يجب ان تتجه إرادة الجاني الى فعل دخول النظام المعلوماتي وان يقصد الحصول على بيانات حكومية أو معلومات سرية تخص منشأة مالية أو تجارية أو اقتصادية.

ثانياً: الإرادة

الإرادة هي العنصر الثاني للقصد الجنائي وبدونها ينتفي القصد الجنائي، وهي عبارة عن قوة نفسية أو نشاط نفسي يوجه كل أعضاء الجسم أو بعضها نحو تحقيق هدف معين غير مشروع[2]، وهي أهم ما يميز الإنسان عن غيره من المخلوقات، والإرادة يعبر عنها الإنسان بسلوكه الخارجي ولكي تكون غير معيبة يجب أن تصدر عن وعي وإدراك وهي بذلك توجه أعضاء الجسم للسلوك وتسيطر عليه[3].

سبق وأن أوضحنا أن الإرادة تتكون من عنصرين الأول هو إرادة النشاط، والثاني هو إرادة النتيجة وتعني أن الجاني اتجهت إرادته إلى تحقيق النتيجة، وتعتبر إرادة النتيجة هي العنصر الهام، وهي التي تفرق بين الجريمة العمدية والجريمة الغير عمدية[4]، ويلاحظ أنه يصعب في كثير من الاحيان معرفة عما إذا كان الدخول للنظام المعلوماتي قد تم عمداً أو أنه تم عن طريق الخطأ، وهذه مسألة موضوعية لا تحسم إلاّ بواسطة الخبراء.

إذ لا يكفي أن يعلم الجاني بأنه يدخل الى نظام معلوماتي لا يجوز له الدخول فيه، وإنما يجب بالإضافة إلى ذلك أن تتجه ارادته إلى ذلك الدخول، ويعد استخدام المتهم وسائل خداعية في

---

[1]- المرجع السابق – ص 41.
[2]- القاضي جلال محمد الزعبي والقاضي أسامة أحمد المناعسة – مرجع سابق – ص 57.
[3]- د.هدى حامد قشقوش - جرائم الحاسب الالكتروني في التشريع المقارن – مرجع سابق – ص 197.
[4]- تنص المادة (38) من قانون العقوبات الاتحادي لسنة 1987 وتعديلاته على أن: (..... يتوفر العمد باتجاه إرادة الجاني إلى ارتكاب فعل أو الامتناع عن فعل متى كان هذا الارتكاب أو الامتناع مجرما قانونا وذلك بقصد إحداث نتيجة مباشرة أو أية نتيجة أخرى مجرمة قانونا يكون الجاني قد توقعها).

تحقيق الدخول في النظام قرينة على توافر القصد الجنائي في حقه، ويتحقق ذلك اذا كان الدخول على النظام يتطلب شفرة أو بطاقة معينة، فقام الجاني بسرقة هذه البطاقة أو بكسر هذه الشفرة[1].

الفرع الثاني: القصد الجنائي الخاص

القصد الجنائي الخاص هو اتجاه نية الجاني إلى تحقيق غاية معينة من وراء ارتكاب الجريمة، وهذا النوع من القصد في حقيقته ما هو إلاّ باعثاً معين يتوافر لدى الجاني[2]، أو هو تعمد إحداث نتيجة معينة يعاقب عليها القانون الجنائي[3]، فالقصد الخاص يشترط فيه المشرع وجود عنصراً إضافياً على عنصري العلم والارادة، هذا العنصر الإضافي هو النية الخاصة[4]، إذ يستلزم المشرع في بعض الجرائم توافر هذا النوع من القصد لوقوع الجريمة، فيلزم أن تنصرف نية الجاني من وراء الركن المادي إلى تحقيق هدف معين[5].

كما قدمنا في بداية هذا المبحث فإنه يلزم في هذه الجريمة توافر القصد الخاص، الذي يتمثل في قصد الجاني الحصول على بيانات حكومية، أو قصد الحصول على معلومات سرية خاصة بالمنشأة المالية أو التجارية أو الاقتصادية، ولا عبرة بالسرية بالنسبة للبيانات الحكومية، بل يكفي أن يقصد الحصول على بيانات حكومية، لذا فإن القصد الجنائي لهذه الجريمة ينتفي إذا كان الجاني يعتقد أن البيانات لا تخص الحكومة، أو كان يعتقد أن هذه البيانات متاحة للجمهور وذلك متى كان اعتقاده مبنياً على مبررات مقبولة ومعقولة، ويجب ان تتجه ارادة الجاني الى فعل الدخول وارادة الحصول على المعلومات[6].

وحتى يتم تطبيق العقاب المقرر لهذه الجريمة، لابد أن يقترن الدخول إلى النظام المعلوماتي بقصد الحصول على أحد أمرين، إما البيانات الحكومية أو بقصد الحصول على

---

[1] - د.محمود أحمد طه – مرجع سابق – ص 33.
[2]- د.غنام محمد غنام - شرح قانون العقوبات الاتحادي لدولة الإمارات العربية المتحدة – مرجع سابق – ص 174.
[3]- المستشار د. ربيع محمود الصغير - مرجع سابق – ص 187.
[4]- د.هدى حامد قشقوش - شرح قانون العقوبات القسم العام – مرجع سابق - ص 198.
[5]- د.غنام محمد غنام - شرح قانون العقوبات الاتحادي لدولة الإمارات العربية المتحدة – مرجع سابق – ص 174
[6]- د.عبد الرازق الموافي عبداللطيف – مرجع سابق – ص 41.

المعلومات السرية الخاصة بالمنشأة المالية أو التجارية أو الاقتصادية[1]، بمعنى أن الجاني عندما دخل إلى النظام المعلوماتي كان يقصد من وراء ذلك الحصول على البيانات الحكومية.

ولا شك أن تشديد العقوبة في هذه المادة يرتبط بالقصد الجنائي الخاص، إذ أن توافر القصد الجنائي الخاص غير من وصف جريمة الدخول الغير مشروع على النظام المعلوماتي، من جنحة يعاقب عليها بالحبس والغرامة إلى جناية يعاقب عليها بالسجن المؤقت والغرامة، وذلك لأهمية البيانات الحكومية، وتعلقها بالأمن القومي أو الاقتصاد القومي أو المصالح العليا للدولة[2]، وكذلك البيانات السرية الخاصة بالمنشآت المالية أو التجارية أو الاقتصادية.

[1]- المستشار علاء فكري اباظة – مرجع سابق – ص 53.
[2]- د.محمود أحمد طه – مرجع سابق – ص 24.

الفصل الثاني: العقوبات والتدابير المقررة لجرائم الدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات الإلكترونية

نتناول في هذا الفصل العقوبات والتدابير المقررة لجرائم الدخول غير المشروع إلى النظام المعلوماتي، حيث نفرد المبحث الأول لاستعراض ودراسة العقوبات المقررة لجريمة الدخول غير المشروع إلى النظام المعلوماتي في صورتها المجردة، وذلك في مطلبين، حيث نتناول في المطلب الأول العقوبات البسيطة المقررة لهذه الجريمة، ثم نتناول في المطلب الثاني الظروف المشددة لعقوبة هذه الجريمة وذلك عندما يكون الدخول غير المشروع إلى النظام المعلوماتي بقصد الإضرار بالبيانات أو المعلومات الشخصية أو غير الشخصية، أو عندما يكون قصد الإضرار بالبيانات بمناسبة أو بسبب تأدية العمل.

ثم نتناول في المبحث الثاني العقوبات المقررة لجريمة الدخول بدون تصريح إلى النظام المعلوماتي بقصد الحصول على بيانات حكومية أو معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية، وذلك في مطلبين، نخصص الاول منهما لدراسة العقوبات البسيطة المقررة لهذه الجريمة، ثم نتناول في المطلب الثاني الظروف المشددة لعقوبة هذه الجريمة، ونوضح من خلال هذا المطلب كيف أن المشرع الوطني تدرج في العقوبة على هذه الجريمة.

ثم نتناول في المبحث الثالث التدابير المقررة لجرائم الدخول غير المشروع إلى النظام المعلوماتي في ثلاثة مطالب نخصص الأول لوضع المحكوم عليه تحت الإشراف أو المراقبة، ثم المطلب الثاني لدراسة تدبير حرمان المحكوم عليه من استخدام أي شبكة معلوماتية أو نظام المعلومات الالكتروني أو أي وسيلة تقنية معلومات أخرى، أو وضع المحكوم عليه في مأوى علاجي أو مركز تأهيل، وفي المطلب الثالث نتناول إبعاد المحكوم عليه الأجنبي عن الدولة.

المبحث الأول: العقوبات المقررة لجريمة الدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات الإلكترونية

يكاد أن يُجمِع الفقه على تعريف العقوبة (punishment) بأنها الجزاء الذي يقرره القانون[1]، إذ الأصل أن وقوع الجريمة من شأنه أن يرتب مسؤولية جزائية على عاتق مرتكبها تجعله محلاً للعقاب في حال ثبوتها، فالعقوبة هي رد الفعل الاجتماعي على الجريمة التي وقعت.

يختص القاضي بتوقيع هذا الجزاء بمقتضى حكم صادر من محكمة مختصة على شخص تثبت مسئوليته عن الجريمة[2]، فكون العقوبة جزاء يجب أن تنطوي على إيلام وإيذاء لمن تنزل به ابتغاء تحقيق أغراض العقوبة[3] ويتحقق الإيلام عن طريق المساس بحق من حقوق من توقع عليه العقوبة نظير مخالفته نصوص القانون[4].

تتميز العقوبة بخصائص عدة، تميزها عن التدابير المانعة للجريمة[5]، والجزاءات الأخرى المدنية والتأديبية التي قد تشابهها[6]، ويمكن إجمال هذه المميزات في أن العقوبة شخصية[7]، ولا توقع إلاّ على المحكوم عليه ولا ترتب آثارها على سواه[8]، وهي محددة مسبقاً قبل وقوع الجريمة،

---

[1]- د.هدى حامد قشقوش – شرح قانون العقوبات القسم العام – مرجع سابق – ص 372.

[2]- د.محمود محمد مصطفى – شرح قانون العقوبات – القسم العام – دار النهضة العربية القاهرة 1983 - ص 555

[3]- د.محمود نجيب حسني – شرح قانون العقوبات – مرجع سابق – ص808.

[4]- المرجع السابق – ص723.

[5]- يعرف د.غنام محمد غنام في صفحة 318 من مؤلفه شرح قانون العقوبات الاتحادي - مرجع سابق - التدبير الجنائي بأنه جزاء على ارتكاب جريمة يرمي إلى معالجة خطورة إجرامية في الفاعل بالنسبة للمستقبل وتوقي عودته إلى الإجرام.

[6]- د. رمسيس بهنام - النظرية العامة للقانون الجنائي – دار النهضة العربية 1971 – ص 1088.

[7]- وفي ذلك تنص المادة 28من دستور دولة الإمارات لسنة 1971 بأن: (العقوبة شخصية، والمتهم برئ حتى تثبت إدانته في محاكم قانونية وعادلة، وللمتهم الحق في أن يوكل من يملك القدرة للدفاع عنه أثناء المحاكمة، ويبين القانون الأحوال التي يتعين فيها حضور محام عن المتهم، وإيذاء المتهم جسمانياً أو معنوياً محظور)

[8]- د.هدى حامد قشقوش – شرح قانون العقوبات القسم العام – مرجع سابق – ص 374.

ومنصوص عليها وفقاً لمبدأ الشرعية[1]، وأنها قضائية فالقاضي هو الشخص الوحيد الذي يوثق في حرصه على الحريات والعدالة وابتعاده عن الأهواء السياسية[2]، ومتساوية لجميع أفراد المجتمع.

يتعين أن يكون الجزاء مقابلاً للجريمة، فلا عقوبة ما لم ترتكب جريمة تنشأ المسئولية عنها، ولا بد أن يكون هناك تناسباً بين العقوبة والجريمة تحقيقاً لشرط العدالة في تطبيقها، والتناسب بين العقوبة والجريمة لابد أن يتحقق من وجهة مزدوجة، بأن تتناسب العقوبة مع كافة ماديات الجريمة ومع مقدار الخطيئة فيها[3].

تنطبق قاعدة التناسب بين الجريمة والعقوبة التي أشرنا إليها على ما حدث من تطور تشريعي في العقوبة في جرائم تقنية المعلومات في دولة الإمارات العربية المتحدة بصفة عامة، وجريمة الدخول غير المشرع إلى النظام المعلوماتي بصفة خاصة، حيث كان القانون الاتحادي رقم (2) لسنة 2006 (الملغي) يعاقب على هذه الجريمة بالحبس والغرامة أو بإحدى العقوبتين.

فإذا ترتب على فعل الدخول العبث بالموقع أو المعلومات فيعاقب بالحبس مدة لا تقل عن ستة أشهر والغرامة أو بإحدى العقوبتين، أما إذا كانت البيانات أو المعلومات شخصية فتكون العقوبة الحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن عشرة آلاف درهم أو بإحدى العقوبتين.

ولخطورة جرائم تقنية المعلومات واتساع مجالها في التأثير على مختلف فئات المجتمع، لا سيما في ظل الإقبال على استخدام وسائل التواصل الاجتماعي في الدولة، خاصةً وأن إحصائيات الهيئة العامة للاتصالات أثبتت أنه في نهاية فبراير 2012 وصل عدد مستخدمي الهواتف

---

[1]- تنص المادة (27) من دستور دولة الإمارات العربية المتحدة لسنة 1971: (يحدد القانون الجرائم والعقوبات، ولا عقوبة على ما تم من فعل أو ترك قبل صدور القانون الذي ينص عليها)

[2]- د.محمود نجيب حسني – مرجع سابق – ص728.

[3]- د.هدى حامد قشقوش – شرح قانون العقوبات القسم العام – مرجع سابق – ص 372.

المتحركة في الدولة عدد 18.590.811 مشترك، وعدد مشتركي الانترنت على الخطوط الثابتة 2.225.989 مشترك[1].

بالإضافة إلى ذلك فإن دولة الإمارات تحتل المركز الأول عربياً في استخدام (فيس بوك)، حيث يصل عدد المستخدمين عدد 3.000.000 مستخدم، تشكل الفئة العمرية 18 إلى 34 سنة نسبة 68٪ منهم، فيما اقترب عدد مشتركي (بلاك بيري) في الدولة من مليون مشترك في عام 2011، تبادلوا أكثر من أربعة أمثال الرسائل التي تبادلها جميع مشتركي الهواتف المتحركة الأخرى في الدولة خلال نفس العام[2].

من هذا الواقع ولِما تشكل لدى المشرع من قناعات عن خطورة جرائم تقنية المعلومات فقد اتجه إلى تشديد العقوبة عليها حتى تتناسب مع مستوى التأثير السلبي لهذه الجرائم على الفرد والمجتمع فقد جاء إصدار المرسوم اتحادي بقانون رقم (5) لسنة 2012 ليسهم في تطبيق آليات التعامل الصحيح مع وسائل الاتصال الحديثة، الآخذة في الانتشار بسرعة كبيرة، ومحاصرة الآثار السلبية لوسائل تقنية المعلومات والحد من تضاعفها.

المطلب الأول: العقوبات البسيطة

العقوبات البسيطة هي العقوبات التي يقررها القانون دون ظروف مشددة، وهي متنوعة وتختلف فيما بينها من حيث مقدار جسامتها وطبيعتها ومدتها ومدى أهميتها كجزاء للجريمة، وأهم تقسيمات العقوبات هو تقسيمها إلى عقوبات جنايات وعقوبات جنح وعقوبات مخالفات[3].

---

[1]- تقرير منشور على موقع هيئة تنظيم الاتصالات على الرابط https://www.tra.gov.ae

[2]- العميد د. صلاح عبيد الغول السلامي – مدير مكتب ثقافة احترام القانون بوزارة الداخلية – الندوة التي أقامتها مؤسسة الإمارات للاتصالات -https://www.emaratalyoum.com/local-section/accidents/2012-06-05-1.489614

[3]- د.محمود نجيب حسني – شرح قانون العقوبات – القسم العام ط4 – مرجع سابق – ص 738.

إلاّ أن التقسيم الأساسي الذي يكفل التمييز بين أنواع العقوبات بمختلف أحكامها القانونية هو تقسيمها إلى عقوبات أصلية وأخرى تبعية أو تكميلية، وأن أساس هذا التقسيم هو الاختلاف بين العقوبات من حيث كفايتها لتحقيق معنى الجزاء المقابل للجريمة[1].

العقوبات الأصلية بعضها يمس جسد الإنسان أو حريته أو ذمته المالية، أما التبعية أو التكميلية وهي تطبق تبعاً للحكم بعقوبة أصلية[2]، ويعتمد هذا التقسيم الأخير على كون العقوبة كافية بذاتها لتحقيق الهدف المقصود منها بأنها تكون الجزاء الوحيد الذي يوقعه القاضي[3].

نص المرسوم اتحادي بقانون رقم (5) لسنة 2012 في المادة (2) منه على عقوبة جريمة الدخول غير المشروع إلى النظام المعلوماتي في صورتها المجردة بالحبس والغرامة، ويلاحظ أنه تدرج في تنزيل هاتين العقوبتين بحسب تدرج واختلاف النشاط المكون للجريمة، ويتضح ذلك من خلال الآتي:

1- عقوبة الحبس والغرامة التي لا تقل عن 100.000 درهم ولا تزيد على 300.000 درهم أو بإحدى العقوبتين في حال الدخول غير المشروع إلى النظام المعلوماتي.

2- عقوبة الحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن مائة وخمسين ألف درهم ولا تجاوز سبعمائة وخمسون ألف درهم أو بإحدى العقوبتين، إذا ترتب على فعل الدخول أو البقاء أي نشاط أدى إلى إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أي بيانات أو معلومات .

3- عقوبة الحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين إذا كانت البيانات أو المعلومات محل الأفعال الواردة في الفقرة أعلاه بيانات أو معلومات شخصية .

---

[1]- المرجع السابق – ص 746.
[2]- د.هدى حامد قشقوش – شرح قانون العقوبات القسم العام – مرجع سابق – ص 386.
[3]– المرجع السابق – ص 387.

الفرع الأول: العقوبات الأصلية

العقوبات الأصلية هي الجزاء الأساسي للجريمة، ولا توقع العقوبة الأصلية إلاّ إذا نطق بها قاضي وحدد نوعها ومقدارها[1]، وتختلف العقوبات الأصلية فيما بينها من حيث طبيعتها والأحكام التي يخص بها القانون كلاً منها تبعاً لاختلافها في نوع الحق الذي تمسه وتحقق الإيلام المقصود عن طريق المساس به، فثمة عقوبات بدنية مثل الإعدام، وعقوبات ماسة بالحرية مثل الحبس والسجن، وعقوبات مالية مثل الغرامة[2].

تنص المادة (66) من قانون العقوبات الاتحادي لدولة الإمارات العربية المتحدة لسنة 1987 المعدل على أن العقوبة الأصلية هي: أ- عقوبات الحدود والقصاص والدية، ب- عقوبات تعزيرية وهي: 1- الإعدام 2- السجن المؤبد 3- السجن المؤقت 4- الحبس 5-الحجز 6-الغرامة[3].

