كليـــة الحقـوق
قسـم القـانون الجنائي

بحث فى

النماذج الجرمية للاعتداء على البيانات الشخصية

تحت إشراف

الأستاذ الدكتور/ اكمل يوسف السعيد

أستاذ القانون الجنائى كلية حقوق المنصورة

إعداد الباحث

محمد بن سليم بن حمدان البادى

باحث دكتوراة بقسم القانون الجنائى

كليه الحثوق جامعه المنصورة

١٤٤٢هـ/ ٢٠٢١م

النماذج الجرمية للاعتداء على البيانات الشخصية

سنتناول هذا الموضوع صورا من النماذج الجرمية للاعتداء على البيانات الشخصية في ثلاث مباحث على النحو التالي:

- المبحث الأول: المعالجة غير المشروعة على البيانات الشخصية.
- المبحث الثاني: الإفشاء غير المشروع للبيانات الشخصية .
- المبحث الثالث: جرائم الاعتداء على سلامة البيانات الشخصية .

المبحث الأول

المعالجة غير المشروعة على البيانات الشخصية

تمثل النظم الإلكترونية حالة فريدة، تعبّر عن مدى التطور الذي وصلت إليه الأمم والشعوب في عصرنا، وقد رافق هذا التّطوّر ظهور فئة جديدة من الجرائم، المتمثلة في الاعتداء على النظام المعلوماتي ومحتوياته، أو الدّخول غير المشروع أو غير المصرح به إلى النظام المعلوماتي، فدخول النظام دون إذن مالكه بحدّ ذاته جريمة، وقد يقترن هذا الدخول بعدد من الأفعال التي تُعتبر جرائم مستقلة بذاتها، أو سبباً في مضاعفة الجزاء.

ونظراً لأهمية البالغة للنظم الإلكترونيّة، ومدى تأثيرها على حياة الإنسان، فقد حاول المشرّع العماني من خلال قانون مكافحة جرائم تقنية المعلومات رقم ١٢ لسنة ٢٠١١، حماية الأنظمة الإلكترونيّة جزائيًا، حيث نصت المادة (٣) على عددٍ من الجرائم والأفعال، التي تشكل اعتداءً على النظام المعلوماتي أو الموقع الإلكتروني، كالدُخول العمد ودون وجه حق موقعاً الكترونيا أو نظاما معلوماتيا أو وسائل تقنية المعلومات أو جزءا منها أو تجاوز الدخول المصرح به إليها أو استمر فيها بعد علمه بذلك بهدف تغيير أو تعديل أو تشويه أو إتلاف أو نسخ أو تدمير معلومات إلكترونية مخزنة في النظام المعلوماتي.

كما نصت المادة (٥) من ذات القانون، على جريمة إدخال أو نشر برنامج حاسوبي يؤدّي إلى ذات النّتائج، كالإيقاف أو التعطيل عن العمل ، أو ألغاء أو تغيير أو تعديل أو تشويه أو إتلاف أو تدمير البرامج أو البيانات أو المعلومات الالكترونية المستخدمة أو المخزنة في أي منها ، وبما أنّه يؤدّي إلى ذاتِ الأفعال، فإنّه يمثل اعتداءً يوجب العقاب، وسوف نتناول من خلال هذا الفصل، شرح جريمة الدّخول غير المشروع الى النّظام الإلكتروني أو المعلوماتي، المنصوص عليها في قانون مكافحة جرائم تقنية المعلومات العماني رقم ١٢ لسنة ٢٠١١ والمستحدثات التي أدخلت على من القانون العماني الجديد ٢٠١٨م من خلال مطلبين رئيسين، هما:

- المطلب الأول: الركن المادي لجريمة الدّخول غير المشروع.
- المطلب الثاني: الركن المعنوي لجريمة الدّخول غير المشروع والعقوبات.

المطلب الأول

الرُكن المادي لجريمة الدّخول غير المشروع

يتمثّل الركن المادي في أي جريمة، بسّلوك الجاني الإجرامي، الذي يتّخذه لأجل تحقيق نتيجة مُعيّنة، ويختلف الركن المادي من جريمة إلى أخرى حسب الطبيعة القانونية للجريمة، وفي جريمة الدخول غير المشروع إلى النظام المعلوماتي، فقد نصت المادة (٣) من قانون مكافحة جرائم تقنية المعلومات العماني رقم ١٢ لسنة ٢٠١١ ، على ماهية الأفعال التي تشكل الركن المادي لهذهِ الجريمة بقولها: "أ- يُعاقب بالسجن مدة لا تقل عن شهر ولا تزيد على ستة أشهر وبغرامة لا تقل عن مائة ريال عماني ولا تزيد عن خمسمائة ريال عماني أو بإحدى هاتين العقوبتين ، كل من دخل عمداً ودون وجه حق موقعاً إلكترونيا أو نظاما معلوماتيا أو وسائل تقنية المعلومات أو جزءا منها أو تجاوز الدخول المصرح به إليها أو استمر فيها بعد علمه بذلك .

فإذا ترتب على ما ذكر في الفقرة الأولى إلغاء أو تغيير أو تعديل أو تشويه أو إتلاف أو نسخ أو تدمير أو نشر أو إعادة نشر بيانات أو معلومات إلكترونية مخزنة في النظام المعلوماتي أو وسائل تقنية المعلومات أو تدمير ذلك النظام أو وسائل تقنية المعلومات أو الشبكة المعلوماتية أو إلحاق ضرر بالمستخدمين أو المستفيدين ، تكون العقوبة السجن مدة لا تقل عن ستة أشهر ولا تزيد على سنة وغرامة لا تقل عن خمسمائة ريال عماني ولا تزيد على ألف ريال عماني أو بإحدى هاتين العقوبتين.

فإذا كانت البيانات أو المعلومات المنصوص عليها في الفقرة الثانية شخصية تكون العقوبة السجن مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات وغرامة لا تقل عن الف ريال عماني ولا تزيد على ثلاثة آلاف ريال عماني أو بإحدى هاتين العقوبتين".

كذلك نصت المادة (٦) من ذات القانون، على الدخول غير المشروع، حيث جاء فيها: يُعاقب بالسجن مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن ألف ريال عماني ولا تزيد على ثلاثة آلاف ريال عماني أو بإحدى هاتين العقوبتين ، كل من دخل عمدا ودون وجه حق موقعا إلكترونيا أو نظاما معلوماتيا بقصد الحصول على بيانات أو معلومات إلكترونية حكومية سرية بطبيعتها أو بموجب تعليمات صادرة بذلك ، وتكون العقوبة السجن مدة لا تقل عن ثلاث سنوات ولا تزيد على عشر سنوات وغرامة لا تقل عن ثلاثة آلاف ريال عماني ولا تزيد على عشرة آلاف ريال عماني إذا ترتب على الفعل المجرم إلغاء أو تغيير أو تعديل أو تشويه أو إتلاف أو نسخ أو تدمير أو نشر البيانات أو المعلومات الإلكترونية .

وتعد البيانات والمعلومات الإلكترونية السرية الخاصة بالمصارف والمؤسسات المالية فى حكم البيانات والمعلومات الإلكترونية الحكومية السرية في نطاق تطبيق حكم هذه المادة"

كذلك نصت المادة (٦) من ذات القانون، على أنه " يُعاقب بالسجن مدة لا تقل عن شهر ولا تزيد على سنة وبغرامة لا تقل عن ألف ريال عماني ولا تزيد على ثلاثة آلاف ريال عماني أو بإحدى هاتين العقوبتين ، كل من دخل عمدا ودون وجه حق موقعا إلكترونيا بقصد تغيير تصميمه أو تعديله أو إتلافه أو إلغائه أو شغل عنوانه".

وقد عرّفت المادة (٣) من مكافحة جرائم تقنية المعلومات العماني رقم ١٢ لسنة ٢٠١١ الدخول غير المشروع بأنه " الدخول دون وجه حق أو تجاوز الدخول المصرح به أو الاستمرار في الموقع الإلكتروني بعد علمه بذلك.

وتُقسم جريمة الدخول غير المشروع أو غير المصرّح به إلى نوعين: الأول هو الدخول المُجرّد إلى النظام المعلوماتي، أو ما يُعرف لدى التقنيين باسم الاختراق (Hacking)، أمّا النوع الثاني: فهو الدّخول بهدف إتلاف النظام المعلوماتي أو تعديله، عن طريق الحذف أو الإضافة، أو ما يُعرف لدى التقنيين بالتخريب (Cracking)، وتعتبر هذه الجريمة من الجرائم التي تعتمد في جسامتها على نوع الفعل ومدى تطوره، فجريمة الدّخول تتطوّر تبعاً للأفعال التي يقوم بها المخترق أو المخرّب، فتختلف الجريمة تبعاً لاختلاف الرُكن المادّي فيها، وتُشدّد العقوبة تبعاً لذلك[١].

ويمثل الرّكن المادي في أي جريمة، كل فعل أو امتناع عن فعل، وهذا ما سنراه من خلال دراستنا للرُكن المادي، ومدى تحققه بصورتيه (الفعل والامتناع) بالنّسبة لجريمة الدّخول غير المشروع، وحتى نتمكّن من ذلك، لا بدّ من تحديد ماهية الرُكن المادي لهذه الجريمة، بصورتيها البسيطة والمشدّدة، (الدّخول غير المشروع والدّخول بهدف الإتلاف)، حسب قانون مكافحة جرائم تقنية المعلومات العماني رقم ١٢ لسنة ٢٠١١من قانون الجرائم الإلكترونية، وقد قسمنا هذا المبحث إلى مطلبين رئيسين، هما:

- المطلب الأول: جريمة الدّخول غير المشروع بصورتها البسيطة
- المطلب الثاني: جريمة الدّخول غير المشروع بصورتها المُشدّدة.

المطلب الأول

جريمة الدّخول غير المشروع بصورتها البسيطة

(١) الجنبيهي، منير محمد، والجنبيهي، ممدوح محمد (٢٠٠٦)، أمن المعلومات الإلكترونية، الاسكندرية: دار الفكر الجامعي.

إنّ النّظام المعلوماتي يتكون من مجموعة من البيانات والمعلومات التي كفل القانون الحماية لها، وتتمثّل جريمة الدّخول غير المشروع للنظام المعلوماتي، بصورتها البسيطة وفق المواد (٣، ٤، ٩) من قانون مكافحة جرائم تقنية المعلومات العماني رقم ١٢ لسنة ٢٠١١، بفعل الدّخول المُجرّد إلى النظام المعلوماتي، بشكل مباشر أو بشكل غير مباشر، أي عن طريق استخدام الحاسب الآلي مباشرةً للدّخول، أو عن طريق استخدام برامج للدخول عن بُعد [٢].

ويقصد بالدّخول المباشر، أن يقوم أحد الأشخاص باختراق النظام المعلوماتي أو الشبكة المعلوماتية أو الموقع الإلكتروني، أو الولوج له دون تصريح أو بما يجاوز أو يخالف التصريح، من خلال استخدام أحد الأجهزة المتصلة بجهاز الحاسوب، المتواجد عليه النّظام المعلوماتي بشكلٍ مباشر، أو من خلال استخدام أجهزة الإخراج المُتصلة به، كالشاشة أو الطابعة أو وحدات الإدخال كالفأرة ولوحة المفاتيح، أو وحدات المعالجة المركزيّة، أو باستخدام الرقم السرّي لشخص آخر دون علمه، أو مفتاح الشيفرة المخوّل للدّخول[٣].

ومن صوّر الدّخول المباشر، أن يقوم أحدُ الأشخاص بفتح جهاز مغلق، مُثبت عليه النّظام المعلوماتي، ويقوم بالاطلاع على البيانات والمعلومات والتنقل داخل النظام المعلوماتي باستخدام لوحة المفاتيح والفأرة"، ويُشترط حتى تتحقق الجريمة بصورتها هذه، أن يكون صاحب النظام المعلوماتي، يضع قيودا للوصول إلى البيانات والمعلومات المحفوظة في جهاز الحاسوب[٤].

ويُلاحظ أن المشرّع العماني في هذه الصورة البسيطة، يُعاقب الفاعل على الدّخول المُجرّد إلى النّظام المعلوماتي أو الشبكة الإلكترونية، ذلك أنّ مُجرّد الدخول تقوم به الجريمة، حتى ولو لم يترتب على دخوله ضرّراً لشخص أو جهة معيّنة، أو لم يتحقق له فائدةً من وراء هذا الدّخول، طالما كان دخوله دون تصريح، أو بما يخالف أو يجاورُ التّصريح.

---

(٢)احمد خليفة الملط، ، مرجع سابق، ص ٢٢٤.

(٣) حنان ريحان مبارك المضحكي، الجرائم الإلكترونية، دراسة مقارنة، (ط١)، بيروت: منشورات الحلبي الحقوقية،٢٠١٤م، ص ١٠١.

(٤) محمد علي قطب، الجرائم الإلكترونية وطرق مواجهتها، (ج٢)، مملكة البحرين: الاكاديمية الملكية للشرطة، ٢٠١٠م ، ص ١٠.

أمّا الدّخول غير المباشر، فإنّه يعني أن يقوم المجرم المعلوماتي بالدّخول إلى النظـــام المعلوماتي عن بُعد، باستخدام وسائل الاتّصال الحديثة أو برامج الكمبيوتر، فيتم التحكم بجهـــاز المجني عليه أو نظامه المعلوماتي من خلال هذه البرامج، ويتم من خلال هذه العمليّة الـــدّخول إلى النظام الإلكتروني، والتقاط أو اعتراض البيانات والمعلومات ومعالجتها عن بعد، ومن ثـــم إدخالها إلى النظام المعلوماتي[٥]، ومن أشهر البرامج الخبيثة التي يتم من خلالها الدخول إلـــى النظام المعلوماتي عن بعد ما يلي:

١. برامج حصن طروادة. ٢. الفيروسات.

٣. القنابـــل المعلوماتيـــة (المنطقيـــة والزمانيّة).

ويمكن لهذه البرامج أيضا أن تعمل على الإتلاف والحذف والإضافة[٦].

١) برامج حصن طروادة (**Trojan Horses Program**):

تعتبر هذه البرامج من أخطر البرامج الخبيثة، التي تُستخدم في عمليات الاختراق للنظم الإلكترونية، فهذا النّوع من البرامج يحتوي على خصائص تمكنّه من الاختراق بسهولة، وعـــدم ترك أي آثار جانبية مع صعوبة اكتشافه[٧].

وقد أنشئت هذه البرامج لأسباب مُفيدة في البداية، كمراقبة أعمال الموظفين، والأطفـــال على أجهزة الكمبيوتر في غياب المسؤولين والوالدين، لكنّها طوّرت بحيث أصبحت من أهـــم برامج الاختراق التي عرفها التاريخ، وتزداد خطورة هذا النوع من البـــرامج، فـــي إمكانيّـــة الحصول على كلمات السّر المُخزّنة على النظام المعلوماتي والقدرة على التخفي[٨].

٢) الفيروسات (**Viruses**):

---

(٥) جلال محمد الزعبي، أسامة أحمد والمناعسة ، جرائم تقنية نظم المعلومات الإلكترونية، دراسة مقارنة، (ط١)، عمان: دار الثقافة للنشر والتوزيع، ٢٠١٠م، ص ٢٤٨.

(٦) السعدي، خالد حربي، مرجع سابق، ص ٧٨.

(٧) القحطاني، عبد الله بن حسين، مرجع سابق، ص ٤٢.

(٨) الجنبيهي، منير محمد، والجنبيهي، ممدوح محمد، مرجع سابق، ص ٣٦.

يُعتبر فيروس الحاسوب برنامج مُصمّم بهدف الوصول إلى البرامج الأخرى، والـنّظم المعلوماتية المملوكة للغير، والسيطرة عليها والانتشار فيها، ومن ثم تعطيلها أو تدميرها، وقـد انتشرت هذه الفيروسات بشكل ملفت في الفتـرة الـأخيرة، وقـد عـرّف علمـاء الحاسـوب الفيروسات على أنها: البرامج التي لها القدرة على الدّخول والاختباء فـي أي مـن البـرامج الأخرى الموجودة على الحاسب، أيّاً كان نوعها، دون أن يكون صاحب الجهـاز علـى علـم بوجودها"[٩].

وتتميّز الفيروسات التي يستخدمها المجرم المعلوماتي فـي عمليـات الـدخول غيـر المشروع، وما يقترن بها من أفعال مشدّدة بعدّة ميزات، ومنها[١٠]:

١. القدرة على تكرار نفسها ونسخها في حافظـة النظـام عـدّة مرّات.

٢. سرعة انتشار الفيروس داخل النظام عن طريـق الشـبكات الإلكترونيّة.

٣. القدرة على التخفي داخل النظام، فلا يستطيع المجنـي عليـه الشعور بوجود هذه البرامج الخبيثة.

٤. القدرة على مسح البيانات المخزّنة على النّظـام المعلومـاتي والوسائط المرتبطة به، دون علم المجني عليه.

