جريمة الدخول للمنصات الإلكترونية.

The crime of entering electronic platforms.

بحث مشترك مقدم من قبل
الاستاذ المساعد الدكتور خالد مجيد عبد الحميد الجبوري
الباحث علي عبدالله علوان محمد
جامعة كربلاء / كلية القانون

الخلاصة.
شهد العصر الحالي تقدماً وتطوراً في مجالات متعددة ، وكان من أبرزها الثورة المعلوماتية 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 مفهوم المنصات الإلكترونية ويجعلها مواكبة للتطورات الحديثة ، كما تتميز المنصات الإلكترونية باختصار الوقت والجهد والسرعة في إنجاز العديد من الأعمال سواء بالقطاع الخاص أو العام ، وعلى الرغم من هذه المزايا للمنصات الإلكترونية فإنها لا 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 الالكترونية ، لذلك عمدت الدول على إقرار القوانين والاتفاقيات التي من شأنها توفير الحماية للمنصات الإلكترونية ، بتشريع قوانين خاصة تجرّم الأفعال التي تندرج ضمن الجرائم الإلكترونية.
الكلمات المفتاحية : جريمة ، الدخول للمنصات ، الإلكترونية.

Abstract.
The current era has witnessed progress and development in various fields, the most prominent of which was the information 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 concept of electronic platforms and makes them keep pace with modern developments, and electronic platforms are characterized by short time, effort and speed in accomplishing many works, whether in the private or public sectors, 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 availability of their infrastructure, which makes them exposed to many electronic crimes, including the crime of entering electronic platforms, so countries have decided to pass laws and agreements that would Providing protection for electronic platforms, by enacting special laws that criminalize acts that fall under cybercrime.
Key words : The crime ,entering electronic, platforms.

المقدمة.

اولًا/ التعريف بموضوع البحث .

يعد النظام الإلكتروني من الأنظمة الحديثة والمتطورة لتكنولوجيا المعلومات للقيام بالعديد من التعاملات الإلكترونية المختلفة على عدة مستويات تمكن الافراد من الاستفادة منها ، في ظل الانماط الحديثة للتعاملات الإلكترونية وعلى مستوى المنصات الإلكترونية المثبتة على أجهزة الحاسوب أو أي جهاز إلكتروني آخر عبر شبكة الانترنت ،وان أي تطور حديث يصاحبهُ العديد من الانتهاكات والاعتداءات من قبل بعض الاشخاص الذين لديهم الخبرة التقنية في الأنظمة الإلكترونية ،كما وتكمن خطورة هذهِ الاعتداءات في تعرض المعلومات التي يتم تداولها إلكترونياً عن طريق المنصات الإلكترونية التي تتم عبر الدخول غير المشروع ، بحيث تكون سلسلة متكاملة ومتواصلة إلى حد بعيد ومرتبطة بجوانب عديدة للتعاملات الإلكترونية ، وهذه التعاملات تتطلب اسباغ الحماية الجزائية للمنصات الإلكترونية وما تحتويها من معلومات التي يمكن دمجها بسهولة وسرعة غير مسبوقين ونقلها وتداولها في إطار واسع عبر المنصات الإلكترونية ، وقد تشكل تهديداً خطراً لها من تعرضها للاختراق ، لذا وجب توفير حمايه لها من خلال تشريع قوانين عقابية خاصة تجرّم وتعاقب مثل هكذا افعال ترتكب عن طريق التكنولوجيا الحديثة ، بواسطة جهاز الحاسوب أو المنصات الإلكترونية وعبر شبكة الانترنت أو ضدها ، وأن يتصف بالمرونة ، من أجل استيعاب ومواكبة التطورات في مجال تكنولوجيا الحديثة بصفة عامة ، مما يجعل منها تساير جميع المبتكرات والتقنيات الراهنة والمستقبلية التي تستخدم في التعامل مع مختلف المنصات الإلكترونية .

ثانيًا / أهمية البحث .

تتمثل أهمية الدراسة لتعلقها بموضوع هام أوجدته الوسائل التقنية الحديثة التي تؤدي لارتكاب الأفعال الإجرامية من قبل جناة يتمتعون بمهارات وبخبرات تقنية ويمتلكون طرق احترافيه لم تكن معروفه من قبل ، كما يرافق صعوبات كبيره في التعرف على الجناة خصوصاً أن موضوع المنصات الإلكترونية يعاني من قصور التشريعات القائمة في مكافحة الجرائم التي تتعرّض لها، كما هو حال التشريعات العراقية على العكس من بعض تشريعات الدول الأجنبية والعربية التي سارعت لوضع تشريعات تعاقب على الجرائم التي ترتكب بواسطة الوسائل الإلكترونية .

ثالثًا / مشكلة البحث .

يثير موضوع جريمة الدخول للمنصات الإلكترونية العديد من المشاكل من أهمها قصور الحماية التشريعية ومدى قابلية وكفاية النصوص التقليدية في مكافحة الجرائم الإلكترونية التي تتعرض لها المنصات الإلكترونية ، خصوصا وإن جانب من الفقه الجنائي يعتبر تطبيق النصوص التقليدية فيه خرق للنص الدستوري الذي يتعلق بقانونية الجرائم والعقوبات ، كذلك لم يجُرّم الدخول للمنصات الإلكترونية بقانون خاص ، وهذ يعد نقصاً تشريعياً على الرغم من تقديم مشروع قانون جرائم الإلكترونية في العراق لسنة (2011).

رابعًا / منهجية البحث .

فرضت حداثة الدراسة وعدم وجود قواعد محددة وقائمة في بعض تشريعات العديد من الدول منهج الدراسة ، ، فكان البحث ضمن المنهج المقارن بين الولايات المتحدة الإمريكية وفرنسا والأردن والإمارات العربية المتحدة والعراق والاتفاقيات الدولية والمحلية

خامسًا / خطة البحث .

من أجل معالجة الإشكاليات التي تم طرحها ولاستكمال الاجراءات المنهجية المتبعة في هذه الدراسة ، ولان الموضوع يترك آثاره على الحياة الاجتماعية والاقتصادية والأمنية للأفراد ، عليه تناولنا موضوع (جريمة الدخول للمنصات الإلكترونية- دراسة مقارنة) لذا سنقسم هذا البحث على مبحثين نتناول في المبحث الاول التشريعات والاتفاقيات المقارنة وموقفها من جريمة الدخول للمنصات الإلكترونية ونتطرق في المبحث الثاني إلى أركان جريمة الدخول للمنصات الإلكترونية .

جريمة الدخول للمنصات الإلكترونية دراسة مقارنة.

