# الجوانب الموضوعية لجرائم الدخول غير المشروع إلى الأنظمة المعلوماتية

## ( دراسة مقارنة )

إعداد

**د. شريف نصر أحمد**

أستاذ القانون الجنائي المساعد

بقسم القانون - كلية الشريعة والقانون – جامعة الجوف - المملكة العربية السعودية

والمدرس بكلية الحقوق - جامعة جنوب الوادي – مصر

## موجز عن البحث

تناولت الدراسة جرائم الدخول غير المشروع إلى الأنظمة المعلوماتية، وركزت على الجوانب الموضوعية لهذه الجرائم في قوانين مصر، والسعودية، والإمارات، وفرنسا، وذلك من خلال بيان مفهوم الجريمة، ومفهوم النظام المعلوماتي ومفرداته، ومدى تطلب الحماية التقنية له كشرط للتجريم، والإطار التشريعي لهذه الجرائم، كما تناولت الدراسة البنيان القانوني لجرائم الدخول غير المشروع، وذلك بتحليل الأحكام المشتركة بين جرائم الدخول المختلفة، وتحليل الأحكام الخاصة بكل جريمة على حدة.

وقد انتهت الدراسة إلى مجموعة من النتائج، منها أن الحماية التقنية التي وقع بشأنها الخلاف بين الفقهاء كشرط لتجريم الدخول غير المشروع هي الحماية التقنية المتخصصة، وليست الحماية العادية، وقد انقسم الفقه بشأنها إلى اتجاهين، اتجاه يرى أن هذه الحماية شرط لتجريم الدخول غير المشروع، واتجاه آخر وهو الراجح يرى أنها ليست شرطًا للتجريم، كما انتهت إلى أن القانون المصري فرق في التجريم والعقاب

بين الدخول غير المشروع إلى الأنظمة المعلوماتية للدولة، والدخول إلى الأنظمة المعلوماتية الخاصة، ووضع للأولى عقوبات أشد تتناسب مع طبيعة المصالح المحمية، أما القوانين الأخرى محل الدراسة فلم تفرق بين الأنظمة المعلوماتية للدولة، والأنظمة الخاصة، وإن كان المشرع الإماراتي قد شدد عقوبة الدخول غير المشروع بقصد الحصول على بيانات حكومية.

**الكلمات المفتاحية:** الدخول غير المشروع ، اختراق ، أنظمة معلوماتية ، جريمة معلوماتية ، تقنية المعلومات ، الكترونية .

**The Objective Aspects Of Crimes Of Unlawful Entry Into Information Systems ( Comparative Study )**

**Sherif Nasr Ahmed**
**Department of Law, College of Sharia and Law, Al-Jouf University, Saudi Arabia.**
**Email : dr.sherefnasr@gmail.comAbstract**

This study dealt with Crimes of Illegal Access, and focused on the objective aspects of these crimes in the laws of Egypt, Saudi Arabia, the Emirates, and France, by explaining the concept of the crime, concept of the information system and its elements, and the extent to which technical protection is required as a condition for criminalization, and the legislative framework for these crimes.

The study also examined the legal structure of Crimes of Illegal Access, by analyzing the provisions common to the various Crimes of Illegal Access, and analyzing the provisions for each crime separately.

The study ended with a set of results, including that technical protection on which the dispute between the jurists occurred as a condition for criminalizing Crimes of Illegal Access, is limited in technical protection, not ordinary protection, and jurisprudence was divided –in this matter- into two directions, a trend that sees this protection as a condition for criminalizing Illegal Access, while the second trend, which is the most correct view, deciding that it is not a condition for criminalization, as followed in the Egyptian law differs in criminalization and penality, between Illegal Access state's information systems, and Illegal Access private information systems. By imposing severe penalties to match the nature of protected interests, while the other laws in the study did not differentiate between Illegal Access state's information systems and Illegal Access to private information systems, although UAE hardens the penalty of Crimes of Illegal Access committed to obtain the governmental data.

**Key words:** Illegal access, Hacking, information systems, information crime, information technology, electronic.

# المقدمة

رغم الفوائد الجمة التي حققها التطور التقني في مجال الحواسب الآلية، والأنظمة المعلوماتية، والانترنت؛ فقد رافقته انتهاكات عديدة لكثيرٍ من الحقوق، ومساس بكثيرٍ من المصالح ذوات الصلة بهذه المجالات، وهو ما حدا بكثيرٍ من البلدان إلى سن قوانين مكافحة جرائم تقنية المعلومات، ولعل أهم الأفعال المحظورة التي تصدرت كافة هذه القوانين "الدخول غير المشروع" إلى الأنظمة المعلوماتية؛ باعتبار أن الأنظمة المعلوماتية أصبحت مستودعاً للمعلومات، والبيانات، والأسرار التجارية، والشخصية، والقومية، وباعتبار لما قد يترتب علي دخول هذه الأنظمة أو يعقبه من جرائم أخرى، كإتلاف البيانات، أو تدميرها، أو تعطيل النظام، أو الاطلاع على أسرار ما كان المتطفل ليعلم بها لولا دخوله النظام.

## إشكالية الدراسة:

نظراً لحداثة تجريم الدخول غير المشروع إلى الأنظمة المعلوماتية، فإنه يثير العديد من الإشكاليات، لعل أهمها تحديد محل هذا الدخول، ونطاقه، ومدى اعتبار الحماية التقنية شرطاً لتجريم الدخول، وتحديد مفهوم السلوك الإجرامي، وبيان أحكام الركن المعنوي لهذه الجرائم، والجزاءات المقررة لها.

## نطاق الدراسة:

يتحدد نطاق هذه الدراسة بالجوانب الموضوعية لجرائم الدخول غير المشروع في قانون مكافحة جرائم تقنية المعلومات المصري، ونظام مكافحة جرائم المعلوماتية السعودي، وقانون مكافحة جرائم تقنية المعلومات الإماراتي، وقانون(GODFRAIN) الفرنسي.

## أهداف الدراسة:

تهدف الدراسة إلى تحديد مفهوم الدخول غير المشروع إلى الأنظمة المعلوماتية، ومدى جدوى تجريمه، وتحديد مفهوم النظام المعلوماتي، ومفرداته، وبيان مفهوم الحماية التقنية للنظام المعلوماتي، ومدى اشتراطها للتجريم، كما تهدف الدراسة إلى تحديد طبيعة جريمة الدخول غير المشروع، والوقوف على المقصود بعدم مشروعية الدخول، ونطاقه، وتحديد صور السلوك المجرم وتحليلها، فضلاً عن بيان أحكام الركن المعنوي للجريمة، وبيان الجزاءات المقررة لهذه الجرائم لحماية المصالح المقصودة.

## مناهج الدراسة:

قامت الدراسة على عدة مناهج؛ حيث استخدم المنهج الوصفي في وصف جرائم الدخول غير المشروع، وبيان أحكامها المختلفة، واستخدم المنهج الاستقرائي في الوقوف على الأحكام الفرعية، والجزئيات المتعلقة بالدخول غير المشروع، واستخلاص المبادئ العامة التي تحكمها، أما المنهج الاستنباطي فقد تم بمقتضاه البحث في القواعد، والمبادئ القانونية العامة؛ وتطبيقها على الجزئيات والفروع المختلفة في جريمة الدخول غير المشروع، فضلاً عن استخدام المنهج المقارن في المقارنة بين أحكام الدخول المجرم في القوانين محل الدراسة، والمقارنة بين الآراء الفقهية في المسائل محل الاختلاف.

## تقسيم الدراسة:

تنقسم الدراسة إلى ثلاثة مباحث، يتناول المبحث الأول ماهية جريمة الدخول غير المشروع والإطار التشريعي لها، ويتناول المبحث الثاني الأحكام المشتركة بين جرائم الدخول غير المشروع، أما المبحث الثالث فينصب على الأحكام الخاصة بكل جريمة من جرائم الدخول غير المشروع.

# المبحث الأول
# ماهية جريمة الدخول غير المشروع وإطارها التشريعي

ينقسم هذا المبحث إلى مطلبين، يتناول أولهما ماهية جريمة الدخول غير المشروع إلى الأنظمة المعلوماتية، بينما يتناول المطلب الآخر إطارها التشريعي، وذلك على النحو التالي:

## المطلب الأول
## ماهية جريمة الدخول غير المشروع إلى الأنظمة المعلوماتية

يقتضى الوقوف على ماهية هذه الجريمة بيان مفهومها، وبيان علة تجريمها، وأعرض لكل نقطة في فرع مستقل.

### الفرع الأول
### مفهوم جريمة الدخول غير المشروع إلى الأنظمة المعلوماتية

يمثل مجرد الدخول غير المشروع إلى الأنظمة المعلوماتية خطراً على سلامة وسرية البيانات، والنظم المعلوماتية، وقد يتحول هذا الخطر إلى الإضرار بهذه الأنظمة المعلوماتية حال المساس بها، أو بسريتها، ورغم تعدد مسميات هذه الجريمة، إذ يطلق عليها الدخول غير المشروع، والدخول غير القانوني، والدخول غير المصرح به، والدخول غير الشرعي، واختراق الأنظمة المعلوماتية، والدخول الاحتيالي، والدخول بالغش؛ بيد أن هذه المسميات تتوافق في مضمونها ودلالتها، إذ تنصرف إلى الولوج إلى نظام معلوماتي دون وجه حق.

وقد عرفت بعض قوانين مكافحة جرائم تقنية المعلومات هذه الجريمة، ومنها قانون

مكافحة جرائم تقنية المعلومات المصري[١]، حيث عرف الاختراق في المادة الأولى بأنه: " الدخول غير المرخص به أو المخالف لأحكام الترخيص، أو الدخول بأي طريقة غير مشروعة إلى نظام معلوماتي أو حاسب آلي أو شبكة معلوماتية وما في حكمها"؛ أما نظام مكافحة جرائم المعلوماتية السعودي[٢] فقد عرف جريمة الدخول غير المشروع في مادته الأولى بأنها:" دخول شخص بطريقة متعمدة إلى حاسب آلي، أو موقع إلكتروني، أو نظام معلوماتي، أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها".

وعرف قانون مكافحة جرائم تقنية المعلومات الكويتي رقم ٦٣ لسنة ٢٠١٥م الدخول غير المشروع في مادته الأولى بأنه: "النفاذ المتعمد غير المشروع لأجهزة الحاسب الآلي، أو لنظامٍ معلوماتي أو شبكة معلوماتية أو موقع الكتروني من خلال اختراق وسائل واجراءات الحماية أو بالتجاوز للتفويض الممنوح". أما القانون الفرنسي فلم يعرف الدخول المجرم[٣]، وكذلك القانون الإماراتي[٤].

ويرى البعض أن التشريعات التي لم تعرف الدخول المجرم هي الأكثر، ومسلكها هو

---

(١)القانون المصري ١٧٥ لسنة ٢٠١٨م في شأن مكافحة جرائم تقنية المعلومات، تم نشره في الجريدة الرسمية، العدد ٣٢ مكرر(ج) في ١٤ أغسطس ٢٠١٨م، ونص في المادة ٤٥ منه على أن يعمل به من اليوم التالي لتاريخ نشره.

(٢)صدر نظام مكافحة الجرائم المعلوماتية السعودي بالمرسوم الملكي رقم م/ ١٧ بتاريخ ٨/ ٣/ ١٤٢٨ه، وقرار مجلس الوزراء رقم ٧٩ بتاريخ ٧/ ٣/ ١٤٢٨هـ.

(3) Ibtissem Maalaoui: op.cit., p.26.

وقد عرف قاموس larousse الوصول accès بأنه: " إمكانية دخول شخص ما في شيء ما" .

❖ https://www.larousse.fr/dictionnaires/francais/acc%C3%A8s/420

(٤) صدر المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات بتاريخ ١٣ أغسطس٢٠١٢.

الأفضل، لأن تجريم الدخول غير المشروع يرتبط بأمور تقنية متغيرة ومتطورة؛ ومن ثم فإن وضع تعريف له قد يضيق من نطاق التجريم حال عجزه عن مجاراة واستيعاب المستجدات التقنية(١).

أما على الصعيد الفقهي فقد انصرف أغلب الباحثين والفقهاء إلى تعريف الدخول غير المشروع باعتباره السلوك المحظور في هذه الجريمة، لذلك نرجئ تفصيل التعريفات الفقهية إلى موضعها في الركن المادي للجريمة.

## الفرع الثاني
## علة تجريم الدخول غير المشروع إلى الأنظمة المعلوماتية

تكمن علة تجريم الدخول غير المشروع في أنه يمثل تهديداً لمستودع السر الرقمي، وانتهاكاً لخصوصية الأفراد الإلكترونية، والأسرار الخاصة بأمن الدولة، وأسرار الشركات والبنوك، فقد يترتب علي مجرد كشف هذه الأسرار، أو الاطلاع عليها خسائر مالية، أو معنوية فادحة(٢)، كما أن أفعال الدخول غير المشروع والاختراق انتشرت بصورة واسعة بسبب تزايد استخدام الإنترنت والحواسب الآلية، وعدم اهتمام كثير من الأفراد، والشركات بتوفير الأمن والحماية التقنية لأنظمتهم المعلوماتية، وعلى الجانب الآخر فقد أصبحت برامج الاختراق وطرقه متاحة عبر الانترنت، وهو ما زاد معه عدد

(١) د/ عبد الإله النوايسة: جريمة الدخول غير المشروع في تشريعات الجرائم الإلكترونية العربية، دراسة مقارنة، المجلة القانونية والقضائية، مركز الدراسات القانونية والقضائية، وزارة العدل، قطر، ع١، س١٠، ٢٠١٦م ، ص٣٣.

(٢) د/ عبدالإله النوايسة: مرجع سابق، ص١٣.

من يرتكبون هذه الجريمة[1].

ورغم وضوح علة تجريم الدخول غير المشروع، فقد اتجه البعض إلى أنه لا جدوى، ولا ضرورة لهذا التجريم، وبرروا رأيهم هذا بأن الإحصائيات لم تكشف عن الحاجة إلى هذا التجريم، وأن دخول الأنظمة المعلوماتية – ولو بدون وجه حق – هو مجرد استعراض للقدرات من قبل المتطفل، وهو فعل لا يستأهل التجريم، كما أن كثير من حالات الدخول غير المشروع لا تترك أثراً يدل علها، خاصة إذا لم يترتب عليها إضرار بالبيانات أو المعلومات، ومن ثم يصعب على جهات التحقيق إثبات الدخول[2].

بيد أن أغلب الفقهاء والباحثين يرفضون هذا الرأي، ويقولون بضرورة هذا التجريم، إذ يرون أن هذه الجريمة هي أم الجرائم الالكترونية، وتمثل تهديداً حقيقيـًا لمستودع السر الإلكتروني[3]، وتعد مدخلاً أساسيـًا ولازمـًا لارتكاب كثير من الجرائم المعلوماتية الأخرى[4]، كما أن تجريم الدخول غير المشروع له أهمية فائقة تظهر في الحالات التي لا ينطبق علي الواقعة نص تجريمي آخر، إذ يمكن أن يطبق عليها وصف الدخول غير المشروع[5].

---

(١) د/ أسامة غانم العبيدي: جريمة الدخول غير المشروع إلى النظام المعلوماتي ، دراسة قانونية في ضوء القوانين المقارنة، مجلة دراسات المعلومات، ع١٤، مايو ٢٠١٢م ، ص١٢.

(٢) راجع في عرض مبررات هذا الاتجاه: أ/ نجاة عباوي: الإشكاليات القانونية في تجريم الاعتداء على أنظمة المعلومات، مجلة دفاتر السياسة والقانون، ع١٦، يناير٢٠١٧م ، ص٢٨٢.

(٣) د/ عبدالإله النوايسة: مرجع سابق، ص١٣.

(٤) د/ سامى الرواشدة، د/ أحمد الهياجنة: مكافحة الجريمة المعلوماتية بالتجريم والعقاب، القانون الإنجليزي نموذجـًا، المجلة الأردنية في القانون والعلوم والسياسة، مج١، ع٣، ٢٠٠٩م ، ص١٦٦

(٥) أ/ وسيم طعمة: السرقة المعلوماتية، دراسة مقارنة، مجلة جامعة البعث، مج٣٩، ع٦٨، ٢٠١٧م، ص١٧٠.

كما برروا ضرورة تجريم الدخول غير المشروع بأن عدم تجريمه يجعل بيانات النظام المعلوماتي ومحتوياته هدفاً مغرياً لكل من يملك القدرة على اختراق الأنظمة، ومن ثم الاطلاع عليها، أو نسخها، أو تدميرها(١)، وحتى إن لم يكن الدخول مصحوباً بنية ارتكاب جريمة أخرى فقد تتولد هذه النية بعد الدخول(٢)، كما قيل أن تجريم الدخول غير المشروع إجراء حاسم لبقاء الشركات والحفاظ على قدرتها التنافسية(٣)، إذ إن الدخول غير المشروع له أضرار ومخاطر قد تطال الأفراد، والمؤسسات، والشركات، والدول، وقد ازدادت في الآونة الأخيرة حجم الخسائر الناجمة عنه(٤)، فقد يعقب الدخول غير المشروع تعطيل لخدمات النظام، أو سرقة معلومات، أو ابتزاز، وقد يصل الأمر إلى حد الإضرار بالأصول والمنشآت التي يتحكم فيها النظام(٥)، كما أن المعلومات في النظام المخترق قد تكون على قدر كبير من الأهمية، كالمعلومات العسكرية والبنكية(٦).

كما أن الدخول غير المشروع سواءً كان مقصوداً لذاته، أم كان بغرض ارتكاب جريمة أخرى، فإن له آثاراً سلبية كثيرة أقلها تعريض المعلومات لخطر السرقة،

---

(١) د/ موفق علي عبيد، د/ ساهر ماضي ناصر: ماهية جريمة الاحتيال المعلوماتي، مجلة جامعة تكريت للعلوم القانونية، س٧، ع٢٥، ٢٠١٥م ، ص١١.

(٢) د/ محمد نصر محمد: الوسيط في شرح الجرائم المعلوماتية، مركز الدراسات العربية للنشر والتوزيع، ط١، ٢٠١٥م، ص٢٨٢.

(3) Romain Boos: op.cit., p66.

(٤) د/ عبيد صالح حسن: سياسة المشرع الإماراتي لمواجهة الجرائم الإلكترونية، مجلة الفكر الشرطي، مج٢٤، ع٩٥، أكتوبر ٢٠١٥م، ص١١.

(5) BREGANT, Jessica; BREGANT, Robert: op. cit., p.١.

(٦) د/ سامى الرواشدة، د/ أحمد الهياجنة، مرجع سابق، ص١٣٣.

أو الإفشاء، أو المحو، وقد يستمر الدخول، أو يتكرر فيتطلب وقفه، وقد تكون تكلفة هذا الوقف باهظة[١].

وإذا كان البعض يرى أنه لا حاجة إلى تجريم الدخول غير المشروع استناداً إلى أن الإحصائيات لم تكشف عن هذه الحاجة، فإن ذلك مرده حداثة تجريمه في التشريعات الوطنية[٢]، علاوة على أن أغلب الشركات تفضل عدم الإبلاغ عن اختراق مواقعها، خوفًا من الإضرار بسمعتها، وخوفًا من إفشاء معلومات، أو بيانات تحرص على سريتها أثناء التحري والتحقيق[٣]، لذا يتعين على الشركات الإبلاغ عن أي دخول غير مشروع لأنظمتها المعلوماتية[٤].

وفي مقام الموازنة بين الاتجاهين السابقين فإن الاتجاه القائل بجدوى تجريم الدخول غير المشروع هو الراجح؛ لقوة مبرراته وأسانيده، فضلاً عن أن شيوع جرائم اختراق الأنظمة المعلوماتية لشركات وبنوك وجهات سيادية وأمنية يؤكد ضرورة هذا التجريم والحاجة إليه، وما يؤكد غلبة هذا الاتجاه وصحة رأيه أن جريمة الدخول غير المشروع أصبحت تتصدر جرائم تقنية المعلومات في التشريعات الوطنية، ولا أدل على ذلك من تصدر هذه الجريمة كافة قوانين مكافحة جرائم تقنية المعلومات، والاتفاقيات الإقليمية

---

(١) أ/ نجاة عباوى، مرجع سابق، ص٢٨٢.

(٢) أ/ المرجع السابق، ذات الموضع.

(3) SUKHAI, Nataliya B: op. cit., p.132.

(٤) د/ هالة كمال نوفل، د/ اسماعيل محمود حسن: جرائم اختراق البيئة المعلوماتية، استشراف الاتجاهات الحديثة في مجال أمن المعلومات، دراسة إبستيمولوجية في ضوء أراء عينة من المتخصصين، المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية، كلية علوم الحاسب والمعلومات ، جامعة الإمام محمد بن سعود الإسلامية ، الرياض، ٢٠١٥م، ص١٩.

بشأن جرائم تقنية المعلومات. كما أن مؤتمر الأمم المتحدة لمنع الجريمة صنف الجرائم المعلوماتية إلى عدة فئات وكانت أولها جرائم الدخول غير المشروع(١).

إذن تكمن علة تجريم الدخول غير المشروع في كونه وسيلة فاعلة في الحفاظ على مستودعات الأسرار الإلكترونية، التي أصبحت جزءً لا يتجزأ من الحياة،؛ لما تحويه من بيانات ومعلومات في غاية الأهمية، فضلاً عن تعدد المصالح المعتبرة ذوات الصلة بالأنظمة المعلوماتية، سواءً ما تعلق منها بالحياة الخاصة، أو أسرار الشركات وبياناتها، وأعمالها، أو ما تعلق منها بالدولة ومصالحها المختلفة.

## المطلب الثاني
## الإطار التشريعي لجرائم الدخول غير المشروع إلى الأنظمة المعلوماتية

ينقسم هذا المطلب إلى فرعين، يتناول الفرع الأول الإطار التشريعي لهذه الجرائم في المواثيق الإقليمية، ويتناول الفرع الثان هذا الإطار في التشريعات الوطنية، وذلك على النحو التالي:

### الفرع الأول
### الإطار التشريعي لجرائم الدخول غير المشروع في المواثيق الإقليمية

لم يقتصر تجريم الدخول غير المشروع على القوانين الوطنية، بل نالت هذه الجريمة قسطًا من الاهتمام على المستوى الإقليمي، وقد تجسد هذا الاهتمام في اشتمال بعض الاتفاقيات وبعض القوانين النموذجية على أحكام بشأن الدخول غير المشروع، كاتفاقية بودابست، والاتفاقية العربية لمكافحة جرائم تقنية المعلومات، وقانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها.

(1) SUKHAI, Nataliya B: op. cit., p.132.

فقد أوجبت اتفاقية بودابست على الدول الأطراف أن تتخذ ما يلزم من تدابير تشريعية لتجريم الدخول إلى الأنظمة المعلوماتية إذا ارتكبت عمداً وبدون وجه حق، سواء كان الدخول على كامل النظام، أو على جزء منه، كما أجازت للدول الأطراف أن تستلزم لتجريم الدخول حصوله عن طريق مخالفة التدابير الأمنية، بقصد الحصول على بيانات ما، أو بقصد آخر غير أمين[1].

كما ألزمت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الدول الأطراف بتجريم الدخول غير المشروع إلى "تقنية المعلومات" سواء كان دخولاً كليـًا، أو جزئيـًا، وأوجبت تشديد العقوبة إذا ترتب على الدخول غير المشروع إضراراً بالبيانات، أو الأجهزة، أو الأنظمة الإلكترونية، أو شبكات الاتصال، سواء تمثل ذلك في نسخ البيانات، أو محوها، أو تعديلها، أو تدميرها، أو نقلها، مما يلحق الضرر بالمستخدمين والمستفيدين، كما نصت على تشديد العقوبة إذا ترتب على هذا الدخول الحصول على معلومات سرية تخص الحكومة[2].

كذلك نص القانون العربي الاسترشادى لمكافحة جرائم تقنية المعلومات وما في حكمها على تجريم الدخول غير المشروع إذا حدث الدخول عمداً وبدون وجه حق إلى موقع أو نظام معلوماتي، على أن يشدد العقاب إذا كان الدخول بقصد الإضرار بالبيانات، أو بمعلومات شخصية، أو إعادة نشرها، كما يشدد العقاب إذا كان الدخول

(١) المادة الثانية من اتفاقية بودابست.

(٢) المادة السادسة من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

غير المشروع أثناء أو بسبب أداء الوظيفة[1].

وقد تأثرت التشريعات الوطنية بهذه الاتفاقيات الاقليمية والقوانين الاسترشادية، وظهر هذا التأثر جلياً في تجريم أغلب التشريعات الوطنية للدخول غير المشروع، فضلاً عن تقارب أحكام التجريم والعقاب الخاصة بهذه الجرائم.

## الفرع الثاني
## الإطار التشريعي لجرائم الدخول غير المشروع في القوانين الوطنية

احتلت جرائم الدخول غير المشروع مكانة متميزة في قوانين مكافحة جرائم تقنية المعلومات، إذ جاءت في بدايات الفصول أو الأبواب الخاصة بأحكام التجريم والعقاب، وهذا ما يؤكد على أهمية هذه الجريمة، وأنها أصل غالبية الجرائم المعلوماتية.

فقد جرم المشرع المصري الدخول غير المشروع في المادة الرابعة عشر من قانون مكافحة جرائم تقنية المعلومات، والتي تنص على أن :" يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين كل من دخل عمداً، أو دخل بخطأ غير عمدي وبقي بدون وجه حق على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه. فإذا نتج عن ذلك الدخول إتلاف أو محو أو تغيير أو نسخ أو إعادة نشر للبيانات أو المعلومات الموجودة على ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي تكون العقوبة الحبس مدة لا تقل

(١) راجع في ذلك: المادة الثالثة والمادة السادسة من جرائم تقنية أنظمة المعلومات وما في حكمها، والذى اعتمده مجلس وزراء العدل العرب في دورته التاسعة عشر بالقرار رقم ٤٩٥ - د١٩ – ٨/ ١٠/ ٢٠٠٣م، ومجلس وزراء الداخلية العرب في دورته الحادية والعشرين بالقرار رقم ٤١٧ – د ٢١/ ٢٠٠٤م.

عن سنتين، وغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين".

كما جرم تجاوز حدود الحق في الدخول، حيث تنص المادة ١٥ من قانون مكافحة جرائم تقنية المعلومات على أن: " يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسين ألف جنيه، أو بإحدى هاتين العقوبتين كل من دخل إلى موقع أو حساب خاص أو نظام معلوماتي مستخدمًا حقًا مخولاً له، فتعدى حدود هذا الحق من حيث الزمان أو مستوى الدخول"[1].

أما المنظم السعودي وبعد تعريفه للدخول غير المشروع فقد جرمه في عدة مواضع؛ حيث جرمت المادة الثالثة منه الدخول غير المشروع لتهديد شخص أو ابتزازه، والدخول إلى المواقع الالكترونية، إذ تنص على أن : " يعاقب بالسجن مدة لا تزيد عن

---

(١) تجدر الإشارة إلى أن المشرع المصري جرم الدخول غير المشروع إلى المواقع الالكترونية الحكومية قبل إصداره قانون مكافحة جرائم تقنية المعلومات؛ في نطاق محدود للغاية في المادة ٢٩ من قانون مكافحة الإرهاب رقم ٩٤ لسنة ٢٠١٥ م، والتي تنص على أن: " ويعاقب بالسجن المشدد مدة لا تقل عن عشر سنين كل من دخل بغير حق أو بطريقة غير مشروعة موقعًا الكترونيًا تابعًا لأية جهة حكومية، بقصد الحصول على البيانات أو المعلومات الموجودة عليها أو الاطلاع عليها أو تغييرها أو محوها أو إتلافها أو تزوير محتواها الموجود بها، وذلك كله بغرض ارتكاب جريمة من الجرائم المشار إليها بالفقرة الأولى من هذه المادة أو الإعداد لها".

بيد أن هذا التجريم الوارد في قانون مكافحة الإرهاب نطاقه ضيق جداً؛ لقصره الدخول المجرم على نوع واحد من الأنظمة المعلوماتية، وهو المواقع الالكترونية التابعة للجهات الحكومية، دون المواقع الأخرى غير الحكومية، وحتى الدخول على هذه المواقع يجرم فقط إذا كان بغرض ارتكاب جريمة إرهابية من الجرائم التي حددتها الفقرة الأولى من المادة ٢٩ من القانون.