٣) برنامج القنبلة المعلوماتية (informatics bomb program):

وهو برنامج يُعدّه مصمم النظام المعلوماتي، ويثبته بداخله، بُغية أن يعمل بعد انقضـاء مدّة محدّدة على استعمال النظام المعلوماتي، بهدف تدميره أو تعطيله أو محو البيانـات التـي يحتويها، وهي على نوعين: القنبلة المنطقيّة والقنبلة الزمنيّة، أمّا القنبلة المنطقيّة فإنّهـا تُعتبـر جزءاً من برنامج يقوم بتنفيذ أمر مُعيّن خلال فترة زمنية منتظمة، وتقوم القنبلة المنطقيّة بمسح النظام الالكتروني بهدف تنفيذ عمل غير مشروع، ولا تُظهر القنبلة المنطقية ايـةً فعاليـة فـي

(٩) الجنبيهي، منير محمد، و الجنبيهي، ممدوح محمد، مرجع سابق، ص ٤٧ وما يليها.

(١٠) الخليفة، محسن بن سليمان (١٤٢٣هـ)، جرائم الحاسب الآلي وعقوباتها في الفقه والنظام، رسالة ماجستير الرياض، أكاديمية نايف العربية للعلوم الأمنية، ص ١٤٤.

النظام، بل هي تتخذ سلوكاً ساكناً، لهذا لا يُمكن اكتشافها بسهولة، وبالغالب يتم اكتشافها بعد فترة طويلة من وجودها في النظام، وقد سُمّيت بالقنبلة المنطقيّة كونها تنتظر أن يتم أحد الشروط المنطقيّة في النظام قبيل بدء عملها التخريبي، وعادةً ما يتم عملها التخريبي خلال ثوان معدودة، وفي حالِ بدأ عملها التُخريبي الذي يشبه الانفجار، فإنّه لا يُمكن تداركه من قِبل المجني عليه(١١).

أمّا القنبلة الزمنيّة فهي تعمل في وقتٍ مُحددٍ وفي يوم مُعيّن، مثل فيروس (shernobel) الذي اكتشف في العام ١٩٩٨م، والذي ينشط في تاريخ مُعيّن ويبدأ نشاطه التدميري.

يُلاحظ في هذا الإطار، أنّ المشرّع العماني لم ينص على وسيلة محدّدة للدخول إلى النظام المعلوماتي، فقد استخدم عبارة أجهزة الحاسب الآلى وأجهزة الاتصال " في المادة (١/و) من قانون مكافحة جرائم تقنية المعلومات العماني رقم ١٢ لسنة ٢٠١١ ، ويرى الباحث بأنّ المشرّع كان موفقاً في استخدام هذه العبارة، ويعود ذلك لأنّ الوسائل التي من الممكن استخدامها للدّخول غير المشروع إلى النظم الإلكترونية لا يمكن حصرها، وإن أمكن حصرها جدلاً، فلا يمكن للتشريع أن يواكب التطور المستمر في تكنولوجيا المعلومات، التي يمكن استخدامها في عمليات الاختراق.

وقد عرّفت المادة (٣) من قانون مكافحة جرائم تقنية المعلومات العماني رقم ١٢ لسنة ٢٠١١ الدخول غير المشروع بأنه " الدخول دون وجه حق أو تجاوز الدخول المصرح به أو الاستمرار في الموقع الإلكتروني بعد علمه بذلك ، بهذا يكون الركن المادي لجريمة الدّخول غير المشروع متمثلاً بصدور أي فعل من قبل المجرم المعلوماتي، بهدف الوصول إلى البيانات أو المعلومات التي يتكون منها النظام المعلوماتي بطريقة غير مشروعة، وبأي وسيلة كانت، دون رضا أصحابها(١٢).

---

(١١) المساعدة، نائل علي (٢٠٠٥)، أركان الفعل الضار الإلكتروني في القانون الاردني، مجلة دراسات الشريعة والقانون، مجلد ٣٢، (ع١)، ص٦٢.

(١٢) زين الدين، بلال أمين (٢٠٠٨)، جرائم نظم المعالجة الآلية للبيانات، الإسكندرية: دار الفكر الجامعي، ص ٢٧١.

كما يتحقق الرُكن المادي لهذه الجريمة، في حال الدّخول غير المشروع إلى جزء من النظام المعلوماتي أو كله، فقد يكون صاحب النظام المعلوماتي أو الموقع الإلكتروني، يسمح للجميع بالولوج إلى جزء منه، ويحظره في جزء آخر، كما أن الركن المادي يتحقق في حال دخول المستخدم للنظام المعلوماتي بعد انتهاء اشتراكه أو لمدّة تجاوزت الحد المسموح به.(١٣)

إنّ أغلب المجرمين المعلوماتيّين (القراصنة)، يستخدمون برامج حاسوبيّة لإتمام الاختراق عن بعد، فلا يمكن أن يكون النظام المعلوماتي مُتاحاً أمام الجميع من الناحية التقنية، ونظراً لأن استخدام البرامج الحاسوبيّة بشكل كبير في هذه العملية، فقد نصت المادة (٣) من قانون مكافحة جرائم تقنية المعلومات العماني رقم ١٢ لسنة ٢٠١١، على تجريم إلغاء أو تغيير أو تعديل أو نشر أو إعادة نشر بيانات أو معلومات إلكترونية مخزنة في النظام المعلوماتي أو وسائل تقنية المعلومات أو تدمير ذلك النظام أو وسائل تقنية المعلومات، ويقع الركن المادي هنا الجريمة الدخول غير المشروع، باستخدام وسائل تقنية المعلومات بهدف الدّخول إلى النظام المعلوماتي، ويُشترط لتحقيق الركن المادي في جريمة الدّخول غير المشروع وجود ثلاثة شروط(١٤):

١. وجود نظام معالجة آلية للبيانات:

ويقصد بالنظام الآلي لمعالجة البيانات، أن يتمّ استخدام الأساليب الآليّة في معالجة البيانات، وحفظها واخراجها وبثها وتحليلها واستعادتها عن حاجتها، وتحويلها إلى معلومات يمكن الاستفادة منها، دون الحاجة لعنصر بشري(١٥).

٢. وجود نظام لحماية البيانات والمعلومات:

ويقصد بنظام الحماية ما يُعرف بكلمات المرور، أو تعريف الهويّة للشخص الذي يريد الولوج إلى النظام، فإن كان النظام متاحاً للجميع، وفي مرمى يد جميع المستخدمين، فإنّه لا

---

(١٣) المضحكي، حنان ريحان، مرجع سابق، ص ١٠٤.

(١٤) زين الدين، بلال أمين، مرجع سابق، ص ٢٦٢.

(١٥) نظم المعلومات المحوسبة، موقع إلكتروني:
http://www.minshawi.com/other/gendelgy.htm

يترتّب على الدّخول إليه أي عقوبة، لأنّه لا يُعقل أن تُترك معلوماتِ على درجة كبيرة من الأهمّيّة، في مرمى يد الجميع ودون حماية لها.(١٦)

إلا أنّ هذا الشرط قد أثار جدلاً واسعاً بين الفقهاء، فقد رأى جانب من الفقه، بأنّ الحماية مفروضة على النُظم الإلكترونيّة، سواء أكانت هذه النُظم قد اتُخذت تدابير للحماية أم لا، ويستند أصحاب هذا الرأي في ذلك، إلى أنّ ذلك سوف يؤدّي إلى توسيع دائرة الإفلات من العقاب، فيعتبر أنصار هذا الرّأي، أنّ وجود حماية للنظام المعلوماتي، يُعتبرُ قرينة على القصد الجرمي وليس سبباً للإفلات من العقاب(١٧).

ومن الأمثلة على النظم الإلكترونيّة المُتاحة أمام الجميع، تقارير معلومات البورصة، لأنّ ما يردُ من معلومات تتناول موضوع البورصة وأسعار الأسهم، تمثل معلومات مُتاحة أمام الجميع، وعلى الرّغم من ذلك، فإنّ الحماية تُفرض لمن يجمع هذه المعلومات، وذلك مراعاةً لِما يُبذل من مجهود في جمع المعلومات وتنسيقها وحفظها.(١٨).

٣. أن يكون الدّخول دون تصريح أو بما يخالف أو يتجاوز التصريح:

يُقصد بالدّخول المخالف للقانون، ألا يبيح القانون الدخول الى الموقع الإلكتروني بدون تصريح، أما الدّخول بتصريح وبما لا يتجاوز هذا الصريح، كأن يكون لدى الشخص الحق في الدّخول إلى النظام بصفته مالكاً له، أو أنّ لديه تصريحاً من مالكه بالدّخول إليه أو لجزء منه، أو أنّ هذا النظام مُتاحاً أمام الجميع بالمجان، ولا يوجد ما يمنع الدّخول إليه، ففي هذه الحالة لا تقوم المسؤوليّة الجزائيّة بحق من يقوم بالدخول للنّظام المعلوماتي.

ويتحقق الرُكن المادي في جريمة الدّخول غير المشروع، وفق المادة (٣) من قانون مكافحة جرائم تقنية المعلومات العماني رقم ١٢ لسنة ٢٠١١ في حال تجاوز التصريح الممنوح، كأن يدخل الشخص إلى أجزاء لا يتضمنها الصريح الممنوح له.

كما يتحقّق الرّكن المادي لجريمة الدخول غير المشروع، في حالة البقاء غير المصرّح به داخل النّظام المعلوماتي، وقد نص المشرّع العماني عليها صراحة، حيث نصت المادة (٣)

---

(١٦) المومني، نهلا، مرجع سابق، ص ١٥٩.

(١٧) الصغير، جميل عبد الباقي (١٩٩٢)، الجرائم الناشئة عن استخدام الحاسب الآلي (ط١)، القاهرة: دار النهضة العربية، ص ١٥١.

(١٨) الشحات، ابراهيم محمد منصور (٢٠١١)، الجرائم الإلكترونية في الشريعة الإسلامية والقوانين الوضعية، بحث فقهي مقارن، (ط١)، الإسكندرية: دار الفكر الجامعي، ص ٢٧.

على أنه: كل من دخل عمدا ودون وجه حق موقعا إلكترونيا أو نظاما معلوماتيا أو وسائل تقنية المعلومات أو جزءا منها أو تجاوز الدخول المصرح به إليها أو استمر فيها بعد علمه بذلك .

المطلب الثاني

جريمة الدّخول غير المشروع بصورتها المُشدّدة:

إنّ الصورة السابقة من جريمة الدّخول غير المشروع إلى النظام المعلوماتي التي تحدّثنا عنها، قد تُمثل شكلاً من أشكال انتهاك الخصوصيّة الإلكترونيّة، وقد وفّر المشرع الحماية القانونية للنظام المعلوماتي وجرّم الدّخول غير المشروع له، ولكنّ الدّخول المُجرّد يُعتبر أبسط صور الجرائم الإلكترونيّة، وقد يكون لهذا الدّخول أهدافاً أخرى، غير التّجوّل والبقاء في النّظام المعلوماتي بشكل غير مشروع.

فعند الرّجوع إلى نصوص الموادّ (٣) و(٨) من قانون مكافحة جرائم تقنية المعلومات العماني رقم ١٢ لسنة ٢٠١١، نجد أنّ المشرّع قد نص على نوعين من الجرائم ذاتِ العقوبة المُغلظة، وهي جرائم الإلغاء أو التعديل أو إتلاف أو نسخ أو تدمير أو نشر أو إعادة نشر بيانات أو معلومات إلكترونية.

ويتمثل الرُكن المادي لجريمة الدخول بصورتها المُشدّدة حسب نص المادتان (٦) و(٩) من قانون مكافحة جرائم تقنية المعلومات العماني رقم ١٢ لسنة ٢٠١١، في الولوج إلى النظام المعلوماتي، بهدف إلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو حجب أو تعديل، أو تغيير أو نقل أو نسخ بيانات أو معلومات أو إعاقة أو تشويه أو توقيف، أو تعطيل عمل الشبكة المعلوماتيّة أو نظام معلومات، أو تغيير موقع إلكتروني أو إلغاءه أو إتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفة أو شخصيّة مالكه، ويكفي لتوافر الظرف المُشدّد، أن يكون هناك علاقة سببيّة ما بين الدّخول غير المشروع وبين النّتيجة الجرميّة التي تحققت، وهي إلغاء أو حذف البيانات أو المعلومات أو التُعدّي على النظام المعلوماتي أو الموقع الإلكتروني.

جميع هذه الأفعال التي تكون الرُكن المادي للجريمة، تشكل الصورة المشدّدة لجريمة الدّخول غير المشروع، وسوف نتناول هذه الأفعال على النحو التالي :

أولاً: إلغاء أو حذف أو إضافة أو تدمير أو إتلاف أو تغيير البيانات أو المعلومات:

إنّ الهدف الرّئيس من الدّخول أو الولوج إلى النّظام المعلوماتي، ينصبُ في غالب الأمر على العبث في البيانات والمعلومات التي يحتوي عليها النّظام المعلوماتي، سواء أكانت معلومات إسمية أم موضوعية[١٩]، وتستوي هذه الصورة من صور جريمة الدّخول غير المشروع، في حال كون الدّخول مباشر أو غير مباشر عبر الشبكات، فالجاني هنا لا يتوقف عند دخول النظام المعلوماتي والتجول به، بل يتعدى ذلك إلى إلغاء أو حذف أو إضافة أو تدمير أو إتلاف أو تغيير البيانات والمعلومات داخل النظام المعلوماتي.

وتعتبر هذه الصورة من أخطر صور الاعتداء على البيانات والمعلومات داخل النظام المعلوماتي وهذا الأمر يُظهر أهميّة معرفة الدّافع من ارتكاب هذه الجريمة، والهدف من عمليّة العبث في النظام المعلوماتي، رغم عدم تقيّد المشرّع بالباعث أو الهدف إلا بوجود نص صريح[٢٠]، فقد تتجاوز الأعمال مجرّد العبث إلى غيرها من الجرائم الإلكترونيّة أو التقليديّة، فمن الممكن أن يقوم شخص بحذف معلومات شخصية أو شركة بعد تسجيلها بفترةٍ معيّنة، أو محو بعض بياناتها، وهذا في حقيقته قد يعني أمرّين بحسب الباعث من عمليّة الحذف، فقد يمثل هذا الفعل احتيال معلوماتي، أو مجرّد إتلاف أو حذف معلوماتي[٢١].

فالركن المادي للجريمة يتمحور وفق هذه الصورة، حول الإضرار بالبيانات والمعلومات الموجودة داخل النظام، ولا يتعدّاه لغيره من الأفعال المرتبطة بجرائم أخرى، كالتزوير أو الاحتيال الإلكتروني، كأن يقوم الجاني بمحو ملفات التشغيل الخاصة بالنّظام، مما

---

(١٩) منصور، الشحات أبراهيم، مرجع سابق، ص ٢٥ وما يليها.

(٢٠) انظر المادة (٢٨) من قانون الجزاء العماني الصادر بالمرسوم السلطاني رقم ٢٠١٧/٧ " لا يسأل شخص عن الجريمة ما لم تكن نتيجة لسلوكه الإجرامي، ويسأل عنها ولو كان قد أسهم مع سلوكه الإجرامي في إحداثها سبب آخر سابق أو معاصر أو لاحق، متى كان هذا السبب متوقعا أو محتملا وفقا للسير العادي للأمور، أما إذا كان ذلك السبب وحده كافيا لإحداث نتيجة الجريمة، فلا يسأل الفاعل في هذه الحالة إلا عن الفعل الذي ارتكبه.."

(٢١) السعدي، خالد حربي (٢٠١٢)، جريمة إتلاف برامج ومعلومات الحاسب الآلي في التشريع الكويتي والمقارن، (ط١)، القاهرة: دار النهضة العربية، ص ٧٧.

يؤدّي إلى تعطله، ففي هذه الحالة نكون أمام جريمة الدّخول غير المشروع بصورتها المشدّدة، بخلاف المثال السابق الذي قد تعدّى إلى جريمة الاحتيال المعلوماتي[٢٢].

ثانياً: إفشاء البيانات أو المعلومات:

إنّ البيانات والمعلومات التي يحتوي عليها النظام المعلوماتي، تمثّل بالنّسبة لمالكها أو من يتعلق لهم حق بها، شيئاً من الخصوصيّة التي سعى قانون مكافحة جرائم تقنية المعلومات العماني رقم ١٢ لسنة ٢٠١١ إلى حمايتها، وكذلك قانون الجزاء العماني الصادر بالمرسوم السلطاني رقم (٧) لسنة ٢٠١٨م حيث نصت المادة (٣٣٢) يعاقب بالسجن مدة لا تقل عن (١٠) عشرة أيام، ولا تزيد على (٣) ثلاثة أشهر، كل من اعتدى على حرمة الحياة الخاصة للأفراد في غير الأحوال المصرح بها قانونا، وذلك بارتكاب أحد الأفعال الآتية:

أ – فض رسالة أو برقية خاصة موجهة لغيره من الأفراد.

ب – استرق السمع في مكالمة هاتفية.

ج – سجل أو نقل محادثات بواسطة جهاز، أيا كان نوعه.

د – التقط أو نقل صورا لفرد أو أفراد بواسطة جهاز أيا كان نوعه.

