جمهورية العراق

وزارة التعليم العالي والبحث العلمي

جامعة كربلاء / كلية القانون

الحماية الجزائية للمنصات الإلكترونية

(دراسة مقارنة)

رسالة مقدمة إلى مجلس كلية القانون – جامعة كربلاء

وهي جزء من متطلبات نيل شهادة الماجستير في القانون العام

كتبت بواسطة :

علي عبدالله علوان محمد

بإشراف

الدكتور خالد مجيد عبد الحميد الجبوري

أستاذ القانون الجنائي المساعد

تموز / ٢٠٢٢ م ذي الحجة / ١٤٤٣ هـ

بِسْمِ اللّهِ الرَّحْمَنِ الرَّحِيمِ

(قَالُواْ سُبْحَٰنَكَ لَا عِلْمَ لَنَآ إِلَّا مَا عَلَّمْتَنَآ إِنَّكَ أَنتَ
ٱلْعَلِيمُ ٱلْحَكِيمُ)

صدق الله العليّ العظيم

[سورة البقرة: الاية ٣٢]

إقـــرار المشرف

أشهد إن رسالة الماجستير الموسومة بـ (**الحماية الجزائية للمنصات الإلكترونية – دراسة مقارنة**) المقدمة من قبل الطالب (**علي عبدالله علوان**) إلى مجلس كلية القانون – جامعة كربلاء بوصفها جزء من متطلبات نيل درجة الماجستير في القانون العام قد جرت تحت اشرافي ورشحت للمناقشة ... مع التقدير ...

التوقيع :

الاسم : أ.م.د. خالد مجيد عبد الحميد الجبوري

الدرجة العلمية : أستاذ مساعد دكتور

الاختصاص : القانون الجنائي

جامعة كربلاء – كلية القانون

التاريخ : / / ٢٠٢٢

إقرار المقوم اللغوي

أشهد أني قرأت رسالة الماجستير الموسومة بـ (**الحماية الجزائية للمنصات الإلكترونية دراسة مقارنة**) المقدمة من الطالب (**علي عبدالله علوان**) إلى مجلس كلية القانون – جامعة كربلاء ، وقد وجدتها صالحة للمناقشة من الناحيتين اللغوية والتعبيرية ، بعد أن أخذ الطالب بالملاحظات المسجلة على متن الرسالة .

مع التقدير ....

التوقيع:

الاسم: أ. م. د. رافد ناجي وادي

الاختصاص: اللغة العربية

إقرار لجنة مناقشة ماجستير

نحن رئيس لجنة المناقشة وأعضائها نُقر أننا اطلعنا على هذه الرسالة الموسومة بـ (الحماية الجزائية للمنصات الالكترونية " دراسة مقارنة ")،و ناقشنا الطالب(علي عبد الله علوان) في محتواها، وفيما له علاقة بها، ونعتقد إنها جديرة بالقبول لنيل درجة الماجستير في القانون / فرع القانون العام وبدرجـــة ( ) .

التوقيع :

الاسم: أ.د. علي حمزة عسل

(رئيساً)

التاريخ: / / 2022

التوقيع :

الاسم: أ.م.د. منى عبد العال موسى

(عضواً)

التاريخ: / / 2022

التوقيع :

الاسم: أ.م .د. منى محمد عبد الرزاق

(عضواً)

التاريخ: / / 2022

التوقيع :

الاسم: أ.م.د. خالد مجيد عبد الحميد

(عضواً ومشرفاً)

التاريخ: / / 2022

صادق مجلس كلية القانون / جامعة كربلاء على قرار لجنة المناقشة

التوقيع:

أ.د. ضياء عبدالله عبود الجابر

عميد كلية القانون / جامعة كربلاء

التاريخ: / / 2022

الإهداء

أهدي ثمرة هذا الجهد المتواضع

إلى:

روح أمي الطاهرة راجياً من الله تعالى أن يسكنها فسيح جناته ويجعل مثواها الجنة إن شاء الله تعالى وأحقق أمنيتها بحصولي على شهادة الماجستير ومن بعدها الدكتوراه وأفرحها وهي في قبرها وفاءً مني لها.

وروح أخي الطاهرة الشهيد عبدالحسين عبدالله علوان... رحمه الله وجعل مثواه الجنة .

من تنحني هامتي له خجلاً والدي العزيز ... أطال الله في عمره وأبقاه الشمعة التي تنير دربي ما حييت .

من كان ولا يزال ظهري الذي استند إليه أخوتي وأخواتي ربي يحفظهم

من تشاركني الحياة بالسراء والضراء ... زوجتي الغالية

من أرى المستقبل في عيونهم أبنائي ... حسين وعباس

جميع أساتذتي في كلية القانون جامعة كربلاء .

كل موظفي مكتبة القانون جامعة كربلاء .

جميع الاصدقاء

الباحث

شكر وعرفان

في البداية أشكر الله تعالى واحمده على جزيل فضله ونعمة توفيقة لنا ، وأحمد الله الذي أعطانا القوة والصبر لإتمام هذا العمل العلمي المتواضع .

يقول الامام الرضا عليه السلام

" من لم يشكر المنعم من المخلوقين لم يشكر الله عز وجل " .

انطلاقاً من هذا القول فلا يسعني إلا أن أتقدم بجزيل الشكر والامتنان والعرفان والوفاء لأستاذي القدير الفاضل المشرف على رسالتي أستاذ القانون الجنائي المساعد الدكتور (خالد مجيد عبدالحميد الجبوري)؛ لتفضله بقبول الإشراف على هذه الرسالة ، إذ لم يبخل علي بإرشاداته وتوجيهاته القيمة لإثراء هذه الرسالة على الرغم من مشاغله الكثيرة إلا أنه قد شملني بعلمه الغزير وخلقه الرفيع وفضله الوفير وهمته العالية .

كما أتقدم بالشكر والتقدير إلى أساتذتي في هذه الكلية المعطاء كلية القانون جامعة كربلاء، كما لا يمكنني أن أنسى كل من مدّ لي يد العون من قريب أو بعيد في سبيل إنجاز هذه الرسالة، وأخص بالشكر أخي الأستاذ الدكتور (براء منذر كمال عبداللطيف)، الذي ساعدني بالكثير، وكما أتقدم بالشكر إلى موظفي مكتبة كلية القانون، جامعة كربلاء، ومكتبة كلية القانون، جامعة بابل، ومكتبة معهد العلمين.

الباحث

الملخص

شهد العصر الحالي تقدماً وتطوراً في مجالات متعددة ، وكان من أبرزها الثورة الإلكترونية التي أدت إلى ظهور أحدث الأنظمة الإلكترونية ومنها المنصات الإلكترونية التي استخدمت في العديد من المجالات التي تمس حياة الفرد والمجتمع بصورة عامة ، لما لها من تأثير كبير على مستوى التقدّم والتطور والثقافة العامة والمعرفة المتبادلة ، وهذ ما يزيد في ترسيخ ماهية المنصات الإلكترونية ويجعلها مواكبة للتطورات، وتتميز المنصات الإلكترونية باختصار الوقت والجهد والسرعة في إنجاز العديد من الأمور سواء بالقطاع الخاص أم العام ، وعلى الرغم من هذه المزايا للمنصات الإلكترونية فإنها ما تزال في بدايتها مما يجعلها تواجه عقبات وتحديات كثيرة ولا سيما على مستوى توفر البنى التحتية لها ، مما يجعلها تتعرض للكثير من الجرائم الإلكترونية منها، جريمة الدخول للمنصات الإلكترونية دون ترخيص وجريمة إتلاف معلومات المنصات الإلكترونية و جريمة سرقة معلومات المنصات الإلكترونية وجريمة الاحتيال للمنصات الإلكترونية ، لذلك عمدت الدول على سن القوانين والاتفاقيات التي من شأنها توفير الحماية للمنصات الإلكترونية ، اما بتشريع قوانين خاصة تجرّم الأفعال التي تندرج ضمن الجرائم الإلكترونية مثل الولايات المتحدة الأمريكية وأما بتعديل قوانينها مثل فرنسا اما على مستوى الدول العربية فتعد الإمارات العربية المتحدة من أولى الدول التي قامت بسن قانون يجرّم هذه الأفعال الإجرامية وكذلك الاردن، اما العراق لم يجرّم الأفعال ضمن الجرائم الإلكترونية لا في قوانينه العقابية ولا في قانون خاص سوى مشروع قانون الجرائم الإلكترونية لعام ٢٠١١الذي لم يرَ النور إلى الان ، وعليه أصبح من الضروري التصويت على القانون المشار إليه أعلاه لمكافحة أغلب الجرائم الإلكترونية التي من الممكن أن يتعرّض لها الفرد أو المجتمع سواء بالقطاع العام أم الخاص ، كذلك من أجل مواكبة التطور الحاصل في التكنولوجيا الحديثة .

قائمة المحتويات

الموضوع	الصفحة
المقدمة	5-1
المبحث التمهيدي: ماهية المنصات الالكترونية	31-6
المطلب الاول: تعريف المنصات الإلكترونية وأنواعها	19-7
الفرع الاول: تعريف المنصات الإلكترونية	12-8
الفرع الثاني: انواع المنصات الإلكترونية	19-12
المطلب الثاني : ذاتية المنصات الإلكترونية	31-19
الفرع الاول: خصائص المنصات الإلكترونية وأدواتها	26-19
الفرع الثاني: تمييز المنصات الإلكترونية عن غيرها	31-26
الفصل الأول: الجرائم المتعلقة بنظم المعالجة الألية للمنصات الإلكترونية	70-32
المبحث الاول: جريمة الدخول للمنصات الإلكترونية دون ترخيص	51-33
المطلب الاول: موقف الاتفاقيات و التشريعات المقارنة من جريمة الدخول للمنصات الإلكترونية دون ترخيص	43-34
الفرع الاول: موقف الاتفاقيات والدولية والإقليمية من جريمة الدخول للمنصات الإلكترونية دون ترخيص	37-35
الفرع الثاني: موقف التشريعات المقارنة من جريمة الدخول للمنصات الإلكترونية دون ترخيص	43-37
المطلب الثاني: أركان جريمة الدخول للمنصات الإلكترونية دون ترخيص	51-43
الفرع الاول: الركن المادي في جريمة الدخول للمنصات الإلكترونية دون ترخيص	48-44
الفرع الثاني: الركن المعنوي في جريمة الدخول للمنصات الإلكترونية دون ترخيص	51-48
المبحث الثاني: جريمة إتلاف معلومات المنصات الإلكترونية	70-51
المطلب الاول: موقف التشريعات المقارنة من جريمة إتلاف معلومات المنصات الإلكترونية	63-53
الفرع الاول: موقف التشريعات الاجنبية المقارنة من جريمة إتلاف معلومات المنصات الإلكترونية	58-53
الفرع الثاني: موقف التشريعات والاتفاقيات المقارنة من جريمة إتلاف معلومات المنصات الإلكترونية	63-58
المطلب الثاني: أركان جريمة إتلاف معلومات المنصات الإلكترونية	70-63

الفرع الأول: الركن المادي في جريمة إتلاف معلومات المنصات الإلكترونية	67-64
الفرع الثاني : الركن المعنوي في جريمة إتلاف معلومات المنصات الإلكترونية	70-67
الفصل الثاني: الحماية الجزائية من جرائم الاعتداء على المنصات الإلكترونية	117-71
المبحث الاول: الحماية الجزائية من جريمة سرقة معلومات المنصات الإلكترونية	93-72
المطلب الاول: مفهوم جريمة سرقة معلومات المنصات الإلكترونية	81-73
الفرع الاول: تعريف جريمة سرقة معلومات المنصات الإلكترونية	75-73
الفرع الثاني: جريمة سرقة معلومات المنصات الإلكترونية على المستوى الفقهي والقضائي	81-75
المطلب الثاني: أركان جريمة سرقة معلومات المنصات الإلكترونية	93-81
الفرع الاول: الركن المادي في جريمة سرقة معلومات المنصات الإلكترونية	91-82
الفرع الثاني: الركن المعنوي في جريمة سرقة معلومات المنصات الإلكترونية	93-91
المبحث الثاني: الحماية الجزائية من جريمة الاحتيال للمنصات الإلكترونية	117-93
المطلب الاول: مفهوم جريمة الاحتيال للمنصات الإلكترونية	104-94
الفرع الاول: تعريف جريمة الاحتيال للمنصات الإلكترونية	98-94
الفرع الثاني: صور الاحتيال للمنصات الإلكترونية	104-98
المطلب الثاني: أركان جريمة الاحتيال للمنصات الإلكترونية	117-104
الفرع الاول: الركن المادي في جريمة الاحتيال للمنصات الإلكترونية	112-104
الفرع الثاني: الركن المعنوي في جريمة الاحتيال للمنصات الإلكترونية	117-112
الخاتمة	123-118
المصادر	136-124
Summary	iii-ii

المقدمة

المقدمة

أولاً: موضوع الدراسة:

يشهد العالم تطوراً متسارعاً وملحوظاً في مختلف التكنولوجية الحديثة ، ومن أهم انجازاتها للإنسان هو الحاسب الآلي والانترنت والمنصات الإلكترونية ، وما يقدمه من فوائد عديدة في مجال التقدم وتذليل الكثير من عقبات الحياة التي تواجه الانسان في شتى مجالاته المتنوعة ، كما يرافقه مجموعة من الجرائم التي تؤدي إلى زعزعة أمن المجتمع ، من اشخاص يتمتعون بالخبرة والمهارة في تطويع التقنيات الحديثة للقيام بالعديد من الجرائم في العالم الافتراضي ، وهي بالأصل جرائم تقليدية معروفة ومجرّمة بنصوص عقابية لدى جميع الدول ، والفرق بين الجريمتين تحويلها من صفتها التقليدية إلى صفة لها أبعاد جديدة تعتمد كلياً على التقنيات الحديثة في تنفيذ الافعال المجرّمة ، بأساليب مبتكرة ووسائل جديدة يستخدمها الجاني لم تكن معروفة من قبل مما سهُل ذلك للجناة القيام بجرائمهم وصعوبة التعرُف عليهم والوصول إليهم ، وجرائم المنصات الإلكترونية تكون على حالتين ، قد تكون المنصات الإلكترونية الوسيلة والاداة لارتكاب الجريمة كجرائم السرقة والاحتيال الإلكترونية ، وقد تكون معلومات المنصات الإلكترونية المخزنة إلكترونياً هدفها ومحلها، كجريمة الدخول وجريمة الإتلاف الإلكتروني ، ومن أجل توفير الحماية الجزائية للمنصات الإلكترونية من الاعتداءات التي تتعرض لها بجميع أنواعها ، اتجهت أغلب التشريعات للتدخل في مكافحة هذه الجرائم أو الحد منها أما من خلال تعديل قوانينها العقابية أو بسن قوانين خاصة تجرّم الأفعال التي تندرج ضمن الجرائم الإلكترونية، كذلك أهتمت الاتفاقيات الاجنبية والعربية لمكافحة الجرائم الإلكترونية أو الحد منها قدر الإمكان.

ثانياً: أهمية الدراسة:

نظرا لما يشهده العالم من تطور في تكنولوجيا المعلومات الحديثة وظهور العديد من التطبيقات التي تستخدم فيها، تظهر أهمية الدراسة من خلال ازدياد أعداد المستخدمين للمنصات الإلكترونية سواء من قبل الافراد أم مؤسسات الدولة أم الشركات الخاصة مما يعرضها للكثير من الجرائم التي ترتكب بوساطتها وعليه سنحاول من خلال هذه الدراسة ان نتوصل إلى توفير الحماية الجزائية اللازمة للحد من الجرائم التي تتعرض لها المنصات الإلكترونية .

ثالثاً: مشكلة الدراسة:

يثير موضوع الحماية الجزائية للمنصات الإلكترونية العديد من المشاكل من أهمها قصور الحماية التشريعية ومدى قابلية وكفاية النصوص التقليدية في مكافحة الجرائم الإلكترونية التي تتعرض لها المنصات الإلكترونية ، وتثور مشكلة توفير الحماية الجزائية للمنصات الإلكترونية في حال تعرُضها لجريمة الدخول والإتلاف الإلكتروني والسرقة والاحتيال وقصور قانون العقوبات العراقي رقم ١١١لسنة ١٩٦٩النافذ في مكافحة الجرائم الإلكترونية التي تتعرض لها المنصات الإلكترونية ، خصوصاً في ظل غياب قانون خاص بالجرائم الإلكترونية في العراق على الرغم من تقديم مشروع قانون الجرائم الإلكترونية العراقي لسنة ٢٠١١ ، اما بقية دول المقارنة فقد مكافحة الجرائم الإلكترونية أما من خلال تعديل قوانينها العقابية أو بتشريع قوانين خاصة لمكافحة الجرائم الإلكترونية . كما تثور مشكلة التعرُف على الجناة خصوصاً أن موضوع المنصات الإلكترونية يعاني من قصور التشريعات القائمة في مكافحة الجرائم التي تتعرّض لها، كما هو حال المشرّع العراقي على العكس من بعض تشريعات الدول الأجنبية والعربية التي سارعت لوضع تشريعات تعاقب على الجرائم التي ترتكب بوساطة الوسائل الإلكترونية .

رابعاً: اسباب اختيار موضوع الدراسة

ولعل من أهم أسباب اختيار موضوع الدراسة هو حداثة المنصات الإلكترونية وما تتعرض لها من الجرائم إلكترونية المختلفة ، على الرغم من تطورها المستمر وتزايد خطورتها من أجل توفير الحماية الجزائية لها من خلال تشريع قوانين جديدة تتلاءم مع حداثة تلك الجرائم وتطورها لتكون قادرة على الحد منها ومكافحتها ، وسبب أخر هو مكافحة الجرائم الإلكترونية لدول المقارنة محل الدراسة وعدم التصويت على مشروع قانون الجرائم الإلكترونية لسنة ٢٠١١في العراق .

خامساً: هدف الدراسة :

تهدف الدراسة إلى وضع الاساس التشريعي الذي يمكن من خلاله توفير الحماية الجزائية للمنصات الإلكترونية ، مما تنعكس آثاره إيجابياً على تحقيق مصلحة الفرد والمجتمع من خلال اشاعة الاستقرار والامن الإلكتروني ، كما أن الآثار الإيجابية التي توفرها الحماية الجزائية ، تكون كافية لتحقيق الردع العام والخاص ، ومعالجة النقص الخاص بالتشريعات العقابية الحالية ، إذ تتضمن الدراسة العديد من المعالجات التي يمكن الاعتماد عليها كقواعد عامة والرجوع إليها

في حالة تعرّض المنصات الإلكترونية لأي من الجرائم التي ترتكب بواسطتها أو ضدها هذا من جانب ، ومن جانب آخر في حالة إذا تم تشريع قانون خاص بالجرائم الإلكترونية فلابد أن يكون القانون كفيلاً بتحقيق الحماية الجزائية ويكون مواكباً لجميع التطورات التقنية الحالية والمستقبلية، كون الجرائم الإلكترونية تمتاز بسرعتها لمواكبة التطور والاستفادة من معالجات الباحثين ومنها دراستنا الخاصة بالمنصات الإلكترونية.

سادساً: منهج الدراسة ونطاقها

فرضت حداثة الدراسة عدم وجود قواعد محددة وقائمة في بعض تشريعات الدول منهج الدراسة ، فكانت ضمن المنهج الوصفي والتحليلي والمقارن ، من وصف مفاهيم المنصات الإلكترونية واستقراء النصوص التشريعية الخاصة بالجرائم الإلكترونية التي تتعرض لها المنصات الإلكترونية في التشريعات الأجنبية والعربية ، والبحث في جزئيات المشكلة موضوع الدراسة ، مع بيان كيفية المعالجة في تلك الدول لمسألة تنظيم الحماية الجزائية للمنصات الإلكترونية ، كذلك التعرّض لمشروع قانون الجرائم الإلكترونيةِ العراقي لسنة ٢٠١١ ومن ثم القيام بتحليلها والوقوف على مضامينها مع بيان أوجه قصورها والمعالجات القانونية لذلك والبحث في فعالية الحماية المقررة لها ، وبذلك قمنا بمقارنة التشريعات المختلفة محل الدراسة وهي كل من القوانين الامريكي والفرنسي والاماراتي والاردني والعراقي وتحديد القصور التشريعي بينها .

سابعا: خطة الدراسة

من أجل معالجة الإشكاليات التي تم طرحها ولاستكمال الاجراءات المنهجية المتبعة في هذه الدراسة ، ولان الموضوع يترك آثاره على الحياة الاجتماعية والاقتصادية والأمنية للافراد ، عليه تناولنا موضوع (الحماية الجزائية للمنصات الإلكترونية – دراسة مقارنة-) الذي قسمناه على مبحث تمهيدي وفصلين تسبقها مقدمة وتعقبها خاتمة ببيان أبرز ما توصلنا إليه من استنتاجات ومقترحات ، تطرقنا في المبحث التمهيدي ماهية المنصات الإلكترونية وقسمنا ذلك على مطلبين ، تناولنا في المطلب الاول تعريف المنصات الإلكترونية وأنواعها وفي المطلب الثاني ذاتية المنصات الإلكترونية ، ثم بعد ذلك تطرقنا في الفصل الاول الجرائم المتعلقة بنظم المعالجة الآلية للمنصات الإلكترونية وقسمناه على مبحثين تطرقنا في المبحث الاول إلى جريمة الدخول للمنصات الإلكترونية دون ترخيص وفي المبحث الثاني تناولنا جريمة إتلاف معلومات المنصات الإلكترونية ثم بعدها تناولنا في الفصل الثاني الحماية الجزائية من جرائم الاعتداء على المنصات الإلكترونية وقسمنا ذلك على مبحثين ، تناولنا في المبحث الاول الحماية الجزائية

من جريمة سرقة معلومات المنصات الإلكترونية ، اما المبحث الثاني فخصصنا للحماية الجزائية من جريمة الاحتيال للمنصات الإلكترونية ، لنختم دراستنا بخاتمة أوجزنا فيها ما توصلنا إليه من استنتاجات ومقترحات .

المبحث التمهيدي

ماهية المنصات الإلكترونية

المبحث التمهيدي

ماهية المنصات الإلكترونية

يشهد العصر الحديث تطورًا وتقدّماً سريعاً في التكنولوجية الحديثة التي فرضت وجودها بمختلف مجالات الحياة المتعددة ، منها التجاري والرقمي والمالي وفي مجال التربية والتعليم إذ أدى التقدّم التكنولوجي إلى ظهور أساليب وطرق حديثة وجديدة تعتمد على توظيف المستحدثات التكنولوجية الحديثة لتحقق التقدم ، تتمثل بقدرات الحاسب الآلي الذي أحدث تغيرًا جذريًا شمل جميع مجالات الحياة وخصوصًا مجالات الاتصالات والمعلومات والتجارة والتعلم ، كما أظهر لنا تطبيقات حديثة وفعالة تمثلت في المنصات الإلكترونية التي امتازت بإمكانية التحكم بالمعلومات ومعالجتها إلكترونياً والتغييرات التي يستهدفها العالم ودخول عصر المنصات الإلكترونية وثورة الاتصالات الإلكترونية وتطور برامج المؤسسات الحكومية والمدنية ومراكز التجارة الرقمية التي واكبت تلك التغييرات، والمنصات الإلكترونية تعد من الأنظمة الإلكترونية الحديثة في مجالات التعليم والتجارة وغيرها إذ يمكن القول أنها تمثل نموذجاً جديداً يسعى إلى تغيير النظام التقليدي بالكامل في المؤسسات العامة والخاصة وتحويلها الى نمط ٱلإلكتروني ،

كما تُعد المنصات الإلكترونية بيئة تفاعلية متكاملة تعمل على تقديم الخدمات عبر شبكة الانترنت ويتم تثبيتها على الحاسب الآلي أو أي جهاز إلكتروني آخر ، وللبحث في ماهية المنصات الإلكترونية لابد من تعريفها وبيان انواعها ليكون معناها واضحا، ومن ثم بيان ذاتيتها ، وعليه قُسَم هذا المبحث على مطلبين خصص المطلب الاول للبحث في تعريف المنصات الإلكترونية وأنواعها ، وفي المطلب الثاني ذاتية المنصات الالكترونية.

المطلب الاول

تعريف المنصات الإلكترونية وأنواعها

لبيان معنى المنصات الالكترونية سنقسم هذا المطلب على فرعين نخصص الفرع الاول منه لبيان تعريف المنصات الإلكترونية ، وفي الفرع الثاني نبين أنواع المنصات الإلكترونية .

الفرع الاول

تعريف المنصات الإلكترونية

للمنصات الإلكترونية أهمية كبيرة في مجالات الحياة المختلفة ، كما تعد المنصات الإلكترونية الوسيلة الحديثة في مواكبة تطورات التكنولوجيا ، لأنها توظف التقنيات الحديثة للإنترنت ويتم بواسطتها التفاعل بين المستخدمين ، كذلك جميع ما تحتويه من نشاطات تمكنها من استخدام مجموعة أدوات التواصل والاتصال .

أولاً: تعريف المنصات الإلكترونية لغةً

من خلال معنى كلمة منصة موضوع الدراسة نجد أنَ الأصل اللغوي لكلمة المنصة :بكسر الميم وفتح النون وتشديد الصاد : الثياب المرفعة والفرش الموطأة . مأخوذ من الفعل : نصَ ، من قولهم : نصصت المتاع إذا جعلت بعضه على بعض ، وكل شيء أظهرته فقد نصصته[١] ،وتأتي بمعنى (نص) الشيء رفعه وبابه رد ومنه (منصة) العروس بكسر الميم و (نص) الحديث الى فلان رفعهُ اليه ، و(نص) كل شيء منتهاه ، وفي حديث للأمام علي عليه السلام عنه "إذا بلغ النساء نص الحقاق " يعني منتهى بلوغ العقل[٢].

أيضًا تأتي منصة بمعنى كرسي مرتفع أو سرير يعد للخطيب ليخطب ، أو للعروس لتجلى ، وقد يزين بثياب وفرش ، ويقال وضع فلان على المنصة : افتضح وشهر ، (والجمع) مناص ، والمنصوص عليه : المبين المعين[٣].

وتأتي المنصة بمعنى أيضًا ، وكما أطلقها مجمع دار العلوم على الأستراد (المكان يصعد إليه بدرج) كما يطلق على المنصة : الحجلة على المنصة ، وهي الثياب والفرش الموطأة عليها[٤] ، ومفردها منصة ، وجمعها مناص ومنصات : وتعني مرتفع من خشب يعد للخطيب أو المعلم أو نحوها[٥] ، وتأتي أيضًا بمعنى متعدد منها : منصة الشهود : منصة مغلقة في قاعة المحكمة يقف

(١) يُنظر. د. رجب عبد الجواد إبراهيم ، المعجم العربي لأسماء الملابس ، ط١ ، دار الافاق العربية ، القاهرة ، ٢٠٠٢ ، ص٤٩٣.

(٢) يُنظر. محمد بن أبي بكر بن عبدالقادر الرازي ، مختار الصحاح ، دار المعاجم ، بيروت ، ١٩٨٦ ، ص٢٧٦.

(٣) يُنظر. د. شوقي ضيف ، المعجم الوسيط ، ط٤، مكتبة الشروق الدولية ، مصر ، ٢٠٠٤ ، ص٩٢٦.

(٤) يُنظر. أحمد رضا ، معجم متن اللغة ، ج ٥ ، دار مكتبة الحياة ، بيروت ، ١٩٦٠ ، ص٤٧٣.

(٥) يُنظر. جبران مسعود ، الرائد ، ط٧، دار العلم للملايين ، بيروت ، ١٩٩٢ ، ص٧٧٤.

أو يجلس فيها الشاهد ليدلي بشهادته ، منصة القيادة : منصة أو غرفة فوق ظهر المركب منها يتم قيادة السفينة ،ومنصة ميكروسكوب : مكان وضع الشريحة في ميكروسكوب ، وتأتي بمعنى حكم وسلطة : أي سعى الى منصة الحكم[١]

يتضح لنا مما تقدم اتفاق المعاجم على معنى المنصة بأنها مكان مرتفع من الخشب يعد للخطيب وغيره ، كما يتضح لنا أيضًا ان المنصة تحمل أكثر من معنى والباحث يرى أن المنصة لغة تعرف بأنها : المكان المرتفع الذي تتم القيادة منه .

واما في اللغة الانكليزية فيطلق على المنصة (Stage) و (Platform)[٢] ، وفي اللغة الفرنسية يطلق عليها .Plate-forme,tribune,estrade,rostre كذلك تأتي بمعنى منصة الخطابة ، او المنبر Pupitre [٣] وباللغة الايطالية يطلق عليها Podio [٤]

واما معنى مفردة حماية في اللغة : ١- مص. حمَى ٢- حفظ ، صيانة. ٣- (حماية التجارة) في الاقتصاد . مذهب اقتصادي يرمي إلى حماية البضائع الوطنية بتقييد عمليات الاستيراد وبفرض الرسوم الجمركية المرتفعة على السلع الاجنبية[٥].

واما معنى جزائية في اللغة : جزائية [مفرد]: "أسم مؤنث منسوب إلى جزاء :"عقوبة جزائية" ، إجراءات جزائية : مجموعة القواعد القانونية التي تتصل بالتحقيق في الجرائم واقامة الدعوى وتنفيذ الاحكام على المتهمين ، محكمة جزائية : محكمة الجزاء ؛ نوع من المحاكم له صلاحية النظر في الجرائم والدعاوي الجنائية"[٦].

---

(١) يُنظر. أحمد مختار عمر ، معجم اللغة العربية المعاصرة ، ط١، مجلد١، عالم الكتب ، القاهرة ، ٢٠٠٨ ، ص٢٢٢١.

(2) A.FARAH: English Language , R.N.KARIM English Language , M.SAID: Arabic Language, S.K.EDUARD: Revision, The dictionary, English- Arabic,E1,Dar Al-Kotob Al-ilmiyah, Beirut, Lebanon,2004, 812.

(٣) يُنظر. فريال علوان وأخرون ، القاموس عربي – فرنسي ، ط٢ ، دار الكتب العلمية ، بيروت ، لبنان ، ٢٠٠٤ ، ص٦٩٠.

(٤) يُنظر. إيلي ضناوي ، معجم الطلاب ، عربي إيطالي ، دار الكتب العلمية ، ط٢، بيروت ، لبنان ، ٢٠٠٥ ، ص٢٠٠.

(٥) يُنظر. جبران مسعود ، مصدر سابق ، ص٣١٥.

(٦) يُنظر. أحمد مختار عمر ، مصدر سابق ، ص٣٧٣.

جزاء : "تأتي بمعنى المكافأة والثواب ، كما تتخذ معنى العقاب وحدة ، كما في قولنا :نال جزاء أعماله السيئة"(١)

واما معنى (إلكترون) : "دقيقة ذات شحنات كهربائية سالبة ، شحنتها هي الجزاء الذي لا يتجزأ من الكهربائية"(٢).

ثانيا: تعريف المنصات الالكترونية اصطلاحاً

تعد المنصات الإلكترونية من أشهر مستحدثات تكنولوجيا المعلومات الحديثة ، التي أدت إلى اهتمام الناس بها في كافة انحاء العالم عبر الانترنت ، إذ لم تنشأ جامعات أو شركات إلكترونية فحسب بل أنشئت مواقع ومنصات إلكترونية عديدة ولأغراض مختلفة في جميع مجالات الحياة المختلفة ، واشتهرت المنصات الإلكترونية عالميًا أغلبها ناطق باللغة الانكليزية ؛ وبعضها ناطق باللغة العربية ، وهناك من عرّف المنصات الإلكترونية بشكل عام ، وأخرون عرّفها بتعريفات متعددة ومن التعريفات التي عرّفت المنصات الإلكترونية بأنها (المكان أو الحيز الذي يسمح لأصحاب المصلحة المختلفة بالتجمع فيه وفق ضوابط اشتباك محددة بوضوح تسمح لهم بتبادل الأفكار والآراء والسلع والخدمات عن طريق جهاز الحاسب الآلي أو أي جهاز يعمل بالنيابة عن الانسان) (٣) ، وهناك من عرّفها بأنها (بيئة تفاعلية تهتم بتوظيف تقنيات الجيل الثاني للويب ،عن طريق برمجيات مختلفة من خلال استخدام أدوات متعددة تسهل على مستخدميها الاستفادة منها)(٤) ، وهناك من عرّفها بأنها (بيئة تعليمية تفاعلية توظف تقنية الويب وتجمع بين مميزات أنظمة إدارة المحتوى الإلكتروني وبين شبكات وتطبيقات التواصل الاجتماعي المختلفة ، وتساعد على تبادل الافكار والآراء بين المعلمين والطلاب، ومشاركة

(١) يُنظر. د. جرجس جرجس ، معجم المصطلحات الفقهية والقانونية ، ط١، الشركة العالمية للكتاب ، بيروت ، ١٩٩٦، ص١٢٦.

(٢) يُنظر. د. شوقي ضيف ، مصدر سابق ، ص٢٤.

(٣) يُنظر. فاطمة دحماني ، استخدامات الطلبة الجامعيين للمنصات التعليمية الإلكترونية موودل Moodle - والاشباعات المتحققة منها ، رسالة ماجستير ، كلية العلوم الانسانية والاجتماعية ، جامعة محمد بوضياف ، المسيلة ، ٢٠٢٠م ص١٥.

(٤) يُنظر. د. بلقيس بنت إسماعيل داغستاني ، هيفاء جار الله معيص المالكي ، دور المنصات التعليمية الإلكترونية في النمو المهني لمعلمات الطفولة المبكرة (دراسة تقويمية) ، بحث منشور في المجلة التربوية ، كلية التربية ، جامعة الملك سعود ، العدد ٧٣، ٢٠٢٠م ،ص ١١٣٣.

المحتوى العلمي، لتحقق المخرجات التعليمية ذات الجودة العالية)[١] ، وهناك من عرّفها بأنها(منصات قائمة على التكنولوجيا الحديثة للويب ، التي تسمح بالاتصال والتفاعل وتسهل عملية تبادل المعلومات والبضائع والخدمات بين الاطراف المختلفة)[٢] ، وهناك من عرّفها بأنها(منصات تعمل على توفر الحزمات المتكاملة من البرنامج أو التطبيق أو المواقع إلكترونيه التي تمكن من عمل متجر إلكتروني لتحقيق عمليات بيع المنتجات عبر الانترنت ، وتمكن العملاء من التعرّف على معلومات المنتجات المعروضة ، وامكانية البحث عن منتج معين وإدارة عملية الشراء)[٣] وهناك من عرّفها بأنها(أرضيات للتكوين عن بعد عن طريق التكنولوجيا الحديثة للويب ، ويتم عرض كل ما يتعلق بالتعليم الإلكتروني من خلالها ، حيث تشمل المقررات الإلكترونية وما تحتوي من نشطات لتحقق عملية التعلم باستخدام أدوات الاتصال والتواصل)[٤] ، وهناك من عرّفها بأنها(عبارة عن منصات تواصل شبكي تتيح لأصحاب المصالح المشتركة المستخدمين أو المستفيدين ، بالاتصال عبر شبكة الانترنت تبادل الحوار والافكار والمناقشة ، ويتم الانضمام إليها عبر إنشاء حساب على موقعها مجاناً)[٥] ، وعرّفتها اليونسكو بأنها(موارد التعليم والتعلم والبحث المتاحة من خلال أي وسيلة -رقمية أم غير رقمية -والتي تندرج في الملك العام أو تم إصدارها بموجب ترخيص مفتوح يتيح للآخرين الانتفاع المجاني بها واستخدامها وتكييفها واعادة توزيعها بدون أي قيود أو بقيود محدودة)[٦].

---

(١) يُنظر. داليه خليل عبدالكريم الشواربة ، درجة استخدام طلبة الدراسات العليا في الجامعات الأردنية الخاصة للمنصات التعليمية الإلكترونية واتجاهاتهم نحوها ، رسالة ماجستير مقدمة لمجلس كلية العلوم التربوية ،جامعة الشرق الأوسط ، الاردن ، ٢٠١٩م، ص ١٢.

(٢) يُنظر. ياسر محمد خيابا، دور المنصات الرقمية في دعم وتطوير تعليم العلوم لطلاب المرحلة المتوسطة ، بحث منشور في المجلة العربية للتربية النوعية ، العدد ٧، ٢٠١٩م، ص ١٤٨.

(٣) يُنظر. مجدي كميل ، أفضل منصات التجارة الإلكترونية لبناء متجر إلكتروني ، مقال منشور على الموقع الإلكتروني https://www.alrab7on.com/best-ecommerce-platforms أخر زيارة للموقع (٢٠٢١/٧/١٢).

(٤) يُنظر. رضوان عبد النعيم ، المنصات التعليمية المقررات التعليمية المتاحة عبر الأنترنت ، ط١، دار العلوم للنشر والتوزيع ، ٢٠١٦معرفت ، ص١١٠.

(٥) يُنظر. د. محمد أحمد المعداوي ، حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي (دراسة مقارنة)، بحث منشور في مجلة كلية الحقوق ، جامعة بنها ، ج ٤، العدد٣٣، ص١٩٣٣.

(٦) يُنظر. د. سهام بنت سلمان محمد الجريوي ، واقع استخدام الصورة الرمزية (Avatars) في تصميم مقررات المنصات التعليمية الإلكترونية المفتوحة هائلة الالتحاق (MOOCs) ، بحث منشور في مجلة كلية التربية ، جامعة عين شمس ، ج٣، العدد٤١، ٢٠١٧، ص٢٠.

يتضح مما تقدم ، إن التعريفات السابقة للمنصات الإلكترونية تتفق في مضمونها وأن اختلفت في صياغتها إذ ترى بأنها عبارة عن مكان ، أو بيئة تفاعلية ، أو حزم متكاملة ، أو أرضيات للتعلم ، أو موارد توظف تقنيات الانترنت وتجمع بين إدارة المحتوى وشبكات التواصل الاجتماعية المختلفة ، وتبادل المعلومات وتبادل الافكار والحوار ، ويتفق الباحث مع تعريف المنصات الإلكترونية بأنها عبارة عن بيئة تفاعلية تهتم بتوظيف تقنيات الجيل الثاني للويب ،عن طريق برمجيات مختلفة من خلال استخدام أدوات متعددة تسهل على مستخدميها الاستفادة منها، لأنه الاقرب لموضوع دراستنا إذ يجمع فيه جميع أدوات التواصل الإلكتروني عبر الانترنت، ويعرف الباحث المنصات الإلكترونية بأنها (عبارة عن بيئة تفاعلية تهتم بتوظيف تقنيات الانترنت وتكنولوجيا الاتصال الحديثة مع المحتوى الكائن في شبكات التواصل الاجتماعي المختلفة وتعمل على مشاركة المحتوى وعلى تبادل الحوار والمعلومات والافكار).

الفرع الثاني

انواع المنصات الإلكترونية

يوجد العديد من المنصات الإلكترونية ، الاجنبية والعربية ، ولا تقتصر المنصات الإلكترونية على نوع واحد فمنها منصات إلكترونية عامة ومتخصصة ومرخصة وتجارية ومنصات إلكترونية خاصة بالتعليم بعضها مجانية مفتوحة المصدر والبعض الاخر منصات تجارية مغلقة المصدر التي سنبينها تباعًا.

اولاً: المنصات الإلكترونية العامة

تتجلى المنصات الإلكترونية العامة بأنها تقوم بعرض المعلومات العامة من خلال روابط متعددة تمكن لمستخدمين الانترنت استخدامها ، وهذهِ المنصات الإلكترونية تعمل على تقديم خدمات الاتصال والبحث [1].

ثانياً: المنصات الإلكترونية المتخصصة :

يقصد بها المنصات الإلكترونية التي تستهدف في تعاملها فئة معينه أو محددة من المستخدمين فقط ، أي إنها عكس المنصات الإلكترونية العامة في طبيعة تعاملها

(١) يُنظر. رضوان عبد النعيم ، مصدر سابق ، ص١١٠.

والـدخول اليهـا عبـر رمـوز معينـة ولا تكـون موجهـة للجميـع ، إذ إنهـا تقـدم دورات تدريبيـة في تخصص معين ، ومنها البوابات الطبية ومنصات العمل الحرة(١).

ثالثاً: المنصات الإلكترونية المرخصة :

عبارة عن المنصات الإلكترونية عبر الأنترنت تمكن صاحب العمل من استخدامها وامكانية تطويرها وصيانة المشاكل التي تطرأ عليها من مستخدمين آخرين ، وارسال الرموز الخاصة بعد تطويرها إلى المسؤولين عنها ، وهذه الطريقة تعد من الطرق السهلة بالنسبة لأصحاب هذه المشاريع ، والاعتماد على فريق العمل والاعضاء في تطويرها ، وتمكنهم من أنشاء المتاجر الناجحة وحصولهم على صيانة وبرمجة هذه المنصات وتقديم الافكار المختلفة من قبل الاعضاء مجاناً ، من دون أن يبذل أي جهد من أصحابها(٢).

رابعاً: المنصات الالكترونية التجارية :

مجموعـة مـن الحلـول البرمجيـة التـي تمكـن مـن الحصـول علـى الخـواص والامكانيـات التقنيـة مـن أجـل عمـل المتـاجر الإلكترونيـة المتكاملـة والجـاهزة وتحقيـق عمليـات البيـع والشـراء لمسـتخدمي الانترنـت فـي جميـع أنحـاء العـالم(٣) ، ويوجـد العديـد مـن المنصـات الإلكترونيـة التجاريـة التـي تسـتطيع المسـاعدة فـي أنشـاء المواقـع التجاريـة وتمكنهـا مـن عـرض منتجاتهـا المختلفـة فـي المتـاجر الإلكترونيـة مـع مـا يتوافـق مـع مشـروعها التجـاري الـذي يـوفر الجهـد والمـال لأصـحاب هـذهِ المشـاريع ، ومـن أهـم المنصـات الإلكترونيـة وأكثرها شهرة وهي أوبن كارت و ووكومرس ومجنتو التي نتناولها تباعاً.

١- المنصة الإلكترونية التجارية أوبن كارت(OPEN CART) :

تُعدَّ من المنصات الإلكترونية التجارية مفتوحة المصدر المجانية وسهلة الاستخدام والأكثر شهرة عالميا لأنشاء المتاجر الإلكترونية وتمتاز في إمكانية تعديلها حسب الشكل الذي يريده

(١) يُنظر. د. شريف الأتربي ، التعليم بالتخيل إستراتيجية التعليم الإلكتروني وأدوات التعلم ، ط١، العربي للنشر والتوزيع ، القاهرة ، ٢٠١٩، ص٨٤.

(٢) يُنظر. فاطمة دحماني ، مصدر سابق ، ص٣٣.

(٣) يُنظر. حيدر محمد ، المنصة الإلكترونية ، مقال منشور على الموقع الإلكتروني ، https://www.zyadda.com/what-is-an-online-platform/ أخر زيارة للموقع (٢٠٢١/٧/١٤).

صاحب المتجر وهذهِ المنصات الإلكترونية مناسبة للمتاجر الصغيرة والمتوسطة[١].

٢- المنصات الإلكترونية التجارية ووكومرس (WOO COMMERCE):

تُعدَّ من المنصات الإلكترونية مفتوحة المصدر والمجانية إذ إنها في الأصل ملحق يقوم على تحويل مواقع وورد بريس إلى متاجر إلكترونية جاهزة للاستخدام ، وأيضاً لها القابلية المتقدمة للتخصيص ،لأنها الأكثر شهرة في عالم التجارة الإلكترونية ، وتتميز بتهيئتها لمحركات البحث العالمية من خلال توفر العدد الهائل لها من القوالب والتصميمات لوورد بريس واستخدامها في المتاجر الإلكترونية ، فضلاً عن أنها لا تحتاج للدفع مقابل استخدام ووكومرس ، لكنها تحتاج لاستضافة تعمل عليها حالها حال أي من منصات الإلكترونية التجارية المستقلة ، ولا تواجه أي مشكلة ممن لديهم التجربة والخبرة في استخدمها على عكس الذين ليس لديهم تجربة وخبرة في استخدامها ويمكن معالجة هذا الامر من خلال توفر الموارد الكثيرة لهذهِ المنصات الإلكترونية ، وتستطيع من إنجاز عمليات البيع بنقرة واحدة[٢].

٣- المنصات الإلكترونية التجارية الماجنتو(MEGANETO):

عبارة عن منصات إلكترونية مفتوحة المصدر تقوم بانشاء المتاجر الإلكترونية على الانترنت ، واصدرت لأول مرة عام ٢٠٠٨ ومنذ إصدارها شهدت تطوراً ملحوظا لما تمتع به من سهولة في الاستخدام التي جعل منها الاكثر شعبية في العالم ، إذ إنها تحتوي على أكثر من (٢٥٠٠٠٠) متجر في عموم العالم ، ما يمثل نسبة ٣٠% من الاجمالي لحصة السوق ، فضلاً عن كبر النظام الاقتصادي الذي تتمتع به الماجنتو فمن الطبيعي ان تختلط على المستخدمين الجدد طرق استخدام هذهِ المنصات الإلكترونية[٣] ، وفي عام ٢٠١٥ تم إصدار ماجنتو٢ الذي يعدَّ أكثر تعقيداً من سابقتها لأنها تحتاج إلى جهد لتثبيتها وخبرة فنية لاستخدامها وفهم مبدا عملها لتلافي احراج المستخدمين الجدد، على الرغم من ذلك فإن ماجنتو٢ تسمح بتطوير المتجر وتخصيصها وايجاد الملحقات التي تلبي احتياجات المستخدمين بسهولة لكن هذه الملحقات مرتفعة السعر

(١) يُنظر. عبدالله نجاوي ، مقال منشور على الموقع الإلكتروني، https://howarabic .com/2018/02/install-opencart/ أخر زيارة للموقع (٢٠٢١/٧/١٤).

(٢) يُنظر. محمد المختار ، شرح إضافة ووكومرس ، مقال منشور على الموقع الإلكتروني ، https://propassiveincome.com/woocommerce-begginer-guide/ أخر زيارة للموقع (٢٠٢١/٧/١٤).

(٣) يُنظر. حسام برهان ، مقدمة إلى نظام ماجنتو ومفهوم التجارة الإلكترونية ، مقال منشور على الموقع الإلكتروني https://academy.hsoub.com/apps/web/magento/ أخر زيارة للموقع (٢٠٢١/٧/١٥).

مقارنة بالإصدار الاول بسبب الخبرة اللازمة لأنشائها[١] ، والمنصات الإلكترونية ماجنتو تحتوي على جميع الخصائص والمميزات ومدعومة من الشركة ، وتستخدم من قبل الشركات والمتاجر الكبيرة على الرغم من أنها مدعومة لكنها تحتاج لاستئجار فريق فني خاص من المطورين لتفعيلها وبرمجة الخصائص المتقدمة فيها ، وتمتاز بكلفتها العالية إلا أنَّ أغلب المتاجر الكبيرة تتعامل بها لإعطاء أفضل خدمة تسوق للعملاء ، إما ما يتعلق بمستخدمين الماجنتو١ يتم استخدامها من قبل الافراد والتجار الصغار أو المبتدئين للتجارة لأنها سهلة ولا تحتاج إلى تحديثات صعبة على مستخدميها [٢].

خامساً: المنصات الإلكترونية الخاصة بالتعليم:

تختلف منصات التعليم الإلكتروني فمنها المنصات الإلكترونية مغلقة المصدر التجارية (المملوكة) أي تملكها شركات ربحية وتعمل على تطويرها ولا يتم استخدامها إلا بترخيص من الشركات ، أما المنصات الإلكترونية الأخرى مفتوحة المصدر المجانية التي تسمح للجميع في استخدامها.

١- المنصات الإلكترونية مغلقة المصدر (التجارية):

يطلق عليها المنصات الإلكترونية التجارية أو الانظمة التجارية التي تملكها شركات ربحية تعمل على تطويرها ولا يتم استخدامها إلا بترخيص ومن هذهِ المنصات الإلكترونية التجارية أو الانظمة التجارية ما يأتي:

أ- المنصات الإلكترونية أو النظام ويب سي تي لإدارة التعلم الإلكتروني (WebCT):

هو نظام إدارة تعلم مغلق المصدر تجاري تستخدمه آلاف من المؤسسات التعليمية التي تهتم بالتعليم الإلكتروني ويستخدم هذا النظام في أكثر من سبعين دولة ، وهذا النظام تنتجه شركة WebCT يحتوي على أربع عشرة لغة منها الإنجليزية والعربية وغيرها[٣]، ويقدّم هذا النظام الأدوات اللازمة لأنشاء بيئة تعليمية إلكترونية متكاملة تعمل بكل سهولة ومرونة من بداية إعداد

(١) يُنظر. أسامة دمراني ، الدليل الشامل لأشهر أنظمة إنشاء إدارة المتاجر الإلكترونية ، مقال منشور على الموقع https://academy.hsoub.com/entrepreneurship/ecommerce/ أخر زيارة للموقع(٢٠٢١/٧/١٥).

(٢) يُنظر. هارون بو كرش ، رحلة إلى أعلى هرم أنظمة التجارة الإلكترونية ، مقال منشور على الموقع الإلكتروني https://academy.hsoub.com/apps/web/magento/ أخر زيارة للموقع (٢٠٢١/٧/١٥).

(٣) يُنظر. فاطمة دحماني ، مصدر سابق ، ص٣١.

المقرر الإلكتروني وحتى في مدة التعلم مما يدل على سهولة استخدامها من قبل المعلم أو المتعلم فضلا عن ذلك تتم مشاركة المقرر مع الأساتذة المتخصصين لأخذ الملاحظات المهمة بطرق إلقاء وشرح المحاضرة فضلاً عن متابعة عمليات التعلم لدى المتعلمين من الطلبة وكيفية استقبال الواجبات عبر النظام والاستفسارات بشكل مباشر(١)، ويسمح النظام بإدارة المناقشات المباشرة بين المتعلم والمعلم حسب تنظيم الأستاذ وعمل سجلات يمكن الرجوع إليها وتثبت فيها المحادثات التي دارت بينهم اثناء المنتديات والمناقشات ، كل هذه العمليات تكون مدعومة بجميع أنواع الوسائط المتعددة ومنها الرسومات والصور والفيديو فضلاً عن ذلك يتم عرض للشرائح ومواقع الانترنت وغيرها ، كذلك يسمح النظام لإنشاء الاختبارات الذاتية الموضوعية أو المقالية وذلك إما بتحديد الوقت أو دون التحديد للوقت(٢).

ب- نظام المنصات الإلكترونية بلاك بورد (Block board):

تعد المنصات الإلكترونية أو نظام إدارة التعلم التجاري مغلق المصدر من إنتاج شركة بلاك بود للخدمات التعليمية الإلكترونية على الخط المباشر ومقرها في واشنطن العاصمة(٣) ، ويتميز هذا النظام بالقوة بالنسبة للأنظمة الأخرى ، إذ يقدّم هذا النظام الفرص التعليمية المتنوعة من خلال كسر كل الحواجز والعوائق التي يمكن أن تواجهها المؤسسات التعليمية والمتعلمين ، وهذا النظام يعمل على مساعدة الكثير من المؤسسات التعليمية في نشر التعليم بقوة عبر الإنترنت ، كما ويمتاز بالمرونة والقابلية للتطور والتوسع(٤).