سنة وبغرامة لا تزيد خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين، كل شخص يرتكب أيـًا من الجرائم المعلوماتية التالية:١-....٢- الدخول غير المشروع لتهديد شخص أو ابتزازه؛ لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعـًا. ٣- الدخول غير المشروع إلى موقع الكتروني، أو الدخول إلى موقع الكتروني لتغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه. ٤ ..... ٥-....".

كما نصت المادة الخامسة من النظام السعودي على أن:" يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد عن ثلاثة ملايين ريال أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيـًا من الجرائم المعلوماتية الآتية:١-الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها، أو تغييرها، أو إعادة نشرها. ٢-..... ٣-.....".

ونصت المادة السابعة على أن: " يعاقب بالسجن مدة لا تزيد على عشر سنوات، وبغرامة لا تزيد على خمسة ملايين ريال، أو بإحدى هاتين العقوبتين كل شخص يرتكب أيـًا من الجرائم المعلوماتية الآتية: " ١-..... ٢- الدخول غير المشروع إلى موقع إلكتروني، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني".

وأما المشرع الإماراتي فقد جرم الدخول وعاقب عليه في المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات؛ حيث تنص المادة الثانية منه على أن: "١-يعاقب بالحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تزيد عن

ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين كل من دخل موقع إلكتروني أو نظام معلومات الكتروني أو شبكة معلومات أو وسيلة تقنية معلومات بدون تصريح أو بتجاوز حدود التصريح، أو بالبقاء فيه بصورة غير مشروعة. ٢- تكون العقوبة الحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن مائة وخمسين ألف درهم ولا تجاوز سبعمائة وخمسون ألف درهم أو بإحدى هاتين العقوبتين إذا ترتب على أي فعل من الأفعال المنصوص عليها بالفقرة (١) من هذه المادة أي إلغاء، أو حذف، أو تدمير، أو إفشاء، أو إتلاف، أو تغيير، أو نسخ، أو نشر، أو إعادة نشر أي بيانات أو معلومات. ٣- تكون العقوبة الحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين إذا كانت البيانات أو المعلومات محل الأفعال الواردة في الفقرة (٢) من هذه المادة شخصية".

كما جرم المشرع الإماراتي الدخول غير المشروع إذا وقع بمناسبة أو بسبب تأدية عمله، وجرم الدخول بقصد الحصول على بيانات حكومية وما في حكمها، وجرم الدخول إلى موقع الكتروني للإضرار به، ونعرض للنصوص الخاصة بهذه الجرائم عند تناول أحكامها.

أما المشرع الفرنسي فقد أصدر قانون " Godfrain " في ٥ يناير ١٩٨٨م، ووضع بموجبه ردع شامل للجريمة المعلوماتية، ثم أدرجت أحكامه في المادة ٣٢٣-١ وما يليها من قانون العقوبات في الفصل الثالث الموسوم بـ "انتهاكات نظم معالجة البيانات الآلية"[1]، وجاء تجريم الدخول الاحتيالي بموجب المادة ٣٢٣/ ١؛ حيث عاقب على

(1) Romain Boos : op. cit., p.66.

هذا الدخول بالحبس لمدة سنتين وغرامة ٦٠ الف يورو، وتشدد العقوبة لتكون الحبس ثلاث سنوات وغرامة ١٠٠ الف يورو إذا ترتب على الدخول إلغاء، أو تعديل البيانات الموجودة بالنظام، أو تغيير نظام التشغيل، وإذا تم الدخول الاحتيالي ضد نظام المعالجة الآلية للبيانات الشخصية التي تنفذها الدولة، أو ترتب عليه تعديل، أو الغاء البيانات، أو تغيير نظام التشغيل تشدد العقوبة إلى السجن لمدة خمس سنوات و ١٥٠ ألف يورو غرامة.

# المبحث الثاني
# الأحكام المشتركة بين جرائم الدخول غير المشروع إلى الأنظمة المعلوماتية

نظراً لاشتراك جرائم الدخول غير المشروع في كثير من الأحكام، فقد آثرت تناولها في هذا المبحث؛ لتجنب تكرارها في كل جريمة، وأعرض لهذه الأحكام على النحو التالي:

## المطلب الأول
## محل السلوك الإجرامي

حتى تقوم المسئولية الجنائية عن الدخول غير المشروع يتعين أن يقع الدخول على المحل الذى يحدده القانون، ولا شك في أهمية تحديد هذا المحل، وبيان مفهومه، ثم بيان مدى تطلب الحماية التقنية لمحل الدخول كشرط للتجريم، وذلك على النحو التالي:

### الفرع الأول
### تحديد محل الدخول ومفهومه

**أولاً- تحديد محل الدخول غير المشروع:** وسعت بعض القوانين محل الدخول المجرم، بينما ضيقت قوانين أخرى منه، وهذا ما ينعكس بدوره على نطاق التجريم. ويصنف القانون الفرنسي ضمن الاتجاه الموسع لمحل الدخول غير المشروع، بينما يصنف القانون الإنجليزي باعتباره أبرز مثال للاتجاه المضيق لمحل الدخول المجرم[1]. وهذا المحل وإن تم تحديده في نصوص تجريم الدخول، بيد أن القول بأنه يصلح محلاً للدخول المجرم من عدمه قد يحتاج لرأى خبراء تقنية المعلومات[2].

---

(١) د/ أيمن عبدالله فكرى: مرجع سابق، ص٣٢.

(٢) د/ عبدالإله النوايسة: مرجع سابق، ص٢٧.

وقد حدد المشرع المصري محل الدخول في المادة الأولى من قانون جرائم تقنية المعلومات في تعريفه للاختراق بأنه **الأنظمة المعلوماتية**، أو **الحواسب الآلية**، أو **الشبكات المعلوماتية** أو **ما في حكمها**، وحدده في نص تجريم الدخول غير المشروع في المادة ١٤ من القانون بأنه **المواقع**، أو **الحسابات الخاصة**، أو **الأنظمة المعلوماتية**، وحدد النظام السعودي هذا المحل في المادة الأولى منه عندما عرف الدخول غير المشروع؛ حيث تمثل في الحواسب الآلية، وشبكاتها، والمواقع الالكترونية، والأنظمة المعلوماتية، وحدده المشرع الإماراتي بأنه المواقع الإلكترونية، أو أنظمة المعلومات، أو شبكات المعلومات، أو وسائل تقنية المعلومات.

وعلى ذلك؛ فقد اتفقت القوانين الثلاثة في بعض المفردات كمحل للدخول غير المشروع، وهي الأنظمة المعلوماتية، والمواقع الالكترونية، وشبكات الحاسب، والحواسب الآلية، ثم زاد المشرع المصري على ذلك الحساب الخاص، وقد أطلق المشرع الإماراتي على الحواسب الآلية وما يقوم بمثل وظائفها وسائل تقنية المعلومات.

أما المشرع الفرنسي فقد حدد محل جريمة الدخول غير المشروع بأنه **"نظام معالجة البيانات الآلية"** STAD(١)، وذلك وفقًا لنص المادة ٣٢٣-١ من قانون العقوبات الفرنسي؛ لكنه لم يعرفه؛ رغم أهمية التعريف لتطبيق القانون(٢)، وينصرف هذا المحل إلى البيانات والمعلومات والنظام الذي يحتويها، وشبكات المعلومات التي تربط بينها(٣).

(1) Systèmes de Traitement Automatisé de Données)

(2) Ibtissem Maalaoui: Les infractions portant atteinte à la sécurité du système informatique d'une entreprise , thèse de magistère , Université de Montréal , Septembre 2011, p.16.

(٣) د/ أيمن عبدالله فكري: الجرائم المعلوماتية، دراسة مقارنة في التشريعات العربية والأجنبية، مكتبة القانون

أما المشرع الإنجليزي فقد جعل محل الجريمة "البرامج والبيانات الموجودة بأجهزة الحاسب الآلي"، وذلك وفقاً لقانون اساءة استعمال الكمبيوتر، باعتبار أن هذه البرامج والبيانات هي التي يتم المساس بسريتها، أو إتلافها، أو تعديلها، أما الكمبيوتر ذاته فلا يعد سوى وعاء، أو حاوية لهذه البيانات والبرامج[1]، لذلك صنف القانون الانجليزي باعتباره أبرز مثال للاتجاه الذي ضيق من محل الدخول؛ ومن ثم فإن اعتراض البيانات أثناء انتقالها عبر الشبكات لا يعد دخولاً غير مشروع[2].

**ثانيـًا- مفهوم النظام المعلوماتي وما في حكمه:** بعد تحديد محل الدخول المجرم، فقد تبين تعدد مفرداته، كما تبن أن النظام المعلوماتي يعد أهم هذه المفردات، باعتباره موضع توافق بين أغلب التشريعات، وباعتبار أن مفهومه يتسع ليشمل الكثير من المفردات الأخرى، لذلك يستخدم مصطلح النظام المعلوماتي للدلالة على محل الدخول غير المشروع، ومن ثم يلزم بيان مفهومه، وبيان ما يندرج في حكمه.

**مفهوم النظام المعلوماتي:** عرف قانون مكافحة جرائم تقنية المعلومات المصري النظام المعلوماتي في مادته الأولى بأنه: "مجموعة برامج وأدوات معدة لغرض إدارة ومعالجة البيانات والمعلومات، أو تقديم خدمة معلوماتية"، بينما عرفه المنظم السعودي بأنه:" "مجموعة برامج وأدوات معدة لمعالجة البيانات وإدارتها وتشمل الحاسبات الآلية"، وعرف المشرع الإماراتي نظام المعلومات الإلكتروني في مادته

---

والاقتصاد، ط١، ٢٠١٤م ، ص٣٠٢.

(1) WANG, Q: A Comparative Study of Cybercrime in Criminal Law: China, US, England, Singapore and the Council of Europe. 2016. PhD Thesis. Erasmus School of Law. p.161.

(٢) د/ أيمن عبدالله فكري: مرجع سابق، ص٣٠٢.

الأولى بأنه: "مجموعة برامج معلوماتية ووسائل تقنية المعلومات المعدة لمعالجة وإدارة وتخزين المعلومات الالكترونية، أو ما شابه ذلك".

ويلاحظ التقارب في مضمون النظام المعلوماتي في التعريفات السابقة، كما أن هذا المضمون يتفق مع تعريف الاتفاقية العربية لمكافحة جرائم تقنية المعلومات للنظام المعلوماتي والذي ورد في المادة الثالثة منها، ويتفق مع التعريف الوارد في قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها.

أما القانون الفرنسي فلم يعرف نظام المعالجة الآلية للمعطيات[١]، بيد أن مجلس الشيوخ الفرنسي اقترح تعريفـًا له بأنه: " كل مركب يتكون من وحدة أو أكثر من وحدات المعالجة، والتي تتكون كل منها من الذاكرة، والبرامج، والمعطيات، وأجهزة الإدخال، والإخراج، وأجهزة الربط، تربط بينها مجموعة من العلاقات تتحقق من خلالها معالجة المعطيات على أن يكون هذا المركب خاضعـًا لنظام المعالجة التقنية "[٢]، ووفقًا لهذا التعريف[٣] يشير مفهوم نظام معالجة البيانات الآلي إلى مجموعة تتألف من وحدة، أو أكثر من وحدات معالجة البرامج والبيانات وأجهزة الإدخال والإخراج والروابط التي تسهم في نتيجة معينة[٤].

(1) Géraldine Péronne et Emmanuel Daoud: cyberattaques: la lutte s'intensifie, Actualité Juridique Pénal. Septembre 2015, n° 9, p.397.

(2) DIMITRIOU, Philippe: L'application du droit de la cryptologie en matière de sécurité des réseaux informatiques. 2002. PhD Thesis. thesis dari DEA Défense Nationale option Sécurité européenne et internationale, Université de Lille 2. p.26

(٣) لم تتم الموافقة على هذا التعريف بحجة عدم إمكان ربط التجريم بحالة تقنية متغيرة قد لا يتسع لها التعريف مستقبلاً ( أ/ نسيمة جدي: جرائم المساس بأنظمة المعالجة الآلية للمعطيات، رسالة ماجستير، جامعة وهران، الجزائر، ٢٠١٤م ، ص٥٢).

(4) Romain Boos : op. cit., p.69.

وعلى ذلك فلم يقصر المشرع الفرنسي نظام المعالجة على الكمبيوتر؛ بل يشمل كل نظام، أو جهاز، بإمكانه المعالجة الآلية للمعطيات المعلوماتية؛ ومن ثم فإن شبكة الانترنت تعد نظام معالجة آلية، وكذلك البريد الالكتروني، وبطاقة الائتمان البنكية، والبطاقات الالكترونية، والقرص النقال، والقرص المرن، والقرص المضغوط الذي يحتوي على قاعدة المعطيات، والبرنامج المعلوماتي الذي يسمح بالدخول إلى هذه القاعدة، والأشرطة الممغنطة، والأقراص المضغوطة، أو أي دعامة مادية يتم فيها تخزين المعلومات والتي تحمل ضمنها برنامج خاص[١].

وقد أصبح للقضاء الفرنسي تصور واسع لمفهوم "نظم معالجة البيانات الآلية"، ومن أمثلته شبكة فرانس تليكوم، وشبكة البطاقات المصرفية[٢]، والأقراص الصلبة، والهواتف اللاسلكية[٣]، وأجهزة الكمبيوتر، ولو كانت معزولة[٤].

**ما يعد في حكم الأنظمة المعلوماتية:** حددت قوانين مكافحة جرائم تقنية المعلومات بعض المفردات التقنية الأخرى وجعلت منها محلاً للدخول غير المشروع، وهي:

**الحواسب الآلية ووسائل تقنية المعلومات:** عرف قانون مكافحة جرائم تقنية المعلومات المصري الحاسب الآلي بأنه: "كل جهاز أو معدة تقنية تكون قادرة على

---

(١) أ/ مختارية بوزيدي: ماهية الجريمة الالكترونية، بحث مقدم في الملتقى الوطني: آليات مكافحة الجرائم الالكترونية في التشريع الجزائري، مركز جيل البحث العلمي، الجزائر، ٢٩ / ٣/ ٢٠١٧م ، ص١٤، وأنظر إشارته إلى: نسيم دردور، المرجع السابق، ص٢٣.

(2) Tribunal correctionnel de Paris, 25 février 2000.
❖https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-paris-13eme-ch-correctionnelle-jugement-du-25-fevrier-2000/

(3) la Cour d'appel de Douai, 7 octobre 1992
❖http://www.assemblee-natinationale.fr/13/propositions/pion3412.asp

(4) la Cour d'appel de Paris, 18 November 1992.
❖http://www.assemblee-nationale.fr/13/propositions/pion3412.asp

التخزين وأداء عمليات منطقية أو حسابية، وتستخدم لتسجيل بيانات أو معلومات أو تخزينها أو تحويلها أو تخليقها أو استرجاعها أو ترتيبها أو معالجتها أو تطويرها أو تبادلها أو تحليلها أو للاتصالات". وعرفه نظام مكافحة جرائم المعلوماتية السعودي بأنه: "أي جهاز الكتروني ثابت أو منقول، سلكي أو لا سلكي يحتوي على نظام معالجة البيانات أو تخزينها، أو إرسالها، أو استقبالها، أو تصفحها، يؤدي وظائف محددة بحسب البرامج والأوامر المعطاة له"؛ بينما أطلق المشرع الإماراتي على الحواسب الآلية وما يقوم بوظيفتها مصطلح وسائل تقنية المعلومات(١)، وعلى ذلك يشمل مفهوم الحاسب الهواتف النقالة التي تقوم بوظائف الحاسب الآلي أيـًا كان مسماها، أو حجمها.

**الشبكات المعلوماتية:** عرف القانون المصري الشبكة المعلوماتية بأنها: "مجموعة من الأجهزة أو نظم المعلومات تكون مرتبطة معـًا، ويمكنها تبادل المعلومات والاتصالات فيما بينها، ومنها الشبكات الخاصة والعامة وشبكات المعلومات الدولية، والتطبيقات المستخدمة عليها".

**وعرفها النظام السعودي بأنها:** " ارتباط بين أكثر من حاسب آلي أو نظام معلوماتي للحصول على البيانات وتبادلها، مثل الشبكات العامة والخاصة، والشبكة العالمية(الانترنت)"، وعرفها القانون الإماراتي بأنها: " ارتباط بين مجموعتين أو أكثر

(١) عرف القانون الإماراتي وسائل تقنية المعلومات بأنها: "أي أداة الكترونية مغناطيسية بصرية، كهروكيميائية، أو أي أداة أخرى تستخدم لمعالجة البيانات الالكترونية وأداء العمليات المنطقية والحسابية أو الوظائف التخزينية، ويشمل أي وسيلة موصلة أو مرتبطة بشكل مباشر تتيح لهذه الوسيلة تخزين المعلومات الالكترونية أو إيصالها للآخرين".

من البرامج المعلوماتية ووسائل تقنية المعلومات".

**الموقع**: عرف القانون المصري الموقع بأنه: "مجال أو مكان افتراضي له عنوان محدد على شبكة معلوماتية، يهدف إلى إتاحة البيانات والمعلومات للعامة أو الخاصة"، وعرفه النظام السعودي بأنه: " مكان إتاحة البيانات على الشبكة المعلوماتية من خلال عنوان محدد".

**الحساب الخاص**: ذكر المشرع المصري الحساب الخاص كمحل للدخول غير المشروع، وعرفه بأنه: "مجموعة من المعلومات الخاصة بشخص طبيعي أو اعتباري، تخول له دون غيره الحق في الدخول على الخدمات المتاحة أو استخدامها من خلال موقع أو نظام معلوماتي".

أما المشرع الإماراتي والمنظم السعودي فلم ينصا صراحةً على الحسابات الخاصة كمحل للدخول غير المشروع؛ بيد أن ذلك لا يعني استبعادها من نطاق حظر الدخول غير المشروع، ذلك أن اختراق الحسابات الخاصة، أو دخولها دخولاً غير مشروع لن يتم إلا من خلال نظام معلوماتي، أي أن الحسابات الخاصة تعد جزءً من الأنظمة المعلوماتية، فيخضع دخولها بطريق غير مشروع للتجريم.

ويتضح من تحديد المشرعين المصري، والإماراتي، والمنظم السعودي لمحل الاختراق والدخول غير المشروع أنهم أخذوا بالاتجاه الموسع في تحديد محل الدخول، وهو مسلك محمود؛ لأنه وسع من نطاق هذا المحل بما يشمل كافة صور وأنواع ومسميات الوسائل التي تستخدم في الاتصال والتواصل مما يعد في حكم الحواسب الآلية، ويعمل عبر أنظمتها، أو أنظمة مشابهة، سواءً كان متصلاً بالإنترنت، أو غير متصل به.

وعلى ذلك؛ فلا يتحقق الدخول المجرم إذا وقع على برامج معروضة للبيع، أو على حاسب لم يدخل الخدمة، أو على عنصر مودع بالمخازن، أو قطع غيار، أو أجهزة لا زالت في طور التجربة، أو أنظمة خرجت من الخدمة(١)؛ بينما يتحقق إذا وقع على النظام خارج ساعات تشغيله العادية، أو إذا كان النظام معطلاً كليًا أو جزئيًا(٢).

وجميع هذه المفردات، سواءً الموقع الالكتروني، أو الشبكة المعلوماتية، أو وسائل تقنية المعلومات، أو الحاسب الآلي كلها يمكن أن يستوعبها مصطلح النظام المعلوماتي إن تم ضبط مفهومه لغةً، وصياغةً، وتقانةً(٣)؛ لذلك أقترح تعريف للنظام المعلوماتي بأنه: " كل أداة أو مجموعة من الأدوات تعمل بطريقة الكترونية من خلال برنامج أو أكثر، لإنشاء، أو معالجة، أو تخزين، أو استرجاع، أو إرسال أو استقبال، أو عرض بيانات، أو معلومات الكترونية".

## الفرع الثاني
## مدى اشتراط الحماية التقنية لتجريم الدخول غير المشروع

انقسم الفقه حول مدى تطلب الحماية التقنية كشرط لتجريم الدخول غير المشروع، وكذلك القوانين إلى اتجاهين، على النحو التالي:

---

(١) د/ محمد مزاولي: المسئولية الجنائية للأشخاص الاعتبارية عن جريمة المساس بأنظمة المعالجة الآلية للمعطيات، مجلة الفقه والقانون، المغرب، ع٢٣، ٢٠١٤م، ص٤٣.

(٢) أ/ سفيان سوير: الجريمة المعلوماتية، رسالة ماجستير، جامعة أبو بكر بلقايد – تلمسان، ٢٠١١م، ص٩٦.

(٣) انتقد البعض إفراط قوانين مكافحة جرائم تقنية المعلومات العربية في مسألة التعريفات؛ لعدم دقة الكثير منها، ولأن ذلك خارج عن المألوف في التجريم، وفضل ترك هذه المهمة للفقه والقضاء. (أ/ مداوي سعيد القحطاني: الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، مجلس التعاون لدول الخليج، الأمانة العامة، ٢٠١٦م، ص٤٠).

**الاتجاه الأول- الحماية التقنية شرط لتجريم الدخول غير المشروع**

**و يبرر أنصار هذا الاتجاه رأيهم بما يلي:**

**أولاً-** إن وجود حماية تقنية للنظام تتيح للأفراد العلم بحظر دخول النظام، بينما عدم وجودها قد يؤدي إلى وقوع الكثيرين تحت طائلة المسئولية الجنائية، فضلاً عما فرضه المشرع على الجهات التي تتعامل مع البيانات الشخصية من توفير الحماية الملائمة لها ضد الانتهاكات، وفرض عقوبات على الجهات التي لا توفر هذه الحماية(١).

**ثانيـًا-** من غير المقبول ترك بيانات ومعلومات مهمة دون إجراءات تكفل لها الحماية؛ إذ إن فعل الدخول إلى الحاسب الآلي لا يدل بذاته على عدم المشروعية؛ لذا يجب على المشرع أن يجرم الدخول بالغش والاحتيال، وهو ما يتحقق باختراق أنظمة الحماية الأمنية(٢).

**ثالثـًا-** إن من شأن الحماية كشرط للتجريم دفع أصحاب الأنظمة المعلوماتية لاستخدام أنظمة الكترونية للحماية. إذ إن عدم اهتمام الشركات بالحماية التقنية من أهم

---

(١) د/ محمد نصر القطري: الإشكاليات القانونية لحماية سلامة المعلومات، دراسة تطبيقية على الحماية الجنائية من الإتلاف المعلوماتي، مجلة الفكر الشرطي، مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، مج٢٤، ع٩٣، أبريل ٢٠١٥م، ص١٧١، د/ فضيلة عاقلي: الجريمة الالكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، بحث مقدم ضمن أعمال المؤتمر الدولي الرابع عشر، الجرائم الالكترونية، طرابلس،٢٤-٢٥ مارس ٢٠١٧م، ص٩.

(٢) راجع في عرض هذه المبررات د/ مهند وليد الحداد: التنظيم القانوني لجريمة الدخول غير المصرح به إلى نظام الحاسب الآلي، مجلة العلوم الشرعية، جامعة القصيم، المملكة العربية السعودية، مج١١، ع١، سبتمبر ٢٠١٧م، ص٥٥٠.

أسباب الدخول غير المشروع[١].

**رابعًا**- إن خضوع الأنظمة لحماية فنية يسهل اكتشاف أي اختراق أو تعد؛ حيث يترك ذلك أثراً ماديًا، كإلغاء كلمة السر، أو تغييرها، فضلاً عن أن وجود حماية للنظام يسهل إثبات القصد الجنائي لدى المتهم[٢].

وقد تطلبت بعض القوانين لتجريم الدخول غير المشروع أن يكون النظام المعلوماتي محميًا بوسائل حماية أمنية، كالقانون الإيطالي[٣]، والقانون الفيدرالي الأمريكي، والقانون المكسيكي، والفنلندي، واليوناني، والألماني، والسويسري[٤]. ويصنف قانون مكافحة جرائم تقنية المعلومات الكويتي ضمن هذا الاتجاه؛ إذ اشترط عند تعريفه للدخول غير المشروع أن يتم من خلال" اختراق وسائل وإجراءات الحماية لها بشكلٍ جزئي أو كلي... "، ومفاد ذلك أن الدخول المجرم يتعين أن يكون محله محميًا بوسائل فنية.

**الاتجاه الثاني- عدم تطلب الحماية التقنية للنظام لتجريم الدخول**

يرى أنصار هذا الاتجاه أن الأنظمة المعلوماتية جديرة بالحماية الجنائية في مواجهة الدخول غير المشروع، سواءً كانت تتوافر لها الحماية التقنية أم لا، واستندوا إلى ما يلي:

**أولاً**-إن قصر تجريم الدخول غير المشروع على الحالات التي يكون فيها النظام محميًا يضيق من نطاق الحماية الجنائية للأنظمة المعلوماتية في مواجهة الدخول غير

---

(١) د/ أسامة العبيدي: مرجع سابق، ص١٢.

(٢) راجع في عرض هذا الرأي أ/ نسيمة جدي : مرجع سابق، ص٢٤.

(3) Pradel, Jean: "Les infractions relatives à l'informatique." Revue internationale de droit comparé 42, no. 42 (1990): 815-828, p.822.

(٤) د/ عبد الإله النوايسة: مرجع سابق، ص ٢٧.

المشروع[1].

**ثانيًا**- قياس جريمة الدخول غير المشروع على جريمة السرقة، فكما تقع السرقة على المال المنقول سواءً كان متمتعًا بحماية صاحبه أم لا؛ فإن جريمة الدخول غير المشروع تقع على النظام المعلوماتي سواءً كان محميًا أم لا[2].

**ثالثًا**-إن الحماية التقنية ليست شرطًا لتجريم الدخول غير المشروع؛ وإنما قرينة على توافر القصد الجنائي أو الاحتيال في الدخول[3]، أي أن الحماية الفنية للنظام تعد وسيلة لإثبات سوء نية المتهم وعدم مشروعية دخوله[4].

**رابعًا**- إن الدخول غير المشروع إلى الأنظمة المعلوماتية يخضع للتجريم سواءً كان النظام المعلوماتي محميًا أم لا؛ إلا إنه يجب تشديد العقوبة حال وقوع الجريمة على نظام معلوماتي محمى، وهذا ما فعله المشرع البرتغالي؛ إذ شدد العقاب على الدخول إلى الأنظمة المحمية[5].

**خامسًا**- إن أغلب قوانين مكافحة جرائم تقنية المعلومات لم تتضمن شرط الحماية الفنية، ومن ثم فهي غير مطلوبة كشرط لتجريم الدخول غير المشروع[6].

---

(١) د/ عبد الإله النوايسة: مرجع سابق، ص٢٨.

(٢) د/ مهند الحداد: مرجع سابق، ص٥٥٠.

(3) Christian Le Stanc: Ne commet pas le délit d'accès et de maintien frauduleux dans un système de traitement automatisé de données l'internaute qui utilise un logiciel répandu pour pénétrer dans un système non protégé , Recueil Dalloz , 2003 , p.2827.

(٤) د/ صالح شنن: الحماية الجنائية للتجارة الإلكترونية، دراسة مقارنة، رسالة دكتوراه، جامعة أبو بكر بلقايد – تلمسان، ٢٠١٣م، ص٧٩.

(٥) د/ عبد الإله النوايسة: مرجع سابق، ص٢٨.

(٦) د/ عزيزة رابحي: الأسرار المعلوماتية وحمايتها الجزائية، رسالة دكتوراه، جامعة أبو بكر بلقايد – تلمسان،

ويبدو أن هذا الاتجاه هو الغالب؛ فلم تشترط قوانين مكافحة جرائم تقنية المعلومات العربية الحماية الأمنية صراحةً عند تجريمها للدخول غير المشروع، باستثناء القانون الكويتي، كما أن القانون الفرنسي لم يشترط هذه الحماية[١].