وقد اتفقت الدساتير والتشريعات الحديثة، والاتفاقيات الدولية والإقليميّة، على حماية الحق في الحياة الخاصة، ورغم ذلك، فإنّ تعريف الحياة الخاصة لا يزال مدار جدل واسع، فقد اتّفق الفقه على صعوبة وضع تعريف جامع مانع، لاختلاف الخصوصيّة من مجتمع إلى آخر ومن شخص إلى آخر، نتيجة اختلاف القيم والتقاليد، لهذا فإنّ بعض الفقهاء قد اتّجه لوضع قائمة بما يُمثل خصوصيّة الشخص في مجتمع ما، كالحق في الاسم، وماضي الإنسان، وكشف الضرائب، وكشف الرّاتب، والعبادات وغيرها [٢٣].

ويُقصد بمصطلح الخصوصيّة الإلكترونيّة، حق من طبيعة ماديّة يرتبط بالشخصيّة الإنسانيّة التي لها عليه سلطة تقديريّة كاملة، وذلك من حيث السّلطة التي تتكون من مجموعة

---

(٢٢) شمس الدين، أشرف توفيق (٢٠٠٦)، الحماية الجنائية للمستند الإلكتروني، دراسة مقارنة، (ط١)، بدون دار أو مكان نشر، ص ١٢٠.

(٢٣) ربيع، عماد (٢٠١٦)، الاعتداء على حرمة الحياة الخاصة، مجلة العلوم القانونية والسياسية، (م١١)، (ع١)، الدنمارك: اكاديمية البورك للعلوم، ص١٦-١٧.

من الوقائع والعلاقات التي تُساهم في تحديد الشخصيّة، وتضم كافّة العلاقات ذات الطابع الشخصي للإنسان، مثل الحياة العاطفيّة والحالة الصحيّة والحالة المدنية والحالة الدّينيّة وغيرها من الحالات"[٢٤]

وهكذا فقد تحتوي هذه النظم الإلكترونية، على أسماء وأرقام وأسرار ووسائط متعددة، لا يُريد صاحب هذا النظام إطلاع العامّة عليها، فمع التطور الهائل في تكنولوجيا المعلومات، أصبحت الشبكات ووسائل الاتصال الحديثة، وسيلة للحصول على المعلومة الخاصة، فمثلاً يُمكن استخراج معلومات عن الأوراق الثبوتيّة أو تأشيرات السفر عن طريق الإنترنت، ويتطلّب ذلك وجود قاعدة بيانات محوسبة من خلال نظام حوسبة الي، لذلك فقد ارتفعت وتيرة قرصنة المواقع الإلكترونيّة والشبكات المعلوماتيّة، لتحقيق مصالح مختلفة من قِبل الجاني[٢٥]، حيث يهدِف الجاني من دخوله غير المشروع للنّظام المعلوماتي أو الموقع الإلكتروني إلى إفشاء البيانات أو سرقتها.

ثالثاً: حجب البيانات والمعلومات:

وتشمل هذه الصورة في منع المستخدمين المصرّح لهم، من الوصول إلى البيانات والمعلومات الموجودة على النّظام المعلوماتي، وتفترض هذه الصورة من الجريمة، عدم وقوع أي إتلاف على البيانات والمعلومات بذاتها، ولكنها قد تنطوي على إتلاف جزء من النّظام المعلوماتي المسؤول عن الدّخول إلى البيانات والمعلومات، أو إظهارها لمنع الوصول إلى البيانات والمعلومات المحفوظة فيه[٢٦]

ومن الممكن أن يتمثل حجب البيانات والمعلومات، في عدم إظهار البيانات مع وجودها داخل النظام المعلوماتي، لكنّها تصبح غير مرئية، بحيث لا يشعر المستخدم بوجودها على وجه الحقيقة، وتختلف هذه الطريقة عن طريقة التشفير، والتي تكون البيانات والمعلومات ظاهرة فيها، إلا أنّه يصعب فهمها أو الوصول إلى مكنونها الحقيقي، فالحجب أكثر أمناً من

---

(٢٤) مصطفي، أحمد محمود (٢٠١٠)، جرائم الحاسبات الآلية في التشريع المصري، (ط١)، القاهرة: دار النهضة العربية، ص ٥٠.

(٢٥) قورة، نائلة عادل، مرجع سابق، ص ٢٧٥.

(٢٦) قطب، محمد علي، مرجع سابق، ص ٦.

التشفير، كون تشفير البيانات المعلومات يمكن تجاوزه في حال فك الشيفرة، إلا أنّه يصعب ذلك في حالة الحجب، إلا من خلال الوصول إلى مصدر البيانات والمعلومات الجهاز الخادم[٢٧]

رابعاً: نقل البيانات أو المعلومات:

لقد صاحب الثورة التكنولوجيّة في الآونة الأخيرة، ظهور نظام تبادل البيانات إلكترونيّاً (EDI)، وهو نظام بديل عن نظام الرسائل الإلكترونيّة، ويقوم هذا النظام بالسماح بنقل البيانات والمعلومات من جهاز لأخر عن طريق الشبكة، إلا أنّ هذه التقنيات الحديثة قد أسيئ استخدامها، ومن مظاهر إساءة استخدام التكنولوجيا، نقل البيانات أو المعلومات التي لا يُسمح بنقلها.[٢٨]

وتتمثل هذه الصورة في الاستحصال على أصل المعلومات المحفوظة على النّظام المعلوماتي، ونقلها من النظام المعلوماتي إلى آخر، أو من وسيلة لأخرى لحفظ البيانات والمعلومات، ويختلف الأثر المترتب على عملية النقل، فقد يترتب على هذه العمليّة إتلاف للنظام المعلوماتي أو انتهاك للخصوصيّة والسّرّيّة.[٢٩].

خامساً: نسخ البيانات أو المعلومات:

إنّ الحماية الجزائيّة في قانون الجرائم الإلكترونية، تشمل قيام الجاني بعمل نسخة من النظام المعلوماتي كاملاً أو لجزء منه دون تصريح من مالكه، وتتمثّل هذه العملية بقيام الجاني بتخزين ما يحتويه النظام المعلوماتي على أداة معينة، دون أن يترك وراءه أثر على النظام المعلوماتي، فلا يحذف ولا يضيف بل يأخُذ نسخه فقط، فهذه الصورة تتميّز بعدم التعرّض لأصل البيانات والمعلومات المحفوظة في النظام المعلوماتي.[٣٠]

---

(٢٧) جاكسون، سنثيا إلى (٢٠٠٧)، التخطيط الآن لإدارة البيانات الإلكترونية وتجنب المخاطر القانونية في المستقبل، دون مكان او دار نشر، ص ٣٧.

(٢٨) الابراهيم، مروان، والجزائري، هاشم (٢٠٠٧) دور البنوك التجارية في الحد من عمليات الاحتيال في الاعتمادات المستندية، مجلة اباحث اليرموك، (م ٢٣)، (ع٤)، ص ١٢١٧.

(٢٩) العايد، عطا الله، وخريسات، الاء (٢٠١٠)، ملخص عن قطاع تكنولوجيا المعلومات والاتصالات، عمان، وزارة الصناعة والتجارة، مديرية التنمية الصناعية، ص٢.

(٣٠) البداينة، ذياب (٢٠٠٢)، الأمن وحرب المعلومات، عمان: دار الشروق للنشر والتوزيع، ص١١٣.

والأصل أن تكون المعلومات متاحة للاطلاع لبعض الأشخاص، أو حتى للجميع لكن يُحظر نسخها، ويعتبر ذلك إضافةً إلى خرق قانون الجرائم الإلكترونية اعتداء على الخصوصية، ويندرج تحت ذلك؛ ما يقوم به الشخص من نسخ لمحتويات المواقع الإلكترونية، عن طريق الخادم الذي يحتفظ بمعلومات هذه الصفحات والمواقع والشبكات.

ومن الأمثلة على هذه الحالة، أن يقوم الجاني بالدخول إلى النّظام المعلوماتي، لقاعدة بيانات أسماء وإعداد ورواتب الموظفين، ومن ثم يقوم بنسخها على طرفيّة موصولة بجهاز حاسوبه، ومن ثم حصوله على معلومات تختص بها الشركة أو المؤسسة الحكوميّة، مثل أعداد الموظفين ورواتبهم التي قد يكون الاطلاع عليها مسموحاً مع عدم جواز نسخها.

سادساً: توقيف أو تعطيل عمل النّظام المعلوماتي:

وتتمثل هذه الصورة بمنع المستخدمين من الدّخول إلى النظام المعلوماتي بشكل تام، أو منع النظام المعلوماتي من العمل بشكل تام، ويكون تعطيل النّظام المعلوماتي وتوقيف الدخول إليه، من خلال منع النظام عن العمل سواء تمّ العبث ببياناته أو برامجه كلّيّاً أو جزئياً، أو تدميرها بطرق إلكترونية، أو أن يتم تشويه المعلومات بحيث يصبح عمل النظام المعلوماتي غير ممكن بشكل دائم أو مؤقت، ويكون الإتلاف كلياً عند محو وتدمير جميع البيانات والبرامج في النظام أو الجزء المسؤول عن دخول الأشخاص المصرّح لهم[٣١]. ومن الأمثلة على ذلك؛ أن يقوم الجاني بإتلاف الجهاز الخادم، او البرنامج الذي يقوم بالسماح بالدخول إلى النظام ممّا يؤدّي إلى تعطله، وعدم قدرة المستخدمين المصرّح لهم للدّخول إليه.

سابعاً: تغيير موقع إلكتروني موجود على الشبكة أو إلغائه أو إتلافه أو تعديله أو إشغاله أو انتحال صفته أو انتحال شخصيّة مالكه:

وتقوم هذه الجريمة عند اتلاف أحد المواقع الإلكترونية الموجودة على الشبكة، أو إلغاؤه بشكل كامل، او تعديله أو إشغاله او انتحال صفة مالكه، بهدف القيام بعمل احتيالي، أو بهدف الاطلاع على معلومات من مستخدمي الموقع الإلكتروني الموجود على الشبكة المعلوماتيّة.

---

(٣١) سلامة، محمد عبد الله (٢٠٠٦)، جرائم الكمبيوتر والإنترنت، الاسكندرية: منشأة المعارف، ص ١٥٢.

وبالعودة إلى الرُكن المادّي لجريمة الدخول غير المشروع بصورتها المُشـــدّدة، فـــإنّ الدّخول غير المشروع إلى النظام المعلوماتي، يتطلّـــب معرفـــة خاصـــة بعلـــوم الكمبيـــوتر والشبكات، واستخدام بعض البرمجيّات الخبيثة، والتي تعمل على إحداث ذات الـــأثر الجرمـــي بصورته المشدّدة، ويمكننا تعريف البرمجيّات على أنّها: الطريقة أو أسلوب عمـــل، تنطـــوي على مجموعة من التعليمات، يتلقاها الحاسب الآلي، ويُترجمها إلى خطوات متسلسلة بهدف حل مشكلة معيّنة، أو هو عبارة عن مجموعة من التعليمات، موجّهة للحاسب تُوضـــح الخطـــوات المرسومة لحل مشكلة ما".[٣٢]

يضم الرُكن المعنوي العناصر النفسيّة للجريمة، ويعني ذلك أنّ الجريمة ليســـت كيانـــا ماديّاً خالصاً قوامه الفعل وآثاره، ولكنّها كذلك كيان نفسي، فالرُكن المعنـــوي يُمثّـــل الأصـــول النفسيّة لماديّات الجريمة والسيطرة النفسيّة عليها، ذلك أنّ هذه الماديّات لا تعني الشارع إلـــا إذا صدرت عن إنسان يُسأل عنها ويتحمّل العقاب المقرر لها، واشتراط صدورها عن إنســـان، أي اشتراط نسبتها إليه في كل أجزائها، يقتضي أن تكون لها أصول في نفسيّته، وأن تكـــون لـــه عليها سيطرة ممتدة إلى كل أجزائها، ومن ثم كان هذا الركن في جوهره قوةً نفسيّة" من شأنها الخلق والسيطرة، وهذه القوة هي الإرادة، ولكنّ الرّكن المعنوي لا يقوم بأي إرادةٍ أيّـــا كانـــت، وإنما لا بد أن تكون إرادة جرميّه".

وتستمدّ الإرادة هذه الصفة من اتّجاهها إلى ماديّات غير مشروعة، هي الماديّات التـــي تقوم عليها الجريمة، ويحدّد القانون صوّر هذا الاتّجاه وكيفيّتـــه، ولاتّجـــاه الـــإرادة الجرميّـــة صورتان رئيستان:

- **الأولى: القصد الجرمي وبه تقوم الجرائم المقصودة،**

والثانية: الخطأ وبه تقوم الجرائم غير المقصودة[٣٣].

وقد عرّف المشرّع العماني القصد الجرمي بالمادة (٣٣) من قانون الجـــزاء العمـــاني الصادر بالمرسوم السلطاني رقم ٧ لسنة ٢٠١٨م بأنّه " اتجاه إرادة الجاني إلى ارتكاب فعـــل

---

(٣٢) الغريب، انتصار نوري (١٩٩٤)، أمن الكمبيوتر والقانون، بيروت، دار الراتب الجامعية، ص٢١.

(٣٣) حسني، محمود نجيب (١٩٨٤)، شرح قانون العقوبات اللبناني، القسم العام، ص ٣٧٨ وما بعدها. انظر كذلك، نجم، محمد صبحي (١٩٩٦)، قانون العقوبات العام، القسم العام، النظرية العامة للجريمة، ص ٢٨٩.

أو الامتناع عن فعل متى كان هذا الارتكاب أو الامتناع مجرما قانونا، وذلك بقصد إحداث نتيجة مباشرة أو أي نتيجة أخرى مجرمة قانونا يكون الجاني قد توقعها وقبل المخاطرة بها." ويبدو من نص المادة (٣٣) أن جوهر القصد هو الإرادة، ومن التُحليل الدّقيق لفكرة القصد أو العمد ، يثبت أنّ الإرادة لا تتوافر عقلاً، ولا يُتاح لها أداء دورها في بنيان القصد، ما لم تكن مستندة إلى العلم" ومن ثم ساغ القول أنّ القصد " علم وإرادة "، وعليه؛ يعرف القصد الجرمي بأنه علم بعناصر الجريمة، وإرادة متجهة لتحقيق هذه العناصر أو إلى قبولها"[٣٤].

وجريمة الدّخول غير المشروع إلى النظام المعلوماتي، جريمة قصديّه أو عمدية في كل صور السلوك الإجرامي فيها، وقد عبّر المشرّع العماني عن القصد الجرمي لهذه الجريمة بالمادة (٣) قانون مكافحة جرائم تقنية المعلومات العماني رقم ١٢ لسنة ٢٠١١ بقوله ": كل من دخل عمداً ودون وجه حق...)، وكذلك بالمادة (٦) من نفس القانون بقوله: كل من عمدا ودون وجه حق موقعا إلكترونيا أو نظاما معلوماتيا ....." ويُفهم من سياق هذا النص أنّ جريمة الدخول غير المشروع إلى النظام المعلوماتي جريمة عمدية أو مقصودة لا يُتصوّر وقوعها عن طريق الخطأ.

وصورة القصد الجرمي فيها هو القصد العام بعنصرية العلم والإرادة، فلا بُدّ أن تنصرف إرادة الجاني إلى فعل الدخول أو الولوج إلى النّظام المعلوماتي أو الموقع الإلكتروني العائد للغير، مع علمه بأنّ دخوله غير مشروع، أي دون تصريح أو بما يخالف أو يجاوز الصريح، فإذا لم تجه إرادة الجاني إلى الدّخول إلى النظام المعلوماتي أو الموقع الإلكتروني، ولكنّه وجد نفسه داخل النّظام المعلوماتي عن طريق الخطأ أو الصدفة، فأوقف سلوكه عند هذا الحدّ وخرج فورا، ولم يتعدّى سلوكه إلى البقاء أو الجوال أو الاطلاع أو غير ذلك، فإنّه لا يتوافر في هذه الحالة القصد الجرمي بحقه، ولا عقاب على فِعله لانتفاء القصد الجرمي.

ويرى الباحث أنّ هذه الجريمة بصورتها البسيطة، لا تتطلّب قصداً أو عمداً خاصاً، فبمجرّد توافر القصد العامّ تقوم الجريمة، ولا أهميّة بعد ذلك الباعث الجاني على الدّخول إلى النظام المعلوماتي، سواء أكان الفضول أو إثبات القدرة على تحدّي النظام المعلوماتي أو نيّة الإضرار بالغير، وبخاصة أن المادة (٣٣) من قانون الجزاء العماني الصادر بالمرسوم رقم ٧ لسنة ٢٠١٨م قد نصت على أنها " الركن المعنوي للجريمة هو العمد في الجرائم المقصودة، والخطأ في الجرائم غير المقصودة.

---

(٣٤) حسني، محمود نجيب، مرجع سابق، ص ٣٨٥.

ويتوفر العمد باتجاه إرادة الجاني إلى ارتكاب فعل أو الامتناع عن فعل متى كان هـذا الارتكاب أو الامتناع مجرما قانونا، وذلك بقصد إحداث نتيجة مباشـرة أو أي نتيجـة أخـرى مجرمة قانونا....."

