جـامعـــة النجاح الوطنية

كليـــة الدراســـات العليـــا

جرائم الاعتداء على البيانات الشخصية

إعداد

ربى ظافر وليد حنتولي

إشراف

د. فادي شديد

قدمت هذه الرسالة استكمالا لمتطلبات الحصول على درجه الماجستير في القانون الجنائي من كلية الدراسات العليا، في جامعة النجاح الوطنية، نابلس- فلسطين.

2023

جرائم الاعتداء على البيانات الشخصية

إعداد

ربا ظافر وليد حنتولي

نوقشت هذه الرسالة بتاريخ: وأجيزت:

د. فادي شديد
المشرف الرئيسي
التوقيع

د.
الممتحن الداخلي
التوقيع

د.
الممتحن الخارجي
التوقيع

الإهداء

إلى أمي وحبيبة قلبي التي كانت سبب دخولي للماجستير فلولاها لما أكملت الطريق رحمها الله

وإلى أبي وأخواني أحمد ومهند ومحمد وسالي الذين كانوا بمثابة الغطاء و الصدر الرحب من كل ضيق

إلى خالاتي اللواتي منحن من الحنان ما لا يقدر بثمن ولا يمكن جنيه

إلى صديقاتي ورفيقات دربي اللواتي لم أعرف الحزن معهن وكنَ المرهم الذي يشفي من كل جرح

إلى أسرة مكتب الأستاذ عبد المجيد أبو عجور، حيث تدربت به وتتلمذت فيه وكان كنز من العطاء

والاجتهاد العلمي في مجال المحاماة وكان بمثابة مكتبة علمية لكل من يقصده

أقدم عملي هذا.

الشكر

الحمدُ للهِ لأنّ أرزاقَنا في خزائنِه، ونَواصينا بيدِه، والتدبيرَ تدبيرُه، الحمدُ للهِ أنّ الأمرَ أمرُه لا أمرَ عبادِه، والرحمةَ رحمتُه لا رحمةَ مخلوقاتِه، والهِباتِ والعَطايا كلُّها منهُ لا مِن سِواه.

أشكر مشرفي د. فادي شديد لإشرافه على رسالتي حيث كان معطاء ولم يبخل على بأي معلومة احتجتها أثناء دراستي ممتنة له كثيراً.

كما أشكر أعضاء لجنة المناقشة لقبولهم المشاركة في عضوية لجنة المناقشة متطلعة لما سوف يقدمه من نصح وارشاد .

الإقرار

أنا الموقع أدناه مقدم الرسالة التي تحمل عنوان:

جرائم الاعتداء على البيانات الشخصية

أقر بأن ما اشتملت عليه هذه الرسالة هي نتاج جهدي الخاص، باستثناء ما تمت الإشارة اليه حيثما ورد، وأن هذه الرسالة ككل أو أي جزء منها لم يُقدم من قبل لنيل أية درجة أو لقب علمي أو بحثي لدى أية مؤسسة تعليمية أو بحثية أخرى.

اسم الطالب: _____

التوقيع: _____

التاريخ: _____

فهرس المحتويات

جرائم الاعتداء على البيانات الشخصية

إعداد

ربى ظافر وليد حنتولي

اشراف

د. فادي شديد

الملخص

إن جرائم الاعتداء على البيانات الشخصية أصبحت جرائم العصر، ويعتبر موضوع جرائم الاعتداء على البيانات الشخصية من المواضيع الجديدة نوعاً ما، حيث أن قليلاً من الدول لاحظت خطورة الموضوع وتنبهت له عن طريق سن قوانين تحمي البيانات الشخصية وتجرم الاعتداء عليها ونتيجة لذلك انقسمت الدول إلى ثلاثة أقسام، القسم الأول سن تشريعاً خاصاً لجرائم الاعتداء على البيانات الشخصية مثل التشريع الفرنسي، والقسم الثاني وضع نصاً تشريعياً خاصاً بجرائم الإعتداء على البيانات الشخصية ولكنه جاء نص تنظيمي وغير كاف لتغطية جرائم الاعتداء على البيانات الشخصية جميعها مثل فلسطين، أما القسم الثالث فلم يشرع أي تشريع لحماية البيانات الشخصية بل اكتفى في حال وقوع أي اعتداء على البيانات الشخصية فقد غطى هذا الموضوع عن طريق التشريعات السارية داخل الدول مثل قانون الجرائم الإلكترونية وقانون الاتصالات وغيرها من القوانين ذات العلاقة، وتكمن الأهمية العلمية التي عالجتها الرسالة أنها تطرقت لجرائم الاعتداء على البيانات الشخصية منها استراق السمع، والتشهير، وتسجيل ونقل محادثات خاصة، والتقاط صور غير مشروعة، وبالتالي استخدامها بشكل مسيء، حيث أنه أصبح استخدام الوسائل التكنولوجية الحديثة وبالأخص الهواتف الذكية يسهل عملية الوصول إلى الملفات الخاصة منها الكاميرا والنصوص وتسجيل الصوت وغيرها وبالتالي تشكل اعتداءاً على البيانات الشخصية، بحيث يتم استخدام هذه البيانات لتحقيق أرباح مادية من قبل الشركات.

لتكون دولتنا متطورة وتحترم حقوق الإنسان وخصوصيته لابد من سن تشريع خاص بجرائم الاعتداء على البيانات الشخصية ينص على الجرائم التي يمكن أن تقع على البيانات الشخصية ومن أجل إيجاد تشريع مميز لا مانع من تطبيق فكرة الربط الأكاديمي للتحديد بدقة الجرائم التي يمكن أن تقع على البيانات الشخصية وما هي العقوبات الرادعة والتي تؤلم الجاني، ومن العقوبات الرادعة التي يمكن سنها بالتشريعات لتحقيق ردع للجناة هي عدم الاكتفاء بالغرامات المالية وذلك لأن الأرباح المالية التي سوف تعود على الشخص من الاعتداء على البيانات الشخصية أكبر بكثير من الغرامة وبالتالي عقوبة حجب الموقع أو الإغلاق الكلي أو الجزئي حققت ردعاً أكبر، ومن الاقتراحات التي يمكن تطبيقها الزام أصحاب الشركات ومقدمي الخدمات في حال وقع اختراق لأي من البيانات الشخصية الخاصة بالمواطنين أو الموظفين إخطار صاحب الشأن خلال 72 ساعة.

الكلمات المفتاحية: البيانات الشخصية، الجرائم الإلكترونية، قانون الاتصالات.

المقدمة

تعتبر البيانات الشخصية من الأمور الأساسية التي يستخدمها الأفراد بالحياة اليومية بشكل كبير من خلال التعامل مع الشركات أو أصحاب المصانع أو غيرهم، بحيث يقدم المواطن معلومات عن شخصه بما فيها العمر، والسكن، والجنس ، والحالة الاجتماعية، والحالة الصحية وهي تعتبر جزء من خصوصية الأفراد، ويقدمها بهدف الحصول على خدمات معينة مثل خدمة الإنترنت وغيرها من الخدمات، بالتالي يمكن أن يتم إساءة استخدام هذه البيانات سواء من سرقة، وانتحال الصفة، والدخول غير المصرح فيه، اصطناع الحسابات الشخصية، ربط البيانات الشخصية بمحتوى غير أخلاقي، سرقة البيانات البنكية وبطاقة الدفع الإلكتروني، والمساعدة في عملية نصب، أو التشهير (صيادي، 2019) ؛ ولحماية خصوصية المواطن سنت مجموعة من القوانين من أجل هذا الغرض منها قرار مجلس الوزراء بخصوص حماية البيانات الشخصية وقانون مكافحة الجرائم الالكترونية، ، قانون الاتصالات.

وقد كفلت القوانين احترام هذه الخصوصية كون الدستور قد كفل هذا الحق وأكد عليه، فجأت هذه القوانين لتحمي هذه الخصوصية من خلال فرض التزامات على الجهة المخولة بجمع البيانات الشخصية أو معالجتها، والنص على حقوق لأصحاب هذه البينات منها عدم جمع هذه البيانات إلا بإذنه وإخطاره بالغرض التي جمعت لأجله، والمدة التي سوف تحفظ فيها البيانات، وكذلك يجب أن يكون جمع هذه البيانات لأغراض مشروعة وملائمة للغرض التي جمعت لأجله، وإلا سوف يُسأل قانوناً ويكون أمام جريمة قد نص عليها القانون وفق مبدأ لا جريمة ولا عقوبة إلا بنص (القانون الأساسي الفلسطيني المعدل لسنة 2003).

كما أن التطور التكنولوجي الكبير كان سبب في أن يتم اختراق هذه البيانات وتسريبها خاصة أنه في فضاء الانترنت يكون متاح للمجرم الدخول بشكل أسرع لهذه البيانات، كذلك تنظيف مسرح الجريمة والخروج منها، وبالتالي أصبح هناك اعتراف بالدليل الرقمي بحيث أصبح يقدم لنيابة و المحكمة وهناك معاير محددة للأخذ به (الحارث م.، 2018) .

وقد لجأت الكثير من الدول حديثاً لوضع قانون خاص لحماية البيانات الشخصية مثل فرنسا، فمنها من وضع تعريفاً للبيانات الشخصية حيث عرفها أنها البيانات التي تهم الشخص وتشكل بياناً له مثل السكن، العمر، مكان الإقامة، الرأي السياسي، الصحة العقلية، الصحة النفسية، الدخل الشهري، المستوى الاقتصادي، وغيرها من البيانات التي لا يرغب الشخص بالإفصاح عنها أو نشرها على وجه العموم إلا بإذنه (الحارث و الطويريقي، 2018)، وهناك فرق بين البيانات الشخصية العادية و البيانات الشخصية الحساسة مثل التوجيه السياسي وبالتالي رفع مستوى الحماية لمثل هذه البيانات مع الإشارة إلى أن أغلب القوانين كفلت الحماية ليس فقط للمواطنين بل للأجانب أيضاً.

وبخصوص التطور التاريخي لموضوع حماية البيانات الشخصية من الاعتداء، نجد أن المجتمعات الغربية قد التفتت لحماية هذا الموضوع قبل المجتمعات الشرقية، وخاصة من ناحية وضع تشريعات تسعى لحماية الحق في الخصوصية ومن هذه الوثائق وثيقة المانغا كارتا عام 1215 والتي كان بموجبها قد وضع حدود لتحكم السلطات السياسية في الدولة، ثم تطور الأمر لمواد الاثني عشر في ألمانيا عام 1525 وبعد ذلك جاء إعلان الجمعية الوطنية الفرنسية حول حقوق الإنسان عام 1789 كوليدة لثورة الفرنسية، وبعد ذلك صدرت شريعة الحقوق في الولايات المتحدة الأمريكية عام 1791 وهذه النصوص أكدت على احترام خصوصية وحقوق الانسان بعد ما كان الانسان يعامل معاملة السلعة يباع ويشترى ومع تتطور النصوص ازداد احترام حقوق الانسان وخصوصيته أما بخصوص الدول العربية فلجأت لسن قوانين تحمي حق الانسان إلا أنها في بداية الأمر لم تصدر تشريعات تنص على حق الخصوصية أو حماية البيانات الشخصية بشكل صريح أو واضح انما جاء في دساتيرها نص على كفالة حق الشخص في الحرية الشخصية ومثال ذلك الدستور المصري في المادة خمس واربعين منه " إن لحياة المواطن حرمة يحميها القانون" والدستور القطري نص فيه في المادة 37 على" أن لخصوصية الإنسان حرمتها فلا يجوز تعرض أي شخص لأي تدخل في خصوصيته أو شؤون أسرته أو مسكنه أو مراسلاته أو أي تدخلات تمس شرفه أو سمعته إلا وفقاً لأحكام القانون وبالكيفية المنصوص عليها فيه"، وبعد ذلك تطورت قوانين حماية

البيانات الشخصية بتطور الزمن وبإدراك الدول لضرورة وجود تشريع يحمي البيانات الشخصية كونها أصبحت تستخدم بشكل أكبر وخصوصاً أن الإنترنت ووسائل الاتصالات الالكترونية أصبحت تستخدم بشكل أسرع (فجم، 2021).

أهمية الدراسة

أهمية نظرية:

تكمن في بيان وجهات النظر في ضرورة حماية البيانات الشخصية، حيث أن هناك بعض من وجهات النظر المختلفة فالمشرع الفرنسي تبنى وجهة نظر قائمة على ضرورة إدراج قانون خاص لحماية البيانات الشخصية، أما وجهة النظر الأخرى فقد لجأت بعض الدول إلى عدم سن قانون يحمى البيانات الشخصية ويجرم الاعتداء عليها بل استندت إلى قوانين وطنية أخرى مثل قانون الجرائم الالكترونية وهذا ما تبناه المشرع العراقي، وهناك دول أخرى جمعت بين الجهتان عن طريق إدراج قانون لحماية البيانات الشخصية وفي حال لم يغطي هذا القانون حماية كافية للبيات يتم اللجوء إلى قوانين أخرى مثل قانون الجرائم الالكترونية وخير مثال على ذلك فلسطين حيث سن قرار صادر عن مجلس الوزراء نظم موضوع حماية البيانات الشخصية لكنه احتوى على مادة واحدة وفي حال وقع اعتداء على البيانات الشخصية يتم اللجوء لقانون الجرائم الالكترونية وقانون الاتصالات ، وسوف تبين الباحثة وجهة نظرها من خلال هذه الدراسة.

أهمية عملية:

تكمن أهمية الدراسة من الناحية العملية في أنها عالجت أمور حياتية نعيشها بشكل يومي، حيث أنه في كثير من الأحيان نتعرض لمضايقات في حياتنا اليومية لبيناتنا الشخصية منها استراق السمع، والتشهير، وتسجيل ونقل محادثات خاصة، وبالتالي استخدامها بشكل مسيء، حيث أنه أصبح استخدام الوسائل التكنولوجية الحديثة وبالأخص الهواتف الذكية يسهل عملية الوصول إلى الملفات الخاصة منها الكاميرا والنصوص وتسجيل الصوت وغيرها أي تسهيل عملية الوصول للبيانات الشخصية مع العلم أنه في حال

تم استغلال هذه البيانات دون اذن صاحبها نكون أمام اعتداء على البيانات الشخصية، بحيث يتم استخدام هذه البيانات لتحقيق أرباح مادية من قبل الشركات وبالتالي جاءت الحاجة لسن قانون لحماية البيانات الشخصية.

وبالاطلاع إلى الواقع العملي نجد أن بياناتنا الخاصة أكثر من يستخدمها هي مؤسسات الإقراض، والبنوك، ومؤسسات الاتصالات، والخدمات عن طريق منح ترخيص لشركات؛ لتوفير خدمات مثل الانترنت، بالتالي هناك معاير لالتزام هذه الشركات بحفظ البيانات الشخصية خاصة خدمات الإنترنت، بحيث تبحث هذه الدراسة في مدى التزام هذه الشركات والمؤسسات بالحفاظ على البيانات الشخصية للفرد.

كما تبحث هذه الدراسة في بيان ومعرفة النصوص التي تجرم الاعتداء على البيانات الشخصية وفق مبدأ لا عقوبة ولا جريمة إلا بنص، كذلك تطرقت الباحثة لموضوع هذه الجرائم من الناحية الدولية كونها أصبحت جرائم عابرة للقارات، وبالتالي بيان النصوص القانونية التي يتم الارتكاز عليها لتجريم الاعتداء على البيانات الشخصية دولياً، وماهي الاتفاقيات التي جرمت هذه الاعتداء .

أهداف الدراسة

1. توضيح ماهية البيانات الشخصية.
2. بيان أنواع جرائم الاعتداء على البيانات الشخصية التي يتم ارتكابها سواء داخل إقليم الدولة أو كانت الجريمة خارج إقليم الدولة والقوانين التي تغطيها داخلياً او دولياً.
3. توضيح أهمية حماية البيانات الشخصية من العبث.
4. بيان الالتزامات التي تقع على الجهات التي تجمع هذه البيانات سواء شركات خاصة أو جهات عامة مثل دوائر الإحصاء.
5. توضيح ما هي طرق حماية بياناتنا الشخصية من الاعتداء، وما هي الوسائل التي يمكن اعتمادها لحماية بياناتنا الشخصية .

6. بيان النصوص القانونية التي نظمت موضوع حماية البيانات الشخصية.

محددات الدراسة

المحددات الموضوعية: إن الحدود الموضوعية في هذه الدراسة تكمن في القرار بقانون بشأن الجرائم الإلكترونية رقم 10 لسنة 2018، وقانون الاتصالات الفلسطينيين رقم 3 لسنة 1996، ، والقرار الصادر عن مجلس الوزراء بخصوص حماية البينات الشخصية رقم 3 لسنة 2019، من خلال دراسة النصوص التي تتعلق بتجريم الاعتداء على البيانات الشخصية وتحليل هذه النصوص، كما تطرقت الباحثة إلى الاتفاقيات الدولية التي حفظت حق الانسان بحفظ بيانته الشخصية مثل الاتفاقية الأوربية لحقوق الإنسان 1950 والنظام الأوربي العام لحماية البيانات الشخصية 2016، وما هي القوانين التي استندت عليها هذه الاتفاقيات وغطت الدراسة القوانين والقرارات السارية في الضفة الغربية .

منهج الدراسة

استخدمت الباحثة المنهج الوصفي التحليلي من خلال تحليل النصوص التي تجرم الاعتداء على البيانات الشخصية، ودراستها لمعرفة غاية المشرع من وراء التجريم، وكذلك استرشدت الباحثة بالمنهج المقارن وذلك من خلال الاطلاع على القوانين في الدول الأخرى مثل القانون الفرنسي ، وكيفية حماية خصوصية البيانات الشخصية وتجريم الاعتداء عليها وتوضيح أنواع الجرائم التي يمكن أن تقع على البيانات الشخصية وطرق الحماية منها وبيان الالتزامات التي وضعتها القوانين المختلفة على الجهة المتحكمة والمعالجة للبيانات .

الدراسات السابقة

تمثلت أبرز الدراسات السابقة التي تناولت الموضوع بما يلي:

1. **سوزان عدنان الاستاذ، انتهاك حرمة الحياة الخاصة عبر الانترنت** :قسم القانون الجنائي كلية الحقوق جامعة دمشق، المجلد 29 العدد الثالث 2013، تحدثت هذه الرسالة عن حق الخصوصية

وحرمة الحياة الخاصة في الجانب الأول، ومن ثم تناولت الاعتداء على الحياة الخاصة بواسطة الوسائل الحديثة مثل الإنترنت والنصوص القانونية التي تجرم الاعتداء على حرمة الحياة الخاصة.

2. **د. مروان الزعبي، انتهاك خصوصية المعلومات المتداولة على مواقع التواصل الاجتماعي التي يرتكبها الزوجين ضد بعضهم البعض في التشريع الأردني.** إربد الأردن، تحدثت الرسالة عن صور انتهاك خصوصية المعلومات المتداولة على مواقع التواصل الاجتماعي وفق قانون العقوبات الأردني وتحدثت أيضاً عن صور انتهاك خصوصية المعلومات المتداولة على مواقع التواصل الاجتماعي وفق قانون الجرائم الالكترونية وفي نهاية الرسالة تحدثت عن دور العلاقات الزوجية في تبرير جرائم انتهاك خصوصية المعلومات المتداولة على مواقع التواصل الاجتماعي.

3. **بارق منتظر عبد الوهاب لامي، جريمة انتهاك الخصوصية عبر الوسائل الالكترونية في التشريع الاردني (دراسة مقارنة)، قسم القانون العام،** كلية الحقوق جامعة الشرق الأوسط أيار 2017 تحدثت الرسالة عن تعريف الحياة الخاصة في الفقه والقضاء والقوانين الوضعية وبيان مفهوم الحياة الخاصة وتحديد نطاق ومجال الخصوصية عبر الانترنت كذلك تطرقت الرسالة للحماية الدولية للحق في الحياة الخاصة وبيان صور انتهاك هذا الحق، وبيان موقف التشريعات المقارنة مثل العراقي والاردني في حماية الحياة الخاصة وقد بينت الدراسة أيضاً لموضوع حرية الوصول للمعلومات في العصر التقني.

4. **أسماء علي سالم رشيد الشامسي، جرائم الاعتداء على حرمة الحياة الخاصة للأشخاص** (في ظل المرسوم بقانون رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات) دراسة مقارنة، جامعة الإمارات العربية المتحدة، كلية القانون، قسم القانون العام 2018 تحدثت الدراسة عن محل السلوك الجرمي والركن المادي وشروط تحققه في جرائم الاعتداء على خصوصية الأشخاص ومحل السلوك الجرمي والركن المادي لتجريم المتعلق بالمحادثات والاتصالات وتحدثت أيضاً محل السلوك الجرمي

والركن المادي لتجريم المتعلق بتعديل أو معالجة الأحاديث والصور وتحدثت أيضاً عن أسباب إباحة الاعتداء على خصوصية الأشخاص.

قد تميزت هذه الدراسة عن الدارسات السابقة في أنها تحدثت عن تعريف البيانات الشخصية، وأهمية حفظها على صعيد المواطن وخصوصيته، بالإضافة إلى الالتزامات التي تقع على الجهة المناط بها جمع البيانات الشخصية، ومن ثم تطرقت الباحثة إلى موضوع جرائم الاعتداء على البيانات الشخصية، وأنواعها، والحماية التشريعية (قرار مجلس الوزراء للبيانات الشخصية، قانون الجرائم الإلكترونية، قانون التجارة، قانون الاتصالات الفلسطيني)، وتطرقت الباحثة إلى طرق الحماية من جرائم الاعتداء على البيانات الشخصية، وفي نهاية الدراسة تطرقت الباحثة لموضوع جرائم البيانات الشخصية على المستوى الدولي من حيث طبيعتها وكيفية ارتكابها وملاحقتها، والسند القانوني والاتفاقات الدولية التي يمكن من خلالها تجريم الاعتداء على البيانات الشخصية.

إشكالية الدراسة

سوف تعالج الباحثة من خلال هذه الدراسة اشكالية عامة تتمثل في ما مدى كفاية الحماية القانونية الجزائية للبيانات الشخصية من أية اعتداءات تقع عليها في التشريعات السارية في فلسطين؟ وتفرع عن هذه الإشكالية العديد من التساؤلات :

1. ما هيه البيانات الشخصية ؟
2. ما هي الالتزامات التي تقع على الجهة المنوط بها جمع البيانات الشخصية؛ لكي لا يتشكل اعتداء على هذه البيانات ؟ .
3. توضيح طبيعة وأنواع جرائم الاعتداء على البيانات الشخصية سواء تم ارتكابها على مستوى محلي أو على مستوى دولي؟.
4. ما هي النصوص التشريعية السارية في فلسطين والتي تجرم الاعتداء على البيانات الشخصية ؟.

مخطط الدراسة

سوف تقوم الباحثة بالإجابة عن الإشكالية العامة، من خلال بيان حماية البيانات الشخصية من الاعتداء عليها في الفصل الأول، ومن ثم البحث في خرق قواعد الحماية المقررة للبيانات الشخصية في الفصل الثاني.

الفصل الأول

حماية البيانات الشخصية من الاعتداء عليها

تعتبر البيانات الشخصية من الأمور الخاصة بالإنسان والتي يحظر الاطلاع عليها أو الاعتداء عليها بأي نوع من أنواع الاعتداء، سواء الاعتداء على الرسائل أو المحادثات أو استراق السمع أو نقل المحادثات وغيرها، وبمراجعة مراحل التجريم التشريعي لجرائم الاعتداء على البيانات الشخصية نجد أن المشرع بدأ حديثاً بالاهتمام بموضوع البيانات الشخصية، وجاء ذلك استناداً إلى التطور التكنولوجي السريع عن طريق الإنترنت، حيث بدأت الشركات العالمية تستغل البيانات الشخصية لأهداف تجارية دون موافقة أصحابها، وكذلك الجهات السياسية التي بدأت تستغل هذه البيانات لخدمة مصالحها مثل الدعايات الانتخابية وغيرها ولكي نفهم موضوع حماية البيانات الشخصية من الاعتداء عليها سوف نتطرق لموضوع ماهية البيانات الشخصية في المبحث الأول والأساس القانوني لحماية البيانات الشخصية في المبحث الثاني.

المبحث الأول: ماهية البيانات الشخصية

تعتبر البيانات الشخصية من الأمور الخاصة بالإنسان مثل الصور الخاصة، تسجيل الصوت، المكالمات الخاصة، وغيرها وبالتالي الشخص الطبيعي أو حتى المعنوي لا يرغب بتحويل هذه البيانات من خاصة إلى عامة يطلع عليها جميع الناس ومن هنا جاءت علة تجريم الاعتداء على هذه البيانات، وسوف تدرس الباحثة في هذا المبحث تعريف البيانات الشخصية وأنواعها في المطلب الأول، وأهمية حفظ البيانات الشخصية في المطلب الثاني.

المطلب الأول: تعريف البيانات الشخصية وأنواعها

وتعتبر الحياة الخاصة بالإنسان من الأمور التي تخصه والتي لا يجوز الاطلاع عليها من قبل الأخرين، وبالاطلاع على واقع حماية الحياة الخاصة للإنسان نجد أن احترام الحياة الخاصة موجود منذ القدم ، فقد ورد في كتاب الله عز وجل الكثير من الآيات جاءت لتحدثنا عن آداب الحياة الخاصة، وانه لا بجوز

الدخول إلى الأماكن الخاصة بالأفراد إلا بعد الحصول على إذن من أصحابها أي الاستئذان، قال تعالى في كتابه الكريم : ﴿يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ لَا تَدۡخُلُواْ بُيُوتًا غَيۡرَ بُيُوتِكُمۡ حَتَّىٰ تَسۡتَأۡنِسُواْ وَتُسَلِّمُواْ عَلَىٰٓ أَهۡلِهَاۚ ذَٰلِكُمۡ خَيۡرٞ لَّكُمۡ لَعَلَّكُمۡ تَذَكَّرُونَ ٢٧ فَإِن لَّمۡ تَجِدُواْ فِيهَآ أَحَدٗا فَلَا تَدۡخُلُوهَا حَتَّىٰ يُؤۡذَنَ لَكُمۡۖ وَإِن قِيلَ لَكُمُ ٱرۡجِعُواْ فَٱرۡجِعُواْۖ هُوَ أَزۡكَىٰ لَكُمۡۚ وَٱللَّهُ بِمَا تَعۡمَلُونَ عَلِيمٞ ٢٨ لَّيۡسَ عَلَيۡكُمۡ جُنَاحٌ أَن تَدۡخُلُواْ بُيُوتًا غَيۡرَ مَسۡكُونَةٖ فِيهَا مَتَٰعٞ لَّكُمۡۚ وَٱللَّهُ يَعۡلَمُ مَا تُبۡدُونَ وَمَا تَكۡتُمُونَ ٢٩﴾ صدق الله العظيم سورة النور من القران الكريم أية رقم 26،27،28 (النور).