ج- نظام المنصات الإلكترونية تدارس:

وهذه المنصات الإلكترونية أو النظام لإدارة التعلم المغلقة المصدر التجارية التي تحتوي على جميع والوظائف والتطبيقات للتعلم الإلكتروني الحديث والمتقدم ، كما أن الكثير من المعاهد والجامعات والمدارس ومراكز التدريب والشركات تحاول

---

(١) يُنظر. رضوان عبد النعيم ، مصدر سابق ص١١١.

(٢) يُنظر. د. طارق عبد الرؤوف ، التعليم الإلكتروني (اتجاهات عالمية معاصرة) ، ط١، المجموعة العربية للتدريب والنشر ، القاهرة ، مصر ، ٢٠١٤، ص١٣٢.

(٣) محمد محمد عبدالهادي بدوي ، فعالية برنامج مقترح في التعليم الإلكتروني لتنمية مهارات تصميم الإختبارات الإلكترونية والاتجاه نحو التقويم الإلكتروني لدى طلاب الدراسات العليا بحث منشور في المجلة الدولية التربوية المتخصصة ، كلية التربية بالدقهلية ، جامعة الازهر، العدد٥ ، المجلد٣، ٢٠١٤م، ص١٥٥.

(٤) يُنظر. دالية خليل عبد الكريم الشوارية، مصدر سابق ، ص٢٠.

تطبيقه أو التحول إليه في جميع مفاصلها التعليمية ، لأنها متوافقة مع معايير الجودة العالمية للتعلم الإلكتروني مثل SCORM و IMS و AIC الذي تم إنشائه باللغة العربية[١].

٢- المنصات الإلكترونية مفتوحة المصدر

وهي المنصات الإلكترونية التي لا تسمح لأي جهة ببيعها وتستخدم مجاناً ، والعديد من المتخصصين في مجال المنصات الإلكترونية يمكنهم تعديلها وتطويرها إذ توجد الكثير من هذهِ المنصات الإلكترونية لكننا نذكر اشهرها وهي على ما يأتي

أ- نظام المنصات الإلكترونية مودل(Moodle):

تعد من المنصات الإلكترونية مفتوحة المصدر مجانية الذي يمكن استخدامها من قبل الجميع ، كما يمكن نشره وتعديله وتحميله ، ويعد من أشهر المنصات الإلكترونية التي تم استخدامها في العديد من المدارس والجامعات فضلاً عن استخدامها في مراكز التدريب والمؤسسات الحكومية [٢]، ويمكن تطويره من قبل المساهمين والمطورين هذا من جانب ، وفي جانب أخر صممت تقنية المنصات الإلكترونية باستخدام لغة (PHP) وقواعد البيانات (MySQL) ،) وكثير من الجامعات الاجنبية والعربية تستخدم هذهِ المنصات الإلكترونية ومنها جامعة كوينزلاند الأسترالية وجامعة السلطان قابوس في عمان[٣].

ب-نظام المنصات الإلكترونية أتوتر(ATutor) :

تعدَّ من المنصات الإلكترونية مفتوحة المصدر، التي تم إطلاقها عام ٢٠٠٢ من قبل جامعة تورنتو المنتجة له ، إذ صمم بطريقة سهلة تمتاز في سرعة التركيب، كما أنه سهل الاستخدام بالنسبة للمدرب والمتدرب فضلاً عن إمكانية التحديث والتغير السريع للواجهات من قبل المدربين ، ويتم استخدام هذهِ المنصات الإلكترونية في المؤسسات التعليمية الصغيرة والجامعات الكبيرة التي

(١) يُنظر. د. شريف الأتربي ، مصدر سابق ، ص٦٩.

(٢) يُنظر. د. بشائر مولود توفيق ، التعليم الإلكتروني (فوائده ونظم إدارته) بحث منشور في مجلة البحوث التربوية والنفسية ، جامعة بغداد ، المجلد١٦، العدد٦٣، ٢٠١٩، ص٢٨١.

(٣) يُنظر. أبو عبيدة محمد حمودة ، إيناس جاسم هادي ، أثر استخدام منصة التعليم الإلكتروني (Moodle) على مستوى طلاب قسم المعلومات والمكتبات (دراسة تجريبية)، بحث منشور في مجلة آداب المستنصرية ، الجامعة المستنصرية ، العدد٨٧، ٢٠١٩، ص٨٦.

تعتمد على التعلم الإلكتروني عبر الإنترنت ، وتدعم هذهِ المنصات ثلاثين لغة جميعها مكتملة الترجمة ، فضلاً عن أنها تحتوي على واجهة عربية تمكنها من الاستخدام معربة بالكامل ، وهذهِ المنصات الإلكترونية متوافقة مع معايير (SCORM) و (IMS) ومن ناحية التقنية فإنها صممت باستخدام لغة (PHP) واستخدم لقواعد البيانات لغة (MySQL) [1]

ت- نظام المنصات الإلكترونية كارلين(Caroline):

تعد من المنصات الإلكترونية مفتوحة المصدر إذ إنها تستخدم من قبل ١٢٠٠ منظمة وأكثر في حوالي 65 دولة إذ تقوم بتفعيل التعاون بين المجموعات المختلفة ، وتسمح للمدرب بأنشاء المحتوى التعليمي العالي الجودة والتمارين التفاعلية وله أن يقوم بالتواصل والمتابعة لإداء المتدربين، هذهِ المنصات الإلكترونية متوافقة مع معايير(SCORM) إما من الناحية التقنية فإن تصميم هذهِ المنصات الإلكترونية (PHP) وتم استخدم لغة (MySQL) لقواعد البيانات[٢].

ث- نظام المنصات الإلكترونية دوكيز(D0keos):

وهي من المنصات الإلكترونية مفتوحة المصدر تسمح للمدربين إنشاء الاختبارات عن طريق استخدام الرسومات الثنائية والثلاثية الابعاد ،كذلك يمكنها إقامة الدورات وتتبع التقدّم الذي يتم تحقيقه من قبل الطلاب فضلاً عن إعداد التقارير وإدارة الشهادات والدردشة والرسائل ، والسماح للمدرسين بالتواصل مع طلابهم المتعلمين الذين يقمون بنشر المحتوى التعليمي بالوقت الفعلي [٣]

ومما سبق يتضح لنا أن للمنصات الإلكترونية أنواعاً عديدة منها العامة والمتخصصة والمرخصة والتجارية ولكل منها منصاتها الخاصة ، التي تم ذكر الاشهر منها فقط ، وتؤدي

---

(١) يُنظر. د. الغريب زاهر إسماعيل ، التعليم الإلكتروني من التطبيق إلى الاحتراف والجودة ، ط١، عالم الكتب ، القاهرة ، ٢٠٠٩، ص٥٥٨.

(٢) يُنظر. د. شريف الأتربي ، مصدر سابق ، ص٦٨.

(٣) يُنظر. د. نجلاء محمد فارس ، د. محمود محمد حسين ، د. علي حسن عبادي ، فاعلية منصة تعليمية قائمة على القصص التشاركية الرقمية لتنمية التنظيم التعاوني والانتماء إلى الوطن ، بحث منشور في المجلة التربوية ، كلية التربية ، جامعة سوهاج ، العدد٦٨، ٢٠١٩، ص ٥٣٢.

هذهِ المنصات مهمات واعمال في مختلف المجالات للمستخدمين ، والباحث يؤيد استخدام المنصات الإلكترونية في العديد من مجالات الحياة العلمية والعملية ، وذلك اختصاراً للوقت والجهد والتكلفة ومواكبة التطورات التقنية الحديثة للمنصات الإلكترونية .

المطلب الثاني

ذاتية المنصات الإلكترونية

شهد العالم طفرة نوعية غير مسبوقة على صعيد المنصات الإلكترونية والتي أثرت بشكل ملحوظ على مختلف ميادين الحياة ، واصبحت ضرورة حتمية إذ أنها تتمتع بخصائص مهمة تميزها عن غيرها من الأنظمة الإلكترونية لذا سنقسم هذا المطلب على فرعين نتناول في الفرع الاول خصائص المنصات الإلكترونية وأدواتها وفي الفرع الثاني نتناول تمييز المنصات الإلكترونية عن غيرها.

الفرع الاول

خصائص المنصات الإلكترونية وأدواتها

مما لا شك أن هناك الكثير من الخصائص التي تتميز بها المنصات الإلكترونية لما لها من قدر كبير فيما تقدمه من خدمات في مجالات مختلفة، تميزها عن غيرها من الأنظمة الإلكترونية الاخرى التي سنتناولها تباعاً.

اولًا: خصائص المنصات الإلكترونية :

المنصات الإلكترونية عبارة عن بيئة تفاعلية خاصة لكل أنواع النشر من معلومات أو منتجات أو تعليم وغيرها ، إذ تعمل على توظيف تقنيات الويب من إدارة المحتوى أو على شبكات التواصل الاجتماعي المختلفة ، وتقوم في المشاركة للمحتوى وتبادل المعلومات وتبادل الافكار والحوار بين المستخدمين ، وتمتاز هذه المنصات بخصائص عديدة منها .

١- قابلية المنصات الإلكترونية للتفاعل :

تعمل المنصات الإلكترونية على تفاعل المستخدمين وإعطائهم فرصة التعامل مع بعضهم وتبادل الخبرات فيما بينهم ، والتفاعلية الأسلوب الأكثر فاعلية للحصـــــول علـــى المعلومات

والخدمات ،والعنصر الأساس الذي يميزها عن غيرها من الوسائل الاخرى[١] .

٢- قابلية المنصات الإلكترونية للتواصل :

تقوم المنصات الإلكترونية على تسهيل عملية التواصل والاتصال من خلال توفر الأدوات المختلفة المدمجة والتي تمثل بنظامها عملية التواصل ، عبر وسائل عديدة منها منتديات النقاش والبريد الإلكتروني والمدونات ولوحات الإعلانات[٢].

٣- قابلية المنصات الإلكترونية للتعديل والتطوير والتحديث:

قابلية المنصات الإلكترونية للتطوير أما عن طريق الشركة المصنعة للمنصات الإلكترونية إذا كانت المنصات الإلكترونية مغلقة المصدر ويكون ذلك التطوير مقابل أجور محددة ، أو عن طريق عدد من المطورين والمستخدمين إذا كانت المنصات الإلكترونية مفتوحة المصدر ، وتقدم للمستخدمين كل ما هو حديث من البرمجة الإلكترونية الحديثة[٣].

٤- قابلية المنصات الإلكترونية على توفير الوقت والمال:

تتيح المنصات الإلكترونية البرمجة الحديثة بما يتماشى مع احتياجات المستخدمين التي تؤدي لتقليل التكاليف مقارنة بالأنظمة التقليدية ، كما وتسهل عليهم إنجاز الاعمال في مواقعهم من دون الحاجة إلى السفر الذي يحتاج إلى المال والوقت[٤]

٥- قابلية المنصات الإلكترونية على التحرر من قيود الزمان والمكان:

تسمح المنصات الإلكترونية للمستخدمين في الوصول إلى المعلومات التي يحتاجونها بسهولة ويسر متخطية بذلك جميع الحواجز الزمانية والمكانية [٥]

---

(١) يُنظر. د. نجلاء محمد فارس واخرون ، مصدر سابق ، ص٥٢٧.

(٢) يُنظر. د. منال عبد العال مبارز ، د. أحمد محمود فخري ، التعليم الإلكتروني (مفهومه – بيئاته – مقرراته – إدارته – تقويمه – تطبيقاته المتقدمة) ، ط١ ، دار الزهراء للنشر والتوزيع ، الرياض ، السعودية ، ٢٠١٣م، ص٥٨.

(٣) يُنظر. رضوان عبد النعيم مصدر سابق ، ص١٢.

(٤) يُنظر. د. نجلاء محمد فارس وأخرون، المصدر نفسه ، ص٥٢٧.

(٥) يُنظر. د. باسم بن نايف محمد الشريف ، واقع اتجاهات طلبة الجامعات نحو توظيف المنصات الرقمية في التعلم الجامعي بالمملكة العربية السعودية ، بحث منشور في مجلة جامعة طيبة للآداب والعلوم الانسانية ، العدد٢٢، ٢٠٢٠، ص٣٦٤.

٦- قابلية المنصات الإلكترونية على الملائمة :

يستطيع مستخدمو المنصات الإلكترونية التركيز في وظائفهم العملية والتعليمية ممن لم يواجهوا أي مشاكل في التواصل مع الاخرين ، وتوفر المناخ الملائم للذين لديهم مشاكل وصعوبة في التركيز وتسهل عليهم عملية استخدامها(١).

٧- قابلية المنصات الإلكترونية على الترابط :

٨- المنصات الإلكترونية تعمل على توفر جميع أدوات الاتصال المتزامنة وغير المتزامنة والتي تمكن المستفيدين من تبادل المناقشات والحوار وتبادل الافكار والمعلومات فيما بينهم(٢).

٩- قابلية المنصات الإلكترونية للتكييف :

تمتاز المنصات الإلكترونية على التنويع والتغيير للمحتوى حسب قدرة وإمكانية مستخدمين المنصات الإلكترونية(٣).

١٠-قابلية المنصات الإلكترونية للمرونة :

تمكن المنصات الإلكترونية المراجعة للمستخدمين لمعرفة ما موجود فيها حسب ظروفهم ووقت فراغهم وفي أي مكان يتواجدون فيه(٤).

١١-قابلية المنصات الإلكترونية للتنوع:

تعمل المنصات الإلكترونية على تنوع ادوات الاتصال للمستخدمين حسب ميولهم واختيار طريقة الاتصال التي يختارونها للتواصل سواء بالنص المكتوب أو بالصوت والصورة ، أو بالرسائل الإلكترونية(٥).

---

(١) يُنظر. د. كمال عبدالحميد زيتون ، تكنولوجيا التعلم في عصر المعلومات والاتصالات ، ط٢، عالم الكتب ، ٢٠٠٤، ص٤٣٢.

(٢) يُنظر. سعيد نعيم عبد الغفور ، أثر استخدام بعض الوسائل التعليمية المقترحة عبر الشبكة العالمية على التحصيل لدى طلاب الصف التاسع ، رسالة ماجستير ، كلية التربية ، جامعة الازهر ، ٢٠١٥، ص٢٢.

(٣) يُنظر. رضوان عبد النعيم ، مصدر سابق ، ص١١.

(٤) يُنظر. د. مناهل مصطفى العمري ، د. افتخار محمد مناحي الرفيعي ، د. انتصار محي الخطيب ، واقع ومتطلبات وسائل التعليم الحديثة ، بحث منشور في مجلة دنانير ، العدد٩، ٢٠١٦، ص٤٢.

(٥) يُنظر. حسين حسن موسى ، استخدام الوسائط المتعددة في البحث العلمي (التعليم الإلكتروني ودور الوسائط) ، دار الكتاب الحديث ، القاهرة ، ٢٠٠٩، ص٧٦.

١٢-قابلية المنصات الإلكترونية على إدارة المحتوى :

الأدوات المستخدمة في المنصات الإلكترونية ، التي تسهل من الوصول إلى ادارة المحتوى الإلكتروني ، سواء تم إضافتها من الشركة المصنعة أم من المستخدمين ،كما يتم اقامة الدورات وتخزينها واعادة توظيفها ، وسهولة الوصول للمحتوى عبر الإنترنت(١).

١٣- قابلية المنصات الإلكترونية على الإدارة من قبل المدربين والمتدربين :

تقوم المنصات الإلكترونية بتتبع جميع المستخدمين، من المدربين والمتدربين ، وذلك من خلال اختبارات التقييم الخاصة بالمنصات الإلكترونية ، والتي تتيح لها معرفة معلومات المستخدمين واعدادهم ، فضلاً عن معرفة اوقات حضورهم ومكان تواجدهم(٢) .

يتضح مما تقدم إن المنصات الإلكترونية تتميز بخصائص تميزها عن غيرها من المنصات الإلكترونية الاخرى والتي تسمح لجميع المستخدمين وبكافة الاعمار، حتى الذين عندهم اعاقات في سمعهم أو بصرهم أو مصابين بطيف التوحد ، فإنها تمكنهم من استخدامها بكل سهوله ويسر ، كما وتعمل على اختصار الوقت والجهد وتوفير المال لجميع المستخدمين وقابليتها للتحديث ومواكبة التطورات الحديثة .

ثانيًا : أدوات المنصات الإلكترونية

تمتاز المنصات الإلكترونية ببعض الأدوات التي يمكن استعمالها داخل منصات الإلكترونية، وتكون هذه الادوات أما متزامنة (مباشرة) تتطلب وجود طرفي الاتصال اثناء التواصل ، وأما غير متزامنة (غير مباشرة) لا تتطلب وجود طرفي الاتصال في الوقت نفسه ، ومن تلك الادوات ما يأتي :

١- ادوات المنصات الإلكترونية المتزامنة :

تسمح هذه الأدوات للمستخدم الاتصال المباشر مع المستخدمين الآخرين عبر شبكة، وهذه الأدوات ما يأتي:

---

(١) يُنظر. د. بشائر مولود توفيق ، مصدر سابق ، ص٢٨٠.

(٢) يُنظر. ضيف الله نسيمة ، استخدام تكنولوجيا المعلومات والاتصال وأثره على تحسين جودة العملية التعليمية ، إطروحة دكتوراة ، كلية العلوم والاقتصادية والتجارية وعلوم التسيير ، جامعة الحاج لخضر – باتنه ، ٢٠١٧، ص١١٣.

أ- المحادثة(Chat):

تتيح هذه الأداة إمكانية التحدث على شبكة الإنترنت مع المستخدمين الآخرين في وقت واحد، وذلك عن طريق التفاعل بين المتحدثين عبر الإنترنت من جميع انحاء العالم ، للتحدث كتابة وصوتاً وقد تضاف اليه الصورة من خلال برنامج معد لهذا الغرض[١].

ب-المؤتمرات الصوتية(Conferences Audio) :

نقصد بها التقنية الإلكترونية التي تعتمد عبر الإنترنت من خلال استخدام هاتفاً عادياً وآلية للمحادثة على الخطوط الهاتفية التي توصل المتحدث (المدربين) بعدد من المستقبلين (المستخدمين أو الزبائن) في أماكن متفرقة[٢].

ت- مؤتمرات الفيديو(Conferences Video) :

تمكن المنصات الإلكترونية بتواصل الأفراد على الرغم من بعد المسافات التي تفصل بينهم عبر شبكة الانترنت التي تمكن المستخدمين المتواجدين في مكانات متفرقة وغير محددة أن يرى بعضهم البعض، عبر مؤتمرات الفيديو وتمكنهم من خلالها بتوجيه الاسئلة والاستفسارات وإجراء الحوارات بينهم ، وتعمل هذه التقنية على نقل المؤتمرات المرئية والمسموعة بالصورة والصوت[٣].

ث- اللوح الأبيض(Board White) :

يطلق عليها اللوح الأبيض أو السبورة البيضاء وهي عبارة عن سبورة شبيهة بالسبورة التقليدية، وتُعد من الأدوات الرئيسة اللازم توافرها في الفصول الافتراضية، ويمكن من خلالها تنفيذ الشرح والرسوم التي يتم نقلها إلى شخص آخر، كما تسمح لمجموعة من الاشخاص في التفاعل فيما بينهم [٤].

---

(١) يُنظر. فاطمة دحماني ، مصدر سابق ، ص٥٤.

(٢) يُنظر. بثينة سيواني ، واقع استخدام الاستاذ لتقنيات التعليم الإلكتروني في تدريس الطلبة بالجامعة ، رسالة ماجستير ، كلية العلوم الاجتماعية والانسانية ، جامعة العربي بن مهيدي – ام البواقي ، ٢٠١٨ ، ص٣٠.

(٣) يُنظر. د. محمد رفعت حسنين ، مصدر سابق ، ص٢٤.

(٤) يُنظر. د. وليد سالم محمد الحلفاوي ، التعليم الإلكتروني تطبيقات مستحدثة ، ط١، دار الفكر العربي ، القاهرة ، ٢٠١١م، ص٣٧.

ج-برامج القمر الصناعي(Programs Satellite) :

تعمل على توظيف برامج القمر الصناعي المقترن بنظم الحاسب الآلي والمتصل بخط مباشر مع شبكة اتصالات، والذي يسهل إمكانية الاستفادة من القنوات السمعية والبصرية في عمليات التواصل عبر المنصات الإلكترونية ،وجعلها أكثر تفاعلا وحيوية، وهذه التقنية توحد لنا المحتوى في أنحاء متفرقة كثيرة ، لأن مصدرها واحد شرط أن يتم تزود جميع مراكز الاستقبال بأجهزة استقبال وبث خاصة تكون متوافقة مع النظام المستخدم(١).

٢- ادوات المنصات الإلكترونية غير المتزامنة :

للمنصات الإلكترونية ادوات تسمح للمستخدم في التواصل بشكل غير مباشر مع المستخدمين الآخرين أي أنها لا تتطلب تواجد المستخدم والمستخدمين الآخرين معاً على الشبكة أثناء التواصل، ومن أهم هذه الأدوات ما يأتي(٢).

أ- البريد الإلكتروني :(E-mail)

عبارة عن برنامج يستخدم لتبادل الرسائل والوثائق بين المستخدمين عبر شبكة الإنترنت، ويتصدر البريد الإلكتروني ادوات المنصات الإلكترونية غير المتزامنة ، لما يتمتع به من المزايا التي تتمثل بسهولة استخدامه ، والتي جعلته من أكثر الخدمات على الإنترنت استخداماً(٣)، وعلى الرغم من أن هذه الأداة لا توفر لنا التفاعل المتزامن المستمر ، بسبب الفروق الزمنية بين ارسال الرسالة واستقبالها والرد عليها ، لكن مع هذا تمتاز بسرعة تبادل الرسائل مع المستخدمين مهما تباعدت المسافات بينهم(٤) ، وإنخفاض التكلفة ، كما تمكن هذه الاداة ارسال رسالة واحدة الى العديد من المستخدمين في الوقت نفسه في أماكن متفرقة من العالم (٥).

---

(١) يُنظر. سعدية الاحمري ، التعليم الالكتروني ، ٢٠١٥، ص٣٨، رسالة ماجستير منشور على الموقع الإلكتروني: www.kutubpdfbook.com //https أخر زيارة للموقع (٢٠٢١/٥/٣).

(٢) يُنظر. د. حذيفة مازن عبدالمجيد ، د. مزهر شعبان العاني التعليم الإلكتروني التفاعلي ، ط١، مركز الكتاب الاكاديمي ، عمان ، ٢٠١٥م، ص٨٥.

(٣) يُنظر. د. وليد سالم محمد الحلفاوي ، مصدر سابق ، ص٣٧.

(٤) يُنظر: نهلا عبدالقادر المومني ، الجرائم المعلوماتية ، ط٢، دار الثقافة للنشر والتوزيع ، عمان ، ٢٠١٠، ص٣٩.

(٥) يُنظر: د. محمد رفعت حسنين ، التعليم الإلكتروني ، ط١، دار الزهور المعرفة والبركة ، مصر ، ٢٠١٧ ، ص٣٤.

ب- الشبكة العنكبوتية (Web Wide World) :

عبارة عن نظام معلومات أو دائرة معارف هائلة ممتدة عبر بلدان العالم ، التي تقوم بعرض المعلومات المختلفة على الصفحات المترابطة، وتسمح للمستخدمين بالدخول لخدمات الإنترنت المختلفة ، فضلاً عن تتعدد أشكال عرض المعلومات عبر الانترنت ، أما بعرضها على شكل صورة مكتوبة أو مصورة أو فيديو[١].

ت-القوائم البريدية(Mailing Lists) :

عبارة عن قائمة من عنوانات بريدية مضافة لدى شخص أو مؤسسة التي يتم تحويل الرسائل إليها من عنوان بريدي واحد ، ويقوم بتحويل جميع الرسائل المرسلة اليه إلى كل عنوان في القائمة ، والقوائم البريدية، كما وتعد من أشهر أدوات المنصات الإلكترونية عبر الإنترنت والتي تسمح الى مجموعة من المستخدمين لهم الاهتمامات المشتركة نفسها ، من مناقشة موضوعات تهمهم من خلال استخدام هذه القوائم[٢].

ث-منتديات النقاش(Discussion Groups) :

يقصد بها إحدى أدوات الاتصال غير التزامنية ، عبر شبكة الإنترنت ، تكون بين مجموعة من الأفراد يجمعهم موضوع مشترك في تخصيص معين تتم المشاركة عن طريقها كتابياً في موضوع معين أو الاستفسار إلى المجموعة المشاركة أو المشرف على هذه المجموعة دون الحاجة الى التواجد في وقت واحد[٣].

ج- نقل الملفات(File Exchange) :

تختص هذهِ الأداة بنقل الملفات من المنصات الإلكترونية إلى منصات إلكترونية أخرى متصلة معها عبر شبكة الانترنت أو الشبكة العنكبوتية[٤].

---

(١) يُنظر: د. علي عبود جعفر ، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الاشخاص والحكومة (دراسة مقارنة) ، ط١، مكتبة زين الحقوقية والادبية ، ٢٠١٣، ص٤٦٧.

(٢) د. أبو عبيدة محمد حمودة ، إيناس جاسم هادي ، مصدر سابق ، ص ٨٦.

(٣) حليمة الزاجي ، التعليم الإلكتروني بالجامعة الجزائرية مقومات التجسيد وعوائق التطبيق (دراسة ميدانية بجامعة سكيكدة) ، رسالة ماجستير مقدمة لمجلس كلية العلوم الإنسانية والعلوم الاجتماعية ، جامعة منتوري – قسنطينة ، الجزائر ، ٢٠١٢، ص ١٠٠.

(٤) يُنظر: رضوان عبد النعيم ، مصدر سابق ، ص ٧٧.

ح- الفيديو التفاعلي(Interactive Video) :

تتيح هذه التقنية إمكانية التفاعل بين المتدرب أو المستخدم والمادة المعروضة المشتملة على الصور المتحركة المصحوبة بالصوت وذلك لغرض جعلها أكثر تفاعلية، وهذه التقنية من وسائل الاتصال من اتجاه واحد لأنه لا يمكنه التفاعل مع المتدرب(١).

يتضح لنا مما تقدم أن المنصات الإلكترونية تسمح بالاتصال والتواصل من خلال ادواتها الخاصة بها التي تمكنها من اداء المهام التي تتم من خلالها سواء عن طريق ادواتها المباشرة أو غير المباشرة ، التي تمكن الزبائن أو المستخدمين من الاستفادة من خدمات المنصات الإلكترونية المختلفة وفي جميع المجالات.

الفرع الثاني

تمييز المنصات الإلكترونية عن غيرها

لمعرفة أهم ما يميّز المنصات الإلكترونية عن كل من الموقع الإلكتروني والمكتبات الإلكترونية ، علينا التطرق الى اهم الاختلافات بينهما :

أولا : تمييز المنصات الالكترونية عن المواقع الالكترونية

تتشابه المنصات والمواقع الإلكترونية في العديد من الخصائص والمزايا إلا أنها تختلف فيما بينها بحسب الخدمة التي أنشئت من أجلها ، إذ ظهرت العديد المنصات الإلكترونية و المواقع الإلكترونية ، مع تطور استخدام الأنشطة الإلكترونية عبر الإنترنت التي تنمو وتتطور حتى تصبح وجهة لـملايين المستخدمين يوميًا ، فضلاً عن حقيقة أن العديد من الحكومات كانت تقدم العديد من الخدمات الحكومية عبر منصاتها الإلكترونية ، ويمكن التطرق للمنصات الإلكترونية والموقع الإلكتروني ومعرفة الاختلاف بينهم من خلال الآتي :

المنصات الإلكترونية (platform)

عبارة عن مجموعة متكاملة من الخدمات التفاعلية التي تعمل على توظيف التقنيات عبر الانترنت ، وتجمع بين مواقع التواصل الاجتماعي المختلفة والمحتوى وتســـــمـح على تبادل

(١) يُنظر: منتهى عبد الكريم جاسم ، الدراسات العليا عن بعد رؤيا مستقبلية للتعليم الافتراضي في جامعة بغداد ، سلسلة ثقافية جامعية ، المجلد ٢، العدد١، ٢٠١٠، ص٦١.

المعلومات والافكار والاراء بين الزبائن [١].

الموقع الإلكتروني (website):

عبارة عن مجموعة من ملفات الشبكة العنكبوتية التي تتشابه فيما بينها من حيث الصلة ، والتي يعمل على تصميمها اما فرد أو مجموعة من الافراد أو مؤسسة خاصة ، إذ يتكون كل موقع منها من اعداد غير محددة بذاتها من الصفحات وتكون على أشكال عدة حسب وظيفتها بالموقع[٢] .

ولما تقّدم ذكره دوّن الباحث الاختلافات بين الاثنين كما يآتي

١- من حيث التسمية :

جميع المنصات إلكترونية يمكن تسميتها موقع الكتروني[٣] ، بينما الموقع الإلكتروني لا يمكن تسميته منصات إلكترونية[٤]

٢- من حيث التفاعل :

تقدم المنصات الإلكترونية خدمات تفاعلية فضلاً عن المعلومات ، مما يؤدي الى زيادة التفاعل وعدد الزوار لها[٥] ،اما الموقع الإلكتروني يعرض المعلومات فقط وفي بعض الاحيان قد يعرض معلومات لكن مع عدد قليل جداً من الخدمات التفاعلية الذي يؤدي لقلة التفاعل وقلة عدد الزوار لها[٦].

---

(١) يُنظر: د. عبدالله بن فالح بن راشد السكران ، عبدالله بن أحمد بن عبدالله الراشدي ، المتطلبات التربوية لتوظيف المنصات التعليمية الإلكترونية في العملية التعليمية ، بحث منشور في مجلة البحث العلمي في التربية ، العدد١٩، ٢٠١٨، ص٥٦١.

(٢) يُنظر: د. نهله أبو رشيد ، الصحافة الإلكترونية والنشر الإلكتروني ، الجامعة الافتراضية السورية ، سوريا ، ٢٠٢٠، ص١٤٢.

(٣) يُنظر: د. أحمد محمد محمد السيد الحفناوي ، معايير سهولة الوصول للمنصات التعليمية مفتوحة المصدر Moocs لذوي الإعاقة بالتعليم الجامعي ، بحث منشور في المجلة العربية للتربية النوعية ، كلية التربية ، جامعة الملك سعود ، العدد ١ ، ٢٠١٧، ص٢١.

(٤) يُنظر: د. شريف درويش اللبان ، الصحافة الإلكترونية دراسات في التفاعلية وتصميم المواقع ، ط١، الدار المصرية اللبنانية ، القاهرة ، ٢٠٠٥، ص١٧٣.

(٥) دالية خليل عبد الكريم الشواربة ، مصدر سابق ، ص١٤.

(٦) جاسم رمضان هلالي ، الدعاية والإعلان والعلاقات العامة في المدونات الإلكترونية ، دار النفائس للنشر والتوزيع ، عمان ، ط١، ٢٠١٣، ص٥٣.

٣- من حيث معرفة اذا كان منصات إلكترونية أم مواقع إلكترونية :

اذا كان يسمح بتسجيل العضوية وشراء الخدمات وترك تقييمك للبائعين والتراسل معهم وغيرها من أساليب التفاعل بين المستخدمين فأننا امام منصات إلكترونية [١] ، اما اذا كان يمكنا ترك تعليق على الخبر أو المقال ، أو يسمح بمشاهدة فيديو مع السماح بالتعليق عليه ، ولكن لا يوجد تفاعل بينك وبين الصفحة فأننا أمام مواقع الكترونية[٢] .

٤- من حيث الادارة :

المنصات الإلكترونية يعمل على إدارتها فريق تقني وبرمجي متخصص فضلاً عن المختصين في عالم الحواسيب ، من أجل الاستعداد والمتابعة والتواصل مع الزوار لتحقيق الهدف المنشود منها[٣] ، اما المواقع الإلكترونية يعمل عليها عدد محدود من المبرمجين ذوي الخبرة ، كذلك يمكن لمدير الموقع تلبية احتياجات الزوار والمستخدمين[٤]

٥- من حيث الثقة :

المنصات الإلكترونية اكثر ثقة واقبالا من المواقع الإلكترونية[٥].

٦- من حيث الكلفة :

المنصات الإلكترونية تحتاج الى التقنيات الحديثة والمتقدمة جداً ، وذلك من أجل الاستيعاب لأكبر عدد ممكن من الزوار فضلاً عن الحجم الكبير للمحتوى وعدد المستخدمين للخدمات التفاعلية يوميا حيث يجعلها مكلفة أكثر من المواقع [٦] ، بينما

---

(١) يُنظر: نسرين بسام فريد فرحات ، المنصات الاجتماعية مفتوحة المصدر ، بحث منشور في مجلة دراسات العلوم التربوية ، الجامعة الاردنية ، المجلد ٤٧، العدد٤، ٢٠٢٠، ص٣٤٦.

(٢) يُنظر: د. نهله أبو رشيد ، مصدر سابق ، ص١٤٧.

(٣) يُنظر: د. نجلاء محمد فارس واخرون ، مصدر سابق ،ص٥٢٩.

(٤) يُنظر. جاسم رمضان هلالي ، مصدر سابق ،ص٥٤

(٥) يُنظر. د. محمد رفعت حسنين ، مصدر سابق ، ص٢٢.

(٦) يُنظر. د. سهام بنت سلمان محمد الجريوي ، مصدر سابق ، ص٢٨.

الموقع الإلكتروني يتطلب القدرة على حمل عدد كبير من الزوار له يوميا ، وبهذا تكون تكلفة المواقع الإلكتروني اقل من تكلفة المنصات الإلكترونية[١].

٧- من حيث التخصيص :

المنصات الإلكترونية في كثير من الأحيان تكون مخصصة للبحث أو الاتصال ، أوتكون مخصصة للترفيه ، أو تكون مخصصة للخدمات الحكومية وغيرها [٢]، اما المواقع الإلكترونية في الغالب تكون شامله لكافة التخصصات ولا يقتصر على تخصص نادر[٣] .

نجد مما تقدم أن المستخدمين يهتمون بالمنصات الإلكترونية التي تقدم الخدمات التفاعلية التي ممكن استمرارها للمستقبل، على عكس المواقع الإلكترونية التي تقدم معلومات فقط ، والذي يؤدي تهديد قوة نجاحها واستمرارها ، بسبب عدم تقديم أية من الخدمات التفاعلية .

ثانيا: تمييز المنصات الإلكترونية عن المكتبات الإلكترونية

تتشابه المنصة والمكتبات الإلكترونية في العديد من الخصائص والمزايا إلا أنها تختلف فيما بينها بحسب الخدمة التي أنشئت من أجلها المنصة والمكتبة الإلكترونية ، وعليه دون الباحث بعض الاختلافات .

المنصة الإلكترونية (platform)

وهي البيئة التفاعلية التي تعمل على توظيف جميع التقنيات المختلفة والتي ترتبط بالويب ، كما وتجمع بين مميزات إدارة المحتوى وبين شبكات التواصل الاجتماعي المختلفة وتسهم في مشاركة المحتوى وتبادل المعلومات والافكار[٤].

(١) يُنظر. د. شريف درويش اللبان ، مصدر سابق ، ص١٧٨.

(٢) يُنظر. د. بلقيس بنت إسماعيل داغستاني، هيفاء جار الله معيض المالكي ، ، مصدر سابق ، ص١١٣٢.

(٣) يُنظر. د. رحاب فايز أحمد ، أحمد فايز أحمد ، الجيل الثاني من الويب وأدواته دراسة مقارنة ، بحث منشور في المجلة العلمية ، كلية الأداب ، جامعة بني سويف ، المجلد ٢ ، العدد١٤، ٢٠٠٩، ص١٩.

(٤) يُنظر. دالية خليل عبد الكريم الشواربة ، مصدر سابق ، ص٩.

المكتبة الإلكترونية Electronic library:

نقصد بها الاتاحة لمحتويات وخدمات المكتبات من مصادر المعلومات من بعيد وغيرها ، إذ تعكس على الموقع كل من الاوعية والمواد الجارية والمستخدمة بكثرة سواء المطبوعة أم الإلكترونية منها ، وذلك بالاستعانة بشبكة الإنترنت التي تزودنا بإمكانيات الوصول الى المكتبة أو المصادر العالمية اضافة الى استلام الوثائق منها [١].

١- تقدم المنصات الإلكترونية خدمات تفاعلية عن طريق الويب فضلاً عن تبادل المعلومات[٢] ، أما المكتبة الإلكترونية فأنها تقدم مخزونا من المعلومات التي تساعد الباحثين في بناء المعرفة[٣].

المنصات الإلكترونية تحتاج الى التقنيات الحديثة والمتقدمة جداً ، وذلك من أجل الاستيعاب لأكبر عدد ممكن من الزوار فضلاً عن الحجم الكبير للمحتوى وعدد المستخدمين للخدمات التفاعلية يوميا إذ يجعلها مكلفة[٤] ، اما المكتبة الكترونية تتيح لمستخدميها أليات البحث والاسترجاع وسهولة الوصول لمحتواها ، من اجل تحقيق الاستخدام الفعلي لها ، وهذا يجعلها داخل نطاق الموقع الإلكتروني[٥] .

٢- من حيث التخصص فإن المنصات الإلكترونية في كثير من الأحيان تكون مخصصة للبحث أو الاتصال ، أو تكون مخصصة للترفيه ، أو تكون مخصصة بالخدمات الحكومية وغيرها[٦] ، أما المكتبة الإلكترونية من حيث التخصيص فأنها تكون مخصصة لجميع المصادر التي من شأنها التزويد بالمعرفة من الكتب والدوريات الإلكترونية[٧] .

٣- المنصات الإلكترونية تتطلب شبكة متكاملة من الفنيين والمهندسين والمتخصصين في عالم الحواسيب الآلية ، ذلك من أجل الاستعداد والتواصل والمتابعة مع زوارها ،

---

(١) يُنظر. د. ربحي مصطفى عليان ، المكتبات الإلكترونية والمكتبات الرقمية ، ط٢، دار صفاء للنشر والتوزيع ، عمّان ، ٢٠١٥م، ص١٥٨.
(٢) يُنظر. د. بلقيس بنت إسماعيل داغستاني ، هيفاء جار الله معيض المالكي، مصدر سابق ،١١٣٣.
(٣) يُنظر. د. جميل إطميزي ، مصدر سابق ، ص٧٥.
(٤) يُنظر. د. أحمد محمد محمد السيد الحفناوي ، مصدر سابق ، ص١٩.
(٥) يُنظر. د. وليد سالم محمد الحلفاوي ، مصدر سابق ، ص٣٦.
(٦) يُنظر. د. طارق عبد الرؤوف ، مصدر سابق ، ص١١٥.
(٧) يُنظر. د. ربحي مصطفى عليان ، مصدر سابق ، ص١٦٠.

لتحقيق الهدف المنشود من المنصات الإلكترونية(١) أما المكتبة الإلكترونية فأن البعض من الانظمة الاخرى يمكن ربط مقرراتها معها ومع مواقع اخرى تكون متاحة عبر شبكة الانترنت(٢).

٤- توفر المنصات الالكترونية الجهد والوقت لكنه اكثر كلفة من المكتبة الإلكترونية(٣) .

يتضح لنا مما تقدم ان المنصات الإلكترونية والمكتبات الإلكترونية الاختلاف بينهم في الهدف الذي تم من أجله انشاؤها ولكل واحدة منها اهدافها التي تميزها عن غيرها في التخصيص وعدد الزوار والتكلفة وغيرها ، الباحث يجد ان الاثنين يقدمان خدمة للزبائن او المستخدمين لكن في الوقت الحالي اتجاه اغلبية المستخدمين على المنصات الإلكترونية لأنها تواكب التطورات التكنولوجيا الحديثة ، لما تتمتع بهِ من صفات تميزها عن غيرها .

(١) يُنظر د. حشمت قاسم ، الدوريات الإلكترونية والمكتبات الرقمية ، ط١ ، دار غريب للطباعة والنشر والتوزيع ، القاهرة ، ٢٠١٠، ص١٠٢.

(٢) يُنظر طارق حسين فرحان العواودة ، صعوبات توظيف التعليم الإلكتروني في الجامعات الفلسطينية بغزة كما يراها الأساتذة والطلبة ، رسالة ماجستير ، كلية التربية ، جامعة الازهر غزة ، ٢٠١٢، ص ٣٥.

(٣) يُنظر. د. الغريب زاهر اسماعيل ، تكنولوجيا المعلومات وتحديث التعليم ، ط١، عالم الكتب ، مصر ، ٢٠٠١، ص٣٦.

الفصل الأول

الجرائم الماسة بنظم المعالجة الآلية للمنصات الإلكترونية

الفصل الأول

الجرائم الماسة بنظم المعالجة الآلية للمنصات الإلكترونية

يعد النظام الإلكتروني من الأنظمة المتطورة للتكنولوجيا الحديثة لقيامها بالعديد من التعاملات الإلكترونية المختلفة على عدة مستويات تمكن الافراد الاستفادة منها ، في ظل الانماط الحديثة ومنها المنصات الإلكترونية المثبتة على أجهزة الحاسوب أو أي جهاز إلكتروني آخر عبر شبكة الانترنت ،وان أي تطور حديث يصاحبهُ العديد من الإنتهاكات من بعض الاشخاص الذين لديهم الخبرة التقنية في الأنظمة الإلكترونية ، كما وتكمن خطورة هذهِ الانتهاكات في تعرض المنصات الإلكترونية إلى العديد من الجرائم ومنها جريمة الدخول وجريمة إتلاف المنصات الإلكترونية ، إذ تكون سلسلة متكاملة ومتواصلة إلى حد بعيد ومرتبطة بجوانب عديدة للتعاملات الإلكترونية ، وهذه التعاملات تتطلب اسباغ الحماية الجزائية للمنصات الإلكترونية وما تحتويها من معلومات الإلكترونية ، التي يمكن دمجها بسهولة وسرعة غير مسبوقين ونقلها وتداولها في إطار واسع ، لذا وجب توفير الحماية لها من خلال تشريع قوانين عقابية خاصة تجرّم وتعاقب مثل هكذا إنتهاكات ترتكب عبر التكنولوجيا الحديثة ، بوساطة المنصات الإلكترونية المثبتة على جهاز الحاسب الآلي وعبر شبكة الانترنت أو ضدها ، وأن تتصف القوانين الخاصة التي يتم تشريعها في مكافحة الجرائم الإلكترونية بصورة عامة ومكافحة جرائم المنصات الإلكترونية بصورة خاصة بالمرونة من أجل استيعاب ومواكبة التطورات الحديثة ، مما يجعلها تساير جميع المبتكرات والتقنيات الراهنة والمستقبلية التي تستخدم في التعامل الإلكتروني مع مختلف المنصات الإلكترونية ، وعليه سنقسم هذا الفصل على مبحثين نتناول في المبحث الاول جريمة الدخول للمنصات الإلكترونية دون ترخيص ونتناول في المبحث الثاني جريمة إتلاف معلومات المنصات الإلكترونية.

المبحث الاول

جريمة الدخول للمنصات الإلكترونية دون ترخيص

تعد جريمة الدخول من الجرائم المستحدثة والخطرة التي تتعرض لها الاجهزة الإلكترونية ، ومنصاتها الإلكترونية والشبكات الإلكترونية ، ونتيجة للتطور والتقدم اللامتناهي في مجال التكنولوجيا الحديثة، وما تفرزه من الجوانب الإيجابية المختلفة التي تسهل

على مختلف المجتمعات التواصل فيما بينها التي أصبحت الحل الأمثل للعديد من مفاصل الحياة في تقديم الخدمات ، إذ انها أصبحت تشكل تهديداً خطراً للكثير من الافراد ومؤسسات الدولة والشركات بسبب اساءة استخدامها من قبل البعض وقيامهم بعمليات الاختراق التي سببت خسائر كبيرة مقابل استفادة المخترقين الذين يتمتعون بقدرات عالية في مجال التكنولوجيا الحديثة مما سهل لهم ذلك الوصول إلى المعلومات المخزنة إلكترونياً والاطلاع عليها والعبث بها وافشائها [١]، وإنَّ صعوبة التعرّف عليهم أدت إلى ازدياد اعدادهم وبمحو أثار جرائمهم التي تمكنهم الافلات من العقاب[٢] ،وعليه سنقسم هذا المبحث على مطلبين نتطرق في المطلب الاول إلى موقف الاتفاقيات والتشريعات المقارنة من جريمة الدخول للمنصات الإلكترونية دون ترخيص ، ونتطرق في المطلب الثاني إلى أركان جريمة الدخول للمنصات الإلكترونية دون ترخيص.

المطلب الأول

موقف الاتفاقيات و التشريعات المقارنة من جريمة الدخول للمنصات الإلكترونية دون ترخيص

تعد جريمة الدخول من الجرائم العمدية الأكثر خطورة في ظل التطورات الإلكترونية الحديثة ، التي يتعرض لها النظام الإلكتروني بصورة عامة والمنصات الإلكترونية المثبتة على جهاز الحاسب الآلي أو أي جهاز إلكتروني آخر بصورة خاصة ، مما أدى ببعض التشريعات الدولية بسن قوانين خاصة لمكافحة هذه الجرائم ، اما البعض الآخر فقد ضمّن ذلك من خلال تعديل القوانين العقابية في مكافحة الجرائم التي تتعرض لها المنصات الإلكترونية ، ومنها قانون العقوبات الامريكي والفرنسي وغيرها ، أما الدول العربية فقد تضمنت قوانين خاصة تجريم الأفعال التي تندرج ضمن الجرائم الإلكترونية وهي كل من الأردن والإمارات ، اما العراق لم ينظم تجريم الجرائم الإلكترونية في قانون خاص على الرغم من وجود مشروع قانون الجرائم الإلكترونية لسنة ٢٠١١ في مجلس النواب العراقي الذي تمت قراءته مما يجعل العراق يعاني من قصور تشريعي خاص بالجرائم الإلكترونية ، وعليه سنقسم هذا المطلب على فرعين نتناول في الفرع الاول موقف الاتفاقيات الدولية والإقليمية من جريمة الدخول للمنصات الإلكترونية دون

---

(١) يُنظر: جلال محمد الزغبي ، اسامة أحمد المناعسة ، جرائم تقنية نظم المعلومات الإلكترونية (دراسة مقارنة) ، ط١، دار الثقافة ، عمان ، ٢٠١٠، ص٢١.

(٢) يُنظر: محمد كمال محمود الدسوقي ، الحماية الجنائية لسرية المعلومات الإلكترونية (دراسة مقارنة) ، ط١، دار الفكر والقانون للنشر والتوزيع ، مصر ، ٢٠٢١، ص٥٥.

ترخيص ، وفي الفرع الثاني موقف التشريعات المقارنة من جريمة الدخول للمنصات الإلكترونية دون ترخيص.

الفرع الأول

موقف الاتفاقيات الدولية والإقليمية من جريمة الدخول للمنصات الإلكترونية دون ترخيص

جرّمت الاتفاقيات الدولية بنصوص صريحة جريمة الدخول دون ترخيص ومن هذه الاتفاقيات اتفاقية بودابست لعام ٢٠٠١ ، والاتفاقية العربية لعام ٢٠١٠ من جريمة الدخول للمنصات الإلكترونية دون ترخيص.

اولاً: اتفاقية بودابست لمكافحة جرائم المعلوماتية لعام ٢٠٠١

اختلفت العديد من القوانين والاتفاقيات على تسمية جريمة الدخول إلا أن مضمونها واحد ، فنجد المادة الثانية من اتفاقية بودابست لمكافحة جرائم المعلوماتية لعام ٢٠٠١ اطلقت عليها تسميات مختلفة منها الولوج غير القانوني أو الدخول غير المصرح به أو الدخول غير المشروع فجميعها تدل على معنى واحد ، كما ان المادة ذاتها أوجبت على كل طرف من اطراف الاتفاقية ان تتبنى الاجراءات التشريعية أو أي تدابير اخرى بحسب قانونها الداخلي ، لتجريم الدخول غير القانوني أو غير المصرح به لكل أو لجزء من النظام ، بهدف الحصول على البيانات أو المعلومات ، بأي نيه إجرامية اخرى ، شرط ان يكون ارتكاب الجريمة عن طريق الحاسب الالي المرتبط بشبكة الانترنت بحاسب آلي أخر[١] ، كما أشارت المذكرة التفسيرية إلى ان الدخول غير القانوني يضم الاختراق سواء كان لكل النظام أو جزئه مهما كان ذلك الاختراق في جزء مادي أو برامج جزئية أو بيانات مخزنة في نظام التنصيب أو الفهارس أو البيانات التي تكون متعلقة بالمحتوى أو ربما يكون ذلك لنظام المعلومات المتصل بالشبكات العامة ، أو متصل بالشبكة نفسها ، أو كانت شبكة محلية أو شبكة خاصة أو عن طريق الانترنت[٢]، وتعد جريمة

([١]) يُنظر: د. هلالي عبد اللاه أحمد ، إتفاقية بودابست لمكافحة جرائم المعلوماتية ، ط١، دار النهضة العربية ، القاهرة ، ٢٠٠٧ ، ص٤٨.

([٢]) يُنظر: رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن ، ط١، منشورات الحلبي الحقوقية ، ٢٠١٢ ، ص ٢٢٥.

الدخول إلى النظام الإلكتروني ظاهرة إجرامية ذات خطورة [١] ، كونها تعبر عن قوة تأثير تكنولوجيا المعلومات الحديثة في عالم الجريمة[٢] .

ثانياً: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠.

تم عقد هذه الاتفاقية عام ٢٠١٠ وعدد الدول التي وقعت عليها هي سبع عشرة دولة [٣] كما أن العراق كان طرفاً في هذه الاتفاقية من خلال تصديق قانون الاتفاقية العربية لمكافحة جرائم تقنية المعلومات رقم (٣١) لسنة ٢٠١٣ المنشور بجريدة الوقائع العراقية بالعدد ٤٢٩٢في ٢٠١٣/٩/٣٠ [٤] ، إذ جرّمت الدخول غير المصرح به وذلك في الفصل الثاني المتعلق بأحكام التجريم في الفقرة الأولى من المادة السادسة التي جرّمت " الدخول وكل اتصال غير مشروع

---

(١) أشارت المذكرة التفسيرية لاتفاقية بودابست بأن الولوج غير القانوني يعد الجريمة الرئيسية التي تنطوي على تهديد وتعد على الأمن بمعنى السرية والسلامة وإتاحة النظم والبيانات المعلوماتية ، إذ أن هناك ضرورة لتوفير حماية ملائمة لمصالح المنظمات ، وبالأخص لرجل الادارة حتى يكون بمقدورهم أن يديروا ، ويستثمروا ويتحكموا في نظمهم بدون تشويش أو عقبة من أي نوع ، وذلك على أساس أن هذه الافعال يمكن أن تخلق عقبات أمام المستخدمين الشرعيين للنظم والبيانات ، كما يمكن ان تؤدي إلى إتلاف أو تدمير باهظ التكلفة في حالة إعادة البناء ، كما أن هذا التدخل يمكن أن يترتب عليه الوصول إلى بيانات سرية ، مثل كلمات المرور أو معلومات عن النظام الهدف واسرار تسمح باستخدام النظام مجاناً ، بل وتشجع القراصنة على ارتكاب أنواع أكثر خطورة من الجرائم المتصلة بالحاسب يُنظر: د . هلالي عبد اللاه أحمد ، إتفاقية بودابست لمكافحة جرائم المعلوماتية ، مصدر سابق ، ص ٤٩-٥٠.

