مجلة الحقوق

فصلية علمية محكمة - تصدر عن مجلس النشر العلمي - جامعة الكويت

التنظيم الموضوعي لجرائم الدخول الإلكترونية سنداً لقانون الجرائم الإلكترونية الأردني رقم (٢٧) لسنة ٢٠١٥ "دراسة مقارنة"

الدكتور/ مأمون "محمد سعيد" إبراهيم أبو زيتون
الأستاذ الدكتور/ مؤيد محمد علي القضاة

جامعة الكويت
KUWAIT UNIVERSITY

ISSN: 1029 - 6069

العدد ٢ - السنة ٤٧

ذو الحجة ١٤٤٤هـ - يونيو ٢٠٢٣م

التنظيم الموضوعي لجرائم الدخول الإلكترونية سنداً لقانون الجرائم الإلكترونية الأردني رقم (٢٧) لسنة ٢٠١٥ دراسة مقارنة

الدكتور/ مأمون "محمد سعيد" إبراهيم أبو زيتون*

الأستاذ الدكتور/ مؤيد محمد علي القضاة**

ملخص:

يعالج البحث جريمة مستحدثة ظهرت في قانون الجرائم الإلكترونية الأردني رقم (٢٧) لسنة ٢٠١٥، ألا وهي جرائم الدخول الإلكترونية، والتي تتمثل، سنداً للمادتين (٣ و١٢) من القانون السابق الذكر، بالدخول دون تصريح، أو بما يخالف أو يجاوز التصريح إلى الشبكة المعلوماتية أو إلى نظام معلوماتي، أو إلى موقع إلكتروني. وتتمثل أهم النتائج التي توصل إليها البحث بضرورة النص بصورة صريحة على السلوك الجرمي المتمثل بالدخول خطأ والاستمرار بالبقاء في النظام المعلوماتي بعد العلم بخطئه.

الكلمات الدالة: جرائم الدخول الإلكترونية، النظام المعلوماتي، المجرم المعلوماتي، جريمة عابرة للحدود، الدخول دون تصريح، تجاوز التصريح.

مقدمة:

تعد جرائم الدخول الإلكترونية من أخطر الجرائم الواردة في قانون الجرائم الإلكترونية الأردني، حيث تعتبر حجر الأساس لكل الجرائم الإلكترونية الأخرى، فأي شخص يريد أن يرتكب أي جريمة من الجرائم الواردة في هذا القانون بداية من جرائم تزوير المستندات الإلكترونية، ومروراً بجرائم الابتزاز أو التهديد، ووصولاً إلى جرائم الإضرار بمصالح الدولة والإساءة إلى هيبتها، كل ذلك يتطلب أولاً إما الدخول دون تصريح، أو بما يخالف أو يجاوز التصريح إلى الشبكة المعلوماتية أو إلى الأنظمة المعلوماتية[١].

(*) الباحث الرئيس: عضو هيئة تدريس في جامعة الشارقة، وأستاذ القانون الجنائي المشارك في جامعة اليرموك.

(**) الباحث المشارك: عضو هيئة تدريس في جامعة الإمارات – دولة الإمارات العربية المتحدة، وأستاذ القانون الجنائي في جامعة اليرموك.

(١) محمد الشناوي، إستراتيجية مكافحة جرائم النصب المستحدثة، الإنترنت، بطاقات الائتمان، الدعاية التجارية الكاذبة، سنة ٢٠٠٦، ص٧١.

وتهدف هذه الدراسة إلى تحليل النصوص القانونية الناظمة لهذه الجرائم، للتعريف بها[٢]، وبيان أركانها، وعناصرها، وشروطها، وكيفية تجنبها، واكتشافها في حال وقوعها، وتبصير المجني عليهم بها، وحثهم، تحت طائلة المسؤولية القانونية، للتبليغ عنها لملاحقتها والحد منها[٣].

إضافة إلى ذلك تهدف هذه الدراسة إلى تتبع الخطوات التشريعية التي انتهجها المشرع الأردني بدءاً من قانون جرائم أنظمة المعلومات المؤقت رقم (٣٠) لسنة ٢٠١٠، وانتهاءً بقانون الجرائم الإلكترونية رقم (٢٧) لسنة ٢٠١٥، وذلك بقصد مقارنة هذه الخطوات التشريعية مع مثيلاتها من التشريعات المقارنة لمعرفة مواطن القوة والضعف فيها، وما إذا كانت قد أدت الغرض والغاية منها أم لا؟

علاوة على ذلك تهدف هذه الدراسة إلى بيان موقف القضاء، والفقه المحلي والمقارن، هذا بالإضافة إلى موقف التشريعات المقارنة من المسائل القانونية التي لم يتعرض لها التشريع الأردني، وذلك لتطوير النصوص القانونية الناظمة لهذا النوع من الجرائم أولاً، والحد من **الظاهرة الإجرامية** ثانياً. أخيراً تهدف هذه الدراسة إلى تقديم مقترحات وتوصيات تساعد في سد الثغرات القانونية **والعيوب** التشريعية التي تعاني منها تلك النصوص القانونية.

وتتمثل أهمية هذه الدراسة في أن هذا النوع من الجرائم بدأ يتزايد ويتطور بشكل كبير نظراً للتطور التكنولوجي، كما أنه بدأ يهز ثقة كثير من الناس بالتقنية المعلوماتية، ويهدد اقتصاديات كثير من الدول[٤]، الأمر الذي أصبح معه من الضروري مسايرة ذلك التطور بأبحاث ودراسات تركز على البعد القانوني لهذه الجرائم، وتبيّن الطريق السليم الذي يجب على المشرع اتخاذه لإعادة النظر، والتوازن، والاستقرار في

(٢) سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الإنترنت، دار الفكر الجامعي٢٠٠٧م، ص٣٥.

(٣) من الأسباب القانونية لتزايد هذه الجريمة هو عدم معرفة المجني عليهم بتعرض أنظمتهم المعلوماتية لهذا النوع من الاعتداء. كما وترجع الأسباب إلى إحجام عدد لا بأس به من المجني عليهم عن التبليغ عن هذا النوع من الجرائم، وذلك لعدم اهتزاز ثقة الناس بهم.

(٤) ففي دراسة قانونية، تم التصريح عنها في فعاليات وجلسات مؤتمر (أثر الاقتصاد الإلكتروني على تنمية منطقة الشرق الأوسط وشمال إفريقيا) المنعقد في قاعة الحمرا للمؤتمرات في رأس الخيمة، في دولة الإمارات العربية المتحدة، فقد قُدر حجم خسائر العالم من جرائم الإنترنت لعام (٢٠١٤) وحده ما بين (١٠٠ إلى ٥٠٠ مليار) دولار أمريكي.

القوانين الناظمة لها، وإلا فستظهر ثغرات، وفراغات قانونية وتشريعية، نتيجة لذلك التطور، تساعد على الإفلات من العقاب، وعدم تحقيق الغاية المرجوة من القانون.

إضافة إلى ذلك تتمثل أهمية هذه الدراسة في أن هذا النوع من الجرائم لم يعد يرتكب من قبل الجناة، بقصد إثبات البراعة الإلكترونية، أو بقصد ارتكاب بعض الجرائم التقليدية البسيطة كجرائم الاعتداء على الحياة الخاصة للأفراد(٥)، أو على البنوك، أو على الشركات، وإنما بدأت ترتكب بقصد الاعتداء على كثير من القطاعات الهامة في الدولة، كقطاع الموانئ، والطيران، والصحة، والتعليم، والسياحة، هذا بالإضافة إلى قطاع الأمن الداخلي والخارجي للدول، فالمتابع للتطور الحقيقي والسريع لهذا النوع من الجرائم يجد بأنه قد بات يشكل اعتداءً صارخاً على استقلال، وسلامة، ودستور، وهيبة، وأمن كثير من الدول، هذا بالإضافة إلى أمن الشعوب، ووحدتها، واستقرارها ونظام الحكم لدى كثير من الدول(٦).

كذلك الأمر تتمثل أهمية هذه الدراسة في أن هناك دولاً لم تضع **حتى** الآن قواعد قانونية ناظمة لهذا النوع من الجرائم، مما جعل منها قواعد آمنة تنطلق منها جرائم الدخول الإلكترونية العابرة للقارات(٧)، مهددة أمن واستقرار كثير من الدول، وواضعة إياها أمام تحديات كبيرة جداً تتمثل بملاحقة هذا النوع من الجرائم، وضبط مرتكبيها. ومما يعزز من أهمية هذه الدراسة هو أن هذا النوع من الجرائم ساعد الجناة على اقتراف جرائمهم التقليدية، والإفلات من العقاب خصوصاً مع ظهور شبكة الإنترنت، التي ساعدت على اقتراف الجرائم عن بعد، ودون آثار أو أدوات، تساعد في كشف الجريمة، الأمر الذي كبّد كثيراً من الدول مليارات الدولارات لملاحقة هذا النوع من الجرائم الإلكترونية(٨).

---

(٥) بولين أنطونيوس أيوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، لبنان، منشورات الحلبي الحقوقية، ٢٠٠٩، ص٤٠. عدد كبير من الجناة أصبحوا يلجؤون إلى هذا النوع من الجرائم للاعتداء على الحياة الخاصة للأفراد، التي صانتها الحضارات القديمة، والأديان السماوية، والدساتير والقوانين الوضعية في غالبية دول العالم، خصوصاً وأن التطور التكنولوجي أدى إلى ظهور وسائل التواصل الاجتماعي بأنواعها كافة التي باتت تزخر بكم هائل من المعلومات الشخصية، والفيديوهات، والصور وغير ذلك من المواضيع المتعلقة بالخصوصية.

(٦) سامي جاد عبد الرحمن واصل، إرهاب الدولة في إطار قواعد القانون الدولي العام، دار النهضة العربية، الطبعة الأولى، ٢٠٠٣، ٢٠٠٤، ص ١.

(٧) حسين، محمد، المسؤولية القانونية في مجال شبكات الإنترنت، دار النهضة العربية القاهرة، ٢٠٠٢. ص ٨.

(٨) Dannecker, BB 1996, S. 1285ff.; Tilch, ComputerkriminalitÌt, Deutsches Rechts-Lexikon, Bd. 1 1993, S. 883.

أخيراً تتمثل أهمية هذه الدراسة في قلة عدد البحوث المتخصصة في هذا النوع من الجرائم على صعيد القانون الأردني، الأمر الذي حدا بنا إلى طرق باب هذه الجرائم آملين أن نصل إلى نتائج، ومقترحات، وتوصيات قادرة على تقديم إضافة علمية بسيطة ومتواضعة للمكتبة القانونية الأردنية، وقادرة على الحد من هذا النوع من الجرائم التي أصبح يئن تحت وطأتها كثير من دول العالم.

وتتركز أبعاد هذه الدراسة ومحدداتها على التنظيم الموضوعي لجرائم الدخول الإلكترونية، أما بالنسبة للتنظيم العقابي والإجرائي فسيتم التعرض له في دراسة مستقلة بشيء من التفصيل.

وللوقوف على أهداف هذه الدراسة، وأهميتها، وأبعادها، ولمعرفة موقف التشريع الأردني منها، ولإعطاء رؤية واضحة ودقيقة عن الموضوع، وعن أبعاده، وسماته، وعلاقته بغيره من المواضيع، ولمقارنة التشريع الأردني بغيره من التشريعات المقارنة، فقد اعتمدنا على المنهج الوصفي، والتحليلي، والمقارن، ليس فقط من أجل عرض أحكام كل قانون وبيان الاختلاف والتشابه بينهما، بل أيضاً لتفسير أسباب ومظاهر الخلاف بين هذه القوانين، ومعرفة أيهما أفضل في كل مسألة قانونية، لنخلص إلى توصيات تخدم التشريع الوطني.

المشكلة البحثية:

تتمثل المشكلة البحثية الرئيسة بدراسة ما إذا كانت النصوص القانونية الأردنية الناظمة لهذا النوع من الجرائم، العابرة للحدود وللقارات، موفقة أم لا، خصوصاً في ظل عدم الانسجام التشريعي الدولي في هذا الخصوص، وإقليمية قانون العقوبات، ويتفرع عن هذه المشكلة الرئيسة عدة تساؤلات، وهي:

١ – هل يجب أن يكون النظام المستهدف محمياً بكلمة سر، حتى يمكن القول بقيام جرائم الدخول الإلكترونية؟

٢ – إذا كان هناك تصريح بالدخول، وحصل تجاوز للوقت المسموح به، أو للموضوع المصرح له الدخول إليه، فهل يعد هذا السلوك صورة من صور جرائم الدخول الإلكترونية، خصوصاً وأن الغاية من التجريم والمتمثلة بحماية المعلومات والبيانات الإلكترونية غير متوافرة؟

٣ – هل تتحقق النتيجة الجرمية بمجرد الدخول، أم أنه يجب على الفاعل أن يطّلع على معلومات، أو على بيانات إلكترونية؟

٤ – ما هو أثر العدول على جرائم الدخول الإلكترونية، وما هو الوضع القانوني للأعمال

التحضيرية المتعلقة بالاتفاق الجنائي على ارتكاب جرائم الدخول الإلكترونية بشكل خاص، والجرائم الأخرى بشكل عام؟

فرضيات الدراسة:

١ – تزداد جرائم الدخول الإلكترونية في الدول التي تشهد تطوراً تكنولوجياً سريعاً عن الدول التي لا تشهد مثل ذلك التطور.

٢ – هناك علاقة إيجابية دالة إحصائية بين التعديل المستمر للقوانين الناظمة لجرائم الدخول الإلكترونية وبين معدل ارتفاع الجريمة.

٣ – الملاحقة الناجعة لهذا النوع من الجرائم يتأثر بجودة القوانين، وبمدى التعاون الدولي في مجال التحقيق الابتدائي، والنهائي، وفي مجال تسليم المجرمين.

٤ – إخضاع عقوبة الشروع في جرائم الدخول الإلكترونية للقواعد العامة يؤثر سلباً على الحد من هذا النوع من الجرائم.

٥ – لا تتأثر الجريمة بالوسيلة المستخدمة لارتكابها في كثير من الحالات.

وللإجابة عن الإشكالية البحثية الرئيسة، وعلى التساؤلات المتفرعة عنها، فقد تم تقسيم هذه الدراسة إلى مبحثين: خصصنا الأول منهما لدراسة الركن المادي لجرائم الدخول الإلكترونية، والثاني لدراسة الركن المعنوي لجرائم الدخول الإلكترونية، كذلك الأمر فقد اختتمنا هذا البحث بخاتمة وتوصيات متواضعة، نأمل أن تترجم إلى واقع عملي، وأن ترى الضوء في أول تعديل للقانون.

المبحث الأول
الركن المادي لجرائم الدخول الإلكترونية

يقسم هذا المبحث إلى مطلبين: خصصنا الأول منهما لدراسة صور جرائم الدخول الإلكترونية، والثاني لدراسة نتائج جرائم الدخول الإلكترونية.

المطلب الأول
صور جرائم الدخول الإلكترونية

يقسم هذا المطلب إلى فرعين: خصصنا الأول منهما لدراسة الدخول إلى الشبكة المعلوماتية أو النظام المعلوماتي، والثاني لدراسة الدخول إلى الموقع الإلكتروني.

الفرع الأول: الدخول إلى الشبكة المعلوماتية أو النظام المعلوماتي

يعالج التشريع الأردني جرائم الدخول إلى الشبكة المعلوماتية أو إلى النظام المعلوماتي في المادتين (٣ /أ، ب) و(١٢/أ، ب) من قانون الجرائم الإلكترونية[٩]، حيث يتمثل السلوك الجرمي لهاتين الجريمتين بالدخول دون تصريح، أو بما يخالف أو يجاوز التصريح إلى الشبكة المعلوماتية أو النظام المعلوماتي[١٠]. ويتوافر الدخول

(٩) تقضي المادة (٣) بأنه: أ. يعاقب كل من دخل قصداً إلى الشبكة المعلوماتية أو نظام معلومات بأي وسيلة دون تصريح أو بما يخالف أو يجاوز التصريح، بالحبس مدة لا تقل عن أسبوع ولا تزيد على ثلاثة أشهر أو بغرامة لا تقل عن (١٠٠) مائة دينار ولا تزيد على (٢٠٠) مائتي دينار أو بكلتا هاتين العقوبتين. ب. إذا كان الدخول المنصوص عليه في الفقرة (أ) من هذه المادة لإلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو توقيف أو تعطيل عمل الشبكة المعلوماتية، أو نظام معلومات الشبكة المعلوماتية، فيعاقب الفاعل بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن (٢٠٠) مائتي دينار ولا تزيد على (١٠٠٠) ألف دينار". تقضي المادة (١٢) من القانون نفسه بأنه: "أ. يعاقب كل من دخل قصداً دون تصريح أو بما يخالف أو يجاوز التصريح إلى الشبكة المعلوماتية أو نظام معلومات بأي وسيلة كانت بهدف الاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني بالحبس مدة لا تقل عن أربعة أشهر وبغرامة لا تقل عن (٥٠٠) خمسمائة دينار ولا تزيد على (٥٠٠٠) خمسة آلاف دينار. ب. إذا كان الدخول المشار إليه في الفقرة (أ) من هذه المادة، بقصد إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو تعديلها أو تغييرها أو نقلها أو نسخها أو إفشائها، فيعاقب الفاعل بالأشغال الشاقة المؤقتة وبغرامة لا تقل عن (١٠٠٠) ألف دينار ولا تزيد على (٥٠٠٠) خمسة آلاف دينار".