تعد جريمة الدخول من الجرائم المستحدثة والخطرة التي تتعرض لها الاجهزة الإلكترونية ، ومنها الحاسبات الآلية والمنصات الإلكترونية والشبكات المعلوماتية ، 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 ،وذلك بسبب اساءة استخدامها من قبل البعض ، وقيامهم بعمليات الاختراق التي سببت خسائر كبيرة ، مقابل استفادة المخترقين[1] ، الذين يتمتعون بقدرات عالية في مجال تقنية المعلومات ، وسهل لهم ذلك للوصول إلى المعلومات المخزنة إلكترونياً ، والاطلاع عليها والعبث بها وافشائها ، ليس هذا فقط بل أن صعوبة التعرّف عليهم أدت إلى ازدياد اعدادهم ، وبمحو أثار جرائمهم يمكنهم من الافلات من العقاب[2] ، مما دفع أغلب تشريعات الدول الاجنبية والعربية لتوفير الحماية الجنائية لأجهزة الحاسب الآلي ومنصاتها المختلفة ، وشبكاتها المعلوماتية من خلال تشريع نصوص خاصة تجريم الدخول للنظم المعلوماتية المختلفة ، ومنها القانون الفيدرالي للولايات المتحدة الامريكية ، والدول العربية منها (الامارات العربية المتحدة والاردن)[3] ، ، كما وتقوم الجريمة بمجرد ان يتم الدخول إلى المنظومة ، سواء كان الدخول كلي أو جزئي ، ويشترط في أية جريمة يعاقب عليها القانون تحقق ركنيها المادي والمعنوي وجريمة الدخول أو (الاختراق)[4] ، لم نجد اتفاقاً على تسميتها بين التشريعات وانما تتعدد المسميات للجريمة والمضمون واحد[5] ، فقد اطلق عليها قانون العقوبات الفرنسي الجديد تسمية "الدخول إلى النظام الآلي لمعالجة المعطيات عن طريق الغش"[6] ، واطلق عليها في القانون الاتحادي لمكافحة جرائم تقنية المعلومات الاماراتي " التوصيل بغير وجه حق إلى موقع أو نظام معلوماتي" [7] ، وفي قانون الجرائم الإلكترونية الاردني اطلق عليها " الدخول قصداً إلى الشبكة المعلوماتية أو نظام معلومات دون تصريح "[8] ،اما في القانون العربي النموذجي اطلق عليها " التوصيل بطريق التحايل لاختراق نظام المعالجة الآلية للبيانات "[9]، وعليه سنقسم هذا البحث على مبحثين نتناول في المبحث الاول التشريعات والاتفاقيات المقارنة وموقفها من جريمة الدخول للمنصات الإلكترونية ونتطرق في المبحث الثاني إلى أركان جريمة الدخول للمنصات الإلكترونية .

المبحث الاول/ التشريعات والاتفاقيات وموقفها من جريمة الدخول للمنصات الإلكترونية.

تعد جريمة الدخول من الجرائم العمدية الأكثر خطورة في ظل التطورات الإلكترونية الحديثة ، التي يتعرض لها النظام المعلوماتي بصورة عامة ونظام الحاسب الآلي والمنصات الإلكترونية أو أي جهاز إلكتروني آخر بصورة خاصة ، مما أدى بالبعض من تشريعات الدول بسن قوانين خاصة لمعالجة هذه الجرائم ، اما البعض الآخر ضمّن ذلك من خلال تعديل التشريعات العقابية ، وتضمين تلك النصوص العقابية لمعالجة الاعتداءات التي تتعرض لها المنصات الإلكترونية ، ومنها قانون العقوبات الامريكي والفرنسي وغيرها ، وبالنسبة للدول العربية التي تضمنت تشريعات خاصة لتجريم الأفعال التي تندرج ضمن الجرائم الإلكترونية ،وهي كل من الأردن والإمارات ، أما العراق يعاني من فراغ تشريعي خاص بالجرائم الإلكترونية ، وعليه سنقسم هذا المطلب على فرعين نتناول في الفرع الأول موقف بعض التشريعات الأجنبية والعربية من جريمة الدخول للمنصات الإلكترونية ، وفي الفرع الثاني موقف بعض الاتفاقيات الاجنبية العربية من جريمة الدخول للمنصات الإلكترونية.

المطلب الاول/ موقف بعض التشريعات الاجنبية والعربية من جريمة الدخول للمنصات الإلكترونية.

أغلبية التشريعيات الاجنبية والعربية جرَمت هذه الجريمة وذلك من خلال تضمين نصوص عقابية ضمن قانون العقوبات ، أو بسن تشريعات خاصة تجرم الدخول أما بعض الدول تعاني من فراغ تشريعي بخصوص الجرائم المعلوماتية ومنها العراق .

الفرع الاول/ موقف بعض التشريعات الاجنبية لجريمة الدخول للمنصات الإلكترونية.

غالبية التشريعات الأجنبية والعربية جرّمت أفعال هذه الجريمة 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 1984 التي نصت على

الدخول عمداً دون تصريح لحاسب آلي أو لنظام الحاسب الالي أو الدخول عن طريق الشبكة لنظام الحاسب أو المنصة الإلكترونية [10] ، الذي صدر في العام نفسه سمي بقانون الاحتيال واساءة استخدام الحاسوب لسنة 1984[11] ، ومن عمليات الاختراق التي تعرضت لها الولايات المتحدة الأمريكية هي قضية الجحيم العالمي[12]. اما المشرّع الفرنسي فقد جرّم الدخول داخل نظام المعالجة الآلية للمعلومات في معناها الواسع في المادة (1/323) من قانون العقوبات الجديد رقم 1336لسنة 1994، والتجريم يكون على الدخول سواء على النظام بأكمله أو 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 والبيانات ، والنظام الذي يحتوي عليها سواء كان نظام الحاسب الآلي أو المنصات الإلكترونية أو أي جهاز إلكتروني آخر[13] ، بالإضافة إلى شبكات المعلومات ، وان المناقشات السابقة كان لها الدور الكبير في تبني القانون لتعريف نظام المعالجة الآلية للمعلومات ، وهو في الأصل وارد في القانون رقم (17) لسنة 1978، 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 البيانات ، والعمليات التي تتم بواسطة الوسائل الإلكترونية ، من أجل استغلال المعلومات وربطها وتقريبها ودمجها مع البيانات الاخرى والقيام بتحليلها للحصول على معلومات لها دلالة خاصة ، فضلاً عن إلتقاط الاشارات وتبادل المعلومات والبيانات عبر نظام الحاسب الآلي أو المنصات الإلكترونية و شبكة الانترنت فإنها جميعها تُعد دخولاً لنظام المعالجة الالية ، ويمثل هذا الدخول نتيجة للتوسع في مفهوم المعالجة الآلية حسب القانون الفرنسي[14]. نجد المشرّع الفرنسي كان أكثر دقة وحرصاً على تجرّيم الدخول 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 وبالتالي توفير الحماية للمعلومات التي تحتويها المنصات الإلكترونية.

الفرع الثاني/ موقف بعض التشريعات العربية من جريمة الدخول للمنصات الإلكترونية.

اتجهت بعض الدول العربية إلى تجريم الدخول من خلال تشريعات خاصة ، ومن هذه الدول الامارات والاردن ، أما العراق فقد اكتفى بتقديم مشروع قانون جرائم المعلوماتية لسنة 2011 الذي لم ير النور إلى الان. فبالنسبة لدولة الامارات العربية فقد اتخذت تشريعات عديدة تجرّم الدخول للنظام الإلكتروني والحاسب الآلي وحماية المعلومات وذلك ، بمرسوم قانون اتحادي رقم (5) لسنة 2012فقد عرّفت المادة الأولى منه المعلومات الإلكترونية ونظام المعلومات الإلكتروني ووسيلة تقنية المعلومات[15] ، 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"[16] ، 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[17] ، وعاقبت المادة التاسعة من القانون ذاته في حالة قيام الجاني بالتحايل على العنوان البروتوكولي لشبكة المعلومات ، قاصداً ارتكاب الجريمة دون اكتشافه بالسجن المؤقت والغرامة[18]. نجد 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 بيانات ومعلومات 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 دون اكتشافه .