(٢) يُنظر: د. محمود رجب فتح الله ، الوسيط في الجرائم المعلوماتية ، دار الجامعة الجديدة ، ٢٠١٩ ،ص٣٣٢.

(٣) تم عقد هذه الاتفاقية بتاريخ ٢٠١٠/١٢/٢١ وعدد الدول التي وقعت على هذه الاتفاقية هي سبع عشرة دولة عربية ، وان هذه الاتفاقية جاءت بعد المطالبة الشديدة من قبل بعض المختصين على اصدارها وفي أكثر من مناسبة ، وان لإعلان القاهرة لمكافحة الجريمة الإلكترونية لعام٢٠٠٧الذي صدر عن المؤتمر الاقليمي الاول حول الجريمة الإلكترونية الذي تم انعقاده في القاهرة كان السبب في دعوة الدول العربية من أجل الاسراع بسن تشريعات تكافح الجرائم الإلكترونية جميعها ، كذلك الاسترشاد باتفاقية بودابست عند إعداد قوانين الاتفاقية سواء الموضوعية والاجرائية منها ، وعبرة المادة الاولى من الاتفاقية عن الهدف الذي تسعى إليه هذه الاتفاقية من خلال تعزيز التعاون المشترك بين الدول العربية من أجل مكافحة جرائم تقنية المعلومات التي تُعد من الجرائم الخطرة التي تهدد أمن الدول ومصالحها وسلامة مجتمعاتها، عن طريق تبني سياسة جنائية مشتركة لحماية أمن المجتمع العربي من الجرائم الإلكترونية يُنظر: د. محمد كمال محمود الدسوقي ، مصدر سابق ، ص٢٠٢.

(٤) قانون تصديق الاتفاقية العربية لمكافحة جرائم تقنية المعلومات رقم (٣١) لسنة ٢٠١٣ وتم نشرها في جريدة الوقائع العراقية بالعدد (٤٢٩٢) في (٢٠١٣/٩/٣٠).

مع كل أو جزء من تقنية المعلومات أو الاستمرار به[١] ، وشددت العقوبة في الفقرة الثانية من المادة ذاتها إذا نتج عن الدخول أو الاتصال أو الاستمرار بهذا الاتصال:

أ-"محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة وللأجهزة والانظمة الإلكترونية وشبكات الاتصال وإلحاق الضرر بالمستخدمين والمستفيدين

ب- الحصول على معلومات حكومية سرية"[٢].

يتضح لنا مما تقدم أن الجرائم الإلكترونية وما يصاحبها من خطورة على أمن المجتمع ومصالحة ، دفعت المختصين إلى المطالبة بتشريع اتفاقية دولية عربية من أجل معاقبة الجناة في جميع الدول العربية ، وتوفير الحماية للنظام الإلكتروني ، وان لإعلان القاهرة الدور الكبير في تشجيع الدول للإنضمام إلى هذه الاتفاقية يكون أساسها ومرجعها اتفاقية بودابست في اعداد القوانين الموضوعية والاجرائية ونلاحظ أن نصوص الاتفاقيتين متشابهتين فلا مانع من إنضمام الدول التي خارج حدود هذه الاتفاقية ، وان العراق صادق على هذه الاتفاقية وتم نشرها في جريدة الوقائع العراقية بالعدد (٤٢٩٢) في (٢٠١٣/٩/٣٠) وتم ذلك رسمياً بالقانون رقم (٣١) لسنة ٢٠١٣، لمكافحة جرائم تقنية المعلومات .

نستنتج مما تقدم أن قانون تصديق الاتفاقية العربية لمكافحة جرائم تقنية رقم ٣١لسنة ٢٠١٣ أغفلت تحديد العقوبة ومدتها.

الفرع الثاني

موقف التشريعات المقارنة من جريمة الدخول للمنصات الإلكترونية دون ترخيص

أغلبية قوانين دول المقارنة جرمت الدخول دون ترخيص من خلال نصوص عقابية ضمن قانون العقوبات ، أو بسن قوانين خاصة تجرّم الدخول للمنصات الإلكترونية دون ترخيص

---

(١) يُنظر .د. عمار عباس الحسيني ، جريمة الإتلاف المعلوماتي (دراسة قانونية مقارنة) ، ط١، منشورات زين الحقوقية ، بيروت ،٢٠١٩ ، ص٢٣٤.

(٢) يُنظر: نص المادة (السادسة /ثانياً| أ ، ب) من قانون تصديق الاتفاقية العربية لمكافحة جرائم تقنية المعلومات رقم (٣١) لسنة ٢٠١٣.

،والبعض الآخر من الدول يعاني من قصور تشريعي بخصوص الجرائم الإلكترونية ومنها العراق .

اولاً: موقف التشريعات الاجنبية المقارنة من جريمة الدخول للمنصات الإلكترونية دون ترخيص

غالبية التشريعات الأجنبية المقارنة جرّمت أفعال الدخول دون ترخيص وذلك من خلال تضمين نصوص عقابية ضمن قانون العقوبات ، وتعد الولايات المتحدة الأمريكية من أولى الدول التي جرّمت هذهِ الافعال وذلك في المادة الثانية من مشروع القانون الفدرالي لحماية نظم الحاسبات لسنة ١٩٨٤ التي نصت على الدخول عمداً دون ترخيص لنظام الحاسب الالي أو الدخول عن طريق الشبكة لنظام الحاسب أو المنصات الإلكترونية [١] ، والذي صدر في العام نفسه سمي بقانون الاحتيال واساءة استخدام الحاسوب لسنة ١٩٨٤[٢] ، وقد عرّف المشرّع الامريكي الحاسب الآلي في الفقرة الاولى من المادة ١٠٣٠من القانون الفيدرالي بأنه " كل جهاز إلكتروني، أو كيميائي كهربائي ، أو جهاز سريع لمعالجة المعلومات ، يقوم بإجراء عمليات منطقية وحسابية ، كما يشمل أيضاً كل وسيلة آلية لتخزين المعلومات ، وكذلك كل وسائل الاتصالات التي تعمل بالاتصال مع أي من هذه الاجهزة"[٣] ، ومن عمليات الاختراق التي تعرضت لها الولايات المتحدة الأمريكية هي قضية الجحيم العالمي[٤].

([١]) يُنظر: د. محمود رجب فتح الله ، مصدر سابق ، ص٣٣٥.

([٢]) الذي تم تعديله لأكثر من مرة في عام ١٩٨٦ و١٩٩٤ وتناول القسم ١٨ الخاص بالجرائم والاجراءات الجنائية ، الذي جرم الدخول غير المصرح به لنظام الحاسب الآلي التابع للحكومة الفدرالية الامريكية وبعد ذلك صدور قانون حماية المعلومات القومية لسنة ١٩٩٦ ، الذي وسعت من نطاق الحماية من خلال تجريمها الدخول غير المصرح به ليس فقط لأنظمة الحاسب الآلي التابعة للحكومة ، بل جرّم تبادل الشفرات الخاصة بالدخول إلى نظام الحاسبات الآلية في المادة (١٠٣٠/أ) من القانون الفدرالي لجرائم الحاسب الألي لسنة ١٩٩٦، كذلك المعلومات التي تساعد على الدخول غير المصرح به إلى نظام الحاسب الآلي ، من خلال اختراق المعلومات الامنية داخل نظام الحاسبات الآلية يُنظر: علي عبود جعفر ، مصدر سابق ، ص١٤٠.

([٣]) يُنظر: د. محمود محمد محمود جابر ، الجرائم الناشئة عن إستخدام الهواتف النقالة (جرائم نظم الإتصالات والمعلومات) ، ط١، المكتب الجامعي الحديث ، ٢٠١٨ ، ص٤٦٧.

([٤]) ويدور مضمون هذه القضية في تمكن مجموعه من المخترقين من اختراق مواقع البيت الابيض والشركة الفيدرالية الأمريكية والجيش الامريكي ووزارة الداخلية الأمريكية ، الذي ادين اثنين من المجموعات التي قامت بالاختراق ، وبعد قيام مكتب التحقيقات الفدرالية بإجراء التحقيقات ، فقد تبين من خلالها ان المجموعات التي تم

اما المشرّع الفرنسي فقد جرّم الدخول داخل نظام المعالجة الآلية للمعلومات في معناها الواسع في المادة (١/٣٢٣) من قانون العقوبات الجديد رقم ١٣٣٦لسنة ١٩٩٢ النافذ عام ١٩٩٤، والتجريم يكون على الدخول سواء على النظام بأكمله أم جزء منه وهو شرط لتحقق الجريمة ، اما فيما يتعلق بالأعمال التحضيرية للقانون فقد أجمع الفقه أن نظام المعالجة الآلية للمعلومات ، عند تطبيق المادة المشار اليها اعلاه يقع على المعلومات والنظام الذي يحتوي عليها سواء كان نظام الحاسب الآلي أم المنصات الإلكترونية المثبتة عليه أم أي جهاز إلكتروني آخر أم الشبكات الإلكترونية [١] ، وان المناقشات السابقة كان لها الدور الكبير في تبني القانون لتعريف نظام المعالجة الآلية للمعلومات ، وهو في الأصل وارد في القانون رقم (١٧) لسنة ١٩٧٨، الخاص بحماية المعلومات ،و شمل التعريف جميع العمليات التي تتم بواسطة الوسائل الإلكترونية أي كان نوعها التي تتعلق بالتجميع والتسجيل والتخزين والمعالجة والتعديل والاسترجاع والمحو ونقل العمليات التي تتم بواسطة الوسائل الإلكترونية ، من أجل استغلال المعلومات وربطها وتقريبها ودمجها مع المعلومات الاخرى والقيام بتحليلها للحصول على معلومات لها دلالة خاصة ، فضلاً عن إلتقاط الاشارات وتبادل المعلومات عبر المنصات الإلكترونية و شبكة الانترنت فإنها جميعها تُعد دخولاً لنظام المعالجة الالية ، وهذا الدخول يمثل نتيجة للتوسع في مفهوم المعالجة الآلية حسب القانون الفرنسي[٢] .

يتضح لنا أن المشرّع الفرنسي كان أكثر دقة وحرصاً على تجرّيم الدخول دون تصريح للنظام سواء كان كلياً أو جزئياً دون الوصول للمعلومات ، على عكس المشرّع الامريكي الذي اشترط أن يكون الدخول بسوء نية ، واقتصر على الدخول لنظام الحاسب الآلي التابع للحكومة ، وحتى بعد تعديل القانون عاقب على تجاوز الحد المسموح به ، والباحث يؤيد القانون الفرنسي لأنه يعد أكثر صرامة في معاقبة الجاني وتوفير الحماية الجزائية للمنصات الإلكترونية وما تحويها من معلومات.

التعرف عليها كانت تهدف إلى مجرد الاختراق أكثر من هدفها للتدمير أو التقاط المعلومات الحساسة ، في حين استغرق التحقيق مئات الساعات في ملاحقة ومتابعة مجموعة المخترقين عبر الشبكة والقيام بتتبع أثار نشاطهم ، حيث كلفهم ذلك مبالغ طائلة من الوصول للجناة ومعرفتهم وإلقاء القبض عليهم ، يُنظر: أمير فرج يوسف ، الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت ، ط١، مكتبة الوفاء القانونية ، ٢٠١١، ص٣٦٧-٣٦٨.

(١) يُنظر: رشيدة بوكر ، مصدر سابق ، ص٢٢٥.

(٢) يُنظر: د. محمود محمد محمود جابر ، مصدر سابق ، ص٤٦٦.

ثانيا: موقف التشريعات العربية المقارنة من جريمة الدخول للمنصات الإلكترونية دون ترخيص.

اتجهت بعض الدول العربية إلى تجريم الدخول دون ترخيص من خلال تشريعات خاصة ، ومن هذه الدول الامارات والاردن ، أما العراق فقد اكتفى بتقديم مشروع قانون جرائم الإلكترونية لسنة ٢٠١١.

فبالنسبة لدولة الامارات العربية فقد اتخذت تشريعات عديدة تجرّم الدخول للنظام الإلكتروني والحاسب الآلي وحماية المعلومات وذلك ، بمرسوم قانون اتحادي رقم (٥) لسنة ٢٠١٢فقد عرّفت المادة الأولى منه المعلومات الإلكترونية ونظام المعلومات الإلكتروني ووسيلة تقنية المعلومات[١] ، وعاقبت الفقرة الاولى من المادة الثانية من القانون ذاته " كل من دخل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات ، أو وسيلة تقنية معلومات ، بدون تصريح أو بتجاوز حدود التصريح ، يعاقب بالحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تزيد على ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين"[٢] ، أما الفقرة الاولى من المادة الرابعة فقد عاقبت على الدخول بقصد الحصول على بيانات حكومية ، فضلاً عن المعلومات السرية التي تختص بمنشأة مالية أو تجارية أو اقتصادية بالسجن المؤقت والغرامة"[٣] ، وعاقبت المادة

([١]) يُنظر: نص المادة(١) من مرسوم بقانون اتحادي رقم (٥) لسنة ٢٠١٢، التي عرّفت كل من المعلومات الإلكترونية بأنها (أي معلومات يمكن تخزينها ومعالجتها وتوليدها ونقلها بوسائل تقنية المعلومات وبوجه خاص الكتابة والصور والصوت والارقام والحروف والرموز والاشارات وغيرها). اما نظام المعلومات الإلكتروني فتم تعريفه بأنه (مجموعة برامج معلوماتية ووسائل تقنية المعلومات المعدة لمعالجة وإدارة وتخزين المعلومات الإلكترونية أو ما شابه ذلك). أما وسيلة تقنية المعلومات فقد عرّفت بأنها (أي اداة إلكترونية مغناطيسية ، بصرية ، كهروكيميائية ، أو أي اداة اخرى تستخدم لمعالجة البيانات الإلكترونية واداء العمليات المنطقية والحسابية ، أو الوظائف التخزينية ، ويشمل أي وسيلة موصلة أو مرتبطة بشكل مباشر ، تتيح لهذه الوسيلة تخزين المعلومات الإلكترونية أو إيصالها للأخرين).

([٢]) يُنظر: نص الفقرة الاولى من المادة (٢) من مرسوم بقانون اتحادي رقم (٥) لسنة ٢٠١٢.

([٣]) تنص الفقرة الأولى من المادة الرابعة على أن " 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، يعاقب بالسجن المؤقت والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون وخمسمائة ألف درهم".

التاسعة من القانون ذاته في حالة قيام الجاني بالتحايل على العنوان البروتوكولي لشبكة المعلومات ، قاصداً ارتكاب الجريمة من دون اكتشافه بالسجن المؤقت والغرامة[١].

يتضح مما تقدم أن المشرع الاماراتي نص صراحة على وسيلة تقنية المعلومات التي يتم من خلالها فعل الدخول الذي يعاقب عليه وتحديداً في الفقرة الاولى من المادة الثانية، التي من الممكن تطبيقها على الدخول للمنصات الإلكترونية والمعلومات والبيانات التي تحتويها محل الحماية ، وتم تشديد العقوبة وجعلها مؤقته حسب تقدير القاضي أما الغرامة فتكون مضاعفة إذا كان الدخول من أجل الحصول على معلومات حكومية وسرية تتعلق بالنشاط الاقتصادي أو التجاري ، ونجد في المادة التاسعة من القانون نفسه قد شدد العقوبة في حالة الدخول بقصد التحايل على العنوان البروتوكولي ، من خلال استخدامه عنوان وهمي ، ويهدف إلى تحقق الجريمة من دون اكتشافه .

أما المشرع الاردني فقد انتهج منهج المشرع الاماراتي من خلال تشريعه قانون الجرائم الإلكترونية رقم (٢٧) لسنة ٢٠١٥، فقد عرّف في المادة الثانية كل من نظام المعلومات والبيانات والشبكة المعلوماتي والتصريح والبرامج [٢]، وعاقبت الفقرة (أ) من المادة الثالثة الدخول إلى الشبكة والنظام المعلوماتي ، وكان الدخول دون تصريح وعمداً أو مخالفاً أو متجاوزاً حدود التصريح ، ففي هذه الحالة تتحقق جريمة الدخول وتكون العقوبة الحبس أو

---

(١) تنص المادة التاسعة على أن " كل من تحايل على العنوان البروتوكولي للشبكة المعلوماتية باستخدام عنوان وهمي أو عنوان عائد للغير أو بأي وسيلة أخرى ، وذلك بقصد ارتكاب جريمة أو الحيلولة دون اكتشافها".

(٢) يُنظر: نص المادة الثانية من قانون الإلكترونية رقم (٢٧) لسنة ٢٠١٥، التي عرفت كل من نظام المعلومات بأنه:(مجموعة البرامج والادوات المعدة لإنشاء البيانات أو المعلومات إلكترونياً ، أو أرسالها أو تسلمها أو معالجتها أو تخزينها أو إدارتها أو عرضها بالوسائل الإلكترونية "، اما البيانات "فهي الارقام أو الحروف أو الرموز أو الاشكال أو الاصوات أو الصور أو الرسومات التي ليس لها دلالة بذاتها" ، اما المعلومات "فهي البيانات التي تمت معالجتها واصبح لها دلالة "، اما الشبكة المعلوماتية "ارتباط بين اكثر من نظام معلومات لإتاحة البيانات والمعلومات والحصول عليها واما التصريح فهو الإذن الممنوح من صاحب العلاقة إلى شخص أو اكثر أو للجمهور للدخول أو استخدام نظام المعلومات أو الشبكة المعلوماتية بقصد الاطلاع أو إلغاء أو حذف أو اضافة أو تغيير أو إعادة نشر بيانات أو معلومات أو حجب الوصول إليها أو إيقاف عمل الأجهزة أو تغيير موقع إلكتروني أو إلغائه أو تعديل محتوياته" ، أما البرامج "فهي مجموعة من الأوامر والتعليمات الفنية المعدة لإنجاز مهمة قابلة للتنفيذ باستخدام أنظمة المعلومات").

الغرامة[1] وشددت العقوبة بموجب الفقرة (ب) من المادة ذاتها أذا نتج عن الدخول المشار اليه في الفقرة (أ) إتلاف أو تدمير أو حذف أو نقل أو نسخ البيانات أو المعلومات وغيرها ، فتكون العقوبة الحبس والغرامة [2] ، يلاحظ ان المشرع الأردني عاقب على جريمة الدخول بنص خاص ، في قانون الجرائم الإلكترونية ، من أجل توفير الحماية للمعلومات التي يحتويها النظام الإلكتروني أو الشبكة الإلكترونية ، علما إنه ترك أمر الوسيلة التي تتم فيها الجريمة مطلقة ، والمطلق يجري على إطلاقة إذا لم يوجد قانون يقيده ، وبالتالي يمكن تطبيق المادة المشار إليها على المنصات الإلكترونية ، وما تحتويها من معلومات تصلح لأن تكون محلاً لتحقق جريمة الدخول .

اما المشرع العراقي يعاني من عدم وجود قانون خاص يجرّم الجرائم الإلكترونية ومنها جريمة الدخول للمنصات الإلكترونية دون ترخيص ، على الرغم من وجود مشروع قانون جرائم الإلكترونية لسنة ٢٠١١، الذي جرّم العديد من الأفعال التي تنطوي على جريمة الدخول دون ترخيص في مواد عديدة، كما عاقبت الفقرة (ب) ثالثاً من المادة الرابعة التي نصت على " كل من تطفل أو أزعج أو أتصل بمستخدمي أجهزة الحاسوب وشبكة المعلومات من دون تصريح أو اعاق استخدامها من منتفعيها ، يعاقب بالحبس مدة لا تزيد على (٣) ثلاثة أشهر أو بغرامة لا تقل عن (٢٠٠٠٠٠٠) مليوني دينار ولا تزيد على (٥٠٠٠٠٠٠) خمسة ملايين دينار[3] ، كذلك الفقرة (ج) من المادة ذاتها عاقبت على كل من " دخل عمداً بدون تصريح موقعاً أو نظاماً معلوماتياً أو أتصل مع نظام الحاسوب أو جزء منه"[4] ، اما الفقرة (د) من المادة ذاتها عاقبت بنفس العقوبة كل من " استخدم أو تسبب دون تصريح في استخدام الحاسوب العائد للغير بطريقة

---

(1) نص الفقرة (أ) من المادة الثالثة من قانون الجرائم الإلكترونية الأردني رقم (٢٧) لسنة ٢٠١٥ التي تنص على أن : (يعاقب كل من دخل قصداً إلى الشبكة المعلوماتية أو نظام معلومات بأي وسيلة دون تصريح أو يجاوز التصريح بالحبس مدة لا تقل عن أسبوع ولا تزيد على ثلاثة أشهر أو بغرامة لا تقل عن (١٠٠) مائة دينار ولا تزيد على (٢٠٠) مائتي دينار أو بكلتا هاتين العقوبتين).

(2) تنص الفقرة (ب) من المادة الثانية من قانون الجرائم الإلكترونية الأردني رقم (٢٧) لسنة ٢٠١٥ التي تنص على أن " إذا كان الدخول المنصوص عليه في الفقرة (أ) من هذه المادة لإلغاء أو حذف أو اضافة أو تدمير أو افشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو توقيف أو تعطيل عمل الشبكة المعلوماتية أو نظام معلومات الشبكة المعلوماتية فيعاقب الفاعل بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن (٢٠٠) مائتي دينار ولا تزيد على (١٠٠٠) ألف دينار.

(3) يُنظر: الفقرة ب/ثالثاً/ من المادة الرابعة عشر من مشروع قانون الجرائم الإلكترونية لسنة ٢٠١١.

(4) يُنظر: الفقرة ج/ثالثاً/ من المادة الرابعة عشر من المشروع نفسه

مباشرة أو غير مباشرة"[1] ، و تم تشديد العقوبة في حالة تجاوز نطاق التصريح المحدد أو في حالة الاعتراض للمعلومات عند عملية تبادلها ، حيث تكون العقوبة الحبس والغرامة التي لا تقل عن عشرة ملايين ولا تزيد على خمسة عشر مليون وذلك في المادة (١٥/أ| أولاً) [2] ، و نجد المادة (٢١/ب| أولاً) حددت عقوبة الحبس على ان لا تزيد على ثلاث سنوات والغرامة التي لا تزيد على عشرين مليون أو احداهما ، إذا كان الدخول خاص بشركة أو مؤسسة والغرض منه تغيير تصاميم الموقع أو الاتلاف أو التعديل أو الاستغلال غير المشروع سواء كان لنفسه أو لغيره [3].

يتضح لنا مما تقدم ان مشروع قانون الجرائم الإلكترونية العراقي لسنة ٢٠١١ قد جرّم العديد من الجرائم الإلكترونية وجعل لها عقوبات متفاوتة كما وشدد في الوقت نفسه على جريمة الدخول دون تصريح في العديد من فقرات مشروع القانون ، الذي تمت قراءته الاولى عام ٢٠١١لذلك أصبح التصويت على مشروع القانون ولكن بعد إجراء بعض التعديلات عليه من قبل المختصين بالقانون الجنائي من أجل سد القصور التشريعي الذي يعاني منه القضاء العراقي بخصوص الجرائم الإلكترونية ، ومعاقبة جميع المجرمين على الجرائم التي تتم في العالم الافتراضي، كذلك توفير الحماية الجنائية للمحل الذي تقع عليه الجريمة الإلكترونية من المنصات الإلكترونية والمعلومات التي تحتويها ، وتوفير الحماية الجزائية للوسيلة التي يتم بوساطتها الدخول للنظام الإلكتروني أو المنصات الإلكترونية بجميع أنواعها .

المطلب الثاني

أركان جريمة الدخول للمنصات الإلكترونية دون ترخيص

يشترط في أي جريمة يعاقب عليها القانون تحقق أركان الجريمة الركن المادي والركن المعنوي سواء كانت الجريمة تقليدية أو كانت الجريمة إلكترونية ، اما بخصوص جريمة الدخول

---

(١) يُنظر: الفقرة د/ثالثاً/ من المادة الرابعة عشر من المشروع ذاته

(٢) تنص الفقرة (أ) من المادة ١٥على أن: " يعاقب بالحبس وبغرامة لا تقل عن (١٠٠٠٠٠٠٠) عشرة ملايين دينار ولا تزيد على (١٥٠٠٠٠٠٠) خمسة عشر مليون دينار عراقي كل من تجاوز عمداً نطاق التصريح المخول به أو اعترض اية معلومات خلال عمليات تبادلها.

(٣) تنص الفقرة ب/أولاً من المادة ٢١ على أن " يعاقب بالحبس مدة لا تقل عن (٢) سنتين ولا تزيد على (٣) ثلاث سنوات وبغرامة لا تقل عن (١٠٠٠٠٠٠٠) عشرة ملايين دينار ولا تزيد على (٢٠٠٠٠٠٠٠) عشرين مليون دينار أو بإحدى هاتين العقوبتين كل من دخل موقعاً خاصاً بشركة أو مؤسسة أو غيرها لتغيير تصاميم هذا الموقع أو إلغائه أو إتلافه أو تعديله أو استغله لنفسه أو لغيره بدون وجه حق".

للمنصات الإلكترونية لابد من توافر الركن المادي الذي يتمثل في فعل الدخول ، والركن المعنوي يتمثل بالقصد الجنائي وبعض الجرائم تتطلب قصد جنائي خاص بجانب القصد الجنائي العام ، وعليه سنقسم هذا المطلب على فرعين نتناول في الفرع الاول الركن المادي في جريمة الدخول للمنصات الإلكترونية دون ترخيص وفي الفرع الثاني الركن المعنوي في جريمة الدخول للمنصات الإلكترونية دون ترخيص.

الفرع الاول

الركن المادي في جريمة الدخول للمنصات الإلكترونية دون ترخيص

يتخذ الركن المادي في جريمة الدخول للمنصات الإلكترونية دون ترخيص مظهراً خارجياً ، يتكون الركن المادي من ثلاثة عناصر رئيسية وهي كل من السلوك الإجرامي للجاني في الدخول للمنصات الإلكترونية والنتيجة الإجرامية وعلاقة سببية بين السلوك الإجرامي والنتيجة الإجرامية .

اولاً: السلوك الإجرامي في جريمة الدخول للمنصات الإلكترونية دون ترخيص

يعد السلوك الإجرامي العنصر الأول من عناصر الركن المادي ، فضلاً عن ذلك فإنه يمثل العنصر الاهم بين جميع العناصر الأخرى في الجرائم المختلفة ، سواء كانت جرائم تقليدية أم جرائم إلكترونية ، ومن الممكن تحقق السلوك الإجرامي من دون تحقق النتيجة ،لأن السلوك الاجرامي يتحقق بمجرد الدخول اما ، كما ان السلوك الإجرامي يتطلب وجود البيئة الرقمية أوأي جهاز إلكتروني كألحاسب الآلي أو الهاتف النقال أو غيره من الاجهزة التي ممكن ان تثبت عليها المنصات الإلكترونية واستخدامها عبر شبكة الانترنت ، ويقوم الفاعل بتحميل المنصات الإلكترونية ببرامج اختراق قام بشرائها أم قام بتجهيزها واعدادها بنفسه من أجل التحضير لنشرها داخل المنصات الإلكترونية [1] ، والقانون لا يعاقب على الاعمال التحضيرية في الجرائم التقليدية إذا لم يباشر الجاني بتنفيذ الجريمة ، لكن نجد الامر مختلف في العالم الافتراضي فان القانون يعاقب على مجرد قيام الجاني بشراء برامج اختراق ، أو معدات لفك الشفرات أو كلمات المرور وغيرها مما يشكّل جريمة بحد ذاتها سواء كان الدخول للمنصات

(١) يُنظر أمير فرج يوسف ، مصدر سابق ، ص١٢٣.

الإلكترونية كلياً أو جزئياً [١] ، كذلك يكون الدخول للمنصات الإلكترونية غير مشروع إذا تجاوز الجاني الحد المسموح له في الدخول حتى وان كان ذلك الدخول في جزء معين لمعلومات المنصات الإلكترونية ، أما قضية تجريم الدخول إلى النظام الإلكتروني أم المنصات الإلكترونية يرى البعض أنها ليست بالأمر الجديد وإنما تقاس على فعل الاعتداء على حرمة المسكن [٢] ، فقد ادانت محكمة جنايات المثنى بتاريخ ٢٠١٨/١٢/٢ وعدد ٥١٤/ج/٢٠١٨ المتهم الذي قام بالاستيلاء على الصور الشخصية للمجنى عليه من خلال اختراق صفحة التواصل الإجتماعي الشخصية وقيام المتهم بتهديد المجنى عليه بنشر صوره العائلية ومساومته على مبالغ مالية وارصدة بطاقات تعبئه فقد حكمت عليه بالسجن الشديد لمدة خمس سنوات وشهر وفق المادة ١/٤٥٢ من قانون العقوبات العراقي رقم (١١١) لسنة (١٩٦٩) المعدل [٣] ، ففي هذه الحالة تقوم الجريمة ويعاقب فاعلها ، نلاحظ السلوك الإجرامي الذي قام به المتهم هو اختراق الصفحة الشخصية للمجنى عليه والاستيلاء على صوره العائلية وتهديده بنشرها وهذا السلوك الذي قام به يستوجب عقوبة مشدده حتى يكون عبره لغيره لكن لوكان هناك قانون خاص للجرائم الإلكترونية لكانت العقوبة أشد مما هي في قانون العقوبات العراقي .

أما في حالة قيام الجاني في الدخول إلى برنامج منعزل عن النظام الإلكتروني وكان محظور عليه الدخول وقيامه بقراءة الشاشة مثلاً ففي هذه الحالات لا تقوم جريمة الدخول للمنصات الإلكترونية لأن سلوك الجاني كان إيجابي في عدم كسر الحماية الفنية الذي يعمل على توفير الحماية ضد أي أتصال غير مصرح به لمعلومات المنصات الإلكترونية [٤].

ثانياً: النتيجة الإجرامية في جريمة الدخول للمنصات الإلكترونية دون ترخيص

تعد النتيجة الإجرامية العنصر الثاني من عناصر الركن المادي الذي يتخذ مظهر خارجي لسلوك الجاني في جريمة الدخول للمنصات الإلكترونية دون ترخيص التي تقوم على أحداث تغييراً حسياً ملموساً في العالم الخارجي للجريمة، وأن أغلب الجرائم يلزم لتوافرها تحقيق النتيجة

---

(١) يُنظر: د. عبدالفتاح بيومي حجازي ، جرائم الكمبيوتر والانترنت في التشريعات العربية (دراسة مقارنة مع التطبيق على نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية ، ط١، دار النهضة العربية ، القاهرة ، ٢٠٠٩ ، ص٢٨.

(2) vergutch (pascal), la repession des delits informatiques dans une perspective intemational, these, universite de mont pellier 1,1996, p.172.

(٣) يُنظر: مجلس القضاء الأعلى ، محكمة التمييز الاتحاديه ، ت/٤٥٢٦ ، العدد ٣٧٥٨/ الهيئة الجزائية / ٢٠١٩.

(٤) يُنظر: رشيدة بوكر ، مصدر سابق ، ص٢١٣.

الإجرامية ، والنتيجة الإجرامية في الجرائم الإلكترونية بصورة عامة تتحقق بالوصول إلى المعلومات سواء تم تحقيق هذه الجريمة عن طريق المنصات الإلكترونية المثبتة على جهاز الحاسب الآلي أم أي جهاز إلكتروني أخر أم لا، ومسألة تحقق النتيجة الإجرامية مسألة جدل بين أنصار المذهب المادي وأنصار المذهب القانوني ، حول تحديد جريمة الدخول للمنصات الإلكترونية دون ترخيص هل تعد جريمة مادية متخذه مظهراً خارجياً أم جريمة شكلية تتحقق بمجرد الدخول للمنصات الإلكترونية من دون الوصول للنتيجة[١]، من أجل توضيح الجدل الحاصل بين المذهبين نبّين المدلول المادي للنتيجة الاجرامية بوصفها ظاهرة مادية أم ظاهرة قانونية .

النتيجة الإجرامية بوصفها ظاهرة مادية تتمثل في الاعتداء على حق يحميه القانون ويتضمنه النص التشريعي ، والنتيجة في المدلول القانوني عنصراً من عناصر الركن المادي للجريمة ؛ وأن المشرع يُجّرم الاعتداء على الحق أو المصلحة الجديرة بالحماية اما من دون الاعتداء لا يكون للتجريم محل ، وإذا كانت النتيجة كفكرة قانونية فإن الامر يختلف في خصوص النتيجة في مدلولها المادي ، فإذا كانت النتيجة في هذا المدلول تبدو واضحة في كثير من الجرائم إلا أن هناك عدداً من الجرائم تفتقر فيه النتيجة لهذا الوضوح ،مثل الجرائم السلبية التي تقع بمجرد الامتناع دون أن يكون لهذا الامتناع أثر خارجي ، كامتناع الأم عن إرضاع صغيرها[٢].

هذا فيما يتعلق بالمظهر المادي والقانوني فضلاً عن ان بعض التشريعات اكتفت بمجرد الدخول إلى النظام الإلكتروني ، ولم تشترط أن يكون النظام الإلكتروني مشفراً بكلمة مرور من أجل حمايته من قبل الآخرين وبعض الاشخاص تبقى منصاتهم الإلكترونية مفتوحة طوال الوقت ومن ثم أي محاولة دخول لمنصاتهم واستخدامها والاطلاع على معلوماتهم تعد جريمة [٣] وهذا ما ذهب إليه القانون الفرنسي رقم (١٣٣٦)لسنة (١٩٩٢)النافذ عام (١٩٩٤)في المادة (١/٣٢٣)[٤] ، وقانون مكافحة جرائم تقنية المعلومات الإماراتي رقم (٢)لسنة (٢٠٠٦)في المادة

---

(١) يُنظر: د. محمود احمد محمد القرعان ، الجرائم الإلكترونية ، ط١، دار وائل للنشر والتوزيع ، الاردن ، ٢٠١٧، ص٣٤-٣٥.

(٢) يُنظر: د. محمد عبيد الكعبي ، الحماية الجنائية للتجارة الإلكترونية ، دار النهضة العربية ، ٢٠١٠ ، ص٤٤٣،

(3) Alain Bensoussan: lntemet, aspects juridiquse, ed. Hermes, 1998, p. 198.

(٤) تنص المادة ١/٣٢٣ من قانون العقوبات الفرنسي رقم ١٣٣٦ لسنة ١٩٩٤على (الوصول إلى نظام المعالجة أو البقاء فيه بشكل احتيالي في كل أو جزء من نظام المعالجة ويُعاقب على المعالجة الآلية للبيانات بالسجن لمدة عامين وغرامة قدرها ٦٠ ألف يورو عندما ينتج عن ذلك حذف أو تعديل البيانات الموجودة في النظام ، أو العبث بعمل هذا النظام ، والعقوبة هي السجن لمدة ثلاث سنوات و ١٠٠٠٠٠يورو غرامة ، عندما

(١/٢) [١] ، وتمكن الجاني من الدخول عن طريق اختراق برامج الحماية للحاسب الالي ، والحصول على الشفرة الخاصة بالحاسب الالي مما سمح لنفسه بالدخول والتجوال بكل حرية بغض النظر عن وصوله للمعلومات محل الحماية من عدمها ، لان علة التجريم هي حماية المعلومات من الوصول اليها والمساس بسلامتها، وذلك لان هذه الجريمة تمثل عدواناً محتملاً على الحق المحمي[٢] ، وبعض التشريعات تتطلب لتحقق النتيجة الإجرامية الحصول على المعلومات كشرط لقيام الجريمة وليس مجرد الدخول ، ومنها الولايات المتحدة الإمريكية إذ تعاقب على الدخول والحصول على المعلومات في المادة (١٠٣٠/أ | ١) والمادة (١٠٣٠/أ|٢) من القانون الفيدرالي لجرائم الحاسب الآلي لسنة ١٩٨٤ المعدل ، اما المادة (١٠٣٠/أ| ٣) فقد عاقبت على مجرد الدخول دون ترخيص إلى الحاسبات الآلية داخل الحكومة الفيدرالية لكنها اشترطت في الدخول أن يؤثر في مصالح الحكومة وان تكون الحاسبات ترتبط بها بأي شكل من الاشكال [٣] .

ثالثا: العلاقة السببية في جريمة الدخول للمنصات الإلكترونية دون ترخيص.

العلاقة السببية هي العنصر الثالث من عناصر الركن المادي ، يتم خلالها مساءلة الجاني من عدمه ، لأنها تمثّل الصلة التي تربط بين السلوك الاجرامي والنتيجة الإجرامية ، إذ يتم من خلال العلاقة السببية إثبات ارتكاب الفعل وهو سبب في حدوث النتيجة الإجرامية ، كما ان وجود العلاقة السببية بين السلوك والنتيجة شرط أساسي في تحقق المساءلة الجزائية للجاني ، الذي تحققت النتيجة الاجرامية نتيجة لسلوكه الإجرامي ، وان العلاقة السببية تحقق تلازماً مادياً بين السلوك والنتيجة الإجرامية مما يؤدي إلى توقف مسؤولية الجاني [٤] ، ولا يكون مسؤولاً عن النتيجة التي تحققت ونفي العلاقة السببية يؤدي إلى انتفاء المسؤولية الجزائية عن الجاني في الجرائم غير العمدية لأنه لا يتصور الشروع في الجرائم غير العمدية ، على الرغم من أن جريمة الدخول للمنصات الإلكترونية جريمة شكلية تتحقق بمجرد ارتكاب السلوك المادي من دون

تكون الجرائم المنصوص عليها في الفقرتين الأوليتين قد ارتكبت ضد نظام المعالجة الآلية للبيانات الشخصية التي تنفذها الدولة ، وتزيد العقوبة إلى السجن خمس سنوات وغرامة قدرها ١٥٠ ألف يورو.

(١) تنص المادة ١/٢ من قانون مكافحة جرائم تقنية المعلومات الإماراتي رقم ٢لسنة ٢٠٠٦ على أن (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).

(٢) يُنظر: محمد كمال محمود الدسوقي ، مصدر سابق ، ص٧٦.

(٣) يُنظر: د. محمد عبيد الكعبي ، الحماية الجنائية للتجارة الإلكترونية ، مصدر سابق ، ص٤٤٦.

(٤) يُنظر: د. أسامة فرج الله محمود الصباغ ، مصدر سابق ، ص٢٠٠.

الحاجة لتحقق النتيجة الإجرامية ، وعليه لا يعد مجرد حصول الشخص على كلمة المرور للغير جريمة ولا يعد ذلك شروعاً في الجريمة [1] .

نلاحظ مما تقدم أن للركن المادي في جريمة الدخول للمنصات الإلكترونية دون ترخيص ثلاثة عناصر وهي السلوك الإجرامي والنتيجة الإجرامية والعلاقة السببية بينهما ، ويتحقق السلوك الإجرامي من خلال امتناع الفاعل عن قطع الاتصال والخروج من المنصات الإلكترونية أو أي جهاز إلكتروني أخر ، ولا يمكن معاقبة الشخص الذي يقوم بالدخول عن طريق الصدفة أو الخطأ ويبادر بالخروج ، لكن في حالة دخول الجاني حتى وان كان مسموح له لكن تجاوز حدود التصريح ، ففي هذه الحالة تتحقق الجريمة أما النتيجة الاجرامية في بعض التشريعات جرّمت مجرد الدخول دون الحصول على المعلومات مثل فرنسا والامارات العربية المتحدة والبعض الاخر من التشريعات جرمت الحصول على المعلومات نتيجة الدخول للنظام الإلكتروني ، اما العلاقة السببية فإنها من الصعب تحديدها بسبب التطور المستمر وتعدد أساليب الدخول والاتصال بين مختلف الاجهزة الالكترونية ومنصاتها ، فضلاً عن قيام الجاني بإدخال اوامر مختلفة من اجل تحقق النتيجة التي ينوي الحصول عليها ، يؤدي إلى صعوبة معرفة العلاقة السببية بين السلوك والنتيجة في العالم الافتراضي إلا ما اتخذ مظهراً مادياً وتم اثباته نتيجة لسلوك الجاني ، كما لا يتصور الشروع في جريمة الدخول للمنصات الإلكترونية دون تصريح لأنها جريمة من الجرائم الشكلية.

الفرع الثاني

الركن المعنوي في جريمة الدخول للمنصات الإلكترونية دون ترخيص.

يتمثل الركن المعنوي في جريمة الدخول للمنصات الإلكترونية دون ترخيص بالحالة النفسية للجاني مع وجود علاقة تربط بين ماديات الجريمة وشخصية الجاني(٢) ، ولا يكفي لتحقق جريمة الدخول للمنصات الإلكترونية تحقق الركن المادي فحسب لابد من تتحقق الركن المعنوي المتمثل بالقصد الجرمي العام بعنصريه العلم والإرادة لأنها من الجرائم العمدية ، فضلاً عن بعض التشريعات يشترط فيها تحقق القصد الجرمي الخاص المتمثل بغاية الجاني .

---

(١) يُنظر: د. محمد علي سويلم ، مكافحة الجرائم الإلكترونية (دراسة مقارنة بالتشريعات العربية والاجنبية) ، ط١، دار المطبوعات الجامعية ، دون مكان نشر، ٢٠١٩ ، ص١٠٧.

(٢) يُنظر: د. خالد ممدوح إبراهيم ، فن التحقيق الجنائي في الجرائم الإلكترونية ، ط١، دار الفكر الجامعي ، الاسكندرية ، ٢٠٠٩، ص٥٣،

أولاً: القصد الجرمي العام في جريمة الدخول للمنصات الإلكترونية دون ترخيص

يتمثل القصد الجرمي العام في جريمة الدخول للمنصات الإلكترونية من دون ترخيص من عنصرين هما العلم والإرادة ، أن يكون الجاني مدركً لحقيقة السلوك الإجرامي الذي يقوم به ، وعليه أن يعلم بحقيقة الدخول عمداً إلى المنصات الإلكترونية وغير مرخص له في الدخول إليها ، أو يكون الدخول للمنصات الإلكترونية بخطأ غير عمدي ويعلم أن دخوله غير مشروع [١] ، ورغم ذلك يصر على الدخول ولم يبادر في الخروج عند علمه بأن دخوله غير مرخص ، إذ عليه أن يعلم بخطورة سلوكه الإجرامي على المحل الذي يناله الاعتداء عند الدخول للمنصات الإلكترونية دون ترخيص وارتكابه الجريمة[٢] كذلك على الجاني العلم بالتكييف الذي تتصف به الوقائع التي تكتسب الأهمية في نظر القانون [٣].

اما في حالة اعتقاد الجاني ان الدخول للمنصات الإلكترونية مشروع ومسموح به وتم ذلك بطريق الخطأ أو الصدفة أو السهو ، أو كان لا يعلم انه محظور عليه الدخول وبادر فوراً بالخروج ففي هذه الحالة ينتفي القصد الجرمي العام ، أما اذا لم يخرج رغم علمه بأنه محظور عليه الدخول ففي هذه الحالة يتحقق القصد الجرمي العام في حقه[٤] .

يتبين مما سبق ان الجاني عليه ان يعلم بأنه غير مسموح له الدخول للمنصات الإلكترونية أو أي جهاز إلكتروني أخر ويجب ان تتوافر الإرادة لدى الجاني وتتجه إلى ارتكاب الفعل الاجرامي ، وأن إرادة الجاني وحدها كافية لتحقيق السلوك الاجرامي من خلال الدخول للمنصات الإلكترونية دون ترخيص ، ودون تحقيق نتيجة معينه لأنها من الجرائم الشكلية التي لا يتطلب فيها تحقيق النتيجة ، ففي هذه الحالة يتحقق القصد الجنائي العام بعنصريه العلم والإرادة الذي

---

(١) يُنظر: د. محمد علي سويلم ، مكافحة الجرائم الإلكترونية ، مصدر سابق ، ص١١٥.

(٢) يُنظر: د. محمد علي سويلم ، جرائم الكمبيوتر والانترنت (دراسة مقارنة) ، ط١ ، دار المطبوعات الجامعية ، ٢٠١٩ ، ص٢٤٥.

(٣) يُنظر: د. فتحي محمد أنور عزت ، الحماية الموضوعية والجزائية والحق في الخصوصية والكومبيوتر والانترنت في نطاق التشريعات الوطنية والتعاون الدولي ، دار النهضة العربية ، مصر ، ٢٠٠٧، ص١٣١.

(٤) يُنظر: د. عبدالفتاح بيومي حجازي ، جرائم الكمبيوتر والانترنت في التشريعات العربية (دراسة مقارنة مع التطبيق على نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية) ، مصدر سابق ، ص٣٢.

يؤدي لقيام الجريمة ، ولا عبرة للباعث في ارتكاب الجريمة لأن الباعث في هذه الحالة لا يكون سوى محاوله للتفوق على الوسائل التقنية وقهر النظام [١] .

يتضح لنا مما تقدم ان القصد الجرمي العام يتحقق بتوافر عناصره العلم والارادة أي ان الجاني يعلم ان دخوله غير مشروع ورغم ذلك يصر على الدخول وعدم الخروج من المنصات الإلكترونية ، مما يؤدي إلى تحقق النتيجة وهي الاعتداء على المعلومات ، وبالتالي تتم معاقبة الجاني ، في حين اذا كان الدخول بطريق الخطأ أو السهو أو الصدفة ويبادر الجاني بالخروج عند علمه ففي هذه ينتفي القصد الجرمي ولا تتم مساءلة الجاني .

ثانياً: القصد الجرمي الخاص في جريمة الدخول للمنصات الإلكترونية دون ترخيص

بعض التشريعات لا تتطلب القصد الجرمي الخاص واكتفت بالقصد الجرمي العام ومنها فرنسا والامارات ، إلا أنها تتطلب حصول نتيجة إجرامية معينة أو تقع الجريمة بباعث خاص، كما ان بعض الجرائم تستلزم ذلك بحسب طبيعتها حتى ولم يشير إليه المشرع صراحة في نصوص التجريم ، على العكس من بعض التشريعات التي نشير إليها على سبيل الاستدلال على الرغم من أنها خارج نطاق مقارنة الدراسة والتي تتطلب توافر القصد الجنائي الخاص إلى جانب القصد الجنائي العام والسبب في توافر القصد الجنائي الخاص لتشديد العقوبة ، نجد المشرع الاسترالي نص على تشديد العقوبة عندما يرتكب الجاني فعل الدخول بقصد الاضرار بالغير[٢] ، وفي الدنمارك أيضاً تم تشديد العقوبة على فعل الدخول متى كان ذلك بنية الاحاطة بالمعلومات التي تتعلق بالأسرار المتعلقة بعمل إحدى الشركات ، اما بالنروج فقد كان التشديد ملحوظ عندما يرتكب الجاني فعل الدخول بنية الحصول له أو للغير ربح غير مشروع أو يلحق الضرر بالغير نتيجة اطلاعه على المعلومات التي يحتويها النظام ، كما تطلب قانون الجرائم الإلكترونية البرتغالي لسنة ١٩٩١ التي " تعاقب كل من يقوم بالدخول إلى نظم شبكات المعلومات بنية الحصول له أو للغير على ربح أو فائدة غير مشروعة " ، وتشدد العقوبة متى كان هذا الربح أو الفائدة مرتفعين بصورة نسبية كبيرة[٣].

---

(١) يُنظر: رشيدة بوكر ، مصدر سابق ، ص٢٣٧.

(٢) يُنظر: محمد كمال محمود الدسوقي ، مصدر سابق ، ص٨١.

(٣) يُنظر محمد عبيد الكعبي ، الحماية الجنائية للتجارة الإلكترونية ، مصدر سابق ، ص٤٨٨-٤٨٩.

يتضح لنا مما تقدم ان التشريعات التي تتطلب قصد جرمي خاص بجانب القصد الجرمي العام ما هو إلا لتشديد العقوبة والباحث يجد ان توافر القصد الجرمي العام بعنصرية العلم والإرادة يكفي لتحقق الجريمة ، أضف إلى ذلك ان جريمة الدخول للمنصات الإلكترونية دون ترخيص هي جريمة عمدية وشكلية من جرائم الخطر أي تتحقق بمجرد الدخول دون تحقق النتيجة في بعض التشريعات المقارنة ، فضلا عن أن من يقوم بهذه الجريمة من الجناة الذين يتمتعون بمهارات عالية في المجال التقني ، ونشاط الجاني فيها هو نشاط تقني وفني و يحتاج إلى تدريب وممارسة من قبل المخترقين ، والجاني في هذه الحالة عليه ان يكون عالم بخطورة فعله ويجرّمه القانون ، وعلى الرغم من ذلك يصر على ارتكاب الفعل ويقوم بالدخول للمنصات الإلكترونية ، والباحث يتفق مع التشريعات التي تتطلب القصد الجرمي العام بعنصريه العلم والإرادة التي تكفي لتحقق النتيجة الاجرامية لأنها من جرائم الخطر.