قررت الفقرة الأولى من المادة (2) من المرسوم اتحادي بقانون رقم (5) لسنة 2012 عقوبة جريمة الدخول غير المشروع إلى النظام المعلوماتي في صورتها المجردة بالحبس والغرامة[4]، ولم يحدد المرسوم الاتحادي مدة الحبس وبالتالي ترك أمر تحديدها[5] وفقاً للقواعد

---

[1]- عرفت محكمة النقض المصرية العقوبة الأصلية بأنها (تستمد وصفها من أنها تكون العقاب الأصلي أو الأساسي المباشر للجريمة والتي توقع منفردة بغير أن يكون القضاء بها معلقاً على الحكم بعقوبة أخرى)، راجع في ذلك نقض 17 مارس سنة 1959 مجموعة أحكام محكمة النقض س 10 رقم 73 ص 328، وراجع في نفس المعنى د. محمود نجيب حسني – شرح قانون العقوبات – القسم العام ط4 – مرجع سابق – ص 743.

[2]- د.محمود نجيب حسني – المرجع السابق – ص 747.

[3]- الغرامة هي العقوبة المالية الأصلية الوحيدة التي يقررها القانون، وهي إلزام المحكوم عليه بدفع مبلغ من المال إلى خزينة الدولة، ويحدد الحكم القضائي المبلغ المحكوم به، أنظر في نفس المعنى د. السعيد مصطفى السعيد – الأحكام العامة في قانون العقوبات – 1962 – ص 660.

[4]- جاء نص الفقرة على النحو الآتي: (يعاقب بالحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تزيد على ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين كل من دخل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات، أو وسيلة تقنية معلومات، بدون تصريح أو بتجاوز حدود التصريح، أو بالبقاء فيه بصورة غير مشروعة)

[5]- د.عبد الرازق الموافي عبد اللطيف – مرجع سابق– ص 25.

العامة المنصوص عليها في المادة (69) من قانون العقوبات الاتحادي المعدل[1]، والتي تقرر أن الحد الأدنى للحبس هو شهر والحد الأقصى ثلاث سنوات[2].

أما الغرامة فقد حدد مقدارها المشرع بأن لا تقل عن 100.000 درهم ولا تزيد عن 300.000 درهم، وبذلك فقد خول المشرع المحكمة سلطة الحكم بعقوبة الحبس أو بالغرامة أو بالعقوبتين معاً، إذ يتمتع القاضي بسلطة تقديرية، فإذا قضت المحكمة بالعقوبتين كان الحبس عقوبة أصلية[3].

ويبدو من خلال هذا العرض أن جريمة الدخول غير المشروع إلى النظام المعلوماتي في صورتها المجردة تُعد من الجنح[4]، وإذا كان مجرد الولوج يمثل جريمة في حد ذاته، فإن هذه الجريمة تدخل تحت وصف الجريمة الشكلية، ذلك أن الجريمة الشكلية لا يتطلب فيها القانون حدوث نتيجة معينة، وإنما كل ما يتطلبه القانون هو مجرد القيام بسلوك أو نشاط إجرامي، فالمشرع في هذه الجرائم يكتفي لتوقيع العقاب بمجرد حدوث الحدث الإجرامي المتمثل في السلوك، مثل انتهاك مسكن أو السب والقذف[5].

بذلك ولما كانت جريمة الدخول غير المشروع إلى النظام المعلوماتي في صورتها المجردة من الجنح، كان لابد أن نشير إلى أمرين هامين: الأمر الأول هو: أنه وعلى الرغم من جريمة الدخول غير المشروع في النظام المعلوماتي في صورتها المجردة تُعد من الجنح التي يحاكم عليها بالحبس أو الغرامة أو العقوبتين معاً إلاّ أننا نلاحظ أن المشرع الوطني حدد مبلغ

---

[1]- تعرف المادة (69) من قانون العقوبات الاتحادي رقم (5) لسنة 1987 المعدل الحبس بأنه: (هو وضع المحكوم عليه في إحدى المنشآت العقابية المخصصة قانونا 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).

[2]- تقرر المادة 18 من قانون العقوبات المصري أن عقوبة الحبس لا يجوز أن تنقص عن24 ساعة، وأن لا تزيد علي ثلاث سنوات إلاّ في الأحوال الخصوصية المنصوص عليها قانونا.

[3]- د. شيماء عطا الله – الشرط المفترض في الجريمة - محاضرات منشورة على موقع الدكتورة شيما -

[4]- تنص المادة 29 من قانون العقوبات الاتحادي لسنة 1987 المعدل على أن (:الجنحة هي الجريمة المعاقب عليها بعقوبة أو أكثر من العقوبات الآتية: 1- الحبس 2- الغرامة التي تزيد على ألف درهم 3- الدية 4- الجلد .

[5]- المستشار د. ربيع محمود الصغير - القصد الجنائي في الجرائم المتعلقة بالإنترنت والمعلوماتية دراسة تطبيقية – مركز الدراسات العربية للنشر والتوزيع – ص 350.

الغرامة على مرتكب الجريمة في المادة (2) بأن لا تقل عن 100.000 درهم ولا تزيد عن 300.000 درهم.

على الرغم من أن المادة (71) من قانون العقوبات الاتحادي رقم (3) لسنة 1987 المعدل كانت تقرر وكقاعدة عامة أنه لا يجوز أن يزيد الحد الأقصى للغرامة في الجنح عن ثلاثين ألف درهم[1]، ولعل المشرع استند في تحديد الحد الأقصى للغرامة في هذه الجريمة على ما أجازه عجز نص المادة (71) السابق الإشارة اليها بعبارة (وذلك كله ما لم ينص القانون على خلافه)، ثم تلى ذلك صدور المرسوم بقانون اتحادي رقم (7) لسنة 2016 الذي عدل المادة (71) وذلك بأن أصبحت عقوبة الغرامة في الجنح لا يزيد حدها الأقصى عن 300.000 درهم[2].

الأمر الثاني هو: أنه وعلى الرغم من أن جريمة الدخول غير المشروع إلى النظام المعلوماتي في صورتها المجردة تعتبر من جرائم السلوك المجرد، إلاَّ أن الشروع فيها أمر مُتصور[3]، ويقع الشروع مثلاً عندما يقوم المتهم بتشغيل النظام دون أن يتمكن من الدخول فيه، كما أنه قد يرجع ذلك إلى أن المتهم قد تم ضبطه بعد تشغيل الجهاز وقبل أن يتمكن من فتح أي ملف من الملفات المدونة بالكمبيوتر، وقد يكون السبب في عدم تمكن المتهم من الدخول إلي الملفات بعد فتح الجهاز بسبب أن تشغيل الملفات معلقاً على استخدام كلمة سر لم يكن المتهم يعرفها[4].

لذا فإنه ولما كانت جريمة الدخول غير المشروع في النظام المعلوماتي في صورتها المجردة تُعد من الجنح، فإن المادة 40 من المرسوم اتحادي بقانون رقم (5) لسنة 2012 والتي تنص على (يعاقب على الشروع في الجنح المنصوص عليها في هذا المرسوم اتحادي بقانون

---

[1]- تنص المادة (71) من قانون العقوبات الاتحادي لسنة 1987 على أن: (الغرامة هي إلزام المحكوم عليه أن يدفع للخزينة المبلغ المحكوم به، ولا يجوز أن تقل الغرامة عن مائة درهم ولا أن يزيد حدها الأقصى على مائة ألف درهم في الجنايات وثلاثين ألف درهم في الجنح وذلك كله ما لم ينص القانون على خلافه)

[2]- جاء النص المعدل للمادة (71) من قانون العقوبات الاتحادي لسنة 1987 على النحو التالي: (عقوبة الغرامة هي إلزام المحكوم عليه أن يدفع للخزينة المبلغ المحكوم به، ولا يجوز أن تقل الغرامة عن ألف درهم ولا أن يزيد حدها الأقصى على مليون في الجنايات وثلاثمائة ألف درهم في الجنح، وذلك كله ما لم ينص القانون على خلافه)

[3]- د.محمود أحمد طه – مرجع سابق - ص 33.

[4]- المرجع السابق – ص 34.

بنصف العقوبة المقررة للجريمة التامة)، يُمكن أن تنطبق عليها في حال توافر الشروع في الجريمة وفقاً لما أشرنا إليه أعلاه، حيث تطبق نصف العقوبة المقررة للجريمة التامة.

الفرع الثاني: العقوبات الفرعية

هي تلك العقوبات التي لا يحكم بها بمفردها كعقوبة للجريمة بل إنها تضاف إلى غيرها من العقوبات الأصلية[1]، استخدم المشرع الاتحادي في قانون العقوبات تعبير العقوبات الفرعية وقسمها إلى نوعين:

أولاً: العقوبات التبعية: وهي عقوبات تتبع العقوبة الأصلية بقوة القانون، ومنها مراقبة الشرطة[2] والحرمان من بعض الحقوق والمزايا[3]، مثل الحق في الانتخاب أو الحق في عضوية المجالس التشريعية أو الاستشارية، وعضوية المجالس البلدية ومجالس إدارة الهيئات والمؤسسات العامة والجمعيات والمؤسسات ذات النفع العام، وكذلك الحرمان من الحق في عضوية مجالس إدارة شركات المساهمة، أو تولي إدارتها أو أن يكون وصياً أو قيماً أو وكيلاً عن الغير، أو أن يحمل الأوسمة الوطنية والأجنبية، أو أن يحمل السلاح، ولا يجوز أن تزيد مدة الحرمان على ثلاث سنوات من تاريخ الانتهاء من تنفيذ العقوبة، وهي عقوبات تقع بمجرد صدور الحكم بالعقوبة الأصلية دون الحاجة للنطق بها في الحكم[4].

---

[1]- د. غنام محمد غنام - شرح قانون العقوبات الاتحادي – مرجع سابق – ص 331.

[2]- تعتبر المراقبة من التدابير المقيدة للحرية التي نصت عليها المادة 110 من قانون العقوبات الاتحادي رقم (3) لسنة 1987، وقد عرفتها المادة (115) من نفس القانون بأنها: (إلزام المحكوم عليه بكل أو بعض القيود التي يقررها الحكم) فيما قررت أن القيود هي: أن لا يغير محل إقامته إلا بعد موافقة الجهة الإدارية المختصة، وأن يُقدم نفسه إلى الجهة الإدارية المختصة في الفترات الدورية التي تحددها، وأن لا يرتاد الأماكن التي حددها الحكم، وأن لا يبرح مسكنه ليلاً، إلا بإذن من الجهة الإدارية المختصة.

[3]- تنص المادة (75) من قانون العقوبات الاتحادي لسنة 1987 على: (الحكم بالسجن المؤبد أو المؤقت يستتبع بقوة القانون من وقت صدوره حرمان المحكوم عليه من كل الحقوق والمزايا الآتية: 1- أن يكون ناخبا أو عضواً في المجالس التشريعية أو الاستشارية. 2- أن يكون عضواً في المجالس البلدية أو في مجالس إدارة الهيئات أو المؤسسات العامة أو الجمعيات أو المؤسسات ذات النفع العام أو شركات المساهمة أو مديراً لها. 3- أن يكون وصياً أو قيماً أو وكيلاً 4- أن يحمل أوسمة وطنية أو أجنبية. 5- أن يحمل السلاح. ولا يجوز أن تزيد مدة الحرمان على ثلاث سنوات من تاريخ الانتهاء من تنفيذ العقوبة).

[4]- تنص المادة (73) من قانون العقوبات الاتحادي لسنة 1987 وتعديلاته على أن: (العقوبات التبعية هي 1- الحرمان من بعض الحقوق والمزايا 2- مراقبة الشرطة، وتلحق هذه العقوبة المحكوم عليه بقوة القانون دون حاجة إلى النص في الحكم وذلك على النحو المبين في هذا الفرع)

ثانياً: العقوبات التكميلية: وهي العقوبات التي تنطق بها المحكمة بالإضافة إلى العقوبة الأصلية وتتضمن الحرمان من بعض الحقوق والمزايا بصفة تكميلية[1] وكذلك المصادرة، والعقوبات التكميلية قد تكون وجوبيه وقد تكون جوازيه[2].

من واقع المرسوم اتحادي بقانون رقم (5) لسنة 2012 نجد أن العقوبات الفرعية تم النص عليها في المادة (41) من المرسوم اتحادي، حيث قررت هذه المادة حق المحكمة في أن تحكم في جميع الأحوال بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا المرسوم الاتحادي، وكذلك مصادرة الأموال المتحصلة من الجريمة.

والمصادرة عقوبة تكميلية تشمل جميع الأجهزة والبرامج والوسائل المستخدمة في ارتكاب جريمة من الجرائم الماسة بالأنظمة والمعلوماتية مع مراعاة حقوق الغير حسن النية[3]، وقد نظمت أحكام المصادرة المادة (82) من قانون العقوبات الاتحادي لسنة 1987 وتعديلاته حيث نصت على: (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)، كما قررت المادة (41) من المرسوم اتحادي بقانون رقم (5) لسنة 2012 محو المعلومات أو البيانات أو إعدامها[4]، وتجدر الإشارة إلى أن نص المادة (82) المشار إليه هو الوارد في تعديلات قانون العقوبات 2016، وبالتالي نرى أنه يجب على المحكمة أن تحكم

---

[1]- تنص المادة (80) من قانون العقوبات الاتحادي لسنة 1987 وتعديلاته على: (للمحكمة عند الحكم في جناية بالحبس أن تأمر بحرمان المحكوم عليه من حق أو مزية أو أكثر مما نص عليه في المادة (75) وذلك لمدة لا تقل عن سنة ولا تزيد على ثلاث سنوات تبدأ من نهاية تنفيذ العقوبة أو انقضائها لأي سبب أخر).

[2]- د.غنام محمد غنام - شرح قانون العقوبات الاتحادي – مرجع سابق – ص 416.

[3]- د. سعيدي سليمة، الأستاذ حجاز بلال – مرجع سابق - ص 153.

[4]- تنص المادة (41) من المرسوم اتحادي بقانون رقم (5) لسنة 2012 على أن (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 الاتحادي 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)

بغرامة تعادل قيمة أحد أجهزة الحاسب الآلي الذي تم استخدامه من قبل الجاني في جريمة الدخول غير المشروع ولم يتم ضبطه.

يلاحظ أن صياغة المادة (41) جاءت صريحة وموافقة للقواعد العامة التي أشرنا إليها في بداية هذا الفرع من أن المحكمة تنطق بالعقوبات التكميلية، وذلك بأن جاء نص المادة (41): (يحكم في جميع الأحوال بمصادرة..... أو بمحو .....، كما يحكم بإغلاق المحل أو الموقع .....).

أما بالنسبة للعقوبات التبعية الأخرى الواردة في المادة (75) من قانون العقوبات الاتحادي لسنة 1987 وتعديلاته فإن المشرع لم يتعرض إليها من قريب أو بعيد في المرسوم اتحادي بقانون رقم (5) لسنة 2012، ولعله اكتفى بأن ترجع إليها المحاكم عند الإدانة بجريمة من الجرائم الواردة فيه، مستهدياً بنصوص قانون العقوبات الاتحادي باعتباره أصلاً لجميع القوانين الجزائية الخاصة، يتم الرجوع إليه في كل ما لم يرد فيه نصاً خاصاً.

مع ملاحظة أن هذه العقوبات التبعية الأخرى لا تنطبق على جريمة الدخول غير المشروع إلى النظام المعلوماتي في شكلها المجرد، إذ أن هذه الجريمة من الجنح التي تتراوح العقوبة فيها ما بين الحبس والغرامة، علماً بأن تطبيق العقوبات التبعية الواردة في المادة (75) من قانون العقوبات الاتحادي لسنة 1987 وتعديلاته يكون تبعاً للحكم بالسجن المؤبد أو المؤقت.

الفرع الثالث: عقوبة الشخص المعنوي

مع تطور الأوضاع الاقتصادية واتساع نشاط المؤسسات والشركات في ضوء تسارع وتيرة المسيرة التنموية لدولة الامارات اقتضت الحاجة إلى شمول الشركات والمؤسسات الخاصة للمسؤولية الجزائية وفق التشريعات الجزائية بدولة الامارات، حيث نص قانون العقوبات الاتحادي في المادة رقم (65) والمعدل بمرسوم بقانون اتحادي رقم (7) لسنة 2016، والتي نصت على أن " الاشخاص الاعتبارية فيما عدا مصالح الحكومة ودوائرها الرسمية والهيئات والمؤسسات العامة،

مسؤولة جنائياً عن الجرائم التي يرتكبها ممثلوها أو مديروها أو وكلاؤها لحسابها أو باسمها. ولا يجوز الحكم عليها بغير الغرامة والمصادرة والتدابير الجنائية المقررة للجريمة قانوناً فإذا كان القانون يقرر للجريمة عقوبة أصلية غير الغرامة اقتصرت العقوبة على الغرامة التي لا تزيد حدها الأقصى على خمسمائة ألف درهم ولا يمنع ذلك من معاقبة مرتكب الجريمة شخصياً بالعقوبات المقررة لها في القانون".

في ضوء النص السابق يلاحظ أن المشرع قد حدد الأشخاص المعنوية التي لا تخضع للمسؤولية الجنائية وهي: مصالح الحكومة، الدوائر الحكومية، الهيئات والمؤسسات العامة، وبذلك تكون جميع الأشخاص المعنوية غير ما ذكر هي التي تخضع للمسؤولية الجنائية حسب مفهوم النص، وبذلك تكون الجهات المقصودة هي مؤسسات وشركات القطاع الخاص دون غيرها.

وبالاطلاع على المرسوم اتحادي بقانون رقم (5) لسنة 2012 نلاحظ المادة رقم (41) والتي نصت 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".

المطلب الثاني: الظروف المشددة للعقوبة

يسمح المشرع للمحكمة الجزائية بتشديد العقاب عن الذي يقرره النص الأصلي متى ما توافرت ظروف مشددة يقررها القانون[1]، ويقصد بالظروف المشددة مجموعة الأحوال التي إذا توافر أحدها وجب على القاضي إن جاز له أن يحكم بعقوبة أشد نوعاً أو أكبر مقداراً من الحدود

[1]- د.غنام محمد غنام - شرح قانون العقوبات الاتحادي – مرجع سابق - ص 517.

المقررة للعقاب على الجريمة أصلاً[1]، أي أنها عناصر إضافية تتعلق أحياناً بالجريمة ويقدر المشرع خطورتها فيشدد العقوبة المقررة للجريمة[2].

هذا يعني أن قضاء القاضي بالحد الأقصى المقرر أصلاً للعقاب على الجريمة أصلاً ليس تشديداً للعقاب لأنه لم يجاوز العقوبة المقررة أصلاً لا في نوعها ولا في مقدارها، وإنما الصحيح أن القاضي في مثل تلك الحالة قد أخذ المتهم بالشدة، في حدود استخدامه العادي لسلطته التقديرية[3].