(١٠) See S. Al-Rawashdeh, Illegal Access to Information System in the Qatari Criminal Laws: A Comparative Study, Kuwait International Law School Journal, vol (6) Iss. (1), (2018), P 34.

دون تصريح، عندما لا يكون هناك تصريح من الشخص المختص أصلاً[١١]، أو عندما يكون الدخول مشروطاً بأمر معين كدفع ثمن أو رسم أو غير ذلك من الشروط، ويقوم المشتكى عليه على الرغم من ذلك بالدخول[١٢].

وقد يحصل الدخول بصورة إيجابية ومباشرة، كما لو حصل عن طريق الجهاز المعلوماتي نفسه، أو بصورة غير مباشرة عن طريق الإنترنت[١٣]. كذلك الأمر فقد يحصل الدخول بصورة سلبية كما لو امتنع المشتكى عليه المكلف بحماية النظام المعلوماتي عن منع شخص من الدخول إلى ذلك النظام على الرغم من أن هذا الأمر من واجبه وفي مقدوره. ولا تهم وسيلة الدخول والتي قد تكون كلمة السر الحقيقية، أو برامج مشفرة، أو الرقم الكودي، أو عن طريق شخص آخر مصرح له بالدخول، أو عن طريق تحريك الماوس (محرك البحث)[١٤].

أما بالنسبة لمخالفة التصريح، أو التجاوز عليه[١٥] فيتوافران عندما يكون هناك تصريح مقيد بوقت، أو بموضوع، أو بعمل معين، ويخالف المشتكى عليه ذلك

(١١) علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة الإلكترونية، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، سنة ٢٠٠٠، ص٥٠؛ مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية، ص٥١، دار النهضة العربية.

(١٢) محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، سنة ٢٠٠٧، ص١٣٩.

(١٣) يتم الدخول في هذه الحالة عن طريق برامج متوافرة على شبكة الإنترنت، فيعمل الفاعل اتصال بين الحاسب الآلي المستهدف وحاسبه الآلي، ويبدأ يتصرف بالملفات والبيانات الإلكترونية عن بعد، فيتصفح ما يريد ويشطب أو يضيف ما يريد، لذا فمن الأفضل أن يفصل الموظف جهازه عن النت عند مغادرة المكتب. كما قد يتم الدخول عن طريق إرسال ملف تجسسي أتاجمنت عن طريق البريد الإلكتروني، أو عن طريق نظام المحادثة، فيرسل الفاعل إلى المجني عليه برنامجاً ويقول له بأن هذا البرنامج يحمل ألعاباً، فيدوهات، مسابقات، تخفيضات على سلع معينة، فينخدع المجني عليه ويستقبل الملف التجسسي، كما قد يتم إرسال الملف التجسسي عن طريق إغراء المجني عليه وحثه على زيارة برامج ومواقع إلكترونية، فينغري بها ويقوم بتحميلها على جهازه وهي تحمل الملف التجسسي.

(١٤) منير محمد الجنبيهي وممدوح محمد الجنبيهي جرائم الإنترنت والحاسب الآلى ووسائل مكافحتها، دار الفكر الجامعي٢٠٠٥، ص ١٦.

(١٥) على النقيض من ذلك هناك رأي فقهي، سيتم التعرض له بشيء من التفصيل عند الحديث عن النتيجة الجرمية، يقول بأن تجاوز الوقت المعين لا يؤدي إلى قيام هذه الجريمة، وذلك لانتفاء الغاية المتمثلة بحماية البيانات والمعلومات الإلكترونية التي لم تعد تتمتع بحماية عندما أجاز المجني عليه للمشتكى عليه الدخول إليها.

التصريح أو يتجاوز عليه[١٦]، والأمثلة على ذلك كثيرة نذكر منها أن يكون التصريح مقيداً بساعة معينة، ويتجاوز المشتكى عليه ذلك الوقت، أو عندما يكون التصريح مقيداً بموضوع معين كأن يكون مقيداً بالدخول إلى سجل المكالمات مثلاً، ويقوم المشتكى عليه بالدخول إلى ملف الصور أو ملف الفيديوهات، أو عندما يكون التصريح مقيداً بعمل معين كتنزيل برنامج مثلاً على الكمبيوتر، أو كعمل سوفت وير للجهاز، ويقوم المشتكى عليه بفتح ملفات أخرى دون تصريح.

والسؤال الآن، ما هو الوضع القانوني إذا قام شخص مصرح له بالدخول إلى النظام المعلوماتي، بالدخول إلى ذلك النظام والقيام بعمل غير مشروع، ومثال ذلك أن يقوم موظف مصرح له الدخول إلكترونياً إلى مخالفات السير مثلاً بالدخول إلى النظام المعلوماتي وإفشاء، أو شطب مخالفة سير عن صديق له، فهل يمكن القول في هذه الحالة بأن ذلك الموظف قد خالف أو تجاوز على التصريح؟ المتابع للنصوص القانونية السابقة الذكر يجد بأنها تشترط أن يخالف أو يتجاوز المشتكى عليه على التصريح، وليس على العمل الممنوح له، بالاعتماد على ذلك الأمر لا يمكن القول بقيام السلوك الجرمي في هذه الحالة، وذلك لأن هناك تصريحاً ممنوحاً للمشتكى عليه بالدخول[١٧]، أما الذي حصل فهو تجاوز على العمل الذي يقوم به، وليس على التصريح الممنوح له.

والسؤال الآن ما هو الفرق بين مخالفة التصريح، والتجاوز عليه، فهل هناك مبرر قانوني لإدراج هذين السلوكين من قبل المشرع الأردني، أم أنهما عبارة عن مترادفين؟

لم يعرّف التشريع الأردني هذين السلوكين، ولم يبين الفرق بينهما، كذلك الأمر بالنسبة للفقه والقضاء، فالمتابع لهما يجد بأنهما لم يعرفا هذين السلوكين أيضاً، ولم يبينا الفرق بينهما، وفي هذا الخصوص نجد بأن هذين المصطلحين قريبان من بعضها بعضاً، ولا يكاد يكون فرق بينهما، بالاعتماد على ذلك الأمر يمكن القول بأن هناك تزيّداً لا حاجة له من قبل التشريع الأردني، حيث كان من الأفضل أن يقصر

(١٦) يتم التجاوز على العمل كما لو سلم المجني عليه حاسوبه الشخصي لإجراء تصليح مثلاً، وقام المشتكى عليه بحذف أو بنسخ بعض البيانات أو المعلومات الإلكترونية. وإذا كان المجني عليه قد وضع كلمة سر لبعض الملفات، وقام الفاعل أثناء تصليح النظام المعلوماتي مثلاً بتهكير كلمة السر لذلك الملف ودخل إليه، فيعد الدخول في هذه الحالة دون تصريح، وليس بما يجاوز التصريح. وليس هناك أهمية قانونية للتفريق بين هذين السلوكين؛ وذلك لأن العقوبة واحدة.

(١٧) نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، دراسة نظرية وتطبيقية، الطبعة الأولى، سنة ٢٠٠٥، ص٣٣٢، منشورات الحلبي الحقوقية، بيروت - لبنان.

الأمر على أحدهما. ما يؤيد ذلك موقف كثير من التشريعات المقارنة، فالمتابع للمادة (٢\١) قانون مكافحة جرائم تقنية المعلومات الإماراتي رقم (٥) لسنة ٢٠١٢، يجد بأنها لم تتعرض للفظ مخالفة التصريح مكتفية بلفظ الـ "تجاوز"[١٨]. كذلك الأمر بالنسبة للمادة (٣) من قانون مكافحة الجرائم الإلكترونية القطري رقم (١٤) لسنة ٢٠١٤، والتي استخدمت لفظ الدخول عمداً دون وجه حق، ولفظ التجاوز على الدخول المصرح به[١٩]، ولم تستخدم لفظ مخالفة التصريح.

والسؤال الذي يثار في هذا المقام، ما هو الوضع القانوني إذا دخل المشتكى عليه خطأ إلى نظام معلومات مثلاً، واكتشف خطأه، واستمر في البقاء قصداً، فهل يمكن القول بتوافر الدخول دون تصريح، أو بما يخالف أو يجاوز التصريح في هذه الحالة، بتعبير آخر هل يمكن تجريم هذا السلوك حسب المادتين (٣ و١٢) قانون الجرائم الإلكترونية الأردني؟ في البداية تجدر الإشارة إلى أن الدخول خطأ والاستمرار بالبقاء بعد معرفة الخطأ لا يشكل مخالفة للتصريح، أو تجاوز على التصريح؛ وذلك لأن هذين السلوكين يشترطان أن يكون هناك تصريح في البداية ويحصل مخالفة أو تجاوز عليه، وهذا لا يتفق مع الحالة السابقة الذكر، وذلك لأنه لم يكن مع المشتكى عليه منذ البداية تصريح بالدخول، فالذي حصل هو أن المشتكى عليه قد دخل خطأ واستمر بالبقاء في النظام المعلوماتي بعد معرفة خطئه. كذلك الأمر بالنسبة للصورة الأخرى من السلوك الجرمي والمتمثلة بالدخول دون تصريح، فلا يمكن القول، بتقديرنا، بقيام هذه الصورة بالنسبة للحالة السابقة الذكر؛ وذلك لأن الدخول دون تصريح لا يقوم إلا إذا كان لدى المشتكى عليه وقت الدخول قصد جرمي وهو نية الدخول دون تصريح، وهذا لا يمكن تصوره في تلك الحالة السابقة الذكر، وذلك لأن المشتكى عليه وحينما دخل في المثال السابق الذكر كان قد دخل خطأ وليس قصداً[٢٠]. ولا ينتقص من قيمة هذه المداخلة القانونية القول بأن القصد الجرمي في الجرائم المستمرة يتوافر في أي مرحلة من مراحل السلوك الجرمي حتى ولو لم يكن

(١٨) تقضي هذه المادة بأنه: "يعاقب ..... كل من دخل موقعاً إلكترونياً.... بدون تصريح، أو بتجاوز حدود التصريح، أو بالبقاء فيه بصورة غير مشروعة."

(١٩) تقضي المادة (٣) بأنه: "يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (٥٠٠،٠٠٠) خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين، كل من دخل عمداً، دون وجه حق، بأي وسيلة، موقعاً إلكترونياً، أو نظاماً معلوماتياً، أو شبكة معلوماتية، أو وسيلة تقنية معلومات أو جزء منها، أو تجاوز الدخول المصرح به، أو استمر في التواجد بها بعد علمه بذلك

(٢٠) عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونياً، مرجع سابق، ص٥٢.

متوافراً وقت بدء السلوك الجرمي[٢١]، وذلك لأن جرائم الدخول الإلكترونية ليست من الجرائم المستمرة، ما يؤيد ذلك أن الدخول، وهو صلب السلوك الجرمي، قد حصل لمرة واحدة، أما الاستمرار في البقاء فهو أثر للسلوك وليس السلوك الجرمي نفسه.

ما يؤيد ذلك أيضاً موقف كل من التشريعين الإماراتي والقطري فقد نصا بشكل صريح على هذه الحالة وهي الدخول خطأ والبقاء فيه بصورة غير مشروعة، إلى جانب الدخول دون تصريح، وتجاوز التصريح، فلو كان السلوك الجرمي المتمثل بـ "الدخول دون تصريح" كافياً لشمول تلك الحالة وهي الدخول خطأ والاستمرار بالبقاء بعد معرفة الخطأ، لما أوردت تلك التشريعات المقارنة السابقة الذكر تلك الحالة ضمن سلوكات النص القانوني[٢٢].

ويشترط المشرع الأردني لقيام السلوك الجرمي حسب نص المادتين (٣/أ) و(١٢/أ) من قانون الجرائم الإلكترونية أن يقع السلوك الجرمي على الشبكة المعلوماتية، أو على نظام معلومات[٢٣]. أما بالنسبة للموقع الإلكتروني، ولوسائل تقنية

---

(٢١) وتوضيحاً لذلك يمكن القول بأنه لو حاز المشتكى عليه أموالاً متحصلة من سرقة دون علمه بمصدر تلك الأموال، ففي هذه الحالة لا يمكن القول بقيام القصد الجرمي لتلك الجريمة، أما إذا علم أثناء الحيازة بمصدر تلك الأموال وبقي حائزاً لها، ففي هذه الحالة يتوافر القصد الجرمي، وذلك لأن السلوك الجرمي في هذه الجريمة مستمر.

(٢٢) تقضي المادة (١/٢) من قانون مكافحة جرائم تقنية المعلومات الإماراتي بأنه: "يعاقب بالحبس والغرامة التي لا تقل عن (١٠٠) ألف درهم ولا تزيد على (٣٠٠) ألف درهم أو بإحدى هاتين العقوبتين كل من دخل موقعاً إلكترونياً أو نظام معلومات إلكترونياً أو شبكة معلومات، أو وسيلة تقنية معلومات، بدون تصريح أو بتجاوز حدود التصريح، أو بالبقاء فيه بصورة غير مشروعة". وتقضي المادة (٣) من قانون مكافحة الجرائم الإلكترونية القطري بأنه: "يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (٥٠٠،٠٠٠) خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين، كل من دخل عمداً، دون وجه حق، بأي وسيلة، موقعاً إلكترونياً، أو نظاماً معلوماتياً، أو شبكة معلوماتية، أو وسيلة تقنية معلومات أو جزءاً منها، أو تجاوز الدخول المصرح به، أو استمر في التواجد بها بعد علمه بذلك".

(٢٣) تقضي المادة (٣/أ) بأنه: "يعاقب كل من دخل قصداً إلى الشبكة المعلوماتية أو نظام معلومات باي وسيلة دون تصريح أو بما يخالف أو يجاوز التصريح، بالحبس....."؛ تقضي الفقرة (ب) من المادة نفسها بأنه: "إذا كان الدخول المنصوص عليه في الفقرة (أ) من هذه المادة لإلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو توقيف أو تعطيل عمل الشبكة المعلوماتية أو نظام معلومات الشبكة المعلوماتية فيعاقب الفاعل بالحبس....". تقضي المادة (١٢/أ) بأنه: "يعاقب =

المعلومات، فلا يصلحان لأن يكونا محلاً لنص المادتين (٣/أ) و(١٢/أ) من قانون الجرائم الإلكترونية الأردني؛ وذلك لعدم وردهما في النص القانوني. بالاعتماد على ذلك يمكن القول بأن الدخول المجرد إلى الموقع الإلكتروني، أو لوسائل تقنية المعلومات غير مجرم حسب نص المادتين (٣/أ) و (١٢/أ) السابقتي الذكر(٢٤).

ولا ينتقص من قيمة هذا الاستنتاج القول بأن الموقع الإلكتروني ووسائل تقنية المعلومات مشمولان من قبل مفهوم الشبكة المعلوماتية أو النظام المعلوماتي؛ وذلك لأن التشريع الأردني يعرّف الموقع الإلكتروني تعريفاً مخالفاً لتعريف الشبكة المعلوماتية، وللنظام المعلوماتي، ما يؤيد ذلك نص المادة (٢) من قانون الجرائم الإلكترونية الأردني(٢٥).

كذلك الأمر بالنسبة لوسائل تقنية المعلومات، فعلى الرغم من أن المشرع الأردني لم يعرفها في قانون الجرائم الإلكترونية، مخالفاً بذلك الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الموقّع عليها من قبل الأردن في عام (٢٠١٠) والمصادق عليها في عام (٢٠١٣)، إلا أنها تختلف عن النظام المعلوماتي، وعن

= كل من دخل قصداً دون تصريح أو بما يخالف أو يجاوز التصريح إلى الشبكة المعلوماتية أو نظام معلومات بأي وسيلة كانت بهدف الاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني بالحبس....". تقضي الفقرة (ب) من المادة نفسها بأنه: "إذا كان الدخول المشار إليه في الفقرة (أ) من هذه المادة، بقصد إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو تعديلها أو تغييرها أو نقلها أو نسخها أو إفشائها، فيعاقب...".

