الحماية الجنائية للمعاملات الإلكترونية في قانون رقم ٢٠/٢٠١٤

أ. أحمد عبد اللطيف الجار الله
مدرس مساعد - قسم القانون العام
أكاديمية سعد العبد الله للعلوم الأمنية

ملخص:

تشير الدراسات والإحصائيات إلى زيادة مطردة في عدد مستخدمي الإنترنت. كما أن التعامل الإلكتروني بالنسبة للأفراد والشركات زاد بشكل ملحوظ بسبب سهولة وسرعة التعامل الإلكتروني الذي يوفر الوقت والجهد. إلا أن هذه الزيادة في عدد المستخدمين لم يرافقها سرعة إنجاز وصياغة القوانين التي تنظم التعامل الإلكتروني.

إن عالم التكنولوجيا الرقمية يتطلب تدخلاً سريعاً من الحكومة، والمتمثل بسن التشريعات والنظم واللوائح التي تكفل وجود غطاء آمن في عالم التكنولوجيا، وتقديم الخدمات الإلكترونية عالية المستوى للأفراد كي يستفيدوا منها، وهذا الأمر لن يتوفر إلا إذا أحس الأفراد بالأمن والثقة باستخدام التعاملات الإلكترونية عالية الخصوصية. كما أن وجود العقوبات الرادعة لكل من تسول له نفسه العبث في خصوصية الأفراد، يكفل تدني مستوى الجريمة خوفاً من العقاب.

وتأتي أهمية البحث بتسليط الضوء على الحماية الجنائية في التعاملات الإلكترونية وأهميتها. وهل تعتبر الحماية التي أقرها قانون المعاملات الإلكترونية رقم ٢٠/٢٠١٤ كافيه؟ وهل تتفق العقوبات المقررة في قانون التعامل الإلكتروني مع المبادئ العامة لقانون الجزاء؟ وهل تختلط مع بعض الضمانات الدستورية المقررة؟

المقدمة:

تكاد تجمع كل دساتير العالم على أن الخصوصية تعد من الحقوق الدستورية والأساسية للشخص الطبيعي كأصل عام، فهي تعتبر أساس بنيان كل مجتمع متحضر متطور. ولا نبالغ إذا قلنا إن الخصوصية موجودة قبل وجود الدساتير والقوانين.

وبالتالي فإن المجتمعات الديمقراطية تشدد على كفالة هذا الحق، وتجتهد إلى ترسيخه في عقول الناس من خلال القيم والقواعد الأخلاقية والقانونية. وهذه القواعد تلعب دوراً هاماً لمنع المتطفلين من التدخل في خصوصيات الآخرين وكشف أسرارهم وتعاملاتهم المالية أو الإدارية. وقد بدأت الدول تهتم بحماية الخصوصية في المعاملات

الإلكترونية من الناحية الجنائية على مختلف الأصعدة سواء من خلال سن التشريعات القانونية أو إنشاء المنظمات الدولية الخاصة بهذا الشأن.

إن التطور التكنولوجي الحديث، والنقلة النوعية التي أحدثتها البرمجيات في السنوات الأخيرة، وزيادة عدد مستخدمي الإنترنت والهواتف الذكية وتطورها المستمر أسهم في زيادة المخاطر على خصوصية الأفراد وتعاملاتهم، فالتكنولوجيا الحديثة أصبحت اليوم تقيد الفرد بشكل واضح، فتعرف مكانه وصوره وحياته وتحركاته، وهذا التطور التكنولوجي صار بلا شك يهدد الحياة الشخصية والحريات الفردية خاصة. وقد تستغل هذه المعلومات والبيانات لأهداف وأغراض عديدة بدون موافقة أو رضا أصحابها أو حتى بدون علمهم فتتم خلسة.

وتسعى دوله الكويت إلى مجتمع يستخدم تقنيات المعلومات والاتصال، وجميع الخدمات الحكومية الإلكترونية وذلك من خلال تفعيل قانون المعاملات الإلكترونية رقم ٢٠/٢٠١٤. ويعتبر هذا القانون هو أول تشريع كويتي لتنظيم التعاملات الإلكترونية، فهو يعالج العديد من القضايا الأساسية مثل: حماية البيانات، التواقيع الإلكترونية، صلاحية الدفع الإلكتروني، وحماية الخصوصية والعقوبات المقررة.

يقع القانون في (٤٦) مادة مقسمة إلى ثمانية فصول. الفصل الأول تعريفات، والفصل الثاني أحكام عامة، أما الفصل الثالث يتحدث عن المستند أو السجل الإلكتروني، والفصل الرابع يتكلم عن التوقيع الإلكتروني، والفصل الخامس الاستخدام الحكومي للمستندات والتوقيعات الإلكترونية، والفصل السادس الدفع الإلكتروني، والفصل السابع عن الخصوصية وحماية البيانات، والفصل الثامن أخيراً يتحدث عن العقوبات المقررة.

كما أن اللائحة التنفيذية للقانون رقم ٢٠/٢٠١٤ اشتملت على (٣٠) مادة منظمة للمعاملات الإلكترونية، ونصت إحدى المواد على أن يتضمن السجل الإلكتروني البيانات التي تحدد هوية السجل وارتباطه بالتعامل الإلكتروني والسجلات الإلكترونية الأخرى. وفي مادة أخرى نصت اللائحة التنفيذية على إلزام جميع العاملين بها بالشروط والمعايير المتعلقة بحماية الخصوصية المعمول بها في الجهات ولا يجوز الاطلاع عليها إلا من خلال الأشخاص المخولين بذلك.

ويهدف البحث إلى:

أ – إيضاح الخلط الحاصل في العقوبات المقررة لقانون المعاملات الإلكترونية رقم ٢٠/٢٠١٤ وبعض المبادئ العامة في قانون الجزاء.

ب – بيان مخاطر التكنولوجيا الحديثة على الحق في الخصوصية في التعاملات الإلكترونية.

وينقسم البحث إلى محورين، المحور الأول: الجانب الموضوعي ونتطرق فيه إلى ماهية الخصوصية المعلوماتية وأنواعها. وما هو المستند الإلكتروني وبيان أهميته من خلال التفسير الواسع والضيق. وما هي صور الاعتداء على النظام؟ وما هي أوجهه التمييز بين الاعتداء على النظام والاعتداء على المستند الإلكتروني؟ ثم نتحدث عن عناصر الجريمة في المستند الإلكتروني، وأخيراً الغرامة في القانون رقم٢٠/٢٠١٤.

أما المحور الثاني فنتحدث فيه عن الجانب الإجرائي وتطبيقه على قانون التعامل الإلكتروني من خلال بيان اختصاص النيابة العامة في الدعوى الجزائية من حيث الأصل واختصاصها في القانون رقم ٢٠/٢٠١٤ بشأن التعامل الإلكتروني، وما هو الشخص الاعتباري؟ وكيف تحدث جريمة الإهمال والإخلال بالواجبات؟ وما هي حدود الشخص المعنوي؟ وهل تصطدم العقوبات مع الضمانات الدستورية؟ وأخيراً معنى الصلح المقصود في قانون رقم ٢٠ لسنة ٢٠١٤ في شأن المعاملات الإلكترونية.

الفصل الأول
الجانب الموضوعي

ندرس في هذا الفصل ماهية الخصوصية المعلوماتية، واختلاف التشريعات الدولية في الحماية الجنائية للتعامل الإلكتروني، وما هي أنواع الخصوصية؟ وأثر التقنيات الحديثة على الخصوصية وخطورتها. وما هو تعريف المستند الإلكتروني؟ والآثار المترتبة على المساواة التشريعية بين التعامل الإلكتروني والمستند الورقي. وماهي طرق الإثبات في التعامل الإلكتروني والمعوقات التي يمكن أن تواجهها؟

المبحث الأول
ماهية الخصوصية المعلوماتية

أتاحت التكنولوجيا الحديثة لمستخدميها سهولة التواصل ونقل المعلومات والبيانات والتعامل بين الجهات المختلفة بالدولة من وزارات وشركات وغيرها من الأشخاص المعنوية.

وهو ما يوفر الوقت والجهد والمال على الطرفين مقدم الخدمة – الوزارات أو الشركات – ومستعملها وهم الأفراد وبعض الأشخاص المعنوية. فاليوم يمكن للفرد أن يدفع الرسوم ويجدد الرخصة التجارية، ويدفع الضريبة، أو ينهي معاملة المرور وهو خلف جهاز الحاسب الآلي دون الحاجة إلى الذهاب الشخصي أو تسليم النقود الفعلي لتلك الجهات.

إلا أن هذه الخدمات التي تحاول أن تواكب التطور الهائل في مجال المعلومات صارت عرضة للخطر من قبل أشخاص ضعاف النفوس مهمتهم الاحتيال والمساس بالخصوصية؛ لذلك اقتضت الضرورة سن تشريعات تحد من المساس بخصوصية الأفراد ومعلوماتهم وبالتالي تجريم الأفعال التي تنطوي على ذلك.

وترجع أهمية التعامل الإلكتروني على وجه الخصوص إلى أن المستند الإلكتروني – إذا توافرت شروطه – صار يتماثل مع المستند الورقي في كثير من التشريعات من حيث القوة القانونية[١]. إن مفهوم الحكومة الإلكترونية لا يتحقق إلا

(١) أشرف توفيق شمس الدين، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية منظم المؤتمر: أكاديمية شرطة دبي، مركز البحوث والدراسات رقم العدد: ١ السنة: ٢٠٠٣ تاريخ الانعقاد: ٢٦ نيسان ٢٠٠٣ تاريخ الإنهاء: ٢٨ نيسان ٢٠٠٣ الدولة: دبي – الإمارات العربية المتحدة.

من خلال المستند الإلكتروني الذي يتيح للمستخدم جميع الخدمات الممكنة، وبالتالي بات من الضروري حمايته من خلال تشريع قانوني وهو قانون المعاملات الإلكترونية رقم ٢٠/ ٢٠١٤.

أ – المطلب الأول
تنوع مفاهيم الخصوصية

للحق في الخصوصية أساس دستوري كفل بها الحرية الفردية للأشخاص، ويعتبر الحق في الخصوصية أحد عناصر الدستور الأساسية، ونصت أغلب الدساتير حول العالم صراحة على حماية الحق في الحياة الخاصة من مراسلات بريدية وخصوصية الجسم وحرية الانتقال والاتصال وغيرها في حدود القانون.

أولاً – لمحة تاريخية عن الاتفاقيات والمعاهدات والتشريعات الدولية التي تهدف إلى حماية الخصوصية والتعامل الإلكتروني:

حرصت المنظمات الدولية على إرساء قواعد للتعاون والتنسيق الدولي لحماية الخصوصية والتعامل الإلكتروني، وترجم ذلك من خلال اتفاقيات أو معاهدات أو توصيات بتطوير التشريعات الجنائية ومن هذه الاتفاقيات(٢):

١ – موجهات حماية الخصوصية وانسياب البيانات الشخصية عبر الحدود لسنة ١٩٨٠ Guideline on Protection of Privacy and Trans border Flow of Personal Data-Organization of Economic Cooperation and Development.

٢ – اتفاقية الاتحاد الأوروبي الخاصة بحماية التعامل الإلكتروني مع البيانات الشخصية ١٩٨١.

٣ – القانون النموذجي للتجارة الإلكترونية لسنة ١٩٩٨، الصادر عن لجنة الأمم المتحدة لقانون التجارة الدولية UNCITRAL.

٤ – القانون النموذجي لإجراءات التحقيق في الجرائم الإلكترونية، لجامعة دايتون، Model Code of Cyber Crimes Investigation Proceduer,2000.

٥ – الاتفاقية الأوروبية العالمية للجرائم (السايبرانية)، European Convention on Cyber Crime of 2001.

(٢) محمد الأمين البشري، الجرائم الإلكترونية التحقيق الادعاء المحاكمة ومعاملة المذنبين فيها (الإمارات العربية المتحدة، حكومة دبي، ٢٠١٢)، ص٥٠.

٦ – المعاهدة الدولية للجرائم الإلكترونية لسنة ٢٠٠٣، International Treaty of Cyber Crimes.

٧ – المواجهات الدولية لمكافحة الجرائم الإلكترونية، International Guide liner for Combating Cyber Crimes.

٨ – الإستراتيجية الأمريكية لمكافحة محددات الأمن الإلكتروني. Inter-American Strategy to Combat Threats to Cyber Security,200.

٩ – معاهدة المجلس الأوروبي للجرائم (السايبرانية) لسنة ٢٠٠٤، Council of Europe Convention on Cyber Crime. وقد انضمت لها الولايات المتحدة الأمريكية سنة ٢٠٠٦.

أما فيما يتعلق بالتشريعات فنورد أهم هذه التشريعات طبقاً لتواريخ إصدارها ونشرها(٣):

١ – القانون الفرنسي لجرائم الكومبيوتر لسنة ١٩٩٠.

٢ – قانون إساءة استخدام الحاسب الآلي البريطاني لسنة ١٩٩٠.

٣ – قانون المعاملات الإلكترونية الموحد الأمريكي لسنة ١٩٩٩.

٤ – القانون الموحد لمعلومات الحاسب الآلي الأمريكي لسنة ٢٠٠٠.

٥ – قانون تقنية المعلومات الهندي لسنة ٢٠٠٠.

٦ – قانون الجرائم الإلكترونية الباكستاني لسنة ٢٠٠٣.

٧ – قانون مكافحة جرائم تقنية المعلومات الإماراتي لسنة ٢٠٠٦.

ومع هذا الكم الكبير من التشريعات والاتفاقيات الدولية فلا بديل عن نشر الوعي والتعليم بين جميع أفراد المجتمع، وفي ذلك يقول Virgo: "لن يتمكن أي قدر من التشريعات من منع وقوع الجريمة الإلكترونية طالما أن هناك أشخاصاً يمكن التحايل عليهم"(٤).

ونحن نرى أن التطور الحاصل في الجرائم الإلكترونية يحب أن يوازيه تطور نوعي من خلال اختصار إجراءات التشريع أو التعديل عليها، بحيث تصبح مواكبة لمستجدات هذه الجرائم. إن ما يحصل اليوم من جرائم إلكترونية تتم من خلال برامج جاهزة تنفذ الجريمة وتحدد الضحية وموقعها وتحسب العائدات المالية وتقضي على

(٣) محمد الأمين البشرى: مرجع سابق، ص٥٠.

(٤) Philip Virgo, Eurim, 2003, Auailable at www.zdnet.co.uk

الأدلة التي تثبت التهمة[٥]. لذا من الواجب أن تكون لدينا تشريعات على هذه الدرجة من الفاعلية والجاهزية.

إن حرية انتقال المعلومات والبيانات هي إحدى الحريات الأساسية التي تحرص عليها الدساتير، ولاريب أن تقدم وتطور المجتمعات يقاس بجانب الحرية التي يسمح بها الدستور وينظمها القانون، فكلما كانت هناك حرية على أساس قانوني واضح ورصين كان هناك شعب متطور متحضر، وقد كفل الدستور الكويتي حقوق وحريات الأفراد ونص عليها، كما أن الحرية بصورها المختلفة مثل حرية الاعتقاد وحرية التعبير، هي أساس أي مجتمع ديمقراطي حر، فحرية الرأي والتعبير وحرية الصحافة والإعلام مكفولة وفق ما تنظمه الدول من قوانين. ويكمن تعريف الحرية كما في المادة (٤) من إعلان حقوق الإنسان الصادر في ١٧٨٩م بأنها: " القدرة على إتيان كل عمل لا يضر بالآخرين "[٦].

وقد تطرق القانون ٢٠/٢٠١٤ بشأن التعامل الإلكتروني في المادة رقم (٣٢) "لا يجوز في – غير الأحوال المصرح بها قانوناً – للجهات الحكومية أو الهيئات أو المؤسسات العامة أو الشركات أو الجهات غير الحكومية أو العاملين بها الاطلاع دون وجه حق أو إفشاء أو نشر أية بيانات أو معلومات شخصية مسجلة في سجلات أو أنظمة المعالجة الإلكترونية المتعلقة بالشؤون الوظيفية أو بالسيرة الاجتماعية أو بالحالة الصحية أو بعناصر الذمة المالية للأشخاص أو غير ذلك من البيانات الشخصية المسجلة لدى أي من الجهات المبينة في هذه المادة أو العاملين بها بحكم وظائفهم، ما لم يتم ذلك بموافقة الشخص المتعلقة به هذه البيانات أو المعلومات أو من ينوب عنه قانوناً، أو بقرار قضائي مسبب، وتلتزم الجهات المبينة في الفقرة الأولى من هذه المادة ببيان الغرض من جمع البيانات والمعلومات المذكورة، وأن يتم جمع تلك البيانات والمعلومات في حدود ذلك الغرض".

إن الحق في الخصوصية وحمايته حاز على اهتمام كبير من جانب الهيئات والمنظمات الدولية والدساتير والتشريعات، منها على سبيل المثال اتفاقيات دولية كالإعلان العالمي لحقوق الإنسان الصادر من الجمعية العامة للأمم المتحدة بموجب

(٥) Power, Richard: Curvent and Future Danger, San Francisco: Computer Security Institute 1995.

(٦) The Universal Declaration of Human Rights (UDHR) Article(4).

قررها رقم ٢١٧ المؤرخ في ١٠/١٢/١٩٤٨ م في المادة (١٢)[٧]. أما على صعيد المؤتمرات الدولية فهناك العديد منها انعقدت في جميع أنحاء العالم لبحث أفضل الوسائل لحماية الحق في الخصوصية ومن أهمها[٨] ما عقد في مونتريال، وكذلك مؤتمر الإسكندرية.

كما ناقشت دراسة Vasua القوانين التي أقرتها الدول المتقدمة مثل الولايات المتحدة الأمريكية واليابان وإيطاليا وفرنسا وألمانيا لمواجهة الجرائم الإلكترونية. وخلصت هذه الدراسة إلى إصباغ المنظور العالمي على الجريمة الإلكترونية واعتبارها جريمة عابرة للقارات تتطلب تعاوناً دولياً[٩].

وفي هذا الإطار هناك العديد من الاتفاقيات الدولية منها على سبيل المثال لا الحصر، اتفاقية الاتحاد الأوروبي الخاص بحماية التعامل الإلكتروني مع البيانات الشخصية لسنة ١٩٨١، وكذلك المعاهدة الدولية للجرائم الإلكترونية ٢٠٠٣، والقانون النموذجي للتجارة الإلكترونية UNCITRAL لسنة ١٩٩٨[١٠]. إلا أن هذا الكم الهائل من القوانين والمعاهدات والاتفاقيات الدولية لم يمنع الجريمة بشأن سرية المعلومات أو البيانات الخاصة بالأفراد بشكل تام.

ونحن نرى ضرورة نشر الوعي والثقافة بخطورة انتهاك الخصوصية، ومن ثم تقريب الصورة للجمهور من خلال القوانين واللوائح التي تحكم الأفعال التي تمس خصوصياتهم، فبقدر ما يكون هناك ثقافة لدى الناس بقدر ما تنخفض الجريمة، ولا أدل على ذلك مما تقوم به الدول الإسكندنافية من غلق للسجون بسبب انخفاض معدلات الجريمة، بسبب زيادة الوعي لدى شعوبها.

أما على الصعيد المحلي فإن الاهتمام بهذا الحق يبرز من خلال الدساتير

---

(٧) المادة (١٢): "لا يعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه وسمعته، ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات."

(٨) المؤتمر الدولي لحقوق الإنسان المنعقد في طهران في الفترة من ٢٢ إبريل إلى ١٣ مايو – ومؤتمر حقوق الإنسان المنعقد خلال العام الدولي لحقوق الإنسان ١٩٦٨م في مونتريال وكان عن التجسس الإلكتروني – ومؤتمر الحق في حرمة الحياة الخاصة الذي انعقد بمدينة الإسكندرية خلال الفترة من ٤-٦/٦/١٩٨٧م.

(٩) Deva Vasua, E-Crime and Remedies. Delhi: Saujanya Book, 2005.

(١٠) محمد الأمين البشرى: مرجع سابق، ص٥١.

والقوانين الخاصة، ومنها المواد (٤٥) و(٥٧) في الدستور المصري ١٩٧١[١١]، وكذلك الدستور الكويتي في المواد (٣٠)، (٣١)، (٣٦)، (٣٧)، (٣٩)[١٢].

ويمكن تلخيص أهم ملامح القانون رقم ٢٠/٢٠١٤ بشأن التعامل الإلكتروني فيما يلي:

١ – إضفاء حجية الإثبات القانونية للكتابة الإلكترونية وللتوقيع الإلكتروني في نطاق المعاملات المدنية والإدارية، ليكون لهما نفس الحجية القانونية في الإثبات للكتابة العادية وللتوقيع العادي.

٢ – إنشاء ما يسمى بالمحرر الإلكتروني وتعريفه وإعطاؤه نفس مفهوم المحرر الكتابي سواء من جواز اعتباره محرراً إلكترونياً عرفياً أو محرراً إلكترونياً رسمياً.

٣ – اتساع نطاق تطبيق التوقيع الإلكتروني وفقاً لهذا القانون ليشمل جميع المعاملات التي يجوز إتمامها إلكترونياً وهي المعاملات المدنية والإدارية والتجارية بشرط أن تكون موقعة إلكترونياً وفقاً للشروط والضوابط التي وضعها القانون ولائحته التنفيذية.

---

(١١) مادة (٤٥) من الدستور المصري: "لحياة المواطنين الخاصة حرمة يحميها القانون. وللمراسلات البريدية والبرقية والمحادثات التليفونية وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة، ولا تجوز مصادرتها أو الاطلاع عليها أو رقابتها إلا بأمر قضائي مسبب ولمدة محددة ووفقا لأحكام القانون".
مادة (٥٧) من الدستور المصري: "كل اعتداء على الحرية الشخصية أو حرمة الحياة الخاصة للمواطنين وغيرها من الحقوق والحريات العامة التي يكفلها الدستور والقانون جريمة لا تسقط الدعوى الجنائية ولا المدنية الناشئة عنها بالتقادم، وتكفل الدولة تعويضاً عادلاً لمن وقع عليه الاعتداء".