إذن الأنظمة المعلوماتية تستأهل الحماية الجنائية في مواجهة الدخول غير المشروع، سواءً كانت محمية أم لا، المهم أن يكون المتحكم في النظام قد أظهر نيته في تقييد الدخول إليه[٢]، ومن ثم يستوي إذا كان النظام المعني محاطًا بحماية محكمة أم ضعيفة أم بدون حماية؛ إذ إن ذلك ليس شرطًا للتجريم[٣]، كما شددت عليه محكمة الاستئناف في باريس في حكم صدر في ٥ أبريل ١٩٩٤، واعتبرت أنه " لكي يُعاقب علي الدخول، لابد وأن يتم بدون حق، وبمعرفة كاملة بالوقائع، وليس من الضروري لوقوع الجريمة، أن يكون الوصول محدوداً بواسطة جهاز حماية، ولكنه يكفي أن يكون "المتحكم في النظام قد أظهر النية لتقييد الوصول على الأشخاص المصرح لهم فقط[٤].

رأى الباحث: بعد عرض اتجاهات الفقه، وموقف القوانين بشأن مدى تطلب الحماية التقنية كشرط لتجريم الدخول غير المشروع؛ فإنه يبدو لي أنه كان يجب تحديد مفهوم الحماية محل الخلاف، وهل هي الحماية التقنية المتخصصة المتمثلة في برامج الكترونية مصممة لذلك، أم أنها الحماية بصفة عامة التي يمثل حدها الأدنى كلمات المرور، وشفرات الدخول، وحدها الأقصى الحماية التقنية المتخصصة عبر برامج

---

٢٠١٨م، ص٦٢، د/ صالح شنن: مرجع سابق، ص٧٩.

(1) Pradel, Jean: " op.cit., p. 822.
(2) Romain Boos: op.cit., p. 82.
(3) Monika Zwolinska: Sécurité et libertés fondamentales des communications électroniques en droit français, européen et international. Droit. Université Nice Sophia Antipolis, 2015. P. 171.
(4) Cour d'appel de Paris, 5 avril 1994. ( cité par: Ibtissem Maalaoui : op. cit., p. 26)

الكترونية؛ بيد أن الفقه لم يعتني بتحديد هذا المفهوم، وكذلك معظم القوانين، ومنها القوانين محل الدراسة.

بينما عرف القانون الروماني رقم ١٦١/ ٢٠٠٣ في المادة ٣٥ منه التدابير الأمنية بأنها: "استخدام إجراءات أو أجهزة أو برامج كمبيوتر متخصصة لتقييد أو منع الوصول إلى نظام الكمبيوتر، وقصره على فئات معينة من المستخدمين"(١).

والأرجح أن الحماية التقنية المتطلبة لتجريم الدخول غير المشروع هي مجرد الحماية العادية التي يوفرها كل شخص لأنظمته المعلوماتية، أو حساباته الخاصة، أو شبكاته، أو حواسبه؛ ومن ثم يجرم الدخول إلى أي نظام معلوماتي محمي حماية عادية، ولو بمجرد كلمات المرور، أو حماية متخصصة، كما هو الحال في البرامج المصممة خصيصاَ لحماية أنظمة البنوك، والشركات الكبرى.

أما القول بأن الحماية المتطلبة لتجريم الدخول وفقاً لهذا الاتجاه هي الحماية التقنية المتخصصة، أي التي تصمم خصيصاً لحماية انظمة الشركات، والبنوك، وغيرها، من الأنظمة المعلوماتية ذوات الأهمية، فإن ذلك يعنى أن الأنظمة المعلوماتية والمواقع والحسابات الشخصية التي لا تحمى بمثل هذه البرامج التقنية المتخصصة، وإنما يتم حمايتها بكلمات مرور وإجراءات تقنية بسيطة لا تدخل في نطاق الحماية الجنائية من الدخول غير المشروع، وهذه نتيجة غير منطقية لا يمكن التسليم بها، وذلك لتوافر علة التجريم ذاتها.

(1) PICOTTI, Lorenzo; SALVADORI, Ivan:National legislation implementing the Convention on Cybercrime-Comparative analysis and good practices. 2008, P.11. et: MOISE, Adrian Cristian: Modernization of Romanian legislation on preventing and combating cybercrime and implementation gap at European level. Revista de Stiinte Politice, 2015, P.187.

وحسماً لهذا الخلاف أطرح فكرة **"الاستئثار بالنظام المعلوماتي"** كبديل عن الحماية التقنية، واعتمادها كشرط لتجريم الدخول غير المشروع، ومفاد هذه الفكرة أن الأنظمة المعلوماتية وما في حكمها تستأهل الحماية الجنائية، ويصبح دخولها مجرماً إذا كان صاحبها يظهر استئثاراً واختصاصاً بها، ولا يشترط أن يؤمنها بالحماية التقنية، ومن ثم كلما تبين من ظاهر الحال أن صاحب النظام المعلوماتي يستأثر به لنفسه، أو لفئة محددة، ويمنع الغير من الدخول فيه، كلما كان الدخول مجرماً، أما إذا كان ظاهر الحال يشير إلى أن صاحب النظام المعلوماتي ترك النظام مفتوحاً للغير فلا يعد الدخول مجرماً، فإذا كان المكان التقليدي لا يجوز دخوله من قبل الغير إلا بإذن صاحبه، باعتباره مستودعاً لأسراره؛ فإن الأنظمة المعلوماتية بما تحويه من أسرار ومعلومات قد تفوق في أهميتها ما يوجد في المكان الخاص التقليدي، وإذا كانت المنازل والأماكن الخاصة لا يشترط حمايتها من قبل صاحبها حتى تتمتع بحماية القانون الذي يحظر انتهاك حرمتها، فإن الأنظمة المعلوماتية تستأهل الحماية الجنائية في مواجهة الدخول غير المشروع بمجرد أن يظهر صاحبها استئثاراً واختصاصاً بها.

والاستئثار بالنظام المعلوماتي قد يكون صريحاً، وقد يكون ضمنياً، فيكون صريحاً عندما يكون النظام محاطاً بحماية تقنية عادية، أو متخصصة، أو توجد قيود واضحة على دخوله، ككلمة مرور، أو اسم مستخدم، أو شفرة ما، أو تطلب دفع اشتراك مالي، ويكون الاستئثار ضمنياً عندما يكون النظام في وعاء، أو جهاز معين في حيازة صاحبه، أو في مكان ما، وهو يختص بهذا المكان دون غيره، كجهاز الحاسب الآلي في المنزل، أو في مكتب مستقل عن الغير، أو جهاز حاسب آلي محمول، أو هاتف محمول؛ إذ درج العرف على أن مثل هذه الأشياء يختص بها صاحبها، ويستأثر بما فيها، وبالتالي فإنها وما

فيها من حسابات شخصية، كالبريد الالكتروني، وحسابات الكترونية بنكية، أو خاصة بالعمل، أو حسابات مواقع التواصل، أو غير ذلك من برامج وأنظمة وبيانات ومعلومات لا يجوز الدخول إليها، ولو كانت تعمل بمجرد تشغيل الجهاز المثبتة عليه.

أما غياب التعبير عن إرادة تقييد الدخول إلى النظام من قبل المسئول عنه فلا تقع معه جريمة الدخول غير المشروع[1]، ولا يمكن تكييف الدخول إلى نظام معلوماتي مفتوح للجمهور بأنه دخول احتيالي أو غير مشروع، إذ إن نية المتحكم في النظام تكون ظاهرة في عدم تقييد الوصول إلى نظامه[2]،أي أنه كي يتحقق الدخول المجرم يجب أن يكون أسلوب الدخول غير نظامي، ويتم ذلك عندما يعبر المتحكم في النظام عن رغبته في تقييد الوصول إلى النظام المعلوماتي[3].

وتظهر أهمية هذه الفكرة في أن كثيراً من أصحاب الأنظمة المعلوماتية قد لا يلجؤون إلى تأمينها وحمايتها تقنياً؛ باعتبار أن الأوعية أو الأجهزة التي توجد بها مثل هذه الأنظمة بحوزتهم، فتظل مفتوحة وتعمل بمجرد تشغيل الجهاز، أو الوعاء الذي تعمل من خلاله. كالبريد الالكتروني، ومواقع التواصل الاجتماعي التي تترك في وضع التشغيل وتعمل بمجرد تشغيل جهاز الحاسب الآلي[4]، أو الهاتف المحمول، وهنا تظهر أهمية الحماية الجنائية للأنظمة غير المحمية تقنياً، خاصة في حالة فقد أو سرقة الحاسب الآلي، أو الهاتف المحمول، أو سرقته، كما يظهر دور فكرة الاستئثار بالنظام في استحقاق هذه الحماية.

---

(1) T. corr., Paris, 8 décembre 1997, Gaz. Pal., [1998], chron. crim. ( cité par: Romain Boos: op.cit., p. 83).

(2) Christian Le Stanc, op. cit., p.2827

(3) Cécile Duhil de Bénazé : op. cit., p.3.

(٤) د/ سامي الرواشدة: الأدلة المتحصلة من مواقع التواصل الاجتماعي ودورها في الإثبات الجنائي: دراسة في القانونين الإنجليزي والأمريكي، المجلة الدولية للقانون، ٢٠١٧م ، ص٢٠.

## المطلب الثاني
## الركن المادي لجرائم الدخول غير المشروع

يعد الركن المادي وأحكامه من الجوانب المشتركة بين جرائم الدخول غير المشروع بصورها المختلفة، ويقوم بمجرد توافر سلوك "الدخول غير المشروع"؛ إذ إن كافة جرائم الدخول غير المشروع في القانون المصري والإماراتي، والنظام السعودي من الجرائم الشكلية، التي تقوم بمجرد الولوج غير المشروع إلى نظام معلوماتي أو ما في حكمه. كذلك المشرع الفرنسي وفقًا للمادة ٣٢٣-١ فإنه يجرم الدخول الاحتيالي بغض النظر عن النتيجة التي يؤدي إليها[1]، وتميز المادة ٣٢٣-١ من قانون العقوبات بين الدخول البسيط الذي يقتصر على مجرد الدخول دون إحداث ضرر، وبين الدخول الذي يترتب عليه ضرر[2]، وحتى إذا تحقق هذا الضرر فإنه لا يمثل سوى ظرف مشدد للعقاب.

وعلى ذلك؛ أعرض في الفرع الأول الأحكام العامة للسلوك الإجرامي، وأعرض في الفرع الثاني "شرط عدم مشروعية الدخول"

### الفرع الأول
### السلوك الإجرامي في جريمة الدخول غير المشروع

يتمثل السلوك الإجرامي للجريمة في "الدخول"، وأعرض لمدلوله، ووسائله، على النحو التالي:

**أولاً- المقصود بالدخول غير المشروع:** لم يعرف القانون الفرنسي الدخول غير المشروع[3]، وكذلك القانون الإماراتي؛ أما المشرع المصري فقد عرف الاختراق في

(1) Ibtissem Maalaoui : op. cit., p. 26.
(2) Romain Boos :op. cit., p.67.
(3) Ibtissem Maalaoui: op.cit., p.26.

المادة الأولى بأنه: " الدخول غير المرخص به أو المخالف لأحكام الترخيص، أو الدخول بأي طريقة غير مشروعة إلى نظام معلوماتي أو حاسب آلي أو شبكة معلوماتية وما في حكمها". ويستفاد من هذا التعريف أن المشرع المصري جعل الدخول بأية طريقة غير مشروعة يعد اختراقًا للنظام المعلوماتي أو ما في حكمه، واعتبر أن الدخول بدون ترخيص، والدخول الذي يخالف أحكام الترخيص دخولاً غير مشروع، ومن ثم فلا فرق بين الاختراق وبين والدخول بدون تصريح، والدخول بتصريح مخالف للشروط، وكذلك الدخول بأية طريقة أخرى غير مشروعة.

وقد كان الأولى بالمشرع أن يضع تعريفًا لما جرمه وهو الدخول غير المشروع وليس الاختراق؛ أو يجرم ما عرفه وهو الاختراق، أو يبقى على نهجه ومسلكه العام ويسكت عن التعريف، ويترك هذه المهمة للفقه والقضاء؛ ذلك أن مفهوم الدخول غير المشروع أوسع من الاختراق، فكل اختراق يعد دخولاً غير مشروع، والعكس غير صحيح، إذ إن الاختراق معناه النفاذ إلى نظام معلوماتي محمي حماية عادية، أو تقنية؛ بينما الدخول غير المشروع قد يتم دون تجاوز أنظمة الحماية، كما لو تم الدخول خلسةً إلى نظام معلوماتي تصادف أنه مفتوح.

أما نظام مكافحة جرائم المعلومات السعودي فقد عرف الدخول غير المشروع في مادته الأولى بأنه:" دخول شخص بطريقة متعمدة إلى حاسب آلي، أو موقع الكتروني، أو نظام معلوماتي، أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها". ويلاحظ على هذا التعريف أنه قصر الدخول غير المشروع على الحالة التي يدخل فيها

---

وقد عرف قاموس larousse الوصول accès بأنه: " إمكانية دخول شخص ما في شيء ما" .

❖https://www.larousse.fr/dictionnaires/francais/acc%C3%A8s/420

المتهم نظامًا معلوماتيًا، أو ما في حكمه دون التصريح له بذلك، وبمفهوم المخالفة فإن من يدخل وهو مصرح له بذلك لكن يخالف ضوابط وأحكام التصريح فإن ذلك يعد دخولاً مشروعًا، وتظهر أهمية هذا الأمر إذا أخذنا في الاعتبار أن المنظم السعودي لم يجرم تجاوز حدود الحق في الدخول.

ويرى البعض أن التشريعات التي لم تعرف الدخول المجرم هي الأكثر، ومسلكها هو الأفضل، لأن تجريم الدخول غير المشروع يرتبط بأمور تقنية متغيرة ومتطورة؛ ومن ثم فإن وضع تعريف له قد يضيق من نطاق التجريم حال عجزه عن مجاراة واستيعاب المستجدات التقنية(١).

وعلى الصعيد الفقهي يعرف الدخول المجرم بأنه: "الولوج غير المصرح به أو بشكل غير مشروع إلى نظام معالجة البيانات باستخدام الحاسوب"(٢)، وعرف بأنه:" كافة الأفعال التي تسمح بالدخول إلى نظام معلوماتي والإحاطة أو السيطرة على المعطيات التي يتكون منها أو الخدمات التي يقدمها"(٣)، وقيل بأنه يشمل كافة الأعمال التي تسمح بالولوج إلى نظام معلوماتي والإحاطة أو السيطرة على المعطيات التي يتكون منها، أو الخدمات التي يقدمها(٤)، وبأنه ظاهرة معنوية تعني الدخول إلى العمليات التي يقوم بها النظام المعلوماتي(٥)، وأضفي البعض على الدخول مدلولاً مكانيًا يعني التسلل إلى

(١) د/ عبد الإله محمد النوايسة : مرجع سابق ، ص٣٣.

(٢) د/ محمد نصر محمد القطري: مرجع سابق، ١٦٧ .

(٣) د/ أسامة غانم العبيدي : مرجع سابق ، ص١٣ .

(٤) د/ مهند الحداد: مرجع سابق، ص٥٤٠.

(٥) أ/ مختارية بوزيدي: مرجع سابق، ص١٤.

داخل النظام المعلوماتي، ومدلولاً زمانيـًا يتمثل في تجاوز حدود الفترة المصرح بالدخول خلالها[1].

أما الاختراق فيعني وجود نظام حماية تم تجاوزه أو النفاذ منه[2]؛ لذلك عرف البعض الاختراق بأنه اقتحام الأنظمة أو الشبكات عن طريق برامج متخصصة في فك أو سرقة كلمات السر وتصريحات الدخول[3]، فالدخول لا يعني الاختراق، لأن الاختراق هو نوع من الدخول الفني يتم من خلاله التسلل أو الاقتحام[4] والاقتحام لا يكون إلا للأنظمة المحمية.

وعلى ذلك؛ فإن الدخول يتحقق بنشاط إيجابي يمكن المتهم من التواجد داخل النظام أو أيٍ من أجزائه، سواءً طالت مدته أم قصرت، وسواءً تحققت له السيطرة على النظام أم لا؛ ومن ثم فكل فعل لا يفضي إلى تخطي حدود النظام لا يعد دخولاً، فمجرد

---

(١) أ/ حمودي ناصر: الحماية الجنائية للتجارة الإلكترونية، رسالة ماجستير، جامعة الجزائر١، ٢٠١٥م ، ص٨٣، أ/ سامية عبد الرازق: جريمة اختراق أنظمة المعلومات، جامعة البصرة، مجلة العلوم القانونية، مج١٥،ع١، ٢٠١٠م،هامش، ص٢٩.

(٢) عرف البعض الاختراق بأنه أي دخول غير مصرح به إلى نظام معلوماتي (د/ أسامة العبيدي: مرجع سابق، ص١٣، د/ حسن مظفر: الأمن المعلوماتي، معالجة قانونية أولية، مجلة الأمن والقانون، أكاديمية شرطة دبي، مج١٢، ع١، يناير ٢٠٠٤م، ود/ خالد ممدوح إبراهيم: مرجع سابق،ص١٦٦)، وفي ذلك تسوية بين الدخول والاختراق؛ لكن الاختراق أحد صور الدخول؛ ومعناه دخول نظام محمي تقنيـًا، بكسر أو اقتحام جدار الحماية، أما الدخول فهو أعم؛ إذ يعني الولوج إلى نظام محمي أو غير محمي.

(٣) أ/ منصور بن سعيد القحطاني: مهددات الأمن المعلوماتي وسبل مواجهتها، دراسة مسحية على منسوبي مركز الحاسب الآلي بالقوات البحرية الملكية السعودية بالرياض، رسالة ماجستير، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية،٢٠٠٨، ص٣٤.

(٤) د/ عزيزة رابحي: مرجع سابق، ص ١١٢.

الاطلاع على البيانات أو المعلومات التي ظهرت على شاشة نظام معلوماتي، أو في صورة مخرجات لا يعد دخولاً مجرمـًا، ولا يعد دخولاً مجرد إرسال رسالة الكترونية خاصة لشخص ما تحتوي على فيرس[١].

وقد ذهب البعض إلى أن مجرد تشغيل الحاسوب يعد دخولاً غير مشروع[٢]؛ بيد أنه لا يمكن التسليم بذلك؛ إذ إن الدخول يتطلب انتقالاً وولوجـًا إلى داخل النظام، كما أن الحاسوب قد يكون في وضح محمي رغم تشغيله، ومن ثم فإن مجرد تشغيل الحاسوب لا يتجاوز العمل التحضيري.

كما ذهب البعض إلى أن الدخول يبدأ من اللحظة التي يصبح فيها الفاعل قادراً على الاطلاع البصري، أو السمعي على محتويات النظام[٣]، ولا يمكن التسليم بهذا الرأي أيضـًا؛ فقد ينتقل الفاعل إلى داخل النظام بالفعل لكن يفشل في الاطلاع على بيانات أو معلومات النظام لسبب أو لآخر، فلا ينفي ذلك تحقق الدخول غير المشروع.

ولا يقصد بالدخول مدلوله المادي إنما مدلوله المعنوي كأفكار وعمليات ذهنية في نظام المعالجة [٤]، وحتى يتحقق الدخول يجب أن يحدث اتصال فعلي من قبل الجاني بالنظام[٥]، فلا تكفي محاولة إقامة الاتصال، فقد يجري المتهم عدة محاولات للاتصال بالنظام حال تخمينه كلمة السر، فلا يتوافر الدخول إلا بعد الوصول إلى كلمة المرور

---

(١) د/ محمد نصر محمد: مرجع سابق، ص٨١، د/ عبد الإله النوايسة : مرجع سابق، ص٣٥ .

(٢) د/ خالد ممدوح إبراهيم: مرجع سابق، ص١٧١.

(٣) أ/ وسيم طعمة: مرجع سابق، ص١٦٨.

(٤) أ/ سفيان سوير: مرجع سابق، ص٨٨، أ/ نسيمة جدي : مرجع سابق، ص٥١.

(٥) د/ سومية عكور: الجرائم المعلوماتية وطرق مواجهتها، ورقة علمية، الملتقى العلمي: الجرائم المستحدثة في ظل التغيرات والتحولات الإقليمية والدولية، كلية العلوم الاستراتيجية، عمان، الأردن، ٢-٤/ ٩/ ٢٠١٤م، ص٥.

والولوج إلى النظام؛ إذ تقوم الجريمة بفعل الدخول الذي يطلق عليه الدخول المنطقي logical access، مما يوصل إلى نظام الحاسب بمكوناته المنطقية[١].

ويمكن تعريف الدخول غير المشروع بأنه :" كل نشاط يفضي إلى التسلل أو الولوج إلى النظام المعلوماتي أو جزء منه، دون حق أو ترخيص ممن يملك السماح بذلك، أو دون استيفاء شروط الدخول".

**ثانيـًا- وسائل الدخول غير المشروع**

تتعدد الوسائل والطرق التي يمكن من خلالها دخول الأنظمة المعلوماتية[٢]، فقد لا يتطلب الدخول أكثر من تشغيل الحاسب الآلي، أو فتح البرنامج الذي يقوم بتشغيله[٣]، وقد يحتاج إلى وسائل أو برامج تقنية مصممة خصيصـًا لذلك، وقد أكدت بعض قوانين مكافحة جرائم تقنية المعلومات صراحةً على تجريم الدخول غير المشروع أيـًا كانت وسيلته، كالقانون الأردني، وأكد بعضها على تجريم الدخول سواءً كان بطريقة مباشرة، أم غير مباشرة.

ويمكن أن يتم الدخول عن طريق الاتصال بالنظام، والاتصال يفترض نشاطـًا من قبل المتهم، كسرقة كلمة مرور، أو خيانة الأمانة[٤]، أو استخدام حصان طروادة[٥]، لكن لا

---

(١) د/ أسامة العبيدي: مرجع سابق، ص١٦.

(٢) د/ إبراهيم داود، د/ أشرف شعت: الاطلاع على البريد الالكتروني بين متطلبات النظام العام والحق في سرية المراسلة، مجلة دفاتر السياسة والقانون، ع١٦، يناير ٢٠١٧م، ص ٢٩، د/ خالد ممدوح إبراهيم: مرجع سابق، ص١٧١.

(٣) د/ أسامة العبيدي: مرجع سابق، ص١١.

(4) Romain Boos: op. cit., p.82.

(٥) أدانت محكمة جنح Nanterre متهم مقيم في المغرب ارتكب عدة جرائم دخول احتيالي، أشهرها دخوله إلى النظام المعلوماتي لشركة Greenpeace، وثبت أنه كان يستخدم برامج من نمط حصان طروادة للتحكم عن بعد في أنظمة عمل الكمبيوتر، ويثبت برامج تسجل ضربات المفاتيح، فيستعيد كلمات المرور، ويدخل بها،

يشترط أن يتم الدخول بوسيلة معينة؛ فكل الوسائل سواء[١]، فقد جاءت نصوص تجريم الدخول غير المشروع غير مرهونة بوسيلة معينة للدخول[٢]؛ إذ تقع الجريمة في كل حالة يكون فيها الدخول مخالفـًا للشروط التي وضعها القانون، أو الاتفاق، أو بمخالفة إرادة المتحكم في النظام الذي تم الدخول إليه، كوضع نظام للدفع لقاء الدخول، فيعمد الجاني لإيجاد وسيلة للاستفادة منه دون الدفع، ودون إرادة مالكه، وتتعدد وسائل الدخول غير المشروع، كالبرامج المخصصة لتخطي أنظمة الحماية الفنية، وأبواب المصيدة، والمختصرات، وطريقة القناع[٣].

ويمكن أن يتم الدخول عن طريق كود، أو شفرة تم الحصول عليها عن طريق الاحتيال، أو عن طريق الاستفادة من نقاط ضعف في النظام الأمني[٤]، وقد يتم الدخول عن طريق تخمين كلمات المرور، اعتماداً على معرفة بعض بيانات المستخدم، أو عن طريق برامج الكترونية تخمن المطلوب لمليارات المرات في ثوان معدودة، أو عن طريق برنامج Keylogger، وهو برنامج يسجل ما يكتبه المستخدم على نظامه، ولو كان سريـًا

---

وقد أدانته المحكمة، وأدانت مدير وكالة الاستخبارات الاقتصادية الذي استخدم هذا المخترق لصالح شركة كهرباء فرنسا، كما أدينت هذه الأخيرة لاشتراكها معهم واخفائها الجريمة.

- Christiane Féral-Schuhl: L'accès frauduleux au système d'information de Greenpeace puni , Expériences , Juridique , 2012 , article disponible sur le site : http://www.feral-avocats.com/wp-content/uploads/2013/09/01info06022012.pdf. et voi:
- Tribunal correctionnel de Nanterre Jugement du 10 novembre 2011.

❖https://www.legalis.net/jurisprudences/tribunal-correctionnel-denanterre-jugement-du-10-novembre-2011/

(١) د/ عبد الإله النوايسة: مرجع سابق، ص٣٥.

(٢) د/ محمد مزاولي: مرجع سابق، ص٤٤.

(٣) أ/ نسيمة جدي: مرجع سابق، ص٥١.

(4) Ibtissem Maalaoui: op. cit., p.27.

ثم يرسله إلى المتطفل[١]، ومن بين ما يرسله كلمات المرور. ويتحقق الدخول غير المشروع من أي شخص أيـًا كانت صفته، وسواءً كان يعمل في مجال معالجة النظام أم لا[٢]، يستوي كون النظام محمي من عدمه، وكون الدخول قد تحقق مباشرةً بمجرد فتح الحاسب أو النظام، أم بطريق غير مباشر[٣] بفك رمز المرور، أو تخمينه، كما يستوي أن يكون الدخول بدافع وهدف معين، أو لمجرد الفضول، وبغض النظر عن محتوى النظام المعلوماتي، سواءً تضمن معلومات شخصية، أو عامة، وسواءً ترتب عليه ضرر أم لا[٤].

ولا يشترط لتمام النشاط الإجرامي في هذه الجريمة وصول الجاني إلى بيانات، أو معلومات أو برامج، بل يكفي مجرد الدخول غير المشروع، وهذا هو الاتجاه التشريعي الغالب[٥]؛ إذ يعاقب على هذه الجريمة حتى في غياب الضرر؛ لأن الضرر لا يمثل جزءً من الأركان المكونة لها[٦]؛ لكن بعض التشريعات تشترط الوصول إلى المعلومات بالنظام، كالتشريع الأمريكي[٧].

وتعد جريمة الدخول غير المشروع إلى الأنظمة المعلوماتية من الجرائم الوقتية[٨]؛ إذ يتم ارتكابها في وقت قصير، ومجرد محاولة الدخول معاقب عليه باعتباره شروع – كما

---

(1) BREGANT, Jessica; BREGANT, Robert: op. cit., p.2.

(٢) د/ صالح شنن: مرجع سابق، ص٧٦.

(٣) د/ سومية عكور: مرجع سابق، ص٥.

(٤) أ/ نسيمة جدي : مرجع سابق، ص٥٢.

(٥) د/ أسامة العبيدي: مرجع سابق، ص١٦.

(6) Frédérique CHOPIN: Cybercriminalité , Répertoire de droit pénal et de procédure pénale , DALLOZ, 2013, p.10.

(7) WANG, Q: op. cit., p.127.

(٨) أ/ حمودي ناصر: مرجع سابق، ص٨١.

يرى البعض- وفقًا للمادة ٣٢٣-٧ من قانون العقوبات[١]، وتبقى من الجرائم الوقتية سواءً كان التجريم لمجرد الدخول، أم كان مشروطًا بتحقق نتيجة إجرامية، وقد يكون الدخول جريمة متتابعة الأفعال[٢]عندما يتم الدخول إلى نظام ثم الدخول إلى مواقع متفرعة منه؛ إذ يتكرر السلوك الإجرامي على ذات الحق المعتدى عليه لذات الغرض الإجرامي[٣].

وقد ذهب البعض إلى أنه يجب النص صراحة على تجريم الدخول ولو اقتصر على جزء من النظام[٤]، ويبدو لي أنه لا حاجة إلى ذلك؛ وأن النص على ذلك في أي تشريع يعد من قبيل التزيد؛ ذلك أن الدخول إلى جزء من النظام المعلوماتي أو ما في حكمه يعد دخولاً إلى النظام المعلوماتي، إذ لا يعقل – قياسا- أن يشترط لتحقق الدخول إلى منزل ما أن يدخل المتهم جميع طوابقه وغرفه، بل يتحقق الدخول بالوصول إلى أي جزء منه، كما أن المشرع لم يرهن الدخول بالنظام المعلوماتي كله حتى يمكن القول أن الدخول لجزء منه غير مجرم، أيضًا علة التجريم تقتضي حماية كل جزء من النظام دون حاجة إلى النص على ذلك، وكل اعتداء على جزء من النظام هو اعتداء على النظام كله.