وحيث تلاحظ الباحثة بأن البيانات الشخصية للإنسان هي محل حماية في التشريع الإسلامي، حيث تم حماية تلك البيانات من خلال تحريم دخول المساكن بدون استئذان، حيث أن دخول المساكن من شأنه أن يكشف الخصوصية من البيانات والأمور التي لا يرغب الشخص بأن يطلع عليها عمومية الناس ، وبالتالي جاء الإسلام حريصاً على حفظ خصوصية الأفراد حيث نص على ضرورة الاستئذان قبل الدخول لمنازل الأخرين وينعكس ذلك على كل ما يتعلق بما هو خاص من رسائل أو أحاديث خاصة بالأفراد بالتالي ضرورة احترام هذه الخصوصية وحفظها من الاعتداء.

وقد ظهرت هذه الحماية في الطابع الدولي وهذا ما أكد عليه العهد الدولي حيث جاء في المادة 17 منه "من حق كل شخص أن يحميه القانون من التدخل أو المساس في خصوصيته أو شؤون أسرته أو بيته أو مراسلاته ولا لأي حملات غير قانونية تمس شرفه أو سمعته " (العهد الدولي للحقوق المدنية والسياسية المادة 17، 1966). ولكن ترى الباحثة أن العهد الدولي تحدث بوجه العموم عن الحياة الخاصة، ولم يدخل بأي تفصيل بخصوص جرائم الاعتداء على البيانات الشخصية، حيث أنه لم يتحدث عن حق الخصوصية وعن عناصره، وشروط استخدامه أو تبعيات الاعتداء عليه وغيرها من الأمور بل كان حديثه بوجه العموم دون أي تخصيص.

كما نصت المادة 3 من الاتفاقية الأوروبية بشأن حماية الأشخاص من المعالجات الآلية للبيانات ذات الطبيعة الشخصية، الموقعة في 28 يناير عام 1981 حيث عرفت البيانات الشخصية بأنها "معلومات تتعلق أو ترتبط بشخص طبيعي محدد أو قابل للتحديد" (الاتفاقية الأوربية لحقوق الانسان 1950 المادة 3).

ومن التطبيقات العملية لحفظ الحياة الخاصة وضرورة احترامها حكم محكمة النقض المصرية رقم 9542 في قضية قيام محمد رمضان، وهو مغني مشهور في مصر قام بالتقاط صورة في الطائرة وظهر فيها قبطان الطائرة وتم نشر هذه الصورة دون إذن صاحبها، وبالتالي اعتبرت المحكمة القيام بمثل هذه الفعل خطأ يستحق صاحبه التعويض إذا سبب ضرر، وقضت المحكمة أنه يجب بمثل هذه الحالات الأخذ بالأذن الصريح وتفسير الإذن الضمني تفسير ضيق، وبالتالي استقرت محكمة النقض على مبدأ تعويض صاحب الصورة في حال نشرها دون إذن صاحبها تعويضاً يتفق مع الضرر الواقع، وكذلك حكمت المحكمة بأن إذن التصوير لا يشمل إذن النشر حيث جاء في حيثيات القرار أن محكمة النقض رفضت طعن الفنان محمد رمضان على حكم المحكمة الاقتصادية التي ألزمته بدفع 6 مليون جنيه للشخص الذي نشر محمد رمضان صورته في كبينة الطائرة تعويضاُ عن الأضرار المادية والأدبية التي لحقت به، حيث قام رمضان بنشر هذه الصورة في مقطع على اليوتيوب وتسبب ذلك بإقالة الطيار من وظيفته وحرمانه من الطيران مدى الحياة، وقد كان الطيار قد سمح له بالتقاط الصورة دون نشرها (عرب نيوز، 2022) . وهنا المحكمة انصب قرارها بشكل واضح على احترام الخصوصية، حيث حددت بشكل صريح أن الموافقة على التقاط صورة مع شخص ما لا يعني الموافقة على نشرها ووضحت المحكمة أن الموافقة لا بد من أن تكون صريحة وأن الموافقة الضمنية لا بد من تفسيرها تفسيراً ضيقاً ويحسب التعويض بناءً على الضرر الواقع سواء مادي أو معنوي او كليهما.

الفرع الأول: أنواع البيانات الشخصية

يمكن تصنيف البيانات الشخصية على أنها حقول، بحيث تكون البيانات الشخصية المتشابهة في حقل واحد، والقوانين والتشريعات لم تتطرق لموضوع أنواع البيانات الشخصية، ولكن الذين قاموا بتصنيف البيانات الشخصية هم الفقهاء والعلماء؛ لتسهيل التعامل معها وستقوم الباحثة بتوضيح أنواع البيانات الشخصية بشكل تقريبي (موقع الجزيرة ، 2022).

ومن خلال الاطلاع على النصوص القانونية التي تتعلق بالبيانات الشخصية يتضح بأن هناك فرق بين البيانات والمعلومات هو أن البيانات والتي لها مصطلح آخر، وهو المدخلات (المادة الخام للمعلومات)، سواء تم تسجيلها بالحاضر أو بالماضي أو بالمستقبل، و يمكن أن تكون مستقلة مثلاً الاسم فاطمة، العمر 27، أما المعلومات هي الناتجة المفيدة التي يتم استخلاصها من معالجة البيانات أي المخرجات، والمعلومات هي البيانات التي تم استخلاصها ومعالجتها للحصول على الفائدة منها مثال أحمد، 27، قطر، الهندسة، هذه بيانات عملية يتم معالجتها وتنظيمها و تخرج لنا معلومات لتصبح بالشكل التالي أحمد هو مهندس يعمل في قطر ويبلغ من العمر 27 عاماً (بهام، 2019).

وما يؤكد هذا الفرق هو ما توصلت اليه محكمة العدل الأوربية حيث قضت: أن البيانات الشخصية لا تعتبر شخصية إلا اذا كان هذا البيان يؤثر على حق صاحبه بالخصوصية سواء في حياته العملية أو الشخصية وبالتالي ذكر أسم الشخص لدى الجهة المتحكمة لا يعتبر بالضرورة بيان شخصي (الحميد د.، قرار لمحكمة العدل الأوربية في قضية ديوران ضد هيئة الخدمات المالية، 2003).

ويعتبر بصمة الإصبع من البيانات الشخصية وهذا ما جاء بقرار لمحكمة العدل الأوروبية، حيث وضحت المحكمة أن بصمات الأصابع هي بيانات فريدة عن الأشخاص، وهي بيانات تسمح بتحديد هوية الشخص بدقة، وجاء قرار محكمة العدل الأوربية بناءً على دعوى أقامها المدعي للحصول على جواز سفر، حيث قدم طلب للحصول على هذا الجواز وطلبت منه هذه الجهة بصمات إصبع ولكنه رفض، وبالنتيجة توجه

إلى محكمة العدل الأوروبية التي قضت أنه غير ملزم بتقديم بصماته التي تعتبر بياناً شخصياً له (الحميد د.، قرار لمحكمة العدل الدولية قضية شوارز ضد بوشام، 2014). وترى الباحثة أن المحكمة هنا كانت صائبة في قرارها كون بصمات الأصابع بيانات شخصية يترتب على حصول الغير عليه ضرر قد يقع على صاحب الشأن؛ لأنه يمكن أن يكون قد ربط العديد من كلمات المرور أو أقفال البيت ببصمة الإصبع أو خزائن مالية وبالتالي يقع عليه ضرر في حال تم منحها للغير.

وقد عرَف المشرع الفرنسي البيانات الشخصية بأنها البيانات التي تساعد في التعرف على الأشخاص ويكون ذلك بشكل مباشر أو غير مباشر، سواء خضعت هذه البيانات للمعالجة من قبل شخص طبيعي أو معنوي (الحماية القانونية للبيانات الشخصية، 2022).

ولتميز البيانات الشخصية عن غيرها من البيانات العامة التي إذا تم نشرها لا تقع أي مسؤولية جنائية أو مدنيه على الناشر هي أن البيانات الشخصية تتعلق بشخص معين أو بمعيشة محددة أو بمواضيع حساسة مثل الحالة الصحية، الانتماء الديني والسياسي، والظروف الاقتصادية والاجتماعية التي يمر بها الشخصين، بالإضافة إلى أن قائمة البيانات الشخصية ممكن أن تختلف من شخص لآخر مثل الشخصيات السياسية يعتبر مكان السكن قد يكون بيان شخصي أو تعرضه لحالة صحية معينة بيان شخصي أخر لا يرغب بالإفصاح عنه وترتب ضرر على نشر هذه البيانات على المستوى الدول وبالتالي تختلف مستويات الحماية من شخص لآخر وحسب الظروف المحيطة بالشخص، مع العلم أنه في حال سمح الشخص بمشاركه بياناته للعموم هنا نخرج من إطار حمايه البيانات الشخصية لأنه أفصح عنها وبالتالي زالت الحماية القانونية عنها (مكتب حماية البيانات التابعة للاتحاد الدولي لجمعيات الصليب الاحمر والهلال الاحمر.).

الفرع الثاني : أنواع البيانات الشخصية الأكثر انتشارً

بعد الدراسة والبحث وجدت الباحثة عشرة أنواع للبيانات الشخصية وهي كالتالي (موقع الجزيرة، 2021):

1. بيانات تتعلق بشخص المستخدم أي البيانات التي تتعلق بالتعريف عن شخصه، وكيانه مثل الاسم، تاريخ الميلاد، العنوان.
2. البيانات السلوكية: وهي البيانات التي تعنى بسلوك الشخص ونشاطاته، سواءً السياسية أو الاجتماعية أو الاقتصادية وغيرها، ويتم الحصول على هذه البيانات في الوقت الحالي من خلال تتبع سلوك الشخص من خلال مواقع التواصل الاجتماعي باعتبارها طريقة أسرع في الحصول على البيانات بداية من مراقبة حركة الماوس إلى أي التطبيقات أو المواقع الأكثر زيارة (Dynamics ، 2023) .
3. بيانات الموقع الجغرافي حيث قد يقوم الكثير من الأشخاص بتحديد مواقعهم الجغرافية وبالتالي يكونوا قد قدموا بياناً عن موقعهم من خلال تحديد الجي بي اس، وغيرها من التطبيقات، وكذلك يقدم الشخص بياناً لموقعه من خلال رغبته للحصول على خدمات معينة مثل الإنترنت عن طريق تحديد مكان السكن لموظفي الخدمة(aws, 2023) .
4. بيانات عن رغبات الأشخاص : وهذا يظهر بشكل كبير من خلال قيام الشخص بالتفاعل مع منتجات معينة وتخطيه لمنتجات أخرى، وهذه البيانات تساعد شركات التسويق في تحديد من هو المنتج الأكثر طلباً أو أكثر شراء وبالتالي هنا هذه البيانات يمكن استغلالها اقتصادياً من قبل المنتجين دون رغبة الشخص بالإفصاح عنها (ريادة أعمال ، 2023).
5. البيانات الشخصية التي يتم الحصول عليها من خلال التطبيقات المختلفة : وتظهر هذه البيانات من خلال الموافقة على استخدام التطبيق لصور الهاتف وغيرها من المحتويات، وسوف تتطرق الباحثة إلى مدى قانونية هذه الأفعال .

6. البيانات الشخصية الزائدة : وهذا النوع يظهر بشكل كبير من خلال قيام الأشخاص بالإفصاح عنها بشكل مبالغ فيه على مواقع التواصل الاجتماعي مثل الهوايات، الدخل الشهري، وجهة السفر، تفاصيل الحياة الشخصية وكذلك الزوجية .
7. بيانات يتم تقديمها بسبب جهل المستخدم أو عن طريق الخطأ : وهذه البيانات يتم الحصول عليها عن طريق جهل الأشخاص بالتطورات التكنولوجية أو عن طريق الخطأ مثل خانة الإعدادات فتكون عامة، وليست خاصة مثلاً جعل رقم الهاتف أو صور شخصية عامة، وبالتالي يمكن استغلالها بتهديد أو أي جريمة أخرى.
8. بيانات خاصة (ملف خاص) : وتكون هذه البيانات من خلال توفر عدد أكبر من البيانات عن الشخص الواحد، وبالتالي يمكن قيام الشركات بتجميعها بملف واحد ومن ثم بيعها لشركات أخرى، وبالتالي الاستغلال المادي دون موافقة الشخص نفسه .

وقد وجدت الباحثة أن هناك الكثير من البيانات الشخصية التي يمكن تصنيفها، فهي متنوعة وكثيرة، بالإضافة إلى أنها في تطور مستجد فيمكن إيجاد أنواع جديدة مرافقة للتطور التكنولوجي السريع، وهنا قامت الباحثة بعرض أنواع البيانات الشخصية الأكثر انتشارً أو الأكثر استخدماً دون حصرها عند هذا الحد.

المطلب الثاني: أهمية سن قانون خاص لحماية البيانات الشخصية

إن البيانات الشخصية هي البيانات التي يمكن من خلالها التعرف على الشخص أي بيانات خاصة ترتبط بهويته الشخصية، القانون الأساسي كفل الخصوصية ولكن كفلها بوجه عام ولم يدخل بأي تفاصيل تعلق بها، ومع التطور الكبير في التكنولوجيا والاقتصاد جعل هناك حاجة ملحة لصدور قانون خاص بالبيانات؛ للحفاظ على خصوصية الفرد من خلال هذا القانون، و لحماية الأفراد من الاحتيال القائم على البيانات الشخصية وخاصة الاحتيال العابر للقارات (الشمري، 2021).

وبعد قيام الباحثة بالبحث والتحري عن كيفية استغلال البيانات الشخصية وجدت أن استغلالها يكون بعدة صور، ومثال ذلك قضية فيسبوك التي تم فيها ايقاع ضرر على 87 مليون مستخدم نتيجة تسريب بياناتهم، وعلى أثر ذلك تم دعوة مؤسس الشركة مارك للاستجواب، وتكمن فكرة سرقة البيانات الشخصية من خلال استغلال التكنولوجيا الالكترونية الذكية، وخير مثال واضح ونراه بواقعنا هو الإعلانات ومثال ذلك شخص ما يميل لشراء الكتب فتبدأ الإعلانات الخاصة بالكتب بالظهور أمامه من خلال ربط التكنولوجيا الذكية؛ لمعرفة اهتمام الأفراد من خلال الاتصالات والهواتف الذكية، ولم يقتصر الأمر على سرقة البينات الشخصية واستغلالها تجارياً بل تعدى الأمر لموضوع تشويه الصور الشخصية، مع العلم أنه يوجد أشخاص متربصين بالبيانات الشخصية مثلاً شخص مستأجر شقة أو أي عقار ويفاجئ باتصال من شركات للعقارات تعرض عليه شقة للبيع فيتبادل لذهن من أين حصل على المعلومة هذه، وبالتالي هنا يتم استغلال البيانات الشخصية ومن هذه الثغرات تخلق جرائم الاعتداء على البيانات (أهمية حفظ البيانات الشخصية ، 2019).

وتأتي أهمية سن قانون لحماية البينات الشخصية في العموم في ظل الافتقار التشريعي نتيجة الحاجة لسن قانون يتواكب مع التكنولوجيا ، بالإضافة إلى قانون الجرائم الالكترونية؛ لتوفير ضمان قانوني لحماية البيانات الشخصية للمواطنين والمؤسسات؛ وكذلك الأمر ليتواكب مع التشريعات الاجنبية والتي سبقتنا في وضع تشريع خاص لحماية البيانات الشخصية، وتأتي أهمية قانون حماية البيانات الشخصية أيضاً في كونه قانون يسعى لتنظيم استخدام الجهة التي تتحكم بالبيانات جمعها، مدة حفظها، الأشخاص المخولون بالاطلاع عليها (أهمية قانون حماية البيانات الشخصية، 2020).

ولكون التكنولوجيا أصبحت لها القدرة على جمع معلومات متعددة ومن ثم ربطها ببعضها البعض لتكون بيان واضح عن شخص معين وبالتالي ممكن أن تمس بخصوصية المواطن، وهنا تكمن فائدة سن قانون لحماية البيانات الشخصية، حيث يحمي الخصوصية بحيث يأتي دوره من عدة جهات أهمها وضع

خصوصية للبيانات أو الأجهزة التي تتحكم بالبيانات مثل جهاز الهاتف الذي أصبح له خصوصية مثل خصوصية المنزل حيث لا يستطيع أي شخص استخدام أي بيان موجود فيه إلا بأذن صاحبه، بالإضافة إلى أن سن قانون لحماية البيانات الشخصية ينظم استخدام البيانات أي المتحكم بالبيانات يخضع لضوابط معينة لا يستطيع أن يتجاوزها، وهنالك أهمية أخرى لسن قانون لحماية البيانات الشخصية في أنه يساعد في الاستثمار كون أن شركات الخدمات وغيرها تحتاج لمثل هذا القانون لتنظيم تعاملها مع الشركات الأخرى وكذلك المواطنين (اكستر نيوز) .

المبحث الثاني : الأساس القانوني لحماية البيانات الشخصية

خاطب قرار مجلس الوزراء الخاص بحماية البيات الشخصية عدة جهات منها حائز البيانات الشخصية، وهو الشخص أو الجهة التي تحفظ أو تجمع البيانات الشخصية لديها وأما بالنسبة للجهة المعالج للبيانات الشخصية، وهي الجهة التي تتولى معالجة البيانات مثل ترتيبها، إعادة صياغتها، تكييفها وغيرها من الأمور، وبالإضافة إلى المتحكم بالبيانات الشخصية، حيث تطرقت الباحثة لتعريف كل منهم على حدا، وقد وجدت الباحثة بالرجوع إلى قرار مجلس الوزراء الخاص بحماية البيانات الشخصية الفلسطيني أنه لم يدخل بأي تفصيل بخصوص هذه الجهات بل وضع مصطلحات عامة لهذه الجهات، وضع التزامات على هذه الجهات لكن دون تخصيص بل جاء على وجه العموم (مسار)، وسوف تتطرق الباحثة لتعريف وتوضيح ما المقصود بالجهة المتحكمة بالبيانات الشخصية ومن ثم الانتقال لتوضيح الجهة المعالجة للبيانات الشخصية، حيث أن القارئ سوف يميز بين الجهتين بعد قراءة ما تم كتابته عن الجهتين، حيث قامت الباحثة بتقسيم الدراسة إلى مطلبين جاء في المطلب الأول: النصوص القانونية المنظمة للبيانات الشخصية، والمطلب الثاني سوف نتحدث فيه عن الالتزامات التي تقع على الجهات المنوط بها جمع البيانات الشخصية.

المطلب الأول: النصوص القانونية المنظمة للبيانات الشخصية

النصوص القانونية المتعلقة بحماية البيانات الشخصية وتنظيمها تقسم إلى نصوص قانونية على مستوى محلي مثل قانون الاتصالات، وغيرها في الفرع الأول ونصوص يمكن الاستناد إليها لتوفير حماية البيانات الشخصية على مستوى دولي مثل الاتفاقيات الدولية المتعلقة بحماية البيانات الشخصية مثل الاتفاقية الأوروبية عام 1950 والنظام الأوربي لحماية البيانات الشخصية (GDPR) في الفرع الثاني.

الفرع الأول: النصوص القانونية المنظمة للبيانات الشخصية على مستوى محلي

إن حماية البيانات الشخصية كانت محور اهتمام الباحثة في ايجاد وتحليل النصوص القانونية التي تتعلق بقواعد الحماية وقد وجدت الباحثة أنه هناك قواعد قانونية نصت على الحماية بشكل صريح وهناك قواعد بشكل ضمني وسف نبدأ بالنصوص المباشرة.

أولاً: قرار مجلس الوزراء لحماية البيانات الفلسطيني رقم 3 لسنة 2019

جاء دور قرار مجلس الوزراء الخاص بحماية البيانات الشخصية عن طريق توفير حماية للبيانات الخاصة بالأفراد كون حماية هذه البيانات يحقق توازن بين حماية حقوق الأفراد، والتي كفلتها الدساتير، كونها تندرج ضمن الحق في الخصوصية، وما بين مصالح الدول والشركات التي ترغب في الاطلاع على هذه البيانات، وبالتالي جاء لتحقيق التوازن بين الجهتين (الرفاعي).

حيث جاء في المادة الأولى من قرار مجلس الوزراء الخاص بحماية البيات الشخصية رقم 3 لسنة 2019 بخصوص البيانات الشخصية الخاصة بالمواطنين، حظر استخدام البيانات الشخصية الخاصة بالمواطنين من قبل الشركات والمؤسسات المحتفظة بالبيانات الشخصية لأغراض تجارية دون الحصول على الإذن المسبق من أصحاب هذه البيانات (قرار مجلس الوزراء رقم 3 لسنة 2019 بشان حماية البيانات الشخصية المادة1، 2019).

لكن من وجهة نظري كباحثة قرار مجلس الوزراء الخاص بحماية البيات الشخصية ينقصه الكثير من الأمور ويعاني من النقص في مواضيع عديدة أهمها :

1. لم يتطرق لموضوع الجرائم التي ترتكب بحق البيانات لأنه قرار مجلس وزراء ، بل اكتفى بحظر استخدام البيانات الشخصية من قبل الشركات والمؤسسات دون الحصول على اذن مسبق لاستخدامها لأغراض تجارية مع العلم أن قانون العقوبات الفلسطيني لم يتحدث عن هذه الجرائم كذلك.
2. المشرع الفلسطيني لم يضع تعريفاً للبيانات الشخصية، بل ترك الأمر للفقهاء ولم يحدد الجهة المتحكم والمعالجة للبينات كذلك لم يحدد المحكمة المختصة بنظر جرائم البيانات الشخصية.
3. لم يتطرق المشرع لأمور عديد منها عملية معالجة البيانات الشخصية، والجرائم الواقعة عليها وانتهاكها وفي حال الاعتراض على معالجتها.
4. لم يحدد للجهات المختصة بجمع البيانات الشخصية شروط لجمعها، مثلا أن تكون عملية الجمع لأغراض مشروعة، وبإذن صاحبها، ومدة الاحتفاظ بهذه البيانات بل وضع التزام بسيط جداً على الشركات، وهو عدم استخدام البيانات الشخصية لأغراض تجارية إلا بموافقة أصحابها.
5. لم يتطرق قرار مجلس الوزراء الخاص بحماية البيات الشخصية للبيانات الشخصية المتعلقة بالطفل أو فاقد الأهلية أو المجنون، وبالتالي يعاني من قصور في كثير من المواضيع.
6. ولم يتطرق قرار مجلس الوزراء الخاص بحماية البيات الشخصية لموضوع المواطنين التي تم نقلها لدول اجنبية دون موافقتهم، ولم يتطرق أيضاً للمسؤولية الجنائية للشخص الاعتباري في الاعتداء على البيانات الشخصية للأفراد.

وبالتالي لا بد من أن يقوم المشرع بعلاج هذا النقص، عن طريق سن تشريع يتطرق لهذه المواضيع ؛ لكي يكون تشريع شامل ومعالج لوضع البيانات الشخصية ومناسب للتطور التكنولوجي السريع .

ثالثاً: قانون الاتصالات الفلسطيني رقم 3 لسنة 1996

سوف تقوم الباحثة بدراسة قانون الاتصالات الساري في فلسطين، وتوضيح النصوص القانونية التي تتعلق بالبيانات الشخصية وجرائم الاعتداء عليها، حيث وجدت الباحثة بعد دراسة هذا القانون أن ببدايته نظم موضوع البيانات التي يتم تبادلها عبر وسائل التواصل سواء عن طريق الشبكات السلكية أو اللاسلكية، ومن ثم عالج القانون بشكل عام موضوع الاعتداء على البيانات، ووضع لكل جريمة عقوبة مناسبة لها.

فمن الناحية التنظيمية للقانون ومعالجته لموضوع البيانات الشخصية وجدت الباحثة التالي:

أولاً: وهو قانون يضم ويشمل الاتصالات السلكية واللاسلكية، وقد أكد القانون على موضوع السرية في الاتصالات لما تحتويه من بيانات خاصة، بحيث لا يجوز انتهاك هذه الخصوصية إلا بحدود القانون وهذا ما جاء في المادة 3 منه (قانون الاتصالات الفلسطيني رقم 3 لسنة 1996 المادة 4، 1996).

ثانياً: قد وضح القانون أن من مهام وزارة الاتصالات لا يقتصر فقط ضبط عملية تبادل البيانات عبر الاتصالات السلكية واللاسلكية في فلسطين، بل تتولى الوزارة أيضاً عملية ضبط الاتصال بالاتجاه الدولي (قانون الاتصالات الفلسطيني رقم 3 لسنة 1996 المادة 5)، وهنا أعطى القانون لوزارة الاتصالات صلاحية الضبط ليس فقط على المستوى المحلي بل يمتد للمستوى دولي؛ وذلك من أجل توفير حماية وتنظيم عملية تبادل البيانات عبر شبكات التواصل.

ثالثاً: وضح القانون أن من صلاحيات وزارة الاتصالات مراقبة الموجات الراديوية والأجهزة المتعلقة فيها، والتي تعمل على نقلها، وذلك ضمن القوانين السارية في فلسطين والاتفاقيات الدولية المتعلقة بالموضوع (قانون الاتصالات الفلسطيني رقم 3 لسنة 1996، المادة 7 فقرة 15)، وهنا لم يعطي القانون الوزارة حق مفتوح في مراقبة الموجات الراديوية والأجهزة المتعلقة بها؛ وذلك من باب حماية حق الخصوصية من التعسف، وخرق هذا الحق من قبل الشركات بحجة أن القانون أعطى هذا الحق وسمح به، وبالتالي قيد عملية المراقبة بالقوالين السارية داخل الدولة والاتفاقيات الدولية التي وقعت عليها فلسطين.

