جرائم الاعتداء على الحياة الخاصة في مجال المعلوماتية

دراسة مقارنة في التشريع اليمني والتشريع الجزائري

إعداد /

دكتور/ فايز محمد راجح غلاب

أستاذ القانون الجنائي المساعد بأكاديمية الشرطة

2019م

ملخص:

يكتسب موضوع جرائم الاعتداء على الحياة الخاصة في مجال المعلوماتية أهمية كبيرة؛ خاصةً مع تزايد الاعتداء على الحياة الخاصة بواسطة الوسائل الإلكترونية، كما تظهر أهمية هذا البحث أيضاً في بيان دور القانونين اليمني والجزائري في مواجهة هذا النوع من الجرائم.

ويهدف هذا البحث إلى بيان أركان جريمة الاعتداء على الحق في الحياة الخاصة في مجال المعلوماتية، ومعرفة مدى إمكانية تطبيق النصوص القانونية في التشريعين اليمني والجزائري على هذه الجرائم.

وقد تم تقسيم هذا البحث إلى مطلبين، تم تخصيص المطلب الأول منه لبيان أركان جريمة الاعتداء على الحق في الحياة الخاصة، وتم تخصيص المطلب الثاني لمعرفة مدى إمكانية تطبيق النصوص القانونية في التشريعين اليمني والجزائري على جرائم الاعتداء على الحياة الخاصة في مجال المعلوماتية.

وقد اعتمدت في كتابة هذا البحث على المنهج الوصفي التحليلي، وكذا المنهج المقارن، ثم اختتمت البحث بمجموعة من النتائج والتوصيات.

Abstract

The subject of crimes of assault on private life in the field of informatics is of great importance, especially with the increasing assault on private life by electronic means. This research also shows the importance of the role of Yemeni and Algerian laws in confronting this type of crime.

This research aimed to explain the elements of the crime of assaulting the right to private life in the field of informatics, and to know the extent to which the legal provisions in the Yemeni and Algerian legislation can be applied to these crimes.

This research was divided into two requirements, the first of which was devoted to the elements of the crime of assault on the right to private life, and the second request was devoted to the extent to which the legal provisions in the Yemeni and Algerian legislation can be applied to crimes of assault on private life in the field of informatics.

It was based on the descriptive analytical method and the comparative approach in writing this research and then concluded with a set of conclusions and recommendations.

مقدمة:

الحمد الله رب العالمين، نحمده تعالى، ونستعينه ونستهديه، ونعوذ بالله من شرور أنفسنا ومن سيئات أعمالنا، من يهده الله فهو المهتد ومن يضلل فلن تجد له ولياً مرشداً. أما بعد:

يعني الحق في الخصوصية وفقاً للمفهوم التقليدي: "عدم إجراء التفتيش المادي للشخص وممتلكاته، وحقه في الابتعاد والعزلة عن الناس"، ويعني بالمفهوم الواسع: "كل ما يحب الشخص أن يجعله من أسراره وخصوصياته"[1].

وقد تطور مفهوم الحق في الخصوصية في ظل التقدم التكنولوجي بما يضمن حماية كل ما يتم تجميعه أو تخزينه في أنظمة المعالجة الآلية للمعطيات ويتعلق بالحياة الخاصة.

ولا شك فإن التطور التقني في مجال تقنية المعلومات قد قدّم فوائد كثيرة في شتى مجالات الحياة المختلفة للفرد والمجتمع والدولة وللعلاقات الدولية وعلاقات الشركات والمؤسسات والأفراد، وهذا ما أوجد ما يعرف ببنوك المعلومات (Data Bank)، والتي قد تكون مقصورة على بيانات ومعلومات تتصل بقطاع بعينه، وقد تكون شاملة لمختلف الشؤون والقطاعات، كما أنها قد تكون مهيأة للاستخدام على المستوى الوطني العام، وقد تكون كذلك مهيأة للاستخدام الإقليمي أو الدولي، وذلك ما سهل التعامل بدرجة كبيرة عما كان عليه الوضع في السابق؛ فأصبح العالم كأنه يعيش في محيط اجتماعي واحد لا يجد صعوبة في التعامل من خلال الحدود الجغرافية التي أصبحت مفتوحة في ظل العالم الافتراضي[2]، إلا أن ذلك التطور من ناحية أخرى قد أضحى يهدد الحياة الخاصة بالخطر، من خلال تخزين واسترجاع وتحليل كميات هائلة من البيانات الشخصية التي يتم تجميعها من قبل الهيئات والمؤسسات والدوائر الحكومية والشركات الخاصة، وما ينتج عن ذلك من معاملات يتم من خلالها نقل تلك المعلومات من مؤسسة إلى أخرى ومن دولة إلى أخرى، وبالتالي فإن تلك المعلومات قد تكون عرضة للانتهاك ما بين الحين والآخر.

وقد اهتمت معظم التشريعات في حماية الحياة الخاصة من الانتهاك، بل أن بعض التشريعات الحديثة قد تناولت حماية الحياة الخاصة في مجال المعالجة الآلية للمعطيات.

([1]) د. محمود أحمد عباينة، جرائم الحاسوب وأبعادها الدولية، رسالة ماجستير، الجامعة الأردنية، دار الثقافة، عمان، الأردن، 2005، ص70.

(2) د. أحمد خليفه الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2005، ص97، د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، ط1، 1992، ص43.

فهل النصوص التشريعية في القانون اليمني والجزائري تفي بحماية الحياة الخاصة بما فيها البيانات المخزنة في نظم المعالجة الآلية للبيانات وقواعد البيانات؟ أم أن الأمر يستدعي تشريع أو نصوص قانونية تتناسب مع حداثة الجريمة؟ وما هي الأركان التي تقوم عليها تلك الجريمة؟ ذلك ما سيتم تناوله في هذا البحث.

أولاً: مشكلة البحث:

تكمن مشكلة البحث في أننا أمام انتهاك للحياة الخاصة بشكلها الافتراضي والتي تختلف عن الانتهاكات التي كانت تتم في الوضع المادي ويتم إثباتها بطرق مادية ويمكن مواجهتها من خلال القوانين التقليدية.

وذلك يثير التساؤل الآتي: هل جريمة الاعتداء على الخصوصية في مجال المعلوماتية تتطابق مع الافعال التي يمكن أن ترتكب بها الجريمة بصورتها التقليدية؟

وهل تفي النصوص القانونية التقليدية لمواجهة هذا النوع من الجرائم؟ أم أننا بحاجة إلى نصوص قانونية جديدة للتعامل مع الجريمة بصورتها الافتراضية؟

ثانياً: أهمية البحث:

تبدو أهمية هذا البحث في كونه يسلط الضوء على موضوع الحق في الخصوصية، والمخاطر التي تهدد الحياة الخاصة، وبيان موقف التشريع اليمني والتشريع الجزائري في حماية الحياة الخاصة من الانتهاكات؛ خاصةً في المجال الإلكتروني، كما تتجلى أهميته في كون مثل هذه البحوث تساهم في إيجاد توعية رقمية في أمن المعلومات يعتمد على الوعي في كيفية الحفاظ على البيانات الشخصية في أجهزة الحاسوب وأنظمة المعالجة الآلية للمعطيات.

ثالثاً: أهداف البحث:

يهدف هذا البحث إلى تحقيق الآتي:

1. التعرف على أركان جريمة الاعتداء على الحق في الحياة الخاصة بصورتها التقليدية وفي مجال المعلوماتية.
2. بيان مدى انطباق النصوص القانونية في التشريعين اليمني والجزائري ومواجهتهما لجرائم الاعتداء على الحياة الخاصة في مجال المعلوماتية.

رابعاً: منهج البحث:

اعتمدت هذه الدراسة بالدرجة الأساسية على المنهج الوصفي التحليلي؛ من خلال جمع المادة العلمية من المراجع المتخصصة ووصفها وتحليلها، مع استخدام المنهج المقارن بين التشريعات محل الدراسة – اليمني والجزائري – لبيان أوجه التشابه والاختلاف بينهما بشأن موضوع البحث.

خامساً: خطة البحث:

سنقوم بتقسيم هذا البحث إلى مطلبين، على النحو الآتي:

المطلب الأول: أركان جريمة الاعتداء على الحق في الحياة الخاصة.

المطلب الثاني: مدى إمكانية تطبيق النصوص القانونية التقليدية على جرائم الاعتداء على الحياة الخاصة في مجال المعلوماتية.

المطلب الأول

أركان جريمة الاعتداء على الحق في الحياة الخاصة

جريمة الاعتداء على الحق في الخصوصية مثلها مثل غيرها من الجرائم التي تتطلب لاكتمالها توافر أركانها، سواءً الركن المادي أو الركن المعنوي، مع عدم إغفال الركن الشرعي الذي يُعد مناط التجريم في ظل وجود جريمة مستحدثة في نطاق المعلوماتية ووجود نصوص قانونية تقليدية كانت تتناسب مع واقع مادي ملموس، وهذا ما سنتناوله في هذا المطلب؛ من بيان أركان جريمة الاعتداء على الحق في الحياة الخاصة في الجانب التقليدي في النصوص القانونية في القانون اليمني والقانون الجزائري، ونقارنها في الجانب المعلوماتي لإيضاح الفرق، وفي نهاية المطلب نتطرق لعقوبة الجريمة في القانون اليمني والجزائري، وذلك على النحو الآتي:

أولاً: الركن الشرعي للجريمة:

جريمة الاعتداء على الخصوصية وإفشاء الأسرار في مجال المعلوماتية مثلها مثل غيرها من الجرائم تتطلب لقيامها توافر الركن الشرعي للجريمة[1]، ومن خلال الركن الشرعي تتضح صور الجريمة بشكلها التقليدي، وبالمقارنة تتضح صور الجريمة بشكلها المستحدث من خلال ما سيتم عرضه.

نصت العديد من المواد في القانون اليمني والقانون الجزائري على ذلك، ومن تلك النصوص المواد (255، 256، 257، 258) من قانون الجرائم والعقوبات اليمني، والمواد (303، 303 مكرر، 303 مكرر1) من قانون العقوبات الجزائري. حيث نصت المادة (255) من قانون الجرائم والعقوبات اليمني على أنه: "يعاقب بالحبس مدة لا تزيد على سنة أو بغرامة من فتح بغير حق خطاباً مرسلاً إلى الغير أو احتجز رسالة أو برقية هاتفية، ويعاقب بالعقوبة ذاتها من اختلس أو أتلف إحدى هذه

(1) ثار خلاف بين الفقهاء حول مدى اعتبار الركن الشرعي أحد أركان الجريمة، مابين معارض ومؤيد، فبينما يرى أصحاب الاتجاه المعارض: بأن النص القانوني هو عامل ردع، أو شرط أساسي للجريمة، ولا يعد أحد أركانها، لأنه هو الذي يخلقها وليس من الصواب بأن من يخلق يعد جزء ممن يخلقه، ومن ناحية أخرى فإنه إذا ما اعتبر النص القانوني ركن في الجريمة فينبغي إحاطة الجاني به، ويترتب على ذلك انتفاء الجريمة في حالة عدم العلم به، بينما يرى أصحاب الاتجاه المؤيد: بان الركن الشرعي يُعد أحد أركان الجريمة، إذ لا جريمة بدون نص، وهذا الرأي يُعد الصواب من وجهة نظرنا بدليل أن أي ظاهره أو فعل لا يكون مجرماً بنص قانوني يُعد فعلاً مباحاً، ولا يمكن العقاب عليه، وبالنظر كذلك إلى الخلاف الفقهي والقضائي حول مدى خضوع جرائم المعلوماتية ومنها المتعلقة بالحياة الخاصة؛ وخاصة المستحدثة، بحيث يجعلها البعض خارج نطاق التجريم ليؤكد بأن النص القانوني يُعد أحد أركان الجريمة، وأن القول بعدم معرفة الجاني للنص ينفي قيام الجريمة وفقاً للرأي الأول يتعارض مع القاعدة المعروفة" لا يُعذر من يدعي الجهل بالقانون". لمزيد من التفصيل راجع: أحسن بوسقيعة، الوجيز في القانون الجنائي العام، الديوان الوطني للأشغال التربوية، الجزائر، 2002، ص47، 48.