بذلك فإنه لا يعتبر تشديداً للعقوبة إذا حُكِمَ على شخصٍ أُدين بجريمة الدخول غير المشروع في النظام المعلوماتي بالحد الأقصى المحدد للعقوبة، وهو الحبس ثلاث سنوات، وكذلك الحد الأقصى لعقوبة الغرامة وهو 300.000 درهم، وذلك أن الحكم لم يتعدى العقوبة الأصلية نوعاً ومقداراً.

للظروف المشددة أحوال من حيث تأثيرها على عقوبة الجريمة يقدر المجتمع أن وجودها يترتب عليه حتماً زيادة الجسامة الذاتية للجريمة منها ما هو وجوبي يستحق تشديد العقوبة وتعرف بالظروف المشددة الوجوبية مثل سبق الإصرار والترصد في جريمة القتل، ومنها ما هو جوازي بالنسبة للمحكمة، يُترك للقاضي أمر تقديرها حسب كل حالة وتعرف بالظروف المشددة الجوازية[4].

تضمن قانون العقوبات الاتحادي ظروفاً مشددة للعقوبة، بعضها ذو طبيعة عامة يمكن أن تلحق بكل الجرائم ويعتبر العود من صور الظروف المشددة العامة في الجنايات والجنح، وبعضها الآخر ظروف خاصة تتعلق بجريمة معينة مثل ظرف سبق الإصرار وظرف الترصد في جريمة القتل والضرب المفضي إلى الموت[5].

---

[1]- د.محمد زكي أبو عامر – قانون العقوبات القسم العام – الدار الجامعية بيروت 1993 – ص 447.
[2]- د.غنام محمد غنام - شرح قانون العقوبات الاتحادي – مرجع سابق - ص 518.
[3]- د.محمد زكي أبو عامر – المرجع السابق – ص 447.
[4]- المرجع السابق – ص 448.
[5]- د.غنام محمد غنام - شرح قانون العقوبات الاتحادي – مرجع سابق - ص 518.

وقد نصت المادة (102) من قانون العقوبات الاتحادي لسنة 1987 وتعديلاته على عدد من الظروف المشددة، حيث جاء نصها أنه: (مع مراعاة الأحوال التي يبين فيها القانون أسباب خاصة للتشديد يعتبر من الظروف المشددة ما يلي: أ- ارتكاب الجريمة بباعث دنيء، ب- ارتكاب الجريمة بانتهاز فرصة ضعف إدراك المجني عليه أو عجزه عن المقاومة أو في ظروف لا تمكن غيره من الدفاع عنه، ج- ارتكاب الجريمة باستعمال طرق وحشية أو التمثيل بالمجني عليه، د- وقوع الجريمة من موظف عام استغلالا لسلطة وظيفته أو لصفته ما لم يقرر القانون عقاباً خاصاً اعتباراً لهذه الصفة.

كما نص المرسوم اتحادي بقانون رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات في الفقرتين الثانية والثالثة من المادة (2) على تشديد العقوبة على هذه الجريمة في صورتها المصحوبة باعتداءات[1] على البيانات أو المعلومات كنتيجة للدخول غير المشروع[2]، كما أنه تدرج في تشديد العقوبة، وذلك وفقاً لشروط حددها على سبيل الحصر في هاتين الفقرتين، متى كان ارتكاب الجاني لفعل الدخول قد تم بدون تصريح أو بتجاوز حدود التصريح أو أن البقاء في النظام المعلوماتي كان بصورة غير مشروعة.

وحتى نقف على تشديد العقوبة على جريمة الدخول غير المشروع في النظام المعلوماتي والأسس التي انتهجها المشرع الوطني في تشديد العقوبة على هذه الجريمة كان لابد لنا أن نقسم هذا المطلب إلى ثلاثة فروع.

نتعرض في الفرع الأول إلى ظرف الإضرار بالبيانات أو المعلومات غير الشخصية كسبب لتشديد العقوبة، ثم نتناول في الفرع الثاني ظرف الإضرار بالبيانات أو المعلومات الشخصية كسبب آخر لتشديد العقوبة، ثم نتناول في الفرع الثالث ظرف الإضرار بالبيانات بمناسبة

---

[1]- د.عبد الرازق الموافي عبد اللطيف – مرجع سابق – ص 28.
[2]- أ.د. إمام حسنين خليل عطا الله – مرجع سابق - ص 62.

أو بسبب تأدية العمل كسبب لتشديد العقوبة بشكل أكثر شدةٍ من الظرفين السابقين، وذلك على النحو التالي:

الفرع الأول: الإضرار بالبيانات أو المعلومات غير الشخصية

تنص الفقرة الثانية من المادة (2) من المرسوم اتحادي بقانون رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات على: (تكون العقوبة الحبس مدة لا تقل عن ستة أشهر والغرامة التي تقل عن مائة وخمسين ألف درهم ولا تجاوز سبعمائة وخمسون ألف درهم أو بإحدى هاتين العقوبتين إذا ترتب على أي فعل من الأفعال المنصوص عليها بالفقرة 1 من هذه المادة إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أي بيانات أو معلومات).

يلاحظ من هذا النص الآتي: أن المشرع الوطني شدد العقوبة على جريمة الدخول غير المشروع في صورتها المصحوبة باعتداءات على البيانات والمعلومات، فأصبحت العقوبة هي الحبس مدة لا تقل عن ستة أشهر والغرامة التي تقل عن مائة وخمسين ألف درهم ولا تجاوز سبعمائة وخمسون ألف درهم أو بإحدى هاتين العقوبتين، ذلك بدلاً عن العقوبة التي قررتها الفقرة الأولى كعقوبة لجريمة الدخول غير المشروع في نظام المعالجة الآلية للمعطيات الإلكترونية في صورتها المجردة وهي الحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تزيد على ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين.

فجميع هذه الأفعال التي عددتها المادة سالفة الذكر (الدخول بدون تصريح أو تجاوز حدود التصريح أو البقاء بصورة غير مشروعة في نظام المعالجة الآلية للمعطيات الإلكترونية) تبدأ

بالدخول غير المشروع للنظام المعلوماتي، وانتهاك الخصوصية وهذا سبب كافٍ لتجريمها فضلاً عن إلحاق الضرر المادي والمعنوي بالمجني عليهم[1].

يلاحظ من النص القانوني للفقرة الثانية من المادة الثانية من المرسوم اتحادي بقانون رقم (5) لسنة 2012 أن المشرع وضع شرطين لابد من توافرهما ليتم توقيع العقوبة في صورتها المشددة هما:

1- أن يتم الدخول إلى نظام المعالجة الآلية للمعطيات الإلكترونية بدون تصريح أو بتجاوز حدود التصريح أو أن البقاء في النظام المعلوماتي كان بصورة غير مشروعة.

2- أن يترتب على الأفعال الواردة في الفقرة الأولى ضرراً يتمثل في أحد النتائج التالية وهي إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر[2] أو إعادة نشر أي بيانات أو معلومات.

أولاً: صور الإضرار بالمعلومات والبيانات

إن النتائج أو الظروف المشددة للعقوبة حسب ما وردت في المرسوم اتحادي بقانون رقم (5) لسنة 2012 عبارة عن تسعة أفعال وردت على سبيل الحصر وهي، الإلغاء ويقصد به إزالة المعلومات أو البيانات الموجودة داخل النظام المعلوماتي[3]، ويُعد الإلغاء أقصى أنواع الضرر، أما الحذف فهو استبعاد البيانات أو المعلومات[4].

أما التدمير فهو الصورة الأخطر والأبعد أثراً عن باقي صور الإتلاف[5]، ويتحقق بإهلاك البيانات أو المعلومات إهلاكاً كاملاً، فهو ينصب على كل البيانات أو المعلومات في النظام[6]، وقد

---

[1]- د.علي جبار الحسيناوي– جرائم الحاسوب والإنترنت دار اليازوري العلمية للنشر الأردن – سنة 2009 – ص 104

[2]- يلاحظ فعل النسخ والنشر الواردين في الفقرة الثانية، لم ينص عليهما المشرع في القانون رقم (2) لسنة 2006 الملغي، وتمت إضافتهما في هذا المرسوم الاتحادي.

[3]- د.أيمن عبا لله فكري – مرجع سابق – ص 208.

[4]- د.عبد الرازق الموافي عبد اللطيف – مرجع سابق – ص 28.

[5]- د.حسين بن سعيد الغافري – مرجع سابق - ص 420.

[6]- د.عبد الرازق الموافي عبد اللطيف – المرجع السابق – ص 28.

أوصى المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات عام 1994م بتجريم الأفعال التي تؤدي إلى تدمير المعلومات.

وتشمل هذه الأفعال: الإتلاف وهو إفناء مادة الشيء أو هلاكه كلياً أو جزئياً، والتعطيل ويقصد به توقف الشيء عن القيام بوظيفته فترة مؤقتة، والمحو ويقصد به إزالة جزء من المعطيات المسجلة على الدعامة الموجودة داخل النظام، أو تحطيم تلك الدعامة، أو نقل أو تخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة، والتخريب ويعني توقف الشيء تماماً عن أن يؤدي منفعته كلياً أو جزئياً[1].

أما التغيير فهو إحداث تعديلات في المعلومات يجعلها مخالفة للمضمون الأصلي الذي كانت عليه قبل الفعل[2]، بينما يتحقق الإفشاء بإبلاغ الغير بالمعلومات والبيانات أو باطلاعه على البيانات والمعلومات، سواءً كان ذلك بالرسم او التصوير أو القول أو الكتابة أو الرسائل أو غيره، ويستوي أن يكون الإفشاء كلياً أو جزئياً[3].

أما النشر فهو إذاعة بيانات أو معلومات أو إعادة نشرها، أما النسخ فيقصد به نقل البيانات أو المعلومات وكتابتها حرفاً بحرف[4]، والإتلاف هو التأثير في مادة الشيء على نحو يذهب أو يقلل من قيمته الإقتصادية عن طريق الإنقاص من كفاءته للإستعمال المعد له، فجوهر الإتلاف هو إفقاد المال المتلف منفعته أو صلاحيته للإستعمال في الغرض الذي أعد من أجله[5].

يلاحظ أنه على الرغم من توافر الشرطين اللذين سبق الإشارة إليهما، إلاّ أن توافر هذين الشرطين وحدهما دون وجود علاقة السببية بينهما لا ينتج أثراً كاملاً يمكن أن يترتب عليه تطبيق

---

[1]- د.حسين بن سعيد الغافري – المرجع السابق - ص 421.
[2]- د.أيمن عبا لله فكري – المرجع السابق– ص 208.
[3]- د. عبد الرازق الموافي عبد اللطيف – مرجع سابق – ص 29.
[4]- المرجع السابق – ص 29.
[5]- نهلا عبد القادر المومني – المرجع السابق - ص 123.

النص القانوني، إذ تعتبر علاقة السببية شرطاً طبيعياً يلزم توفره[1]، كي تتحقق علاقة السببية بين هذا النشاط (فعل الدخول الغير مشروع أو تجاوز التصريح أو البقاء في النظام دون وجه حق) وبين النتيجة[2]، وهي حدوث أحد النتائج التسعة التي نص عليها المشرع في هذه الفقرة (إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أي بيانات أو معلومات).

لم يحدد المشرع صورة الركن المعنوي للتجريم المشدد الوارد في نص الفقرة (2) من المادة الثانية من المرسوم اتحادي بقانون رقم (5) لسنة 2012 وسار على نفس النهج الذي انتهجه في جريمة الدخول الغير مشروع المجردة[3]، وبأي حال فلا يشترط أن يقصد الجاني تحقيق النتيجة الضارة لتتم إدانته وتوقيع العقاب عليه.

النتائج التي أشارت إليها الفقرة (2) من المادة الثانية من المرسوم اتحادي رقم (5) لسنة 2012 ليست مقصودة لذاتها، إذ أنها نتائج ترتبت عرضاً على فعل الجاني، لذلك فالظرف المشدد ينطبق في حالة ترتبت هذه النتائج بصورة عرضية، كما ينطبق - من باب أولى- إذا كان الجاني قد قصدها[4].

إذ أن الظرف المشدد هنا ظرف مادي عيني يكفي لتحققه وجود علاقة السببية بينه وبين الجريمة الأساسية، فمجرد وجود علاقة السببية بين الفعل والنتيجة يكفي لتوافر الشرط المشدد، والأمر الذي يمكن أن يعفي من تحقق الشرط المشدد هو أن يثبت إنتفاء علاقة السببية، وأن النشاط الذي حدث ونتج عنه الإلغاء أو الحذف أو.... إلخ، يرجع إلى القوة القاهرة أو الحادث المفاجئ[5].

---

[1]- د.عبد الرازق الموافي عبد اللطيف – المرجع السابق – ص 30.
[2]- د. أيمن عبا الله فكري – مرجع سابق – ص 208.
[3]- راجع ما أوردناه في شرح الركن المعنوي لجريمة الدخول غير المشروع في النظام المعلوماتي في صورتها المجردة ص (31)
[4]- المستشار علاء فكري اباظة – مرجع سابق – ص43.
[5]- د. سعيدي سليمة، الأستاذ حجاز بلال – مرجع سابق - ص 150.

مما سبق نجد أن المشرع قصد بهذا النص إسباغ الحماية على محتويات النظام المعلوماتي وهي البيانات والمعلومات[1]، وحدد النتائج التي يشترط تحققها لتشديد العقوبة في تسع حالات نص عليها على سبيل الحصر، وهي إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أي بيانات أو معلومات، وأن وقوع أي واحدة من هذه الأفعال يُعد ظرفاً مشدداً إذ لا يلزم ان تقع كلها، كما أن وقوع أكثر من فعل من هذه الأفعال والنتائج لا يترتب عليه تعدد في الظروف المشددة[2].

ثانياً: العقوبة في صورتها المشددة

شدد المشرع عقوبة جريمة الإضرار بالبيانات أو المعلومات غير الشخصية، وذلك بأن قرر في الفقرة (2) من المادة الثانية من المرسوم اتحادي بقانون رقم (5) لسنة 2012 بأن تكون عقوبتها الحبس مدة لا تقل عن ستة اشهر والغرامة التي لا تقل عن 150.000 درهم، ولا تجاوز 750.000 درهم، أو بإحدى هاتين العقوبتين وقد عُني المشرع بتشديد العقوبة في هذه الفقرة بحسب الآثار الوخيمة التي تترتب على ارتكاب الفاعل لجريمته الواردة في الفقرة (1)، والتي تتمثل في التأثير السلبي على البيانات والمعلومات المحفوظة في النظام المعلوماتي[3].

ويتضح هذا التشديد في أن المشرع وضع حداً أدنى لعقوبة الحبس بأن لا تقل عن ستة أشهر، في الوقت الذي لم يحدد فيه حداً أدنى لهذه العقوبة في جريمة الدخول غير المشروع إلى النظام المعلوماتي في صورتها المجردة وترك أمر تحديد الحد الأدنى للعقوبة للقاعدة العامة وهي الحبس لمدة شهر، والتي نصت عليها المادة (69) من قانون العقوبات الاتحادي لسنة 1987 وتعديلاته: (الحبس هو وضع المحكوم عليه في إحدى المنشآت العقابية المخصصة قانونا لهذا

---

[1]- تعرف المادة (1) من المرسوم اتحادي بقانون رقم (5) لسنة 2012 محتويات النظام بانها: المعلومات والبيانات والخدمات الإلكترونية.

[2]- د.عبد الرازق الموافي عبد اللطيف – مرجع سابق – ص 30.

[3]- المستشار علاء فكري اباظة – مرجع سابق – ص42.

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).

من المقرر فقهاً أن المشرع عندما يلجأ إلى تشديد العقوبة يلجأ إلى تقييد السلطة التقديرية للمحكمة الجزائية بقيود[1]، كأن ينص على حد أدنى لعقوبة الحبس أو السجن لا يجوز للمحكمة ان تنزل عنه[2]، ومن ذلك ما حدث لدينا في عقوبة جريمة الإضرار بالبيانات أو المعلومات غير الشخصية، إذ لم يترك المشرع الأمر لسلطة المحكمة التقديرية، ولكنه ألزمها بأن لا تنزل عن الحد الأدنى لعقوبة الحبس وهو ستة أشهر.

الفرع الثاني: الإضرار بالبيانات أو المعلومات الشخصية

يقصد بالبيانات الشخصية تلك التي تتعلق بسمعة الأفراد واعتبارهم، مثل البيانات التي تتعلق بحالة الشخص الطبية أو بسوابقه القضائية أو بأصوله العنصرية، أما المعلومات الشخصية فيقصد بها تلك المعلومات التي تتعلق بالشخص ذاته وتنتمي إلى كيانه كإنسان مثل الاسم والعنوان ورقم الهاتف وغيرها من المعلومات التي تتعلق بحياته المهنية أو بحياته العامة أو انتمائه السياسي[3].

وقد عُني المشرع بتشديد العقوبة في هذه الفقرة بحسب ما يترتب على ارتكاب الجريمة من آثار وخيمة تؤثر سلباً على البيانات والمعلومات المحفوظة في الموقع أو النظام أو الشبكة أو

---

[1]- تناول د.غنام محمد غنام في مؤلفه شرح قانون العقوبات الاتحادي لدولة الإمارات العربية المتحدة (مرجع سابق) لفكرة تقييد السلطة التقديرية للمحكمة حيث ذكر في صفحة 480 أنه: (على الرغم من أن المشرع يقر بمبدأ السلطة التقديرية للمحكمة الجزائية فإنه يتدخل في صدد بعض الجرائم لكي يقيد تلك السلطة، وغالباً ما يحدث ذلك رغبةً منه في تشديد العقاب، فيورد قيوداً على تلك السلطة، من تلك القيود: 1- أن يكون الحبس وجوبياً. 2- أن يلجأ المشرع إلى عقوبة ذات حد واحد كجزاء للجريمة. 3- أن يورد المشرع حداً أقصى للجريمة. 4- أن يورد حداً أدنى للعقوبة السالبة للحرية. 5- أن يتعلق الأمر بجريمة من الجرائم التي تسري عليها أحكام الشريعة الاسلامية).

[2]- د.غنام محمد غنام - المرجع السابق- ص 481.

[3]- د.محمود أحمد طه – مرجع سابق – ص 59، وفي نفس المعنى راجع د. حسام الدين كامل الأهواني – الحماية القانونية للحياة الخاصة في مواجهة الحاسب الآلي – مؤتمر جامعة الكويت حول القانون والحاسب الآلي – مطبوعات جامعة الكويت ومؤسسة الكويت للتقدم العلمي 1994 – ص 113.

وسيلة تقنية المعلومات، فأراد أن يوفر حماية أكبر للبيانات والمعلومات الشخصية، فلا شك أن الاعتداء على هذه البيانات يشكل خطراً جسيماً على صاحبها[1].