(٢٤) عدنان غسان برانيو، أبحاث في القانون وتقنية المعلومات، شعاع للنشر والتوزيع، سوريا، الطبعة الأولى، ٢٠٠٧، ص ٢٥، ٢.

(٢٥) تعرّف هذه المادة "الشبكة المعلوماتية" على أنها "ارتباط بين أكثر من نظام معلومات لإتاحة البيانات والمعلومات والحصول عليها"، أما "النظام المعلوماتي" فتعرفه على أنه "مجموعة البرامج والأدوات المعدة لإنشاء البيانات أو المعلومات إلكترونياً، أو إرسالها أو تسلمها أو معالجتها أو تخزينها أو إدارتها أو عرضها بالوسائل الإلكترونية". أما الموقع الإلكتروني فتعرفه تلك المادة على أنه: "حيز لإتاحة المعلومات على الشبكة المعلوماتية من خلال عنوان محدد"، والأمثلة على المواقع الإلكترونية كثيرة نذكر منها مواقع التواصل الاجتماعي، مواقع العلماء والدعاة، ومواقع الدردشة والإيميل والمدونات، المواقع الإخبارية، المواقع العلمية المتخصصة بمجال معين مثل الطب، والهندسة، والقانون، وغيرها. بالاعتماد على ذلك يمكن القول بأن مفهوم الموقع الإلكتروني يختلف عن مفهوم الشبكة المعلوماتية وعن مفهوم النظام المعلوماتي أيضاً، ولو لم يكن هناك اختلاف بينهما لما عرّف التشريع الأردني الموقع الإلكتروني بصورة مختلفة عنهما.

الشبكة المعلوماتية، فبينما تركز تقنية المعلومات على الحواسيب وتطبيقات البرمجيات لتوفيرها بعد تخزينها وتحقيق الحماية لها وبالتالي الاسترجاع الآمن لها، تركز نظم المعلومات على البيانات ومعالجتها لإخراجها على هيئة معلومات جاهزة للاستخدام. أما بالنسبة لشبكة المعلومات فهي تركز على أجهزة الحاسوب نفسها، حيث تكون مرتبطة بوسائل اتصال مختلفة، ويتم تبادل البيانات فيما بينها بسرعة مختلفة بناء على نوع وسيلة الاتصال التي تربط الأجهزة[٢٦] .

ولا ينتقص من قيمة هذا الانتقاد القانوني القول بأن الموقع الإلكتروني يصلح لأن يكون محلاً لنص المادتين (٣/ج) و (١٢/ج) من القانون الأردني نفسه، ومن ثم فليس هناك حاجة لأن يكونا محلاً لنص المادتين (٣/أ) و (١٢/أ)، ويرجع السبب في ذلك إلى أن المادتين (٣/أ) و (١٢/أ) يعالجان جرائم الدخول المجردة، والتي تقوم بمجرد الدخول دون أن يكون هناك قصد خاص من الدخول. أما بالنسبة للمادتين (٣/ ج) و (١٢/ج) فهما يعالجان جرائم الدخول المرتبطة بقصد خاص كقصد التغيير أو الإلغاء أو الإتلاف ...إلخ. بتعبير آخر يمكن القول بأن التشريع الأردني لا يجرم الدخول المجرد إلى الموقع الإلكتروني أو لوسائل تقنية المعلومات، إلا إذا كان بقصد التغيير أو الإلغاء، وهذا لا يكفي بتقديرنا، بل من الأفضل تجريم الدخول المجرد إلى الموقع الإلكتروني ولوسائل تقنية المعلومات بمجرد الدخول حتى ولو لم يكن لدى المشتكى عليه قصد خاص.

ما يؤيد ذلك موقف كل من التشريع الإماراتي، والقطري، والكويتي، والمصري فالمتابع لهم يجد بأنهم لم يقصروا جرائم الدخول المجردة على الشبكة المعلوماتية وعلى النظام المعلوماتي، كما فعل التشريع الأردني، وإنما جرموا الدخول المجرد أيضاً إلى المواقع الإلكترونية، أو إلى وسائل تقنية المعلومات، ما يؤيد ذلك نص المادتين (١/٢) و (١/٤) من قانون مكافحة جرائم تقنية المعلومات الإماراتي[٢٧]، ونص

(٢٦) محمد عبد الله أبو بكر سلامة، جرائم الكمبيوتر والإنترنت، منشأة المعارف بالإسكندرية ٢٠٠٦م، ص ٢٧، ٢٨.

(٢٧) تقضي المادة (١/٢) قانون مكافحة جرائم تقنية المعلومات بأنه: "يعاقب.... كل من دخل موقعاً إلكترونياً، أو نظام معلومات إلكترونياً أو شبكة معلومات، أو وسيلة تقنية معلومات....إلخ. يعرف المشرع الإماراتي المواقع الإلكترونية في المادة (٩/١) من قانون مكافحة جرائم تقنية المعلومات على أنها: "مكان إتاحة المعلومات الإلكترونية على الشبكة المعلوماتية ومنها مواقع التواصل الاجتماعي والصفحات الشخصية والمدونات".

المادة (٣) من قانون مكافحة الجرائم الإلكترونية القطري[٢٨]، ونص المادة (٣) مشروع قانون مكافحة الجريمة الإلكترونية المصري[٢٩].

ولم يقف التشريع القطري عند هذا الحد بل جرم أيضاً الدخول غير المصرح به إلى المواقع الإلكترونية أو الأنظمة المعلوماتية الخاصة بأحد أجهزة الدولة أو مؤسساتها أو هيئاتها أو الجهات أو الشركات التابعة لها، ما يؤيد ذلك نص المادة (١/٢) من قانون مكافحة الجرائم الإلكترونية القطري[٣٠] .

الفرع الثاني: الدخول إلى موقع إلكتروني

يعالج التشريع الأردني جرائم الدخول إلى المواقع الإلكترونية في المادتين (٣/ج، ١٢/ج) من قانون الجرائم الإلكترونية، حيث يتمثل السلوك الجرمي، حسب هذين النصين بالدخول؛ تقضي المادة (٣/ج) "يعاقب كل من دخل قصداً إلى موقع إلكتروني لتغييره أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفته أو انتحال شخصية مالكه بالحبس...إلخ، كما وتقضي المادة (١٢/ج) "يعاقب كل من دخل قصداً إلى موقع إلكتروني للاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس بالأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني بالحبس...إلخ[٣١]؛ بالاعتماد على هذين النصين يمكن القول بأن كل صور الدخول تصلح لقيام هذه الجريمة سواء أكان الدخول مصرحاً به أم غير مصرح به، وسواء حصل تجاوز أو مخالفة للتصريح الممنوح

(٢٨) تقضي هذه المادة بأنه: "يعاقب بالحبس....، كل من دخل عمداً، دون وجه حق، بأي وسيلة، موقعاً إلكترونياً، أو نظاماً معلوماتياً، أو شبكة معلوماتية، أو وسيلة تقنية معلومات أو جزءاً منها، أو تجاوز الدخول المصرح به، أو استمر في التواجد بها بعد علمه بذلك".

(٢٩) تقضي هذه المادة بأنه: "يعاقب بالحبس...، كل من دخل عمداً بغير وجه حق، موقعاً أو نظاماً معلوماتياً".

(٣٠) تقضي هذه المادة بأنه: "يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (٥٠٠،٠٠٠) خمسمائة ألف ريال، كل من تمكن عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات، بغير وجه حق، من الدخول إلى موقع إلكتروني أو نظام معلوماتي لأحد أجهزة الدولة أو مؤسساتها أو هيئاتها أو الجهات أو الشركات التابعة لها".

(٣١) تقضي المادة (٣/ج) بأنه: "يعاقب كل من دخل قصداً إلى موقع إلكتروني لتغييره أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفته أو انتحال شخصية مالكه بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن (٢٠٠) مائتي دينار ولا تزيد على (١٠٠٠) ألف دينار". تقضي المادة (١٢/ج) بأنه: "يعاقب كل من دخل قصداً إلى موقع إلكتروني للاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس بالأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني بالحبس مدة لا تقل عن أربعة أشهر وبغرامة لا تقل عن (٥٠٠) خمسمائة دينار".

للمشتكى عليه أم لم يحصل، وسواء حصل الدخول خطأ واستمر المشتكى عليه بالبقاء بعد علمه أم حصل بصورة مقصودة[٣٢].

على خلاف ذلك الأمر جاء كل من التشريع الإماراتي، والقطري، والكويتي، والمصري، حيث تشترط هذه التشريعات أن يكون الدخول إلى الموقع الإلكتروني دون تصريح، أو بغير وجه حق، أو غير مشروع، ما يؤيد ذلك نص المادتين (٤ و٥) قانون مكافحة جرائم تقنية المعلومات الإماراتي[٣٣]، ونص المادتين (٢ و٣) من قانون مكافحة الجرائم الإلكترونية القطري[٣٤]، ونص المادة (٣) من قانون مكافحة جرائم تقنية المعلومات الكويتي[٣٥]ونص المادة (٣) من مشروع قانون مكافحة الجريمة الإلكترونية المصري[٣٦].

وهنا يمكن لنا طرح التساؤل التالي، هل موقف المشرع الأردني من هذه المسألة القانونية موفق، أم كان يجب عليه أن يشترط في الدخول إلى الموقع الإلكتروني أن يتم دون تصريح، كما فعلت التشريعات المقارنة السالفة الذكر؟ بقراءة المادتين (٣/ج) و(١٢/ج) من قانون الجرائم الإلكتروني الأردني السابقتي الذكر، وجدنا بأن هاتين المادتين تشترطان أن يكون الدخول بقصد التغيير، أو الإلغاء، أو الإتلاف، أو الاطلاع على البيانات أو المعلومات الواردة في المادتين، كما سيأتي الحديث عنه لاحقاً في القصد الخاص، ولا تشترطان أن يحصل التغيير، أو الإلغاء، أو

---

(٣٢) خالد المختار والمهندس إسماعيل بابكر محمد، التحقيق الجنائي في جرائم الحاسوب سيكولوجيته - أساليبه القانونية- أدواته العلمية - دار عزة للنشر والتوزيع، السودان ٢٠١٠م، ص ١٢٥.

(٣٣) تقضي المادة (٤/أ) بأنه: "يعاقب... كل من دخل بدون تصريح إلى موقع إلكتروني...، أو نظام معلومات إلكتروني، أو شبكة معلوماتية، أو وسيلة تقنية معلومات، سواء كان الدخول، بقصد الحصول على بيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية، أو تجارية، أو اقتصادية". تقضي المادة (٥) بأنه: "يعاقب...، كل من دخل بغير تصريح موقعاً إلكترونياً بقصد تغيير تصاميمه أو إلغائه أو إتلافه أو تعديله أو شغل عنوانه".

(٣٤) تقضي المادة (٢) بأنه: "يعاقب.....، كل من تمكن عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات، بغير وجه حق، من الدخول إلى موقع إلكتروني أو نظام معلوماتي لأحد أجهزة الدولة أو مؤسساتها أو هيئاتها أو الجهات أو الشركات التابعة لها"؛ تقضي المادة (٣) بأنه: "يعاقب.....، كل من دخل عمداً، دون وجه حق، بأي وسيلة، موقعاً إلكترونياً، أو نظاماً معلوماتياً، أو شبكة معلوماتية، أو وسيلة تقنية معلومات أو جزءاً منها، أو تجاوز الدخول المصرح به، أو استمر في التواجد بها بعد علمه بذلك". For a detailed discussion on this point, See S. Al-Rawashdeh, supra, pp80-84.

(٣٥) تقضي المادة (٣) بأنه: "يعاقب.....، كل من ارتكب دخولاً غير مشروع إلى موقع أو نظام معلوماتي....".

(٣٦) "يعاقب.....، كل من دخل عمداً بغير وجه حق، موقعاً أو نظاماً معلوماتياً...".

الإتلاف، أو الاطلاع على البيانات أو المعلومات السابقة الذكر، كما فعلت تلك التشريعات المقارنة، والتي سيأتي الحديث عنها لاحقاً كما ذكر سابقاً.

وفي هذا السياق قد يتساءل الشخص، كيف يمكن للقاضي، حسب التشريع الأردني، أن يستنتج نية التغيير، أو الإلغاء، ...إلخ، إذا كان الدخول بتصريح، وضُبِط الفاعل بعد الدخول مباشرة وقبل حصول التغيير أو الإلغاء ..إلخ؟ بالاعتماد على ذلك التساؤل يمكن القول بأن عدم اشتراط أن يكون الدخول دون تصريح، كما فعل التشريع الأردني، مخالفاً التشريعات المقارنة السابقة الذكر، قد أفرغ النص القانوني من محتواه، وجعله نصاً غير مفعّل، ولا يمكن تطبيقه في الأحوال العادية. بتعبير آخر يمكن القول بأنه إذا كان الدخول قد حصل بناء على تصريح فلا يمكن أن نستنتج نية التغيير أو الإلغاء، خصوصاً إذا ضُبِط الفاعل قبل التغيير أو الإلغاء، بخلاف الأمر لو كان يشترط في الدخول أن يحصل دون تصريح، أو بغير وجه حق، كما فعلت تلك التشريعات السابقة الذكر، ففي هذه الحالة يمكن القول بأن أي دخول دون تصريح هو مؤشر على أن المتهم كانت لديه نية التغيير، أو الإلغاء، أو الإتلاف، أو الاطلاع على البيانات والمعلومات وعليه إثبات العكس.

ولا ينتقص من قيمة هذه المداخلة القانونية القول بأن اشتراط أن يكون الدخول بدون تصريح كشرط لقيام جرائم الدخول إلى المواقع الإلكترونية سيؤدي إلى إفلات الحالات التي يدخل فيها المشتكى عليه بتصريح ويتجاوز حدود التصريح من العقاب، ويرجع السبب في ذلك إلى أن المجني عليه يكون في هذه الحالة قد قصّر في حماية حقوقه الشخصية، فمن يصرح للغير بالدخول إلى موقعه الإلكتروني يكون قد قبل ضمناً بأي سلوك يمكن أن يقوم به المشتكى عليه.

وفي السياق نفسه يثور التساؤل التالي وهو، هل يشترط أن يكون النظام المستهدف محمياً بكلمة سر حتى يمكن القول بأن الدخول قد حصل دون تصريح؟ لا يشترط التشريع الأردني، أسوة بقانون إساءة استخدام الحاسوب الإنجليزي (Computer Misuse Act 1990)[٣٧] هذا

(٣٧) ما يؤيد ذلك نص المادة (١) من قانون إساءة استخدام الحاسب الآلي الإنجليزي، والتي تقضي بأنه:

(1) Computer Misuse Act 1990: (1) A person is guilty of an offence if-(a) he causes a computer to perform any function with intent to computer secure access to any program or data held in any computer; (b) the access he intends to secure is unauthorised; and (c) he knows at the time when he causes the computer to perform the function that that is the case.(2) The intent a person has to have to commit an offence under this section need not be directed at-(a) =

الأمر[٣٨]، بخلاف التشريع الأمريكي حيث يفرق بالنسبة للحاسبات بين الحاسبات التابعة للحكومة الفدرالية الأمريكية وبين الحاسبات غير التابعة لتلك الحكومة، حيث لا يشترط أن تكون الأولى محمية بكلمة سر، بخلاف الأخرى. ما يؤيد ذلك نص المادة (١٠٣٠ أ/٦) من القانون الفدرالي الأمريكي لإساءة استخدام الحاسبات الآلية. كذلك الأمر بالنسبة للتشريع الألماني، فالمتابع له يجد بأنه يشترط لقيام هذه الجريمة أن يكون النظام المعلوماتي محمياً بكلمة سر، ما يؤيد ذلك نص المادة (٢٠٢أ، ١) من قانون العقوبات الألماني[٣٩] .