**ثالثًا- مدى تصور الشروع في جريمة الدخول غير المشروع**: يرى البعض أن الشروع في الدخول غير المشروع معاقب عليه[٥]، كما أن بعض قوانين مكافحة جرائم تقنية

(1) Frédérique CHOPIN : op. cit., p.10.

(٢) د/ عبد الإله النوايسة: مرجع سابق، ص٤٤.

(٣) أ/ نجاة عباوي: مرجع سابق، ص٢٨٤.

(٤) د/ إمام حسنين عطاالله: جرائم تقنية المعلومات في التشريعات والصكوك العربية، دار جامعة نايف للنشر، الرياض، ١٤٣٩هـ-٢٠١٧م، ص٥٣٤.

(٥) د/ إمام عطاالله: مرجع سابق، ص١٥٣، أ/ حمودي ناصر: مرجع سابق، ص٩٣، د/ دينا عبد العزيز فهمي: المسئولية الجنائية الناشئة عن اساءة استخدام مواقع التواصل الاجتماعي، بحث مقدم في المؤتمر العلمي الرابع لكلية الحقوق، جامعة طنطا، القانون والإعلام، ٢٣-٢٤ أبريل، ٢٠١٧م، ص٢٢.

المعلومات وضعت نصاً عاماً يعاقب على الشروع في الجرائم المعلوماتية بصفة عامة.

ويبدو لي أنه يجب التفرقة بين فرضين فيما يتعلق بالشروع في جرائم الدخول غير المشروع، أولهما أنه إذا كانت جريمة الدخول جريمة ذات نتيجة إجرامية فالشروع فيها متصور، كما هو الحال في القانون الأمريكي، أما الفرض الثاني فيتمثل فيما إذا كانت جريمة الدخول شكلية، أي لا نتيجة إجرامية فيها فالشروع فيها غير متصور ولا يعاقب عليه، وذلك للأسباب التالية:

١-إن فكرة الشروع تقوم على البدء في تنفيذ فعل لا تتحقق نتيجته الإجرامية لأسباب خارجة عن إرادة الجاني[1]، فإذا كان الدخول غير المشروع من الجرائم الشكلية التي لا يتطلب المشرع فيها نتيجة إجرامية، فلا يتصور فيها الشروع.

٢-إن فعل الدخول إلى الأنظمة المعلوماتية يتحقق في لحظة واحدة مهما سبقه من أفعال أخرى، وعلى ذلك فإما أن يتحقق الدخول فتكون الجريمة تامة، وإما ألا يتحقق فلا تقع الجريمة؛ فالدخول كفعل غير قابل للانقسام.

٣-أن وضع المشرع لنص عام يجرم الشروع في الجرائم المعلوماتية لا يعني بالضرورة أن كافة هذه الجرائم متصور فيها الشروع ومعاقب عليه، ولا أدل على ذلك من أن البقاء غير المشروع يدخل ضمن هذه الجرائم والمفترض أن يشمله نص العقاب على الشروع رغم أن البقاء لا يتصور فيه الشروع.

---

(١) الشروع وفقاً للمادة ٤٥ من قانون العقوبات المصري هو: "البدء فى تنفيذ فعل بقصد ارتكاب جناية أو جنحة إذا أوقف أو خاب أثره لأسباب لا دخل لإرادة الفاعل فيها" ، ووفقاً للمادة ٣٤ من قانون العقوبات الإماراتي هو: " البدء في تنفيذ فعل بقصد ارتكاب جريمة إذا أوقف أو خاب أثره لأسباب لا دخل لإرادة الجاني فيها".

٤-إن اتفاقية بودابست عندما وضعت نص يلزم الأطراف بتجريم الشروع حددت الجرائم التي يجرم الشروع فيها تحديداً دقيقاً، ولم يكن من بينها الدخول غير المشروع، وهو ما يعني أن واضعو الاتفاقية لم يغيب عن أذهانهم حينئذٍ أن الدخول غير المشروع لا يتصور فيه الشروع.

## الفرع الثاني
## عدم مشروعية الدخول

لا يكون الدخول إلى نظام معلوماتي أو ما في حكمه مجرماً إلا إذا لحقه وصف عدم المشروعية، وقد عبرت القوانين المقارنة عن ذلك بتعبيرات عدة، منها الدخول **غير المشروع**، والدخول غير **المصرح به**، **والوصول الاحتيالي أو بالغش**، والدخول **غير القانوني**؛ والدخول **بدون إذن**، والدخول **دون حق**؛ بيد أنها جميعاً تعني أن الدخول جاء علي غير إرادة صاحب النظام، ودون حق، ومن ثم يلزم تحليل وصف "عدم مشروعية الدخول".

إن توافر صفة عدم مشروعية الدخول يتطلب عنصرين، أولهما "عدم التصريح أو الترخيص بالدخول"، وثانيهما "تعمد أو نية الدخول"، ونظراً لأن موضع دراسة النية في الركن المعنوي؛ فنقصر دراستنا هنا على عنصر "عدم التصريح"، أي أن وجود التصريح ينتفي معه تجريم الدخول، ويقتضي ذلك بيان مفهوم التصريح بالدخول، ومصدره، وشكله، ومن يملكه.

**مضمون "عدم مشروعية" الدخول**: يرى البعض أن وصف الدخول بأنه غير مشروع، يقصد به أن يكون غير مصرح به من المتحكم في النظام، أو لم يستوفي شروط

الدخول، ككلمة سر، أو اشتراك ما. أو دفع مبلغ مالي[١]، أو كان النظام ممنوع الدخول إليه تمامـًا، وبمعنى آخر إذا وقع من شخص ليس له الحق في الدخول إلى النظام[٢]، أو حسبما عبرت عنه محكمة استئناف Douai الفرنسية أن الدخول يكون غير مشروع عندما لا يكون مأذونـًا به ممن يملك الإذن[٣]، إذ يفترض التجريم أن من يدخل إلى النظام المعلوماتي يدخل احتيالاً دون أن يكون له حق في ذلك، ودون تصريح[٤].

**مفهوم التصريح**: لم تعرف القوانين محل الدراسة التصريح؛ بينما عرفه القانون الأردني في مادته الثانية بأنه: "الإذن الممنوح من صاحب العلاقة إلى شخص أو أكثر أو للجمهور للدخول إلى أو استخدام نظام المعلومات أو موقع الكتروني أو الشبكة المعلوماتية بقصد الاطلاع أو إلغاء أو حذف أو إضافة أو تغيير أو إعادة نشر بيانات أو معلومات أو حجب الوصول إليها أو إيقاف عمل الأجهزة أو تغيير موقع الكتروني أو الغائه أو تعديل محتوياته".

**مصدر التصريح**: يفترض الركن المادي للجريمة أن المتهم قد دخل النظام المعلوماتي دون التقيد بشروط الاتصال القانونية، أو الاتفاقية، أو دون إرادة " المتحكم في النظام[٥]، فكل دخول يتم من قبل شخص غير مخول للوصول إلى النظام المعلوماتي، أو غير مسموح له بالوصول إليه بالطريقة التي حدث بها يعد دخولاً مجرمـًا[٦]. وإن كانت

---

(١) أ/ سامية عبد الرازق: مرجع سابق، ص١٨.

(2) Cour d'appel de Toulouse, 21 janv. 1999.( cité par: Belkasem Hamid, Loi Godfrain: etat de la jurisprudence francais , p17).
❖https://sites.google.com/site/cyberhamid2/loi-godfrain-etat-de-la-jurisprudence-francaise

(3) Cour d'appel de Douai, 7 oct. 1992. ( cité par: Ibtissem Maalaoui: op. cit., p.27).

(4) Romain Boos :op. cit., p.67.

(5) Jacques Francillon: op. citp.99

(6) Romain Boos : op. cit., p.82.

قوانين مكافحة جرائم تقنية المعلومات لم تحدد مصدر التصريح، بيد أنه وفقاً للقواعد العامة قد يكون مصدر التصريح الشخص المتحكم في النظام، سواءً كان طبيعياً أو اعتبارياً. وقد يكون القانون هو مصدر التصريح، وذلك في الحالات التي يسمح فيها لأشخاص بصفاتهم دخول نظام معين لاتخاذ إجراء قانوني، كرجال الضبط الجنائي في الحالات التي يجوز لهم فيها ذلك(١).

**شكل التصريح**: لا يوجد شكل محدد للتصريح بالدخول، ومن ثم يستوي أن يكون مكتوباً، أو شفهياً، ويستوي كونه صادراً لشخص ما، أو فئة ما، وقد يكون صريحاً أو ضمنياً، وعلى ذلك فإن أية صيغة كتابةً، أو شفاهةً تصلح كإذن للدخول، ولا يشترط سوى أن تكون صادرة من المتحكم في النظام أو من فوضه، أو يكون مصدرها نص قانوني، وأن تكون هذه الصيغة تعبر عن الإذن لشخص ما بدخول هذا النظام، كما لو وضع شروط معينة لدخول نظامه، كأن يدفع مبلغ مالي، أو يقوم بإجراءات معينة. وإذا كان عدم وجود التصريح يعني أن الدخول غير مشروع؛ فإنه ومن باب أولي يكون الدخول مجرماً عندما يتم من قبل شخص تعهد بعدم الدخول على النظام. فقد قضي بأن دخول بعض الطلاب على الخادم(السيرفر) الخاص بجامعتهم انتهاكاً لميثاق المعلوماتية الموقع منهم يعد دخولاً مجرماً(٢).

ويشترط في التصريح أن يكون سابقاً على الدخول وإلا كان الدخول مجرماً(٣)، ومن

---

(١) د/ إبراهيم داود، د/ أشرف شعت: مرجع سابق، ص٣٨ وما بعدها.

(2) TGI Vannes, 13 juill. 2005.
❖(REVUE DE DROIT DES TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION, RDTIC n° 49 janvier 2006, p.39)

(٣) د/ إمام حسنين عطاالله: مرجع سابق، ص١٤٦.

ثم فإن الإذن اللاحق على الدخول لا ينفي الجريمة.

**المأذون له بالدخول**: يفترض التصريح أن الدخول قاصر على المتحكم في النظام أو فئة معينة، ومن ثم فإن المأذون له بالدخول يعد من الغير بالنسبة لمن لهم حق دخول النظام، أما إذا كان دخول النظام ليس قاصراً على صاحبه أو فئة محددة فإنه يكون متاحـًا للجمهور، ومن ثم فلا يعد دخول أي شخص إليه مجرمـًا، كذلك إذا كان من دخل النظام ممن ينتمون إلى الفئة المسموح لها بالدخول قانونـًا أو استوفي شروطه فلا يعد دخوله مجرمـًا.

وعلى ذلك؛ فإن غياب التعبير عن إرادة تقييد الدخول إلى النظام من قبل المسئول عنه لا تقع معه جريمة الدخول غير المشروع[1]، ومن ثم فلا تقوم المسئولية الجنائية وفقـًا للمادة ٣٢٣-١ من القانون الفرنسي إذا تم الدخول عن طريق استخدام برنامج متصفح عام[2]، ولا تقوم كذلك إذا كان الدخول من قبل شخص له سلطة الوصول إلى البيانات في نظام الكمبيوتر الخاص بالشركة التي يعمل بها[3]، بينما قضي بأن استخدام المتهم أرقام بطاقات ليست له لدخول شبكة فرانس تليكوم للحصول على خدمات الاتصالات يعد دخولاً مجرمـًا[4].

وقد قضت إحدى محاكم الجنح بإدانة متهم بالدخول الاحتيالي إلى نظام معالجة بيانات شخصية رغم أن الشركة المسؤولة عن النظام لم تتخذ الاحتياطات والتدابير

(1) T. corr., Paris, 8 décembre 1997, Gaz. Pal., [1998], chron. crim.
(2) CA, Paris, 30 oct. 2002 :
❖https://www.legalis.net/jurisprudences/cour-dappel-de-paris-12eme-chambre-section-a-arret-du-30-octobre-2002/
(3) Grenoble,4 mai 2000: Juris-Data n°122622, en ligne: http://www.lexisnexis.com.
(4) TGI Paris, 26 juin 1995, LPA 1er mars 1996, p. 4.

اللازمة لحماية هذه البيانات، واعتبرت أن ذلك ليس عذراً للمتهم[١]؛ إلا أن محكمة الاستئناف ألغت هذا الحكم بسبب نقص الحماية وعدم الإشارة إلى سرية هذه المعلومات[٢].

ولا تثور مشكلة في حالة الدخول غير المشروع من قبل أشخاص من خارج الجهة التي يوجد بها النظام، إذ يعد دخولاً مجرمـًا؛ إلا إن المشكلة قد تثور في حالة الدخول من قبل العاملين في الجهة التي يوجد بها النظام المعلوماتي، ففي هذه الحالة يتجاوز العامل الصلاحيات الممنوحة له، ولذلك يجب تحديد صلاحيات العاملين فيما يتعلق باستخدام الأنظمة المعلوماتية في جهات عملهم تحديداً دقيقـًا[٣]، وقد اختلفت المحاكم الأمريكية في ذلك فبعض المحاكم طبقت الجريمة على العاملين المصرح لهم بالدخول حال دخولهم بطريقة تخالف أحكام وشروط التصريح، أو دخولهم لأغراض غير مصرح بها، وبعض المحاكم لم تطبق الجريمة إلا على من لا يملكون تصريحـًا على الإطلاق[٤].

**تجاوز حدود التصريح**: جرم المشرع المصري تجاوز حدود التصريح أو الحق في الدخول بنص خاص؛ حيث تنص المادة الخامسة عشرة من القانون على أن: " يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن ثلاثين ألف جنيه ولا تجاوز

(1) Tribunal de Grande Instance de Paris 13th Chamber of 13 February ،2002. (https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-paris-13eme-chambre-jugement-du-13-fevrier-2002/)

(2) CA, Paris, 30 oct. 2002.

(٣) د/ أسامة العبيدي: مرجع سابق، ص١٣.

(4) Charles Doyle: Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws, Congressional Research Service , October 15, 2014, p.16.

خمسين ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل إلى موقع أو حساب خاص أو نظام معلوماتي مستخدماً حقاً مخولاً له، فتعدى حدود هذا الحق من حيث الزمان، أو مستوى الدخول"، أما المشرع الإماراتي فقد اعتبر تجاوز حدود التصريح صورة من صور الدخول غير المشروع، حيث جرمهما وعاقب عليهما بنص واحد، أما المشرع الفرنسي، والمنظم السعودي فلم يجرما تجاوز حدود الدخول المصرح به، ويترتب على ذلك أنه حال تجاوز حدود الدخول في النظام الفرنسي؛ فإن الفعل يشكل جريمة البقاء غير المشروع، وإذا حدث هذا التجاوز في النظام السعودي؛ فإن ذلك يظهر حاجة النظام السعودي إلى تجريم البقاء غير المشروع، أو تجاوز حدود الدخول المصرح به.

وقد يكون التصريح بالدخول غير مشروط بوقت أو عدد مرات للدخول، أو استكمال إجراءات أخرى، وفي هذه الحالة لا تثور مشكلة، وقد يكون التصريح بالدخول مقيداً بوقت معين، أو عدد مرات للدخول[1]، أو مرهوناً بإجراءات تسبقه، وقد يكون هذا التقييد صريحاً. وقد يكون ضمنياً يستفاد من طبيعة علاقة بين المأذون له بالدخول وبين النظام، أو من طبيعة الإذن ذاته، وحتى يكون الدخول غير مجرم يجب أن يكون قد تم في نطاق وحدود التصريح، وإن كان منح التصريح له قد تم بناءً على صفة معينة فيه وجب أن تكون هذه الصفة أيضاً قائمة وقت الدخول، وإن كان التصريح لدخول جزء معين أو لبعض البيانات أو المعلومات أو بعض البرامج وجب الالتزام بهذه الحدود وإلا عد ذلك دخولاً مجرماً في النظام الإماراتي، وبقاءً غير مشروع في النظام الفرنسي،

(1) Jacques Francillon: op. cit. , p.99

وتجاوزاً لحدود الدخول في النظام المصري.

وقد قضت محكمة تولوز الفرنسية بأن نسيان أو عدم الغاء كود الدخول الخاص بالموظف بعد فصله لا يمثل ترخيصاً ضمنياً له من جانب صاحب النظام بالاستمرار في الدخول إلى نظام الشركة، ومن ثم فإن دخوله بعد فصله، بهذا الكود يعد دخولاً احتيالياً[١]، وقضي بأن الإذن بالدخول لمرة واحدة على سبيل التجربة لا ينفي جريمة الدخول الاحتيالي إذا استمر المتهم في الدخول بعد ذلك بناءً على كلمة المرور التي أدخلت من قبل[٢].

## المطلب الثالث
## أحكام الركن المعنوي المشتركة بين جرائم الدخول

يكتسب الركن المعنوي أهمية فائقة في جرائم الدخول غير المشروع[٣]، ذلك أن قوانين مكافحة جرائم تقنية المعلومات جرمت فقط الدخول العمدي، ولم تجرم الدخول بالخطأ[٤]، وتنقسم أحكام الركن المعنوي إلى قسمين، قسم منها يمثل أحكاماً مشتركة بين كافة جرائم الدخول غير المشروع، وقسم آخر يمثل أحكاماً خاصة ببعض الجرائم دون بعضها؛ لذلك نرجئ الأحكام الخاصة عند الحديث عن صور الدخول غير المشروع، ونعرض في هذا المطلب للأحكام المشتركة، على النحو التالي:

### الفرع الأول
### صورة الركن المعنوي في جرائم الدخول غير المشروع

جرم المشرع المصري الدخول غير المشروع في صورة العمد؛ كما جرم الدخول إذا

(1) T. corr., 3e ch., Toulouse, 21 janvier 1999.
(2) Cass.Crim. 3 octobre 2007, n° 07-81.045
❖https://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000017917792
(3) Romain Boos :op. cit., p.68.

(٤) أ/ سفيان سوير: مرجع سابق، ص٨٥.

تم بالخطأ شرط البقاء بغير حق في النظام الذي دخله بالخطأ، حيث نص في المادة الرابعة عشرة على أن: "يعاقب.....كل من دخل عمداً، أو دخل بخطأ غير عمدي وبقي بدون وجه حق على موقع أو....."، ويتضح من النص أن المشرع المصري أفصح عن صورة الركن المعنوي في جريمة الدخول غير المشروع وهي العمد أو القصد، أما الدخول بالخطأ فلا جريمة فيه إلا إذا اقترن بالبقاء غير المشروع، ويبدو أن المشرع المصري آثر تجريم البقاء غير المشروع بطريقة تختلف عن التشريعات التي جرمته بنصوص مستقلة؛ حيث جعل البقاء بغير حق جريمة إذا تم عقب دخول بالخطأ، كما جرمه إذا تم بعد دخول مشروع بموجب نص المادة الخامسة عشرة، والتي جرمت الدخول بحق حال تعدي حدود هذا الحق من حيث الزمان، أو مستوى الدخول.

أيضـًا أفصح المنظم السعودي عن صورة الركن المعنوي لجرائم الدخول غير المشروع؛ حيث عرف الدخول غير المشروع بأنه: " دخول شخص بطريقة متعمدة إلى..."، وكذلك المشرع الفرنسي؛ حيث وصف الدخول بأنه احتيالي، أو بالغش[1]، ولن يكون الدخول بالاحتيال، أو الغش، إلا إذا كان عمداً. فلم يعاقب القانون الفرنسي على الدخول إلى النظام عن طريق الخطأ، خاصة إذا خرج المتهم فور علمه بدخوله الخاطئ؛ أما إذا بقي رغم علمه بعدم مشروعية دخوله فقد يسأل عن البقاء غير المشروع في النظام[2]، فالخطأ التقني الذي يؤدي إلى الدخول الخاطئ للمتهم في النظام وإن كان ينفي الدخول المجرم، لكنه لا ينفي عن الواقعة طابع البقاء غير المشروع إن استمر مع إدراكه بعدم حقه في البقاء[3]؛ أما المشرع الإماراتي فلم ينص صراحةً على صورة الركن

(1) Pradel, Jean: " op.cit., p. 824.
(2) Ibtissem Maalaoui: op. cit., p.34.
(3) Cécile Duhil de Bénazé : op. cit., p.3.

المعنوي. بيد أن الأصل في الجرائم أن تكون عمدية حال سكوت المشرع عن بيان صورة ركنها المعنوي[1].

**مدى الحاجة إلى تجريم الدخول عن طريق الخطأ**: يثور التساؤل في هذا المقام حول مدى كفاية تجريم الدخول العمدي، وبمعنى آخر هل توجد حاجة لتجريم الدخول عن طريق الخطأ؟.

بداءةً يمكن القول أن الدخول إلى الأنظمة المعلوماتية عن طريق الخطأ وارد ومتصور، وقد يكثر حدوثه في الواقع، وهذا النوع من الدخول إما يعقبه خروج مباشر فور علم المتدخل أن دخوله تم عن طريق الخطأ، وإما أن يروق الأمر للمتدخل ويظل بالنظام ولا يبادر بالخروج؛ لذلك فإن الحاجة إلى تجريم الدخول عن طريق الخطأ تتوقف على تجريم القانون للبقاء غير المشروع؛ فنفرق بين فئتين من القوانين:

**أولاً**- فئة القوانين التي تجرم البقاء غير المشروع، وهذه لا حاجة فيها إلى تجريم الدخول بالخطأ؛ لأن المتهم إذا خرج فوراً فلا حاجة لعقابه، وإذا لم يخرج من النظام سيخضع لجريمة البقاء غير المشروع، كالقانون الفرنسي.

**ثانيـًا**- فئة القوانين التي لا تجرم البقاء غير المشروع اكتفاءً بتجريم الدخول، وهذه تظهر فيها الحاجة إلى تجريم الدخول بالخطأ؛ لأنه قد يعقب هذا الدخول تجول في النظام وإطلاع على ما فيه من محتوى دون خضوع هذه الحالة لنص تجريم؛ رغم أنها أخطر من الدخول المجرد المتعمد، كالقانون الأردني الذي لم يجرم البقاء غير

(١) د/ خالد خلفان المنصوري: أركان الجريمة في القانون الجنائي الإنجليزي، أكاديمية شرطة دبي، مركز البحوث والدراسات، ط١ ، ٢٠٠٧، ص١٦٢ .

المشروع. وكذلك القانونين الكويتي والسعودي[1]، وقد تنبه المشرع المصري إلى ذلك فجرم البقاء غير المشروع إذا ترتب على دخول بالخطأ، وجرمه إذا ترتب على تجاوز حدود الدخول المشروع.

**نوع القصد الجنائي في جرائم الدخول غير المشروع:** اكتفت تشريعات تقنية المعلومات بالقصد العام في بعض الجرائم، كالدخول البسيط، وتطلبت في بعضها الآخر القصد الخاص، كجريمة الدخول بقصد الحصول على بيانات حكومية، وجريمة الدخول بقصد الإضرار بموقع الكتروني، ومن ثم فإن القصد العام قاسم مشترك بين كافة جرائم الدخول غير المشروع، أما القصد الخاص فهو متطلب في بعضها الآخر؛ ومنعاً للتكرار، نعرض في الفرع التالي للقصد العام المتطلب في كافة جرائم الدخول، وأما القصد الخاص فنعرض له عند تناول الجرائم المتطلب فيها.

## الفرع الثاني
## القصد العام في جرائم الدخول غير المشروع

القصد العام هو اتجاه إرادة الجاني إلى ارتكاب الجريمة مع العلم بأركانها وعناصرها القانونية[2]؛ ومن ثم أعرض في هذا الفرع لنطاق القصد، وعناصره، على النحو التالي:

**أولاً- نطاق القصد الجنائي في جرائم الدخول غير المشروع.**

نظراً للارتباط الوثيق بين ماديات الجريمة ومعنوياتها؛ فإن الركن المعنوي يتحدد

---

(١) د/ عبد الحليم بوقرين: قانون مكافحة جرائم تقنية المعلومات الكويتي، دراسة مقارنة، مجلة كلية القانون الكويتية العالمية، ع٤، س٥، ديسمبر ٢٠١٧م، ص٢٩٤.

(٢) د/ هلالي عبد اللاه أحمد: شرح قانون العقوبات، القسم العام، دار النهضة العربية، ط١، ١٩٨٧، رقم ٢٢٢، ص٢٢٦.

نطاقه دومـًا من خلال مكونات الركن المادي للجريمة، وإذا كانت جرائم الدخول غير المشروع تنتمي إلى طائفة الجرائم الشكلية التي ينهض ركنها المادي على السلوك الإجرامي، دون اشتراط تحقق نتيجة إجرامية؛ فإن القصد الجنائي في هذه الجرائم يضيق نطاقه ليتركز على السلوك الإجرامي دون النتيجة الإجرامية؛ لأنها خارج عناصر الركن المادي للجريمة، فلا يلزم اتجاه إرادة الجاني إليها، ولا يلزم توقعها، أو تصورها، أو العلم بها.

وضيق نطاق القصد على هذا النحو ما هو إلا تطبيق لقاعدة عامة مفادها أن القصد يتقلص في جرائم السلوك المجرد؛ ليوائم تكوينها، بحيث يحيط العلم بماهية السلوك الإجرامي، كما يحيط بمقدار ما ينطوي عليه هذا السلوك من طاقة كافية لتهديد المصلحة المحمية جنائيـًا، وبحيث تنصرف الإرادة إلى هذا السلوك فتستغرقه بمقوماته، ولا شأن للعلم والإرادة بالنتيجة، لأن هذه تخرج من نطاق النموذج القانوني للجريمة، ومن ثم فلا تدخل في بنيته[1].

**ثانيـًا- عناصر القصد العام في جرائم الدخول غير المشروع.**

تتطلب المسئولية الجنائية عن الدخول غير المشروع القصد العام، ومن ثم يجب التحقق من توافر عنصريه، وهما العلم، والإرادة، على النحو التالي:

١- **العلم**: ويتمثل في امتلاك الجاني القدر اللازم من المعلومات عن عناصر الجريمة، على الوجه الذي يحدده القانون[2]؛ ومن ثم يجب أن يعلم بكل العناصر التي تتكون

(١) د/ عبد الفتاح الصيفي: الأحكام العامة للنظام الجنائي في الشريعة الإسلامية والقانون، دار المطبوعات الجامعية، ٢٠١٣، رقم ٢٥٠، ص٢٩٦.

(٢) د/ عبود السراج: شرح قانون العقوبات، القسم العام، ج١، نظرية الجريمة، د.ت، د. ن، ص١٤٣.

منها الجريمة[١]، والعلم يسبق الإرادة، ولا يتصور وجود إرادة في مجال القانون دون علم، ومع ذلك فهناك بعض مقومات الجريمة يفترض القانون العلم بها، إذ يستوي علم المتهم أو جهله بها[٢].

فإذا طبقنا ذلك على التشريع الفرنسي نجده جرم في المادة ٣٢٣-١ الدخول بشكل احتيالي، وهذا الطابع الاحتيالي للدخول هو قوام الركن المعنوي؛ إذ يعني أن يكون المتهم قد ارتكب فعل الدخول طواعيةً، أي بشكل إرادي، وهو على علم تام بأنه يدخل نظام ليس له الحق في دخوله[٣]، ويفترض الطابع الاحتيالي للدخول المجرم إدراك المتهم لعدم قانونية تصرفه[٤]، وبأنه ينتهك إرادة المتحكم في النظام، أو دخل النظام على غير إرادته، أو بإرادته ولكنه تجاوز الإذن الممنوح له[٥]، ويمكن استخلاص هذه النية الاحتيالية من بعض القرائن، كانتهاكه للحماية الأمنية[٦]، أو إدراجه ملف تجسس، أو حصان طروادة، أو اتصال عن بعد بالنظام، أو بقائه في النظام[٧].

ويتطلب الركن المعنوي للدخول غير المشروع علم المتهم ببعض المقومات، أهمها:

**العلم بمحل الجريمة(النظام المعلوماتي)**: إذا كان الدخول المجرم لا يقع إلا على

---

(١) د/ محمود نجيب حسني: النظرية العامة للقصد الجنائي، دراسة تأصيلية مقارنة للركن المعنوي في الجرائم العمدية، دار النهضة العربية، ١٩٨٨، ص٥١.