أما المشرع الاردني فقد انتهج منهج المشرع الاماراتي من خلال تشريعه قانون الجرائم الإلكترونية رقم (27) لسنة 2015، فقد عرّف في المادة الثانية كل من نظام المعلومات والبيانات والشبكة المعلوماتي والتصريح والبرامج [19]، وعاقبت الفقرة (أ) من المادة الثالثة الدخول إلى الشبكة والنظام المعلوماتي ، وكان الدخول دون تصريح وعمداً أو مخالف أو متجاوز حدود التصريح ، ففي هذه الحالة تتحقق جريمة الدخول وتكون العقوبة الحبس أو الغرامة[20] 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 [21] ، يلاحظ ان المشرع الأردني عاقب على جريمة الدخول بنص خاص ، في قانون الجرائم الإلكترونية ، من أجل توفير الحماية للمعلومات والبيانات التي يحتويها النظام المعلوماتي أو الشبكة المعلوماتية ، 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 بيانات ومعلومات تصلح لأن تكون محلاً لتحقق جريمة الدخول . اما المشرع العراقي يعاني من فراغ تشريعي من وجود قانون خاص يجرّم الجرائم الإلكترونية ومنها جريمة الدخول ، بالرغم من وجود مشروع قانون جرائم المعلوماتية لسنة 2011، الذي جرّم العديد من الأفعال التي تنطوي على جريمة الدخول 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 بدون تصريح أو اعاق استخدامها من منتفعيها ، يعاقب بالحبس مدة لا تزيد على (3) ثلاثة أشهر أو بغرامة لا تقل عن (2000000) مليوني دينار ولا تزيد على (5000000) خمسة ملايين دينار[22] ، 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"[23] ، اما الفقرة (د) من المادة ذاتها عاقبت بنفس العقوبة كل من " استخدم أو تسبب دون تصريح في استخدام الحاسوب العائد للغير بطريقة مباشرة أو غير مباشرة"[24] ، في حين 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 (15/أ| أولاً)[25] ، و نجد المادة (21/ب| أولاً) حددت عقوبة الحبس على ان لا تزيد على ثلاث سنوات والغرامة التي لا تزيد عن 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 [26]. يتضح لنا مما تقدم ان مشروع قانون الجرائم المعلوماتية العراقي لسنة 2011 قد جرّم العديد من الجرائم الإلكترونية وجعل لها عقوبات متفاوتة كما وشدد في الوقت نفسه على جريمة الدخول في العديد من فقرات مشروع القانون ، الذي تمت قراءته الاولى عام 2011 لذلك أصبح على مشروع القانون والتصويت عليه لكن بعد إجراء بعض التعديلات عليه من قبل المختصين بالقانون الجنائي من أجل سد الفراغ التشريعي الذي يعاني منه القضاء العراقي بخصوص الجرائم الإلكترونية ، من أجل معاقبة جميع المجرمين على الجرائم التي تتم في العالم الافتراضي ، كذلك توفير الحماية الجنائية للمحل الذي تقع عليه الجريمة الإلكترونية من البيانات والمعلومات ، وتوفير حماية جزائية للوسيلة التي يتم بوساطتها الدخول للنظام المعلوماتي أو المنصات الإلكترونية بجميع انواعها .

المطلب الثاني/ موقف بعض الاتفاقيات الدولية من جريمة الدخول للمنصات الإلكتروني

جرّمت بعض الاتفاقيات بنصوص صريحة جريمة الدخول ومن هذه الاتفاقيات اتفاقية بودابست لعام 2001 ، والاتفاقية العربية لعام 2010 ، كذلك موقف القانون العربي الاسترشادي من جريمة الدخول للمنصات الإلكترونية وعليه سنقسم هذا المطلب على فرعين نتناول في الفرع الاول اتفاقية بودابست لمكافحة جرائم المعلوماتية لعام 2001ونتناول في الفرع الثاني الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010.

الفرع الاول/ اتفاقية بودابست لمكافحة جرائم المعلوماتية لعام 2001.

اختلفت العديد من القوانين والاتفاقيات على تسمية جريمة الدخول إلا أن مضمونها واحد ، فنجد المادة الثانية من اتفاقية بودابست لمكافحة جرائم المعلوماتية لعام 2001 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 عبر شبكة الانترنت بحاسب آلي أخر[27] ، كما أشارت المذكرة التفسيرية إلى ان الدخول غير القانوني يضم الاختراق سواء كان لكل أو جزء من النظام 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 بنفس الشبكة ، أو كانت شبكة محلية أو شبكة خاصة أو عن طريق الانترنت[28] .

الفرع الثاني/الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010.

تم عقد هذه الاتفاقية عام 2010 وعدد الدول التي وقعت عليها هي سبع عشرة دولة [29] كما أن العراق كان طرفاً في هذه الاتفاقية من خلال تصديق قانون الاتفاقية العربية لمكافحة جرائم تقنية المعلومات رقم (31) لسنة 2013 [30] ، حيث جرّمت الدخول في الفصل الثاني المتعلق بأحكام التجريم في الفقرة الأولى من المادة السادسة التي جرّمت " الدخول وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به[31] ، 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"[32].

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 ذلك رسمياً بالقانون رقم (31) لسنة 3013، لمكافحة جرائم تقنية المعلومات

نستنتج مما تقدم أن قانون تصديق الاتفاقية العربية لمكافحة جرائم تقنية رقم 31لسنة 2013 أغفلت تحديد العقوبة ومدتها .

المبحث الثاني/ أركان جريمة الدخول للمنصات الإلكترونية.

تعد هذه الجريمة ظاهرة إجرامية جديدة ذات خطورة [33] ، كونها تعبر عن قوة تأثير تكنولوجيا المعلومات الحديثة في مجال عالم الجريمة[34] ، وان سلوكها الاجرامي غير المشروع يختلف عن جميع السلوكيات في الجرائم الاخرى ، التي ترتكب ضد النظام المعلوماتي ، والسبب يعود للخصوصية التي تمتاز بها هذه الجريمة ، كونها ذات طبيعة ثنائية ، وبالرغم من أنها تعد من الجرائم الشكلية التي تتحقق لمجرد حصول السلوك المادي فيها ، دون تحقق النتيجة ، إلا أنها ممكن أن تتحول إلى جريمة ذات نتيجة[35] ، لها أثر خارجي وعليه فإن جريمة الدخول ، لابد من توافر الركن المادي الذي يتمثل في فعل الدخول ، والركن المعنوي يتمثل بالقصد الجنائي متمثل بالنية الداخلية أو الباطنية التي يضمرها الجاني في نفسه ، وعليه سنقسم هذا المبحث على مطلبين نتناول في المطلب الاول الركن المادي في جريمة الدخول للمنصات الإلكترونية وفي المطلب الثاني الركن المعنوي في جريمة الدخول للمنصات الإلكترونية.