وفي هذا السياق نلفت النظر إلى أنه إذا كان أمر اشتراط كلمة سر من عدمه لا يثير أي مشاكل قانونية عملية بالنسبة لأجهزة الكمبيوتر، أو أنظمة المعلومات، أو الشبكة المعلوماتية، إلا أن هذا الأمر يثير مشاكل كثيرة بالنسبة إلى الهواتف الذكية، أو إلى الأي باد، والتابلت، أو إلى الحاسب المنزلي، وذلك لأن هذه الوسائل متاحة للاستعمال من قبل الغير أكثر من أي وسيلة تقنية معلومات أخرى، لذلك الأمر فلا بد من أن تكون هذه الوسائل محمية بكلمة سر، وإلا فسيتم تجريم الزوجة التي تدخل إلى هاتف الزوج، والأم التي تدخل إلى الأي باد التابع للابن، وغير ذلك من الحالات التي تتشابه مع هذه الحالة في الغرض والغاية. ما يؤيد ذلك أن ترك الزوج أو الابن هاتفه المحمول الذي يشتمل على موقعه الإلكتروني دون كلمة سر هو مؤشر على قبول الدخول إلى المواقع الإلكترونية[٤٠] .

= any particular program or data; (b) a program or data of any particular kind; or (c) a program or data held in any particular computer. (3) A person guilty of an offence under this section shall be liable on summary conviction to imprisonment for a term not exceeding six months or to a fine not exceeding level 5 on the standard scale or to both.

(٣٨) سامي رواشدة وأحمد هياجنة، مكافحة الجريمة المعلوماتية بالتجريم والعقاب: القانون الإنجليزي نموذجاً، بحث منشور في المجلة الأردنية في القانون والعلوم السياسية، المجلد (١)، العدد (٣) شوال ١٤٣٠هـ/تشرين الأول ٢٠٠٩م، ص١٢٨-١٣٠.

(٣٩) Wer unbefugt Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, sich oder einem anderen verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(٤٠) لمزيد من المعلومات حول هذا الموضوع راجع: بحث "جريمة الدخول غير المشروع في تشريعات الجرائم الإلكترونية العربية "دراسة، مقارنة"، عبد الإله محمد النوايسة، المنشور في المجلة القانونية والقضائية الصادرة عن مركز الدراسات القانونية والقضائية في وزارة العدل القطرية، ٢٠١٦، المجلد (١٠)، العدد (١)، ص(١٩).

المطلب الثاني
نتائج جرائم الدخول الإلكترونية

يقسم هذا المطلب إلى فرعين: خصصنا الأولى منهما لدراسة النتائج التامة، والثاني لدراسة الشروع في جرائم الدخول الإلكترونية.

الفرع الأول: النتائج التامة لجرائم الدخول الإلكترونية

تتداخل النتائج الجرمية لجرائم الدخول الإلكترونية مع السلوك الجرمي نفسه بحيث يصعب فصلها عنه؛ وذلك لأن هذا النوع من الجرائم يعد من جرائم الخطر التي تكتفي بالسلوك الجرمي ولا تشترط نتيجة جرمية منفصلة عنه. بالاعتماد على ذلك الأمر يمكن القول بأن النتائج الجرمية لجرائم الدخول الإلكترونية هي نفسها السلوك الجرمي، حيث تتوافر، بالنسبة للفقرتين (أ، ب) من المادتين (٣و١٢) من قانون الجرائم الإلكتروني الأردني بتمام الدخول دون تصريح، أو بما يخالف أو يجاوز التصريح إلى الشبكة المعلوماتية أو إلى النظام المعلوماتي، وبالنسبة للفقرة (ج) من المادتين السابقتي الذكر، والفقرة (د) من المادة (١٢) فتتوافر النتيجة الجرمية بتمام الدخول إلى موقع إلكتروني سواء أكان مصرحاً به أم غير مصرح به.

والسؤال الآن هل يشترط أن يحصل المشتكى عليه على معلومات أو بيانات إلكترونية، حتى يمكن القول بتوافر النتيجة الجرمية التامة، أم أنها تقوم بمجرد الدخول فقط؟ المتابع للتشريع الأردني يجد بأنه لا يشترط لقيام النتيجة الجرمية لجرائم الدخول الإلكترونية الحصول على معلومات أو بيانات إلكترونية، بل يكتفي بمجرد الدخول فقط، ما يؤيد ذلك حرفية نص المادتين السابقتي الذكر.

على خلاف ذلك الأمر جاء التشريع والفقه الألمانيين، فالمتابع لهما يجد بأنهما يشترطان لقيام النتيجة الجرمية لجرائم الدخول الإلكترونية الحصول على معلومات أو بيانات إلكترونية غير مصرح له الحصول عليها، ما يؤيد ذلك نص المادة (٢٠٢أ) من قانون العقوبات الألماني الصادر في ١٨٧١/٥/١٥، وذلك لأن الهدف من قانون الجرائم الإلكترونية، حسب رأي ذلك الفقه[٤١]، ليس هو حماية الشبكة المعلوماتية، أو

(٤١) Ha, Der strafrechliche Schutz von Compuzerprogrammen, in: Lehmann (Hrsg), Rechtsschutz und Verwertung von Computerprogrammen, 2. Aufl. (1993), s. 479; BIr. Polizeilicher Zugriff auf kriminelle Mailboxen, CR, 1995, S.489; Bühler, Ein Versuch, Computerkriminellen das Handwerk zu legen: Das Zweite Gesetz zur BekÌmpfung der WirtschaftskriminalitÌt, MDR 1987, S.448.

النظام المعلوماتي أو المواقع الإلكترونية، نفسها، والتي بدون معلومات أو بيانات إلكترونية ليس لها أي قيمة قانونية، وإنما الهدف منه هو حماية المعلومات أو البيانات الإلكترونية الموجودة على تلك الشبكة المعلوماتية، أو على النظام المعلوماتي أو على المواقع الإلكترونية(٤٢)، فلو اشترى شخص هاتفاً أو جهاز كمبيوتر، أو أنشأ بريداً إلكترونياً جديداً وكان خالياً من أي معلومات أو من أي بيانات إلكترونية، فإن تجريم مجرد الدخول إلى ذلك الهاتف أو الكمبيوتر، أو إلى ذلك البريد الإلكتروني سيكون بلا معنى، وسيجافي الهدف والغاية من النص القانوني، والمتمثلة بحماية المعلومات والبيانات الإلكترونية.

ما يؤيد ذلك أيضاً، حسب رأي ذلك الفقه، أن تجريم مجرد الدخول غير المصرح به، دون شرط الحصول على معلومات أو بيانات إلكترونية غير مصرح للمتهم بالحصول عليها، سيؤدي إلى نتائج غير منطقية، حيث سيؤدي إلى تجريم الموظف الذي يدخل خارج أوقات الدوام الرسمي إلى النظام المعلوماتي المصرح له بالدخول إليه داخل أوقات الدوام الرسمي، وذلك لأن تصريح الدخول الممنوح له خاص بأوقات الدوام الرسمي، فبما أنه دخل خارج أوقات الدوام الرسمي بدون تصريح، والجريمة تقوم بمجرد الدخول، ففي هذه الحالة يمكن القول بتوافر جريمة الدخول الإلكترونية، علماً بأنه مصرح له بالاطلاع على المعلومات الموجودة داخل ذلك النظام المعلوماتي، وهذا لا يتفق مع الهدف والغاية من القانون والمتمثلة، كما ورد سابقاً، بحماية المعلومات والبيانات الإلكترونية.

ما يؤيد ذلك أيضاً، حسب رأي ذلك الفقه، قياس جرائم الدخول الإلكترونية بجرائم خرق حرمة المنازل، فمن المستقر عليه فقهاً وقضاء بأن دخول الشقة المخلاة تماماً للتأجير لا يؤدي إلى قيام جرائم خرق حرمة المنازل، وذلك لعدم توافر الغاية من التجريم والمتمثلة بخرق حرمة الحياة الخاصة، حيث إن الهدف من تجريم جرائم خرق حرمة المنازل ليس هو حماية الجدران، وإنما حماية الحياة الخاصة للأفراد القاطنين داخل تلك الجدران، فإذا كانت الشقة مخلاة تماماً للتأجير فهذا يعني، بتقديرنا، بأنه لا

(٤٢) (202a): (1) Wer unbefugt Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, sich oder einem anderen verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft. (2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

يوجد حياة خاصة فيها، ومن ثم فليس هناك داعٍ لتجريم الشخص الذي يدخل إليها على أساس خرق حرمة المساكن. ما يؤيد ذلك الأمر أسماء القوانين والتشريعات التي قننت وعالجت الجرائم الإلكترونية، فالمتابع لها يجد بأن جميعها تدور حول المعلومات والبيانات الإلكترونية، وليس حول الشبكة أو الأنظمة المعلوماتية أو المواقع الإلكترونية. بالاعتماد على ذلك الأمر، وبقياس جرائم الدخول الإلكترونية على جرائم خرق حرمة المنازل يمكن القول بأن الهدف من تأثيم جرائم الدخول الإلكترونية ليس هو حماية النظام المعلوماتي نفسه، وإنما حماية المعلومات والبيانات الإلكترونية الموجودة على ذلك النظام، والذي بدونها ليس للنظام المعلوماتي أي أهمية أو قيمة قانونية.

الفرع الثاني: الشروع في جرائم الدخول الإلكترونية

والسؤال الآن، ما هو الوضع القانوني إذا ضبط المشتكى عليه مثلاً وهو يحاول الدخول بأسماء مرور غير صحيحة، أو وهو يحاول فتح ملفات غير مصرح له الدخول إليها، أو وهو يحاول مخالفة التصريح، أو التجاوز عليه، فهل يمكن القول بقيام النتيجة الجرمية لجرائم الدخول الإلكترونية؟ بالاعتماد على نص المادتين السابقتي الذكر يمكن القول بعدم قيام النتيجة الجرمية لجرائم الدخول الإلكترونية في هذه الحالات، وإنما الشروع بتلك الجرائم[٤٣]. وفي هذا المجال نلفت النظر إلى أن جرائم الدخول

(٤٣) إذا ضبط المشتكى عليه وهو يحاول الدخول دون تصريح، أو بما يخالف أو يجاوز التصريح إلى الشبكة المعلوماتية أو إلى نظام معلوماتي لمجرد الدخول فقط لا غير، فيقوم الشروع بنص المادة (٣/أ)، وإذا كان يحاول الدخول بقصد إلغاء أو حذف معلومات أو بيانات إلى آخره، ففي هذه الحالة يقوم الشروع بنص المادة (٣/ب)، وإذا كان المشتكى عليه يحاول الدخول إلى موقع إلكتروني لتغييره، أو إلغائه...إلخ، ففي هذه الحالة يقوم الشروع بنص المادة (٣/ج). وإذا ضبط المشتكى عليه وهو يحاول الدخول دون تصريح أو بما يخالف أو يجاوز التصريح إلى الشبكة المعلوماتية أو النظام المعلوماتي بهدف الاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني، ففي هذه الحالة يقوم الشروع بنص المادة (١٢/أ)، وإذا كانت محاولة الدخول السابق ذكرها بقصد إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو تعديلها أو تغييرها أو نقلها أو نسخها أو إفشائها، ففي هذه الحالة يقوم الشروع بنص المادة (١٢/ب). وإذا ضبط المشتكى عليه وهو يحاول الدخول إلى موقع إلكتروني للاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس بالأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني، ففي هذه الحالة يقوم الشروع بنص المادة (١٢/ج)، وإذا كان الدخول السابق ذكره لإلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو تعديلها أو تغييرها أو نقلها أو نسخها، ففي هذه الحالة يقوم الشروع بنص المادة (١٢/د) قانون الجرائم الإلكترونية الأردني.

الإلكترونية الواردة في المادة (٣) من قانون الجرائم الإلكتروني الأردني بفقراتها الثلاث، وفي المادة (١٢/أ، ج) من القانون نفسه هي جنحوية الوصف، والشروع في الجنح غير معاقب عليه حسب نص المادة (٧١\١) قانون العقوبات الأردني، إلا بوجود نص، ولا يوجد نص في قانون الجرائم الإلكترونية الأردني يجرم الشروع في جنح الجرائم الإلكترونية[٤٤]، ويرجع السبب في ذلك إلى نص المادة (١٩/٢ و٣) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات التي أجازت للدول عدم تجريم الشروع في الجرائم الإلكترونية[٤٥].

على خلاف ذلك الأمر جاء كل من التشريع الإماراتي، والقطري، والمصري حيث جرم كل منهم الشروع في الجنح الإلكترونية، ما يؤيد ذلك نص المادة (٤٠) من قانون مكافحة جرائم تقنية المعلومات الاتحادي الإماراتي، والتي تقضي بأن: "يعاقب على الشروع في الجنح المنصوص عليها في هذا المرسوم بقانون بنصف العقوبة المقررة للجريمة التامة". ونص المادة (٥٠) من قانون مكافحة الجرائم الإلكترونية القطري، والتي تقضي "يعاقب كل من شرع في ارتكاب جناية أو جنحة معاقب عليها بموجب أحكام هذا القانون بالحبس مدة لا تجاوز نصف الحد الأقصى للعقوبة المقررة للجريمة التامة"، ونص المادة (٢٩) من مشروع قانون مكافحة الجريمة الإلكترونية المصري والتي تقضي "يعاقب على الشروع في ارتكاب الجرائم المنصوص عليها بهذا القانون بذات العقوبات المقررة للجريمة التامة".

والسؤال الذي يثور الآن، هل موقف المشرع الأردني من مسألة عدم تجريم الشروع بجنح الجرائم الإلكترونية جاء موفقاً، أم كان من الأفضل أن يتبع خطة تلك التشريعات المقارنة، وأن يجرم الشروع بالجنح الإلكترونية؟ المتابع لقانون الجرائم الإلكترونية الأردني يجد بأن الغالبية العظمى من الجرائم الواردة فيه هي جنحوية الوصف، حيث يبلغ عددها (١٢) جريمة إلكترونية، بخلاف الجرائم الجنائية، والتي تشكل أربع جرائم فقط لا غير من **العدد الكلي للجرائم** الواردة في القانون، بالاعتماد على ذلك يمكن القول بأن عدم وجود نص يجرم الشروع بجنح الجرائم الإلكترونية قد أفرغ القانون من محتواه الرامي، إلى جانب كثير من الأهداف، إلى تجريم ومعاقبة

(٤٤) تقضي المادة (٧١) من قانون العقوبات الأردني بأنه: "لا يعاقب على الشروع في الجنحة إلا في الحالات التي ينص القانون عليها صراحة".

(٤٥) تقضي المادة (١٩/٣) بأنه: "يجوز لأي دولة طرف الاحتفاظ بحقها في عدم تطبيق الفقرة الثانية من هذه المادة كلياً أو جزئياً". بمراجعة الفقرة الثانية من هذه المادة وجدنا بأنها تتحدث عن الشروع.

العابثين بالوسائل الإلكترونية. بالاعتماد على ذلك الأمر يمكن القول بأنه من الأفضل أن يتبع التشريع الأردني خطة التشريعات المقارنة، وأن يجرم الشروع بجنح الجرائم الإلكترونية.

وفي سياق الحديث عن الشروع نلفت النظر إلى أن كلاً من التشريع الأردني، والتشريع الإماراتي لم يجرما الأعمال التحضيرية المتعلقة بالاتفاق الجنائي على ارتكاب أي من الجرائم الواردة في قانون الجرائم الإلكترونية، كما فعلت كثير من التشريعات، نذكر منها قانون العقوبات الجزائري، حيث جرم الأشخاص الذين يتفقون على ارتكاب أي من الجرائم الإلكترونية حتى ولو كانت من قبيل الأعمال التحضيرية. ما يؤيد ذلك نص المادة (٤٩٤) مكرر (٥)، والتي تقضي بأنه: "كل ما شارك في مجموعة أو اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم، وكان هذا التحضير مجسداً بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها". ويرجع سبب ذلك إلى أن هناك صعوبة كبيرة جداً في الفصل بين العمل التحضيري، وبين البدء في التنفيذ، وبين السلوك الجرمي نفسه للجرائم الإلكترونية، فشراء برامج اختراق، ومعدات لفك الشيفرات، وكلمات المرور، وحيازة صور دعارة للأطفال أو حتى بعض الفيروسات التي لم يتم إطلاقها على الشبكة العنكبوتية، كل هذه الأفعال تشكل جريمة في حد ذاتها؛ لذا فقد كان من الأفضل تجريم هذه الأفعال حتى ولو كانت من قبيل الأعمال التحضيرية.

المبحث الثاني
الركن المعنوي لجرائم الدخول الإلكترونية

يقسم هذا المبحث إلى مطلبين: خصصنا الأول منهما لدراسة القصد العام، والثاني لدراسة القصد الخاص.

المطلب الأول
القصد العام

يقسم هذا المطلب إلى فرعين: خصصنا الأول منهما لدراسة العلم أثناء الدخول، والثاني لدراسة العلم بعد الدخول.