المراسلات، أو أفضى بمحتوياتها إلى الغير ولو كانت الرسالة قد أرسلت مفتوحة أو فتحت خطأ أو مصادفة، ويقضى بالحبس مدة لا تزيد على سنتين أو بالغرامة إذا ارتكبت الجريمة من موظف عام إخلالاً بواجبات وظيفته"[1].

ويقابلها نص المادة (303) من قانون العقوبات الجزائري، حيث نصت على أنه: "كل من يفض أو يتلف رسائل أو مراسلات موجهة إلى الغير وذلك بسوء نية في غير الحالات المنصوص عليها في المادة (137) يعاقب بالحبس من شهر واحد إلى سنة واحدة وبغرامة من 25.000 دج إلى 100.000 دج أو بإحدى هاتين العقوبتين"[2].

كما تنص المادة (256) عقوبات يمني على أنه: "يعاقب بالحبس مدة لا تزيد على سنة أو بالغرامة كل من اعتدى على حرمة الحياة الخاصة وذلك بأن ارتكب أحد الأفعال الآتية في غير الأحوال المصرح بها قانوناً أو بغير رضاء المجني عليه:

1- استرق السمع أو سجل أو نقل عن طريق جهاز من الأجهزة أياً كان نوعه محادثات جرت في مكان خاص أو عن طريق الهاتف.

2- التقط أو نقل بجهاز من الأجهزة أياً كان نوعه صورة شخص في مكان خاص.

فإذا صدرت الأفعال المشار إليها في الفقرتين السابقتين أثناء اجتماع على مسمع أو مرأى من الحاضرين في ذلك الاجتماع فإن رضاء هؤلاء يكون مفترضاً. ويعاقب بالحبس مدة لا تزيد على ثلاث سنوات أو بالغرامة الموظف العام الذي يرتكب أحد الأفعال المبينة بهذه المادة اعتماداً على سلطة وظيفته. ويحكم في جميع الأحوال بمصادرة الأجهزة وغيرها مما يكون قد استخدم في الجريمة كما يحكم بمحو التسجيلات المتحصلة عنها أو إعدامها"[3].

ويقابل هذا النص ما ورد في قانون العقوبات الجزائري في المادة (303) مكرر والتي نصت على أنه: "يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 50.000 دج إلى 300.000 دج كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأية تقنية كانت وذلك:

3- بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية، بغير إذن صاحبها أو رضاه.

4- بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص، بغير إذن صاحبها أو رضاه.

([1]) القانون رقم 12 لسنة 1994 بشأن الجرائم والعقوبات اليمني.

([2]) القانون رقم (06 – 23) المؤرخ في 20 ديسمبر 2006 المعدل والمكمل لقانون العقوبات. وهذا النص يجرم فض أو إتلاف رسائل مرسله إلى الغير بسوء نية من أي شخص كان، بخلاف الحالات التي أشارت إليها المادة 137 والمتعلقة بإتلاف وفض الرسائل من قبل موظفي ومندوبي مصلحة البريد.

([3]) د. خالد عبد الباقي الخطيب، الجرائم الواقعة على الأشخاص، مكتبة خالد بن الوليد، صنعاء، 2002، 2010م، ص280.

ويعاقب على الشروع في ارتكاب الجنح المشار إليها في هذه المادة بالعقوبات المقررة للجريمة التامة. إن صفح الضحية يضع حداً للمتابعة الجنائية".

كما نصت المادة (257) من قانون الجرائم والعقوبات اليمني على أنه: "يعاقب بالحبس مدة لا تزيد على سنتين، أو بالغرامة كل من أذاع أو سهل إذاعة أو استعمل ولو في غير علانية تسجيلاً أو مستنداً متحصلاً عليه بإحدى الطرق المبينة بالمادة السابقة – 256– وكان ذلك بغير رضاء صاحب الشأن، ويعاقب بالحبس مدة لا تزيد على ثلاث سنوات كل من هدد بإفشاء أمر من الأمور التي تم الحصول عليها بإحدى الطرق المشار إليها لحمل شخص على القيام بعمل أو الامتناع عنه، ويعاقب بالحبس مدة لا تزيد على خمس سنوات الموظف العام الذي يرتكب أحد الأفعال المبينة بهذه المادة اعتمادا على سلطة وظيفته.

وتقابلها في قانون العقوبات الجزائري المادة: (303 مكرر1)، حيث نصت على أنه: "يعاقب بالعقوبات المنصوص عليها في المادة السابقة كل من احتفظ أو وضع أو سمح بوضع في متناول الجمهور أو الغير أو استخدم بأية وسيلة كانت، التسجيلات أو الصور أو الوثائق المتحصل عليها بواسطة أحد الأفعال المنصوص عليها في المادة (303 مكرر من القانون ذاته).

عندما ترتكب الجنحة المنصوص عليها في الفقرة السابقة عن طريق الصحافة تطبق الأحكام المنصوص عليها في القوانين ذات العلاقة، لتحديد الأشخاص المسئولين، ويعاقب على الشروع في ارتكاب الجنحة المنصوص عليها بالعقوبات ذاتها المقررة للجريمة التامة.

وتنص المادة (258) من قانون الجرائم والعقوبات اليمني على أنه: "يعاقب بالحبس مدة لا تزيد على سنة أو بالغرامة من كان بحكم مهنته أو حرفته أو وضعه مستودع سر فأفشاه في غير الأحوال المصرح بها قانوناً أو استعماله لمنفعته أو لمنفعة شخص آخر ما لم يأذن صاحب الشأن في السر بإفشائه أو استعماله ،وتكون العقوبة الحبس مدة لا تزيد على ثلاث سنوات إذا كان الجاني موظفاً عاماً استودع السر أثناء أو بسبب أو بمناسبة تأدية وظيفته".

وتأسيساً على النصوص القانونية السابقة والمتعلقة بالحياة الخاصة، يلاحظ بأن المشرع اليمني والمشرع الجزائري قد تعاملا مع الجريمة على أن المساس بها يشمل الجانب المادي للحياة الخاصة فحسب، ولم يكن في الحسبان آنذاك ما سيئول إليه الأمر من تطور في الجانب التقني والمعلوماتي لتصبح فيه الحياة الخاصة مهددة بسبب المعلومات المخزنة والمعالجة والمنقولة من نظام معلوماتي إلى آخر.

ولم تصدر أغلب التشريعات العربية – ومنها التشريع اليمني والتشريع الجزائري – قانوناً خاصاً لحماية خصوصية الإنسان في مجال المعلوماتية كما فعلت بعض التشريعات الغربية؛ ومنها التشريع الفرنسي[1]، ومع أنه توجد نصوص متناثرة في قوانين العقوبات والإجراءات الجزائية إلا أن مجمل تلك النصوص لا تتضمن نصاً تشريعياً يتعلق بحماية الحياة الخاصة من مخاطر الحاسوب الآلي وبنوك المعلومات، باستثناء ما تناوله المشرع الجزائري في تجريم المساس بأنظمة المعالجة الآلية للمعطيات من حماية للحياة الخاصة بصورة غير مباشرة، نتيجة تجريمه لأفعال تتعلق بالجرائم المعلوماتية المستحدثة؛ ومنها فعل الدخول أو البقاء في نظام المعالجة الآلية للمعطيات أو افعال التلاعب بالبيانات المخزنة في النظام اذ أن تجريم تلك الافعال تحقق نوع من الحماية للبيانات حال كانت تتعلق بالأمور الخاصة.

فضلاً عن ذلك، فإن تزايد مخاطر التقنيات الحديثة على حماية الخصوصية، كتقنيات رقابة (كاميرات) الفيديو، وبطاقات الهوية والتعريف الإلكترونية، وقواعد البيانات الشخصية، ووسائل اعتراض ورقابة البريد والاتصالات، ورقابة بيئة العمل وغيرها تجعل المجتمع يتحول بذلك إلى عالم تصبح فيها أسرارنا وأمورنا الشخصية ومعاملاتنا المالية وحياتنا العقلية والجسمانية مكشوفة[2]، لذلك أضحت الحاجة ملحة إلى تشريعات تتناسب مع تلك المخاطر التقنية على الحياة الخاصة.

ثانيا : الركن المادي لجرائم الاعتداء على الحياة الخاصة:

أضحى العدوان على المعلومات الشخصية في مجال المعلوماتية أمراً سهلاً، فقد أصبحت حياة الافراد وأسرهم تكيف تبعاً لمصالح معينة لجهات تملك معلومات مخزنة في أنظمتها، وبذلك يصبح الإنسان مكشوفاً في أسراره، تتحكم في بياناته أجهزة الكمبيوتر والشبكة المعلوماتية، بحيث تجعلها عرضة للانتهاك ما بين لحظة وأخرى، فقد أصبح الحال في ظل التطور التكنولوجي وثورة المعلوماتية أن يكون بمقدور الشخص الذي يتقن أو على الأقل يستطيع التعامل مع التقنية في أن يطلع على معلومات الآخرين منتهكاً خصوصياتهم.

([1]) اهتم المشرع الفرنسي في موضوع الخصوصية وعلاقتها بالبيانات الاسمية مبكراً، بموجب القانون الصادر بتاريخ 1978/1/6 بشأن المعلوماتية والبطاقات والحريات، ونظراً لأهمية النصوص القانونية التي تضمنها هذا القانون فقد أصبحت نصوصه المتعلقة بالخصوصية جزءً من ق.ع.ف الجديد في المواد من 226 – 6 إلى 226– 28، وبهذا الخصوص فإن المادة (226 –1) من ق.ع.ف الجديد تعاقب بالحبس سنة وبغرامة (45000 euros) كل من يعتدي على قداسة الحياة الشخصية للغير حال قيامه بإجراء معالجة آلية للمعلومات الاسمية دون التقيد بالشروط المقررة في القانون المؤرخ في 1987م.كما يعتبر التشريع الألماني المؤرخ في 1997 هو أول تشريع على مستوى دول الاتحاد الأوربي يتناول موضوع العلاقة بين البيانات الشخصية والإنترنت بموجب الاتفاقيات والتوجيهات الأوربية، يُراجع: عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الإنترنت، رسالة دكتوراه، جامعة، دار النهضة العربية، القاهرة، 2004، ص598، 599.كما يُرجع إلى: نص المادة (261/ 1) من قانون العقوبات الفرنسي بالفرنسي على الرابط الإلكتروني:

http://www.legislationline.org/lawmaking/country/30

(2) هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق، ص182. (نقلاً عن الفقيه: آرثر ميللر (Mellor)، المخاطر التي تهدد الخصوصية وخصوصية المعلومات في العصر الرقمي.