المبحث الثاني

جريمة إتلاف معلومات المنصات الإلكترونية

تعد جريمة إتلاف المعلومات من أكثر الجرائم انتشاراً لنظام الحاسب الآلي أو المنصات الإلكترونية أو أي جهاز إلكتروني آخر مثبته عليه ، وتتخذ هذه الجريمة عدة حالات منها أن يكون الفعل المجرم فيها هو الإتلاف للمعلومات الذي يجعل منها غير صالحة للاستعمال ،أما الحالة الثانية تتمثل بدخول الجاني إلى حاسب آلي خاص للغير ، وقيامه بتغيير المعلومات و البرامج سواء بالزيادة أم النقصان أم الإضافة أم الحذف ، وتُعد الجريمة في هذه الحالة متحققة ، والجاني يعاقب حتى وأن لم يسبب ضرر عند قيامه بتغيير المعلومات ، والسبب في ذلك هو أن الحماية تكون مقررة لمصلحة المجنى عليه وجهازه، اما الحالة الثالثة التي تتمثل بالفعل الإجرامي لمحو المعلومات و البرامج وحرمان صاحبها منها ، ويتم ذلك عن طريق تعديل المعلومات أو التغيير في مسارها أو عن طريق نشر الفايروسات الضارة من أجل ابطاء حركة المنصات الإلكترونية ، وان الجناة يستخدمون الأساليب والوسائل في الجرائم الإلكترونية لإتلاف معلومات المنصات الإلكترونية المثبتة على الحاسب الالي ، المعلومات المعالجة والمخزنة آلياً والتلاعب بها ؛ وتختلف تلك الأساليب أيضاً باختلاف أغراض الجناة من حالة لأخرى ، وللنصوص الخاصة في جريمة الإتلاف أهمية بالغة في توفير الحماية الجزائية للمال

المادي وعدم فقدانه منفعته أو صلاحيته للاستعمال أم الغرض الذي أعد من أجله ، وقد جاء تجريم هذه الافعال في القسم ١٨من قانون الولايات المتحدة الامريكية بعد تعديله للمادة ١٠٣٠/أ عام ١٩٩٦التي جرّمت الإتلاف الإلكتروني ، في البند الأول من الفقرة الخامسة التي نصت على " تعديل المعلومات والبرامج والشفرات والأوامر داخل أنظمة الحاسبات الآلية ، مما يترتب عليه أضرار يلحق للحاسب الآلي الذي يتمتع بالحماية متى ما كان إحداث هذا الضرر قد تم عمداً" ، وأن هذه المادة مقتصره على الأنظمة الحكومية وإداراتها أو التي تستخدم لصالحها قبل التعديل ، أما المشرع الفرنسي عدَّ جريمة الإتلاف جريمة مستقلة بذاتها ، وذلك في المادة (٤٦٢) من قانون العقوبات الفرنسي رقم ١٩ لسنة ١٩٨٨، بعد دمج القانون القديم بالقانون رقم ١٣٣٦لسنة ١٩٩٤النافذ الذي خصص له مجموعة مواد جاءت تحت عنوان (الاعتداءات على نظم المعالجة الالية من المادة ١/٣٢٣إلى ٧/٣٢٣) التي جرّمت العديد من الافعال المعاقب عليها قانوناُ ومنها جريمة الاتلاف ، والمشرّع الاماراتي جرّم أفعال الإتلاف في نص الفقرة الثانية من المادة الثانية من مرسوم بقانون اتحادي رقم ٥لسنة ٢٠١٢[١] ، أما المشرع الأردني جرّم فعل الإتلاف في الفقرة (ب) من المادة الثالثة من قانون جرائم أنظمة المعلومات رقم ٣٠لسنة ٢٠١٠المؤقت[٢] ، وشدد عقوبة الحبس من دون أن يتطرق لعقوبة الغرامة في جريمة الإتلاف في الفقرة (ب) من المادة الثالثة من القانون رقم ٢٧ لسنة ٢٠١٥[٣] ، اما بالنسبة للمشرع العراقي فقد

(١) يُنظر: نص الفقرة الثانية من المادة الثانية من مرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢الاماراتي ، التي تنص على أنه إذا ترتب على الفعل إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أي بيانات أو معلومات ، يعاقب بالحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن مائة وخمسين الف درهم ولا تجاوز سبعمائة وخمسون الف درهم أو بإحدى هاتين العقوبتين.

(٢) يُنظر : نص الفقرة (ب) من المادة الثالثة من قانون أنظمة المعلومات المؤقت رقم ٣٠ لسنة ٢٠١٠التي تنص على انه إذا ترتب عن الفعل إلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو توقيف أو تعطيل عمل نظام معلومات ، يعاقب بالحبس مدة لا تقل عن أسبوع ولا تزيد على ثلاثة أشهر أو بغرامة لا تقل عن (١٠٠) مائة دينار ولا تزيد على (٢٠٠) مائتي دينار أو بكلتا هاتين العقوبتين.

(٣) يُنظر: نص الفقرة (ب) من المادة الثالثة من قانون الجرائم الإلكترونية الاردني رقم ٢٧ لسنة ٢٠١٥التي تنص على انه إذا ترتب عن الفعل إلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو توقيف أو تعطيل عمل الشبكة المعلوماتية أو نظام معلومات الشبكة

جـرّم أفعـال الإتـلاف فـي المـادة (٤٧٧) مـن قـانون العقوبـات العراقـي رقـم (١١١) لسـنة ١٩٦٩المعـدل بفقرتهـا الاولـى[١] ، والمـادة المشـار إليهـا اعـلاه لـم تتطـرق إلـى تجـريم أفعـال إتـلاف معلومـات المنصـات الإلكترونيـة ، وعليـه سنقسـم هـذا المبحـث علـى مطلبـين نتنـاول فـي المطلـب الأول التشـريعات المقارنـة وموقفهـا مـن جريمـة إتـلاف معلومـات المنصـات الإلكترونيـة ونتنـاول فـي المطلـب الثـاني أركـان جريمـة إتـلاف معلومـات المنصات الإلكترونية .

المطلب الأول

موقف التشريعات المقارنة من جريمة إتلاف معلومات المنصات الإلكترونية

العديد من البلدان ذهبت إلى تجريم الاعتداءات المختلفة التي تقع في المجال الإلكتروني ومن هذه الجرائم جريمة إتلاف معلومات المنصات الإلكترونية بمختلف أنواعها ، إذ نجد تشريعات دول المقارنة جرّمت أفعال الإتلاف من خلال تعديل قوانينها العقابية عن طريق تضمين نصوص عقابية تعالج الجرائم الإلكترونية ، كما في القانون الامريكي وقانون العقوبات الفرنسي ، في حين جرّمت بعض الدول الإتلاف من خلال تشريعات خاصة في الجرائم الإلكترونية ، مثل الاردن والامارات ، وبعض الدول العربية لم تسن تشريعات خاصة تجرم الجرائم الإلكترونية ، مثل العراق وعليه سنقسم هذا المطلب على فرعين نتناول في الفرع الاول موقف التشريعات الاجنبية المقارنة من جريمة إتلاف معلومات المنصات الإلكترونية ونتناول في الفرع الثاني موقف التشريعات والاتفاقيات المقارنة من جريمة إتلاف معلومات المنصات الإلكترونية .

الفرع الاول

موقف التشريعات الاجنبية المقارنة من جريمة إتلاف معلومات المنصات الإلكترونية

المعلوماتية ، فيعاقب الفاعل بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن ٢٠٠ مائتي دينار ولا تزيد على ١٠٠٠ألف دينار

(١) يُنظر: الفقرة الاولى من المادة (٤٧٧) التي تنص على " كل من هدم أو خرب أو أتلف عقاراً أو منقولاً غير مملوك له أو جعله غير صالح للاستعمال أو أضر به أو عطله بأية كيفية كانت ، يعاقب بالحبس مدة لا تزيد على سنتين وبغرامة لا تزيد على مائتي دينار ، أو بإحدى هاتين العقوبتين.

صدرت العديد من التشريعات في الولايات المتحدة الامريكية منها على المستوى الفيدرالي والاخرى على مستوى الولايات ، اما على المستوى الفيدرالي الذي تمثّل بنشاط من قبل لجنة الكونجرس الامريكي الخاصة بحماية استخدام الحاسوب الذي اعدت له الدراسات والاحصاءات من قبلها ، وتقديمها مشروع (قانون حماية الحاسوب سنة (١٩٨٤) والغاية من هذا المشروع هو مواجهة انتشار الجريمة عبر الانترنت [١] ، وعندما تم عرض المشروع ودراسته جرت عليه تعديلات جوهرية في احكامه وبعد سلسلة من التعديلات والاضافات لم يصدر حسب اقتراح اللجنة إنما صدر باسم قانون غش الحاسوب وإساءة استخدامه لعام ١٩٨٤، إذ لم تعاقب الفقرة الثالثة من المادة(١٠٣٠/أ) على تجريم إتلاف البيانات والبرامج بصورة عامة ، وانما اقتصر ذلك على تجريم الاتلاف الذي يؤدي إلى إعاقة أنظمة الحاسب الالي عن العمل ، بينما جرّمت الفقرة الثانية من المادة ذاتها من التشريع الفيدرالي الامريكي إتلاف البيانات التي تؤدي إلى إعاقة الحكومة عن إستخدام أنظمة الحاسبات الالية[٢].

وتدخل المشرّع الامريكي سنة ١٩٩٤لوضع حماية ضد الاتلاف الإلكتروني ومعاقبة الأشخاص الذين يرتكبون أفعال عمدية تحدث تشويشاً أو تعترض المعلومات الخاصة بالدفاع الوطني سواء بالتعييب أم التدمير بالسجن لمدة عشر سنوات وبغرامة لا تزيد على عشرة آلاف دولار"[٣] .

وتم تعديل المادة ١٠٣٠/أ التي كانت مقتصرة على الانظمة الإلكترونية التابعة للحكومة وإداراتها بصدور قانون حماية بنية المعلومات القومية عام ١٩٩٦ ، التي توسعت من نطاق حماية الأنظمة الإلكترونية ، لتشمل معها العديد من الانظمة التابعة للمؤسسات الاقتصادية التي تستخدم في مجال التجارة والاتصالات المحلية بين الولايات والدول الاخرى ، والذي أطلق عليها الحاسبات الآلية التي تتمتع بالحماية ، وان النص امتد إلى شمول أعمال الإتلاف التي تقع

---

(١) يُنظر: د. خالد ممدوح إبراهيم ، الحماية القانونية للعلامات التجارية مدنياُ وجنائياً ، دار الفكر الجامعي ، ٢٠١٩، ص ٣٤٤.

(٢) يُنظر .د . علي عبود جعفر ، مصدر سابق ، ص٥٥٠.

(٣) يُنظر .د. نائلة عادل محمد قورة ، جرائم الحاسب الالي الاقتصادية (دراسة نظرية وتطبيقية) ، ط١ ، منشورات الحلبي الحقوقية ، ٢٠٠٥، ص٢١٧.

عمداً من الاشخاص المصرح لهم بالدخول إلى النظام الإلكتروني أو المنصات الإلكترونية المثبتة على جهاز الحاسب الآلي[١].

و اما على مستوى الولايات فقد شرّعت قوانين خاصة تجرّم أفعال إتلاف المعلومات فضلاً عن تعديل قوانين بعض الولايات ،إذ يحتوي النص على تجريم الانشطة لجرائم الحاسب الآلي مع وجود تباين بين القوانين ، وهذا التباين يكمن من حيث صور السلوك المجرّم من جهة أو من آلية التعامل مع محل الاعتداء[٢] ، وبعض قوانين الولايات نصت على المساواة بين معطيات الحاسب الآلي والأموال المادية من ناحية الحكم القانوني ، وبهذا يمكن تطبيق النصوص التقليدية على جرائم الحاسب الالي ، لأنها تكون في هذه الحالة تستهدف المعطيات التي تتخذ حكم الاموال المادية بنص القانون الصريح ، وقانون ولاية ألآسكا الجديد أدخل الإتلاف المعلوماتي ضمن الاموال التي تخضع في حكمها لنصوص الاضرار بالمال فضلاً عن انه قد ساوى بين غش الانسان والآلة، أما قانون ولاية فرجينيا فقد نص على عدَّ خدمات الحاسب الالي أو خدمات المعالجة الالية للمعلومات المخزنة ذات صلة بذلك المال التي يمكن تطبيق النصوص التقليدية عليها[٣] ، كما ان أغلب الولايات الاخرى ذهبت إلى سن نصوص صريحة تجرّم أنشطة إساءة استخدام الحاسوب ومن هذه الولايات ولاية فلوريدا الذي جرم قانونها " أي شخص يقوم بإرادته وعلى علم ومن دون تصريح في العبث أو التعديل في معدات وتجهيزات مستخدمة أو سيتم استخدامها في الكومبيوتر أو نظامه أو البرامج أو شبكة الكومبيوتر ، يعد مرتكباً لجريمة ضد معدات الكومبيوتر"[٤].

يتضح لنا مما تقدم أن المشرّع الامريكي في ضل القانون الفيدرالي لم يعاقب على الإتلاف الإلكتروني بصورة عامة بل فقط إذا تسبب الإتلاف إعاقة استخدام الحكومة لأنظمة الحاسبات الآلية في ضل القانون الصادر لسنة (١٩٨٤) ،وتم تعديل القانون في عام (١٩٩٦) ليشمل بعدها جميع الافعال التي تؤدي إلى الاضرار بالحاسب الآلي وحسناً فعل المشرّع ، ويرى الباحث امكانية تعرض معلومات المنصات الإلكترونية للإتلاف ، كما يمكننا تطبيق نصوص القانون الامريكي على جريمة إتلاف المعلومات التي تتعرض لها المنصات الإلكترونية .

([1]) Heyman (Stephen p), legislating computer crime,h.g.1.,vol,1997,p.379.

([٢]) يُنظر: د. علي عبود جعفر ، المصدر نفسه ، ص١٤٣.

([٣]) يُنظر: محمود محمد محمود جابر ، مصدر سابق ، ص١٩٥.

([٤]) يُنظر: د. عمار عباس الحسيني ، مصدر سابق ، ص٢١٢.

اما المشرع الفرنسي فقد جرّم حالات الاتلاف العمدي لمعلومات الحاسب الالي في قانون العقوبات الفرنسي القديم رقم (١٩) لسنة (١٩٨٨) وشمل بعض الجرام الإلكترونية الذي عدَّ جريمة إتلاف معلومات المنصات الإلكترونية جريمة مستقلة بذاتها[١] ، وذلك بموجب فقرات المادة ٤٦٢[٢].غير ان هذه المادة لم تسلم من الانتقادات الفقهية مما حدى بالمشرع الفرنسي إلى تلافي هذه الانتقادات ، في قانون العقوبات الفرنسي الجديد رقم (١٣٣٦) لسنة (١٩٩٢) والمعمول به منذ عام (١٩٩٤)، والذي اتى بفصل جديد تحت عنوان " الاعتداءات على نظام المعالجة الآلية للمعطيات" في المواد (١/٣٢٣ إلى ٣٢٣/ ٧) نتيجة دمج نصوص قانون العقوبات رقم (١٩) لسنة (١٩٨٨) مع نصوص قانون العقوبات الفرنسي الجديد والذي نص على إتلاف المعطيات الموجودة داخل النظام[٣] ، كما تم تعديل الفصل الثالث الذي كان خاص في الجرائم الماسة بنظم المعالجة الآلية من خلال القانون رقم (٥٧٥) لسنة (٢٠٠٤) إذ شدد العقوبتين الحبس والغرامة المقررة للتلاعب في المعلومات ، وحسب ما جاء بنص المادة (٣/٣٢٣) كما يلي " كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية للمعطيات أو

---

(١) يُنظر: د. فتوح الشاذلي ، عفيفي كامل عفيفي ، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون (دراسة مقارنة) ، توزيع منشأة المعارف بالاسكندرية ، ٢٠٠٣ ، ص٢٠٩.

(٢) يُنظر: نص المادة (٤٦٢) من قانون العقوبات الفرنسي رقم ١٩ لسنة ١٩٨٨.

أ- نصت الفقرة الثانية من المادة (٤٦٢) على انه " كل من ولج أو مكث في نظام المعالجة الالية للبيانات أو في جزء منه بطريق الغش يعاقب بالحبس لمدة تتراوح بين شهرين وسنة والغرامة تتراوح بين ٢٠٠٠و٥٠٠٠فرنك أو بإحدى هاتين العقوبتين ، فإذا نجم عن ذلك محو أو تعديل في البيانات التي يحويها النظام أو نظام تشغيله تكون العقوبة الحبس لمدة تتراوح بين شهرين وسنتين والغرامة التي تتراوح بين ١٠٠٠٠و١٠٠٠٠٠ فرنك".

ب- اما الفقرة الثالثة من المادة (٤٦٢) فقد نصت على ان " كل شخص يسبب عمداً أو بدون مراعاة لحقوق الغير تعطيل أو إفساد تشغيل نظام المعالجة الآلية للبيانات سيعاقب بالحبس مدة تتراوح بين ثلاثة أشهر وثلاثة سنوات والغرامة التي تتراوح بين ١٠٠٠٠و ١٠٠٠٠٠فرنك أو إحدى هاتين العقوبتين ".

ت- اما الفقرة الرابعة من المادة (٤٦٢) فقد نصت على أنه" كل من أدخل عمدا مباشرة أو بطريق غير مباشر وبدون مراعاة لحقوق الغير بيانات في نظام المعالجة الآلية أو محا أو عدل في البيانات التي يحويها أو نقلها يعاقب بالحبس مدة تتراوح بين ثلاثة شهور وثلاث سنوات أو بغرامة تتراوح بين ٢٠٠٠ و ٥٠٠٠٠٠فرنك أو بإحدى هاتين العقوبتين". يُنظر: شمسان ناجي صالح الخيلي ، الجرائم المستخدمة بطرق غير مشروعة لشبكة الإنترنت (دراسة مقارنة) ، دار النهضة العربية ، القاهرة ، ٢٠٠٩، ص٢٢٧- ٢٢٨.

(٣) يُنظر: د. علي عبود جعفر ، مصدر سابق ، ص٥٥٠.

محا أو عدل بطريق الغش المعطيات التي يتضمنها يعاقب بعقوبة الحبس حتى ٥سنوات ، وبغرامة تقدر ب ٧٥٠٠٠يورو"[١] .

نلاحظ مما تقدّم أن المشرّع الفرنسي قام بالعديد من التعديلات في قانون العقوبات من أجل توفير الحماية الجزائية ضد جريمة إتلاف المعلومات إذ نجد الفقرة الثالثة من المادة ٤٦٢ جرّمت حالات الإتلاف الذي ينصب على المكونات المادية للحاسب الالي سواء بتعطيل أم افساد لنظام تشغيل المعالجة الالية وتعطيل المعلومات في هذه المادة يشمل جميع السلوكيات التي تؤدي إلى الإعاقة فضلاً عن ان هذا التعطيل كان بالإتلاف أو التخريب على حد سواء ، وفي الفقرة الثالثة من المادة نفسها تضمنت إدخال معلومات في الاصل لم تكن موجودة سابقا سواء كان هذا الادخال مباشراً أم غير مباشر والغرض من هذه المعلومات التشويش الذي يؤدي على صحة المعلومات الاصلية ، فضلاً عن ذلك وجود عبارة من دون مراعاة حقوق الغير الامر الذي لم يوفق فيه المشرع الفرنسي والباحث يرى امكانية الخلاف الفقهي بخصوص حق الغير الذي يوسع من دائرة الخلاف على عكس المحو للمعلومات سواء جزئياً أو كلياً ففي هذه العبارة كان موفق المشرع في الفقرة الرابعة من ذات المادة ، ونؤيد ما جاء في الفقرة الثانية والرابعة من المادة ٤٦٢من قانون العقوبات القديم رقم (١٩)لسنة (١٩٨٨)، اما ما جاء في قانون العقوبات الجديد رقم (١٣٣٦) لسنة (١٩٩٤) في المواد (١/٣٢٣ إلى ٧/٣٢٣) الذي ادمج وجاء بفصل جديد يعالج الاعتداءات على نظم المعالجة الالية إذ نجد المادة ١/٣٢٣ جرمت الاتلاف الإلكتروني لكن الملاحظ عليها لم تكن العقوبة مشددة في التعديل الاخير لقانون العقوبات رقم (٥٧٥) لسنة (٢٠٠٤) الذي شدد عقوبة الحبس والغرامة ، فضلا عن تبديل العملة من الفرنك إلى اليورو التي اعتمدتها فرنسا عام (٢٠٠٢) العملة الوحيدة ونؤيد المشرع الفرنسي في التشديد العقوبتين .

أما اتفاقية بودابست لمكافحة جرائم المعلوماتية لعام ٢٠٠١ فقد تعرضت إلى جريمة الإتلاف وتدمير المعلومات للمنصات الإلكترونية المثبتة على جهاز الحاسب الالي أو أي جهاز الكتروني آخر وذلك في الفقرة الاولى والثانية من المادة الرابعة التي نصت في الفقرة الاولى من المادة الرابعة على أنه " يجب على كل طرف أن يتبنى الاجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية لتجريم ، تبعاً لقانونه المحلي ، إذا أحدث ذلك عمداً ، ودون حق ، أي أضرار ، أو محو ، أو تعطيل ، أو

---

(١) يُنظر: رشيدة بوكر ، مصدر سابق ، ص٢٤٧.

إتلاف ، أو طمس لبيانات الحاسب"[١] ، أما في الفقرة الثانية من المادة ذاتها التي نصت على أنه " يمكن لأي طرف في الاتفاقية الاحتفاظ بالحق في المطالبة بأن السلوك المنصوص عليه في الفقرة الاولى يؤدي إلى أضرار جسيمة"[٢] .

والهدف من وراء تقرير هذا النص الذي أشارت إليه المذكرة التفسيرية في الاتفاقية هو ضمان توفير الحماية المماثلة للمعلومات والبرامج الإلكترونية ، التي تتمتع بها الأشياء المادية ضد الخسائر والاضرار التي تتعرض لها عن عمد، أما المصالح القانونية المحمية هي سلامة وحسن التشغيل وحسن استخدام المعلومات أو برامج الحاسب الآلي المسجلة[٣].

يتضح لنا مما تقدم إن المذكرة التفسيرية غايتها توفير الحماية للمعلومات وبرامج الحاسب الآلي ، من التلف والتدمير و الاضرار التي قد تصيبها ، وحثت الدول على تبني تشريعات تجرّم وتعاقب على هكذا جرائم ، والباحث يؤيد ما جاء بهذه الاتفاقية من أجل التقليل من الجرائم الإلكترونية التي تتعرض لها جميع الدول نتيجة التطور التكنولوجي الحديث.

الفرع الثاني

موقف التشريعات والاتفاقيات المقارنة من جريمة إتلاف معلومات المنصات الإلكترونية

الدول العربية نجدها متفاوتة من دوله إلى اخرى فقد استجابت بعض الدول في تشريع قوانين ضد الجرائم الإلكترونية ، لكن لم يكن مسلكها موحد في هذا الاتجاه منها جرّم مختلف الجرائم الإلكترونية من خلال تشريعات متخصصة مثل الامارات والاردن ، والبعض الآخر لم ينظم ذلك بقانون مثل العراق ، الذي حاول تشريع قانون خاص يكافح أغلب الجرائم الإلكترونية من خلال مشروع قانون الجرائم الإلكترونية العراقي لسنة ٢٠١١، الذي لم يرَ النور إلى الان.

اما ما يتعلق بالاتفاقيات العربية فقد صدرت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في ٢٠١٠/١٢/٢١ عن جامعة الدول العربية في القاهرة والدول العربية ورغبة منها في تقوية التعاون بينها من أجل معاقبة الجناة على الجرائم الإلكترونية وحفظ امن وسلامة مجتمعاتها ، وحرصت الاتفاقية على توفير الحماية للبيانات والمعلومات المعالجة إلكترونياً من جريمة

---

(١) يُنظر: د. هلالي عبد اللاه أحمد ، اتفاقية بودابست لمكافحة جرائم المعلوماتية ، مصدر سابق ، ص٦٨-٦٩.

(٢) يُنظر: د. هلالي عبد اللاه أحمد ، جرائم الحاسب والانترنت بين التجريم الجنائي وآليات المواجهة ، دار النهضة العربية ، ٢٠٠٦ ، ص٢٠٠.

(٣) يُنظر: د. محمد عبيد الكعبي ، الحماية الجنائية للتجارة الإلكترونية ، مصدر سابق ، ص٥١٢.

الإتلاف الإلكتروني ، وجرّمت الاتفاقية أفعال الاعتداء على سلامة البيانات[١] ، في المادة الثامنة من الاتفاقية التي نصت على أنه " تلتزم كل دولة طرف بتجريم الأفعال وفقاً لتشريع كل دوله ونظامها الداخلي "من تدمير أو محو، أو إعاقة ، أو تعديل ، أو حجب بيانات تقنية المعلومات قصداً ، ومن دون وجه حق وللطرف أن يستلزم تجريم الأفعال المنصوص عليها في هذه المادة ، أن تتسبب ذلك بضرر جسيم"[٢]

أما الفقرة (أ) من البند (١) من المادة التاسعة من الاتفاقية جرمت " إنتاج ، أو بيع ، أو شراء ، أو استيراد ، أو توزيع ، أو توفير أي أدوات أو برامج مصممة أو مكيفة لغايات ارتكاب الجرائم المبينة في المادة الثامنة"[٣].

اما الفقرة (ب) من البند (١) من ذات المادة نصت على " تجريم إنتاج ، أو بيع أو شراء ، أو استيراد ، أو توزيع ، أو توفير كلمة سر نظام معلومات ، أو شفرة دخول ، أو معلومات مشابهة ، يتم بواسطتها دخول نظام معلومات ما بقصد استخدامها لأي من الجرائم المبينة في المادة الثامنة"[٤].

يتضح لنا مما تقدّم ان الاتفاقية العربية جرّمت الكثير من التعاملات التي تؤدي إلى إتلاف المعلومات ، والغاية من هذه النصوص هو لإضفاء الحماية الجزائية على البيانات والمعلومات المعالجة إلكترونياً من الإتلاف أو التعديل أو الإعاقة المتعمدة ممن يحاول الاعتداء على معلومات الاخرين .

اما المشرّع الاماراتي فقد جرم أفعال الاتلاف الإلكتروني في المرسوم بقانون إتحادي رقم (٥) لسنة (٢٠١٢) في الفقرة (١) من المادة الثانية التي نصت على " يعاقب بالحبس والغرامة لا تقل عن مائة الف درهم ولا تزيد على ثلاثمائة الف 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 ، في حين تم تشديد العقوبة في الفقرة الثانية من ذات المادة التي تكون العقوبة الحبس مدة لا تقل عن ستة اشهر

---

(١) يُنظر: د. عمار عباس الحسيني ، مصدر سابق ، ص٢٣٤.

(٢) يُنظر: محمود محمد محمود جابر ، مصدر سابق ، ص١٩٧.

(٣) يُنظر: نص الفقرة (أ) من البند (١) من المادة التاسعة من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ، لعام ٢٠١٠.

(٤) يُنظر: نص الفقرة (ب) من البند (١) من المادة التاسعة من الاتفاقية ذاتها

والغرامة التي لا تقل عن مائة وخمسون الف درهم ولا تجاوز سبعمائة الف درهم أو بإحدى هاتين العقوبتين اذا ترتب على أي فعل من الافعال المنصوص عليها بالفقرة (١) من هذه المادة الغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أي بيانات أو معلومات"[١].

وفي المادة الرابعة من القانون ذاته فإنها تنص على ان " تكون العقوبة السجن مدة لا تقل عن خمس سنوات والغرامة التي لا تقل عن خمسمائة الف درهم ولا تجاوز ٢مليون درهم ، اذا تعرضت هذه البيانات أو المعلومات للالغاء أو الحذف أو الاتلاف أو التدمير أو الافشاء أو التغيير أو النسخ أو النشر أو إعادة النشر"[٢] .

كما ونجد المادة السابعة من القانون نفسه عاقبت على أفعال الإتلاف المتعلق بفحوصات طبية التي نصت على " يعاقب بالسجن المؤقت كل من حصل أو استحوذ أو عدل أو أتلف أو افشى بغير تصريح بيانات أي مستند إلكتروني أو معلومات إلكترونية عن طريق الشبكة المعلوماتية أو موقع إلكتروني أو نظام المعلومات الإلكتروني أو وسيلة تقنية معلومات وكانت هذه البيانات أو المعلومات تتعلق بفحوصات طبية أو تشخيص طبي ، أو علاج أو رعاية طبية أو سجلات طبية"[٣].

وأكد المشرع الإماراتي في المادة العاشرة من القانون ذاته على تجرّيم أفعال الإتلاف الواقعة على المواقع الإلكترونية أو الانظمة أو المعلومات التي تتضمنها ، التي نصت على " يعاقب بالسجن مدة لا تقل عن خمس سنوات والغرامة التي لا تقل عن خمسمائة الف درهم ولا تجاوز ثلاثة ملايين درهم أو بإحدى هاتين العقوبتين كل من أدخل عمداً وبدون تصريح برنامج معلوماتي إلى الشبكة المعلوماتية أو نظام معلومات إلكتروني أو إحدى وسائل تقنية المعلومات ، وادى ذلك إلى إيقافها عن العمل أو تعطيلها أو تدمير أو مسح أو حذف أو إتلاف أو تغيير البرامج أو النظام أو الموقع الإلكتروني أو البيانات أو المعلومات ، كما وتكون العقوبة السجن والغرامة التي لا تجاوز خمسمائة الف درهم أو إحدى هاتين العقوبتين إذا لم تتحقق النتيجة ، في حين تكون

---

(١) يُنظر: نص الفقرة الاولى والثانية من المادة الثانية من مرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢.

(٢) يُنظر: نص المادة الرابعة من مرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢

(٣) يُنظر: المادة السابعة من المرسوم نفسه..

العقوبة الحبس والغرامة أو إحدى هاتين العقوبتين عن أي فعل عمدي يقصد به إغراق البريد الإلكتروني بالرسائل وايقافه عن العمل أو تعطيله أو إتلاف محتوياته"[١]

يتضح لنا مما تقدّم ان المشرّع الاماراتي جرّم الكثير من الأفعال التي تؤدي إلى إتلاف معلومات المنصات الإلكترونية سواء كان الإتلاف في المعلومات الشخصية أم كان في المعلومات الطبية أم كان الاتلاف للنظام الإلكتروني ، كما انه عاقب افعال الاتلاف أو التعطيل أو الحذف حتى وان لم تتحقق النتيجة ، وحسناً فعل المشرع الإماراتي وبدورنا نؤيد ما جاء بالمواد المشار إليها اعلاه في تجريم تلك الافعال التي من شأنها تؤدي إلى الضرر العام والخاص والرادع لكل من تسول له نفسه بإتلاف معلومات الغير.

اما المشرع الاردني فقد جرم أفعال الإتلاف في قانون الجرائم الإلكترونية رقم (٢٧) لسنة (٢٠١٥)في الفقرة (أ) من المادة الثالثة التي نصت على أن: " يعاقب كل من دخل قصداً إلى الشبكة المعلوماتية أو نظام معلومات بأي وسيلة دون تصريح أو بما يخالف أو يجاوز التصريح بالحبس مدة لا تقل عن أسبوع ولا تزيد على ثلاثة أشهر أو بغرامة لا تقل عن ١٠٠ مائة دينار ولا تزيد على ٢٠٠ مائتي دينار أو بكلتا هاتين العقوبتين"[٢] ، وشدد العقوبة في الفقرة ب من المادة ذاتها إذا كان الدخول في الفقرة (أ) أدى إلى " الإلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو توقيف أو تعطيل عمل الشبكة المعلوماتية أو نظام معلومات الشبكة المعلوماتية ، فيعاقب الجاني بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن ٢٠٠ مائتي دينار أردني ولا تزيد على ١٠٠٠ألف دينار أردني"[٣] ، أما الفقرة (ج) من المادة نفسها فقد جرّمت أفعال الإتلاف الذي يقع على البيانات الإلكترونية أو النظام المعلوماتي والتي نصت على أن: " يعاقب كل من دخل قصداُ إلى موقع إلكتروني لتغييرة أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو انتحال شخصية مالكه، بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن ٢٠٠ مائتي دينار أردني ولا تزيد على ١٠٠٠ألف دينار أردني"[٤] .

---

(١) يُنظر: المادة العاشرة من المرسوم ذاته.

(٢) يُنظر: نص الفقرة (أ) من المادة الثالثة من القانون الاردني رقم ٢٧ لسنة ٢٠١٥.

(٣) يُنظر: نص الفقرة (ب) من المادة الثالثة من القانون نفسه

(٤) يُنظر: نص الفقرة (ج) من المادة الثالثة من القانون ذاته

يتضح لنا مما تقدّم أن المشرّع الاردني قد فتح طريق التجريم لأفعال الإتلاف لتشمل في طيها كل فعل يؤدي إلى حرمان المالك من حقه في الحفاظ على بياناته ومعلوماته الخاصة والعامة وعدَّ أي فعل مما تم ذكرة في المادة الثالثة بجميع فقراتها يعاقب عليه في قانون الجرائم الإلكترونية الاردني ، فضلاً عن تجريم أفعال الاتلاف للأنظمة الإلكترونية والمواقع الإلكترونية، وهذه الفقرات تعد حماية أكثر فاعلية ضد أي اعتداء يمكن أن يقع في جميع المجالات الإلكترونية ومنها معلومات المنصات الإلكترونية بجميع أنواعها.

اما المشرع العراقي فلم يجُرّم الإتلاف الإلكتروني بقانون خاص ، وهذ يعد نقصاُ تشريعياً على الرغم من تقديم مشروع قانون جرائم الإلكترونية العراقي لسنة (٢٠١١)[١] ، الذي ذهب باتجاه تجريم الإتلاف الإلكتروني في العديد من مواد مشروع القانون ففي الفقرة الثالثة من المادة السادسة التي نصت على أن " يعاقب بالسجن المؤبد أو المؤقت وبغرامة لا تقل عن خمسة وعشرين مليون دينار ولا تزيد على خمسين مليون دينار ، كل من استخدم أجهزة الحاسوب وشبكة المعلومات بقصد ارتكاب إحدى الافعال الاتية... : إتلاف أو تعطيل أو تعييب أو إعاقة أو الإضرار عمداً بأنظمة أو شبكة المعلومات التابعة لدوائر الدولة بقصد المساس بنظامها والبنى التحتية لها"[٢] ، أما الفقرة (أ) من المادة الثالثة عشر من مشروع ذاته فقد نصت على أن :" العقوبة بالحبس مدة لا تقل عن ثلاث سنوات أو بغرامة لا تقل عن (٥٠٠٠٠٠٠) خمسة ملايين دينار عراقي ولا تزيد على (١٠٠٠٠٠٠٠) عشرة ملايين دينار عراقي أو بكلتا هاتين العقوبتين كل من أتلف أو أضر توقيعاً أو وسيلة أو محرراً إلكترونياً"[٣] ، وشددت العقوبة في الفقرة (أ) أولا من المادة الرابعة عشر التي نصت على أن : " يعاقب بالحبس مدة لا تزيد على ثلاث

---

(١) والجدير بالذكر انه قد صدر من رئيس لجنة الثقافة والإعلام في مجلس النواب العراقي كتاباً يحمل العدد (٢٢ ل ث ع) في (٢٠١٣/١/٢٢) موجهاً إلى رئيس مجلس النواب العراقي ، وموضوع الكتاب (إيقاف تشريع قانون جرائم المعلوماتية) وجاء فيه : (عطفاً على كتابنا ذي العدد ١٤٤ل ث غ في ١١/ ٢٠١٢/٧ ، نود إعلام سيادتكم بأن لجنتنا قد حضرت عدة مؤتمرات وحلقات نقاش لمشروع قانون جرائم المعلوماتية ، وآخرها ما نظمته اليونسكو في بغداد وكانت جميعها رافضة لمشروع القانون وتعده انتكاسة للحريات في العراق ، وتقترح لجنتنا إيقاف تشريعه لقدمه ولان الظرف الأمني الذي أرسل به من قبل الحكومة قد تغير إيجاباً ، وحتى لا يشكل تشريعه إشارة سلبية على عمل مجلسنا الموقر كما نرجو رفعه من الصفحة الإلكترونية للمجلس) ، وقد جاء في هامش رئيس مجلس النواب على أصل المذكرة بالآتي بتاريخ (٢٥/ ٢٠١٣/١) : (موافق حسب طلب اللجنة) يُنظر: د. عمار عباس الحسيني ، مصدر سابق ، ص٢٢٧.

(٢) يُنظر: نص الفقرة الثالثة من المادة السادسة من مشروع قانون الجرائم الإلكترونية العراقي لسنة ٢٠١١ .

(٣) يُنظر: نص الفقرة (أ) من المادة الثالثة عشر من المشروع ذاته .

سنوات أو بغرامة لا تقل عن (١٠٠٠٠٠٠٠) عشرة ملايين ولا تزيد عن (١٥٠٠٠٠٠٠) خمسة عشر مليون دينار عراقي ، كل من أتلف أو عيب أو عطل سنداً إلكترونياً أو بطاقة إلكترونية مثبتة لدين أو تصرف أو أية حقوق مالية أو معنوية أخرى أو أي محرر إلكتروني يستخدم لإثبات الحقوق"[١] ، وفي الفقرة (أ) ثالثاً من المادة ذاتها التي نصت على أن: " يعاقب بالحبس مدة لا تزيد على ثلاثة أشهر أو بغرامة لا تقل عن مليوني دينار ولا تزيد على خمسة ملايين دينار ، كل من عهدت إلية مهمة تشغيل والاشراف على جهاز الحاسوب ، فتسبب بخطئه في تلف أو تعطيل أو إعاقة أو تعييب أجهزة الحاسوب أو أنظمته أو برمجته أو شبكاته وما في حكمها"[٢] ، أما في الفقرة (ب) من المادة الواحد والعشرين من المشروع نفسه شددت العقوبة إذا كان الإتلاف موقعاً لشركة أو مؤسسة ، التي نصت على أن: " يعاقب بالحبس مدة لا تقل عن سنتين ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن عشرة ملايين دينار عراقي ولا تزيد على عشرين مليون دينار عراقي ، أو بإحدى هاتين العقوبتين ، كل من دخل موقعاً خاصاً بشركة أو مؤسسة أو غيرها ، لتغيير تصاميم هذا الموقع أو إلغائه أو إتلافه أو تعديله أو استغله لنفسه أو لغيره بدون وجه حق"[٣].

يتضح لنا مما تقدّم ان المشرع العراقي جرّم الكثير من الافعال التي تتم عن طريق الانظمة الإلكترونية ، بمشروع قانون الجرائم الإلكترونية العراقي لسنة ٢٠١١ الذي لم يرَ النور إلى هذه اللحظة ويمكن استغلال هذا التأخير في إعادة مناقشة المشروع بإضافة فقرات جديدة تحمي معلومات المنصات الإلكترونية من المساس بها أو عرقلتها أو إساءة استخدامها ، ومن الملاحظ على الفقرات التي تم الاشارة اليها في مشروع القانون نجدها في بعض الفقرات شددت العقوبة على من يحاول القيام بأفعال الاتلاف ، وبدورنا نؤيد تشديد العقوبة من أجل توفير الحماية الجزائية للأنظمة الإلكترونية والمنصات الإلكترونية بجميع أنواعها أو أي جهاز إلكتروني آخر ، التي تكون عرضة للعديد من الجرائم ومنها جريمة إتلاف معلومات المنصات الإلكترونية التي تؤدي إلى ضرر عام وخاص في الوقت نفسه ، ونجد طلب رئيس لجنة الثقافة والاعلام في مجلس النواب العراقي المتضمن إيقاف تشريع قانون جرائم الإلكترونية غير مبرر خصوصاً

---

(١) يُنظر: نص الفقرة (أ) أولاً من المادة الرابعة عشر من المشروع نفسه .

(٢) يُنظر: نص الفقرة (أ) ثالثاً من المادة الرابعة عشر من مشروع قانون الجرائم الإلكترونية العراقي لسنة ٢٠١١.

(٣) يُنظر: نص الفقرة (ب) أولاً من المادة الواحد والعشرين من مشروع قانون الجرائم الإلكترونية العراقي لسنة ٢٠١١.

والجرائم الإلكترونية في تزايد مستمر مما يجدر بمجلس النواب العراقي الاسراع في التصويت على مشروع القانون من أجل مكافحة العديد من الجرائم الإلكترونية الحديثة ، ومواكبة الدول التي سبقتنا في سن التشريعات ضد الجرائم الإلكترونية ، وبالتالي توفير الحماية الجزائية التي تؤدي إلى استقرار أمن المجتمع .

المطلب الثاني

أركان جريمة إتلاف معلومات المنصات الإلكترونية

تقع جريمة إتلاف معلومات المنصات الإلكترونية عبر شبكة الإنترنت ، ويستلزم تحقق الجريمة بوجه عام توافر الركن المادي والركن المعنوي ، ويتمثل الركن المادي في محل الجريمة والاعتداء على الوظائف الطبيعية للحاسب الآلي أو أي جهاز إلكتروني آخر ممكن أن تثبت عليه المنصات الإلكترونية بأنواعها وإتلاف المعلومات التي تم تخزينها في المنصات الإلكترونية ، وعليه سنقسم هذا المطلب على فرعين نتناول في الفرع الاول الركن المادي في جريمة إتلاف معلومات المنصات الإلكترونية وفي الفرع الثاني نتناول الركن المعنوي في جريمة إتلاف معلومات المنصات الإلكترونية .

الفرع الأول

الركن المادي في جريمة إتلاف معلومات المنصات الإلكترونية

الركن المادي في جريمة إتلاف معلومات المنصات الإلكترونية يتمثل بالسلوك الإجرامي وهو فعل الإتلاف [1] والإتلاف هو إفناء مادة الشيء أو إحداث التغيرات الشاملة على الاقل ، وجعلها غير صالحة للغرض المخصصة من أجله ، بفقدانها قيمتها مما يؤدي إلى حرمان مالكها من الاستفادة منها[2] ،اما التعييب أو التخريب هو عدم قابلية المال للاستعمال لأنه فقد صلاحيته كلياً أو جزئياً[3] ولما تقدم ذكره للركن المادي فإن علينا بيان السلوك الإجرامي والنتيجة الإجرامية والعلاقة السببية في جريمة إتلاف معلومات للمنصات الإلكترونية .

---

(١) ونقصد بالإتلاف أو التعييب التأثير في مادة الشيء على نحو يذهب أو يقلل من قيمته الاقتصادية عن طريق الإنقاص من كفاءته للاستعمال المعد له. يُنظر: د عمر أبو الفتوح عبد العظيم الحمامي ، الحماية الجنائية للمعلومات المسجلة إلكترونياً (دراسة مقارنة) ، دار النهضة العربية ، ٢٠١٠ ، ص٩٨٤.

(٢) يُنظر: د. محمود محمد محمود جابر ، مصدر سابق ، ص١٨٣.

(٣) يُنظر: د. فتوح الشاذلي ، عفيفي كامل عفيفي ، مصدر سابق ، ص٢٠٣.

اولاً: السلوك الإجرامي في جريمة إتلاف معلومات المنصات الإلكترونية

يعد السلوك الإجرامي العنصر الاول للركن المادي في جريمة إتلاف معلومات المنصات الإلكترونية عبر شبكة الانترنت ويتحقق السلوك الإجرامي في جريمة الإتلاف في إعدام صلاحية معلومات المنصات الإلكترونية وجعلها غير صالحة للاستعمال على نحو يقلل من القيمة الاقتصادية بالتأثير في مادة الشيء أو قد يكون بتعطيل الشيء وإعاقته عن العمل كلياً أو جزئياً [١] وبعض تشريعات الدول المقارنة جاءت بتعبيرات مختلفة للدلالة على السلوك الإجرامي لجريمة الإتلاف منها "الإتلاف والتدمير والتخريب ومحو البرامج و التشوية و مسح البرامج والبيانات وايقاف أو حذف أو سلوك آخر يجعل من معلومات المنصات الإلكترونية غير صالحة للاستعمال كلياً أو جزئياً "[٢] ،إذ نجد السلوك الإجرامي في القانون الامريكي قد جرّم الإتلاف الذي يترتب عليه إعاقة أنظمة الحاسب الآلي للحكومة و لم يجرّم إتلاف المعلومات بصورة عامة في القانون الصادر لعام (١٩٨٤)[٣]، اما السلوك الإجرامي في قانون العقوبات الفرنسي رقم (٥٧٥)لسنة (٢٠٠٤)فقد جاء في لفقرة الثالثة من المادة (٣٢٣)بتعبيرات عديدة منها " الادخال والمحو والتعديل" [٤] ، وفي قانون مكافحة جرائم تقنية المعلومات الاماراتي رقم (٢) لسنة (٢٠٠٦) ، فقد جاء في المادة السادسة تعبيرات عديدة للسلوك الإجرامي في جريمة الإتلاف منها " إيقافها عن العمل أو تعطيلها أو تدمير أو مسح أو حذف أو إتلاف أو تعديل البرامج أو البيانات أو المعلومات " [٥] ، اما السلوك الإجرامي لجريمة الإتلاف في قانون جرائم أنظمة المعلوماتية الأردني المؤقت رقم (٣٠) لسنة (٢٠١٠) فقد جاء في الفقرة (أ) من المادة الثالثة بتعبيرات "

---

(١) يُنظر: نهلا عبد القادر المومني ، مصدر سابق ، ص ١٣٥.

(٢) يُنظر: د. عمار عباس الحسيني ، مصدر سابق ، ص١٥١-١٥٢.

(٣) الذي تم تعديله لأكثر من مرة في الاعوام ١٩٨٦، ١٩٩٤، ١٩٩٦، وورد في المادة (١٠٣٠) تجريم الاعتداء على الحاسب الألي ، والانشطة المتعلقة بالحاسب الآلي ، يتبين من خلال نصوص القانون أنها تنطوي على الكثير من الغموض والقصور مما يمكن المجرمين من عدم إدانتهم وتطبيق القانون عليهم ، لاستخدامهم حاسبات وشبكات تقع خارج الولايات المتحدة الامريكية ، كما ويستطيع المجرمين القيام بجرائم الإتلاف من خارج الولايات المتحدة الامريكية باستخدام الانظمة الموجودة بالدولة الأخرى والاعتداء على الحاسبات الموجودة داخل الولايات يُنظر: محمد عبيد الكعبي ، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت (دراسة مقارنة) مصدر سابق ، ص٢٧١.

(٤) يُنظر: الفقرة الثالثة من المادة ٣٢٣ من قانون العقوبات الفرنسي رقم ٥٧٥ لسنة ٢٠٠٤التي نصت على " كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية للمعطيات أو محا أو عدل بطريق الغش المعطيات التي يتضمنها يعاقب بعقوبة الحبس حتى خمس سنوات وبغرامة تقدر ب ٧٥٠٠٠يورو".

(٥) يُنظر: نص المادة السادسة من القانون الاتحادي رقم ٢ لسنة ٢٠٠٦.

حذف أو إضافة أو تدمير أو إتلاف"[١] ،كذلك قانون الجرائم الإلكترونية رقم (٢٧) لسنة (٢٠١٥) فقد جاء في الفقرة (ب) من المادة الثالثة بتعبيرات للسلوك الإجرامي منها " حذف أو إضافة أو تدمير أو إتلاف أو حجب أو تعديل أو تغيير "[٢] ، أما قانون العقوبات العراقي النافذ رقم (١١١) لسنة (١٩٦٩) فقد أشارت المادة (٢٥٠) للسلوك الإجرامي في إتلاف المحررات الرسمية المقدمة إلى المحكمة بقصد تضليل القضاء [٣] ، وورد في المادة (٢٦٤) السلوك الإجرامي في إتلاف الاوراق أو المستندات أو الاشياء أو الوثائق أو السجلات المتعلقة بالدولة [٤] ، وردّ السلوك الإجرامي للإتلاف المتعلق بإتلاف محرر لدين بسوء نية في المادة (٣٠٠) [٥] ، وورد السلوك الإجرامي للإتلاف الحاصل على عقار أو منقول مملوك للغير في المادة (٤٧٧) [٦] وبينت المادة (٤٧٨) السلوك الإجرامي في إتلاف عقار أو منقول مملوك للغير من لجنة مؤلفة من خمسة أشخاص وجعلته غير صالح للاستعمال [٧] ، وأشارت المادة (٤٨٠) إلى السلوك الإجرامي في جريمة إتلاف المغروسات الثابتة في الأماكن العامة والأماكن المخصصة للمنفعة العامة من دون موافقة السلطة عليها [٨] ، كذلك ورد السلوك الإجرامي لإتلاف إعلانات موضوعة في

---

(١) يُنظر: الفقرة (أ) من المادة الثالثة التي تنص على " ألغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو توقيف أو تعطيل عمل نظام معلومات"

(٢) يُنظر: الفقرة (ب) من المادة الثالثة من قانون الجرائم الإلكترونية الأردني رقم ٢٧ لسنة ٢٠١٥.

(٣) يُنظر: نص المادة (٢٥٠) التي عاقبت بالحبس أو الغرامة أو بإحدى هاتين العقوبتين (كل من اختلس أو أخفى أو أتلف أو غير وثيقة أو مبرزاً أو مادة جرمية مقدمة إلى محكمة أو سلطة من سلطات التحقيق وكان ذلك بقصد تضليل القضاء أو سلطة التحقيق .

(٤) يُنظر: نص المادة (٢٦٤) يعاقب بالسجن مدة لا تزيد على سبع سنوات أو بالحبس (كل من سرق أو اختلس أو نزع أو أتلف أوراقاً أو مستندات أو أشياء أو وثائق أو سجلات أو دفاتر متعلقة بالدولة أو بإحدى السلطات العامة أو أوراق إجراءات قضائية وكانت مودعة في الأماكن المعدة لحفظها أو مسلمة لشخص مكلف بحفظها ولو بصفة مؤقتة.....)

(٥) يُنظر: نص المادة (٣٠٠) يعاقب بالسجن مدة لا تزيد على سبع سنوات أو بالحبس (كل من أتلف أو أفسد أو عيب أو أبطل بسوء نية محرراً موجداً أو مثبتاً لدين أو تصرف في مال أو إبراء أو مخالصة أو أي محرر يمكن استعماله لإثبات حقوق الملكية.....)

(٦) يُنظر: نص المادة (٤٧٧) يعاقب بالحبس مدة لا تزيد على سنتين وبغرامة لا تزيد على مائتي دينار أو بإحدى هاتين العقوبتين من هدم أو خرب أو أتلف عقاراً أو منقولاً غير مملوك له أو جعله غير صالح للاستعمال أو أضر به أو عطله بأية كيفية كانت .....).

(٧) يُنظر: نص المادة (٤٧٨) يعاقب بالحبس كل عضو في عصبة مؤلفة من خمسة أشخاص على الأقل هدمت أو خربت أو أتلفت عقاراً أو منقولاً مملوكاً للغير أو جعلته غير صالح للاستعمال أو أضرت به أو عطلته بأية كيفية كانت .....).

(٨) يُنظر: نص المادة (٤٨٠) يعاقب بالحبس مدة لا تزيد على سنتين وبغرامة لا تزيد على مائتي دينار أو بإحدى هاتين العقوبتين من قطع أو اقتلع أو أتلف شجرة مغروسة أو خضرة نابتة في مكان معدّ للعبادة أو في شارع أو ميدان عام أو في مكان للنزهة أو في حديقة عامة أو غيرها من الأماكن المخصصة للمنفعة العامة دون إذن من سلطة مختصة .

مكانات مرخصة في المادة (٤٩٢) [١] كما ورد تعبيرات (التخريب) في العديد من المواد الاخرى منها (١٩٧، ٣٥٣، ٣٥٥، ٤٧٧) وغيرها من المواد الاخرى ، واحتوت المادة (٤٩٢) على مفردة (التشويه) وبعض المفردات التي تم ذكرها وردت مجتمعة في بعض المواد [٢] .

ثانياً: النتيجة الإجرامية في جريمة إتلاف معلومات المنصات الإلكترونية

تعد النتيجة الإجرامية العنصر الثاني للركن المادي في جريمة إتلاف معلومات المنصات الإلكترونية ، وتتخذ مظهراً خارجيا يتمثل بإتلاف معلومات المنصات الإلكترونية المثبتة على الحاسب الآلي أو أي جهاز إلكتروني آخر ، وتتحقق النتيجة الإجرامية في جريمة إتلاف معلومات المنصات الإلكترونية نتيجة سلوك الجاني في الإتلاف أو المحو أو التدمير أو التشوية في معلومات المنصات الإلكترونية ، مما يؤدي ذلك في حرمان مالكها من المنفعة منها كلياً أو جزئياً والتأثير في إداء عمل معلومات المنصات الإلكترونية على نحو معتاد ، وجميع الأفعال التي تم ذكرها تؤدي إلى السلوك الإجرامي والذي يؤدي بدوره إلى النتيجة الإجرامية في إتلاف صلاحية معلومات المنصات الإلكترونية بشكل كلي أو جزئي[٣].