أما إذا كان الدّخول إلى النّظام المعلوماتي أو الموقع الإلكتروني، لإلغـاء أو حـذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقـل أو نسـخ بيانـات أو معلومات، أو توقيف أو تعطيل عمل نظام معلومات، أو تغيير موقع إلكترونـي أو إلغائـه أو إتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفته ، فإنّ الجريمة تتطلّب قصداً خاصاً، يتمثّل في نيّة الإضرار بالمجني عليه، لأنّ المشرّع العماني طلب ذلك صراحة في نص المـواد (٣) و(٤) و (٨) و (٩) من قانون مكافحة جرائم تقنية المعلومات العماني رقم ١٢ لسـنة ٢٠١١ ، حيث طلب أن يكون الهدف من الدّخول غير المشروع إلـى النظـام المعلومـاتي أو الموقـع الإلكتروني هو إلغاء أو تغيير أو تشويه أو إتلاف أو نسخ أو تدمير أو نشر أو إعـادة نشـر بيانات أو معلومات إلكترونية مخزنة أو اعتراض خط سير البيانات أو المعلومـات المرسـلة عبر الشبكة المعلوماتية أو وسائل تقنية المعلومات أو قطع بها أو استقبالها أو تنصت عليها .

ويرى البعض أنّ جريمة الدّخول غير المشروع إلى النظـام المعلومـاتي أو الموقـع الإلكتروني بصورتها المشدّدة، لا تتطلب قصداً جنائيّاً خاصاً مثـل قصـد الإضـرار أو نيـة الإضرار بالغير، وذلك أنّ الرُكن المادي في الجريمة يتوافر بمجرّد اختراق النظام أو الولـوج فيه، وكذلك بمجرّد ارتكاب فعل الإدخال أو الحذف أو التعديل أو الإتلاف، ذلك أنّ هذه الجريمة هي من جرائم الخطر وليست من جرائم الضرر، بمعنى أن المشرّع يستشعر خطورة الجـاني من السلوك المُجرّد الذي يقوم به، ولا يُرتّب حصول نتيجة معيّنة حتّى يتمّ عقابـه، أي ليسـت من جرائم الضرر [٣٥].

بما أنّ إثبات الرُكن المعنوي في الصورة البسيطة من جريمة الدّخول غير المشـروع إلى النظام المعلوماتي أمراً صعباً، فإنّ قاضي الموضوع هو من يحدد القصد الجرمي، فيقـوم

(٣٥) حجازي، عبد الفتاح بيومي، مرجع سابق، ص ٣٩١.
- انظر كذلك، الخوالدة، محمد سليمان (٢٠١٢)، جريمة الدخول غير المشروع إلى موقع إلكتروني او نظام معلومات وفق التشريع الأردني، دراسة مقارنة، رسالة ماجستير، الجامعة الأردنية، ص ٨٢.

بالبحث حول الرُكن المادي والأدوات المستخدمة في عمليّة الدّخول، ومقدار الحماية المتوافر في النظام المعلوماتي، وطريقة كسر هذه الحماية، وبالطبع فإنّ هذا الأمر ليس بهذه السهولة.

أمّا في الصورة المشدّدة من هذه الجريمة، فإنّ الأمر يبدو أكثر سهولة، حيث يُعتبر الفعل المصاحب للدّخول، قرينة على وجود القصد الجرمي لدى الجاني، كالإتلاف والحذف والإضافة والنّسخ والتعديل، وغيرها من الأفعال المقترنة بفعل الدّخول، فجميع هذه الأفعال تدّل على سوء نيّة الجاني واكتمال الرّكن المعنوي للجريمة.

وقد أثارت مسألة إثبات القصد الجرمي، صعوبة بالغة من قِبل التشريعات والفقهاء، وقد جعل البعض من قرينة وجود نظام حماية للنظام، من الأمور التي تدل على وجود قصد جرمي لدى الجاني، إلا أنّ المادّة الثانية من اتّفاقيّة بودابست لمكافحة الجريمة الإلكترونية لعام ٢٠٠١، قد نصت على حرّيّة الدول الأعضاء في اعتبار أنظمة الحماية جزءاً من الركن المادي للجريمة(٣٦).

الفرع الثاني

العقوبات

نصت المادة (٣) من قانون مكافحة جرائم تقنية المعلومات العماني رقم ١٢ لسنة ٢٠١١ ، على عقوبة الدّخول غير المشروع إلى النظام المعلوماتي حيث جاء فيها: "... السجن مدة لا تقل عن ستة أشهر ولا تزيد على سنة وغرامة لا تقل عن خمسمائة ريال عماني ولا تزيد على ألف ريال عماني أو بإحدى هاتين العقوبتين.

فإذا كانت البيانات أو المعلومات المنصوص عليها في الفقرة الثانية شخصية تكون العقوبة السجن مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات وغرامة لا تقل عن ألف ريال عماني ولا تزيد على ثلاثة آلاف ريال عماني أو بإحدى هاتين العقوبتين" .

كذلك عاقبت المادة (٦) الدخول غير المشروع إلى النظام المعلوماتي وتكون العقوبة السجن مدة لا تقل عن ثلاث سنوات ولا تزيد على عشر سنوات وغرامة لا تقل عن ثلاثة آلاف ريال عماني ولا تزيد على عشرة آلاف ريال عماني إذا ترتب على الفعل المجرم إلغاء أو

---

(٣٦) زين الدين بلال، مرجع سابق، ص ٢٧٩.

تغيير أو تعديل أو تشويه أو إتلاف أو نسخ أو تدمير أو نشر البيانات أو المعلومات الإلكترونية"
.

تلاحظ بأنّ المشرّع العماني، قد أعطى صلاحيّة لقاضي الموضوع في تقييم العقوبة، تبعاً للخطورة التي شكّلها الدّخول غير المشروع على مالك النّظام المعلوماتي، فمُجرّد الدخول إلى النظام المعلوماتي يستوجب العقوبة، التي تتفاوت بحسب ظروف كل جريمة على جدّه، ولذلك قام المشرّع بفرض نوعين من العقوبات (الغرامة، الحبس)، وهذا الأمر يدلّ على أنّه – المشرّع– قدْ جعل من بعض الأسباب الموضوعيّة في الجريمة أسباباً مخفّفة للعقوبة.

كما نصت المادة (٣) مكافحة جرائم تقنية المعلومات العماني رقم ١٢ لسنة ٢٠١١ ، على العقوبة في الصورة المشدّدة لذات الجريمة، حيث جاء فيها:" السجن مدة لا تقل عن ستة أشهر ولا تزيد على سنة وغرامة لا تقل عن خمسمائة ريال عماني ولا تزيد على ألف ريال عماني أو بإحدى هاتين العقوبتين .

فإذا كانت البيانات أو المعلومات المنصوص عليها في الفقرة الثانية شخصية تكون العقوبة السجن مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات وغرامة لا تقل عن ألف ريال عماني ولا تزيد على ثلاثة آلاف ريال عماني أو بإحدى هاتين العقوبتين".

يُلاحظ هنا، أنّ المشرّع قد وضع ذات العقوبات في الصورة البسيطة مع تشديدها، ورفع مجال الاختيار أمام قاضي الموضوع، ويعود ذلك للتفاوت في جسامة الجريمة الإلكترونية، التي تتم بعد الولوج إلى النظام المعلوماتي وبخاصة إذا كانت المعلومات شخصية ، فالإتلاف المعلوماتي أكثر جسامةً من جريمة الدّخول بهدف نسخ المعلومات بالنّسبة إلى النظام المعلوماتي.

وقد نصت المادة (٩) مكافحة جرائم تقنية المعلومات العماني رقم ١٢ لسنة ٢٠١١ ، على عقوبة جريمة إدخال وسائل تقنية المعلومات إلى النظام المعلوماتي، بهدف الإضرار بالبيانات أو المعلومات أو بالنّظام المعلوماتي نفسه، فقد وضع المشرّع ذات العقوبة على من يقوم باختراق النّظام المعلوماتي من خلال وسائل تقنية المعلومات ، حيث جاء في هذه المادّة: يعاقب بالسجن مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن ثلاثة آلاف ريال عماني ولا تزيد على عشرة آلاف ريال عماني أو بإحدى هاتين العقوبتين ، كل من أدخل

عمدا ودون وجه حق في نظام معلوماتي أو شبكة معلوماتية أو وسائل تقنية المعلومات ما من شأنه إيقاف أي منها أو تعطيله عن العمل أو ألغى أو غير أو عدل أو شوه أو أتلف أو دمر البرامج أو البيانات أو المعلومات الإلكترونية المستخدمة أو المخزنة في أي منها مع علمه بأن ذلك من شأنه إيقافها أو تعطيلها عن العمل ، وذلك باستخدام وسائل تقنية المعلومات " .

وهنا تُلاحظ بأنّ المشرّع قد جعل من عقوبة هذه الجريمة، مساوية للعقوبة التي نصت عليها المادّة (٣) من قانون مكافحة جرائم تقنية المعلومات ، ممّا يعني أنّ هنالك مساواةً بين الجريمتين في نظر المشرّع العماني ، تبعا لما تشكُلاه من خطورة، فأن يقوم بالجريمة إنسان بشكل مباشر من خلال لوحة المفاتيح والبرامج المتصلة بالكمبيوتر، لإعطاء الأمر المباشر بالفعل المشدّد المُجرّم، أو عن طريق برنامج خبيث، كالفيروسات أو حصن طروادة، لأنّ الهدف واحد في كلتا الجريمتين، وهو حذف أو إتلاف أو تعديل البيانات أو المعلومات الشخصية .....إلخ، وتقع هذه الجريمة بصورتها البسيطة ضمن اختصاص محاكم الجنح نظراً لعقوبتها.

المبحث الثاني

الإفشاء غير المشروع للبيانات الشخصية

تمهيد وتقسيم:

تتمتع الحياة الخاصة بحرمة تصل إلى درجة التقديس، نظراً لأنها مستودع الأسرار الإنسان، فلكل إنسان منا أسراره الخاصة التي لا يرغب في أن يطلع عليها أحد، لأن في الاطلاع عليها إهدار لحقوقه بوصفه إنساناً.

والمراسلات الخاصة تعتبر جزءاً لا يتجزأ من الحياة الخاصة، إذا تعتبر سرية المراسلات من الحقوق التي أقرتها المواثيق الدولية وجميع الدساتير.

والجدير بالذكر أن المشرع سن نصوصاً قانونية خاصة بالبيانات الشخصية، وقد بينا ما تم الاستقرار عليه في اعتبار الحسابات الشخصية من المراسلات الخاصة، وبذلك نستطيع

تطويع القواعد التقليدية والنصوص الجنائية على البريد الإلكتروني فيما يتعلق بالجرائم التي تحدق به، ومن هذا المنطلق سوف نقوم بتقسيم هذا المبحث إلى مطلبين:

- المطلب الأول: جرائم الاعتداء على سرية مراسلات البريد الإلكتروني في قانون الجزاء العماني.
- المطلب الثاني: جرائم الاعتداء على سرية مراسلات البريد الإلكتروني في قانون تقنية المعلومات ٢٠١١ .

المطلب الأول
جرائم الاعتداء على سرية مراسلات
البريد الإلكتروني فى قانون الجزاء العماني

تمهيد وتقسيم:

كفل المشرع العماني حرمة المراسلات واعتبرها من عناصر الحياة للشخص، وذلك وفق المادة (٣٠) من الدستور الحالي.

وعلى ذلك، فإن البريد الإلكتروني يمكن أن تطبق عليه مفهوم المراسلة الخاصة، وحتى لا يتم إهدار لحقوق الإنسان[٣٧] المتمثلة في حق الإنسان في الحياة الخاصة التي نكون أمام أساسين لا ثالث لهما، الأول: حق الإنسان في الحفاظ على حياته الخاصة والثاني: الحق في الخصوصية، وبالتالي امتدت وتنوعت الجرائم التي تنتهك الحق في حرمة المراسلات الخاصة من حيث الوسائل اللازمة لارتكابها، وخصوصاً في ظل استخدام شبكة الإنترنت مستخدماً وسيلة البريد الإلكتروني في ذلك.

ح الجريمة بكافة أنواعها:

وإزاء ذلك، كان لابد من تدخل القوانين العقابية للحد من هذا الإجرام الخطير، ولكن الأمر ينبع منه مشكلة ألا وهي أن النصوص العقابية التقليدية قد وضعت في مرحلة سابقة لهذا التطور التكنولوجي الذي حدث لوسائل الاتصال، لذا تم استبدال قانون الجزاء العماني رقم ٧ /

---

(٣٧) د. عمر الفاروق الحسيني، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية، دراسة مقارنة، بدون جهة نشر، ط ٢، ١٩٩٠، ص٤٨.

٧٤ بقانون جزاء صادر بمرسوم سلطاني رقم ٧ لسنة ٢٠١٨ ، لمواكبة التطـــور الحاصـــل، وخصوصاً في مجال جرائم تقنية المعلومات، إلا أن ذلك لا يعني عـــدم الاســـتعانة بنصـــوص قانون الجزاء وتطبيقها على جرائم البريد الإلكتروني ، وعلى ذلك سوف نقـــوم بتقســـيم هـــذا المطلب إلى ثلاثة فروع:

- الفرع الأول: جريمة نقل المحادثات الخاصة عبـــر البريـــد الإلكتروني.
- الفرع الثاني: جريمة نقل الصورة عبر البريد الإلكتروني.
- الفرع الثالث: جريمة التهديد بالإفشاء.

الفرع الأول

جريمة نقل المحادثات الخاصة[٣٨] عبر البريد الإلكتروني

تنص المادة (٣٣٢) من قانون الجزاء العماني الصادر بمرسوم ســـلطاني رقـــم ٧ / ٢٠١٨ على أنه " يعاقب بالسجن مدة لا تقل عن (١٠) عشرة أيام، ولا تزيد علـــى (٣) ثلاثـــة أشهر، كل من اعتدى على حرمة الحياة الخاصة للأفراد في غير الأحوال المصرح بها قانونـــا، وذلك بارتكاب أحد الأفعال الآتية:

أ – فض رسالة أو برقية خاصة موجهة لغيره من الأفراد.

ب – استرق السمع في مكالمة هاتفية.

ج – سجل أو نقل محادثات بواسطة جهاز، أيا كان نوعه.

د – التقط أو نقل صورا لفرد أو أفراد بواسطة جهاز أيا كان نوعه....

---

(٣٨) د. محمد الشهاوي، الحماية الجنائية لحرمة الحياة الخاصة، دار النهضـــة العربيـــة، القـــاهرة، ٢٠٠٥، ص٣٠٠. وفي ذات المعني راجع: د. محمد الشهاوي، شرح قانون تنظيم الاتصالات رقـــم ١٠ لســـنة ٢٠٠٣، دار النهضة العربية، ط١، ٢٠١٠، ص ٢٧١. وفي ذات المعني أيضاً راجع: د. آدم عبد البديع، الحـــق فـــي حرمة الحياة الخاصة ومدى الحماية التي يكفلها له القانون الجنائي، رسالة دكتوراه، كليـــة الحقـــوق، جامعـــة القاهرة، ٢٠٠٠، ص٥٨٧.

وردت هذه الجريمة وفق نص المادة سالفة الذكر، حيث تضمنت الحماية الجنائية لحق الأفراد في الخصوصية، وذلك بأن "استرق السمع أو سجل أو نقل المحادثات عن طريق جهاز من الأجهزة أياً كان نوعه محادثات جرت في مكان خاص أو عن طريق التليفون في غير الأحوال المصرح بها قانوناً أو بغير رضا المجني عليه".(٣٩)

ويرى الباحث هنا أن نخص نقل المحادثات بحيث يتم النقل كما قال المشرع عن طريق جهاز من الأجهزة أياً كان نوعه، أو وسيلة يتم بها النقل، وهنا يتم النقل، أي نقل الحديث عن طريق البريد الإلكتروني بأن يقوم الفاعل بإرسال رسالة تحمل هذه الحديث إذ إن البريد الإلكتروني يمكن أن يحمل في طياته صوتاً، صورةً، أو حديثاً.

ولا يشترط الحديث أن يكون بلغة معينة، وبذلك تمتد الحماية لتشمل الحديث الحاصل بالإشارات في حالة الصم والبكم، وعلى ذلك وبمفهوم المخالفة لا تمتد الحماية إلى الأصوات غير المنطوقة مثل الضوضاء والموسيقى(٤٠)، ويقصد المشرع من بسط الحماية في المادة (٣٣٢) من قانون الجزاء العماني على أية معلومات تتعلق بالحياة الخاصة، والمقصود بالحياة الخاصة ما يقوم به الشخص ولا يرضى أن يراه أحد غيره(٤١).