(٢) د/ عبد الفتاح الصيفي : مرجع سابق ، رقم ٢٥٢ ، ص٢٩٦ .

(3) Ibtissem Maalaoui: op. cit., p.31.
(4) Frédérique CHOPIN : op. cit., p.9.
(5) Cass.Crim., 10 déc. 1998, N° 97-85867:
❖https://www.alain-bensoussan.com/wp-content/uploads/2014/05/30658011.pdf
(6) Christian Le Stanc: op. cit., p.2827
(7) Frédérique CHOPIN : op. cit., p.9.

نظام معلوماتي؛ فيجب أن يكون المتهم على وعي وإدراك بأن الدخول الذي يقوم به موجه إلى نظام معلوماتي؛ فإذا اعتقد بأنه غير ذلك انتفى لديه العلم، كما لو اعتقد أنه يتعامل مع برامج معروضة للبيع، أو مع حاسب لم يدخل الخدمة، أو على حاسب مودع بالمخازن، أو قطع غيار، أو أجهزة لا زالت في طور التجربة، أو أنظمة خرجت من الخدمة، أو غير ذلك مما يخرج عن مفهوم النظام المعلوماتي. والقانون هو الذي يحدد محل الدخول، ففي القانون الإنجليزي يجب أن يعلم المتهم أنه يدخل إلى البرامج أو البيانات أو المعلومات المخزنة في الحاسب[١].

وفي النظام السعودي يجب أن يدرك المتهم أنه يدخل على حاسب آلي، أو موقع الكتروني، أو نظام معلوماتي، أو شبكة حاسبات غير مصرح له بدخولها، وفي القانون الإماراتي يجب أن يعلم المتهم أن دخوله على موقع الكتروني، أو شبكة معلومات، أو وسيلة تقنية معلومات، وفي القانون المصري يجب أن يعلم المتهم أنه يدخل على موقع أو حساب خاص، أو نظام معلوماتي محظور الدخول عليه.

وتقع الجريمة طالما أن المتهم دخل نظامـًا ما سواءً كان النظام الذي يقصده بفعله أم لا، فقد يوجه نشاطه نحو نظام بعينه، وقد يوجه نشاطه بشكل عشوائي مستهدفـًا أي نظام معلوماتي ينجح في دخوله[٢]، إذ إن القانون يحمي كافة الأنظمة المعلوماتية.

**العلم بعدم مشروعية دخوله إلى النظام المعلوماتي:** يجب أن يدرك المتهم بأن سلوكه يستهدف نظام معلوماتي ليس له حق دخوله، وأنه لا يملك تصريحـًا بذلك.

(١) د/ سامي الرواشدة، د/ أحمد الهياجنة: مرجع سابق، ص١٢٩.

(٢) د/ أسامة العبيدي: مرجع سابق، ص٢٣.

أو على الأقل يكون على وعي وإدراك بأن دخوله النظام يتم دون استيفاء الشروط أو القيود المتطلبة لذلك؛ أي على غير إرادة صاحب المتحكم في النظام[1]؛ فإذا اعتقد المتهم أن له الحق في الدخول إلى النظام، أو أنه مصرحاً له بدخوله، أو أن الفئة التي ينتمي لها مصرح لها بالدخول، أو أن النظام متاح دخوله للجمهور، انتفى لديه القصد الجنائي. إذ يعد ذلك غلطاً في الواقع ينفي قصده، مادام اعتقاده مبنياً على أسباب معقولة، وكذلك الأمر حال اعتقاده بوجود تصريح بالدخول على غير الحقيقة[2].

كذلك ينتفي العلم إذا جهل المتهم بزوال صفته التي تم السماح له بدخول النظام بناءً عليها، كما لو نقل من قسم إلى آخر داخل المؤسسة، ولم يكن قد أبلغ بالقرار، وظل يدخل النظام باعتباره منتمياً للقسم الذي تم نقله منه، فلا يتوافر لديه العلم، ولا يسأل، فإذا علم بزوال صفته لم يعد له حق الدخول كأصل عام، ولو لم تلغي الشركة حسابه أو تغير كلمة مروره.

**العلم بحقيقة سلوكه الإجرامي**: يقتضي توافر عنصر العلم لدى المتهم أن يدرك حقيقة فعله، وأن ما يقوم به يمثل وصولاً إلى نظام معلوماتي، أو تسللاً إليه، دون حق، ودون تصريح، أما إذا لم يدرك ذلك بأن وجد نفسه داخل نظام معلوماتي بالخطأ، ودون وعي؛ فلا يكتمل الركن المعنوي لانتفاء القصد، كما لو اعتاد المتهم أن يدخل على حسابه بمجرد فتح موقع المؤسسة التي يعمل بها وضغطه على مفتاح " ENTER" في نافذة الدخول نظراً لاعتياده على أن اسم الدخول وكلمة المرور محفوظان بالمتصفح، فإذا به يفاجأ بدخول صفحة زميل له بالعمل كان قد استخدم الحاسوب قبله على غير المعتاد.

---

(1) Jacques Francillon: op. cit. , p.99.

(٢) د/ إمام حسنين عطاالله: مرجع سابق، ص١٥١.

وقد قضي بأن وعي المتهم وإدراكه بأنه يستخدم خدمة مدفوعة بشكل مجاني من خلال نظام معلوماتي يتحقق به الركن المعنوي لجريمة الدخول الاحتيالي[١]، وذهبت بعض المحاكم الأمريكية إلى أن الخرق الواعي لشروط الخدمة يكفي لتشكيل الدخول عمداً إلى الأنظمة المعلوماتية[٢]. ولا يقبل من المتهم الدفع بعدم علمه بالقانون الذي يجرم الدخول غير المشروع، لأن العلم بقانون العقوبات والقوانين المكملة له علم مفترض.

٢- **الإرادة:** الإرادة "نشاط نفسي، يقتضي حرية تمثُل أمر وإبرازه إلى العالم الخارجي"[٣]، والارتباط بين السلوك الإجرامي والإرادة لا تنفصم عراه، يستوي في هذا أن يكون السلوك سلبي أم إيجابي[٤]، والقصد الجنائي يرتبط ارتباطاً وثيقاً بالإرادة، ويدور معها وجوداً وعدماً، لذا فإنه يترتب عليها وينتفي بانتفائها [٥]، والفعل دون إرادة ليس فعلاً، ولكنه خليط حركات مبعثرة، لا تربطها وحدة، ولا تجذبها غاية [٦]، فلا يكفي لتوافر المسئولية أن تكون الإرادة حرة؛ وإنما يلزم أن تكون آثمة، أي تعبر عن اتجاه الجاني نحو الانحراف عن السلوك الذي يتطلبه القانون[٧].

---

(1) Cass.Crim. 3 octobre 2007, n° 07-81.045 :
❖https://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000017917792

(2) Charles Doyle, Cybercrime: op. cit. , p.16.

(٣) د/ عبد المهيمن بكر سالم: القصد الجنائي في القانون المصري والمقارن، رسالة دكتوراه، ١٩٥٩م، رقم ١١٩، ص١٧٤.

(٤) د/ عبد الفتاح الصيفي: مرجع سابق، رقم ٢٢٩، ص٢٧٥ .

(٥) د/ عبد الله حسين حميده: مرجع سابق، ص٢٩٣.

(٦) د/ ختير مسعود: مرجع سابق، ص ٩٧ .

(٧) د/ رأفت جوهري: المسئولية الجنائية عن أعمال وسائل الإعلام، دار النهضة العربية، ٢٠١١م، ص٤١.

وعلى ذلك؛ فإن إرادة المتهم في جرائم الدخول غير المشروع يجب أن تتجه نحو الدخول إلى النظام المعلوماتي، بأن تسيطر إرادته على حركاته وأعضائه وتدفعها للقيام بالفعل الإيجابي اللازم للدخول إلى النظام، والوصول إليه، ولا يشترط اتجاه الإرادة نحو النتيجة الإجرامية باعتبار أن الدخول غير المشروع من الجرائم الشكلية التي لا تدخل النتيجة في بنيانها القانوني، فإذا دخل المتهم إلى النظام دون إرادة منه، أو بإرادة مشوبة بالإكراه، أو الخطأ فلا يتوافر القصد لانتفاء عنصر الإرادة.

ولا أثر للبواعث على قيام المسئولية الجنائية عن الجريمة. ولما كان الباعث على ارتكاب الجريمة ليس ركنا من أركانها، أو عنصراً من عناصرها، فلا يقدح في سلامة الحكم عدم بيان الباعث تفصيلاً، أو الخطأ فيه، أو ابتنائه على الظن [1]، فالباعث والغاية لا يحسبان بين عناصر القصد الجنائي، وإن كانا نبيلين فهما لا ينفيانه [2]، وقد أكدت محكمة استئناف روان الفرنسية أنه لا عبرة بالدوافع التي حركت المتهم لارتكاب جريمة الدخول الاحتيالي[3]، ويعد من قبيل الدوافع الدخول لكشف ثغرات الحماية التقنية، أو بسبب الفضول، أو الترفيه[4]، أو إظهار مهارة اختراق الأنظمة[5].

## المطلب الرابع
## الأحكام المشتركة في الجزاء الجنائي

تتمايز جرائم الدخول غير المشروع إلى الأنظمة المعلوماتية في العقوبات

---

(١) نقض جنائي : الطعن رقم ١٤٣١٨ لسنة ٧١ جلسة ٧/ ٣/ ٢٠٠٢ ، س ٥٣، ص ٣٩٧ ، الطعن رقم ١٢٧٥٤ لسنة ٨٢ جلسة ٢/ ٠٤/ ٢٠١٤ س ٦٥.

(٢) د/ رأفت جوهري رمضان: مرجع سابق، ص٣٦.

(3) Cour d'appel de Rouen,17mars 2005, Juris-Data n°291578.

(4) Christian Le Stanc, op. cit., p.2827

(٥) د/ أسامة العبيدي: مرجع سابق، ص١٢.

الأصلية؛ من حيث مدة الحبس أو مبلغ الغرامة، بيد أنه توجد بعض أحكام الجزاء المشتركة، ليس فقط بين جرائم الدخول، ولكن بين كافة جرائم تقنية المعلومات، ومن أهمها:

**تقرير عقوبة المصادرة:** تحكم المحكمة بمصادرة، الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أيٍ من الجرائم المنصوص عليها في هذا المرسوم بقانون أو الأموال المتحصلة منها، مع مراعاة حقوق الغير حسني النية(١)، والمصادرة وجوبية وفقـًا لنص المادة ٣٨ من قانون مكافحة جرائم تقنية المعلومات المصري، والمادة ٤١ من القانون الإماراتي، وجوازية وفقـًا للمادة ١٣ من النظام السعودي.

**إغلاق محل أو موقع ارتكاب الجريمة:** وفقـًا للمادة ٣٨/ ٢ من القانون المصري إذا أدين شخص اعتباري في جريمة معلوماتية، ولم يكن قد حصل على الترخيص المطلوب؛ فيحكم بإغلاقه، وتنص المادة ٤١ من قانون مكافحة جرائم تقنية المعلومات الإماراتي على أن :"يحكم بإغلاق المحل أو الموقع الذي يرتكب فيه أي من هذه الجرائم، وذلك إما إغلاقـًا كليـًا أو للمدة التي تقدرها المحكمة"، وقد جعل المشرع الحكم بالإغلاق وجوبي، لكنه ترك للمحكمة تقرير ما إذا كان الإغلاق مؤبداً، أم مؤقتـًا بمدة تحددها المحكمة. أما النظام السعودي فقد أجاز وفقـًا للمادة ١٣منه الحكم بإغلاق الموقع الإلكتروني، أو مكان تقديم الخدمة إذا كان مصدراً لارتكاب جريمة

(١) حقوق الغير حسن النية تشمل حق الملكية، والحقوق العينية كالانتفاع والرهن، أما الحقوق الشخصية فلا تحول دون المصادرة؛ لأن محلها ذمة المدين وليس ماله .( د/ محمد خليفة: الأحكام المشتركة لجرائم المعطيات في قانون العقوبات الجزائري والمقارن، مجلة التواصل في العلوم الإنسانية والاجتماعية، جامعة باجي مختار بعناية، الجزائر، ع٣٠، يونيو ٢٠١٢م، ص٩٦).

الدخول غير المشروع، وتم ارتكابها بعلم مالكه، وقد يكون الإغلاق مؤبداً، أو مؤقتاً.

**إبعاد الأجنبي**: وفقاً لنص المادة ٤٢ من القانون الإماراتي يتعين على المحكمة إذا حكمت على أجنبي بالإدانة في جريمة من جرائم تقنية المعلومات أن يتضمن حكمها إبعاده عن البلاد بعد تنفيذ العقوبة المحكوم به[١]؛ فالإبعاد هنا يعد عقوبة تكميلية وجوبية[٢].

أجاز المشرع المصري للمحكمة حال إدانتها لموظف عمومي في جريمة من جرائم تقنية المعلومات أثناء وبسبب تأدية وظيفته أن تعزله من وظيفته عزلاً مؤقتاً.

**المسئولية الجنائية للشخص المعنوي عن جرائم الدخول غير المشروع**: المشرع الفرنسي وفقاً للمادة ٣٢٣-٦ مساءلة الأشخاص المعنوية عن الجرائم المعلوماتية عامة، ومنها الدخول غير المشروع، وذلك في ضوء الأحكام العامة لمساءلة الأشخاص المعنوية وفقاً للمادة ١٢١/ ٢ من قانون العقوبات الفرنسي[٣]؛ أما المشرع الإماراتي فلم يتعرض للمسئولية الجنائية للأشخاص المعنوية في قانون مكافحة جرائم تقنية المعلومات. بيد أنه يقر هذه المسئولية بنص عام في قانون العقوبات الاتحادي[٤]، ومن

---

(١) حكم في الإمارات بحبس باكستاني شهرين وإبعاده عن البلاد بسبب ارتكابه دخولاً غير مشروع إلى نظام معلوماتي، ثم ألغت محكمة الاستئناف الإبعاد وأيدت الحبس، فقضت محكمة النقض بأن الحكم خالف القانون بما يوجب نقضه وتصحيحه بإضافة تدبير الإبعاد.(الطعن رقم ٤٠٢ لسنة ٢٠١٣م ، س٧ ق .أ، محكمة النقض، المكتب الفني، مجموعة الأحكام والمبادئ الصادرة عن الدائرة الجزائية، جلسة ٢٢/ ٥/ ٢٠١٣م، ج٢، ص٣٣٧. ( مشار إليه في: د/ إمام حسنين عطاالله: مرجع سابق، ص١٥٥).

(٢) د. عبد الإله محمد النوايسة : مرجع سابق، ص٦٩.

(3) PICOTTI, Lorenzo; SALVADORI, Ivan: op. cit., P.42.

(٤) د/ محمد سعيد عبد الرحمن: المسئولية الجنائية للأشخاص المعنوية في قانون العقوبات الاتحادي لدولة الإمارات العربية المتحدة، رسالة دكتوراه، جامعة القاهرة، ٢٠١٤م، ص٤٧.

ثم يخضع الشخص المعنوي للمسئولية الجنائية حال ارتكابه إحدى جرائم تقنية المعلومات، ومنها الدخول غير المشروع[1].

أما النظام السعودي فلم يخصص نصاً لتقرير المسؤولية الجنائية للأشخاص المعنوية عن جرائم تقنية المعلومات؛ بيد أنه بدأ نصوص التجريم والعقاب بعبارة " يعاقب ب...كل **شخص** يرتكب أياً من الجرائم المعلوماتية الآتية: ...، وقد عرف الشخص في مادته الأولى بأنه: " أي شخص ذي صفة طبيعية أو اعتبارية، عامة أو خاصة"، كما أن العقوبات المنصوص عليها في أغلب الجرائم كانت الغرامة إحداها، ومن ثم فإن صياغة النظام على هذا النحو يمكن من خلالها مساءلة الشخص المعنوي عن جرائم تقنية المعلومات.

أما المشرع المصري فقد ظل على موقفه التقليدي من المسئولية الجنائية للأشخاص المعنوية في قانون مكافحة جرائم تقنية المعلومات؛ حيث خصص الفصل السابع لهذا النوع من المسئولية، وقرر أنه حال ارتكاب الجريمة باسم ولحساب الشخص الاعتباري فإن الذي يعاقب هو المسئول عن الإدارة الفعلية لهذا الشخص، إذا ثبت

---

(١) تنص المادة ٦٥ من قانون العقوبات الاتحادي على أن: "الأشخاص الاعتبارية فيما عدا مصالح الحكومة ودوائرها الرسمية والهيئات والمؤسسات العامة، مسؤولة جنائياً عن الجرائم التي يرتكبها ممثلوها أو مديروها أو وكلاؤها لحسابها أو باسمها.

ولا يجوز الحكم عليها بغير الغرامة والمصادرة والتدابير الجنائية المقررة للجريمة قانوناً فإذا كان القانون يقرر للجريمة عقوبة أصلية غير الغرامة اقتصرت العقوبة على الغرامة التي لا يزيد حدها الأقصى على خمسين ألف درهم ولا يمنع ذلك من معاقب مرتكب الجريمة شخصياً بالعقوبات المقررة لها في القانون".

علمه بالجريمة، أو تسهيله ارتكابها، وإن كان قد أجاز للمحكمة الحكم بوقف ترخيص مزاولة الشخص الاعتباري لنشاطه مدة لا تزيد عن سنة، أو الحكم بإلغاء الترخيص أو حل الشخص الاعتباري حال العود.

# المبحث الثالث
# الأحكام الخاصة بجرائم الدخول غير المشروع

تعددت صور جريمة الدخول غير المشروع في قوانين مكافحة جرائم تقنية المعلومات، ولأنه سبق تناول الجوانب المشتركة بين هذه الجرائم أيـًا كانت صورتها؛ فإن الدراسة في هذا المبحث تقتصر على بيان الأحكام التي تختص بها كل جريمة من جرائم الدخول غير المشروع، والتي وتميزها عن غيرها، وذلك على النحو التالي:

## المطلب الأول
## جريمة الدخول البسيط

يقصد بجريمة الدخول البسيط الحالة التي يجرم فيها مجرد الدخول غير المشروع إلى نظام معلوماتي أو ما في حكمه دون قصد تحقيق نتيجة إجرامية. وتكمن علة تجريم الدخول البسيط في أنه ينطوي على مساس بحق المسئول على النظام في السيطرة عليه[١]؛ إذ يكون الدخول على غير إرادته، علاوةً على ما قد يترتب عليه من إضرار بالنظام، وإطلاع على بيانات ومعلومات لا يجوز له الاطلاع عليها.

وقد توافقت القوانين محل الدراسة على تجريم الدخول البسيط؛ حيث جرمه المشرع المصري بموجب المادة ١٤/ ١ من القانون، والمنظم السعودي بموجب المادة ٣/ ٣، والمشرع الإماراتي بموجب المادة ٢/ ١، والمشرع الفرنسي بموجب الفقرة الأولى من المادة ٣٢٣-١، والتي تنص على أن: " يعاقب على الوصول أو البقاء بطريقة احتيالية، في كل أو جزء من نظام آلي لمعالجة البيانات، بالسجن لمدة سنتين و ٦٠٠٠٠ يورو غرامة"[٢].

---

(١) د/ أسامة العبيدي: مرجع سابق، ص١٦.

(2) Code pénal français, Chapitre III : Des atteintes aux systèmes de traitement automatisé de

**أركان الجريمة**: لا يختلف البنيان القانوني لهذه الجريمة عما سبق تناوله في الأحكام المشتركة بين جرائم الدخول غير المشروع؛ إذ يجب أن يكون محلها نظام معلوماتي أو ما في حكمه مما لا يحق للمتهم دخوله. والركن المادي فيها قوامه السلوك الإجرامي، وهو مجرد الدخول، دون تطلب تحقق نتيجة إجرامية، والركن المعنوي يتخذ صورة القصد العام(١)، وذلك على النحو السابق بيانه(٢).

وتجدر الإشارة إلى أن المشرع المصري قد ألحق بهذه الجريمة جريمة أخرى هي جريمة البقاء دون وجه حق إذا نتج عن دخول بالخطأ، والمجرم هنا هو البقاء غير المشروع وليس الدخول، وقد ساوى بينهما في العقوبة، أما من دخل النظام دخولاً غير مشروع ثم تعدى حدود هذا الحق من حيث الزمان، أو مستوى الدخول فيسأل عن جريمة تجاوز حدود الحق في الدخول وفقاً للمادة ١٥ من القانون، وعقوبتها أقل من الدخول غير المشروع، والبقاء بدون حق الناتج عن الدخول بخطأ.

أما المشرع الإماراتي فقد جرم الدخول غير المشروع – بدون تصريح–، والبقاء غير المشروع، وتجاوز حدود الدخول بموجب نص واحد وسوى بينهما في العقوبات؛ وكذلك جرم المشرع الفرنسي الدخول بالغش أو الاحتيال، والبقاء غير المشروع وعاقب عليهما بنص واحد، ولم ينص على تجريم تجاوز حدود الدخول المصرح به.

---

données, Modifié par LOI n°2015-912 du 24 juillet 2015 - art. 4, Article 323-1: "Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende".

❖(https://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006418316&cidTexte=LEGITEXT000006070719)

(١) د/ شول ابن شهرة: مرجع سابق، ص٢٠٦.

(٢) يراجع مبحث الأحكام المشتركة من هذ البحث: ص١٢ وما بعدها.

لذلك قضت محكمة النقض الفرنسية بتوافر الدخول الاحتيالي بشأن متهم كان لديه ترخيص بالدخول إلى نظام معلوماتي لمرة واحدة على سبيل التجربة، ثم ظل لمدة عامين يدخل على النظام ويستفيد منه مستغلاً كلمة المرور التي تم تسجيلها عند الدخول المجاني؛ إذ كان يجب عليه بعد المرة الأولى أن يدفع مقابل الخدمة(١).

ويلاحظ أن النظام السعودي جرم الدخول غير المشروع في صورته البسيطة حال وقوعه على موقع الكتروني، وأغفل تجريمه حال وقوعه على المفردات الأخرى التي تضمنها تعريف الدخول غير المشروع، وهي الحواسب الآلية، وشبكاتها، والأنظمة المعلوماتية، أيضـًا لم يجرم تجاوز حدود الدخول المشروع، ولا البقاء غير المشروع، ومن ثم فإن من يدخل نظامـًا معلوماتيـًا بالخطأ، أي دون قصد فلا يسأل وفقـًا للنظام السعودي ولو بقي في النظام عقب هذا الدخول، ومن يدخل نظام معلوماتي دخولاً مشروعـًا ويتجاوز حدود هذا الدخول فلا يسأل؛ وذلك تطبيقـًا لمبدأ شرعية الجرائم والعقوبات؛ وعلى ذلك فقد يكون من الملائم تجريم النظام السعودي للبقاء غير المشروع، وإعادة صياغة نص تجريم الدخول البسيط ليشمل محله الأنظمة المعلوماتية وما في حكمها من مفردات أخرى.

ويبدو لي أن الأفضل الاكتفاء بتجريم البقاء غير المشروع في القانونين المصري والإماراتي، ذلك أن تجريم البقاء غير المشروع يشمل كل بقاء في الأنظمة المعلوماتية دون حق، سواءً كان ناتجـًا عن دخول بالخطأ، أو ناتجـًا عن تجاوز حدود الدخول المشروع، وهو ما انتهجه المشرع الفرنسي.

**العقوبة**: علاوة على الجزاءات التي تشترك فيها جريمة الدخول غير المشروع مع باقي جرائم تقنية المعلومات، كالمصادرة، والإبعاد، والإغلاق، فقد عاقب عليها

(1) Cass.Crim. 3 octobre 2007, n° 07-81.045.

المشرع المصري بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه، ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، وعاقب المشرع الإماراتي عليها بالحبس مدة لا تقل عن شهر ولا تزيد عن ثلاث سنوات والغرامة[1]التي لا تقل عن مائة ألف درهم ولا تزيد عن ثلاثمائة ألف درهم، أو بإحدى هاتين العقوبتين، وعاقب المشرع السعودي على الدخول البسيط إلى موقع الكتروني بالسجن مدة لا تزيد عن سنة وغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين؛ أما المشرع الفرنسي فقد عاقب على هذه الجريمة ، بالسجن لمدة سنتين و ٦٠٠٠٠ يورو غرامة.

**تشديد عقوبة الدخول البسيط**: شددت بعض قوانين مكافحة جرائم تقنية المعلومات عقوبة جريمة الدخول البسيط في حالات معينة، على النحو التالي:

**أولاً-إذا ترتب على الدخول غير المشروع ضرر أو تخريب**: شدد القانون المصري عقوبة الدخول البسيط وفقـًا للمادة ١٤/ ٢ إذا نتج عن الدخول غير المشروع **إتلاف،** أو **محو،** أو **تغيير،** أو **نسخ،** أو **إعادة نشر** للبيانات أو المعلومات الموجودة بالنظام المعلوماتي أو ما في حكمه، ووفقـًا للمادة ٢/ ٢ من القانون الإماراتي تشدد العقوبة إذا ترتب على الدخول إضرار أو مساس بأي بيانات أو معلومات، وقد أورد المشرع صور هذا الإضرار، وهي: **إلغاء،** أو **حذف،** أو **تدمير**[2]، أو **إفشاء،** أو **إتلاف،** أو **تغيير**[3]،

---

(١) يلاحظ أن التشريعات العربية نصت على الغرامة كعقوبة تخييرية مع الحبس في جرائم الدخول المجرد، عدا المشرع السوري الذي عاقب عليها بالغرامة فقط (د/ إمام حسنين عطاالله: مرجع سابق، ص١٤٦) .

(٢) تغيير البيانات عبر عنه المشرع الفرنسي بتعديل المعطيات ويعني استبدالها المعطيات داخل النظام بمعطيات أخرى.

(٣) يقصد بتدمير المعلومات إتلافها أو محوها، والإتلاف يعني إفناء مادة الشيء أو إدخال تغييرات شاملة عليه فيصبح غير صالح للاستعمال لما خصص من أجله.(أ/ سامية عبد الرازق: مرجع سابق، ص١٧).

أو **نسخ**، أو **نشر**، أو **إعادة نشر** بيان، أو معلومة، ويعني ذلك أنه إذا وقف الأمر عند حد دخول المتهم للنظام المعلوماتي خضع للمسئولية عن الدخول البسيط، أما إذا ترتب أي إضرار بأي بيان أو معلومة، سواءً بالحذف، أو التدمير، أو النشر أو غير ذلك مما ورد بالنص شددت العقوبة على المتهم.

وتنص الفقرة الثانية من المادة ٣٢٣-١ من قانون العقوبات الفرنسي على أنه: " وعندما ينتج عن ذلك **حذف** أو **تعديل البيانات** الواردة في النظام، أو **تغيير في تشغيل هذا النظام**، فإن العقوبة تكون السجن لمدة ثلاث سنوات وغرامة قدرها ١٠٠٠٠٠ يورو"[(١)].

ومفاد النص السابق أن المشرع الفرنسي شدد عقوبة الدخول البسيط إذا ترتب عليه تعديل في البيانات، أو إزالتها، أو تغيير في طريقة عمل النظام، إذا كان هذا التخريب غير متعمد، لأن التخريب العمدي مجرم بموجب المادة ٣٢٣-٢[(٢)]، ومعاقب عليه بالسجن لمدة خمس سنوات وغرامة ٧٥٠٠٠ يورو[(٣)]، أي أن الحذف، أو التعديل، في البيانات، أو تغيير نظام التشغيل، يجب أن يكون غير مقصود، حتي يخضع للظرف المشدد المنصوص عليه بالفقرة الثانية من المادة ٣٢٣-١ [(٤)]، وتطبيقاً لذلك أدانت محكمة ليون

(1) Code pénal, Chapitre III : Des atteintes aux systèmes de traitement automatisé de données, Article 323-2 Modifié par Loi n°2004-575 du 21 juin 2004 - art. 45 JORF 22 juin 2004:"Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende ".
❖(https://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006418316&cidTexte=LEGITEXT000006070719)

(2) Code pénal, Chapitre III : Des atteintes aux systèmes de traitement automatisé de données, Modifié par LOI n°2015-912 du 24 juillet 2015 - art. 4, Article 323-1-2 :" Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende".
❖(https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070719&idArticle=LEGIARTI000006418319&dateTexte=20120126)

(3) Romain Boos :op. cit., p.68.