ثالثاً: العلاقة السببية في جريمة إتلاف المنصات الإلكترونية

تتجلى العلاقة السببية في جريمة إتلاف معلومات المنصات الإلكترونية بين السلوك الإجرامي والنتيجة الإجرامية ، وتكون العلاقة مادية بينهما من اللحظة التي يباشر فيها الجاني السلوك الإجرامي المؤدي لحدوث النتيجة الإجرامية ، إذ لا يمكن أن تتحقق جريمة إتلاف معلومات المنصات الإلكترونية مالم تكن النتيجة الإجرامية ناشئة عن السلوك الإجرامي للجاني ، أي لا بد من وجود العلاقة السببية بين السلوك والنتيجة الإجرامية من أجل مساءلة الجاني عن سلوكه الإجرامي وإلا لا يمكن مساءلة الجاني على السلوك الإجرامي في حال لم تتحقق النتيجة الإجرامية ، ويمكن تحقق السلوك الإجرامي في جريمة إتلاف معلومات المنصات الإلكترونية بغض النظرعن الوسيلة التي أدت لحدوث النتيجة الإجرامية المتمثلة في التدمير أو التخريب أو التعطيل أو غيرها من الافعال التي تؤدي إلى عدم صلاحية معلومات المنصات الإلكترونية بشكل

---

(١) يُنظر: نص المادة (٤٩٢) يعاقب بغرامة لا تزيد على عشرة دنانير ، من وضع إعلاناً في غير المحلات المأذون بوضع الإعلانات فيها أو نزع أو أتلف أو شوه بغير حق إعلاناً موضوعاً في تلك المحلات .

(٢) يُنظر: د. عمار عباس الحسيني ، مصدر سابق ، ص١٥٢.

(٣) ونتيجة أتلاف معلومات عندما تمكن طالب أمريكي من إدخال فايروس الدودة إلى شبكة الإنترنت من خلال إحدى وسائل الاتصال وفي مدة لا تتجاوز ٢٤ ساعة كان هذا البرنامج قد انتشر عبر الشبكة وغطى أطرافها ، كما تأثرت به العديد من الشبكات التي ترتبط بشبكة الإنترنت وتقدر بأكثر من ٦٠٠٠حاسب في أرجاء الولايات المتحدة الأمريكية ، إذ قام هذا الفايروس بملء ذاكرتها حتى لم يعد بمقدورها القيام بأي عمل أو تنفيذ أي أمر ، مما أدى لإتلاف المعلومات . يُنظر: د. محمد عبيد الكعبي ، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت (دراسة مقارنة) ، مصدر سابق ، ص٢٧٢.

كلي أو جزئي ، وكان السلوك الإجرامي تدميراً أو تخريباً أو تعطيلاً أو تشويشاً أو إفساداً مما يؤدي للإتلاف الإلكتروني [١].

الفرع الثاني

الركن المعنوي في جريمة إتلاف معلومات المنصات الإلكترونية

يشترط لقيام جريمة إتلاف معلومات المنصات الإلكترونية ليس فقط تحقق الركن المادي ، بل يشترط تحقق الركن المعنوي أيضاً لأنها من الجرائم العمدية ، ويتطلب لقيام الركن المعنوي تحقق القصد الجرمي العام المتمثل بعنصريه العلم والإرادة ، وبعض التشريعات تتطلب تحقق القصد الجرمي الخاص بالإضافة إلى القصد الجرمي العام .

اولاً: القصد الجرمي العام في جريمة إتلاف المنصات الإلكترونية

يتحقق القصد الجرمي متى ما تعمدّ الجاني إلى ارتكاب الفعل المنهي عنه بالصورة التي حددها القانون ، واتجاه إرادته إلى إحداث فعل الإتلاف ، مع علمه بأنه يقوم بفعله الإجرامي بغير حق على مال مملوك للغير[٢]

١- عنصر العلم

يعد العلم أحد عناصر القصد الجرمي العام في الركن المعنوي والجاني يعلم أن النشاط الذي يقوم به غير مشروع ، ويعلم انه يعتدي على مصلحة يحميها القانون وفي الحقيقة ان علم الجاني في هذه الحالة يجب أن ينصرف إلى جميع العناصر الاساسية التي يقوم عليها كيان الجريمة[٣] ، أما في جريمة إتلاف معلومات المنصات الإلكترونية ، فإن الجاني يجب ان يعلم وقت اقترافه للسلوك الإجرامي بأنه يعتدي على أموال إلكترونية مملوكه للغير والتي تتمثل في المعلومات والبرامج والمحررات المعلوماتية ، أما في حالة اعتقاد الجاني انه يعتدي على معلومات وبرامج تعود له بناءً على أسباب معقوله ففي هذه الحالة فإن عنصر العلم ينتفي لديه ، كمن يقوم بمحو المعلومات والبرامج من الحاسب الآلي وفي اعتقاده انها تعود له وهذا الفرض نادر الحدوث جداً[٤] ، أو قيام الوارث

---

(١) يُنظر: د. عمار عباس الحسيني ، مصدر سابق ، ص١٨٤.

(٢) يُنظر: د. محمود محمد محمود جابر ، مصدر سابق ، ص١٨٨.

(٣) يُنظر: د. حسام محمد نبيل الشنراقي ، الجرائم المعلوماتية دراسة تطبيقية مقارنة على جرائم الاعتداء على التوقيع الإلكتروني ، دار الكتب القانونية ، ٢٠١٣ ، ص٣٢٥.

(٤) يُنظر: د. عمار علي الحسيني ، مصدر سابق ، ص١٨٦.

بمحو المعلومات والبرامج من اقراص ممغنطة وهي ليست مملوكه لمورثه التي عثر عليها في التركة عن طريق مورثه وقيامه بالتخلص منها عن طريق إتلافها أو كسرها[١]، أو قيام شخص باستعمال اسطوانة مملوكه له في حين انه لا يعلم بإصابتها بأحد الفايروسات خلال استخدامها في أحد المشاريع مما ادى إلى انتقال الفايروس إليها ، والتي نجم عنها الاعتداء بالإتلاف على المكونات المادية والمعنوية للنظام الإلكتروني الخاص بالمشروع[٢] .

٢- عنصر الإرادة :

وهو العنصر الثاني في القصد الجرمي العام في الركن المعنوي ، الذي يشترط فيه ان تتجه إرادة الجاني إلى إحداث الإتلاف أو التخريب أو التعطيل أو عدم الصلاحية للاستعمال ، أما إذا انتفت هذه الإرادة ينتفي بالتبعية القصد الجرمي ومن ثم انتفاء الجريمة بالكامل ، كما لو وقع شيء من العامل أو الموظف على الجهاز أدى ذلك إلى إتلاف جزء منه ففي هذه الحالة لا تقوم جريمة الإتلاف العمدي التي يتسبب عنها إعاقة النظام الإلكتروني إذ نكون امام إتلاف خطأ نتيجة الاهمال [٣] ، الامر الذي لم نجده لا في قانون مكافحة الجرائم المعلوماتية الاماراتي ولا في قانون العقوبات الفرنسي ، لكن عند العودة إلى نص المادة ٤٠٤من قانون العقوبات الاماراتي ، واستناداً إلى المادة ٤٣من القانون ذاته حيث نص على انه " يسأل الجاني عن الجريمة سواء ارتكبها عمداً أو خطأ ، ما لم يشترط القانون العمد صراحةً" وقضت محكمة التمييز في دبي للقاضي الجزائي ان يقرر ركن الخطأ والتقصير في التسبيب في إلحاق الضرر بالمال ، وله كذلك أن يقيم قضاءه بناءً على أسباب مقبولة يكون لها أصل في الاوراق يستند عليها ، ويكفي لقيام الجريمة صدور الإتلاف عمداً أو خطأ لمال الغير[٤].

---

(١) يُنظر: د. حسني عبد السميع إبراهيم ، الجرائم المستحدثة عن طريق الإنترنت (دراسة مقارنة بين الشريعة والقانون) ط١، دار النهضة العربية ، القاهرة ، ٢٠١١ ، ص٥٣٨.

(٢) يُنظر: د. عمر أبو الفتوح عبد العظيم الحمامي ، مصدر سابق ، ص٩٩٩.

(٣) يُنظر: د. أيمن رمضان محمد أحمد ، الحماية الجنائية للتوقيع الإلكتروني ، دار النهضة العربية ، ٢٠١١ ، ص١٩٣.

(٤) يُنظر: د. محمد عبيد الكعبي ، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت (دراسة مقارنة) ، مصدر سابق ، ص٢٦٣.

ثانيا: القصد الجرمي الخاص في جريمة إتلاف معلومات المنصات الإلكترونية.

تشترط بعض التشريعات بجانب القصد الجرمي العام القصد الجرمي الخاص إذ بوجود العلم والإرادة يشترط توافر نية إحداث الضرر بالغير وعلى سبيل الاستدلال نستدل ببعض تشريعات الدول خارج حدود المقارنة والتي تتطلب توافر القصد الجرمي الخاص ومن هذه التشريعات قانون العقوبات الفنلندي [1] ،كذلك قانون العقوبات الفرنسي رقم ١٩لسنة ١٩٨٨ ايضاً تطلب نية إحداث الضرر بالغير[2] .

يتضح لنا مما تقدّم أن أغلب التشريعات المقارنة تتطلب تحقق القصد العام المتمثل بعنصريه العلم والإرادة ، ولا تشترط وجود قصد خاص ، على عكس بعض التشريعات التي اشترطت توافر القصد الجرمي الخاص المتمثل بنية احداث الضرر بجانب القصد الجرمي العام ، والباحث يؤيد التشريعات التي اكتفت بتحقق القصد الجرمي العام ، لأن الضرر نتيجة حتمية لابد منها ولا يوجد مبرر في اشتراط القصد الجرمي الخاص ، فضلاً عن ان هذا الاشتراط ممكن أن يؤدي إلى إفلات المجرمين من العقاب بحجة إن الاتلاف لم يؤدِ إلى نتيجة الاتلاف والمشرع الفرنسي اشتراط توافر القصد الجرمي الخاص بجانب القصد الجرمي العام في القانون رقم١٩ لسنة ١٩٨٨ في المادة (٣/٣٢٣).

(١) الذي تطلب اتجاه نية الفاعل إلى الاضرار بالغير، وقانون العقوبات البرتغالي ايضاً تتطلب الاضرار بالغير أو تحقيق ربح غير مشروع للجاني أو لغيره ، وقانون العقوبات التركي كذلك تطلب نية إيذاء الغير أو الحصول على ربح مادي يُنظر: د. عمار عباس الحسيني ، مصدر سابق ، ص١٩٤

(٢) يُنظر: د. أيمن رمضان محمد أحمد ، مصدر سابق ، ص١٩٣.

الفصل الثاني

الحماية الجزائية من جرائم الاعتداء على المنصات الإلكترونية

الفصل الثاني

الحماية الجزائية من جرائم الاعتداء على المنصات الإلكترونية

مما لاشك فيه أن التطور التكنولوجي الحديث والمعاصر قد أثر بشكل غير طبيعي على حياة الافراد، وجعلها تأخذ حلة جديدة وحديثة وبشكل إلكتروني ، مما يؤدي إلى سرعة في الإنجاز وتقليل في المسافات وخفض التكاليف ، وكل تطور حديث لابد ان يتعرض إلى اعتداءات وهذه الاعتداءات بحاجة إلى نصوص جزائية تُجّرم الأفعال التي تتعرض لها المنصات الإلكترونية ذاتها أو ما تحويها من معلومات تكون محلاً لتلك الجرائم والنصوص التقليدية غير كفيلة بمعاقبتها ، لأنها لا تتطور بالسرعة نفسها التي تتطور فيها التكنولوجيا الحديثة لذلك لا بد من توفير الحماية الجزائية للمنصات الإلكترونية من جميع الجرائم ، وذلك من خلال تشريع قوانين لمكافحة الجرائم التي تتعرض لها المنصات الإلكترونية ومن أبرز هذهِ الجرائم جريمة السرقة الإلكترونية وجريمة الاحتيال الإلكتروني ، وعليه سنقسم هذا الفصل على مبحثين نتناول بالمبحث الاول الحماية الجزائية من جريمة السرقة معلومات المنصات الإلكترونية وفي المبحث الثاني نتناول الحماية الجزائية للمنصات الإلكترونية من جريمة الاحتيال

المبحث الاول

الحماية الجزائية من جريمة سرقة معلومات المنصات الإلكترونية

تحمل طبيعة الجرائم التي ترتكب ضد المنصات الإلكترونية طبيعة خاصة ، ومحل جريمة السرقة فيها يكون على معلومات الأنظمة الإلكترونية سواء كان ما يقع عليها أو ما يقع ضدها من اعتداءات باستخدام الادوات المادية من الاجهزة والبطاقات الممغنطة ، لذلك علينا توضيح جريمة سرقة معلومات المنصات الإلكترونية وبيان أركانها ، فضلاً عن انها تتطلب تحليل لعناصر الأموال والمعلومات المتداولة إلكترونياً ومعرفة مدى قابلية هذه العناصر إلى الحماية ، خاصة في ظل قصور التشريع العراقي وباقي التشريعات المقارنة؛ والتي لم تتعرض بشكل دقيق للحلول التشريعية في سرقة المال الذي يتم تداوله إلكترونياً هذا من جانب ، وفي جانب أخرعلينا ان نربط بين العناصر المكونة لجريمة السرقة وفقا للنص الجنائي التقليدي، وبين عناصر السرقة للمنصات الإلكترونية ،ونعمل على طرح الاشكاليات الجوهرية حول مدى امكانية تطبيق النص الجنائي التقليدي من عدمه على سرقة معلومات المنصات الإلكترونية ،نظراً لضرورة

بيان مدى تطابق القواعد القانونية العامة في جريمة السرقة مع القواعد الخاصة للمنصات الإلكترونية في جريمة السرقة ،

وعليه سنقسم هذا المبحث على مطلبين نتناول بالمطلب الاول مفهوم جريمة سرقة معلومات المنصات الإلكترونية ونتناول في المطلب الثاني أركان جريمة سرقة معلومات المنصات الإلكترونية .

المطلب الاول

مفهوم جريمة سرقة معلومات المنصات الإلكترونية

تعد جريمة السرقة التقليدية من الجرائم واسعة الانتشار التي جرّمتها أغلب تشريعات الدول المقارنة ، أما جريمة سرقة المنصات الإلكترونية فهي ظاهرة إجرامية حديثة انشأت بفعل التطورات المذهلة في تقنيات الحاسب الآلي ومن أجل التعرف على مفهوم هذه الجريمة لابد من بيان تعريف محدد لها ، ومن ثم بيان محل جريمة سرقة معلومات المنصات الإلكترونية ، وعليه سنقسم هذا المطلب على فرعين نتناول في الفرع الاول تعريف جريمة سرقة معلومات المنصات الإلكترونية ونتناول في الفرع الثاني جريمة سرقة معلومات المنصات الإلكترونية على المستوى الفقهي والقضائي .

الفرع الاول

تعريف جريمة سرقة معلومات المنصات الإلكترونية

نصت أغلب التشريعات على تعريف جريمة السرقة بأنها تنصب على المال المنقول المملوك للغير ، وعرّف قانون الولايات المتحدة الامريكية جريمة السرقة " بأنها الاستحواذ على الممتلكات الشخصية للآخرين ضد ارادتهم سواء أكان ذلك بغيابهم أم بحضورهم عن طريق استعمال القوة أو التخويف وعند ذلك تشكل السرقة جريمة مركبة تتضمن اعتداء على المال والجسد "[1] ، وعرّف المشرع الفرنسي السرقة في المادة (٣٧٩)من قانون العقوبات القديم والمقابلة لها في المادة (١/٣١١)من قانون العقوبات الفرنسي الجديد رقم (١٣٣٦)لسنة (١٩٩٢)النافذ عام (١٩٩٤) بأن السرقة " هي اختلاس الشيء المملوك للغير "[2] ، أما قانون

([1]) يُنظر المادة (١١٩) قانون الاحتيال وإساءة استخدام الكمبيوتر لعام ١٩٨٤.

([2]) يُنظر: د. محمود محمد محمود جابر ، مصدر سابق ، ص٤٢٠.

العقوبات الاماراتي رقم (٣) لسنة(١٩٨٧)المعدل فقد عرّف السرقة في المادة (٣٨٢) على أن " تقع السرقة التعزيرية باختلاس مال منقول مملوك لغير الجاني"[١] ، كذلك عرّف السرقة قانون العقوبات الاردني رقم (١٦) لسنة (١٩٦٠) في المادة (١/٣٩٩)على أن " السرقة هي أخذ مال الغير المنقول دون رضاه"[٢] ، وعرّف السرقة قانون العقوبات العراقي رقم (١١١)لسنة (١٩٦٩) وتعديلاته في المادة (٤٣٩) على أن " السرقة اختلاس مال منقول مملوك لغير الجاني عمداً ، ويعتبر منقولاً لتطبيق أحكام السرقة .... والقوى الكهربائية والمائية وكل طاقة أو قوة محرزة أخرى .... "[٣] .

اما المعلومات فقد عرّفها قانون المعاملات الإلكترونية الموحد الامريكي لسنة (١٩٩٩) في الفقرة العاشرة من المادة الثانية بأنها "البيانات والكلمات والصور والاصوات والوسائل وبرامج الكمبيوتر والبرامج المضغوطة والموضوعة على الاقراص المرنة وقواعد البيانات أو ما شابه ذلك" [٤] ، وعرّف المرسوم بقانون اتحادي رقم (٥)لسنة (٢٠١٢) في المادة الاولى منه المعلومات الإلكترونية على أنها " أي معلومات يمكن تخزينها ومعالجتها وتوليدها ونقلها بوسائل تقنية المعلومات وبوجه خاص الكتابة والصور والصوت والارقام والحروف والرموز والاشارات وغيرها " [٥] ، في حين عرّف قانون المعاملات والتجارة الإلكترونية الاماراتي رقم (١) لسنة (٢٠٠٦) المعلومات بأنها " معلومات ذات خصائص إلكترونية في شكل نصوص أو رموز أو أصوات أو رسوم أو صور أو برامج حاسب إلى أو غيرها من قواعد البيانات " [٦]

كما عرّف المعلومات في قانون المعاملات الإلكترونية الاردني رقم (٨٥) لسنة (٢٠٠١) في المادة الاولى منه بأنها " البيانات والنصوص والصور والاشكال والاصوات والرموز وقواعد البيانات وبرامج الحاسوب وما شابه ذلك " [٧] ، كذلك عرّفت الفقرة الثانية عشرة من المادة الاولى من مشروع قانون جرائم الإلكترونية العراقي لسنة (٢٠١١) المعلومات بأنها "المعلومات والبيانات والنصوص والصور والاشكال والاصوات والرموز وقواعد البيانات وبرامج الحاسوب

---

(١) يُنظر المادة (٣٨٢) من قانون العقوبات الاماراتي رقم ٣لسنة ١٩٨٧المعدل.

(٢) يُنظر المادة (٣٩٩) من قانون العقوبات الاردني رقم ١٦ لسنة ١٩٦٠.

(٣) يُنظر: المادة (٤٣٩) من قانون العقوبات العراقي رقم ١١١لسنة ١٩٦٩المعدل.

(٤) يُنظر: الفقرة عاشراً المادة الثانية من قانون المعاملات الموحد الامريكي لسنة ١٩٩٩.

(٥) يُنظر: المادة الاولى من مرسوم بقانون اتحادي رقم ٢لسنة ٢٠١٢.

(٦) يُنظر: المادة الاولى من قانون المعاملات والتجارة الإلكترونية رقم ١لسنة ٢٠٠٦.

(٧) يُنظر: المادة الاولى من قانون المعاملات الإلكترونية الاردني رقم ٨٥لسنة ٢٠٠١.

وما شابه ذلك التي تنشأ أو تخزن أو تعالج أو ترسل بالوسائل الإلكترونية " [1]. نجد المشرع العراقي في مشروع الجرائم الإلكترونية تعريفه أوسع وأشمل من باقي تعريفات التشريعات السابقة .

على الرغم من تعدد تعريف جريمة سرقة المنصات الإلكترونية واختلافها من حيث الصياغة لكنها تتفق من حيث المضمون فقد تبنى كل تعريف منها بحسب معطيات كل دوله ، وجانب من الفقه عرّفها من الناحية الفنية ، والجانب الآخر عرّفها من الناحية القانونية ، وهناك من عرّفها حسب موضوعها ووسيلة ارتكابها وتوافر المعرفة بتقنية المعلومات لدى مرتكبها [2] .

نستنتج مما تقدم على الرغم من أختلاف تعريف سرقة معلومات المنصات الإلكترونية إلا أن كل مشرّع عرّفها بحسب المفهوم الذي يراه ، ومشروع قانون الجرائم الإلكترونية العراقي لسنة (٢٠١١) كان موفقاً في تعريفه فقد كان أوسع وأشمل من بقية تعاريف القوانين الاخرى ، والباحث يعرف سرقة معلومات المنصات الإلكترونية بأنها عبارة عن أفعال غير مشروعة تكون معلومات المنصات الإلكترونية محلاً لارتكابها ، والمنصات الإلكترونية تكون البيئة التي ترتكب بواسطتها سرقة معلوماتها .

الفرع الثاني

جريمة سرقة معلومات المنصات الإلكترونية على المستوى الفقهي والقضائي

يتجلى محل سرقة المنصات الإلكترونية في الصفة المادية أن يكون مالاً ، وهو كل شيء يصلح محلاً لحق عيني ، ويمكن حيازته حيازة مادية والسيطرة عليه ومباشرة السلطة المادية عليه من قبل الجاني ، ومحل السرقة أن يكون منقولاً ولا يمكن إتلافه عند نقله من مكان إلى آخر والعله في ذلك إن فعل الاختلاس يتطلب اخراج الشي من حيازة المجنى عليه وتغير موضعه ، كذلك يكون محل السرقة مملوك لغير الجاني ، إذ لا تتحقق جريمة السرقة إذا كان المال مملوكاً للجاني ، وأغلب النظم القانونية اتجهت التوسع في دلالة تعبير المال أو الشيء المادي ، في نصوص صريحه في قوانين العقوبات التي أدخلت في نطاقها القوى المحرزة مثل الطاقة

([1]) يُنظر: الفقرة الثانية عشر المادة الاولى من مشروع قانون الجرائم الإلكترونية العراقي لسنة ٢٠١١.

([2]) يُنظر: د. عبد الفتاح بيومي حجازي ، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي ، ط١، دار النهضة العربية ، القاهرة ، ٢٠٠٩، ص١١.

الكهربائية ، اما على عدَّها ذات كيان مادي ملموس تصلح لأن تكون محلاً في جريمة السرقة أو على اعتبار قيمة الكهرباء وأن كانت مجرد حالة للمادة [١]

والفقه والقضاء مستقر على أن المال الإلكتروني يصلح أن يكون محلاً في جريمة السرقة وعند تطبيق النصوص التقليدية على جريمة السرقة لا تثير أي أشكال أو صعوبة ، لكننا بصدد الحديث عن الحماية الجزائية للمنصات الإلكترونية في حالة تعرّض المنصات الإلكترونية لجريمة السرقة وارتكاب الجريمة ضد مادتها الإلكترونية التي تكون على شكل معلومات مخزنه داخلها أو تكون تابعة لنظامها الإلكتروني التي تأخذ شكلاً معنوياً غير ملموس ، ففي هذه الحالة تثار لدينا الاشكالية حول المال الإلكتروني على عدَّه المكونات المعنوية للمنصات الإلكترونية من معلومات صالحة لأن تكون محلاً في جريمة السرقة [٢] ، وهذه الاشكالية أثارت الجدل على المستوى الفقهي والقضائي، عند عدّ المال الإلكتروني محلاً لجريمة السرقة يجب أن نفرق بين أمرين وهما:

الامر الاول : المال الإلكتروني الطبيعي ذو الملمس المادي ويشمل أدوات الحاسب الآلي والمعلومات ، وفي حال ارتكاب الجريمة فإنها ترتكب على مال مادي ، وبالتالي يمكن أن نطبق نصوص جريمة السرقة التقليدية عليها [٣].

الامر الثاني : سرقة معلومات المنصات الإلكترونية بذاتها هل من الممكن أن تنطبق عليها نصوص جريمة السرقة التقليدية أم لا؟ ، وهل يمكن عدها سرقة أم لا؟ [٤].

نتيجة لذلك فقد أنقسم الفقه والقضاء على أتجاهين معارض ومؤيد حول صلاحية المنصات الإلكترونية لأن تكون محلاً لجريمة السرقة الإلكترونية ومدى انطباق النصوص التقليدية عليها.

أولا: الاتجاه الاول عدم صلاحية معلومات المنصات الإلكترونية لأن تكون محلاً لجريمة السرقة

جانب من الفقه الفرنسي يؤيد تطبيق القانون التقليدي الذي يقر بوصف المال على الشيء المادي بحد ذاته ، و يرفض أن تكون المعلومات التي يتم تداولها إلكترونياً أن تكون محلاً في

---

(١) يُنظر: د. محمود رجب فتح الله ، مصدر سابق ، ص٣٣٦.

(٢) يُنظر: د. عمر أبو الفتوح عبد العظيم الحمامي ، مصدر سابق ، ص٥٢٤

(٣) يُنظر: د. محمد عبيد الكعبي ، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت ، مصدر سابق ، ص٢٠٤.

(٤) يُنظر: د. عبدالفتاح بيومي حجازي ، جرائم الكمبيوتر والانترنت في القانون العربي النموذجي (دراسة قانونية متعمقة في القانون المعلوماتي) ، ط١، دار الكتب القانونية ، مصر ، ٢٠٠٧، ص٢٣٣.

جريمة السرقة ؛ بسبب طبيعة المعلومات ذاتها وان جريمة السرقة معروف عنها انها ترد على حق الملكية وفعل الاختلاس أي محل الاعتداء يكون على حقوق الافراد ، وانصار هذا الاتجاه يرون المعلومات على انها ملكية عامة فكيف يتم نسبتها إلى أحد مستندين إلى العديد من الحجج[١] .

١- محل جريمة السرقة يكون ذات طبيعة مادية في الاصل وفرصة الاعتداء والاستغلال وانتقال الحيازة تكتسب من خلال الخاصية المادية للأشياء ، أي صعوبة الاعتراف بالاشياء المادية بطبيعتها غير المحسوسة وصعوبة تملكها وحيازتها [٢] .

٢- ان هذا الاتجاه يزيد في تبرير معارضتهم أو رفضهم قابلية المعلومات للسرقة ، لافتراضهم ان فعل الاختلاس يتم من خلال انتقال الحيازة للشيء من شخص لآخر ، وهذا الامر لا يمكن ان يتحقق أو يقع على المعلومات إلا في حالة الوقوع على الوسط المادي الذي يتم من خلاله تخزين المعلومات عليه، والحصول بطريقة غير مشروعة على المعلومات وبدون علم مالكها [٣].

وأكد القضاء ذلك من خلال الاستقراء لأحكام القضاء الانكليزي الصادرة بهذا الموضوع على سبيل الاستدلال [٤].

أما في فرنسا فقد أكدت محكمة استئناف باريس حكمها التي رفضت فيه التشابه بين سرقة التيار الكهربائي وفك شفرة البرامج، وعدَّت الاول بحاجة إلى دعامة مادية للانتقال من خلالها ، أما الثاني يرد على الموجات الكهرومغناطيسية ، مما يدل على أنها ليس لها أي دعامة مادية ، والمحكمة قد أقرت أن سرقة الكهرباء وسرقة المعلومات تفترض وجود دعامة مادية أياً كانت نوعها ، وهذا غير متوفر في موضوع الدعوى محل النظر، والقضاء الفرنسي بقى لمدة من

---

(١) يُنظر: د. مدحت عبدالحليم رمضان ، جرائم الاعتداء على الاشخاص والانترنت ، ط١، دار النهضة العربية ، ٢٠٠١، ص٣٢.

(٢) يُنظر: د. عبدالفتاح بيومي حجازي ، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي ، مصدر سابق ، ص٢٦٦.

(٣) يُنظر: د. فتوح الشاذلي ، عفيفي كامل عفيفي ، مصدر سابق ، ص١٥٠.

(٤) نجد جانب منها قد رفض فكرة أن معلومات المنصات الإلكترونية كمحل لجريمة السرقة وذلك من خلال الحكم الصادر من محكمة جنح ليفربول التي قررت عدم جعل المعلومات أموالاً ، وأيد ذلك من قبل محكمة الاقليم وجاء في حكمها أنه " إذا كان من الممكن إعطاء المالك حقوق محدودة فيما يتعلق بالمعلومات والتي يمكن أن تدعم من قبل القانون المدني، فان المعلومات ليست أموالاً وتبعاً لذلك لا تصلح لأن تكون محلاً للسرقة" نقلاً عن : د. عمر أبو الفتوح عبدالعظيم الحمّامي ، مصدر سابق ، ص٦٢٤.

الزمن يتبنى الموقف الرافض لفكرة وصف الأموال على المعلومات الإلكترونية ، والتي عدَها محلاً لجريمة السرقة ، وأقرت ذلك محكمة غرونوبل " بعدم وجود ما يسمح بقيام جريمة سرقة الدسكات لعدم وجود أي دعامة مادية للمعلومات"[١].

يتضح لنا مما تقدم ان القضاء الفرنسي يؤكد على ان يكون فعل الاختلاس واقع على أشياء لها ملمس مادي لكي يتحقق فعل الاستيلاء عليها وصدوره من قبل الفاعل ، كما انها رفضت الحكم بالتجريم على محل السرقة الذي يتمثل في معلومات غير منسوخة على دعامة مادية ، لان الدعامة المادية تصلح لان تكون محلاً للسرقة.

ثانياً: الاتجاه الثاني صلاحية معلومات المنصات الإلكترونية لأن تكون محلاً لجريمة السرقة

أنصار هذا الاتجاه استندوا في تأييدهم إلى فكرة قابلية معلومات المنصات الإلكترونية أن تكون محلاً لجريمة السرقة في الرجوع إلى العديد من الأحكام القضائية التي اقرت بهذه الفكرة ، وذلك من خلال الاعتداء عليها بشكل سلبي وغير شرعي على المحتوى الإلكتروني المكون لجريمة السرقة واستند انصار هذا الاتجاه على العديد من الحجج:

١- تجريم سرقة معلومات المنصات الإلكترونية والاعتراف بفكرتها لا يعد اعتراضاً على مبدأ شرعيتها على العكس يعد ذلك تأكيداً لها ، وفعل الاختلاس الذي يقع على المعلومات يتم تحديده طبقاً لطبيعة الشيء الذي يصلح محلاً لجريمة السرقة ، وهذا ما أكده القضاء الفرنسي ، بينما الاستيلاء يتحقق من خلال الاطلاع على المعلومات أو عن طريق النسخ غير المشروع لها الذي يتم دون علم مالكها ، وبهذا يتحقق لنا فعل الاعتداء الذي يتطابق مع الطبيعة لمحل الجريمة[٢].

٢- امكانية حيازة معلومات المنصات الإلكترونية عبر الالتقاط الذهني عن طريق البصر، على الرغم من أن موضوع الحيازة للمعلومات غير مادي ، لكن في هذه الحالة من

([١]) نقلاً عن : د. نائلة محمد فريد قورة ، جرائم الحاسب الالي الاقتصادية (دراسة نظرية وتطبيقية) ، ط١، منشورات الحلبي الحقوقية ، بيروت ، ٢٠٠٥، ص١٤٥.

([٢]) يُنظر .د. فتوح الشاذلي ، عفيفي كامل عفيفي ، مصدر سابق ، ص١٥١

الممكن انتقالها على الرغم من عدم حيازتها [1] ، ومثلها في ذلك مثل التيار الكهرباء الذي يُعدَّ شيئاً مادياً قابل للانتقال على الرغم من عدم حيازته [2]،

٣- وبالرجوع إلى النصوص التقليدية الخاصة في جريمة السرقة فان فعل الاختلاس يقع على الاشياء المادية القابلة للحيازة والانتقال ، كما ان النصوص التقليدية وضعت في ظروف لا تقبل إلا ان يكون محل جريمة السرقة يتصف بالشكل المادي ،ويعد ذلك قصوراً تشريعياً لا يواكب التطورات الحديثة ، فالجرائم المستحدثة التي يتعرض لها العالم الافتراضي أظهرت مفهوم جديد للسرقة وهو "سرقة المنفعة "، ومفادها يمكن ان يتم الاعتداء على المعلومات من دون الحاجة إلى تحقق الوصف المادي من أجل الاعتداء على الحيازة[3] ،

وقد ذهب انصار هذا الاتجاه في تبريرهم وقناعتهم حول امكانية وقوع جريمة السرقة على المعلومات الإلكترونية ، من خلال نشوء فكرة حق الملكية والانفصال عن الدعامة المادية ، وان المعلومات تتمتع بقيمة اقتصادية تترجم في وصف المال ، وخير مثال لها جريمة السرقة لبطاقات العملاء التي تم عدَّها من قبيل البضائع ، إذ تكتسب القيمة المالية من خلال ما تحتويه من معلومات ، التي تصلح ان تكون محلاً لجريمة السرقة[4].

يتضح لنا مما تقدم ان الاعتراف بفكرة معلومات المنصات الإلكترونية بأن تأخذ وصف الاموال ، هو عين الصواب وان الاحكام القانونية تجرّم كل فعل من الافعال غير المشروعة التي تعتمد على الاسلوب والشكل للفعل الإجرامي ، وجريمة سرقة

([1]) يُنظر: د. محمد عبيد الكعبي ، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت ، مصدر سابق ، ص٢٠٩.

([2]) التيار الكهربائي يعتبر شيئاً مادياً يخضع للسيطرة كغيره من الاشياء المادية فهي تعبأ وتنقل وتحاز وتقاس ويتحكم فيها سواء بالاستهلاك أو عدمه وترد عليها الملكية ، وكل هذا يؤكد بوضوح ضرورة صلاحيتها كمحل للاختلاس وهذا ما يجتمع عليه الفقه الآن ويؤكده القضاء دائماً ، ومبدأ اعتبار الكهرباء شيئاً مادياً يصلح كمحل للاختلاس ، يمكن أن يطبق على كل قوة أو طاقة تخضع لسيطرة الانسان ويمكن له التحكم فيها على النحو الذي يحقق منفعته يُنظر: د. علي عبد القادر القهوجي ، جرائم الاعتداء على الانسان والمال ، قانون العقوبات القسم الخاص ، ط١، منشورات الحلبي الحقوقية ، بيروت ، ٢٠١٠، ص٣٢٥.

([3]) يُنظر . د. محمد حماد مرهج الهيتي ، التكنولوجيا الحديثة والقانون الجنائي ، ط١، دار الثقافة ، الاردن ، ٢٠٠٤، ص١٩٧.

([4]) يُنظر .د. عبدالله عبد الكريم عبدالله ، جرائم المعلوماتية والانترنت (الجرائم الإلكترونية) ، ط١، منشورات الحلبي الحقوقية ، بيروت ، ٢٠٠٧، ص١٥.

معلومات المنصات الإلكترونية ، فأنها تمثل فعلاً خطيرً جداً خصوصاً واننا امام تطور كبير في العالم الإلكتروني ، مما يتطلب من المشرع التدخل وتوفير الحماية الجزائية الفعالة ضد الركن المادي في جريمة سرقة معلومات المنصات الإلكترونية المتمثل بفعل الاختلاس ، ونية التملك لمعلومات المنصات الإلكترونية .

فقد اكدت الاحكام القضائية الصادرة من محكمة ولاية تكساس والتي عاقبت فيها أحد العاملين السابقين في شركة Texas Instruments Automatic Computer Corp في القضية التي عرفت باسم قضية Hancock V. Texas ومفادها أن العامل قام بعملية سرقة لكمية من اسطوانات الكمبيوتر التي قام ببيعها إلى واحدة من الشركات المنافسة لها ، وان قانون ولاية تكساس يعاقب على السرقة للأشياء المملوكة اذا كانت قيمة المسروق بلغت خمسين دولار ، وقيمة الاسطوانات المسروقة هي لا تساوي أكثر من خمسة وثلاثين دولار لذلك لم تتحقق الجريمة ، لأن القيمة الحقيقية للبضائع التي تمت سرقتها لا تتمثل في هذه الشرائط بل بما موجود فيها من معلومات ، وعلى هذا الاساس استندت المحكمة في حكمها إلى ان المعلومات الموجودة على الشرائط تُعدَّ استيلاءً حقيقياً على حق من حقوق الملكية بالمعنى الدقيق[١].

اما في فرنسا فإن أحكام القضاء لم تستمر على موقفها الرافض أو المتردد الذي اشرنا اليه سابقاً بل كان لها رأي مخالف للسابق من خلال صدور مجموعة من الاحكام القضائية ، وهذه الاحكام اعترفت بقابلية المعلومات بأن تكون محلاً لجريمة السرقة [٢] وأكدت ذلك من خلال موقفها الصريح بقضية "Antonioli" الذي كان يعمل محاسباً إدارياً في أحد المشروعات عندما قام المتهم بحكم وظيفته بسرقة مستندات حسابية كانت بحوزته وتسليم هذه المستندات إلى شخص ثالث من دون علم رب العمل بذلك ، من أجل انشاء شركة منافسة أذ تمت ادانته بجريمة السرقة من قبل محكمة استئناف pau بسبب قيامه بالاختلاس للمعطيات الحسابية والتجارية المدونة على المستندات ، وقام بتوصيل هذه المعطيات والتي تُعدُّ أموالاً معنوية تم تسليمها لغيره وهي مملوكة لرب العمل[٣] .

---

(١) يُنظر .د. عمر أبو الفتوح عبد العظيم الحمامي مصدر سابق ، ص٦٢٨-٦٢٩.

(٢) يُنظر: د. فتوح الشاذلي ، عفيفي كامل عفيفي ،مصدر سابق ، ص١٥٠

(3).Catala, les transformatique de droit par l'informatiqud emergence du droit de l'informatique et des parques,1983,p264.

اما في قضية "doqualiax" الذي كان يعمل موظفاً وقام بتصوير مستندات سرية من دون علم صاحبها ، فإن المحكمة لم تقم بإدانته لسرقته المستند بل ادانته المحكمة بسبب سرقة المعلومات التي كانت مدونة عليها[1].

يتضح لنا مما تقدم ذكره أن الحكم الاول بقضية" Hancock V. Texas" واضح وصريح على وقوع التجريم على المعلومات وحدها، لا على الشريط أو القرص بل على المعلومات الموجودة في هذا الشريط ، التي عدتها المحكمة استيلاء بالمعنى الحقيقي للملكية ، اما بالنسبة للحكم الثاني في قضية "Antonioli"نجد عدم الوضوح فيما إذا كان الحكم الصادر يتعلق بسرقة المعلومات ذاتها او يتعلق بسرقة المستند المادي الذي يحتوي المعلومات ، اما في الحكم الثالث الصادر في قضية "doqualiax" نجد ان المحكمة واضحة في حكمها بتجريم سرقة المعلومات ذاتها ، ونلاحظ في جميع الاحكام التي صدرت انها تشترك في ان المعلومات التي تم نقلها وحدها تكفي لان تكون محلا لجريمة سرقة معلومات المنصات الإلكترونية.

المطلب الثاني

أركان جريمة سرقة معلومات المنصات الإلكترونية

في جريمة سرقة معلومات المنصات الإلكترونية أركان يجب تحققها حتى نستطيع محاسبة فاعلها حسب النصوص التشريعية للدول الاجنبية والعربية ، لذا يستلزم علينا بيان ركن الاختلاس المتمثل في السلوك المادي للجريمة فضلاً عن بيان خصوصية الركن المعنوي من خلال بيان القصد الجرمي العام والقصد الجرمي الخاص لهذهِ الجريمة وعليه سنقسم هذا المطلب على فرعين نتناول بالفرع الاول الركن المادي في جريمة سرقة معلومات المنصات الإلكترونية وفي الفرع الثاني نتناول الركن المعنوي في جريمة سرقة معلومات المنصات الإلكترونية.

([1]) يُنظر: د. عبدالفتاح بيومي حجازي ، النظام القانوني للحكومة الإلكترونية ، ك٢، ، دار الكتب القانونية ، ٢٠٠٧، ص٢٨٧.

الفرع الاول

الركن المادي في جريمة سرقة معلومات المنصات الإلكترونية

يتكون الركن المادي في أي جريمة من عناصر ثلاثة وهي سلوك إجرامي ونتيجة جرمية وعلاقة سببية سواء كانت جريمة تقليدية أو جريمة إلكترونية ، إذ يتمثل السلوك الإجرامي في جريمة سرقة معلومات المنصات الإلكترونية في الدخول غير المرخص به لمعلومات المنصات الإلكترونية وقيام الجاني بنسخها والاستيلاء عليها ونقلها ، والنتيجة الاجرامية تتمثل في التغير الذي يحدث في العالم الخارجي كأثر لسلوك الجاني ، والعلاقة السببية في جريمة سرقة معلومات المنصات الإلكترونية تمثل الرابطة بين السلوك الاجرامي للجاني والنتيجة الإجرامية المتحققة عنها نسخ معلومات المنصات الإلكترونية والاستيلاء عليها ونقلها ، وعليه سنبين عناصر الركن المادي في جريمة سرقة معلومات المنصات الإلكترونية تباعاً.

أولاً: السلوك الإجرامي في جريمة سرقة معلومات المنصات الإلكترونية

يتجلى السلوك الإجرامي للركن المادي في جريمة سرقة معلومات المنصات الإلكترونية في اختلاس معلومات المنصات الإلكترونية بمختلف أنواعها سواء كانت معلومات خاصة أي شخصية أم عامة تخص الفرد أم المجتمع أم الحكومة ، ويتم فعل الاختلاس للمعلومات بذاتها أما بالتقاطها ذهنياً أو بنسخها أو التقاط الموجات الكهرومغناطيسية الحاملة لتلك المعلومات ومدى اعتراف الفقه والقضاء بركن الاختلاس

١- الاعتراف بركن الاختلاس وموقف القضاء منه

ان بعض احكام القضاء التي استقرت على الاعتراف بفعل الاختلاس الذي يرد على المعلومات يتمثل في صعوبة اثبات انتقال الحيازة فيها ، فقد سنت الولايات المتحدة الامريكية قوانين خاصة وسعت لتعديل قوانينها العقابية بما يكفل تجريم السلوك الإجرامي في الجرائم الإلكترونية مع بعض التباين في قوانينها سواء في صور السلوك المجرم أو ألية التعامل مع محل الاعتداء فقد صدر قانون جرائم الكمبيوتر لسنة ١٩٨٦من أجل مواجهة التطور السريع والحديث في جريمة السرقة ، كما توسع القضاء في تطبيق أحكام السرقة على اختلاس المعلومات الحكومية المتوفرة على قاعدة الخدمات الحكومية ونسخ بعض برامج الحاسب الآلي [1] ، كما رفض جانب من القضاء عدَّ نسخ المعلومات أو الاطلاع عليها والتي تكون مسجلة في الحاسب الآلي مشكلاً

([1]) يُنظر: د. علي عبود جعفر ، مصدر سابق ، ص ١٤٣.

وعائقاً في جرائم الاموال ، فقد اصدر القضاء الامريكي احكاماً لعملية نسخ المعلومات السرية التي تخص بعض المرضى في احدى المستشفيات ، واستبعد وقوع جريمة السرقة على هذه المعلومات واستند في حكمة إلى عدم عدَّ الومضات الإلكترونية من قبل الاشياء المادية يرد عليها فعل السرقة[١] ، اما القضاء الفرنسي فقد تردد حول توافر الاختلاس في جريمة السرقة وذلك قبل صدور قانون رقم (٣) لسنة (١٩٨٥)اما بعد صدور القانون الذي تم ذكرة فقد عاقب القضاء الفرنسي كل من يقوم بسرقة المعلومات والبرامج الإلكترونية لكن في نطاق حماية حق المؤلف ومع وجود النص فإنه لا يمكن الاجتهاد[٢] ، اصدرت محكمة النقض الفرنسية حكمها في قضية (Logabax) في عام (١٩٧٩) والتي قررت فيه بأن إعادة إنتاج مستندات من دون علم ورضا مالكها أو حائزها الشرعي تشكل جريمة سرقة لأن مرتكب هذا الفعل كان مستخدماً بأحد المشروعات وقام بنسخ المستندات السرية التي تحتوي على خطة وهيكلة المشروع وقد استولى عليها عن طريق الغش أثناء المدة اللازمة لإعادة إنتاجها[٣] ،لكن محكمة أول درجة كان لها حكم مختلف بما إنه لا يوجد قانون يعاقب على سرقة المنفعة ، وان المتهم لم يقم بحمل هذه المستندات واخذها الى بيته على سبيل تملكها لذلك برأت المتهم من وقوع جريمة السرقة وعدم توفر ركن الاختلاس في هذه الحالة ، لكن محكمة النقض الفرنسية نقضت حكم محكمة أول درجة ، لوجود مخالفة صريحة في القانون ، والقانون لم يشترط لتوافر الاختلاس في جريمة السرقة الاخذ أو الانتزاع للشيء ، ووقوع الاختلاس يمكن تحققه حتى لو كان الشيء بيد الجاني على سبيل اليد العارضة وقبل الاستيلاء عليه[٤].

نلاحظ مما تقدم أن القضاء الفرنسي ذهب في اتجاهين الاتجاه الاول تردد في تجريم الاختلاس للمعلومات والبرامج ولم يعدّ حدوث جريمة السرقة قبل صدور قانون رقم ٣ لسنة ١٩٨٥، أما الاتجاه الثاني بعد صدور القانون المشار إليه فقد جرّم القضاء الفرنسي جريمة السرقة التي تقع على المعلومات والبرامج ، وبالتالي ممكن تحقق جريمة سرقة معلومات المنصات الإلكترونية لأن الاختلاس يتحقق بمجرد الأخذ أو بانتزاع الشي.

---

(١) يُنظر: شمسان ناجي صالح الخيلي ، مصدر سابق ، ص١٨٧- ١٨٨

(٢) يُنظر .د. عبدالفتاح بيومي حجازي ، النظام القانوني للحكومة الإلكترونية ، مصدر سابق ، ص٢٦٩.

(٣) يُنظر: د. محمد عبيد الكعبي ، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت (دراسة مقارنة) ، مصدر سابق ، ص٢٠٧- ٢٠٨.

(٤) يُنظر: د. فتوح الشاذلي ، عفيفي كامل ، مصدر سابق ص١٣٢.

٢- الاعتراف بركن الاختلاس وموقف الفقه منه

الاختلاس الذي يقع على المكونات المادية للنظام الإلكتروني من الاجهزة الإلكترونية وملحقاتها التي يتم الاستيلاء عليها من دون رضا مالكيها من أجل تملكها تكون خاضعة لقواعد جريمة السرقة التقليدية إذ تقوم بها جريمة السرقة ، إذا توافرت أركانها لكن الخلاف حول المكونات المعنوية ومدى خضوعها وتعرضها لفعل الاختلاس ومعرفة قابلية معلومات المنصات الإلكترونية للاختلاس [١]

أ- قابلية معلومات المنصات الإلكترونية للاختلاس :

يذهب انصار هذا الاتجاه إلى قبول فكرة صلاحية تعرض معلومات المنصات الإلكترونية للاختلاس بسبب تقبلهم لفكرة عدَّ المعلومات أموالاً معنوية لها قابلية التملك والحيازة إذ أنها قابله للاختلاس والاعتداء عليها بأي شكل من الاشكال ، وهذا الرأي أذا تمعنا به نجده يرجعنا إلى سند أخر يمكننا الاستناد إليه في أن المعلومات ذات طبيعة مادية على أساس أنها تمثل مالاً منقولاً قياساً بسرقة الكهرباء التي تمثلها الومضات الكهربائية عن طريق الاسلاك[٢] ، وبالتالي يمكن أن نحدد قيمة وكمية المعلومات المختلفة من خلال الدعامة المادية التي تصلح لفعل الاختلاس الذي يقوم كمحل في جريمة السرقة[٣]، وبرز من يؤيد هذا الاتجاه بتحقق فعل الاختلاس على المعلومة الذي جاء وفقاً للنظرية الحديثة للفقيه جارسون Garcon الذي عرف الاختلاس من خلال فكرة الحيازة بأنواعها الثلاثة الحيازة الكاملة والناقصة واليد العارضة ، بأنه الاستيلاء على الحيازة الكاملة بعنصريها المادي والمعنوي في الوقت نفسه ودون رضا مالكه أو حائزه ، إذ ربط بين الحيازة ومفهومها في القانون المدني ، وبذلك فقد وسع من مدلول الاختلاس بعدم اشتراط نقل المال مادياً أو نزعه من حيازة مالكه إلى حيازة الجاني حيازة تامة[٤] ، ووفقاً لهذه النظرية ممكن أن يتحقق فعل الاختلاس في جريمة السرقة حتى في حالة عدم قيام الجاني في أي سلوك مادي

---

(١) يُنظر: د. محمد عبيد الكعبي ، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت (دراسة مقارنة) ، مصدر سابق ، ص٢١٥-٢١٦.

(٢) يُنظر: .د. إبراهيم محمد منصور ، الجرائم الإلكترونية في الشريعة الإسلامية والقوانين الوضعية بحث فقهي مقارن ، ط١، دار الفكر الجامعي ،٢٠١١، ص٢٩.

(٣) يُنظر: .د. عبدالفتاح بيومي حجازي ، النظام القانوني للحكومة الإلكترونية ، مصدر سابق ، ص٢٦٠

(٤) يُنظر: د. علي عبد القادر القهوجي ، مصدر سابق ، ص٢٨٧.

ملموس لنقل حيازة الشيء محل الجريمة ، وبالتالي يمكن أن نطبق ذلك فعل الاختلاس على سرقة معلومات المنصات الإلكترونية كقاعدة عامة [١]

واذا نظرنا إلى طبيعة المعلومات بعدَّها أموالاً معنوية يمكننا القول ان ذلك يخلق لنا مبرراً يؤدي لحدوث فعل الاختلاس في جنس الشيء محل الاختلاس ، والاشياء المعنوية التي يمكن اختلاسها باستخدام السلوك المادي من خلال عملية نسخ أو تصوير التي تتم عن طريق انتقال المعلومات من الأصل إلى الصورة ، كذلك ممكن أن يتحقق الاختلاس الإلكتروني الذي يتم بوساطة المنصات الإلكترونية ووسائل النظم الإلكترونية عبر تعديل المعلومات المخزنة إلكترونياً فيها أو مسحها لتحقق للجاني العناصر الايجابية في ذمته المالية ، وبهذا يحصل الجاني على الاموال وإخراجها من ذمة صاحبها أو حائزها الشرعي وادخالها في ذمته ، أما المعلومات وما تملكها من قابلية للانتقال والتداول في الأسواق حالها حال السلع والبضائع لاستحواذها على قيمة اقتصادية ومماليه كبيرة [٢] .