(١٢) مادة (٣٠) من الدستور الكويتي "الحرية الشخصية مكفولة".
المادة (٣١) من الدستور الكويتي "لا يجوز القبض على إنسان أو حبسه أو تفتيشه أو تحديد إقامته أو تقييد حريته في الإقامة أو التنقل إلا وفق أحكام القانون، ولا يعرض أي إنسان للتعذيب أو للمعاملة الحاطة بالكرامة".
مادة (٣٦) من الدستور الكويتي "حرية الرأي والبحث العلمي مكفولة، ولكل إنسان حق التعبير عن رأيه ونشره بالقول أو الكتابة أو غيرهما، وذلك وفقا للشروط والأوضاع التي يبينها القانون".
مادة (٣٧) من الدستور الكويتي "حرية الصحافة والطباعة والنشر مكفولة وفقا للشروط والأوضاع التي يبينها القانون".
مادة (٣٩) من الدستور الكويتي "حرية المراسلة البريدية والبرقية والهاتفية مصونة، وسريتها مكفولة، فلا يجوز مراقبة الرسائل، أو إفشاء سريتها إلا في الأحوال المبينة في القانون وبالإجراءات المنصوص عليها فيه."

٤ – حرص القانون على إلزام الجهات التي ستقدم خدمات التصديق الإلكتروني أو الخدمات المتعلقة بالتوقيعات الإلكترونية بالحصول على التراخيص اللازمة لهذا النشاط من هيئة تقنية المعلومات بصفتها الجهة المختصة، وبما يضمن توافر الثقة والرقابة اللازمة لصحة وسلامة المعاملات الإلكترونية.

٥ – ركز القانون على وضع المبادئ والشروط العامة الأساسية لتنظيم التوقيع الإلكتروني، وترك أمر الضوابط الفنية والتقنية التفصيلية لأحكام هذا التنظيم للائحته التنفيذية، وذلك لما لهذه الشروط من أبعاد فنية وتقنية دقيقة يتعذر وضعها في متن القانون، كما أن لوجود هذه الضوابط الفنية داخل اللائحة التنفيذية ضرورة أخرى وهي سهولة تعديلها إذا اقتضى الأمر ذلك، حيث إن تلك الضوابط تكون عرضة للتغيير نظراً للتطور التقني (التكنولوجي) السريع والمستمر في مجال تكنولوجيا المعلومات والاتصالات.

٦ – تعامل القانون مع بعض الجرائم المعلوماتية التي من الممكن أن تقع في مجال المعاملات الإلكترونية، وذلك تحقيقاً لمبدأ الردع العام والخاص في هذا المجال، وبقصد دعم الثقة في التعامل الرقمي واستخدام تكنولوجيا المعلومات وتشجيع التعامل بها دون تخوف من أي فعل إجرامي قد يكون من شأنه هدم التعامل الإلكتروني بصفة عامة.

إن التشريعات اختلفت في الحماية الجنائية للتعامل الإلكتروني على ثلاثة اتجاهات:

الاتجاه الأول: مثل تشريعات الولايات المتحدة الأمريكية ترى إصدار قانون يعاقب على الجرائم بمختلف صورها.

والاتجاه الثاني: مثل المشرع الفرنسي والألماني يرى تعديل التشريعات القائمة على نحو يؤدي إلى استيعابها الصور المستحدثة من الجرائم الإلكترونية.

والاتجاه الثالث: يتمثل في غالبية تشريعات الدول العربية. والتي لم تفرد بعد تجريماً خاصاً للجرائم الإلكترونية، وما زالت تكتفي بالنصوص التقليدية التي ينص عليها في التشريعات المختلفة ومن أهمها قانون العقوبات(١٣).

(١٣) أشرف توفيق شمس الدين، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية منظم المؤتمر: أكاديمية شرطة دبي، مركز البحوث والدراسات رقم العدد: ١ السنة: ٢٠٠٣ تاريخ الانعقاد: ٢٦ نيسان ٢٠٠٣ تاريخ الإنهاء: ٢٨ نيسان ٢٠٠٣ الدولة: دبي – الإمارات العربية المتحدة.

وفي تقديرنا أن التشريعات المقارنة التي تم استعراضها لم تنجح تماماً بتوفير حماية جنائية فعالة للمستند الإلكتروني، من الناحية الأولى فإنه على خلاف ما هو سائد بالنسبة لفكرة المحرر التقليدية فإن هذه التشريعات لم تقم بإرساء معالم واضحة للمستند الإلكتروني، وذلك أن بعضها اقتصر على إصدار قانون للتوقيع الإلكتروني، والبعض الآخر أضاف له السجل الإلكتروني، وبعض التشريعات المقارنة قد خلطت بين فكرة المستند الإلكتروني وبين البيانات والمعلومات الإلكترونية. ونحن نرى أن تجريم أفعال المساس بالمستند الإلكتروني يجب أن يسبقه العمل بسياسة وقائية تحاول أن تضع الضوابط التي تقي من المساس به قبل وقوعه.

وعلى الرغم من اختلاف القوانين بين الدول على الاتجاهات الثلاثة التي أشرنا إليها، إلا أنها تتفق جميعاً وتحرص على الردع العام والخاص في قوانينها، وإلى إعطاء المزيد من الثقة للجمهور في أن تعاملاتهم الإلكترونية آمنة وسليمة.

ثانياً – المقصود بخصوصية المعلومات وأنواعها:

الخصوصية من حيث مفهومها جرى التعامل معها كحق لمنع إساءة استخدام الحكومة للبيانات التي يصار لمعالجتها آلياً أو إلكترونياً أو تقييد استخدامها وفق القانون. ومن المعلوم أن للحياة الشخصية خصوصية حفظها الدستور وعنى بها القانون، ومع ذلك قد يستخدم هذه المعلومات أشخاص غير مصرح لهم أو بدون إذن من صاحب المعلومة، وهو ما يشكل جريمة التعدي على الحياة الخاصة(١٤). كمن يعد ملفاً كاملاً عن شخص سياسي مهم وينشر بياناته الخاصة أو عدد كفالاته أو معاملاته وغيرها.

ثالثاً – أثر التقنيات الحديثة على الخصوصية وخطورتها:

إن وسائل التقنية الحديثة في جمع ومعالجة البيانات الشخصية سواء من الدولة أو القطاع الخاص والاطلاع على شؤون الأفراد ومعلوماتهم، وضعنا في موضع التناقض بين حرية الدولة بالاطلاع على المعلومات الشخصية والحماية الجنائية المقررة لها، فالحق في الحياة الخاصة وحق الدولة في الاطلاع على شؤون الأفراد، يتناقض مع استخدام الدولة المعلومات الشخصية لأغراض تتناقض مع احترامها. وحق الفرد في الاحتفاظ بسريته، والحق في الحياة الخاصة وبين حرية الصحافة التي قد تتدخل في شؤون الأفراد وتكتب بعض التصريحات المبالغ فيها في سبيل تحقيق الأرباح من خلال البيع.

(١٤) خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية (الدار الجامعية، ٢٠٠٨)، ص٧٢.

إن هذه التناقضات عمقت الفجوة بين التشريعات الدستورية في صيانة هذه الحقوق والقوانين الخاصة التي تحمي الخصوصية في التعامل الإلكتروني، إن الهدف الرئيسي للتشريع هو تحقيق التوازن بين المصالح المتعارضة، والشعور بمخاطر تقنية المعلومات وتهديدها للخصوصية بدأ بالتطور مع اتساع دائرة الاعتداء على حق الأفراد في الحياة الخاصة، ولذلك لا بد من العمل على إيجاد التوازن بين حاجة المجتمع للبيانات الشخصية وحمايتها من الاستخدام غير المشروع.

في الماضي كانت المعلومات الشخصية متفرقة ويصعب الوصول إليها، أما اليوم فأصبحت مجمعة ومتاحة للكافة، وهناك الكثير من الحكومات والشركات الخاصة تجمع المعلومات والبيانات عن الأفراد الخاصة بالوضع الصحي أو المادي أو التعليمي أو العائلي أو العادات الاجتماعية أو تاريخ الميلاد وعدد الأبناء أو مقر العمل(١٥)، مما يجعل الوصول إليها بغير إذن أكثر من ذي قبل، ويفتح المجال لإساءة استخدامها ومراقبة الأفراد وتعرية خصوصياتهم.

ومما يدل على خطورة الوضع أن الدول المتقدمة التي تحمي الخصوصية قد ارتكبت العديد من المخالفات في استخدام البيانات الخاصة لأهداف سياسية أو اقتصادية أو لقمع الخصوم السياسيين(١٦). وقد صرح "إريك شفايتسر" رئيس غرفة الصناعة والتجارة الألمانية أنه يعلن تخلي دولتهم عن التجسس الاقتصادي.

كما أن البعض يعتبر الحروب بين الدول لم تعد – كما في السابق – مقتصرة على ميادين وساحات القتال الجغرافية، وإنما أصبحت الآن إلكترونية من الدرجة الأولى. فالصين اليوم تواجه اتهاماً من الولايات المتحدة الأمريكية بأنها اخترقت مواقع حكومية وأخذت بيانات شخصية عن العاملين لدى الحكومة الأمريكية في مواقع حساسة(١٧). عما يقارب من أربعة ملايين موظف فيدرالي على الأقل، في هجوم إلكتروني ضخم مصدره الصين.

رابعاً – خصوصية الجسم:

لجسم الإنسان حرمة فأي شكل من أشكال الاعتداء عليه مرفوض جملة وتفصيلاً، وإن كان قد سمح القانون في بعض الحالات باستباحته خصوصية الجسم

(١٥) Face book: Facebook is an online social networking service headquartered in Menlo Park, California.

(١٦) http://aawsat.com/home/article/373401 مطالبة ألمانية ببحث تجسس واشنطن على شركات أوروبية في قمة الدول السبع.

(١٧) http://www.alyaum.com/article/4071469

في بعض الحالات لخطورتها كالجريمة المشهودة التي تبيح القبض والتفتيش، إلا أن الأصل العام أن للجسم حرمة فلا يجوز تعذيب الإنسان أو إهانته[١٨]. كما إن حقوق الذات الإنسانية مصانة من أي انتهاك جسماني أو معنوي، حتى يحيا الإنسان في حرية يستطيع من خلالها ممارسة كافة حقوقه المدنية، فهناك مبدأ يسمى معصومية جسم الإنسان[١٩]. أي لا يجوز لأحد أن يعتدي على سلامة جسم إنسان آخر بأي وسيلة كانت، ويتكفل القانون الجنائي بعقاب المعتدي، أما القانون المدني ينظر بتعويض المضرور عما لحقه من ضرر.

ويلحق بها **الجرائم المخلة بالآداب العامة:** إن التطبيقات الموجودة على الأجهزة الإلكترونية من فيديو ورسائل نصية وبرامج اجتماعية وصور فوتوغرافية وتسجيلات صوتية سهلت صناعة الإباحية بشكل كبير، بل وصار الإنترنت والتطبيقات البرمجية هي الوسيلة الأسهل للحصول على المتعة أو استغلال الأطفال جنسياً. ويستغل العاملون في مجال الرذيلة شبكة الإنترنت وسهولة اتصال الجميع فيها، فيقومون بعرض الصور كدعايات أو إرسال رسائل عن طريق البريد الإلكتروني أو إنشاء موقع رسمي يدار من قبل محترفين ممن يسمح لهم القانون بذلك كما في الدول الأجنبية.

كما يرتبط نشر المواد الإباحية في الإنترنت بمجالين: الأول ما يتعلق بنشر الصور المخلة الخاصة بالأطفال Child Pornography، والثاني يتعلق بالمواد المخلة بالكبار Adult Pornography. وقد قامت وزارة الداخلية في دولة الكويت في عام ٢٠١٤عن طريق إدارة مكافحة الجرائم الإلكترونية بإغلاق أكثر من ٣٠٠ حساب على موقع الإنستغرام[٢٠] من ضمنها ما هو إباحي أو يحرض على الفسق والفجور أو حتى يقوم ببيع منتجات ممنوعة من مختلف برامج التواصل الاجتماعي. ويتم اتخاذ الإجراءات القانونية بحق أصحاب تلك الحسابات وتحويلهم إلى الجهة المختصة، كما أن إدارة مكافحة الجرائم الإلكترونية تقوم برصد تلك الحسابات وملاحقتها قانونيا واتخاذ ما يلزم بحقهم.

---

(١٨) مادة (٣١) من الدستور الكويتي "لا يجوز القبض على إنسان أو حبسه أو تفتيشه أو تحديد إقامته أو تقييد حريته في الإقامة أو التنقل إلا وفق أحكام القانون، ولا يعرض أي إنسان للتعذيب أو للمعاملة الحاطة بالكرامة".

(١٩) أحمد رشيد المطيري، محمد سليمان الرشيدي: المبادئ العامة للقانون (الطبعة الرابعة، ٢٠٠٩)، ص١٦٤.

(٢٠) إنستغرام (بالإنجليزية: Instagram) هو تطبيق مجاني لتبادل الصور وشبكة اجتماعية أيضا، أطلق في أكتوبر عام ٢٠١٠، يتيح للمستخدمين التقاط صورة، وإضافة فلتر رقمي إليها، ومن ثم مشاركتها في مجموعة متنوعة من خدمات الشبكات الاجتماعية.

خامساً – خصوصية الاتصال والمراسلات:

نص الدستور الكويتي على خصوصية الاتصال والمراسلات[٢١]. وهو أمر ينسحب بالضرورة على جميع وسائل الاتصال من بريد إلكتروني، أو عادي، أو هاتف محمول أو أرضي، أو أي تعامل الإلكتروني آخر فهي مصانة دستوريا. إن مبدأ حماية الحياة الخاصة يجعل حياة الفرد ومراسلاته مصانة من الاطلاع عليها وبعيدة عن العلانية. وكما يحظر على الأشخاص المعنيين نشر أو إفشاء هذه المرسلات أو الأسرار[٢٢]. وقد حرصت التشريعات الأوروبية على سرية الاتصالات الإلكترونية وحظرت التنصت عليها أو الاحتفاظ بها لغير الغرض المخصص من أجله[٢٣]. كما أن فرنسا أنشأت لجنة وطنية للمعلومات والحريات وهدفها تثقيف الناس وتوعيتهم بحقوقهم والتزاماتهم، ومراقبة معالجة بياناتهم بما يضمن السرية والحرية وعدم استخدام هذه البيانات إلا في حدود الغرض الذي خصص من أجله[٢٤].

ومن المؤسف القول إن بعض هيئات المعلومات صارت تستغل المعلومات الشخصية للأفراد كوسيلة لتحصيل الربح وعمل التغطية الدعائية وذلك من خلال بيعها للمعلومات والبيانات؛ لذلك حرصت الدول المتقدمة على أن تتضمن قوانينها مجموعة من المبادئ، وهي على سبيل المثال لا الحصر مبدأ ضمان السرية، والشفافية، ومبدأ المسؤولية، ومبدأ تخصيص البيانات للغرض الذي جمعت المعلومات من أجله[٢٥]. ويمكن التمييز بين المعلومة السرية وغير السرية من خلال صفة المعلومة التي يكون لها طابع سري.

فيعتبر من المعلومات السرية على سبيل المثال ميزانيات الدول، والحالة الصحية للمريض. وكذلك تعد المعلومة سرية إذا وصلت هذه المعلومة إلى شخص مؤتمن بحكم عمله أو وظيفته، وتعتبر جريمة إفشاء السر من الجرائم العمدية التي تتطلب

---

(٢١) مادة (٣٩) من الدستور الكويتي "حرية المراسلة البريدية والبرقية والهاتفية مصونة، وسريتها مكفولة، فلا يجوز مراقبة الرسائل، أو إفشاء سريتها إلا في الأحوال المبينة في القانون وبالإجراءات المنصوص عليها فيه".

(٢٢) أحمد رشيد المطيري، محمد سليمان الرشيدي: مرجع سابق، ص١٦٨.

(٢٣) انظر: التوجيه الأوروبي (توجيه الحياة الخاصة والاتصالات الإلكترونية).

(٢٤) إبراهيم أبو الليل، الجوانب القانونية للتعاملات الإلكترونية (٢٠٠٣) ص٦٠.

(٢٥) نبيل محمد أحمد صبح، حماية المستهلك في التعاملات الإلكترونية – دراسة مقارنة (جامعة الكويت: مجلة الحقوق، مجلس النشر العلمي، العدد ٢، السنة ٣٢، يونيو، ٢٠٠٨)، ص٢٥٠.

القصد الجنائي. والاتجاه الفقهي السائد لا يشترط نية الإضرار في جريمة إفشاء السر المعلوماتي، كما لا يعتد في الباعث على ذلك كالكره أو الربح المالي أو الرشوة(٢٦).

يحق لأي إنسان حجب معلوماته الشخصية عن الآخرين، فأي تطفل على معلومات الشخص من مكتبه أو منزله أو حاسبه الشخصي أو حتى أفكاره يعد انتهاكاً للخصوصية، فالتطفل لا يعني تدمير المعلومات وإنما فقط الاطلاع يعد انتهاكاً لخصوصية الإنسان الفردية(٢٧). وتضمن الدول المتقدمة في دساتيرها نصوصاً على حرمة الحياة الخاصة لجميع الأفراد، وتأتي هذه النصوص غالباً عامة وتحرم الاعتداء على المحادثات الهاتفية أو استراق السمع أو النقل أو التسجيل عن بعد أو عبر شبكات المعلومات بأنواعها، والتي يمكن للجاني التسلل من خلالها لارتكاب أفعاله الإجرامية.

كما وجاءت بعض النصوص تحرم إفشاء المعلومات والبيانات لمن يتعلق عملهم فيها، وحددت على سبيل المثال وليس الحصر مثل المحامي والطبيب والصيدلي والقاضي والعاملين في المصانع والمبرمجين وغيرهم وأغلب أصحاب المهن الحرة. وقد نص قانون العقوبات الفرنسي على "كل مدير أو ممثل أو عامل يطلع أو يحاول إطلاع الأجانب أو الفرنسيين المقيمين في الخارج على أسرار المصنع الذي يعمل فيه سيعاقب بالسجن لمدة تتراوح بين سنتين وخمس سنوات..." (٢٨).

ويثور الجدل حول قضية السبب الرئيسي لانتهاك الخصوصية، هل هي بسبب انتشار استخدام الحاسب الآلي وسهولة الدخول على الإنترنت؟ أم هي بسبب المستخدم وإهماله في تشفير وحماية معلوماته الشخصية وعدم إلمامه بخطورة التعامل الإلكتروني، ونحن نرى أن وجود المعلومات والبيانات في الحاسب الآلي في حيز ضيق محدود واتباع الوسائل الصحيحة في التشفير وحفظ المعلومات وتغيير كلمات السر بصورة مستمرة يجعل البيانات الشخصية أكثر أماناً.

وهناك تساؤل آخر يلقي بظلاله، هل التنصت الحكومي مباح؟ لأن هناك تضارب بين حق الفرد بالخصوصية وبين حاجة الدولة لاختراق الخصوصية لفرض هيبة القانون ومنع الجريمة، بدأ هذا التضارب عالمياً عام ١٩٨٢ عندما لجأت بعض الدول

(٢٦) بلال أمين زين الدين، جرائم نظم المعالجة الآلية للبيانات في التشريع المقارن والشريعة الإسلامية (الإسكندرية: دار الفكر الجامعي، ٢٠٠٨)، ص٢٩٨.

(٢٧) حسن طاهر داوود، جرائم نظم المعلومات (الرياض: الطبعة الأولى، ٢٠٠٠)، ص٥٠.

(٢٨) قانون العقوبات الفرنسي المادة (٤١٨).

إلى التنصت الهاتفي لمكافحة الجريمة[٢٩]. وذلك أن البعض يرى أن اختراق مثل هذه المعلومات يقدم الأدلة ضد المتهمين ويساهم في الحصول على اعترافاتهم بشكل كبير.

ويلحق بها **جرائم السب والقذف عبر الإنترنت**: وتعد جرائم السب والقذف عبر الإنترنت وخصوصاً مواقع التواصل الاجتماعي أمراً شائعاً جداً. وقد نص قانون الجزاء الكويتي في المادة (٢٠٩) "كل من أسند لشخص، في مكان عام أو على مسمع أو مرأى من شخص آخر غير المجني عليه، واقعة تستوجب عقاب من تنسب إليه أو تؤذي سمعته، يعاقب بالحبس مدة لا تجاوز سنتين وبغرامة لا تجاوز ألفي روبية أو بإحدى هاتين العقوبتين".

وكذلك المادة (٢١٠) "كل من صدر منه، في مكان عام أو على مسمع أو مرأى من شخص آخر غير المجني عليه، سب لشخص آخر على نحو يخدش شرف هذا الشخص أو اعتباره، دون أن يشتمل هذا السب على إسناد واقعة معينة له، يعاقب بالحبس مدة لا تجاوز سنة واحدة وبغرامة لا تجاوز ألف روبية أو بإحدى هاتين العقوبتين".

وقد اعتبرت محكمة التمييز الكويتية أن مواقع التواصل الاجتماعي مكان عام، وبالتالي أرست محكمة التمييز الكويتية مبدأ جديداً أن موقع (تويتر)[٣٠] يعتبر مكاناً عاماً ومن ثم يخضع لقانون الجزاء الكويتي، وتطبيقاً لذلك الحكم فإن كل من يغرد في تويتر من داخل دولة الكويت يخضع لقانون الجزاء الكويتي وذلك لتحقق ركن العلانية في موقع التواصل الاجتماعي، فتنطبق أحكام مادتي (٢٠٩) و(٢١٠) من قانون الجزاء الكويتي على المغردين.