كما أن نشر البيانات والمعلومات الشخصية وما يتصل بها من أخبار ومعلومات مثل حالته العاطفية وصداقاته وشؤون أسرته وحالته الصحية، عبر وسائل التواصل الاجتماعي ونظم المعلوماتية بصفةً عامة دون الموافقة الصريحة أو الضمنية من صاحبها، يعتبر اعتداءً على الحياة الخاصة للإنسان وخصوصيتها التي يحميها القانون[2].

قد تنتهك هذه الخصوصية من خلال الوصول للمعلومات والبيانات المخزنة في الحاسوب أو البرمجيات أو الشبكات أو النظام المعلوماتي بصفةٍ عامة، لذا نص المشرع في الفقرة (3) من المادة الثانية من المرسوم اتحادي بقانون رقم (5) لسنة 2012 على: (تكون العقوبة الحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين إذا كانت البيانات أو المعلومات محل الأفعال الواردة في الفقرة (2) من هذه المادة شخصية).

ويشترط في المعلومة الإلكترونية كي تعتبر ذات طابع شخصي، أي كي تعد سراً يستحق الحماية أن تكون هذه الأسرار ذات صلة بالشخص، وأن تحظى بحرص صاحبها في إبقائها سرية بعيدة عن علم الغير، وأن يكون من شأن الاعتداء على سريتها هذه احتمال الإضرار المادي أو المعنوي بصاحبها[3].

---

[1]- المستشار.علاء فكري اباظة – مرجع سابق – ص43.

[2]- المستشار.محمد أحمد الحمادي – تشريعات مكافحة جرائم تقنية المعلومات في دولة الإمارات وأحكام القضاء - ندوة علمية بعنوان شبكات الإنترنت وتأثيراتها الاجتماعية والأمنية – إصدار مركز البحوث والدراسات الأمنية بالقيادة العامة لشرطة أبوظبي – نوفمبر 2006 - ص 21.

[3]- د.محمود أحمد طه – مرجع سابق – ص 60، وفي نفس المعنى راجع د. أسامة العبيدي – حماية الحق في الحياة الخاصة في مواجهة جرائم الحاسب الآلي والانترنت – المجلة العربية للعلوم الأمنية – مجلد 23 – العدد 46.

لكي تقوم الصورة المشددة المتمثلة في هذه الجريمة يلزم توافر ثلاثة شروط وهي:

1- يلزم أن يرتكب الجاني فعل الدخول إلى النظام المعلوماتي بدون تصريح أو بتجاوز حدود التصريح أو أن البقاء في النظام المعلوماتي كان بصورة غير مشروعة.

2- أن يترتب على الأفعال الواردة في الفقرة الأولى ضرراً يتمثل في: إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أي بيانات أو معلومات.

3- أن تكون البيانات والمعلومات التي وقع عليها الإضرار شخصية.

وتتطلب هذه الصورة من التجريم أن تكون البيانات والمعلومات محل الجريمة تتعلق بشخصٍ معين أياً كانت صفته، فيستوي ان يكون الشخص هو صاحب الموقع أو النظام أو وسيلة تقنية المعلومات أو أن يكون شخصاً آخر[1].

من أمثلة البيانات والمعلومات الشخصية أن يؤدي سلوك الجاني إلى إفشاء الأسرار الخاصة بالمجني عليه أو الاطلاع على السجلات الطبية للأفراد والمرضى وسجلات الأحوال المدنية، وبياناته الشخصية وصوره وبيانات أولاده وزوجته ووالديه، وكذلك أمواله الخاصة وتصرفاته الشخصية وتنقلاته ومعتقداته وآرائه الخاصة وحفلاته ولقاءاته الخاصة وعلاقاته وصداقاته[2]، إذ أن الحق في احترام الحياة الخاصة هو أحد الحقوق اللصيقة بالشخصية التي تثبت للإنسان لمجرد كونه إنسان وفي المجتمعات الحديثة يعتبر هذا الحق من أهم الحقوق، وذلك لما له من ارتباط وثيق بحرية الفرد[3].

وقد فرض المشرع في الفقرة (3) من المادة الثانية حماية أكبر للبيانات والمعلومات إذا كانت شخصية، فاعتبر ظرفاً مشدداً ثانياً وقوع الجريمة الواردة في الفقرتين السابقتين على

---

[1]- د.عبد الرازق الموافي عبد اللطيف – مرجع سابق – ص 32.
[2]- أ.د. إمام حسنين خليل عطا الله – مرجع سابق - ص 64.
[3]- نهلا عبد القادر المومني – مرجع سابق - ص 165.

البيانات والمعلومات الشخصية، ويعتبر التشديد هنا اتجاه محمود من المشرع، إذ أن الاعتداء على تلك البيانات يشكل خطراً جسيماً على أصحابها، ومن ثم وجب توفير حماية أكبر لها من خلال تشديد العقوبة على من ينتهك هذه البيانات والمعلومات الشخصية[1].

وتتضح هذه الحماية التي فرضها المشرع من خلال نص الفقرة (3) من المادة الثانية من المرسوم اتحادي رقم (5) لسنة 2012، حيث نص على عقوبة الحبس التي لا تقل مدتها عن سنة والغرامة التي لا تقل عن 250.000 درهم ولا تجاوز 1.000.000 درهم أو بإحدى هاتين العقوبتين إذا كانت البيانات أو المعلومات التي تعرضت لأحد الأفعال الواردة في الفقرة (2) من هذه المادة عبارة عن بيانات أو معلومات شخصية .

وباستقراء نص الفقرة (3) من المادة الثانية نلاحظ كيف أن المشرع غلظ العقوبة عندما تعلق الأمر بالمساس بالبيانات والمعلومات الشخصية التي يعتبر المساس بها اعتداءً جسيماً بالغ الإضرار بالمجني عليه، حيث تم تغليظ عقوبة الحبس بأن أصبح حدها الأدنى هو الحبس الذي لا تقل مدته عن سنة، وذلك بدلاً عن الحد الأدنى في جريمة الإضرار بالبيانات والمعلومات غير الشخصية التي كان الحد الأدنى فيها للحبس هو ستة أشهر.

كما قام المشرع بتغليظ عقوبة الغرامة فأصبحت الغرامة التي لا تقل عن 250.000 درهم ولا تجاوز 1.000.000 درهم، وذلك بعد أن كانت الغرامة في جريمة الإضرار بالبيانات أو المعلومات غير الشخصية هي الغرامة التي لا تقل عن 150.000 درهم ولا تجاوز 750.000 درهم[2].

بالإضافة إلى تلك العقوبات فإن المحكمة توقع على الجاني العقوبات الفرعية والتدابير المتمثلة في المصادرة ومحو وإعدام المعلومات والبيانات وغلق المحل أو الموقع الذي ارتكبت فيه

---

[1]- المستشار علاء فكري اباظة – مرجع سابق – ص43.
[2]- المستشار علاء فكري اباظة – مرجع سابق – ص 44.

أي من هذه الأنشطة الواردة في الفقرة (2) من المادة الثانية من المرسوم اتحادي بقانون رقم (5) لسنة 2012، كما يجوز أن 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 المرسوم بقانون، وذلك بعد تنفيذ العقوبة.

الفرع الثالث: ارتكاب جريمة الدخول أو الإضرار بالبيانات بمناسبة أو بسبب تأدية العمل

تنص المادة (3) من المرسوم اتحادي بقانون رقم (5) لسنة 2012 على: (يعاقب بالحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين كل من ارتكب أي من الجرائم المنصوص عليها في البندين 1 و 2 من المادة 2 من هذا المرسوم، بمناسبة أو بسبب تأدية عمله).

باستقراء النص نجد أنه كي تقوم هذه الجريمة يلزم توافر الشروط التالية:

1- أن يرتكب الجاني فعل الدخول إلى النظام المعلوماتي بدون تصريح أو بتجاوز حدود التصريح أو أن البقاء في النظام المعلوماتي كان بصورة غير مشروعة.

2- أن يترتب على الدخول أو البقاء الغير مشروع في النظام المعلوماتي أحد الأضرار الواردة في الفقرة (2) أو الفقرة (3) من المادة الثانية من المرسوم اتحادي بقانون رقم (5) لسنة 2012.

3- أن يرتكب الجاني الجريمة بمناسبة أو بسبب تأدية عمله، ويستوي أن يقع السلوك الإجرامي من الجاني أثناء تأدية عمله أو غير ذلك، ما دام أن السلوك تم بمناسبته أو بسببه[1].

بالتالي فإنه يشترط أن يكون الجاني من الأشخاص الذين لهم علاقة عمل بالمواقع الإلكترونية أو أنظمة المعلومات الإلكترونية أو شبكة المعلومات، أو وسيلة تقنية معلومات، ويستخلص ذلك من عبارة بمناسبة أو بسبب تأدية عمله.

---

[1]- د.عبد الرازق الموافي عبد اللطيف – مرجع سابق – ص 31.

من ذلك نشير إلى واقعة جنائية كانت أحداثها في إمارة دبي في يونيو من العام 2006، حيث قدمت نيابة دبي اثنين من المتهمين للمحاكمة بارتكاب جرائم تقنية معلومات متعددة من بينها جريمة الدخول غير المشروع للنظام المعلوماتي[1]، وتتلخص وقائع القضية في قيام أحد المتهمين وهو أجنبي يعمل بائع تذاكر في إحدى شركات السفر والسياحة بدبي بتمكين المتهم الثاني من استغلال رقمه السري في الدخول إلى موقع الشركة في أزمنةٍ مختلفةٍ، والحصول على عدد خمسة تذاكر طيران بصورة غير مشروعة.

وعلى الرغم من أن المتهم الثاني ليس له صفة الدخول إلى الموقع الإلكتروني للشركة إلاّ أنه تمكن من ذلك بمساعدة المتهم الأول الذي مكنه من استخدام رقمه السري، فقد أدانتهما المحكمة طبقاً للمواد (2، 10، 23، 25) من قانون مكافحة جرائم تقنية المعلومات (الملغي)، وحكمت على المتهم الأول بالحبس لمدة شهرين وإبعاده خارج الدولة، وعلى المتهم الثاني بالحبس لمدة سنة وإبعاده خارج الدولة.

يلاحظ من خلال هذه القضية الآتي:

1- أن المحكمة طبقت على المتهم الأول نص الفقرة الأولى من المادة (2) من قانون مكافحة جرائم تقنية المعلومات (الملغي)[2].

2- طبقت المحكمة على المتهم الثاني نص المادة الثالثة من القانون الملغي[3]، وهي المتعلقة بجريمة الدخول أو الاضرار بالبيانات بمناسبة أو بسبب تأدية العمل بحكم أن المتهم الثاني يعمل في

---

[1]- المستشار. محمد أحمد الحمادي – مرجع سابق - ص 36.

[2]- تنص الفقرة (1) من المادة الثانية من القانون الملغي على: (كل فعل عمدي يتوصل فيه بغير وجه حق إلى موقع أو نظام معلوماتي سواء بدخول الموقع أو النظام أو بتجاوز مدخل مصرح به، يعاقب عليه بالحبس وبالغرامة أو بإحدى هاتين العقوبتين) وهي كما اشرنا تتفق من حيث العقوبة مع نص المادة الثانية من القانون الحالي وتختلف عنه من حيث اشتراط العمد الذي سبق وان تناولناه بالشرح عند تناولنا للركن المعنوي للجريمة فنشير بالرجوع اليه.

[3]- تنص المادة الثالثة من القانون الملغي على أن: (كل من ارتكب أيٍ من الجرائم المنصوص عليها في البند (2) من المادة (2) من هذا القانون اثناء أو بسبب تأدية عمله أو سهل ذلك للغير يعاقب بالحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن عشرين ألف درهم أو بإحدى هاتين العقوبتين) وهي توافق المادة الثالثة من القانون الحالي (من حيث مدة الحبس وإن اختلفت معها من حيث قيمة الغرامة) والتي تنص على: (يعاقب بالحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين كل من ارتكب أي من الجرائم المنصوص عليها في البندين (1) و (2) من المادة الثانية من هذا المرسوم اتحادي بقانون بمناسبة أو بسبب تأدية عمله).

نفس الشركة واشترك مع المتهم الأول بأن سهل له من استخدام رقمه السري في الدخول إلى الموقع الالكتروني للشركة وارتكاب الجريمة والجرائم الأخرى المرتبطة بها.

3- تم أيضاً إدانة المتهم الثاني بتهمة المساعدة الجنائية للأول في دخول الموقع الإلكتروني والعبث به والاحتيال على الشركة ربة عمله، وذلك وفقاً للمادة 23 من القانون (الملغي) والتي تنص على أن: (كل من حرض أو ساعد أو اتفق مع الغير على ارتكاب جريمة من الجرائم المنصوص عليها في هذا القانون ووقعت الجريمة بناء على هذا التحريض أو المساعدة أو الاتفاق يعاقب بذات العقوبة المقررة لها).

4- تم توقيع عقوبة الإبعاد على المتهمين وفقاً لنص المادة (25) من قانون مكافحة تقنية المعلومات (الملغي)[1] وهي توافق المادة (42) من القانون الحالي قبل تعديلها الأخير الصادر بموجب المرسوم بقانون رقم (2) لسنة 2018 الصادر في 24 يوليو 2018، حيث تم التعديل الأخير في شروط توقيع تدبير إبعاد الأجنبي من الدولة في جرائم تقنية المعلومات، وذلك بأن حصره في إبعاد الشخص الذي يحكم عليه في الجرائم الواقعة على العرض أو عند الحكم بعقوبة الجناية كل ذلك دون إخلال بأحكام المادة (121) من قانون العقوبات الاتحادي لسنة 1987 وتعديلاته، والتي سبق الحديث عنها.

يعتبر هذا النص في حقيقته ظرفاً مشدداً للمادة الثانية من المرسوم اتحادي بقانون رقم (5) لسنة 2012 إذ أن المشرع في هذه المادة ارتأى خطورة وقوع الجريمة الواردة في الفقرات (1) و(2) من المادة الثانية من قِبل الجاني الذي يرتكبها بمناسبة أو بسبب تأدية عمله، ومن ثم اتجه المشرع إلى تشديد العقوبة حال توافر تلك الصفة في مرتكب الجريمة[2].

فلا يشترط لتطبيق الظرف المشدد أن يكون الفاعل موظفاً عاماً، بل يكفي أن يرتكب الجريمة أي شخص بمناسبة أو بسبب تأدية عمله، كما لا يشترط المشرع من جهة أخرى توافر طبيعة معينة في البيانات والمعلومات محل الاعتداء، إذ يتحقق الظرف المشدد متى وقع ذلك

---

[1]- تنص المادة (25) من القانون الملغي على أنه: (فضلا عن العقوبات المنصوص عليها في هذا القانون تقضي المحكمة بإبعاد الأجنبي الذي يحكم عليه بالحبس وفقا لأحكام هذا القانون) وهي توافق المادة (42) من القانون الحالي التي تنص على: (تقضي المحكمة بإبعاد الأجنبي الذي يحكم عليه بالإدانة لارتكاب أي جريمة من الجرائم المنصوص عليها في هذا المرسوم اتحادي بقانون وذلك بعد تنفيذ العقوبة المحكوم بها)، ويلاحظ هنا اختلاف النصين في سبب الإبعاد بين الحبس في القانون الملغي، والإدانة في القانون الحالي.

[2]- المستشار علاء فكري اباظة – مرجع سابق – ص 46.

الاعتداء من الموظف على البيانات والمعلومات بصرف النظر عما إذا كانت هذه البيانات أو المعلومات تخص جهة عمله أم أنها تخص جهة أخرى اتصل بها سبب عمله، إذ أن العبرة في هذه الجريمة هي أن موقع عمل الجاني هو الذي مكنه من التلاعب في البيانات والمعلومات[1].

والقصد الجنائي اللازم لهذه الجريمة هو القصد الجنائي العام، بأن يتوفر للجاني العلم والإرادة، فيجب ان يعلم الجاني بأنه غير مصرح له الدخول إلى هذا النظام المعلوماتي[2]، وأن سلوكه ينصب على موقع أو نظام معلوماتي أو بيانات أو معلومات تُعد محل الحق الذي يحميه القانون وأن سلوكه هذا يحدث بمناسبة أو سبب عمله[3]، وعلى الرغم من ذلك اتخذ سبيله عالماً بالنتائج المترتبة عليه[4]، وينتفي العلم إذا ارتكب الجاني سلوكه وهو يعتقد أنه لا يشكل اعتداء على الحق الذي يحميه القانون وبالتالي ينتفي القصد الجنائي[5].

مما سبق نجد ان المشرع الوطني قد تدرج في العقاب على جريمة الدخول غير المشروع في النظام المعلوماتي، ويتبين هذا التدرج من خلال التدرج في العقوبات والنظام العقابي الذي سعى لمعالجة الخطورة الإجرامية التي قدرها المشرع لهذه التصرفات[6]، إذ نجد سلم خطورة الجريمة يتكون من ثلاث درجات.

الدرجة الأولى: هي جريمة الدخول غير المشروع في النظام المعلوماتي بصورتها المجردة والتي تقوم على أفعال متعددة ومختلفة وهي الدخول بدون ترخيص أو تجاوز حدود الترخيص أو البقاء الغير مشروع في النظام المعلوماتي، حيث نص المرسوم اتحادي على معاقبة

---

[1]- المرجع السابق – ص 47.
[2]- المستشار د. ربيع محمود الصغير - مرجع سابق – ص 365.
[3]- د.عبد الرازق الموافي عبد اللطيف – مرجع سابق – ص 37.
[4]- المستشار د. ربيع محمود الصغير - مرجع سابق – ص 366.
[5]- د.عبد الرازق الموافي عبد اللطيف – المرجع السابق – ص 37.
[6]- د. سعيدي سليمة، الأستاذ حجاز بلال – مرجع سابق - ص 152.

الجاني بالحبس أو الغرامة التي لا تقل عن 100.000 درهم ولا تزيد على 300.000 درهم أو بإحدى هاتين العقوبتين[1].

الدرجة الثانية: شدد المشرع الوطني العقوبة على جريمة الدخول غير المشروع في صورتها المصحوبة باعتداءات على البيانات والمعلومات غير الشخصية، فأصبحت العقوبة هي الحبس مدة لا تقل عن ستة أشهر والغرامة التي تقل عن 150.000 درهم ولا تجاوز 750.000 درهم أو بإحدى هاتين العقوبتين.

الدرجة الثالثة: وهما جريمة الإضرار بالبيانات أو المعلومات الشخصية المنصوص عليها في الفقرة (3) من المادة الثانية من المرسوم اتحادي بقانون رقم (5) لسنة 2012، وجريمة الدخول أو الإضرار بالبيانات بمناسبة أو بسبب تأدية العمل المنصوص عليها في المادة (3) من المرسوم الاتحادي، حيث فرض المشرع في هاتين الحالتين حماية أكبر للبيانات والمعلومات إذا كانت شخصية، أو إذا كان الجاني قد ارتكب جريمة الإضرار بالبيانات بمناسبة أو بسبب تأدية العمل، حيث اعتبرهما المشرع ظرفاً مشدداً ثانياً لوقوع الجريمة، وقرر لأيٍ من هاتين الجريمتين عند وقوعها عقوبة الحبس التي لا تقل مدتها عن سنة والغرامة التي لا تقل عن 250.000 درهم ولا تجاوز 1.000.000 درهم أو بإحدى هاتين العقوبتين .