وأكد أنصار هذا الاتجاه في الحكم الصادر من محكمة النقض الفرنسية في قضية بوركان Bourquin التي تتلخص واقعتها في ، قيام عاملين من عمال المطبعة بتصوير سبعة وأربعين شريطاً بأدواتهما تتعلق بالعملاء الاثرياء الذين يتعاملون مع المطبعة ، ولم يتوقفوا عند هذا الحد بل قاما بأخذ سبعين شريطاً أخرى والقيام بتصويرها خارج المطبعة وعلى ماكنتهم الخاصة ، من أجل إنشاء شركة منافسة للشركة السابقة التي كانوا يعملون بها ، وبعد ذلك تمت ادانتهم من المحكمة بتهمة السرقة لتوافر أركان جريمة السرقة ضدهما [٣]

نلاحظ مما تقدم امكانية تحقق اختلاس معلومات المنصات الإلكترونية وهذا ما ايده الفقيه جارسون من خلال تعريف الاختلاس في النظرية الحديثة التي جاء بها والتي شمل فيها تحقق الاستيلاء على الحيازة بعنصريها المادي والمعنوي على حد سواء من دون علم صاحبها ، أما وجهة النظر القائلة حول رفض وصف الاختلاس على شيء له قيمة اقتصادية ، رفض بعيد عن الواقع بلا نقاش ، وبالتالي فإنه يعتد بالمعلومات باعتبارها أموالاً إلكترونية وحمايتها جزائياً وأجبه من جميع انواع الاعتداء التي تتعرض لها معلومات المنصات الإلكترونية.

([١]) يُنظر: د. فتوح الشاذلي ، عفيفي كامل ، مصدر سابق ، ص١٤٤.

([٢]) يَنظر: د. أحمد خليفة الملط ، الجرائم المعلوماتية ، ط٢، دار الفكر الجامعي ، مصر ، ٢٠٠٦، ص٢٥٥.

([٣]) يُنظر: د. فتوح الشاذلي ، عفيفي كامل ، المصدر نفسه ، ص١٤٧.

ب ـ عدم قابلية معلومات المنصات الإلكترونية للاختلاس

بعد ان بينا قابلية المعلومات للاختلاس من قبل جانب من الفقه الان سنبين عدم قابلية معلومات المنصات الإلكترونية للاختلاس فقد ذهب انصار هذا الاتجاه إلى الفكرة المادية للاختلاس ،وقيام جريمة السرقة في صورتها التقليدية ، وانهم يرون ضرورة أن يتحقق السلوك المادي فعلاً من خلال نقل الشيء أو أخذه أو نزعه من مالكه ، إذ يتضمن ذلك تغيراً في الحيازة القانونية ويحدث في بعض الحالات التي يتحقق فيها الاختلاس حتى في حالة عدم أخذ الشيء من صاحبه ؛ لأنه في هذه الحالة يكون تحت اليد العارضة وهذا لا ينفي عن المحل صفته المادية في أن اليد العارضة تفترض على وجود الشيء في يد الشخص وهذا يعد دليلاً على ماديته(١).

ويستند أنصار هذا الاتجاه برفض الحكم الصادر من محكمة استئناف باريس عام ١٩٩٧والمتضمن عدم تطبيق نصوص السرقة عليه ، وأكدت المحكمة على أن الاختلاس يفترض خروج الشيء من حيازة مالكه الاصلي ، في هذه الحالة فإن المعلومات ماتزال في حيازة مالكها، كذلك عدم توافر القصد الجرمي الخاص في جريمة السرقة والجاني لم يقصد من سلوكه حرمان مالك المعلومة الاصلي منها بصورة دائميه (٢)

يتضح لنا مما تقدم ان معلومات المنصات الإلكترونية يمكن وقوعها وتعرضها لفعل الاختلاس من خلال التعمق بطبيعة الموضوع وحداثة الجرّم الامر الذي يفرض على المشرع العراقي مواكبة الاساليب الحديثة للجرائم التي تتعرض لها معلومات المنصات الإلكترونية إذ ان القصور التشريعي في النصوص التقليدية لا يتماشى مع حداثة هذه الجرائم ، ومن أجل توفير الحماية الجزائية لمعلومات المنصات الإلكترونية الحديثة ومن دون التعصب للقاعدة التقليدية ، وان اغلب التشريعات سعت إلى استحداث نصوص تجرّم الاعتداء على الانظمة الإلكترونية مثل الولايات المتحدة الامريكية وفرنسا والامارات العربية المتحدة والاردن، أما العراق فيعاني من قصور تشريعي على الرغم من وجود مشروع قانون الجرائم الإلكترونية الذي بقى حبيس رفوف مجلس النواب عام ٢٠١١ فقد اصبح التصويت عليه ضرورة ملحة .

نستنتج مما تقدم أن جريمة سرقة معلومات المنصات الإلكترونية ذات طابع خاص ، لذا ندعو المشرع العراقي إلى التصويت على مشروع قانون الجرائم الإلكترونية لسنة ٢٠١١ ، كما نقترح اضافة فقرة ثانية للمادة السابعة تكون الفقرة بالشكل الآتي :

---

(١) يُنظر .د. جميل عبدالباقي الصغير ، القانون الجنائي والتكنولوجيا الحديثة ، ط١، ك١، دار النهضة العربية ، ١٩٩٢، ص٦٩.

(٢) يُنظر: د. عمر أبو الفتوح عبد العظيم الحمّامي ، مصدر سابق ، ص٥٦٦.

المادة -٧- يعاقب بالسجن المؤقت وبغرامة لا تقل عن (١٠٠٠٠٠٠٠) عشرة ملايين دينار ولا تزيد على (٣٠٠٠٠٠٠٠) ثلاثين مليون دينار كل من

اولاً- استخدم عمداً نظام الحاسوب أو شبكة المعلومات العائدة للأشخاص أو الشركات أو الهيئات أو المصارف أو الأسواق المالية وتمكن من الاستيلاء على أموال الغير أو حقوقهم المالية أو حقق لنفسه أو لغيره منفعة مالية أو حرم الغير من حقوقه المالية بأية وسيلة من الوسائل الإلكترونية.

ثانياً- كل من توصل عمداً لنظام الحاسب الآلي أو المنصات الإلكترونية العائدة للأشخاص أو الشركات أو مؤسسات الدولة وتمكن من الاستيلاء لنفسه أو لغيره على مال منقول أو المعلومات الخاصة والعامة وأدى ذلك إلى حرمان اصحابها منها بأية وسيلة من الوسائل الإلكترونية .

كما نقترح تعديل نص المادة ٤٣٩بإضافة النظام الإلكتروني لها من أجل مواكبة التطور الحاصل في الجرائم الإلكترونية ، ويصبح نص المادة المقترحة كما يأتي :

المادة ٤٣٩"السرقة اختلاس مال مادي منقول ومعنوي مملوك لغير الجاني عمداً ، ويعدَّ مالاً مادياً ومعنوياً لتطبيق أحكام السرقة النبات وكل ما هو متصل بالأرض أو مغروس فيها بمجرد فصله عنها والثمار بمجرد قطفها والنظام الإلكتروني وكل ما هو مخزّن فيه من معلومات وبرامج والقوى الكهربائية والمائية وكل طاقة أو قوة محرزة أخرى".

ثانياً: النتيجة الإجرامية في جريمة سرقة معلومات المنصات الإلكترونية

تعد النتيجة الإجرامية العنصر الثاني من عناصر الركن المادي في جريمة سرقة معلومات المنصات الإلكترونية ، ولا يمكن أن تتحقق الجريمة تامة مالم تحصل النتيجة الإجرامية المتمثله بالضرر الذي ينجم عن السلوك الإجرامي للجاني [١] ، إذ تتحقق النتيجة الإجرامية بمجرد الدخول غير المرخص به والقيام بسرقة معلومات المنصات الإلكترونية عن طريق نسخ المعلومات والاستيلاء عليها وبهذا تكون النتيجة الإجرامية عنصراً متطلب ولازم في الركن المادي لجريمة سرقة معلومات المنصات الإلكترونية ، الناتج عن السلوك الاجرامي للجاني إذ أن السلوك الاجرامي في جريمة سرقة معلومات المنصات الإلكترونية يتحقق بصورة تلقائية بمجرود وقوع السلوك وأن هذه الجريمة يتحقق الشروع فيها [٢] ، ففي الولايات المتحدة الامريكية اكد تحقق النتيجة الإجرامية وذلك من خلال القضية التي عرضت على القضاء الامريكي ومفادها قيام

---

(١) يُنظر: د. سمير الشناوي ، الشروع في الجريمة (دراسة مقارنة) ، ط١، دار النهضة العربية ، القاهرة ، ١٩٧١، ص٧٨.

(٢) يُنظر: د. معن أحمد محمد الحياري ، الركن المادي للجريمة ، ط١ ، منشورات الحلبي الحقوقية ، بيروت ، ٢٠١٠، ص١٩٤.

بعض الباحثين في شركة pearsall المالكة لبعض المعارف الفنية في شكل تركيبات كيميائية من شأنها تأخير انتشار النيران عند اندلاع الحرائق ، بسرقة الوثائق المسجل عليها هذه الاسرار التجارية وبيعها إلى إحدى الشركات المنافسة لقاء مبلغ أربعين ألف دولار، وكانت شركة pearsall هي الوحيدة التي تمتلك هذا السر التجاري ، مما كان يمنحها ميزة تنافسية كبيرة في هذا المجال ، وقالت المحكمة في حيثيات حكمها أن هذه الوثائق المسروقة خاصة ومملوكة لشركة pearsall وعلى أوراق خاصة بها ، وهي وثائق هامة لها قيمة كبيرة في سوق المعالجة الكيميائية للحريق ، على أنه وأن كان من المهم الأخذ في الاعتبار الشكل الذي تتجسد فيه هذه المعلومات ، فإن القيمة الحقيقية لها هي ذات المعلومات ، وليس مجرد الأوراق المكتوبة أو المسجلة عليها [١] ، كما جرّم النتيجة الإجرامية في جريمة سرقة معلومات المنصات الإلكترونية في المواد (١/٣١١إلى ١٦/٣١١) من قانون العقوبات رقم ١٣٣٦لسنة ١٩٩٢النافذ عام ١٩٩٤ [٢] ، ونص على حماية المعلومات بصورة مباشرة من خلال قوانين حماية الملكية الفكرية والادبية والفنية [٣].

ونجد المشرع الاماراتي اصدر تشريعات تتعلق بتطبيقات الحاسب الآلي وتجرّم الاعتداء على المعلومات ، ومنها القانون الاتحادي رقم ٢لسنة ٢٠٠٦في المادة ١٠ التي نصت على أن " كل من توصل عن طريق الشبكة المعلوماتية أو أحدى وسائل تقنية المعلومات إلى الاستيلاء لنفسه أو لغيره على سند أو توقيع هذا السند..... يعاقب بالحبس مدة لا تقل عن سنة وبالغرامة التي لا تقل عن ثلاثين ألف أو بإحدى هاتين العقوبتين" [٤] ، كما جرّمت المادة ١٢من المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢ استخدام الشبكة المعلوماتية أو نظام المعلومات الإلكتروني أو وسائل تقنية المعلومات بهدف الحصول على معلومات بطاقة ائتمانية أو الكترونية أو حسابات مصرفية [٥] ، اما النتيجة الإجرامية فقد نص عليها قانون العقوبات الأردني في الفقرة الاولى من المادة/

---

(١) ينُظر: د. عمر أبو الفتوح عبدالعظيم الحمّامي ، مصدر سابق ، ص٦٢٧.

(٢) يُنظر: د. حمزة محمد أبو عيسى ، محمد شبلي الشلبي العتوم ، القانون الجزائي الفرنسي ،ط١، دار وائل للنشر والتوزيع ، ٢٠٢٠، ص٢٧٩.

(٣) يُنظر: د. مدحت عبدالحليم رمضان ، مصدر سابق، ص٣٣.

(٤) يُنظر: نص المادة ١٠ من القانون الاتحادي رقم ٢ لسنة ٢٠٠٦.

(٥) تنص المادة ١٢ من المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢ على (يعاقب بالحبس والغرامة أو بإحدى هاتين العقوبتين كل من توصل بغير حق ، عن طريق استخدام الشبكة المعلوماتية أو نظام معلومات إلكتروني أو احدى وسائل تقنية المعلومات ، على أرقام أو بيانات بطاقة ائتمانية أو إلكترونية أو أرقام أو بيانات حسابات مصرفية ، أو أي وسيلة من وسائل الدفع الإلكتروني ، وتكون العقوبة الحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن مائة ألف درهم ولا تجاوز ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين ، إذا قصد من ذلك استخدام البيانات والارقام في الحصول على اموال الغير ، أو الاستفادة مما تتيحه من خدمات ، فإذا توصل من

٣٩٩ على أن السرقة (أخذ مال الغير المنقول دون رضاه) وبينت الفقرة الثانية من المادة ذاتها فعل (أخذ المال) التي تعني إزالة تصرف المالك فيه برفعه من مكانه ونقله وإذا كان متصلاً بغير منقول فبفصله عنه فصلاً تاماً ونقله ، وفي الفقرة الثالثة من المادة نفسها لفظة (مال) التي تشمل القوى المحرزة [١] ، اما قانون العقوبات العراقي النافذ رقم ١١١لسنة ١٩٦٩ فقد نص في المادة / ٤٣٩ على أن السرقة " اختلاس مال منقول مملوك لغير الجاني عمداً، ويعدُّ مالاً منقولاً لتطبيق أحكام السرقة النبات وكل ما هو متصل بالأرض أو مغروس فيها بمجرد فصله عنها والثمار بمجرد قطفها والقوى الكهربائية والمائية وكل طاقة أو قوة محرزة أخرى " [٢] ، وبالرجوع إلى المادة ٤٣٩ يمكن تطبيقها على جريمة سرقة معلومات المنصات الإلكترونية عند تحقق النتيجة الإجرامية التي جرّمت سرقة المال المادي وأي قوة محرزة أخرى ، ادانت رئاسة محكمة استئناف كربلاء الاتحادية محكمة جنايات كربلاء الهيأة الأولى وذلك من خلال حكمها الصادر بحق المتهم الذي كان يعمل سائق دراجة نارية نوع تك- تك الذي قام بسرقة جهاز موبايل من احد المواطنين حيث قام المتهم بالاستيلاء على معلومات منصة التواصل الاجتماعي (الفيس بوك) ومراسلة زوجة المجنى عليها ومساومتها بإقامة علاقة غير مشروعه ومبلغ من المال مقابل عدم نشر صورهم الشخصية ، حيث تم ارسال كارت تعبئة للجاني حسب طلبه ، ولم يتوقف الجاني عند هذا الحد بل قام بالاتصال على زوج شقيقة المجنى عليه وطلب منه مبالغ مالية كبيرة أو يقوم بنشر الصور على منصات التواصل الاجتماعي ، ولما تقدم ذكره من أفعال قام بها الجاني وتحقق النتيجة الاجرامية وهي الاستيلاء على معلومات وصور خاصه للمجنى عليه قررت محكمة جنايات كربلاء الهيأة الأولى بالحبس الشديد لمدة خمس سنوات وفق أحكام المادة ١/٤٣٠من قانون العقوبات رقم (١١١) لسنة (١٩٦٩) النافذ[٣].

نلاحظ مما تقدم في قرار الحكم الصادر من محكمة جنايات كربلاء المقدسة بأنها حكمت على المتهم وفق المادة ١/٤٣٠ من قانون العقوبات العراقي بينما كان الافضل محاكمة المتهم على السرقة لأن سرقة جهاز الموبايل والاستيلاء على معلومات المنصات المثبته عليه كانت السبب

ذلك إلى الاستيلاء لنفسه أو لغيره على مال مملوك للغير فيعاقب بالحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن مائتي ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين)

(١) يُنظر: نص المادة ٣٩٩ من قانون العقوبات الأردني رقم ١٦ لسنة ١٩٦٠

(٢) يُنظر: نص المادة ٤٣٩من قانون العقوبات العراقي النافذ رقم ١١١لسنة ١٩٦٩.

(٣) يُنظر: مجلس القضاء الأعلى ، رئاسة محكمة استئناف كربلاء الاتحادية ، محكمة جنايات كربلاء الهيأة الأولى، العدد: ٩٠٤/ج ه ٢٠٢١/١، في ٢٠٢١/١٢/٢٣.

في تحقق النتيجة الإجرامية وهي تهديد زوجة المجنى عليه وابتزازها بعلاقة غير مشروعه وأموال من قبل الجاني .

اما مشروع قانون الجرائم الإلكترونية العراقي لسنة ٢٠١١ فقد جرّم في الفقرة أولاً من المادة السابعة الاستخدام عمداً لنظام الحاسب الآلي أو شبكة المعلومات من أجل الاستيلاء على أموال الغير بأية وسيلة من الوسائل الإلكترونية [١]، وعليه يمكننا أن نعرف النتيجة الإجرامية في جريمة سرقة معلومات المنصات الإلكترونية بأنها (الأثر الطبيعي الذي يتولد عن السلوك الاجرامي ويحدث تغييراً محسوساً في العالم الخارجي يعتد به القانون [٢] .

ثالثاً: العلاقة السببية في جريمة سرقة المنصات الإلكترونية.

تعد العلاقة السببية العنصر الثالث من عناصر الركن المادي إذ لا يكفي لتحقق جريمة سرقة معلومات المنصات الإلكترونية السلوك الإجرامي والنتيجة الإجرامية بل يجب أن يرتبط السلوك الاجرامي والنتيجة الإجرامية برابطة سببية ، إذ في أغلب الاحيان يبدي محامي الدفاع أمام المحاكم المختصة بإنعدام العلاقة السببية بين سلوك الجاني والنتيجة الإجرامية ، بهدف تبرئة المتهم من المسؤولية الجزائية على اعتبار أن العلاقة السببية هي عنصر ضروري وحتمي في الركن المادي لجريمة سرقة معلومات المنصات الإلكترونية بدون قيام العلاقة السببية تنهار المسؤولية الجنائية للمتهم [٣] ، ومن أجل إسناد الجريمة إلى المتهم ومساءلته جنائياً عن العلاقة السببية من عدمها فإن أغلب التشريعات الجنائية ترى بأن العلاقة السببية لها وجهان الاول وجه مادي وذلك من خلال إسناد النتيجة الإجرامية مادياً إلى سلوك المتهم الجرمي ، سواء كان فعلاً أم امتناعاً وارتباط السلوك الاجرامي والنتيجة الإجرامية برابطة السببية المادية كارتباط السبب بالمسبب ، أما الوجه الثاني وجه معنوي وذلك من خلال إسناد النتيجة الإجرامية إلى إرادة أم توقع

---

(١) تنص الفقرة أولاً من المادة السابعة في مشروع قانون الجرائم الإلكترونية العراقي لسنة ٢٠١١على أن كل من استخدم عمداً نظام الحاسوب أو شبكة المعلومات العائدة للأشخاص أو الشركات أو الهيئات أو المصارف أو الأسواق المالية وتمكن من الاستيلاء على أموال الغير أو حقوقهم المالية أو حقق لنفسه أو لغيره منفعة مالية أو حرم الغير من حقوقه المالية بأية وسيلة من الوسائل الإلكترونية يعاقب بالسجن المؤقت وبغرامة لا تقل عن (١٠٠٠٠٠٠٠) عشرة ملايين دينار ولا تزيد على (٣٠٠٠٠٠٠٠) ثلاثين مليون دينار.

(٢) يُنظر. د. جلال ثروت ، قانون العقوبات القسم العام ، ط١، منشورات الحلبي الحقوقية ، بيروت ، ٢٠٠٥، ص١١٩.

(٣) يُنظر. د. مصطفى إبراهيم الزلمي ، أساليب إجرامية بالتقنية الرقمية ، ط١، دار الكتب القانونية ، مصر ، ٢٠٠٥ ، ص٥٥.

متهم خالف أمر الشارع بالنهي عن إرتكاب الفعل أو الامتناع عنه مع تمتعه بالاهلية الجزائية التي تحقق معها المسألة الجزائية [١].

وتعرف العلاقة السببية المادية بأنها الصلة التي تربط ما بين الفعل المجرم والنتيجة وتثبت أن ارتكاب الفعل هو الذي ادى إلى حدوث النتيجة [٢] ، كذلك تعرف بأنها (الرابطة بين السلوك الاجرامي والنتيجة الإجرامية التي بها يكتمل الركن المادي في جريمة سرقة معلومات المنصات الإلكترونية ويتخلف بانعدامها) [٣].

يتضح لنا مما تقدم ان النتيجة الإجرامية والعلاقة السببية تتحقق إذا أدى الدخول غير المرخص به إلى معلومات المنصات الإلكترونية والقيام بتغييرها أو نسخها أو نقلها سواء كانت هذه المعلومات خاصة بالأشخاص الطبيعية والمعنوية كمن يقوم بتحويل الارصدة من حسابات الاخرين إلى حسابه الخاص بغرض الاستيلاء عليها.

الفرع الثاني

الركن المعنوي في جريمة سرقة معلومات المنصات الإلكترونية

بعد أن تطرقنا في الفرع السابق إلى معرفة الركن المادي في جريمة سرقة معلومات المنصات الإلكترونية ، ومن أجل أن تكتمل الجريمة وتحديد العقاب المناسب لها علينا بيان الركن المعنوي في جريمة سرقة معلومات المنصات الإلكترونية إذ إن الجريمة ليست ظاهرة مادية فقط تقوم على السلوك الاجرامي ، بل لابد من توافر خصائص نفسية لها ، وتجتمع هذه العناصر جميعها وتبرز وتظهر تحت مسمى الركن المعنوي للجريمة ، والقانون الجنائي استقر على مبدأ بأنّ المسؤولية لا تقوم فقط على ماديات الجريمة التي لا تستوجب العقاب بذاتها مالم تجتمع معها العناصر النفسية المشترط توافرها لقيام الجريمة ، وللركن المعنوي أهمية كبيرة في تحديد الجريمة إذ لا يتصور حدوث جريمة من دون ركن معنوي ؛ لأن الركن المعنوي الوسيلة التي يستند إليها في تحديد المسؤول عن الجريمة من قبل المشرّع[٤] ، وهذا ما تنص عليه القواعد العامة لارتكاب الجرائم ومنها جريمة السرقة إذ يتطلب توافر الركن المعنوي المتمثل في القصد الجنائي العام ، ويتحقق القصد الجرمي العام في جريمة سرقة معلومات المنصات الإلكترونية ،

---

(١) يُنظر. د. رؤوف عبيد ، السببية في القانون الجنائي ، ط٢ ، مطبعة نهضة مصر ، ١٩٦٦، ص٣.

(٢) يُنظر. د. عبد الحكم فوده ،أحكام رابطة السببية في الجرائم العمدية وغير العمدية ، دار الفكر الجامعي ، الاسكندرية ، ١٩٧٧، ص٨.

(٣) يُنظر. د. عمر فاروق الحسيني ، تعذيب المتهم لحمله على الاعتراف الجريمة والمسؤولية ، المطبعة العربية الحديثة ، ١٩٨٦، ص١٧٧.

(٤) يُنظر. د. فخري عبد الرزاق الحديثي ، شرح قانون العقوبات القسم العام ، ط٢، العاتك لصناعة الكتب ، بغداد ، ٢٠١٠، ص٢٧٣.

من خلال توافر عنصري العلم والارادة ، على الجاني أن يعلم بان المال ليس ملكاً له ، وعلى الرغم من ذلك تنصرف إرادته إلى ارتكاب فعل الحيازة مما يحقق النتيجة الاجرامية[١] ، ولا يكفي في جريمة سرقة معلومات المنصات الإلكترونية من تحقق القصد الجرمي العام فقط والمتمثل بعنصري العلم والارادة ، وانما يشترط معهما نية التملك أي قصد جرمي خاص والجاني يحل محل المالك في ممارسة سلطاته على الشيء والتصرف فيه وعندئذ يكون الجاني قد ظهر بمظهر المالك من خلال نية التملك والاستئثار بالشيء[٢] ، وذهب جانب من الفقه إلى أن سحب العميل مبالغ تتجاوز رصيده من خلال منصات النقود الإلكترونية لا تُعدَّ سرقة على اساس أن البنك قد فتح اعتماداً تلقائياً لمصلحة العميل لاعتقاده أن المبلغ الزائد عن رصيده من ملكه ، ففي هذه الحالة لا يتوفر لديه القصد الجرمي العام[٣].

وتثار ايضا صعوبة أخرى متعلقة بالركن المعنوي في جريمة السرقة ، وذلك من خلال توافر القصد الجرمي الخاص والذي يتمثل في تملك معلومات المنصات الإلكترونية من قبل الجاني واتجاه إرادته للاستيلاء على معلومات المنصات الإلكترونية من أجل الاحتفاظ بها واستخدامها من قبله لأغراض غير مشروعة وهذهِ الاغراض تضر بمصلحة المالك الاصلي للشيء وإن جرائم السرقة التقليدية لا تواجه صعوبة في اثبات القصد الجرمي الخاص لدى الجاني ، لان محل السرقة معروف وهي اشياء مادية قابلة للتملك والحيازة ، كما إن فعل الاختلاس صدر بسوء نية من الجاني ، وهي الاستيلاء على الاشياء محل السرقة بعلم وإرادة الجاني من أجل حرمان المالك أو الحائز أو صاحب الشيء من السيطرة على ما يملك [٤] .

وعند تعمقنا في تصور قيام جريمة سرقة معلومات المنصات الإلكترونية على المستوى الافتراضي أننا سنصطدم بفكرة وهي نية الشخص ومدى قيامها في الاعتداء على معلومات المنصات الإلكترونية من أجل تملكها وحرمان مالكها منها وإن المجرى للسلوك الإجرامي المرتكب في المجال الإلكتروني ، في حقيقة الامر يعد اعتداءً غير واضح المعالم ولا يظهر بمظهره الحقيقي في كشف الفعل المرتكب من قبل الجاني ، وأغلب الاعتداءات المرتكبة تتمثل

---

(١) يُنظر . د. غنام محمد غنام ، شرح قانون العقوبات (القسم الخاص) ، منشورات جامعة المنصورة ، مصر ، ٢٠٠٤، ص٤٥٨.

(٢) يُنظر .د. واثبة داوود السعدي ، قانون العقوبات (القسم الخاص) ، شركة العاتك لصناعة الكتاب ، القاهرة ، ص١٦٧.

(٣) يُنظر: د. محمد حماد مرهج الهيتي ، الحماية الجنائية لبطاقات الائتمان الممغنطة ، دار الكتب القانونية ، مصر ، ٢٠٠٩، ص١٩٦- ٢٠٠.

(٤) يُنظر: شمسان ناجي صالح الخيلي ، مصدر سابق ، ص١٨٨.

في فعل الاختلاس للمعلومات على الرغم من بقاء المعلومة لدى مالك المعلومة الاصلي ، كالاعتداءات التي تحدث في سرقة أرقام بطاقات الائتمان أو الدفع ففي هذه الحالة لا تظهر نية الجاني في تملك تلك المعلومات على عدَّ انه يستولي عليها من دون أن ينتزع حيازتها من مالكها[١]، وأن التشريع الجنائي يتجه الى قيام القصد الجرمي الخاص والاعتراف بوجوده في جريمة سرقة معلومات المنصات الإلكترونية على أن لها قيمة مالية ونية التملك عليها تظهر من خلال الاعتداء على ملكية المعلومات والاستئثار بها من قبل الجاني ، ويؤدي ذلك الى الاضرار بمصلحة المالك[٢].

بناءً لما تقدم ذكره أن السلوك الإجرامي للجاني في الركن المعنوي الذي يتمثل في اختلاس المعلومة واتجاه إرادة الجاني للاستيلاء بكامل علمه وإرادته على معلومات المنصات الإلكترونية ونيته في تملك تلك المعلومات التي يسعى إليها من ارتكاب الجريمة اصلاً ، وبالتالي لا نتصور ارتكاب الجريمة دون أن يتحقق فيها الركن المادي والركن المعنوي معاً ، أما بالنسبة من توافر القصد الجرمي الخاص في جريمة سرقة معلومات المنصات الإلكترونية، ممكن أن يتبين لنا سهولة اثباته من خلال نية التملك التي تكون ظاهرة وواضحة في المجال الإلكتروني ، وان بداية الجريمة تكون في المنصات الإلكترونية ، وبعد ذلك يتم الاعتداء على معلومات المنصات الإلكترونية ، وهذا الفعل يفسر لنا سلوك الجاني واستحواذه على المعلومات فيما بعد

نستنتج مما تقدم أن القصد الجنائي الخاص يتم اثباته من خلال نية تملك الجاني لمعلومات المنصات الإلكترونية من اجل سرقتها والاستحواذ عليها.

المبحث الثاني

الحماية الجزائية من جريمة الاحتيال للمنصات الإلكترونية

ان جريمة الاحتيال التي تتعرض لها المنصات الإلكترونية من اهم الجرائم التي تقع على الاموال والمعلومات التي يكون الحاسب الإلكتروني والانترنت بمثابة الوسيلة أو الأداة لارتكاب الجريمة فيها ، كما وتعد الأكثر انتشاراً في الوقت الحالي نظراً لتعدد طرق ارتكابها ، وارتباطها بالواقع الحقيقي مما دفع أغلب تشريعات الدول المقارنة للتصدي لها من خلال اصدار تشريعات خاصة لمكافحة هذهِ الجرائم ، التي تكون قائمة على العناصر والاركان نفسها في جريمة الاحتيال

---

(١) يُنظر .د. محمد حمادة مرهج الهيتي ، التكنولوجيا الحديثة والقانون الجنائي ، ط١، دار الثقافة ، عمان ، ٢٠٠٤، ص١٩٩.

(٢) يُنظر .د. عبد الفتاح بيومي حجازي ، النظام القانوني للحكومة الإلكترونية ، مصدر سابق ، ص٢٤٧.

التقليدية ، لكن تختلف الوسيلة والأداة في ارتكابها ، وان بعض التشريعات أهملت أو اغفلت في اصدار نصوص خاصة تتلاءم في مكافحة جريمة الاحتيال للمنصات الإلكترونية ، ومن بين هذه التشريعات المشرَع العراقي الذي قدم مشروع قانون الجرائم الإلكترونية إلى مجلس النواب في عام ٢٠١١ ولم يتم التصويت عليه إلى الان ، واكتفى بنصوص قانون العقوبات التقليدية التي لا تتماشى مع التطور التكنولوجي الحديث ، وعليه سنقسّم هذا المبحث على مطلبين نتناول في المطلب الأول مفهوم جريمة الاحتيال للمنصات الإلكترونية وفي المطلب الثاني نتناول محل جريمة الاحتيال للمنصات الإلكترونية.

المطلب الاول

مفهوم جريمة الاحتيال للمنصات الإلكترونية

تعد جريمة الاحتيال من الجرائم التقليدية التي جرّمتها أغلب التشريعات الاجنبية والعربية، وهذه الجرائم موجودة قبل ظهور الانترنت ، اما بعد ظهور الانترنت أصبحت ترتكب هذه الجرائم بوساطة التقنية الحديثة لتبدو وكأنها جرائم جديدة ، مثل جريمة الاحتيال الإلكتروني للمنصات الإلكترونية التي تعد من أبرز الجرائم الإلكترونية الحديثة التي انتشرت انتشاراً كبيراً في البيئة الافتراضية الإلكترونية والتي تمكن الجاني من التخفي وتشويه معالم الجريمة الامر الذي يدعو المشرع إلى ضرورة مكافحتها، لذا سنقسم هذا المطلب على فرعين نتناول في الفرع الاول تعريف جريمة الاحتيال للمنصات الإلكترونية وفي الفرع الثاني نتناول صور جريمة الاحتيال للمنصات الإلكترونية .

الفرع الاول

تعريف جريمة الاحتيال للمنصات الإلكترونية

تعددت التعريفات التي عرّفت الاحتيال بصفته التقليدية لكن لا يوجد تعريف محدد ومقبول للاحتيال الإلكتروني يمكننا الاستناد عليه ، بل تعددت التعريفات وأن كانت قد اتفقت في المضمون واختلفت في العناصر التي يجب توافرها لتحقيقها ، إذ عرّفت جريمة الاحتيال عموماً في القانون الجنائي بأنها" فعل غير مشروع صادر عن إرادة جنائية يقرر له القانون عقوبة أو تدبيراً احترازياً"[1] .

([1]) يُنظر : د. هدى قشقوش ، جرائم الحاسب الآلي في التشريع المقارن ، ط١، دار النهضة العربية ، القاهرة ، ١٩٩٢، ص٢٠.

وهناك من عرف الاحتيال بأنه" أي سلوك احتيالي ينتهج منهج الحوسبة بنية الحصول على امتياز مالي"[1] ، وهناك من عرف الاحتيال المعلوماتي بأنه" التلاعب العمدي بمعلومات وبيانات تمثل قيماً مادية يختزنها نظام الحاسب الآلي ، أو الادخال غير المصرح به لمعلومات وبيانات صحيحة ، أو التلاعب في الاوامر والتعليمات التي تحكم عملية البرمجة ، أو أية وسيلة أخرى من شأنها التأثير في الحاسب الآلي ، حتى يقوم بعملياته بناءً على هذه البيانات أو الاوامر أو التعليمات، من أجل الحصول على ربح غير مشروع وإلحاق الضرر بالغير"[2] ، كما عرفت وزارة العدل الامريكية الاحتيال بأنه " شكل من التخطيط الاحتيالي الذي يستخدم محتويات الانترنت ، مثل : الدردشة ، البريد الإلكتروني ، المواقع الإلكترونية ... لتقديم صفقات احتيالية أو لإرسال نتائج الاحتيال إلى المؤسسات المالية"[3] ،كما يعرف المكتب لتقيم التقنية في الولايات المتحدة الامريكية الاحتيال بأنه "الجريمة التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسياً"[4]

يتضح لنا مما تقدم حول تعريف الاحتيال نرى بأن التعريف الاول عرف الاحتيال على انه فعل غير مشروع وهذا الفعل اما يستوجب العقوبة أو التدابير ، وفي الثاني وصف الاحتيال بأنه سلوك يتم عن طريق الحواسيب الآلية والغاية منه المال ، وفي الثالث نجد انه ركز على التلاعب في المعلومات كما ان التعريفين نرى انهما لم يفرقا بين الاحتيال الإلكتروني وبين الاحتيال الذي يتم عبر الانترنت إذ ان الاحتيال الإلكتروني يكون ذات مفهوم أوسع لأنه يشمل الاحتيال عبر أجهزة الحاسب الآلي والاحتيال عبر الانترنت اما الثاني فان الاحتيال يتم حصرا عن طريق الشبكة فبهذا يكون مفهومه اضيق من الذي سبقه ، اما الرابع فانه اشار إلى الاحتيال لكن ركز على الصفقات الاحتيالية ، في حين نجد الخامس ركز على المعلومات دون الاشارة إلى الاداة التي يتم عن طريقها الاحتيال ، كما أن الباحث يرى ان الاحتيال الإلكتروني

---

(1) يُنظر: د. عمر بن يونس ، الجرائم الناشئة عن استخدام الانترنت ، ط١، دار النهضة العربية ، القاهرة ، ٢٠٠٤، ص٤١١.

(2) يُنظر . د. نائلة عادل محمد فريد قورة ، جرائم الحاسب الآلي الاقتصادية ، ط١ ، منشورات الحلبي الحقوقية ، بيروت ، ٢٠٠٥، ص٤٢٥.

(3) يُنظر . د. محمد طارق عبد الرؤوف الخن ، جريمة الاحتيال عبر إلانترنت (الاحكام الموضوعية والاحكام الاجرائية) ، ط١، منشورات الحلبي الحقوقية ، بيروت ، ٢٠١١، ص٣٨.

(4) يُنظر سامر سلمان الجبوري ، جريمة الاحتيال الإلكتروني (دراسة مقارنة) ، ط١، مكتبة زين الحقوقية والادبية ، بيروت ، ٢٠١٨، ص٢٢.

ممكن أن يتم عن طريق المنصات الإلكترونية بجميع أنواعها سواء كانت هذه المنصات مثبته على جهاز الحاسب الالي أم أي جهاز إلكتروني أخر يمكن تنصيب تلك المنصات عليه.

كما وعرّفته لجنة المراجعة البريطانية بأنه "كل سلوك غير مشروع يتصل بالحاسبات الآلية ويهدف لتحقيق ربح مادي"[١] ، كما نصت المذكرة التفسيرية لاتفاقية بودابست لمكافحة جرائم المعلومات الموقعة عام ٢٠٠١ في الفقرة ب من المادة الثامنة على ان " التلاعبات في المكونات المادية للحاسب والتلاعبات المعلوماتية الاحتيالية تكون مجرّمة إذا سببت ضرراً اقتصادياً أو مادياً للغير ، أو أن يكون الجاني قد نفذ الجريمة بنية الحصول على منفعة اقتصادية غير مشروعة له أو للغير ، ومصطلح الضرر يشمل النقود والاشياء غير المادية ذات القيمة الاقتصادية"[٢] .

يتضح لنا مما تقدّم ان اللجنة البريطانية وصفت الاحتيال أنه سلوك غير مشروع والهدف تحقيق الربح ويتم ذلك عن طريق المنصات الإلكترونية المنصبة على الحاسب الالي أو أي جهاز الكتروني اخر ، اما اتفاقية بودابست وصفت الاحتيال في المادة الثامنة في الفقرة ب بالتلاعبات في المكونات المادية ، وتكون مجرمة اذا سببت ضرراً اقتصادياً أو مادياً وان تكون نية الجاني للحصول على منفعة وهذه المنفعة غير مشروعة حتى يطلق عليها جريمة احتيال ، بمعنى لو كانت المنفعة مشروعة وحيازة الجاني عليها لم يسبب ضرراً مادياً أو اقتصادياً ففي هذه الحالة لا نكون امام جريمة احتيال سواء كان تقليدي أو الكتروني .

وعند المقارنة بين الاحتيال التقليدي والإلكتروني يتبين لنا ان جوهرهما واحد ، فان الجاني في كلتا الحالتين يقوم بوسائل احتيالية من اجل الاستيلاء على مال الغير ، ونجد الفرق بينهما في محل السلوك الاجرامي ونوع الوسائل الاحتيالية التي يستخدمها الجاني [٣].

وان المحل للاحتيال الإلكتروني يتكون من المعلومات التي بدورها تمثل القيمة المالية أو الاقتصادية داخل النظام الإلكتروني وأغلب حالات الاحتيال الإلكتروني تحدث من خلال التلاعب بهذه المعلومات التي تتعلق بالفواتير والارصدة سواء البنكية منها والحسابية ، كذلك ارقام الارباح التي تتعلق بالصفقات المالية والتجارية والتي تكون عرضة للاحتيال ، خصوصا بعد اتجاه أغلب

---

(١) يُنظر . د. حسام محمد نبيل الشنراقي ، مصدر سابق ، ص١٨٤.
(٢) يُنظر .د. هلالي عبد اللاه أحمد ، مصدر سابق ، ص١٠٣.
(٣) يُنظر . محمد عبدالله أبو بكر سلامة ، جرائم الكمبيوتر والانترنت ، منشأة المعارف بالاسكندرية ، ٢٠٠٦، ص١٦٧.

الدول المتقدمة إلى ما يسمى بمجتمع اللانقود الذي يتم عن طريق تحويل الاموال بدل التعامل النقدي المباشر التقليدي الذي أيضاً لا يخلو من عمليات الاحتيال لكن بصورته التقليدية [١] .

كما يمكن تمييز الاحتيال في مجال المنصات الإلكترونية الذي يتم بالاستعانة بأجهزة الحاسوب أو أي جهاز إلكتروني أخر من خلال تنصيب المنصات الالكترونية على تلك الاجهزة ، التي تكون وسيلة للاحتيال وكمحل لها في الوقت نفسه ، فضلاً عن جميع الوسائط التي تسهل عملية نقل المعلومات الإلكترونية من خلالها مثل شبكة الانترنت التي كان لها الدور الفاعل والرئيسي في خلق بيئة مرنة وسهلة التفاعل مع هذا النوع من الجرائم ، إذ ان كثير من التشريعات المقارنة اتجهت في تشريعاتها لتضمين نصوص خاصة تعمل على معاقبة الاحتيال الإلكتروني ، بعيداً عن القواعد العامة من أجل ازالة الشك الحاصل بين الاحتيال بصورته التقليدية والاحتيال الإلكتروني وتشديد الجزاء لمرتكبي هذه الجرائم .

وقد عرّف المشرع الفرنسي جريمة الاحتيال في قانون العقوبات بالمادة ١/٣١٣ بأنه "الفعل الذي يتم باتخاذ اسم كاذب أو صفة غير صحيحة أو بالاستعمال غير المشروع لصفة صحيحة ، أو باستعمال الطرق الاحتيالية ، وذلك لخداع شخص طبيعي أو معنوي ، وحمله على تسليم نقود أو مال أو تقديم منفعة ، أو قبول تصرف ينطوي على التزام أو مخالصة ، وذلك إضراراً بالمجني عليه أو الغير"[٢]، اما المشرع الاماراتي فقد عرّف جريمة الاحتيال بالمادة (١١) من القانون الاتحادي " معاقبة الجاني في حال استيلائه لنفسه أو لغيره بغير حق على مال منقول أو منفعة ، أو توقيع سند ، بالاستعانة بأي طريقة احتيالية ، أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة عن طريق الشبكة المعلوماتية أو نظام معلوماتي إلكتروني ، أو إحدى وسائل تقنية المعلومات "[٣] ، اما المشرع العراقي فقد عرف جريمة الاحتيال من خلال القواعد العامة في نص المادتين (٤٥٦،٤٥٧) من قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩المعدل ، إذ تناول جريمة الاحتيال بالتفصيل في المادة (٤٥٦)[٤] اما المادة ٤٥٧ فقد جرمت حالة خاصة بالاحتيال وهي

---

(١) يُنظر .د. محمد طارق عبد الرؤوف الخن ، مصدر سابق ، ص٦٢.

(٢) يُنظر المادة (١/٣١٣) من القانون الفرنسي رقم (١٣٣٦) لسنة ١٩٩٢.

(٣) يُنظر المادة (١١) من القانون الاتحادي رقم (٥) لسنة ٢٠١٢لمكافحة جرائم أنظمة المعلومات .

(٤) يُنظر نص المادة (٤٥٦) من قانون العقوبات العراقي : ١- يعاقب بالحبس كل من توصل إلى تسلم أو نقل حيازة مال منقول مملوك للغير لنفسه أو إلى شخص آخر وذلك بإحدى الوسائل التالية:

أ- باستعمال طرق احتيالية

ب- باتخاذ اسم كاذب أو صفة غير صحيحة أو تقرير أمر كاذب عن واقعة معينة متى كان من شأن ذلك خداع المجنى عليه وحمله على التسليم .

حالة التصّرف في مال منقول أو عقار من أجل الاضرار بالغير[1] .

نجد ان المشرّع الفرنسي قد توسع في تعريف جريمة الاحتيال وعدم اقتصارها على عنصر المال فقط بل تشمل عنصر الخدمات كما ان المشرع استخدم القيم التي يمكن من خلالها اسقاط الحكم سواء على القيم المادية والقيم المعنوية وليس على واحده منها ، وبما ان النص جاء موسعا يمكننا تطبيقه على العناصر ذات الطبيعة المعنوية فضلاً عن القيم الاقتصادية أو المالية ومن ذلك يمكننا ايضا تطبيقه على المنصات الإلكترونية، أما المشرّع الاماراتي فإنه بين الوسيلة المستخدمة في جريمة الاحتيال والتي تتمثل في الشبكة الإلكترونية أو أي نظام معلوماتي إلكتروني فضلاً عن توسعة في محل جريمة الاحتيال لتشمل المال أو المنفعة أو توقيع سندات إذ يمكننا ان نغطي جميع الاحتمالات التي تقوم في مجال التعاملات الالكترونية ، الامر الذي يجعل من الحكم موسعاً أو مشدداً من أجل تفعيل الحماية الفّعالة إلى الضحايا عن طريق المنصات الإلكترونية ، والمشرع العراقي فصّل جريمة الاحتيال التقليدية ووضع لها نصوصاً عقابية لكنه لم يتطرق لجريمة الاحتيال للمنصات الإلكترونية، وعلى الرغم من ذلك يمكن تطبيق نص الفقرة من المادة (٤٥٦) من قانون العقوبات العراقي رقم (١١١) لسنة (١٩٦٩) النافذ في حالات خاصة مثل استخدام الماستر كارت من قبل شخص غير الشخص صاحب الماستر كارت في جريمة الاحتيال للمنصات الإلكترونية.

الفرع الثاني

صور الاحتيال للمنصات الإلكترونية

من أجل معرفة معالم الاحتيال التي تحدث عن طريق المنصات الإلكترونية ، علينا توضيح بعض انواع الاساليب الاحتيالية التي تحدث في المجال الافتراضي ، وفي الخصوص التي تحدث عبر شبكة الانترنت وعن طريق المنصات الإلكترونية بجميع أنواعها ، على الرغم من إنه لا يمكن حصر تلك الاساليب الاحتيالية لكن يمكننا اختيار ابرز صورها مثل الاحتيال التجاري ،

٢- يعاقب بالعقوبة ذاتها كل من توصل بإحدى الطرق السابقة إلى حمل أخر على تسليم أو نقل حيازة سند موجه لدين أو تصرف في مال أو إبراء أو على أي سند أخر يمكن استعماله لإثبات حقوق الملكية أو أي حق عيني آخر ، أو توصل بإحدى الطرق السابقة إلى حمل آخر على توقيع مثل هذا السند أو إلغائه أو إتلافه أو تعديله.

(١) يُنظر نص المادة (٤٥٧) التي نصت على أن " يعاقب بالحبس من تصرف في مال منقول أو عقار يعلم أنه لا يملكه أو ليس له حق التصرف فيه أو تصرف في هذا المال مع علمه بسبق تصرفه فيه أو التعاقد عليه وكان من شأن ذلك الإضرار بالغير".

والاحتيال عن طريق البريد الالكتروني ، والاحتيال الواقع على اموال المصارف والاستثمارات .

اولاً: الاحتيال التجاري المباشر :

الاحتيال الذي يتم عبر شبكة الانترنت وعن طريق المنصات الإلكترونية في التعاملات التجارية المباشرة يمتاز بخاصية السرعة والكفاءة ، على الرغم من وقوعه تحت طائلة الاحتيال؛ بسبب عنصر السرعة الذي تجري فيه الصفقات التجارية ، ويحدث ذلك نتيجة لعدم توفر فرصة التأكد من اطراف المتعاملين [١] ، الامر الذي يؤدي في الغالب لحدوث عمليات الاحتيال واكتشافها بعد التسليم ، الامر الذي اكدته احصائيات لجنة التجارة الفيدرالية مع لجنة مراقبة الاحتيال عبر الانترنت ، وتعد هذه الطريقة من الطرق الاكثر انتشاراً في العالم الإلكتروني الافتراضي[٢] .

ففي قضية حدثت في مقاطعة (كولورادو) في ١٠ أيار عام ٢٠٠١إذ أدانت هيأة المحلفين الاتحادية المتهم (دانيال كتلسن) لقيامه بالاحتيال عبر الانترنت ، وذلك لاستخدامه اسماً كاذباً كما وقام باستلام المال عن كمية قطع للحاسوب قد عرضها للبيع من خلال موقع e-bay ، على الرغم من أنه لم يقم بتسليم البضاعة ، إذ تم رفع الكثير من الشكاوي بحقه نتيجة قيامه بالاحتيال على الكثير من العملاء ، ولم يكتفِ بهذا القدر بل قام كتلسن برفع شكوى ضد شركة التأمين ، والذي زعم بأن بضاعته قد سُرقت من مَرآبه ، وهو في حقيقة الأمر لا يملك اية بضاعة بل أراد الاحتيال على شركة التأمين أيضاً هذا ما تم كشفه من خلال المحققين في مؤسسة البريد الامريكية بعد التحقيق بالموضوع ، واكتشافهم انه أراد ايضاً الحصول على المال عن طريق غير مشروع واحتيالي[٣].

ومن أجل تجنب عمليات الاحتيال عبر الانترنت عند الشراء وأن الشبكة تحتوي على خدمة تسمى (Escrow House) عبارة عن مؤسسة مالية تعمل على تسليم الاموال من المشترين في المواقع التجارية عن طريق الانترنت وتعمل على تجميدها لديها ، لحين وصولها إخطار بأنه تم استلام البضاعة المتفق عليها وحسب المواصفات المطلوبة من قبل المشترين بعدها تقوم المؤسسة بتسليم الاموال ففي هذه الحالة تكون نسبة الاحتيال ضئيلة جداً ، أما في حالة عدم

---

(1) Richard Hillman, securities fraud, the internet poses challenges to regulaters and Inverstors, united states General accounting office, 2017,p5.

(٢) يُنظر. د. محمد شناوي ، جرائم النصب المستحدثة ، ط١، دار الكتب القانونية ، القاهرة ، ٢٠٠٨، ص٨٨.

(٣) يُنظر .د. محمد طارق عبد الرؤوف الخن ، مصدر سابق ، ص٥٠.

وصول البضاعة المتفق عليها أو كانت غير مطابقة للمواصفات فمن حق الزبون أو المشتري استرداد امواله من تلك المؤسسة[١].

يتبيّن لنا مما تقدّم ان الاحتيال التجاري صورة من صور الاحتيال الإلكتروني إذ يتم التعامل عبر شبكة الانترنت وعن طريق المنصات الإلكترونية التي يتم تنصيبها على جهاز الحاسوب أو أي جهاز الكتروني ممكن أن تثبّت عليه المنصات الإلكترونية ، إذ تجري عن طريقه الصفقات التجارية ويتم تحويل المال عن طريقها ، لكنها تكون عرضه لجريمة الاحتيال في الغالب وهذا ما تبين لنا من ادانة المتهم دانيال كتلسن الذي احتال على الكثير من الزبائن فضلاً عن قيامه بالاحتيال على شركة التأمين ووقوعه في شر أعماله ، ومن أجل تلافي جرائم الاحتيال يجب التعامل مع شركات أو مؤسسات تتمتع بالمصداقية وهي تكون كفيلة بين الطرفين سواء كان البائع أم المشتري وان تكون لها الخبرة الكافية في هذا المجال ، وتضمن حق الطرفين.