ب – المطلب الثاني
تعريف المستند الإلكتروني وبيان أهميته

إن التعامل الإلكتروني يعتبر من المواضيع القانونية الجديدة التي حازت على اهتمام الفقه القانوني، وبسبب هذا التطور صار بالإمكان نقل وتبادل البيانات عن بعد بين أجهزة الكومبيوتر الخاصة بالأفراد والدولة، وهو ما أحدث انعكاسات من الناحية

(٢٩) حسن طاهر داوود: مرجع سابق، ص٥٤.

(٣٠) أحد أشهر الشبكات الاجتماعية ووسائل التواصل الاجتماعي، يقدم خدمة التدوين المصغر والتي تسمح لمستخدميه بإرسال "تغريدات" عن حالتهم أو عن أحداث حياتهم أو إبداء آرائهم بحد أقصى ١٤٠ حرفاً للرسالة الواحدة.

القانونية على الإثبات بالطرق التقليدية المقررة وفقاً للضوابط التي يحددها القانون، وأهمية المساواة بين المستند الإلكتروني الرسمي إذا تم وفقا لشروطه والمستند الورقي الرسمي.

أولاً – مفهوم المستند الإلكتروني:

يمكن تعريف المستند أو السجل الإلكتروني بأنه مجموعة بيانات أو معلومات يتم إنشاؤها أو تخزينها أو استخراجها أو نسخها أو إرسالها أو إبلاغها أو استقبالها كلياً أو جزئياً بوسيلة إلكترونية، على وسيط ملموس أو على أي وسيط إلكتروني آخر، وتكون قابلة للاسترجاع بشكل يمكن فهمه(٣١). من الملاحظ أن المشرع الكويتي لم يفرق بين السجل والمستند فكلاهما يحمل نفس الخصائص تقريباً، إلا أن هناك تفسيراً واسعاً وآخر ضيقاً للمستند الإلكتروني. **فأما من يرى بفكرة التفسير الواسع للمستند** يحتجون بأن "المستند" يمكن أن يمتد ليشمل المستند الورقي والإلكتروني، ذلك أن الأصل اللغوي يشمل الكتابة على الورق والكتابة الإلكترونية، وأي وسيلة تحديد هوية الموقع تعتبر بمثابة توقيع طالما انصرفت إرادته الجازمة لتلك المعاملة(٣٢).

أما أنصار المذهب الضيق للمستند الإلكتروني: يرون أن النصوص الحالية وضعت لتنظيم ما يتعلق بالمستند الورقي، وبالتالي يجب صدور قانون للتعامل الإلكتروني، ومثالهم في ذلك بجريمة التزوير المرتبطة بوجود فكرة المحرر، ويترتب على انتفاء المحرر انتفاء الجريمة ذاتها.

ما هي الآثار المترتبة على المساواة التشريعية بين التعامل الإلكتروني والمستند الورقي:

أ – من حيث القوة القانونية تقع جميع التصرفات في التعامل الإلكتروني صحيحة ولا يجوز أن تجحد حجية ما يتضمنه المستند الإلكتروني من تصرفات طالما تمت وفق الشروط التي نص عليها القانون.

ب – ولا يجوز الدفع بعدم نفاذ التعامل الإلكتروني لأن إنشاءه أو صياغته أو التوقيع عليه كان باستخدام وسائل أو شكل إلكتروني.

---

(٣١) المادة رقم (١) من قانون رقم ٢٠ لسنة ٢٠١٤ في شأن المعاملات الإلكترونية.

(٣٢) أشرف توفيق شمس الدين، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، منظم المؤتمر: أكاديمية شرطة دبي، مركز البحوث والدراسات رقم العدد: ١ السنة: ٢٠٠٣ تاريخ الانعقاد: ٢٦ نيسان ٢٠٠٣ تاريخ الإنهاء: ٢٨ نيسان ٢٠٠٣ الدولة: دبي – الإمارات العربية المتحدة.

ثانياً – الإثبات في التعامل الإلكتروني:

يخضع الإثبات في التعامل الإلكتروني أمام المحاكم للقواعد العامة في الإثبات المقررة في التجاري والمدني، وقد تطلب تحقيق المساواة بين المستند الإلكتروني والورقي تعديل التشريعات السارية على نحو يجيز إمكانية قبول المستند الإلكتروني كدليل أمام القضاء إذا توافرت فيه الشروط التي تطلبها المشرع.

الإثبات: يمكن تعريفه بأنه "تقرير نسبة جريمة إلى شخص، باللجوء إلى إحدى البيانات التي يقبلها القانون"(٣٣). فلا بد أن يصل القاضي إلى اليقين المطلق قبل الحكم، لأن أي شك في القانون أو في الوقائع يفسر لمصلحة المتهم، وبالتالي يحول دون عقابه. إن الإثبات يتم من خلال الوسائل والظروف التي يمكن اللجوء إليها مثل القرائن، والكتابة، وشهادة الشهود، الإقرار، واليمن. ويسري في الإثبات أحكام القانون القائم وقت حدوث الوقائع والتصرفات المراد إثباتها.

فلو حصل تصرف يجيز القانون إثباته بشهادة الشهود ثم صدر قانون جديد لا يجيز إثبات هذا التصرف بالشهادة، فإن التصرف هنا يمكن إثباته بشهادة الشهود وفقا للقانون المطبق وقت حدوث الواقعة(٣٤).وهو ما أكدته محكمة التمييز إنه من المقرر أن إثبات التصرفات القانونية يخضع في الأصل لقواعد الإثبات وفقا للقانون الذي كان سارياً وقت نشوء الواقعة محل الإثبات أو إبرام التصرف المراد إثباته.

عبء الإثبات:

يقع عبء الإثبات على المدعي، فالأصل براءة الذمة، فكل من يخالف البراءة عليه تقديم الدليل على التهمة التي ينسبها إلى المتهم، وفي حال عجزه وجب على القاضي أن يعلن البراءة(٣٥).

وقد خلق الواقع التكنولوجي العديد من التحديات منها إقناع الفرد الذي يتعامل مع الدولة أو الشركات أن التعامل الإلكتروني آمن ومحل ثقة ويحظى بالسرية. والأمر الآخر مواكبة التشريعات القانونية لهذا التطور حتى لا يفلت الجاني من العقاب، فزمن

(٣٣) عبد الوهاب حومد، الوسيط في الإجراءات الجزائية الكويتية (الكويت: جامعة الكويت، الطبعة الرابعة) ص١٧٦.

(٣٤) محكمة التمييز، طعن رقم ١٣، لسنة ١٩٨٠ تجاري، مجلة القضاء، ص٤٤٣.

(٣٥) عبد الوهاب حومد: مرجع سابق، ص١٨٥.

الإثبات في الكتابة قد أصبح قديماً خصوصاً في ظل المناداة بالحكومة الإلكترونية والتجارة الإلكترونية وغيرها(٣٦).

وغني عن البيان أن هناك تصرفات أباح المشرع حرية الإثبات فيها، وأخرى اشترط الكتابة لإثباتها إذا تجاوزت مبلغاً معيناً، وتصرفات اشترط لإثباتها وجوب الكتابة دون النظر إلى قيمتها، مثل العقود الخاصة بالصلح والكفالة وعقد العمل(٣٧). والواقع إن مفهوم الكتابة يؤخذ بالمعنى الواسع والشامل، فالرسائل والمذكرات وكشوفات الحسابات البنكية تؤخذ في عين الاعتبار(٣٨).

إن القانون الفرنسي قد ذهب إلى ما هو أبعد من ذلك فهو يثبت الكتابة لاعتراف الشخص وحضوره في التحقيق، أو قد يكون من خلال موقف سلبي للخصم أثناء الخصومة(٣٩). ويشترط أن تكون الكتابة صادرة من الخصم الذي يحتج عليه فيها ويحدد مصدرها وموقع عليها أو يمكن أن يستدل أنها بخط يده، وللقاضي حرية تقدير هذا الدليل كإثبات.

أ – أهم معوقات الإثبات لجرائم المعلومات أو التعامل الإلكتروني:

إن الإثبات في جرائم المعلومات أو التعامل الإلكتروني ليس بالأمر اليسير، لأن الجريمة في التعامل الإلكتروني تنصب على البيانات والمعلومات المخزنة في نظم المعلومات، وبالتالي يصعب الحصول على آثار مادية لإثبات الجريمة المعلوماتية، فلا توجد أعمال العنف أو تكسير على أجهزة الكومبيوتر، وعلى العكس في الجرائم العادية؛ لذا من أهم معوقات الإثبات لجرائم المعلومات أو التعامل الإلكتروني الآتي:

أولاً – انعدام الدليل المرئي: إن معظم البيانات التي يتم التلاعب فيها أو مسحها قد لا تشير بالضرورة إلى شخصية مرتكب هذه الأفعال، لأن المجرم بمجرد فكه لشفرة الدخول صار بإمكانه العمل كيفما يشاء، فانعدام الصلة بين المجرم والجريمة يحول دون معرفة شخصية المجرم(٤٠).

---

(٣٦) ثروت عبد الحميد، التوقيع الإلكتروني ماهيته، مخاطره، وكيفية مواجهتها، ومدى حجيته في الإثبات (دار الجامعة الجديدة، ٢٠٠٧)، ص٦.

(٣٧) ثروت عبد الحميد: مرجع سابق، ص١٢٥.

(٣٨) ثروت عبد الحميد: مرجع سابق، ص١٢٩.

(٣٩) القانون الفرنسي الصادر في ٩ يوليو ١٩٧٥، المادة ٣/١٣٧٤ مدني فرنسي.

(٤٠) الشحات إبراهيم محمد منصور، الجرائم الإلكترونية في الشريعة الإسلامية والقوانين الوضعية بحث فقهي مقارن (الإسكندرية: دار الفكر الجامعي، ٢٠١١)، ص١٩١.

ثانياً – سهولة محو الدليل بفترة وجيزة: قد يستغل الجاني قدراته بمحو جميع الأدلة والآثار التي تشير إلى دخوله خلال فترة زمنية قصيرة يصعب اكتشافها وتعقبها[٤١].

ثالثاً – صعوبة الوصول إلى الدليل[٤٢]: بمجرد فك المجرم للشفرة قد يضع هو شفرته الخاصة والمعقدة على النظام وبالتالي يصعب الوصول إليها إلا من خلال أشخاص لهم مثل قدراته وإمكاناته، أو أفضل منه من الناحية التكنولوجية.

رابعاً – مكان ارتكاب الجريمة[٤٣]: لا تقف جرائم المعلومات عند حدود الدول فهي تمتد إقليمياً مما يضاعف صعوبة اكتشافها لأن القوانين متفاوتة بين الدول، وكذلك الاتفاقيات الدولية لا تلزم الدول غير الموقعة عليها، وهذا ما يعزز فرصة إفلات الجناة من العقاب[٤٤].

ب – الآثار القانونية لعدم تقرير الإثبات في التعامل الإلكتروني:

هناك العديد من المشكلات القانونية التي تظهر بشأن التعامل الإلكتروني، ومنها ما يتعلق بالإثبات المدني والتجاري، ومنها التصرفات التي يتطلب الشارع عدم جواز إثباتها إلا كتابة إذا تجاوزت مبلغاً معيناً. وبالتالي إن التعامل الإلكتروني الذي يتجاوز القيمة المحددة لن يؤدي بالطبع إلى قبول هذا المستند في إثبات التصرف.

وحيث إن القانون الجنائي في إثبات جريمة خيانة الأمانة يشترط وجود العقد، وفي حال نفي الجاني وجود هذا العقد فلا بد من إثبات وجوده كتابة في حال إذا كان قد تجاوزت قيمته المبلغ الذي لم يجز الشارع إثباته إلا كتابة[٤٥].

ومن وجه نظرنا نستغرب وضع الاستثناء في المادة رقم (٢) من القانون رقم ٢٠/٢٠١٤ بشأن التعامل الإلكتروني[٤٦] الفقرة – د – "أي مستند يستلزم القانون

---

(٤١) الشحات إبراهيم محمد منصور: مرجع سابق، ص١٩٢.

(٤٢) الشحات إبراهيم محمد منصور: مرجع سابق، ص١٩٢.

(٤٣) الشحات إبراهيم محمد منصور: مرجع سابق، ص١٩٣.

(٤٤) غالباً ما يكون مركز عمليات القرصنة دول نامية أو حكومات غير مستقرة، وبالتالي يسهل عليهم مزاولة نشاطهم الإجرامي بعيداً عن القانون.

(٤٥) أشرف توفيق شمس الدين، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، منظم المؤتمر: أكاديمية شرطة دبي، مركز البحوث والدراسات رقم العدد: ١ السنة: ٢٠٠٣ تاريخ الانعقاد: ٢٦ نيسان ٢٠٠٣ تاريخ الإنهاء: ٢٨ نيسان ٢٠٠٣ الدولة: دبي – الإمارات العربية المتحدة.

(٤٦) المادة رقم(٢) من قانون رقم ٢٠ لسنة ٢٠١٤ في شأن المعاملات الإلكترونية "تسري أحكام هذا القانون على السجلات والرسائل والمعلومات والمستندات والتوقيعات الإلكترونية =

إفراغه في محرر رسمي أو توثيقه، أو ورد في تنظيمه نص خاص في قانون آخر".

وهنا يجب أن نفرق بين أمرين وجود العقد إلكترونيا من خلال الإيجاب والقبول، وبين إثباته، فالعقد ينعقد بمجرد توافر أركانه، أما إثباته فهو أمر آخر يخضع إلى القوانين التي تنظم عملية الإثبات فيه، كما أن هناك العديد من الحالات التي تستثنى من قاعدة الإثبات في الكتابة.

ج – المطلب الثالث
التمييز بين الاعتداء على النظام والاعتداء على المستند الإلكتروني

إن الحماية الجنائية في مجال التعامل الإلكتروني تعزز الثقة بين الأفراد، وبالتالي يزداد عدد التعاملات الإدارية والتجارية وغيرها، إلا أن الزيادة الهائلة والمطردة في التعامل الإلكتروني حول العالم كانت دافعاً أساسياً إلى وضع تشريعات قانونيه تعزز ثقة الأفراد في هذه التعاملات. وقد صرحت منظمة الأونكتاد أن التجارة الإلكترونية نمت بشكل هائل(٤٧). لذلك بات من الضروري الاستعانة بسلاح التجريم والعقاب في التعامل الإلكتروني؛ لأن الطريق الجنائي أكثر فعالية لما فيه من الإكراه والجبر(٤٨). وهو لا يتعارض مع طريق نشر الوعي والثقافة.

الثقة العامة في مجال المعاملات الإلكترونية: هي تلك الثقة التي يضعها المجتمع، في مختلف المظاهر الضرورية لاستقرار العلاقات والروابط الاجتماعية(٤٩). فتعد الثقة الضمان القانوني اللازم لاستقرار التعامل الإلكتروني. كما أن القانون رقم ٢٠/ ٢٠١٤

= ذات العلاقة بالمعاملات المدنية والتجارية والإدارية، وعلى كل نزاع ينشأ عن استخدامها مالم يتفق الأطراف على غير ذلك أو يتبين أن قانوناً آخر هو الواجب التطبيق.

ولا تسري أحكام هذا القانون على ما يأتي:

أ – المعاملات والمسائل المتعلقة بالأحوال الشخصية والوقف والوصية.

ب – سندات ملكية الأموال العقارية وما ينشأ عنها من حقوق عينية أصلية أو تبعية.

ج – السندات الإذنية والكمبيالات القابلة للتداول.

د – أي مستند يستلزم القانون إفراغه في محرر رسمي أو توثيقه، أو ورد في تنظيمه نص خاص في قانون آخر".

(٤٧) الأونكتاد: هيئة حكومية دائمة أنشئت عام ١٩٦٤ تبع الأمم المتحدة من خلال إحصائيات موقعها الرسمي http://unctad.org/en/Pages/Home.aspx

(٤٨) حازم حسن أحمد متولي، الحماية الجنائية للثقة العامة في المعاملات التجارية الإلكترونية في التشريع الإماراتي، مجلة الفكر الشرطي، المجلد رقم ٢٣العدد رقم ٩١ اكتوبر ٢٠١٤، ص٤٨.

(٤٩) Rigaux(M) et Trouss (P.E): Les Crimes et les delits du code penal.T2.Bruxelles-Paris1952.p.455.

بشأن التعامل الإلكتروني يهدف إلى حماية قيمة ومضمون فكرة الثقة كأساس ضروري وحتمي لاستقرار واستقامة ونمو العناصر الإيجابية. وعند إمعان النظر في منطق السياسة الجنائية للمشرع الكويتي نرى أن نية المشرع تتجه دائما إلى إحاطة مظاهر الثقة بكثير من الضمانات القانونية.

قد تتداخل الحماية للمستند الإلكتروني مع حماية نظم تشغيل الحاسب الآلي، لأن محل الإعداء في الحالتين ينصب على البيانات التي يحتويها المستند أو نظام التشغيل. هو الذي جعل بعض الفقهاء يرون بأن البيانات المدخلة إلكترونياً لا تنفصل عن البرامج التي تنظمها، فمن حيث طبيعة البيانات المدخلة إلكترونياً والبرامج يمكن باعتبارهما كياناً معنوياً، وأن حماية هذه البرامج تعد في الوقت ذاته حماية للبيانات المعالجة إلكترونياً، وقد أخذ بهذا الرأي المشرع الكويتي عندما نص في المادة (٣٧) من القانون رقم ٢٠/٢٠١٤ بشأن التعامل الإلكتروني(٥٠).

ونحن نرى أن هذا الرأي محل نظر، لأن مصلحة حماية نظام التشغيل تختلف عن مصلحة حماية المستند التي لها أهمية في الإثبات، ومن المتصور أن يتم المساس بأحد المصلحتين دون الأخرى، فيمكن أن ينصب التزوير على مستند إلكتروني دون أن يمتد الفعل إلى تعطيل أو إتلاف نظام التشغيل، وعلى العكس يمكن أن يمس الجاني النظام دون أن يزور المستند الإلكتروني.

---

(٥٠) المادة رقم (٣٧) من قانون رقم ٢٠/٢٠١٤ بشأن التعامل الإلكتروني "مع عدم الإخلال بأي عقوبة أشد منصوص عليها في قانون آخر يعاقب بالحبس لمدة لا تزيد على ثلاث سنوات وبغرامة لا تقل عن خمسة آلاف دينار ولا تزيد على عشرين ألف دينار أو بإحدى هاتين العقوبتين كل من:

أ – تعمد الدخول بغير وجه حق إلى نظام المعالجة الإلكترونية أو عطل الوصول إلى هذا النظام أو تسبب في إتلافه أو حصل على أرقام أو بيانات بطاقات ائتمانية أو غيرها من البطاقات الإلكترونية لاستخدامها للحصول على أموال الغير.

ب – أصدر شهادة تصديق إلكترونية أو زاول أي من خدمات التصديق الإلكتروني دون الحصول على ترخيص بذلك من الجهة المختصة.

ج – أتلف أو عيب توقيعاً أو نظاماً أو أداة توقيع أو مستنداً أو سجلاً إلكترونياً أو زور شيئاً من ذلك بطريق الاصطناع أو التعديل أو التحويل بأي طريقة أخرى.

د – استعمل توقيعاً أو نظاماً أو أداة توقيع أو مستنداً أو سجلاً إلكترونياً معيباً أو مزوراً مع علمه بذلك.

هـ – توصل بأية وسيلة – بغير حق – على توقيع أو نظام أو مستند أو سجل إلكتروني أو اختراق هذا النظام أو اعترضه أو عطله عن أداء وظيفته".

وهنا يقوم القاضي بتوقيع عقوبة الجريمة الأشد، غير أن ذلك لا ينفي التعدد في هذه الحالة[٥١]. لذلك نحن نرى أنه من الأولى إفراد عقوبة مختلفة لكل فعل وليس النص عليهما في مادة واحدة. كما أن المشرع الفرنسي فرق بين تلك الأفعال التي تنصب على إفساد نظام التشغيل في المادة ١-٣٢٣، والأفعال الأخرى التي تقع على إتلاف المعلومات أو محوها باستعمال الخداع في المواد ٢-٢٣٢[٥٢].

أنواع المساس بالخصوصية للتعامل الإلكتروني:

اختلفت الآراء حول طبيعة التعامل مع المستند الإلكتروني فهل تكفيه الحماية المقررة للمنقولات أم أن له طبيعة خاصة، فجانب من الفقهاء يرون بأنه يمكن تطبيق الحماية المقررة للمنقولات للمستند الإلكتروني لأنه يعد مالاً معنوياً، وذلك لأن العبرة بتفسير النص تكون من خلال الوقوف على المصلحة التي رآها المشرع وأراد حمايتها وليس التفسير الحرفي للنص.

وذهب الرأي الآخر إلى أن المنقولات لا يمكن إلا أن تكون شيئاً مادياً يخرج عن مدلوله المعلومات المخزنة، وهو ما حدا بالتشريعات إلى إفراد نصوص خاصة تجرم المساس بالبيانات الإلكترونية الخاصة بالأفراد والشركات والدولة دون وجه حق.

أولاً - الجرائم الإلكترونية وجرائم المعلومات:

حرصت التشريعات على وضع تعريف لجرائم[٥٣] المعلومات، وقد فرق بعض الفقهاء بين جريمة المعلومات والجريمة الإلكترونية، ونحن نرى أن التفريق بينهما لا محل له طالما تم الأخذ بالمفهوم الواسع لجرائم المعلومات، فهي مؤسسة على حماية المصلحة العامة التي يحميها القانون كالحق في السرية والخصوصية، إلا أن الخلاف كان بشأن توسيع مفهوم الجريمة الإلكترونية أو تضييقه.