والمقصود بالموجات الراديوية : وهي موجات تستخدم لنقل كافة أنواع المعلومات، حيث منذ مئة عام ظهرت الاتصالات اللاسلكية بين الناس وبدأوا باستخدامها إلى وقتنا الحالي الذي أصبحت فيه البيانات تنقل عن طريق الوايف فاي والبلوتوث وشبكات الجيل الثالث والرابع، وجميع هذه الوسائل تستخدم موجات الراديوية لنقل البيانات، بحيث أنها موجات كهربائية ومغناطيسية، ولهذا السبب تسمى بالموجات الكهرومغناطيسية، بحيث تطلق الموجات الراديوية موجات تسمى موجات كهرومغناطيسية، وهي إشعاعات غير خطيرة على الإنسان بالمقارنة بالإشعاع النووي، وتنتقل هذه الموجات بسرعة الضوء، مع العلم أن معدات شركات الاتصالات في هذا المجال مكلفة للغاية، وتستخدم هذه الموجات الهواء لتتنقل من نقط لأخرى (موجات الراديو – –فلم وثائقي مترجم من قبل الباحثون المسلمون).

رابعاً: قد حدد القانون على الوزارة تنظيم الترددات الوطنية، وتنظيم الموجات اللاسلكية، ويقصد بعملية التنظيم تأمين وصولها دون أي اعتداء على البيانات المرسلة من خلالها، حيث يكون على الوزارة حماية البيانات المنقولة لاسلكياً (الترددات) من أي اعتداء قد يقع على البيانات من تشويش أو حذف أو اتلاف أو سرقة وغيرها من أوجه الاعتداء غير المشروع (قانون الاتصالات الفلسطيني رقم 3 لسنة 1996، المادة 18 منه)؛ ولتوفير الحماية تسعى الوزارة أي وزارة الاتصالات لتشغيل أيدي عاملة لديها الكفاءة العالية بتوفير الحماية البيات الشخصية خلال عملية نقلها وارسالها وتبادلها (موقوع وزارة الاتصالات وتكنولوجيا المعلومات ، 2015)، ولا تتوقف الوزارة عند هذا الحد بل تسعى لتطوير الأيدي العاملة لدى الوزارة عن طريق الدورات وتطوير الخبرات وبالإضافة إلى تكريم الموظفين الناجحين لتشجيعهم على تطوير الذات (موقوع الاتصالات وتكنولوجيا المعلومات ووزارة الاتصالات، 2016).

خامساً: وضع القانون فصل خاص لمراقبة تنظيم تعامل شركات الاتصالات مع المواطنين، حيث وضع بموجب هذا القانون التزامات على الشركات أي (المرخصين)؛ وذلك من أجل حماية المستفيدين أي ضبط العلاقة التي تربط الجهة المرخصة مع المستفيدين (المواطنين)، ووضع بموجب ذلك التزام على الشركات

المرخصة بفتح قسم لشكاوى، بحيث يتقدم بها المستفيد لشكوى عن اعتداءات وقعت عليه (قانون الاتصالات الفلسطيني رقم 3 لسنة 1996، المادة 58)، وهذه الخطوة تعتبر خطوة جيدة من قبل الوزارة؛ لأنه في بعض الأحيان قد يقع مخالفات من الموظفين سواء استراق السمع على المكالمات أو إتلاف بيانات شخصية مهمة للفرد، وبالتالي إلحاق ضرر به، ولكن يمكن تدارك هذا الموضوع في بدايته عن طريق هذه المادة من خلال التوجه للوزارة نفسها وتقديم الشكوى بدلا من التوجه للقضاء والدخول في أزمة طول التقاضي وطول فترة الإجراءات، و بالتالي بهذه الخطوة يمكن معالجة هذه المخالفة بأسرع الطرق وبوقت أقل.

سادساً: ويحق للوزارة مراقبة الاتصالات الخاصة بالمستفيد، وذلك بناءً على طلب منه، من أجل وضع هاتفه تحت المراقبة لتعرضه لمشكلة ما قد تكون مكالمات تهدفه لإزعاجه أو لديه شك أن هاتفه مراقب بحيث تتولى الوزارة معالجة الموضوع بموجب إجراءات تبدأ بالإنذار الخطي وغيرها من الإجراءات التي ذكرها القانون التي قد تنتهي بالتوجه للقضاء لرفع شكوى من صاحب الشأن (قانون الاتصالات الفلسطيني رقم 3 لسنة 1996 المادة 62 فقرة ج).

سابعاً: أعطى القانون لوزارة الاتصالات القيام بعمل التفتيش على المحطات اللاسلكية، بحيث يحق لها الرقابة والتفتيش على الأجهزة ولها ضبط هذه الأجهزة اذا وقعت مخالفة للقانون من خلالها، وخاصة في ظل التطور التكنولوجي السريع الذي أنتج العديد من الأجهزة التي تستعمل بالتنصت (قانون الاتصالات الفلسطيني رقم 3 لسنة 1996، المادة 77منه.).

ثامناً: أعطى القانون لموظفي الوزارة صلاحية الضبط والتفتيش، وذلك في حال اكتشاف وجود أجهزة تعمل على تشويش البيانات المرسلة عبر وسائل الاتصالات أو وجود أي مخالفة قد نص عليها القانون، حيث أعطى القانون لموظفي وزارة الاتصالات صفة الضبط القضائي (قانون الاتصالات الفلسطيني رقم 3 لسنة 1996، المادة 83 منه.).

ترى الباحثة أن القانون كان جيداً بتنظيم موضوع تناقل البيانات والمعلومات عبر وسائل التواصل؛ كونه نظم هذا الموضوع في بداية القانون، ومن ثم وضع فصلاً تحدث فيه عن عدة جرائم ممكن أن يتم ارتكابها عن طريق شبكات التواصل، وقد تطرق لبعض جرائم الاعتداء على البيانات الشخصية، سوف تذكرهم الباحثة خلال الدراسة .

ويمكن أن يتم ارتكاب جرائم تتعلق بالبيانات الشخصية ولا يقتصر تأثيرها على الأشخاص فقط، بل يمتد ليؤثر على الأمن القومي، ومن الأمثلة على ذلك قيام محكمة صلح رام الله بإصدار قرار يتضمن حجب 59 موقع إلكتروني، حيث قامت هذه المواقع بنشر صور، أفلام، عبارات، أرقام، من شأنها التأثير على الأمن القومي في الدولة والنظام العام، والآداب العامة، وأسست المحكمة قرارها على قانون الجرائم الالكترونية رقم 10 لسنة 2018 بناء على المادة 39 منه، وكان قرارها قد صدر بناء على طلب قدم من النائب العام أو أحد مساعديه، حيث جرى حجب هذه المواقع دفعة واحدة وتم محاكمة صحفيين على عملهم الصحفي وقضايا النشر (قرار لمحكمة صلح رام الله بشأن الجرائم الالكترونية وحجب مواقع الالكترونية، 2019) .

الفرع الثاني: النصوص القانونية المنظمة للبيانات الشخصية على مستوى دولي

أكد العهد الدولي في كثير من نصوص مواده على احترام الخصوصية، حيث جاء في المادة ١٤ منه أنه نظر القضايا أمام القضاء هي علنية، ولكن يمكن أن تكون سرية؛ ولذلك حفاظاً على حرمة الحياة الخاصة لأطراف الدعوى وبالإضافة إلى الكثير من المواد التي أكدت على احترام خصوصية الفرد منها ما جاء في المادة 17 ايضاً فيما معنى المادة لا يجوز التدخل في حياة أي شخص الخاصة سواءً خصوصيته أو أمور اسرته أو بيته أو المحادثات السرية أو أي تصرف غير قانوني قد يؤدي إلى انتهاك حياته الخاصة، ومن حق كل شخص حفظ هذه الحقوق من أي انتهاك قد يقع وأكد العهد أيضاً على حرية الأديان والآراء

السياسية وحرية التعبير والأمن والنظام والصحة في المواد 18–19 (العهد الدولي الخاص بالحقوق المدنية والسياسية 1966 المواد 14–17–19–18) .

أولاً: الاتفاقية الأوربية لحقوق الانسان–اتفاقية حماية حقوق الانسان في نطاق مجلس أوروبا –روما في نوفمبر 1950

وقد نصت الاتفاقية الأوروبية لحقوق الانسان على عدة مواد في مضمونها تكفل حماية الحياة الخاصة بالأفراد، وقد كانت هذه الاتفاقية نقطة انطلاق لكثير من القوانين والاتفاقيات، حيث كانت الأساس لنظام الأوربي لحماية البيانات الشخصية، حيث جاء في موادها ما نص على احترام حقوق الحياة الخاصة والعائلية واحترام حرمة المسكن والمحادثات الخاصة والمراسلات، ولا يجوز للسلطة العامة في الدولة انتهاك أي من هذه الحقوق إلا وفقاً للقانون، وذلك بناءً على ضرورة ملحة مثل الأمن، النظام العام، الآداب العامة، ضبط السياسة العامة في الدولة وتحقيق الأمان لمواطنيها، وأكدت الاتفاقية على ضرورة احترام حرية الأديان والرأي والتفكير والتعبير وحرية عقد الاجتماعات السرية في المواد8–9–10–11 (الاتفاقية الأوربية لحقوق الانسان–اتفاقية حماية حقوق الانسان في نطاق مجلس أوروبا –روما في نوفمبر 1950.).

ثانياً :النظام الأوربي لحماية البيانات الشخصية .

يتكون النظام من 99 مادة ويختصر النظام بالرمز التالي GDPR قانون رقم 2016/679–27 إبريل 2016، ويتعلق القانون بحماية البيانات الشخصية وحرية نقلها ومعالجتها ويطبق هذا القانون ضمن نطاق الاتحاد الأوربي الجغرافي، ويمكن أن ينطبق هذا القانون على عضو ليس من الاتحاد الأوربي في حال كان موجود أحد الأطراف بمكان ينطبق فيه قانون الدول الأعضاء، وقد عرف النظام البيانات الشخصية، ووضع تعريفات لصاحب البيانات والمتحكم بالبيانات والمعالج للبيانات، ومن الأمور الجيدة جداً أن النظام وضع تعريفات شاملة لكل من له علاقة باستخدام البيانات الشخصية، وحتى وضع تعريف لعملية خرق البيانات الشخصية وعرف ما يسمى بالبيانات الوراثية والبيانات البيومترية والبيانات المتعلقة بالصحة وعالج

النظام مشكلة وجود شركة بأكثر من عضو، حيث نص في المادة 16 منه أنه في حال وجود أكثر من عضو ضمن مؤسسة فأن تطبيق النظام يكون في حال وجود المركز الرئيسي ضمن الإطار الجغرافي للاتحاد، وفي حال لم يكن مركز إدارتها الرئيس في الاتحاد يخضع للبيانات الشخصية ما يكون ضمن الأنشطة المتعلقة بمعالجة البيانات ضمن الاتحاد (د.مصطفى).

وتنطبق اللائحة العامة لحماية البيانات GDPR على المنظمات التي أنشأت داخل الاتحاد الأوربي وعلى المنظمات المنشأة خارج الاتحاد ما دامت هذه البيانات تتعلق معالجتها بأفراد داخل الاتحاد الأوروبي (موقع، aws) .

وقد أقرت اللائحة عدت حقوق أساسية منها (موقع aws):

1. الحق في الموافقة: ويعني هذا الحق وضع التزام على الشركات لاستخدام بيانات الأفراد الحق للفرد بإصدار الموافقة الصريحة، أما بخصوص السكوت فلا يعتبر ذلك موافقة على استخدام البيانات.
2. القابلية لنقل: أقر النظام بحق الأفراد بنقل بياناتهم لشركات أخرى، وذلك حسب رغباتهم مثل الحصول على خدمة مغاير للخدمة التي تقدمها الشركة الموجدة عندهم بياناتهم.
3. الحق في المحو: وينص هذا الحق على إمكانية تقديم الفرد بطلب بمسح بياناته الشخصية الموجودة لدى الشركة.
4. الحق في النسيان: جاء هذا الحق نتيجة اصدار محكمة أوربية حكم أعطت فيه الحق لمواطنين أوربيين الحق بمسح أي بيانات لا يردون تقديمها وربطها في الفضاء الرقمي، وفي حال عدم التزام أي شركة تتعامل مع البيانات الشخصية للمستخدمين بتعليمات النظام، يتم فرض غرامة تصل إلى ٤٪ من القيم السوقية لتداول الشركة أو فرض غرامات مالية تصل إلى عشرين مليون يورو.

وهذا النظام عند الاطلاع عليه قد يعتقد الشخص أنه لم يؤثر كثيراً على الواقع، إلا أنه احدث تغيراً كبير على عمل الشركات، حيث أنه وضع التزامات على عملية جمع ومعالجة وتخزين البيانات الشخصية،

وبالتالي حدث تغير كبير في نمط عمل هذه الشركات لضمان عدم وقوع أي انتهاك لبيانات الأفراد كون الغرامات التي سوف تفرض في حال وقوع أي اعتداءات كبيرة، ومن أبرز هذه الالتزامات، معرفة البيانات وإدارتها وتحديد المسؤول عنها وتشفير البيانات التي لا ترغب الشركة بالكشف عنها ونشر ثقافة الحفاظ على أمن وخصوصية البيانات في الشركة (سيد، 2022) .

ومن القضايا العملية بخصوص حظر نقل البيانات الشخصية من الولاية الموجد فيها أصحاب هذه البيانات، حيث قدم محامي يدعى ماكس شريمز شكوى أمام محكمة العدل الأوربية ضد فيس بوك، حيث قام فيس بوك بنقل بيانات المحامي ومواطني الاتحاد الأوروبي من أوروبا إلى الولايات المتحدة الأمريكي، وبموجب ذلك حكمت المحكمة بإلغاء العمل باتفاقية نقل البيانات من الولايات المتحدة الأمريكية والاتحاد الأوربي؛ نتيجة لسرية وطبيعة هذه البيانات وحكمت المحكمة أيضاً ب 25000 ألف جنيه استرليني كتعويض للمدعي (الحميد د.، قرار لمحكمة العدل الاوروبية بخصوص قضية ماكسشريمز ضد مركز حماية البيانات الايرلندية، 2013).

المطلب الثاني: الالتزامات التي تقع على الجهات المنوط بها جمع البيانات الشخصية

سوف تتطرق الباحثة في هذا المطلب إلى موضوع الالتزامات التي تقع على الجهة المنوط بها جمع البيات الشخصية سواء كانت هذه الجهات خاصة مثل الشركات أو جهات حكومية عامة مثل دوائر الإحصاء أو الوزارات مثل وزارة الصحة وغيرها وذلك في الفرع الأول الذي يتطرق للجهة المتحكمة بالبيانات الشخصية والفرع الثاني تطرقت فيه الباحثة للجهة المعالجة للبيانات الشخصية.

الفرع الأول : الجهة المتحكمة بالبيانات الشخصية

وبرجوع الباحثة للتشريعات المختلفة المتعلقة بحماية البيانات الشخصية نجد أنها لم تضع تعريف لما يسمى المتحكم أو المعالج للبيانات، إنما هي أمور فنية تركت لأصحاب الخبرة وقد عرفت المتحكم : " هو أي شخص طبيعي أو اعتباري يكون له بحكم أو بطبيعة عمله، الحق في الحصول على البيانات الشخصية،

وتحديد طريقة وأسلوب ومعايير الاحتفاظ بها، أو معالجتها والتحكم فيها طبقاً للغرض المحدد أو نشاطه" (فتحي، كل ما تريد معرفته عن شروط معالجة البيانات الشخصية ، 2022).

على أثر البحث والتحري من قبل الباحثة عن جهات توصف بجهات متحكمة بالبيانات الشخصية استطاعت جمع بعض المعلومات عن هذا الموضوع، حيث التقيت بأحد العاملين في مجال البيانات الشخصية وهو شخص يتولى أخذ بيانات شخصية من المواطنين لتسليمهم الشرائح (يتولى بيع الشرائح الهواتف وحزم الانترنت) وأفاد أنه يتولى جمع البيانات الشخصية من خلال قيام المواطن أو الشخص الذي يريد شراء شريحة أو حزمة إنترنت بتقديم بيانات شخصية عن نفسه مثل الاسم الرباعي، رقم الهوية، تاريخ الميلاد، مكان السكن، توقيع الشخص المشتري لشريحه، حيث أضاف السيد محمود أن يتم تسجيل هذه البيانات على طلب خارجي مطبوع من الشركة باليد، ثم يتم نقل هذه البيانات إلى برنامج مزود من قبل الشركة يطلق عليه برنامج فوري يرسل إلى الشركة بعدها، وأضاف أن أي شريحة يسجل لها رقم تسلسلي (باركود) وهذه الشريحة والتي تحمل بيانات معينة لكل شخص يكون محدد عليها أنها تم بيعها من نقطة بيع محددة أي محل البيع، حيث نوه السيد محمود أنه يمكن أن يتم استغلال البيانات بطريقة غير مشروعة عن طريق شراء شرائح عن طريق أشخاص لا يملكون صفة أو شخص قام بسرقة هوية شخص أخر ويريد تسجيل الشريحة على أسمه، وبالتالي يستطيع انتحال شخصية صاحب الهوية وارتكاب جرائم من خلالها وهنا يقع التزام على صاحب المحل التجاري بالتحري والتأكد من صاحب الهوية قبل بيع أي شريحة لأي شخص وأضاف السيد محمود أنه في فلسطين يوجد ثغرة يجب أن يتم علاجها من قبل الشركات، وهي أنه بعد قيام الشخص بشراء شريحة معينة وتركت هذه الشريحة لمدة ٦ أشهر أو أكثر يتم طرحها بالأسواق وتباع مرة أخرى، وبالتالي هناك مشكلة كبيرة بالبيانات الشخصية وهي أن الأشخاص يربطون الشريحة بأشياء تتعلق بالبيانات الشخصية مثل الفاسبوك واتس أب و الجي ميل وغيرها التي تحتوي على صور شخصية وبيانات خاصة، بالتالي يوصي السيد محمود قبل قيام الشركة بطرح الشريحة

لا بد من قيام صاحب الشريحة بتقديم طلب بإلغاء شريحته وطلب بيعها قبل قيام الشركة من تلقاء نفسها ببيعها وطرحها للأسواق وبالتالي الوقوع بمشكلة اعتداء على بينات شخصية (قاسم، 2022).

الفرع الثاني: الجهة المعالجة للبيانات الشخصية

وكذلك الأمر بالنسبة إلى مصطلح معالج البيانات الشخصية فالمشرع هنا ترك تعريفه إلى أصحاب الخبرة، فقد عُرف بأنه "أي شخص طبيعي أو اعتباري مختص بطبيعة عمله، بمعالجة البيانات الشخصية لصالحه أو لصالح المتحكم بالاتفاق معه وفقاً لتعليماته" (فتحي، كل ما تريد معرفته عن شروط معالجة البيانات الشخصية، 2022) .

وصرحت محكمة العدل الدولية بقرار لها أن أعمال معالجة البيانات هي عملية تعديل أو تغيير في البيانات الشخصية، ويمكن أن يتم عمل معالجة للبيانات الشخصية دون أن يطرأ تعديل عليها، وقيام محرك البحث بإتاحة البيانات الشخصية للأفراد يعتبر أيضاً من قبيل المعالجة ومثال ذلك قيام محرك البحث بتخزين وتسجيل وتنظيم بيانات شخصية بطريقة منهجه وتلقائية ومستمرة وهذا كله يعتبر من قبيل المعالجة (الحميد د.، قرار لمحكمة العدل الدولية بخصوص قضية جوجل اسبانيا ضد مركز حماية البيانات الاسباني ، 2013).

وبعد البحث والتحري عن موضوع معالجة البيانات الشخصية، وجدت الباحثة أن يتم تنظيم البيانات الشخصية؛ لتسهيل التعامل معها في بطاقة تسمى بطاقة تعريفية وهذه البطاقة جاءت فيها الشركة عن طريق تعليمات لتسهيل التعامل مع البيانات الشخصية، بحيث يتم تجميع هذه البيانات ومن ثم ترسل إلى مقر الشركة لحفظها في ما يسمى الأرشيف، و يتم الاحتفاظ فيها لمدة معينة بحيث يتم تصنيف هذه البيانات إلى عدة تصنيفات بتسهيل التعامل معها، ويمكن لمعالج البيانات الشخصية أن يتولى علاجها في حال وجود خلل مثلا في حال وقع خطأ بالاسم فيتولى المعالج معالجة هذا البيان عن طريق تصحيح الاسم بما يتماشى مع الاسم المذكور بالهوية، وهذه التعليمات تنسجم مع ما يسمى سياسة الشركة لإدارة

هذه البيانات ومع الإشارة إلى أن كل موظف يوقع على تعهد بخصوص البيانات الشخصية يتعهد فيه بالحفاظ على البيانات الشخصية بحيث أن هذه البيانات الشخصية لا يتم الإفصاح عنها أو نشرها إلا بطلب من النيابة أو المحكمة (فارس، 2022).

وبعد قيام الباحثة بالبحث ملياً لإيجاد نص قانوني يوضح التزامات الجهة المتحكمة أو المعالجة للبيانات، وجدت نصوص قانونية بمواد مختلفة في فلسطين ، وهنا ترى الباحثة أن هذا ضعف تنظيمي ، حيث أن كان من المستحسن أن يتم تنظيم الأمور المتعلقة بالبيانات الشخصية بقانون واضح وملم وليس لكل من يرغب بالاطلاع على القوانين المتعلقة بالبيانات الشخصية يجب عليه أن يبحث في عدة قوانين وقرارات صادرة عن مجلس الوزراء ، بالإضافة إلى أن قرار مجلس الوزراء الذي تم سنه للبيانات الشخصية بعد دراسته يتسم بالضعف، حيث أن لم يتطرق إلى مواضيع متنوعة تهم البيانات الشخصية مثل موضوع جرائم الاعتداء على البيانات الشخصية أو مدة الاحتفاظ بالبيانات الشخصية من قبل المتحكم أو المعالج، حيث تطرق لموضوع واحد وهو استخدام البيانات الشخصية بشكل مباشر أو غير مباشر لهدف تجاري، وهنا سوف تقوم الباحثة بالتطرق لموضوع الالتزام التي تقع على الجهات المنوط بها جمع البيانات الشخصية وذلك بالرجوع للقوانين والقرارات ذات العلاقة.

وبعد البحث ملياً وجدت الباحثة أنه هناك كثير من القوانين وضعت التزامات على الجهة المتحكم والمعالجة للبيانات الشخصية، ولكن هذه الالتزامات اتسمت أنها انسجمت لحدٍ ما مع طبيعة كل قانون والموضوع الذي جاء لينظمه (قرار مجلس الوزراء الخاص بحماية البيات الشخصية)، ولكن تشد الباحثة على موقفها بخصوص وضع قانون شامل لموضوع البيانات الشخصية باعتبار أن هذه القوانين التي سوف تعرضها الباحثة كفلت الخصوصية بخصوص البيانات الشخصية، ولكن ليس كما يجب، حيث أنه في ظل وجود قانون أشمل يكون أفضل وذلك لسببين الأول وجود قانون خاص بالبيانات الشخصية يكفل بشكل أشمل حق الخصوصية للفرد، والسبب الثاني أن وجود قانون خاص يسهل التعامل مع التشريع من الناحية

التنظيمية حيث أنه يكون أسهل للفرد وغيره من أصحاب الحق الرجوع للقانون نفسه إذا ما احتاج ذلك بدلاً من التشتت بأكثر من نص قانوني (قوانين حماية البيانات الشخصية).

هنا سوف تعرض الباحثة بعض القوانين والقرارات التي وضعت التزامات على الجهة المتحكم والجهة المعالجة للبيانات الشخصية.

أولاً: قرار مجلس الوزراء رقم (3) لسنة 2019 المتعلق بالبيانات الشخصية الخاصة بالمواطنين

حيث جاء في المادة الأولى منه حظر استخدام البيانات الشخصية لأغراض تجارية دون الحصول على إذن مسبق من صاحبها (قرار مجلس الوزراء رقم (3) لسنة 2019 المتعلق بالبيانات الشخصية الخاصة بالمواطنين،المادة1)، حيث جاء نص المادة صريح وليس مبهم، حظر المشرع أي استعمال أو استغلال للبيانات الشخصية لأهداف تجارية دون الحصول إذن مسبق من صاحبها، وتلاحظ الباحثة أنه من واقع الحال أن المادة تخاطب شركات الإنترنت والشركات الأخرى التي توفر خدمات معينة للمواطنين ولأغراض تجارية، حيث بطبيعة عملها وبموجبه ترتكز بشكل أساسي في تعاملاتها على البيانات الشخصية للمواطنين وبالتالي شرط أساسي للتعامل مع هذه البيانات الحصول على إذن مسبق لذلك.

ثانياً: قرار بقانون رقم (15) لسنة 2017 بشأن المعاملات الالكترونية.

حيث جاء بالمادة السادسة من القرار أنه على وزارة الاتصالات وتكنولوجيا المعلومات تحديد آليات ومدد وشروط حفظ البيانات الالكترونية (قرار بقانون رقم (15) لسنة 2017 بشأن المعاملات الالكترونية المادة 6 منه.)، **وبالإضافة إلى نص المادة 31** التي جاء فيها توضيح أن سلطة النقد مسؤولة عن إصدار التعليمات والإجراءات اللازمة لتنظيم أعمال التحويل الالكتروني للأموال بما في ذلك الاحتفاظ وتخزين السجلات والبيانات الالكترونية الخاصة بتعاملات المؤسسات الخاضعة؛ لإشراف سلطة النقد (من) وفي نصوص المواد وضع التزام على الشخص مقدم البيانات في حال رغب بالحصول على رخصة من وزارة الاتصالات يجب عليه اخطارها بأي تغير بالبيانات الشخصية وإلا يترتب على ذلك عقوبة حبس مدة

لا تزيد عن ستة أشهر وبغرامة لا تزيد عن الفين دينار أو بإحدى العقوبتان وذلك في المادة (45) من القانون.

ثالثاً: قرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الالكترونية.