ثانياً: الاحتيال المصرفي :

تتعرّض المواقع الإلكترونية للمصارف إلى عمليات القرصنة والاحتيال من خلال اقتحام تلك المواقع ، الأمر الذي يسمح لهم بالاعتداء على كشوفات وحسابات العملاء فضلاً عن نقل الاموال إلى حساباتهم الشخصية ، ويقوم المحتالون بذلك عن طريق الحصول على بعض الوسائل التي ترتبط بحماية المعلومات الخاصة بالعملاء مثل كلمة المرور ، فضلاً عن تفاصيل الحسابات وعن طريقها تتم عملية الاحتيال ، إذ ان الانترنت أتاح لعملاء المصارف والبنوك امكانية الاطلاع على حساباتهم وإمكانية إجراء التحويلات المالية عن طريق المواقع الإلكترونية العائدة لهذه المصارف الامر الذي سهل عملية الإحتيال الذي تتم من خلال نقل الارصدة أو إضافة بضعة اصفار إلى رقم ما في هذا الحساب أو ذاك [٢]، وتعد جريمة الاحتيال التي حدثت في الولايات المتحدة الامريكية في بنك الباسيفيك الوطني ، عندما قام المواطن الأمريكي ستانلي مارك الذي كان يعمل في البنك اخصائياً للحاسبات ، والذي اكتشف عن طريق الصدفة شفرة تحويل حسابات العملاء بين مصرف وآخر ، حيث قام بانتهاز الفرصة وأصدر أوامر إلكترونية لعدة فروع للبنك لتحويل مبالغ قدّرت في وقتها بأربعة ملايين دولار أمريكي إلى حسابه الذي قام بفتحه في أحد البنوك السويسرية ، وبعدها أنتقل مارك إلى جنيف وقام بسحب المبلغ المذكور ، واشترى به ماساً وقام بإيداع الماس في خزانة خاصة في أحد المصارف هناك ، ولم يكتشف ما

---

(١) يُنظر: محمود أحمد عبابنة ، جرائم الحاسوب وابعادها الدولية ، ط١، دار الثقافة للنشر ، الاردن ، ٢٠٠٩، ص١٣٦.

(٢) يُنظر. د. جميل عبد الباقي الصغير ، مصدر سابق ، ص٣٤.

قام به مارك أحداً لكنه كان مخمور في أحد الأيام واعترف بعملية الاحتيال التي قام بها وعلى إثرها تم كشفه[١] .

ثالثاً: الاحتيال عن طريق الأوراق المالية :

النمو والتطور السريع للأنترنت أدى إلى الكثير من التغيرات الهامة في مجال المال والأعمال ، إذ يستخدم الانترنت حالياً بصورة كبيرة وبشكل أكثر تنظيماً في المجالات الحياتية والعملية كافة وخصوصاً الشركات إذ تتوسع في مجال تقديمها للخدمات فاقت حدود تقديم العروض والتجارة في الأسهم ، كما ويلاحظ المراقبون التزايد في شعبية الانترنت عند أغلب المستثمرين ، إذ أنها تسمح لهم ببيع وشراء الأسهم عن طريق حواسيبهم الشخصية ومن بيوتهم فضلاً عن ذلك تكون نسبة العمولة التجارية مخفضة مقارنة بالمكاتب أو الشركات الخاصة لهذا الغرض[٢] .

وان هذا النوع من التعاملات قد أظهر لنا نوعاً جديداً من انواع الاحتيال المرتبطة بسوق الأسهم ، الذي يعد من الأساليب الاحتيالية الاكثر انتشاراً في استخدام الانترنت عن طريق نشر المعلومات الوهمية من أجل جذب المستثمرين، ويقوم المحتالين على نشر المعلومات الكاذبة عن وجود أسهم لبعض الشركات معروضة للبيع حتى يزيدوا أكبر عدد ممكن من المستثمرين ، في حين هذه الزيادة من المستثمرين انما تزيد من قيمة الأسهم أولاً وتبعد شباك الجريمة ثانياً ، وفي بعض الحالات يكون لدى المحتالين أسهماً حقيقية لكن تكون قيمتها قليلة ، فيقوم المستثمرون ببيعها على أنها ذات قيمة عالية وعند بيعها للمستثمرين يكتشفون بان هذه الأسهم التي تم شرائها تم الاحتيال عليهم بها وعند بيعها مرة أخرى من المستثمرين يتعرضون الى خسارة كبيرة[٣] .

ومن أمثلة الاحتيال بهذا الأسلوب أكبر قضية احتيال مالي بالتأريخ وهي قضية (مادوف) الذي كان يعمل مستشاراً استثمارياً أمريكي الجنسية له من العمر (٧٢) عاماً يملك خبرة كبيرة في مجال عمليات الأسهم والبورصة ، وتولى في عام ١٩٩٠ حتى عام ١٩٩٣ منصب رئيس سوق ناسداك للأسهم وهو إحدى بورصتي نيويورك العملاقتين ، كما قام بتأسيس شركة عرفت بإسم (بيرنارد إل ما دوف انفستمنت سيكو ريتيز) في عام ١٩٩٥ والتي اتسعت على نطاق واسع

---

(١) يُنظر. د. محمد طارق عبد الرؤوف الخن ، مصدر سابق ، ص٤٨-٤٩.

(٢) يُنظر. د. محمد طارق عبد الرؤوف الخن ، المصدر نفسه ، ص٥١.

(٣) يُنظر. د. محمد سامي الشوا ، ثورة المعلومات وانعكاساتها على قانون العقوبات ، ط١، دار النهضة العربية ، القاهرة ، ١٩٩٨، ص١٢٣.

حول العالم ، إذ تم اتهام بيرنارد مادوف في نهاية عام ٢٠٠٨ بالاحتيال على مستثمرين عن طريق خطة استثمارية وهمية بلغت قيمتها حوالي خمسين مليار دولار أمريكي ، كما وحصل من عملية الاحتيال هذه على مبالغ كبيرة جداً من عملائه بحجة استثمارها ، إذ ادعى خسارتها جميعها وكانت أكبر عملية احتيال في العالم قام بها مادوف وفي عام ٢٠٠٩ تم الحكم على مادوف بالسجن لمدة ١٥٠ عام على أثر جريمة احتيال قام بها قدرت خسارتها بحوالي (٢٠) و(٦٥) مليار دولار أمريكي [١].

نجد ان لشبكات الانترنت الدور البارز والكبير في إدارة عمليات بيع وشراء الأسهم التي تدار عن طريق منصات إلكترونية ، مثبتة على أجهزة الحاسوب الخاصة بالمستثمرين ومن منازلهم ، لكن هذه العمليات تتعرض لجريمة الاحتيال المنظمة وأغلب القائمين بهذه الجرائم هم من المتمرسين في عمليات الاسهم والاستثمار وابرز مثال تم التعرض اليه سابقاً قضية احتيال مادوف الذي قام بأكبر عملية احتيال بالعالم وفي نهاية المطاف حكم عليه بالسجن لمدة ١٥٠عام .

رابعاً: الاحتيال الهرمي :

يُعد من أكثر أنواع الاحتيال الإلكتروني انتشاراً والذي برز في السنوات الأخيرة ، والاحتيال الهرمي عبارة عن مجموعة من البرامج التسويقية الاحتيالية ، والتي تتم عن طريق اعطاء مكافأة مجزية للمشاركين عند اقناعهم أفراداً آخرين أن ينظموا إلى هذه البرامج التسويقية[٢] ، كما ان الهرم يتشكّل عندما يقوم شخص واحد بجمع الأموال من المشتركين الجدد، ويعمل على اقناع المشتركين أن يقنعوا أشخاص اخرين ، عندها تكون سلسلة من المشتركين ، وان المجموعة الاولى من سلسلة المشتركين تكون بداية سلسلة الاحتيال ، وتعتمد مشاريعهم التسويقية الهرمية عن طريق تبادل الأموال ، كما ان هذا العمل لا يتعلق ببيع وشراء السلع انما هو غطاء لعمليات احتيالية كبيرة تحدث هدفها الاستيلاء على أموال الغير بطريق غير مشروع[٣].

([١]) يُنظر. عبد الفتاح سليمان ، الاحتيال في العمل المصرفي في الدول العربية وطرق مكافحتها ، ٢٠١٢، ص٣٤٧-٣٥٠.

([٢]) يُنظر. عبد الفتاح سليمان ، مصدر سابق ، ص٣٤٧.

([٣]) يُنظر. د. حسني عبد السميع إبراهيم ، مصدر سابق ، ص٢٥٠.

يتضح لنا مما تقدّم ان الاحتيال الهرمي صورة من صور الاحتيال الإلكتروني والتي انتشرت بصورة كبيرة في الوقت الحالي ، والتي تتم عن طريق استقطاب أفراد هدفهم الربح من دون تعب فيقوم كل فرد منهم بأقناع مجموعة أفراد وهؤلاء الأفراد أيضاً يقومون بإقناع آخرين وهكذا ، ولا يعلمون انهم تحت طائلة الاحتيال والمجموعة الاولى تعد هي المجموعة المحتال عليها وفي الوقت نفسه تعد محتالة ، إذ غرّتهم المكافأة التي تصرف لهم من قبل العقل المدبر لهذه العملية ، على الرغم من إن الفائدة التي يحصلون عليها من هذا العمل هي جزء من أموالهم وبالتالي فانهم يفقدون أموالهم ويصابون بالخيبة والخسارة عندما يعلمون انهم تم الاحتيال عليهم.

خامساً: الاحتيال عن طريق البريد الإلكتروني:

يُعد البريد الإلكتروني وسيلة أو نظام للتراسل وذلك بإستخدام شبكات الحاسبات والمنصات الإلكترونية ، الذي يمكن من خلالها الاتصال بملايين الناس حول العالم كبديل عن البريد التقليدي، كما ويمكن من خلاله أيضاً كتابة الرسائل فضلاً عن تضمينها الملفات أو الصور أو المستندات ، كل هذا بعد معرفة عنوان البريد الإلكتروني للمرسل له ، كما يمكن استقبال الرسائل من أي شخص يستخدم شبكة الانترنت ويملك بريد إلكتروني[١] ، ويتعرض البريد الإلكتروني لجريمة الاحتيال ومثالها ، البريد الإلكتروني النيجيري Neigeran letter fraud الذي يتلقى الضحية من المحتال رسالة إلكترونية يدعي فيها أنه الوريث الوحيد ولا أحد سواه لابن رئيس نيجيريا الميت ، وأنه سوف يرث الكثير من الدولارات تقدّر بالملايين والمخزنة في اغلب مصارف العالم ، وان مستلم هذه الرسالة سوف يكون له نصيب من هذه الثروة لكن المحتال يدعي بانه لا يملك أجور المحامي فكل ما يحتاج إليه هو كم الآف من الدولارات من أجل اعطائها للمحامي للحصول على الملايين المخزنة في حسابات المصارف ، وهكذا تتم عملية الاحتيال وان الاشخاص الذين قاموا بارسال الأموال وقعوا ضحية لهذه الجريمة إذ لم يحصلوا على نقودهم من الثروة التي وعدهم بها المحتال[٢].

كما وتتم عملية الاحتيال الإلكتروني عن طريق ارسال رسائل بريدية خادعة للاستيلاء على معلومات عملاء المصارف ، إذ بلغ عدد الرسائل الخادعة في بنوك أمريكا حوالي اكثر من ٥٠ مليون رسالة ، والتي وقع ضحيتها أكثر من مليون عميل وأغلب الضحايا من العملاء الذين يتعرضون لجريمة الاحتيال اغلبهم من الدول

---

(١) يُنظر .د. علي عبود جعفر ، مصدر سابق ، ص٣٦٤.

(٢) يُنظر. د. محمد طارق عبد الرؤوف الخن ، مصدر سابق ، ص٦٥-٦٦.

المتقدمة التي يكثر فيها استعمال الخدمات الإلكترونية بشكل يومي ومن هذه الدول امريكا ودول غرب أوربا ، وان أغلب رسائل البريد الإلكتروني الخادعة تتسم بالرقي والتهذيب والمحاولة في دفع العملاء بالرد على تلك الرسائل لأهميتها ، على الرغم من أن اغلب الرسائل تحتوي على أخطاء كتابية مثل اسم البنك[1].

المطلب الثاني

أركان جريمة الاحتيال للمنصات الإلكترونية

تعد جريمة الاحتيال التقليدية من الجرائم التي يكون الاتصال مباشر بين الجاني والضحية التي يمارس من خلالها السلوك الاجرامي ، اما في حالة الاحتيال الإلكتروني فليس من السهل ان يُسلّم بوجود احتيال قائم بين شخصين بشكل مباشر ، إذ نستطيع التسليم بوجود عملية احتيال بين الجاني وبين الانظمة الحاسوبية عن طريق المنصات الإلكترونية ، بوساطة مجموعة من الوسائل الاحتيالية التي تطبق على المعلومات والبيانات التي تسهّل على الجاني ان يحقق عملية الاحتيال ، وان الحالات التي يتم من خلالها تحويل الأموال إلكترونياً وعدم تدخل أي عنصر بشري فيها ، ففي هذه الحالة هل من الممكن ان تكون مكونات النظام المعلوماتي وما يحوية من أموال ومعلومات يتم تداولها إلكترونياً محلاً لجريمة الاحتيال؟، وان لتحقق جريمة الاحتيال للمنصات الإلكترونية يجب أن يتحقق فيها الركن المادي المتمثل في السلوك الإجرامي ، والركن المعنوي المتمثل بالقصد الجرمي ، وعليه سنقسم هذا المطلب على فروعين نتطرف في الفرع الاول إلى الركن المادي في جريمة الاحتيال للمنصات الإلكترونية إما في الفرع الثاني نتطرق إلى الركن المعنوي في جريمة الاحتيال للمنصات الإلكترونية.

الفرع الاول

الركن المادي في جريمة الاحتيال للمنصات الإلكترونية

يتمثل الركن المادي في جميع الجرائم على مجموعة من الافعال التي يقوم بها الجاني والتي تضر بمصالح الناس أو تضر بمصلحة المجتمع ، كما وان الافعال التي يقوم بها الجاني تختلف باختلاف الجرائم ، إذ ان المشرع نص على تجريمها من أجل تحقيق مصلحة الفرد أو مصلحة المجتمع ، ولبيان جريمة الاحتيال للمنصات الإلكترونية علينا التطرق إلى عناصر الركن المادي

([1]) يُنظر . عبد الفتاح سليمان ، مصدر سابق ، ص ٤٢٠.

وهما السلوك الاجرامي المتمثل بفعل الاحتيال والنتيجة الاجرامية المتمثلة بعنصر التسليم والعلاقة السببية بينهما .

أولا: السلوك الإجرامي في جريمة الاحتيال الإلكتروني (فعل الاحتيال)

لقد اوضح الفقه الجنائي الاساس في الطرق الاحتيالية في ضوء القواعد العامة هو الكذب البالغ إضافة لأمور أخرى تؤدي بوقوع المجني عليه في الغلط ، إذ يؤدي ذلك إلى قناعة المجني عليه بالمظهر المادي الخارجي فينخدع ويقوم بتسليم المال[١] .

كما علينا معرفة بعض الامور التي تتعلق بالسلوك الاجرامي في جريمة الاحتيال للمنصات الإلكترونية ومنها:

أ- تمتع الجاني بالخبرة التقنية في استخدام الحاسوب والمباشرة في النشاط التقني من أجل ارتكاب جريمة الاحتيال للمنصات الإلكترونية لأنها الوسيلة في الوصول إلى شبكة المعلومات[٢].

ب- يعد الدخول للمنصات الإلكترونية دون ترخيص جريمة بحد ذاته ، كما انه يعدَّ الأداة والوسيلة إلى ارتكاب جرائم متعددة لان الدخول إلى أي نظام إلكتروني يخص الغير ، يعدَّ من العناصر الضرورية لبعض اساليب جريمة الاحتيال للمنصات الإلكترونية[٣].

ت- التطور الحديث لتكنولوجيا المعلومات وتقدم التقنية الإلكترونية سهل للمحتالين امكانية الاتصال بالعديد من الضحايا حول العالم ، في حين كانت وسائل الاتصال التقليدية ذات كلفة عالية في السابق[٤] ، كما ان المشكلة في تحديد السلوك الإجرامي في جريمة الاحتيال للمنصات الإلكترونية ، يرجع في الاساس حسب التشريع الجنائي إلى التلاعب في المعلومات والبرامج ، من خلال استخدام الطرق الاحتيالية على النظام الإلكتروني ، والذي يعدَّ الاساس في ممارسة فعل

---

(١) يُنظر. د. عمر أبو الفتوح عبد العظيم الحمامي ، مصدر سابق ، ص٦٧٥.

(٢) يُنظر . د. عبدالله عبد الكريم عبدالله ، مصدر سابق ، ص٦٣.

(٣) يُنظر .د. عبد الفتاح بيومي حجازي ،التزوير في جرائم الكمبيوتر والانترنت دراسة مقارنة ، ط١، منشأة المعارف، ٢٠١٠، ص٤٤.

(٤) يُنظر. محمد كمال محمود الدسوقي ، الحماية الجنائية لسرية المعلومات الإلكترونية دراسة مقارنة ، ط١، دار الفكر والقانون ، ٢٠٢١، ص٦٢.

الاحتيال[1] ، كما ان الفقه اختلف بين مؤيد ومعارض في تحقق السلوك الإجرامي على الاحتيال للمنصات الإلكترونية إذ علينا ان نبين هذا الخلاف الفقهي وترجيح الرأي الراجح وهذا ما سنبينه كالاتي :

الاتجاه الاول يرى ان التلاعب في المعلومات يؤدي إلى قيام السلوك الإجرامي في جريمة الاحتيال للمنصات الإلكترونية ، من خلال ايهام الضحية أو المجني عليه بأنها صحيحة وبالتالي فانه يسلم بها ، وفي هذه الحالة ممكن تطبيق النص المتعلق في الجرائم الاحتيالية ، على عدّ التلاعب بالمعلومات أو البرامج وسيلة من وسائل الاحتيال ، واما جهاز الحاسوب والمنصات الإلكترونية المثبتة عليه أو أي جهاز إلكتروني أخر ماهي إلا وسيلة للتحايل ، يؤيد انصار هذا الاتجاه فكرة تحقق سلوك الجاني في الاحتيال للمنصات الإلكترونية من خلال إمكانية تطبيق النصوص الخاصة في جريمة الاحتيال على الانظمة الإلكترونية ، معللين ذلك ان المنصات الإلكترونية هي الأداة والوسيلة التي يقوم عن طريقها تجسيد الافعال المجرّمة ، في حين يذهب جانب من الفقه الفرنسي إلى تأكيد تحقق جريمة الاحتيال للمنصات الإلكترونية ايضاً من خلال توافر السلوك الاجرامي والذي يتمثل لنا من خلال الأكاذيب التي يتم دعمها من وقائع خارجية ؛ متمثلة في معلومات يتم ادخالها عن طريق جهاز الحاسوب تعد من الطرق الاحتيالية[2] وخير مثال على ما تقدم حكم محكمة النقض الفرنسية إذ ادانت المتهم الذي دخل بسيارته في مرآب لوقوف السيارات إذ استخدم السائق عمله نقدية قديمة بدلاً من استخدام النقود الاصلية ، وادى هذا الفعل إلى تشغيل الماكنة الذي ادى إلى تحريك عقارب الماكنة ، وأسست محكمة النقض حكمها على استخدام القطعة النقدية عديمة الفائدة واعتبرتها من الطرق الاحتيالية ، واخذ بهذا الاتجاه على سبيل الاستدلال بعض الدول الأنجلوسكسونية ومنها بريطانيا واستراليا وكندا [3] ، الذي يوسع في تطبيق نصوص جريمة الاحتيال على التعبير الإلكتروني ، وفي عام ١٩٨٣تدخل المشرع الانكليزي في عدَّ خداع الالة الإلكترونية بنية ارتكاب غش مالي طريقة من طرق الاحتيال ، التي تستوجب العقاب عليها جنائياً من خلال تطبيق نصوص التجريم للاحتيال الإلكتروني على النظام الإلكتروني إذ سار على هذا النهج كل من القضاء الكندي والاسترالي[4] ، كما ان المحاكم اتجهت إلى التوسع بقبول فكرة الاحتيال من خلال جميع الوسائل الإلكترونية بمختلف منصاتها عن طريق

---

(1) ينُظر. د. محمد علي حسن الطوالبة ، التفتيش الجنائي على نظم الحاسوب والانترنت ، ط١، عالم الكتب الحديثة ، ٢٠٠٤، ص١٧٤.

(2) يُنظر: محمد عبد الله ابو بكر سلامة ، مصدر سابق ، ص١٧٠.
(3) يُنظر: د. حسني عبد السميع إبراهيم ، مصدر سابق ، ص٤١١.
(4) يُنظر: سامر سلمان الجبوري ، مصدر سابق ، ص٤٠.

جهاز الحاسوب وشبكة الانترنت التي تعمل كوسيط يتم من خلاله عملية الاحتيال ، إذ قضت محكمة النقض الفرنسية بتحقق السلوك الإجرامي ووقوع جريمة الاحتيال التي تمت بالوسائل الإلكترونية ذات المظاهر المادية الخارجية إذ ترى المحكمة "إن الاوراق تشكل مظهراً خارجياً إذا كانت طبيعتها أن تولد الاقتناع بوجود ائتمان غير حقيقي ما دامت تأتي من استعمال وسيلة إلكترونية للحساب أو الإدارة تضفي عليها مصداقية "[١] .

كما ان لتكنولوجيا المعلومات وما صاحبها من تطور حديث ادى للبحث عن معيار جديد غير المعيار الذي كان متبع وهو مادية الشيء ، الذي من خلاله نستطيع ان نطلق صفة المال على الشيء المعنوي ، إذ تبنى اصحاب هذا الاتجاه معيار القيمة الاقتصادية للشيء ، وبهذا فان الشيء يعدَّ مالاً عند النظر إلى قيمته الاقتصادية ، ولا ننظر إلى ماله من كيان مادي [٢].

وبناءً لما تقدم ان هذا الاتجاه يؤيد ارتكاب جريمة الاحتيال للمنصات الإلكترونية والعبرة عندهم الوسيلة المستخدمة بالاحتيال لا الشخص الذي خلف هذه الاجهزة وامكانية وقوع جريمة الاحتيال للمنصات الإلكترونية التي هي جزء من الوسائل الحديثة ، كما يمكن التسليم الضمني ايضاً على توجيه الطرق الاحتيالية باتجاه شخص يمكن ان يقع عن طريق الغلط من خلال التعامل المباشر عبر المنصات الإلكترونية إلى جريمة احتيال إلكترونية.

الاتجاه الثاني يرى اصحاب هذا الاتجاه امكانية تحقق السلوك الإجرامي في جريمة الاحتيال على الاشخاص الطبيعية ، وعدم تعرض الانظمة الإلكترونية للخداع والاحتيال ، وبالتالي عدم تطبيق النصوص التقليدية في جريمة الاحتيال على الانظمة الإلكترونية والمنصات الإلكترونية [٣] ، وهذه الدول ترفض فكرة تحقق جريمة الاحتيال معلله ذلك بأن عملية الاحتيال تنصرف إلى الشخص الذي يوجد خلف الحاسوب ، كما ان جريمة الاحتيال تتم عن طريق خداع المجنى عليه والتأثير عليه من قبل الجاني إذ يحمله على تسليم المال ، وان التسليم بوقوع التأثير على إرادة المجني عليه هو قول بعيد عن الواقع في حالة التلاعب ببرامج الكمبيوتر و المنصات الإلكترونية ، وهذا يعد توسعا في تطبيق قانون العقوبات ، كما انه لا يتفق مع مبدأ الشرعية الجنائية [٤] ، وتعد

([١]) يُنظر: د. محمد طارق عبد الرؤوف الخن ، مصدر سابق ، ص١٣٨.

([٢]) يُنظر: د. محمد عبيد الكعبي ، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت (دراسة مقارنة) ، مصدر سابق ، ص ٢٣٦.

([٣]) وهذا الاتجاه تتبناه كل من تشريعات الدول منها (مصر وألمانيا والدنمارك واليابان والنروج والسويد ولكسمبورغ) يُنظر: سامر سلمان الجبوري ، مصدر سابق ، ص٣٩.

([٤]) يُنظر: د. عمر أبو الفتوح عبد العظيم الحمامي ، مصدر سابق ، ص٦٤٧.

قضية "R.V Gold"من ابرز القضايا في المملكة المتحدة في هذا الموضوع [1] ،اما الفقه الفرنسي فقد ذهب إلى وقوع جريمة الاحتيال وعدم تحققها في الحاسوب ، وان استخدام الغش والخداع التي تحصل في انظمة الحاسوب لا تكون ضمن النطاق للطرق الاحتيالية، لان الاحتيال يجب ان يكون بين شخصي الجاني والمجني عليه[2].

يتضح أن الاتجاه الرافض لفكرة تحقق السلوك الإجرامي في جريمة الاحتيال للمنصات الإلكترونية التي يتم تثبيتها على جهاز الحاسوب أو أي جهاز إلكتروني أخر ، لا يمكن ان تحقق جريمة الاحيال لاستبعاد طرق الاحتيال والغش من نطاق الطرق الاحتيالية ، وانما تتحقق جريمة الاحتيال عند وجود شخصين وهما الجاني الذي يكون خلف تلك المنصات الإلكترونية والمجني عليه الذي يتعرض لفقدان ماله بطريقة غير مشروعة ، ونحن بدورنا لا نؤيد هذا الاتجاه إذ من الممكن تتحقق جريمة الاحتيال للمنصات الإلكترونية المثبتة على جهاز الحاسوب أو أي جهاز إلكتروني آخر من خلال الاحتيال على بعض المستخدمين أو العملاء وخداعهم ، وقيامهم بالوقوع تحت تاثير الجاني .

الاتجاه الثالث اما انصار هذا الاتجاه المتمثل بالولايات المتحدة الامريكية التي تطبق النصوص المتعلقة بالغش والاحتيال في مجال البريد والاتصالات والمصارف على السلوك الإجرامي في جريمة الاحتيال الإلكتروني ، وان بعض من القوانين المحلية في الولايات الامريكية اصدرت قوانين بهذا الخصوص تجرّم السلوك الإجرامي ومنها (كاليفورنيا وجورجيا واريزونا ومونتانا ومشجان وفلوريدا) و زادت تعريفاً موسعاً للأموال بأنه" كل شيء ينطوي على قيمة" وبهذا فان كل ما يندرج تحت هذا التعريف من اموال معنوية وبيانات المعالجة ، و تعاقب هذه القوانين جميع الاستخدامات غير المسموح بها للحاسب الالي بغرض اختراق أفعال الغش والاحتيال أو الاستيلاء على الاموال[3] ، اما على المستوى الفدرالي فان الحكومات الامريكية تقدمت بمشروع قانون يستهدف بصورة مباشرة الغش المعلوماتي ، إذ يعاقب مشروع القانون كل من يقوم

([1]) يُنظر: تتلخص أحداث هذه القضية في الحصول على شفرة تمكن المتهم وشريكة من الدخول إلى نظام المعلومات الذي توفره هيئة الاتصالات البريطانية إلى المهندسين التابعين لها ، وذلك مقابل رسوم محددة هذا بصفة عامة وحسب المعلومات المصرح الحصول عليها ، حيث قام المتهمان بالدخول والحصول على المعلومات دون دفع أي رسوم، وعند تقديمهما للمحاكمة رفضت المحكمة إدانتهما وتطبيق النص الخاص لجريمة الاحتيال =بسبب حصولهم على خدمات ، الامر الذي لا يستطيع تصوره في مواجهة العقل البشري من خلال ايقاعه في الغلط من أجل الحصول على المعلومات يُنظر: .د. حسام محمد نبيل الشنراقي ، مصدر سابق ، ص١٩٧.

([2]) يُنظر: د. أحمد حسام طه تمام ، الجرائم الناشئة عن استخدام الحاسب الآلي (دراسة مقارنة) ط١، دار النهضة العربية للنشر والتوزيع ، القاهرة ، ٢٠٠٠ ، ص٥٤٣.

([3]) يُنظر: د. حسني عبد السميع إبراهيم ، مصدر سابق ، ص٤٠٩-٤١٠.

باستخدام أي اسلوب احتيالي سواء بتصميم الخطط أو الحيلة بغرض ارتكاب غش أو الاستيلاء على مبالغ مالية ، أو حتى في حالة ولوج أو محاولة الولوج لأجهزة الحاسوب بغرض تنفيذ أو محاولة ارتكاب أفعال احتيالية[١].

يتضح لنا مما تقدم ان مشروع القانون المشار اليه اعلاه شمل جميع الوسائل التي تستخدم في حالات الاحتيال ، والتي تحمل في طياتها كل المكونات الإلكترونية فضلاً إلى الكيانات المنطقية التي تشمل المعلومات والبرامج ، وجميع قيمة سواء ذات طابع مادي كانت أو معنوي ، ومن جانبنا نؤيد الاتجاه الذي يقر بصلاحية وقوع الاحتيال على الانظمة الإلكترونية .

ثانيا: النتيجة الاجرامية في جريمة الاحتيال للمنصات الإلكترونية (التسليم)

يعد التسليم النتيجة الاجرامية في تحقق جريمة الاحتيال عن طريق استخدام الجاني وسائل الاحتيال لإيقاع المجني عليه في غلط يدفعه إلى تسليم ماله للجاني ، كما لا يختلف الامر في الاحتيال الإلكتروني ، إذ يقوم الجاني باستخدام اسلوب معين يؤدي إلى نتيجة مفادها الاستيلاء على مال الغير ، إذ يقوم المجني عليه بتسليم المال تحت تأثير الغلط الذي احدثه فعل الاحتيال[٢] ، ويتبادر سؤال في الاذهان هل ممكن ان يقع فعل التسليم الإلكتروني للأموال عن طريق المنصات الإلكترونية؟ ، في حقيقة الامر ان التسليم هو عبارة عن سلوك يصدر عمن وقع عليه الفعل الاحتيالي من قبل الجاني ، والذي يتم من خلاله خداع وتضليل المجني عليه ودفعه لتسليم المال ، اما في الاحتيال للمنصات الإلكترونية نجد ان المنصات الإلكترونية المثبتة على جهاز الحاسب الالي تقوم بفعل التسليم بالمفهوم المادي للكلمة ، كما يتم التسليم بالمناولة اليدوية في الاستعمال غير المشروع للبطاقات الائتمانية ، وان لا ننظر اليه بالشكل المادي فقط ، بل ننظر اليه على انه عمل قانوني والعنصر الجوهري فيه هو إرادة المجنى عليه المعيبة بالخداع التي تدفعه للتسليم ، اما المناولة المادية فهي مجرد مظهر مادي أو آثر[٣]، و في حالات اخرى فإن تسليم المال يتم بصورة غير مادية ، ففي هذه الحالة لا يمكن

---

(١) يُنظر: د . محمد امين الشوابكة ، جرائم الحاسب والانترنت ، ط١، دار الثقافة للنشر والتوزيع ، عمان ، ٢٠٠٤،ص١١٥.

(٢) يُنظر: د. حسام محمد نبيل الشراقي ، مصدر سابق ، ص٢٠٣.

(٣) يُنظر: د. حسام محمد نبيل الشراقي ، المصدر نفسه ، ص٢٠٣.

النظر للتسليم على انه واقعة مادية متمثلة بالمناولة اليدوية ، كما ان التسليم هو تصرف مالي قد تكون المناولة المادية إحدى صوره المتنوعة[١].

ففي حالة أذا اخذنا بالتسليم بهذا المعنى فلا يوجد أي اشكال او خلاف حول تحقق جريمة الاحتيال في مجال المنصات الإلكترونية ، لان التسليم ليس دائما تسليم مادي للاموال ، بل ممكن ان يكون التسليم بصورته المعنوية الذي يتلائم وطبيعة هذا النوع من التعاملات .

وان الاحتيال للمنصات الإلكترونية لا يختلف كثيراً عن الاحتيال التقليدي ، اذا تمت المناولة اليدوية للمال محل الجريمة ، والتسليم المعنوي في جريمة الاحتيال للمنصات الإلكترونية اساساً لا يقوم على انتفاء المناولة اليدوية ، بل ان جوهر التسليم يتعلق في اتجاه إرادة المجنى عليه إلى تسليم المال في يد الجاني ، وذلك من خلال قيامه في الاحتيال على المنصات الإلكترونية المثبتة على الحاسب الالي أو أي جهاز إلكتروني آخر.

كما لا يوجد اشكال في تحقق الاحتيال للمنصات الإلكترونية إذا كان الاستيلاء قائم على تسليم اموال منقولة مادية ، مثل التلاعب الذي يتم في المعلومات والبرامج المدخلة والتي يقوم عن طريقها استخراج صكوك أو فواتير بمبالغ غير مستحقة يستولي عليها الجاني ، إلا ان الاشكال الذي ممكن ان يثار في حالات اخرى يكون المحل فيها نقود كتابية ، كما لو تم التلاعب من قبل الجاني في البيانات أو البرامج والمعلومات المصرفية من أجل تحويل كل أو بعض الاموال أو الارصدة من حسابات الغير إلى حسابه[٢] ، ففي هذه الحالة هل يتم التسليم ام لا؟.

تختلف تشريعات الدول حول قابلية النقود الكتابية لان تكون محلاً لجريمة الاحتيال الإلكتروني وعليه يمكننا التمييز بين اتجاهين:

الاتجاه الاول رفضت بعض التشريعات المقارنة عدَّ النقود الكتابية من صنف الديون ، ولا يمكن الاعتراف لها بالصفة المادية ، وعليه لا تصلح لان تكون محلاً لجريمتي السرقة أو الاحتيال ومن هذه التشريعات ألمانيا والدنمارك وفلندا واليابان ومصر وقانون العقوبات الاماراتي [٣] ،اما الاتجاه الثاني فقد اتجهت بعض التشريعات الاخرى إلى عدَّ النقود الكتابية صنفاً من اصناف الاموال التي تصلح لان تكون محل لجريمة الاحتيال ومن هذه التشريعات كندا وهولندا وسويسرا وفي اغلب الولايات المتحدة الامريكية وانجلترا[٤].

---

(١) يُنظر: د. محمد طارق عبد الرؤوف الخن ، مصدر سابق ، ص١٦٩.

(٢) يُنظر: . سامر سلمان الجبوري ، مصدر سابق ، ص١٠٤.

(٣) يُنظر: د. عبدالفتاح بيومي حجازي ، جرائم الكمبيوتر والانترنت في التشريعات العربية (دراسة مقارنة مع التطبيق على نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية ، مصدر سابق ، ص١٢٨.

(٤) يُنظر: د. حسني عبد السميع إبراهيم ، مصدر سابق ، ص٤١٨-٤١٩.

وقد سبقت الاشارة إلى ان القوانين الفدرالية في الولايات المتحدة الامريكية عرفت المال بأنه (كل شيء يمثل قيمة ، بحيث يشمل جميع الاموال الكتابية أو المصرفية) ، وان القضاء الفرنسي ابتدع نظرية (التسليم المعادل) التي أقرتها محكمة النقض الفرنسية ، ومفاد النظرية التي عدت بأن الدفع الذي يتم عن طريق القيد الكتابي يكون معادلاً لتسليم النقود وبناءً على هذه النظرية فإن المادة ٣١٣من قانون العقوبات الفرنسي لعام ١٩٩٢ والتي تتعلق بالاحتيال تنطبق على جميع افعال التلاعب في عملية البرمجة أو البيانات المدخلة إلى الحاسوب والمنقولة عبر الانترنت[١] .

وان جميع عمليات التحويل غير المشروع والتي تتم عن طريق الانترنت ، أي بالدخول إلى انظمة المصارف والتلاعب بها ، والتي يترتب عليها الاستيلاء على كل أو بعض الارصدة العائدة للغير يعد التسليم بها محققاً معادلاً لتسليم النقود ، كما ويدعم ذلك اتجاه القضاء الفرنسي جانب من الفقه المصري الذي يرى أن التسليم في جريمة الاحتيال يتحقق بوضع الشيء تحت تصرف الجاني ، بحيث يتمكن من حيازته بغير عائق[٢] .

ثالثاً: العلاقة السببية في جريمة الاحتيال للمنصات الإلكترونية

تعد العلاقة السببية العنصر الثالث الذي يكتمل به الركن المادي الذي يتجلى بقيام الرابطة السببية ما بين طريقة الاحتيال التي يستخدمها الجاني وبين النتيجة الاجرامية التي تتمثل في تسليم المال محل الجريمة نتيجة الخداع الذي وقع به المجنى عليه ، وبالرجوع للقواعد العامة نجد ان العلاقة السببية تنحصر بثلاثة عناصر وهي أن يكون التسليم لاحق على فعل الاحتيال ، والتسليم يتم بناءً على غلط المجنى عليه ، والتسليم يتم نتيجة لانخداع المجنى عليه ،عند تحقق العناصر فإن الجاني يستحق العقاب لأنها عناصر جوهرية لتحقق العلاقة السببية ، اما إذا لم تكن النتيجة بسبب سلوك الجاني فإن الرابطة السببية تنعدم بينهم مما يؤدي لأنتفاء عنصر من عناصر العلاقة السببية لعدم وجود علاقة بين السلوك الإجرامي والنتيجة الإجرامية وبالتالي انتفاء الجريمة [٣]، اما العلاقة السببية في الاحتيال الإلكتروني تتمثل باستعمال الطرق الاحتيالية التي تؤدي بالمجنى عليه أن يسلم ماله للجاني ، لوقوعه في خطأ وانخداعه من قبل الجاني سواء حدث ذلك من شخص الجاني ذاته أم النظام الإلكتروني أم عن طريق المنصات الإلكترونية فإن النتيجة الإجرامية حصلت نتيجة لسلوك الجاني ، أي تحقق

---

(١) يُنظر: د. محمد طارق عبد الرؤوف الخن ، مصدر سابق ، ص١٧١-١٧٢.
(٢) يُنظر: د. نائلة عادل محمد فريد قورة ، مصدر سابق ، ص١٧٥.
(٣) يُنظر: د. عمر أبو الفتوح عبد العظيم الحمّامي ، مصدر سابق ، ص٧١٠.

العلاقة السببية بينهما ، مثل تقديم المستندات المستخرجة من الأنظمة الإلكترونية أم المعلومات المدخلة للمنصات الإلكترونية بالتلاعب فيها ليستولي الجاني على الاموال ليس له حق فيها [1].

ومن جانبنا نؤيد التشريعات التي اعترفت بالاستيلاء على الاموال الكتابية أو الإلكترونية ، ومنها القضاء الفرنسي لان التلاعب في المعلومات أو البرامج والقيام بإجراء التحويلات الإلكترونية لحساب الجاني من حساب المجني عليه ، من خلال القيام بالأفعال الاحتيالية ، وهذه نتيجة محتملة جداً ممكن تحققها في الجرائم التقليدية ، لكن التطور الحديث لتكنولوجيا المعلومات فرض ضرورة عملية تحتم علينا ، للنظر إلى طبيعة الجرائم الخاصة بالاحتيال الذي يقع عن طريق المنصات الإلكترونية ، والابتعاد عن القياس مع القواعد التقليدية والحث على وضع قوانين وتشريعات خاصة التي تحقق لنا الحماية الجزائية لأغلب الجرائم الإلكترونية الحديثة ومواكبة التطور.

الفرع الثاني

الركن المعنوي في جريمة الاحتيال للمنصات الإلكترونية

تعد جريمة الاحتيال من الجرائم العمدية إذ لا يتصور وقوع جريمة احتيال غير عمدية، ولتحقق جريمة الاحتيال الإلكتروني لا يكفي تحقق الركن المادي فقط ، يجب ان يتحقق معه الركن المعنوي والذي يتمثل بصورة القصد الجنائي العام بعنصريه العلم والإرادة أما القصد الجنائي الخاص يتمثل بنية التملك ، اما الباعث لا يعد من عناصر القصد الجنائي في جريمة الاحتيال ، ففي حالة تحقق الركن المادي والركن المعنوي في أي جريمة فلا عبرة للباعث على قيام الجريمة ، لكن الباعث يكون مؤثراً في مقدار العقوبة التي تفرض على الجاني من حيث التخفيف أو التشديد.

أولا: القصد الجرمي العام في جريمة الاحتيال للمنصات الإلكترونية

يتحقق القصد الجنائي العام في جريمة الاحتيال الإلكتروني عند تحقق عناصر القصد العام المتمثل بالعلم والارادة ، أي علم الجاني بأن ما يقوم به من فعل محاسب قانوناً ، ورغم ذلك تتجه إرادته إلى ذلك السلوك وتحقق النتيجة الإجرامية.

١- العلم :

يعد العلم عنصراً من عناصر القصد الجنائي العام لان الجاني يجب ان يعلم بأن الافعال التي يقوم بارتكابها تؤدي للخداع والتضليل ، مما يؤدي ذلك لا يقاع المجني عليه في الغلط الذي

([1]) يُنظر: د. محمود رجب فتح الله ، مصدر سابق ، ص٣٥٤

يدفعه لتسليم ماله ، وان الجاني يعلم ان ما يصدر عنه هو كذب وخلاف الحقيقة ، إذ ان الكذب هو جوهر الخداع في جريمة الاحتيال في شكلها التقليدي[١] ، اما في جرائم الاحتيال الإلكتروني فإن علم الجاني يتحقق عندما يتلاعب الجاني أو المحتال بالمعلومات ، وهو يعلم ان ما يقوم به فعل غير مشروع ، فضلاً عن علمه بان المعلومات التي قام بإدخالها للمنصات الإلكترونية المثبتة على جهاز الحاسب الآلي من شأنها ان تجعل المنصات الإلكترونية تستجيب لتلك المعلومات التي قام بإدخالها ، ويسلمه المعلومات التي كان يرغب في الحصول عليها ففي هذه الحالة يتحقق عنصر القصد الجنائي العام وهو العلم [٢] ، كما لو ان الجاني كان لا يعلم بالمعلومات التي قام بإدخالها بأنها صحيحة ، وان فعله مشروع أو اعتقد ان من حقه ادخال المعلومات للمنصات الإلكترونية ففي هذه الحالة فإن القصد الجرمي العام غير متوفر ، وبالتالي لا تتحقق الجريمة بحقه كما انه من غير اللازم ان يكون لدى الفاعل أو الجاني العلم بأن الوسيلة الاحتيالية هي مجرمة قانونا ، بل فقط ان يكون الجاني على علم بأن الوسيلة التي كان يستخدمها تؤدي للتلاعب بالمعلومات من أجل الحصول على ربح غير مشروع ، وان قانون العقوبات اليوناني أخذ بهذا الاتجاه [٣] ، كما اكدت ذلك ايضاً المذكرة التفسيرية للاتفاقية الاوربية لمكافحة جرائم المعلوماتية لعام ٢٠٠١وذلك من خلال الفقرة ب من المادة الثامنة التي نصت على " ان الجريمة ترتكب عمداً والعنصر العام للقصد ينطبق على التلاعب أو التدخل الإلكتروني الذي يسبب ضرراً اقتصادياً أو مادياً للغير"[٤].

يتضح لنا مما تقدم إن الحالتين سواء القصد الجرمي العام في الجرائم التقليدية أو الجرائم الإلكترونية ، فإن الجاني يكون على علم بان الفعل الذي يقوم به هو فعل غير مشروع ، الغاية منه الحصول على منفعة شخصية للجاني ، من خلال الكذب الذي يعد جوهر الخداع سواء كان ذلك الخداع مباشر للمجني عليه أو خداع المنصة الإلكترونية ، ففي الحالتين يتحقق عنصر العلم للقصد الجنائي العام والباحث يؤيد ما تم طرحه اعلاه ويضيف الباحث رأي جديد مفاده ان الجاني بمجرد الشروع في الخداع او التضليل سواء كان ذلك للإنسان أو لأي جهاز إلكتروني أخر فيجب ان تطبق عليه النصوص العقابية حتى لا يتحجج الجاني في المستقبل بأنه لا يعلم بان الفعل الذي قام به غير مشروع .

---

(١) يُنظر. د. عمر أبو الفتوح عبد العظيم الحمامي ، مصدر سابق ، ص٧١٦-٧١٧.

(٢) يُنظر: عبد الفتاح سليمان ، مصدر سابق ، ص٤٠٣.

(٣) يُنظر: د. حسام محمد نبيل الشنراقي ، مصدر سابق ، ص٢٢٣.

(٤) يُنظر: د. هلالي عبد اللاه أحمد ، إتفاقية بودابست لمكافحة جرائم المعلوماتية ، مصدر سابق ، ص ١٠٤.

١- الإرادة :

الإرادة العنصر الثاني للقصد الجرمي العام الذي يتحقق في اتجاه إرادة الجاني لتحقيق النتيجة الاجرامية ، في سلب مال الغير عن طريق خداع المجني عليه ووقوعه في خطأ يدفعه إلى تسليم ماله ، كما ان من البديهي لتحقق القصد الجرمي العام ان يتحقق عنصر الارادة بجانب عنصر العلم ، اما بالنسبة للجرائم التي يقوم بها الجاني في الاحتيال على المنصات الإلكترونية فإن إرادته تتجه للتلاعب في المعلومات وإدخالها بأية وسيلة من الوسائل الاحتيالية التي نصت عليها التشريعات الاجنبية والعربية ، وان تتجه ارادة الجاني لتحقيق النتيجة الإجرامية المجرّمة قانوناً وهي الحصول على المعلومات عن طريق إدخال معلومات صحيحة إلى النظام الإلكتروني ، بعلم وإرادة الجاني من أجل الحصول على منفعة شخصية مخالفة للقانون[١].

بناءً لما تقدّم ذكره يتضح لنا عدم قيام القصد الجرمي العام دون توافر عنصري العلم والإرادة معاً لذلك لا يمكن تصور تحقق القصد الجنائي العام دون تحققهما مطلقاً ففي جميع الاحوال يجب ان يعلم الجاني بأن فعله يعد جريمة كذلك يجب ان تتجه إرادته لتحقيق النتيجة الإجرامية ، وفي حال طبقنا ذلك على المنصات الإلكترونية فالباحث يؤيد امكانية تحقق الركن المعنوي عن طريقها وتحقق القصد العام بعنصريه العلم والإرادة.

ثانياً: القصد الجرمي الخاص في جريمة الاحتيال للمنصات الإلكترونية

يتمحور القصد الجنائي الخاص بنية التملك لدى الحاني على مال الضحية أو المجنى عليه وممارسة جميع حقوق الملكية على ذلك المال من تصرف واستئثار ، ففي هذه الحالة تنشأ جريمة الاحتيال ، كما ان النية لا تخرج عن نطاق عناصر القصد الخاص ، كما لو قام الجاني باستخراج فواتير ومبالغ غير مستحقه باسمه أو باسم شركائه ثم تقاسموها فيما بينهم[٢].

اما في مجال معلومات للمنصات الإلكترونية فيجب ان تتجه إرادة الجاني إلى تحقيق ربح غير مشروع له أو لغيره ، كما ان الفقرة ب من المادة الثامنة من اتفاقية بودابست لمكافحة جرائم المعلوماتية " ان يكون الجاني قد نفذ الجريمة بنية الحصول على منفعة اقتصادية غير مشروعة له أو للغير"[٣] ، والتي فسرت بأن جريمة الاحتيال في نطاق المعلومات الإلكترونية والتي يتطلب توافر القصد الجرمي العام اضافة لتوافر القصد الجرمي الخاص المتمثل "بنية

---

(١) يُنظر: د. محمد طارق عبد الرؤوف الخن ، مصدر سابق ، ص١٨٢.

(٢) يُنظر: د. عمر أبو الفتوح عبد العظيم الحمامي ، مصدر سابق ، ص٧١٨.

(٣) يُنظر: د. هلالي عبد اللاه أحمد ، إتفاقية بودابست لمكافحة جرائم المعلوماتية ، مصدر سابق ، ص١٠٣.

الغش ، أو بتعبير أخر نية غير أمينة أو غير شريفة بغرض الحصول على منفعة اقتصادية لنفسه أو للغير"[١].

والقصد الجرمي في الجرائم التي تتعرض لها المنصات الإلكترونية يختلف حسب نوع الجرائم المرتكبة ، بالاضافة للأساليب المستخدمة فيها اذ ان نية الجاني في الاستيلاء على مال المجني عليه من خلال استهداف حساباته الشخصية ومعلوماته الخاصة والغاية من ذلك سحب امواله من قبل الجاني ، في حين ان الاعتداء على مواقع الاستثمار فضلاً عن الاعتداء على سرية المعلومات الخاصة بها ، يدل على نية الجاني في خداع وتضليل المستثمرين والحصول على اموالهم ، يعد طريقة من طرق الاحتيال المعاقب عليها قانوناً ، ويتم اثبات القصد الجرمي للجاني في جريمة الاحتيال للمنصات الالكترونية من خلال القرائن ، أو عن طريق تفتيش أداة الجريمة ، فضلاً عن معرفة المواقع التي قام بتصفحها الجاني والاتصالات التي أجراها من أجل الوصول إلى دليل إدانته في جريمة الاحتيال[٢] .

اما المشرع الاماراتي فقد نص في المادة (١١) من القانون رقم ٥ لسنة ٢٠١٢ على معاقبة الجاني بأنه" كل من استولى لنفسه او لغيره بغير حق على مال منقول او منفعة او على سند او توقيع هذا السند ، وذلك بالاستعانة بأي طريقة احتيالية او باتخاذ اسم كاذب او انتحال صفة غير صحيحة عن طريق الشبكة المعلوماتية او نظام معلومات الكتروني او احدى وسائل تقنية المعلومات[٣] .