ويمكن تعريف الجرائم الإلكترونية: هي كل أفعال الدخول غير المشروع على

---

(٥١) أشرف توفيق شمس الدين، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، منظم المؤتمر: أكاديمية شرطة دبي، مركز البحوث والدراسات رقم العدد: ١ السنة: ٢٠٠٣ تاريخ الانعقاد: ٢٦ نيسان ٢٠٠٣ تاريخ الإنهاء: ٢٨ نيسان ٢٠٠٣ الدولة: دبي - الإمارات العربية المتحدة.

(٥٢) يجرم المشرع الفرنسي صور الاعتداء الناجمة عن المعالجة الآلية للبيانات والتي تنطبق بلا شك على صور الاعتداء على شبكة الإنترنت، حيث أصدر نصوصاً قانونية عدة تكفل الحماية الجنائية.

(٥٣) تعرف الجريمة: "فعل أو امتناع عن فعل يحظره القانون ويقرر عقوبة لمرتكبه".

أجهزة الحاسب الآلي أو الشبكة بقصد الإضرار بها أو بواسطتها[٥٤]. وتكمن خطورة الجريمة المعلوماتية في أنها متسعة النطاق الجغرافي وعابرة للحدود وهو ما يزيد من صعوبة اكتشافها، فهي إن صح التعبير جرائم عابرة للقارات.

كما أن جرائم المعلومات ثير النزاع حول الاختصاص والقانون الواجب التطبيق، ولا يمكن التنبؤ بعدد الأشخاص المتضررين وغالباً ما يتم التغاضي عن الإبلاغ عنها خشية التشهير، فهناك فجوة كبير بين العدد الحقيقي لهذه الجرائم والعدد الذي يتم الإبلاغ عنه[٥٥]، ويصعب تحديد الخسائر المالية فيها، وفي بعض الحالات تخشى الحكومات الإفصاح عن الخسائر المالية الحقيقة الناتجة عن الجرائم الإلكترونية خوفاً من أن تثور عليها شعوبها.

ثانياً – الاعتداء على النظام:

وفقاً لاتفاقية بودابست المؤرخة في ٢٣ نوفمبر ٢٠٠١[٥٦] فإن الغرض من تجريم الأفعال المتعلقة بسرية البيانات هو حماية نظام التشغيل، وبالتالي يدخل في نطاق التجريم جريمة الولوج أو البقاء غير المشروع، وجريمة إفشاء الأسرار المعلوماتية والاعتراض غير القانوني لانتقال البيانات.

أ – البقاء غير المشروع:

إن علة التجريم هي الحفاظ على سلامة النظام وحمايته، وبالتالي فإن الولوج أو البقاء غير المشروع يعتبر سطواً أو قرصنة[٥٧]. وكما يعتبر عملاً لا يتفق مع القوانين والاتفاقيات الدولية[٥٨]. لذلك هناك شروط مفترضة لهذه الجريمة. الأول وجود نظام معالجة البيانات، والثاني شمول هذا النظام بالحماية، والثالث الولوج أو البقاء بدون وجه حق.

ب – الدخول غير المشروع:

يقصد بالولوج: "الاختراق غير المشروع الذي يحدث من قبل الغير للنظام

---

(٥٤) محمد الأمين البشرى: مرجع سابق، ص٢٤٣.

(٥٥) خالد إبراهيم: مرجع سابق، ص٥١.

(٥٦) Convention on Cybercrime, Budapest, 23.XI.2001.

(٥٧) ما تعرضت له وزارة الدفاع الأمريكية من قرصنة من قبل مراهق برازيلي تجول في أنظمة التشغيل الخاصة بها.

(٥٨) بلال أمين زين الدين: مرجع سابق، ص٢٦١.

المعلوماتي بأكمله أو بجزء منه"[٥٩] كما يشترط بالدخول غير المشروع أن يكون من شخص غير مصرح له وبدون رضا أو إذن من مالك النظام، ويفرق بعض الفقهاء بين فعل الدخول غير المشروع الذي يتسم بالوقتية، وجريمة البقاء غير المشروع التي تعتبر جريمة مستمرة لها طابع الاستمرارية، فكلا الجريمتين لهما طابع العمدية ويتوافر فيهما القصد الجنائي (العلم والإرادة)[٦٠].

ونحن نرى أن المجرم الإلكتروني شخص غالباً ما يكون ذكياً وملماً بعلوم الكومبيوتر؛ لذا يجب التعامل معه بحذر وبصورة توازي إمكانياته، لأنه ببساطة قد يخدع الجميع. فالأولى احتواؤه واستغلال مهاراته، وألا تكون عقوبته تقليدية مثل (السجن–الغرامة) بل تكون بتجنيده للعمل لصالح الدولة واستغلاله لحماية أنظمتها وسلامتها الإلكترونية.

ثالثاً – الاعتداء على مكونات النظام: الأفعال التي تقع على طبيعة المستند الإلكتروني:

هناك فروق مهمة بين المستند الإلكتروني والمستند الورقي من حيث المساس بمحتوى كل منهما، فالمساس بمحتوى المستند الإلكتروني وتغييره قد يتم في أي وقت ولا يتسنى كشفه أو الوقوف عليه أو يصعب إقامة الدليل على وقوعه.

ومن ناحية ثانية فإن عدداً كبيراً من الأشخاص الذين يجوز لهم الاطلاع على المستندات الإلكترونية والتعامل معها، وهو ما يفوق بكثير عدد المتعاملين في المستندات الورقية. وأخيراً فإن المساس بمحتوى المستند الإلكتروني يبدو أكثر سهولة من المساس بالمستند العادي. فعلى سبيل المثال فإن تزوير التوقيع على المستند الورقي يترك أثراً في كثير من الأحوال يدل عليه، بخلاف التزوير المنصب على التوقيع الإلكتروني الذي يتألف من شفرة تحدد هوية الموقع، وهذه الشفرة يمكن التدخل فيها أو محوها، وتزويرها قد يكون أسهل من التوقيع الكتابي، كما أن اكتشاف التزوير والوقوف على مرتكب الجريمة قد يصعب في كثير من الأحيان.

أ – أهمية تجريم التزوير في المستند الإلكتروني:

إن المشرع الكويتي في القانون رقم ٢٠ لسنة ٢٠١٤ بشأن المعاملات الإلكترونية تنبه إلى ضرورة تجريم أفعال التزوير التي قد تقع على المستند الإلكتروني وذلك بهدف حمايته وإعطاء الثقة والأمان لكل من يتعامل إلكترونياً.

(٥٩) بلال أمين زين الدين: مرجع سابق، ص٢٧١.

(٦٠) بلال أمين زين الدين: مرجع سابق، ص٢٧٧.

ب – تزوير المستند الإلكتروني:

يمكن تعريف التزوير: كل تغيير للحقيقة بقصد الغش(٦١). وقد جرم قانون الجزاء الكويتي التزوير(٦٢) من خلال المواد (٢٥٧-٢٦٢) وقسمها إلى تزوير في محرر رسمي ومحرر عرفي، وتشدد في العقوبة إذا كان محل التزوير محرراً رسمياً.

كما أن الجريمة تتحقق من خلال الركن المادي المتمثل بكل ما يعد تغييراً للحقيقة، أما الركن المعنوي فهو العلم والإرادة، ويضاف إلى ذلك الشروط المفترضة وهي وجود محرر وهو ورقه تحمل تعبيراً منسوباً لشخص منافي للحقيقة ممكن أن يثبت علاقة قانونية تحظى باعتراف القانون، والشرط الآخر المفترض هو أن ينصب التغيير على بيان جوهري أي أمر له قيمة في إثبات الحق بمعنى أي بيان يعتد به مثل تغيير تاريخ الجواز(٦٣).

إن التزوير في التعامل الإلكتروني يمثل صورة لا تقل أهمية عن التزوير في المستندات الورقية، وتتمثل هذه الأهمية من خلال نص المادة (٣) من قانون رقم ٢٠/٢٠١٤ "..... والمستند الإلكتروني والرسالة الإلكترونية والمعاملة الإلكترونية والتوقيع الإلكتروني في مجال المعاملات المدنية والتجارية والإدارية منتج لذات الآثار القانونية المترتبة على الوثائق والمستندات والتوقيعات الكتابية من حيث إلزامه لأطرافه أو قوته في الإثبات أو حجيته متي أجري وفقاً لأحكام هذا القانون".

فهنا المشرع الكويتي أعطى حجية للمستند الإلكتروني أو التعامل الإلكتروني

---

(٦١) فايز عايد الظفيري، قانون الجزاء الخاص (الكويت: وزارة الداخلية الإدارة العامة للتدريب) ص٤٥.

(٦٢) المادة رقم (٢٥٧) "يعد تزويراً كل تغيير للحقيقة في محرر بقصد استعماله على نحو يوهم بأنه مطابق للحقيقة، إذا كان المحرر بعد تغييره صالحاً لأن يستعمل على هذا النحو، ويقع التزوير إذا اصطنع الفاعل محرراً ونسبه إلى شخص لم يصدر منه، أو أدخل تغييراً على محرر موجود سواء بحذف بعض ألفاظه أو بإضافة ألفاظ لم تكن موجودة أو بتغيير بعض الألفاظ، أو وضع إمضاء أو خاتم أو بصمة شخص آخر عليه دون تفويض من هذا الشخص، أو حمل ذلك الشخص عن طريق التدليس على وضع إمضائه أو خاتمه أو بصمته على المحرر دون علم بمحتوياته أو دون رضاء صحيح بها. ويقع التزوير أيضاً إذا غير الشخص المكلف بكتابة المحرر معناه أثناء تحريره بإثباته فيه واقعة غير صحيحة على أنها واقعة صحيحة، ويقع التزوير من استغل حسن نية المكلف بكتابة المحرر فأملى عليه بيانات كاذبة موهماً أنها بيانات صحيحة".

(٦٣) فايز عايد الظفيري: مرجع سابق، ص٥٢.

بشكل عام، وساوى بين التعامل الإلكتروني إذا تم بالشروط المنصوص عليها قانوناً وبين التعامل في المحرر الرسمي، إلا إنه وفي المادة (٣٧) من ذات القانون الفقرة "ج –.... سجلاً إلكترونياً أو زور شيئاً من ذلك بطريق الاصطناع أو التعديل أو التحويل بأي طريقة أخرى".

وفي هذه الحالة عاقب المشرع بالحبس مدة لا تجاوز ثلاث سنوات واعتبرها جنحة، مع إن عقوبة التزوير في المحرر الرسمي تعد جناية(٦٤). كما في المادة رقم (٢٥٩) من قانون الجزاء الكويتي.

وهنا يظهر التناقض في القانون رقم ٢٠١٤/٢٠ بشأن المعاملات الإلكترونية حيث إن التزوير في محرر رسمي جناية تصل إلى – سبع سنوات – سجن، والتزوير في محرر رسمي إلكتروني جنحه. ونحن نرى أن المحررات الرسمية والعرفية صار لها الشكل الإلكتروني، فأي تغيير في محتواها يعتبر تزويراً، فكان من الأولى بالمشرع التشديد في العقوبة إذا وقع التزوير على مستند إلكتروني رسمي لا أن يعدها جنحة، أو على الأقل المساواة في العقوبة بين التزوير في محرر رسمي والمستند الإلكتروني.

والأغرب في القانون الجديد ٢٠١٤/٢٠ بشأن المعاملات الإلكترونية ما ورد في المادة (٣٨)" يعاقب بالحبس مدة لا تزيد على سنة والغرامة التي لا تقل عن ثلاثة آلاف دينار ولا تزيد على عشرة آلاف دينار، أو بإحدى هاتين العقوبتين كل من رخص له بإصدار خدمات التصديق الإلكترونية إذا قام بتقديم بيانات غير صحيحة في طلب التسجيل الذي يقدم إلى الجهة المختصة أو خالف شروط الترخيص".

فهنا صارت عقوبة الجهة المرخص لها بالتصديق أقل من ناحية الغرامة أو الحبس، فكيف يخفف المشرع العقوبة عمن يقدم بيانات خاطئة وهي جهة يفترض أن تكون مؤتمنة على تقديم خدمات التصديق الإلكتروني، أو تخالف شروط الترخيص فهي في الحالة الأولى قد تقع في التزوير – إذا قدمت بيانات خاطئة – وفي الحالة

(٦٤) المادة رقم ٢٥٩ إذا ارتكب التزوير في محرر رسمي أو في ورقة من أوراق البنوك، كانت العقوبة الحبس مدة لا تجاوز سبع سنوات، ويجوز أن تضاف إليها غرامة لا تجاوز سبعة آلاف دينار، وإذا ارتكب التزوير في المحرر الرسمي من الموظف المكلف بإثبات البيانات التي غيرت الحقيقة فيها، كانت العقوبة الحبس مدة لا تجاوز عشر سنوات، ويجوز أن تضاف إليها غرامة لا تجاوز عشرة آلاف دينار.

الثانية قد تتعرض لإلغاء الترخيص، كما ورد في المادة (١٩)[٦٥] من اللائحة التنفيذية من قانون رقم ٢٠ لسنة ٢٠١٤ في شأن المعاملات الإلكترونية.

ونحن نرى أن التخفيف للعقوبة الواردة في المادة (٣٨) من قانون رقم ٢٠ لسنة ٢٠١٤ في المعاملات الإلكترونية لا محل له، بل من باب أولى زيادة الغرامة أو تغليظ العقوبة على هذه الجهات لأنها مؤتمنة.

ت – إتلاف المستند الإلكتروني:

يمكن حماية المستند الإلكتروني من الأفعال التي تعتبر إتلافاً له بصورة غير مباشرة من خلال تجريم الأفعال التي تؤدي إلى إتلاف نظام التشغيل الذي يحتوي على المستند الإلكتروني، والثانية من خلال إتلاف بيانات المستند الإلكتروني نفسه.

د – المطلب الرابع
عناصر الجريمة في المستند الإلكتروني

إن الركن المادي في الجريمة الإلكترونية يتكون من السلوك المجرَم والنتيجة وعلاقة السببية، كما يمكن أن يتحقق الركن المادي دون النتيجة مثل الإبلاغ عن جريمة قبل تمام وقوعها، كمن يجمع معلومات سرية دون وجه حق ويحملها على موقعه الخاص استعدادا لنشرها، فعلى الرغم من عدم تحقق النتيجة – التشهير – إلا أنه لا مناص من معاقبة المجرم عن سوء سلوكه، ويمكن تقسيم عناصر الجريمة في المستند الإلكتروني إلى الآتي:

١ – **الجاني:** "هو من يتصل بجهاز كمبيوتر مشمول بالحماية بدون أن يكون مأذوناً له

(٦٥) مادة (١٩) من اللائحة التنفيذية من قانون رقم ٢٠ لسنة ٢٠١٤ في شأن المعاملات الإلكترونية "للجهة المختصة إلغاء ترخيص مزود خدمات التصديق أو عدم التجديد له في الحالات التالية:
١ – إذا تبين للجهة المختصة أن مزود خدمات التصديق مستمر في الاخلال أو القصور في أعماله، وتم إيقافه مؤقتاً بناء على المادة (١٨) من هذه اللائحة ولم يتخذ الإجراءات المطلوبة لتلافي القصور أو الإخلال خلال المدة الزمنية المحددة له.
٢ – إذا تكررت حالات الإيقاف المؤقت.
٣ – إذا تكررت الشكاوى وثبتت صحتها بشكل ملحوظ.
٤ – إذا صدرت ضده عقوبة وفقاً لأحكام المادتين ٣٧و٣٨ من القانون.
٥ – إذا ثبت في حقه خطأ نتج عنه ضرر بذوي الشأن أو بالمصلحة العامة".

بذلك"[٦٦] ويمكن أن ترتكب من قبل أي شخص سواء أكانت له صفة أم لا، ويخرج عن هذا التجريم من لهم سلطة الإشراف على النظام والحماية طالما التزموا بالشروط المقررة قانونا[٦٧].

٢ - **الدخول غير المشروع:** بمجرد الدخول غير المشروع تتم الجريمة، ولم تحدد التشريعات الوسيلة في ذلك الدخول، فقد يكون الدخول غير المشروع باستعمال كلمه السر الخاصة بزميله في العمل[٦٨] أو محاولته كسر شفرة النظام، ويعد بعض الفقهاء الدخول غير المشروع جريمة وقتية، وذلك بفرض أن الدخول مصرح به لأناس خاصين وغير متاح للجمهور، ولا فرق في الدخول غير المشروع أن يتم على قواعد البيانات كلها أو جزء من نظام التشغيل.

٣ - **البقاء غير المشروع:** فهو دخول قد تم بصورة مشروعة لكن المستخدم تجاوز صلاحياته أو استمر في بقائه داخل النظام أكثر من الفترة المصرح له فيها، ويعتبر البعض البقاء غير المشروع جريمة مستمرة، ونحن نرى أنه من اللازم أن يكون الدخول بطريق الخداع، حتى ننفي احتمالية الخطأ وبالتالي يكون دخوله غير مشروع.

٤ - **استعمال الطرق الخداعية:** يفسر "الخداع" تفسيراً واسعاً، فيكفي أن يتحقق دون أن يكون الجاني مأذوناً له به، متى كان القصد الجنائي متوافراً لديه، وقد فسر القضاء الفرنسي تعبير "الدخول بطريق الخداع"[٦٩]. ويتوافر الخداع إذا تم فك الشفرة الخاصة بالدخول، ولا فرق إذا كان الدخول على النظام قد حدث بصورة مباشرة أو غير مباشرة.

تتوفر جريمة الاتصال غير المشروع ولو لم يترتب ضرر بالمجني عليه،

---

(٦٦) أشرف توفيق شمس الدين، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، منظم المؤتمر: أكاديمية شرطة دبي، مركز البحوث والدراسات رقم العدد: ١ السنة: ٢٠٠٣ تاريخ الانعقاد: ٢٦ نيسان ٢٠٠٣ تاريخ الإنهاء: ٢٨ نيسان ٢٠٠٣ الدولة: دبي – الإمارات العربية المتحدة.

(٦٧) تقوم وزارة الداخلية في دولة الكويت بمحاسبة جميع من يثبت عدم التزامه بالشروط المقررة للعمل على أنظمتها ومنها فقدان كلمة الدخول على النظام بشكل دائم أو الإيقاف الموقت، إضافة الى توقيع العقوبات الإدارية طالما أن المخالفة المرتكبة لم ترقَ إلى القانون الجنائي.

(٦٨) يتم محاسبة الطرفين إذا استعمل الموظف كلمة السر الخاصة بزميله.

(٦٩) التي نص عليها الشارع الفرنسي في المادة (٣٢٣-١) بأنها تشمل كل الوسائل غير المشروعة التي يتمكن بها الجاني من الدخول في نظام معالجة آلية للمعلومات.

فالتشريع الكويتي في القانون رقم ٢٠/٢٠١٤ بشأن التعامل الإلكتروني لم يتطلب لإتمام جريمة الدخول غير المشروع أن يحصل ضرر بالمجني عليه، فهي جريمة من جرائم السلوك المجرد التي لا تفترض تحقق نتيجة من أي نوع، فالحق في السرية يتم اختراقه بمجرد قيام الجاني بالاتصال غير المشروع(٧٠).

القصد الجنائي في التعامل الإلكتروني:

لم يحدد القانون الكويتي تعريفاً للجريمة وانتهج منهج أغلب التشريعات الأخرى، وقد أحسن صنعاً في ذلك فالجرائم دائماً متطورة، فالتعريف السائد في الفقه "إن الجريمة فعل أو امتناع يجرمه المشرع وينص على عقوبة لمرتكبه"(٧١) وهذا تعريف عام متعلق من حيث النظرة الموضوعية للفعل والنتيجة ويغفل الأمور الشخصية المتعلقة بالإرادة الآثمة.

أولاً – القصد الجنائي:

إن جريمة الدخول إلى النظام أو البقاء فيه هي جريمة عمدية، وبالتالي يتوفر لدى الجاني العلم والإرادة، وبالمقابل لا تتوافر هذه الجريمة إذا كان الدخول أو البقاء في النظام قد تم بطريق الصدفة أو الخطأ، ويمكن الكشف عن الدخول غير المشروع إذا حاول الجاني فك شفرة النظام أو حاول التجربة أكثر من مرة بكلمات السر المشفرة مع العلم أن الأنظمة الحديثة تسجل جميع البيانات للمستخدمين من أوقات الدخول وعدد المحاولات التي تم إدخال كلمه السر فيها بشكل خاطئ(٧٢).

كما أن الدخول غير المشروع قد يكون بحسن نية وأقرب مثال على ذلك انتهاء الاشتراك للمستخدم مع محاولته للدخول، وفي حال توافر القصد الجنائي فإنه لا عبرة بالبواعث، فيستوي أن يكون هذا الدخول قد تم بدافع الفضول أو القيام بأي عمل إجرامي غير مشروع.

---

(٧٠) أشرف توفيق شمس الدين، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، منظم المؤتمر: أكاديمية شرطة دبي، مركز البحوث والدراسات رقم العدد: ١ السنة: ٢٠٠٣ تاريخ الانعقاد: ٢٦ نيسان ٢٠٠٣ تاريخ الإنهاء: ٢٨ نيسان ٢٠٠٣ الدولة: دبي – الإمارات العربية المتحدة.

(٧١) سمير الشناوي، النظرية العامة للجريمة والعقوبة في قانون الجزاء الكويتي دراسة مقارنة، قانون العقوبات المصري والفرنسي والألماني والنرويجي، الكتاب الأول الجريمة (الكويت: وزارة الداخلية، كلية الشرطة، ١٩٨٨)، ص١٥٣.

(٧٢) كما تحرص بعض الحكومات التي تقدم خدمات إلكترونية للجمهور على حماية نظامها في حالة محاولة الدخول أكثر من ثلاث مرات بالرمز الخطأ بقفل النظام لمدة محددة حسب أهمية المعاملة.