(4) Frédérique CHOPIN :op. cit., p.12, Monika Zwolinska. op. cit., p.171, Belkasem Hamid: op. cit. , p10.

الكبرى[1] موظفاً قام بتغيير نظام تشغيل النظام المعلوماتي لصاحب عمله السابق بعد الدخول غير المشروع إليه.

كما أن التخريب المتعمد جرمه المشرع المصري بموجب المادة ١٧ من القانون حال وقوعه على البيانات والمعلومات والنظم المعلوماتية، أما المشرع الإماراتي فلم يجرم التخريب أو صور الضرر السابقة تجريماً مستقلاً إذا وقعت عمداً، وفي الوقت ذاته لم يحدد في المادة ٢/ ٢ ما إذا كان الضرر الذي يترتب على الدخول ويشدد بموجبه العقاب ضرر مقصود أم غير مقصود، ومن ثم يجب تشديد العقاب حال وقوع ضرر بسبب الدخول، سواءً كان الضرر مقصود أم غير مقصود؛ لأنه لو تم قصر التشديد على الضرر غير المقصود كالقانون الفرنسي، لأدى ذلك إلى نتيجة غير منطقية، وهي أن من يتعمد حدوث الضرر تكون عقوبته أقل ممن لم يتعمده، ولو تم قصر التشديد على الضرر المقصود لأفلت من العقاب من دخل النظام ووقع الضرر بخطأ منه.

ولذلك أهيب بالمشرع الإماراتي أن يجرم الإضرار العمدي بالبيانات والمعلومات بصفة عامة تجريماً مستقلاً، دون قصره على بيانات ومعلومات معينة، كالبيانات الطبية، وبيانات بطاقات الائتمان، ويضع له عقوبة أشد من العقوبة المنصوص عليها في المادة ٢/ ٢، ومن ثم تتدرج العقوبات، فيكون للدخول البسيط عقوبة، ويكون للدخول الذي يترتب عليه ضرر غير مقصود عقوبة، ويكون للدخول الذي يترتب عليه ضرر مقصود عقوبة.

ويلاحظ أن القانونين المصري، والإماراتي قد وسعا من صور الضرر الموجب

(1) TGI Lyon, 20 févr. 2001.
❖https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-lyon-jugement-du-20-fevrier-2001/

للتشديد؛ أما المشرع الفرنسي فقد ضيق منها، وهي تعديل البيانات[١]، أو إزالتها، أو تغيير طريقة عمل النظام، وعلى ذلك فلا تشدد العقوبة في القانون الفرنسي إذا ترتب على الدخول إفشاء، أو نشر، أو نسخ بيانات من النظام، أيضاً لم يكن من بين صور الضرر في القانون الإماراتي تغيير طريقة تشغيل النظام.

وقد انتقد البعض-بحق- عدم إدراج المشرع الإماراتي لبعض الآثار الأخرى ضمن صور الضرر هذه كظرف مشدد للدخول، من ذلك "تعديل البيانات"، و "ضعف أداء النظام" [٢]، ويقصد بالتعديل استبدال البيانات أو المعلومات الموجودة في النظام بمعلومات أخرى تختلف عنها[٣].

كما يلاحظ أن المشرع الفرنسي حدد البيانات محل الضرر بـ **"البيانات الواردة في النظام"**، وحددها المشرع المصري بأنها **"البيانات أو المعلومات الموجودة على محل الدخول"** فلا تشدد العقوبة إذا وقع الضرر بسبب هذا الدخول على بيانات نظام آخر، أما القانون الإماراتي فحددها بأنها **"أي بيانات أو معلومات"**، فهل يقصد بذلك أي بيانات داخل النظام الذي دخله المتهم، أم يقصد أي بيانات ولو كانت في نظام آخر غير الذي دخله المتهم.

---

(١) يقصد بتعديل البيانات تغييرها داخل النظام باستبدالها ببيانات أخرى تؤدي إلى نتائج مغايرة لتلك التي صمم البرنامج لأجلها.(د/ صالح شنن: مرجع سابق، ص٨٦، أ/ سامية عبد الرازق: مرجع سابق، ص٢١).

(٢) د/ خالد حامد مصطفى: المسئولية الجنائية لناشري الخدمات التقنية ومقدميها عن سوء استخدام شبكات التواصل الاجتماعي، مجلة رؤى استراتيجية، مركز الإمارات للدراسات والبحوث الاستراتيجية، مج١، ع٢، مارس٢٠١٣م، ص١٤.

(٣) د/ شول ابن شهرة: مرجع سابق، ص٢١٤.

الأرجح أن عبارة **"أي بيانات أو معلومات"** توسع نطاق تطبيق هذا النص على حالات الدخول البسيط التي يمكن أن يترتب عليها إضرار بالبيانات، أو المعلومات، ولو كانت في نظام آخر، خاصةً وأن ذلك وارد ومتصور، بيد أنه يجب تقييد هذا التطبيق بشرط مفاده ألا يكون دخوله للنظام الآخر أو اتصاله به متعمداً، بل كان بالخطأ من خلال النظام الأول الذي قصده، لأنه لو دخل النظام الآخر عمداً لقامت مسئوليته عن جريمة دخول أخرى، ولما كانت هناك حاجة إلى تطبيق هذا النص بهذه الفرضية التوسعية[1].

ويتفق ما انتهيت إليه مع ما ذهب إليه البعض من أن لفظ بيانات أو معلومات ينصرف إلى أي بيانات أيـًا كان نوعها أو نطاقها أو مجالها أو قدرها أو أهميتها، وسواءً كانت بالنظام محل الدخول، أو نظام آخر[2]، ويتقارب مع انتقاد البعض للقانون الكويتي لعدم تحديده لنوع البيانات المقصودة، وهل هي الموجودة داخل النظام، أم المتعلقة بسيره[3].

**الركن المعنوي**: لا يختلف الركن المعنوي لهذه الجريمة في صورتها المشددة عن الركن المعنوي في جريمة الدخول في صورتها البسيطة، فهي من الجرائم العمدية التي

---

(١) ومثالاً لذلك لو أن المتهم دخل عمداً إلى النظام المعلوماتي لإحدى المؤسسات، وتسبب دخوله غير المشروع في تصدير رسالة الكترونية دون قصد إلى نظام معلوماتي لفرع من فروع الشركة، أو لشركة أخرى؛ فترتب على ذلك الإضرار بالبيانات في النظام الآخر؛ ففي هذا الفرض طبقـًا للقانون الفرنسي لا ينطبق الظرف المشدد؛ لأن القانون حدد محل الضرر بالبيانات والمعلومات الواردة في النظام، أما في القانون الإماراتي فإن الظرف المشدد ينطبق؛ لأن المشرع لم يقصر محل الضرر على البيانات الواردة في النظام، ولم يتركها دون تحديد، بل سبقها ب" أي" التي تعني لغويـًا التعميم.

(٢) د/ إمام حسنين عطاالله: مرجع سابق، ص١٤٦.

(٣) د/ عبد الحليم بوقرين: مرجع سابق، ص٢٩٥.

تقوم على القصد الجنائي بعنصريه العلم والإرادة، ولا يشترط أن تنصرف إرادة الجاني وقت دخول النظام إلى الإضرار بالبيانات أو المعلومات أو تغيير نظام التشغيل، إذ يستوي في القانون الإماراتي تعمد المتهم الإضرار بالبيانات والمعلومات، أو عدم تعمده ذلك. أما في القانونين الفرنسي والمصري فإنه يشترط لتطبيق هذا الظرف المشدد ألا يكون المتهم قد قصد تعديل أو حذف البيانات، أو تغيير نظام التشغيل عند الدخول؛ لأنه لو قصد ذلك لما خضع لهذا الظرف المشدد؛ وإنما سيخضع للجريمة المنصوص عليها في المادة ٣٢٣-٢ من القانون الفرنسي، أو المادة ١٧ من القانون المصري.

أما النظام السعودي فلا يوجد به نص يشدد العقاب على الدخول البسيط إذا ترتب عليه محو البيانات أو المعلومات، أو إتلافها، أو إعادة نشرها، أو غير ذلك من صور؛ بيد أنه جرم الدخول غير المشروع إذا كان قصد المتهم التلاعب بالبيانات أو تخريبها، وعاقب على ذلك كجريمة مستقلة عقوبتها أشد من الدخول المجرد، وذلك بموجب المادة الخامسة من النظام.

**العقوبة**: عاقب المشرع الإماراتي المتهم الذي قصد مجرد الدخول إلى النظام ثم ترتب على دخوله إضرار بأي بيان أو معلومة بالحبس مدة لا تقل عن ستة أشهر، وغرامة لا تقل عن مائة وخمسين ألف درهم ولا تزيد عن سبعمائة وخمسون ألف درهم أو بإحدى هاتين العقوبتين؛ وعاقب المشرع المصري على ذلك بالحبس مدة لا تقل عن سنتين، وغرامة لا تقل عن مائة ألف جنيه، ولا تزيد عن مائتي ألف، أو بإحدى هاتين العقوبتين؛ بينما عاقب المشرع الفرنسي من قصد مجرد الدخول ثم حدث حذف أو تعديل البيانات الواردة في النظام، أو تغيير في تشغيل هذا النظام، بدون قصد بالسجن لمدة ثلاث سنوات وغرامة قدرها ١٠٠٠٠٠ يورو.

**ثانيـًا-إذا ترتب على الدخول الإضرار بالبيانات أو المعلومات الشخصية.**

يقصد بالبيانات الشخصية تلك التي تتصل بحياة الفرد، كبياناته الشخصية، وصوره، وصور وبيانات أسرته، وما يتعلق بأمواله، وتصرفاته الشخصية، وتنقلاته، ومعتقداته، وعلاقاته المختلفة[١]، وإجمالاً كل البيانات والمعطيات التي تسمح برسم صورة لاتجاهاته السياسية، ومعتقداته الدينية، وتعاملاته المالية، وتحدد جنسيته، أو هويته[٢].

وقد عرفها قانون حماية البيانات الشخصية الفرنسي بأنها أي معلومة تتعلق بشخص طبيعي محددة هويته، أو من الممكن تحديد هويته، بطريقة مباشرة، أو غير مباشرة[٣]، أي البيانات التي تسمح بتحديد هوية الشخص الطبيعي بطريقة مباشرة، أو غير مباشرة[٤]، مثل صورته، وصوته، واسمه، ولقبه، أرقامه الشخصية(تحقيق شخصية، تأمين، سيارة، اشتراكات، هاتف، حساب بنكي)، وحالته الصحية، وأصوله العرقية، وجنسيته، وبريده

---

(١) د/ إمام حسنين عطاالله: مرجع سابق، ص١٦٤.

(٢) أ/ حمودي ناصر: مرجع سابق، ص٩٧.

(3) Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés .

(٤) د/ مروة زين العابدين صالح: الحماية القانونية الدولية للبيانات الشخصية عبر الانترنت بين القانون الدولي الاتفاقي والقانون الوطني، ط١، مركز الدراسات العربية للنشر والتوزيع، ٢٠١٦م ، ص٧٣، د/ إبراهيم داود: مرجع سابق ، ص٣٨٠؛ بيد أن البعض يرى أن تعريف القانون الفرنسي للبيانات الشخصية مفاده أن أي بيان يتعلق بشخص طبيعي يعد بيانـًا شخصيـًا شريطة أن يكون الشخص محدد الهوية أو من الممكن تحديد هويته (د/ سامح عبد الواحد التهامي: الحماية القانونية للبيانات الشخصية، دراسة في القانون الفرنسي، مجلة الحقوق، الكويت، مج٣٥، ع٣، سبتمبر ٢٠١١م، ص٣٨٦)، فطبقـًا للرأي الأول فإن البيانات الشخصية هي التي يمكن من خلالها تحديد هوية الشخص، وطبقـًا للرأي الثاني فإن البيانات الشخصية هي التي تتعلق بشخص محدد الهوية أو يمكن تحديد هويته.

الالكتروني، وحالته الاجتماعية[١]. وعرفها قانون مكافحة جرائم تقنية المعلومات المصري في مادته الأولى بأنها: " أي بيانات متعلقة بشخص طبيعي محدد أو يمكن تحديده، بشكل مباشر أو غير مباشر، عن طريق الربط بينها وبين بيانات أخرى"، أما القانونين السعودي والإماراتي فلم يحددا المقصود بالبيانات والمعلومات الشخصية.

وقد أصبحت البيانات والمعلومات الشخصية ثروة هائلة لبعض الشركات العملاقة التي تجني من وراء معالجتها، وتداولها، والاتجار بها، أرباحاً طائلة، دون أدنى اعتبار لخصوصية الأفراد، ونظراً لأن الأنظمة المعلوماتية مصدر غني بمثل هذه البيانات فقد تعددت صور الاعتداء عليها[٢]، كالحصول عليها من خلال قواعد البيانات، والإضرار بها نتيجة الدخول غير المشروع، لذلك شدد المشرع العقاب في هذه الحالة. إذ تنص المادة ٢/ ٣ من القانون الإماراتي على أن: " تكون العقوبة الحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين إذا كانت البيانات أو المعلومات محل الأفعال الواردة في الفقرة (٢) من هذه المادة **شخصية**".

وتنص الفقرة الثالثة من المادة ٣٢٣-١ من قانون العقوبات الفرنسي على أنه: "عندما تُرتكب الجرائم المنصوص عليها في الفقرتين السابقتين ضد نظام المعالجة الآلية للبيانات **الشخصية التي تنفذها الدولة**، تزداد العقوبة إلى السجن لمدة خمس

(١) د/ سامح التهامي: مرجع سابق، ص٣٨٨، د/ مروة زين العابدين صالح: مرجع سابق، ص٧٥ .

(٢) د/ إبراهيم داود: الحماية القانونية للبيانات الشخصية من منظور الحق في الخصوصية، دراسة تحليلية مقارنة، مجلة الحقوق للبحوث القانونية والاقتصادية، مصر، ٢٠١٧م ، ص٣٨٠.

سنوات و ١٥٠٠٠٠ يورو غرامة "[1]، كما تنص الفقرة الرابعة من المادة ٣٢٣-١ على تشديد العقوبة إلى السجن لمدة عشر سنوات وغرامة قدرها ٣٠٠٠٠٠ يورو إذا ارتكبت جرائم الدخول الاحتيالي ضد نظام المعالجة الآلية للبيانات الشخصية التي تنفذها الدولة من قبل جماعات إجرامية منظمة.

وبموجب المادة ٣/٢ فقد شدد المشرع الإماراتي الدخول البسيط إلى النظام المعلوماتي إذا ترتب عليه إضرار بأي بيانات أو معلومات شخصية؛ سواءً كانت موجودة في نظام معلوماتي خاص بالدولة، أو خاص بالشخص صاحب هذه البيانات، أو خاص بشخص آخر، أو شركة، إذ إن وجود هذه البيانات أو المعلومات في أيٍ من هذه الأنظمة لا ينفي عنها طابعها الشخصي، ولا يكفي للتشديد مجرد الدخول إلى الأنظمة التي تحوي هذه البيانات والمعلومات، إنما يجب أن يؤدي هذا الدخول إلى الإضرار بها، وأن يتخذ إحدى الصور التي حددتها المادة ٢/ ٢، كالحذف أو الإتلاف، أو النشر، ويستوي أن يكون الإضرار مقصوداً أو غير مقصود.

أما المشرع الفرنسي فقد شدد العقاب إذا تعلق الأمر بالبيانات الشخصية في ثلاث حالات: الأولى- عند مجرد الدخول إلى أنظمة البيانات الشخصية، ولو لم يترتب على ذلك حذف، أو تعديل للبيانات، أو تغيير نظام التشغيل، والحالة الثانية- إذا ترتب على الدخول البسيط حذف، أو تعديل للبيانات، أو تغيير في نظام التشغيل، غير مقصود، لكنه

(1) Code pénal, Chapitre III : Des atteintes aux systèmes de traitement automatisé de données, Modifié par LOI n°2015-912 du 24 juillet 2015 - art. 4, Article 323-1: " Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 150 000 € d'amende".
❖(https://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006418316&cidTexte=LEGITEXT000006070719)

اشترط للتشديد أن تكون البيانات الشخصية يحويها نظام معلوماتي تنفذه الدولة، أي مسئولة عنه. كالنظام المعلوماتي الخاص بالأحوال المدنية، وقاعدة البيانات الشخصية المستخدمة لإصدار جوازات السفر[١]، والحالة الثالثة- إذا ارتكبت جريمة الدخول غير المشروع ضد نظام المعالجة الآلية للبيانات الشخصية التي تنفذها الدولة من قبل جماعة إجرامية منظمة[٢].

وعلى ذلك؛ فإذا كان المشرع الإماراتي قد وسع من نطاق هذا الظرف المشدد ليشمل كافة البيانات الشخصية، في أي نظام معلوماتي، ولو كان لشخص عادي، فقد قصر المشرع الفرنسي التشديد على البيانات الشخصية التي تحويها الأنظمة المعلوماتية للدولة، هذا من ناحية؛ ومن ناحية أخري فقد قصر المشرع الإماراتي هذا التشديد على الدخول الذي يترتب عليه ضرر مقصود، أو غير مقصود بالحذف، أو النشر، أو غير ذلك من صور الضرر المحددة في المادة ٢/ ٢، أما المشرع الفرنسي فلم يقصر هذا التشديد على الدخول الذي يترتب عليه ضرر غير مقصود، بل طبقه ولو اقتصر سلوك المتهم على مجرد الدخول دون حدوث أي ضرر، بل وسوى بينهما في العقوبة.

وإن كان يحمد للمشرع الإماراتي تشديد العقاب عندما ينتج عن الدخول الإضرار بالبيانات الشخصية[٣]، ولو لم تكن في أنظمة معلوماتية تابعة للدولة؛ بيد أنه لم يشدد العقاب على مجرد الدخول إلى انظمة تحوي هذا النوع من البيانات، واشترط للتشديد أن يترتب على الدخول الإضرار بالبيانات الشخصية بالحذف أو الإلغاء أو التدمير،

(1) Frédérique CHOPIN : op. cit., p.12, Monika Zwolinska. op. cit., p.170.

(٢) د/ دينا عبد العزيز فهمي: مرجع سابق، ص٢٠.

(٣) د/ إمام حسنين عطاالله: مرجع سابق، ص١٦٤.

أو غير ذلك من الصور المحددة؛ رغم أن طبيعة هذه البيانات تجعل من مجرد الاطلاع عليها ضرر بما تتيحه للمتدخل من معرفة معلومات يحرص صاحبها على سريتها؛ وعليه يجدر بالمشرع تشديد العقوبة على مجرد الدخول إلى نظام معلوماتي به بيانات أو معلومات شخصية، وعدم الاكتفاء بعقوبة الدخول البسيط.

وينطبق على هذا الظرف كل ما ينطبق على الظرف السابق من أحكام، بما فيها الركن المعنوي؛ إلا إنه يتطلب وفقـًا للقانون الإماراتي أن تكون البيانات والمعلومات التي وقع عليها الضرر ذات طابع شخصي، ووفقـًا للقانون الفرنسي أن تكون البيانات ذات طابع شخصي وفي نظام معلوماتي خاص بالدولة.

وقد عاقب النظام السعودي على الدخول غير المشروع للإضرار بالبيانات الخاصة كجريمة مستقلة بموجب نص المادة ٥/ ١ التي تنص على أن: "يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين، كل شخص يرتكب أيـًا من الجرائم المعلوماتية الآتية: ١- الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها، أو تغييرها، أو إعادة نشرها". ويعاقب وفقـًا لهذا النص من يدخل نظامـًا معلوماتيـًا أو ما في حكمه قاصداً إلغاء البيانات الخاصة، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها، أو تغييرها، أو إعادة نشرها، ومجرد الدخول بهذا القصد تقوم به هذه الجريمة دون اشتراط تحقق ما قصد إليه المتهم، أما إذا كان فعله مجرد الدخول إلى نظام به بيانات شخصية دون قصد الإضرار بها فتقوم في حقه جريمة الدخول غير المشروع البسيط المنصوص عليها في المادة ٣/ ٣ من النظام.

ويلاحظ أن هذه الجريمة في النظام السعودي من الجرائم ذوات القصد الخاص؛

فلا يكفي القصد العام لقيام الركن المعنوي لها؛ بل يجب أن تتجه نية المتهم وقت دخول النظام إلى إلغاء بيانات خاصة فيه، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها، أو تغييرها، ولا يشترط تحقق ما قصد إليه، ولا تختلف أحكام القصد العام عما سبق تناوله في جريمة الدخول البسيط.

وأما المشرع المصري فلم يخص البيانات الشخصية بحماية خاصة في مواجهة الدخول غير المشروع، ومن ثم فإن الدخول إلى نظام معلوماتي به بيانات شخصية تقوم به جريمة الدخول البسيط وفقـًا للمادة ١٤/ ١، وإذا نتج عن هذا الدخول الإضرار بهذه البيانات الشخصية فيشدد العقاب وفقـًا لنص المادة ١٤/ ٢، وفي كلتا الحالتين لا تختلف حماية البيانات الشخصية عن حماية البيانات العادية. ولكن تجدر الإشارة إلى أنه جرم في المادة ٢٥ من القانون منح بيانات شخصية إلى نظام إلكتروني لترويج السلع أو الخدمات دون موافقة صاحبها.

**العقوبة**: شدد المشرع الإماراتي العقوبة إذا توافر هذا الظرف لتكون الحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين. أما المشرع الفرنسي فشدد عقوبة هذا الظرف إلى السجن لمدة خمس سنوات و ١٥٠٠٠٠ يورو غرامة، وقد تجد هذه العقوبة الشديدة مبررها في أن الاعتداء لم يقع فقط على بيانات شخصية؛ وإنما وقع عليها وهي في حماية الدولة أو تحت إشرافها، كما أن الاعتداء هنا لا يتيح الاطلاع على بيانات شخصية لفرد واحد فقط أو الإضرار بها؛ إنما يتيح ذلك بالنسبة لبيانات عدد كبير من الأفراد غالبـًا ما تمثل قواعد بيانات ضخمة.

ويلاحظ أن المنظم السعودي جعل عقوبة الدخول غير المشروع بقصد الإضرار

بالبيانات الخاصة السجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين؛ بينما عاقب على الدخول المجرد بالسجن مدة لا تزيد عن سنة، وغرامة لا تزيد عن خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين، ويعكس تشديد عقوبة الدخول غير المشروع بقصد الإضرار بالبيانات الخاصة عناية المنظم السعودي بالبيانات الشخصية وحمايتها.

**ثالثًا- الدخول بمناسبة أو بسبب تأدية العمل، وصفة الجاني.**

تفاوتت القوانين محل الدراسة في تشديدها للعقاب حال ارتكاب الجريمة بسبب العمل؛ حيث شدد المشرع الإماراتي عقوبة الدخول غير المشروع إذا كان الدخول بمناسبة العمل أو بسبب تأديته، ولم يشترط للتشديد أن يكون الجاني موظفًا عامًا، أما المشرع المصري فقد شدد الجزاء على الجاني إذا كان موظفًا عامًا وتم الدخول غير المشروع أثناء وبسبب تأدية وظيفته، وتمثل التشديد في عزل الجاني من وظيفته، وجاء تشديد المشرع لهذه الحالة قاصراً على الموظف العام اذا ارتكب الجريمة من خلال اختصاصه الوظيفي، أو من خلال استغلال نفوذه الوظيفي. ولم ينص المشرع الفرنسي على ظرف مماثل للتشديد.

وقد نصت المادة الثالثة من القانون الإماراتي على أن: " يعاقب بالحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين كل من ارتكب أيًا من الجرائم المنصوص عليها في البندين (١) و (٢) من المادة (٢) من هذا المرسوم بقانون بمناسبة أو بسبب تأدية عمله".

ومفاد هذا النص أن من يدخل دون حق إلى نظام معلوماتي بسبب عمله، أو بمناسبته،

يشدد عليه العقاب، سواءً وقف الأمر عند مجرد الدخول، أو أفضى هذا الدخول إلى الإضرار بالبيانات على النحو الذي نصت عليه الفقرة الثانية من المادة الثانية، وعلة التشديد هنا هي إساءة العامل للثقة والأمانة التي وضعت فيه، ومن ثم يستوي في العقوبة من وقف فعله عند حد الدخول، ومن أفضى تدخله إلى الإضرار بالبيانات أو المعلومات؛ إذ لم يشترط المشرع سوى أن يكون الدخول بمناسبة أو بسبب تأدية المتهم عمله.

والدخول غير المشروع إلى النظام المعلوماتي "بسبب تأدية العمل" يعني وجود علاقة بين العمل، وبين الدخول، بمعنى أن يكون العمل هو السبب المباشر في الدخول غير المشروع، كما لو كلف خبير تقني بالقيام بعمل صيانة لأحد الأنظمة المعلوماتية في شركة ما، وقام بالدخول إلى جزء من النظام محظور عليه الدخول إليه، أما "بمناسبة تأدية العمل" فتعني أن أداء العمل لم يكن هو السبب المباشر في الدخول غير المشروع، لكنه هيأ له الظروف بطريقة غير مباشرة للدخول غير المشروع إلى النظام، كما لو حصل على بيانات شخصية تقليدية لأحد العملاء في شركة يعمل بها ثم استخدمها في تخمين كلمة المرور الخاصة بهذا العميل، فدخل نظاماً معلوماتياً خاصاً بهذا العميل. ولا يشترط في القانون الإماراتي أن يكون العمل حكومياً[1]، وكل استغلال للعمل بطريق مباشر أو غير مباشر في الدخول غير المشروع يتحقق به التشديد؛ فلا يشترط الاختصاص الكلي أو الجزئي.

أما القانون المصري فقد شدد الجزاء بعزل الموظف العمومي الذي تثبت إدانته في

(١) د/ إمام حسنين عطاالله: مرجع سابق، ص١٦٨.

إحدى جرائم تقنية المعلومات، ومنها الدخول غير المشروع، وذلك في حالتين:

**الحالة الأولى- العزل الجوازي**: حيث أجاز المادة ٣٩/ ١ للمحكمة حال حكمها بالإدانة على موظف عمومي في أية جريمة من جرائم تقنية المعلومات أن تقضي بعزله من وظيفته مؤقتًا، وذلك إذا ثبت ارتكابه للجريمة أثناء وبسبب تأديته لوظيفته، وترك مدة العزل للمحكمة.

**الحالة الثانية- العزل الوجوبي**: حيث أوجبت المادة ٣٩/ ٢ على المحكمة عزل الموظف العام من وظيفته إذا كان ارتكابه للجريمة أثناء وبسبب تأديته لوظيفته وبغرض الإخلال بالنظام العام، أو تعريض سلامة المجتمع وأمنه للخطر، أو الإضرار بالأمن القومي للبلاد، أو بمركزها الاقتصادي، أو منع، أو عرقلة ممارسة السطات العامة لأعمالها، أو تعطيل أحكام الدستور أو القوانين أو اللوائح، أو الإضرار بالوحدة الوطنية والسلام الاجتماعي، ولم ينص على تأبيد العزل، ومن ثم يبقى على أصله وفقًا للفقرة الأولى وهو التأقيت.

أما النظام السعودي فقد نص في المادة الثامنة على ألا تقل عقوبة السجن أو الغرامة عن النصف إذا كان مرتكب الجريمة موظفًا عموميًا، واتصلت جريمته بوظيفته، أو كان ارتكابه لها عبر استغلال نفوذه أو سلطاته، وهو ما يعنى تشديد العقاب سواءً كان ارتكابه للجريمة متصلاً باختصاصه الوظيفي، أو كان قد استغل نفوذه ومركزه الوظيفي في ارتكاب الجريمة.