المطلب الاول/ الركن المادي في جريمة الدخول للمنصات الإلكترونية.

يتخذ الركن المادي في جريمة الدخول للمنصات الإلكترونية مظهراً خارجياً ، لماديات الجريمة ، ويتكون الركن المادي من ثلاثة عناصر رئيسية وهي السلوك الإجرامي الذي يتمثل بالنشاط الايجابي

والسلبي للفاعل ، والنتيجة الأثر الخارجي المتمثل في الاعتداء على الحق الذي يحميه القانون ، واخرها العلاقة السببية بينهما[36] وعليه سنقسم المطلب على ثلاثة فروع نتناول في الفرع السلوك الإجرامي في جريمة الدخول للمنصات الإلكترونية وفي الفرع الثاني نتناول النتيجة الإجرامي في جريمة الدخول للمنصات الإلكترونية وفي الفرع الثالث نتناول العلاقة السببية في جريمة الدخول للمنصات الإلكترونية.

الفرع الاول/ السلوك الإجرامي في جريمة الدخول للمنصات الإلكترونية.

يعد السلوك الإجرامي من أهم عناصر الركن المادي ، فضلاً عن ذلك فإنه يمثل العنصر الاهم بين جميع العناصر الأخرى في الجرائم المختلفة ، سواء كانت جرائم تقليدية أو جرائم إلكترونية[37] ، ومن الممكن تحقق السلوك الإجرامي دون تحقق النتيجة ،لأن السلوك الإجرامي يتحقق بمجرد الدخول اما ، بسلوك ايجابي يتمثل في ارتكاب الفعل الذي جرمه القانون ، أو سلوك سلبي يتمثل الامتناع عن تنفيذ فعل أمر به القانون [38] ، كما ان السلوك الإجرامي يتطلب وجود البيئة الرقمية أو أي جهاز إلكتروني كألحاسب الآلي أو الهاتف النقال أو غيره من الاجهزة التي ممكن ان تنصب عليها المنصات الإلكترونية ، وربطها بشبكة الانترنت ، ويقوم الفاعل بتحميل الحاسب الالي أو المنصة الإلكترونية ببرامج اختراق ، أو ربما يقوم بتجهيزها واعدادها بنفسه[39] ، كما يقوم ايضاً بأعداد برامج الفيروسات من أجل التحضير لبثها ، وان الاعمال التحضيرية في الجرائم التقليدية لا يعاقب عليها القانون إذا لم يباشر الجاني بتنفيذ جريمته ، لكن الامر مختلف في مجال الجرائم الإلكترونية ، فان القانون يعاقب على مجرد قيام الجاني بشراء برامج إختراق ، أو معدات لفك الشفرات أو كلمات المرور وغيرها مما يشكّل جريمة بحد ذاتها ، ويتحقق فعل الدخول للمنصات الإلكترونية والنظام كلياً أو جزئياً ، كالدخول إلى الحاسب الالي والمنصات الإلكترونية [40] ، ويكون الدخول غير مشروع أيضاً في حالة تجاوز الفاعل الحد المسموح له حتى وان كان ذلك الدخول لجزء معين في البرامج ، وفي قضية تجريم الدخول إلى النظام الإلكتروني يرى البعض أنها ليست بالأمر الجديد وإنما تقاس على فعل الاعتداء على حرمة المسكن [41] وفي هذه الحالة تقوم الجريمة ويعاقب فاعلها ، على عكس قيام الجاني الذي يقوم بالدخول إلى برنامج منعزل عن النظام الإلكتروني ويكون محظور عليه الدخول ، أما دخول الشخص وقيامه بقراءة الشاشة مثلاً ففي هذه الحالات لا تقوم جريمة الدخول ، ويجب ان يتخذ الجاني سلوك إيجابي في كسر الحماية الفنية ، الذي يعمل على توفير الحماية ضد أي أتصال غير مصرح به للمعلومات في الانظمة الإلكترونية أو المنصات الإلكترونية[42] ، اما السلوك السلبي يتمثل في الامتناع عن فعل أمر به القانون أو الدخول بطريق الخطأ والبقاء ، ويقصد بالبقاء " التواجد داخل نظام المعالجة الالية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام"[43] ، أو هو " مشاركة ذات سيطرة من المخترق على تفاعل الحاسوب مع حركة الدخول والخروج "[44] ، كما أن بقاء واستمرار الشخص داخل النظام الإلكتروني والمنصات الإلكترونية هو الفيصل في المعاقبة على سلوكه الإجرامي ، وبقاء الشخص بصورة غير مشروعة اما ان يتم دون قصد أو بطريق الخطأ ، ففي هذه الحالة يكون على الشخص بعد ان علم ان دخوله غير مشروع ان يخرج حال علمه بالدخول غير المشروع حتى لا يعرض نفسهُ للعقوبة [45]. نلاحظ مما تقدم أن السلوك الإجرامي في جريمة الدخول للمنصات الإلكترونية يتحقق من خلال امتناع الفاعل عن قطع الاتصال والخروج من نظام الحاسب الالي أو المنصات الإلكترونية أو أي جهاز إلكتروني أخر ، ولا يمكن معاقبة الشخص الذي يقوم بالدخول عن طريق الصدفة أو الخطأ ويبادر بالخروج عند علمه ، لكن في حالة بقاء الشخص حتى وان كان مسموح له الدخول وتجاوز حدود التصريح ، وعلى الرغم من ان عملية دخوله يكون مشروع ففي هذه الحالة تتحقق الجريمة ، لان بقاء الشخص في هذه الحالة بحد ذاته يشكّل جريمة بمجرد البقاء أو يقوم بالتحكم على نظام الحاسب الالي أو المنصات الإلكترونية ، وأن جريمة البقاء من الجرائم التي ليس من السهل تقديم دليل على اثباتها ، كما ان الاختلاف بين الدخول والبقاء يكمن في ان جريمة الدخول من الجرائم التي تمتاز بالسلوك الايجابي ، فضلاً عن انها جرائم وقتية ، وجريمة البقاء من الجرائم التي تمتاز بالسلوك السلبي ، فضلاً عن أنها جريمة مستمرة لأن الاعتداء فيها على مصلحة يحميها القانون يجعلها مستمرة .

الفرع الثاني/ النتيجة الإجرامية في جريمة الدخول للمنصات الإلكترونية.