الفرع الأول: العلم أثناء الدخول

ويشترط لتوافر القصد العام أن يكون المشتكى عليه عالماً ومريداً لجميع عناصر الركن المادي من سلوك، ومحل، ونتيجة وعلاقة سببية علماً وإرادة مباشرة أو احتمالية، وذلك بقصد إحداث نتيجة مباشرة مقصودة، أو أية نتيجة أخرى غير مقصودة يكون الفاعل قد توقع حصولها فقبل بالمخاطرة، ما يؤيد ذلك نصوص المواد (٦٣-٦٤) من قانون العقوبات الأردني[٤٦].

وتطبيقاً لذلك يجب أن يكون المشتكى عليه عالماً بالسلوك الجرمي بصورتيه الإيجابية والسلبية، علماً مباشراً أو احتمالياً ومريداً له؛ بتعبير آخر يمكن القول بأنه يجب أن يكون المشتكى عليه عالماً علماً مباشراً أو احتمالياً بأنه يدخل دون تصريح، أو بما يخالف أو يجاوز التصريح، ومريداً لذلك الأمر، بغض النظر عن الدافع[٤٧]، وذلك لأن الدافع ليس عنصراً من عناصر الجريمة. أما بالنسبة للعلم بالسلوك الجرمي السلبي فيتوافر إذا امتنع المشتكى عليه عن علم وإرادة عن منع الآخرين الذين

(٤٦) يشترط المشرع الأردني لقيام القصد الجرمي توافر نية لدى الفاعل، وتعرف المادة (٦٣) النية على أنها: "إرادة ارتكاب الجريمة على ما عرفها القانون"، وتعد الجريمة حسب نص المادة (٦٤) مقصودة وإن تجاوزت النتيجة الجرمية الناشئة عن الفعل قصد الفاعل إذا كان قد توقع حصولها فقبل بالمخاطرة، ويكون الخطأ إذا نجم الفعل الضار عن الإهمال أو قلة الاحتراز أو عدم مراعاة القوانين والأنظمة.

(٤٧) علي عبد الله القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، بيروت، ١٩٩٩، ص٧.

يدخلون دون تصريح أو بما يخالف أو يجاوز التصريح، شريطة أن يكون ذلك الأمر من واجبه وفي مقدوره(٤٨).

وإذا ارتكب المشتكى عليه ذلك الفعل تحت تأثير غلط في الوقائع، تحددت مسؤوليته على أساس الوقائع التي اعتقد بوجودها إذا كان من شأنها أن تنفي مسؤوليته، أو أن تخففها، بشرط أن يكون اعتقاده قائماً على أسباب معقولة وعلى أساس من البحث والتحري(٤٩). وتطبيقاً لذلك فإذا دخل المشتكى عليه دون تصريح ظناً منه أنه يدخل بتصريح، أو إذا خالف أو تجاوز على التصريح الممنوح له خطأ، ففي هذه الحالة ينتفي القصد الجرمي لديه، ومن ثم لا يمكن معاقبته على أساس جريمة مقصودة، شريطة أن يكون اعتقاده قائماً على أسباب معقولة وعلى أساس من البحث والتحري. كذلك الأمر لا يمكن معاقبته على أساس جريمة غير مقصودة، وذلك لأن المشرع الأردني لم يجرم الدخول غير المقصود.

كذلك الأمر يجب أن يكون المشتكى عليه عالماً علماً مباشراً أو احتمالياً بمحل أو موضوع الجريمة، وهو أنه يدخل دون تصريح أو بما يخالف أو يجاوز التصريح إلى الشبكة المعلوماتية أو إلى النظام المعلوماتي الخاص بالغير. وتطبيقاً لذلك فإذا ثبت للقضاء بأن المشتكى عليه كان يتوقع خطأ بأن النظام المعلوماتي الذي دخل عليه، أو خالف أو تجاوز حدود التصريح بشأنه هو خاص به وليس للغير، فلا يتوافر القصد العام في هذه الحالة؛ وذلك لانتفاء العلم المباشر أو الاحتمالي بمحل أو موضوع الجريمة.

إضافة إلى ذلك يشترط لتوافر القصد العام أن يكون المشتكى عليه عالماً بالنتيجة الجرمية، أو أن يتوقع حدوثها كأثر حتمي أو محتمل لسلوكه الجرمي ويقبل بها؛ لذا فإذا ثبت للقضاء بأن المشتكى عليه كان عالماً بأنه يدخل دون تصريح أو بما يجاوز أو يخالف التصريح إلى النظام المعلوماتي الخاص بالغير، ففي هذه الحالة يتوافر العلم بالنتيجة الجرمية. كذلك الأمر إذا لم يكن لدى المشتكى عليه قصد الدخول دون تصريح، أو بما يخالف أو يجاوز التصريح، ولكنه توقع أن يحصل ذلك الأمر كأثر لفعله، ففي هذه الحالة

(٤٨) إبراهيم، خالد، أمن مراسلات البريد الإلكتروني، الدار الجامعية- الإسكندرية، ٢٠٠٨. ص ٨.

(٤٩) وإذا لم تتوافر هذه العناصر فتقوم الجريمة المقصودة على أساس القصد الاحتمالي، ما يؤيد ذلك نص المادة (٦٤) من قانون العقوبات الأردني والتي تقضي بأنه: "تعد الجريمة مقصودة وإن تجاوزت النتيجة الجرمية الناشئة عن الفعل قصد الفاعل إذا كان قد توقع حصولها فقبل بالمخاطرة، ويكون الخطأ إذا نجم الفعل الضار عن الإهمال أو قلة الاحتراز أو عدم مراعاة القوانين والأنظمة".

يتوافر عنصر العلم بالنتيجة الجرمية على أساس القصد الاحتمالي، ما يؤيد ذلك نص المادة (٦٤) من قانون العقوبات الأردني والتي تقضي بأنه: "تعد الجريمة مقصودة وأن تجاوزت النتيجة الجرمية الناشئة عن الفعل قصد الفاعل إذا كان قد توقع حصولها فقبل بالمخاطرة.." . كذلك الأمر يتوافر عنصر العلم بالنتيجة الجريمة إذا دخل المشتكى عليه إلى نظام معلومات خاص بالغير لم يرد الدخول إلى هذا النظام وإنما إلى نظام معلوماتي خاص بشخص آخر، وذلك لأن الغلط بمحل أو موضوع الجريمة ليست محل اعتبار إذا كانت الجريمة لا تتطلب وسيلة معينة لإتمام النتيجة الجرمية، ما يؤيد ذلك نص المادة (٦٥) من قانون العقوبات الأردني التي تقضي بأنه: "لا عبرة للنتيجة إذا كان القصد أن يؤدي إليها ارتكاب فعل إلا إذا ورد نص صريح على أن نية الوصول إلى تلك النتيجة تؤلف عنصراً من عناصر الجرم الذي يتكون كله أو بعضه من ذلك الفعل".

أخيراً يشترط لتوافر القصد العام أن يكون المشتكى عليه عالماً بعلاقة السببية أو أن يتوقعها كأثر لسلوكه ويقبل بها، ولا يشترط أن يكون التسلسل السببي الذي توقعه المشتكى عليه هو نفسه التسلسل السببي الذي حصل فعلاً، فإذا أراد المشتكى عليه الدخول بوسيلة معينة كالدخول عن طريق (الرقم السري) الخاص بالغير ودخل عن طريق وسيلة أخرى لم يرد من خلالها الدخول، ففي هذه الحالة يتوافر القصد الجرمي لجرائم الدخول الإلكترونية؛ وذلك لأن هذه الجريمة لا تشترط وسيلة معينة للدخول(٥٠).

الفرع الثاني: العلم بعد الدخول الخاطئ

يعتبر العلم من العناصر الجوهرية والرئيسية لقيام القصد العام، والسؤال الآن ما هو الوضع القانوني إذا دخل المشتكى عليه خطأ، وبعد الدخول اكتشف خطأه، واستمر بالبقاء في النظام المعلوماتي مثلاً، فهل يمكن القول في هذه الحالة بتوافر القصد العام بكل جزئياته السابقة الذكر؟ ترى الدراسة بأنه وبالاعتماد على حرفية النص القانوني لا يمكن القول بتوافر القصد العام في هذه الحالة، وذلك لأن المشتكى عليه وعند الدخول لم يكن قاصداً فعلاً الدخول دون تصريح.

ولا ينتقص من قيمة هذه المداخلة القانونية القول بأن توافر القصد الجرمي في السلوكات المستمرة تؤدي إلى قيام الجريمة المقصودة حتى ولو لم يتوافر القصد العام منذ البداية، وذلك لأن الجرائم التي يطبق عليها هذا القول هي الجرائم التي لم تذكر لفظ "قصداً" في النص القانوني بصورة مباشرة، فلو أن المشرع الأردني لم

(٥٠) آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري – الطبعة الثانية، دار هومة للنشر والتوزيع ٢٠٠٧، ص ١٨.

يذكر ذلك اللفظ بصورة صريحة لأمكن تطبيق هذه الرأي الفقهي عليها، ويرجع السبب في ذلك إلى أن ذكر لفظ قصداً في النص القانوني يقيد النص ويحد منه بشكل لا يخدم تلك المسألة القانونية السابقة الذكر. وتوضيحاً لذلك يمكن القول بأن التشريع الأردني ذكر لفظ قصداً بالنص القانوني بشكل صريح، ما يؤيد ذلك الفقرة (أ) من المادة (٣) من قانون الجرائم الإلكترونية الأردني، والتي تقضي بأنه: "يعاقب كل من دخل قصداً إلى الشبكة المعلوماتية أو نظام معلومات بأي وسيلة دون تصريح أو بما يخالف أو يجاوز التصريح....إلخ"، والفقرة (ب) من المادة نفسها والتي تقضي بأنه: "يعاقب كل من دخل قصداً إلى موقع إلكتروني لتغييره...."، والفقرة (أ) من المادة (١٢) من القانون نفسه، والتي تقضي بأنه: "يعاقب كل من دخل قصداً دون تصريح أو بما يخالف أو يجاوز التصريح...إلخ"، والفقرة (ج) من المادة نفسها، والتي تقضي بأنه: "يعاقب كل من دخل قصداً إلى موقع إلكتروني للاطلاع على بيانات...".

على خلاف ذلك الأمر جاء كثير من التشريعات المقارنة، حيث لم تذكر بشكل صريح لفظ قصداً في النص القانوني، على الرغم من أنها تشترط قصداً جرمياً لقيام هذا النوع من الجرائم، ما يؤيد ذلك نصوص المواد (١/٢، ١/٤، ١/٥) من قانون مكافحة جرائم تقنية المعلومات الإماراتي[٥١]، ونص المادة (٢) من قانون مكافحة جرائم تقنية المعلومات الكويتي رقم (٦٣) لسنة ٢٠١٥[٥٢]، ونص المادة (٢) من قانون مكافحة الجرائم الإلكترونية القطري رقم (١٤) لسنة ٢٠١٤[٥٣].

(٥١) تقضي المادة (١/٢) بأنه: "يعاقب بالحبس والغرامة..... كل من دخل موقعاً إلكترونياً أو نظام معلومات إلكترونياً أو شبكة معلومات، أو وسيلة تقنية معلومات، بدون تصريح أو بتجاوز حدود التصريح، أو بالبقاء فيه بصورة غير مشروعة". تقضي المادة (١/٤) بأنه: "يعاقب.... كل من دخل بدون تصريح إلى موقع إلكتروني، أو نظام معلومات إلكتروني، أو شبكة معلوماتية، أو وسيلة تقنية معلومات، سواء كان الدخول بقصد الحصول على بيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية، أو تجارية، أو اقتصادية". تقضي المادة (١/٥) بأنه: "يعاقب..... كل من دخل بغير تصريح موقعاً إلكترونياً بقصد تغيير تصاميمه...".

(٥٢) تقضي هذه المادة بأنه: "يعاقب بالحبس مدة لا تجاوز ستة أشهر وبغرامة لا تقل عن خمسمائة دينار ولا تجاوز ألفي دينار أو بإحدى هاتين العقوبتين، كل من ارتكب دخولاً غير مشروع إلى جهاز حاسب آلي أو إلى نظامه أو إلى نظام معالجة إلكترونية للبيانات أو إلى نظام إلكتروني مؤتمت أو إلى شبكة معلوماتية".

(٥٣) تقضي هذه المادة بأنه: "يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (٥٠٠،٠٠٠) خمسمائة ألف ريال، كل من تمكن عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات، بغير وجه حق، من الدخول إلى موقع إلكتروني أو نظام معلوماتي لأحد أجهزة الدولة أو مؤسساتها أو هيئاتها أو الجهات أو الشركات التابعة لها".

والسؤال الآن، هل جاء موقف المشرع الأردني من ذكر لفظ قصداً في النص القانوني موفقاً، أم كان من الأفضل أن يتبع خطة التشريعات المقارنة السالفة الذكر، وأن لا يذكر لفظ قصداً في النص القانوني؟

المتابع للاتجاهات التشريعية يجد بأن المشرعين لا يلجؤون إلى ذكر لفظ (قصداً) في النص القانوني كشرط لقيام الجريمة المقصودة، إلا إذا كان الفعل يقوم بوصف غير المقصود؛ وذلك لأن ذكر لفظ (قصداً) في النص القانوني بشكل صريح يدل بمعنى المخالفة على أن هناك جريمة من النوع نفسه تقوم بوصف غير المقصود، ما يؤيد ذلك موقف المشرع الأردني نفسه من جرائم القتل والإيذاء على جهة، والاغتصاب، وهتك العرض، والفعل المنافي للحياء، والسرقة والاحتيال، وإساءة الأمانة والجرائم الملحقة بها على جهة أخرى، فالمتابع لهذه الجرائم يجد بأن المشرع الأردني لم يذكر لفظ (قصداً) في النصوص القانونية الناظمة لها بشكل صريح إلا في جريمتي القتل والإيذاء فقط، وذلك لأن هاتين الجريمتين وهما القتل والإيذاء هما اللذان يقومان بوصف غير المقصود، بخلاف الأمر بالنسبة للجرائم الأخرى السالفة الذكر وهي الاغتصاب وهتك العرض إلى آخر تلك الجرائم، فالمتابع لهذه الجرائم يجد بأن التشريع الأردني لم يذكر لفظ (قصداً) في النص القانوني؛ وذلك لأن هذه الجرائم لا تقوم بوصف غير المقصود.

بالاعتماد على ما سبق يمكن القول بأنه ليس من الموفق أن يذكر التشريع لفظ (قصداً) في النص القانوني كمؤشر على القصد الجرمي، إذا كانت الجريمة المقننة في ذلك النص القانوني لا تقوم بوصف غير المقصود، بتعبير آخر يمكن القول بأن المشرع الأردني لم يكن موفقاً عندما ذكر لفظ (قصداً) في النصوص القانونية الناظمة لجرائم الدخول الإلكترونية؛ وذلك لأن هذه الجرائم لا تقوم بوصف غير المقصود؛ لذا فإنه سيكون من الأفضل إلغاء ذلك اللفظ من النص القانوني.

المطلب الثاني
القصد الخاص

يقسم هذا المطلب إلى فرعين: خصصنا الأول منهما لدراسة القصد الخاص المتعلق بالبيانات أو المعلومات الإلكترونية الماسة بالأفراد، والثاني لدراسة القصد الخاص المتعلق بالبيانات أو المعلومات الإلكترونية الماسة بالدولة.

الفرع الأول: القصد الخاص المتعلق بالبيانات أو المعلومات الإلكترونية الماسة بالأفراد

يشترط التشريع الأردني في جرائم الدخول المتعلقة بالبيانات أو المعلومات الإلكترونية الماسة بالأفراد قصداً خاصاً إلى جانب القصد العام، وهو أن يكون الدخول بقصد الإلغاء أو الحذف إلى آخر ما ورد في النص القانوني من ألفاظ، ما يؤيد ذلك نص المادة (٣/ب) من قانون الجرائم الإلكتروني الأردني، والتي تقضي بأنه: "إذا كان الدخول المنصوص عليه في الفقرة (أ) من هذه المادة لإلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو توقيف أو تعطيل عمل الشبكة المعلوماتية أو نظام معلومات الشبكة المعلوماتية فيعاقب...." . ما يؤيد ذلك أيضاً الفقرة (ج) من المادة نفسها والتي تقضي بأنه: "يعاقب كل من دخل قصداً إلى موقع إلكتروني لتغييره أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفته أو انتحال شخصية مالكه بالحبس...."(٥٤).