إن عملية إثبات القصد الجنائي أثارت الجدل الفقهي حول ضرورة وجود نظام حماية للتعامل الإلكتروني حتى يتم تحديد سوء نية الجاني، وكذلك إن نظام الحماية هو الحد الفاصل بين ما هو مسموح بالاطلاع عليه من غيره، ولا عبرة بالبواعث على ارتكاب جرائم المعلومات فليس لها أي اعتبار في حكم القاضي.

وقد يكون الباعث اللهو أو الفضول وإثبات القدرة على التفوق أو التهديد(٧٣) أو إفشاء الأسرار(٧٤). ويعتبر موقع (ويكي ليكس) من أشهر المواقع الذي قدم وثائق سرية وفضح حكومات عديده بوثائق رسمية سرية منها استهداف الطائرات الأمريكية للمدنيين في العراق عام ٢٠٠٧، وذلك من خلال نشر الفيديو كاملاً للعملية العسكرية عبر الإنترنت(٧٥).

هـ – المطلب الخامس
الغرامة في القانون رقم٢٠/٢٠١٤

تعريف الغرامة: هي إلزام المحكوم عليه بدفع مبلغ من النقود يقدره الحكم القضائي إلى خزانة الدولة(٧٦). والغرامة في القانون المصري عقوبة أصلية أو عقوبة تكميلية، ولا تكون تبعية.

أنواع الغرامة:

١ – **الغرامة كعقوبة أصلية:** يقرر القانون الغرامة كعقوبة أصلية في المخالفات والجنح، فالغرامة في المخالفات هي العقوبة العادية، والغرامة في الجنح ذات أهمية كبيرة فقد يقررها القانون وحدها في جنح غير ذات أهمية كبيرة، وقد يقررها إلى جانب الحبس كعقوبة وجوبية أو جوازية، وقد يقررها مع الحبس على سبيل التخيير.

٢ – **الغرامة كعقوبة تكميلية:** يقرر الشارع الغرامة كعقوبة تكميلية إلى جانب عقوبة أصلية سالبة للحرية، وأكثر ما يفعل الشارع ذلك إنما يكون في الجنايات، وهو ينتقي لذلك في الغالب الجنايات التي يدفع إلى ارتكابها باعث الإثراء غير المشروع

(٧٣) غالبا ما يتم اختراق مواقع حكومية للدول إذا كانت في حالة حرب ويتم تهديدها بنشر رسائل التهديد على موقعها الإلكتروني.

(٧٤) بلال أمين زين الدين: مرجع سابق، ص٢٨١.

(٧٥) ويكي ليكس هي منظمة دولية غير ربحية تنشر تقارير وسائل الإعلام الخاصة والسرية من مصادر صحفية وتسريبات إخبارية مجهولة. بدأ موقعها على الإنترنت سنة ٢٠٠٦.

(٧٦) رمسيس بهنام، النظرية العامة للقانون الجنائي؛ (منشأة المعارف، الإسكندرية، الطبعة الثالثة، ١٩٩٧)، ص ٧٨٢.

٣ – **الغرامة المختلطة:** وهي التي تختلط فيها فكرة العقوبة مع فكرة التعويض، ويبدو ذلك في غرامة المصادر والغرامة النسبية، والغرامة الضريبية.

أ – غرامة المصادرة: يقصد بها: الغرامة التي يتعين الحكم بها بدلاً من الحكم بالمصادرة إذا لم تضبط المواد موضوع الجريمة لأي سبب كان، وقد نص قانون الجمارك وقانون الرقابة على النقد في مصر على هذا النوع من الغرامات.

ب – فالغرامة النسبية هي: الغرامة التي لا يحددها القانون بكيفية ثابتة بل يجعلها نسبية تتماشى مع الضرر الناتج من الجريمة أو الفائدة التي حققها الجاني أو حاول تحقيقها، وتتميز بحكم هام عن الغرامة العادية: مؤداه أنه إذا تعدد المتهمون بالجريمة المستوجبة للغرامة النسبية فاعلين كانوا أو شركاء فلا يحكم عليهم جميعاً إلا بغرامة واحدة تقاس بضرر الجريمة أو بفائدتها، أي وفقاً لضابط التناسب الذي حدده النص الخاص بهذه الجريمة ويلتزمون بها متضامنين، ولكن يجوز للقاضي إعفاؤهم من هذا التضامن.

ت – الغرامة الضريبية: تتحدد عادة بنسبة معينة مما لم يؤد من الضريبة، وقد ذهبت بعض الأحكام إلى اعتبار هذه الغرامة ذات طبيعة مختلطة أي تجمع بين صفتي العقوبة والتعويض، وذهبت بعض التشريعات إلى إطلاق لفظ التعويض على هذه الغرامة وهو ما لا يتفق مع تكيفها القانوني كعقوبة وإن خالطها معنى التعويض.

وتعتبر الغرامة عقوبة جنائية تتميز بخواص العقوبة، فالغرامة تعد شخصية ويصدر بها حكم قضائي، ويجب مراعاة درجة الإثم وجسامة الفعل وظروف الجاني الشخصية حتى تحقق هذه العقوبة الردع(٧٧). كما أن المادة (٦٤) في قانون الجزاء الكويتي عرفت الغرامة بأنها "إلزام المحكوم عليه بأن يدفع للدولة المبلغ الذي تقدره المحكمة طبقاً لنص القانون..."(٧٨).

---

(٧٧) محمد أبو شادي، مبادئ علم العقاب دراسة مقارنة لطبيعة العقوبة والتدبير الاحترازي وأساليب التنفيذ العقابي مع التطبيق لأحكام القانون رقم ٢٦ لسنة ١٩٦٢بتنظيم السجون في الكويت (الكويت: وزارة الداخلية أكاديمية سعد العبد الله للعلوم الأمنية، ١٩٩٣، ص١٧٣.

(٧٨) المادة رقم (٦٤) من قانون الجزاء الكويتي "العقوبة بالغرامة هي إلزام المحكوم عليه بأن =

فالغرامة تختلف عن التعويض المدني الذي يحكم للمضرور بتعويض عادل جابر للضرر الذي أصابه، وتختلف عن المصادرة التي تعني انتقال ملكية الشيء للدولة فور صدور الحكم(٧٩). وكما هو معلوم إن أحكام الغرامة لا تقبل الصلح أو التنازل. وتختلف بطبيعتها إذا كانت غرامة جنائية صادرة بحكم من محكمة الجنايات عنها إذا كانت غرامة مدنية صادرة من محكمة تجارية أو مدنية، فالأخيرة لا تخضع من حيث الموضوع والإجراءات إلى قواعد القانون الجنائي.

ويثور التساؤل ما هي طريقة تنفيذ الغرامة، ففي المادة (٣٩) من قانون رقم ٢٠ لسنة ٢٠١٤ في شأن المعاملات الإلكترونية، فقد نص القانون المشار إليه على المسؤولية التضامنية بين الطرفين مرتكب الفعل غير المشروع والمدير الذي أخل بواجبه في الرقابة.

ويبقى التساؤل هل ستدفع الغرامة بالتناصف فيما بينهما وهو ما ينافي مبدأ شخصية العقوبة، وماذا لو امتنع المدير أو الشخص المعنوي عن الدفع هل سيعاقب على فعل لم يرتكبه وافترض المشرع علمه بذلك، وبالتالي يتم حبسه إذا امتنع عن الدفع وهذا قصور لم يعالجه المشرع، فالعقوبة عندما تحدد تراعى فيها اعتبارات عامة من حيث نوع الجريمة والحق المعتدى عليه، هل هو حق عام ملك الدولة أو خاص للأفراد؟ وما هو مقدار الضرر الناجم. وكذلك ينظر المشرع في الجانب المعنوي هل الجريمة عمدية أو غير عمدية؟ ومدى خطورة الأفعال التي ارتكبها الجاني وهل سبق له ارتكاب مثل هذه الجرائم؟(٨٠).

إن المشرع في المادة (٣٧) في القانون رقم ٢٠/٢٠١٤ بشأن التعامل الإلكتروني قد وضع حداً أدنى للغرامة (خمسة آلاف دينار كويتي كحد أدنى وثلاثين ألف دينار كويتي كحد أقصى) ونحن نرى أنه من المهم اعتماد فكرة الغرامة النسبية

= يدفع للدولة المبلغ الذي تقدره المحكمة طبقاً لنص القانون، ولا يجوز أن يقل عن عشرة دنانير. وإذا لم يدفع المحكوم عليه مبلغ الغرامة حصل عن طريق التنفيذ الجبري على ماله، فإذا لم يتيسر التنفيذ الجبري جاز إخضاع المحكوم عليه للإكراه البدني وفقاً للقواعد المقررة في قانون الإجراءات الجزائية".

(٧٩) سمير الشناوي، النظرية العامة للجريمة والعقوبة في قانون الجزاء الكويتي، دراسة مقارنة قانون العقوبات المصري والفرنسي والألماني والنرويجي الكتاب الثاني المسؤولية الجنائية والعقاب (الكويت: وزارة الداخلية، كلية الشرطة، ١٩٨٨)، ص١٩٩.

(٨٠) سمير الشناوي: مرجع سابق، ص٢٣١.

التي تتناسب مع مقدار الضرر والخطر الناشئ عن الجريمة، وبالتالي من الأولى عدم النص على تحديد سقف أعلى للغرامة خصوصاً في جرائم التعامل الإلكتروني.

لأن التعامل الإلكتروني فيه معلومات وبيانات شخصية مهمة وفي كثير من الأحيان حساسة، ومن الممكن أن تكون قيمة الأسرار أو المعلومات الخاصة بالشركات الكبرى(٨١) أو الحكومات الفيدرالية تعادل الملايين، فلا يكون هناك عدالة بين الضرر الواقع على المجني عليه وقيمة الغرامة، لذا من الأولى عدم تحديد قيمة الحد الأعلى للغرامة وتركها للقاضي.

(٨١) لبعض الشركات العالمية مثل شركة أبل وشركة قوقل ميزانيات تعادل مجموعة دول مجتمعة، فأي معلومة سرية قد تتسرب تكلفها أموالاً طائلة؛ ولذلك تحرص هذه الشركات على وضع أنظمتها تحت الحماية والرقابة الصارمة وتتعامل مع المعلومات كأنها أسرار عسكرية.

الفصل الثاني
الجانب الإجرائي

ندرس في هذا الفصل تصنيف الجرائم الجنائية في قانون المعاملات الإلكترونية وتقسيماتها، ثم نميز بين مسؤولية الشخص الاعتباري وجريمة الإهمال والإخلال بالواجبات، وما هي حدود الشخص المعنوي، ثم نتطرق إلى الناحية الإجرائية من خلال معرفة من هم أهل الضبطية القضائية – جهة التحقيق – جهة التحري والاستدلال في القانون رقم ٢٠/٢٠١٤ بشأن التعامل الإلكتروني. وأخيرا نتكلم عن الصلح المقصود في قانون رقم ٢٠ لسنة ٢٠١٤ في شأن المعاملات الإلكترونية.

المبحث الأول
تصنيف الجرائم الجنائية في قانون المعاملات الإلكترونية وصورها بشكل عام

ويمكن تعريف الجريمة: فعل غير مشروع صادر عن إرادة جنائية يقرر له القانون عقوبة أو تدبير احترازي(٨٢).

خصائص الجريمة المعلوماتية:

١ – الجريمة المعلوماتية جريمة عابرة للحدود:

تتسم الجريمة المعلوماتية بأنها عابره للحدود والقارات وغالباً ما يكون لها طابع دولي، ومن خلال الإنترنت ترتكب العديد من الجرائم منها جرائم التعدي على قواعد البيانات، وتزوير واتلاف المستندات الإلكترونية وسرقة البطاقات وغسيل الأموال.

وهذا الطابع الدولي يثير إشكالية التعارض مع سيادة الدولة والقانون الواجب التطبيق(٨٣).

٢ – صعوبة إثبات الجريمة المعلوماتية:

تكمن الصعوبة في أن هذه الجريمة لا تترك آثاراً مادية ولا يوجد مسرح جريمة، وإنما أرقام ولغة البرمجة المعلوماتية فقط، ويسهل مسح الدليل الرقمي في ثواني وتحتاج إلى خبرة فنية يصعب على المحقق التقليدي الإحاطة بها، وتعتمد بشكل كبير

(٨٢) محمود نجيب حسني، شرح قانون العقوبات القسم العام (دار النهضة العربية، الطبعة السادسة، ١٩٨٩)، ص٤٠.

(٨٣) خالد ممدوح إبراهيم: مرجع سابق، ص٤٤.

على الخداع والتضليل، كما أن البنوك والشركات العملاقة تحجم في كثير من الأوقات عن الإبلاغ عن جرائم معلوماتية خشية أن تهتز ثقتها وسمعتها، وهو ما يزيد فرصة إفلات الجناة من العقاب، وتعد الجريمة المعلوماتية من جرائم الذكاء ولها دوافع مثل الانتقام والطمع والجشع أو إثبات الذات، فهذا النوع من المجرمين على درجة عالية بأصول التكنولوجيا وخباياها(٨٤).

٣ – عدم وجود مفهوم مشترك للجريمة المعلوماتية:

التنسيق الدولي في مجال الجريمة المعلوماتية لا يزال بطيء بعض الشيء؛ لأن النظم القانونية بين الدول تختلف بتعريف الجريمة ومفهومها، فما يعد جريمة كالمخدرات في دولة الكويت لا يعتبر جريمة في الدول الإسكندنافية، فيجب على الدول التعاون فيما بينها والحرص على المعاهدات الدولية والدخول فيها حتى لا يستفيد مجرمو المعلومات من القصور التشريعي(٨٥).

٤ – وقوع الجريمة المعلوماتية أثناء معالجة البيانات:

يمكن أن تقع الجريمة المعلوماتية في أي مرحلة من مراحل معالجة البيانات الأساسية لتشغيل النظام. المرحلة الأولى وهي مرحلة الإدخال والثانية أثناء معالجتها والثالثة أثناء إخراج المعلومات، ويمكن التلاعب في برامج نظم المعلومات بإدخال بيانات غير مصرح فيها أو استبدالها.

٥ – قلة الإبلاغ عن وقوع الجرائم المعلوماتية:

لا يتم الإبلاغ عن هذه الجرائم في الغالب لسببين لعدم اكتشاف الضحية أو الخوف والخشية من التشهير، وتشير الدراسات أن أغلب جرائم المعلومات يتم اكتشافها صدفة أو بعد مرور وقت طويل على ارتكابها.

٦ – حداثة الجرائم المعلوماتية:

الطفرة والنقلة النوعية في عالم الإنترنت والتكنولوجيا الحديثة والعولمة التي دخلت كل القارات، يستغلها بعض ضعاف النفوس في ارتكاب جرائمهم من تهريب المخدرات وغسيل الأموال والإتجار بالبشر والجرائم الجنسية وغيرها الكثير، وهذا لا يعني أن نبخس المنافع والإيجابيات في عالم الإنترنت(٨٦).

---

(٨٤) خالد ممدوح إبراهيم: مرجع سابق، ص٤٧.

(٨٥) خالد ممدوح إبراهيم: مرجع سابق، ص٤٩.

(٨٦) خالد ممدوح إبراهيم: مرجع سابق، ص٥٢.

ويمكن تصنيف جرائم نظم المعلومات إلى أكثر من قسم. **فالأول الجرائم العامة:** التي تشمل التقصير والإهمال، أخطاء الأداء المتعمدة، التآمر والتواطؤ. وهناك **النوع الثاني من جرائم المعلومات**: ويشمل الجرائم المادية ومنها التجسس بأنواعه العسكري والصناعي، التدمير والإتلاف وأخيراً سرقة البيانات.

وقد تعرضت العديد من الدول المتقدمة إلى عمليات تهديد الأمن القومي والعسكري وقرصنة معلوماتية، وذلك للحصول على الأسرار العسكرية المخزنة في أجهزة الحاسب الآلي المستعملة فيها، وهو ما حدث لسلاح البحرية الفرنسي في صيف عام ١٩٩٤ فقد تم الحصول على المعلومات الخاصة والمهمة عن السفن التي يستعملها حلف شمال الأطلنطي مما أثار حفيظة الفرنسيين. إن تكنولوجيا المعلومات سهلت بشكل كبير في انتشار انتهاك الخصوصية على المستوى العالمي، حيث يتعرض الأفراد والحكومات والبنوك إلى انتهاك الخصوصية بشكل متكرر من قبل العصابات الإجرامية أو الهاكرز أو المتطفلين أو من الموظفين أنفسهم، وهو ما يتطلب من هذه الجهات تقوية أنظمة الحماية ووضع الرقابة الصارمة على موظفيها.

أما النوع الثالث: يسمى بالجرائم الاقتصادية ويشمل النصب والاحتيال، الرشوة، الابتزاز، انتهاك الأسرار الاقتصادية. **والنوع الرابع:** جرائم ضد الأفراد مثل انتهاك الخصوصية، تسهيل الدعارة والتحرش الجنسي(٨٧).

إن تكنولوجيا المعلومات ساهمت بشكل كبير بانتشار الجرائم الاقتصادية بل وأصبحت منظمة عالمياً، لها عصابات متخصصة وتدار من قبل أشخاص محترفين لهم إمكانيات وقدرات علمية ومهنية خاصة. وأصبحت جرائم المعلومات تشكل ضغطاً على الحكومات من حيث صعوبة التنبؤ فيها، وذلك لعدم توافر أدلة مادية أو شهود، كما إن التطور التشريعي لا يسير بنفس السرعة التي تتطور فيها جرائم المعلومات(٨٨).

تخريب المعلومات وإساءة استخدامها: تعد هذه الجريمة من أخطر الجرائم وتزداد بشكل ملحوظ إذا انخفض مستوى الرقابة على الموظفين ممن يملكون صلاحيات واسعة على النظام(٨٩). وتعتبر صلاحية الموظف بتعديل المعلومات

(٨٧) حسن طاهر داوود: مرجع سابق، ص٣٨.

(٨٨) الشحات إبراهيم محمد منصور: مرجع سابق، ص١٥٠.

(٨٩) تقوم وزارة الداخلية في دولة الكويت بمجهود كبير في جانب الرقابة على الموظفين المصرح لهم بالدخول على بيانات الأفراد، فعلى سبيل المثال يفقد الموظف صلاحية للدخول على النظام مؤقتا إذا أتهم في جنحه أو جناية حتى يصدر حكم البراءة، وفي حال نقل الموظف إلى إدارة أخرى أو خروجه في ندب أو إجازة رسمية توقف صلاحيته للدخول مؤقتاً حتى عودته.

وتشفيرها من أخطر الصلاحيات التي قد تكلف الشركات خسائر فادحة إذا تم إساءة استخدامها(٩٠).

وترتفع نسبة هذه الجريمة كذلك كلما قل الانضباط بين الموظفين في الشركات أو المؤسسات الحكومية، فكلما تراخت الرقابة على الموظفين المعنيين، أي من يملكون كلمات السر وصلاحيات التشفير كلما أدت هذه الجريمة إلى أضرار كبيرة(٩١). إن قدرة الموظف على تشفير المعلومات يعد ثغرة أمنية ففي بعض الأحيان، قد يقوم الموظف بتشفير الأسرار التجارية ونقلها بطريقة مشفرة إلى شركة منافسة وبالتالي يفلت من العقوبة بسبب عدم تمكن أحد من قراءة المعلومات المشفرة.

تزوير البيانات: من أشهر الجرائم وأوسعها على الإطلاق؛ لأن التزوير يتضمن تعمد إدخال بيانات مغلوطة، وهناك حادثة مشهورة في كاليفورنيا لمدخلة بيانات كانت تعمل على تغيير ملكية السيارات على النظام الإلكتروني مقابل مبلغ من المال لكي تصبح السيارة ملك للص السارق على الورق، ثم يقوم اللص بسرقتها فعلياً وببيعها كأنه المالك الأصلي(٩٢).

انتهاك الخصوصية: للفرد الحق في خصوصية معلوماته الشخصية فيمكنه حجبها عمن يشاء، فلا يصح فتح أي مستند شخصي للفرد إلا بإذن من صاحبه. ويحدث انتهاك الخصوصية بمجرد الاطلاع على مستند شخصي غير مصرح للشخص بالاطلاع عليه.

إن انتهاك خصوصية الأفراد بدأ بالتزايد مع انتشار الإنترنت وتطبيق التعامل الإلكتروني بين الدول المختلفة والأفراد والشركات وغيرها. كما أصبح الغرض من نشر خصوصيات الأفراد هو الابتزاز والحصول على الأموال والتشهير وخدش الحياء أو في بعض الأحيان مجرد إثبات الذات(٩٣). ومثال ذلك من ينشر تاريخ الميلاد الخاص بممثلة مشهورة أو ينشر تاريخ حصول شخصية تجارية معينة على الجنسية. وحيث إنه لا يستطيع أحد أن يسيطر بنسبة كاملة على الخصوصية وإنما هناك خطوات تحفظ الخصوصية بالقدر الممكن من الحماية.

(٩٠) حسن طاهر داوود: مرجع سابق، ص٤٠.
(٩١) حسن طاهر داوود: مرجع سابق، ص٣٩.
(٩٢) حسن طاهر داوود: مرجع سابق، ص٤٦.
(٩٣) ثروت عبد الحميد: مرجع سابق، ص٦٧.

خطوات وقف تسرب المعلومات الشخصية:

١ – تحديد نوع البيانات التي يجب أن تبقى سرية وتقييد الوصول إليها.

٢ – تزويد البيانات الشخصية للجهات الحكومية وإتلافها من قبلها بمجرد الانتهاء منها.

٣ – الموافقة الكتابية من صاحب العلاقة بتداول معلوماته.