تعد النتيجة الإجرامية ، العنصر الثاني من عناصر الركن المادي الذي يتخذ المظهر الخارجي لسلوك الجاني في الجريمة، التي تقوم على أحداث تغييراً حسياً ملموساً في العالم الخارجي للجريمة، وأن أغلب الجرائم يلزم لتوافرها تحقيق النتيجة الإجرامية ، وأن النتيجة الإجرامية في جرائم الانترنت بصورة عامة والمنصات الإلكترونية بصورة خاصة تتحقق بالوصول إلى المعلومات سواء تم تحقيقها عن طريق الحاسب الآلي أو المنصات الإلكترونية المثبتة عليها أو أي جهاز إلكتروني أخر ، ومسألة تحقق النتيجة الإجرامية مسألة جدل بين أنصار المذهب المادي وأنصار المذهب القانوني ، حول تحديد جريمة الدخول هل تعد جريمة مادية متخذه مظهراً خارجياً أم جريمة شكلية ، تتحقق بمجرد الدخول دون الوصول للنتيجة[46]. لتوضيح الجدل الحاصل بين المذهبين نبّين المدلول المادي للنتيجة الاجرامية ، بوصفها ظاهرة مادية أم ظاهرة قانونية . النتيجة الإجرامية تمثل الاثر الخارجي في الاعتداء على حق يحميه القانون الذي يتضمنه النص التشريعي ، كما وتعد النتيجة في المدلول القانوني عنصر من عناصر الركن المادي للجريمة ؛ وأن المشرع يُجّرم الاعتداء على الحق أو المصلحة الجديرة بالحماية ، اما بدون 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 ، كالجرائم السلبية التي تقع بمجرد الامتناع دون أن يكون لهذا الامتناع أثر خارجي ، كامتناع الأم عن إرضاع صغيرها[47]. هذا فيما يتعلق بالمظهر المادي والقانوني فضلاً عن ان بعض التشريعات اكتفت بمجرد الدخول إلى النظام الإلكتروني ، ولم تشترط أن يكون مشفراً بكلمة مرور من أجل حمايته من قبل الآخرين إذ أن بعض الاشخاص تبقى منصاتهم الإلكترونية مفتوحة طوال الوقت ومن ثم أي محاولة دخول لمنصاتهم واستخدامها والاطلاع على معلوماتهم تعد جريمة [48] ، وهذا ما ذهب إليه القانون الفرنسي رقم 1336لسنة 1992النافذ عام 1994في المادة (1/323)[49] ، وقانون مكافحة جرائم تقنية المعلومات الإماراتي رقم 2لسنة 2006في المادة (1/2) [50] ، وتمكن الجاني من الدخول عن طريق اختراق برامج الحماية للحاسب الالي ، والحصول على الشفرة الخاصة بالحاسب الآلي أو المنصات الإلكترونية المثبته عليها مما سمح لنفسه بالبقاء داخلها والتجوال بكل حرية ، بغض النظر عن وصوله للمنصات محل الحماية من عدمها ، لان علة التجريم هي حماية المنصات الإلكترونية وما تحويها من معلومات بغية عدم الوصول اليها والمساس بسلامتها ، والجريمة تمثل عدواناً محتملاً على الحق المحمي[51] ، وبعض التشريعات تتطلب لتحقق النتيجة الإجرامية الحصول على المعلومات كشرط لقيام الجريمة وليس مجرد الدخول ، ومنها الولايات المتحدة الإمريكية إذ تعاقب على الدخول غير المصرح به والحصول على المعلومات في المادة (1030/أ | 1) والمادة (1030/أ|2) من القانون الفيدرالي لجرائم الحاسب الآلي لسنة 1984 المعدل، اما المادة (1030/أ| 3) فقد عاقبت على مجرد الدخول إلى الحاسبات الآلية داخل الحكومة الفيدرالية ، لكنها اشترطت في الدخول أن يؤثر على مصالح الحكومة وان تكون الحاسبات ترتبط بها بأي شكل من الاشكال [52] . نجد مما تقدم 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 مثل الولايات المتحدة الامريكية.

الفرع الثالث / العلاقة السببية لجريمة الدخول للمنصات الإلكترونية.

العلاقة السببية هي العنصر الثالث من عناصر الركن المادي ، التي يتم من 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 الجنائية للجاني ، الذي تحققت النتيجة الاجرامية نتيجة لسلوكه الاجرامي ، وان العلاقة السببية تحقق تلازماً مادياً بين السلوك والنتيجة الإجرامية مما يؤدي إلى توقف مسؤولية الجاني [53] ، ولا يكون مسؤولاً عن النتيجة التي تحققت ، كما ان نفي العلاقة السببية يؤدي إلى انتفاء المسؤولية الجنائية عن الجاني في الجرائم غير العمدية لأنه لا يتصور الشروع في

الجرائم غير العمدية ، على الرغم من أن جريمة الدخول جريمة شكلية تتحقق بمجرد ارتكاب السلوك المادي من دون الحاجة لتحقق النتيجة الإجرامية ، وعليه لا يعد مجرد حصول الشخص على كلمة المرور للغير جريمة ولا يعد ذلك شروعاً في الجريمة [54] . يتضح لنا أن العلاقة السببية في جريمة الدخول للمنصات الإلكترونية من الصعب تحديدها لأن 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 ، جميع ما ذكر 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 على الرغم من أنها جريمة من الجرائم الشكلية.

المطلب الثاني/ الركن المعنوي في جريمة الدخول للمنصات الإلكترونية .

الركن المعنوي يتمثل بالحالة النفسية للجاني ، كذلك وجود علاقة تربط بين ماديات الجريمة وشخصية الجاني[55] ، ولا يكفي لتحقق جريمة الدخول تحقق الركن المادي فحسب بل لابد ان يتحقق الركن المعنوي ، المتمثل بالقصد الجنائي العام بعنصريه العلم والإرادة ، لأنها من الجرائم العمدية ، فضلاً عن أن بعض التشريعات يشترط فيها تحقق القصد الخاص المتمثل بغاية الجاني .

الفرع الاول/ القصد الجنائي العام في جريمة الدخول للمنصات الإلكترونية.

يتمثل القصد الجنائي العام في جريمة الدخول من عنصرين هما العلم والإرادة ، وأن يكون الجاني مدركًا لحقيقة السلوك الإجرامي الذي يقوم به ، وعليه أن يعلم بحقيقة الدخول عمداً إلى الحاسب الآلي أو المنصة الإلكترونية غير مصرح له بالدخول إليها ، أو يكون الدخول بخطأ غير عمدي وبقائه غير مشروع [56] ، ورغم ذلك يصر على البقاء ولم يبادر بالخروج عند علمه بأن بقائهُ غير مشروع ، إذ عليه أن يعلم بخطورة سلوكه الإجرامي على المحل الذي يناله الاعتداء عند ارتكابه الجريمة[57] كذلك على الجاني العلم بالتكييف الذي تتصف به الوقائع التي تكتسب الأهمية في نظر القانون ، ففي حالة انتفاء القصد الجنائي تتجرد الافعال من الاهمية القانونية مما يؤدي ذلك في جعلها غير صالحة لتقوم بها الجريمة[58]. اما في حالة اعتقاد الجاني ان دخوله مشروع وبقائه داخل النظام أو المنصة الإلكترونية مسموح به ، وتم ذلك بطريق الخطأ أو الصدفة أو السهو ، أو كان لا يعلم انه محظور عليه الدخول والبقاء ، وبادر فوراً بالخروج ففي هذه الحالة ينتفي القصد الجنائي ، أما اذا لم يخرج رغم علمه بأنه محظور عليه الدخول ففي هذه الحالة تحقق القصد الجنائي العام في حقه[59] . يتبين مما سبق ان الجاني عليه ان يعلم بأنه غير مسموح له بالدخول أو البقاء في نظام الحاسب الالي أو المنصات الإلكترونية أو أي جهاز إلكتروني أخر ، كما يجب ان تتوافر الإرادة لدى الجاني وتتجه إلى ارتكاب الفعل الاجرامي ، وأن علم وإرادة الجاني تكون كافية لتحقيق السلوك الاجرامي من خلال الدخول ، 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 يؤدي لقيام الجريمة ، ولا عبرة للباعث في ارتكاب الجريمة لأن الباعث في هذه الحالة لا يكون سوى محاوله للتفوق على الوسائل التقنية وقهر النظام [60] . يتضح لنا مما تقدم ان القصد الجنائي العام يتحقق بتوافر عناصره العلم والارادة أي ان الجاني يعلم ان دخوله غير مشروع وبقائه داخل النظام غير مصرح به ورغم ذلك يصر على البقاء وعدم الخروج من المنصة الإلكترونية ، مما يؤدي إلى تحقق النتيجة وهي الاعتداء على البيانات والمعلومات ، وبالتالي تتم معاقبة الجاني ، في حين اذا كان الدخول بطريق الخطأ أو السهو أو الصدفة ويبادر الجاني بالخروج عند علمه ففي هذه ينتفي القصد الجنائي ولا تتم مساءلة الجاني .