وقد زاد الأمر خطورة في مجال الاعتداء على الحياة الخاصة ما توفره شبكة الإنترنت من معلومات عن خصوصيات الأفراد بسبب عدم توفر السرية الكاملة والأمان في الشبكة، حيث أضحت الشركات التي تقوم بتجميع معلومات شخصية تخص الأفراد مثل شركات التأمين وغيرها، وكذلك مواقع التواصل الاجتماعي تعرف تفاصيل الحياة الخاصة للأفراد أكثر مما يعرفه الخطيب عن خطيبته حسب تعبير أحد الكتاب الأمريكيين[1].

ويقوم الركن المادي في جرائم الاعتداء على الحياة الخاصة على عدد من الأفعال التقليدية، أو التقنية، بحسب ما إذا كانت الجريمة مرتكبة بوسائل تقليدية أو بوسائل رقمية، وتتمثل أهم تلك الاعتداءات في الآتي:

1. **إساءة استعمال البيانات والمعلومات الاسمية:**

تعرف البيانات الاسمية بأنها: "تلك البيانات التي من شأنها تحديد شخصية الشخص الطبيعي تحت أي شكل مباشر أو غير مباشر، سواءً أجريت المعالجة المعلوماتية بواسطة شخص طبيعي أم معنوي".

كما تُعرف بأنها: "البيانات الشخصية التي تتعلق بالحق في الحياة الخاصة للفرد؛ كالبيانات المتعلقة بالجانب الصحي، أو المالي، أو المهني، أو العائلي، عندما تكون هذه البيانات محلا للمعالجة الآلية[2].

والبيانات والمعلومات الاسمية التي يتم تجميعها وتخزينها لابد أن يكون ذلك لغرض وهدف محدد ينحصر فيما جمعت وخزنت من أجله، بحيث يقتصر استخدامها على ذلك الغرض فحسب، فمثلاً البيانات التي جمعت من أجل التعداد السكاني لا ينبغي أن تستخدم من قبل الأجهزة الأمنية[3].

فإذا ما تم جمع البيانات والمعلومات من قبل جهة معينة أو شخص ما لغرض محدد ثم اتضح أن تلك البيانات والمعلومات قد انتقلت إلى جهة غير تلك التي قامت بجمع المعلومات، أو إلى شخص آخر فإن جريمة الاعتداء على الحق في الخصوصية تكون قد تحققت.

([1]) محمد عبد الله الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع الشبكة الإنترنت، رسالة ماجستير، كلية الحقوق، جامعة القاهرة، 2004، ص139.

([2]) يُراجع في التعريف الأول الذي تضمنه القانون الفرنسي رقم 78 -17 الصادر في 6 يناير 1978، والمتعلق بالمعلوماتية والمعالجة الإلكترونية والحريات: عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، بدون ذكر دار النشر، ط2، 2000، ص291. وفي التعريف الثاني: نائل صالح عبد الرحمن، واقع جرائم الحاسوب الآلي في التشريع الجزائي الأردني، ورقة عمل مقدمة إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، الإمارات العربية المتحدة، 2000، ص15. (مشاراً إليه لدى: نهلا عبد القادر المؤمني، الجرائم المعلوماتية، رسالة ماجستير، الجامعة الأردنية، دار الثقافة، عمان، الأردن، ط1، 2007، ص 168.

([3]) تطبيقاً لمخالفة استعمال البيانات للهدف الذي جمعت من أجله فقد أبطلت المحكمة الألمانية العمل باستمارات إحصاء سكاني في 1984 بعد أن ثبت لها أن وزارة الداخلية قد استخدمت استمارات الإحصاء في الحصول على عناوين مجموعة متطرفة، الأمر الذي يُعد إساءة لاستخدام البيانات التي جمعت من أجل غاية محددة وهي الإحصاء السكاني. يُراجع: عفيفي كامل عفيفي، المرجع السابق، ص259.

كما يتم الاستخدام السيئ للمعلومات الاسمية من خلال استخدام المعلومات المعالجة والمخزنة في بنوك المعلومات، أو في أنظمة شركات خاصة استخداماً يسيء إلى الحياة الخاصة للأفراد فيشوهها ويترك آثاراً سلبية حيالها قد تؤثر على مستقبل أولئك الأشخاص[1]، الأمر الذي يتطلب وضع ضوابط وقيود يتم من خلالها المحافظة على الحق في الخصوصية، وسن قوانين أو نصوص قانونية لمنع أي جهة من إعطاء معلومات إلى جهة أخرى مختلفة عنها في الهدف، وإذا ما سمح بمثل هذا الأمر فلابد وأن تحكمه ضوابط وقيود يتم من خلالها المحافظة على الحق في الخصوصية .

2. جمع البيانات وتخزينها على نحو غير مشروع:

يتمثل فعل الانتهاك للحق في الحياة الخاصة للأفراد في هذه الصورة في عملية جمع وتخزين بيانات عنهم، وقد تكون البيانات أو المعلومات التي يتم جمعها صحيحة، إلا أن عملية الجمع أو التخزين قد تتم على نحو غير قانوني[2]، ويكون ذلك إما من مضمون المعلومات نفسها أو عن طريق الأساليب غير المشروعة المستخدمة للحصول على تلك البيانات والمعلومات، ويرجع السبب في ذلك إلى أن مضمونها يتعلق بكافة المعلومات الخاصة بالفرد والتي لا يرغب في إطلاع الغير عليها.

وجميع البيانات والمعلومات الاسمية التي تتعلق بالحياة الخاصة يجب أن يحظر تجميعها وتخزينها ومعالجتها داخل جهاز الحاسوب[3]، حيث من المفترض أن مضمون البيانات والمعلومات التي تتعلق بالأفراد تدخل في إطار الأمور التي يحرص الأفراد على سريتها، لأن فكرة الحياة الخاصة تشتمل على قدر من المرونة يكون لإرادة الشخص دور في تحديد ما يدخل في إطارها.

أما عن الوسائل غير المشروعة التي يتم بها جمع المعلومات المتعلقة بالحياة الخاصة، فيكون إما عن طريق التقاط البيانات أثناء انتقالها من وحدة طرفية إلى أخرى[4]، أو من خلال تحليل ومعالجة الأصوات عقب ارتطامها في جدران إسمنتية وتحويلها إلى

([1]) وكمثال للاستخدام السيئ للبيانات والمعلومات الشخصية المعالجة والمخزنة بنظم المعلوماتية لدى جهات معينة أو شركات أو في بنوك المعلومات والاعتماد عليها في تقييم السلوك الشخصي والمهني وغيره، ما حدث في فرنسا عام 1965 عندما فُصل شخص من الشركة التي كان يعمل بها، ومكث خمس سنوات يبحث عن وظيفة لدى شركة أخرى، وكان يواجه برفض الطلب البالغ 625 طلباً، اتضح في نهاية الأمر أن السبب في ذلك هو البيانات المعالجة إلكترونياً والتي كانت تقدم من شركتين تعملان في مجال جمع المعلومات، وكانت المعلومات الخاصة به والتي تم جمعها ومعالجتها سيئة وتتعلق بحياته الشخصية، فمثل هذه الحالة وغيرها تؤكد بأن اتخاذ القرارات أو إصدار الأحكام بموجب بيانات معالجة ومخزنة قد لا تجانب الصواب، وخاصةً عندما تكون تلك البيانات والمعلومات غير صحيحة. يُراجع: نهلا عبد القادر المومني، الجرائم المعلوماتية، مرجع سابق، ص173.

(2) نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي، القاهرة، ط1، 2005، ص236.

([3]) ومثال ذلك قيام عصابة في إيطاليا بأخذ صور شخصية تتضمن مشاهد مخلة بالحياء يتم التقاطها عبر كاميرا رقمية صغيرة يصل حجمها إلى حجم علبة الثقاب، وذلك من خلال وضعها في دورات المياه العامة، وغرف الفنادق، وحمامات السونا البخار، وغير ذلك من الأماكن التي يظن فيها الشخص عدم المساس بخصوصياته، بعد ذلك يتم نشر تلك الصور من خلال مواقع بالإنترنت، بمقابل 15دولار للكتلوج من تلك الصور. يُراجع: مصطفى محمد موسى، أساليب إجرامية بالتقنية الرقمية، دار الكتب والوثائق القومية المصرية، القاهرة، ط1، 2003، ص185.

([4]) كذلك من الأمثلة الواقعية لاستخدام وسيلة أو أكثر لتجميع البيانات وتخزينها، ما قام به مراهق ألماني لا يتجاوز عمرة 26 عام بنصب مصيدة بيانات نجح من خلالها في التقاط المعلومات الشخصية بمستعملي نظام فديو تكس، بالإضافة إلى قيامة بإتلاف بيانات بعض المستخدمين وتغيير كلمات السر التي يستخدمونها للتعامل مع النظام مما تسبب في حرمانهم من الخدمة. يُراجع: عفيفي كامل عفيفي، مرجع سابق، ص253.

كلمات مفهومة، أو عن طريق توصيل أسلاك وربطها بالحاسوب أو الشبكة المراد التعدي على حقوق الأفراد الخاصة من خلالها[1]، أو عن طريق ملفات الكوكيز[2]، فهذه الوسائل وغيرها من الوسائل المستخدمة في مجال التقنية الحديثة، والتي يتم بواسطتها الاطلاع على مضمون البيانات الشخصية المتعلقة بالأفراد، فإذا تم الاطلاع على المعلومات المتعلقة بالحياة الخاصة باعتبار أن الاطلاع على تلك المعلومات يعد أمراً غير مشروع، أو إذا تم استخدام وسائل غير مشروعة للحصول على تلك المعلومات أو الاطلاع عليها، فإن جريمة الاعتداء على الحق في الخصوصية تكون متحققة، ولا يهم بعد ذلك نوع البيانات التي تم جمعها وتخزينها فقد تتعلق بالجانب المالي، وقد تتعلق بالجانب الصحي، أو الائتماني، وغير ذلك من البيانات ذات الطبيعة الشخصية واللصيقة بصاحبها.

3. مخالفة القواعد المنظمة لجمع ومعالجة ونشر البيانات ذات طبيعة شخصية:

تُعد الأفعال التي تخالف القواعد الشكلية لجمع ومعالجة ونشر البيانات من الأفعال التي يقوم عليها الركن المادي لجرائم الاعتداء الحق في الخصوصية. فإذا تطلب قانون معين سبق الحصول على ترخيص بجمع معلومات تتعلق بشخص أو بأشخاص، فإن الحصول على تلك البيانات دون سابق الحصول على الترخيص يُعد اعتداءُ على الحق في الخصوصية[3]، ومن أمثلة هذه

([1]) هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق، ص193.