تحدث عن التزام مزود الخدمة 1: تزويد الجهات المختصة بمعلومات المشترك التي تساعد في كشف الحقيقة، بناءً على طلب من النيابة أو المحكمة المختصة 2: حجب رابط أو محتوى أو تطبيق على الشبكة الالكترونية بناءً على الأوامر الصادرة إليها من الجهات القضائية، مع مراعات الإجراءات الواردة في **المادة 30** من هذا القرار بقانون 3 الاحتفاظ بمعلومات المشترك لمدة لا تقل عن ثلاثة سنوات لغاية ما ورد في الفقرة (1) 4 التعاون ومساعدة الجهات المختصة وبناءً على قرار قاضي المحكمة المختصة في جمع أو تسجيل المعلومات أو البيانات الالكترونية والاحتفاظ المؤقت بها (قرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الالكترونية، المادة 30 منه.) .

وبالإضافة إلى المادة (33) من ذات القرار بقانون التي أعطت صلاحية للنيابة العامة بالحصول على الأجهزة أو الأدوات أو الوسائل أو البيانات أو المعلومات الإلكترونية أو بيانات المرور أو البيانات المتعلقة بحركة الاتصالات أو بمستعمليها أو معلومات المشترك ذات الصلة بالجريمة الإلكترونية (قرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الالكترونية المادة 33 منه.):

"2- للنيابة العامة الإذن بالضبط والتحفظ على كامل نظام المعلومات أو جزء منه أو أي وسيلة من وسائل تكنولوجيا المعلومات التي من شأنها أن تساعد على كشف الحقيقة.

3- إذا لم يكن الضبط والتحفظ على كامل نظام المعلومات أو جزء منه أو أي وسيلة من وسائل تكنولوجيا المعلومات.

4- إذا استحال إجراء الضبط والتحفظ بصفة فعلية، يتعين حفاظاً على أدلة الجريمة استعمال كافة الوسائل المناسبة لمنع الوصول والنفاذ إلى البيانات المخزنة بنظام المعلومات.

5- تتخذ الاحتياطات الضرورية للحفاظ على سلامة المضبوط المتحفظ عليه، بما في ذلك الوسائل الفنية لحماية محتواها".

بالإضافة إلى المادة (35) منه التي جاء في مضمونها أنه على الجهات المختصة اتخاذ التدابير اللزمة والإجراءات الضرورية للحفاظ على سلامة البيانات والمعلومات الإلكترونية المحفوظة على الأجهزة التي تستخدمها هذه الجهات لأغراض الحفظ إلى حين صدور الأمر من قبل الجهات القضائية المختصة (الالكترونية).

هناك انتقاد فيما يتعلق بتجميع البيانات الشخصية من قبل الجهات المسؤولة عن جمعها سواء قامت هذه الجهات بجمعها أو تخزينها أو تحليلها أو استخدامها أو مشاركتها وذلك لأنها لها تأثير كبير على موضوع الخصوصية والأمان وبالتالي حدوث الجرائم الإلكترونية يعرض هذه البيانات للانتهاكات ومن الطرق التي لجأت إليها بعض الدول مثل الفلبين لتقليل من هذه الجرائم هي اشتراط إخطار صاحب هذه البيانات في حال خرقها بأسرع وقت (unodc، 2021).

رابعاً: تعليمات رقم (1) لسنة 2008 بشأن المحافظة على سرية المعلومات .

المادة 5 والتي تحدثت عن اعتبار البيانات والسجلات التالية داخلة لدى الهيئة ولا يجوز الاطلاع عليها إلا من قبل الموظفين المختصين من خلال دخولهم على نظام التداول والتي تشمل على سبيل المثال لا الحصر، ما يلي :أ_ المعلومات المتعلقة بحجم أوامر البيع والشراء الخاصة بالعملاء أو محفظة الشركة المدخلة من قبل الأعضاء. ب_ المعلومات المتعلقة بالتداول وحسابات العملاء.٢_ المعلومات والبيانات التي يطلع عليها موظفو الهيئة المختصون من خلال استخدامهم لنظام مركز الإيداع والتحويل والتي تشمل على سبيل المثال لا الحصر، ما يلي :أ - المعلومات المتعلقة بعمليات الرهن والحجز والتحولات المستثناة

من التداول ب- المعلومات الخاصة بأسماء المتعاملين بالأوراق المالية وحجم تعاملاتهم ج- المعلومات الخاصة بأسماء مالكي الأوراق المالية ومقدار ملكيتهم . د- المعلومات الخاصة بشركات الأوراق المالية. هـ- المعلومات الخاصة بالشركات المدرجة. و- المعلومات الخاصة بالحافظ الأمين .ز- المعلومات الخاصة ببنك التسوية.3- المعلومات والبيانات والوثائق التي تحصل عليها الهيئة من خلال عمليات الإشراف والرقابة والتحقيق والتفتيش على شركات الأوراق المالية والسوق (تعليمات رقم (1) لسنة 2008 بشأن المحافظة على سرية المعلومات، المادة 5 من).

وتتضمن البيانات السرية جميع البيانات الغير عامة وهذه البيانات قد تكون ذات قيمة بالنسبة للمستثمرين أو الجهات الخارجية وكما ذكرت الباحثة أن هناك التزامات تقع على الجهات التي تحتفظ بهذه البيانات وتقع عليهم مسؤولية حماية هذه البيانات والحفاظ على سريتها سواء كانت إلكترونية أو بيانات مخزنة بشكل يدوي ولكن مما بجدر الإشارة اليه أن هذا الالتزام لا يؤخذ على إطلاقه بل يمكن في بعض الحالات تبادل هذه البيانات مع أعضاء الفريق لإنجاز مهمة معينة داخل الشركة أي أن متطلبات العمل تتطلب ذلك وبالتالي تبقى هذه البيانات ضمن الفريق ولا يجوز الإفصاح عنها لغير إطار العمل (بيانات حماية وأمن المعلومات قواعد السلوك المهني).

وهنا قامت الباحثة بعرض بعض القوانين والقرارات التي وضعت التزامات على الجهة المتحكمة والجهة المعالجة للبيانات الشخصية، مع العلم أنه يوجد الكثير من القوانين والقرارات بقانون تحدثت عن هذا الموضوع، ولكن لا يمكن عرضها جميعًا لذلك اكتفت الباحثة بعرض بعض هذه القوانين والقرارات بقانون على سبيل المثال (القوانين التي وضعت حماية للبيانات الشخصية ونظمت موضوعها.)، وترى الباحثة أنه لابد من تدخل المشرع ووضع تشريع عام يوضح التزامات الجهات المتحكمة والمعالجة للبيانات الشخصية بدلاً من التوجه للقوانين الأخرى والقرارات التي أصدرها المشرع لمعالجة جرائم معينة شرعت من أجلها مثل قانون الجرائم الإلكترونية ولسبب أخر يتمثل في أنه ليس في كل مرة يقع اعتداء على البيانات الشخصية

نلجأ لقوانين مشابهة مثل قانون الجرائم الالكترونية وغيرها التي هي بالأساس غير مختصة ولسبب ثالث وهو إيجاد تنظيم تشريعي بخصوص هذا الموضوع.

وبخصوص القضاء الفلسطيني فأنه ما زال يرتكز في تطبيقه للنصوص القانونية بخصوص جرائم البيانات الشخصية على قانون الجرائم الالكترونية، حيث بعد قيام الباحثة بالاطلاع على الواقع العملي والنصوص القانونية التي يتم الإدانة بناء عليها.

الفصل الثاني

خرق قواعد الحماية المقررة للبيانات الشخصية

بدايةً للحديث عن جرائم الاعتداء على البيانات الشخصية لابد من وصفها وصفاً تعريفاً لتميزها عن باقي الجرائم، فهي جرائم تختلف بطبيعتها عن الجرائم التقليدية مثل السرقة والخطف والقتل باعتبارها جرائم يتم ارتكابها بالغالب بوسائل تكنولوجية حديثة تساعد الجاني على اختراق هذه البيانات، علماً أنه يمكن أن يتم ارتكابها بوسائل تقليدية مثل لجوء الجاني لسرقة البيانات الشخصية ومن ثم إتلافها بطريقة تقليدية إلا أنه حالياً يتم اللجوء إلى استخدام الوسائل التكنولوجية الحديثة والعمل على اختراقها من خلال المواقع والأنظمة التي تضم بيانات شخصية خاصة بالأفراد (شحاته، درويش، و سالم ، 2019)، حيث يلجأ الجناة لهذه الطرق؛ كونها أسرع ، حيث أن من الصعب على الشرطة إمساك أدلة إدانة ضده والكثير من المميزات تسهل على الجاني ارتكابها بوسائل تكنولوجية (جرائم الانترنت مقال)، بحيث أن الواقع العملي يفرض نفسه، حيث أصبحت الوزارات والمكاتب والمؤسسات تعتمد على حفظ البيانات الشخصية بطريقة تكنولوجية عن طريق أجهزة التكنولوجيا والقليل من المؤسسات ما يعتمد على حفظ البيانات بطريقة تقليدية.

وقد يكون الدافع النفسي أو ما يسمى جنون العظمة السبب وراء الاعتداء على البيانات الشخصية، حيث يسعى الشخص من خلال هذا الاعتداء إلى إظهار نفسه أو تحقيق أهداف نفسية في مخيلته مثل السيطرة على شركة معينة أو الانتقام وغيرها من الأهداف (سعيد ف.، 2019).

وقد ظهر مصطلح يسمى أمن المعلومات أو أمن البيانات أي حفظها من أي اعتداء قد يقع عليها سواء كان هذا الاعتداء من داخل الدول أو خارجها، وقد تعددت طرق الاعتداء على البيانات منها الدخول غير المشروع لهذه البيانات وإحداث تغير فيها أو بمحتواها أو إتلافها أو الإضافة إلى هذه البيانات بيانات وهمية أو إحداث خلل في هذه البيانات، مما يجعل عملية نقلها في غاية الصعوبة أو قيام الجناة خلال عملية نقل هذه البيانات باعتراضها وإتلافها أو احداث تغير عليها أو عمل تخريب بالنظام الحافظ لهذه

البيانات أو القيام بسرقة هذه البيانات لأغراض متنوعة قد تكون شخصية أو إتلاف هذه البيانات أو استغلال هذه البيانات لتحقيق أهداف مادية وغيرها من اوجه الاعتداء التي سوف تتطرق لهم الباحثة خلال الدراسة (محمد، 2014).

وبخصوص جرائم الاعتداء على البيانات الشخصية لابد من الإشارة إلى أنه لقيام هذه الجرائم يجب أن تكون هذه البيانات بينات شخصية، وليست بيانات عامة متوفرة في يد الجميع، أي تلك البيانات التي يعترض صاحبها على نشرها، حيث يعتبر صاحبها عملية نشرها تهديد لحياته الخاصة، وبالإضافة تُعتبر البيانات التي يعترض صاحبها على عملية تجميعها أو تخزينها أو نقلها لجهات أخرى بدون أي مبرر قانوني أو سبب مشروع، وقد يلجأ كثير من الأفراد لحماية بياناتهم الشخصية عن طريق شركات أمن متخصصة لحماية هذه البيانات من الاختراق أو انتهاك الخصوصية من قبل الغير كون بياناتهم بيانات خاصة وحساسة خوفاً من نشرها أو استغلالها (شحته، تجريم الاعتداء على المعلومات الالكترونية ذات الطابع الشخصي بين الواقع والمأمول، 2019).

وللإشارة إلى موضوع البيانات الشخصية المتعلقة بالحالة الصحية للمريض باعتبارها بيانات شخصية تدخل ضمن البيانات الخاصة فقد أصبح في وقتنا الحالي كل مريض لديه ملف خاص يحفظ فيه بياناته الشخصية المتعلقة بمرضه، وتعتبر هذه البيانات مرجع لكثير من الأطباء لتسهيل التعامل مع المريض وتشخيص مرضه، بالتالي يجب حماية هذه البيانات من أي اعتداء قد يقع عليها كونها بيانات حساسة يلجأ لها الأطباء لوضع العلاج المناسب للشخص، بالإضافة إلى أن نشر بعض البيانات الشخصية قد يوقعه في مشكلة في التعامل مع العام من الاشخاص، وخير مثال على ذلك فايروس كورونا أو غيره من الأمراض المعدية بحيث قد بكون شخص منبوذ اجتماعياً أو قد يكون أصيب بمرض ولا يرغب بإعلام العامة بمرضه أو أمر خاص به قد يؤدي نشره إلى احراجه أمام الناس.

وهذا كان سبباً كافياً للجوء المشرع لتجريم كل هذه الاعتداءات على البيانات الشخصية، وهذا ما فعلته أغلب تشريعات دول العالم بحيث جرمت الدخول غير المشرع للبيانات الشخصية وكل صور الاعتداء عليها، علماً أن أغلب التشريعات لم تضع تعريفاً محدداً لجرائم الاعتداء على البيانات الشخصية، وقد انقسم الفقهاء بخصوص تعريف جرائم الاعتداء على البيانات الشخصية إلى قسمان فبعض التشريعات تبنت موقف عدم وضع تعريف معين؛ وذلك لعدة أسباب منها : 1- عدم حصر الأفعال التي تشكل جريمة اعتداء على البيانات الشخصية بنص قانوني وحصرها بنطاق تطبيق محدد 2- كون جرائم الاعتداء على البيانات الشخصية ضمن جرائم الانترنت ويمكن أن يتم استغلال التكنلوجيا فيها، بالتالي هي جرائم متنوعة وقابلة لتطور مع الزمن، ويمكن أن يتم تطوير أنواع جديدة منها مع التطور التكنولوجي السريع، وبالتالي في حال حصرها يمكن أن تكون وسيلة لهروب الكثير من الجناة من العقاب استناداً لمبدأ لا جريمة ولا عقوبة الا بنص وعلى العكس لجأ بعض المشرعين بوضع تعريف محدد لهذه الجرائم ومثال ذلك فرنسا، والكويت وسوريا (الدرياني، 2021).

المبحث الأول : جرائم الاعتداء على البيانات الشخصية داخل الدولة.

جاءت الحاجة إلى سن تشريع يجرم الاعتداء على البيانات الشخصية؛ نتيجة لجوء الأفراد إلى تبادل بياناتهم الشخصية بشكل يومي سواء عن طريق المعاملات التجارية أو الالكترونية أو الشركات التي تقدم خدمات معينة، وكذلك الأمر عند طلب سلع معينة، فقد يلجأ بعض الأفراد إلى إيداع بياناتهم الشخصية للتجار أصحاب هذه السلع، وبالتالي لابد من وضع حماية تشريعية لحماية هذه البيانات الشخصية (واقع الخصوصية وحماية البيانات الرقمية في فلسطين، دراسة أطلقها المركز العربي لتطوير الاعلام الاجتماعي خلال يوم دراسي حول قضية الخصوصية وحماية البيانات الرقمية للفلسطينيين، 2021)، وكذلك الأمر فيما يخص الموظفين العاملين لدى الشركات، حيث يقوموا بإيداع بياناتهم الشخصية لأصحاب هذه الشركات، وبالتالي يمكن أن تتعرض هذه البيانات لاعتداءات، ومن هنا جاءت الحاجة لسن قانون حماية

البيانات الشخصية من جميع أوجه الاعتداء عليها (شهرة ش.، :برنامج الحماية الجنائية للبيانات الشخصية في معاملات التجارة الالكترونية).

وجرائم البيانات الشخصية لا تقتصر على الشخص الطبيعي، فيمكن أن يتم ارتكابها من قبل الشخص المعنوي ولكن هناك عدة شروط منها: أن يكون الجرم الذي ارتكبه الشخص المعنوي ضمن الجرائم المنصوص عليها في القانون، وذلك وفق مبدأ شرعية الجرائم والعقوبات، حيث أنه لابد من أن يشير النص القانون لوضع الشخص المعنوي وبالعادة يكون ذلك في الجرائم الاقتصادية، والشرط الثاني هو أن تكون الجريمة قد ارتكبت بواسطة أحد أعضاؤه أو ممثلي الشخص المعنوي، حيث يكون الشخص المعنوي قد حدد أشخاص ليقوموا بالأعمال الخاصة فيه، وبالتالي تقوم المسؤولية الجنائية عن طريق هؤلاء الاشخاص، حيث يكون ادارة الشركة والتصرف والتكلم من خلالهم، ويكون ارتكاب الجريمة لحساب هذه الشركة، وبالتالي اذا ارتكبت الجريمة من قبل اشخاص لا يملكون التصرف او الادارة فهنا لا يسأل الشخص المعنوي عنها، والشرط الأخير هو أن ترتكب هذه الجريمة لحساب الشخص المعنوي أي تعود على الشخص المعنوي بفوائد و مصالح وأرباح ولا تقتصر الفائدة على الأمور المادية، فيمكن أن تكون ربح معنوي، ومن الفوائد التي حققها المشرع من ايقاع المسؤولية الجنائية على الشخص المعنوي هي تسهيل مهمة الادعاء ففي الاثبات يكفي اثبات انعدام الوفاء بالواجبات الملقى على الشخص المعنوي مثل لوائح مع الاخذ بعين الاعتبار بطبيعة كل جريمة (دكداك، 2014).

وجرائم الاعتداء على البيانات الشخصية قد يتم ارتكابها داخل إقليم الدولة أو خارج اقليم الدولة، سوف تبدأ الباحثة بدارسة هذه الجرائم داخل اقليم الدولة نفسها، حيث سوف توضح صور الاعتداء على البيانات الشخصية في الفرع الأول كذلك تطرقت الباحثة في الفرع الثاني لجرائم الاعتداء على البيانات الشخصية وفق التشريع الفرنسي، ومن ثم أتى دور النصوص التشريعية المنظمة لموضوع البيانات الشخصية حيث درست الباحثة في المطلب الأول النصوص العقابية التي تتعلق بجرائم الاعتداء على البيانات الشخصية

وفق التشريع الفلسطيني (قانون الجرائم الالكترونية،، قانون الاتصالات الفلسطيني) ومن ثم تطرقت الباحثة لموضع طرق الحماية من جرائم الاعتداء على البيانات الشخصية في المطلب الثاني، ومن ثم جاء دور المبحث الثاني الذي تطرق لجرائم الاعتداء على البيانات الشخصية خارج اقليم الدولة .

المطلب الأول: النصوص العقابية التي تتعلق بجرائم الاعتداء على البيانات الشخصية وفق التشريع الفلسطيني (قانون الجرائم الالكترونية، قانون الاتصالات الفلسطيني)

سوف تقوم الباحثة في هذا المطلب بالتطرق لأبرز القوانين التي تحدثت عن حماية البيانات الشخصية في فلسطين وجرمت الاعتداء عليها وكذلك سوف تذكر أوجه النقص ووضع الحلول البديلة لمعالجة النقص التشريعي بعد استقراء النصوص التشريعية.

وقد أوردت بعض التشريعات استثناءات على جرائم الاعتداء على البيانات الشخصية بحيث سمحت بالتعرض لهذه البيانات وبدون اذن صاحبها ويكون ذلك في حالات حددها القانون وكان للمشرع غاية من اتحات التعرض لهذه البيانات سوف تتحدث عنها الباحثة، حيث أجاز المشرع التعرض للبيانات الشخصية وذلك لمنع وقوع جريمة أو لتتبع مرتكبيها وكشفهم ولكن للقيام بهذه المهمة لابد من أن يكون هذا التعرض بناءً على قرار قضائي أو أمر من المدعي العام، اذا كان التعرض للبيانات الشخصية جاء بناءً على تشريع صادر أو تنفيذاً لهذا التشريع أو بناءً على قرار صادر من المحكمة، اذا كان التعرض للبيانات الشخصية من أجل انقاذ حياة شخص ما، اذا كانت هذه البيانات الشخصية متاحة للجمهور، كذلك الأمر يسمح بالتعرض للبيانات الشخصية اذا كان لأهداف احصائية أو تاريخية او علمية، اذا كان عرض البينات الشخصية من أجل تنفيذ عقد للحصول على خدمة أو سلعة وكانت البيانات الشخصية ضرورية للحصول على السلعة او الخدمة وهاذا ما أكدت عليه المادة15 من مشروع القانون الخاص بحماية البيانات الشخصية الاردني (مشروع قانون حماية البيانات الشخصية الاردني المعروض على اللجنة الوزارية المادة 15 منه) .

الفرع الأول: حماية البيانات الشخصية بالنصوص القانونية المباشرة .

ولا بد من الاشارة إلى النص القانوني المباشر كان قرار مجلس الوزراء رقم 3 لسنة 2019 ولم يكن تجمي جاء لتنظيم تعامل الشركات مع البيانات الشخصية تحدثت عنه سابقاً.

الفرع الثاني: حماية البيانات الشخصية بالنصوص القانونية الغير مباشرة

إن بعد الغزو التكنولوجي لجميع أنحاء العالم وفي ظل عدم وجد نصوص قانونية خاصة تحمي الخصوصية أو بالأحرى تختص بجرائم الاعتداء على البيانات الشخصية، ولمواجهة تلك المشكلة لجأت بعض الدول مثل فرنسا إلى نص تشريع خاص ومستقل لحماية البيانات الشخصية وكذلك تونس وقطر وهناك بعض الدول لم تقم بسن تشريع خاص لحماية البيانات الشخصية بل وضعت نصوص في قوانين مشابه مثل قانون الجرائم الالكترونية مثل دولة عمان أما الصنف الثالث فقد لجأت فيه الدول لحماية البيانات الشخصية بموجب تشريعات متعددة تحتوي على نصوص قانونية تحمى الحياة الخاصة وهذا ما فعله التشريع الفلسطيني (راشد، 2019).

وقد استفادت كثير من الدول من الوثائق والاتفاقيات الدولية بخصوص سن تشريعات خاصة بحماية البيانات الشخصية حيث قدر ذلك بحوال اربعة واربعين دولة، ومع العلم أن كثير من الدول تبذل جهداً لتعديل النظام القائم لمواكبة التطور الرقمي مع العلم أن أغلب الدول وضعت قيوداً على جمع البيانات الشخصية بحدود الغرض التي جمعت من أجله ولا يجوز تغيير الغرض الا بأذن من الشخص المعني، كذلك أن الدول التي لم تسن تشريع خاص لحماية البيانات الشخصية اجتهدت فيها المحاكم بتوسيع تطبيق النصوص الخاصة بحماية الحياة الخاصة أو أسندت في تطبيقها إلى نصوص قانونية خاصة وردت في اتفاقيات دولية كانت قد وقعت عليها، ولابد من الاشارة إلى أن الدول التي وضعت تشريع خاص لحماية البيانات الشخصية بخلاف الدول العربية بشكل عام قامت بأنشاء هيئات مستقلة؛ لتساعد في توفير حماية أكبر للبيانات الشخصية وذلك عن طريق التوفيق بين النصوص القانونية وموضوع حماية البيانات الشخصية من الانتهاك (جيور).

قانون الجرائم الالكترونية رقم 10 لسنة 2018.

قامت الباحثة بقراءة قانون الجرائم الالكترونية الساري في فلسطين، ودراسة النقاط التي تتعلق بالبيانات الشخصية ووجدت التالي:

1- تحدث القانون عن الجرائم التي ترتكب بحق البيانات الشخصية، فجرم عملية الدخول عمداً إلى موقع أو شبكة أو نظام يحتوي علي بيانات خاصة، وكذلك جرم الدخول بموجب تصريح ومن ثم تجاوز هذا التصريح، وقد لجأ المشرع إلى رفع سقف العقوبة في حال ترتب على الدخل اعتداء فعلي، ويكون الاعتداء أما بحذف البيانات أو شطبها أو اتلافها، تغييرها، نشرها أو الحاق ضرر بالمستخدمين أو المستفيدين، ونرى هنا أن المشرع لم يحدد صور الاعتداء علي سبيل الحصر بل على سبيل المثال حيث ذكر عبارة ما يلحق ضرر بالمستفيد أو المستخدم، وسواء كان ضرر مادي أو معنوي وقام المشرع أيضاً مرة أخرى برفع سقف العقوبة اذا ارتكب هذا الاعتداء على بيانات تخص الحكومة وقد عاقب المشرع بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، (قرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الالكترونية المادة 4 منه).

2- عاقب المشرع أيضاً على القيام بالاعتراض او التنصت على البيانات والمعلومات المرسل عبر وسائل التكنولوجيا أو عملية تسجيل هذه البيانات دون وجه حق وضع المشرع عقوبة الحبس مدة لا تقل عن سنة أو بغرامة من الف إلى ثلاثة ألاف دينار أو بكلى العقوبتين. (قرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الالكترونية المادة 7 منه)

3- عاقب المشرع أيضاً على الاعتداء على البيانات الشخصية المشفرة أو الاعتداء الذي يقع على التوقيع الالكتروني، وقد كان المشرع موفقاً بالالتفات إلى هذه النقطة حيث قامت الباحثة بقراءة نصوص قانونية بالدول المجاورة، ولم تذكر هذه النصوص موضوع التشفير والتوقيع الالكتروني

وضع المشرع عقوبة الحبس مدة لا تقل عن سنة أو بغرامة من الف إلى ثلاثة ألاف دينار أو بكلى العقوبتين (قرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الالكترونية المادة 8 منه.).

يقصد بالتشفير قيام المرسل بأرسال معلومات الى المرسل اليه، ولكن هذه المعلومات لا يستطيع سوى المرسل والمرسل اليه قراءتها، أي أن المعلومات مشفرة ومحجوبة عن الغير أي سرية ؛ وذلك لحماية البيانات من السرقة أو غيرها من الاعتداء الذي قد يقع عليها (ملاح).

التوقيع الالكتروني: "هو توقيع عادي، ولكن عن طريق الاجهزة الحديثة أي هو مخزن أي بدل الامضاء اليدوي يتم التوقيع الإلكتروني، وقد لجأت الدولة الى استخدامه، وكذلك شركات التامين وغيرها" (جامعة اكتوبر) .

هل له حجية: له حجية وقد اعتمدته محكمة النقض وجاء نتيجة اعتراف المحكمة بالمحررات الالكترونية والتي تحمل تواقيع الكترونية بين اميلات من امريكا ومول في مصر، حيث تحمل نفس حجية التوقيع العادي، لكن لا بد من تحقق شروط حددها القانون من ضمنها ارتباط التوقيع بالموقع وغيرها من الشروط (بسادة).