الفرع الثاني/ القصد الجنائي الخاص في جريمة الدخول للمنصات الإلكترونية.

بعض الدول لا تتطلب القصد الجنائي الخاص واكتفت بالقصد الجنائي العام ومنها فرنسا والامارات والجزائر ، 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 وان السبب في توافر

القصد الجنائي الخاص لتشديد العقوبة ، ونجد المشرع الاسترالي نص على تشديد العقوبة عندما يرتكب الجاني فعل الدخول بقصد الاضرار بالغير[61] ، 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 المعلوماتية البرتغالي لسنة 1991 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[62]. يتضح لنا مما تقدم ان التشريعات التي تتطلب قصد جنائي خاص بجانب القصد الجنائي العام ما هو إلا لتشديد العقوبة والباحث يجد ان توافر القصد الجنائي العام بعنصرية العلم والإرادة يكفي لتحقق الجريمة ، أضف إلى ذلك ان جريمة الدخول هي جريمة عمدية ، وشكلية في نفس الوقت أي تتحقق بمجرد الدخول دون تحقق النتيجة في بعض التشريعات ، فضلا عن أن من يقوم بهذه الجريمة من الجناة الذين يتمتعون بمهارات عالية في المجال التقني ، أي ان نشاط الجاني فيها هو نشاط تقني وفني و يحتاج إلى تدريب وممارسة من قبل المخترق ،والجاني في هذه الحالة عليه ان يكون عالم بخطورة فعله ويجرّمه القانون ، وبالرغم من ذلك يصر على ارتكاب الفعل ويقوم بالدخول إلى نظام الحاسب الالي أو المنصة الإلكترونية ، والبقاء بها دون تصريح ، والباحث يتفق مع التشريعات التي تتطلب القصد الجنائي العام بعنصريه العلم والإرادة التي تكفي لتحقق النتيجة الاجرامية.

الخاتمة .

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

اولًا/ الاستنتاجات.

1. اتضح لنا 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 كلي أو بجزء من النظام ، من أجل توفير الحماية للنظام نفسه أو الجرائم التي تقع ضده.
2. نستنتج ان القصد الجنائي العام يتحقق بتوافر عناصره العلم والارادة أي ان الجاني يعلم ان دخوله غير مشروع ورغم ذلك يصر على البقاء وعدم الخروج من المنصات الإلكترونية ، مما يؤدي إلى تحقق النتيجة وهي الاعتداء على المعلومات ، وبالتالي تتم معاقبة الجاني ، أما اذا كان الدخول بطريق الخطأ أو السهو أو الصدفة ويبادر الجاني بالخروج عند علمه ففي هذه ينتفي القصد الجنائي ولا تتم مساءلة الجاني.
3. تبّين لنا ان سلوك الجاني في جرائم المنصات الإلكترونية يختلف بحسب نوع الجريمة فإن السلوك الإجرامي في جريمة الدخول يختلف عن غيره من الجرائم الإلكترونية الأخرى ، كذلك تكييف القانوني لها أيضاً يختلف من جريمة إلى أخرى في إذ نجد النصوص التقليدية عاجزة امام مكافحة الجرائم الإلكترونية
4. تعرّفنا على الدور المهم من قبل الاتحاد الاوربي من خلال الاتفاقية الاوربية المتمثلة باتفاقية بودابست لعام 2001 والتي تعتبر 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 .

ثانيًا / المقترحات .

1- ندعو المشرع العراقي لضرورة وضع نصوص تشريعية تجرَم الأفعال الإجرامية المستحدثة مثل جريمة الدخول للمنصات الإلكترونية.

2- ندعو مجلس النواب العراقي للإسراع في التصويت على مشروع قانون مكافحة الجرائم الإلكترونية العراقي لسنة 2011 ، من أجل توفير الحماية الجزائية للمنصات الإلكترونية التي تحقق جزءاً من الأمن الإلكتروني للفرد والمجتمع على حد سواء .

3- نقترح تعديل المادة السادسة من قانون تصديق الاتفاقية العربية لمكافحة جرائم التقنية رقم 31 لسنة 2013 التي أغفلت تحديد العقوبة ومدتها وأكتفت فقط بذكر جريمة الدخول.

الهوامش.

(1) يُنظر: جلال محمد الزغبي ، اسامة أحمد المناعسة ، جرائم تقنية نظم المعلومات الإلكترونية (دراسة مقارنة) ، ط1، دار الثقافة ، عمان ، 2010، ص21.

(2) يُنظر: محمد كمال محمود الدسوقي ، الحماية الجنائية لسرية المعلومات الإلكترونية (دراسة مقارنة) ، ط1، دار الفكر والقانون للنشر والتوزيع ، مصر ، 2021، ص55.

(3) ينظر . رشيدة بوكر ، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن ، ط1، منشورات الحلبي الحقوقية ، 2012 ، ص152.

(4) يُنظر: نص المادة (السادسة /ثانياً أ ، ب) من قانون تصديق الاتفاقية العربية لمكافحة جرائم تقنية المعلومات رقم (31) لسنة 2013.

(5) يقصد بالاختراق الدخول غير المصرح به أو غير المشروع لنظام المعالجة الالية للبيانات ، وذلك عن طريق انتهاك الإجراءات الأمنية . يُنظر: د. محمود محمد محمود جابر ، مصدر سابق ، ص457.

(6) يُنظر: د. عمار عباس الحسيني ، مصدر سابق ، ص156.

(7) يُنظر: المادة (323) من القانون الفرنسي الجديد رقم (1336) لسنة 1994.

(8) يُنظر: المادة الثانية من قانون مكافحة جرائم تقنية المعلومات رقم 2 لسنة 2006.

(9) يُنظر: المادة الثالثة من قانون الجرائم الإلكترونية رقم 27 لسنة 2015.