([2]) كلمة كوكيز في عالم الإنترنت تعني الملفات النصية الصغيرة حيث يتم إرسالها عن طريق السيرفر الخاص بالموقع الذي يتم زيارته، فبمجرد الدخول علي صفحة معينة يقوم السيرفر الخاص بالموقع الذي يتم زيارته بإنشاء ملفين الأول يحتفظ به، والثاني يرسله إلى جهاز المتصفح ليتم تخزينه في مجلد الكوكيز بداخل مجلد النوافذ، وبطريقة مشابهة عند استعراض البريد الإليكتروني، وهي تتيح للموقع معرفة كثير من المعلومات الشخصية عن الشخص وعن جهازه – نوع الجهاز، نوع المعالج، رقم IP – وطريقة الاتصال بالإنترنت، نوع المودم، المواقع التي يتم زيارتها، عدد الساعات التي يتم البقاء فيها متصلا بالشبكة، والأخطر من هذا هو اهتمام المتصفح، ما الذي يبحث عنه، وما الذي يريد شرائه، بالإضافة لكافة المعلومات التي يتم كتابتها في استمارات التسجيل مثل الاسم، العنوان، الكود البريدي، أرقام التليفون، أرقام بطائق الائتمان، وكل تلك الأفعال تشكل اعتداءً كبيراً على الخصوصية، مع أن الكثير لا ينتبهون أثناء تصفحهم للشبكة أنهم يتركون أثارهم أينما ذهبوا. يُراجع: منديات الفلاش، ساعة الدخول 12 مساءً، الخميس 29 /2018/10، منشور على الرابط الإلكتروني:
http://www.alflash.com/vb/showthread.php?t=2808

([3]) ومن الأمثلة على مخالفة القواعد الشكلية لعملية تجميع وتخزين ونشر البيانات، ما قامت به شركة (skf) الفرنسية بتخزين بيانات الموظفين المتعلقة بالحياة الخاصة والاتجاهات السياسية، والتي حصلت عليها عن طريق استمارات طلبات التوظيف التي كانت محفوظة لديها بالطرق اليدوية دون موافقة مسبقة من لجنة المعلوماتية والحريات، وهو ما يُعد تسجيلاً وحفظاً غير مشروع يعاقب عليه القانون الفرنسي الخاص بالمعالجات الإليكترونية للبيانات الاسمية. يُراجع: هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق، ص200. وكذلك نص المادة (20/226) من ق،ع.ف لعام 2004 والتي تحظر الإبقاء على معلومات أكثر من المدة التي ينص عليها القانون، أو في الحالات التي يتطلب القانون موافقة مسبقة من لجنة الحريات، حيث يعاقب بالحبس لمدة خمس سنوات والغرامة 300.000. ونص المادة بالفرنسي:

(Le fait de conserver des données à caractère personnel au-delà de la durée prévue par la loi ou le règlement, par la demande d'autorisation ou d'avis, ou par la déclaration préalable adressée à la Commission nationale de l'informatique et des libertés, est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende, sauf si cette conservation est effectuée à des fins historiques, statistiques ou scientifiques dans les conditions prévues par la loi.
Est puni des mêmes peines le fait, hors les cas prévus par la loi, de traiter à des fins autres qu'historiques, statistiques ou scientifiques des données à caractère personnel conservées au-delà de la durée mentionnée au premier alinéa).
منشور على الرابط الإلكتروني: http://www.legislationline.org/lawmaking/country/30

القوانين، القانون الفرنسي حيث ينص على أن: "يعاقب بعقوبة الحبس من ستة أشهر إلى ثلاث سنوات والغرامة من 2000 فرنك إلى 200.000 فرنك أو بإحدى هاتين العقوبتين كل من يجري أو يقوم بإجراء المعالجة الإلكترونية للبيانات الشخصية دون ترخيص من اللجنة المختصة بذلك وفقاً لأحكام المادتين (15، 16) من هذا القانون، وللمحكمة أن تأمر بنشر الحكم كله أو ملخصه في جريدة أو أكثر بالشروط التي يحددها الحكم"[1]، كما ينطبق ذات الأمر في حال مخالفة القواعد الشكلية لنشر المعلومات المتعلقة بالخصوصية عندما يتم تسريب أو استخدام البيانات من قبل جهة أخرى[2].

4. الإفشاء غير المشروع للبيانات والمعلومات الاسمية:

تخزين البيانات ذات الطابع الشخصي أو التي تتعلق بالخصوصيات لا يعني بأنها قد انتقلت من الخصوصية إلى العلنية، كما أن رضاء صاحب الشأن في التجميع أو التخزين لا يعني إعطاء الحرية في تبادل وتناقل المعلومات إلى جميع الناس[3]. وقد يتم تجميع تلك المعلومات من قبل بعض الأجهزة التي تعمل في مجال الشرطة، فيتم الاحتفاظ بكم هائل من المعلومات الخاصة بملايين الأشخاص في بنوك المعلومات للجهات ذاتها، وبالتالي فإن خطر إفشائها وارد من أشخاص قد يكونوا أمناء عليها[4].

ويتميز الحاسوب بدور كبير في إفشاء الأسرار، نظرا للدخول في عالم الشبكات، .والأقمار الصناعية، والبث الفضائي، حيث أصبحت الدول لا تستطيع التحكم في ذلك المجال[5]، وفي عصر المعلومات ازدادت حوادث الاختراق والقرصنة من أجل الحصول على البيانات والمعلومات المخزنة في ذاكرة الحاسوبات المستخدمة[6].

([1]) المادة (41) من القانون الفرنسي المؤرخ في 6 يناير 1978 والخاص بالمعالجات الإليكترونية للبيانات الاسمية.

([2]) من القضايا التي تتعلق بانتهاك الحق في الخصوصية في مجال المعالجة الآلية بمخالفة القواعد الشكلية قضية تتعلق بإحدى شركات التأمين الفرنسية بالاشتراك مع عاملين بشركة كهرباء فرنسا، وتتلخص وقائعها في استلام عدد من الأشخاص كانوا قد انتقلوا من منازلهم للسكن في منازل جديدة خطابات من أحدى شركات التامين تعرض عليهم إجراء التأمين الخاص بالمنازل الجديدة من خلالها وبعد تحري هؤلاء الأشخاص عن المصدر الذي توصلت شركة التأمين من خلاله إلى البيانات الخاصة بهم تبين لهم أن هذا المصدر هي شركة الكهرباء خاصة أن بعض الأخطاء الإملائية في الأسماء التي انطوت عليها العقود المبرمة بين هؤلاء وشركة الكهرباء قد ظهرت في الخطابات التي ارسلت اليهم، وبناءً على ذلك، تقدم هؤلاء الأشخاص بشكوى إلى اللجنة الوطنية للمعلومات والحريات والتي قامت بدورها بالانتقال إلى شركة التأمين للتحري تمشياً مع ما تخوله إياها المادة ٢١ من القانون رقم ٧٨ – ١٧ لسنة ١٩٧٨، مما أسفر عن اكتشاف اللجنة أن شركة التأمين تدير أعمالها من خلال نظام المعالجة الآلية للمعلومات الشخصية ولم تحصل بشأنه على ترخيص، وأن المعلومات التي تمت برمجتها قد حصلت عليها بطريقة غير مشروعة بمساعدة بعض العاملين بشركة الكهرباء نظير مبالغ نقدية، وقد تقدمت اللجنة بناءً على ما تقدم ببلاغ إلى النائب العام حيث تم توجيه عدة اتهامات إلى مسئولي شركة التامين وإلى عاملين بشركة الكهرباء. يُراجع: نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، مرجع سابق، ص239.

([3]) نهلا عبد القادر المومني، الجرائم المعلوماتية، مرجع سابق، ص177.

([4]) ومن تلك الجهات التي يوجد بها عدد كبير من ملفات المواطنين، المملكة المتحدة، حيث يضم الحاسوب الآلي الوطني للشرطة ملفات 22 مليون شخص، وفي الولايات المتحدة الأمريكية يضم مركز معلومات الجريمة التابع لمكتب التحقيقات الفدرالي سجلات تتعلق بحوالي 9 ملايين شخص. يُراجع: هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق، ص194.

([5]) أيمن عبد الحفيظ عبد الحميد سليمان، استراتيجية مكافحة الجرائم الناشئة عن استخدام الحاسوب الآلي، دراسة مقارنة، رسالة دكتوراه في علوم الشرطة، أكاديمية الشرطة، القاهرة، 2003، ص131.

(6) د.عبد الفتاح بيومي حجازي، الأحداث والإنترنت، دار الفكر الجامعي، الإسكندرية، ط1، 2002، ص230.

وبناءً على ذلك، فإن هذه المخاطر المشار إليها في صور الاعتداء على المعلومات المتعلقة بالحياة الخاصة في مجال المعلوماتية أظهرت الأهمية الاستثنائية للحماية القانونية – إلى جانب الحماية التقنية – للبيانات الشخصية، ومن العوامل الرئيسة في الدفع نحو وجوب توفير حماية تشريعية وسن قوانين في هذا الحقل، أنه وقبل اختراع الكمبيوتر، فإن حماية هؤلاء الأشخاص كانت تتم بواسطة النصوص الجنائية التي تحمي الأسرار التقليدية، وعلى الرغم من ذلك فإن النصوص التقليدية لحماية الحياة الخاصة لا تغطي إلا جانباً من الحقوق الشخصية وبعيدة عن حمايته من مخاطر الوسائل التقنية الجديدة.

هذه المخاطر الجديدة التي تستهدف الخصوصية دفعت العديد من الدول لوضع تشريعات ابتداءً من السبعينات، تتضمن قواعد إدارية ومدنية وجنائية من أجل حماية الخصوصية من الاعتداء عليها، وتوصف بأنها تشريعات السرية وليست فقط مجرد تشريعات تحمي من أفعال مادية تطال الحياة الخاصة.

كما أن هذه المخاطر، وما يتفرع عنها من مخاطر أخرى كتلك الناتجة عن معالجة البيانات في شبكات الحواسيب المتصلة ببعضها والتي تتيح تبادل المعلومات بين المراكز المتباعدة و المختلفة كانت محل اهتمام دولي وإقليمي ووطني أفرز قواعد ومبادئ تتفق وحجم هذه المخاطر، كوجوب مراعاة الدقة في جمع البيانات وكفالة صحتها وسلامتها، واتخاذ تدابير أمنية لمعالجتها وخزنها ونقلها، وإقرار مبدأ حق المشاركة الفردية في تعديل وتصحيح وطلب إلغاء البيانات، ووجوب تحديد الغرض من جمعها ومدة استخدامها، وإقرار مبدأ مسؤولية القائمين على وظائف بنوك المعلومات عند أي تجاوز أو مخالفة للمبادئ الموضوعية والشكلية في جمع ومعالجة وتخزين ونقل البيانات الشخصية[1].

5. الافعال التي ترتكب بها الجرائم المعلوماتية المستحدثة اذا استهدفت الحق في الخصوصية:

تُعد الأفعال التي يمكن أن ترتكب بها إحدى جرائم المعلوماتية بصورتها المستحدثة إذا ما كان الهدف من ارتكابها التعدي على الحق في الخصوصية بكافة صورها ضمن الافعال التي تمثل الركن المادي للجريمة، ومن تلك الأفعال فعل الدخول إلى نظام

([1]) تم التوقيع على الكثير من الاتفاقيات، كما صدرت عدد من التوجيهات والتوصيات في مجال حماية الحياة الخاصة من الانتهاك، منها: الاتفاقيات والتوصيات الأوروبية المتعلقة بحماية الأفراد بالنظر إلى المعالجة الآلية للبيانات، ومن ذلك اتفاقية سنة 1981م الصادرة عن مجلس أوروبا التي تضمنت مفهوم حماية البيانات الشخصية في إطار الحاسوب، والتوجيه الأوربي لسنة 1995م، والتوجيه الأوربي رقم CE-85-2002 بتاريخ 12 يوليو 2002 م بشأن معالجة البيانات الشخصية والحياة الخاصة في إطار الإنترنت، والذي تضمن موعد تنفيذه بتشريعات الدول الأوربية ابتداءً من 31 أكتوبر 2003، وقد تضمنت تلك الاتفاقيات الأطر والضمانات التي يجب على الدول مراعاتها أثناء تجميع وتخزين ومعالجة وتبادل البيانات، فتقرر المسؤولية والجزاء لكل من يملك معلومات خاصة إذا تم نشرها بشكل غير دقيق، وقررت معاقبة كل من يُعد بياناً بالمعالجة حول طبيعة المعلومات، كما تقوم تلك الاتفاقيات والتوجيهات على ردع كل محاولة رقابية على الإنترنت، بحيث ألزمت الدول الأعضاء بفرض عقوبات على العدوان على البيانات الشخصية. يُراجع: عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص598، 599.