المبحث الثاني: العقوبات المقررة لجريمة الدخول بدون تصريح إلى نظام المعالجة الآلية للمعطيات الإلكترونية بقصد الحصول على بيانات حكومية أو معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية

تمهيد:

سبق وأن أشرنا في المبحث الأول من هذا الفصل إلى قاعدة التناسب بين الجريمة والعقوبة، وإلى التدرج في العقوبة الذي انتهجه المشرع الوطني، كما أشرنا إلى التطور التشريعي

[1]- راجع المادة الثانية الفقرة (1) من المرسوم اتحادي رقم (5) لسنة 2012.

في العقوبة في جرائم تقنية المعلومات في الدولة، وذلك عند تناولنا للعقوبات التي قررها المشرع لجريمة الدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات الإلكترونية في صورتها المجردة أو المصحوبة بقصد.

وأوضحنا كيف أن المشرع الوطني تشكلت وتبلورت قناعاته بخطورة جرائم تقنية المعلومات، وكيف أنه اتجه إلى اتخاذ إجراءات عاجلة نحو تشديد العقوبة، كانت أولها إصدار المرسوم اتحادي بقانون رقم (5) لسنة 2012 الذي أعاد ترتيب بعض مواد القانون (الملغي) وعمد إلى تشديد العقوبة في العديد من الجرائم، إلاّ ان السِمَّة الغالبة في هذا المرسوم الاتحادي هي تشديد العقوبة في جرائم الدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات الإلكترونية، وذلك حتى تتناسب العقوبة مع مستوى التأثير السلبي لهذه الجرائم على الفرد والمجتمع.

كما لاحظنا في المبحث الأول من هذا الفصل كيف أن المرسوم اتحادي بقانون رقم (5) لسنة 2012 تدرج في عقوبة جريمة الدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات الإلكترونية في صورتها المجردة بحسب تدرج واختلاف النشاط المكون للجريمة، واضعاً في الحسبان تأثير الجريمة على المجتمع، ومدى إخلالها بقواعد السلامة والأمان والخصوصية في نظام المعالجة الآلية للمعطيات الإلكترونية.

وتتضح معالم تطبيق قاعدة التناسب بين الجريمة والعقوبة، والتدرج في العقوبة، من خلال ما نص عليه المشرع في معاقبة الجاني على جريمة الدخول غير المشروع إلى النظام المعلوماتي في صورها المجردة بالحبس والغرامة التي لا تقل عن 100.000 درهم ولا تزيد على 300.000 درهم أو بإحدى هاتين العقوبتين.

فإذا ترتب على فعل الدخول العبث بالبيانات أو المعلومات بصفةٍ عامة، فإنه يعاقب بالحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن 150.000 درهم ولا تجاوز

750.000 درهم، أو بإحدى هاتين العقوبتين، أما إذا كانت البيانات أو المعلومات التي تم العبث بها شخصية، أو أن الجاني ارتكب الجريمة بمناسبة أو بسبب تأدية عمله، فإن العقوبة تكون الحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن 250.000 درهم ولا تجاوز 1.000.000 درهم أو بإحدى هاتين العقوبتين.

وسيراً على نفس التدرج في العقوبة، والتناسب بين العقوبة والجريمة، ولأهمية الحماية القانونية لجريمة الدخول بدون تصريح إلى النظام المعلوماتي بقصد الحصول على بيانات حكومية أو معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية، حيث تعتبر هذه الجريمة أكثر جرأة، وأعظم تأثيراً على الأمن المعلوماتي واستقراره.

وذلك لما في هذه الجريمة من مساس بالمصالح العليا للدولة، وأمنها واقتصادها الوطني، وما يمكن أن يترتب عليها من جرائم أخرى، يمكن أن تدخل في استغلال البيانات الحكومية أو الأسرار الخاصة بالمنشآت المالية والتجارية والاقتصادية، بما يسبب الضرر للدولة ونظامها المالي ومناخ الاستثمار فيها.

لكل ذلك نجد أن المشرع قد شدد العقوبة فيها بدرجة أعلى من العقوبات السابقة، وذلك بأن صنفها ضمن الجنايات، ثم تدرج في العقوبات التي توقع على الجاني وذلك على مرحلتين، واضعاً في الاعتبار طبيعة النشاط الإجرامي الذي يرتكبه الجاني، والنتيجة الإجرامية التي تترتب على هذا النشاط.

لذا وحتى نقف على العقوبات البسيطة والمشددة المقررة لجريمة الدخول بدون تصريح إلى النظام المعلوماتي بقصد الحصول على بيانات حكومية أو معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية نقسم هذا المبحث إلى مطلبين نخص الأول منهما للعقوبات البسيطة، والمطلب الثاني للظروف المشددة للعقوبة وذلك على النحو التالي:

المطلب الأول: العقوبات البسيطة

عرفنا أن العقوبات البسيطة هي العقوبات التي يقررها القانون دون ظروف مشددة، وهي متنوعة وتختلف فيما بينها من حيث مقدار جسامتها وطبيعتها ومدتها ومدى أهميتها كجزاء للجريمة[1]، وأن أهم تقسيمات العقوبات هو تقسيمها إلى عقوبات جنايات وعقوبات جنح وعقوبات مخالفات[2]، كما تقسم العقوبات إلى عقوبات أصلية[3]، وعقوبات تبعية أو تكميلية، والتقسيم الأخير من حيث كفاية العقوبة في تحقيق معنى الجزاء المقابل للجريمة من عدمه[4].

تستمد العقوبة الأصلية وصفها من أنها العقاب الأصلي أو الأساسي المباشر للجريمة[5]، ذلك أنه يُمكِن أن توقع على الجاني منفردة، بغير أن يكون القضاء بها معلقاً على عقوبة أخرى[6]، وقد نص عليها المشرع الوطني في المادة (66) من قانون العقوبات الاتحادي رقم (5) لسنة 1987 وتعديلاته.

لذا ولما كانت عقوبتي السجن المؤقت والغرامة من العقوبات الأصلية التي نص عليها المشرع الوطني في الفقرتين (ب/3) و (ب/6) من المادة (66) السابق الإشارة اليها، وفي إطار دراستنا للعقوبات البسيطة لجريمة الدخول بدون تصريح للنظام المعلوماتي بقصد الحصول على بيانات حكومية أو معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية، نرى أنه من الأفضل تقسيم هذا المطلب إلى ثلاثة فروع نخصص الأول لعقوبة السجن المؤقت والفرع الثاني لعقوبة الغرامة والفرع الثالث للعقوبات الفرعية، وذلك على النحو التالي:

---

[1]- د.محمود نجيب حسني – شرح قانون العقوبات – القسم العام ط4 – مرجع سابق – ص 738.
[2]- المرجع السابق – ص 738.
[3]- تنص المادة (66) من قانون العقوبات الاتحادي لسنة 1987 وتعديلاته على أن العقوبة الأصلية هي: (أ- عقوبات الحدود والقصاص والدية. ب- عقوبات تعزيرية وهي: 1- الإعدام 2- السجن المؤبد 3- السجن المؤقت 4- الحبس 5- الحجز 6- الغرامة)
[4]- د. محمود نجيب حسني – مرجع سابق – ص 746.
[5]- راجع في ذلك نقض 17 مارس سنة 1959 مجموعة أحكام محكمة النقض س 10 رقم 73 ص 328.
[6]- د. محمود نجيب حسني – شرح قانون العقوبات – القسم العام ط4 – مرجع سابق – ص 743.

الفرع الأول: عقوبة السجن المؤقت

تقرر الفقرة الأولى من المادة الرابعة من المرسوم اتحادي بقانون رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات عقوبة السجن المؤقت والغرامة التي لا تقل قيمتها عن 250.000 ولا تجاوز 1.500.000 درهم على الشخص الذي يرتكب جريمة الدخول إلى النظام المعلوماتي بدون تصريح يخوله ذلك، متى كان دخوله بقصد الحصول على بيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية المنصوص عليها.

كما أسلفنا فإن عقوبة السجن المؤقت من العقوبات الأصلية التي نص عليها المشرع الوطني في الفقرة (ب/3) من المادة (66) من قانون العقوبات الاتحادي رقم (3) لسنة 1987 وتعديلاته، وهي إحدى العقوبات التي يمكن أن توقع على الجنايات، والتي نصت عليها المادة (28) من قانون العقوبات الاتحادي لسنة 1987 وتعديلاته[1]، ولا يجوز أن تقل مدة السجن المؤقت عن ثلاث سنوات، ولا أن تزيد على خمس عشرة سنة ما لم ينص القانون على خلاف ذلك[2].

بذلك فقد اعتبر المشرع جريمة الدخول إلى النظام المعلوماتي بدون تصريح بقصد الحصول على بيانات حكومية أو معلومات سرية خاصة بالمنشآت المالية أو التجارية أو الاقتصادية، جناية عقوبتها السجن المؤقت والغرامة، وهما عقوبتان وجوبيتان يتعين القضاء بها معاً[3].

مما سبق نجد أنه وبالنسبة لعقوبة السجن يكون القاضي ملزماً بالحكم بها فيما بين حديها الأدنى والأقصى، وذلك بحيث لا يقل حدها الأدنى عن ثلاث سنوات ولا تزيد على خمس عشر

---

[1]- تنص المادة (28) من قانون العقوبات الاتحادي لسنة 1987 وتعديلاته على أن: (الجناية هي الجريمة المعاقب عليها بإحدى العقوبات الآتية: 1- أية عقوبة من عقوبات الحدود أو القصاص فيما عدا حدي الشرب والقذف 2- الإعدام 3- السجن المؤبد 4- السجن المؤقت) .

[2]- تنص المادة (68) (..... لا يجوز أن تقل مدة السجن المؤقت عن ثلاث سنوات ولا أن تزيد على خمس عشرة سنة ما لم ينص القانون على خلاف ذلك).

[3]- المستشار علاء فكري اباظة – مرجع سابق – ص 58.

سنة، بالإضافة إلى عقوبة الغرامة التي يكون القاضي ملزماً بأن يحكم بها على ألاّ تقل عن 250.000 درهم ولا تتجاوز 1.500.000 درهم[1].

الفرع الثاني: عقوبة الغرامة

الغرامة عقوبة مالية يقررها القانون، وهي من العقوبات الأصلية التي نصت عليها المادة (66) من قانون العقوبات الاتحادي رقم (3) لسنة 1987 وتعديلاته، وكانت المادة (71) من هذا القانون تقرر أن الغرامة هي إلزام المحكوم عليه أن يدفع للخزينة المبلغ المحكوم به، ولا يجوز أن تقل الغرامة عن 100 درهم ولا أن يزيد حدها الأقصى في الجنايات عن 100.000 درهم، أما في الجنح فإن حدها الأقصى لا يزيد عن 30.000 درهم.

قررت الفقرة الأولى من المادة الرابعة من المرسوم اتحادي بقانون رقم (5) لسنة 2012 معاقبة الجاني بالسجن المؤقت والغرامة التي لا تقل عن 250.000 درهم ولا تجاوز 1.500.000 درهم عن جريمة الدخول بدون تصريح إلى النظام المعلوماتي بقصد الحصول على بيانات حكومية أو معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية، والغرامة عندما يتم تقريرها كعقوبة للجناية بالإضافة إلى عقوبة أخرى أصلية كالإعدام أو السجن المؤبد أو السجن المؤقت تعد عقوبة تكميلية.

باستقراء المادة (22) من القانون (الملغي) نلاحظ أنها لم تكن تنص على عقوبة الغرامة ضمن العقوبة المقررة لهذه الجريمة، مما يعني أن المرسوم اتحادي بقانون الجديد هو الذي أضاف عقوبة الغرامة إلى عقوبة السجن المؤقت، وفرضهما معاً على سبيل الوجوب، بحيث لا تستطيع المحكمة إلاّ أن تقضي بهما معاً، على أن يتم ذلك في إطار الحد الأدنى والأقصى الذي يحدده

[1]- د.عبد الرازق الموافي عبداللطيف – مرجع سابق – ص 41.

القانون بالنسبة لعقوبة السجن المؤقت[1]، أو الذي يحدده النص القانوني بالنسبة لعقوبة الغرامة الواردة في الفقرة الأولى من المادة الرابعة من المرسوم اتحادي بقانون رقم (5) لسنة 2012.

الفرع الثالث: العقوبات الفرعية

أولاً: العقوبات التبعية

عرفت المادة رقم (73) من قانون العقوبات الاتحادي لدولة الامارات العقوبات الفرعية التبعية بأنها: (1- الحرمان من بعض الحقوق والمزايا. 2- مراقبة الشرطة، وتلحق هذه العقوبات المحكوم عليه بقوة القانون دون حاجة إلى النص في الحكم وذلك على النحو المبين في هذا الفرع).

من الواضح أن المصادرة تعتبر من العقوبات الفرعية التبعية التي تنطق بها المحكمة بقوة القانون. لذا نجد أن صياغة المادة (41) من المرسوم اتحادي بقانون رقم (5) لسنة 2012 جاءت آمرة بعبارة[2]: (مع عدم الإخلال بحقوق الغير حسني النية يحكم في جميع الأحوال بمصادرة الأجهزة...).

لذا فإن المحكمة ملزمة بتوقيع عقوبة المصادرة وإغلاق المحل أو الموقع باعتبارها عقوبة تبعية بالإضافة الى عقوبتي السجن المؤقت والغرامة اللتان قررتهما الفقرة الأولى من المادة الرابعة من المرسوم اتحادي بقانون رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات، وتشمل مصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب هذه الجريمة، وكذلك مصادرة الأموال المتحصلة منها و إغلاق المحل أو الموقع الذي ترتكب فيه هذه الجرائم مع الأخذ في الاعتبار حقوق الغير حسني النية.

---

[1]- د.عبد الرازق الموافي عبداللطيف – مرجع سابق – ص 41.

[2]- تنص المادة (41) من المرسوم اتحادي بقانون رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات على: (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).

كما نصت المادة رقم (42) من المرسوم اتحادي بقانون رقم (5) لسنة 2012 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).

فنرى أن المحكمة ملزمة أيضاً بتوقيع عقوبة إبعاد الأجنبي الذي يرتكب أي من الجرائم المنصوص عليها في المرسوم السالف ذكره.

ثانياً: العقوبات التكميلية

بالرغم من إشتراك العقوبات التكميلية مع العقوبات التبعية في صفة الفرعية أو الثانوية، والتي تعني أنه لا يمكن توقيع أياً من العقوبتين على المحكوم عليه إستقلالاً عن الحكم بعقوبة أصلية، فإن الأولى تختلف عن الثانية في أمر هام يتمثل ذلك في أن العقوبات التبعية تلحق بالمحكوم عليه بقوة القانون كما اسلفنا، فلا يشترط أن يتضمنها الحكم، إلا أن العقوبات التكميلية لا يمكن توقيعها على المحكوم عليه إلا إذا نص على ذلك الحكم الصادر صراحة، حتى ولو كانت العقوبة التكميلية وجوبية، ذلك أن العقوبة التكميلية قد تكون وجوبية وقد تكون جوازية، فإذا كانت وجوبية فلا يمكن مع ذلك توقيعها إلا إذا نص عليها القاضي في حكمه بالإدانة[1].

لعلنا نلاحظ الاختلاف بين صياغة المادة (42) ونص المادة (43) من المرسوم اتحادي بقانون رقم (5) لسنة 2012 والتي جاءت بعبارة: (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...)، مما يعني أن للمحكمة سلطة جوازيه، خاضعة لسلطتها التقديرية، بينما الحكم بالمصادرة في المادة (42) مُلزِم للمحكمة بشرط أن ينفذ دون إخلال بحقوق الآخرين حسني النية.

[1]- د.مصطفى فهمي الجوهري – النظرية العامة للجزاء الجنائي – كلية شرطة دبي 2007، ص243

المطلب الثاني: الظروف المشددة

يقصد بالظروف المشددة للعقاب العناصر الإضافية التي تتعلق أحياناً بالجريمة، ويقدر المشرع خطورتها فيشدد العقوبة المقررة عليها[1]، منها ما هو وجوبي يلزم بتشديد العقوبة مثل سبق الإصرار والترصد في جريمة القتل وظرف الليل في جريمة السرقة، ومنها ما هو جوازي يُعرف (بالظروف المشددة الجوازية) يُترك أمر تقديره والأخذ به للقاضي، وذلك حسب كل حالة[2].

وقد لاحظنا في الفصل الأول من هذه الدراسة المنهج الذي اتبعه المشرع الوطني في التدرج في تشديد العقوبة على جرائم الدخول غير المشروع لنظام المعالجة الآلية للمعطيات الإلكترونية، بحسب اختلاف النشاط المكون للجريمة، ومدى إخلال الجريمة بالسلامة والأمان والخصوصية في النظام المعلوماتي، وذلك وفقاً للشروط القانونية التي يحددها في كل نص تشريعي.

الفرع الأول: أن يترتب على الدخول غير المشروع قصد الحصول على بيانات حكومية أو معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية

نصت المادة الرابعة من المرسوم اتحادي بقانون رقم (5) لسنة 2012 على: (يعاقب بالسجن المؤقت والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون وخمسمائة ألف درهم كل من دخل بدون تصريح إلى موقع إلكتروني، أو نظام معلومات إلكتروني، أو شبكة معلوماتية، أو وسيلة تقنية معلومات، سواء كان الدخول، بقصد الحصول على بيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية، أو تجارية، أو اقتصادية).

وتكون العقوبة السجن مدة لا تقل عن خمس 5 سنوات والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز 2 مليون درهم، إذا تعرضت هذه البيانات أو المعلومات للإلغاء أو الحذف أو الإتلاف أو التدمير أو الإفشاء أو التغيير أو النسخ أو النشر أو إعادة النشر).

---

[1]- د.غنام محمد غنام - شرح قانون العقوبات الاتحادي – مرجع سابق - ص 518.
[2]- د. محمد زكي أبو عامر – مرجع سابق – ص 448.

يتضح من هذا النص ما نعنيه بمفهوم التناسب بين الجريمة والعقوبة، والتدرج في تشديد العقوبة من خلال العقوبة المشددة لجريمة الدخول بدون تصريح المنصوص عليها في الفقرة الأولى من هذه المادة، حيث أن الدخول الغير مشروع في هذه المادة جاء بقصد الحصول على بيانات حكومية أو معلومات سرية خاصة بمنشآت ذات طبيعة هامة.

هذه المنشآت إما أن تكون منشآت مالية أو تجارية أو اقتصادية، خصها المشرع بحماية خاصة، ميَّزها بها لأهمية النشاط الذي تمارسه، وأثره على الاقتصاد الوطني، وحركة تدفق الاستثمار الأجنبي وعنايةً من المشرع بمفاهيم اقتصادية عليا واجبة الحماية، في ظل اقتصاد السوق الحر والتجارة الإلكترونية والسوق الإلكترونية.