(10) يُنظر: د. محمود رجب فتح الله ، الوسيط في الجرائم المعلوماتية ، بدون طبعة ، دار الجامعة الجديدة ، الاسكندرية ، ص335.

(11) الذي تم تعديله لأكثر من مرة في عام 1986 و1994 وتناول القسم 18 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 1996 ، 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 (1030/أ) من القانون الفدرالي لجرائم الحاسب الألي لسنة 1996، 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 ، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الاشخاص والحكومة (دراسة مقارنة) ، ط1، مكتبة زين الحقوقية ، بيروت ، 2013 ، ص140.

(12) يُنظر: د. محمود محمد محمود جابر ، الجرائم الناشئة عن إستخدام الهواتف النقالة (جرائم نظم الإتصالات والمعلومات) ، ط1، المكتب الجامعي الحديث ، 2018 ، ص467.

(13) 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 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 ، ط1، مكتبة الوفاء القانونية ، 2011 ، ص367-368.

(14) يُنظر: رشيدة بوكر ، مصدر سابق ، ص225.

(15) يُنظر: د. محمود محمد محمود جابر ، مصدر سابق ، ص466.

(16) يُنظر: نص المادة(1) من مرسوم بقانون اتحادي رقم (5) لسنة 2012، 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).

(17) يُنظر: نص الفقرة الاولى من المادة (2) من مرسوم بقانون اتحادي رقم (5) لسنة 2012.

(18) 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".

(19) 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".

(20) يُنظر: نص المادة الثانية من قانون الإلكترونية رقم (27) لسنة 2015، 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).

(21) نص الفقرة (أ) من المادة الثالثة من قانون الجرائم الإلكترونية الأردني رقم (27) لسنة 2015 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 (100) مائة دينار ولا تزيد على (200) مائتي دينار أو بكلتا هاتين العقوبتين).

(22) تنص الفقرة (ب) من المادة الثانية من قانون الجرائم الإلكترونية الأردني رقم (27) لسنة 2015 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 (200) مائتي دينار ولا تزيد على (1000) ألف دينار.

(23) يُنظر: الفقرة ب/ثالثاً/ من المادة الرابعة عشر من مشروع قانون جرائم المعلوماتية لسنة 2011.

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

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

(26) تنص الفقرة (أ) من المادة 15على أن: " يعاقب بالحبس وبغرامة لا تقل عن (10000000) عشرة ملايين دينار ولا تزيد على (15000000) خمسة عشر مليون دينار عراقي كل من تجاوز عمداً نطاق التصريح المخول به أو اعترض اية معلومات خلال عمليات تبادلها.

(27) تنص الفقرة ب/أولاً من المادة 21 على أن " يعاقب بالحبس مدة لا تقل عن (2) سنتين ولا تزيد على (3) ثلاث سنوات وبغرامة لا تقل عن (10000000) عشرة ملايين دينار ولا تزيد على (20000000) 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".

(28) يُنظر: د. هلالي عبد اللاه أحمد، إتفاقية بودابست لمكافحة جرائم المعلوماتية ط1 ،دار النهضة العربية،القاهرة ص48.

(29) يُنظر: رشيدة بوكر، مصدر سابق ، ص 225.

(30) نصت المادة السادسة من اتفاقية بودابست على أن : الانتاج أو البيع أو الحيازة أوالاستيراد أو نشر أي أجهزة أو الادوات ، فضلاً عن ذلك كلمات المرور أو شفرات الدخول أو أي بيانات أو معلومات مماثله يستطيع من خلالها الجاني الدخول غير المشروع إلى كل أو جزء من النظام المعلوماتي يُنظر: د. محمود محمد محمود جابر ، مصدر سابق 470.

(31) تم عقد هذه الاتفاقية بتاريخ 2010/12/21 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 لعام2007الذي 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 ، ص202.

(32) قانون تصديق الاتفاقية العربية لمكافحة جرائم تقنية المعلومات رقم (31) لسنة 2013 وتم نشرها في جريدة الوقائع العراقية بالعدد (4292) في (2013/9/30).

(33) يُنظر .د. عمار عباس الحسيني ، جريمة الإتلاف المعلوماتي (دراسة قانونية مقارنة) ، ط1، منشورات زين الحقوقية ، بيروت ،2019 ، ص234.

(34) يُنظر: المادة (1) من القانون العربي النموذجي لسنة 1996.

(35) 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 ، مصدر سابق ، ص 49-50.

(36) يُنظر: د. محمود رجب فتح الله ، الوسيط في الجرائم المعلوماتية ، دار الجامعة الجديدة ، 2019 ،ص332.

(37) يُنظر: رشيدة بوكر ، مصدر سابق ، ص159-160.

(38) يُنظر: د. أسامة فرج الله محمود الصباغ ،الحماية الجنائية للمصنفات الإلكترونية،دار الجامعة الجديدة2016،ص104.

(39) السبب في اختيار مفرد أو مصطلح المعلوماتية بدل من مفردة الإلكترونية هو ان المعلوماتية أكثر اتساقاً مع اللغة العربية ، فضلاً عن أن اغلب التشريعات العربية استخدمتها في معالجة الجرائم المعلوماتية ، ومنها المشرع الاماراتي والسعودي والسوداني وغيرهم ، في حين مفردة الإلكترونية اصلها أجنبية وتم تعريبها ، ينظر: د. عمار عباس الحسيني ، مصدر سابق ، ص9.

(40) يُنظر: نص المادة 28 من قانون العقوبات العراقي رقم 111لسنة 1969المعدل " الركن المادي للجريمة سلوك إجرامي بارتكاب فعل جرمه القانون أو الامتناع عن فعل أمر به القانون"