وسوف نتناول هذا الفرع في ثلاثة غصون وهي: الركن المادي (الغصن الأول)، الركن المعنوي (الغصن الثاني)، العقوبة (الغصن الثالث) وذلك كما يلي:

الغصن الأول: الركن المادي:

يتحقق الركن المادي للجريمة المنصوص عليها في المادة (٣٣٢) من قانون الجزاء العماني استرق السمع أو سجل أو نقل المحادثات عن طريق جهاز من الأجهزة أياً كان نوعه محادثات جرت في مكان خاص أو عن طريق التليفون في غير الأحوال المصرح بها قانوناً أو بغير رضا المجني عليه، ومن ثم يلزم لقيامه توافر أربعة عناصر مهمة:

العنصر الأول: وهو سلوك إجرامي، أي النشاط الإجرامي المكون الركن المادي لهذه الجريمة الذي يتخذ شكل نقل المحادثات الخاصة عن طريق البريد الإلكتروني، ونلاحظ أن

---

(٣٩) د. محمد الشهاوي، شرح قانون تنظيم الاتصالات رقم ١٠ لسن ٢٠٠٣، مرجع سبق ذكره، ص ٢٧٣.

(٤٠) د. محمد نجيب حسني، القسم الخاص، دار النهضة، ١٩٩٤، ص ٧٨٩.

(٤١) د. محمد الشهاوي، الحماية الجنائية لحرمة الحياة الخاصة، مرجع سبق ذكره، ص ٣٠٩.

السلوك الإجرامي المكون للركن المادي في قانون العقوبات المصري ينطبق على حالات التنصت عن طريق وسائل التكنولوجيا الحديثة والمتطورة ومنها الحاسوب الشخصي، أو الموجودة في الملفات الشخصية بالبريد الإلكتروني للأشخاص، وكذلك على شبكة الإنترنت وذلك للمحادثات التي تقع بين الأفراد أو تسجيلها أو نقلها(٤٢).

ونجد هنا أنه لابد من استخدم جهاز أياً كان نوعه في استراق السمع أو تسجيل المحادثة أو نقلها، بيد أن القانون المصري اشترط أن يكون هذا السلوك قد تم عن طريق جهاز من الأجهزة أياً كان نوعه، ويقصد بذلك استخدام أية وسيلة أتيحت للجاني بفعل التقدم العلمي والتقنية الحديثة المتطورة تم اكتشافها بعد النص على هذه الجريمة أو أخرى لم تكتشف بعد، لأن عبارات المادة تسمح بذلك، حيث ورد فيها استخدام جهاز من الأجهزة أياً كان نوعه، فيمكن استخدام الحاسب الآلي والكاميرات المثبتة لاستراق السمع أو تسجيله في مكان خاص أو نقل الحديث عبر الإنترنت مستخدماً في ذلك البريد الإلكتروني كوسيلة نقل، وقد عرّف أحد الفقهاء(٤٣) بأن استراق السمع يمكن باستخدام جهاز المحادثة في مكان خاص، أو من خلال التليفون لإرسالها من المكان الذي وجد فيه المجني عليه إلى مكان آخر باستخدام كبسولة الإرسال.

ويرى الباحث أننا نستطيع تعريف نقل الحديث بأنه "نقل المحادثة الخاصة التي تمت، باستخدام البريد الإلكتروني لإرسالها من المكان الذي وجد فيه المجني عليه إلى مكان آخر عبر الإنترنت".

ولكي يتحقق السلوك الإجرامي على أكمل وجه، وهو المكون الركن المادي، يجب أن تكون المحادثات التي تم نقلها قد جرت في مكان خاص أو عن طريق التليفون.

وفي الواقع نجد أن هذه المادة في قانون العقوبات الفرنسي الجديد قد مدت نطاق التجريم إلى الأقوال التي تصدر من الأشخاص حتى في الأماكن العامة، ولكن بصفة خاصة أو

---

(٤٢) منى فتحي أحمد عبد الكريم، الجريمة عبر الشبكة الدولية للمعلومات – صورها ومشاكل إثباتها، رسالة دكتوراه، كلية الحقوق جامعة القاهرة، ٢٠٠٨، ص٤٨.

(٤٣) د. محمد الشهاوي، شرح قانون تنظيم الاتصالات رقم ١٠ لسنة ٢٠٠٣، مرجع سبق ذكره، ص ٢٧٤.

سرية[٤٤]، أي بعبارة أخرى لقد اعتد قانون العقوبات الفرنسي الجديد في المادة (٢/٢٢٦) بطابع السرية والخصوصية للأقوال التي يتم الحصول عليها عن طريق الاحتيال أو الغش، واعتبر المشرع الفرنسي في المادة (٢٢٤-١)[٤٥]، إما بالنقاط أو التسجيل أو إرسال أقوال بدون موافقة من قام بنطق تلك الكلمات.

وهكذا نرى أنه ينبغي أن يعتد فقط بمضمون الأحاديث، وليس بمكان الحصول عليها، لأن الأخذ بمعيار طبيعة الحديث يتفق مع ضرورة إضفاء الحماية للحياة الخاصة بغض النظر عن المكان الذي يجري فيه الحديث الذي يعتبر بلا أدنى شك أهم صورها وهو جوهرها، إذ كثيراً من الأحيان يتم التحدث في أمور خاصة في أماكن عامة، وقد تكون هذه الأمور وثيقة الصلة بالحياة الخاصة، كما يحدث حالياً في اللقاءات والاجتماعات الخاصة في بعض النوادي الاجتماعية[٤٦]

فعلى سبيل المثال في فرنسا نرى أن تسجيل محادثة بين محام وموكله في صالة الجلسة، وتعتبر صالة الجلسة في هذه الحالة من الأماكن العامة، ولكن يعتد بمضمون هذا الحديث، وليس بالمكان الذي وقعت فيها الجريمة[٤٧].

ويرى الباحث، أن استخدام تليفون كوسيلة لنقل أو تسجيل المحادثات التي تجري في مكان خاص يمكن تطبيقها على الاعتداءات التي تقع على حرمة الحياة الخاصة عن طريق شبكة الإنترنت، فإن نقل المحادثات عبر البريد الإلكتروني عن طريق شبكة الإنترنت يمكن تطبيقها أو تقع تحت طائلة المادة (٣٣٢) من قانون الجزاء العماني الصادر بالمرسوم السلطاني رقم **2018 / 7**، والتي تتلخص في عمل "أو نقل عن طريق جهاز من الأجهزة..."،

---

(٤٤) أيمن عبد الحفيظ عبد الحميد سليمان، الأحكام الموضوعية للقانون الجنائي والجرائم المعلوماتية، رسالة ماجستير، كلية الحقوق جامعة القاهرة، ٢٠١٠، ص١٩٨.

(٤٥) حيث جاء نص المادة (٢٢٦-١) من قانون العقوبات الفرنسي، وسوف نوردها باللغة الفرنسية:

Article 226-1

Modifié par Ordlonnance n92000) -916 clut 19 septembre 2000 - drt. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002.

"Est puni d'un an d'emprisonnement et de 45 000 euros d'amende le fait, au moyen d'um procédé quelconque, volontairement de porter atteinte a l'intimité de la vie privée d'autrui:"

"1° En captant, enregistrant ou transmettant, Sans le consentement de leur auteur, des paroles prononcéesa titre privé ou confidentiel".

(٤٦) أسماء حسن سيد محمد رويعي، الحق في حرمة الحياة الخاصة في مواجهة الجرائم المعلوماتية، رسالة دكتوراه، كلية الحقوق جامعة القاهرة، ٢٠١٣، ص ٥٩١.

(47) Veron (Michel) , Droit penal spécial, Armand Colin, Edition 1996, P. 132.

وبذلك ترك المشرع الباب مفتوحاً، لأن التقدم العلمي لا يتوقف[٤٨]. ولا يشترط في المحادثات أن تكون بلغة، بل يمكن أن تكون من خلال الإشارات الخاصة، ولكن كما أشرنا في السابق "لا حماية للأصوات غير المنطوقة والضوضاء والموسيقى"[٤٩].

أما عن العنصر الرابع والأخير لقيام هذه الجريمة، هو أن يكون استراق السمع أو تسجيل أو نقل المحادثات قد تم بعدم رضاء المجني عليه، وهنا نخص النقل الذي هو أحد السلوك الإجرامي المكون للركن المادي في هذه الجريمة، إذ يقوم بنقل المحادثة الخاصة عن طريق البريد الإلكتروني عبر الإنترنت.

حيث إنه إذا توافر سبب لإباحة الفعل فلا جريمة[٥٠]، وعلى ذلك يفترض الرضا عندما يرتكب الفعل على مرأى ومسمع صاحب الشأن دون إبداء أي اعتراض منه على ذلك، في حين أنه كان بوسعه الاعتراض[٥١]، لأن ذلك يعد من عناصر الركن المادي للجريمة، فإذا توافر الرضا فلا جريمة.

وأساس النص على أن رضا المجني عليه سبب لإباحة الفعل، هو أن ذلك الرضا يزيل عن الحديث صفة السرية، وبالتالي لا يكون هناك أي اعتداء على الحياة الخاصة والمتمثلة في انتهاك سرية المراسلات المتمثلة في البريد الإلكتروني.

الغصن الثاني: الركن المعنوي:

إن الجريمة المنصوص عليها في المادة (٣٣٢) من قانون الجزاء العماني الصادر بمرسوم سلطاني رقم **2018 / 7** فيها صورة القصد الجنائي العام، والذي يتحقق بتوافر عنصرين هما العلم والإرادة. [٥٢]

علماً أن الفقه الجنائي اختلف بين نظريتين تنازعتا حول تعريف القصد والعناصر التي تدخل فيه، إلا أنه يمكن القول في نهاية المطاف إلى أن الإرادة المتجه –عن علم– إلى إحداث

---

(48) Laure Rassat (M), Droit penal special, Dalloz, Edition 2006, P. 366.

(٤٩) د. شريف سيد كامل، حقوق الإنسان في القانون الجنائي، دار النهضة العربية، القاهرة، ط١، ٢٠١٤، ص ٤٢١.

(٥٠) د. محمد الشهاوي، شرح قانون تنظيم الاتصالات رقم ١٠ لعام ٢٠٠٣، مرجع سبق ذكره، ص٢٧٥.

(٥١) المستشار أحمد محمود موافي، شرح قانون تنظيم الاتصالات، دار الحقوق للنشر والتوزيع، ط١، ٢٠١٢، ص١٤٥.

(٥٢) آدم عبد البديع آدم، مرجع سبق ذكره، ٥٩٣.

نتيجة يجرمها القانون ويعاقب عليها، مفادُها هو الوصول أن القصد يقوم على العلم والإرادة معاً[٥٣].

ولقد قضت محكمة النقض المصرية بأنه "من المقرر أن القصد الذي يتطلبه الشارع في جريمة استراق السمع المنسوبة إلى المطعون ضده والمعاقب عليها بنص المادة ٣٠٩ مكرر من قانون العقوبات هو القصد العام الذي يتحقق بمجرد ارتكاب الفعل المادي، وتستوي البواعث التي دفعت المتهم إلى فعله، وأن مجرد الاعتداء على حرمة الحياة الخاصة باستراق السمع يفترض فيه القصد إذا ما توافر عنصراه العلم والإرادة"[٥٤].

ويتم التطبيق بالتالي في دراستنا على فعل "النقل" وفق التقنية الحديثة، حيث إن المشرع ترك الباب مفتوحاً للتقنية المتطورة .

وبناء على ما تقدم نجد أن الجريمة التي عاقب عليها المشرع بنص المادة (٣٣٢) من قانون الجزاء العماني الصادر بمرسوم سلطاني رقم ٧ لسنة ٢٠١٨م تقوم بالقصد الجنائي العام[٥٥] فقط وليس الخاص[٥٦].

---

(٥٣) د. إبراهيم عيد نايل، أثر العلم في تكوين القصد الجنائي، بدون دار نشر، ١٩٩٢، ص ٩-٣٣.

(٥٤) وهذا ما جاء في الطعن رقم ١٦٣٦٨ لعام ٥٥ق، جلسة ١٨/١/٢٠٠٨، مجموعة أحكام محكمة النقض، القاعدة رقم ٨، ١٢٤.

راجع نص المادة (٣٠٩) مكرر: "يعاقب بالحبس مدة لا تزيد على سنة كل من اعتدى على حرمة الحياة الخاصة للمواطن، وذلك بأن ارتكب أحد الأفعال الآتية فى غير الأحوال المصرح بها قانونا أو بغير رضاء المجنى على (ب) التقط أو نقل بجهاز من الأجهزة أيا كان نوعه صورة شخص فى مكان خاص". "ولا يقتصر التجريم على الشخص القائم بالتقاط الصورة فقط وفقا للنص السابق، ولكن التجريم يمتد ليشمل كلا من سهل أو أذاع أو شارك فى نشر الصورة"..

(٥٥) د. مدحت عبد الحليم رمضان، جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية، القاهرة، ٢٠٠٠، ص ١٢١.

(٥٦) يكاد يجمع الفقه في فرنسا ومصر على أن القصد الخاص عبارة عن عنصر إضافي على العناصر الموجودة في القصد العام. وهذا العنصر يتطلبه القانون صراحة أو ضمناً لأن به تكتمل أركان القصد الجنائي في بعض الجرائم، بمعنى أن القصد العام أي العلم والإرادة لا يعد كافياً لقيام العمد في تلك الجرائم وهذا العمد لا يكتمل إلا بإضافة القصد الخاص، ولكن بالرغم من إجماع الفقه على أن القصد الخاص عنصر إضافي على القصد العام، إلا أن الفقهاء لم يجمعوا على مضمون هذا القصد الخاص، فنجد أن أغلب الفقه يرى أن القصد الخاص عبارة عن الباحث الدافع لارتكاب الجريمة ويتطلبه القانون استثناء من الأصل العام الذي لا يقيم أي وزن للباعث في القانون الجنائي.

وعلى ذلك يتعين أن تتجه إرادة الجاني إلى نقل المحادثات الخاصة في مكان خاص أو باستخدام التليفون، وهنا ورد النقل عن طريق جهاز من الأجهزة، فالنص متروك كما قلنا في السابق مفتوح لأي نوع، وبالتالي ينطبق على البريد الإلكتروني الذي يتم به نقل الأحاديث الخاصة عبر الإنترنت وفق أي جهاز سواء تليفون أو حاسب أو غيره من الأجهزة التقنية، ويتعين أن تتجه إرادة الجاني إلى ارتكاب الفعل وتحقيق النتيجة وهي النقل في مثالنا هذا عبر الإنترنت بواسطة استخدام البريد الإلكتروني.

ويرى الباحث أنه يشاطر الرأي[٥٧] القائل الركن المعنوي لجريمة نقل المحادثات الخاصة تقوم بتوافر القصد العام فقط بعنصرية العلم والإرادة، فالغاية التي يبتغيها المشرع من وضعه لنص المادة (٣٣٢) من قانون الجزاء العماني الصادر بمرسوم سلطاني رقم ٧ لسنة ٢٠١٨م هي الحفاظ على حرمة الحياة الخاصة وبسط حماية كافية من اعتداءات الآخرين.

أما الفقه الفرنسي، فقد تباين في تصور الركن المعنوي للجريمة، أي على ماهية القصد، إذ اتجه جانب كبير من الفقهاء[٥٨] يفترض لهذه الجنحة قصداً عاماً يقوم على إدراك فعل غير مشروع، وينبغي أن يضاف إلى هذا القصد العام قصد خاص يقوم على إرادة الاعتداء على حرمة الحياة الخاصة، إذ يرى أن القانون يتطلب قصداً خاصاً فالمتهم ينبغي أن يبحث للوصول إلى نتيجة معينة، هي الاعتداء على حرمة الحياة الخاصة".

ويرى جانب آخر من الفقه[٥٩] الفرنسي مؤيداً للرأي السابق، إذ يرى أن "إدراك ارتكاب عمل غير مشروع" ينبغي أن يضاف إليه قصداً خاص بجانب القصد العام.

الغصن الثالث: العقوبة:

إن جريمة استراق السمع في مكالمة هاتفية أو سجل أو نقل محادثات بواسطة جهاز، أيا كان نوعه أو التقط أو نقل صورا لفرد أو أفراد بواسطة جهاز أيا كان نوعه نصت عليها

---

(٥٧) د. محمد الشهاوي، شرح قانون تنظيم الاتصالات رقم ١٠ لعام ٢٠٠٣، مرجع سبق ذكره، ص ٢٧٨. وراجع في ذات المعني: د. محمد الشهاوي، الحماية الجنائية لحرمة الحياة الخاصة، مرجع سبق ذكره، ص٣١٣.

(58) Chavanne (A), Les atteintes a l'intimité de la vie privée au sens de l'article 368 du code penal, P. 28.

(59) Ravanas, La protection des personnes contre la réalisation et la publication de leur image, 1981, P. 522.

المادة (٣٣٢) من قانون الجزاء العماني الصادر بمرسوم سلطاني رقم ٧ لسنة ٢٠١٨م ، وهي جنحة وعقوبتها السجن مدة لا تقل عن (١٠) عشرة أيام، ولا تزيد على (٣) ثلاثة أشهر ، وذلك لاقترافها من شخص عادي، فإذا ارتكبت الجريمة من موظف عام اعتماداً على وظيفته والسلطة التي تمنحه أياً ما تكون العقوبة السجن مدة لا تقل عن شهر، ولا تزيد على سنة .