يلاحظ أن المشرع في هذه المادة صنف هذه الجريمة ضمن الجنايات وقرر لها عقوبة السجن المؤقت والغرامة التي لا تقل عن 250.000 درهم ولا تجاوز 1.500.000 درهم دون أن يترك للمحكمة خياراً بتطبيق إحدى العقوبتين وإنما جعلهما وجوبيتين يتعين على المحكمة القضاء بهما معاً.

ذلك على خلاف عقوبات الحبس والغرامة، التي كان المشرع قد قررهما في المادة الثانية والثالثة على جرائم الدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات الإلكترونية السابقة لهذه الجريمة، والتي كنا قد تناولناها في الفصل الأول من هذه الدراسة، حيث تم تصنيف تلك الجرائم ضمن الجنح، كما أن المشرع ترك للمحكمة خياراً بأن توقع أي من العقوبتين أعلاه على الجاني إذا رأت ذلك.

ثم أن المشرع تدرج في العقوبة التي توقع على هذه الجريمة على مرحلتين، المرحلة الأولى عندما تتعلق واقعة الجريمة بالدخول على النظام المعلوماتي بدون تصريح بقصد الحصول على بيانات حكومية أو معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية، فقد قرر

المشرع عقوبتها بالسجن المؤقت والغرامة التي لا تقل عن 250.000 درهم ولا تجاوز 1.500.000 درهم.

أما المرحلة الثانية التي شدد فيها المشرع العقوبة وتدرج فيها، بأن قرر فيها عقوبة تتعرض البيانات الحكومية أو المعلومات السرية الخاصة بالمنشآت المالية أو للإلغاء أو الحذف أو الإتلاف أو التدمير أو الإفشاء أو التغيير أو النسخ أو النشر أو إعادة النشر، وذلك بأن جعل العقوبة هي السجن مدة لا تقل عن خمس سنوات والغرامة التي لا تقل عن 500.000 درهم ولا تجاوز 2.000.000 درهم، وهذا ما سنتناوله في الفرع التالي.

الفرع الثاني: العقوبة المشددة

تنص الفقرة الثانية من المادة الرابعة من المرسوم اتحادي بقانون رقم (5) لسنة 2012 في شان مكافحة جرائم تقنية المعلومات على: (وتكون العقوبة السجن مدة لا تقل عن خمس (5) سنوات والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز (2) مليون درهم، إذا تعرضت هذه البيانات أو المعلومات للإلغاء أو الحذف أو الإتلاف أو التدمير أو الإفشاء أو التغيير أو النسخ أو النشر أو إعادة النشر).

تتجسد هذه الجناية في جريمة الدخول بدون تصريح والإضرار ببيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية سواءً تمثل هذا الإضرار في الإلغاء أو الحذف أو الإتلاف أو التدمير أو الإفشاء أو التغيير أو النسخ أو النشر وإعادة النشر، فالمشرع اعتبر هذا الإضرار ظرفاً مشدداً[1].

حين تتعرض البيانات الحكومية أو البيانات السرية الخاصة بالمنشآت المالية أو التجارية أو الاقتصادية لأيٍ من الأضرار التي اشتمل عليها نص الفقرة الثانية من المادة الرابعة من المرسوم اتحادي بقانون رقم (5) لسنة 2012 فالجاني في هذه الحالة دخل إلى النظام المعلوماتي

[1]- د.عبد الرازق الموافي عبد اللطيف – مرجع سابق – ص 45.

بدون تصريح بقصد الحصول على البيانات أو المعلومات السرية، وقد أدى ذلك إلى المساس بسلامة البيانات أو التأثير السلبي عليها بإحدى الصور التسع الواردة في النص[1].

مع ملاحظة أن المشرع لم يشترط في هذه الحالة ان يكون دخول الجاني إلى النظام المعلوماتي بقصد إلغاء أو حذف أو إتلاف أو تدمير أو إفشاء أو تغيير أو نسخ أو نشر أو إعادة نشر البيانات أو المعلومات المذكورة في النص[2]، بل يكفي نية الجاني الدخول بدون تصريح بقصد الحصول على البيانات أو المعلومات السرية المذكورة في النص، دون أن ينصرف قصده الجنائي إلى تحقيق النتائج التسع الواردة في النص، لذا فإن الظرف المشدد ينطبق في حالة ترتب هذه النتائج بصورة عرضية، كما ينطبق – ومن باب أولى – إذا كان الجاني قد قصد إحداثه[3].

وكان المشرع في القانون (الملغي) يقصر نطاق تطبيق الظرف المشدد على الحالة التي يترتب فيها على الدخول إلغاء البيانات والمعلومات أو إتلافها أو تدميرها أو نشرها، إلاّ أنه جاء في المرسوم بقانون الحالي ووسع من ذلك النطاق، فأضاف إلى ما سبق حذف أو إفشاء أو تغيير أو نسخ أو إعادة نشر البيانات أو المعلومات السرية على النحو الوارد في النص[4].

تعد صورة التجريم الواردة في الفقرة الثانية من المادة الرابعة من المرسوم بقانون ضمن طائفة الجرائم المشددة بحدوث النتيجة[5]، وتتميز الأفعال التي تُعدُ ظروفاً مشددة الواردة في هذه الفقرة بأن وقوع أي فعلٍ منها يكفى لتشديد العقوبة، ولا يلزم ان تقع جميعها، كما أن وقوع أكثر من فعلٍ من هذه الأفعال والنتائج لا يترتب عليه تعدداً في الظروف المشددة، بل يتوافر به ظرف واحد فقط.

---

[1]- المستشار علاء فكري اباظة – مرجع سابق – ص 56.
[2]- د.عبد الرازق الموافي عبد اللطيف – المرجع السابق – ص 45.
[3]- المستشار علاء فكري اباظة – المرجع السابق – ص 56.
[4]- المرجع السابق – ص 56.
[5]- د.عبد الرازق الموافي عبد اللطيف – المرجع السابق – ص 46.

لكي تقوم هذه الجريمة في صورتها المشددة يلزم ارتكاب الجاني لفعل الدخول وقوع إضرار بالبيانات الحكومية، أو بمعلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية في أي صورة من الصور التسع التي وردت في نص الفقرة الثانية من المادة الرابعة من المرسوم اتحادي بقانون بشأن مكافحة جرائم تقنية المعلومات، مع ملاحظة أن نص هذه الفقرة يتفق مع نص الفقرة الثانية من المادة الثانية من نفس المرسوم بقانون في بعض الامور[1].

فإذا كان الدخول بهدف ارتكاب أي من تلك الأفعال أو تحقيق أي من النتائج التي ينص عليها في الفقرة الثانية من المادة الرابعة، فإن العقوبة يتم تشديدها بحق الجاني على النحو المذكور في النص.

كما يلزم توافر رابطة سببية بين فعل الدخول بدون تصريح، وبين الإضرار الذي حدث، ويعتبر هذا شرطاً طبيعياً لكي تقوم هذه الجريمة، وفي حال عدم توافر رابطة السببية لا يتوافر الظرف المشدد ويعاقب الجاني على الجريمة في صورتها البسيطة المنصوص عليها في الفقرة الأولى من المادة الرابعة[2].

الجريمة المنصوص عليها في الفقرة الثانية من المادة الرابعة من المرسوم الاتحادي جريمة عمدية، وهي لا تختلف من حيث الركن المعنوي عن مثيلتها الواردة في الفقرة الأولى، إذ يأخذ الركن المعنوي فيها صورة القصد الجنائي، وينصرف هذا القصد إلى القصد العام، والقصد الخاص، فيجب أن يتوافر لدى الجاني القصد العام بعنصريه العلم والإرادة، وأن يتوافر ليه ايضاً قصداً خاصاً يتمثل في قصد الحصول على بيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية.

---

[1]- د. عبد الرازق الموافي عبد اللطيف – المرجع السابق – ص 46.
[2]- المرجع السابق – ص 47.

قررت الفقرة الثانية من المادة الرابعة من المرسوم اتحادي بقانون رقم (5) لسنة 2012 تشديد عقوبة جريمة الدخول بدون تصريح على نظام معلوماتي بقصد الحصول على بيانات حكومية أو معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية، إذا تعرضت هذه البيانات الحكومية أو المعلومات السرية للإلغاء أو الحذف أو الإتلاف أو التدمير أو الإفشاء أو التغيير أو النسخ أو النشر أو إعادة النشر.

حيث نصت هذه الفقرة على أن تكون العقوبة السجن مدة لا تقل عن خمس سنوات، والغرامة التي لا تقل عن 500.000 درهم و لا تجاوز 2.000.000 درهم، من ذلك نلاحظ أن المشرع قد شدد العقوبة في هذه الجريمة بدرجة أعلى من العقوبة المقررة على الجريمة في الفقرة الأولى من نفس المادة، واستناداً إلى هذه العقوبة فإن المشرع اعتبرها من الجنايات، ثم شدد العقوبة بأن جعل الحد الأدنى من السجن خمس سنوات بدلاً عن عقوبة السجن المؤقت التي كانت مقررة في الفقرة الأولى من هذه المادة، كما رفع من قيمة الغرامة بأن جعل حدها الأدنى لا يقل عن 500.000 درهم ورفع حدها الأعلى بأن نص على أنه لا يجاوز 2.000.000 درهم.

علماً بأن المحكمة لها الحق في أن تحكم بالعقوبات الفرعية والعقوبات التكميلية الأخرى، لا سيما توقيع التدابير الجنائية التي يلزم المرسوم اتحادي بقانون رقم (5) لسنة 2012 بشأن جرائم تقنية المعلومات المحكمة بتوقيعها على الجاني عند الإدانة بأي من جرائم تقنية المعلومات بصفةٍ عامة، وجرائم الدخول غير المشروع إلى النظام المعلوماتي بمختلف أنواعها على وجه الخصوص.

المبحث الثالث: التدابير المقررة لجرائم الدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات الإلكترونية

لم تعد العقوبة وحدها وسيلة المجتمع في كفاحه ضد الجريمة، لأن العقوبة قد أخفقت في مواطن عدة عن تحقيق الهدف المنشود منها في مكافحة الجريمة، الأمر الذي استلزم البحث عن جزاء بديل يحل محل العقوبة أو يقوم معها على تحقيق الهدف المأمول منها[1].

يقصد بالتدابير الجنائية الإجراءات التي تأمر بها المحكمة بالإضافة إلى العقوبات الأصلية[2]، أوهي مجموعة الإجراءات العلاجية التي يرصدها المجتمع للدفاع عن نفسه ومواجهة حالات الخطورة الإجرامية[3]، مع ملاحظة أن بعض هذه التدابير في طبيعتها عبارة عن علاج للمجرم والمقصود منها إفادته ومعالجة خطورته، مثل الإلزام بالعمل والإبعاد وحظر ممارسة عمل معين، والتي يجوز للمحكمة أن تأمر بأحدهما بدلاً من الحكم بعقوبة سالبة للحرية.

تنقسم التدابير الجنائية إلى تدابير مقيدة للحرية وأخرى سالبة للحقوق وتدابير مادية[4]، حيث قررت ذلك المادة (109) من قانون العقوبات الاتحادي رقم (3) لسنة 1987 وتعديلاته، ونصت على أن التدابير الجنائية إما أن تكون مقيدة للحرية أو سالبة للحقوق أو مادية، فيما أوضحت المادة (110) من قانون العقوبات الاتحادي رقم (3) لسنة 1987 وتعديلاته أن التدابير المقيدة للحرية هي: 1- حظر ارتياد بعض المحال العامة 2- منع الإقامة في مكان معين 3- المراقبة 4- الخدمة المجتمعية 5- الإبعاد عن الدولة.

أما المادة (122) من قانون العقوبات الاتحادي فقد نصت على أن التدابير السالبة للحقوق والتدابير المادية هي 1- إسقاط الولاية أو الوصاية أو القوامة أو الوكالة عن الغائب 2- حظر ممارسة عمل معين 3- سحب ترخيص القيادة 4- إغلاق المحل.

---

[1]- د.محمد زكي أبو عامر – مرجع سابق – ص 402.
[2]- د.غنام محمد غنام - شرح قانون العقوبات الاتحادي – مرجع سابق – ص 564.
[3]- د.محمد زكي أبو عامر – المرجع السابق – ص 402.
[4]- د.غنام محمد غنام - شرح قانون العقوبات الاتحادي – المرجع السابق – ص 564.

أما في شأن مكافحة جرائم تقنية المعلومات، فقد اختص المشرع الوطني جرائم تقنية المعلومات بالعديد من التدابير الجنائية التي نص عليها في المواد (41، 42، 43) من المرسوم بقانون اتحادي رقم (5) لسنة 2012 وتعديلاته، فنجد أن المادة (41) اشتملت على[1] تدبير محو وإعدام المعلومات أو البيانات المستخدمة في ارتكاب الجريمة و تدبير إغلاق المحل أو الموقع الذي يرتكب فيه أي من جرائم تقنية المعلومات، أما المادة (42) فقد نصت على تدبير إبعاد الأجنبي عن الدولة[2]، فيما اشتملت المادة (43) على تدبير وضع المحكوم عليه تحت الإشراف أو المراقبة، وتدبير الحرمان من استخدام النظام المعلوماتي، وتدبير وضع المحكوم عليه في مأوى علاجي أو مركز تأهيل للمدة التي تراها المحكمة مناسبة[3].

وبناء عليه نتناول في هذا المبحث التدابير الجنائية وذلك في مطلبين نخصص الأول منهما لدراسة التدابير المقيدة للحرية حيث نتناول بالدراسة في الفرع الأول تدبير وضع المحكوم عليه تحت الإشراف أو المراقبة، والفرع الثاني لتدبير إبعاد الأجنبي عن الدولة، ونتناول في الفرع الثالث تدبير محو وإعدام المعلومات أو البيانات، أما المطلب الثاني فنخصصه لدراسة التدابير السالبة للحقوق والتدابير المادية، حيث نتناول في الفرع الأول تدبير حرمان المحكوم عليه من استخدام النظام المعلوماتي، وفي الفرع الثاني تدبير وضع المحكوم عليه في مأوى علاجي أو مركز تأهيل والفرع الثالث تدبير إغلاق المحل أو الموقع، وذلك على النحو التالي:

---

[1]- تنص المادة (41) من المرسوم بقانون اتحادي رقم (5) لسنة 2012 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)

[2]- تنص المادة (42) من المرسوم بقانون اتحادي رقم (5) لسنة 2012 بعد تعديلها في 24 يوليو 2018 بموجب المرسوم بقانون اتحادي رقم (2) لسنة 2018 على أنه: (مع مراعاة الفقرة الثانية من المادة (121) من قانون العقوبات 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) .

[3]- تنص المادة (43) من المرسوم بقانون اتحادي رقم (5) لسنة 2012: (مع عدم الإخلال بالعقوبات المنصوص عليها في هذا المرسوم اتحادي 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).

المطلب الأول: التدابير المقيدة للحرية

لا تنفذ هذه التدابير داخل مؤسسات مغلقة وإنما في وسط حر، فسلب الحرية ليس هدفاً فيها بل هي تترك الجاني حراً من حيث الأصل، وإن كانت هذه الحرية يوجد عليها بعض القيود على ممارستها وهي قيود لا تفرض بطبيعة الحال على الشخص العادي وسوف أتطرق لأهم هذه التدابير.

الفرع الأول: وضع المحكوم عليه تحت الإشراف أو المراقبة

علمنا أن المادة (43) من المرسوم اتحادي رقم (5) لسنة 2012 تنص على أنه: (مع عدم الإخلال بالعقوبات المنصوص عليها في هذا المرسوم اتحادي 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).

تقضي المحكمة بوضع المحكوم عليه تحت الإشراف أو المراقبة[1]، ونلاحظ من ظاهر هذا النص أن سلطة المحكمة في توقيع عقوبة الاشراف أو المراقبة عند الإدانة بجريمة من جرائم تقنية المعلومات سلطة جوازيه وليست إلزامية تخضع لسلطة المحكمة التقديرية متى توافرت شروطها وفقاً ًلأحكام قانون العقوبات الاتحادي والمرسوم رقم (5) لسنة 2012 في شأن جرائم تقنية المعلومات.

لم يحدد المشرع في هذه المادة أو المرسوم اتحادي بقانون رقم (5) مدة الوضع تحت الإشراف أو المراقبة، حيث جاءت عبارتها في عجز المادة (43): (..... للمدة التي تراها

[1]- تعتبر المراقبة من التدابير المقيدة للحرية التي نصت عليها المادة 110 من قانون العقوبات الاتحادي رقم (3) لسنة 1987، وقد عرفتها المادة (115) من نفس القانون بأنها: (إلزام المحكوم عليه بكل أو بعض القيود التي يقررها الحكم) فيما قررت أن القيود هي: أن لا يغير محل إقامته إلا بعد موافقة الجهة الإدارية المختصة، وأن يُقدم نفسه إلى الجهة الإدارية المختصة في الفترات الدورية التي تحددها، وأن لا يرتاد الأماكن التي حددها الحكم، وأن لا يبرح مسكنه ليلاً، إلا بإذن من الجهة الإدارية المختصة.

المحكمة مناسبة)، وقد يفهم من هذا النص أن المشرع ترك للمحكمة أمر تحديد مدة المراقبة، إلاّ أنه وإن كان ذلك المفهوم متحقق بالفعل، إلاّ أن سلطة تحديد المدة تكون في إطار القيد العام لمدة المراقبة والذي تنص عليه المادة (117) من قانون العقوبات الاتحادي المعدل[1].

وفقاً للمادة (117) من قانون العقوبات الاتحادي المعدل فإنه يجوز للمحكمة أن تأمر بوضع المحكوم عليه تحت المراقبة إذا حكمت في مواد الجنايات بعقوبة سالبة للحرية مدة تزيد على سنة، ولا يجوز أن تزيد مدة المراقبة في هذه الحالة عن خمس سنوات ولا تزيد على مدة العقوبة[2].

ويمكن تعريف الوضع تحت المراقبة بأنه إلزام المحكوم عليه بكل أو بعض القيود التي تقررها المادة 115 من قانون العقوبات الاتحادي رقم (3) لسنة 1987 لدولة الإمارات العربية المتحدة وتعديلاته وفقاً لما يقرره الحكم والقيود هي[3]:

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

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

3- أن لا يرتاد الأماكن التي حددها الحكم.

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

5- وفي جميع الأحوال تطبق القواعد التي يصدر بتحديدها قرار من وزير الداخلية بهذا الشأن.

---

[1]- تنص المادة (117) من قانون العقوبات الاتحادي لسنة 1987 وتعديلاته على: (إذا حكم على شخص بالسجن المؤبد أو المؤقت لجناية ماسة بأمن الدولة الخارجي أو الداخلي تعين الحكم بالمراقبة مدة لا تزيد على خمس سنوات، وللمحكمة عند الحكم في جناية بعقوبة سالبة للحرية مدة تزيد على سنة أن تحكم بالمراقبة مدة لا تجاوز خمس سنوات ولا تزيد على مدة العقوبة).