(41) يُنظر: مهيمن مهدي عيسى ، جريمة الاعتداء على وسائل الاتصال السلكية واللاسلكية (دراسة مقارنة) ، رسالة ماجستير مقدمة إلى مجلس كلية القانون والعلوم السياسية ، الجامعة العراقية ، 2019، ص64.
(42) يُنظر أمير فرج يوسف ، مصدر سابق ، ص123.
(43) يُنظر: د. عبدالفتاح بيومي حجازي ، جرائم الكمبيوتر والانترنت في القانون العربي النموذجي (دراسة قانونية متعمقة في القانون المعلوماتي) ، ط1 ، دار الكتب القانونية ، مصر ، 2007 ، ص28.
(44) vergutch (pascal), la repession des delits informatiques dans une perspective intemational, these, universite de mont pellier 1,1996, p.172.
(45) يُنظر: رشيدة بوكر ، مصدر سابق ، ص213.
(46) يُنظر: د. محمد علي سويلم ،جرائم الكمبيوتر والانترنت (دراسة مقارنة) ط1، دار المطبوعات الجامعية ، 2019، ص233.
(47) يُنظر: نهلا عبد القادر المومني ، الجرائم المعلوماتية ، ط2، دار الثقافة ، عمّان ، 2010، ص162.
(48) يُنظر: د. محمد علي سويلم ، مكافحة الجرائم الإلكترونية (دراسة مقارنة بالتشريعات العربية والاجنبية) ، ط1، دار المطبوعات الجامعية ، دون مكان نشر، 2019،ص104.
(49) يُنظر: د. محمد علي سويلم ،جرائم الكمبيوتر والانترنت (دراسة مقارنة) مصدر سابق ، ص234.
(50) 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 ، ص32.
(51) يُنظر: د. محمود احمد محمد القرعان ، الجرائم الإلكترونية ، ط1، دار وائل للنشر والتوزيع ، الاردن ، 2017، ص34-35.
(52) يُنظر: د. محمد عبيد الكعبي ، الحماية الجنائية للتجارة الإلكترونية ، دار النهضة ، 2010 ، ص443،
(53) Alain Bensoussan: lntemet, aspects juridiquse, ed. Hermes, 1998, p. 198.
(54) تنص المادة 1/323 من قانون العقوبات الفرنسي رقم 1336 لسنة 1994على (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 60 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 100000يورو غرامة ، عندما 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 150 ألف يورو.
(55) تنص المادة 1/2 من قانون مكافحة جرائم تقنية المعلومات الإماراتي رقم 2لسنة 2006 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).
(56) يُنظر: محمد كمال محمود الدسوقي ، مصدر سابق ، ص76.
(57) يُنظر: د. محمد عبيد الكعبي ، الحماية الجنائية للتجارة الإلكترونية ، مصدر سابق ، ص446.
(58) يُنظر: د. أسامة فرج الله محمود الصباغ ، مصدر سابق ، ص200.
(59) يُنظر: د. محمد علي سويلم ، مكافحة الجرائم الإلكترونية ، مصدر سابق ، ص107.
(60) يُنظر: د. خالد ممدوح إبراهيم ، فن التحقيق الجنائي في الجرائم الإلكترونية ، ط1، دار الفكر الجامعي ، الاسكندرية ، 2009، ص53،
(61) يُنظر: د. محمد علي سويلم ، مكافحة الجرائم الإلكترونية ، مصدر سابق ، ص115.
(62) يُنظر: د. محمد علي سويلم ،جرائم الكمبيوتر والانترنت (دراسة مقارنة) مصدر سابق ، ص245.
(63) يُنظر: د. فتحي محمد أنور عزت ، الحماية الموضوعية والجزائية والحق في الخصوصية والكومبيوتر والانترنت في نطاق التشريعات الوطنية والتعاون الدولي ، دار النهضة العربية ، مصر ، 2007، ص131.
(64) 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 ، ص32.
(65) يُنظر: رشيدة بوكر ، مصدر سابق ، ص237
(66) يُنظر: محمد كمال محمود الدسوقي ، مصدر سابق ، ص81.
(67) يُنظر محمد عبيد الكعبي ، الحماية الجنائية للتجارة الإلكترونية ، مصدر سابق ، ص488-489.

المصادر.

اولًا/ الكتب .

1. أسامة فرج الله محمود الصباغ ، الحماية الجنائية للمصنفات الإلكترونية ، دار الجامعة الجديدة ، 2016.
2. أمير فرج يوسف ، الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت ، ط1، مكتبة الوفاء القانونية ، 2011.
3. جلال محمد الزغبي ، اسامة أحمد المناعسة ، جرائم تقنية نظم المعلومات الإلكترونية (دراسة مقارنة) ، ط1، دار الثقافة ، عمان ، 2010.
4. خالد ممدوح إبراهيم ، الحماية القانونية للعلامات التجارية مدنياً وجنائياً ، دار الفكر الجامعي ، 2019.
5. رشيدة بوكر ، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن ، ط1، منشورات الحلبي الحقوقية ، 2012.
6. عمار عباس الحسيني ، جريمة الإتلاف المعلوماتي (دراسة قانونية مقارنة) ، ط1، منشورات زين الحقوقية ، بيروت ،2019.

7. علي عبود جعفر ، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الاشخاص والحكومة (دراسة مقارنة) ، ط1، مكتبة زين الحقوقية ، بيروت ، 2013.
8. عبدالفتاح بيومي حجازي ، جرائم الكمبيوتر والانترنت في القانون العربي النموذجي (دراسة قانونية متعمقة في القانون المعلوماتي) ، ط1، دار الكتب القانونية ، مصر ، 2007.
9. فتحي محمد أنور عزت ، الحماية الموضوعية والجزائية والحق في الخصوصية والكومبيوتر والانترنت في نطاق التشريعات الوطنية والتعاون الدولي ، دار النهضة العربية ، مصر ، 2007.
10. محمد علي سويلم ، مكافحة الجرائم الإلكترونية (دراسة مقارنة بالتشريعات العربية والاجنبية) ، ط1، دار المطبوعات الجامعية ، دون مكان نشر، 2019.
11. محمد كمال محمود الدسوقي ، الحماية الجنائية لسرية المعلومات الإلكترونية (دراسة مقارنة) ، ط1، دار الفكر والقانون للنشر والتوزيع ، مصر ، 2021.
12. محمود احمد محمد القرعان ، الجرائم الإلكترونية ، ط1، دار وائل للنشر والتوزيع ، الاردن ، 2017.
13. محمود رجب فتح الله ، الوسيط في الجرائم المعلوماتية ، بدون طبعة ، دار الجامعة الجديدة ، الاسكندرية ، 2019.
14. محمود محمد محمود جابر ، الجرائم الناشئة عن إستخدام الهواتف النقالة (جرائم نظم الإتصالات والمعلومات) ، ط1، المكتب الجامعي الحديث ، 2018 .
15. محمد عبيد الكعبي ، الحماية الجنائية للتجارة الإلكترونية ، دار النهضة العربية ، 2010 .
16. نهلا عبدالقادر المومني ، الجرائم المعلوماتية ، ط2، دار الثقافة للنشر والتوزيع ، عمان ، 2010.
17. هلالي عبد اللاه أحمد ، إتفاقية بودابست لمكافحة جرائم المعلوماتية ، ط1، دار النهضة العربية ، القاهرة ، 2007.

ثانيًا / الرسائل .

1. مهيمن مهدي عيسى ، جريمة الاعتداء على وسائل الاتصال السلكية واللاسلكية (دراسة مقارنة) ، رسالة ماجستير مقدمة إلى مجلس كلية القانون والعلوم السياسية ، الجامعة العراقية ، 2019.

ثالثًا / القوانين ومشروعات القوانين.

1. قانون العقوبات العراقي رقم 111لسنة 1969المعدل .
2. قانون مكافحة جرائم تقنية المعلومات الإماراتي رقم 2لسنة 2006
3. مشروع قانون الجرائم الإلكترونية العراقي لسنة 2011.
4. قانون تصديق الاتفاقية العربية لمكافحة جرائم تقنية المعلومات رقم (31) لسنة 2013 وتم نشرها في جريدة الوقائع العراقية بالعدد (4292) في (2013/9/30).
5. قانون الجرائم الإلكترونية الأردني رقم 27 لسنة 2015.

رابعاً/ المصادر الاجنبية.

1) Alain Bensoussan: lntemet, aspects juridiquse, ed. Hermes, 1998 .
2) vergutch (pascal), la repession des delits informatiques dans une perspective intemational, these, universite de mont pellier 1,1996.