٤ – فرض سياسة عامة لتداول المعلومات الشخصية وأي اختراق يعرض صاحبه للمسؤولية(٩٤).

أ – المطلب الأول

اختصاص النيابة العامة في الدعوى الجزائية من حيث الأصل واختصاصها في القانون رقم ٢٠ / ٢٠١٤ بشأن التعامل الإلكتروني

مفهوم الدعوى العمومية: يرجع تاريخ الدعوى العمومية أو الجزائية ونشأتها في فرنسا، حيث كانت النيابة العامة مؤسسة ملكية خالصة، يعود تاريخها إلى القرن الرابع عشر، عندما كان محامو الملك ونوابه يمثلون مصالح التاج الخاصة أمام المحاكم، واستمرت سلطتهم في التوسع، حتى أصبحوا ممثلي السلطة العامة لدى المحاكم، وأنيطت بهم مهمة تمثيل المجتمع(٩٥).

فالنيابة العامة: هي تلك الجهة التي تتولى التحقيق والتصرف والاتهام في الجنايات، ويتكون جهاز النيابة العامة من نيابة كلية واحدة يرأسها النائب العام وعدد من المحامين العامين وعدد من رؤساء النيابة، كما تتكون من نيابات متخصصة مثل نيابة الشؤون التجارية، ونيابة المخدرات والخمور، ونيابة الأحداث، ونيابة الأموال العامة، ونيابة شؤون الصحافة والنشر، وجهاز حماية المديونيات العامة، ونيابة الأحوال الشخصية، بالإضافة إلى ست نيابات جزئية في محافظات الدولة الست وهي (العاصمة – حولي – الفروانية – الجهراء – الأحمدي – مبارك الكبير).

إن السلطة بالنيابة العامة تكون رئاسية أي متدرجة على رأسها النائب العام وحده ويليه عدد من المحامين العامين الذي يكون لأقدمهم حق القيام بأعمال النائب العام في حالة خلو منصبه أو غيابه أو قيام أي مانع لديه، وبعد المحامين العامين تكون مرتبة رؤساء النيابة، وبعد ذلك وكلاء النيابة، وهذا التدرج الوظيفي هو التدرج العام في وظيفة وكيل النيابة.

---

(٩٤) حسن طاهر داوود: مرجع سابق، ص٥٣.

(٩٥) http://www.kna.kw/clt/run.asp?id = 1658#sthash.WAQMpFGW.dpuf.

يهدف قانون الإجراءات الجزائية إلى حماية المجتمع من المجرمين والكشف عن الجريمة، وحماية المتهم من خلال الضمانات التي تحقق فيها دفاعه عن نفسه(٩٦). وأخيراً إلى حماية الحرية الفردية وتوظيف العقوبة بالردع العام والخاص(٩٧).

وتنص المادة (١٦٧) من الدستور الكويتي على أنه: "تتولى النيابة العامة الدعوى العمومية باسم المجتمع، وتشرف على شؤون الضبط القضائي وتسهر على تطبيق القوانين الجزائية وملاحقة المذنبين وتنفيذ الأحكام، ويرتب القانون هذه الهيئة وينظم اختصاصاتها، ويعين الشروط والضمانات الخاصة بمن يولون وظائفها. ويجوز أن يعهد لجهات الأمن العام بتولي الدعوى العمومية في الجنح على سبيل الاستثناء ووفق الأوضاع التي يبينها القانون".

بحسب الأصل إن النيابة العامة تعد وكيلة عن المجتمع، فهي المكلفة برفع الدعوى الجزائية لأنها خصم شريف تسعى إلى استظهار الحقيقة المجردة وإن كانت لصالح المتهم، ولما كانت الدعوى الجزائية تحتاج إلى شكليات وإجراءات مرتبة ومعينة فإن المشرع يهدف من وراء هذه الإجراءات الشكلية إلى تحقيق مصلحتين متعارضتين.

المصلحة الأولى: هي مصلحة المجتمع بعقاب المجرم عن جريمته وتطبيق العدالة، والثانية: هي مصلحة المتهم بمراعاة الضمانات التي كفلها له الدستور والقانون(٩٨). وقد نص الدستور الكويتي على اختصاص النيابة في الجرائم بشكل عام دون تحديد الجنحة أو الجناية(٩٩)، وأن تعهد إلى الجهات الأخرى على سبيل الاستثناء إلا أن هذا الاستثناء طال عمره إلى ما يزيد عن خمسين عاماً، فإلى اليوم يختص المحققون في الجنح ووكلاء النيابة في الجنايات بشكل عام، وكما أن هناك بعض

(٩٦) إقبال القلاف، مبادئ قانون الإجراءات الجزائية في القانون الجزائي الكويتي (الكويت: دار العلم، الطبعة الأولى، ٢٠٠٥)، ص٥.

(٩٧) سمير الشناوي: مرجع سابق، ص٢٢.

(٩٨) أحمد حبيب السماك، قانون الإجراءات والمحاكمات الجزائية (الكويت: وزارة الداخلية أكاديمية سعد العبد الله للعلوم الأمنية)، ص٦.

(٩٩) دستور الكويت مادة (١٦٧) "تتولى النيابة العامة الدعوى العمومية باسم المجتمع، وتشرف على شؤون الضبط القضائي، وتسهر على تطبيق القوانين الجزائية وملاحقة المذنبين وتنفيذ الأحكام. ويرتب القانون هذه الهيئة وينظم اختصاصاتها ويعين الشروط والضمانات الخاصة بمن يولون وظائفها. ويجوز أن يعهد بقانون لجهات الأمن العام بتولي الدعوى العمومية في الجنح على سبيل الاستثناء، ووفقاً للأوضاع التي يبينها القانون".

الجنح الخاصة تتولى النيابة العامة التحقيق فيها كما هو الحال في الجرائم التي تقع على التعامل الإلكتروني.

وقد انتقد الفقهاء في السابق أن يتولى التحقيق جهات تنفيذية غير مستقلة، كما هو الوضع في الكويت بالنسبة للمحققين لأنهم يتبعون السلطة التنفيذية – وزارة الداخلية –. فذلك من شأنه أن يزيد من استخدام وسائل التعسف أو الاتهام لمجرد الشبهات، وإن من الأولى ترك التحقيق إلى جهات قضائية مستقله(١٠٠).

ولا تتبع النيابة العامة في الكويت وزارة العدل من حيث السلطة الرئاسية بل تتبع السلطة القضائية المتمثلة بمجلس القضاء الأعلى الذي يهيمن على النيابة العامة وكافة محاكم الدولة، فالنيابة العامة مستقلة عن السلطة التنفيذية في شؤون الدعوى الجزائية وما يتعلق بتحريكها ومباشرتها وتحقيقها والتصرف والادعاء فيها(١٠١).

ونحن نميل وبشدة إلى ضرورة العمل على إيقاف الاستثناء والعمل على إسناد التحقيق في الجرائم إلى جهات قضائية مستقلة، وهو أمر يتماشى مع الواقع فالاستثناء لا يجوز التوسع فيه أو القياس عليه، فمن المفترض الانتهاء من العمل بهذا الاستثناء بمجرد زوال الأسباب التي دعت إليه، وبالتالي عودة الاختصاص إلى النيابة العامة فهي صاحبه الاختصاص الأصيل وفقاً للدستور(١٠٢).

مستدلين بقول الخبير الدستوري الدكتور عثمان خليل عثمان في محضر الجلسة رقم (١٢) أن: "الأمر الأول والأخير في الدعوى العمومية يجب أن يكون بيد النيابة العامة فهي التي تمثل المجتمع وهي الأمينة على الدعوى العمومية بهذه الصفة"(١٠٣). إن ضم الإدارة العامة للتحقيقات للنيابة العامة وتوحيد الدعوى العمومية، هو أمر حيوي ومهم وهو يعيد الأمور إلى نصابها الصحيح.

(١٠٠) عبد الوهاب حومد: مرجع سابق، ص٢٢٩.

(١٠١) https://www.moj.gov.kw/sites/ar/PublicProsecution/pages/default.aspx.

(١٠٢) أحمد حبيب السماك، قانون الإجراءات والمحاكمات الجزائية: مرجع سابق، ص١٥٢.

(١٠٣) محاضر اجتماعات لجنة الدستور والمجلس التأسيسي.

ب – المطلب الثاني
من الناحية الإجرائية من هم أهل الضبطية القضائية – جهة التحقيق – جهة التحري والاستدلال في القانون رقم ٢٠/٢٠١٤ بشأن التعامل الإلكتروني

نصت اللائحة التنفيذية من القانون رقم ٢٠ لسنة ٢٠١٤ المشار إليه. مادة (١) في تطبيق أحكام هذه اللائحة يقصد بالكلمات والمصطلحات التالية المعنى المبين قرين كل منها: "الجهة المختصة: الجهة التي يعهد إليها مجلس الوزراء الإشراف على إصدار التراخيص اللازمة لمزاولة خدمات التصديق الإلكتروني والتوقيع الإلكتروني وغير ذلك من الأنشطة في مجال المعاملات الإلكترونية والمعلومات".

وقد بينت المادة (١٨) من اللائحة التنفيذية الخاصة بالقانون رقم ٢٠/٢٠١٤ بشأن المعاملات الإلكترونية اختصاصات جهة التحقيق والمدد المحددة للإيقاف المؤقت وغيرها[١٠٤]. وحسنا فعل المشرع الكويتي عندما ترك التفصيل للائحة، بحيث لو استجد أمر أو واجهت الجهات التنفيذية صعوبات فنية أو إدارية يسهل تغييرها من خلال اللائحة؛ لأن القانون كي يتغير لابد أن يمر من خلال السلطة التشريعية – مجلس الأمة – الذي قد يحتاج إلى مراحل عديدة كالتصويت والإقرار في أكثر من مداولة، ومن ثم النشر في الجريدة الرسمية حتى يصبح القانون الجديد أو أي تعديل لقانون سابق نافذ.

---

(١٠٤) تنص المادة(١٨) من اللائحة التنفيذية من قانون رقم ٢٠ لسنة ٢٠١٤ في شأن المعاملات الإلكترونية على أنه: "إذا كان هناك قصور أو إخلال في أعمال مزود خدمات التصديق، يستدعي الإيقاف المؤقت من قبل مدير جذر التصديق، تطبق الإجراءات التالية: "١– يقوم مدير جذر التصديق بتقديم تقرير تفصيلي للجهة المختصة بوجود إخلال أو قصور في أعمال مزود خدمات التصديق، مبيناً حالات وجوانب الإخلال والقصور في الأعمال مع الإشارة إلى عمليات قام بها مزود خدمة التصديق تدعم ذلك.

ويستثنى من ذلك إذا كان الإخلال أو القصور بناء على الفقرة ٢ أو ٤ من المادة ١٣ من هذه اللائحة.

٢ – تقوم الجهة المختصة بدراسة تقرير مدير جذر التصديق أو الشكوى المقدمة من ذوي الشأن والبدء بالتحقيق مباشرة، ويتم ذلك بالتنسيق مع مدير جذر التصديق وباستدعاء ممثل لمزود خدمات التصديق، كما يتم استدعاء ذوي الشأن في حالة الشكوى.

٤ – يلتزم مزود خدمات التصديق بتطبيق الإجراءات المتبعة والخاصة بالإيقاف المؤقت والمشار إليها في المادتين ٨ و١٥ من هذه اللائحة إذا ما تم إيقافه مؤقتاً بناء على هذه المادة..."

ويثور التساؤل عن كيفية التغلب على الصعوبات التي تواجه جهة التحقيق والاستدلال، ونحن نرى إمكانية العمل على حل هذه الصعوبات في التحقيق والادعاء في الجرائم الإلكترونية من خلال الآتي:

١ – التنسيق والتعاون بين الأجهزة المعنية (المحقق أو كيل النيابة – وخبير المعلومات – جهاز الشرطة) منذ البداية والعمل على أسس واضحة دون انفراد بالقضية أو تنصيب أحد الأطراف نفسه مسؤولاً عنها.

٢ – قناعة الأطراف الثلاثة بحدود معرفته ومهاراته واختصاصاته واحترام أدوار الغير في القضية.

٣ – يجب على خبراء تقنية المعلومات الإلمام بالإجراءات الشكلية الخاصة بنظام العدالة؛ حتى لا تبطل الأدلة التي يتحصلون عليها وتثقيفهم من الناحية القانونية.

٤ – يجب تقبل بعض المعوقات القانونية المتعلقة بمسائل الاختصاص وتنازع القوانين من خلال التحضير لها، بحيث لا تكون محبطة لسير القضية بل متوقعة ويسهل التعامل معها.

٥ – يجب أن يسعى كل من (المحقق أو كيل النيابة وجهاز الشرطة) المخصص للنظر في مثل هذه الجرائم إلى فهم لغة الحاسب الآلي والمختصرات التي يذكرها خبراء المعلومات والاتفاق حول معانيها؛ لأن الاختلاف حول المفردات يكون مدعاة للشك والريبة وقد تبطل التهمة.

٦ – على جميع الأطراف (المحقق أو كيل النيابة – وخبير المعلومات – جهاز الشرطة) التشاور في خطوات القضية والعمل بطريقة متسلسلة وخصوصا فيما يتعلق في الأولويات الإجرائية؛ حتى لا تتبعثر الجهود وتبطل التهم نتيجة اجتهاد أو تسرع أحد الأطراف.

٧ – التأكيد على أن التحقيق السليم هو المدخل الصحيح لبناء القضية من خلال المعرفة بالقانون الواجب التطبيق واستخدام أدوات التحقيق المعيارية الصحيحة(١٠٥).

ويمكن إجمال هذه الأدوات بالآتي: تحليل الشكوى – جمع الأدلة المادية – الحصول على استشارة الخبراء – مقابلة الشهود واستجواب المشتبه فيهم – بناء

(١٠٥) John R. Vacca: Computer Forensics- Computer Crime Scene Investigation (Snd.ed) Massachus -Etts. Charles River Midia.2005.

ملف القضية وتحليها وأخيراً اتخاذ قرار الادعاء[١٠٦]. كما يعتمد الادعاء بشكل رئيسي على الشاكي نفسه وقوة الأدلة التي يقدمها.

الاستعانة بالخبرة الفنية:

منذ بدء ظهور الجرائم ذات الصلة بالحاسب الآلي، تستعين الشرطة وسلطات التحقيق أو المحاكم بأصحاب الخبرة الفنية في مجال الحاسب الآلي، وذلك بغرض كشف غموض الجريمة، أو تجميع أدلتها، أو مساعدة المحقق في فهم جوانب الغموض في العمليات الإلكترونية الدقيقة ذات الصلة بالجريمة محل التحقيق.

وإذا كانت الاستعانة بخبير فني أمر جوازي للمحقق أو لجهة التحقيق والحكم، إلا أنه في المسائل الفنية البحتة التي لا يمكن للقاضي أن يقطع فيها برأي دون استطلاع رأي أهل الخبرة، في هذه الحالة يجب عليه أن يستعين بالخبير، فإذا تصدى القاضي للمسألة الفنية وفصل فيها دون تحقيقها بواسطة خبير[١٠٧] كان حكمه معيباً مستوجباً نقضه، وهذا المبدأ استقر عليه قضاء محكمة النقض المصرية.

وبناء عليه فإذا كانت الاستعانة بخبير فني في المسائل الفنية البحتة أمراً واجباً على جهة التحقيق والقاضي، فهي أوجب في مجال الجرائم الإلكترونية، حيث تتعلق بمسائل فنية آية في التعقيد ومحل الجريمة فيها غير مادي، والتطور في أساليب ارتكابها سريع ومتلاحق، ولا يكشف غموضها إلا متخصص وعلى درجة كبيرة من التميز في مجال تخصصه، فإجرام الذكاء والفن، لا يكشفه ولا يحله إلا ذكاء وفن مماثلين.

اختلف الفقهاء حول تحديد الطبيعة القانونية للخبرة حيث اعتبرها البعض وسيلة من وسائل الإثبات. فيما اعتبرها البعض الآخر وسيلة لتقدير الدليل، وهناك من يرى بأنها مجرد وسيلة لمساعدة القاضي على فهم المسائل الفنية، وقيل إنها نوع من الشهادة.

وأهمية الاستعانة بالخبيرة في مجال الجرائم الإلكترونية، تظهر عند غيابهِ، فقد تعجز الشرطة عن كشف غموض الجريمة، وقد تعجز هي أو جهة التحقق عن جميع الأدلة حول الجريمة وقد تدمر الدليل أو تمحوه بسبب الجهل أو الإهمال عند التعامل معه.

---

(١٠٦) محمد الأمين البشرى، الجرائم الإلكترونية التحقيق الادعاء المحاكمة ومعاملة المذنبين فيها (الإمارات العربية المتحدة، حكومة دبي، ٢٠١٢)، ص٢١٥.

(١٠٧) الخبرة لغته: يقال خبرت الشيء أي عرفته على حقيقته.

ومن التشريعات الحديثة التي نظمت أعمال الخبرة في مجال الجرائم الإلكترونية، القانون البلجيكي الصادر في ٢٣ نوفمبر سنة ٢٠٠٠. فقد نصت المادة (٨٨) من القانون المذكور على أنه: "يجوز لقاضي التحقيق، وللشرطة القضائية أن يستعينا بخبير ليقدم وبطريقة مفهومة المعلومات اللازمة عن كيفية تشغيل النظام، وكيفية الدخول فيه، أو الدخول للبيانات المخزونة أو المعالجة أو المنقولة بواسطته". ويعطي القانون كذلك لسلطة التحقيق أن تطلب من الخبير تشغيل النظام، أو البحث فيه، أو عمل نسخة من البيانات المطلوبة للتحقيق، أو سحب البيانات المخزنة أو المحولة أو المنقولة، على أن يتم ذلك بالطريقة التي تريدها جهة التحقيق. ولجهة التحقيق السلطة الكاملة في أن تطلب من الخبير تشغيل النظام أو عمل نسخة من البيانات المطلوبة للتحقيق، أو سحب البيانات المخزنة أو المحولة أو المنقولة.

ووفقاً للقانون المشار إليه فإن الالتزام بتشغيل النظام واستخراج البيانات المطلوبة منه، يرجع إلى قاضي التحقيق بصفة أصلية، ويجوز ذلك للنيابة العامة على سبيل الاستثناء في حالة التلبس بالجريمة، أو عند الرضاء بعملية التفتيش هذه فمهمة الخبير وفقاً للنص السابق تتمثل من ناحية في تشغيل النظام، ومن ناحية أخرى في تقديم البيانات المطلوبة، حسب الطريقة التي تريدها جهة التحقيق.

مسؤولية الخبير:

إن التزام الخبير هو التزام ببذل عناية وليس بتحقيق نتيجة، فلا يسأل الخبير إذا لم يصل إلى النتيجة المطلوبة نتيجة ضعف الخبرة، أو بسبب العقبات التي واجهته أثناء مباشرته لمهمته، كأن تكون الأجهزة التي تم نقل المعلومات والبيانات منها لا تتماشى مع أجهزة الدولة.

إلا أن ذلك لا يعني عدم مسؤوليته الجنائية إذا رفض القيام بالمهمة المكلف بها، أو أتلف عمداً البيانات المطلوب منه التعامل معها، أو حفظها، فضلاً عن التزام الخبير بأداء مهمته التي حددتها له جهة التحقيق، ويجب على الخبير كذلك المحافظة على سر المهنة، وفي حالة إفشائه السر، يعاقب بالعقوبة المقررة لهذه الجريمة.

ج – المطلب الثالث
مسؤولية الشخص الاعتباري في القانون رقم ٢٠ / ٢٠١٤ مادة (٣٩) جريمته الإخلال بواجباته والإهمال

يحتل الشخص المعنوي أهمية بالغة في القانون العام، ويوفر القانون للشخص المعنوي كياناً قانونياً مستقلاً يتحمل الشخص بموجبه الالتزامات وتفرض له الحقوق،

وهو ما يبرر الكثير من الأوضاع القانونية[١٠٨]. فالأشخاص المعنوية مثل الدولة والمحافظات والهيئات والمؤسسات لها أشخاص وأموال وأهداف مشتركة، فهي لها إرادة مفترضة تختلف عن إرادة الشخص الطبيعي[١٠٩].

ولذلك ذهب الرأي أن الشخصية المعنوية لا تكتسب وجودها القانوني إلا باعتراف المشرع بها، بعد أن يضع شروطه المقررة وقد يحدد صلاحياتها ووقت انتهائها[١١٠]. والحقيقة التي ليست هي محل خلاف هو اعتراف القانون بالشخصية المعنوية للصياغة القانونية، بالتالي وجود أشخاص أو أموال تستهدف تحقيق مصلحة مستقلة، وهذا المركز القانوني يحميه القانون طالما توافرت فيه العناصر اللازمة لقيامه[١١١].

غير أن مسؤولية الشخص المعنوي جنائياً كانت ولا تزال محل خلاف في الفقه القانوني، فالبعض يرى أن الشخص المعنوي له وجود حقيقي طالما أن المشرع اعترف به، وأعطاه صلاحية كسب الحقوق وتحمل الالتزامات، واعترف له بذمة مالية مستقلة فهو يقف على قدم المساواة كالشخص الطبيعي، فلا يستساغ الاعتراف للشخص المعنوي في مجال المسؤولية التعاقدية والتقصيرية ثم ننكرها عليه في الجنائية[١١٢]. إلا أن هذا الرأي لم يلق قبولاً عند معظم الفقهاء؛ لأن الشخص المعنوي ليس له إرادة ذاتية وطبيعته المعنوية لا تمكنه من ارتكاب الأفعال المادية في الجريمة.