جرم المشرع أيضاً في قانون الجرائم الالكترونية القيام باستخدام شبكة الكترونية أو وسائل تعامل الكترونية بالوصول الى البيانات وايقاع اعتداء عليها، وضمن نص المادة نفسه في الفقرة ٤ من قانون الجرائم الالكترونية، حيث جرم المشرع القيام بالاعتداء على بيانات الغير بهدف تحقيقه مصالح (قرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الالكترونية المادة 12 منه).

المادة 22 من قانون الجرائم الالكترونية قد لخصت جرائم الاعتداء على البيانات الشخصية، حيث وضحت تجريم الاعتداء على الخصوصية، وذلك بدون تصريح قانوني أو اذن من صاحب الشخص حيث جاء بالمادة تجريم التدخل التعسفي في خصوصيات الاخرين، والفقرة الثانية من القانون جرمت عملية نشر

بيانات خاصة، وقد وضحت الباحثة هذه البيانات الشخصية في بداية الدراسة، سواء من صور، تسجيلات صوت، مراسلات خاصة، أي بيانات خاصة حتى لو كانت صحيحة، بحيث اذا لم يوافق صاحبها يكون فعل الجاني ضمن دائرة التجريم وتتطبق عليه احكام هذه المادة، وسوف نتحدث هنا عن جريمة يستند اليها القضاء الفلسطيني بشكل كبير بالتطبيقات العملية وقد تحدثنا مسبقاً أنه لضعف التشريع صاحب الاختصاص الأصيل في التجريم وهو قانون حماية البيانات الشخصية؛ لذلك يتم اللجوء لهذا القانون وهذه المادة بالأخص والفقرة الثانية نصت على حظر انشاء موقع أو تطبيق أو حساب إلكتروني أو نشر معلومات على الشبكة الالكترونية أو وسائل التواصل الاجتماعي مثل فيسبوك أو تويتر، أما بخصوص الركن المادي فهو يتمثل بالقيام ب 1- بإنشاء موقع أو تطبيق أو حساب الكتروني على الشبكة الالكترونية مثل حساب فيسبوك أو تويتر أو أي حساب على مواقع التواصل الاجتماعي وذلك من أجل نشر بيانات شخصية مثل صور أخبار تسجيلات صوت أو مرئية سواء كانت تتعلق بالمجني عليه بشكل مباشر أو مسجلة له وبالتالي هذا التصرف يشكل تدخل خارق بالحياة الشخصية حتى لو كانت البيانات التي تم نشرها صحيحة، أما بخصوص الركن المعنوي فيقوم على القصد العام المتمثل بالعلم والارادة أي علم الجاني بأنه قيام نشر بيانات شخصية خاصة بالمجني عليه وتعلقه بحياته الخاصة واتجاه ارادة الجاني لتحقيق هذا الفعل عن طريق نشر هذه البيانات عبر الحساب الالكتروني الخاص بالجاني، وضع المشرع عقوبة الحبس مدة لا تقل عن سنة أو بغرامة من الف إلى ثلاثة ألاف دينار أو بكلى العقوبتين لهذه الجريمة . (قرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الالكترونية المادة 22 منه.).

قانون الاتصالات الفلسطيني رقم 3 لسنة 1996

سوف تقوم الباحثة بدراسة قانون الاتصالات الساري في فلسطين، وتوضيح النصوص القانونية التي تتعلق بالبيانات الشخصية وجرائم الاعتداء عليها، حيث نصت المادة 4 من القانون على حفظ سرية الاتصالات على الاراضي الفلسطينية والمادة 86 نصت على جريمة النشر والتحريض ووضع عقوبة الحبس مدة لا تزيد عن سنة أو بغرامة لا تزيد عن (300) دينار أو بكلتا العقوبتين والمادة 92تحدثت عن جريمة التغيير

في محتوى الرسائل والتحريض عليه ووضع المشروع عقوبة الحبس مدة لا تقل عن شهر ولا تزيد عن ستة أشهر أو بغرامة لا تقل عن شهر ولا تزيد عن (200) دينار أو بكلتا العقوبتين والمادة 93 تحدثت عن جريمة كتم الرسائل والعبث فيها ووضع المشرع عقوبة هذه الجريمة بالحبس مدة لا تزيد عن ستة أشهر أو بغرامة لا تزيد عن ألف دينار أو بكلتا العقوبتين وسوف توضح الباحثة هذا الموضوع خلال الدراسة، حيث وجدت الباحثة بعد دراسة هذا القانون نظم موضوع البيانات التي يتم تبادلها عبر وسائل التواصل سواء عن طريق الشبكات السلكية او اللاسلكية، ومن ثم عالج القانون بشكل عام موضوع الاعتداء على البيانات، ووضع لكل جريمة عقوبة مناسبة لها .

وقد وضع قانون الاتصالات الفلسطيني رقم 3 لسنة 1996 فصل خاص للحديث عن الجرائم والعقوبات التي يمكن أن تقع خلال عمليات الاتصال والتواصل التي تجرى بين الناس، ولكن الباحثة سوف تتطوق لموضوع الجرائم التي يمكن الاستناد اليها لتجريم الاعتداء على البيانات الشخصية .

أولاً: جريمة النشر والتحريض.

تقع هذه الجريمة في حال قيام الجاني بنشر أو اشاعة أو مضمون حصل عليه بحكم وظيفته، ومن ثم قام بتسجيله، استغل موقعه الوظيفي وقام بارتكاب جريمة النشر والتحريض، وهنا كان المشرع واضحاً في تحديد هذه الجريمة (قانون الاتصالات الفلسطيني رقم 3 لسنة1996 المادة86 منه.).

ثانياً: التغيير في محتوى الرسائل أو التحريض عليه .

تقوم هذه الجريمة في حال قيام الجاني باعتراض الرسائل والمعلومات والبيانات المرسلة عبر شبكات التواصل، والقيام بتغيير محتواها أو حذف هذا المحتوى أو شطبه أو تغيره (قانون الاتصالات الفلسطيني رقم 3 لسنة1996 المادة 92 منه).

ثالثاً: كتم الرسائل أو رفض نقلها أو العبث بالبيانات.

تقوم هذه الجريمة في حال رفض الشخص المفروض عليه القيام بنقل البيانات بموجب القانون، حيث قام بكتمها ولم ينقلها أو قام بإفشاء محتوى رسائل خاصة بأحد المشتركين أو عبث فيها أو حذفها أي مارس أوجه الاعتداء على البيانات الشخصية الخاصة بالمشتركين. (قانون الاتصالات الفلسطيني رقم 3 لسنة1996 المادة 93 منه)

ترى الباحثة أن القانون هنا كان جيداً بتنظيم موضوع نقل البيانات والمعلومات عبر وسائل التواصل؛ كونه نظم هذا الموضوع في بداية القانون، ومن ثم وضع فصلاً تحدث فيه عن عدة جرائم ممكن أن يتم ارتكابها عن طريق شبكات التواصل، وقد تطرق لبعض جرائم الاعتداء على البيانات الشخصية، وقد ذكرتهم الباحثة في هذا البند.

وهنا قد قامت الباحثة بذكر بعض النصوص الغير مباشرة التي تخص موضوع حماية البيانات الشخصية من الاعتداء مثل قانون الاتصالات الذي نظم بعض النقاط التي تختص بالبيانات الشخصية وقانون الجرائم الالكترونية

المطلب الثاني: جرائم الاعتداء على البيانات الشخصية في التشريعات الأخرى وطرق الحماية منها

الفرع الأول : صور الاعتداء على البيانات الشخصية.

سوف تتطرق الباحثة لجرائم الاعتداء على البيانات الشخصية التي يمكن وقوعها من قبل الموظف المسؤول عن البيانات الشخصية بموجب عمله في الفرع الأول والاعتداءات التي قد تقع على البيانات الشخصية في الحياة العامة وقد تطرقت الباحثة للقانون الفرنسي عن طريق كُتب قانونية وضحت نصوص المواد التي تحدثت عن هذا الموضوع .

أولاً: اعتداءات تقع من قبل الموظف المسؤول عن البيانات الشخصية بموجب عمله.

سوف تتطرق الباحثة للاعتداءات التي تقع على البيانات الشخصية من قبل الموظف ولكن النصوص التشريعية التي سوف تتطرق لها الباحثة هنا ليست نصوص وطنية أي صادرة في فلسطين؛ وذلك نتيجة النقص التشريعي في هذا المجال، لذلك سوف تعرض الباحثة أنماط من صور هذه الجرائم وفق التشريعات المختلفة.

1- جريمة عدم اتخاذ الاجراءات الأولية لإجراء معالجة البيانات (شهرة ش.، حماية الخصوصية في المعاملات المالية الاسلامية، 2011).

يقوم الركن المادي في هذه الجريمة عند قيام الموظف بإجراء معالجة الكترونية للبيانات الاسمية، ولكن دون اتخاذ الاجراءات الأولية التي نص عليها القانون وأوجب القانون اجراءها قبل القيام بعملية المعالجة الالكترونية للبيانات الاسمية وذلك نتيجة اهمال أو تقاعس، وبخصوص الركن المعنوي فقد ساوى المشرع بين الخطأ والعمد أي وضع نفس العقوبة وهي الحبس أو الغرامة وهذا ما جاء في المادة 226-16 من قانون العقوبات الفرنسي .

مع الاشارة الى أن هذه البينات لابد من أن تكون متعلقة بكينونة الشخص أي متعلقة بذاتية الشخص.

وتشمل عملية معالج البيانات : كل اجراء يتم من خلاله تنظيم هذه البيانات سواء من عملية جمع أو نقل أو نشر أو حفظ أو تسجيل أو تنظيم أو تعديل أو محو أو اتلاف أو اغلاق أو الكشف عنها أو وضع معايير للوصول إليها وغيرها من العمليات التي تهدف إلى معالجة أو تنظيم أو تسهيل عملية الوصل إلى هذه البيانات من قبل أصحاب الشأن، وجميع هذه العمليات تندرج ضمن معالجة البيانات (هجيج،، 2007).

2- جريمة عدم اتخاذ الاحتياطات اللازمة لحماية البيانات المعالجة (موقع الشرق، 2017).

يقوم الركن المادي في هذه الجريمة على قيام الموظف المؤتمن بموجب وظيفته إلى عدم اتخاذ الاحتياطات اللازمة لحماية البيانات الشخصية وبالتالي ايقاع ضرر كبير بالاطلاع على هذه البيانات الذي بدوره يؤدي الى احداث ضرر على الحياة الخاصة سواء أكان الضرر على شكل تخزين أو استعمال بيانات شخصية أو كان الضرر على شكل تخزين بيانات شخصية دون اذن أو افشاء بيانات شخصية دون اذن، وبخصوص الركن المعنوي فأن المشرع الفرنسي عاقب على حدوث الركن المادي ولم يشترط للعقاب حدوث ضرر فعلي وساوى بين الخطأ و العمد، (شهرة ش.، برنامج الحماية الجنائية للبيانات الشخصية في معاملات التجارة الالكترونية).

لم تشترط النصوص القانونية لقيام جريمة الاعتداء على البيانات الشخصية أن تكون هذه البيانات سرية بطبيعتها، بل يكفي أن لا يرغب الشخص بنشرها أو يلحق به ضرر اذا تم نشرها أو الاطلاع عليها دون موافقته (الزعبي ا.، 2017).

3- جريمة المعالجة غير المشروعة للبيانات (شهرة ش.، برنامج الحماية الجنائية للبيانات الشخصية في معاملات التجارة الالكترونية).

تقوم هذه الجريمة من خلال قيام الجاني بعمليات المعالجة الالكترونية للبيانات الشخصية من خلال التسجيل أو التعديل أو الاضافة أو عملية حذف أو محو هذه البيانات، وتقع هذه الجريمة اما بوصول الجاني لجهاز الحاسوب واتصاله به مادية ومن ثم القيام بهذه العمليات أو من خلال استغلال التكنولوجيا والوصول غير المشرع لهذه البيانات، وثم احداث تغيير على البيانات الشخصية دون ترخيص مع العلم انها جريمة لا تتطلب تحقيق نتيجة جرمية أي يمكن وقوعها في حال تم الدخول لهذه البيانات دون ترخيص حتى وإن لم يستطيع الجاني الحاق ضرر ببيانات المجني عليه، وبخصوص الركن المعنوي، حيث تقوم هذه الجريمة على القصد العام اي العلم والارادة وهذه الجريمة أيضاً نص عليها المشرع الفرنسي في المادة 226-18من قانون العقوبات الفرنسي (الزعبي ع.، 2017).

4- جريمة حفظ بيانات شخصية أو تتعلق بماض أشخاص مصنفين بطريقة غير مشروعة.

حيث يقوم الركن المادي في هذه الجريمة على تسجيل وحفظ بيانات شخصية بطريقة غير مشروعة مثل الغش او التدليس أو تخزين بيانات محظور حفظها، أما الركن المعنوي فيقوم على اتجاه ارادة الجاني إلى القيام بالفعل رغم علمه بحظر حفظ هذه البيانات وتسجيلها وهي من الجرائم العمدية ولا يعتد بالباعث في هذه الجريمة ولا يتصور ارتكابها عن طريق الاهمال او السهو وهذا ما جاء في المادة 226-19من قانون العقوبات الفرنسي (الزعبي ع.، حق الخصوصية: جريمة التسجيل والحفظ غير المشروع للبيانات الشخصية).

5- جريمة حفظ بيانات شخصية خارج الوقت المخصص (الزعبي ع.، برنامج الحماية الجنائية للبيانات الشخصية في معاملات التجارة الالكترونية).

أسس الركن المادي في هذه الجريمة على أساس قيام الموظف بحفظ بيانات شخصية حصل عليها بموجب وظيفته ومن ثم قام بالاحتفاظ بهذه البيانات بعد انتهاء الوقت المخصص، وبالتالي تجاوز حدود وظيفته بعد استغلاله لنفوذ وظيفته أما بخصوص الركن المعنوي فأن المشرع هنا ساوى بين العمد والخطأ وادرج لكل منهم العقوبة نفسها وهذا ما جاء في المادة 226-20من قانون العقوبات الفرنسي (شهرة ش.، برنامج الحماية الجنائية للبيانات الشخصية في معاملات التجارة الالكترونية).

وقد اشارت الباحثة مسبقاً الى أن أغلب التشريعات لم تضع مفهوم محدد للبيانات الشخصية، وبالتالي الأمر متروك لسلطة القاضي (قاضي الموضوع) دون مراقبة محكمة النقض، الا أن محكمة النقض تراقب في تسبيب الاحكام، ويحكم القاضي بناءً على الوقائع المعروضة أمامه لتحديد ما اذا كان هذا الفعل يدخل ضمن نطاق التجريم أم لا، ومثال ذلك اعتبار الرقم السري للهاتف بيان شخصي، وهذا لم يكن موجود قبل تطور التكنولوجيا ولم يكن من ضمن نطاق التجريم بل دخل نتيجة التقدم التكنولوجي وبالتالي لا يمكن حصرها بتعريف معين.

6- جريمة تغيير الغرض المحدد لجمع البيانات الاسمية (مصطفى، 2016).

يقوم الركن المادي في هذه الجريمة على أساس تغيير الغرض الذي جُمعت من أجله البيانات الشخصية، حيث في بادئ الأمر قبل جمع البيانات الشخصية يوافق أصحابها على تقديمها؛ وذلك لغرض محدد مثل الحصول على خدمة معينة مثل خدمات الاتصالات إلا أن الموظف المسؤول عن جمع هذه البيانات غَير الغرض من جمعها واستخدمه لمأرب أخرى مثل بيع هذه البيانات لأهداف تجارية أو سياسية، وبالتالي انتهاك سرية وخصوصية هذه البيانات وبخصوص الركن المعنوي فأن المشرع الفرنسي عاقب على حدوث الركن المادي ولم يشترط للعقاب حدوث ضرر فعلي وساوى بين الخطأ و العمد وهذا ما جاء في المادة 226-20من قانون العقوبات الفرنسي (موقع مراجع جامعية، 2022).

ويمكن اعتبار البيانات التي تتعلق بأموال الاشخاص أو عملهم أو مصدر دخلهم ضمن البيانات الشخصية، ولا يقتصر الأمر على البيانات التي تتعلق بالحياة الخاص بالفرد اي بشخصيته بل يمكن أن تمتد للوضع المالي للشخص (شحته، تجريم الاعتداء على المعلومات الالكترونية ذات الطابع الشخصي بين الواقع والمأمول، 2019).

7- جريمة إفشاء البيانات الشخصية بما يضر صاحب الشأن (شحته، : تجريم الاعتداء على المعلومات الالكترونية ذات الطابع الشخصي بين الواقع والمأمول، 2019).

يتمثل الركن المادي في هذه الجريمة بقيام الموظف المسؤول عن البيانات الشخصية سواء كان مسؤولًا عن جمعها أو معالجتها أو تنظيميها أو الاطلاع عليها بحكم عمله أي مسؤول عن الحفاظ عليها إلا أنه قام بإفشاء هذه البيانات أو الإفصاح عنها لجهات غير مصرح بالقانون الافصاح عنها أو قام بالإفصاح عنها دون موافق صاحب هذه البيانات، وبخصوص الركن المعنوي فأن المشرع الفرنسي عاقب على حدوث الركن المادي ولم يشترط للعقاب حدوث ضرر فعلي وساوى بين الخطأ والقصد (علي، 2021).

مع الاشارة إلى أن لرفع الدعوى يكفي لتأسيسها وقوع ضرر معنوي، ولا يشترط أن يكون هناك ضرر مادي ملموس بحيث يقع الضرر المعنوي بمجرد الاطلاع على هذه البيانات وهذا ما جاء في المادة 226–22من قانون العقوبات الفرنسي (شهرة ش.، برنامج الحماية الجنائية للبيانات الشخصية في معاملات التجارة الالكترونية). ومن الأمثلة التطبيقية على ضرورة احترام الخصوصية للعاملين وعدم انتهاك البيانات الشخصية للأفراد، حيث قضت محكمة العمل القطرية أنه لا يحق لصاحب العمل مراقبة المراسلات الشخصية التي يقوم بها الموظفين إلا في ظروف استثنائية وفق شروط معينة وبعد الحصول على موافقة الموظف، واعتبرت المحكمة أيضاً موافقة الموظف على الرقابة خوفاً من الفيروسات لا تعتبر موافقة من أجل الرقابة العينية، ولا يوجد ما يبرر مراقبة مراسلات البريد الالكتروني للموظف وجمع المعلومات واستخدامها بل يعتبر ذلك انتهاكاً للخصوصية (قرار محكمة العمل القطرية، رقم الملف 8/90، 2022).

ثانياً: صور الاعتداءات التي قد تقع على البيانات الشخصية في الحياة العامة.

1. تخزين بيانات شخصية بدون إذن الشخص ودون صفة قانونية.
2. نشر هذه البيانات بقصد إلحاق الضرر بالغير.
3. استعمال البيانات الشخصية بطريقة خاطئة نتيجة الإهمال أو قلة الاحتراز (شهرة ش.، برنامج الحماية الجنائية للبيانات الشخصية في معاملات التجارة الالكترونية)

وهنا قامت الباحثة بعرض صور للاعتداء على البيانات الشخصية، وسوف تتطرق خلال الدراسة للجرائم التي نصت عليها التشريعات، والانظمة، وموقف التشريع الفلسطيني من هذه الاعتداء، وما هي النصوص التي تحكم هذه الجرائم.

وجاء في قرار للمحكمة العليا التركية في تعريفها للحياة الخاصة: أن مفهوم الحياة الخاصة لا يقتصر على حياة الشخص وخصوصيته بعيداً عن العين، ولا على الأمور التي لا يتم مشاركتها مع الاخرين خلف الأبواب المغلقة بين أربع جدران، بل يمتد ليشمل جميع ما يتعلق بالحياة الخاصة والبيانات التي لا يرغب

بمعرفتها الأخرين، وبناءً على ذلك، التواجد في منطقة عامة لا يعني السماح بتسجيل صوت أو صورة ومن ضمن احترام الخصوصية أن الأشياء التي يفعلها الشخص في الأماكن العامة لا يريد أن يعرفها الأخرين، وبالتالي الحياة الخاصة غير محددة بنطاق البيئة المادية ومكانة الشخص في المجتمع بل يجب أيضاً مراعات معايير الجمهور وسلوكياته وموافقته ومثال على ذلك، قيام المتهم بالتقاط صور للعامة من نساء وفتيات وتركيز الكاميرا والصور على خصوصيتهن الجسدية دون موافقتهن، في أعمار مختلفة وأثناء مرورهن في الشارع، مثل الوجه والركبتين ، وهنا اعتبرت فعل المتهم انتهاكاً للخصوصية وأن صور النساء قد لا يردن أن يعلم بها اخرون عن طريق المتهم واعتبرت المحكمة منتهكاً للخصوصية ، وفي حكم آخر لها اعتبرت قيام المتهم بارتداء قبعة وملاحقة الضحية والتقاط صوراً لها لإثبات العلاقة بينه وبين زوجته يعنبر جريمة، وقرار أخر اعتبار التقاط صور لنساء على الرصيف من مسافة 25متر انتهاكاً للخصوصية. (قرار للمحكمة العليا التركية، جريمة انتهاك الحياة الخاصة 134 tck، 2022).

الفرع الثاني : جرائم الاعتداء على البيانات الشخصية وفق التشريع الفرنسي.

1- جريمة التقاعس عن الإجراءات المبدئية لمعالجة البيانات:

ويقصد بمعالجة البيانات: إجراء عمليات أو مجموعة من العمليات التي يتم تنفيذها باستخدام أدوات معينة ليتم عمل تنظيم أو جمع أو تخزين أو تسجيل أو تحديثات أو حذف أي عمليات تستهدف معالجة هذه البيانات لتسهيل التعامل معها (سياسة الخصوصية للبيانات الشخصية).

يتحقق الركن المادي فيها في حال فرض القانون التزامات مبدئية على الشخص المتولي معالجة البيانات؛ لحمايتها قبل عملية المعالجة، ولم يقم بها، أما الركن المعنوي فيقوم في حال تحقق القصد العام أو الخطأ، أي ساوى المشرع هنا بالمسؤولية الجنائية في حال الخطأ أو القصد العام المتمثل بالعلم والارادة (شهرة ش.، برنامج الحماية الجنائية للبيانات الشخصية في معاملات التجارة الالكترونية) .

وترى الباحثة أن المشرع أتخذ هذه الخطوة لأغلاق باب الهروب من العقاب من قبل الأشخاص عن طريق إغلاق باب الخطأ أي أن يهرب الشخص من المسؤولية بحجة الخطأ وينفي مسؤوليته الجنائية.

2- جريمة تغير الغرض من جمع البيانات الشخصية:

تقع هذه الجريمة اذا تم تغير الغرض او الغاية من معالجة البيانات الشخصية أي الهدف من معالجة البيانات أي تحَصل على البيانات الشخصية بصورة مشروعة ومن ثم غير العرض من جمعها وخير مثال على ذلك استغلال هذه البيانات بهدف الكشف عن ثروة صاحب هذه البيانات وبخصوص الركن المعنوي فانه يقوم على القصد الجنائي العام أي العلم والارادة دون الالتفات للبواعث (عودة، 2018).

وترى الباحثة أن جرائم البيانات الشخصية تعتبر جرائم مرافقة للتطور التكنولوجي، بحيث أن الوسائل التكنولوجية تعتبر عامل مساعد بشكل كبير لها، وبالتالي في حال حصر المشرع هذه الجرائم بنوع معين منها يكون قد جانب الصواب، فمن المستحسن أن يترك الباب مفتوحاً لما يستجد منها لأنه باختصار لا يمكن ضبطها بنص تشريعي يحصر فيه الجرائم الواقعة على هذه البيانات.

وقد يلجأ الجاني إلى عدة طرق ووسائل؛ من أجل تمكينه من الدخول غير المشروع لنظام المعلوماتي، فبعض الأحيان قد يتمكن الجاني من الدخول ببساطة وسرعة، مثال ذلك عن طريق تشغيل جهاز الحاسب الالي أو قد يحتاج لبذل جهد مثل الحصول على شيفرة خاصة؛ لإتمام عملية الدخول أو فك هذه الشيفرة ومن الطرق الدارجة استخدام برامج فايروسيه؛ من أجل الدخول إلى الحاسب الالي، ومن ثم اختراق نطام المعلومات وقد ساعدت التكنولوجيا في تنفيذ مثل هذه الجرائم خارج نطاق الدولة وتختلف أهداف الجاني فقد يكون هدفه إظهار ضعف الأمن في دولة معينة وإظهار اختراق النظام المعلوماتي أو قد يكون هدفه إزالة تلك المعلومات أو تدميرها أو قد يكون هدفه هو تنفيذ جريمة أخرى بعد التمكن من اختراق هذا النظام (الحمداني، 2019).

ومن الأمثال التطبيقية على ذلك توجيه هذه التهمة لأحد الأشخاص في دبي بعد قيامه بإساءة استخدام الانترنت لأغراض غير مشروعة، حيث قام باستخدام برنامج قرصنة تمكن من خلاله من كسر كلمة المرور لموظف مؤسسة الإمارات للإيصالات والدخول لأماكن غير مصرح بالدخول اليها وقام بنسخ العديد من كلمات المرور الخاصة بالموظفين والعديد من البيانات الشخصية الخاصة فيهم (القاسمي، 2018).

أما بخصوص الركن المعنوي: تقوم هذه الجريمة على القصد العام، وهو العلم والارادة أي أن الجاني يعلم أنه يدخل على نظام معين، وكذلك لم يحصل على إذن من صاحبها، ولا تقع الجريمة خطأً، ولا تتطلب قصد خاص لوقوعها، وهي من الجرائم المقصودة(الزعبي م.، 2021)

وقد قررت المحكمة أنه يحظر على الجهات المقدمة للخدمات القيام باعتراض أو اختراق للبيانات الشخصية، والاعتراض يشمل كل مشاهدة للبيانات الشخصية أو المعلومات أو الحصول عليها بغرض التنصت أو تغيير المحتوى أو التعطيل أو التنصت أو نسخ أو تغيير المسار أو اعادة توجيه البيانات دون اذن صريح من صاحبها ودون مبرر مشروع والاختراق يشمل الدخول غير المشروع والغير مصرح فيه والمخالف لأحكام الترخيص أي الدخول بطريقة غير مشروعة (الجواد، 2020).