## المطلب الثاني
## جريمة الدخول غير المشروع إلى الأنظمة المعلوماتية للدولة والبيانات الحكومية

جرم المشرع المصري الدخول غير المشروع إلى الأنظمة المعلوماتية الخاصة

بالدولة بموجب المادة ٢٠ من قانون مكافحة جرائم تقنية المعلومات[١]، والمادة ٢٩/ ٢ من قانون مكافحة الإرهاب رقم ٩٤ لسنة ٢٠١٥م[٢]، وجرمها المشرع الإماراتي في المادة الرابعة من القانون[٣]، أما النظام السعودي فلا يوجد به نص خاص بتجريم دخول

---

(١) تنص المادة ٢٠ من قانون مكافحة جرائم تقنية لمعلومات المصري على أن: " يعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين كل من دخل عمداً، أو دخل بخطأ غير عمدي وبقي بدون وجه حق، أو تجاوز حدود الحق المخول له....، أو اخترق موقعًا، أو بريداً إلكترونيًا، أو حسابًا خاصًا أو نظامًا معلوماتيًا يدار بمعرفة أو لحساب الدولة، أو أحد الأشخاص الاعتبارية العامة، أو مملوكًا لها، أو يخصها. فإذا كان الدخول بقصد الاعتراض أو الحصول بدون وجه حق على بيانات أو معلومات حكومية، تكون العقوبة السجن والغرامة التي لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه. وفي جميع الأحوال إذا ترتب على أي من الأفعال السابقة إتلاف تلك البيانات أو المعلومات، أو ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي أو البريد الإلكتروني، أو تدميرها، أو تشويهها، أو تغييرها، أو تغيير تصاميمها، أو نسخها، أو تسجيلها، أو تعديل مسارها، أو إعادة نشرها، أو إلغاؤها كليًا، أو جزئيًا، بأي وسيلة كانت، تكون العقوبة السجن، والغرامة التي لا تقل عن مليون جنيه ولا تجاوز خمسة ملايين جنيه".

(٢) تنص المادة ٢٩/ ٢ من قانون مكافحة الإرهاب المصري رقم ٩٤ لسنة ٢٠١٥ على أن: " ويعاقب بالسجن المشدد مدة لا تقل عن عشر سنين كل من دخل بغير حق أو بطريقة غير مشروعة موقعًا الكترونيًا تابعًا لأية جهة حكومية، بقصد الحصول على البيانات أو المعلومات الموجودة عليها أو الاطلاع عليها أو تغييرها أو محوها أو إتلافها أو تزوير محتواها الموجود بها، وذلك كله بغرض ارتكاب جريمة من الجرائم المشار إليها بالفقرة الأولى من هذه المادة أو الإعداد لها".

(٣) تنص المادة الرابعة من القانون الإماراتي على أن: " يعاقب بالسجن المؤقت والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون وخمسمائة ألف درهم كل من دخل بدون تصريح إلى موقع إلكتروني، أو نظام معلومات إلكتروني، أو شبكة معلوماتية، أو وسيلة تقنية معلومات، سواءً كان الدخول **بقصد الحصول على بيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية، أو تجارية، أو اقتصادية**. وتكون العقوبة السجن مدة لا تقل عن (٥) خمس سنوات والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز (٢) مليون درهم، إذا تعرضت هذه البيانات أو المعلومات للإلغاء، أو الحذف، أو الإتلاف، أو التدمير، أو الإفشاء، أو التغيير، أو النسخ، أو النشر، أو إعادة النشر".

أنظمة الدولة، واقتصر القانون الفرنسي على تشديد العقاب إذا وقع الدخول على أنظمة معلوماتية تنفذها الدولة مما يخص البيانات الشخصية.

**علة التجريم**: إذا كان الدخول غير المشروع إلى الأنظمة المعلوماتية من أجل الحصول على المعلومات مسألة بالغة الخطورة[1]، فلا شك أن هذه الخطورة تبلغ مبلغها حال وقوع الجريمة على أنظمة وبيانات الدولة والجهات العامة، باعتبار أن الاعتداء على المصلحة العامة أشد وأخطر من الاعتداء على نظيرتها الخاصة[2].

ونظراً لاختلاف سياسة التجريم والعقاب في هذه المسألة في القانونين المصري والإماراتي؛ نقسم هذا المطلب إلى فرعين، يتناول أحدهما موقف المشرع المصري، ويتناول الآخر موقف المشرع الإماراتي.

## الفرع الأول
## الدخول غير المشروع إلى الأنظمة المعلوماتية للدولة في القانون المصري

**تقوم هذه الجريمة في صورتها البسيطة على ركنين، على النحو التالي:**

**الركن المادي**: يتحقق الركن المادي لهذه الجريمة وفقاً للمادة ٢٠ من قانون مكافحة جرائم تقنية المعلومات المصري بمجرد الدخول غير المشروع إلى نظام معلوماتي خاص بالدولة، أو اختراقه، سواءً وقع الدخول، أو الاختراق على موقع، أو بريد إلكتروني، أو حساب خاص، أو نظام معلوماتي تديره الدولة، أو أحد الأشخاص الاعتبارية العامة، أو كان مملوكاً لها، أو يخصها، أما إذا كان الدخول إلى موقع إلكتروني تابع لأية جهة حكومية بقصد الحصول على بياناته أو معلوماته، أو الاطلاع

(١) د/ هالة نوفل، د/ محمود اسماعيل: مرجع سابق، ص٤.

(٢) د/ محمد خليفة: مرجع سابق، ص٩٦.

عليها، أو إتلافها، أو محوها، أو تغييرها، أو تزوير محتواها، وكان ذلك بغرض ارتكاب جريمة إرهابية؛ فإنه يسأل وفقًا المادة ٢٩/ ٢ من قانون مكافحة الإرهاب المصري رقم ٩٤ لسنة ٢٠١٥م.

**الركن المعنوي**: لا يختلف الركن المعنوي لجريمة الدخول غير المشروع إلى الأنظمة المعلوماتية للدولة في صورتها البسيطة عما سبق تناوله في الأحكام المشتركة بشأن الركن المعنوي؛ إذ إن هذه الجريمة من جرائم العمد، ويتخذ الركن المعنوي فيها صورة القصد العام، والذي يقوم على العلم والإرادة بالتفصيل السابق، فضلاً عن تطلب علم المتهم بأن النظام المعلوماتي الذي يدخله أو يخترقه من أنظمة الدولة، أو أحد الأشخاص الاعتبارية العامة.

**العقوبة**: عاقب المشرع المصري على هذه الجريمة بالحبس الذي لا تقل مدته عن سنتين، والغرامة التي لا تقل عن خمسين ألف جنيه ولا تزيد عن مائتي ألف جنيه، أو بإحدى العقوبتين.

**وقد شدد المشرع المصري العقوبة على هذه الجريمة في حالتين:**

**الأولى- الدخول بقصد الاعتراض أو الحصول على بيانات أو معلوماتية حكومية**: إذا دخل الجاني أحد الأنظمة المعلوماتية للدولة بدون وجه حق، وكان قصده من الدخول اعتراض بيانات أو معلومات حكومية، أو الحصول عليها بدون وجه حق؛ فإنه يعاقب وفقًا للمادة ٢٠/ ٢ من القانون بعقوبة أشد من عقوبة الدخول المجرد، فتكون العقوبة السجن بين حديه الأدنى والأقصى، والغرامة التي لا تقل عن مائة ألف جنيه ولا تزيد عن خمسمائة ألف جنيه، وهي عقوبة أشد بكثير من مجرد الدخول وفقًا للفقرة السابقة، حيث يتغير وصف الجريمة من جنحة إلى جناية، ويعاقب عليها بالسجن والغرامة

المحددة، ويكون الجمع بينهما وجوبي.

**الحالة الثانية- الإضرار بالبيانات الحكومية أو الأنظمة المعلوماتية للدولة:** وفقاً للمادة ٢٠/ ٣ من القانون إذا دخل الجاني نظام معلوماتي للدولة دون وجه حق، وقصد اعتراض البيانات أو المعلومات الحكومية، أو الحصول عليها دون حق، أو لم يقصد، وترتب على هذا الدخول إضرار بالبيانات أو المعلومات، أو النظام المعلوماتي محل الدخول؛ فإن عقوبة السجن تبقى كما هي بين حديها الأدنى والأقصى؛ لكن عقوبة الغرامة يكون حدها الأدنى مليون جنيه، وحدها الأقصى خمسة ملايين جنيه، ويبقى الجمع بين العقوبتين وجوبي.

وقد حدد المشرع صور الضرر الذي يقع على البيانات الحكومية، أو الأنظمة المعلوماتية للدولة بسبب الدخول غير المشروع، ويترتب عليه هذا التشديد، وهي الإتلاف، والتدمير، والتشويه، والتغيير، والنسخ، والتسجيل، وتعديل المسار، وإعادة النشر، والإلغاء الكلي، أو الجزئي.

وعرف القانون المصري البيانات الحكومية بأنها:" بيانات متعلقة بالدولة أو إحدى سلطاتها، أو أجهزتها أو وحداتها، أو الهيئات العامة، أو الهيئات المستقلة، أو الأجهزة الرقابية، أو غيرها من الأشخاص الاعتبارية العامة وما في حكمها، والمتاحة على الشبكة المعلوماتية، أو على أي نظام معلوماتي، أو على حاسب أو ما في حكمها".

## الفرع الثاني
## الدخول بقصد الحصول على بيانات حكومية في القانون الإماراتي

جرم المشرع الإماراتي الدخول غير المشروع إلى الأنظمة المعلوماتية إذا كان قصد الجاني من دخوله الحصول على بيانات حكومية، أو معلومات سرية خاصة بمنشأة

مالية، أو تجارية، أو اقتصادية بنص المادة الرابعة من القانون، وجعل عقوبته أشد من الدخول المجرد. ويتحقق الركن المادي لهذه الجريمة بمجرد الدخول غير المشروع إلى أي نظام معلوماتي بقصد الحصول على البيانات المذكورة، دون تطلب تحقق نتيجة إجرامية معينة، فلا يشترط الحصول على البيانات المقصودة؛ ولكن يشترط اتجاه نيته إلى ذلك، يستوى بعد ذلك أن يحصل عليها أم لا.

وتجدر الإشارة إلى أن المشرع الإماراتي نص في هذه المادة على ذات العقوبة لمن يكون قصده من الدخول غير المشروع الحصول على معلومات سرية خاصة بمنشأة مالية أو اقتصادية أو تجارية. ووفقاً لهذا النص فإن كافة المعلومات والبيانات الحكومية مشمولة بالحماية؛ أما المعلومات الخاصة بالمنشآت المالية، أو التجارية، أو الاقتصادية، فلا تشملها هذه الحماية إلا إذا كانت معلومات **سرية**.

وقد جاءت صياغة المشرع الإماراتي لنص المادة الرابعة من قانون مكافحة جرائم تقنية المعلومات صياغة عامة؛ فلم يقصر الدخول على الأنظمة المعلوماتية الحكومية للحصول على بيانات أو معلومات حكومية؛ ولم يقصر الدخول على أنظمة المنشآت المذكورة للحصول على بيانات أو معلومات سرية تتعلق بها؛ ومن ثم فلا يشترط لوقوع هذه الجريمة الدخول إلى نظام معلوماتي يخص الحكومة أو المنشآت الخاصة، بل يشترط فقط أن تكون نيته من دخول أي نظام هو الحصول على بيانات حكومية أو معلومات سرية لمنشأة خاصة.

ولا شك أن هذه الصياغة تعزز حماية مثل هذه البيانات والمعلومات، إذ إن المتهم قد لا يدخل إلى النظام المعلوماتي الحكومي مباشرة بل يدخل إلى نظام عادي قاصداً التسلل من خلاله إلى النظام الحكومي، فإذا نجح في الوصول إليه فلا تثور مشكلة حينئذٍ

إذ يعد دخولاً غير مباشر، وتقوم به الجريمة، لكن تظهر أهمية الصياغة العامة للنص في الحالة التي يفشل فيها المتهم في الانتقال من النظام غير الحكومي الذي دخله إلى النظام الحكومي؛ فيطبق عليه النص لأن نيته وقت دخول النظام غير الحكومي كانت الحصول على بيانات حكومية؛ بل ينطبق النص إذا دخل إلى نظام ما بقصد الحصول على بيانات حكومية أو ما في حكمها من هذا النظام، ولو ثبت فيما بعد عدم احتوائه على مثل هذه البيانات من الأساس.

وقد عرف المشرع الإماراتي البيانات الحكومية بأنها: "البيانات أو المعلومات الإلكترونية الخاصة أو العائدة إلى الحكومة الاتحادية أو الحكومات المحلية لإمارات الدولة أو الهيئات العامة أو المؤسسات العامة الاتحادية أو المحلية"، وعرف المنشآت المالية أو التجارية أو الاقتصادية بأنها: "أي منشأة تكتسب وصفها المالي أو التجاري أو الاقتصادي بموجب الترخيص الصادر لها من جهة الاختصاص بالدولة"، وعلى ذلك فكل معلومة الكترونية سرية [1] تخص إحدى هذه المنشآت تأخذ حكم المعلومات والبيانات الحكومية.

وإذا كانت علة هذا التشديد بشأن البيانات الحكومية تفرضها طبيعة هذه البيانات وتعلقها بمصالح الدولة والمجتمع؛ فإن علة التشديد بشأن أسرار المنشآت التجارية، والمالية، والاقتصادية تكمن في أن هذه البيانات هي الأكثر تعرضاً لجرائم تقنية المعلومات، والأكثر تأثراً بها. حيث تتركز عمليات الدخول غير المشروع في مجالات

(١) عرف المشرع الإماراتي المعلومات والبيانات السرية بأنها:" أي معلومات أو بيانات غير مصرح للغير بالإطلاع عليها أو بإفشائها إلا بإذن مسبق ممن يملك هذا الإذن".

الأنشطة التجارية على كشف الأسرار التجارية، والتسويقية، وعناوين العملاء، وتراكيب المنتجات، ونتائج الأبحاث والتطوير[١]، فضلاً عن تخفيض أسعار السلع على مواقع التجارة الالكترونية، أو تغيير، أو حذف محتويات قواعد البيانات لتغيير الوضع الضريبي للشركة[٢].

**الركن المعنوي للجريمة**: تشترك هذه الجريمة مع جرائم الدخول الأخرى في القصد العام، وتتطلب فوق ذلك قصداً خاصاً يتمثل في نية الحصول على بيانات حكومية، أو معلومات سرية، خاصة بمنشآت مالية، أو تجارية، أو اقتصادية، إذ يجب اتجاه نية المتهم لحظة دخول النظام إلى الحصول على بيانات حكومية أو معلومات سرية خاصة بالمنشآت المذكورة بالنص، والمهم هو توافر هذه النية لحظة الدخول، يستوي أن يحقق من الدخول ما أراده بعد ذلك أم لا؛ لأن الحصول على البيانات أو المعلومات المذكورة لم يتطلبه المشرع كنتيجة في عناصر الركن المادي للجريمة، وإنما تطلبه كنية خاصة في الركن المعنوي لها.

ويرى البعض أنه يجب تجريم الدخول بقصد الحصول على معلومات أو بيانات خاصة بمنشأة مالية أو تجارية أو اقتصادية، سواءً كانت سرية، أو غير سرية[٣]؛ بيد أنه لا حاجة إلى ذلك؛ إذ إن هذا التجريم يتناسب مع سرية المعلومات التي تعكس أهميتها بالنسبة لهذه المنشآت، أما المعلومات غير السرية فيكفي تجريم الدخول إلى الأنظمة التي تحويها طبقاً للمادة الثانية الخاصة بالدخول البسيط وحالات تشديده.

---

(١) د/ أسامة العبيدي: مرجع سابق، ص١٩.

(2) Belkasem Hamid: op. cit. , p14.

(٣) د/ خالد حامد مصطفى: مرجع سابق، ص٢٨.

**عقوبة الجريمة في صورتها البسيطة**: عاقب المشرع الإماراتي على جريمة الدخول بقصد الحصول على بيانات حكومية أو ما في حكمها بموجب المادة ٤/ ١ بالسجن المؤقت[١]، والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون وخمسمائة ألف درهم، وذلك إذا دخل المتهم إلى النظام بقصد الحصول على البيانات أو المعلومات المذكورة، ولم تتعرض للإلغاء، أو الحذف، أو الإتلاف، أو التدمير، أو غير ذلك، وتطبق هذه العقوبة سواءً تمكن من الحصول على البيانات والمعلومات المقصودة أم لا.

**عقوبة الجريمة في صورتها المشددة**: إذا دخل المتهم إلى النظام بقصد الحصول على البيانات أو المعلومات المذكورة، وترتب على دخوله تعرض البيانات أو المعلومات المقصودة للإلغاء، أو الحذف، أو الإتلاف، أو التدمير، أو الإفشاء، أو التغيير، أو النسخ، أو النشر، أو إعادة النشر فإنه يعاقب بعقوبة الجريمة في صورتها المشددة وفقاً للمادة ٤/ ٢ بالسجن مدة لا تقل عن خمس سنوات والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز (٢) مليون درهم.

ويرى البعض أنه لا يشترط لتشديد العقوبة حدوث إلغاء، أو حذف، أو غير ذلك بالفعل، إنما يكفي مجرد أن تكون هذه البيانات قد هددها خطر من هذه الأخطار[٢]، ويبدو لي أن المقصود هنا هو حدوث ضرر من هذه الأضرار، ذلك أن عبارة "إذا تعرضت هذه البيانات أو المعلومات للإلغاء،..."، تعني أن المعلومة تتعرض للإلغاء

---

(١) تنص المادة ٦٨/ ٢ من قانون العقوبات الاتحادي على أن: " لا يجوز أن تقل مدة السجن المؤقت عن ثلاث سنوات ولا أن تزيد على خمس عشرة سنة ما لم ينص القانون على خلاف ذلك".

(٢) د/ إمام حسنين عطاالله: مرجع سابق، ص١٧٨.

وليس لخطر الإلغاء.

**تخفيف العقوبة أو الإعفاء منها:** وفقاً للمادة ٤٤ من قانون مكافحة جرائم تقنية المعلومات الإماراتي تعد الجريمة المنصوص عليها في المادة الرابعة من الجرائم الماسة بأمن الدولة، وتنص المادة ٤٥ من القانون الإماراتي على أن: "تقضي المحكمة بناء على طلب من النائب العام، بتخفيف العقوبة أو بالإعفاء منها، عمن أدلى من الجناة إلى السلطات القضائية أو الإدارية بمعلومات تتعلق بأي جريمة من الجرائم المتعلقة بأمن الدولة وفقاً لأحكام هذا المرسوم بقانون، متى أدى ذلك إلى الكشف عن الجريمة ومرتكبيها أو إثباتها عليهم أو القبض على أحدهم".

وعلى ذلك؛ إذا توافرت الشروط التالية تعين تخفيف العقوبة أو إعفاء المتهم منها:

١-إدلاء أحد الجناة بمعلومات تتعلق بجريمة الدخول بقصد الحصول على بيانات حكومية، أو معلومات سرية لمنشأة خاصة، يستوي أن تقدم المعلومات للسلطات الإدارية أو القضائية.

٢-أن تؤدي هذه المعلومات إلى أمر من ثلاثة؛ **إما الكشف عن الجريمة ومرتكبيها،** وهو ما يعني أن الجريمة لم يكن أمر وقوعها معلوماً للجهات المختصة ولا مرتكبيها، **وإما إثباتها عليهم،** وهو ما يعني أن المتهم قدم أدلة أو قرائن تم إثبات الجريمة على المتهمين بمقتضاها، **وإما القبض على أحد مرتكبيها.**

٣-أن يطلب النائب العام من المحكمة تخفيف العقوبة أو الإعفاء منها لمن أدلى بالمعلومات.

ويلاحظ أنه إذا توافرت الشروط تعين على المحكمة أن تقضي بتخفيف العقوبة عن المتهم أو إعفائه منها، أي لها أن تختار بين التخفيف والإعفاء.

## المطلب الثالث
## جريمة دخول البريد والمواقع والحسابات الإلكترونية الخاصة

تنص المادة ١٨/ ١ من القانون المصري على أن:" يعاب بالحبس مدة لا تقل عن شهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين كل من أتلف أو عطل أو أبطأ ، أو **اخترق** بريداً إلكترونيـًا، أو موقعـًا، أو حسابـًا خاصـًا بآحاد الناس. فإذا وقعت الجريمة على بريد إلكتروني أو موقع أو حساب خاص بأحد الأشخاص الاعتبارية الخاصة تكون العقوبة الحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين".

وتنص المادة ٣/ ٣ من نظام مكافحة جرائم المعلوماتية السعودي على أن: " يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد عن خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين كل شخص يرتكب أيـًا من الجرائم المعلوماتية الآتية: ٣- الدخول غير المشروع إلى موقع إلكتروني، أو الدخول إلى موقع إلكتروني لتغيير تصاميم هذا الموقع أو إتلافه، أو تعديله، أو شغل عنوانه".

وتنص المادة الخامسة من القانون الإماراتي على أن: "يعاقب بالحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تجاوز ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين كل من دخل بغير تصريح موقعـًا إلكترونيـًا بقصد تغيير تصاميمه أو إلغائه أو إتلافه أو تعديله أو شغل عنوانه".

وتكمن علة هذا التجريم في كثرة استهداف هذه الأنظمة بالدخول غير المشروع، بهدف تغيير معلوماتها، أو تصميماتها، أو البيانات والمعلومات التي توجد بها،

أو الاطلاع عليها، أو الإضرار بها، أو حتى مجرد الدخول. فقد يقوم المتهم بالدخول إلى موقع للتجارة الالكترونية بهدف تخفيض أسعار السلع عليه، أو بقصد تغيير، أو حذف محتوياته، من بيانات أو معلومات[١]، وقد يبدو الضرر الذي ينتج عن دخول المواقع الالكترونية بسيطًا؛ كوضع صور غير لائقة عليه[٢]، أو تعديل بعض العناوين؛ لكن في حقيقته قد يدمر الثقة في المؤسسة أو الشركة التابع لها الموقع[٣]، وكذلك الحسابات الخاصة.

**الركن المادي**: تعد هذه الجريمة من الجرائم الشكلية؛ ومن ثم فهي تشترك مع جرائم الدخول في السلوك الإجرامي، وهو الاختراق أو الدخول غير المشروع، ولا يشترط تحقق نتيجة إجرامية، أي أن قوام الركن المادي لها هو السلوك الإجرامي، وذلك على النحو السابق بيانه في الأحكام المشتركة.

ويلاحظ أن المشرع المصري جرم مجرد الدخول إلى البريد والمواقع والحسابات الخاصة بالأشخاص الطبيعيين بموجب المادة ١٨، وعاقب عليه بعقوبة أقل من عقوبة الدخول المنصوص عليها في المادة ١٤ من القانون، رغم أن محل الدخول واحد، ولا فرق بين النصين سوى أن المادة ١٨ عبرت عن السلوك الإجرامي بلفظ " الاختراق"،

---

(1) Belkasem Hamid: op. cit. , p14.

(٢) مثلما حدث عند وضع صورة مخجلة لزعيمة أحد الأحزاب الأسترالية الشهيرة على موقع الحزب الالكتروني(م/ حسن طاهر داود: جرائم نظم المعلومات، ط١، أكاديمية نايف العربية للعلوم الأمنية، الرياض، ٢٠٠٠م، ص٨٣).

(٣) مثلما حدث عندما أنشأت شركة متخصصة في أمن المعلومات موقعًا لها للإعلان عن خدماتها ومنتجاتها، ووضعت عليه عبارة We are always UP، فقام شخص باختراق الموقع وعدل العبارة لتصبح We are always DOWN.( م/ حسن طاهر داود: مرجع سابق، ٢٠٠٠م).

والمادة ١٤ عبرت عنه بلفظ الدخول العمدي، مع الأخذ في الاعتبار تعريف المشرع للاختراق بأنه دخول بأي طريقة غير مشروعة، ومن ثم فلم تكن هناك حاجة إلى تجريم الاختراق في المادة ١٨ من القانون.

أما المشرع الإماراتي فقد جرم دخول المواقع بصفة عامة دون أن يقصرها على المواقع الخاصة بأفراد أو شركات، أو المواقع الحكومية، كما أنه جرم مجرد الدخول الى المواقع بموجب المادة ٢/ ١، بينما جرم بموجب المادة الخامسة دخول المواقع بقصد الإضرار بها، إذ جعلها جريمة مستقلة، وعقوبتها أشد من عقوبة الدخول المجرد للمواقع. أما المنظم السعودي فقد جرم الدخول المجرد للمواقع، والدخول بقصد الإضرار بها بموجب نص واحد وساوى بينهما في العقوبة.

**محل السلوك الإجرامي**: تقع هذه الجريمة في القانون المصري على أنظمة معلوماتية خاصة، وهي البريد، أو الموقع الالكتروني، أو الحساب الخاص. وتتحقق في القانونين السعودي والإماراتي بالدخول إلى موقع الكتروني، وذلك بخلاف الجرائم السابقة التي كان محلها الأنظمة المعلوماتية[1]، وما في حكمها، ومنها المواقع الالكترونية، وقد حدد المشرع الإماراتي المقصود بالموقع الإلكتروني بأنه: "مكان إتاحة المعلومات الإلكترونية على الشبكة المعلوماتية، ومنها مواقع التواصل الاجتماعي، والصفحات الشخصية والمدونات"، وعرفه القانون المصري بأنه: " مجال أو مكان افتراضي له عنوان محدد على شبكة معلوماتية، يهدف إلى إتاحة البيانات والمعلومات للعامة أو الخاصة"، أما النظام السعودي فعرفه بأنه: " مكان إتاحة البيانات على الشبكة المعلوماتية من خلال عنوان محدد".

(١) د/ إمام حسنين عطاالله: مرجع سابق، ص١٨٣.

وإذا كانت القوانين الثلاثة محل الدراسة قد نصت صراحة على المواقع الإلكترونية كمحل لهذه الجريمة؛ فقد زاد عليها القانون المصري البريد الإلكتروني، والحسابات الخاصة، أما المشرع الإماراتي فقد توسع في تعريف الموقع الإلكتروني ليضم مواقع التواصل الاجتماعي، والصفحات الشخصية والمدونات، أما النظام السعودي وإن لم ينص صراحة على تجريم الدخول إلى الحسابات الخاصة والبريد الالكتروني؛ بيد أنه قد جرم الدخول لتهديد شخص أو ابتزازه لحمله على عمل ما أو امتناع، ولا شك أن هذه الجريمة تتحقق أيـًا كان محل الدخول.

وقد عرف القانون المصري في مادته الأولى الحساب الخاص بأنه: " مجموعة من المعلومات الخاصة بشخص طبيعي أو اعتباري تخوله دون غيره الحق في الدخول على الخدمات المتاحة أو استخدامها من خلال موقع أو نظام معلوماتي"، وعرف البريد الالكتروني بأنه: "وسيلة لتبادل رسائل إلكترونية على عنوان محدد، بين أكثر من شخص طبيعي أو اعتباري، عبر شبكة معلوماتية، أو غيرها من وسائل الربط الإلكترونية من خلال أجهزة الحاسب الآلي وما في حكمها".

**الركن المعنوي**: تعد هذه الجريمة في النظام السعودي والقانون الإماراتي من الجرائم ذوات القصد الخاص، ومن ثم تشترك مع جرائم الدخول في القصد العام بعنصريه العلم والإرادة حسبما سبق بيانه في مبحث الأحكام المشتركة[1]؛ مع مراعاة أنه فيما يتعلق بمحل الجريمة هنا يجب أن يكون المتهم على وعي وإدراك بأن فعله ينصب على موقع الكتروني، وليس شيء آخر من الأنظمة المعلوماتية.

(١) راجع ص ٥٢ وما بعدها من هذا البحث.

أما فيما يتعلق بالقصد الخاص فقد تطلب القانون انصراف نية الجاني لحظة الدخول إلى تغيير تصاميم الموقع، أو إلغائه، أو إتلافه، أو تعديله، أو شغل عنوانه، ويكفي توافر هذه النية لحظة الدخول، ويستوي أن تستمر بعد الدخول أو تتغير. كما يستوي أن يتحقق ما قصد إليه الجاني من الغاء الموقع أو تعديله، أو غير ذلك أو لا يتحقق[1].

أما في القانون المصري فتعد من الجرائم ذوات القصد العام، ومن ثم يتوافر ركنها المعنوي بتوافر العلم والإرادة على النحو السابق بيانه.

**العقوبة:** عاقب المشرع الإماراتي من يدخل موقع بقصد الإضرار به على النحو السابق بالحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تجاوز ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين، ولا أثر في العقوبة لتحقق أو عدم تحقق ما قصد إليه الجاني. وعاقب المنظم السعودي على دخول المواقع الإلكترونية دخولاً مجرداً، أو بقصد الإضرار بها، أو بقصد التهديد والابتزاز بالسجن الذي لا تزيد مدته على سنة، والغرامة التي لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين.