[2]- د. غنام محمد غنام - شرح قانون العقوبات الاتحادي - مرجع سابق – ص 567.

[3]- المرجع السابق – ص 566.

بالنسبة لوضع المحكوم عليه تحت الإشراف، فلم يشر قانون العقوبات الاتحادي وتعديلاته إلى هذا التدبير ضمن نصوصه، كما أن المادة (43) من المرسوم اتحادي بقانون رقم (5) لسنة 2012 لم يحدد مدة الوضع تحت الإشراف، لذا فالوضع تحت الإشراف تدبير جوازي وليس ملزماً، يُمكن أن تقضي به المحكمة عند الإدانة بجريمة من جرائم تقنية المعلومات متى توافرت شروطه ووفقاً لسلطتها التقديرية، وللمدة التي تراها مناسبة عن أي جريمة وردت في المرسوم[1].

الفرع الثاني: إبعاد المحكوم عليه الأجنبي عن الدولة

كانت المادة (42) من المرسوم اتحادي رقم (5) لسنة 2012 تنص على أن: (تقضي المحكمة بإبعاد الأجنبي الذي يحكم عليه بالإدانة لارتكاب أي جريمة من الجرائم المنصوص عليها في هذا المرسوم اتحادي بقانون وذلك بعد تنفيذ العقوبة المحكوم بها)، إلاّ أنه في 24 يوليو 2018 تم تعديل هذه المادة بموجب المرسوم اتحادي بقانون رقم (2) لسنة 2018، والذي نص على (مع مراعاة الفقرة الثانية من المادة (121) من قانون العقوبات 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) .

الإبعاد عن الدولة أحد التدابير الجنائية المقيدة للحرية وفقاً للفقرة (5) من المادة (110)[2] من قانون العقوبات الاتحادي 1987 وتعديلاته، وتقرر المادة (121)[3] من قانون العقوبات الاتحادي وتعديلاته نوعين من الإبعاد، الأول هو الإبعاد الوجوبي، أما الثاني فهو الإبعاد الجوازي وتكون للمحكمة فيه سلطة جوازيه[4].

---

[1]- المستشار علاء فكري اباظة – مرجع سابق – ص264.

[2]- سبق ان اوردنا نص المادة (110) في بداية هذا المطلب فنحيل اليه، منعاً للتكرار.

[3]- تنص المادة (121) من قانون العقوبات الاتحادي لسنة 1987 وتعديلاته على: (إذا حكم على أجنبي في جناية بعقوبة مقيدة للحرية أو في الجرائم الواقعة على العرض وجب الحكم بإبعاده عن الدولة، ويجوز للمحكمة في مواد الجنح الأخرى أن تأمر بإبعاده عن الدولة أو الحكم بالإبعاد بدلا من الحكم عليه بالعقوبة المقيدة للحرية).

[4]- د.غنام محمد غنام - شرح قانون العقوبات الاتحادي - مرجع سابق – ص 573.

ووفقاً للقواعد العامة في قانون العقوبات الاتحادي يكون إبعاد الأجنبي عن الدولة وجوبياً إذا حكم عليه في جناية واقعة على العرض بعقوبة مقيدة للحرية، ويكون الإبعاد جوازياً للمحكمة عندما تحكم على أجنبي بعقوبة مقيدة للحرية في مواد الجنح الأخرى، كما يجوز للمحكمة في مواد الجنح الحكم بالإبعاد بدلاً عن الحكم على الأجنبي بالعقوبة المقيدة للحرية المقررة للجنحة، وذلك وفقاً للمادة (121) السابق الإشارة إليها.

أما المادة (42) من المرسوم اتحادي رقم (5) فقد كانت تقرر إبعاد الأجنبي عن الدولة وجوبياً عند الإدانة بارتكاب أي جريمة من الجرائم المنصوص عليها في المرسوم، ووضعت شرطاً بأن يتم إبعاده بعد تنفيذ العقوبة المحكوم بها، ثم تم تعديلها بالمرسوم بقانون اتحادي رقم (2) لسنة 2018 والذي حصر الإبعاد الوجوبي في الجرائم الواقعة على العرض والجنايات، وذلك دون الاخلال بالمادة 121 من قانون العقوبات الاتحادي السابق الاشارة اليها.

لذا وسيراً على هدى قانون مكافحة جرائم تقنية المعلومات لسنة 2006 (الملغي) فقد قضت محكمة النقض[1]: (بوجوب الحكم بإبعاد الأجنبي عن الدولة متى قضي بحبسه في إحدى الجرائم المنصوص عليها في القانون رقم (2) لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات، وأن مخالفة ذلك يعتبر خطأ في تطبيق القانون توجب نقض الحكم جزئياً وتصحيحه بإضافة عقوبة الإبعاد إلى عقوبة الحبس المقضي بها).

وفي حكم آخر صدر من محكمة النقض قبل تعديل المرسوم اتحادي بقانون رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات فقد قضت محكمة النقض[2] بأنه: (لما كانت المادة (42) من القانون رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات قد أوجبت على المحكمة أن تقضي بإبعاد الأجنبي الذي يحكم عليه بالإدانة لارتكاب اي جريمة من الجرائم

---

[1]- الطعن رقم 769 لسنة 2010 س 4 ق.أ، مجموعة الأحكام والمبادئ القانونية الصادرة عن محكمة النقض من الدائرة الجزائية - السنة القضائية الرابعة 2010 – الجزء الثالث – ص 1086

[2]- الطعن رقم 402 لسنة 2013 س 7 ق.أ، سبق الاشارة إليه في هذه الدراسة ص 21

المنصوص عليها في هذا القانون بعد تنفيذ العقوبة المحكوم بها، لما كان ذلك وكان الحكم المطعون فيه قد أدان المطعون ضده وهو أجنبي بالحبس لمدة شهرين وألغى تدبير الإبعاد فإنه يكون قد خالف القانون، بما يوجب نقضه وتصحيحه بإضافة تدبير الإبعاد).

لابد أن نشير إلى أن المرسوم اتحادي رقم (5) لسنة 2012 بشأن جرائم تقنية المعلومات احدث تطوراً فيما يتعلق بتدبير إبعاد الأجنبي عن الدولة، وذلك على النحو التالي:

1- أن القانون (الملغي) كان يقرر في المادة (25) منه إبعاد الأجنبي عن الدولة عندما يحكم عليه بالحبس وفقا لأحكام هذا القانون.

2- وسع المرسوم اتحادي بقانون رقم (5) لسنة 2012 من دائرة إبعاد الأجنبي عن الدولة، حيث ألزم المحكمة بأن تبعد الأجنبي عن الدولة متى ما قضت بإدانته بأي من الجرائم المنصوص عليها في قانون مكافحة جرائم تقنية المعلومات بغض النظر عما تكون عليه عقوبتها، وهل هي الحبس أو الغرامة.

3- عاد المشرع في التعديل الأخير في 24 يوليو 2018 وحصر تدبير الإبعاد في جرائم تقنية المعلومات الواقعة على العرض وفي الجنايات.

مما سبق نجد أنه ووفقاً لنص المادة (42) فإن شرط وجوب إبعاد الأجنبي عن الدولة هو أن تتم إدانته بارتكاب إحدى الجرائم الواقعة على العرض وفي الجنايات المنصوص عليها في المرسوم اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات، وأن تنفيذ أمر الإبعاد عن الدولة لا يتم إلاّ بعد تنفيذ العقوبة المحكوم بها.

الفرع الثالث: محو وإعدام المعلومات أو البيانات

تدبير محو وإعدام المعلومات والبيانات استحدثه المشرع بنص المادة (41) من المرسوم بقانون رقم (5) لسنة 2012، حيث لم يرد النص عليه في القانون (الملغي)، كما أنه لم يرد النص

عليه ضمن التدابير المقيدة للحرية المنصوص عليها في المادة (110) من قانون العقوبات الاتحادي رقم (3) لسنة 1987 وتعديلاته، أو ضمن التدابير السالبة للحرية المنصوص عليها في المادة (122) من قانون العقوبات الاتحادي، كما أنه لم يرد ضمن تدابير الدفاع الإجتماعي المنصوص عليها في المادة (136) من قانون العقوبات الاتحادي.

إذ أن التدابير الجنائية تستهدف القضاء على خطورة الجاني الإجرامية، وتستعين في سبيل تحقيق ذلك بمجموعة من الأساليب العلاجية، كما هو الأمر في أسلوب إيداع المجرم المجنون في المحل المخصص له، أو الأساليب التهذيبية كمعظم التدابير التي تتخذ مع المجرم الحدث، والتي تؤدي إما إلى تأهيل المجرم وإصلاحه أو المباعدة بينه وبين الظروف أو الوسائل التي تتيح له الإجرام.

ويلاحظ أنه وإن كان مفهوماً فكرة محو المعلومات أو البيانات، فإنه من غير المفهوم البتة تقبل فكرة إعدام هذه المعلومات أو تلك البيانات التي أشار اليها النص القانوني، فالإعدام لا يرد إلاّ على المحتوى المادي الملموس، أما المعلومات والبيانات فيرد عليها المحو والحذف أو الإلغاء[1].

باستقراء نص المادة (41) من المرسوم بقانون اتحادي رقم (5) لسنة 2012 نجد أن تدبير محو المعلومات أو البيانات أو إعدامها، هو تدبير وجوبي ملزم للمحكمة لا تملك أي سلطة تقديرية بشأنه حيث جاءت عبارة نص المادة (41) ملزمة: (يحكم في جميع الأحوال).

المطلب الثاني: التدابير السالبة للحقوق والتدابير المادية

سوف أتطرق في هذا المطلب إلى بعض التدابير السالبة للحقوق والتدابير المادية التي توقع على مرتكبي الجرائم المنصوص عليها في المرسوم بقانون السالف ذكره، والتي تم تقسيمها إلى ثلاثة أفرع وهي كالتالي:

---

[1]- المستشار علاء فكري اباظة – مرجع سابق - ص 250.

الفرع الأول: حرمان المحكوم عليه من استخدام أي شبكة معلوماتية أو نظام المعلومات الإلكتروني أو أي وسيلة تقنية معلومات أخرى

قررت هذا التدبير أيضاً المادة (43) من المرسوم اتحادي رقم (5) لسنة 2012 حيث أجازت للمحكمة أن تأمر بحرمان الجاني من استخدام أي شبكة معلوماتية أو النظام المعلوماتي الإلكتروني أو أي وسيلة تقنية معلومات أخرى، وذلك للمدة التي تراها مناسبة ، ودون الإخلال بالعقوبات المنصوص عليها في هذا المرسوم اتحادي.

يلاحظ أن قانون العقوبات الاتحادي رقم (3) لسنة 1987 وتعديلاته خلت تماماً من أي إشارة إلى تدبير حرمان المحكوم عليه من استخدام شيء من ضمن التدابير التي نص عليها، فهناك تدابير تتعلق بحظر ارتياد محال عامة أو منع الإقامة في مكان معين[1]، كما لم ينص القانون (الملغي) على هذا التدبير.

بموجب تدبير الحرمان فإنه يجوز للمحكمة أن تأمر بحرمان المحكوم عليه من استخدام شبكة الانترنت أو أي وسيلة تقنية معلومات أو نظام المعلومات الإلكتروني، وبوجه عام تحرمه من استخدام نظام المعلوماتية. ولم ينص المرسوم بقانون على مدة الحرمان، إلاّ أن قانون العقوبات الاتحادي لسنة 1987 وتعديلاته نصّ في المادة (75) منه على أنه لا يجوز أن تزيد مدة الحرمان على ثلاث سنوات من تاريخ الانتهاء من تنفيذ العقوبة وذلك بالنسبة للمزايا التي اشتمل عليها نص المادة (75).

ويعتبر الحرمان من بعض المزايا من العقوبات التكميلية التبعية التي تلحق بالعقوبة المحكوم بها بقوة القانون دون حاجة الى النص عليه في الحكم و ذلك على النحو والشروط التي

[1]- المستشار علاء فكري اباظة – المرجع السابق - ص 265 .

يحددها القانون من حيث نوع العقوبة التي يطبق عليها تدبير الحرمان، وهي السجن المؤبد والسجن المؤقت، والجنايات التي يحكم فيها بالحبس[1].

ووفقاً لما تقدم فإن من الواجب على الجهة التشريعية أو التنفيذية أن تضع اللوائح المنظمة لتنفيذ تدبير الحرمان من النظام المعلوماتي، إذ أن تنفيذ هذا الحرمان على أرض الواقع ستتبعه الكثير من التعقيدات.

الفرع الثاني: وضع المحكوم عليه في مأوى علاجي أو مركز تأهيل

الهدف من وضع المحكوم في مأوى علاجي أو مركز تأهيل هو علاج خطورته على المجتمع بمختلف الأساليب الطبية والنفسية والعلمية، بقصد تأهيله للحياة الإجتماعية وتحويله إلى عضو نافع لمجتمعه، وقد يكون إدراك التأهيل أمراً عسيراً ولكن ليس أمام المجتمع أو الدولة سوى أن تحاول إصلاح مواطِنها وتأهيله[2].

كما سبق وأن أشرنا فقد ورد النص على تدبير وضع المحكوم في مأوى علاجي أو مركز تأهيل في المادة (43) من المرسوم اتحادي رقم (5) لسنة 2012 التي أجازت للمحكمة أن تأمر بوضع المحكوم عليه في مأوى علاجي أو مركز تأهيل للمدة التي تراها المحكمة مناسبة ، وذلك دون الإخلال بالعقوبات المنصوص عليها في هذا المرسوم اتحادي.

---

[1]- تنص المادة (80) من قانون العقوبات الاتحادي لسنة 1987 وتعديلاته على أن: (للمحكمة عند الحكم في جناية بالحبس أن تأمر بحرمان المحكوم عليه من حق أو مزية أو أكثر مما نص عليه في المادة (75) وذلك لمدة لا تقل عن سنة ولا تزيد على ثلاث سنوات تبدأ من نهاية تنفيذ العقوبة أو انقضائها لأي سبب أخر).

[2]- د. محمد زكي أبو عامر – مرجع سابق – ص 410.

يعتبر وضع المحكوم عليه في مأوى علاجي من تدابير الدفاع الاجتماعي[1]، وهو وسيلة من وسائل مواجهة الخطورة الاجتماعية[2] للشخص المصاب بجنون أو عاهة في العقل أو بمرض نفسي يفقده القدرة على التحكم في تصرفاته بحيث يخشى على سلامته الشخصية أو على سلامة الغير، والمعلوم أن القاعدة العامة - وفق ما يقرره قانون العقوبات الاتحادي وتعديلاته- هي أن المواجهة الاجتماعية تكون بالتدخل قبل وقوع الجريمة حمايةً للمجتمع وحرصاً على علاج المريض[3].

تنفيذ حكم الإيداع في مأوى علاجي وفقاً لنص الفقرة الأخيرة من المادة (43) من المرسوم اتحادي رقم (5) لسنة 2012 يتم من خلال إرسال المحكوم عليه إلى منشأة مخصصة لهذا الغرض، حيث يتلقى العناية التي تدعو إليها حالته[4]، ويتم تنفيذ الإيداع وفقاً لمقتضيات المادة (137) من قانون العقوبات الاتحادي رقم (3) لسنة 1987 وتعديلاته، ويلاحظ أن تدبير وضع المحكوم عليه في مركز تأهيل للمدة التي تراها المحكمة مناسبة ، هو تدبير مستحدث لم يرد ضمن نصوص قانون العقوبات الاتحادي المتعلقة بالتدابير الجنائية[5].

أما ما يتعلق بمدة الإيداع فقد ترك المشرع أمر تحديدها لسلطة المحكمة التقديرية، واكتفى بعبارة (للمدة التي تراها المحكمة مناسبة)، وذلك بالطبع دون أن يخل بالعقوبات المنصوص عليها في المرسوم اتحادي رقم (5) لسنة 2012.

---

[1]- نشير في ذلك إلى المادة (136) من قانون العقوبات الاتحادي رقم (3) لسنة 1987 وتعديلاته والتي تنص على: (تدابير الدفاع الاجتماعي هي: 1- الإيداع في مأوى علاجي . 2- الإيداع في إحدى مؤسسات العمل. 3- المراقبة. 4- الإلزام بالإقامة في الموطن الأصلي).

[2]- تنص المادة (135) من قانون العقوبات الاتحادي رقم (3) لسنة 1987 وتعديلاته على أنه: (تتوفر الخطورة الاجتماعية في الشخص إذا كان مصابا بجنون أو عاهة في العقل أو بمرض نفسي يفقده القدرة على التحكم في تصرفاته بحيث يخشى على سلامته شخصيا أو على سلامة غيره وفي هذه الحالة يودع المصاب مأوى علاجيا بقرار من المحكمة المختصة بناء على طلب النيابة العامة)

[3]- د. غنام محمد غنام - شرح قانون العقوبات الاتحادي - مرجع سابق – ص 588.

[4]- المستشار علاء فكري اباظة – مرجع سابق - ص 267 .

[5]– المرجع السابق - ص 269.

الفرع الثالث: إغلاق المحل أو الموقع

نصت على تدبير إغلاق المحل أو الموقع الفقرة الأخيرة من المادة (41) من المرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن جرائم تقنية المعلومات، وكان القانون رقم (2) لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات (الملغي) يشتمل أيضاً على تدبير إغلاق المحل أو الموقع، وذلك في المادة (24) التي تنص على: (مع عدم الإخلال بحقوق الغير حسن النية يحكم في جميع الأحوال بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا القانون أو الأموال المتحصلة منها، كما يحكم بإغلاق المحل أو الموقع الذي يرتكب فيه أي من هذه الجرائم اذا كانت الجريمة قد ارتكبت بعلم مالكه أو مديره، وذلك إغلاقا كليا أو للمدة التي تقدرها المحكمة).

ويلاحظ من خلال هذا النص أن القانون (الملغي) كان يشترط أن تكون الجريمة قد ارتكبت بعلم مالك المحل أو الموقع أو مديره، إلاّ أن المشرع ألغى هذا الشرط في المادة (41) من المرسوم اتحادي بقانون الحالي، مكتفياً بعبارة مع عدم الإخلال بحقوق الغير حسن النية التي تصدرت النص.

يعتبر إغلاق المحل من التدابير المادية السالبة للحقوق التي نصت عليها المادة (122) من قانون العقوبات الاتحادي رقم (3) لسنة 1987 وتعديلاته والتي سبق وأن أوردناها في بداية هذا المبحث، والهدف من تدبير إغلاق المحل أو الموقع للمباعدة بين الجاني ووسائل إجرامه.

يتم إغلاق المحل أو الموقع للمباعدة بين الجاني ووسائل إجرامه، ويأخذ إغلاق المحل شكلاً مادياً ينصب على المحل الذي استخدمه الجاني في جريمته أو عاد إليها منه[1]، ويتم تنفيذ تدبير إغلاق المحل بواسطة السلطات الادارية المختصة بالكيفية التي تراها مناسبة لكل حالة على حده، كأن تضع عليه الحراسة لمنع الدخول أو الخروج منه، أو أن تغلق أبوابه إغلاقاً فعلياً يحول

[1]- د. محمد زكي أبو عامر – مرجع سابق – ص 411.