المعالجة الآلية للمعطيات أو البقاء في النظام، أو افعال التلاعب بالمعطيات المخزنة بنظام المعالجة الآلية للمعطيات، سواءً تمثلت بالمحو أو الازالة أو التعديل ،كذلك أي فعل من الأفعال التي تتم عن طريق التعامل مع المعطيات غير الشرعية التي ترتكب بها الجرائم المعلوماتية أو الناتجة عن ارتكاب جريمة معلوماتية؛ ومنها أفعال النشر لمحتوى الخصوصية المتحصل عليه من اقتراف إحدى جرائم المعلوماتية إذا كان يمس الخصوصية، وكذلك فعل التصميم للبرامج التي يمكن أن يتم بواسطتها انتهاك خصوصيات الأشخاص من خلال بياناتهم المخزنة في نظم المعلومات وأجهزة الحاسوب والهواتف الذكية[1]، إضافةً إلى الدخول على مواقع التواصل الاجتماعي[2]. وقد نكون بصدد تعدد مادي للجرائم في مثل هذه الحالات؛ ومثال ذلك: ارتكاب جريمة دخول إلى نظام المعالجة الآلية للمعطيات، وجريمة اعتداء على الخصوصية.

6. الأفعال التقليدية المكونة للركن المادي:

يقوم الركن المادي في جرائم الاعتداء على الخصوصية في القانون اليمني والقانون الجزائري على عدة أفعال، منها:

- فض أو احتجاز أو إتلاف المراسلات.
- الاستماع أو التسجيل أو النقل للمحادثات التي تجري في مكان خاص أو عن طريق الهاتف.
- الالتقاط أو النقل لصورة شخص من مكان خاص.
- التهديد بإذاعة الأسرار الخاصة.

وهذه الأفعال من شأنها أن تؤدي إلى فض أو احتجاز أو إتلاف المراسلات، أو الاستماع أو التسجيل أو النقل للمحادثات التي تجري في مكان خاص أو عن طريق الهاتف، أو الالتقاط أو النقل لصورة شخص من مكان خاص أو التهديد بإذاعة الأسرار الخاصة.

---

(1) بلغ عدد مستخدمي الهاتف حتى نهاية 2017 (3,790 مليار)، وهذا العدد الهائل من مستخدمي الهاتف الذكي يدل على أن خصوصيات الافراد باتت معرضة للانتهاك بشكل أكثر من ذي قبل وبات الهاتف الذكي بما يحوي أو يمكن تحميل البرامج الخاصة بالاختراق واستخدامه في ذلك يمثل خطورة على الحق في الخصوصية. يُراجع: بارق منتظر عبدالوهاب لامي، جريمة انتهاك الخصوصية عبر الوسائل الالكترونية في التشريع الأردني، رسالة ماجستير، جامعة الشرق الأوسط، عمان، الأردن، 2017، ص27.

(2) بلغ عدد مستخدمي الإنترنت في عام 2018 حوالي (4.021 مليار)، بزيادة تبلغ 7٪ سنوياً، وعدد مستخدمي وسائل التواصل الاجتماعي في عام 2018 أصبح (3.196 مليار)، أي بزيادة 13٪ سنوياً، كما بلغ عدد مستخدمي الهواتف المحمولة في عام 2018 حوالي (5.135 مليار)، بزيادة 4٪ سنوياً، يُراجع: جريدة ايلاف الالكترونية س.د11:15يوم الجمعة الموافق2019/9/6على الرابط:
https://elaph.com/Web/Opinion/2018/3/1196481.html

فإذا ما تحققت الأفعال السابقة فإن الركن المادي في جريمة الاعتداء على الحق في الخصوصية يكون متوافر، ومن ذلك قيام الجاني بنشر صور أو تعليقات أو أخبار تتعلق بالحياة الخاصة بطريق العلانية ولو كانت هذه الصور أو الأخبار صحيحة[1].

وتأسيساً على ذلك، فلا يجوز الاطلاع على المراسلات إلا من مرسلها أو المرسل إليه بصرف النظر عن المعلومات التي تتضمنها، حتى لو لم تتضمن معلومات تتعلق بالحياة الخاصة، لما للمراسلات من حرمة تقتضي احترامها وعدم الاطلاع عليها أو كشف مضمونها. وكذلك فإن المكالمات الهاتفية قد تكون محلاً لتبادل الأسرار، ومن ثم فإن فعل التصنت عليها ومعرفة فحواها يدخل في إطار التجريم إذا تم التسجيل أو النقل أو الاستماع بأي جهاز كان. وبالتالي تقوم الجريمة إذا قام الجاني بإذاعة أو تسهيل أو استعمال مستند تم الحصول عليه عن طريق الالتقاط بأي جهاز كان.

ثالثاً: الركن المعنوي:

يتخذ الركن المعنوي في هذه الجريمة صورة القصد الجنائي العام باعتبار أنها جريمة عمدية، يكفي لتحققها أن يكون الشخص عالماً بحقيقة الفعل الذي يقوم به وقت فضه للرسالة، أو سماعه للمحادثة، أو التقاطه للصورة في مكان خاص، أو إذاعته للسر، أو تسهيل أو استعمال مستند مما يعد محصوراً عليه استعماله أو إذاعته، كونه يتعلق بالحياة الخاصة للآخرين، أو غير ذلك من الأفعال المشار إليها أثناء إيضاح الركن المادي للجريمة. كما يشترط بجانب العلم أن تكون إرادة الجاني متوفرة آنذاك وتهدف إلى الإقدام على ارتكاب الجريمة ، وأن تكون الإرادة حرة وواعية.

ويتطلب لتوافر الركن المعنوي في بعض جرائم المعلوماتية القصد الخاص؛ كأن تكون الجريمة المرتكبة هي جريمة الدخول إلى النظام، ويكون لدى الجاني نية بارتكاب جريمة أخرى قد تتمثل في إحدى جرائم الاعتداء على الخصوصية في مجال المعلوماتية؛ مثل الاعتداء على البيانات المتعلقة بالخصوصية أو افشائها مع علم المجرم أنه يقوم بجريمة دخول إلى نظام المعالجة الآلية للمعطيات ولا يشترط أن تتعاصر نية الدخول الى نظام المعالجة مع نية اقتراف الجريمة الأخرى[2].

([1]) محمد عبدالله الكعبي، مرجع سابق، ص113.

(2) جرمت بعض التشريعات الافشاء غير المشروع للمعلومات المبرمجة آليا بغض النظر عن طبيعة المعلومات التي تم افشاؤها قد تم الحصول عليها نتيجة دخول غير مشروع لنظام الحاسب الآلي، ومن تلك القوانين القانون الفدرالي لجرائم الحاسب الآلية لعام 1984، يُراجع: نائلة عادل محمد فريد قورة، مرجع سابق ص276، 370.

رابعاً: العقوبة:

فيما يلي نبين نصوص قانوني الجرائم والعقوبات اليمني وقانون العقوبات الجزائري حول هذه الجرائم كما يلي:

1. عقوبة جرائم الاعتداء على الحياة الخاصة في مجال المعلوماتية في القانون اليمني.

أورد قانون الجرائم والعقوبات اليمني عدداً من النصوص التي تعاقب على الاعتداء على الحياة الخاصة، نبينها كما يلي:

- الحبس مدة لا تزيد على سنة أو الغرامة لكل من فتح بغير حق خطابا مرسلاً إلى الغير أو احتجز رسالة أو برقية هاتفية، أو اختلس، أو أتلف إحدى هذه المراسلات، أو أفضى بمحتوياتها إلى الغير ولو كانت الرسالة قد أرسلت مفتوحة أو فتحت خطأ أو مصادفة، وتضاعف العقوبة إلى سنتين أو الغرامة إذا ارتكبت الجريمة من موظف عام إخلالا بواجبات وظيفته (255 ق.ج.ع.ي).
- الحبس مدة لا تزيد على سنه أو بالغرامة كل من اعتدى على حرمة الحياة الخاصة، وذلك بأن أرتكب أحد الأفعال الآتية في غير الأحوال المصرح بها قانوناً أو بغير رضاء المجني عليه المادة (256 ق.ج.ع.ي):

أ- استرق السمع أو سجل أو نقل عن طريق جهاز من الأجهزة أياً كان نوعه محادثات جرت في مكان خاص أو عن طريق الهاتف.

ب- ألتقط أو نقل بجهاز من الأجهزة أياً كان نوعه صورة شخص في مكان خاص.

- فإذا صدرت الأفعال المشار إليها في الفقرتين السابقتين أثناء اجتماع على مسمع أو مرأى من الحاضرين في ذلك الاجتماع فإن رضاء هؤلاء يكون مفترضاً، المادة (256 ق.ج.ع.ي).
- ويعاقب بالحبس مدة لا تزيد على ثلاث سنوات أو بالغرامة الموظف العام الذي يرتكب أحد الأفعال المبينة بهذه المادة اعتماد على سلطة وظيفته. ويحكم في جميع الأحوال بمصادرة الأجهزة وغيرها مما يكون قد استخدم في الجريمة كما يحكم بمحو التسجيلات المتحصلة عنها أو إعدامها، المادة (256 ق.ج.ع.ي).
- الحبس مدة لا تزيد على سنتين أو الغرامة لكل من أذاع أو سهل إذاعة، أو استعمل ولو في غير علانية تسجيلاً أو مستنداً متحصلاً عليه بإحدى الطرق المبينة بالمادة السابقة- 256 - و كان ذلك بغير رضاء صاحب الشأن، المادة (257 ق.ج.ع.ي).

- يعاقب بالحبس مدة لا تزيد على ثلاث سنوات كل من هدد بإفشاء أمر من الأمور التي تم الحصول عليها بإحدى الطرق المشار إليها لحمل شخص على القيام بعمل أو الامتناع عنه، ويعاقب بالحبس مدة لا تزيد على خمس سنوات الموظف العام الذي يرتكب أحد الأفعال المبينة بهذه المادة اعتمادا على سلطة وظيفته، المادة (257 ق.ج.ع.ي).
- ويحكم في جميع الأحوال بعقوبة تكميلية تتمثل بمصادرة الأجهزة وغيرها مما يكون قد استخدم في الجريمة ومحو التسجيلات المتحصلة عنها، المادة (257 ق.ج.ع.ي).

2. **عقوبة جرائم الاعتداء على الحياة الخاصة في مجال المعلوماتية في القانون الجزائري:** أورد قانون العقوبات الجزائري عدداً من النصوص التي تعاقب على الاعتداء على الحياة الخاصة، نبينها كما يلي:

- الحبس من شهر واحد (1) إلى سنة (1) واحدة، وبغرامة من 25.000 دج إلى 100.000دج أو بإحدى هاتين العقوبتين لكل من يفض أو يتلف رسائل أو مراسلات موجهة إلى الغير وذلك بسوء نية في غير الحالات المنصوص عليها في المادة (137)[1].
- الحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 50.000 دج إلى 300.000 دج لكل من التقط أو سجل أو نقل مكالمات أو أحاديث أو صور خاصة أو سرية، بغير إذن صاحبها أو رضاه.
- ويعاقب بنفس العقوبة المذكورة في الفقرة السابقة كل من احتفظ، أو وضع، أو سمح بوضع في متناول الجمهور أو الغير، أو استخدم بأية وسيلة كانت، التسجيلات أو الصور أو الوثائق المتحصل عليها بواسطة أحد الأفعال المشار إليها في الفقرة الأولى.
- يعاقب على الشروع في ارتكاب الجنحة المنصوص عليها بالعقوبات ذاتها المقررة للجريمة التامة.