وقد نص قانون التعامل الإلكتروني ٢٠/٢٠١٤ في المادة رقم (٣٩) "مع عدم الإخلال بالمسؤولية الجزائية الشخصية لمرتكب الجريمة، يعاقب المسؤول عن الإدارة الفعلية للشخص المعنوي بذات العقوبات المقررة عن الأفعال التي ترتكب بالمخالفة

(١٠٨) عبد المنعم فرج الصده، أصول القانون العام (القاهرة: ١٩٧٢)، ص٤٦٨.

(١٠٩) فقد جاء في حكم محكمة التمييز في الطعن رقم ٩٠/٢٨٥ تجاري الصادر في جلسة ٢٦ يناير ١٩٩٢ (على أنه يجب لنشوء الشخص الاعتباري توافر عنصرين – عنصر موضوعي وهو وجود جماعة من الأشخاص أو مجموعة من الأموال بقصد تحقيق غرض معين، وعنصر شكلي هو اعتراف القانون لهذه المجموعة بالشخصية الاعتبارية وفقاً للشروط والأوضاع التي يحددها) راجع مجموعة القواعد التي قررتها محكمة التمييز عن المدة من ١٩٢/١ حتى ٩٦/١٢/٣١، القسم الثالث، المجلد الاول، يوليو ١٩٩٩، ص٥٥٣.

(١١٠) مجدي عز الدين يوسف، أصول القانون الإداري أسس التنظيم الإداري وسائل الإدارة العامة في القانون المقارن والكويتي (الكويت: وزارة الداخلية أكاديمية سعد العبد الله للعلوم الأمنية) ص١١٠.

(١١١) مجدي عز الدين يوسف: مرجع سابق، ص١١٤.

(١١٢) سمير الشناوي: مرجع سابق، ص١١.

لأحكام هذا القانون إذا كان إهماله وإخلاله بالواجبات التي تفرضها عليه تلك الإدارة قد أسهم في وقوع الجريمة مع علمه بذلك، ويكون الشخص المعنوي مسؤولاً بالتضامن عما يحكم به من عقوبات مالية وتعويضات إذا كانت المخالفة قد ارتبكت من أحد العاملين باسم الشخص المعنوي أو لصالحه".

وفي هذه المادة العديد من الإشكالات:

أولاً: أقام المشرع مسؤولية جنائية للشخص المعنوي في المادة(٣٩) من القانون رقم ٢٠/٢٠١٤ على غير أساس الخطأ الشخصي. وهذا إهدار للمبدأ الدستوري في المادة (٣٣) من الدستور "العقوبة شخصية"(١١٣). وهنا قد تم مساءلة شخص عن جريمة لم يرتكبها بنفسه إلا إذا كان شريكاً مع الفاعل الأصلي، ومن غير المستساغ القول بتوافر عناصر المساهمة الجنائية بين الشخص المعنوي وممثليه.

ثانياً: تفترض المادة (٣٩) وجود شخصين الأول هو الموظف الذي تعمد فعل الدخول غير المشروع، أو قام بأي عمل مجرم منصوص عليه في المادة (٣٧) من قانون ٢٠/٢٠١٤ بشأن التعامل الإلكتروني، ووجود شخص آخر وهو الممثل أو "**المسؤول عن الإدارة الفعلية للشخص المعنوي**" وهنا جريمته غير عمدية نتيجة الإهمال والإخلال بواجباته.

وحيث إن المشرع في هذه الحالة قد ساوى في العقوبة بين الجريمة العمدية للشخص الأول والجريمة غير العمدية للشخص الثاني، وهو أمر يخالف المبادئ العامة المقررة في قانون الجزاء، فلا يصح أن نكافئ صاحب الجريمة العمدية الذي يتوافر لدية القصد الجنائي مع مرتكب الجريمة غير العمدية في العقاب، ويكون مسؤولا بالتضامن عما يحكم به من عقوبات مالية وتعويضات.

كما أن المشرع في ذات المادة نص على: "إذا كان إهماله وإخلاله بالواجبات التي تفرضها عليه تلك الإدارة قد أسهم في وقوع الجريمة مع علمه بذلك"(١١٤) فكيف يعتبر المشرع الطرف الثاني مهملاً مع علمه بذلك، فالإهمال والعلم نقيضان لا يجتمعان، وبالتالي لا يتصور وقوع العلم والإهمال لدى الشخص نفسه وتقع عليه مسؤولية تضامنية مع مرتكب الجريمة.

وحيث إن قانون الجزاء لم يحدد الشخص المعنوي في مواده ولم ينص على

(١١٣) الدستور الكويتي مادة (٣٣).
(١١٤) المادة رقم (٣٩) من قانون رقم ٢٠ لسنة ٢٠١٤ في شأن المعاملات الإلكترونية.

المسؤولية التضامنية وإنما وضع العقوبة حسب موقف الجاني من الجريمة (فاعل أصلي – شريك). وفي حالة العود نص قانون الجزاء في المادة (٨٦) "إذا سبق الحكم على المتهم بعقوبة جنحة لارتكابه جريمة سرقة أو نصب أو خيانة أمانة أو تزوير أو شروع في إحدى هذه الجرائم، أو ثبت ارتكابه خلال خمس سنوات من تاريخ الحكم المذكور جريمة من الجرائم السابقة أو الشروع في إحداها، جاز للمحكمة أن تقضي عليه بأكثر من الحد الأقصى المقرر قانوناً بشرط عدم مجاوزة هذا الحد بأكثر من نصفه"(١١٥).

وهذا نص واضح وصريح من قانون الجزاء يبين فيه حالة العود للمجرم إلى أحد الجرائم المذكورة، وحدد له العقوبة في قانون الجزاء، وهو ما أغفله المشرع في قانون رقم ٢٠/٢٠١٤ بشأن التعامل الإلكتروني، فهل يسأل الشخص المعنوي مرة أخرى عن إهماله؟

خصائص العقوبة في التشريع الجنائي:

القاعدة العامة في التشريعات الجنائية أن كل شخص طبيعي، مميز، حر الإرادة، يتحمل شخصياً تبعية ما يتسبب به من أفعال يجرمها القانون. والفعل المجرم إما أن يكون بقصد أو بغير قصد كالإهمال والخطأ. والعقوبات تعتبر وسيلة للردع تتدرج حسب جسامة الفعل وظروف المتهم. إلا أن أي عقوبة لا بد أن تتوافر فيها هذه الخصائص:

أولاً: أن تكون العقوبة شرعية: وهو مقتضى مبدأ الشرعية "فلا جريمة ولا عقوبة إلا بنص" وهو منصوص عليه في صلب الدستور وهو يهدف إلى حماية حقوق الفرد من التعسف(١١٦). إن الفقه الحديث يعطي مبدأ الشرعية مفهوماً يشمل جميع سلطات الدولة ومن ضمنها السلطة التشريعية التي يجب أن تلتزم بالدستور. ثانياً: شخصية العقوبة: لا توقع العقوبة إلا بعد الإدانة في محاكمة عادلة تتوافر فيها الضمانات للمتهم، ولا يجوز أن تمتد هذه العقوبة إلى أحد غير المتهم. بخلاف المسؤولية المدنية التي يسأل فيها المتبوع عن أعمال تابعه(١١٧) قال تعالى: ﴿وَلَا تَزِرُ وَازِرَةٌ وِزْرَ أُخْرَىٰ﴾(١١٨). ثالثاً: عدالة العقوبة: أي يكون هناك شيء من التناسب

(١١٥) مادة رقم (٨٦) من قانون الجزاء الكويتي.
(١١٦) محمد أبو شادي: مرجع سابق، ص٢٠.
(١١٧) محمد أبو شادي: مرجع سابق، ص٢١.
(١١٨) سورة الزمر آية ٧.

بين الجرم وبين العقوبة، ويقدر ذلك بجسامة الفعل أو مدى الخطأ الذي ينسب إلى إرادة الفاعل[١١٩]. رابعاً: المساواة في العقوبة: أي لا يتم التمييز بين الأفراد حسب مراكزهم أو ميولهم فالجميع يقف على قدم المساواة أمام العقوبة، وهذا لا يتعارض مع الحرية التي أباحها القانون للقاضي أن يحكم بين الحد الأعلى أو الأدنى للعقوبة حسب ظروف كل قضية وملابساتها[١٢٠].

وبحسب الأصل ألا يسال الشخص جنائياً إلا عن الجرائم التي يرتكبها بنفسه أو يسهم فيها – كشريك – ومع ذلك قد يخرج المشرع عن هذه القاعدة الراسخة بأحوال خاصة وشروط معينة تفرضها الظروف فيقضي بمسؤولية الشخص عن جريمة ارتكبها غيره وهو ما يطلق عليه المسؤولية عن فعل الغير.

وحتى يسأل الشخص عن فعل الغير يشترط أن يكون عالماً بتوافر أركان الجريمة، واتجهت إرادته إلى المساهمة فيها[١٢١]. وقد أشارت محكمة النقض إلى مبدأ شخصية المسؤولية وجواز الاستثناء منه في عدة أحكام "من المقرر في التشريعات الحديثة ألا يسأل الإنسان بصفته فاعلاً أو شريكاً إلا عما يكون لنشاطه دخل في وقوعه من الأعمال التي نص القانون على تجريمها، سواء أكان ذلك بالقيام بفعل أم الامتناع الذي يجرمه القانون، ولا مجال للمسؤولية المفترضة أو المسؤولية التضامنية إلا استثناء وفي الحدود التي نص عليها القانون"[١٢٢]. ولا يتصور ذلك الاستثناء إلا في الجرائم العمدية التي يكون فيها العلم والإرادة، فالاستثناء لا يجوز أن يتوسع فيه كما ورد في المادة (٣٩) من القانون رقم ٢٠/ ٢٠١٤ بشأن التعامل الإلكتروني.

وفي تقديرنا أن هذا الرأي قد حمل النص أكثر مما يحتمل فهو يتناقض مع مبدأ شخصية العقوبة، فالجرائم العمدية لا يمكن أن تتحقق لمجرد الإهمال أو الإخلال بجانب الرقابة، ولكن يجب التأكد من توافر القصد الجنائي أولاً، كما يناقض ويخل بمبدأ الشرعية فلا يصح الاكتفاء بخطأ غير عمدي لتوقيع العقوبة المقررة لجريمة عمدية.

إن المشرع الكويتي أشار إلى المسؤولية عن فعل الغير بالنسبة لجرائم النشر في عقاب رئيس التحرير وكاتب المقال. كما في المادة رقم (٢٧) من قانون

(١١٩) محمد أبو شادي: مرجع سابق، ص٢١.
(١٢٠) محمد أبو شادي: مرجع سابق، ص٢١.
(١٢١) محمود مصطفى، مجلة الشرق الأدنى، عدد يناير سنة ١٩٦٨ ف ٥٢.
(١٢٢) مجموعة أحكام النقض (١٨ مايو، سنة ١٩٦٥، س١٦ رقم ٩٨) ص٤٨٢.

المطبوعات والنشر" مع عدم الإخلال بأي عقوبة أشد ينص عليها قانون آخر يعاقب رئيس التحرير وكاتب المقال أو المؤلف: ١ – إذا نشر في الصحيفة ما حظر في المادة (١٩) بالحبس مدة لا تجاوز سنة واحدة وغرامة لا تقل عن خمسة آلاف دينار ولا تزيد عن عشرين ألف دينار، أو بإحدى هاتين العقوبتين...."[١٢٣] لأن مسؤولية رئيس التحرير تقتضي العلم المفترض بما ينشر في صحيفته.

إن تفسير النصوص الجنائية والبحث في دلالاتها وألفاظها لمعرفة المعنى الذي يقصده المشرع ليس سهلاً. ففي بعض الأحيان يأتي النص عاماً وواضحاً فلا مشكلة تثور في مثل هذه الحالة، فالقاعدة تقول: "لا اجتهاد مع النص". أما إذا اتسم النص بالغموض أو كانت دلالات الألفاظ واسعة فمن الأولى الالتزام بروح القانون لا بعبارته. فمن الوارد ألا يوفَق المشرع في صياغة واختيار الألفاظ وبالتالي يبتعد التفسير عن معناه الحقيقي.

لذلك من الأولى البحث بأسلوب منطقي وتجاوز اللفظ إلى الغاية التي قصدها المشرع، فالوسيلة المثلى لتفسير النصوص هي البحث في معنى اللفظ والوقوف على إرادة المشرع وغايته معا. لذلك يقول أنتوليزي: "إن اللفظ هو نقطة البداية في التفسير وقصد المشرع هو نقطة الوصول"[١٢٤].

د – المطلب الرابع
الصلح في القانون رقم ٢٠/٢٠١٤ بشأن التعامل الإلكتروني

يعتبر الصلح سلاحاً ذا حدين، فهو يقصر مدد التقاضي ويخفف ازدحام القضايا في أروقة المحاكم، فالجاني قد يتعمد ارتكاب الجريمة معتمداً على علاقته القوية مع المجني عليه فيطلب الصلح، أو بالعكس يستغل المجني عليه يسار الجاني ويبتزه ليحصل على المال وبالتالي يتم الصلح.

أولاً – مفهوم الصلح:

وقد عرف القانون الكويتي الصلح في القانون الجنائي بأنه: نزول الهيئة الاجتماعية عن حقها في الدعوى الجنائية مقابل عفو المجني عليه عن التهم في الإطار الذي حدده المشرع الجزائي[١٢٥]. أما في القانون المدني: يعرف الصلح بأنه عقد يحسم به عاقداه

(١٢٣) قانون رقم ٣ لسنة ٢٠٠٦ في شأن المطبوعات والنشر (٢٠٠٦/٣).
(١٢٤) سمير الشناوي: مرجع سابق، ص٢٥٥.
(١٢٥) قانون رقم ١٧ لسنة ١٩٦٠ بإصدار قانون الإجراءات والمحاكمات الجزائية.

نزاعاً قائماً بينهما أو يتوقيان به نزاعاً محتملاً، وذلك بأن ينزل كل منهما على وجه التقابل عن جانبه من ادعائه. كما أن القانون الفرنسي[١٢٦] في المادة ٢٠٤٤ . يعرف الصلح: أنه "عقد يحسم به المتعاقدان نزاعاً قائماً أو يتوقيان به نزاعاً محتملاً". وعرف القانون المصري[١٢٧] الصلح في المادة (٦٣٥) "الصلح عقد به يترك كل من المتعاقدين جزءاً من حقوقه. على وجه التقابل لقطع النزاع الحاصل أو لمنع وقوعه".

كما أن للصلح الجنائي ركنين الأول التراضي والثاني محل الصلح. ويقصد بالتراضي: هو قبول الصلح من المجني عليه والسلطة القضائية. أما المحل: فهي الجريمة التي ارتكبها المتهم ضد المجني عليه.

ومن أهم مزايا الصلح: يسرع بإنهاء الخصومة، ويقلل من القضايا المنظورة أمام القضاء، ويحد من وصول النزاعات إلى درجات التقاضي الثلاث، ومن أهم سلبيات الصلح: الإخلال بمبدأ المساواة أمام القانون، فقد يفلت الجاني من العقاب، وقد يستخدمه البعض وسيلة للتمادي في الجرائم، ومن عناصر الصلح: الأركان العامة (رضا – محل – سبب). ووجود نزاع قائم أو محتمل، والنزول عن ادعاءات متقابلة. وأخيراً نية حسم النزاع[١٢٨].

الصلح القضائي: عندما يرى طرفا الخصومة في دعوى منظورة أمام القضاء أنه من الأفضل والأجدى لهما أن يصطلحا، وفي هذه الحالة قد يقدَّمان شفوياً الصلح الذي تم بينهما إلى المحكمة. وبالتالي على المحكمة أن تثبته كتابة في المحضر ولها أن تطلب من الخصمين أن يوَقَّعا عليه إذا رأت ذلك ضرورياً، أما إذا قَدَّما لها صلحاً مكتوباً تم بينهما، فعليها أن تأمر بضمه لمحضر الدعوى بعد أن تتأكد من أنه لا يتعارض مع القانون والآداب العامة.

الصلح غير القضائي: وقد يثور نزاع بين طرفين ولا ترفع بشأنه دعوى أمام القضاء ويعقد الطرفان بينهما صلحاً يحسم هذا النزاع منعاً من الالتجاء إلى القضاء، ويسمي هذا الصلح في هذه الحالة بالصلح غير القضائي، كما يجوز للمحكمة بناء على طلب الخصوم أن تصدر حكماً وفقاً لذلك الاتفاق بعد أن تقتنع بأنه لا يتعارض مع القانون والآداب العامة.

---

(١٢٦) القانون المدني الفرنسي مادة (٢٠٤٤).

(١٢٧) القانون المدني المصري مادة (٦٣٥).

(١٢٨) صفوت عوض كبلو، بحث قانوني معمق حول قضاء الصلح وأثره في إنهاء الخصومات في الشريعة الإسلامية والقانون الوضعي (١٩٩٥) http://www.mohamah.net.

ثانياً – الصلح في الفقه الإسلامي:

عقد رضائي يكفي في انعقاده التراضي بالإيجاب والقبول دون حاجة إلى اتباع شكل مخصوص، وقد يكون منجزاً أو مضافاً أو معلقاً على حسب الأحوال، والأمر كذلك بالنسبة في الفقه الوضعي: فالصلح عقد رضائي أيضا وإن كان التقنين المدني المصري قد اشترط الكتابة لإثباته، فإن الكتابة هنا للإثبات وليست ركناً للعقد، ويعتبر عقداً ملزماً للجانبين إذ ينشئ التزامات متقابلة في ذمة كل من الطرفين.

تعريف الخصومة: يقصد بالخصومة الحالة القانونية التي تنشأ منذ رفع الدعوى إلى القضاء، كما يقصد بها مجموعة الأعمال التي ترمي إلى تطبيق القانون في حالة معينة بواسطة القضاء، فالخصومة بهذا الاعتبار الأخير هي أداة تطبيق القانون بوساطة القضاء، وبعبارة أخرى أداة تحقيق الحماية القضائية، وتتميز الخصومة باعتبارها عملاً قانونياً مركباً. بمعنى أنها تبدأ وتسير وتنتهي سواء بحكم قضائي يفصل في الدعوي أو بغير حكم فيها بصرف النظر عن وجود الحق الموضوعي أو المركز القانوني الذي تحمله الدعوى، وأحياناً يصدر الحكم بناء على تصالح الخصوم من قضاء الصلح أو محاكم الصلح.

إن القوانين الوضعية الإجرائية تهتم بالصلح بين الخصوم وقد تجعل له محاكم أو مجالس خاصة بالصلح، كما في – فرنسا وجمهورية مصر العربية والجمهورية السورية – ففي فرنسا: يسمى قاضي الدرجة الأولى قاضي الصلح Juge de paix.

ثالثاً – الصلح حسب قانون هيئة أسواق المال ٧/٢٠١٠ وذلك لمقتضيات اقتصادية بحتة:

نصت المادة (١٣١) من قانون هيئة أسواق المال "يجوز للهيئة، في أي مرحلة من مراحل الدعوى الجزائية وإلى أن يصدر فيها حكم بات، عرض الصلح أو القبول به مع أي شخص ارتكب إحدى الجرائم المنصوص عليها في هذا القانون وذلك مقابل أداء مبلغ لا يقل عن الحد الأدنى للغرامة المقررة ولا يزيد عن الحد الأقصى، ويشترط للصلح..... رد قيمة أي منفعة محققة أو خسائر تم تجنبها، وألا يكون المتهم عائدا. وتحدد الهيئة المهلة التي يجب خلالها على المتهم استيفاء شروط الصلح طبقا للقواعد المتقدمة، وفي حال إتمام الصلح تنقضي الدعوى الجزائية". وقد تم وضع هذه المادة لضرورات اقتصادية بحتة، حيث إن سوق الأوراق المالية يعتبر عصب اقتصاد الدولة، والصلح هنا يؤدي إلى سرعة الفصل والتسوية حتى لا يزيد الضرر في حق الشركات والمساهمين.

إن نظام الصلح في قانون الإجراءات الجزائية يقرر من جهة (المجني عليه)

ومحدد في جرائم معينة (٢٤٠-٢٤١-٢٤٢) والنص عليه في قانون رقم ٢٠ لسنة ٢٠١٤ في شأن المعاملات الإلكترونية في المادة رقم (٤٢)[١٢٩] يتعارض مع قانون الجزاء. من حيث إن الصلح يقبل به المجني عليه الذي وقع عليه الضرر حسب الأصل، ولا يطلب من الجاني فقد يكون المضرور – المجني عليه – سحبت جميع أسرار شركته وذلك فيه إهدار لحقوق المجني عليه، فبدلاً من أن يتم الصلح بين الجاني والمجني عليه أشارت المادة (٤٢) من قانون رقم ٢٠ لسنة ٢٠١٤ في شأن المعاملات الإلكترونية إلى أن يدفع المتهم مبلغ ألف دينار كويتي للنيابة، ويدخل المال في خزينة الدولة وكأن القانون اختزل الأشخاص المعنوية في الدولة فقط.

وقد نصت المادة (٢٤١) من قانون الإجراءات الجزائية "يترتب على الصلح أو العفو الفردي ما يترتب على الحكم بالبراءة من آثار، ولكن في غير الجرائم التي يشترط لرفع الدعوى فيها شكوى المجني عليه، لا يترتب على الصلح أو العفو الفردي آثاره إلا بموافقة المحكمة. وإذا رغب المجني عليه في العفو عن المحكوم عليه أو الصلح معه بعد صدور حكم نهائي بإدانته، قدم طلباً بذلك إلى المحكمة التي أصدرت هذا الحكم لتنظر فيه وفقاً للأحكام السالفة الذكر". فهي التي تبيح الصلح فقط في جرائم معينة والتوسع في مفهوم الصلح يغل يد المشرع بتطبيق القانون على من يرتكب الأفعال المجرمة في المادة(٣٧) من قانون رقم ٢٠ لسنة ٢٠١٤ في شأن المعاملات الإلكترونية.