والسؤال الآن، هل القصد الخاص الوارد في النصوص القانونية السابقة الذكر وهو قصد الإلغاء والحذف والتغيير والاطلاع إلى آخر ما جاء في تلك النصوص القانونية من ألفاظ واردة على سبيل المثال أم على سبيل الحصر؟ وهل يشترط التشريع الأردني تحقق القصد الخاص لإمكانية القول بتوافره أم لا؟ وهل هناك حاجة قانونية لتعريفه؟ وما هو الوضع القانوني إذا دخل شخصان بناء على اتفاق جرمي إلى نظام معلوماتي وكان لدى الأول منهما قصد خاص وهو الإلغاء، بخلاف الثاني الذي كان لديه فقط قصد الدخول البسيط، فهل يسري القصد الخاص المتعلق بالشخص الأول على الشخص الثاني، علماً بأن الشخص الثاني لا يعلم بالقصد الخاص وهو الإلغاء المتوافر في الشخص الأول؟ كذلك الأمر ما هو الوضع القانوني

(٥٤) تقضي الفقرة (ب) من المادة (٣) بأنه: "إذا كان الدخول المنصوص عليه في الفقرة (أ) من هذه المادة لإلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو توقيف أو تعطيل عمل الشبكة المعلوماتية أو نظام معلومات الشبكة المعلوماتية فيعاقب الفاعل بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن (٢٠٠) مائتي دينار ولا تزيد على (١٠٠٠) ألف دينار". تقضي الفقرة (ج) من المادة (٣) بأنه: "يعاقب كل من دخل قصداً إلى موقع إلكتروني لتغييره أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفته أو انتحال شخصية مالكه بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن (٢٠٠) مائتي دينار ولا تزيد على (١٠٠٠) ألف دينار".

إذا دخل شخص بقصد الدخول فقط، وليس بقصد الإلغاء، وقام شخص آخر، مستغلاً مغادرة الشخص الأول للنظام المعلوماتي المفتوح، ودون أي اشتراك جرمي مع الشخص الأول بالجلوس أمام النظام المعلوماتي المفتوح بقصد الإلغاء، فهل يسري القصد الخاص عليهما؟

بالاعتماد على الغاية والهدف من إيجاد تلك النصوص القانونية والمتمثلة بمكافحة الجرائم الإلكترونية والحد منها يمكن القول بأن تلك الألفاظ واردة على سبيل المثال لا الحصر، ما يؤيد ذلك لفظ "أو" الوارد في النصوص القانونية السالفة الذكر، فلو أراد المشرع الأردني أن يقصر تلك النصوص القانونية على تلك الألفاظ فقط لاستخدم لفظ "و" وليس لفظ "أو". ما يؤيد ذلك أيضاً أن هذا النوع من الجرائم يتطور بشكل سريع وقد لا يستطيع المشرع أن يجاري ذلك التطور بتعديل مستمر للنصوص القانونية، خصوصاً إذا كانت هناك ألفاظ غير واردة بشكل حرفي في النصوص القانونية إلا أنها قريبة منها، والأمثلة على ذلك كثيرة نذكر منها الدخول بقصد نشر أو إعادة نشر، أو التقاط بيانات أو معلومات إلكترونية، فلو قلنا بأن الألفاظ القانونية الواردة في النصوص القانونية السابقة الذكر واردة على سبيل الحصر لما أمكن القول: بتوافر القصد الخاص السالف الذكر حيال المشتكى عليه الذي يدخل بقصد نشر أو إعادة نشر أو التقاط بيانات أو معلومات إلكترونية، وذلك لعدم ورودها بشكل صريح ومباشر في النصوص القانونية. ولا ينتقص من قيمة هذا الاستنتاج القانوني القول بأن المشرع لو أراد أن تكون تلك الألفاظ واردة على سبيل المثال لا الحصر لقال: "أو ما شابه ذلك"، ويرجع السبب في ذلك الأمر إلى أن هذا اللفظ يشكل اعتداءً صارخاً على مبدأ الشرعية، وذلك لأنه يخالف الشروط الواجب توافرها في النصوص القانونية وهي الإيجاز والوضوح والدقة.

وفي سياق الحديث عن القصد الخاص نلفت النظر إلى أن التشريع الأردني لا يشترط تحقق القصد الخاص وهو الإلغاء أو الحذف لإمكانية القول بتوافر القصد الجرمي، وتطبيقاً لذلك فإذا دخل المشتكى عليه بقصد الإلغاء فيتوافر القصد الخاص حتى ولو لم يقم المشتكى عليه بالإلغاء، وذلك لأن النص القانوني يشترط أن يكون الدخول بقصد الإلغاء، ولا يشترط تحقق الإلغاء، أما إذا كان الدخول بقصد الدخول البسيط فقط، أي ليس بقصد الإلغاء مثلاً، وحصل خطأ أدى إلى إلغاء بعض البيانات أو المعلومات الإلكترونية فلا يتوافر القصد الخاص في هذه الحالة، سنداً للنص القانوني السالف الذكر؛ وذلك لأن الدخول لم يكن بقصد الإلغاء، وإنما بقصد الدخول البسيط.

ويؤخذ على هذا الاتجاه التشريعي، الذي يشترط تحقق القصد الخاص لإمكانية القول بقيام القصد الجرمي، أنه يفرغ النص القانوني من محتواه ويحيّده عن التطبيق في الواقع العملي، وذلك لصعوبة إثباته في بعض الحالات؛ وتوضيحاً لذلك فإذا دخل المشتكى عليه إلى الشبكة المعلوماتية مثلاً بقصد الإلغاء وضُبط قبل الإلغاء مثلاً، أو بعد المحاولة وقبل حصول الإلغاء، ففي هذه الحالة سيعتد أمام القضاء بأنه دخل بقصد الدخول فقط وليس بقصد الإلغاء، ومن ثم سيطبق عليه جريمة الدخول البسيطة المقننة في المادة (٣/أ) من قانون الجرائم الإلكتروني الأردني فقط وليست جريمة الدخول بقصد الإلغاء المقننة في المادة (٣/ب) من القانون نفسه، وذلك لصعوبة إثبات القصد الخاص المتمثل بقصد الإلغاء لدى المشتكى عليه. ولا ينتقص من قيمة هذا الانتقاد القانوني القول بأن القصد الخاص مفترض في كل شخص يدخل إلى الشبكة المعلوماتية أو النظام المعلوماتي بدون تصريح أو بما يخالف أو يجاوز التصريح، وعليه أن يثبت العكس؛ وذلك لأن هذا القول يحيد الفقرة (أ) من المادة (٣) السالفة الذكر عن التطبيق العملي ولا يكون لها حاجة إذاً، كما أنه يلقي بعبء كبير على النيابة العامة والمحكمة المختصة، وذلك لأنهما سيكونان بحاجة إلى مؤشرات خارجية يستدلان بهما على القصد الخاص، ولا يوجد مؤشرات خارجية في مثل هذا النوع من الجرائم الذي يفتقر لمسرح جريمة، أو لوسائل أو أدوات.

على خلاف ذلك الأمر فقد تبنت بعض التشريعات المقارنة اتجاهاً مغايراً لما جاء في التشريع الأردني، ما يؤيد ذلك نص المادة (٢) من قانون مكافحة جرائم تقنية المعلومات الإماراتي(٥٥)، والمادة (٣) من قانون مكافحة الجرائم الإلكترونية

(٥٥) تقضي هذه المادة بأنه: "يعاقب بالحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تزيد على ثلاث مائة درهم أو بإحدى هاتين العقوبتين كل من دخل موقعاً إلكترونياً أو نظام معلومات إلكترونياً أو شبكة معلومات، أو وسيلة تقنية معلومات، بدون تصريح أو بتجاوز حدود التصريح، أو بالبقاء فيه بصورة غير مشروعة. وتكون العقوبة الحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن مائة وخمسين ألف درهم ولا تجاوز سبع مائة وخمسين ألف درهم أو بإحدى هاتين العقوبتين إذا ترتب على أي فعل من الأفعال المنصوص عليها بالفقرة (١) من هذه المادة إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر بيانات أو معلومات. وتكون 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 الثانية من هذه المادة شخصية".

القطري[٥٦]، والمادة (٢) من قانون مكافحة جرائم تقنية المعلومات الكويتي[٥٧]، واللواتي **يقابلن** المادة (٣) من قانون الجرائم الإلكتروني الأردني، فالمتابع لهذه النصوص القانونية يجد بأنها لم تتبن فكرة القصد الخاص، كما فعل التشريع الأردني في جرائم الدخول إلى البيانات أو المعلومات الإلكترونية العادية؛ وتطبيقاً لذلك فإذا دخل المشتكى عليه إلى نظام معلوماتي خاص بالغير مثلاً، ففي هذه الحالة يتوافر الدخول البسيط المقنن في تلك المواد، سواء كان الدخول بقصد الإلغاء أو لا، وبهذا تكون تلك التشريعات المقارنة قد نجت من الانتقاد السالف الذكر للتشريع الأردني، والمتمثل بصعوبة إثبات القصد الخاص، خصوصاً إذا ضبط المشتكى عليه بعد الدخول وقبل البدء بالإلغاء.

وفي صميم الحديث عن القصد الخاص، وبالاعتماد على الحديث السابق الذكر، نلفت النظر إلى أنه ليس هناك حاجة لأن تقوم الدراسة بتعريف تلك الألفاظ القانونية؛ وذلك لأن التشريع الأردني لا يشترط، كما ذكر سابقاً، تحقق تلك الألفاظ لقيام القصد

---

(٥٦) تقضي هذه المادة بأنه: "يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (٥٠٠،٠٠٠) خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين، كل من دخل عمداً، دون وجه حق، بأي وسيلة، موقعاً إلكترونياً، أو نظاماً معلوماتياً، أو شبكة معلوماتية، أو وسيلة تقنية معلومات أو جزءاً منها، أو تجاوز الدخول المصرح به، أو استمر في التواجد بها بعد علمه بذلك. وتُضاعف العقوبة المنصوص عليها في الفقرة السابقة، إذا ترتب على الدخول إلغاء أو حذف أو إضافة أو إفشاء أو إتلاف أو تغيير أو نقل أو التقاط أو نسخ أو نشر أو إعادة نشر بيانات أو معلومات إلكترونية مخزنة في النظام المعلوماتي، أو إلحاق ضرر بالمستخدمين أو المستفيدين، أو تدمير أو إيقاف أو تعطيل الموقع الإلكتروني أو النظام المعلوماتي أو الشبكة المعلوماتية، أو تغيير الموقع الإلكتروني أو إلغائه أو تعديل محتوياته أو تصميماته أو طريقة استخدامه أو انتحال شخصية ماله أو القائم على إدارته.

(٥٧) تقضي هذه المادة بأنه: "يعاقب بالحبس مدة لا تجاوز ستة أشهر وبغرامة لا تقل عن خمسمائة دينار ولا تجاوز ألفي دينار أو بإحدى هاتين العقوبتين، كل من ارتكب دخولاً غير مشروع إلى جهاز حاسب آلي أو إلى نظامه أو إلى نظام معالجة إلكترونية للبيانات أو إلى نظام إلكتروني مؤتمت أو إلى شبكة معلوماتية. فإذا ترتب على هذا الدخول إلغاء أو حذف أو إتلاف أو تدمير أو إفشاء أو تغيير أو إعادة نشر بيانات أو معلومات، فتكون العقوبة الحبس مدة لا تجاوز سنتين والغرامة التي لا تقل عن ألفي دينار ولا تجاوز خمسة آلاف دينار أو بإحدى هاتين العقوبتين. فإذا كانت تلك البيانات أو المعلومات شخصية فتكون العقوبة الحبس مدة لا تجاوز ثلاث سنوات والغرامة التي لا تقل عن ثلاثة آلاف دينار ولا تجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين. ويعاقب بالحبس مدة لا تجاوز خمس سنوات وبغرامة لا تقل عن ثلاثة آلاف دينار ولا تجاوز عشرين ألف دينار أو بإحدى هاتين العقوبتين كل من ارتكب أياً من الجرائم المنصوص عليها أعلاه أو سهل ذلك للغير وكان ذلك أثناء أو بسبب تأدية وظيفته.

الخاص، بل يكتفي بالدخول بقصد تحقيقها، بتعبير آخر يمكن القول لو كان هناك فرق في العقوبة بين الدخول بقصد الإلغاء وعدم تحقق الإلغاء من جهة، وبين الدخول بقصد الإلغاء وتحقق الإلغاء من جهة أخرى، لأمكن القول بأن هناك ضرورة لتعريف تلك الألفاظ، حتى نميز متى يقوم الإلغاء ومتى لا يقوم.

وفيما يتعلق بالتساؤل السابق الذكر والذي يدور حول مسألة الاشتراك الجرمي ومدى سريان القصد الخاص المتوافر في الفاعل على باقي المساهمين في الجريمة، نلفت النظر إلى أن قانون الجرائم الإلكتروني الأردني لم يتعرض لأحكام الاشتراك الجرمي؛ لذا نعود إلى القواعد العامة لحل هذه المسائل القانونية، إلا أنه وفي البداية يجب الإشارة إلى أنه يجب التمييز بين حالتين وهما: هل القصد الخاص من قبيل الظروف المشددة؟ فإذا كانت الإجابة بنعم، ففي هذه الحالة يمكن القول بسريان القصد الخاص المتوافر في الشخص الأول على الشخص الثاني، شريطة أن يكون الظرف المشدد (القصد الخاص) المتوافر في الشخص الأول قد سبب[٥٨] اقتراف الجريمة بالنسبة للشخص الثاني، ما يؤيد ذلك نص المادة (٢/٧٩) من قانون العقوبات الأردني، وشريطة أن يكون الشخص الثاني على علم بالقصد الخاص المتوافر في الشخص الأول، ما يؤيد ذلك نص المادة (٢/١٥٤) من قانون العقوبات. وإذا لم يكن القصد الخاص من قبيل الظروف المشددة، ففي هذه الحالة يمكن القول باستقلال كل شخص بقصده، ومن ثم فلا يسري القصد الخاص المتوافر في الشخص الأول على الشخص الثاني سواء علم به هذا الأخير أم لم يعلم به.

أما بالنسبة للمسألة الأخرى والمتمثلة بدخول الشخص الأول بقصد الدخول فقط، وقيام شخص آخر ودون أي اتفاق جرمي مع الشخص الأول بالجلوس أمام النظام المعلوماتي بقصد الإلغاء، ففي هذه الحالة لا يمكن القول بقيام القصد الخاص حيال الشخص الأول؛ وذلك لأنه دخل بقصد الدخول البسيط فقط وليس بقصد الإلغاء، ولم يكن بينه وبين الشخص الثاني أي اتفاق جرمي، فلو كان بينهما اتفاق جرمي لأمكن القول بقيام القصد الخاص حيال الشخص الأول. أما بالنسبة للشخص الثاني فيتوافر بحقه القصد الخاص؛ وذلك لأن قيامه بالجلوس أمام النظام المعلوماتي بعد فتحه من قبل الشخص الأول يعتبر من قبيل الدخول بقصد الإلغاء، ما يؤيد ذلك

(٥٨) لقد وقع التشريع الأردني في خطأ مطبعي، حيث كان يريد استخدام لفظ (سهّل) وليس لفظ (سبب) بدليل أن لفظ (سهّل) ورد في التشريع اللبناني وهو المصدر التاريخي لقانون العقوبات الأردني.

أن لفظ الدخول لا يشترط إجراءات معينة كفتح الجهاز مثلاً أو كتابة الرقم السري، بل يتوافر بمجرد الجلوس أمام النظام المعلوماتي المفتوح بقصد الإلغاء، أو بمجرد هز الماوس (محرك البحث)، أو بالنقر على بعض البيانات بقصد الدخول والإلغاء. كذلك الأمر يتوافر القصد الخاص حيال الشخص الثاني إذا جلس أمام النظام المعلوماتي المفتوح من قبل الشخص الأول بقصد المشاهدة فقط، إلا أنه تبادر إلى ذهنه بعد المشاهدة إلغاء أو تعديل بعض البيانات أو المعلومات الإلكترونية.