دون ارتياده[1]، أما إغلاق الموقع فهو يأخذ شكلاً معنوياً من خلال قيام السلطات المختصة باتخاذ الوسائل الفنية الكفيلة بحجب ذلك الموقع من على شبكة الانترنت والحيلولة دون التعاطي معه[2].

[1]- المستشار علاء فكري اباظة – مرجع سابق - ص 253.
[2]– المرجع السابق - ص 254.

الخاتمة

بحمد الله وفضله وتوفيقه نكون قد أنهينا هذا البحث، الذي لا شك أنه يعتريه النقص، ولكن حسبي أنه عمل انساني لا بد أن يعتريه النقص، فالكمال لله وحده، وخلال هذا السفر بين سطور البحث ومراجعه، فقد خلصت إلى العديد من النتائج التي تجيب على تساؤلات البحث، كما توصلت إل العديد من القناعات التي يمكن أن تطرح من خلال التوصيات.

النتائج:

1- جريمة الدخول غير المشروع إلى النظام المعلوماتي من الجرائم المستحدثة التي عالجتها قوانين مكافحة جرائم تقنية المعلومات، وقد أوصت المؤتمرات الدولية لمكافحة جرائم تقنية المعلومات والحاسب الآلي بالنص عليها ضمن قوانين مكافحة جرائم تقنية المعلومات.

2- صدر أو تجريم للدخول غير المشروع إلى النظام المعلوماتي في الدولة بالمادة (2) من القانون الاتحادي رقم (2) لسنة 2006م بشأن مكافحة جرائم تقنية المعلومات ، ثم تلى ذلك المرسوم اتحادي بقانون رقم (5) لسنة 2012م بشأن مكافحة جرائم تقنية المعلومات، الذي عدّل في المادة (2) من القانون بأن حذف كلمة (عمداً) من النص السابق وبذلك غير من صفة الركن المعنوي للجريمة، وأصبح الجاني يُسأل عن جريمة الدخول غير المشروع إلى النظام المعلوماتي سواءً وقعت عمداً أم بطريق الخطأ.

3- جريمة الدخول غير المشروع إلى النظام المعلوماتي في صورتها المجردة تتمثل في ثلاث صور هي الدخول إلى النظام المعلوماتي بدون تصريح، أو بتجاوز حدود تصريح الدخول إلى النظام المعلوماتي، أو بالبقاء بصورة غير مشروعة في النظام المعلوماتي.

4- تعتبر جريمة الدخول غير المشروع إلى النظام المعلوماتي جريمة خطر وليست جريمة ضرر، ولا يشترط أن يترتب على الدخول غير المشروع أي نتيجة، مثل حدوث ضرر للشبكة

أو البيانات أو حدوث فائدة للجاني، وتُعد جريمةً تامةً بمجرد ارتكاب النشاط الإجرامي، وهو التدخل في النظام المعلوماتي دون موافقة صاحبه، حتى وإن لم يجد الجاني في الملفات ما يبحث عنه من معلومات أو بيانات، إذ أن دخول الجاني للنظام المعلوماتي دون أن يكون لديه تصريح بالدخول يُعد انتهاكاً أو اختراقاً لقواعد خصوصية وسائل تقنية المعلومات.

5- جريمة الدخول غير المشروع بقصد الحصول على بيانات حكومية أو معلومات سرية تتعلق بمنشآت مالية أو تجارية أو اقتصادية، من الجرائم التي يلزم للإدانة بها أن تتجه إرادة الجاني إلى فعل الدخول، مع توافر القصد الجنائي الخاص الذي يتمثل في قصد الجاني الحصول على بيانات حكومية، أو قصد الحصول على معلومات سرية خاصة بالمنشأة المالية أو التجارية أو الاقتصادية، وينتفي القصد الجنائي لهذه الجريمة إذا كان الجاني يعتقد أن البيانات لا تخص الحكومة، أو كان يعتقد أن هذه البيانات متاحة للجمهور وذلك متى كان اعتقاده مبنياً على مبررات مقبولة ومعقولة.

6- شدد المشرع العقوبة على جريمة الدخول غير المشروع إلى النظام المعلوماتي في صورتها المصحوبة باعتداءات على البيانات أو المعلومات، كما أنه تدرج في تشديد العقوبة، وذلك وفقاً لشروط حددها على سبيل الحصر في الفقرتين الثانية والثالثة من المادة (2)، وذلك متى ما كان ارتكاب الجاني لفعل الدخول قد تم بدون تصريح أو بتجاوز حدود التصريح أو أن البقاء في النظام المعلوماتي كان بصورة غير مشروعة.

7- شدد المشرع عقوبة جريمة الدخول غير المشروع بقصد الحصول على بيانات حكومية أو معلومات سرية تتعلق بمنشآت مالية أو تجارية أو اقتصادية، من جنحة يعاقب عليها بالحبس والغرامة إلى جناية يعاقب عليها بالسجن المؤقت والغرامة، وذلك لأهمية البيانات الحكومية، والمعلومات السرية الخاصة بالمنشآت المالية أو التجارية أو الاقتصادية، وتعلقهما بالأمن القومي أو الاقتصاد القومي أو المصالح العليا للدولة.

8- تدرج المشرع في العقاب على جرائم الدخول غير المشروع في النظام المعلوماتي، بأن صنف الجريمة في صورتها المجردة ضمن الجنح، وجعل العقوبة عليها الحبس أو الغرامة التي لا تقل عن 100.000 درهم ولا تزيد على 300.000 درهم أو بإحدى هاتين العقوبتين[1]، ثم شدد العقوبة عندما يكون الدخول غير المشروع مصحوباً باعتداءات على البيانات والمعلومات غير الشخصية، فأصبحت العقوبة الحبس لمدة لا تقل عن ستة أشهر والغرامة التي تقل عن 150.000 درهم ولا تجاوز 750.000 درهم أو بإحدى هاتين العقوبتين، ثم تدرج في التشديد وساوى بين عقوبة جريمة الإضرار بالبيانات أو المعلومات الشخصية، وجريمة الدخول أو الإضرار بالبيانات بمناسبة أو بسبب تأدية العمل وفرض عليهما عقوبة الحبس التي لا تقل مدتها عن سنة والغرامة التي لا تقل عن 250.000 درهم ولا تجاوز 1.000.000 درهم أو بإحدى هاتين العقوبتين .

أما عندما تعلق الدخول بقصد الحصول على بيانات حكومية أو معلومات سرية تخص المنشآت المالية والتجارية والاقتصادية فقد صنف هذه الجريمة ضمن الجنايات وقرر لها عقوبة السجن المؤقت والغرامة التي لا تقل عن 250.000 درهم ولا تجاوز 1.500.000 درهم، ثم شدد العقوبة بأن جعلها السجن مدة لا تقل عن خمس سنوات والغرامة التي لا تقل عن 500.000 درهم ولا تجاوز 2.000.000 درهم، وذلك عندما تتعرض هذه البيانات الحكومية أو المعلومات السرية الخاصة بالمنشآت للإلغاء أو الحذف أو الإتلاف أو التدمير أو الإفشاء أو التغيير أو النسخ أو النشر أو إعادة النشر.

9- اختص المشرع الوطني جرائم تقنية المعلومات بالعديد من التدابير الجنائية، بعضها مقيده للحرية مثل وضع المحكوم عليه تحت الإشراف أو المراقبة، وإبعاد المحكوم عليه الأجنبي عن الدولة، ومحو وإعدام المعلومات أو البيانات، والنوع الآخر تدابير مادية سالبة للحقوق مثل حرمان المحكوم عليه من استخدام أي شبكة معلوماتية أو نظام المعلومات الالكتروني أو أي

[1]- راجع المادة الثانية الفقرة (1) من المرسوم اتحادي رقم (5) لسنة 2012.

وسيلة تقنية معلومات أخرى، وضع المحكوم عليه في مأوى علاجي أو مركز تأهيل، وإغلاق المحل أو الموقع، وذلك في المواد (41، 42، 43) من المرسوم بقانون رقم (5) لسنة 2012.

التوصيات:

1- أن يضع المشرع في المرسوم الاتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات تعريفاً واضحاً لفعل الدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات الإلكترونية، وذلك أسوة بالمشرع الكويتي والذي عرفه في المادة الأولى من القانون رقم (63) لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات بأنه: (النفاذ المتعمد غير المشروع لأجهزة وأنظمة الحاسب الآلي أو لنظام معلوماتي أو شبكة معلوماتية أو موقع الكتروني من خلال اختراق وسائل وإجراءات الحماية لها بشكل جزئي أو كلي لأي غرض كان بدون تفويض في ذلك أو بالتجاوز للتفويض الممنوح).

2- أن ينص المشرع الوطني على عمدية فعل الدخول الغير مشروع إلى النظام المعلوماتي في صورتها المجردة حتى لا يتم تفسير النص الحالي على أنه يجيز وقوع الجريمة بشكل عمدي أو بشكل غير عمدي إعمالاً بنص المادة (43) من قانون العقوبات، خصوصاً أن أغلب التشريعات العربية قد نصت بشكل صريح على عمدية الدخول غير المشروع إلى النظام المعلوماتي.

3- أن يعتبر المشرع الاضرار بالبيانات بمناسبة أو بسبب تأدية العمل جناية يعاقب عليها بالسجن المؤقت والغرامة التي لا تقل عن 250.000 درهم ولا تجاوز 1.500.000 درهم، بدلاً عن عقوبة الحبس والغرامة الحالية، وذلك لخطورة مرتكب الجرم الذي يستغل مهنته وعمله في الإضرار بالآخرين، وذلك اسوةً بتشديد العقوبة في جريمة سرقة العاملين في قانون العقوبات الاتحادي.

4- أن يضيف المشرع إلى عقوبة جريمة الدخول بقصد الحصول على بيانات حكومية أو معلومات سرية تخص المنشآت المالية والتجارية والاقتصادية، ظرفاً مشدداً آخر غير الوارد في النص يتمثل في ارتكاب الجريمة بمناسبة أو بسبب تأدية العمل.

والحمد لله رب العالمين،،،

المراجع

أولاً: الكتب

1. د. أحمد خليفة الملط - الجرائم المعلوماتية - دار الفكر الجامعي الإسكندرية 2006.
2. د. أحمد فتحي سرور- الوسيط في قانون العقوبات القسم العام ط6 - دار النهضة العربية القاهرة 1996.
3. د. أحمد حسام طه تمام – جرائم الحاسب الآلي – دار النهضة العربية القاهرة ط1 سنة 2000.
4. د. أشرف توفيق شمس الدين – الحماية الجنائية للمستند الالكتروني – دراسة مقارنة ط1 – دار النهضة العربية – سنة 2006.
5. أ.د. إمام حسنين خليل عطا الله – الحماية الجنائية لوسائل تقنية المعلومات في التشريعات العربية – مركز الدراسات والاستطلاعات وزارة الداخلية دولة الامارات العربية المتحدة – سنة 2016.
6. د. أمير فرج يوسف – جرائم تقنية المعلومات بدول الخليج العربي – دار الكتب والدراسات العربية 2016.
7. د. أيمن عبدالله فكري – جرائم نظم المعلومات دراسة مقارنة – دار الجامعة الجديدة الاسكندرية -2007.
8. القاضي جلال محمد الزعبي والقاضي أسامة أحمد المناعسة – جرائم تقنية نظم المعلومات الإلكترونية – دراسة مقارنة – دار الثقافة للنشر والتوزيع الأردن – سنة 2010.
9. د. حسين بن سعيد الغافري – السياسة الجنائية في مواجهة جرائم الانترنت –دار النهضة العربية القاهرة 2009.
10. د. خالد ممدوح ابراهيم – الجرائم المعلوماتية – دار الفكر الجامعي الاسكندرية 2009.
11. المستشار د. ربيع محمود الصغير - القصد الجنائي في الجرائم المتعلقة بالإنترنت والمعلوماتية دراسة تطبيقية – مركز الدراسات العربية للنشر والتوزيع.
12. د. رمسيس بهنام - النظرية العامة للقانون الجنائي – دار النهضة العربية 1971
13. د. سعيدي سليمة، الأستاذ حجاز بلال – جرائم المعلومات والشبكات في العصر الرقمي – دار الفكر الجامعي الاسكندرية 2017.
14. شمسان ناجي صالح الخيلي – الجرائم المستخدمة بطرق غير مشروعة لشبكة الانترنت – دار النهضة العربية 2009.

15. د. عبد الرازق الموافي عبد اللطيف – شرح قانون مكافحة جرائم تقنية المعلومات لدولة الإمارات العربية المتحدة المرسوم اتحادي بقانون الاتحادي رقم 5 لسنة 2012– الكتاب الأول – إصدارات معهد دبي القضائي.

16. د. عبد الرؤوف مهدي - شرح القواعد العامة لقانون العقوبات – دار النهضة العربية – 2011.

17. د. عبد المهيمن بكر – شرح القسم الخاص في قانون العقوبات جرائم الاعتداء على الأشخاص والأموال ط7 – دار النهضة العربية القاهرة 1977.

18. د. عبد العظيم مرسي وزير- الشروط المفترضة في الجريمة - دار الجليل للطباعة مصر 1983.

19. عفيفي كامل عفيفي – جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون – منشورات الحلبي2007.

20. د. علي جبار الحسيناوي – جرائم الحاسوب والإنترنت دار اليازوري العلمية للنشر الأردن – سنة 2009.

21. د. علي عادل إسماعيل – الجرائم الماسة بحقوق الملكية الفكرية الالكترونية – منشورات الحلبي 2017.

22. د. عمر الفاروق- المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية – ط2 1995.

23. د. عمر محمد أبو بكر بن يونس - الجرائم الناشئة عن استخدام الإنترنت – دار النهضة العربية.

24. د. عوض محمد عوض - قانون العقوبات القسم العام – دار المطبوعات الجامعية 1998.

25. المستشار علاء فكري اباظة – جرائم تقنية المعلومات دراسة تحليلية للمرسوم بقانون اتحادي رقم (5) لسنة 2012 – منشورات دائرة القضاء ابوظبي 2014.

26. د. غنام محمد غنام - شرح قانون العقوبات الاتحادي لدولة الإمارات العربية المتحدة – مطبوعات جامعة الإمارات 2003.

27. د. محمد سامي الشوا – ثورة المعلومات وانعكاساتها على قانون العقوبات – دار النهضة العربية القاهرة 1998.

28. د. محمد عزت فاضل ود. نوفل علي الصفو- جرائم تقنية المعلومات المخلة بالآداب العامة دراسة مقارنة – دار السنهوري بيروت 2017.

29. د. محمد نجيب حسني - شرح قانون العقوبات القسم العام النظرية العامة للجريمة والنظرية العامة للعقوبة والتدبير الاحترازي– دار النهضة العربية القاهرة 1977.

30. القاضي د. محمد عبيد الكعبي - الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت دراسة – دار النهضة العربية 2009.

31. د. محمود أحمد طه - المواجهة التشريعية لجرائم الكمبيوتر والانترنت دراسة مقارنة - دار الفكر والقانون المنصورة.

32. محمود أحمد عبابنة – جرائم الحاسوب وأبعادها الدولية – دار الثقافة للنشر والتوزيع الأردن 2005.

33. د. محمود نجيب حسني – شرح قانون العقوبات – القسم العام ط6 – دار النهضة العربية القاهرة 1989.

34. د. محمود محمد مصطفى - شرح قانون العقوبات القسم العام - دار النهضة العربية - القاهرة ط1 1983.

35. د.مصطفى فهمي الجوهري – النظرية العامة للجزاء الجنائي – كلية شرطة دبي - سنة 2007.

36. د. نائلة عادل محمد فريد قدوره - جرائم الحاسب الآلي الاقتصادية - دراسة نظرية وتطبيقية - منشورات الحلبي الحقوقية بيروت 2005م.

37. د. نهلا عبد القادر المومني – الجرائم المعلوماتية – دار الثقافة 2008.

38. د. هدى حامد قشقوش – جرائم الحاسب الالكتروني في التشريع المقارن – دار النهضة العربية1992.

39. د. هدى حامد قشقوش – الحماية الجنائية للتجارة الالكترونية عبر الإنترنت – دار النهضة العربية 2000.

البحوث والدراسات:

1- د. تركي بن محمد اليحيى - بحث مقدم للمؤتمر الدولي الرابع لمكافحة جرائم تقنية المعلومات المنعقد في أبو ظبي بدولة الإمارات العربية المتحدة بتاريخ 2011/12/14م

2- د. صالح سليمان عبد العظيم - الندوة العلمية – بحث بعنوان الأبعاد والتأثيرات الاجتماعية المرتبطة باستخدام الانترنت على الأسرة العربية.

3- د. شيماء عطا الله – الشرط المفترض في الجريمة - محاضرات منشورة على موقع الدكتورة شيما.

4- د.علي عبد القادر القهوجي – الحماية الجنائية للبيانات المعالجة الكترونياً - بحث مقدم لمؤتمر القانون والكمبيوتر والانترنت الذي نظمته كلية الشريعة والقانون بجامعة الإمارات بالتعاون مع مركز الإمارات للدراسات والبحوث الاستراتيجية ومركز تقنية المعلومات بالجامعة – المجلد الأول – مايو 2000.

5- المستشار. محمد أحمد الحمادي – تشريعات مكافحة جرائم تقنية المعلومات في دولة الإمارات وأحكام القضاء - ندوة علمية بعنوان شبكات الإنترنت وتأثيراتها الاجتماعية والأمنية – إصدار مركز البحوث والدراسات الأمنية بالقيادة العامة لشرطة أبوظبي – نوفمبر 2006.

التقارير:

1- تقرير منشور على موقع هيئة تنظيم الاتصالات على الرابط https://www.tra.gov.ae

2- العميد د. صلاح عبيد الغول السلامي – مدير مكتب ثقافة احترام القانون بوزارة الداخلية – الندوة التي أقامتها مؤسسة الإمارات للاتصالات
https://www.emaratalyoum.com/local-section/accidents/2012-06-05-1.489614

اعتمدت الأطروحة من قِبل:

1) عميد كلية القانون: الأستاذ الدكتور / محمد حسن على محمد

التوقيع: _____ التاريخ : ١٨/١١/٢٠٠٩

2) عميد كلية الدراسات العليا بالإنابة الدكتور/ على المرزوقي

التوقيع: Ali Hamad Al Marzouqi التاريخ: 16/12/2018

جامعة الإمارات العربية المتحدة
United Arab Emirates University
UAEU
UAEU Libraries
DigitizationDepatment
United Arab Emirates

Digitally signed by Shrieen
DN: cn=Shrieen, o=UAEU, ou=Libraries Deanship, email=shrieen@uaeu.ac.ae, c=AE
Date: 2019.04.08 08:44:47 +04'00'