وفي العراق وعلى الرغم من تطور التكنولوجيا وكثرة استخدام الانترنت في الوقت الحاضر إلا انه لا يوجد أي قانون يقوم بتنظيم مقدمي خدمات الانترنت الذي ازداد عددهم في الاونه الاخيرة ، كما ان قانون العقوبات العراقي رقم ١١١لسنة ١٩٦٩المعدل في المادتين ٤٥٦و٤٥٧ جرمت جرائم الاحتيال بشكله التقليدي[٤] ، اما الاشكال الذي يثار في حالة حدوث جريمة احتيال إلكترونية ، هل ستطبق عليها النصوص التقليدية ام يرفض القضاء السماع للدعوى؟ ، للإجابة على هذا الاشكال اتجهت محكمة جنح الكوت بتاريخ ٢٠٢٠/١٢/٢٩ حيث ادانة المتهم على ثلاثة كل واحدة منها وفق أحكام المادة (١/٤٣٨) [٥] من قانون العقوبات العراقي والحكم على

---

(١) يُنظر: د. حسام محمد نبيل الشنراقي ، مصدر سابق ، ص٢٢٥.
(٢) يُنظر: د. محمد طارق عبد الرؤوف الخن ، مصدر سابق ، ص١٨٣.
(٣) يُنظر المادة ١١ من مرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢ لمكافحة جرائم أنظمة المعلومات الاماراتي .
(٤) يُنظر: د. حسني عبد السميع إبراهيم ، مصدر سابق ، ص٧٥-٧٦.
(٥) يُنظر: المادة (١/٤٣٨) من قانون العقوبات العراقي رقم (١١١) لسنة (١٩٦٩) النافذ التي نصت على (يعاقب بالحبس مدة لا تزيد على سنة وبغرامة لا تزيد على مائة دينار ، أو بإحدى هاتين العقوبتين ،

كل واحدة منها بالحبس البسيط لمدة ثمانية أشهر تنفذ بحقه بالتعاقب بادر محامي المدعي الأول بتميز القرار طالباً فيه تشديد العقوبة للأسباب التي ذكرها في لائحته المؤرخة في ٢٠٢١/١/٢٦كذلك قدم محامي المتهم لائحة تمييزية بتاريخ ٢٠٢١/١/٢٨طالباً فيها الافراج عن موكله لما ورد ورد من أسباب في لائحته التي تم الاشارة إليها ، ولتعلق الامر بموضوع واحد قرر توحيدهما معاً وعرضهما على السيد المدعي العام في واسط لبيان الرأي القانوني أعيدت الدعوى من قبل المدعي العام بموجب المطالعة المرقمة ١٢٨في ٢٠٢١/٢/١٥التي طلب فيها نقض القرار المميز ، ووضع الاضبارة موضع التدقيق والمداولة، وبعدها صدر القرار حيث وجدت المحكمة أن القرار الصادر بحق المتهم جاء صحيح وموافق لأحكام المادة ١/٤٣٨من قانون العقوبات العراقي للأسباب والحيثيات الواردة فيه ، كما أن العقوبة المفروضة بحق المتهم جاءت متفقة واحكام القانون لذا قررت المحكمة تصديق القرار ورد الطعن التمييزي ، أما بخصوص بقية المشتكين الاخرين وجدت أن الادلة المتحصلة ضده لا تكفي لإدانة المتهم لأنها اقتصرت على أقوال المشتكي ولم يرد ضدها اعترافات المتهم الإساءة إلى المشتكي أنف الذكر حيث أن وقائع القضية والظروف تشير إلى قيام المتهم بإختراق صفحة التواصل الإجتماعي للمشتكي من خلال تزوير هويته عن طريق برنامج (الفوتوشوب) وارسالها إلى فيس بوك منتحلاً شخصيته لذا قررت اشعار محكمة التحقيق بإتخاذ الإجراءات القانونية بحق المتهم وفق أحكام المادة (٢٩٢) [1]من قانون العقوبات العراقي رقم (١١١) لسنة (١٩٦٩) النافذ ، وقيد الرسم ايراداً إلى خزينة الدولة وصدر القرار بالإتفاق استناداً لأحكام المادة (٢٥٩/أ/١،٦) من قانون أصول المحاكمات الجزائية وبدلالة القرار (١٢٤) لسنة (١٩٨٨) في (٢٠٢١/٢/٢٢) [2].

يتضح لنا مما تقدم عند حدوث جريمة احتيال للمنصات الإلكترونية وعدم وجود قانون خاص بالجرائم الإلكترونية فإن القضاء العراقي يطبق النصوص العقابية التقليدية ، وحسناً فعل القضاء العراقي من أجل عدم إفلاة الجناة ، على الرغم من أن بعض العقوبات لا تنسجم مع الجريمة المرتكبة إذ نجد في قرار الحكم المشار إليه تم محاكمة المتهم وفق المادة ١/٤٣٨

١- من نشر بإحدى طرق العلانية أخباراً أو صوراً أو تعليقات تتصل بأسرار الحياة الخاصة أو العائلية للأفراد ولو كانت صحيحة إذا كان من شأن نشرها الأساءة إليهم).

(١) يُنظر: المادة (٢٩٢) من قانون العقوبات العراقي رقم (١١١) لسنة (١٩٦٩) النافذ التي نصت على (يعاقب بالحبس وبالغرامة التي لا تزيد على ثلاثمائة دينار أو بإحدى هاتين العقوبتين من توصل بانتحال اسم كاذب أو شخصية كاذبة إلى الحصول على أية رخصة رسمية أو تذكرة هوية أو تذكرة أنتخاب عام أو تصريح نقل أو انتقال أو مرور داخل البلاد).

(٢) يُنظر: مجلس القضاء الأعلى ، رئاسة استئناف واسط الاتحادية الهيئة التمييزية ، قرار التمييز ذو العدد (٢١١/ت/جنح/٢٠٢١) ، بتاريخ (٢٠٢١/٢/٢٢).

الخاصة بنشر الامور الخاصة بطرق العلانية ، وعند تمييز القرار لاحظ وجود أكثر من جريمة لان المتهم قام بالتزوير وانتحال شخصية الغير فيحاكم وفق المادة ٢٩٢.

الخاتمة

الخاتمة

بعد أن أنهينا دراستنا (الحماية الجزائية للمنصات الإلكترونية - دراسة مقارنة -) نقدّم مجموعة من الاستنتاجات والمقترحات التي توصلنا إليها من خلال دراستنا وفق الآتي :

أولاً: الاستنتاجات:

١- أتضح أن غالبية التشريعات لم تعرّف المنصات الإلكترونية تعريفاً دقيقاً وصريحاً ، بل تركت تعريفه للفقه الجنائي ، الذي أختلف أغلبهم من حيث الصياغة التشريعية والتسمية لكنها تتفق من حيث المضمون ، وعدم تحديد تعريف معين يعد من الامور الايجابية إذا تم تعيين تعريف محدد للمنصات الإلكترونية فإنه يؤدي إلى الجمود وعدم التوسع مما يعني ذلك عدم مواكبة التطورات السريعة في عالم التكنولوجيا.

٢- استنتجنا أن الحماية الجزائية للمنصات الإلكترونية أصبحت من الأمور المهمة والضرورية لأنها تمس جميع المصالح الحياتية للفرد والمجتمع ، فمصلحة الفرد التي يحميها القانون أصبحت محل للاعتداءات من قبل الجناة على مختلف فئاتهم ، وعدم توفير الحماية لمصالح الافراد والمؤسسات الحكومية وغير الحكومية ، يؤدي إلى زعزعة أمن واستقرار المجتمع.

٣- تبيَن لنا أن المنصات الإلكترونية تكون أما هدف الجريمة أو الوسيلة في ارتكاب الجريمة أو محل ارتكاب الجريمة.

٤- أتضح ان قوانين الدول محل الدراسة عند تطبيقها للنصوص الخاصة في جريمة سرقة المنصات الإلكترونية ، فأنها تتعرض لمجموعة من العقبات التي لا تتفق مع الطبيعة غير المادية لمعلومات المنصات الإلكترونية في تحقق الاختلاس المكون لجريمة السرقة ، وأهم تلك العقبات ضرورة أن يكون الشي محل جريمة السرقة قابل للتملك وأن يكون ذا طبيعة مادية ملموس وأن يكون قابلاً للنقل من حيازة إلى أخرى.

٥- بعض قوانين الدول محل الدراسة اتجهت إلى سن قوانين خاصة أو تعديل قوانينها العقابية لتجريم الاحتيال الإلكتروني ، بينما قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩المعدل يعاني من قصور تشريعي في مكافحة جريمة الاحتيال الإلكتروني.

٦- الهدف من الحماية الجزائية للمنصات الإلكترونية هو حماية المعلومات التي تحتويها من الجرائم التي تتعرض لها ، كذلك حماية المعلومات الشخصية لبعض الاشخاص خوفاً من استغلالها لتحقيق أغراض سياسية أو طائفية ، أو ربما يكون اثبات قدرة المخترقين وتفوقهم على التقنية الحديثة للمنصات الإلكترونية.

٧- لاحظنا اهتمام الدول المقارنة بمواكبة التطور التكنولوجي من خلال سن تشريعات خاصة لمكافحة الجرائم الإلكترونية ، وتوفير الحماية لأنظمتها ووسائلها الإلكترونية من شتى الاعتداءات التي تتعرض لها ومن أمثلتها القانون الامريكي لسنة ١٩٨٤ وتعديلاته وقانون العقوبات الفرنسي رقم ١٩ لسنة ١٩٨٨وتعديلاته ومرسوم بقانون اتحادي الاماراتي رقم ٥لسنة ٢٠١٢وقانون الجرائم الإلكترونية الاردني رقم ٢٧لسنة ٢٠١٥، مقابل القصور التشريعي في القانون العراقي على الرغم من وجود مشروع قانون الجرائم الإلكترونية العراقي لسنة ٢٠١١ .

٨- تعرّفنا على الدور المهم من قبل الاتحاد الاوربي من خلال الاتفاقية الاوربية المتمثلة باتفاقية بودابست لعام ٢٠٠١ والتي تُعدَّ القدوة للكثير من الدول في سن تشريعات خاصة لمكافحة الجرائم المعلوماتية ، لاحظنا انها بدأت تشعر بالخطر من ظاهرة الاجرام الإلكتروني ، الذي بدأ بالتزايد في الدول العربية لذا صدرت العديد من القوانين التي تكافح الجريمة الإلكترونية .

٩- تبيَن أن توفير الحماية الجزائية للمنصات الإلكترونية هو من أهم المتطلبات لإقامة حكومة إلكترونية ، من أجل التسهيل والتخفيف عن الافراد والمؤسسات الحكومية وغير الحكومية في جميع التعاملات الإلكترونية ، فضلاً عن ان هذه الحماية تحقق الردع العام والخاص ، وبالتالي ينعكس إيجاباً توفير الحماية على رفاهية وتطوير الاقتصاد للبلد.

١٠- تبين لنا قصور الحماية التشريعية لعدم كفاية القوانين التقليدية لمكافحة الجرائم المستحدثة ، كذلك قصور الأمن التقني في تعزيز الحماية للمنصات الإلكترونية ، مما يجعلها عرضة للكثير من محاولات الاعتداء بمختلف الجرائم التي تكون المنصات الإلكترونية محلا لوقوعها أو وسيلة لارتكابها.

١١- استنتجنا أن أغلب الجناة في جرائم المنصات الإلكترونية هم ممن يمتلكون المعرفة التقنية والفنية باستخدام التكنولوجيا الحديثة ، وتطويعها للقيام بجرائمهم من دون أن يعلم بهم ضحاياهم ، وبالمقابل نرى سكوت أغلب الضحايا لخوفهم من الإساءة لهم أو لسمعتهم التي يتمتعون بها .

١٢- لاحظنا أن جرائم المنصات الإلكترونية من الجرائم العابرة للحدود ، أي لا تتحدد بالمكان ولا تتوقف على زمن معين ، فتطور الوسائل التقنية الحديثة ومنها المنصات الإلكترونية أدى إلى تمكن الجناة من سرقة معلومات المنصات الإلكترونية والاحتيال عليها واختراقها ، خصوصاً المعلومات السرية والشخصية التي تحتويها.

١٣- اتضح لنا أن الجرائم التي يتم ارتكابها ضد المنصات الإلكترونية يمكن ان تتم من قبل شخص واحد أو قد ترتكب من قبل مجموعة من الاشخاص ، كما ويمكن أن ترتكب من قبل

اشخاص يتمتعون بمراكز مهمة في دوائرهم والحصول لأنفسهم أو لغيرهم فائدة غير مشروعة على حساب الغير.

١٤- تبيَن لنا ان سلوك الجاني في جرائم المنصات الإلكترونية يختلف بحسب نوع الجريمة فهو يختلف بجريمة السرقة الإلكترونية عن جريمة الاحتيال الإلكتروني وكذلك عن جريمة الدخول وجريمة الاتلاف ، فإن تكييفها يختلف من جريمة إلى أخرى في حين نجد النصوص التقليدية عاجزة امام مكافحة الجرائم الإلكترونية خصوصاً في العراق.

١٥- اتضح أن حظر جريمة الدخول للمنصات الإلكترونية ، يعد حماية للمنصات الإلكترونية لأن الدخول يؤدي إلى الاعتداء والانتهاك للمعلومات أو التقاطها دون علم صاحبها وأغلب التشريعات عاقبت على الدخول سواء كان الدخول كُلي أو بجزء في النظام ، من أجل توفير الحماية للنظام نفسه أو الجرائم التي تقع ضده.

١٦- استنتجنا أن أغلب الدول تعتمد على العقوبة كأسلوب وقائي ورادع يهدد كل من يحاول الاعتداء على المنصات الإلكترونية وما تحتويها من معلومات ، إلا أن قصور التشريعات واضح في مكافحة الجرائم الإلكترونية التي تتعرض لها الوسائل الإلكترونية بكل أنواعها .

١٧- نستنتج مما تقدم أن قانون تصديق الاتفاقية العربية لمكافحة جرائم تقنية رقم ٣١لسنة ٢٠١٣ أغفلت تحديد العقوبة ومدتها

ثانيا: المقترحات:

١- ندعو المشرَع العراقي إلى إضافة الجرائم الإلكترونية المستحدثة ومنها جرائم المنصات الإلكترونية بجميع أنواعها في مقترح تعديل قانون العقوبات العراقي رقم١١١لسنة ١٩٦٩قبل التصويت عليه

٢- نقترح التصويت على مشروع قانون مكافحة الجرائم الإلكترونية العراقي لسنة ٢٠١١، من أجل توفير الحماية الجزائية للمنصات الإلكترونية بجميع أنواعها ومواكبة التطورات التكنولوجية الحديثة التي تحقق جزءاً من الامن الإلكتروني للفرد والمجتمع على حد سواء.

٣- ضرورة تشديد العقوبات في القوانين التي لها صلة بالجرائم الإلكترونية ، من أجل توفير حماية لجميع الانظمة الإلكترونية أو المنصات الإلكترونية أو أي جهاز إلكتروني آخر .

٤- ضرورة اضافة منهج جديد لكليات الشرطة يتضمن التقنيات الحديثة ومنها المنصات الإلكترونية ، ومعرفة الجرائم التي تتعرض لها وسبل مكافحتها .

٥- العمل على تحديث وتطوير البرامج التدريبية التي تؤدي إلى تنمية قدرات الذين يعملون في مكافحة الجرائم الإلكترونية ، فضلاً عن إقامة دورات في خارج البلد مع دول لها تجارب ناجحة

في هذا المجال للاستفادة من خبراتهم في الحد أو التقليل من خطر الجرائم الإلكترونية ، من أجل توفير الحماية واستقرار المجتمع .

٦- من أجل مواكبة التطورات التكنولوجية الحديثة والجرائم التي تتعرض لها المنصات الإلكترونية ندعو المشرع العراقي إلى تعديل قانون أصول المحاكمات الجزائية وتضمينه إجراءات صريحة تسهل على القضاء الرجوع إليها عند تطبيق النصوص العقابية على الافعال الاجرامية المستحدثة مثل جرائم سرقة معلومات المنصات الإلكترونية والاحتيال وجريمة الدخول وجريمة إتلاف معلومات المنصات الإلكترونية وغيرها من الجرائم الإلكترونية الآخرى التي تتعرض لها المنصات الإلكترونية بجميع أنواعها.

٧- الحث على إعداد الكوادر البشرية وتدريبها وفق أعلى المستويات على يد منظومة متكاملة من الكوادر الفنية المتخصصة ، الذين يتمتعون بالخبرة والكفاءة التقنية في جميع مجالات التكنولوجيا الحديثة ، من أجل رصد الأفعال الإجرامية المستحدثة التي تتعرض لها المنصات الإلكترونية .

٨- الحث على توعية مستخدمي المنصات الإلكترونية بحقوق وواجبات وضوابط الاستخدام الصحيح من خلال وسائل الاعلام والورش العلمية من أجل الحد من الجرائم التي يتعرض لها المجتمع .

٩- نقترح تشديد العقوبة على الأفعال العمدية التي تتضمن التعديل أو الاخفاء أو التدمير أو المحو للمعلومات المعالجة آلياً والتسبب بإتلافها أو إتلاف معلومات المنصات الإلكترونية ، سواء كان الإتلاف كلياً لمعلومات المنصات الإلكترونية أو جزئياً ، لان غالبا الجناة يحاولون التخريب والتعطيل واخفاء أدوات الجريمة من أجل ان لا تتمكن السلطة من معرفتهم والقاء القبض عليهم .

١٠- العمل على استحداث غرفة خاصة للتحقيق في الجرائم الإلكترونية على ان يكون المحققين فيها ممن لديهم خبرة تقنية في التكنولوجيا الحديثة فضلاً عن الخبرة القانونية مما يسهم في حسم القضايا في الجرائم الإلكترونية والوصول للجناة في أسرع وقت.

١١- نقترح وضع نصوص عقابية تضمن عدم ارتكاب الجرائم الإلكترونية من خلال تعديل قانون الاتفاقية العربية لمكافحة جرائم المعلومات رقم ٣١لسنة ٢٠١٣، ليس فقط الاشارة للجرائم.

١٢- نقترح عند التقديم للتعيين في التخصصات القانونية اضافة شرط للمتقدمين وهو ان يكون المتقدم ملم بجميع الجرائم الإلكترونية ، وكيفية ارتكابها وسبل الحماية منها .

١٣- كما نقترح اضافة فقرة ثانية للمادة السابعة من مشروع قانون الجرائم الإلكترونية العراقي لسنة ٢٠١١ وتكون الفقرة المضافة بالشكل التالي

المادة -٧- يعاقب بالسجن المؤقت وبغرامة لا تقل عن (١٠٠٠٠٠٠٠) عشرة ملايين دينار ولا تزيد على (٣٠٠٠٠٠٠٠) ثلاثين مليون دينار كل من

اولاً- استخدم عمداً نظام الحاسوب أو شبكة المعلومات العائدة للأشخاص أو الشركات أو الهيئات أو المصارف أو الأسواق المالية وتمكن من الاستيلاء على أموال الغير أو حقوقهم المالية أو حقق لنفسه أو لغيره منفعة مالية أو حرم الغير من حقوقه المالية بأية وسيلة من الوسائل الإلكترونية.

ثانياً- كل من توصل عمداً لنظام الحاسب الآلي أو لمعلومات المنصات الإلكترونية العائدة للأشخاص أو الشركات أو مؤسسات الدولة وتمكن من الاستيلاء لنفسه أو لغيره على مال منقول أو معلومات خاصة أوعامة وأدى ذلك إلى حرمان اصحابها منها بأية وسيلة من الوسائل الإلكترونية .

١٤-كما نقترح تعديل نص المادة ٤٣٩بإضافة النظام الإلكتروني لها من أجل مواكبة التطور الحاصل في الجرائم الإلكترونية ، ويصبح نص المادة المقترحة كما يأتي

المادة ٤٣٩"السرقة اختلاس مال مادي منقول أومعنوي مملوك لغير الجاني عمداً ، ويعدَّ مالاً مادياً لتطبيق أحكام السرقة النبات وكل ما هو متصل بالأرض أو مغروس فيها بمجرد فصله عنها والثمار بمجرد قطفها ومالاً معنوياً النظام الإلكتروني وكل ما هو مخزّن فيه من معلومات وبرامج والقوى الكهربائية والمائية وكل طاقة أو قوة محرزة أخرى".

المصادر

المصادر

القران الكريم :

أولا: المعاجم

١- أحمد رضا ، معجم متن اللغة ، ج ٥ ، دار مكتبة الحياة ، بيروت ، ١٩٦٠

٢- أحمد مختار عمر ، معجم اللغة العربية المعاصرة ، ط١، مجلد١، عالم الكتب ، القاهرة ، ٢٠٠٨.

٣- إيلي ضناوي ، معجم الطلاب ، عربي إيطالي ، دار الكتب العلمية ، ط٢، بيروت ، لبنان ، ٢٠٠٥.

٤- جبران مسعود ، الرائد ، ط٧، دار العلم للملايين ، بيروت ، ١٩٩٢

٥- جرجس جرجس ، معجم المصطلحات الفقهية والقانونية ، ط١، الشركة العالمية للكتاب ، بيروت ، ١٩٩٦.

٦- رجب عبد الجواد إبراهيم ، المعجم العربي لأسماء الملابس ، ط١ ، دار الافاق العربية ، القاهرة ، ٢٠٠٢.

٧- شوقي ضيف ، المعجم الوسيط ، ط٤، مكتبة الشروق الدولية ، مصر ، ٢٠٠٤.

٨- عبدالغني أبو العزم ، معجم الغني ، موقع معاجم صخر ، ٢٠١١.

٩- فريال علوان وأخرون ، القاموس عربي – فرنسي ، ط٢ ، دار الكتب العلمية ، بيروت ، لبنان ، ٢٠٠٤.

١٠- محمد بن أبي بكر بن عبدالقادر الرازي ، مختار الصحاح ، دار المعاجم ، بيروت ، ١٩٨٦.

ثانيا: الكتب

١- إبراهيم محمد منصور ، الجرائم الإلكترونية في الشريعة الإسلامية والقوانين الوضعية بحث فقهي مقارن ، ط١، دار الفكر الجامعي ،٢٠١١.

٢- أحمد حسام طه تمام ، الجرائم الناشئة عن استخدام الحاسب الآلي (دراسة مقارنة) ط١، دار النهضة العربية للنشر والتوزيع ، القاهرة ، ٢٠٠٠.

٣- أحمد خليفة الملط ، الجرائم المعلوماتية ، ط٢، دار الفكر الجامعي ، مصر ، ٢٠٠٦.

٤- أحمد عبابنة ، جرائم الحاسوب وابعادها الدولية ، ط١، دار الثقافة للنشر ، الاردن ، ٢٠٠٩.

٥- أحمد محمد فخري ، منال عبد العال مبارز، التعليم الإلكتروني (مفهومه – بيئاته – مقرراته – إدارته – تقويمه – تطبيقاته المتقدمة) ط١ ، دار الزهراء للنشر والتوزيع ، الرياض ، ٢٠١٣.

٦- أسامة فرج الله محمود الصباغ ، الحماية الجنائية للمصنفات الإلكترونية ، دار الجامعة الجديدة ،٢٠١٦ .

٧- أمير فرج يوسف ، الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت ، ط١، مكتبة الوفاء القانونية ، ٢٠١١.

٨- أيمن رمضان محمد أحمد ، الحماية الجنائية للتوقيع الإلكتروني ، دار النهضة العربية ، القاهرة ،٢٠١١.

٩- جاسم رمضان هلالي ، الدعاية والإعلان والعلاقات العامة في المدونات الإلكترونية ، ط١، دار النفائس للنشر والتوزيع ، عمان ، ٢٠١٣.

١٠- جلال محمد الزغبي ، اسامة أحمد المناعسة ، جرائم تقنية نظم المعلومات الإلكترونية (دراسة مقارنة) ، ط١، دار الثقافة ، عمان ، ٢٠١٠، ص٢١.

١١- جميل إطميزي ، فتحي السالمي ، الموارد التعليمية المفتوحة الاستخدام والمشاركة والتبني ، بلا طبعة ، المنظمة العربية للتربية والثقافة والعلوم (الألكسو) ، جامعة الدول العربية ، تونس ، ٢٠١٩.

١٢- جميل عبدالباقي الصغير ، القانون الجنائي والتكنولوجيا الحديثة ، ط١، ك١، دار النهضة العربية ، ١٩٩٢.

١٣- حذيفة مازن عبد المجيد ، مزهر شعبان العاني ، التعليم الإلكتروني التفاعلي ، ط١ ، مركز الكتاب الاكاديمي ، عمان ، ٢٠١٥.

١٤- حسام محمد نبيل الشنراقي ، الجرائم المعلوماتية دراسة تطبيقية مقارنة على جرائم الاعتداء على التوقيع الإلكتروني ، دار الكتب القانونية ، ٢٠١٣.

١٥- حسين حسن موسى ، استخدام الوسائط المتعددة في البحث العلمي (التعليم الإلكتروني ودور الوسائط) ، دار الكتاب الحديث ، القاهرة ، ٢٠٠٩.

١٦- حسني عبد السميع إبراهيم ، الجرائم المستحدثة عن طريق الإنترنت (دراسة مقارنة بين الشريعة والقانون) ، ط١، دار النهضة العربية ، القاهرة ، ٢٠١١.

١٧- حشمت قاسم ، الدوريات الإلكترونية والمكتبات الرقمية ، ط١ ، دار غريب للطباعة والنشر والتوزيع ، القاهرة ، ٢٠١٠.

١٨- حمزة محمد أبو عيسى ، محمد شبلي الشلبي العتوم ، القانون الجزائي الفرنسي ،ط١، دار وائل للنشر والتوزيع ، ٢٠٢٠.

١٩- خالد ممدوح إبراهيم ، الحماية القانونية للعلامات التجارية مدنياُ وجنائياً ، دار الفكر الجامعي ، ٢٠١٩.

٢٠- خالد ممدوح إبراهيم ، فن التحقيق الجنائي في الجرائم الإلكترونية ، ط١، دار الفكر الجامعي ، الاسكندرية ، ٢٠٠٩.

٢١- رأفت عبد العزيز البوهي ، الجودة الشاملة في التعليم ، ط١ ، دار العلم والايمان للنشر والتوزيع ، كفر الشيخ ، ٢٠١٨.

٢٢- ربحي مصطفى عليان ، المكتبات الإلكترونية والمكتبات الرقمية ، ط٢، دار صفاء للنشر والتوزيع ، عمّان ، ٢٠١٥.

٢٣- رشيدة بوكر ، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن ، ط١، منشورات الحلبي الحقوقية ، ٢٠١٢ .

٢٤- رضوان عبد النعيم ، المنصات التعليمية المقررات التعليمية المتاحة عبر الأنترنت ، ط١، دار العلوم للنشر والتوزيع ، ٢٠١٦.

٢٥- رفد عيادة الهاشمي ، الارهاب الإلكتروني القانوني ، ط١، دار أمجد للنشر والتوزيع ،٢٠١٩.

٢٦- رؤوف عبيد ، السببية في القانون الجنائي ، ط٢ ، مطبعة نهضة مصر ، ١٩٦٦.

٢٧- سامر سلمان الجبوري ، جريمة الاحتيال الإلكتروني (دراسة مقارنة) ، ط١، مكتبة زين الحقوقية والادبية ، بيروت ، ٢٠١٨.

٢٨- شريف الإتربي ، التعليم الإلكتروني والخدمات المعلوماتية ، ط١، العربي للنشر والتوزيع ، القاهرة ، ٢٠١٥.

٢٩- شريف الأتربي ، التعليم بالتخيل إستراتيجية التعليم الإلكتروني وأدوات التعلم ، ط١، العربي للنشر والتوزيع ، القاهرة ، ٢٠١٩.

٣٠- شريف درويش اللبان ، الصحافة الإلكترونية دراسات في التفاعلية وتصميم المواقع ، ط١، الدار المصرية اللبنانية ، القاهرة ، ٢٠٠٥.

٣١- شمسان ناجي صالح الخيلي ، الجرائم المستخدمة بطرق غير مشروعة لشبكة الإنترنت (دراسة مقارنة) ، دار النهضة العربية ، القاهرة ، ٢٠٠٩.

٣٢- طارق عبد الرؤوف ، التعليم الإلكتروني (اتجاهات عالمية معاصرة) ، ط١، المجموعة العربية للتدريب والنشر ، القاهرة ، مصر ، ٢٠١٤.

٣٣- عبد الفتاح بيومي حجازي ، النظام القانوني لحماية التجارة الإلكترونية ، ط١، دار الفكر الجامعي ، الاسكندرية ، ٢٠٠٢.

٣٤- عبد الفتاح بيومي حجازي ، النظام القانوني للحكومة الإلكترونية ، ك٢، دار الكتب القانونية ، ٢٠٠٧.

٣٥- عبد الفتاح بيومي حجازي ، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي ، ط١، دار النهضة العربية ، القاهرة ، ٢٠٠٩ .

٣٦- عبد الفتاح بيومي حجازي ،التزوير في جرائم الكمبيوتر والانترنت دراسة مقارنة ، ط١، منشأة المعارف، ٢٠١٠.

٣٧- عبدالفتاح بيومي حجازي ، جرائم الكمبيوتر والانترنت في التشريعات العربية (دراسة مقارنة مع التطبيق على نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية ، ط١، دار النهضة العربية ، القاهرة ، ٢٠٠٩.

٣٨- عبدالفتاح بيومي حجازي ، جرائم الكمبيوتر والانترنت في القانون العربي النموذجي (دراسة قانونية متعمقة في القانون المعلوماتي) ، ط١، دار الكتب القانونية ، مصر ، ٢٠٠٧.

٣٩- عبد الحكم فوده ،أحكام رابطة السببية في الجرائم العمدية وغير العمدية ، دار الفكر الجامعي ، الاسكندرية ، ١٩٧٧.

٤٠- عبد الفتاح سليمان ، الاحتيال في العمل المصرفي في الدول العربية وطرق مكافحتها ، ٢٠١٢.

٤١- عبدالله عبد الكريم عبدالله ، جرائم المعلوماتية والانترنت (الجرائم الإلكترونية) ، ط١، منشورات الحلبي الحقوقية ، بيروت ، ٢٠٠٧.

٤٢- علي عبد القادر القهوجي ، جرائم الاعتداء على الانسان والمال ، قانون العقوبات القسم الخاص ، ط١، منشورات الحلبي الحقوقية ، بيروت ، ٢٠١٠.

٤٣- علي عبود جعفر ، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الاشخاص والحكومة (دراسة مقارنة) ، ط١، مكتبة زين الحقوقية والادبية ، ٢٠١٣.

٤٤- عمار عباس الحسيني ، جريمة الإتلاف المعلوماتي (دراسة قانونية مقارنة) ، ط١، منشورات زين الحقوقية ، بيروت ،٢٠١٩.

٤٥- عمر أبو الفتوح عبد العظيم الحمامي ، الحماية الجنائية للمعلومات المسجلة إلكترونياً (دراسة مقارنة) ، دار النهضة العربية ، ٢٠١٠.

٤٦- عمر بن يونس ، الجرائم الناشئة عن استخدام الانترنت ، ط١، دار النهضة العربية ، القاهرة ، ٢٠٠٤.

٤٧- عمر فاروق الحسيني ، تعذيب المتهم لحمله على الاعتراف الجريمة والمسؤولية ، المطبعة العربية الحديثة ، ١٩٨٦.

٤٨- الغريب زاهر إسماعيل ، التعليم الإلكتروني من التطبيق إلى الاحتراف والجودة ، ط١، عالم الكتب ، القاهرة ، ٢٠٠٩.

٤٩- الغريب زاهر اسماعيل ، تكنولوجيا المعلومات وتحديث التعليم ، ط١، عالم الكتب ، مصر ، ٢٠٠١.

٥٠- غنام محمد غنام ، شرح قانون العقوبات (القسم الخاص) ، منشورات جامعة المنصورة ، مصر ، ٢٠٠٤.

٥١- فتحي محمد أنور عزت ، الحماية الموضوعية والجزائية والحق في الخصوصية والكومبيوتر والانترنت في نطاق التشريعات الوطنية والتعاون الدولي ، دار النهضة العربية ، مصر ، ٢٠٠٧.

٥٢- فتوح الشاذلي ، عفيفي كامل عفيفي ، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون (دراسة مقارنة) ، توزيع منشأة المعارف بالاسكندرية ، ٢٠٠٣.

٥٣- فخري عبد الرزاق الحديثي ، شرح قانون العقوبات القسم العام ، ط٢، العاتك لصناعة الكتب ، بغداد ، ٢٠١٠.

٥٤- كمال عبدالحميد زيتون ، تكنولوجيا التعلم في عصر المعلومات والاتصالات ، ط٢، عالم الكتب ، ٢٠٠٤.

٥٥- محمد امين الشوابكة ، جرائم الحاسب والانترنت ، ط١، دار الثقافة للنشر والتوزيع ، عمان ، ٢٠٠٤.

٥٦- محمد حماد مرهج الهيتي ، التكنولوجيا الحديثة والقانون الجنائي ، ط١، دار الثقافة ، الاردن ، ٢٠٠٤.

٥٧- محمد حماد مرهج الهيتي ، الحماية الجنائية لبطاقات الائتمان الممغنطة ، دار الكتب القانونية ، مصر ، ٢٠٠٩.

٥٨- محمد رفعت حسنين ، التعليم الإلكتروني ، ط١، دار الزهور المعرفة والبركة ، مصر ، ٢٠١٧.

٥٩- محمد سامي الشوا ، ثورة المعلومات وانعكاساتها على قانون العقوبات ، ط١، دار النهضة العربية ، القاهرة ، ١٩٩٨.

٦٠- محمد شناوي ، جرائم النصب المستحدثة ، ط١، دار الكتب القانونية ، القاهرة ، ٢٠٠٨.

٦١- محمد طارق عبد الرؤوف الخن ، جريمة الاحتيال عبر إلانترنت (الاحكام الموضوعية والاحكام الاجرائية) ، ط١، منشورات الحلبي الحقوقية ، بيروت ، ٢٠١١.

٦٢- محمد عبدالله أبو بكر سلامة ، جرائم الكمبيوتر والانترنت ، منشأة المعارف بالاسكندرية ، ٢٠٠٦.

٦٣- محمد عبيد الكعبي ، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت ، ط٢، دار النهضة العربية ، القاهرة ، ٢٠٠٩.

٦٤- محمد عبيد الكعبي ، الحماية الجنائية للتجارة الإلكترونية ، دار النهضة العربية ، ٢٠١٠.

٦٥- محمد علي حسن الطوالبة ، التفتيش الجنائي على نظم الحاسوب والانترنت ، ط١، عالم الكتب الحديثة ، ٢٠٠٤ .

٦٦- محمد علي سويلم ، مكافحة الجرائم الإلكترونية (دراسة مقارنة بالتشريعات العربية والاجنبية) ، ط١، دار المطبوعات الجامعية ، دون مكان نشر، ٢٠١٩.

٦٧- محمد علي سويلم ، جرائم الكمبيوتر والانترنت (دراسة مقارنة) ، ط١ ، دار المطبوعات الجامعية ، ٢٠١٩ .

٦٨- محمد كمال محمود الدسوقي ، الحماية الجنائية لسرية المعلومات الإلكترونية (دراسة مقارنة) ، ط١، دار الفكر والقانون للنشر والتوزيع ، مصر ، ٢٠٢١.

٦٩- محمود احمد محمد القرعان ، الجرائم الإلكترونية ، ط١، دار وائل للنشر والتوزيع ، الاردن ، ٢٠١٧.

٧٠- محمود رجب فتح الله ، الوسيط في الجرائم المعلوماتية ، بدون طبعة ، دار الجامعة الجديدة ، الاسكندرية ، ٢٠١٩.

٧١- محمود محمد محمود جابر ، الجرائم الناشئة عن إستخدام الهواتف النقالة (جرائم نظم الإتصالات والمعلومات) ، ط١، المكتب الجامعي الحديث ، ٢٠١٨.

٧٢- مدحت عبدالحليم رمضان ، جرائم الاعتداء على الأشخاص والانترنت ، بدون طبعة ، دار النهضة العربية ، القاهر ة ، ٢٠٠٠.

٧٣- منال عبد العال مبارز ، د. أحمد محمود فخري ، التعليم الإلكتروني (مفهومه – بيئاته – مقرراته – إدارته – تقويمه – تطبيقاته المتقدمة) ، ط١ ، دار الزهراء للنشر والتوزيع ، الرياض ، السعودية ، ٢٠١٣.

٧٤- مصطفى إبراهيم الزلمي ، أساليب إجرامية بالتقنية الرقمية ، ط١، دار الكتب القانونية ، مصر ، ٢٠٠٥.

٧٥- معن أحمد محمد الحياري ، الركن المادي للجريمة ، ط١ ، منشورات الحلبي الحقوقية ، بيروت ، ٢٠١٠.

٧٦- سمير الشناوي ، الشروع في الجريمة (دراسة مقارنة) ، ط١، دار النهضة العربية ، القاهرة ، ١٩٧١.

٧٧- نائلة عادل محمد فريد قورة ، جرائم الحاسب الآلي الاقتصادية ، ط١ ، منشورات الحلبي الحقوقية ، بيروت ، ٢٠٠٥.

٧٨- نهلا عبدالقادر المومني ، الجرائم المعلوماتية ، ط٢، دار الثقافة للنشر والتوزيع ، عمان ، ٢٠١٠.

٧٩- نهله أبو رشيد ، الصحافة الإلكترونية والنشر الإلكتروني ، الجامعة الافتراضية السورية ، سوريا ، ٢٠٢٠.

٨٠- هدى قشقوش ، جرائم الحاسب الآلي في التشريع المقارن ، ط١، دار النهضة العربية ، القاهرة ، ١٩٩٢.

٨١- هلالي عبد اللاه أحمد ، إتفاقية بودابست لمكافحة جرائم المعلوماتية ، ط١، دار النهضة العربية ، القاهرة ، ٢٠٠٧.

٨٢- هلالي عبد اللاه أحمد ، جرائم الحاسب والانترنت بين التجريم الجنائي واليات المواجهة ، دار النهضة العربية ، ٢٠١٦.

٨٣- واثبة داوود السعدي ، قانون العقوبات (القسم الخاص) ، شركة العاتك لصناعة الكتاب ، القاهرة ، بدون سنة طباعة.

٨٤- وليد سالم محمد الحلفاوي ، التعليم الإلكتروني تطبيقات مستحدثة ، ط١، دار الفكر العربي ، القاهرة ، ٢٠١١.

ثالثاً: الرسائل والاطاريح:

١- بثينة سيواني ، واقع استخدام الاستاذ لتقنيات التعليم الإلكتروني في تدريس الطلبة بالجامعة ، رسالة ماجستير ، كلية العلوم الاجتماعية والانسانية ، جامعة العربي بن مهيدي – ام البواقي ، ٢٠١٨.

٢- حليمة الزاجي ، التعليم الإلكتروني بالجامعة الجزائرية مقومات التجسيد وعوائق التطبيق (دراسة ميدانية بجامعة سكيكدة) ، رسالة ماجستير مقدمة لمجلس كلية العلوم الإنسانية والعلوم الاجتماعية ، جامعة منتوري – قسنطينة ، الجزائر ، ٢٠١٢.

٣- داليه خليل عبدالكريم الشواربة ، درجة استخدام طلبة الدراسات العليا في الجامعات الأردنية الخاصة للمنصات التعليمية الإلكترونية واتجاهاتهم نحوها ، رسالة ماجستير مقدمة لمجلس كلية العلوم التربوية ،جامعة الشرق الأوسط ، الاردن ، ٢٠١٩.

٤- سعيد نعيم عبد الغفور ، أثر استخدام بعض الوسائل التعليمية المقترحة عبر الشبكة العالمية على التحصيل لدى طلاب الصف التاسع ، رسالة ماجستير ، كلية التربية ، جامعة الازهر ، ٢٠١٥.

٥- ضيف الله نسيمة ، استخدام تكنولوجيا المعلومات والاتصال وأثره على تحسين جودة العملية التعليمية ، اطروحة دكتوراه ، كلية العلوم والاقتصادية والتجارية وعلوم التسيير ، جامعة الحاج لخضر – باتنه ، ٢٠١٧.

٦- طارق حسين فرحان العواودة ، صعوبات توظيف التعليم الإلكتروني في الجامعات الفلسطينية بغزة كما يراها الأساتذة والطلبة ، رسالة ماجستير ، كلية التربية ، جامعة الازهر غزة ، ٢٠١٢.

٧- فاطمة دحماني ، استخدامات الطلبة الجامعيين للمنصات التعليمية الإلكترونية موودل Moodle - والاشباعات المتحققة منها ، رسالة ماجستير ، كلية العلوم الانسانية والاجتماعية ، جامعة محمد بوضياف ، المسيلة ،٢٠٢٠.

٨- مهيمن مهدي عيسى ، جريمة الاعتداء على وسائل الاتصال السلكية واللاسلكية (دراسة مقارنة) ، رسالة ماجستير مقدمة إلى مجلس كلية القانون والعلوم السياسية ، الجامعة العراقية ، ٢٠١٩.

رابعاً: البحوث:

١- أبو عبيدة محمد حمودة ، إيناس جاسم هادي ، أثر استخدام منصة التعليم الإلكتروني (Moodle) على مستوى طلاب قسم المعلومات والمكتبات (دراسة تجريبية)، بحث منشور في مجلة آدب المستنصرية ، الجامعة المستنصرية ، العدد٨٧، ٢٠١٩.

٢- أحمد محمد محمد السيد الحفناوي ، معايير سهولة الوصول للمنصات التعليمية مفتوحة المصدر Moocs لذوي الإعاقة بالتعليم الجامعي ، بحث منشور في المجلة العربية للتربية النوعية ، كلية التربية ، جامعة الملك سعود ، العدد ١ ، ٢٠١٧.

٣- باسم بن نايف محمد الشريف ، واقع اتجاهات طلبة الجامعات نحو توظيف المنصات الرقمية في التعلم الجامعي بالمملكة العربية السعودية ، بحث منشور في مجلة جامعة طيبة للآداب والعلوم الانسانية ، العدد٢٢، ٢٠٢٠.

٤- بشائر مولود توفيق ، التعليم الإلكتروني (فوائده ونظم إدارته) بحث منشور في مجلة البحوث التربوية والنفسية ، جامعة بغداد ، المجلد١٦، العدد٦٣، ٢٠١٩.

٥- بلقيس بنت إسماعيل داغستاني ، هيفاء جار الله معيص المالكي ، دور المنصات التعليمية الإلكترونية في النمو المهني لمعلمات الطفولة المبكرة (دراسة تقويمية) ، بحث منشور في المجلة التربوية ، كلية التربية ، جامعة الملك سعود ، العدد ٧٣، ٢٠٢٠.

٦- رحاب فايز أحمد ، أحمد فايز أحمد ، الجيل الثاني من الويب وأدواته دراسة مقارنة ، بحث منشور في المجلة العلمية ، كلية الأداب ، جامعة بني سويف ، المجلد ٢ ، العدد١٤، ٢٠٠٩.

٧- سهام بنت سلمان محمد الجريوي ، واقع استخدام الصورة الرمزية (Avatars) في تصميم مقررات المنصات التعليمية الإلكترونية المفتوحة هائلة الالتحاق (MOOCs) ، بحث منشور في مجلة كلية التربية ، جامعة عين شمس ، ج٣، العدد٤١، ٢٠١٧.

٨- عبدالله بن فالح بن راشد السكران ، عبدالله بن أحمد بن عبدالله الراشدي ، المتطلبات التربوية لتوظيف المنصات التعليمية الإلكترونية في العملية التعليمية ، بحث منشور في مجلة البحث العلمي في التربية ، العدد١٩، ٢٠١٨.

٩- محمد محمد عبدالهادي بدوي ، فعالية برنامج مقترح في التعليم الإلكتروني لتنمية مهارات تصميم الإختبارات الإلكترونية والاتجاه نحو التقويم الإلكتروني لدى طلاب الدراسات العليا

بحث منشور في المجلة الدولية التربوية المتخصصة ، كلية التربية بالدقهلية ، جامعة الازهر، العدد٥ ، المجلد٣، ٢٠١٤.

١٠- مناهل مصطفى العمري ، د. افتخار محمد مناحي الرفيعي ، د. انتصار محي الخطيب ، واقع ومتطلبات وسائل التعليم الحديثة ، بحث منشور في مجلة دنانير ، العدد٩، ٢٠١٦.

١١- منتهى عبد الكريم جاسم ، الدراسات العليا عن بعد رؤيا مستقبلية للتعليم الافتراضي في جامعة بغداد ، سلسلة ثقافية جامعية ، المجلد ٢، العدد١، ٢٠١٠.

١٢- نجلاء محمد فارس ، د. محمود محمد حسين ، د. علي حسن عبادي ، فاعلية منصة تعليمية قائمة على القصص التشاركية الرقمية لتنمية التنظيم التعاوني والانتماء إلى الوطن ، بحث منشور في المجلة التربوية ، كلية التربية ، جامعة سوهاج ، العدد٦٨، ٢٠١٩.

١٣- نسرين بسام فريد فرحات ، المنصات الاجتماعية مفتوحة المصدر ، بحث منشور في مجلة دراسات العلوم التربوية ، الجامعة الاردنية ، المجلد ٤٧، العدد٤، ٢٠٢٠.

١٤- ياسر محمد خيابا، دور المنصات الرقمية في دعم وتطوير تعليم العلوم لطلاب المرحلة المتوسطة ، بحث منشور في المجلة العربية للتربية النوعية ، العدد ٧، ٢٠١٩.

خامساً: المقالات:

١- أسامة دمراني ، الدليل الشامل لأشهر أنظمة إنشاء إدارة المتاجر الإلكترونية ، مقال منشور على الموقع https://academy.hsoub.com/entrepreneurship/ecommerce/ أخر زيارة للموقع(٢٠٢١/٧/١٥).

٢- حسام برهان ، مقدمة إلى نظام ماجنتو ومفهوم التجارة الإلكترونية ، مقال منشور على الموقع الإلكتروني https://academy.hsoub.com/apps/web/magento/ أخر زيارة للموقع (٢٠٢١/٧/١٥).

٣- حيدر محمد ، المنصة الإلكترونية ،مقال منشور على الموقع الإلكتروني ، https ://www .zyadda.com/what-is-an-online-platform/ أخر زيارة للموقع (٢٠٢١/٧/١٤).

٤- سعدية الاحمري ، التعليم الالكتروني ، ٢٠١٥، ص٣٨، رسالة ماجستير منشور على الموقع الإلكتروني: https// www.kutubpdfbook.com أخر زيارة للموقع (٢٠٢١/٥/٣).

٥- عبدالله نجاوي ، مقال منشور على الموقع الإلكتروني، https://howarabic .com /2018 /02/install-opencart/ أخر زيارة للموقع (٢٠٢١/٧/١٤).
٦- مجدي كميل ، أفضل منصات التجارة الإلكترونية لبناء متجر إلكتروني ، مقال منشور على الموقع الإلكتروني https://www.alrab7on.com/best-ecommerce-platforms أخر زيارة للموقع (٢٠٢١/٧/١٢).
٧- محمد أحمد المعداوي ، حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي (دراسة مقارنة)، بحث منشور في مجلة كلية الحقوق ، جامعة بنها ، ج ٤، العدد٣٣.
٨- محمد المختار ، شرح إضافة ووكومرس ، مقال منشور على الموقع الإلكتروني ، https:// propassiveincome.com/woocommerce-begginer-guide/ أخر زيارة للموقع (٢٠٢١/٧/١٤).
٩- هارون بو كرش ، رحلة إلى أعلى هرم أنظمة التجارة الإلكترونية ، مقال منشور على الموقع الإلكتروني https://academy.hsoub.com/apps/web/magento/ أخر زيارة للموقع (٢٠٢١/٧/١٥).

سادساً: القوانين الاجنبية:

١- قانون الاحتيال وإساءة الاستخدام الحاسوبي لعام ١٩٨٤.
٢- قانون العقوبات الفرنسي رقم ١٩ لسنة ١٩٨٨.
٣- قانون العقوبات الفرنسي الجديد رقم (١٣٣٦) لسنة ١٩٩٤.
٤- قانون المعاملات الموحد الامريكي لسنة ١٩٩٩.

سابعاً: القوانين العربية:

١- قانون العقوبات الاردني رقم ١٦ لسنة ١٩٦٠.
٢- قانون العقوبات العراقي النافذ رقم ١١١لسنة ١٩٦٩.
٣- قانون العقوبات الاماراتي رقم ٣لسنة ١٩٨٧المعدل.
٤- قانون المعاملات الإلكترونية الاردني رقم ٨٥ لسنة ٢٠٠١.
٥- قانون مكافحة جرائم تقنية المعلومات الإماراتي رقم ٢ لسنة ٢٠٠٦.
٦- قانون أنظمة المعلومات الاردني المؤقت رقم ٣٠ لسنة ٢٠١٠.
٧- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة ٢٠١٠.

٨- مشروع قانون الجرائم الإلكترونية العراقي لسنة ٢٠١١.
٩- مرسوم بقانون اتحادي رقم (٥) لسنة ٢٠١٢.
١٠- قانون تصديق الاتفاقية العربية لمكافحة جرائم تقنية المعلومات رقم (٣١) لسنة ٢٠١٣ وتم نشرها في جريدة الوقائع العراقية بالعدد (٤٢٩٢) في (٢٠١٣/٩/٣٠).
١١- قانون الجرائم الإلكترونية الأردني رقم ٢٧ لسنة ٢٠١٥.

ثامناً: القرارات القضائية:

١- مجلس القضاء الأعلى ، محكمة التمييز الاتحاديه ، ت/٤٥٢٦ ، العدد ٣٧٥٨/ الهيئة الجزائية / ٢٠١٩.
٢- مجلس القضاء الأعلى ، رئاسة محكمة استئناف كربلاء الاتحادية ، محكمة جنايات كربلاء الهيأة الأولى، العدد: ٩٠٤/ج ه ٢٠٢١/١، في ٢٠٢١/١٢/٢٣.
٣- مجلس القضاء الأعلى ، رئاسة استئناف واسط الاتحادية الهيئة التمييزية ، قرار التمييز ذو العدد (٢١١/ت/جنح/٢٠٢١) ، بتاريخ (٢٠٢١/٢/٢٢).

تاسعاً: المصادر الاجنبية:

(1) A.FARAH: English Language , R.N.KARIM English Language , M.SAID: Arabic Language, S.K.EDUARD: Revision, The dictionary, English- Arabic,E1,Dar Al-Kotob Al-ilmiyah, Beirut, Lebanon,2004, 812.

(2) Vergutch (pascal), la repession des delits informatiques dans une perspective intemational, these, universite de mont pellier 1,1996, p.172.

(3) Alain Bensoussan: lntemet, aspects juridiquse, ed. Hermes, 1998, p. 198.

(4) Heyman (Stephen p), legislating computer crime,h.g.1.,vol,1997.

(5) Catala, les transformatique de droit par l'informatiqud emergence du droit de l'informatique et des parques,1983.

(6)Richard Hillman, securities fraud, the internet poses challenges to regulaters and Inverstors, united states General accounting office, 2017.

Summary

The current era has witnessed progress and development in various fields, the most prominent of which was the electronic revolution that led to the emergence of the latest electronic systems, including electronic platforms that were used in many areas that affect the life of the individual and society in general, because of their significant impact on the level of progress and development, general culture and knowledge This is what increases the consolidation of the nature of electronic platforms and makes them keep pace with developments, and electronic platforms are characterized by short time, effort and speed in accomplishing many things, whether in the private or public sector, and despite these advantages of electronic platforms, they are still in their infancy, which makes them face many obstacles and challenges. Especially at the level of the availability of its infrastructure, which makes it exposed to many electronic crimes, including the crime of entering electronic platforms without a license and the crime of destroying information on electronic platforms and the crime of stealing information on electronic platforms and the crime of fraud for electronic platforms, so countries have enacted laws and agreements that would Providing protection for electronic platforms, either by enacting special laws that criminalize the acts Which fall within the cybercrime, such as the United States of America. As for amending its laws, such as France, as for the Arab countries, the United Arab Emirates is one of the first countries to enact a law criminalizing these criminal acts, as well as Jordan. As for Iraq, it did not criminalize acts within cybercrime, neither in its

punitive laws nor In a special law, except for the draft cybercrime law of 2011, which has not yet seen the light, and therefore it has become necessary to vote on the aforementioned law to combat most of the cybercrime that an individual or society may be exposed to, whether in the public or private sector, as well as in order to keep pace with development Happening in modern technology.

Republic of Iraq

Ministry of Higher Education and Scientific Research

University of Karbala - College of Law

Penal protection for electronic platforms

(A Comparative Study)

To the Council of the College of Law – University of Karbala

It is part of the requirements for obtaining a master's degree in public law

A Thesis Submitted by The student

Ali Abdallah Alwan

Supervised by

Dr- Khaled Majid Abdul Hamid AL- Juburi

Associate Professor of Criminal Law

1443 A.H. **2022A.D.**