الفرع الثاني: القصد الخاص المتعلق بالبيانات والمعلومات الإلكترونية الماسة بالدولة

يشترط التشريع الأردني في جرائم الدخول المتعلقة بالبيانات أو المعلومات الإلكترونية الماسة بالدولة قصداً خاصاً إلى جانب القصد العام، وهو أن يكون الدخول بهدف الاطلاع أو الإلغاء إلى آخر ما جاء في النصوص القانونية من ألفاظ، ما يؤيد ذلك نص المادة (١٢/أ، ب، ج) من قانون الجرائم الإلكتروني الأردني، والتي تقضي في الفقرة (أ) منها بأنه: "يعاقب كل من دخل قصداً دون تصريح أو بما يخالف أو يجاوز التصريح إلى الشبكة المعلوماتية أو نظام معلومات بأي وسيلة كانت بهدف الاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني بالحبس ...." . كما وتقضي الفقرة (ب) من المادة نفسها بأنه: "إذا كان الدخول المشار إليه في الفقرة (أ) من هذه المادة، بقصد إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو تعديلها أو تغييرها أو نقلها أو نسخها أو إفشائها، فيعاقب ..." . أما الفقرة (ج) من المادة نفسها فتقضي بأنه: "يعاقب كل من دخل قصداً إلى موقع إلكتروني للاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني بالحبس..."[٥٩].

(٥٩) تقضي الفقرة (أ) من المادة (١٢) بأنه: "يعاقب كل من دخل قصداً دون تصريح أو بما يخالف أو يجاوز التصريح إلى الشبكة المعلوماتية أو نظام معلومات بأي وسيلة كانت بهدف الاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني بالحبس مدة لا تقل عن أربعة أشهر وبغرامة لا تقل عن (٥٠٠) خمسمائة دينار ولا تزيد على (٥٠٠٠) خمسة آلاف دينار. تقضي الفقرة (ب) من المادة نفسها بأنه: "إذا كان الدخول المشار إليه في الفقرة (أ) من هذه المادة، بقصد إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو تعديلها أو تغييرها أو نقلها أو نسخها أو إفشائها، فيعاقب الفاعل بالأشغال الشاقة المؤقتة وبغرامة لا تقل عن (١٠٠٠) ألف دينار ولا تزيد على (٥٠٠٠) خمسة آلاف دينار". تقضي الفقرة (ج) =

على خلاف ذلك الأمر فقد جاءت بعض التشريعات المقارنة كالتشريع الإماراتي والكويتي بخطة تشريعية مشابهة للتشريع الأردني في جزء ومخالفة له في جزء آخر، فالمتابع للتشريعين الإماراتي والكويتي يجد أنهما يشترطان قصداً خاصاً في نصوصهما القانونية الموازية لنص المادة (١٢/أ) من قانون الجرائم الإلكتروني الأردني فقط، ما يؤيد ذلك نص المادة (١/٤) من قانون مكافحة جرائم تقنية المعلومات الإماراتي، والتي تقضي بأنه: "يعاقب ....كل من دخل بدون تصريح إلى موقع إلكتروني، أو نظام معلومات إلكتروني، أو شبكة معلوماتية، أو وسيلة تقنية معلومات، سواء كان الدخول، بقصد الحصول على بيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية، أو تجارية، أو اقتصادية"(٦٠). ما يؤيد ذلك أيضاً نص المادة من (١/٣) قانون مكافحة جرائم تقنية المعلومات الكويتي، والتي تقضي بأنه: "يعاقب ... كل من ارتكب دخولاً غير مشروع إلى موقع أو نظام معلوماتي مباشرة أو عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات بقصد الحصول على بيانات أو معلومات حكومية سرية بحكم القانون"(٦١).

على خلاف ذلك الأمر فلم يشترط كل من التشريع الإماراتي والكويتي قصداً خاصاً في النصوص القانونية الموازية لنص المادة (١٢/ب) من قانون الجرائم الإلكتروني الأردني السابقة الذكر، والتي تشترط أن يكون الدخول بقصد إلغاء أو إتلاف بيانات أو معلومات إلكترونية ماسة بالدولة، ما يؤيد ذلك نص المادة (٢/٤) من قانون مكافحة جرائم تقنية المعلومات الإماراتي والتي تقضي بأنه: "وتكون العقوبة

= من المادة نفسها بأنه: "يعاقب كل من دخل قصداً إلى موقع إلكتروني للاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني بالحبس مدة لا تقل عن أربعة أشهر وبغرامة لا تقل عن خمسمائة دينار".

(٦٠) تقضي المادة (٤) من قانون مكافحة جرائم تقنية المعلومات الإماراتي بأنه: "يعاقب بالسجن المؤقت والغرامة التي لا تقل عن (٢٥٠) ألف درهم ولا تجاوز مليون وخمسمائة ألف درهم كل من دخل بدون تصريح إلى موقع إلكتروني، أو نظام معلومات إلكتروني، أو شبكة معلوماتية، أو وسيلة تقنية معلومات، سواء كان الدخول، بقصد الحصول على بيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية، أو تجارية، أو اقتصادية".

(٦١) تقضي المادة (١/٣) من قانون مكافحة جرائم تقنية المعلومات الكويتي بأنه: "يعاقب بالحبس مدة لا تجاوز ثلاث سنوات وبغرامة لا تقل عن ثلاثة آلاف دينار ولا تجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين كل من ارتكب دخولاً غير مشروع إلى موقع أو نظام معلوماتي مباشرة أو عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات بقصد الحصول على بيانات أو معلومات حكومية سرية بحكم القانون".

السجن مدة لا تقل عن خمس سنوات والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز اثنين مليون درهم، إذا تعرضت هذه البيانات أو المعلومات للإلغاء أو الحذف أو الاتلاف أو التدمير أو الافشاء أو التغيير أو النسخ أو النشر أو إعادة النشر". ما يؤيد ذلك أيضاً الجزئية الثانية من الفقرة الأولى من المادة (٣) من قانون مكافحة جرائم تقنية المعلومات الكويتي، والتي تقضي بأنه: "فإذا ترتب على ذلك الدخول إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو نشرها أو تعديلها، تكون العقوبة الحبس مدة لا تجاوز عشر سنوات والغرامة التي لا تقل عن خمسة آلاف دينار ولا تجاوز عشرين ألف دينار أو بإحدى هاتين العقوبتين". المتابع لهاتين المادتين يجد أنهما لم يشترطا أن يكون الدخول بقصد إلغاء أو إتلاف بيانات أو معلومات إلكترونية ماسة بالدولة، كما فعل التشريع الأردني، وإنما شددا العقوبة في حال ما إذا ترتب على الدخول إلغاء بعض البيانات أو المعلومات الإلكترونية الماسة بالدولة سواء أحصل الإلغاء أو الإتلاف بصورة مقصودة أم بصورة غير مقصودة، وحسناً فعل هذان التشريعان؛ وذلك لأن اشترط أن يكون الدخول بقصد الإلغاء لإمكانية القول بقيام نص المادة (١٢/ب) من قانون الجرائم الإلكتروني الأردني يحيد النص القانوني عن التطبيق في الواقع العملي، كما ذكر سابقاً، وذلك لصعوبة إثبات قصد الإلغاء في حال ضبط المتهم بعد الدخول وقبل الإلغاء. علاوة على ذلك فإن هذا الشرط والمتمثل بوجوب أن يكون الدخول بقصد الإلغاء لإمكانية القول بقيام نص المادة (١٢/ب) من قانون الجرائم الإلكتروني الأردني، يؤدي إلى نتائج متناقضة، كما ذكر سابقاً، فالذي يدخل بقصد الإلغاء يعاقب حسب نص المادة (١٢/ب) من قانون الجرائم الإلكترونية الأردني بخلاف الشخص الذي يدخل بقصد الدخول البسيط ويترتب على دخوله خطأ إلغاء لبعض البيانات أو المعلومات الإلكترونية الماسة بالدولة، ففي هذه الحالة لا يمكن معاقبته على أساس نص المادة (١٢/ب) من قانون الجرائم الإلكتروني الأردني، وذلك لأن المشتكى عليه وأثناء الدخول لم يكن يقصد الإلغاء. أما بالنسبة للفقرة (ج) من المادة (١٢) من التشريع الأردني والتي تعالج القصد الخاص في جرائم الدخول إلى المواقع الإلكترونية، فلم يوجد كل من التشريعين الإماراتي والكويتي فقرة مستقلة موازية لهذه الفقرة؛ وذلك لأنهما دمجا المواقع الإلكترونية بالفقرة الأولى من المادة نفسها.

أما بالنسبة للتشريع القطري فقد انتهج نهجاً مخالفاً تماماً للتشريع الأردني والتشريعات المقارنة السالفة الذكر، فالمتابع له يجد أنه لم يوجد نصوصاً قانونية تجرم الدخول إلى الأنظمة المعلوماتية والمواقع الإلكترونية العادية بقصد الاطلاع أو

إلغاء بيانات أو معلومات ماسة بالدولة، كما فعلت تلك التشريعات السابقة الذكر، وإنما أوجد نصوصاً قانونية تعالج الدخول إلى الأنظمة المعلوماتية والمواقع الإلكترونية الخاصة بأحد أجهزة الدولة أو مؤسساتها أو هيئاتها أو الجهات أو الشركات التابعة لها ولو لم يكن لدى المشتكى عليه قصد الاطلاع أو الإلغاء مثلاً، ما يؤيد ذلك نص المادة (١/٢) من قانون مكافحة الجرائم الإلكترونية القطري، والتي تقضي بأنه: "يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (٥٠٠،٠٠٠) خمسمائة ألف ريال، كل من تمكن عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات، بغير وجه حق، من الدخول إلى موقع إلكتروني أو نظام معلوماتي لأحد أجهزة الدولة أو مؤسساتها أو هيئاتها أو الجهات أو الشركات التابعة لها"(٦٢).

وفي سياق الحديث عن كل من التشريع الإماراتي والكويتي كأحد التشريعات المقارنة التي يمكن أن يقتفي التشريع الأردني أثرها نلفت النظر إلى أن الإلغاء أو الحذف، إلى آخره قد يحصل، بصورة مباشرة من الجاني أو غير مباشرة عن طريق مثلاً فيروسات استخدمها للحذف، كما أنها قد تحصل بصورة مادية أو معنوية، ومثال الصورة المعنوية شطب الرقم التسلسلي لأحد الكتب الموجودة على كمبيوترات مكتبة الجامعة مثلاً، ففي هذه الحالة يكون الكتاب موجوداً من ناحية مادية لا معنوية. كذلك الأمر فقد تحصل تلك السلوكات عن طريق الترك، ومثال ذلك أن يكون هناك شخص ملزم بالمحافظة على المعلومات، ولم يمنع المشتكى عليه من ذلك على الرغم من مقدرته على ذلك(٦٣). علاوة على ذلك فقد تحصل تلك السلوكات حتى ولو لم يتغير محتوى المعلومات، وذلك عن طريق تشفيرها، أو تحويلها إلى لغة برامج لا تفهم إلا من مختصين، أو بتغييرها إلى لغة أخرى غير معلومة من المجني عليه، وذلك لأن هذا

(٦٢) وفي سياق الحديث عن التشريعين الإماراتي والكويتي كأحد التشريعات المقارنة التي يمكن للتشريع الأردني أن يقتفي أثره يمكن القول بأن هذين التشريعين لم يفرقا في العقوبة بين ما إذا كان قد حصل الإلغاء بصورة مقصودة أم غير مقصودة، كما أنهما لم يميزا بين ما إذا كان المشتكى عليه قد دخل بقصد الإلغاء أم بقصد الدخول البسيط وترتب على دخوله إلغاء، بتعبير آخر يمكن القول بأن هذه التشريعات المقارنة تشترط أن يحصل الإلغاء أو الإتلاف إلى آخر ذلك من صور سواء بصورة مقصودة أم غير مقصودة حتى يمكن تشديد العقوبة على أساس القصد الخاص.

(٦٣) محمد أمين الشوابكة، جرائم الحاسوب والإنترنت، الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، الطبعة الأولى ٢٠٠٧، م، ص ٢١٦، ٢١٧.

الأمر يحرم المجني عليه من الرجوع إلى معلوماته. إضافة إلى ذلك فقد تحصل تلك السلوكات عن طريق أي سلوك آخر غير وارد في الفقرة الثانية، إذا حقق الغاية منها وهي حرمان المجني عليه من معلوماته، ومثال ذلك الإخفاء بنوعيه المادي والمعنوي، ومثال الإخفاء المادي أخذ جهاز الحاسوب، أو حافظة البيانات المخزن عليهما المعلومات، وأما الإخفاء المعنوي فمثاله تغيير كلمة السر، بحيث لا يستطيع المجني عليه الدخول إلى تلك المعلومات.

وفي سياق الحديث عن التشريعات المقارنة السالفة الذكر كلها نلفت النظر إلى أن الإلغاء أو الحذف إلى آخر ما ورد في النصوص المقارنة من ألفاظ تتوافر حتى ولو حصل الإلغاء لمعلومات أو بيانات إلكترونية أخرى ليس لدى المشتكى عليه قصد إلغائها؛ وذلك لأن هذه التشريعات تشترط إلغاء بيانات بغض النظر عن مالكها.

والسؤال الآن، هل يتوافر الإلغاء أو الحذف الوارد في النصوص المقارنة السابقة الذكر، إذا كانت المعلومات الملغاة مخزنة على حافظة ويمكن استرجاعها بوقت قصير ودون تكلفة مادية؟ أو إذا كان النظام المعلوماتي يصلح نفسه بنفسه ويستعيد البيانات أو المعلومات الملغاة أو المحذوفة من تلقاء نفسه بعد مدة معينة من الإلغاء؟ أو إذا حصل الإلغاء أو الحذف خلال فترة لم يحتاجهما فيها المجني عليه وتم استرجاع تلك البيانات أو المعلومات الإلكترونية بصورة تلقائية من النظام المعلوماتي نفسه؟ حسب النصوص القانونية المقارنة السالفة الذكر، يمكن القول بتوافر الإلغاء أو الحذف بمجرد إلغاء أو حذف البيانات، حتى ولو كان بالإمكان استرجاعها؛ وذلك لأن معيار التشديد حسب تلك النصوص القانونية، هو إلغاء أو حذف البيانات. على النقيض من ذلك، يرى بعض الفقه الألماني، عدم توافر الإلغاء أو الحذف في هذه الحالة، وذلك لانتفاء الغاية منه والمتمثلة بحرمان المجني عليه من معلوماته، إلا إذا كان استرجاع المعلومات والبيانات الإلكترونية الملغاة أو المحذوفة يأخذ وقتاً طويلاً نوعاً ما، أو يكلف تكلفة مادية مرتفعة نوعاً ما، وذلك لأنه وخلال فترة استرجاع تلك المعلومات أو البيانات الإلكترونية يكون المجني عليه قد تم حرمانه من معلوماته أو بياناته الإلكترونية، بتعبير آخر يمكن القول بما أن الهدف من تشديد العقوبة هو حرمان المجني عليه من معلوماته أو بياناته الإلكترونية، لذا فلا يتوافر الإلغاء أو الحذف إذا كان بإمكان المجني عليه استرجاع معلوماته وبياناته الإلكترونية في وقت قصير ودون تكلفة مادية مرتفعة(٦٤).

(٦٤) Hilgendorf, Juristische Schulung (JuS) 1996, S. 891; Sch, nke/Schr,der-Stree, 303a, Rdnr. 4; Mhrenschlager, wistra 1986, S. 141.

الخاتمة:

نختتم هذا البحث بنتائج، وتوصيات، نأمل أن ترى الضوء في أول تعديل للقانون.

أولاً: النتائج

١ – يتمثل السلوك الجرمي لجريمة الدخول إلى الشبكة المعلوماتية أو النظام المعلوماتي بالدخول دون تصريح أو بما يخالف أو يجاوز التصريح.

٢ – ويتوافر الدخول دون تصريح، عندما لا يكون هناك تصريح من الشخص المختص أصلاً، أو عندما يكون الدخول مشروطاً بأمر معين كدفع ثمن أو رسم أو غير ذلك من الشروط، ويقوم المشتكى عليه على الرغم من ذلك بالدخول.

٣ – وقد يحصل الدخول بصورة إيجابية ومباشرة، كما لو حصل عن طريق الجهاز المعلوماتي نفسه، أو بصورة غير مباشرة عن طريق الإنترنت. كذلك الأمر فقد يحصل الدخول بصورة سلبية، كما لو امتنع المشتكى عليه المكلف بحماية النظام المعلوماتي عن منع شخص من الدخول إلى ذلك النظام، على الرغم من أن هذا الأمر من واجبه وفي مقدوره.

٤ – لا تهم وسيلة الدخول والتي قد تكون كلمة السر الحقيقية، أو برامج مشفرة، أو الرقم الكودي، أو عن طريق شخص آخر مصرح له بالدخول، أو عن طريق تحريك الماوس.