وأجاز المشرع العماني بعقوبة تكميلية في المادة رقم (٥٩) من قانون الجزاء العماني الصادر بمرسوم سلطاني رقم ٧ لسنة ٢٠١٨م للمحكمة عند الحكم بالإدانة في جناية أو جنحة أن تحكم بمصادرة الأشياء المضبوطة التي تحصلت من الجريمة، أو التي استعملت في ارتكابها، أو التي كانت معدة للاستعمال فيها.

كذلك المادة (٣٢) من قانون مكافحة جرائم تقنية المعلومات الصادر بالمرسوم السلطاني رقم ١٢ لسنة ٢٠١١ حيث نصت على أنه " دون إخلال بحقوق الغير حسن النية ، على المحكمة المختصة الحكم فى جميع الأحوال بالآتى :

أ – مصادرة جميع الأجهزة والأدوات والبرامج وغيرها من الأشياء التى استعملت فى ارتكاب جريمة تقنية المعلومات وكذلك الأموال المتحصلة منها .

ب– غلق الموقع الإلكتروني والمحل الذى ارتكبت فيه جريمة تقنية المعلومات أو الشروع فيها إذا كانت الجريمة قد ارتكبت بعلم مالكه وعدم اعتراضه ، ويكون الغلق دائما ، أو مؤقتا المدة التي تقدرها المحكمة في ضوء ظروف وملابسات الجريمة .

ج – طرد الأجنبي المحكوم عليه بعقوبة إرهابية أو بعقوبة تأديبية إذا كانت الجريمة شائنة .

وهنا ونحن بصدد النقل عن طريق البريد الإلكتروني عبر الإنترنت، تعد هذه الجريمة معاقباً عليها بموجب نص المادة (٣٣٢) ، وبالتالي فإن هذه الأحكام تطبق على البريد الإلكتروني بوصفه يدخل ضمن وسائل الاتصال والمراسلة.

الفرع الثاني

جريمة نقل الصورة عبر البريد الإلكتروني:

إن جريمة نقل الصورة للغير المنصوص عليها في المادة (٣٣٢) من قانون الجزاء العماني، وهنا نخص نقل الصورة عن طريق البريد الإلكتروني، أي إرسالها عن طريقه، أي يستخدم البريد الإلكتروني في نقل وإرسال الصورة "أي صورة المجني عليه حال وجوده في مكان خاص"، أي فعل الالتقاط هنا ليس لنا به حاجة، إذ إن ما يخصنا النقل.

وهذه الجريمة يستلزم توافر شرطين لقيامها، أولهما أن تكون هناك صورة الشخص، فلا تقوم الجريمة إذ كان هناك صورة مستند أو مكان عادي، وثانيهما وجود الشخص في مكان خاص، وأساس هذا الشرط حماية الحياة الخاصة للأفراد، فلا تقع الجريمة إذا تم نقل صورة لشخص وجد المجني عليه في مكان عام، وتطبيقا لذلك فلا تتوافر هذه الجريمة إذا نقل صورة شخص حال وقوفه أو جلوسه في شرفة منزله المطلة على الطريق العام.(٦٠)

وبالتالي إن جريمة نقل الصورة هنا تتطلب لقيامها ركنين أولهما مادي يتمثل في نقل صورة شخص في مكان خاص بغير رضاه باستخدام جهاز أيا كان نوعه، وثانيهما معنوي يتخذ صورة بقصد جنائي، وفيما يلي سوف نتناول في هذا الفرع في ثلاثة غصون وهي: الركن المادي (الغصن الأول)، الركن المعنوي (الغصن الثاني)، العقوبة (الغصن الثالث)، وذلك كما يلي:

الغصن الأول: الركن المادي:

يتحقق الركن المادي لهذه الجريمة بالتقاط أو نقل الصورة الخاصة لشخص ما، ولما كان الأمر متعلقاً بالبريد الإلكتروني فإن النشاط الإجرامي المتعلق بالتقاط الصور غير متصور هنا، فنحن نختص بالفعل أو النشاط الإجرامي المتعلق بالنقل بما أن البريد الإلكتروني إحدى وسائل المراسلات والاتصالات المتداولة أكثر انتشاراً كما سبق لنا وذكرنا، وعليه فإن الركن المادي هنا يتحقق بنقل صورة شخص في مكان خاص بغير رضاه، باستخدام جهاز أو وسيلة فنية أياً كانت، فيلزم لقيامه إذا توافرت العناصر الأربعة الآتية:

١- سلوك أو نشاط إجرامي يتخذ شكل نقل الصورة.

٢- استخدام جهاز أياً كان نوعه في نقل الصورة.

---

(٦٠) د. محمد الشهاوي، مرجع سبق ذكره، ص ٢٨٤.

٣- تواجد من نقل شكله في مكان خاص.

٤- عدم رضاء المجني عليه.

وفيما يلي شرح هذه العناصر:

أولاً: سلوك أو نشاط إجرامي يتخذ شكل نقل الصورة:

إن النشاط الإجرامي المكون للركن المادي يتمثل في النقل الذي عرفه أحد الفقهاء بأنه تمكين شخص يوجد في مكان مختلف عن المكان الذي يوجد فيه المجني عليه من الاطلاع على صورته، ويستوي أن يكون المكان الذي تنقل إليه الصورة مكاناً عاماً أو خاصاً [٦١]. أما في اللغة فنقل الشيء يعني تحويله من مكان موضوع إلى موضح[٦٢]

ويرى بعض الفقه إلى أن نقل صورة الشخص يعني تحويلها أو إرسالها من مكان تواجده إلى مكان آخر عام أو خاص، بحيث يستطيع الغير مشاهدة قسمات وملامح شكل المجني عليه وما يأتيه من حركات أو أفعال[٦٣].

وبالتالي قانون الجزاء العماني نراه لا يحمي حرمة الحياة الخاصة ضد المساس بها عن طريق النقل إلا بشرط مؤداه أن تكون صورة المجني عليه قد نقلت وهو في مكان خاص، وبالتالي لا أهمية لهيئة أو شكل المجني عليه أو مظهره، أو الحالة التي هو عليها في المكان ساعة نقل الصورة، وعلى ذلك تقع الجريمة حتى لو تم نقل الصورة وهو في مسكنه مرتدياً ملابسه أو في وضع لا يخجله اطلاع الغير عليه [٦٤].

ثانياً: استخدام جهاز أياً كان نوعه في نقلها:

إن المشرع وفقاً لنص المادة (٣٣٢) من قانون الجزاء العماني قد حدد الأداة أو الوسيلة الارتكاب الجريمة وهي جهاز أياً كان نوعه.

---

(٦١) د. محمد زكي أبو عامر، الحماية الجنائية للحريات الشخصية، منشأة المعارف، الإسكندرية، ١٩٧٩، ص٩٣. وراجع في ذات المعني: د. محمد الشهاوي، مرجع سبق ذكره، ص ٢٨٩.

(٦٢) د. محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، دار النهضة، ط٢، فقرة رقم ٥٥، ص٩٧٧.

(٦٣) د. محمد الشهاوي، مرجع سبق ذكره، ص ٣٢٠.

(٦٤) د. أحمد محمد حسان، نحو نظرية عامة لحماية الحق في الحياة الخاصة في العلاقات بين الدولة والأفراد، دار النهضة العربية، القاهرة، ط١، ٢٠٠١، ص ٤٩.

وبناء على ذلك، فإن الأمر قد يتصور في حالة نقل صورة شخص مسجلة أو موضوعة على جهازه الشخصي الذي تم اختراقه من قبل الجاني بوسيلة من وسائل الاختراق، ونقل الصورة الموجودة عليه وقام باستعمالها دون رضائه، فإن ذلك يعد نقلاً للصورة من مكان خاص، حيث يعد الحاسوب بمثابة المكان الخاص الذي يقوم صاحبه بوضع كل ما يخصه عليه من بيانات وصور(٦٥)، وبهذا المثال يكون النشاط الإجرامي مكوناً من فعلين؛ هما الاختراق وهذه جريمة مستقلة بذاتها، أما الثاني وهو النقل (٦٦).

وتطبيقاً لذلك، فإن تعبير "بجهاز من الأجهزة أياً كان نوعه" فإنه يتسع ليشمل جميع الأجهزة أو المستحدثات العلمية في هذا المجال(٦٧)، ومنه الحاسب الآلي واستخدام البريد الإلكتروني كأحد الوسائل المستخدمة في النقل في العصر الحديث، وأكثر شيوعاً.

ثالثاً: تواجد من نقل قسمات شكله في مكان خاص:

المشرع في جريمة نقل الصورة أوجب أن يتم ذلك في حال وجود المجني عليه في مكان خاص(٦٨)، وتطبيقاً لذلك فإن قيام الجاني بنقل صورة لشخص كانت موجودة على موقع من المواقع التي تسمح لكافة الجمهور المتابعين للشبكة الدولية بدخوله.

وكذلك الاطلاع على ما فيه من صور، فإن ذلك يعد مكاناً عاماً مطروحاً للكافة، وبالتالي فإن نقل ما فيه من صور عبر البريد الإلكتروني لأي أحد أو أي مكان لا يعد جريمة، وكذلك إذا تم استعمالها، لأن واضع الصورة عالم بأن هذا الموقع مطروح للكافة، وبالتالي يعد متنازلاً ضمنياً على حقه في الصورة، ويكون رضاؤه مفترضاً، والأمر مختلف عن المثال الذي أوردناه في العنصر السابق، الذي نقل فيه الجاني صورة شخص موضوعة على جهازه الشخصي ونقل ما هو موجود به من محتوى ومنها الصور، حيث اعتبر جهاز الحاسب الآلي

---

(٦٥) منى فتحي عبد الكريم، الجريمة عبر الشبكة الدولية للمعلومات – صورها – ومشاكل إثباتها، رسالة دكتوراه، كلية الحقوق جامعة القاهرة، ٢٠٠٨، ص ٤٩.

(66) Mais (H), et Huet (J), Droit de l'information et des telecommunication, éd Litec 1993, P. 842.

(٦٧) د. محمد الشهاوي، مرجع سبق ذكره، ص ٢٨٧.

(٦٨) د. سليمان أحمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، القاهرة، ٢٠١٣، ص٥٠.

مكاناً خاصاً، ويعتبر الاطلاع على محتواه مرتكباً لجريمة الاعتداء على الحياة الخاصة متمثلاً في نقل محتواه من سر أو أسرار[٦٩].

ويذهب أحد الفقهاء إلى أن نقل الصورة للمجني عليه حالة وجوده في مكان خاص لا تقوم به الجريمة إذا كان الشخص يتحدث بصوت مرتفع يستطيع من كان في مكان عام سماعه، وبالتالي ليس له حرمة[٧٠].

رابعا: عدم رضاء المجنى عليه[٧١] :

إن طبيعة الحياة الخاصة وحرمتها تفرض عدم رضاء المجني عليه وهي موضوع الحماية، وبالتالي يتيقن أن يتوافر في الرضا المعلم للجريمة مجموعة شروط، فيلزم أن يكون معاصراً لنقل الصورة، فإن كان سابقاً تعين أن يظل قائماً حتى لحظة وقوعها، أما الرضا اللاحق فلا يمنع من قيام الجريمة[٧٢]

وبالتالي، فإن نص المادة (٣٣٢) من قانون الجزاء العماني أقام قرينة على الرضا بما أفادت به المادة من أنه إذا كان نقل الصورة في غير الأحوال المصرح بها ، وعليه إذا تم نقل الصورة أثناء اجتماع على مسمع أو مرأى من الحاضرين في ذلك الاجتماع، فإن رضاء هؤلاء يكون مفترضاً، فعدم رضاء المجني عليه عنصر مادي، فإذا تخلف هذا العنصر فلا جريمة، فرضاء المجني عليه يزيل عن التدخل في الحياة الخاصة صفة غير المشروعية[٧٣].

لذلك قد أوجبت المادة (٣٣٠) من قانون الجزاء العماني أن يكون فعل نقل الصورة قد تم دون موافقة للمجني عليه وفي غير الأحوال المصرح بها ، وهكذا نستطيع أن نؤكد ما ذهب إليه المشرع الفرنسي وفق نص المادة (٢٢٦-١) في الفقرة الثانية.[٧٤]

---

(٦٩) د. علي عبود جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، دار منشورات زين الحقوقية، ط١، ٢٠١٣، ص ٣٩٩.

(٧٠) د. محمد الشهاوي، مرجع سبق ذكره، ص٣٢٢.

(٧١) أسماء حسن سيد، مرجع سبق ذكره، ص٥٦٩. وفي ذات المعني: د. محمد الشهاوي، مرجع سبق ذكره، ص ٢٨٨.

(٧٢) د. احمد محمد حسان، مرجع سبق ذكره، ص ٥٠.

(٧٣) د. محمد الشهاوي، مرجع سبق ذكره، ص ٣٢٢.

(٧٤) جاء نص (٢٢٩-١) الفقرة الثانية على أنه:

"2° En fixant, enregistrant ou transmettant, Sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé."

الغصن الثاني: الركن المعنوي:

إن نقل الصورة من مكان خاص بغير رضاء المجني عليه، وباستخدام جهاز أو وسيلة فنية هي جريمة عمدية يأخذ الركن المعنوي صورة القصد الجنائي العام بعنصرية العلم والإرادة، بحيث لا يكفي لقيامها توافر الخطأ غير العمدي.

وبذلك يجب أن يعلم الجاني بأنه يقوم بنقل الصورة، وأن المجني عليه يوجد في مكان خاص، وتتجه إرادته لإتيان هذا الفعل.

أولاً: علم الجاني:

يجب على الجاني أن يكون عالماً بأنه يقوم بنقل الصورة مستخدماً جهازاً أو أي وسيلة فنية، ونحن في هذا المضمار يكون البريد الإلكتروني هو الوسيلة التي يستخدمها الجاني في نقل الصورة، وأن المجني عليه يوجد في مكان خاص، فإذا ما انتفى علم الجاني بأي عنصر من العناصر السابقة "عنصر بأنه يعلم بأنه يقوم بنقل الصورة وعنصر بأنه يعلم بأن المجني عليه في مكان خاص"، فلا قيام للقصد الجنائي وتنتفي الجريمة، وتطبيقاً لذلك فلا تقوم الجريمة في حالة قيام أحد الأشخاص بنقل صورة منزل أثري من الخارج يقع في الطريق العام، فتضمنت الصورة مالك هذا العقار دون أن يعلم المالك بالتصوير(٧٥)

ثانياً: اتجاه إرادة الجاني:

يتعين أن تتجه إرادة الجاني في هذه الجريمة إلى نقل صورة الشخص في مكان خاص، وإثبات هذا القصد يسهل التدليل عليه.

ولا عبرة بالبواعث في توافر القصد الجنائي، فيستوي أن يكون الباعث في ارتكابها الرغبة في إيذاء المجني عليه، أو في الحصول على فائدة، أو حتى مجرد الفضول.

وعلى أية حال فإننا مع الرأي(٧٦) القائل بأن القصد الجنائي في هذه الجريمة هو قصد عام وليس مطلوباً فيه القصد الخاص، كما يرى البعض.

---

(٧٥) د. محمد الشهاوي، الاعتداء على الحياة الخاصة بواسطة القنوات الفضائية ووسائل الإعلام والاتصال، دار النهضة العربية، القاهرة، ط١، ٢٠١٥، ص ١٠١.

(٧٦) د محمد الشهاوي، مرجع سبق ذكره، ص ١٠٢..

الغصن الثالث: العقوبة:

تضمن قانون الجزاء العماني عقوبتين لجريمة نقل الصورة الأولى للموظف العام حيث نصت المادة (٣٣٠) من قانون الجزاء العماني على عقوبة نشر الصور التي تمس حرمة الحياة الخاصة حيث نصت على " يعاقب بالسجن مدة لا تقل عن شهر، ولا تزيد على سنة كل من نشر أخبارا، أو صورا، أو تعليقات، تسيء إلى الحياة الخاصة أو العائلية للأفراد، ولو كانت صحيحة إذا كان ذلك بدون رضا ذوي الشأن" .

والثانية للأفراد العاديين حيث نصت المادة (٣٣٢) على أنه " يعاقب بالسجن مدة لا تقل عن (١٠) عشرة أيام، ولا تزيد على (٣) ثلاثة أشهر " .

وتشدد هذه العقوبة على الموظف العام الذي نقل الصور اعتماداً على سلطته ووظيفته ، وبالإضافة إلى هذه العقوبة الأصلية، يحكم بعقوبة تكميلية وجوبية، وهي مصادرة الأجهزة وغيرها مما يكون قد استخدمت في الجريمة ومحو التسجيلات المتحصلة عنها أو إعدامها.

الفرع الثالث

جريمة التهديد بالإفشاء(٧٧):

إن المشرع قد أورد هذه الجريمة في المادة (٣٣١) من قانون الجزاء العماني، والتي جاء نصها كالآتي " يعاقب بالسجن مدة لا تقل عن شهر، ولا تزيد على سنة كل من علم بحكم مهنته أو حرفته أو عمله سرا فأفشاه في غير الأحوال المصرح بها قانونا، أو استعمله لمنفعته الخاصة، أو لمنفعة شخص آخر، وذلك ما لم يأذن له صاحب الشأن.