الخاتمة:

استعرضنا فيما سبق الحماية الجنائية للمعاملات الإلكترونية في قانون رقم ٢٠/٢٠١٤ من خلال زاويتن، الأولى: موضوعية وتحدثنا فيها عن الخصوصية المعلوماتية، واختلاف التشريعات الدولية في الحماية الجنائية للتعامل الإلكتروني، وما هو تعريف المستند الإلكتروني، والآثار المترتبة على المساواة التشريعية بين التعامل الإلكتروني والمستند الورقي، وماهي طرق الإثبات في التعامل الإلكتروني ومعوقات إثباته.

(١٢٩) المادة رقم (٤٢) من قانون رقم ٢٠ لسنة ٢٠١٤ في شأن المعاملات الإلكترونية "يجوز للنيابة العامة قبول طلب الصلح ممن ارتكب للمرة الأولى جريمة من الجرائم المنصوص عليها في هذا القانون، متى قام المتهم بتقديم طلب الصلح للنيابة العامة ودفع مبلغ ألف دينار لخزينة المحكمة قبل إحالة الدعوى للمحكمة المختصة، ويترتب على قبول الصلح انقضاء الدعوى الجزائية وجميع آثارها".

أما الزاوية الثانية: فهي الجانب الإجرائي وفيها تطرقنا إلى تصنيف الجرائم الجنائية في قانون المعاملات الإلكترونية وتقسيماتها، ثم ميزنا بين مسؤولية الشخص الاعتباري وجريمة الإهمال والإخلال بالواجبات، وماهي حدود الشخص المعنوي، ثم تحدثنا عن أهل الضبطية القضائية، جهة التحقيق، جهة التحري والاستدلال في القانون رقم ٢٠/٢٠١٤ بشأن التعامل الإلكتروني، وأخيراً ما هو الصلح المقصود في قانون رقم ٢٠ لسنة ٢٠١٤ في شأن المعاملات الإلكترونية.

إن التطور السريع للإنترنت والزيادة غير المسبوقة في عدد مستخدمي البرامج والتطبيقات الإلكترونية خلق نوعاً من التحدي للمشرع القانوني بضرورة الإسراع والعمل على سن قوانين تحقق الردع العام والخاص وتحفظ الخصوصية للأفراد.

وباستقراء القوانين في الدول الأوروبية نجدها أسرع في التعامل مع المستجدات القانونية التي تكون متعلقة بالتعامل الإلكتروني، وتأتي الدول النامية بدرجة ثانية. ولاتزال بعض الدول العربية تسير ببطء شديد ولم تضع تشريعاً مستقلاً يحدد الأفعال التي يعاقب عليها القانون إذا تم هذا الفعل من خلال الوسائط الإلكترونية.

وقد حرصت دولة الكويت على مواكبة التطور فوضعت تشريعاً قانونياً خاصاً بالتعامل الإلكتروني، ويمكن تلخيص أهم ملامح قانون رقم ٢٠/٢٠١٤ بشأن المعاملات الإلكترونية بالآتي:

يعطي القانون حجية الإثبات للمعاملات الإلكترونية وللتوقيع الإلكتروني في نطاق المعاملات المدنية والإدارية والتجارية، ليكون لهما نفس الحجية في الإثبات للتوقيع والكتابة العادية. كما عرَف المحرر الإلكتروني وتم إعطاؤه نفس مفهوم المحرر الكتابي. شمول التوقيع الإلكتروني جميع المعاملات التي يجوز إتمامها إلكترونياً وهي المعاملات المدنية والإدارية والتجارية وفقاً للشروط والضوابط التي وضعها القانون ولائحته التنفيذية.

كما شدد القانون رقم ٢٠/٢٠١٤ بشأن المعاملات الإلكترونية بالنسبة للجهات التي ستقوم بتقديم خدمات التصديق الإلكتروني بضرورة الحصول على التراخيص المطلوبة من الجهة المختصة لضمان صحة وسلامة المعاملات الإلكترونية. وأخيراً وضع القانون المبادئ والشروط العامة الأساسية لتنظيم التعامل الإلكتروني، وترك الضوابط الفنية للائحة التنفيذية التي وضعت الشروط الفنية والتفصيلات الخاصة بكل معاملة.

ونحن نرى إنه من المناسب أن يحدد المشرع الكويتي بصورة واضحة الخطأ

بالمعنى الواسع؛ لأن التطبيق العملي قد يتعذر على القاضي التحقق من صورة الخطأ الذي يحدد المسؤولية الجنائية وهو ما يمتد أثره السلبي على العدالة بوجه عام.

وفي تقديرنا أن المشرع قد خلط بهذا القانون رقم ٢٠ لسنة ٢٠١٤ في شأن المعاملات الإلكترونية مع بعض الضمانات الدستورية، كما أنه لم يراعِ بعض المبادئ العامة والمستقرة في قانون الجزاء ومنها شخصية العقوبة، كما أنه قد ساوى في العقوبة بالنسبة للجريمة العمدية وغير العمدية.

كما أقام المسؤولية التضامنية على الشخص المعنوي على غير أساس، وخفض عقوبة التزوير في محرر رسمي إلكتروني إلى جنحة، وكما هو معلوم إن جريمة التزوير في محرر رسمي تعتبر جناية، ففعل التزوير واحد وكلاهما محرر رسمي إلا أن الفرق بينهما أن أحدهما إلكتروني وهو ما خفف فيه المشرع العقوبة وكان من الأولى التشديد. وخرج المشرع عن القواعد العامة في الصلح وهو أمر قد يسفر عن صعوبة التطبيق أو إفلات بعض الجناة من العقاب. ومما لا شك فيه إن القانون يعتبر مزيجاً من الجوانب العملية والنظرية، فهو تصارع بين ما هو كائن وبين ما هو مفترض أن يكون(١٣٠). لذا كان لزاماً علينا أن نبين هذه الملاحظات على وجه الدقة والله ولي التوفيق.

أهم التوصيات:

١ – لدى جميع الدول قناعة تامة في أن مخاطر الخصوصية المعلوماتية قد زادت بشكل ملحوظ في السنوات الخمس الأخيرة؛ لذا صار لزاماً عليها سن تشريعات تجرم أفعال التعدي وتنظم التعامل الإلكتروني، وتعتبر ظاهرة عدم التوافق التقني وتباين التشريعات بين الدول من أهم المعوقات التي تقرر الحماية الجنائية للتعامل الإلكتروني، بل وتهدده دائماً، غير أن دخول الدول في اتفاقيات ومعاهدات مشتركة يسهل من الحصول على أرضية مشتركة في التجريم مما يسهل القبض على الجاني.

٢ – هذا التزايد في الجرائم المعلوماتية وانتهاك الخصوصية زاد العبء على المحققين ورجال الشرطة والقضاء، وبالتالي صار من الضروري أن تستعين الحكومات وتلجأ إلى خبراء للتعامل مع البيانات والمعلومات كأدلة جنائية رقمية.

---

(١٣٠) مشاعل عبد العزيز الهاجري، قلاع وجسور الدراسات البينية وأثرها في الاتصال بين الحقول المعرفية – دراسة في القانون بوصفه حقلاً معرفياً مستقلاً وعلاقته بغيره من العلوم (مجلة الحقوق، جامعة الكويت، مجلس النشر العلمي، العدد ٣، السنة ٣١ سبتمبر، ٢٠٠٧) ص١٩٦.

٣ – تعتبر المعاملات الإلكترونية ذات ثقة ومصداقية في الإثبات ويعتد بها كدليل إذا تمت بالشروط التي حددها القانون، وهو ما سيحدث نقلة نوعية في اختصار الوقت[١٣١] والجهد على كافة الأصعدة.

٤ – ضرورة إنشاء وحدات للتحقيق في جرائم المعلومات بالقدر الذي لا يخرق الضمانات الدستورية ولا يتعدى فيه على حرية الأفراد. وكذلك تعزيز التدابير الاحتياطية التي تحفظ أمن المعلومات والبيانات الشخصية وكذلك التعامل الإلكتروني. والعمل على إنشاء مختبرات للبحث التقني وتقصي الأدلة الرقمية ومختبرات للذكاء الاصطناعي ولاستفادة منها في مجال الأدلة الجنائية الرقمية.

٥ – العمل على نشر الوعي والثقافة والمعرفة بين الناس والهيئات والشركات بأهمية الخصوصية المعلوماتية، فالاعتماد على سن القوانين وتغليظ العقوبات فقط لا يكفي، خصوصاً في ظل المناداة بالحكومة الإلكترونية الخالية من الأوراق.

٦ – إيجاد أنظمة حماية قوية من خلال العمل المنظم باتخاذ نسخ احتياطية[١٣٢] وتخزينها في الخارج ووضع التدابير الاحتياطية في حالة حدوث أي اختراق أمني للنظام أو كوارث طبيعية.

٧ – الإعداد العلمي لرجال الشرطة والمحققين ووكلاء النيابة وتزويدهم بالمعرفة الفنية بهذا النوع من الجرائم، وكذلك إحاطة الخبراء الفنيين بالأمور والإجراءات القانونية. وعقد الدورات التدريبية المشتركة بهدف تبادل الخبرات والعمل بروح الفريق الواحد.

٨ – كما نوصي بضرورة عمل قاعدة بيانات تتبع مجلس وزراء الداخلية العرب وزيادة الجهود الدولية في مجال مكافحة الجريمة، والتعرف على أصول ونظريات تقنية المعلومات الحديثة، وبالتالي تنظيم عملية بناء وجمع الأدلة بالقدر الذي يحفظ الحقوق الدستورية وسرية التعامل الفردية، لأنه في مثل هذه الجرائم غالباً ما يكون فيها مصطلحات تكنولوجية خاصه وأمور برمجية يصعب على الشخص المعتاد فهمها.

---

(١٣١) تعتبر حكومة دبي رائدة الخليج في التعاملات الإلكترونية وهي في المرتبة الـ٢٢ عالمياً بحسب تقرير ممارسة الأعمال الصادر من البنك الدولي عام ٢٠١٣، كما أن إنجاز الرخصة التجارية في دبي لا يستغرق أكثر من نصف ساعة.

(١٣٢) يوجد بنوك خاصة بحفظ المعلومات والبيانات مهمتها تخزينها وحمايتها حتى ضد الحريق والظروف القاهرة كالزلازل والأعاصير وغيرها. وتقوم وزارة الداخلية في الكويت بحفظ جميع المعاملات الموثقة من خلال أجهزتها على شكل نسخ احتياطية خارج البلاد وذلك بهدف حمايتها.

٩ – إيجاد شرطة ونيابة متخصصة وتدريب الكوادر: طبيعة الجرائم ذات الصلة بالحاسب الآلي تقتضي معرفة متميزة بنظم الحاسبات، وكيفية تشغيلها، ووسائل إساءة استعمالها من قبل مستخدميها، ولن تتحقق هذه المعرفة إلا بالتدريب والتعليم لمباشرين للتحقيق في مجال الجرائم الإلكترونية، إلى الحد الذي دعا البعض إلى القول بضرورة وجود شرطة متخصصة(١٣٣)، ونيابة متخصصة في هذا المجال.

ويجب أن يشتمل التدريب على كيفية تشغيل الحاسبات، بعد التعرف على أنواعها ونظمها المختلفة، لاكتساب مهارات ومعارف تتعلق ببرمجة الحاسبات، والمعالجة الإلكترونية للبيانات والجرائم التي تقع على الحاسبات، أو تستخدم الحاسبات وسيلة لارتكابها، وأساليب ارتكاب هذا النوع من الجرائم، مع دراسة حالات تطبيقه لجرائم وقعت سلفاً، وكيف تم مواجهتها. كما هو الحال في أمريكا وإنجلترا، وكندا.

١٠– في نطاق سياسة تجريم ظاهرة الاعتداء على الثقة العامة في مجال التعامل الإلكتروني نجد أن المشرع الكويتي حرص على فكرة الثقة الإيجابية والحماية المادية والمعنوية. لذلك نرى أنه من الملائم أن يقرر المشرع الكويتي سريان بعض الأحكام والقواعد على الأفعال التي ترتكب في الخارج إذا كان من شأن هذه الأفعال المساس بالثقة العامة للتعامل الإلكتروني حتى لا يفلت الجاني من العقاب.

١١– هناك حاجة غير محدودة لخبراء البحث التقني، وتأتي الصعوبة في استقطابهم للعمل في مجال العدالة الجنائية والجرائم الإلكترونية، وهو أمر يمثل تحدياً كبيراً أمام الحكومات، فيجب إعطاء الخبراء في مجال البحث التقني المزيد من الأهمية وتوفير الحوافز المالية وكل ما يحتاجونه حتى لا ينفروا من العمل في مجال العدالة الجنائية الذي فيه الكثير من المسؤولية.

١٢– الحكومة الإلكترونية اليوم أصبحت دليل تطور الشعوب وقيادتها الحكومية، فتسعى الدول المتطورة إلى وضع جميع المعاملات الإدارية الحكومية والمدنية والتجارية بشكل عام بطريق إلكتروني خالي من الأوراق مما يوفر في عدد الموظفين وازدحام الطرقات ويسهل على الناس معيشتهم، ويستهدف هذا كله رفع كفاءة العمل الإداري، والارتقاء بمستوى أداء الخدمات الحكومية بما يتفق مع إيقاع العصر.

---

(١٣٣) أنشأت وزارة الداخلية في الكويت إدارة مكافحة الجرائم الإلكترونية وتهدف إلى الكشف عن الجرائم الإلكترونية مثل إتلاف وتشويه البيانات والمعلومات الخاصة بالأفراد والمؤسسات أو انتحال الشخصية.

قائمة المراجع

أولاً – اللغة العربية:

أ – الكتب والرسائل العلمية والمجلات:

١ – إبراهيم أبو الليل، الجوانب القانونية للتعاملات الإلكترونية (٢٠٠٣).

٢ – أحمد حبيب السماك، قانون الإجراءات والمحاكمات الجزائية (الكويت: وزارة الداخلية أكاديمية سعد العبد الله للعلوم الأمنية).

٣ – أحمد رشيد المطيري، محمد سليمان الرشيدي، المبادئ العامة للقانون (الطبعة الرابعة، ٢٠٠٩).

٤ – أشرف توفيق شمس الدين، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، منظم المؤتمر: أكاديمية شرطة دبي، مركز البحوث والدراسات رقم العدد: ١ السنة: ٢٠٠٣ تاريخ الانعقاد: ٢٦ نيسان ٢٠٠٣ تاريخ الإنهاء: ٢٨ نيسان ٢٠٠٣ الدولة: دبي – الإمارات العربية المتحدة.

٥ – إقبال القلاف، مبادئ قانون الإجراءات الجزائية في القانون الجزائي الكويتي (الكويت: دار العلم، الطبعة الأولى، ٢٠٠٥).

٦ – الشحات إبراهيم محمد منصور، الجرائم الإلكترونية في الشريعة الإسلامية والقوانين الوضعية بحث فقهي مقارن (الإسكندرية: دار الفكر الجامعي، ٢٠١١).

٧ – بلال أمين زين الدين، جرائم نظم المعالجة الآلية للبيانات في التشريع المقارن والشريعة الإسلامية (الإسكندرية: دار الفكر الجامعي، ٢٠٠٨).

٨ – ثروت عبد الحميد، التوقيع الإلكتروني، ماهيته، مخاطره، وكيفية مواجهتها، مدى حجيته في الإثبات (دار الجامعة الجديدة، ٢٠٠٧).

٩ – حازم حسن أحمد متولي، الحماية الجنائية للثقة العامة في المعاملات التجارية الإلكترونية في التشريع الإماراتي، (مجلة الفكر الشرطي، المجلد رقم ٢٣، العدد رقم ٩١، أكتوبر ٢٠١٤).

١٠– حسن طاهر داوود، جرائم نظم المعلومات (الرياض: الطبعة الأولى، ٢٠٠٠).

١١– خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية (الدار الجامعية، ٢٠٠٨).

١٢– رمسيس بهنام، النظرية العامة للقانون الجنائي؛ (منشأة المعارف، الإسكندرية، الطبعة الثالثة، ١٩٩٧).

١٣– سمير الشناوي، النظرية العامة للجريمة والعقوبة في قانون الجزاء الكويتي دراسة

مقارنة قانون العقوبات المصري والفرنسي والألماني والنرويجي الكتاب الأول الجريمة (الكويت: وزارة الداخلية، كلية الشرطة، ١٩٨٨).

١٤- سمير الشناوي، النظرية العامة للجريمة والعقوبة في قانون الجزاء الكويتي دراسة مقارنة قانون العقوبات المصري والفرنسي والألماني والنرويجي الكتاب الثاني المسؤولية الجنائية والعقاب (الكويت: وزارة الداخلية، كلية الشرطة، ١٩٨٨).

١٥- صفوت عوض كبلو، بحث قانوني معمق حول قضاء الصلح وأثره في إنهاء الخصومات في الشريعة الإسلامية والقانون الوضعي (١٩٩٥).

١٦- عبد المنعم فرج الصده، أصول القانون العام (القاهرة: ١٩٧٢).

١٧- عبد الوهاب حومد، الوسيط في الإجراءات الجزائية الكويتية (الكويت: جامعة الكويت، الطبعة الرابعة).

١٨- فايز عايد الظفيري، قانون الجزاء الخاص (الكويت: وزارة الداخلية الإدارة العامة للتدريب).

١٩- مجدي عز الدين يوسف، أصول القانون الإداري أسس التنظيم الإداري وسائل الإدارة العامة في القانون المقارن والكويتي (الكويت: وزارة الداخلية أكاديمية سعد العبد الله للعلوم الأمنية).

٢٠- مجموعة أحكام النقض (١٨مايو، سنة ١٩٦٥، س١٦ رقم ٩٨).

٢١- مجموعة القواعد التي قررتها محكمة التمييز عن المدة من ١/١٩٢ حتى ٩٦/١٢/٣١، القسم الثالث (المجلد الأول، يوليو، ١٩٩٩).

٢٢- محمد أبو شادي، مبادئ علم العقاب دراسة مقارنة لطبيعة العقوبة والتدبير الاحترازي وأساليب التنفيذ العقابي مع التطبيق لأحكام القانون رقم ٢٦ لسنة ١٩٦٢بتنظيم السجون في الكويت (الكويت: وزارة الداخلية أكاديمية سعد العبد الله للعلوم الأمنية، ١٩٩٣).

٢٣- محمد الأمين البشرى، الجرائم الإلكترونية التحقيق الادعاء المحاكمة ومعاملة المذنبين فيها (الإمارات العربية المتحدة، حكومة دبي، ٢٠١٢).

٢٤- محمود مصطفى، مجلة الشرق الأدنى، عدد يناير، سنة ١٩٦٨، ف٥٢.

٢٥- محمود نجيب حسني، شرح قانون العقوبات القسم العام (دار النهضة العربية، الطبعة السادسة، ١٩٨٩).

٢٦- مشاعل عبد العزيز الهاجري، قلاع وجسور الدراسات البينية وأثرها في الاتصال بين الحقول المعرفية – دراسة في القانون بوصفه حقلاً معرفياً مستقلاً وعلاقته

بغيره من العلوم (جامعة الكويت: مجلة الحقوق، مجلس النشر العلمي، العدد ٣، السنة ٣١، سبتمبر، ٢٠٠٧).

٢٧- نبيل محمد أحمد صبح، حماية المستهلك في التعاملات الإلكترونية – دراسة مقارنة (جامعة الكويت: مجلة الحقوق، مجلس النشر العلمي، العدد ٢، السنة ٣٢، يونيو، ٢٠٠٨).

ب – القوانين

١ – الدستور الكويتي ١٩٦٢.

٢ – قانون رقم ١٦ لسنة ١٩٦٠ بإصدار قانون الجزاء.

٣ – قانون رقم ١٧ لسنة ١٩٦٠ بإصدار قانون الإجراءات والمحاكمات الجزائية.

٤ – قانون رقم ٢٠ لسنة ٢٠١٤ في شأن المعاملات الإلكترونية.

٥ – قانون رقم ٣ لسنة ٢٠٠٦ في شأن المطبوعات والنشر.

٦ – الدستور المصري.

٧ – القانون المدني المصري.

٨ – اللائحة التنفيذية الخاصة بالقانون رقم ٢٠ لسنة ٢٠١٤ في شأن المعاملات الإلكترونية.

٩ – محاضر اجتماعات لجنة الدستور والمجلس التأسيسي.

ثانياً – اللغة الإنجليزية:

1 - Convention on Cybercrime, Budapest, 23.XI.2001.

2 - Deva Vasua, E-Crime and Remedies. Delhi:Saujanya Book, 2005.

3 - The Universal Declaration of Human Rights (UDHR).

4 - John R. Vacca: Computer Forensics- Computer Crime Scene Investigation (Snd.ed) Massachus -Etts. Charles River Midia. 2005.

5 - Philip Virgo,Eurim,2003,Auailable at www.zdnet.co.uk.

6 - Power, Richard: Curvent and Future Danger, San Francisco: Computer Security Institute 1995.

7 - Rigaux(M) et Trouss (P.E): Les Crimes et les delits du code penal.T2.Bruxelles-Paris1952.p.455.

8 - http://aawsat.com/home/article/373401.

9 - http://unctad.org/en/Pages/Home.aspx.

10 - http://www.mohamah.net.

11 - http://www.alyaum.com/article/4071469.

12 - https://www.moj.gov.kw/sites/ar/PublicProsecution/pages/defaul-t.aspx.

13 - http://www.kna.kw/clt/run.asp?id=1658#sthash.-WAQMpFGW.dpuf.

ثالثاً – اللغة الفرنسية:

١ – القانون الفرنسي الصادر في ٩ يوليو١٩٧٥، المادة ٣/١٣٧٤ مدني فرنسي.

٢ – قانون العقوبات الفرنسي المادة (٤١٨).