وبعد إطلاع الباحثة على كثير من الأبحاث والدراسات السابقة المتعلقة بموضوع الاعتداء على البيانات الشخصية، وجدت أن التشريعات الأخرى كانت داخلة في تنوع كبير في دائرة التجريم واختلاف بمسميات وأنواع هذه الجرائم، كذلك بدول العالم الثالث، تختلف النصوص التشريعية عن الدول المتقدمة تكنولوجياً، بحيث أن التشريعات في كل من البلدين تختلف وينعكس ذلك على أنواع الجرائم؛ لذلك لجأت الباحثة لذكر أنوع لجرائم الاعتداء على البيانات الشخصية الأساسية منها والموجودة بأغلب التشريعات، وذلك لعدة أسباب منها أنه لا يمكن كتابة جميع أنواع هذه الجرائم في رسالة واحدة.

وجرائم الاعتداء على البيانات الشخصية لا تقتصر فقط على الأفراد العادين، بل يمكن أن يتم ارتكابها بحق أشخاص عاملين بالدولة، بحيث يتم الاعتداء على الأنظمة الخاصة بالدولة أو الأنظمة الخاصة

لشخصيات اعتبارية عامة بالدولة، ويكون ذلك إما بغرض سرقة بيانات أو اتلافها أو تدميرها أو في بعض الأحيان يلجأ الجاني لسرقة كلمة المرور لنظام معين مثلا هذا النظام يتعلق بالأشخاص الموقفين، ومن ثم تدمير هذه البيانات أو تغيير محتواها وخير مثال على ذلك برنامج ميزان (نظام تابع لمجلس القضاء الأعلى)، فقد يلجأ الجاني لتغيير ضبوط الجلسات وتغيير البيانات الشخصية الموجودة فيها؛ بهدف حماية شخص معين، كذلك قد يتم اختراق النظام الخاص بجهاز معين وتغيير بيانات معينة بما يخدم مصالح شخصية للجاني، مثل وضع اسم بعض الموقفين ضمن قائمة الأشخاص الذين سوف يتم اطلاق سراحهم بهدف الهروب من العقوبة (السعيد، 2021).

الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة: يقوم الركن المادي في هذه الجريمة على قيام الجاني بالدخول إلى النظام المعلوماتي التابع للدولة سواء باختراقه أو عن طريق القرصنة أو غيرها من الطرق غير المشروعة وقد يكون الدخول عن طريق الخطأ، وبقى مستمر في البقاء في النظام وسواء كان هذا النظام لحساب الدولة أو شخص اعتباري عام فيها، وقد شدد المشرع في العقوبة المستحقة على الجاني في حال ترتب على فعل الدخول تدمير أو حذف أو إلغاء أو تغيير في محتوى البيانات الخاصة بالدولة حيث شدد هنا العقوبة في أغلب التشريعات (البدوي، ، ماهي عقوبة الاعتداء على الأنظمة المعلوماتية لدولة، 2022).

وترى الباحثة أن الاعتداء على البيانات الخاصة في الدولة سواء كانت أنظمة أو بيانات تابعة لأحد المسؤولين فيها تعتبر من الجرائم الحساسة؛ ولهذا السبب وسع المشرع دائرة التجريم بحيث أن بمجرد دخول الشخص دخول غير مشروع للنظام أو دخل بالخطأ، واستمرار بالبقاء فيه يكون قد دخل في دائرة التجريم، أيضاً بالإضافة إلى أنه في حال دخل الشخص بتصريح إلى النظام وانتهى تصريحه واستمر بالدخول إليه، يكون أيضاً ضمن دائرة التجريم، وكان المشرع موفقاً في ذلك كون نظام الدولة يعبر عن قوتها وثقة

المواطن فيها وكلما كانت بياناتها وبيانات الاشخاص العالمين فيها محمية يكون ذلك دليل واضح على قوتها والعكس صحيح.

ومن الأمثلة على ذلك القضية التي حكمت بها المحكمة الادارية العليا في مجلس الدولة والتي قضت بإدانة المتهم الطاعن وحكمت عليه بالفصل من الخدمة، والمتهم الثاني حكمت عليه بخفض من وظيفته إلى المستوى الادنى مباشرة وذلك لأن المتهم الأول قام باختراق أجهزة الحاسب الآلي لبعض العاملين بالهيئة، وبالتالي انتهاك سرية البيانات والمتهم الثاني هو من زوده بكلمة المرور الخاصة بالحاسب الآلي، وأكدت المحكمة على حظر الاعتراض أو اختراق البيانات الحكومية وأن حماية البيانات وأسرار الدولة هي من مسائل الأمن القومي؛ وذلك لحفظ استقلال واستقرار الأمن القومي ووحدته وسلامة أراضيه، وتم اثبات التهمة عن طريق الدليل الرقمي وليس الورقي بحيث أتم المتهم جريمته عن طريق استخدام برامج تجسسيه من جهازه للحصول على بيانات من أجهزة أخرى، واستخدم الجاني فلاش ميموري وهارد دسك لحفظ البيانات السرية، وتبين وجود عمليات اختراق على الجهاز الذي يعمل عليه حيث اخترق نظام معلوماتي لحساب الدولة، وأكدت المحكمة أن دفع الطاعن بعدم وجود سندات ورقية بحوزته ليس بمحله، حيث ثبتت التهمة عليه عن طريق الدليل الرقمي وتم كشفت الجريمة عم طريق اختراقه لحسابات تحتوي علي بيانات سرية خاصة بالدولة، وأكدت المحكمة في حكمها أن العقاب جاء لتحقيق الردع لأن الفعل الذي تسيب فيه الطاعن يؤثر على اقتصاد الدولة ويؤدي إلى زعزعة الاستقرار فيها وبالتالي يستحق أشد العقاب (علاء، 2022) .

الفرع الثاني : طرق الحماية من جرائم الاعتداء على البيانات الشخصية.

بخصوص موضوع حماية البيانات الشخصية، يعتبر هذا الموضوع من أهم المواضيع التي يجب أن يلتفت لها الأشخاص؛ وذلك لأن الشخص نفسه يتعامل مع هذه البيانات ويقدمها للجهات الأخرى بشكل دوري أو

بالأحرى بشكل يومي، وبالتالي لا بد من أن يكون هناك طرق لحماية هذه البيانات وهذا ما سوف تعرضه الباحثة في هذا المطلب.

الفرع الأول : نصائح وارشادات وقائية للقارئ بصفته يستخدم البيانات الشخصية بشكل يومي

1. لجأ بعض أصحاب الشركات الكبرى أو أصحاب المشاريع الكبيرة إلى استخدام وسائل تكنولوجية تُوضع على جهاز الحاسوب أو أجهزة العمل الاخرى لمراقبة العاملين (دريزو، 2017)، وبغض النظر هل تصرف صاحب العمل هذا كان قانوني أم لا، لا بد من أن يكون الشخص حذر ولا يدخل بياناته الشخصية في أي مكان يعمل فيه؛ وذلك من أجل حمايته بالدرجة الأولى ومنع استغلال هذه البيانات من قبل الغير.
2. ولابد للأشخاص الانتباه لنقطة مهمة وخصوصاً الأشخاص الذين طبيعة عملهم تكون على شكل فرق ولأننا بعصر التقدم التكنولوجي السريع واستخدام الوسائل التكنولوجية السريعة والتي تسهل انجاز العمل بأسرع وقت وأقل جهد فقد ظهرت على الساحة حديثاً مواقع للتواصل بين الأشخاص الذين يعملون بروح الفريق، ومن هذه البرامج goggle hangout slack وغيرها من البرامج التي خصصت لتبادل الرسائل للفريق الواحد، وبالتالي لابد من الحذر وعدم إتاحة الأشخاص لبياناتهم الشخصية في هذه المواقع، وهذا بسبب أن هذه البرامج تحتفظ بالرسائل ويمكن اعادة استخراجها بأي وقت (برنامج جوجيل هنجوتس، هو برنامج صنعته الشركات لتسهيل التواصل وانجاز المهام أثناء العمل كفريق حيث سهل عملية التواصل مع الأفراد بدل من اجراء المكالمات بين بعضهم البعض، كذلك يوجد يه ميزة مفيدة ويحفظ الرسائل المتبادلة بين العاملين.).
3. أما النصيحة الثالثة، فهي البقاء على عنصر الحذر عند استخدام وسائل التكنولوجيا، حيث لجأت في الآونة الأخيرة العصابات إلى استدراج الأفراد عن طريق الدخول إلى حساباتهم عن طريق حسابات وهمية وإيهام الفرد بربح مبلغ كبير أو سيارة أو ذهب، ومن ثم يطلب الجاني بيانات شخصية من المجني عليه لتحويل المبلغ لرصيده بالبنك أو الباسورد لحساب إيميل أو فيسبوك، ومن ثم سرقت

حسابه بالبنك أو حصوله على بينات شخصية ومن ثم تهديده بهذه البيانات (، 7 أشياء لا تفعلها على مواقع التواصل الاجتماعي، 2019).

4. ولا بد من الاشارة إلى موضوع أخر أيضاً دارج في الفترة الأخيرة، هو طلب يلجأ إليه بعض الجناة عن طريق برنامج يتيح التحكم عن بعد بجهاز الشخص المراد الدخول اليه، ويكون ذلك بعد طلب الإذن من صاحب الجهاز، ولكن لا بد من الحذر لأنه في الواقع يدخل لسرقة بيانات خاصة؛ لأن هذا البرنامج يتيح للشخص التحكم عن بعد ومن ثم استغلال البيانات الشخصية ولكن يجدر الإشارة إلى أن هذه البرامج تستخدمه أيضاً شركات الدعم الفني، وبالتالي لا مانع من السماح لهذه الشركات كونها تكون معروفة الغرض من دخولها للجهاز.
5. لا مانع من مجارات التكنولوجيا واستخدام برامج تحمي الجهاز من التهديدات الخارجية وبرامج مكافحة الفيروسات التي قد تكون موجودة على الجهاز (حماية الكمبيوتر من الفيروسات، 2019).
6. لا بد من الإشارة إلى حماية المصدر الرئيسي لخصوصية الأشخاص أي شبكة الانترنت ذاتها لأنها قد تكون مصدر دخول لكثير من المتطفلين، ولا بد من حماية هذه الشبكات عن طريق وضع كلمة مرور لشبكة الانترنت؛ لمنع دخل المخترقين أو غيرهم من الأشخاص الذين يرغبون بالدخول إلى الشبكة (نصائح ذهبية لحماية البيانات الشخصية، 2019).
7. لا بد من الحذر من مشاركة الخصوصية عبر وسائل التواصل الاجتماعي، حيث قد يلجأ الشخص إلى مشاركة خصوصيته وبياناته الشخصية عن طريق الخطأ من ثم يقع في مشكلة استغلالها من قبل أشخاص قد يكونوا يتصيدوا لمثل هذه المواقف، وقد حدث ذلك فعلاً عند قيام الأشخاص بمشاركة بياناتهم الشخصية عبر مواقع التواصل الاجتماعي مثل مكان السكن، وقت الذهاب للعمل ووقت الرجوع منه، الراتب الشهري، رقم الهاتف، الأموال ومصادر الدخل المملوكة لشخص وغيرها من البيانات الشخصية، بحيث قد يتم استغلالها لمراقبة الشخص وسرقته أو قد يستخدم الجاني الوسائل

التكنولوجية والدخول لأنظمة خاصة بالشخص وإتلاف بياناته الخاصة وتدميرها، وبالتالي الأمور الخاصة لا يجب عرضها للناس (موسى، 2014).

8. لا يقتصر موضوع حفظ الحياة الخاصة على حفظ البيانات الشخصية العادية بل يمتد الموضوع لكثير من البيانات التي يشاركها الأشخاص عبر مواقع التواصل الاجتماعي مثل فيسبوك، ويتم استغلالها دون علمهم ومنها تحركات الشخص مثل السفر والعودة منه والموقع الجغرافي ؛ لأن هذه البيانات تساعد الجاني بعملية سرقة قد يشنها أثناء غياب الشخص عن بيته أو خروجه من بيته (قواعد أساسية لحماية بياناتك علة شبكة التواصل الاجتماعي، 2018).
9. لا بد من تجنب نشر بيانات أخرى مثل محل العمل، تاريخ الميلاد، عنوان المنزل؛ لأنها بيانات شخصية بأي لحظة ممكن أن يتم استغلالها.
10. كذلك الأمر في مواقع التواصل الاجتماعي تظهر هناك العديد من التطبيقات أو الألعاب أثناء تصفح صفحات التواصل الاجتماعي، وتهدف هذه التطبيقات لسرقة البيانات الشخصية بشكل أو بأخر، وبالتالي لابد من الحذر وعدم التعاطي معها، بحيث يمكن استغلال هذه التطبيقات باستدراج الأطفال واستغلال بياناتهم الشخصية مثل اسم المدرسة، وقت الدوام، وقت العودة من المدرسة، العمر، مكان السكن، الطول، الوزن، وبالتالي بعد استغلال هذه البيانات تساهم هذه البيانات في تسهيل عملية ارتكاب جرائم اخرى للجاني.
11. ولا بد من الحذر من موضوع استغلال الناس عن طريق الهدايا والمسابقات التي تهدف إلى استغلال البيانات الشخصية بدرجة أولى ومن ثم فتح باب لارتكاب ما يرغب الجاني من ارتكابه ، ولاسيما أن جرائم الاحتيال المنتشرة بشكل كبير تبدأ عن طريق البيانات الشخصية، حيث من خلالها يتم معرفة من هم الأشخاص الذين يملكون المال من غيرهم.

12. ولتحصين وحماية البيانات الشخصية لا بد من قيام الشخص بوضع كلمة مرور مميزة صعب اختراقها؛ وذلك لأنه نتج عن التقدم التكنولوجي أنظمة افتراضية تعمل على تخمين كلمة المرور ومن ثم الدخول على النظام، وبالتالي لا بد من الحذر من هذه النقطة.
13. وكذلك وضع كلمة مرور على الهواتف النقالة، ولا بد من أن تكون كلمة المرور صعبة التخمين، ولا بد من أخذ الحيط والحذر بحيث يتم تنزيل الألعاب فقط من متاجر التطبيقات الرسمية والموثوق بها، وفي حال رغب الشخص بإصلاح هاتف ممكن أن يلجأ لطريقة تنزيل برامج خاصة تتولى حذف البيانات الشخصية الموجدة على الهاتف، وفي حال رغب بالاحتفاظ بهذه البيانات ممكن ان يقوم بنقلها لبرنامج آخر، ومن ثم استخدام برنامج معين لحذفها، وكذلك لا بد من الحذر من فتح الروابط المجهولة (القادر، 2021).
14. ومما يجب الحذر منه أيضاً، وجود بعض التطبيقات التي تتطلب الوصول للكاميرا الخاصة بالشخص أو الميكروفون أو تسجيل الصوت أو استديو الصور وغيرها من البيانات الشخصية، وبالتالي لا بد من حماية البيانات الشخصية من أي اختراق قد تتعرض له (كيف تمنع التطبيقات من استغلال بياناتك، 2022).
15. ومن وسائل التسلل للبيانات الشخصية استخدام طريقة انتحال الشخصية لأحد البنوك أو المؤسسات أو كبار التجار، بحيث يلجأ هؤلاء الأشخاص منتحلي الشخصيات إلى التسلل للبيانات الشخصية عن طريق روابط معينة بهدف سرقة البيانات الشخصية للأفراد (الاحتيال الإلكتروني... مواجهة مع التهديدات السيبرانية في قطر، 2019).
16. يمكن استخدام برامج ذات تقنيات عالية؛ لزيادة الأمان وحفظ الخصوصية، بحيث يتطلب هذا البرنامج نموذج آخر للتحقيق من هويتك بالإضافة إلى الباسورد مثل بصمة الإصبع أو بصمة العين أو صورة الهوية الشخصية، وكل هذا لحفظ البيانات الشخصية من العبث، وقد لجأت له الدول في مواجهة جائحة كورونا ومن أجل حفظ البيانات الشخصية للمريض او المشتبه بإصابته، بحيث يحصل

الشخص على نتيجة فحصه للمرض عن طريق إضافة الهوية الشخصية (موقع وزارة الصحة الفلسطيني، 2022).

17. قيام الشخص بعد استخدام جوجل الدخول إلى خانت أنشطتي، وهي خدمة لتعزيز الخصوصية بحيث تحتوي هذه الخانة على جميع الأنشطة التي دخلت عليها وقمت بها وبالتالي يمكن مسح الأنشطة التي قام بها، وبهذه الخطوة لن تتمكن شركة جوجل من الحصول على بياناتنا الخاصة بكل الأوقات، حيث وفرت هذه الخدمة شركة جوجل نفسها (عنتر، كيفية حماية البيانات الشخصية بخطوات بسيطة، 2019).

18. وهناك طريقة أخرى لحماية البيانات الشخصية هي استخدام محركات بحث أخرى غير جوجل، مثل Duck go محرك بحث، بحث تحفظ الخصوصية حيث أن هذا التطبيق يحفظ الخصوصية بشكل أكبر ومن مميزاته منع تعقب أي من المستفيدين، ويمنع الإعلانات المزعجة (عنتر، كيفية حماية البيانات الشخصية بخطوات بسيطة ، 2019).

كل موقع ندخل عليه سواء موقع تسوق أو موقع تواصل اجتماعي نكون قد قدمنا كم كبير من بياناتنا الشخصية؛ ولأهمية حماية البيانات الشخصية لجأت بعض الدول مثل فرنسا، بلجيكا، السويد، النمسا وغيرها من الدول لوضع نظام لحماية البيانات الشخصية، وشكلت هيئة يكون دورها وضع قواعد تنظيمية لجمع واستخدام ومعالجة ونقل البيانات الشخصية، وهذه الهيئة تكون مستقلة وتتكون من قضاة ومحامين ومتخصصين وأعضاء منتخبين يكون دورهم ضمان حماية بيانات الناس الموجودة بالوزارات والهيئات والمؤسسات والشركات العامة والخاصة، بحيث تساعد هذه الهيئة بحماية بياناتنا الشخصية (حماية البيانات الشخصية، 2016).

19. من الطرق التي يمكن للفرد العادي استخدامها لحماية بياناته الشخصية، أن يطلع على سياسة الخصوصية قبل الدخول لأي موقع أو تطبيق، وفي إعدادات الوصول عدم السماح لهذا التطبيق

بالوصول إلى جهات الاتصال أو الموقع الخاص بك و حتى محتوى الهاتف (أعددنا في سدايا سياسة حماية البيانات الشخصية ؛ للمحافظة على خصوصية الأفراد في كل الميادين ٢٠٢١).

20. ومن الطرق الأخرى التي يمكن اللجوء لها لحامية البيانات الشخصية، العمل على حذف البيانات الشخصية الموجودة على الجهاز في حال رغب الشخص ببيعه أو إعارته لأحد الأفراد، وممكن استخدام برامج تأتي مهمتها بحذف البيانات الشخصية، وممكن التحقق من الشركة المصنعة للجهاز بخصوص موضوع حفظ البيانات الشخصية وكيفية حذفها عن الجهاز، ويمكن من أجل عملية تسهيل حذف البيانات المخزنة على الجهاز، يمكن الرجوع إلى موقع الشركة والاستفادة منه، أما بالنسبة لأجهزة الهاتف النقال فيمكن ازالة بطاقة التخزين وحذف سجلات الهاتف وتسجيلات الصوت وكل ما يتعلق بالبيانات الشخصية كإجراءات وقائية لحماية الشخص وحماية حياته الخاصة (نصر، 2018).

21. ولا بد من قيام الدولة بالتدخل بموضوع حماية البيانات الشخصية، وذلك من خلال المراقبة العامة والتأكيد على الامتثال للقوانين والاتفاقيات الدولية التي ركزت على احترام الخصوصية، ولا بد من قيام الدول من فرض رقابة عامة على شركات الاتصالات، والتأكد أن البيانات الشخصية لديها محمية (مجلة العلوم الانسانية العدد السابع الجزء، 2017).

22. إنشاء هيئة لحماية البيانات الشخصية للأفراد، وتكون هذه الهيئة مكونة من محامين ومستشارين وأعضاء منتخبين؛ وذلك لمتابعة موضوع حماية البيانات الشخصية، ومن الممكن أن تقوم الدولة بعمل دورات تثقيفية بخصوص البيانات الشخصية وتجنب إفشاؤها (مجلة العلوم الانسانية العدد السابع الجزء1).

23. ويمكن لجوء الشخص لعدة أساليب يمكن من خلالها تفادي الاعتداءات التي قد تقع على بياناته الشخصية، عن طريق وسائل الاتصال والتواصل الالكترونية منها وسائل فنية انتجتها التكنولوجيا، ومن هذه الوسائل استخدام أنظمة منها نظام كشف الدخلاء، ونظام تحرير العنوان، ونظام المرشحات الإلكترونية (ناصر، حماية البيانات الشخصية لمستخدمي شبكات التواصل الاجتماعي).

24. لا بد من التأكيد على معرفة الشخص الذي سوف يقدم بياناته لشركة معينة بالغرض الذي جمعت بياناته من أجله أي على الشركة إخطاره بالغرض الذي جمعت بياناته من أجله، وهذا ما نصت عليه أغلب التشريعات، مثل القانون العماني، حيث جاء في المادة٤٣ من القانون الخاص بحماية البيانات الشخصية "يجوز لأي جهة حكومية أو مقدم خدمات تصديق أن يجمع بيانات شخصية مباشرة من الشخص الذي تجمع عنه البيانات أو من غيره، بعد الموافقة الصريحة لهذا الشخص؛ وذلك لغرض اصدار شهادة أو المحافظة عليها أو تسهيل ذلك ، ولا يجوز جمع البيانات أو معالجتها أو استخدامها لأي غرض آخر دون الموافقة الصريحة لشخص المجموع عنه البيانات"، وبالتالي حددت المادة القانونية بصريح العبارة شرط موافقة الشخص صاحب البيانات، مع وجود بعض الاستثناءات منها اذا كانت هذه البيانات ضرورية لكشف جريمة أو مثلا هذه البيانات مطلوبة لأغراض الاحصاء والضريبة بالدولة حيث جرت العادة على التحري عنها (ناصر، حماية البيانات الشخصية لمستخدمي شبكات التواصل الاجتماعي).

25. والطريقة الأخرى هي ضمان سرية البيانات الشخصية: بحيث يقع التزام على الشركات المقدمة لخدمات الاتصالات القيام بإجراءات أمنية؛ لحفظ سرية البيانات الشخصية، وعدم الإهمال بحفظها ومن ضمن حمايتها أن لا يتم نشرها أو إفشاءها أو نقلها لشركات أخرى إلا بموافقة صاحبها، وهذا ما أكد عليه المشرع في تشريعات أغلب الدول من ضمنها التشريع العماني (ناصر، حماية البيانات الشخصية لمستخدمي شبكات التواصل الاجتماعي).

والمشرع هنا لم يحدد الإجراءات، ولم يذكرها بصريح العبارة أي أنه تركها مفتوحة؛ وذلك لأن التطور التكنولوجي لا يمكن حصره، وتكون هذه الإجراءات من خلال استخدام أنظمة مثل تشفير البيانات أو طريقة الجدران النارية لحماية البيانات أو برامج مضادة للفيروسات وأي طرق أخرى مشروعة لا يوجد فيها تعدي على الاخرين أو خصوصياتهم وبنفس الوقت تحمي البيانات الشخصية واشترط المشرع

هنا السرية؛ وذلك لتحقيق الأمان لدى المواطن كون هذه البيانات يجب حفظها وعدم التشهير فيها (ناصر، حماية البيانات الشخصية لمستخدمي شبكات التواصل الاجتماعي).

لا بد من الإشارة إلى أن قيام الشركات بالإجراءات اللازمة لحماية البيانات الشخصية هي بذل عناية، وليس تحقيق نتيجة، وبالتالي تكون الشركة مسؤولة عن أي اعتداء يقع على البيانات الشخصية في حال وجود خطأ من الشركة نفسها أو أحد العاملين فيها (ناصر، حماية البيانات الشخصية لمستخدمي شبكات التواصل الاجتماعي).

26. من الأنظمة التي يمكن استخدامها لحماية البيانات الشخصية في دول الخليج والتي أثبت فعاليتها النظام international privacy Protection policy ومن مميزات هذا النظام يمكن لجميع الدول التي ترغب في حماية البيانات الشخصية لمواطنيها تفعيله عن طريق استخدامه بالوزارات مثل وزارة التجارة أو الصحة أو غيرها من الوزارات، حيث أثبت من خلال التجربة العملية فعاليته، حيث أن النظام متفق ومنسجم مع النصوص القانونية المتعلقة بحماية البيانات الشخصية، حيث يقوم في مبدأه على تحديد الضوابط المتعلقة بحماية هذه البيانات، وتحديد الهوية الشخصية والبيانات الشخصية وحمايتها لعملاء الوزارة التي تستخدم هذا النظام، ويقوم النظام على حفظ سرية البيانات الشخصية التي يقدمها المواطن للوزارة، وهذا النظام لا يقوم بجمع البيانات شخصية عن أي مواطن إلا اذا رغب بنفسه بتقديمها للوزارة، ويطلع المواطن على شروط هذا النظام قبل تقديم أي بيانات عن شخصه، ويحفظ هذا النظام البيانات الشخصية، ويكفل جميع الوسائل التي يمكن من خلالها زيادة الأمان على البيانات الشخصية، ومن ضمن مهام هذا النظام اتخاذ التدابير والإجراءات المناسبة لحماية البيانات الشخصية، ويعمل هذا النظام على استخدام الوسائل المستحدثة والمتطورة لحفظ وحماية البيانات الشخصية، وتدريب الموظفين على هذا النظام لحفظ البيانات الشخصية للأفراد، ويتمثل عمل هذا النظام ب :1 يكون لكل مستخدم اسم وكلمة مرور ويتم حفظ الip الخاص بالمستخدم وتاريخ ووقت الزيارة والعنوان (موقع وزارة التجارة _السعودية) .