ويتضح أن هذه الجريمة يتطلب لقيامها توافر ركنين؛ الركن المادي والركن المعنوي، وبذلك سوف نقوم بتوضيحها ونبين العقوبة المقررة لها، وذلك من خلال الغصون الآتية:

الغصن الأول: الركن المادي:

يتخذ الركن المادي صورة لهذه الجريمة، وهي التهديد بإفشاء أمر من الأمور المتحصلة عليها بإحدى الطرق المنصوص عليها في المادة (٣٣٢) من قانون الجزاء العماني، وذلك قد يكون عن طريق الوعيد بشر معين سوف يلحقه الجاني بالمجني عليه، ولم يشترط

(٧٧) د. محمد الشهاوي، مرجع سبق ذكره، ص ١٠٩.

المشرع هنا أن يكون الفعل الإجرامي اعتداءً بطريقة علنية أو بوسيلة معينة، وبالتالي فإن الجريمة تتحقق إذا تم هذا النشاط بطريق الإنترنت ومن خلال استخدام البريد الإلكتروني[٧٨].

ويستوي التهديد أن يكون شفوياً أو مكتوباً، ولم يحدد المشرع العماني كيفية الحصول على مضمون هذا النشاط.

الغصن الثاني: الركن المعنوي:

إن هذه الجريمة المسماة جريمة التهديد بالإفشاء المنصوص عليها في المادة (٣٣١) من قانون الجزاء العماني، ويتخذ الركن المعنوي صورة القصد الجنائي العام والخاص معاً، وبناء على ذلك فإن القصد العام يقوم على عنصري العلم والإرادة حيث استلزم المشرع أن يكون الجاني عالماً بأن الأمر الذي يهدد المجني عليه بإفشائه قد تحصل عليه بإحدى الطرق الواردة بالمادة (٣٣٢) من القانون المذكور ، كما أوصت المادة (٣٤٦) أيضاً أن تتجه الإرادة الخاصة بالجاني إلى فعل التهديد وإلى التأثير به في إرادة المجني عليه، أما عن القصد الخاص فيتمثل في نية حمل الشخص على القيام على عمل أو الامتناع عنه، ويستوي أن يكون العمل أو الامتناع المستهدف بالتهديد مشروعاً أو غير مشروع، كما يستوي أن يكون الشخص الذي يريد الجاني حمله على العمل أو الامتناع هو صاحب الحديث أو الصورة أو المستند أو شخص آخر له عليه سلطان.

الغصن الثالث: العقوبة:

إن عقوبة التهديد بالإفشاء التي نصت عليها المادة (٣٣١) من قانون الجزاء العماني هي جنحة حيث قرر لها الشارع عقوبة السجن مدة لا تقل عن شهر ولا تزيد على سنة .

---

(٧٨) أصبح البريد الإلكتروني كوسيلة مراسلة عبر شبكة الإنترنت وسيلة للتهديد نظراً لقلة تكاليفه وسرعته بالإضافة إلى توافر قدر كبير له من الأمان من عدم تتبعه واكتشافه، ويمكن القول بأن معظم جرائم الإنشاء أو التهديد أصبحت تتم عن طريق البريد الإلكتروني، وعلى ذلك يمكن للحقوق محمل الحماية الجنائية الواردة بهذه النصوص أن يتم إنشاؤها أو التهديد بإفشائها باستخدام هذه الوسيلة التي استحدثتها المعلوماتية، وغالباً ما تدور طلبات المهدد بالإفشاء حول فدية من المال أو إقامة علاقة غير مشروعة مع الطرف الآخر، أو قيام الأخير بعمل أو الامتناع عن عمل.

ويلاحظ أن المشرع العماني لم يشدد في توقيع العقوبة في التهديد بالإفشاء لـذا يجـب على المشرع العماني تشديد العقوبة أسوة بالمشرع المصري والذي نص فـي المـادة (٣٠٩) مكرر على أنه " ويعاقب بالسجن مدة لا تزيد على خمس سنوات كل من هدد بإفشاء أمر مـن الأمور التي تم التحصل عليها بإحدى الطرق المشار إليها لحمل شخص على القيـام بعمـل أو الامتناع عنه، ويعاقب بالسجن الموظف العام الذى يرتكب أحد الأفعال المبينـة بهـذه المـادة اعتمادا على سلطة وظيفته" .

المطلب الثاني

جرائم الاعتداء على سرية مراسلات

البريد الإلكتروني في قانون تقنية المعلومات

تمهيد وتقسيم:

لقد أصدر المشرع العماني في إطار محاولته وملاحقته للتطورات العالمية الحاصلة في مجال الاتصالات قانون مكافحة جرائم تقنية المعلومات رقم ١٢ لسنة ٢٠١١.

وقد أدت ثورة الاتصالات ونقل المعلومات[٧٩] إلى ظهور أنماط جديدة من الجرائم التي تنتهك الحق في حرمة الحسابات الخاصة ، وإزاء ذلك كان للمشرع التدخل بإصداره القـانون السابق للحد من هذه الجرائم والاستعانة به وتطبيقه على جرائم البريد الإلكتروني، وعلى ذلـك سوف نقوم بتقسيم هذا المطلب إلى فرعين:

- الفرع الأول: جريمة الامتناع عمداً عن إرسال رسالة الاتصالات.
- الفرع الثاني: جريمة إفشاء معلومات خاصة بمستخدمي شبكات الاتصال أو عما يجرونه أو يتلقونه من اتصالات.

الفرع الأول

جريمة الامتناع عمداً عن إرسال رسالة الاتصالات

(٧٩) د. محمد الشهاوي، مرجع سبق ذكره، ص ٢.

تعتبر هذه الجريمة من الجرائم الواردة بقانون مكافحة جرائم تقنية المعلومات رقم ١٢ لسنة ٢٠١١، والتي تمس الحياة الخاصة، حيث نصت المادة (٤) من القانون المذكور على أنه " يعاقب بالسجن مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن ألف ريال عماني ولا تزيد على ثلاثة آلاف ريال عماني أو بإحدى هاتين العقوبتين، كل من ارتكب إحدى الجرائم المنصوص عليها في المادة (٣) من هذا القانون أثناء أو بمناسبة تأدية عمله" . ومن هذه الجريمة التي تختص بفعل الامتناع عمداً عن إرسال رسالة اتصالات[٨٠] حيث إن البريد الإلكتروني يعد الوسيلة الأكثر شيوعاً في استخدامها من الأشخاص في مواجهة مورد منافذ الدخول إلى الإنترنت، وأن مبدأ سرية البريد الإلكتروني يحتج في مواجهة موردي منافذ الدخول على الإنترنت من حيث الامتناع عن إرسال هذه الرسالة أياً كانت.

وتعتبر هذه الجريمة جنحة في القانون العماني وتدخل ضمن الجرائم السلبية[٨١]، وهي تعبر عن جرائم الحظر فيكفي تحقق ركنها المادي بتوافر النشاط الإجرامي المتمثل في الامتناع، وسوف ندرس في هذا الفرع الركن المادي (الغصن الأول)، والركن المعنوي (الغصن الثاني)، ثم نتناول العقوبة المقررة لهذه الجريمة الغصن الثالث).

الغصن الأول: الركن المادي:

لما كانت جنحة الامتناع العمدي عن إرسال رسالة اتصالات تدخل في طائفة جرائم الخطر والتي يتكون ركنها هذا من فعل إجرامي فقط، والمتمثل في سلوك سلبي قوامه امتناع أحد العاملين في مجال الاتصال عمداً عن إرسال الرسالة المرسلة من المرسل إلى المرسل إليه [٨٢].

---

(٨٠) جاءت نص المادة (٣) من قانون مكافحة جرائم تقنية المعلومات رقم ١٢ لسنة ٢٠١١ على أن "... يعاقب بالسجن مدة لا تقل عن ستة أشهر ولا تزيد على سنة وغرامة لا تقل عن خمسمائة ريال عماني ولا تزيد على ألف ريال عماني أو بإحدى هاتين العقوبتين ، فإذا كانت البيانات أو المعلومات المنصوص عليها في الفقرة الثانية شخصية تكون العقوبة السجن مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات وغرامة لا تقل عن ألف ريال عماني ولا تزيد على ثلاثة آلاف ريال عماني أو بإحدى هاتين العقوبتين.

(٨١) د. محمد الشهاوي، مرجع سبق ذكره، ص٣٠٨.

(٨٢) د. محمد الشهاوي، مرجع سبق ذكره، ص٣٠٨.

ويتعين أن يكون أحد العاملين قد ارتكب هذه الجريمة في مجال الاتصالات، وذلك بأن يكون ذلك أثناء تأديته لعمله أو بسبب وظيفته، وبذلك لا قيام لهذه الجريمة إذا كان من ارتكبها شخص لا يعمل في مجال الاتصالات، حيث إن المشرع أوجب توافر هذا الشرط، وذلك مستفاد من نص التجريم الذي أوردته نص المادة (٤) من قانون مكافحة جرائم تقنية المعلومات .

ولما كان الموظف مناطاً إليه مهمة إرسال الرسالة الخاصة بالمشتركين حال تكليفهم إياه، فيوجب على الشركة أو مورد الخدمة أن يقدم ويقوم بالمهام المناط إليه وظيفته، وهي تقديم الخدمات أي إرسال الرسالة في هذه الحالة بأسرع وأحسن كفاءة وأقل سعر، وبالتالي فإذا لم يقم بذلك عمداً أي "النشاط السلبي"، فهو بذلك تقاعس عن أداء وظيفته المكلف بها ويعتبر هذا النشاط السلبي مؤتماً يستحق العقاب المقرر قانوناً.

الغصن الثاني: الركن المعنوي:

يتخذ الركن المعنوي لهذه الجنحة صورة القصد الجنائي العام الذي يتكون من عنصرين ألا وهما العلم والإرادة، حيث إن الجاني لابد وأن يعلم أنه بعدم إرسال الرسالة من المرسل إلى المرسل إليه قد اقترف ذلك "امتنع" عمداً رغم تكليفه بذلك، فإذا جهل بذلك فلا قيام للجريمة، وعلى ذلك إذا لم يرسل الموظف الرسالة أي امتنع عن إرسال رسالة الاتصالات اعتقاداً منه في أن المرسل قد تراجع عن إرسال الرسالة الخاصة به فلا قيام للجريمة حين ذاك[٨٣].

وعلى ذلك فإن توافر عنصر العلم بمفرده لا يكفي فيجب أن تتجه إرادة الجاني "الموظف" إلى الامتناع العمدي "السلوك الإجرامي السلبي" عن إرسال رسالة اتصالات مع علمه بذلك، أي أن من واجبات وظيفته المناطة إليه تلزمه بالإرسال إلا أنه لم يقم عمداً بذلك.

الغصن الثالث: العقوبة:

نصت المادة (٤) من القانون المذكور على أنه " يعاقب بالسجن مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن ألف ريال عماني ولا تزيد على ثلاثة آلاف

---

(٨٣) د. محمد الشهاوي، مرجع سبق ذكره، ص ٣٠٩.

ريال عماني أو بإحدى هاتين العقوبتين ، كل من ارتكب إحدى الجرائم المنصوص عليها في المادة (٣) من هذا القانون أثناء أو بمناسبة تأدية عمله".

الفرع الثاني

جريمة إفشاء معلومات خاصة بمستخدمي شبكة الاتصال

أصدر المشرع العماني كما أشرنا في السابق قانون مكافحة جرائم تقنية المعلومات وعاقب المشرع في المادة (٤) كل من قام أثناء تأدية وظيفته في مجال الاتصالات أو بسببها بإفشاء أو تدمير أية معلومات خاصة بمستخدمي شبكات الاتصال، أو عما يجرونه أو يتلقونه وذلك بدون وجه حق.

ويتسم موضوع الحفاظ على سرية المعلومات بأهمية بالغة، وقد أهتم المشرع العماني وجرم إفشاء الأسرار وفق نص المادة (٣٣١) [٨٤] من قانون الجزاء العماني.

ولما كانت جميع الجرائم المنصوص عليها في نص المادة (٤) لا تتحقق إلا إذا كان مقترفها أحد العاملين في مجال الاتصالات، وبالتالي تعتبر الرسائل عبر البريد الإلكتروني من وسائل الاتصالات التي تستطيع قيد هذه الوقائع بنص هذه المادة.

---

(٨٤) جاء نص المادة (٣٣١) من قانون الجزاء العماني رقم ٧ لسنة ٢٠١٨م والتي نصت على أنه " يعاقب بالسجن مدة لا تقل عن شهر، ولا تزيد على سنة كل من علم بحكم مهنته أو حرفته أو عمله سرا فأفشاه في غير الأحوال المصرح بها قانونا، أو استعمله لمنفعته الخاصة، أو لمنفعة شخص آخر، وذلك ما لم يأذن له صاحب الشأن.

المبحث الثالث

الاعتداء الالكتروني على سلامة البيانات الشخصية

تمهيد وتقسيم:

تعتبر الحسابات الخاصة من الخدمات المهمة التي تقدمها شبكة الإنترنت التي تحتوى على بيانات شخصية، وهو شكل من أشكال الاتصال الإلكتروني الذي يسمح لمستخدمي الإنترنت بتبادل الرسائل بشكل فوري، ونظراً لصعوبة إيجاد رقابة محكمة على هذه الشبكة فإنه لا يوجد ضوابط تحكم هذا الحسابات الشخصية، الأمر الذي ينتج عنه استخدامات غير مشروعة لهذه الحسابات، وحيث تقع الجرائم باستخدام[٨٥] الحسابات، وقد تقع الجرائم على البريد الإلكتروني مثل جريمة تضخيم البريد الإلكتروني، أو حرمة الدخول غير المصرح به في البريد الإلكتروني، وعلى ذلك سوف نقسم هذا المبحث إلى مطلبين:

- المطلب الأول: جريمة إغراق البريد الإلكتروني.
- المطلب الثاني: جريمة الدخول أو البقاء غير المصرح في البريد الإلكتروني.

المطلب الأول

جريمة إغراق البريد الإلكتروني

إن خدمة البريد الإلكتروني هي إحدى الخدمات التي تقدمها الشبكة الدولية للمعلومات "الشبكة العنكبوتية"، فهي وسيلة تساعد على تبادل المعلومات وتبادل الملفات بين الأفراد عبر الشبكة الدولية باستخدام تقنيات وبرمجيات خاصة تسمى بروتوكول البريد الإلكتروني والتي تتيح إرسال رسائل مكتوبة أو صور ومقاطع فيديو كملحقات للبريد الإلكتروني.

وبالرغم من أهمية هذه الوسيلة إلا أنها قد تكون سبباً للعدوان على البريد الإلكتروني، وذلك يتمثل من خلال إرسال مئات الرسائل إلى البريد الإلكتروني الشخص ما بقصد الإضرار

---

(٨٥) الجرائم التي تستخدم البريد الإلكتروني كوسيلة على سبيل المثال تهديد الغير، أو إرسال رسائل تنطوي على عبارات سب وتخويف وترويع.

به، حيث يؤدي ذلك إلى إحداث خلل في السعة التخزينية للموقع وعدم قدرته على استقبال أية رسائل، وهذا ما يسمى بتضخيم البريد الإلكتروني، فتلك الرسائل قد تكون محملة بملفات كبيرة الحجم الغاية منها الإضرار بمستخدم البريد الإلكتروني نظراً لصغر مساحته، حيث تصل إلى الجهاز مرة واحدة وفي وقت واحد تقريباً فتؤدي إلى توقفه عن العمل فوراً (٨٦).

ويعرف مصطلح تضخيم البريد الإلكتروني بأنه "تراسل نسخ مكررة بعدد كبير من نفس الرسالة عبر النظام التراسلي لبريد إلكتروني بما يترتب عليه عدم انتظام سير النظام التقني للمعلومات(٨٧).

وقد أوردته المادة الثالثة من اتفاقية بودابست(٨٨) لسنة ٢٠٠١ فيما يتعلق بالاعتراض غير القانوني(٨٩) حيث تفرد المذكرة التفسيرية أن هدف هذه المادة هو حماية الحق في نقل البيانات، وأن هذه الجريمة تمثل انتهاكاً للحق في احترام المراسلات وهو مكفول عن طريق المادة الثامنة من الاتفاقية الأوروبية لحقوق الإنسان، وقد بينت هذه المادة أن الاعتراض غير القانوني ينطبق على وسائل النقل غير العلنية لبيانات الحاسب ويلاحظ أن مصطلح غير العلنية "non publiques" صفة تتبع طبيعة وسيلة النقل أو الاتصال وليس طبيعة البيانات المرسلة، فالبيانات المرسلة يمكن أن تكون مهيأة لكن الأطراف يرغبون في الاتصال بطريقة سرية de fagon confidentielle، على ذلك فإن مصطلح غير العلنية لا يستبعد الاتصالات في حد ذاتها عبر الشبكات العامة، فاتصالات العاملين les communications des salaries سواء

---

(٨٦) د. علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسوب، دار الجامعة الجديدة، الإسكندرية، ١٩٧٧، ص ٧٧.

(٨٧) د. خالد ممدوح إبراهيم، التقاضي الإلكتروني، دار الفكر الجامعي، الإسكندرية، ٢٠٠٧، ص ٣٧٢.