كما أن العقوبات التي تضمنها قانون العقوبات الجزائري في الفصل الخاص بتجريم المساس بأنظمة المعالجة الآلية للعقوبات لا تقتصر على جريمة الدخول والبقاء أو التلاعب بالمعطيات إلى غير ذلك من الجرائم، ولا علاقة لها بعقوبة الاعتداء على الخصوصية التي يفترض أن تكون لها العقوبة الخاصة بها ما لم تنطبق عليها العقوبة التقليدية.

([1]) الحالات المنصوص عليها في المادة (137)ع.ج تتعلق بعقوبة فض أو اختلاس أو إتلاف الرسائل أو البرقيات من قبل موظفي ومستخدمي مصلحة البريد أو البرق أو المندوبين، حيث تكون العقوبة الحبس من ثلاثة اشهر إلى خمس سنوات وبغرامة من 10.000 دج إلى 100.000 دج.

المطلب الثاني

مدى إمكانية تطبيق النصوص القانونية التقليدية على جرائم الاعتداء على الحياة الخاصة

بالنظر إلى نصوص قانوني العقوبات اليمني والجزائري ومدى إمكانية تطبيقها على جريمة الاعتداء على البيانات الاسمية المعالجة آلياً يثار التساؤل حول مدى إمكانيتهما؟ وهل أخذا بالرأي القائل بصلاحية النصوص التقليدية للانطباق على جريمة الاعتداء على الخصوصية في مجال المعلوماتية؟ لأن الفارق في ارتكاب الجريمة لا يكمن سوى في تغيير الوسيلة، فبينما كانت الجريمة ترتكب بالوسائل التقليدية أصبحت ترتكب بوسائل حديثة، وذلك لا يغير من نوع الجريمة، وبالتالي فإن العقوبة التي كانت تطبق عليها في صورتها التقليدية هي ذات العقوبة التي يجب أن تطبق عليها في صورتها المستحدثة[1].

أم أن النصوص التقليدية في قانوني العقوبات اليمني والجزائري لا تفي بمواجهة جرائم الاعتداء على البيانات الاسمية المعالجة آلياً، أخذاً بالرأي القائل بعدم صلاحية النصوص التقليدية لمواجهة جرائم الاعتداء على الخصوصية في مجال المعلوماتية، نبين ذلك على النحو الآتي:

أولاً: بالنظر إلى الأفعال وفقاً للنصوص القانونية:

من خلال استعراض نصوص مواد قانوني العقوبات اليمني والجزائري، ومنها المواد: (255، 256، 257) من قانون العقوبات اليمني، والمواد: (303، 303 مكرر، 303 مكرر1) من قانون العقوبات الجزائري، يتضح بأن تلك المواد تقرر حماية الحياة الخاصة للأفراد، بإحاطة مراسلاتهم، أو محادثاتهم العادية أو الهاتفية بالحماية، المتمثلة بعدم فض الرسائل، أو إتلافها، أو الاطلاع على مضمونها، وكذا إحاطة أوضاعهم الحياتية بسياج من السرية بما يكفل منع الاعتداء عليها من فرد أو سلطة[2].

ومحل التجريم وفقاً لهذه المواد، يتمثل في الحصول على حديث أو صورة لشخص في مكان خاص، أو الحديث في الهاتف بصورة غير قانونية، إضافة إلى تجريم الاعتداء على سرية الاتصالات الشخصية عن طريق تجريم إذاعة أو تسهيل إذاعة المستندات أو التسجيلات المتحصل عليها، وبالتالي فإن الأفعال الداخلة في نطاق التجريم هي فعل الإذاعة لمضمون تسجيل أو مستند، وكذلك فعل تسهيل الإذاعة ويقصد به تقديم العون والمساعدة لإفشاء مضمون التسجيل أو المستند. بالإضافة إلى فعل الاستعمال للتسجيل أو المستند.

([1]) محمد عبيد الكعبي، مرجع سابق، ص 138 وما بعدها، كذلك فقد أخذ بهذا الرأي: حسام الدين اللاهوتي، الحماية القانونية للحياة الخاصة في مواجهة الحاسوب الآلي، ص10. وعمر الفاروق الحسيني، المشكلات الهامة في الجرائم المتصلة بالحاسوب الآلي وأبعادها الدولية، دراسة نقدية وتحليلية لنصوص التشريع المصري مقارنةً بالتشريع الفرنسي، ط2 ،1995، ص9، مشاراً إليهما لدى: عفيفي كامل عفيفي، مرجع سابق، ص294.

([2]) عفيفي كامل عفيفي، مرجع سابق، ص274.

وبهذا الشأن، نرى أن من تلك الأفعال ما يمكن أن ترتكب بواسطة النظم المعلوماتية، ومنها ما لا يمكن ارتكابها بواسطتها، ومن التي يمكن ارتكابها بواسطة نظم المعلوماتية على سبيل المثال جريمة فتح الرسائل البريدية، إذ يمكن أن تتحقق بفض الرسائل الإلكترونية المخزنة في البريد الإليكتروني، والفارق في الجريمتين هي الوسيلة فقط، حيث يتم فضها إما بطريقة يدوية للرسائل العادية، أو بطريقة إلكترونية للرسائل الإليكترونية، بعد القيام بعملية اختراق أو دخول إلى النظام المعلوماتي[1].

وإذا كان ذلك بالنسبة لفتح الرسالة، فإن نص المادة (255) من قانون الجرائم والعقوبات اليمني قد أوردت ألفاظاً أخرى في مجال الاعتداء على خصوصية الرسائل، وهي احتجاز الرسالة، أو إتلافها، أو اختلاسها، واقتصرت المادة (303) من قانون العقوبات الجزائري على فعل الإتلاف بجانب الفض، وبالنظر إلى تلك الأفعال يلاحظ بأنها أفعال مادية تقتضي إما الإتلاف المادي للرسالة بتمزيقها، أو الاختلاس كفعل مادي يتم به اختلاس الرسالة وحيازتها مادياً، أو احتجازها، بخلاف الألفاظ التي يمكن التعامل معها في مجال المعلوماتية؛ ومنها بدل الإتلاف التلاعب بالبيانات التي تضمنتها الرسالة أو محو تلك البيانات، وبالتالي فإذا كان بالإمكان تطبيق المادتين فيما يخص فتح أو فض الرسالة على الرسائل المخزنة في البريد الإلكتروني، فقد لا تتناسب مع باقي الأفعال، ويترتب على ذلك أن على المشرع اليمني والمشرع الجزائري إعادة النظر في نصي المادتين، وإضافة ما يدل على شمولية النص لخصوصية الرسائل الإلكترونية.

أما بالنسبة فيما يتعلق بخصوصية المحادثات التي تتم في مكان خاص، وذلك بعدم جواز التقاطها، أو تسجيلها، أو نقلها، وكذلك الصور، وفقاً لنص المادة (256) من قانون الجرائم والعقوبات اليمني، والمادة (303 مكرر) من قانون العقوبات الجزائري، فالملاحظ بأن القانون الجزائري بالنسبة لالتقاط أو تسجيل أو نقل المكالمات أو الأحاديث الخاصة أو السرية ، وكذلك التقاط وتسجيل ونقل صور شخص من مكان خاص، قد توسع في تجريمها أكثر من المشرع اليمني بالنص على تجريم ارتكاب تلك الأفعال بأي تقنية كانت، مما يوحي بإمكانية ارتكاب تلك الأفعال بالوسائل الإلكترونية، فيمكن إدخال التقاط أو تسجيل أو نقل المحادثات التي تتم عبر الإنترنت كمحادثات تتمتع بالخصوصية في التجريم، طالما تمكن المتهم من التقاطها أو تسجيلها أو نقلها، ويلاحظ أيضا بأن المشرع الجزائري قد اعتمد في تقرير خصوصية المحادثة على نوع المحادثة نفسها وليس على

([1]) ففي إحدى القضايا قضت محكمة دبي الابتدائية ببراءة متهم من تهمة فض الرسائل الواردة إلى بعض موظفي مؤسسة الإمارات للاتصالات، والمسجلة على البريد الإلكتروني للمؤسسة، وذلك بقيام المتهم بكسر كلمة السر التي تحول دون علم الغير واطلاعهم على الرسائل، ونسخ صور منها احتفظ بها على جهاز الحاسوب الخاص به، حيث اعتبرت المحكمة أن تلك الرسائل المنصوص عليها في قانون العقوبات لا تشمل الرسائل الإليكترونية، باعتبار أن هذه الرسائل استحدثت بعد صدور القانون. إلا أن محكمة الاستئناف ألغت هذا الحكم وأدانت المتهم عن هذه التهمة استنادا إلى أن المادة (380) من ق.ع التي تعاقب على فض رسالة بغير رضاء من أرسلت إليه، بغض النظر عن الوسيلة المستخدمة. يُراجع: محمد عبيد الكعبي، مرجع سابق، ص 143، هشام محمد فريد رستم ، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق، ص141.

المكان الذي تمت فيه من خلال العبارة: "المكالمات أو الأحاديث الخاصة أو السرية"، بخلاف المشرع اليمني الذي اعتمد في تفسير خصوصية المحادثة على خصوصية المكان وخصوصية المكالمة بقوله: "في مكان خاص أو عن طريق الهاتف"[1].

كما أن المشرع الجزائري قد توسع في تجريم جريمة التقاط أو تسجيل أو نقل المحادثات التي تجرِي في مكان خاص وكذلك الصور، وذلك ما لم يفعله المشرع اليمني، حيث جرم الشروع في تلك الجريمة[2].

أما نص المادة (256) من قانون الجرائم والعقوبات اليمني فإنه يلاحظ عليه بأنه قد جرم استراق السمع أو تسجيل أو نقل المحادثات في مكان خاص أو عن طريق الهاتف، وكلها أفعال يستدل من خلالها أنها تتم بطرق تقليدية دون تدخل التقنية الإلكترونية، ويتضح ذلك من ربط تلك الأفعال بالمكان الخاص أو عن طريق الهاتف كشرط لتحقق الجريمة، وبالتالي فإن نص المادة سالفة الذكر يقتصر تطبيقه على تلك الأفعال، ونفس الشيء بالنسبة لالتقاط الصور من مكان خاص، ويتميز التشريع اليمني بهذا الخصوص بتجريمه لاستراق السمع للمحادثات التي تجرِي في مكان خاص حتى وإن لم يكن الجاني مستخدماً في ذلك أي جهاز أو تقنية، بل إنه يكفي للتجريم الاستماع خلسة لتلك المحادثات بالأذن، وذلك لم يتضمنه التشريع الجزائري.

إضافةً إلى أن أفعال الإذاعة أو الإفشاء لمضمون تسجيل أو مستند، أو التسهيل لإذاعة مضمون التسجيل، أو المستند، أو الاستعمال لمضمون التسجيل أو المستند ولو في غير علانية، ولو كان ذلك أيضاً بغير رضاء صاحب الشأن. فهي كذلك مثلها مثل الأفعال السابقة تقتصر على الجانب المادي لا المعنوي.