27. وعند زيارة الموقع يحفظ ملف صغير على القرص الصلب الخاص بجهاز الزائر، وهذا الملف يحتوي على معلومات نصية تتيح للموقع الذي حفظت عليه أن يسترجعها عندما يحتاجها ومع الملاحظة أنه عند استخدام هذا النظام من قبل الوزارات، تكون حفظ بياناته الشخصية وتقديم أفضل الخدمات الحكومية للمواطن هي الغاية الأساسية لنظام، ويمكن أن يتم تبادل البيانات الشخصية للمواطن ما بين الوزارات عن طريق هذا النظام لتسهيل مبدأ عمل الوزارات، وليس مع أي جهات اخرى غير حكومية مع العلم أنه في حال تبادل البيانات يكون ذلك بعد موافقة الشخص (موقع وزارة التجارة _السعودية).

ومن ضمن مميزات هذا النظام:

1) أنه ينظم البيانات الشخصية للمواطن ويضمن عدم تعارضها مع بيانات أخرى للمواطنين.
2) جمع البيانات يكون لهدف واضح وصريح، وهو الهدف الذي أستخدم النظام بالأساس من أجله، وهو تحقيق المصلحة العامة دون الحاق أي ضرر سواء مادي أو معنوي بمصالح الوزارات أو مصالح الأفراد وخصوصياتهم.
3) وبما أن النظام يحفظ البيانات الشخصية للمواطن، فأنه بذلك يسهل عمل الموظفين العامين بالوزارات عند حاجتهم الوصول إلى البيانات الشخصية للمواطن، وبالتالي طريقة أسهل وأسرع في تقديم الخدمات.
4) يهتم النظام بحفظ البيانات الشخصية للمواطنين، ويسعى كذلك لتطوير نفسه باتباع ما انتجته التكنولوجيا من وسائل حديثة يمكن استخدامها لأغراض حماية البيانات الشخصية، وأيضاً يتولى النظام بالقيام بالتخلص من البيانات الشخصية وفق آلية معينة.
5) يؤخذ بعين الاعتبار في استخدام النظام القانون الساري بالدولة المتعلق بحماية البيانات الشخصية والاتفاقيات الموقعة عليه الدولة.

6) عند مشاركة البيانات الشخصية مع أي جهات أخرى يتم مراعاة المبادئ الأخلاقية العامة ضمن إطار العدالة والأمانة في حفظ البيانات الشخصية وحمايتها من أي اعتداء (موقع وزارة التجارة _السعودية).

وقد وجدت الباحثة بعد الاطلاع على مختلف الأنظمة التي أنتجتها التكنولوجيا العديد من النتائج أهمها:

1) أن هذه الأنظمة تختلف من دول لأخرى، فالأنظمة الموجودة في دول الاتحاد الاوروبي وأمريكا وغيرها تختلف عن الأنظمة الموجودة في دول الخليج مثلاً، وهذا يعتمد بشكل أساسي على مدى تطور الدولة تكنولوجياً مع العلم أنه كثير من الدول المتطورة تستخدم هذه الأنظمة؛ لحماية الشخصيات العسكرية الكبرى لديها وأغلب هذه الدول تخفي هذه الأنظمة عن الدول الأخرى، وعادة ما يتم بيع هذه الأنظمة بعد استهلاكها، وايجاد أنظمة أكثر حماية فيتم بيع القديم منها.
2) عند قيام الدول بشراء نظام معين لحماية البيانات الشخصية لمواطنيها، لابد من أن تراعي عدة مواضيع منها القوانين والتشريعات السارية داخل الدولة، وبالإضافة إلى المعاهدات والاتفاقات الموقعة عليها الدولة؛ حتى لا نكون بثغرة انتهاك النظام لأمور احترمتها الدولة ضمن اتفاقية دولية، أو نصوص تشريعية سارية فيها، وبالتالي لابد من أن يكون هناك انسجام بين النظام والنصوص القانونية المتعلقة بحماية البيانات الشخصية.
3) وقد ذكرت الباحثة ما تقوم به الدول بخصوص انظمة حماية البيانات الشخصية وكيف يتم اخفاؤها عن الغير، وبالتالي ترى الباحثة أن لتجاوز هذه النقطة وإيجاد حل هو أن تقوم الدولة نفسها عن طريق تنمية مواردها البشرية بإنتاج أنظمة حماية تناسب الدولة، وهنا نكون قد حصلنا على فائدتنا الأولى :هي التخلص من التبعية للدول الأخرى بخوص شراء الأنظمة منها والثانية: هي ضمان أكثر حماية للبيانات الشخصية؛ كونه لا يوجد ضمان أن يكون هناك تجسس عن طريق النظام الذي تم بيعه، والفائدة الثالثة هي :تشغيل الأيدي العاملة في الدول وتعزيز وزرع الثقة لدى الأيدي العاملة بأنه

يمكن أن يتم بناء الدولة بالأيدي العاملة الوطنية، وضمان عدم هجرة العقول الذكية إلى دول أخرى واستغلالهم هناك .

4) عندما تقوم الدولة بتبني نظام معين داخل وزاراتها لابد من وضع أشخاص لديهم الخبرة الكافية بالتعامل مع هذه الأنظمة، ولا مانع من قيام الدولة بإرسال الموظفين لأخذ دورات خارج البلاد للاستفادة من خبرات الدول المتقدمة.

المبحث الثاني: جرائم الاعتداء على البيانات الشخصية خارج إقليم الدولة

جرائم البيانات الشخصية يمكن أن يتم ارتكابها داخل الدول، أما بين المواطنين أنفسهم ، ويمكن أن يتم الاعتداء على هذه البيانات من قبل الشراكات التي توفر خدمات التواصل، بحيث يتم استغلال البيانات الشخصية لأغراض تجارية دون الموافقة الصريحة من أصحابها، وفي الطرف الأخر يمكن أن يتم الاعتداء على البيانات الشخصية من قبل جهات خارج الدول؛ لأغراض سياسية مثل التجسس، سرقة بيانات شخصية لأشخاص ذوي اعتبار بالدولة وفضحها ونشرها على مواقع التواصل الاجتماعي، وقد حدثت مرارًا وتكراراً، حيث تم سرقة بيانات شخصية خاصة برئيس وحدات عسكرية ونشرها بهدف إظهار ضعف الدولة وقدرتها على حماية بياناتها (مطر، 2016)، وقد يتم الاعتداء على البيانات الشخصية الخاصة بالأطفال دولياً عن طريق استغلال موضوع البيانات الشخصية، بحيث يكون ذلك من خلال منظمات ارهابية استغلت موضوع البيانات الشخصية في ارتكاب جرائمها، وسهلت عملية التسلل لهؤلاء الأطفال (موقع الانتربول، 2021)، وقد يتم الاعتداء على البيانات الشخصية خارج الدولة عن طريق قيام الشركات الكبرى العالمية ببيع البيانات الشخصية لشركات اخرى، دون الحصول على الموافقة من أصحابها، وقد حصل هذا بشركة فيسبوك حيث أتهم صاحبها ببيع بيانات الأفراد لشركة أخرى واستغلال هذه البيانات مادية، وجرت محاكمته، وحكم بعد ذلك بدفع غرامة سوف تتطرق الباحثة لهذه القضية خلال الدراسة، وسوف تتطرق الباحثة أيضاً خلال الدراسة لموضوع الاتفاقيات والمعاهدات الدولية التي اهتمت بموضوع حماية البيانات الشخصية الاعتداء (فيسبوك تخسر 119 مليار دولار في يوم واحد، 2019).

وسوف تتحدث الباحثة في هذا المبحث عن جرائم الاعتداء على البيانات الشخصية خارج اقليم الدولة من حيث طبيعتها على الصعيد الدولي وكيفية ارتكابها وملاحقتها في المطلب الأول، ومن ثم السند القانوني والاتفاقات الدولية التي يمكن من خلالها تجريم الاعتداء على البيانات الشخصية، وفي الفرع الأول تحدثت الباحثة عن الاتفاقية الأوروبية المتعلقة بحقوق الانسان(روما) نوفمبر 1950 وفي الفرع الثاني اختتمت الباحثة بالنظام الاوربي لحماية البيانات الشخصية.

المطلب الأول: طرق ارتكاب جرائم الاعتداء على البيانات الشخصية على الصعيد الدولي

قد ابدع المجرمون في ارتكاب اعتداءات علي البيانات الشخصية، وبخاصة أن هناك كثير من الدول لا يوجد لديها نصوص تشريعية تغطي جرائم الاعتداء على البيانات الشخصية، فقد مارسوا أسواء أنواع الاعتداء وخاصة أنه أصبح الاعتداء ليس فقط داخل حدود الدول بل امتد عبر القارات، حيث لجأ البعض لاستغلال ضعف اللاجئين السورين حيث لجأ الكثير من الأشخاص لسرقة البيانات الشخصية للاجئين عن طريق نسبة لهم جرائم لم يرتكبونها من خلال استغلال بياناتهم الشخصية مثل أرقام هواتف، جوازات سفر، بحيث قاموا بفتح خطوط وارتكاب جرائم، وتلقائياً يكون اللاجئ هو المتهم الأول، حيث وجُهت الكثير من التهم لأصحاب هؤلاء البيانات مثل النصب، والاحتيال من خلال استغلال بياناتهم الشخصية، وطُلبوا للقضاء (سرقة البيانات الشخصية ....سوريون ضحايا انتهاك الخصوصية في تركيا 2021/2/7 ، 2021).

ولجرائم الاعتداء على البيانات الشخصية طبيعة خاصة تختلف عن الجرائم التقليدية سواء من خلال أدواتها، حيث في الوقت الحالي الوسائل التكنولوجية هي الوسيلة الأكثر استعمالاً للجناة لارتكاب مثل هذه الجرائم مع العلم أنه يمكن ارتكابها بوسائل تقليدية مثل إتلاف بيانات شخصية مسجلة لدى أرشيف شركة أو وزارة، ولكن بطريقة تقليدية أي على الورق وليس ع جهاز أو نظام معين، ولا يقف الأمر عند اختلاف جرائم البيانات الشخصية داخل الدولة فقط، كذلك طبيعتها تختلف عن جرائم البيانات الشخصية التي

ترتكب دولياً مثل استغلال البيانات الشخصية للاجئين أو استغلال البيانات الشخصية لسرقة الأعضاء للاجئين، كذلك المنظمات الإرهابية التي تستغل سرقة البيانات الشخصية للأطفال أو أي فئة مهمشة أو ضعيفة؛ لارتكاب جرائم واستغلالهم مادياً وسوف تتطرق الباحثة لهذه الأمور خلال الدراسة (خضر، 2021).

ولأن كل ما أنتجته التكنولوجيا الحديثة كان له إيجابيات وسلبيات مع الأسف استغل الجناة الإنترنت لارتكاب جرائم الاعتداء على البيانات الشخصية حتى على الصعيد الدولي، وما يميزها صعوبة الاكتشاف وتحصيل أدلة للإدانة وخصوصاً بهذه الحال، حيث يكون الجاني من دولة أخرى، وبالتالي مشكلة امتثاله أمام القضاء، وثانياً قدرة الجاني على تدمير أدلته وخاصة أنه خارج حدود دولته، وبالتالي أصبح الموضوع أكثر سهولة، وثالثاً محو الآثار المادية بعد ارتكاب الجريمة، حيث يتم استخدام النبضات الإلكترونية الغير مرئية لتسلل والاعتداء على البيانات الشخصية بطريقة أو بأخرى، وكذلك برامج وفيروسات تخترق الأنظمة ومن ثم يقع الاعتداء على البيانات الشخصية وتتلف جميع آثار هذا الفايروس، وبالتالي هذه مشكلة أمام القضاء من حيث الإثبات وخاص أن الجاني ليس من داخل الدولة، وما يميز جرائم الاعتداء على البيانات الشخصية اذا ما تم ارتكابها من طرف خارج الدولة أن النشاط الجرمي غير مرئي، فقد يدخل الجاني وينفذ عمليته ويخفي الآثار ومن ثم بعد فترة من الزمن يمكن أن يتم اكتشاف سرقة هذه البيانات أو الاعتداء عليها، ولكن بعد فترة قد يكتشف صاحبها هذا الاعتداء أو لا، وخامساً مع الأسف الشديد أن طبيعة ارتكاب جرائم الاعتداء على البيانات الشخصية دولياً تحتاج إلى كادر تقتني يتم تدريبه تدريب دولي لمواكبة ما انتجته كل دولة من أنظمة لحماية البيانات الشخصية لمواطنيها وهذا يحتاج ميزانية مادية من الدولة، وسادساً من الأمور التي تختلف فيها طبيعة الاعتداء على البيانات الشخصية دولياً أنه في حال وقع الاعتداء فعلياً على أحد مسؤولي الدولة أو أحد المؤسسات الكبرى فيها فأنه يمس اعتبارها وهيبتها وكينونتها أمام الدول الأخرى، وبالتالي مع الاسف بالعادة يتم اخفاء هذه الجرائم؛ كي لا تؤثر على مكانة الدولة ومحل اعتبارها بخصوص سيطرتها أو سيادتها فتلجأ الكثير من الدول لا خفائها إلا اذا تم نشر

ارتكاب هذه الجرائم من قبل الدولة المعتدية؛ لفضح ضعف الدولة التي تم الاعتداء عليها والسيطرة عليها، وبالتالي هذه الجرائم في حال تم ارتكابها على مستوى دولي ليس بموضوع سهل على الدولة نفسها من حيث الملاحقة أو جمع الأدلة أو القبض على الجناة (عيشة).

في هذا المطلب سوف تتحدث الباحثة عن ارتكاب جرائم الاعتداء على البيانات الشخصية من الناحية الدولية، وجدت الباحثة أن ارتكاب مثل هذه الجرائم على مستوى دولي يتم بطريقتين الأولى بشكل تقليدي والثاني عن طريق الوسائل التكنولوجية، سوف تبدأ الباحثة بالطريقة الأولى:

الطريقة الأولى: الوسائل التقليدية لارتكاب جرائم الاعتداء على البيانات الشخصية على مستوى دولي

ومن الجرائم التي تعتمد بشكل كبير على البيانات الشخصية هي جريمة الإتجار بالأعضاء (تجارة الأعضاء: هي تجارة بالأعضاء البشرية أو الانسجة أو أجزاء أخرى من الجسم بقصد زرع أعضاء لأشخاص أخرين)، وغالباً ما يتم مع الأسف استغلال الجهات الضعيفة بالمجتمع مثل اللاجئين الذين يلجؤون إلى بيع أعضاؤهم؛ بهدف الحصول على لقمة العيش وكذلك المهاجرين الذين هاجروا بطريقة غير شرعية ولجأوا إلى دول أجنبية بهدف الحصول على مستوى معيشة أفضل من الدولة التي كانوا فيها؛ ولعدم حصولهم على تصريح هجرة شرعية؛ لجأ الكثير إلى استخدام الهجرة الغير شرعية ومع الأسف يتم استغلالهم نتيجة ضعفهم، بحيث يتم تهديدهم بالإخبار عنهم السلطات لترحيلهم إلى بلادهم الأصلية، وبالتالي هم جهات مستضعفة بالمجتمع ويلجأ سماسرة الإتجار بالأعضاء إلى استغلالهم، ولكي ينفذوا جرائمهم فأن هذه الجريمة تعتمد بشكل أساسي على استغلال البيانات الشخصية من حيث عمر الشخص ومكان سكنه وهل لديه أمراض جسدية أم لا، و نوع الدم وهل لديه مرض وراثي؟، وهل يعاني من السمنة؟، وبالإضافة إلى وزن هذا الشخص وطوله، وبالتالي هذه البيانات الشخصية مهمة لإتمام الجريمة؛ وذلك لتسهيل عملية بيع العضو لأشخاص آخرين بعد مطابقة بياناتهم الشخصية مع البيانات الشخصية للمجني عليه، وهذه الجريمة لا يمكن الاستهتار بها، حيث أن الولايات المتحدة الأمريكية يوجد

بها حوالي 90000 شخص ينتظرون أعضاء تزرع لهم وينتظر المريض الذي يحتاج زراعة العضو في المتوسط ٣سنوات ونصف للحصول على عضو صالح لزراعته ولا يقتصر الوضع على أمريكا فقط، ففي ألمانيا هناك ثلاث أشخاص يومياً يتوفون وهم ينتظرون أعضاء لزراعتها و أوروبا يوجد بها 40000 مريض ينتظرون زراعة كلى، وكذلك هناك أشخاص ينتظرون أعضاء بشرية لاستخدامها بالسحر ومع الأسف؛ كون هذه الفئات ضعيفة قد يتم استغلال فقرها وحاجتها الماسة للمال وقد ورد في تقرير أن 18000 ألف سوري قاموا ببيع كلاهم، و في تقرير أخر أنه في احدى المرات أن الصين تعاملت مع سجين محكوم بالإعدام بأخذ أعضاؤه وبيعها، ومن الوسائل التي يتم فيها استغلال البيانات الشخصية في الدولة للتجار بالأعضاء هو قيام الشخص بالتوجه لعلاج معين في المستشفيات ويقدم بياناته الشخصية لإجراء عمليات أو فحوصات معينة، ومن ثم مع الأسف يتم سرقة أعضائه ولكن يكتشف الأمر بعد فترة من الزمن عن طريق قيامه بفحص أخر أو تعرضه لحادث فيكتشف الأمر ولكن بوقت متأخر، كذلك المنظمات الإرهابية مثل داعش لجأت إلى استخدام البيانات الشخصية للمصابين الذين يقعوا تحت قبضتهم وسرقة أعضاؤهم، وبالتالي هذا مصدر تمويل للمنظمة، وقد أشارت الدراسات أن تجارة الأعضاء سوف تزيد مع الوقت لعدة أسباب أهمها؛ هو زيادة عمر المريض نتيجة التقدم الطبي وبالتالي هؤلاء المرضى قد يحتاجون أعضاء بشرية، ولكن ممكن للعلم أن يقلب الموازين عن طريق تطوير زراعة الأعضاء التي تقوم على أن المريض نفسه يمكن أن يتم أخذ خزعة منه لزراعة عضو له، وبالتالي حل مشكلة الاتجار بالأعضاء البشرية (حقيقة سرقة الأعضاء ماذا تعني ، 2020).

ومن الطرق التقليدية لجمع البيانات الشخصية وهذه الطريقة موجدة منذ القدم حيث تلجأ فيها الدول لجمع بيانات مواطنيها بموجب قوانين تقوم بسنها؛ بغرض تنظيم أمور إدارية بالدولة وبموجب هذه القوانين تحصل الدول على كم هائل من البيانات الشخصية مثل الدخل لكل مواطن، الإقامة، عدد أفراد الأسرة، الأملاك، الحالة الاجتماعية و استهلاك الكهرباء والمياه وتستفيد الدولة من هذه البيانات استفادة كبرى، حيث تساعد على تنظيمها وتساعدها في عملية جني الضرائب، ويكمن الخطر باستغلال هذه البيانات و

الاعتداء عليها سواء من الحكومة نفسها أو اختراقها من طرف ثاني سواء من داخل الدولة أو خارجها؛ وذلك تنفيذاً لجرائم أو سرقات أو عمليات نهب لخزينة الحكومة، وبالتالي على الحكومة عدم السكوت عن هذا الموضوع واتخاذ كافة الوسائل والتدابير اللازمة لحماية البيانات الشخصية، ولا بد من قيام الدولة بالاطلاع على أحدث الوسائل الحديثة؛ لحماية البيانات الشخصية لمواطنيها حتى لا تقع بمشاكل مع المواطنين نتيجة عدم اتخاذ الإجراءات اللازمة لحماية البيانات الشخصية (اشتية و اياس خطيب، واقع الخصوصية وحماية البيانات الرقمية في فلسطين، 2021).

وفي بداية جرائم الاعتداء على البيانات الشخصية كانت البداية عن طريق وسائل بسيطة منها تتمثل بالدخول إلى نظام الحاسب الألي، ومن ثم ايقاع الاعتداء على هذه البيانات من سرقتها أو تدميرها أو إتلافها أو خربشتها أو حذفها، وبالتالي بطريقة تقليدية دون استخدام وسائل حديثة متل برامج فيروسات أو غيرها (ميلاد، الجرائم الالكترونية ، 2022).

ومن الوسائل التقليدية أيضاً وتمثل اعتداء على البيانات الشخصية هي الاستيلاء على حقوق المؤلف، بحيث يتم سرقة ما كتبه المؤلف الأصلي دون إذن من صاحبها أو بطباعتها أو تسويقها أو استغلالها بأي صورة دون الالتفات إلى موضوع الملكية الفكرية (ميلاد، الجرائم الالكترونية).

أما عن استغلال البيانات الشخصية لارتكاب جرائم الاعتداء على هذه البيانات دولياً عن طريق وسائل تكنولوجيا حديثة وليست تقليدية، فقد تم استغلال ما انتجته التكنولوجيا لسرقة البيانات الشخصية واستغلالها مادياً، حيث أن هذه الأجهزة سواء الهاتف أو السيارة أو جهاز التلفاز وأجهزة قياس الطاقة وشاشات الأطفال تخزن كم كبير عن بياناتنا الشخصية دون موافقتنا المسبقة ويتم استغلالها لأغراض تخدم المصلحة الشخصية لشركات أو لأفراد معينة أو قد يتم استغلال هذه البيانات سياسياً من قبل دول أخرى ومن الأمثلة على ذلك استغلال السيارات الشخصية للمواطن لسرقة البيانات الشخصية وارسالها لشركة

تأمين مثل السرعة أو اذا كان السائق استخدم المرآة أو لا أو مشغول أو هادئ وبالتالي تستفيد شركات التأمين من هذه البيانات في التهرب من مسؤوليتها تجاه المؤمن.

ومن الوسائل التكنولوجية الحديثة التي تخزن بيانات شخصية عن المستخدم أيضاً هي الثلاجة عن طريق إخبار صاحب العمل مثلاً عن كمية المشروبات التي يتم شربها أسبوعياً، ولم يقتصر الموضوع إلى هذا الحد بل امتد إلى الشركات الكبرى بتوجيهات سياسية من الدول نفسها لسرقة بيانات شخصية تتعلق بالآراء السياسة أو مستوى الدخل وغيرها من البيانات عن الأفراد، وقد يظن الشخص أن هذه البيانات لن يأتي منها فائدة إلا أن القيام بجمع هذه البيانات لتكوين صورة واضحة عن الشخص يمكن بعدها استغلالها بصورة أفضل حيث تعمل على تكوين ما يسمى شبيه رقمي يخزن بيانات شخصية كاملة عن الفرد ومن الوسائل التي يمكن استخدامها، لأغراض جمع البيانات الشخصية هي متاجر التسوق، بحيث يمكن لشركات عمل تسويق بناءً على البيانات الشخصية التي تم جمعها من خلال تسويق لشخص ما يطلبه ويمكن بناءً على ذلك قيام الشرطة بتفقد اذا ما كانت مشترياتك عليها اشارة استفهام أم لا، كذلك ممكن للبنوك رفض منحك قرض؛ لان الشبيه الرقمي يوحي بعدم السداد.

وتكمن هناك مشكلة اخرى بموضوع أن تكون البيانات الشخصية التي جمعت وخزنت في الشبيه الرقمي، هي خاطئة وفي جميع الحالات هذا استغلال واضح للبيانات الشخصية، ولابد من سن قانون يوقف هذا الانتهاك؛ وذلك لتوفير الحماية للبيانات الشخصية وأن يكون للشخص قدرة على السيطرة على بياناته.

ومن الوسائل الحديثة التي يستخدمها الجناة لتنفيذ اعتداء على البيانات الشخصية هي شبكة الانترنت، حيث تساهم بشكل كبير في مساعدة الجناة بالاعتداء على البيانات الشخصية، حيث يتم الدخول لشبكة الدولية ومن ثم سرقة البيانات الشخصية الموجودة فيها أو تعطيلها أو تدميرها وبعدها يخرج الجناة دون ترك دليل ورائهم، ويمكن أن يتم بيع هذه البيانات لجهات أخرى بعد الاستيلاء عليها ويستخدم الإنترنت أيضاً في استغلال البيانات الشخصية للأفراد مادياً وذلك بعد معرفة مستواهم المالي، وبالتالي العمل على

اختراق حساباتهم الموجودة بالبنوك ومن الأمثل الأكثر شهرة استخدام الهاكر وسرقة الأموال الموجودة في البنك وتحويلها إلى حسابات أخرى ومن المواقع الاجتماعية التي يستخدمها الجناة لتحصيل أكبر قدر ممكن من البيانات الشخصية، هو موقع توتر حيث يوجد فيها مئات من المشتركين المسجلين بياناتهم الشخصية، وكذلك الملاين من الأفراد غير المشتركين يدخلون بشكل يومي على هذا الموقع تاركين ورائهم بياناتهم الشخصية (مهدي، 2020).

ومن الوسائل التي انتجتها التكنولوجيا والمستخدمة حالياً بكثرة في جمع وتحليل البيانات الشخصية، هي ملفات تعريف الارتباط (الكوكيز)(cookies)، وتقوم هذه التقنية بعملها عن طريق جمع بيانات بشكل كبير عن مستخدمي الانترنت مثل نوع الجهاز المستخدم، رقم ip الخاص بالمستخدم، المواقع التي زارها، الهوايات، اماكن التسوق، الأماكن الجغرافية التي يتردد عليها، ومشترياته، ومستوى دخله، رقم الهاتف، أو بطاقة الاتمان والكثير من البيانات الشخصية التي يمكن جمعها، والكثير من المستخدمين لشبكات الانترنت لا يعلموا بأنه يتم جمع بياناتهم الشخصية بهذه الطريقة، وليس لديهم الموافقة على ذلك وبالتالي لا يتم جمع هذه البيانات من غير سبب، وانما يجرى استخدامها والاستفادة منها تجارياً من قبل الشركات الكبرى، حيث من أوجه استغلال هذه البيانات هي بث اعلانات وفق هذه البيانات وبالتالي استغلال تجاري دون موافقة صاحب الشأن (اشتية و الخطيب ، واقع الخصوصية وحماية البيانات الرقمية في فلسطين، 2021).