(88) V. KAISER, « La protection des mineurs Stir Internet: la problematique de la pedopornographie et les contenus juges prejudiciables », 2010, p. 15 disponible sur le site: http://www.fundp.ac.be/droit/dtic/publications.html

(٨٩) وقد جاء نص المادة الثالثة من اتفاقية بوادبست الموقعة في ٢٣ نوفمبر ٢٠٠١ بقولها: (وسوف نوردها باللغة الفرنسية).

Article 3- Interception illegal:
Chaque Partie adopte les mesures législatives et autres qui se révelent nécessaires pour triger en infraction penale, conformement a son droit interne l'interception international et sans droit, effectuée par des moyens techniques, de données informatiques , lors de transmissions non publiques, a destination, en provenance ou a l'intérieur d'un Systeme informatique transportant de tells données informatiques. Une partie peut exiger que l'infraction soit commise dans une intention delictueuse ou soit en relation avec un systeme informatique connected un autre systeme informatique

لأغراض العميل أم لا والتي تشمل وسائل النقل غير العلنية لبيانات الحاسب هي أيضاً محمية ضد الاعتراض بموجب المادة التاسعة[٩٠] من الاتفاقية، وبالتالي فإن البند الثالث والذي مفاده النشر أو النقل لمادة إباحية عبر نظام معلوماتي، وهذا قد يتم عن طريق استخدام البريد الإلكتروني كوسيلة للنقل أو النشر.

وعلى ذلك تتم جريمة تضخم البريد الإلكتروني عن طريق وصول عدد ضخم من رسائل مجهولة المصدر إلى حساب البريد الإلكتروني للمستلم النهائي، ويستخدم في إرسالها برامج معدة خصيصاً لذلك، وهي برامج محظورة لكونها تهدد قواعد البيانات بتضخيم قاعدة عمل البريد الإلكتروني، مما قد يسبب خسائر اقتصادية ضخمة، خاصة بالنسبة للشركات والمؤسسات العاملة في مجال التجارة الإلكترونية، أو أي مجال يستخدم البريد الإلكتروني أو على ذلك إذا ارتكبت هذه الجريمة في نطاق المحاكم أو النيابات إذا افترضنا أن المحاكم

---

(٩٠) وقد جاء نص المادة التاسعة من اتفاقية بودابست الموقعة في ٢٣ نوفمبر ٢٠٠١ بقولها: (وسوف نوردها باللغة الفرنسية):

Article 9- Infractions se rapportant a la pornographie enfantine

1- Chaque Partie adopte les mesures législatives et autres qui se revelent nécessaires pour ériger en infraction penale, conformément a son droit interne, les comportements suivants lors qu'ils sont commis intentionnellement et sans droit:
   a. la production de pornographie enfantine en vue de sa diffusion par le biais d'un Systeme informatique;
   b. l'offre ou la mise a disposition de pornographie enfantine par le biais d'un Systeme informatique;
   c. la diffusion ou la transmission de pornographie enfantine par le biais d'un Systeme informatique;
   d. le fait de se procurer ou de procurer a autrui de la pornographie enfantine par le biais d'un Systeme informatique;
   e. la possession de pornographie enfantine dans un systeme informatique ou un moyen de stockage de données informatiques.
2- Aux fins du paragraphel ci-dessus, le terme (pornographie enfantine comprend toute matiere pornographique representant de maniere visuelle:
   a. un mineur se livrant a un comportement sexuellement explicite;
   b. une personne qui apparat comme un mineur se livrant a un comportement sexuellement explicite;
   c. des images realistes representant un mineur se livrant a un comportement
   d. sexuellement explicite.
3- Aux fins du paragraphe 2 ci-dessus, le terme mineur designe toute personne agée de moins de 18 ans. Une Partie peut toute fois exiger une limite d'age interieure, qui doit etre au minimum de 16 ans.
4- Une Partie peut se reserver le droit de ne pas appliquer, en tout ou en partic, les paragraphes 1, alintas d. cte, et 2, alinas b. etc.

والنيابات جل عملها يستخدم البريد الإلكتروني مثل استقبال صحف الدعاوى أو أية مستندات أخرى، الأمر الذي سيؤدي إلى حالة ارتباك شديدة في حساب المواعيد القانونية لإقامة الدعاوى، إذا أثبت الشخص مرسل المستندات القضائية أن عملية الإرسال تمت في المواعيد المقررة قانوناً ولم تتم عملية الاستلام بسبب خارج عن إرادته وهو امتلاء صندوق بريد قلم كتاب المحكمة المختصة بمثل هذا النوع من الرسائل.

ويفترض لدى الشخص مرتكب جريمة تضخم البريد الإلكتروني أن يقوم بفتح حساب عبر الإنترنت لدى أحد مواقع الويب التي تقدم هذه الخدمة عبر الإنترنت، وعادة يتم إرسال رسائل التضخم عبر الحصول على عناوين البريد الإلكتروني من خلال شبكة الإنترنت.

وقد جرم المشرع الفرنسي هذا السلوك في المادة (٢/٤٣) من قانون العقوبات الجديد عام ١٩٩٤. عاقبت عليه بالحبس مدة لا تزيد على ٣ سنوات وغرامة لا تزيد على ثلاثمائة ألف فرنك، وكذلك جرمت بعض الولايات في أمريكا فعل تضخيم البريد الإلكتروني، وعلى سبيل المثال قانون ولاية نيفادا في يوليو ١٩٩٧ والذي تم تعديله في عام ٢٠٠١، ٢٠٠٣، حيث اشترط موافقة المجني عليه على قبول مثل هذه الرسائل، وقد صدر في بعض الولايات الأخرى[٩١] قوانين تمنع ذلك.

أما قانون الجزاء العماني الصادر بالمرسوم السلطاني رقم ٧ لسنة ٢٠١٨م فقد خلا من نص يمكن تطويعه بحيث ينطبق على تلك الجريمة التي الهدف منها منع الوصول إلى الخدمة المطلوبة لصعوبة استدعاء صندوق البريد الإلكتروني، الأمر الذي لا يقف المشرع عند صدور تشريع جديد يجرم ذلك النوع، بل يجب استخدام منهج دفاع تكنولوجي يكون بمثابة خط صد. إلا أن قانون مكافحة جرائم تقنية المعلومات الصادر بالمرسوم السلطاني رقم ١٢ لسنة ٢٠١١ قد عاقب هذا الجرم حيث نصت المادة (١٠) من القانون المذكور على أنه " يعاقب بالسجن مدة لا تقل عن ستة أشهر ولا تزيد على سنتين وبغرامة لا تقل عن خمسمائة ريال عمانى ولا تزيد على ألفى ريال عمانى أو بإحدى هاتين العقوبتين ، كل من أعاق أو

(٩١) حيث صدر قانون في ولاية واشنطن لمكافحة تضخيم البريد الإلكتروني عام ١٩٩٨ والمعدل في مايو ١٩٩٩، وكذلك قانون ولاية أوهايو الصادر في ٢٠٠٢ والذي نص على تجريم رسائل البريد الإلكتروني مجهولة المصدر.

عطل عمدا ودون وجه حق الوصول إلى خدمات مزود الخدمة أو الدخول إلى نظام معلوماتي أو وسائل تقنية المعلومات ، وذلك باستخدام وسائل تقنية المعلومات.

المطلب الثاني

الدخول والبقاء غير المصرح به في البريد الإلكتروني

وتقع هذه الجريمة بانتهاك كلمة السر أو ما يعرف بفك التشفير أو باستخدام الكود لشخص ما أو من خلال استخدام شخص معين يسمح له بالدخول إلى البريد الإلكتروني أو القيام باعتراض المعلومة واقتحامها أو أي طريقة يتم بها الدخول دون رضا صاحب البريد الإلكتروني، فيتوصل الجاني من خلال ذلك إلى المعلومة المخزنة أياً كان المحتوى المسجلة عليه وقد أشارت المادة الثانية[٩٢] من اتفاقية بودابست عام ٢٠٠١ أن الدخول غير المصرح به بمعنى القرصنة Le piratage أو السطو Le craquage أو الدخول غير المشروع في النظام المعلوماتي L'intrusion illicite dans un systeme informatique، وذلك على أساس أن هذه الأفعال قد تؤدي إلى اتلاف L'alteration أو تدمير la destruction باهظ التكلفة في حالة إعادة البناء Reconstruction، كما أن هذا الفعل يمكن أن يترتب عليه الوصول إلى بيانات سرية مثل كلمات المرور mots d'acces وأسرار Les pirates تسمح باستخدام النظام، وقد جرمت العديد من التشريعات في كل من فرنسا وأمريكا وتونس والإمارات فعل الدخول غير المصرح به فالجريمة ترتكب بمجرد الدخول للبريد أو الخروج منه بعد ذلك، أما إذا بقي الجاني في داخل البريد فإننا نكون أمام جريمة البقاء غير المشروع ضمن المنظومة الإلكترونية.

---

(٩٢) جاء نص المادة الثانية من اتفاقية بودابست بقولها: (وسوف نوردها باللغة الفرنسية):

Article 2- Acces illegal:

Chaque Partie adopte les mesures législatives et autres qui se révelent nécessaires pour triger en infraction penale, conformément a son droit interne l'acces intentionnel et sans droit a tout out partie d'un systeme informatique. Une Partie peut exiger que l'infraction soit coinmise en violation des mesures de sécurité, lans l'intention d'obtenir des données informatiques ou dans une autre intention delictueuse, ou soit en relation avec un systeme informatique connected un autre Systeme informatique.

ويرى الباحث أن بقاء الجاني في البريد وعدم مغادرته له يكون هنا توافر لديه قصد البقاء في داخله مع علمه أن بقاءه غير مشروع بغض النظر عن طبيعة دخوله فعل الدخول أو البقاء لا يشكل فعلاً غير مشروع بذاته، وإنما يستمد عدم مشروعيته من كون فعل الدخول أو البقاء بدون رضا صاحب النظام أو صاحب السيطرة عليه برغم إراداته، أما العقوبات فلم تتواجد العقوبات بين التشريعات الجنائية المقارنة[٩٣]، فمنهم من جمع بين العقوبة السالبة للحرية والغرامة، ومنهم من اقتصر على العقوبة السالبة، وكذلك التشريعات العربية[٩٤].

أما قانون الجزاء العماني، فقد خلا من نصوص يمكن تطويعها بحيث تنطبق على تلك الجريمة التي يمكن أن تكيف على أنها دخول أو البقاء غير المصرح به في البريد الإلكتروني أو النظام المعلوماتي، ولكن المشرع العماني تعرض لذلك في قانون مكافحة جرائم تقنية المعلومات الصادر بالمرسوم السلطاني رقم ١٢ لسنة ٢٠١١ والذي نص في المادة (٣) على أنه " يعاقب بالسجن مدة لا تقل عن شهر ولا تزيد على ستة أشهر وبغرامة لا تقل عن مائة ريال عماني ولا تزيد على خمسمائة ريال عماني أو بإحدى هاتين العقوبتين ، كل من دخل عمدا ودون وجه حق موقعا إلكترونيا أو نظاما معلوماتيا أو وسائل تقنية المعلومات أو جزءا منها أو تجاوز الدخول المصرح به إليها أو استمر فيها بعد علمه بذلك".

---

(٩٣) نجد أن المشرع الأمريكي قد جرم الدخول أو البقاء بدون تصريح من خلال إصداره قانون إساءة استخدام الحسابات الآلية رقم ١٨ لسنة ١٩٨٤ وفق المادة (JP/١٠٣٠) وجاءت المادة (٢٧٠١) من القانون الفيدرالي على مرتكب الجريمة بالحبس والغرامة، ونجد أن المشرع الإنجليزي الذي صدر عام ١٩٩٠ والذي جرم قانون إساءة استخدام الحاسبات الآلية هذا الفعل وعاقب عليه بالحبس بحد أقصى ستة أشهر أو بغرامة قدرها ألفا جنيه استرليني أو كليهما معاً، وفي فرنسا بعد صدور قانون العقوبات الجديد رقم ٩٢-٣٣٩ لعام ١٩٩٢ بموجب نص المادة (٣٢٣-J) والتي عاقبت مرتكبي هذه الجريمة بالحبس ثلاثة سنوات وغرامة مقدارها ٤٥٠٠٠ ألف يورو.

(٩٤) نجد أن المشرع السعودي من خلال نظام مكافحة جرائم المعلوماتية رقم ١٧ لسنة ٢٠٠٧، حيث واجه هذه الجريمة ونص في المادة (٣/٢-٣) بالحبس مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى العقوبتين. أما في دولة الإمارات المتحدة فإن قانون جرائم تقنية المعلومات رقم ٢ لعام ٢٠٠٦ في المادة الثانية تنص بالحبس مدة لا تقل عن ستة أشهر وبالغرامة أو بإحدى هاتين العقوبتين. أما في دولة الجزائر عاقب المشرع على هذه الجريمة في المادة ٣٩٤ مكرر بالحبس من ثلاثة أشهر إلى سنة وبغرامة من ٥٠٠٠٠ إلى ١٠٠٠٠٠ (د.ج). أما القانون العربي الاسترشادي لمكافحة جرائم المعلوماتية فقد واجه هذه الجريمة بنص المادة (٣) وعاقب عليها بالحبس... والغرامة... أو بإحدى هاتين العقوبتين.

الخاتمة

في نهاية هذا البحث توصلت لمجموعة من النتائج والتوصيات وهي كالتالي :

أولا: النتائج :

١- تعتبر جريمة الدخول غير المشروعة على البيانات الشخصية من الجرائم التي تعتمد في جسامتها على نوع الفعل ومدى تطوره، فجريمة الدّخول تتطوّر تبعاً للأفعال التي يقوم بها المخترق أو المخرّب، فتختلف الجريمة تبعاً لاختلاف الرُكن المادّي فيها، وتُشدّد العقوبة تبعاً لذلك.

٢- أنّ المشرّع العماني لم ينص على وسيلة محدّدة للدخول إلى النظام المعلوماتي، فقد استخدم عبارة أجهزة الحاسب الآلي وأجهزة الاتصال " في المادة (١/و) من قانون مكافحة جرائم تقنية المعلومات العماني رقم ١٢ لسنة ٢٠١١ ، ويرى الباحث بأنّ المشرّع كان موفقاً في استخدام هذه العبارة، ويعود ذلك لأنّ الوسائل التي من الممكن استخدامها للدّخول غير المشروع إلى النظم الإلكترونية لا يمكن حصرها، وإن أمكن حصرها جدلاً، فلا يمكن للتشريع أن يواكب التطور المستمر في تكنولوجيا المعلومات، التي يمكن استخدامها في عمليات الاختراق.

٣- يعتبر العبث في البيانات والمعلومات التي يحتوي عليها النّظام المعلوماتي من أخطر صور الاعتداء على البيانات والمعلومات داخل النظام المعلوماتي وهذا الأمر يُظهر أهميّة معرفة الدّافع من ارتكاب هذه الجريمة، والهدف من عمليّة العبث في النظام المعلوماتي، رغم عدم تقيّد المشرّع بالباعث أو الهدف إلا بوجود نص صريح.

ثانيا التوصيات

١- نوصى المشرع العماني بضرورة التدخل بالعقاب على مجرد الولوج إلى النظام دون وجود تدابير حمايه ، فالحماية مفروضة على النُظم الإلكترونيّة، سواء أكانت هذه النُظم قد اتُخذت تدابير للحماية أم لا، ذلك أنّ وجود حماية للنظام المعلوماتي، يُعتبرُ قرينة على القصد الجرمي وليس سبباً للإفلات من العقاب. ومن الأمثلة على النظم الإلكترونيّة المُتاحة أمام الجميع، تقارير معلومات البورصة.

٢- يرى الباحث أنّ جريمة الدّخول غير المشروع إلى النظام المعلوماتي بصورتها البسيطة، لا تتطلّب قصداً أو عمداً خاصاً، فبمجرّد توافر القصد العامّ تقوم الجريمة، ولا أهمّيّة بعد ذلك الباعث الجاني على الدّخول إلى النظام المعلوماتي، سواء أكان الفضول أو إثبات القدرة على تحدّي النظام المعلوماتي أو نيّة الإضرار بالغير، وبخاصة أن المادة (٣٣) من قانون الجزاء العماني الصادر بالمرسوم رقم ٧ لسنة ٢٠١٨م قد نصت على أنها " الركن المعنوي للجريمة هو العمد في الجرائم المقصودة، والخطأ في الجرائم غير المقصودة. ويتوفر 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 أي نتيجة أخرى مجرمة قانونا....." .

٣- نوصى بخصوص مسألة إثبات القصد الجرمي، يمكن القول وجود قرينة بوجود نظام حماية للنظام، من الأمور التي تدل على وجود قصد جرمي لدى الجاني، استنادا لنص المادّة الثانية من اتّفاقيّة بودابست لمكافحة الجريمة الإلكترونية لعام ٢٠٠١، قد نصت على حرّيّة الدول الأعضاء في اعتبار أنظمة الحماية جزءاً من الركن المادي للجريمة[١].

.

(١) زين الدين بلال، مرجع سابق، ص ٢٧٩.