ثانياً: بالنظر إلى النصوص المتعلقة بالاعتداء على الحياة الخاصة ومدى امكانية تطبيقها في حماية البيانات الاسمية المعالجة إلكترونياً:

لا جدل في أن دستور الجمهورية اليمنية، وكذلك دستور جمهورية الجزائر الديمقراطية الشعبية لم يتضمنا نصوصاً تتعلق بحماية البيانات الشخصية وحرية الوصول إلى المعلومات في مجال المعلوماتية، واقتصرت النصوص الموجودة على حماية المساكن

([1]) تعتمد بعض التشريعات والاتجاهات في تحديد خصوصية المحادثات المتعلقة بالحياة الخاصة على معيار المكان الذي ارتكبت فيه جريمة الاعتداء على الحياة الخاصة، فإذا كان مكاناً خاصاً فإن الجريمة تكون متحققة، أما إذا كان المكان عام فلا تتحقق الجريمة، بينما يعتد أصحاب الاتجاه الآخر في تفسير الخصوصية بالنظر إلى موضوع الخصوصية ذاتها، فلا تتحقق الجريمة إلا إذا كانت المحادثة تتعلق بأمور خاصة بالشخص، بغض النظر عن المكان الذي تم من خلاله الاستماع أو التقاط المحادثات الخاصة، أي حتى لو تمت تلك الأفعال في مكان عام. لمزيد من التفصيل يُراجع: عفيفي كامل عفيفي، مرجع سابق، ص277 وما بعدها.

([2]) الفقرة (3) من المادة 303 مكرر من قانون العقوبات الجزائري رقم (06- 23) المؤرخ في 20 ديسمبر 2006.

ودور العبادة ودور العلم من المراقبة أو التفتيش وكذا حرمة المراسلات والاتصالات وسريتها[1].كما أن دساتير الدول العربية لم تتضمن نصوصاً دستورية تقرر حماية للبيانات الشخصية[2]، مثلما فعلت أغلب الدساتير في الدول الأجنبية[3].

إضافة إلى أنه لا يوجد قانون يمني أو جزائري خاص بحماية الحياة الخاصة والبيانات الاسمية التي يتم تجميعها عن الأفراد من المخاطر الناتجة عن استخدام المعلوماتية وإنشاء بنوك المعلومات، وكذلك القوانين في الدول العربية، بخلاف القوانين في الدول الأوروبية والدول ذات التقدم التكنولوجي، حيث كيفت تشريعاتها مع ذلك التقدم وتأثيراته على الحياة الخاصة[4].

([1]) يُراجع: نص المادة (51) والمادة (52) من دستور الجمهورية، والمادة (39) والمادة (40) من الدستور الجزائري.

([2]) لم تتضمن أي من الدساتير العربية ذكر للبيانات الشخصية أو مسائل المعالجة الإلكترونية على نحو ما هو موجود في دساتير الدول الأجنبية، عدا النصوص المتضمنة لحماية الخصوصية كمبدأ عام، فلا يوجد أي دستور عربي ينص على حماية البيانات الشخصية صراحة، أو على حق المواطنين في معرفة بياناتهم الشخصية والسيطرة عليها بأي مظهر من مظاهر السيطرة، أو حتى طلب التصحيح أو التحديث أو التعديل. كما لا يوجد أي دستور عربي يقيد إجراءات جمع البيانات وتخزينها واستخدامها من قبل السلطات العامة بالخضوع للقانون أو للغرض المشروع. ولا يوجد حظر على استخدام وسائل التعريف وكشف الحريات المستخدمة في النظم القانونية العربية. يُراجع: يونس عرب، حماية الخصوصية، مقال منشور على موقع عرب قانون، على الرابط الإلكتروني:
www.arablaw.org/Download/Privacy_ArabWorld_Article.doc

([3]) تضمنت غالبية إن لم يكن كافة دساتير التسعينات في الدول الأجنبية نصوصاً واضحةً وصريحةً بشأن حماية البيانات الشخصية بما فيها: مفهوم خصوصية المعلومات، والحق في الوصول للمعلومات، حرية المعلومات، فقد أقرت صراحة حماية الحياة الخاصة ومنع انتهاكها والحق في خصوصية المعلومات وحماية البيانات الشخصية وتقييد أنشطة جمعها ومعالجتها ونقلها واستخدامها على نحو يوفر حماية لحياة الأفراد الخاصة من مخاطر تقنية المعلومات واستخداماتها في أنشطة معالجة البيانات الشخصية، كما أقرت الحق في الحصول على المعلومات من أي مصدر والوصول للسجلات والوثائق والمعلومات العامة، وقيدته باعتبارات المصالح الوطنية العليا وحقوق الأفراد، ومن تلك الدساتير: الدستور النمساوي تناول ذلك في المادة (1)، والدستور الإسباني في المادة (18)، والدستور البرتغالي في الفقرة (1) من المادة (35)، وفي أواخر عام 2004م، قامت كافة الدول الأعضاء بالاتحاد الأوربي بالتوقيع على الاتفاقية المنشأة لدستور أوروبا، والذي يقرر بأن كل فرد لديه الحق في حماية بياناته الشخصية أو الاسمية المتعلقة به. يُراجع: عفيفي كامل عفيفي، مرجع سابق، ص287، 288، ويُراجع أيضاً: يونس عرب، الخصوصية وحماية البيانات في البيئة العربية، منشور على الرابط الإلكتروني: www.arablaw.org/Download/Privacy_ArabWorld_Article.doc
وكذلك يُراجع: التقرير الدولي للخصوصية وحقوق الإنسان 2005، ترجمة: عمر محمد أبو بكر يونس، موقع الجمعية الليبية للقانون والإنترنت، تاريخ الدخول: السبت 2008/11/1، على الرابط الإلكتروني:
http://www.cyberlaw.org.ly/modules/news/print.php?storyid=13

([4]) تم إصدار قوانين جديدة تتعلق بحماية حق الفرد في الخصوصية وحماية البيانات ومنها: القانون الأسترالي الصادر في 9مارس 1982 والمعدل في 1983 بشأن حرية المعلومات، وينظم القواعد التي يتم بها نقل البيانات عبر الحدود، وقانون السجلات الخاصة الدنماركي رقم (293) الصادر في 8 يونيو 1978حيث يتطلب الحصول على ترخيص لنقل البيانات خارج الدنمرك في حالة تطلب تصريح بذلك لنشرها داخل الدنمرك، والقانون السويدي رقم (289) الصادر في 11 مارس 1972 والمعدل بالقانون رقم (334) لسنة 1979 والقانون رقم (446) لسنة 1982 حيث يتطلب لنقل البيانات عبر الحدود الحصول على تصريح بذلك من هيئة الرقابة على البيانات، والقانون رقم (78– 17) الصادر في 6 يناير 1978 والخاص بالمعلوماتية وملفات البيانات والحريات الفردية والعامة، كذلك قانون لوكسمبرج الصادر في 31 مارس 1979 الخاص بتنظيم المعالجة الآلية للبيانات الاسمية والذي يتطلب الحصول على تصريح قبل إنشاء أو استغلال أو استعمال بنك البيانات، وقانون نيوزلندا الصادر في 17 ديسمبر 1982 بشأن المعلومات الرسمية، والقانون الكندي الخاص بالتوصل للمعلومات، ونظيره الخاص بالخصوصية الصادران في 28 يونيو 1982 واللذان بدأ نفاذهما في أول يوليو 1983، والقانون الأمريكي الخاص بتقرير الائتمان العادل، لمزيد من التفصيل يُراجع: هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق، ص362 وما بعدها.

وبالرجوع إلى النصوص القانونية المتعلقة بالحياة الخاصة في القانون اليمني والقانون الجزائري، نجد أنهما قد اقتصرتا على حماية الحياة الخاصة بمظهرها المادي فحسب وذلك بتجريم فض، أو الاطلاع على المراسلات، أو إتلافها، وكذلك التقاط أو تسجيل أو نقل المحادثات التي جرت في مكان خاص أو عن طريق الهاتف، بالإضافة إلى التقاط الصور في مكان خاص، وغيرها من الأشياء المتعلقة بالخصوصية –إفشاء الأسرار من قبل المؤتمنين عليها، ضمانات التفتيش أو الضبط –واشترطت في كل تلك الأفعال أن تكون بدون رضاء صاحب الشأن.

وإذا ما أردنا تطبيق تلك النصوص على المساس بالبيانات الاسمية المتعلقة بالحياة الخاصة سواء أكانت مخزنة أم معالجة أم منقولة من نظام إلى آخر نجد بأن من تلك النصوص، نصوص اقتصرت على توفير الحماية الجنائية للمحادثات العادية، أو الهاتفية أو صورة الإنسان، وذلك يؤكد عدم صلاحيتها لتوفير الحماية الجنائية للمعلومات والبيانات المحررة أو المسجلة بأي وسيلة أخرى، حيث أن موضوع الحياة الخاصة أكبر بكثير من مجرد توفير الحماية للمحادثات والصور والمراسلات[1].

الجدير بالذكر، إن تلك النصوص ليس لها علاقة بمواجهة الاعتداء على الحياة الخاصة المتعلقة بالبيانات الاسمية، لأن تلك البيانات ذات كيان معنوي – موجات كهرومغناطيسية– بخلاف تلك النصوص التي وضعت لمواجهة الجريمة في صورتها المادية.

ويرجع ذلك إلى أن:

1. الحاسوبات تُعد إضافة ذات أوجه مستجدة وخطيرة نتيجة لما تقوم به من تخزين الكم الهائل من البيانات، ومعالجتها، ونقلها، بحيث تفوق ما كانت عليه الطرق اليدوية، ولا وجه للمقارنة[2].
2. إن مخاطر الحاسوبات لا تقتصر على تخزين الكم الهائل من البيانات ولا على السرعة في عملها، بل تتعدى ذلك إلى إمكانية استخراج تلك البيانات من ذاكرة الحاسوب، ومن ثم الاطلاع عليها، وقد تكون تلك البيانات متصلة بالحياة الخاصة، وبالتالي فإن ثمة خطورة ناتجة عن الحاسوبات الآلية تتمثل في تميزها عن الوسائل التقليدية بأنها تكون ذات ذاكرة مستديمة، يحتمل أن لا تُمْحَى البيانات المخزنة فيها، بل أنه توجد برامج يستطاع بواسطتها استعادة ما تم محوه[3].
3. إن الحاسوبات تمثل خطورة من حيث إمكانية مقارنة البيانات المخزنة بها، خاصةً عندما تكون مرتبطة بشبكة معلومات، ويترتب على ذلك إمكانية التوصل إلى بيانات تتعلق بالحياة الخاصة، ما كان سيتم التوصل إليها لولا تلك الأنظمة[4].

([1]) عفيفي كامل عفيفي، مرجع سابق، ص281.

([2]) عفيفي كامل عفيفي، المرجع السابق، ص294.

([3]) هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق، ص180.

([4]) هشام محمد فريد رستم، المرجع السابق، ص183.

وقد أظهرت الجهود الدولية إضافة إلى الدراسات الجنائية عدم كفاية النصوص التقليدية المتعلقة بإفشاء الأسرار، وحماية المحادثات والرسائل وغيرها من النصوص التي اقتصرت على الجانب المادي في الخصوصية، لحماية خصوصيات الأفراد في مواجهة تهديدات ومخاطر تقنية المعلومات، ويتطلب من المشرع اليمني والمشرع الجزائري أن يستجيبا لتلك الجهود بإصدار قانون لكل منهما لحماية الخصوصية، والتركيز على حماية البيانات في مواجهة أخطار الحاسوبات كبنوك للمعلومات، أو على الأقل أن يضمنا قانونا العقوبات في كلا البلدين نصوصاً قانونيةً لحماية الخصوصية في مجال المعلوماتية بما فيها البيانات الاسمية ذات العلاقة بالحياة الخاصة، كما فعلت مؤخرا بعض التشريعات العربية[1]، وخاصة المشرع الجزائري الذي عليه أن يستكمل المشوار الذي بدأ به في تجريمه المساس بأنظمة المعالجة الآلية للبيانات، وبهذا الصدد فإن على المشرع في كلا البلدين أن يستفيد من الاتفاقيات والتوصيات الدولية والتشريعات الاتفاقية الأوربية لحماية الأشخاص من مخاطر المعلومات المعالجة آلياً والتي أصبحت سارية المفعول من سنة 1985[2]، حيث راعت أمور أساسية لا يجب إغفالها ومنها:

أ- أن يكون الحصول على المعلومات بطرق وأساليب مشروعة مع توفر علم ورضاء صاحب الشأن.