أما المشرع المصري فقد عاقب على اختراق البريد، أو المواقع، أو الحسابات الإلكترونية الخاصة بآحاد الناس بالحبس مدة لا تقل عن شهر وغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، وإذا وقعت هذه الجريمة على بريد الكتروني أو موقع أو حساب خاص بشخص اعتباري فتكون العقوبة الحبس مدة لا تقل عن ستة أشهر، وغرامة لا تقل عن مائة ألف جنيه ولا تزيد عن مائتي ألف جنيه، أو بإحدى هاتين العقوبتين.

---

(١) د/ عبد الإله النوايسة: مرجع سابق، ص ٤٩.

# خاتمة الدراسة

انتهت الدراسة إلى مجموعة من النتائج والتوصيات، أعرض لأهمها، على النحو التالي:

## نتائج الدراسة

- ❖ جرمت التشريعات محل الدراسة الدخول غير المشروع إلى الأنظمة المعلوماتية، وجاءت هذه الجريمة في مقدمة الجرائم التي تضمنتها هذه التشريعات، وهذا ما يعكس أهميتها وخطورتها.
- ❖ جرائم الدخول غير المشروع في التشريعات محل الدراسة من الجرائم الشكلية، والتي تقع تامة بمجرد الدخول دون تطلب تحقق نتيجة إجرامية.
- ❖ تعريف النظام المعلوماتي بأنه: " كل أداة أو مجموعة من الأدوات تعمل بطريقة الكترونية من خلال برنامج أو أكثر، لإنشاء، أو معالجة، أو تخزين، أو استرجاع، أو إرسال أو استقبال، أو عرض بيانات أو معلومات الكترونية"، وصلاحية هذا التعريف لأن يشمل كافة مفردات التقنية التي يمكن أن تكون محلاً للدخول غير المشروع.
- ❖ تعريف الدخول غير المشروع بأنه: "كل نشاط يفضي إلى التسلل أو الولوج إلى النظام المعلوماتي أو جزء منه، دون حق، ودون ترخيص ممن يملك السماح بذلك، أو دون استيفاء شروط الدخول".
- ❖ إن قانون مكافحة جرائم تقنية المعلومات المصري وضع تعريفـًا للاحتراق، معتبراً أن الاختراق هو الدخول غير المشروع، أو غير المصرح به؛ لكن مفهوم الدخول غير المشروع أوسع من الاختراق، فكل اختراق يعد دخولاً غير مشروع، والعكس

غير صحيح، إذ إن الاختراق معناه النفاذ إلى نظام معلوماتي محمي حماية عادية، أو تقنية؛ بينما الدخول غير المشروع قد يتم دون تجاوز أنظمة الحماية، كما لو تم الدخول خلسةً إلى نظام معلوماتي تصادف أنه مفتوح.

- ❖ إن الحماية التقنية التي وقع بشأنها الخلاف بين الفقهاء كشرط لتجريم الدخول غير المشروع هي الحماية التقنية المتخصصة، وليست الحماية العادية، وقد انقسم الفقه بشأنها إلى اتجاهين، اتجاه يرى أن هذه الحماية شرط لتجريم الدخول غير المشروع، واتجاه آخر يرى أنها ليست شرطًا للتجريم، وقد تم ترجيح الاتجاه الثاني الذي يرى أنها ليست شرطًا للتجريم، وهو الاتجاه الغالب فقهًا وتشريعًا.
- ❖ إن فكرة **"الاستئثار بالنظام المعلوماتي"** كشرط لتجريم الدخول أفضل من الحماية؛ لأن الاستئثار يعني الاستحواذ على الشيء، والاختصاص به، وهو ما يفترض أن المتحكم في النظام يقيد الدخول إليه، بينما الحماية قد لا تتوافر رغم أن صاحب النظام لا يرغب في دخول أحد إلى نظامه، كما أن وجود الحماية يلزم عنه توافر الاستئثار، بينما الاستئثار قد لا تتوافر معه حماية، مما يعني أن تطبيق فكرة الاستئثار يجعل نطاق الحماية الجنائية أوسع.
- ❖ عدم تصور الشروع في جرائم الدخول غير المشروع إذا كانت من الجرائم الشكلية، كما هو الحال في القوانين محل الدراسة، رغم أن البعض يرى عكس ذلك؛ تأسيسًا على تجريم القوانين للشروع في الجرائم المعلوماتية بنص عام؛ بيد أن ذلك لا يعني بالضرورة تصور الشروع في هذه الجرائم كافة، كما أن فعل الدخول غير قابل للانقسام، ولا توجد نتيجة مجرمة تتخلف رغم اتيان الفاعل لسلوكه؛ حتى يمكن القول بتصور الشروع، كما أن اتفاقية بودابست حددت الجرائم التي يمكن تجريم

الشروع فيها، ولم يكن من بينها الدخول غير المشروع. أما إذا كانت جريمة الدخول غير المشروع من الجرائم التي يتطلب فيها المشرع نتيجة إجرامية، كما هو الحال في القانون الأمريكي فالشروع فيها متصور.

- ❖ تظهر الحاجة إلى تجريم الدخول عن طريق الخطأ في القوانين التي لا تجرم البقاء غير المشروع؛ كالنظام السعودي، لأنه قد يعقب الدخول بالخطأ تجول في النظام وإطلاع على ما فيه من محتوى، وقد ينتج عن ذلك تخريب بالنظام، دون خضوع هذه الحالة لنص تجريمي؛ رغم أنها أخطر من الدخول المجرد المتعمد؛ أما القوانين التي تجرم البقاء غير المشروع فلا حاجة فيها إلى تجريم الدخول بالخطأ؛ لأن المتهم إذا خرج فوراً فلا إثم عليه، وإذا لم يخرج من النظام سيخضع لجريمة البقاء غير المشروع.
- ❖ إن المشرع الإماراتي سوى في العقاب بين الدخول إلى الأنظمة الخاصة بالبيانات الشخصية، وبين غيرها من الأنظمة، ولم يشدد العقاب إلا إذا نتج عن الدخول الإضرار بالبيانات الشخصية، ولم يشدد العقاب على مجرد الدخول إلى أنظمة تحوي هذا النوع من البيانات؛ ذلك أن طبيعة هذه البيانات تجعل من مجرد الاطلاع عليها ضرر بما تتيحه للمتدخل من الاطلاع على معلومات يحرص صاحبها على سريتها؛ وعليه يجدر بالمشرع تشديد العقوبة على مجرد الدخول إلى نظام معلوماتي به بيانات شخصية، وعدم الاكتفاء بعقوبة الدخول البسيط.
- ❖ -أن المشرع المصري لم يخص البيانات الشخصية بحماية خاصة في مواجهة الدخول غير المشروع، ومن ثم فإن الدخول إلى نظام معلوماتي به بيانات شخصية تقوم به جريمة الدخول البسيط وفقًا للمادة ١٤/ ١، وإذا نتج عن هذا الدخول

الإضرار بهذه البيانات الشخصية فيشدد العقاب وفقاً لنص المادة ١٤/ ٢، وفي كلتا الحالتين لا تختلف حماية البيانات الشخصية عن حماية البيانات العادية.

- ❖ أن المشرع المصري جرم تجاوز حدود الحق في الدخول بنص خاص؛ هو نص المادة الخامسة عشرة من القانون، أما المشرع الإماراتي فقد جرم تجاوز حدود التصريح مع الدخول غير المشروع بنص واحد وعقوبة واحدة، أما المشرع الفرنسي، والمنظم السعودي فلم يجرما تجاوز حدود الدخول المصرح به، ويترتب على ذلك أنه حال تجاوز حدود الدخول في النظام الفرنسي؛ فإن الفعل يشكل جريمة البقاء غير المشروع، وإذا حدث هذا التجاوز في النظام السعودي؛ فإن ذلك يظهر حاجة النظام السعودي إلى تجريم البقاء غير المشروع.
- ❖ أن النظام السعودي جرم الدخول غير المشروع في صورته البسيطة حال وقوعه على موقع الكتروني، وأغفل تجريمه حال وقوعه على المفردات الأخرى التي تضمنها تعريف الدخول غير المشروع، وهي الحواسب الآلية، وشبكاتها، والأنظمة المعلوماتية، رغم نصه على هذه المفردات في تعريف الدخول غير المشروع. أيضاً لم يجرم تجاوز حدود الدخول المشروع، ولا البقاء غير المشروع، ومن ثم فإن من يدخل نظاماً معلوماتياً بالخطأ، أي دون قصد فلا يسأل وفقاً للنظام السعودي ولو بقي في النظام عقب هذا الدخول، ومن يدخل نظام معلوماتي دخولاً مشروعاً ويتجاوز حدود هذا الدخول فلا يسأل.
- ❖ أن النظام السعودي لا يوجد به نص يشدد العقاب على الدخول البسيط إذا ترتب عليه محو البيانات أو المعلومات، أو إتلافها، أو إعادة نشرها، أو غير ذلك من صور؛ بيد أنه جرم الدخول غير المشروع إذا كان قصد المتهم التلاعب بالبيانات

أو تخريبها، وعاقب على ذلك كجريمة مستقلة عقوبتها أشد من الدخول المجرد، وذلك بموجب المادة الخامسة من النظام.

- ❖ أن المشرع المصري فرق في نصوص التجريم والعقاب بين الدخول غير المشروع إلى الأنظمة المعلوماتية للدولة، وبين الدخول إلى الأنظمة المعلوماتية الخاصة، ووضع للأولى عقوبات أشد تتناسب مع طبيعة المصالح المحمية، أما القوانين الأخرى محل الدراسة فلم تفرق بين الأنظمة المعلوماتية للدولة، والأنظمة الخاصة، وإن كان المشرع الإماراتي قد شدد عقوبة الدخول غير المشروع بقصد الحصول على بيانات حكومية.

## توصيات الدراسة

- ❖ أهيب بالفقه والقضاء تبني فكرة **"الاستئثار بالنظام المعلوماتي"** كشرط لتجريم الدخول غير المشروع، وإحلالها محل فكرة الحماية، ومفاد فكرة الاستئثار بالنظام أنه كلما تبين من ظاهر الحال أن صاحب النظام المعلوماتي يستأثر به لنفسه، أو لفئة محددة، كلما كان دخوله من الغير مجرماً، أما إذا كان ظاهر الحال يشير إلى أن صاحب النظام تركه مفتوحاً لعموم الناس فلا يعد الدخول مجرماً، ويستوي أن يكون الاستئثار صريحاً، أو ضمنياً، كما يستوي أن يستأثر به لنفسه، أو لفئة ما، إذ يظل من الغير كل من لا ينتمي للفئة المصرح لها بالدخول.
- ❖ يجب أن تنص تشريعات مكافحة جرائم تقنية المعلومات على استثناء الدخول غير المشروع من تجريم الشروع فيه، أو يحدد الجرائم التي يجرم فيها الشروع ويستبعد الدخول والبقاء منها، على غرار ما نصت عليه اتفاقية بودابست، خاصة وأن الدخول في أغلب القوانين جريمة شكلية؛ وذلك قطعاً لدابر الخلاف في هذه المسألة.

- ❖ قد يكون من الأفضل الاكتفاء بتجريم البقاء غير المشروع في القانونين المصري والإماراتي، وعدم تجريم تجاوز حدود الحق في الدخول؛ ذلك أن تجريم البقاء غير المشروع يشمل كل بقاء في الأنظمة المعلوماتية دون حق، سواءً كان ناتجاً عن دخول بالخطأ، أو ناتجاً عن تجاوز حدود الدخول المشروع، وهو ما انتهجه المشرع الفرنسي.
- ❖ يجب تشديد عقوبة الدخول غير المشروع حال ارتكابه من قبل المتخصصين في المجالات التقنية، والمعلوماتية، كالعاملين في مجال البرمجة، وصيانة الأنظمة المعلوماتية، ومصممي المواقع الالكترونية؛ إذ إن خبراتهم ومعارفهم الفنية تتيح لهم ارتكاب مثل هذه الجرائم بسهولة.
- ❖ -قد يكون من الملائم أن يفرق القانون السعودي والقانون الإماراتي بين الدخول غير المشروع إلى الأنظمة المعلوماتية الخاصة بالدولة، وبين الدخول غير المشروع إلى الأنظمة المعلوماتية الخاصة، على غرار ما انتهجه القانون المصري، وهو ما يجعل الجزاء متناسباً، أو متدرجاً حسب أهمية المصالح المحمية.
- ❖ -توصي الدراسة بأهمية إعادة صياغة بعض التعريفات، خاصة تعريف الاختراق في القانون المصري، وتعريف النظام المعلوماتي في القوانين محل الدراسة؛ حيث إن ضبط هذا التعريف يمكن أن يجعله شاملاً لكل المفردات الأخرى التي تقع عليها جرائم الدخول غير المشروع.
- ❖ -توصي الدراسة بضرورة تجريم البقاء غير المشروع في النظام السعودي، وضرورة التفرقة في العقوبة بين مجرد دخول المواقع، والدخول بقصد الإضرار بها.
- ❖ -توصي الدراسة بضرورة تشديد العقاب على الدخول غير المشروع في القانون المصري عندما يكون محله الأنظمة المعلوماتية التي تحوي البيانات الشخصية.

# قائمة المراجع

## أولاً - مراجع باللغة العربية

### ١- الكتب العامة، والمتخصصة


- د/ **إمام حسنين عطاالله**: جرائم تقنية المعلومات في التشريعات والصكوك العربية، دار جامعة نايف للنشر، الرياض، ١٤٣٩هـ-٢٠١٧م.
- د/ **أيمن عبدالله فكري**: الجرائم المعلوماتية، دراسة مقارنة في التشريعات العربية والأجنبية، مكتبة القانون والاقتصاد، ط١، ٢٠١٤م.
- م/ **حسن طاهر داود**: جرائم نظم المعلومات، ط١، أكاديمية نايف العربية للعلوم الأمنية، الرياض، ٢٠٠٠م.
- د/ **خالد خلفان المنصوري**: أركان الجريمة في القانون الجنائي الإنجليزي، أكاديمية شرطة دبي، مركز البحوث والدراسات، ط١ ، ٢٠٠٧م.
- د/ **رأفت جوهري**: المسئولية الجنائية عن أعمال وسائل الإعلام، دار النهضة العربي ، ٢٠١١م.
- د/ **رمسيس بهنام**: النظرية العامة للقانون الجنائي ، منشأة المعارف ، الإسكندرية ، ١٩٩٥م.
- د/ **عبد الفتاح الصيفي**: الأحكام العامة للنظام الجنائي في الشريعة الإسلامية والقانون، دار المطبوعات الجامعية، ٢٠١٣م.
- د/ **عبود السراج** : شرح قانون العقوبات ، القسم العام، ج١، نظرية الجريمة، د . ت، د . ن.
- د/ **محمد نصر محمد**: الوسيط في شرح الجرائم المعلوماتية، مركز الدراسات العربية للنشر والتوزيع، ط١، ٢٠١٥م.

- **د/ محمود نجيب حسني** :
  - شرح قانون العقوبات، القسم الخاص، دار النهضة العربية، ١٩٩٨م.
  - جرائم الامتناع والمسئولية الجنائية عن الامتناع، دار النهضة العربية، ١٩٨٦م.
  - النظرية العامة للقصد الجنائي، دراسة تأصيلية مقارنة للركن المعنوي في الجرائم العمدية، دار النهضة العربية، ١٩٨٨م.
- **أ/ مداوي سعيد القحطاني**: الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، مجلس التعاون لدول الخليج، الأمانة العامة، ٢٠١٦م.
- **د/ مروة زين العابدين صالح**: الحماية القانونية الدولية للبيانات الشخصية عبر الانترنت بين القانون الدولي الاتفاقي والقانون الوطني، ط١، مركز الدراسات العربية للنشر والتوزيع، ٢٠١٦م.
- د/ هلالي عبد اللاه أحمد: شرح قانون العقوبات، القسم العام، دار النهضة العربية، ط١، ١٩٨٧م.

**٢-رسائل الدكتوراه والماجستير**

- **أ/ حمودي ناصر**: الحماية الجنائية للتجارة الإلكترونية، رسالة ماجستير، جامعة الجزائر١، ٢٠١٥م.
- **د/ ختير مسعود**: النظرية العامة لجرائم الامتناع، رسالة دكتوراه، كلية الحقوق والعلوم السياسية ، جامعة أبو بكر بلقايد، تلمسان، ٢٠١٤م.
- **أ/ سفيان سوير**: الجريمة المعلوماتية، رسالة ماجستير، جامعة أبو بكر بلقايد، تلمسان، ٢٠١١م.
- **د/ صالح شنن**: الحماية الجنائية للتجارة الإلكترونية، دراسة مقارنة، رسالة دكتوراه، جامعة أبو بكر بلقايد، تلمسان، ٢٠١٣م.

- د/ **عبد المهيمن بكر سالم**: القصد الجنائي في القانون المصري والمقارن، رسالة دكتوراه، جامعة القاهرة، ١٩٥٩م.
- د/ **عزيزة رابحي**: الأسرار المعلوماتية وحمايتها الجزائية، رسالة دكتوراه، جامعة أبو بكر بلقايد، تلمسان، ٢٠١٨م.
- د/ **محمد سعيد عبد الرحمن**: المسئولية الجنائية للأشخاص المعنوية في قانون العقوبات الاتحادي لدولة الإمارات العربية المتحدة، رسالة دكتوراه، جامعة القاهرة، ٢٠١٤م.
- أ/ **منصور بن سعيد القحطاني**: مهددات الأمن المعلوماتي وسبل مواجهتها، دراسة مسحية على منسوبي مركز الحاسب الآلي بالقوات البحرية الملكية السعودية بالرياض، رسالة ماجستير، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية،٢٠٠٨م.
- أ/ **نسيمة جدي**: جرائم المساس بأنظمة المعالجة الآلية للمعطيات، رسالة ماجستير، جامعة وهران، الجزائر، ٢٠١٤ م.

**٣- المقالات والأبحاث والمؤتمرات والندوات**

- د/ **إبراهيم داود، د/ أشرف شعت**: الاطلاع على البريد الالكتروني بين متطلبات النظام العام والحق في سرية المراسلة، مجلة دفاتر السياسة والقانون، ع١٦، يناير ٢٠١٧م.
- د/ **إبراهيم داود**: الحماية القانونية للبيانات الشخصية من منظور الحق في الخصوصية، دراسة تحليلية مقارنة، مجلة الحقوق للبحوث القانونية والاقتصادية ، ٢٠١٧م.

- د/ **أسامة غانم العبيدي** : جريمة الدخول غير المشروع إلى النظام المعلوماتي ، دراسة قانونية في ضوء القوانين المقارنة، مجلة دراسات المعلومات، ع١٤، مايو ٢٠١٢م.
- د/ **حسن مظفر**: الأمن المعلوماتي، معالجة قانونية أولية، مجلة الأمن والقانون، أكاديمية شرطة دبي، مج١٢، ع١، يناير ٢٠٠٤م.
- د/ **خالد حامد مصطفى**: المسئولية الجنائية لناشري الخدمات التقنية ومقدميها عن سوء استخدام شبكات التواصل الاجتماعي، مجلة رؤى استراتيجية، مركز الإمارات للدراسات والبحوث الاستراتيجية، مج١، ع٢، مارس٢٠١٣م.
- د/ **خالد ممدوح إبراهيم**: الحماية الجنائية للتجارة الإلكترونية في القانون الاتحادي رقم ٢ لسنة ٢٠٠٦م بشأن مكافحة جرائم تقنية المعلومات، مجلة الفكر الشرطي، مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، مج٢٣، ع٨٨، يناير ٢٠١٤م.
- د/ **دينا عبد العزيز فهمي**: المسئولية الجنائية الناشئة عن اساءة استخدام مواقع التواصل الاجتماعي، بحث مقدم في المؤتمر العلمي الرابع لكلية الحقوق، جامعة طنطا، القانون والإعلام، ٢٣-٢٤ أبريل، ٢٠١٧م.
- د/ **سامح عبد الواحد التهامي**: الحماية القانونية للبيانات الشخصية، دراسة في القانون الفرنسي، مجلة الحقوق، الكويت، مج٣٥، ع٣، سبتمبر ٢٠١١م.
- د/ **سامي الرواشدة، د/ أحمد الهياجنة**: مكافحة الجريمة المعلوماتية بالتجريم والعقاب، القانون الإنجليزي نموذجاً، المجلة الأردنية في القانون والعلوم والسياسة، مج١، ع٣، ٢٠٠٩م.
- د/ **سامي الرواشدة**: الأدلة المتحصلة من مواقع التواصل الاجتماعي ودورها في الإثبات الجنائي: دراسة في القانونين الإنجليزي والأمريكي المجلة الدولية للقانون، ٢٠١٧م.

- **أ/ سامية عبد الرازق:** جريمة اختراق أنظمة المعلومات، جامعة البصرة، مجلة العلوم القانونية، مج١٥، ع١، ٢٠١٠م.
- **د/ سومية عكور:** الجرائم المعلوماتية وطرق مواجهتها، ورقة علمية، الملتقى العلمي: الجرائم المستحدثة في ظل التغيرات والتحولات الإقليمية والدولية، كلية العلوم الاستراتيجية، عمان، الأردن، ٢-٤/ ٩/ ٢٠١٤م.
- **شول ابن شهرة:** آليات مكافحة الجريمة المعلوماتية، مواقع التجارة الالكترونية نموذجـًا، مجلة دراسات، الجزائر، ع١٣، مارس ٢٠١٠م.
- **د/ عبد الإله النوايسة:** جريمة الدخول غير المشروع في تشريعات الجرائم الإلكترونية العربية، دراسة مقارنة، المجلة القانونية والقضائية، مركز الدراسات القانونية والقضائية، وزارة العدل، قطر، ع١، س١٠، ٢٠١٦م .
- **د/ عبد الحليم بوقرين:** قانون مكافحة جرائم تقنية المعلومات الكويتي، دراسة مقارنة، مجلة كلية القانون الكويتية العالمية، ع٤، س٥، ديسمبر ٢٠١٧م.
- **د/ عبيد صالح حسن:** سياسة المشرع الإماراتي لمواجهة الجرائم الإلكترونية، مجلة الفكر الشرطي، مج٢٤، ع٩٥، أكتوبر ٢٠١٥م.
- **د/ فضيلة عاقلي:** الجريمة الالكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، بحث مقدم ضمن أعمال المؤتمر الدولي الرابع عشر، الجرائم الالكترونية، طرابلس،٢٤-٢٥ مارس ٢٠١٧م.
- **د/ محمد خليفة:** الأحكام المشتركة لجرائم المعطيات في قانون العقوبات الجزائري والمقارن، مجلة التواصل في العلوم الإنسانية والاجتماعية، الجزائر، ع٣٠، يونيو ٢٠١٢م.

- **د/ محمد مزاولي**: المسئولية الجنائية للأشخاص الاعتبارية عن جريمة المساس بأنظمة المعالجة الآلية للمعطيات، مجلة الفقه والقانون، المغرب، ع٢٣، سبتمبر٢٠١٤م.
- **د/ محمد نصر القطري**: الإشكاليات القانونية لحماية سلامة المعلومات، دراسة تطبيقية على الحماية الجنائية من الإتلاف المعلوماتي، مجلة الفكر الشرطي، مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، مج٢٤، ع٩٣، أبريل ٢٠١٥م.
- **أ/ مختارية بوزيدي**: ماهية الجريمة الالكترونية، بحث مقدم في الملتقى الوطني: آليات مكافحة الجرائم الالكترونية في التشريع الجزائري، مركز جيل البحث العلمي، الجزائر، ٢٩ / ٣/ ٢٠١٧م.
- **د/ مهند وليد الحداد**: التنظيم القانوني لجريمة الدخول غير المصرح به إلى نظام الحاسب الآلي، مجلة العلوم الشرعية، جامعة القصيم، المملكة العربية السعودية، مج١١، ع١، سبتمبر ٢٠١٧م.
- **د/ موفق علي عبيد، د/ ساهر ماضي ناصر**: ماهية جريمة الاحتيال المعلوماتي، مجلة جامعة تكريت للعلوم القانونية، س٧، ع٢٥، ٢٠١٥م.
- **د/ نجاة عباوي**: الإشكاليات القانونية في تجريم الاعتداء على أنظمة المعلومات، مجلة دفاتر السياسة والقانون، ع١٦، يناير٢٠١٧م.
- **د/ هالة كمال نوفل، د/ اسماعيل محمود حسن**: جرائم اختراق البيئة المعلوماتية، استشراف الاتجاهات الحديثة في مجال أمن المعلومات، دراسة إبستيمولوجية في ضوء أراء عينة من المتخصصين، المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية، كلية علوم الحاسب والمعلومات ، جامعة الإمام محمد بن سعود الإسلامية ، الرياض، ٢٠١٥م.

- أ/ **وسيم طعمة**: السرقة المعلوماتية، دراسة مقارنة، مجلة جامعة البعث، مج٣٩، ع٦٨، ٢٠١٧م .


## ثانياً- مراجع باللغة الفرنسية


- **Bernard Bouloc** : Maintien frauduleux dans un système de traitement automatisé de données , RTD. Com., 2015.
- **Belkasem Hamid**: Loi Godfrain: état de la jurisprudence français.
- https://sites.google.com/site/cyberhamid2/loi-godfrain-etat-de-la-jurisprudence-francaise
- **BOOS, Romain**: La lutte contre la cybercriminalité au regard de l'action des États. 2016. PhD Thesis. Université de Lorraine.
- **Cécile Duhil de Bénazé** : Maintien frauduleux dans un fichier et vol de données: l'occasion peut faire le larron, Dalloz actualité, 5 juin 2015 .
- **Christiane Féral-Schuhl**: L'accès frauduleux au système d'information de Greenpeace puni , Expériences , Juridique , 2012 , article disponible sur le site :
  - http://www.feral-avocats.com/wp- content/uploads/2013/09/01info06022012.pdf
- **Christian Le Stanc:** Ne commet pas le délit d'accès et de maintien frauduleux dans un système de traitement automatisé de données l'internaute qui utilise un logiciel répandu pour pénétrer dans un système non protégé , Recueil Dalloz , 2003.
- **DIMITRIOU, Philippe**: L'application du droit de la cryptologie en matière de sécurité des réseaux informatiques. 2002. PhD Thesis. thesis dari DEA Défense Nationale option Sécurité européenne et internationale, Université de Lille 2.
- **Frédérique CHOPIN**: Cybercriminalité , Répertoire de droit pénal et de procédure pénale , DALLOZ, 2013.
- **Géraldine Péronne et Emmanuel Daoud**: cyberattaques: la lutte s'intensifie, Actualité Juridique Pénal. Septembre 2015, n° 9.
- **Ibtissem Maalaoui**: Les infractions portant atteinte à la sécurité du système informatique d'une entreprise , thèse de magistère , Université de Montréal , Septembre 2011.
- **Jacques Francillon**: Piratage informatique. Collecte de renseignements commerciaux. Délit de maintien frauduleux dans un système de traitement automatisé de données , RSC , 2008.
- **Monika Zwolinska**. Sécurité et libertés fondamentales des communications électroniques en droit français, européen et international. Droit. Université Nice Sophia Antipolis, 2015.
- **Pradel, Jean**: "Les infractions relatives à l'informatique." Revue internationale de droit comparé 42, no. 42 (1990): 815-828.


## ثالثاً- مراجع باللغة الانجليزية


- **BREGANT, Jessica; BREGANT, Robert**: Cybercrime and Computer Crime. The Encyclopedia of Criminology and Criminal Justice, 2014

- **DOYLE, Charles**: Cybercrime: an overview of the federal computer fraud and abuse statute and related federal criminal laws. Diane Publishing, 2011.
- **MOISE, Adrian Cristian**:Modernization of Romanian legislation on preventing and combating cybercrime and implementation gap at European level. Revista de Stiinte Politice, 2015.
- **PICOTTI, Lorenzo; SALVADORI, Ivan**: National legislation implementing the Convention on Cybercrime-Comparative analysis and good practices. 2008.
- **SUKHAI, Nataliya B**: Hacking and cybercrime. In: Proceedings of the 1st annual conference on Information security curriculum development. ACM, 2004.
- **WANG, Q**: A Comparative Study of Cybercrime in Criminal Law: China, US, England, Singapore and the Council of Europe. 2016. PhD Thesis. Erasmus School of Law.

# فهرس الموضوعات