٥ – يتوافر السلوك الجرمي المتمثل بمخالفة التصريح، أو التجاوز عليه عندما يكون هناك تصريح مقيد بوقت، أو بموضوع، أو بعمل معين، ويخالف المشتكى عليه ذلك التصريح أو يتجاوز عليه.

٦ – إذا قام شخص مصرح له بالدخول إلى النظام المعلوماتي، بالدخول إلى ذلك النظام والقيام بعمل غير مشروع، فلا يتوافر في هذه الحالة ذلك السلوك الجرمي؛ وذلك لأن النصوص القانونية الناظمة لتلك الجرائم تشترط أن يخالف أو يتجاوز المشتكى عليه على التصريح، وليس على العمل الممنوح له.

٧ – استخدم التشريع الأردني لفظ مخالفة التصريح والتجاوز عليه، بخلاف كثير من التشريعات المقارنة التي اكتفت بلفظ "التجاوز".

٨ – لم يتعرض التشريع الأردني للسلوك الجرمي المتمثل بالدخول خطأ والاستمرار بالبقاء بعد العلم بخطئه، كما فعل كثير من التشريعات المقارنة.

٩ – يشترط التشريع الأردني لتجريم الدخول دون تصريح أو بما يخالف أو يجاوز

التصريح أن يقع السلوك الجرمي على الشبكة المعلوماتية أو على النظام المعلوماتي، أما بالنسبة للدخول دون تصريح أو بما يخالف أو يجاوز التصريح إلى الموقع الإلكتروني، أو لوسائل تقنية المعلومات فلا يجرمه التشريع الأردني، بخلاف كثير من التشريعات المقارنة إلا إذا كان بقصد تحقيق القصد الخاص الوراد في الفقرة (ج) من المادتين (٣و١٢) من قانون الجرائم الإلكترونية الأردني.

١٠- لا يشترط التشريع الأردني لتجريم الدخول إلى الموقع الإلكتروني أن يكون الدخول دون تصريح، أو بغير وجه حق، أو غير مشروع، كما فعل كثير من التشريعات المقارنة، وإنما يجرم الدخول حتى ولو حصل بتصريح أيضاً.

١١- لا يشترط التشريع الأردني، شأنه كشأن كثير من التشريعات العربية المقارنة، أن يكون النظام المعلوماتي محمياً بكلمة سر حتى يمكن القول بأن الدخول قد حصل دون تصريح، **كما فعل التشريع الألماني.**

١٢- لا يشترط التشريع الأردني، شأنه كشأن كثير من التشريعات العربية المقارنة، أن يحصل المتهم على معلومات أو بيانات إلكترونية، حتى يمكن القول بتوافر النتيجة الجرمية التامة، كما فعلت بعض التشريعات الغربية المقارنة.

١٣- لا يجرم التشريع الأردني **الشروع** بالجنح الإلكترونية، كما فعل كثير من التشريعات المقارنة.

١٤- يعاقب التشريع الأردني على الشروع بالجنايات فينزل من العقوبة **المحكوم** بها من الثلث إلى النصف، بخلاف بعض التشريعات المقارنة التي تعاقب على الشروع بالجنايات بذات عقوبة الفعل التام.

١٥- لم يجرم التشريع الأردني الأعمال التحضيرية المتعلقة بالاتفاق الجنائي على ارتكاب أي من الجرائم الواردة في قانون الجرائم الإلكترونية، كما فعلت بعض التشريعات المقارنة.

١٦- لا يجرم التشريع الأردني الدخول غير المقصود إلى النظام المعلوماتي.

١٧- تقوم الجريمة إذا أراد المشتكى عليه الدخول إلى نظام معلوماتي خاص بشخص، ودخل إلى نظام معلوماتي خاص بشخص آخر لم يرد الدخول إليه.

١٨- يذكر التشريع الأردني لفظ (قصداً) في النص القانوني بشكل صريح مخالفاً بذلك جميع التشريعات المقارنة.

١٩- يشترط التشريع الأردني تحقق القصد الخاص، بخلاف كثير من التشريعات المقارنة.

ثانياً: التوصيات

في ضوء النتائج التي تم التوصل إليها في هذا البحث، يمكن عرض مجموعة من التوصيات تتمثل في:

١ – عدم استخدام لفظي "... يخالف أو يجاوز التصريح..."، في المادتين (٣/أ، ب) و(١٢/أ، ب)، والاكتفاء بلفظ التجاوز على التصريح، وذلك لعدم وجود فرق بين مخالفة التصريح والتجاوز عليه.

٢ – تضمين نص المادتين السابقتي الذكر السلوك التالي "الدخول خطأ والبقاء فيه بصورة غير مشروعة".

٣ – تضمين نص المادتين (٣/أ) و(١٢/أ) الموقع الإلكتروني، ووسائل تقنية المعلومات، وعدم قصر السلوك الجرمي المتمثل بالدخول المجرد دون تصريح أو بما يجاوز التصريح على الشبكة المعلوماتية والنظام المعلوماتي.

٤ – تقييد الدخول الوارد في المادتين (٣/ج) و(١٢/ج) على الدخول دون تصريح، أو بغير وجه حق، أو غير مشروع.

٥ – تعديل نص المادتين (٣/ج) و(١٢/ج) من قانون الجرائم الإلكترونية الأردني وأن يشترط أن يكون الدخول دون تصريح، أو بغير وجه حق، أو غير مشروع، وذلك لأنه لا يمكن استنتاج نية التغيير أو الإلغاء أو الإتلاف أو الاطلاع على البيانات أو المعلومات التي تمس الأمن الوطني، وغير ذلك من الغايات الواردة في هاتين المادتين إلا إذا كان الدخول دون تصريح، أو بغير وجه حق، أو غير مشروع؛ وإذا لم يقتنع المشرع الأردني بذلك الأمر فنقترح عليه أن يشترط لتمام هاتين المادتين أن يشترط حصول تغيير، أو إلغاء، أو إتلاف، أو الاطلاع على البيانات أو المعلومات، وذلك لأن أي تغيير، أو إلغاء، أو إتلاف في هذه الحالة سيكون مؤشراً قوياً على أن الدخول كان بقصد إحداث ذلك الأمر.

٦ – اشتراط أن يكون النظام المعلوماتي المستهدف محمياً بكلمة سر حتى يمكن القول بأن الدخول قد حصل دون تصريح، أو بما يجاوز التصريح.

٧ – اشتراط أن يحصل المشتكى عليه على معلومات أو بيانات إلكترونية، حتى يمكن القول بتوافر النتيجة الجرمية التامة لجرائم الدخول الإلكترونية.

٨ – تجريم الشروع في جنح الجرائم الإلكترونية، وأن يعاقب عليها بذات عقوبة الفعل التام.

٩ – تضمين قانون الجرائم الإلكترونية الأردني نصاً قانونياً يعالج عقوبة الشروع في

جنايات الجرائم الإلكترونية، وعدم الاعتماد على القواعد العامة، وذلك لأن الاعتماد على القواعد العامة في هذه المسألة القانونية قد يؤدي إلى أن تكون عقوبة الشروع في جنايات الجرائم الإلكترونية أشد من عقوبة الجريمة التامة.

١٠- تجريم الأعمال التحضيرية المتعلقة بالاتفاق الجنائي على ارتكاب أي من الجرائم الواردة في قانون الجرائم الإلكترونية.

١١- عدم ذكر لفظ (قصداً) في النص القانوني بشكل صريح؛ وذلك لأن جرائم الدخول الإلكترونية لا تقوم بوصف غير المقصود.

١٢- اشتراط تحقق الإلغاء إلى آخر ما جاء في النص القانوني من صور، كشرط لقيام الجريمة، أو الشروع به شروعاً ناقصاً أو تاماً، وعدم الاكتفاء بنية تحقيق الإلغاء، وذلك لأن الاكتفاء بنية تحقيق الإلغاء يجافي مبدأ تدرج العقوبة، حيث إنه يؤدي إلى معاقبة المشتكى عليه الذي دخل بقصد الإلغاء وضبط قبل الشروع به بذات عقوبة المتهم الذي دخل بقصد الإلغاء ونجح بالإلغاء. كما نقترح أيضاً أن يفرق المشرع الأردني في العقوبة بين الذي شرع بالإلغاء شروعاً ناقصاً أو تاماً، وبين الذي أتم الإلغاء، وبين الذي يدخل بقصد الإلغاء ويلغي أو يشرع به شروعاً تاماً أو ناقصاً، وبين الذي يدخل بقصد الدخول فقط ويحصل الإلغاء خطأ.

١٣- اشتراط حصول المتهم على معلومات أو بيانات إلكترونية غير مصرح له الحصول عليها، وذلك لقيام النتيجة الجرمية لجرائم الدخول الإلكترونية.

١٤- تجريم الدخول إلى الموقع الإلكتروني ولوسائل تقنية المعلومات بمجرد الدخول حتى ولو لم يكن لدى المشتكى عليه قصد خاص.

١٥- الإشارة إلى عدم توافر القصد الخاص إذا كانت المعلومات الملغاة مخزنة لدى المجني عليه وبإمكانه استرجاعها بسهولة دون أي تكلفة مادية أو معنوية، وذلك لانتفاء الغاية منه والمتمثلة بحرمان المجني عليه من معلوماته.

١٦- تجريم الدخول غير المصرح به إلى المواقع الإلكترونية أو الأنظمة المعلوماتية الخاصة بأحد أجهزة الدولة أو مؤسساتها أو هيئاتها أو الجهات أو الشركات التابعة لها، وتشديد العقوبة أكثر من عقوبة الدخول غير المصرح به إلى المواقع الإلكترونية أو الأنظمة المعلوماتية الخاصة بالأفراد.

قائمة المراجع:

أولاً: المراجع باللغة العربية

١ – إبراهيم، خالد، أمن مراسلات البريد الإلكتروني، الدار الجامعية– الإسكندرية، ٢٠٠٨. ص٨.

٢ – آمال قارة: الحماية الجزائية للمعلوماتية في التشريع الجزائري – الطبعة الثانية، دار هومة للنشر والتوزيع ٢٠٠٧، ص ١٨.

٣ – بولين أنطونيوس أيوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، لبنان، منشورات الحلبي الحقوقية، ٢٠٠٩، ص٤٠.

٤ – حسين، محمد، المسؤولية القانونية في مجال شبكات الإنترنت، دار النهضة العربية القاهرة، ٢٠٠٢. ص ٨.

٥ – خالد المختار والمهندس إسماعيل بابكر محمد، التحقيق الجنائي في جرائم الحاسوب سيكولوجيته – أساليبه القانونية– أدواته العلمية – دار عزة للنشر والتوزيع، السودان ٢٠١٠م، ص ١٢٥.

٦ – سامي جاد عبد الرحمن واصل، إرهاب الدولة في إطار قواعد القانون الدولي العام، دار النهضة العربية، الطبعة الأولى، ٢٠٠٣، ٢٠٠٤، ص ١.

٧ – سامي رواشدة وأحمد هياجنة، مكافحة الجريمة المعلوماتية بالتجريم والعقاب: القانون الإنجليزي نموذجاً، بحث منشور في المجلة الأردنية في القانون والعلوم السياسية، المجلد (١)، العدد (٣) شوال ١٤٣٠هـ/تشرين الأول ٢٠٠٩م.

٨ – سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الإنترنت، دار الفكر الجامعي، ٢٠٠٧م، ص٣٥.

٩ – عبد الإله محمد النوايسة، "جريمة الدخول غير المشروع في تشريعات الجرائم الإلكترونية العربية "دراسة، مقارنة"، بحث منشور في المجلة القانونية والقضائية الصادرة عن مركز الدراسات القانونية والقضائية في وزارة العدل القطرية، ٢٠١٦، المجلد (١٠)، العدد (١)، ص(١٩).

١٠– عدنان غسان برانيو، أبحاث في القانون وتقنية المعلومات، شعاع للنشر والتوزيع، سوريا، الطبعة الأولى، ٢٠٠٧، ص ٢٥، ٢.

١١– علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، بيروت، ١٩٩٩، ص٧.

١٢- علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة الإلكترونية، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، سنة ٢٠٠٠، ص٥٠.

١٣- محمد أمين الشوابكة، جرائم الحاسوب والإنترنت، الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، الطبعة الأولى، ٢٠٠٧م، ص ٢١٦،٢١٧.

١٤- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، سنة ٢٠٠٧، ص١٣٩.

١٥- محمد الشناوي، إستراتيجية مكافحة جرائم النصب المستحدثة، الإنترنت، بطاقات الائتمان، الدعاية التجارية الكاذبة، سنة ٢٠٠٦، ص٧١.

١٦- محمد عبد الله أبو بكر سلامة، جرائم الكمبيوتر والإنترنت، منشأة المعارف بالإسكندرية ٢٠٠٦م، ص ٢٧،٢٨.

١٧- مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية، ص٥١، دار النهضة العربية.

١٨- منير محمد الجنبيهي وممدوح محمد الجنبيهي جرائم الإنترنت والحاسب الآلى ووسائل مكافحتها، دار الفكر الجامعي، ٢٠٠٥، ص ١٦.

١٩- نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، دراسة نظرية وتطبيقية، الطبعة الأولى، سنة ٢٠٠٥، ص٣٣٢، منشورات الحلبي الحقوقية، بيروت – لبنان.

ثانياً: المراجع الأجنبية:

1 - Al-Rawashdeh, Illegal Access to Information System in the Qatari Criminal Laws: A Comparative Study, Kuwait International Law School Journal, vol (6) Iss. (1), (2018), P 34.

2 - BÌr. Polizeilicher Zugriff auf kriminelle Mailboxen, CR, 1995, S.489.

3 - Bühler, Ein Versuch, Computerkriminellen das Handwerk zu legen: Das Zweite Gesetz zur BekÌmpfung der WirtschaftskriminalitÌt, MDR 1987, S.448.

4 - Dannecker, BB 1996, S. 1285ff.; Tilch, ComputerkriminalitÌt, Deutsches Rechts-Lexikon, Bd. 1 1993, S. 883.

5 - Ha, Der strafrechliche Schutz von Compuzerprogrammen, in: Lehmann (Hrsg), Rechtsschutz und Verwertung von Computer-programmen, 2. Aufl. (1993), S. 479.

6 - Hilgendorf, Juristische Schulung (JuS) 1996, S. 891.

7 - Mwistra 1986, S. 141.

8 - Sch§ 303a, Rdnr. 4.

The Substantive Rules of the Offences of legal Access to Information System Under the Jordanian Cybercrime Act 2015 No 27: A Comparative Study

Dr. Mamoun Mohamad Saed Abu-Zayton
Prof. Mouaid Al-Qudah

Abstract:

This paper provides a comparative study of the offences of illegal access to information system pursuant to the Jordanian Cybercrime Act 2015 No 27. It explores the substantive law on these offenses as established in Articles (3 and 12) of the Jordanian law in comparison with other Acts. It basically addresses the offences of accessing a given information system or website without authorization or contrary to the granted authorization or by overriding it. Through analyzing the relevant law on this issue, the paper tends to trace the gaps and defects and any substantive flaws or imbalances in the laws governing such offences. Central to its purpose is to provide insight into how this comparative study might contribute to any potential law reform on this contentious issue. To this end, it is suggested that the Jordanian Act should be amended to explicitly criminalize the conduct of mistaken access to a given information system and with knowledge the offender persist to do so.

Key words: offences of illegal access, information system, cybercriminal, cross-border crime, access without authorization, overriding of authorization.

للاستشهاد:

أبو زيتون، مأمون. والقضاة، مؤيد. (2023). التنظيم الموضوعي لجرائم الدخول الإلكترونية سنداً لقانون الجرائم الإلكترونية الأردني رقم (27) لسنة 2015– دراسة مقارنة. *مجلة الحقوق، 47*(2)، 395–439.

To Cite:

Abu-Zayton, Mamoun. Al-Qudah, Mouaid.

(2023). The Substantive Rules of the Offences of lllegal Access to lnformation System Under the Jordanian Cybercrime Act 2015 No 27: A Comparative Study. *Journal of Law, 47*(2), 395-439.

JOURNAL OF LAW

A Refereed Academic Quarterly, Published by the Academic Publication Council - University of Kuwait

The Substantive Rules of the Offences of legal Access to Information System Under the Jordanian Cybercrime Act 2015 No 27: A Comparative Study

Dr. Mamoun Mohamad Saed Abu-Zayton
Prof. Mouaid Al-Qudah

جامعة الكويت
KUWAIT UNIVERSITY

ISSN: 1029 - 6069

No. 2, Vol. 47

Thul Hijja 1444 - June 2023