ب- أن تستخدم البيانات في الغرض الذي أنشئت من أجله وفي أضيق الحدود، وأن تكون دقيقة وكاملة.

ج- أن تحاط البيانات بإجراءات وتدابير أمنية أثناء جمعها ومعالجتها وتخزينها و نقلها.

د- أن يكون للأشخاص الذين تخصهم حق الوصول إليها وحق الرقابة عليها لمعرفة مدى صحتها.

هـ- أن تكون السياسة العامة للتطوير والخطط والتطبيقات المتعلقة بالبيانات ذات الطبيعة الشخصية متاحة للكافة معرفتها.

و- مسألة المقصرين المنوط بهم التعامل مع تلك البيانات والمعلومات الهامة ذات الصبغة الشخصية.

([1]) ومن القوانين العربية التي جرمت الاعتداء على الخصوصية في مجال المعلوماتية قانون الإمارات العربية المتحدة رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات، وكذلك المرسوم السلطاني رقم (2001/72) المنشور في الجريدة الرسمية العمانية رقم 698 تاريخ 2001/7/1، وقانون مكافحة الجرائم المعلوماتية السعودي 2007، والقانون المصري رقم (175) لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات، وأفرد فصلاً خاصاً بالجرائم المتعلقة بالحياة الخاصة في مجال المعلوماتية مادة (25)، وقانون جرائم تقنية المعلومات الكويتي رقم (36) لسنة 2015.

([2]) تضمنت المبادئ المذكورة القواعد الإرشادية لمنظمة التعاون الاقتصادية والتنمية والتي أصبحت سارية المفعول من أول أكتوبر 1985بعد التوقيع عليها من عدد من الدول منها: النمسا، وبلجيكا، وكندا، والدنمرك، وفنلندا، وفرنسا، وألمانيا الاتحادية قبل اتحاد الألمانيتين، واليونان، وإيطاليا، واليابان، ولوكسمبورج، والمملكة المتحدة، والولايات المتحدة، وهولندا، والنرويج، وإسبانيا، وسويسرا، وتركيا. وهذه القواعد تعتبر إرشادية وغير ملزمة من وجهة نظر قانونية للدول الأعضاء ونطاق تطبيقها يشمل القطاعين الحكومي والخاص، وكذلك المعالجة الآلية وغير الآلية للبيانات، ونطاق تطبيقها يقتصر على الأشخاص الطبيعيين، وهي تتشابه مع القواعد الإرشادية من خلال المبادئ العشرة التي تضمنتها، إلا أنها أكثر تحديد ودقة، حيث تشمل المحاور التي تدور هذه المبادئ حولها على ضرورة كون البيانات صحيحة ودقيقة ومستمدة بطرق مشروعة، ومدة حفظها محدودة زمنياً، وعدم إفشائها في غير الأغراض المحددة لها، وحق الشخص المعني في التعرف عليها وتصحيحها ومحوها وتعديلها، وإحاطتها بسياج أمني يكفل حمايتها، وتحديد الأشخاص والجهات المخصص لهم الاطلاع أو الوصول إليها وإخضاعهم لقيد الالتزام بالسر المهني، كما أقرت مبدأ الانفتاح والمساءلة، للمزيد يُراجع: هشام محمد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق، ص356 وما بعدها.

الخاتمة:

من خلال ما تم عرضه في إطار هذا البحث الذي بيّن أركان جريمة الاعتداء على الخصوصية بصورتها التقليدية ومقارنها بالأفعال التي تقترف بواسطة تكنولوجيا المعلومات والاتصالات، ومن ثم معرفة مدى أمكانية تطبيق النصوص التقليدية في قانوني العقوبات اليمني والجزائري لمواجهة ذلك النوع المستحدث من الإجرام، ومدى الاحتياج لنصوص قانونية مستحدثة، فقد تم التوصل إلى عدد من النتائج إضافةً إلى عدد من التوصيات نوردها على النحو الآتي:

أولاً: النتائج: تبين من خلال هذا البحث:

1. إن الدساتير العربية لم تتناول الحماية للبيانات الشخصية والرسائل الإلكترونية، خلافاً للدساتير والقوانين الأجنبية.
2. إن القوانين العربية باستثناء بعض القوانين- في السنوات الأخيرة – لم تتناول الحماية للبيانات الشخصية والرسائل المعالجة إلكترونياً، أسوةً بالقوانين الأجنبية؛ ومنها القانون اليمني والجزائري، حيث لم يتضمنا نصوصاً قانونية تعنى بالحماية الجنائية للبيانات الشخصية المعالجة آلياً، باستثناء النصوص المستحدثة بالقانون الجزائري التي وفرت حماية للجرائم المعلوماتية المستحدثة.
3. تعامل المشرع اليمني والمشرع الجزائري مع جريمة الاعتداء على الخصوصية في مجال المعلوماتية على أن المساس بها يشمل الجانب المادي للحياة الخاصة فحسب دون الإخذ في الاعتبار التطور في الجانب التقني والمعلوماتي لتصبح فيه الحياة الخاصة مهددة بسبب المعلومات المخزنة والمعالجة والمنقولة من نظام معلوماتي إلى آخر.
4. إن أغلب التشريعات العربية – ومنها التشريع اليمني والتشريع الجزائري – لم تصدر قانوناً خاصاً لحماية خصوصية الإنسان والبيانات الاسمية عندما ترتكب الجريمة بواسطة تقنية المعلومات، كما لم تتضمن نصوصاً مستحدثة في قانوني الجرائم والعقوبات لكلا الدولتين بذات الخصوص.
5. اقتصرت الحماية الجنائية للحق في الخصوصية في قانوني الجرائم والعقوبات القانون اليمني الجزائري، على النصوص التقليدية، وهذه النصوص لا تفي كل صور الاعتداءات على الخصوصية.
6. عدم وجود الوعي الرقمي لاستخدام الهاتف الذكي ومواقع التواصل الاجتماعي ومواقع الانترنت كجزء أساسي في توفير الحماية للبيانات الشخصية.

ثانيا: التوصيات:

1- يوصي الباحث المشرع اليمني إصدار قانون للجرائم المعلوماتية وتضمينه النصوص القانونية التي توفر الحماية الجنائية للخصوصية في مجال المعلوماتية، أو تعديل نصوص قانون العقوبات وتضمينه النصوص التي توفر الحماية الجنائية من مخاطر الجرائم المعلوماتية؛ بما فيها الجرائم المتعلقة بالحياة الخاصة .

2- يوصي الباحث المشرع الجزائري بإدخال تعديلات في النصوص القانونية لقانون العقوبات وبالتحديد بالقسم السابع المعدل والمتمم لقانون العقوبات والخاص بتجريم المساس بأنظمة المعالجة الآلية للمعطيات، تتضمن تجريم الافعال التي ترتكب بها جريمة الاعتداء على الخصوصية في مجال المعلوماتية.

3- يوصي الباحث المشرع اليمني أن يقوم بالتدخل بنصوص قانونية تمنع أي جهة من إعطاء معلومات إلى جهة أخرى مختلفة عنها في الهدف، وإذا ما سمح قانوناً بمثل هذا الأمر فلابد وأن تحكمه ضوابط وقيود يتم من خلالها المحافظة على الحق في الخصوصية.

4- يوصي الباحث الجهات المعنية المرتبطة بتكنولوجيا المعلومات والاتصالات والجهات المعنية بتشريع وتطبيق القانون وضع برنامج توعوي وتكثيف الجهود في مجال التوعية، للحد من جرائم الاعتداء على الخصوصية في مجال المعلوماتية، ويتعين نشر الوعي الرقمي لمستخدمي أجهزة الحاسوب والأجهزة الذكية وكل ما يتعلق بوسائل تكنلوجيا المعلومات.

قائمة أهم المراجع

أولاً: المراجع العامة والمتخصص:.

1. د. أحسن بوسقيعة، الوجيز في القانون الجنائي العام، الديون الوطني للأشغال التربوية، الجزائر، 2002.
2. د. أحمد خليفه الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2005م.
3. د.خالد عبد الباقي الخطيب، الجرائم الواقعة على الأشخاص، مكتبة خالد بن الوليد، صنعاء، ج2، 2010م.
4. د.عبد الفتاح بيومي حجازي، الأحداث والإنترنت، دار الفكر الجامعي، الإسكندرية، ط1، 2002.
5. د. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، بدون ذكر دار النشر، ط2، 2000م.
6. د.مصطفى محمد موسى، أساليب إجرامية بالتقنية الرقمية، دار الكتب والوثائق القومية المصرية، القاهرة، ط1، 2003.
7. د.نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي، القاهرة، ط1، 2005.
8. د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، جمهورية مصر العربية، بدون تاريخ طبعة.

ثانياً: الرسائل العلمية:

1. د. أيمن عبد الحفيظ عبد الحميد سليمان، استراتيجية مكافحة الجرائم الناشئة عن استخدام الحاسوب الآلي دراسة مقارنة، رسالة دكتوراه في علوم الشرطة، أكاديمية الشرطة، القاهرة، 2003.
2. بارق منتظر عبد الوهاب لامي، جريمة انتهاك الخصوصية عبر الوسائل الالكترونية في التشريع الأردني، رسالة ماجستير، جامعة الشرق الأوسط، الأردن، 2017.
3. عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الإنترنت، رسالة دكتوراه، جامعة القاهرة، دار النهضة العربية، القاهرة، 2004.
4. محمد عبد الله الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع الشبكة الإنترنت، رسالة ماجستير، كلية الحقوق، جامعة القاهرة، 2004.
5. محمود أحمد عباينة، جرائم الحاسوب وأبعادها الدولية، رسالة ماجستير، الجامعة الأردنية، دار الثقافة، عمان، الأردن، 2005.

6. نهلا عبد القادر المومني، الجرائم المعلوماتية، رسالة ماجستير، الجامعة الأردنية، دار الثقافة، عمان، الأردن، الطبعة الأولى، 2007م.

ثالثاً: التشريعات:

1. دستور الجمهورية اليمنية.
2. دستور الجزائر.
3. القانون رقم 12 لسنة 1994 بشأن الجرائم والعقوبات اليمني.
4. القانون رقم (06 – 23) المؤرخ في 20 ديسمبر 2006 المعدل والمكمل لقانون العقوبات الجزائري.

رابعاً: مراجع الإنترنت:

http://www.legislationline.org/lawmaking/country/30

http://www.alflash.com/vb/showthread.php?t=2808

http://www.legislationline.org/lawmaking/country/30

www.arablaw.org/Download/Privacy_ArabWorld_Article.doc

www.arablaw.org/Download/Privacy_ArabWorld_Article.doc (1)

http://www.cyberlaw.org.ly/modules/news/print.php?storyid=13

http://www.openarab.net/laws/2006/laws8.shtml

http://www.escwa.un.org/information/meetings/editor/Download.asp?table_name=eventDetails&field_name=id&FileID=2030