ومن الوسائل أيضاً التي تساهم بجمع البيانات الشخصية بشكل سريع هو استخدام الهواتف المحمولة الذكية، حيث يمكن للشركات الكبرى التجارية بث إعلاناتها على مواقع جغرافية حصلت عليها عن طريق قيام الاشخاص بمشاركة هذه البيانات على مواقع التواصل الاجتماعي وفق الجمهور المستهدف واحتياجاته مثلا الأطفال يتم بث لهم إعلانات لهم تختلف عن كبار السن يكون بحيث يكون الإعلان فيها يتناسب مع احتياجات الفئة العمرية ولم يتوقف الأمر عند الإعلانات التجارية فقط، فقد امتد الأمر إلى استخدام برامج

الهاكر لسرقة البيانات الشخصية؛ تمهيداً لجرائم الاحتيال والنصب، حيث بعد جمع البيانات الشخصية المتعلقة بأرصدة الأشخاص بالبنوك ومستواهم الاقتصادي بعدها تأتي مرحلة بث اعلان للاحتيال على الفرد وسرقة ما لديه من أموال أو تهديده بنشر بياناته الشخصية حيث يتم استخدام برامج الهاكر في الحصول على العديد من البيانات الشخصية ومن ثم التهديد بنشرها أو بيعها حتى لو كان الجاني بدولة والمجني عليه بدولة أخرى، فيمكن أن يطلب منه تحويلها لدولة الموجد فيها الجاني ومن الأمور المستجدة على الساحة الدولية بخصوص البيانات الشخصية، هو لجوء الشركات الدولية الكبرى لبيع هذه البيانات الشخصية للمستخدمين لشركات أخرى بمبالغ كبيرة ودون موافقة أصحاب هذه البيانات؛ لكي تقوم الشركة التي اشترت هذه البيانات بالاستفادة منها تجارياً أو لأغراض أخرى (الخطيب، 2021).

ومن القضايا المشهورة والتي عملت ضجة كبيرة في الآونة الأخيرة، هي قضية بيع وتسريب البيانات الشخصية المخزنة لدى شركة فيس بوك، وقد جرت محاكمة صاحب شركة فيس بوك في الكونجرس مع العلم أنه في بداية إجراءات المحاكمة قد دافع عن الموظفين العاملين بالشركة بحجة أنه ليس لديه علم بتورط الموظفين بالتسريب، وكانت إجراءات القضية كالتالي حيث جرى تسريب بيانات شخصية لأكثر من 78 مليون مستخدم وكان التسريب لشركة استشارات سياسية مقرها في الولايات المتحدة الأمريكيين (كامبرج أنالتيكا)، وكانت هذه الشركة قد قدمت مساعدة لدونالد ترامب خلال دعايته الانتخابية التي جرت في 2016، وخلال الجلسات فشل مارك مؤسس شركة فيس بوك بتخليص نفسه من هذه القضية، حيث كان يتهرب من الأسئلة الموجه له خلال إجراءات المحاكمة فمرة يقول بأنه ليس لديه معلومات حول تورط الموظفين بهذا الأمر، ومرى أخرى ينفي هذا الموضوع، وقد كان موقف مارك مؤسس فيس بوك حرجاً، حيث جاءت قضية تسريب البيانات الشخصية بوقت صعب، حيث ظهرت شائعة في الآونة الأخيرة تقضي بتدخل الروس بالانتخابات الرئاسية للولايات الامريكية، وكان هناك شائعة تتعلق بتجسس شركة فيس بوك على المكالمات الهاتفية ورسائل المستخدمين لديهم، وأثناء جلسات المحاكمة وجهت لمارك العديد من الأسئلة أهمها كيف كانت طبيعة تعامل الموظفين مع الشركة المسؤولة عن تسريب بيانات 87

مليون مستخدم لصالح الحملة الانتخابية لدونالد ترامب، وقد أجاب مارك أنه لا يعلم إذا ما كان موظفو الشركة متورطين أم لا، ولكن اعترف بأنه قد قدم المساعدة لحملة الانتخابات الرئاسية لدونالد ترامب مع تصريحه بأن المساعدة كانت مثل الطرق الأخرى التي تساعد بها الحملات الانتخابية، وتم سؤاله إذا ما كانت شركة فيس بوك سوف تدعم قانون يجبر على إعلام المستخدمون في غضون 72 ساعة في حال اختراق بياناتهم، وصرح مارك بموجب هذا السؤال أنه لا مانع لديه وقد وجه لديه سؤال أخر حول فشل فيس بوك في مواجهة ما حدث في ميانمار، حيث يوجد فيها تحريض ضد المسلمين حيث تم نشر الكثير من المنشورات التي تدعو لقتل صحفي مسلم، ولكن كان رد مارك ذكياً حيث أجاب أن ما يحدث في ميانمار هي مأساة كبرى ونحتاج إلى بذل الكثير من الجهد لوقف هذه الاعتداءات، وأضاف أنه يوظف العشرات من مراجعين محتوى اللغة البورمية كان عملهم مخصص بإزالة الحسابات التي تدعو للكراهية، وخلال جلسات المحاكمة وضح الكونجرس فيها أنه لابد من الالتزام بمعنى الخصوصية وخاصة في ظل النشاط الروسي على شبكة فيس بوك، ولابد من قيام شركة فيس بوك بتطوير طرق وأساليب لتعزيز معايير الخصوصية، وقد قدم الرئيس التنفيذي لشركة فيس بوك اعتذاره بخصوص تسريب بيانات المستخدمين، وبالمقابل حاول مارك توضيح دور الذي لعبه فيس بوك حيث كشف عن الدور في الأحداث والكوارث التي واجهت العالم في الفترات الأخيرة، وقد صرح مارك باعتراف له خلال جلسات المحاكمة، حيث اعتذر عن التقصير الذي حدث بخصوص تسريبات البيانات الشخصية، وكذلك تقصيره في الحد من منشورات الكراهية ونشر الأخبار الزائفة والتدخل الأجنبي بالانتخابات، وقال أنه مسؤول عما حدث واعتذر عن ذلك وقد أضاف أنهم في شركة فيس بوك قد درسوا خطوات جديدة؛ لعدم تكرار الفعل هذا مرة أخرى، وقد أخطرت الشركة المستخدمين المتضررين وأوضح أن الشركة سوف تعمل خطوات جديدة لوقف وعدم تكرار هذا الفعل وخلال إجراء المحاكمة كان هناك مجموعة من الشبان يحملون يافطات تطالب بحماية الخصوصية، وكان مارك قد قدم اعتذارات ليس فقط أمام الكونجرس بل نشره عبر حسابه الرسمي على فيس بوك، وخلال مقابلات تلفزيونية وصحفية حيث نشرها في صحف ورقية مهمة في أمريكا و بريطانيا،

وكانت خسائر فيس بوك كالتالي ما يزيد عن 60 مليار (10 مليار خسارة شخصية و50 مليار دولار تراجع في القيمة التسويقية للموقع، وجاءت هذه الخسارة بعد خروج شاب كندي عن صمته، وكشف أن خطأ ما تسبب بتسريب بيانات 50 مليون مستخدم ومع العلم أنه تم استغلالها خلال الفترة الانتخابية، وهذا الشاب يعمل في شركة كامبريدج انتالتيك، وهي شركة تحليل بيانات بريطانية تستغل البيانات عن طريق معرفة ميول الأفراد واهتماماتهم وعمل عملية تسويق؛ لإعلانات ودعاية وفق ميول الأفراد واهتماماتهم وتقوم بمهمة الوسيط بين المستهلك والمعلن ومع العلم أن الشركة توظف الكثير من خبراء علم النفس وخبراء التسويق الرقمي لتحقيق أكبر قدر ممكن من الأرباح (حواس، 2018).

وقد وافقت الشركة على دفع أكبر غرامة مالية قدرت ب خمسة مليار دولار؛ لتسوية قضية انتهاك خصوصية المستخدمين واتسع التحقيق ليشمل قضايا أخرى مثل خاصية التعرف على وجه المستخدم وبالتالي تحديد هويته من خلال التعرف على وجهه (موقع عرب نيوس).

ومن طرق جمع البيانات الشخصية التقليدية في أصلها، ولكنها أثبت قدرتها على جمع البيانات الشخصية رغم ايجاد طرق لحماية البيانات الشخصية للأفراد الا أنها أثبت أنها من أفضل والوسائل التي تحدت التكنولوجيا، هي قرصنة البيانات الشخصية وهذا ما أشار له الاستاذ ليفي من خلال مؤلفاته في عالم القرصنة، وقد وضح أن عمل القراصنة يقوم على أساسين الأول أن الدخول إلى أنظمة الحاسب الآلي يفتح الأفق للفرد حول استكشاف العالم، والمبدأ الثاني يقوم على أن يتم جمع المعلومات دون أي قيود أو شروط على الاختراق، يكون دون أي موانع بحيث يكون هناك فريق وبعد أن يتم جمع البيانات يتم تقسيمها بينهم، وبعدها يتم الاحتفال بقهر النظام والتفوق عليه وتحقيق مكاسب مادية واقتصادية، واثبات السيطرة على ما أنتجته التكنولوجيا وإلحاق ضرر بجهات معينة (ميلاد، الجرائم الالكترونية– جامعة المرقب، 2022).

أما الطريقة الثانية عن طريق الوسائل الحديثة:

ومن الوسائل الحديثة التي تهدف إلى استغلال البيانات الشخصية، هي استغلال التجُار للبيانات الاسمية والعناوين الالكترونية عبر الإنترنت؛ وذلك لتوجيه الدعايات التجارية بناءً على ما تم جمعه من ميول ورغبات المستهلكين، بحيث يتم الحصول على البيانات الشخصية عن طريق تتبع رغبات المستخدمين، ومن الوسائل التي تساعد في توفير بيانات شخصية كبيرة هي استخدام برتوكولات الاتصالات، حيث من خلال هذا التطبيق يتم ضخ الكثير من البيانات الشخصية المتنقلة عبر أجهزة الحاسوب، وكذلك عنوان ال الاي بي يساعد بتوفير بيانات عن عنوان المستخدم، ومن الأنظمة الحديثة أيضاً ما يسمى بالكعك المحلي co حيث يتم ارسالها لمواقع تجارية، وبعدها وبموجب هذه البيانات يتم تحديد شكل الميول الاستهلاكي ومن ثم ارسال kiss، حيث يعمل هذا البرنامج على جمع معلومات خاصة عن المتعاملين، وبعد جمع هذه البيانات يتم الدعاية وفق ميول المستخدم وهذه الإعلانات لا تؤثر فقط من ناحية تحقيق ازعاج للمستخدمين، بل يتمدد الأمر إعاقة شبكة الاتصالات أحياناً، وبالتالي لابد من توفير آليات لوقف مثل هذه الاعتداءات على البيانات الشخصية وخاصة في ظل ظهور شركات كبرى تختص في عملها في الإتجار بالبيانات الشخصية (أعزان).

المطلب الثاني : كيفية ملاحقة مرتكبو جرائم الاعتداء على البيانات الشخصية دولياَ.

تعتبر جرائم الاعتداء على البيانات الشخصية من ناحية دولية جرائم تختلف في طبيعتها عن الجرائم التقليدية، وتختلف أيضاً في حال تم ارتكابها داخل الدولة نفسها، فكون الجريمة دولية هنا تختلف في عدة أوجه منها أنها عابرة للقارات وليست محصورة بنطاق جغرافي معين، والانترنت جعلها أسهل للوصول والتواصل، وبالتالي امتدت هذه الجرائم عبر القارات وبالعادة يكون الجاني في دولة والمجني عليه في دولة أخرى، وقد يقع ضرر يتوزع على أكثر من شخص في دول معينة مثل تسريب بيانات بشكل عشوائي لمستخدمي فيس بوك، بالتالي الأشخاص المتضررين هنا من دول متعددة وعندما نكون أمام جريمة دولية عابرة للقارات نضع صوب أعيننا أننا نكون أمام اختلاف بالثقافات، وبالإضافة للنصوص القانونية وقد

تكون دولة الجاني أو المجني عليه موقعة على اتفاقية بالمقابل الدولة الأخرى غير موقعة وخاصة أنها جرائم ناعمة لا تتطلب عنف أو أدوات مثل أسلحة أنما أنظمة وبرامج وفيروسات ومن سلبياتها والأمورالتي تجعل اثباتها أمراً صعباً هو صعوبة اثباتها، بحيث لا يمكن تتبع بصمات الجاني أو دلائل تركها في مسرح الجريمة مثل قطرات من الدم أو أدوات تم لمسها، بل الدليل الالكتروني سهل التخلص منه في زمن قصير، بالإضافة إلى أن أكثر الدول لديها ضعف تكنولوجي في هذا المجال، وبالإضافة إلى قدم النصوص القانونية المنظمة لهذه الجرائم، ومن السلبيات أيضاً لمثل هذه الجرائم هو عدم الإبلاغ عنها من قبل الشخص الذي تم ارتكب الجريمة ضده خوفاً من الفضيحة أي الخوف من ردة فعل المجتمع تجاهه أو قد يتم ارتكابها وتسريب البيانات الشخصية والمجني عليه مع الأسف لا يعلم بأن نظامه قد أخترق، بالإضافة إلى أن الشخص المسؤول عن ملاحقة هذه الجرائم لا بد من أن لا يكون شخصاً عادياً، بل يجب أن يكون شخص لديه مستوى ذكاء عالي كون الجاني أصلاً مسبقاً يكون لديه مهارات عالية، ومن الأمور التي تجعل ملاحقة جرائم الاعتداء على البيانات الشخصية صعبة هي أن الفئات المستهدفة في كثير من الأحيان هم الأطفال، بحيث يتم استغلالهم وبالتالي هذه الصعوبات التي تواجه السلطات في ملاحقة مرتكبي جرائم الاعتداء على البيانات الشخصية من الناحية الدولية، وسوف تبين الباحثة ألية ملاحقتها خلال الدراسة (سعادات، 2015).

وتختلف عن سلطات القاضي المدني فهو لا يتقيد بوسائل معينة بالإثبات إلا في بعض الجرائم المذكورة بالقانون مثل جريمة الزنا، وله الحرية كذلك في وزن البينة، وله أن يصدر الأحكام بناءً على قناعته، وممكن أن يصدر حكم بالبراءة أو الإدانة بناءً على دليل قدم في الدعوى، وهذا الدليل كون لدى القاضي عقيدة وقناعة معينة، وبالتالي ارتاح له ضميره وتصدر الإدانة أو البراءة بناءً على هذا الدليل وجرائم البيانات الشخصية في إثباتها لها آلية معينة فالدليل فيها ليس مادياً، وانما قد نحتاج إلى تقنية معينة في مجال الحاسب الآلي والإنترنت، وخاصة أن جرائم الاعتداء على البيانات الشخصية تتم عن طريق محو أو تغيير أرقام أو بيانات من السجلات المخصصة لحفظها، و المشرع لم يحدد طرق معينة للأثبات ولكن

تكمن المشكلة في كشف جرائم الاعتداء على البيانات الشخصية أن مرتكبها يستخدم نبضات إلكترونية غير مرئية للعبث لإخفاء الدليل بسرعة، وممكن للمحكمة الاستعانة بالخبراء الفنيين لاستخلاص الدليل الفني في هذه الجرائم، ولكن لابد من الاشارة إلى أن القاضي عليه أن يلتفت لموضوع سرعة اختفاء الدليل وبالتالي لابد من السرعة بالإجراءات، وترتكز جرائم الاعتداء على البيانات الشخصية في اثباتها بشكل أساسي، بالإضافة إلى الأدلة الأخرى إلى ما يسمى الدليل الرقمي اي الدليل المأخوذ من العالم الافتراضي وله تعريف أخر "الدليل المأخوذ من أجهز الحاسب الآلي في شكل مجلات ونبضات مغناطيسية أو كهربائية ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات تكنولوجية خاصة" الدليل الرقمي يقدم معلومات، أما على شكل رموز أو صور أو أصوات أو أشكال أو رسوم تعبر عن فكر أو قول، وما يميز الدليل الرقمي ليس فقط أنه دليل غير ملموس بل هو أيضاً دليل يستخرج من الآلة وللاستفادة من هذا الدليل لابد من وجود أنظمة تختص بتجميع هذا الدليل وتنظيمه وتثبيته، وللدليل الرقمي ثلاث أنواع الأول مخرجات ذات طبيعة ورقية تسجل فيها البيانات والمعلومات على الورق مثل الطابعات، والثاني مخرجات ذات طبيعة الكترونية تخزن المعلومات بدل من تخزينها على الورق مثل الشريط المغناطيسي والأوراق المغناطيسية، والنوع الأخير هي مخرجات مرئية معروضة بواسطة شاشة حاسب آلي بحيث يتم عرض البيانات المعالجة آلياً على شاشة خاصة، أما أنواع الدليل الرقمي من حيث انتاجيته بالإثبات دليل يكون معد مسبقاً، ليكون دليل للثبات مثل السجلات الموجودة بالحاسب الألي نفسه أو يتم انشأوه في الحاسب الألي، أما النوع الأخر فهو دليل غير موجود بالأساس في الحاسب الألي ولم يتم إنشاه أيضاً إنما تركه الجاني في مسرح الجريمة الرقمي دون رغبته بتركه، وبالتالي يتم التحفظ عليه قبل أن يقوم الجاني بإرسال فيروسات لاختراق النظام وتدميره (اكاديمية التحكميم الدولي للمستشارين العرب) .

ولأن جرائم الاعتداء على البيانات الشخصية، وخاصة من ناحية دولية غالباً ما يتم استخدام التكنولوجيا فيها، وبالتالي جمع الدليل الفني هو أساس في إثبات الدعوى، ولكن الدليل الفني يجب أن يكون قد استوفى شروط معينة لقبوله بالدعوى أي ليكون منتجاً فيها، وهذه الشروط حماية لدليل نفسه خوفاً من أن يتعرض

الدليل لتغيير محتواه أو جعله غير منتج، وخاصة أن السرعة هي أمر ضروري لحفظ الدليل وأغلب الدول قد تنبهت لموضوع الدليل الفني في هذه الجرائم، وقد نصت على شروط لقبوله في الدعوى منها أن يتم تحديد الجهة المقدمة للدليل الجنائي أي الجهة المخرجة للدليل، وأن يتم المحافظة على الدليل أي تخزين ما يحتوي عليه من اثبات بطريقة تحفظ الدليل لاستخدامه في الإثبات، وحفظها بصورتها الأصلية التي تم استخراج الدليل بناءً عليها بصورة تحمي الدليل من التلف أو الاختراق، وأن تكون البيئة المحفوظة فيها آمنة والقائمين على حفظها ذو كفاءة واختصاص (أكاديمية التحكيم الدولي للمستشارين العرب).

وقد كان للمحكمة الليبية رأي في هذا المجال حيث جاء في حكمها في الطعن الجنائي رقم 18/166 ق "ليس لمحكمة الاستئناف أن تخوض في صميم المسائل الفنية التي أبدي فيها الخبير رأيه الفني؛ لان استعانة القاضي بأهل الخبرة في المسائل الفنية التي يتعذر عليه إدراكها يتطلب منه أن يضع في الاعتبار رأي الخبراء فيما يتعلق بالمسائل الفنية التي أبدى فيها الخبير رأيه الفني؛ لأن استعانة القاضي بأهل الخبرة في المسائل الفنية التي يتعذر عليه ادراكها يتطلب منه أن يضع بالاعتبار رأي الخبراء فيما يتعلق بالمسائل الفنية وألا يطرح رأيهم إلا لأسباب سائغة مقبولة" (طعن جنائي صادر عن المحكمة الليبية –رقم الطعن 18/166 لمحكمة الاستئناف بخصوص استعانة القاضي بالمسائل الفنية).

الفرع الأول: تقديم الدليل الالكتروني في جرائم الاعتداء على البيانات الشخصية دولياً:

الكثير من التشريعات تحدثت في نصوصها عن الدليل الالكتروني وضوابط تقديمه للأثبات في الدعوى وخاصة أن الدليل الإلكتروني عرضة للتحريف بشكل أكبر من الدليل التقليدي، وكما ذكرت الباحثة على الأشخاص المخولون بجمع الأدلة الالكترونية عمل كل ما يلزم من أجل ضمان حفظ الدليل وحماية محتواه لأكبر فترة ممكنة، ولابد أن يكون هناك نص تشريعي داخل الدولة يعالج موضوع جمع الأدلة الإلكترونية من خارج الدولة، وقد تحدث عن هذا الموضوع مكتب الأمم المتحدة المعني بجرائم المخدرات، والجريمة السيبرانية، حيث جاء فيه أنه يجوز للدول في سبيل تحقيق العدالة وإظهار الحق أن تسن نصوص تشريعية

تمنح من خلالها للسلطات الوطنية تنفيذ قوانين ذات صلة، وللدول أيضاً صلاحية التحقيق الخاص الذي يشمل حدود الدولة، كذلك التحقيق العام الذي يكون في الفضاء السيبراني ولها الصلاحية باتخاذ جميع التدابير والاجراءات القانونية اللزمة لجمع الأدلة الالكترونية من هذا الفضاء أي ممارسة تحليل التحقيقات الجنائية عن بعد، وهذا عاد بأهمية كبرى لدى الدول والجهات التي حققت تعاون في هذا المجال من حيث جمع الأدلة، حيث عاد ذلك بفائدة كبرى من حيث اتاحة الوصول للأدلة الإثباتية الإلكترونية، وهذه المبادئ التي أكدت عليها الأمم المتحدة حيث أعدها مجلس أوربا، ولذلك لوقف الجرائم السيبرانية وعلماً أن هذه المبادئ هي مرنة ويمكن أن يتم تطبيقها في أي بلد ودمجها مع التشريع الوطني داخل الدولة، بحيث أنها أكدت في أحد جوانبها على احترام حقوق المواطنين ومن مبادئها أيضاً، أنها شجعت تطبيق القوانين وضعت مبادئ لتسهيل التعاون وتبادل المعلومات، وضعت إجراءات لتحقيق تعاون متبادل، ودعت لإنشاء شركات لحماية خصوصية الأفراد ومن الأمور التي أشارت إليها مبادئ الأمم المتحدة ضرورة وضع جهاز تخزين الكترونية؛ للاحتفاظ بالأدلة الالكترونية، ومن الحلول التي قدمتها الأمم المتحدة هي تدعيم الشركات مع أفرقة البحث العلمي، ومن المشاكل التي تواجه جرائم الاعتداء على البيانات الشخصية في ملاحقتها وجمع الأدلة، هي في حال طلب دليل من ولاية أخرى يكون هناك في أغلب الأحيان تأخر بالاستجابة، وكذلك عدم الالتزام بتقديم الدليل وخاصة في حال كون الجاني هو أحد مواطنيها، وكذلك اختلاف النظم القانونية من دولة لأخرى فقد ترى دولة أن الفعل لا يشكل جريمة اعتداء على البيانات الشخصية بالمقابل في دولة أخرى يعتبر اعتداء على البيانات الشخصية مع العلم أنه هناك ما يسمى نمط تعاوني غير رسمي بين الدول، وذلك للمساعدة في جمع الأدلة وهو ما يسمى بالصكوك الثنائية؛ لغرض الحصول على دليل خارج الحدود الجغرافية للدول، ولكن مع الأسف الاستجابة لطلبات المساعدة القانونية بخصوص الجرائم السيبرانية تستغرق للرد عليها 150 يوم، وممكن أن تتجاوز هذه المدة الفترة الزمنية المحددة لاحتفاظ مقدمي الخدمات بالبيانات، ومن السلبيات أيضاً أن طول هذه المدة يمكن للجناة تغيير ملامح الدليل أو حذفه بشكل نهائي، وبالتالي لابد أن تقوم الدولة بإجراءات معينة لحفظ الدليل وعدم إتلافه

من قبل الغير، وهناك العديد من الاتفاقيات الدولية التي تحدثت عن التعاون في تحقيق تبادل الأدلة الجنائية مثل اتفاقية مجلس أوروبا، مع العلم أنه ممكن لدولة اللجوء لعقد اتفاقيات ثنائية أو اتفاقيات مع أكثر من دول؛ لتبادل الأدلة القانونية في حال الاحتياج لها وذلك بموجب نصوص الاتفاقية التي يتم الاتفاق عليها بين الأطراف (مؤتمر الأطراف في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة غير الوطنية–الفريق العامل المعني بالتعاون فينا2015).

ومن القضايا التي تثبت التزامات تقع على الشركات التي تعمل بمعالجة البيانات الشخصية، حيث نتج عن عدم التزام شركة M and H hennes and mauritz فرض مفوض هامبرج لحماية البيانات الشخصية وحرية المعلومات غرامة ٣٥،٣ مليون على الشركة نتيجة خرق الشركة لالتزاماتها بخصوص البيانات الشخصية لموظفيها؛ وذلك نتيجة احتفاظها بسجلات لموظفيها تحتوي على بيانات خصوصية واستخدام هذه البيانات في تقييم عمل الموظفين، كذلك الاحتفاظ في هذه البيانات تم لفترة زمنية طويلة، مع العلم أن الاحتفاظ بهذه البيانات لم يكن للموظفين علم به وأن الموضوع قد كُشف نتيجة خطأ فني في حواسيب الشركة مما جعل هذه البيانات متاحة لعدة ساعات وبالتالي نتيجة لهذه الأسباب جاء حكم المحكمة (قرار لمحكة العدل الاوروبية بخصوص قضية h and m ضد مركز حماية البيانات وحرية المعلومات بهامبرج h and m v. Data protection commissioner of hamburg).

الخاتمة

تعتبر جرائم الاعتداء على البيانات الشخصية هي جرائم العصر، وعلى الرغم من صعوبة الموضوع كونه موضوع جديد والقليل من الدول التي تنبهت لخطورة الموضوع من حيث سن تشريعات تكفل حماية خاصة للبيانات الشخصية للمواطنين، إلا أن الباحثة حاولت بكل مجهودها طرح الموضوع بطريقة سلسة يفهمها القارئ ووضع حلول فنية وتشريعية للحد من هذه الجرائم، وقد ظهر من خلال الدراسة أن دول الاتحاد الأوروبي هي كانت السباقة لحل هذه المشكلة من خلال قوانين كفيلة بتوفير الحماية، وبالتالي لا مانع من استعانة الدول ومنها فلسطين بهذه التشريعات لتحسين تشريعاتها الداخلية بما يلائم التطورات التكنولوجية ولإنقاذ وحماية البيانات الشخصية للأفراد سواء على مستوى وطني أو دولي.

وفي الخاتمة نضع بين يدي القارئ جملة من النتائج والتوصيات التي كشفت عنها الدراسة:

النتائج

1. لم يقف استغلال البيانات الشخصية عند حد وطني أو جغرافي معين بل أصبح يمتد لنطاق دولي، بحيث قدمت الوسائل التكنولوجية خدمة كبير للجناة لتسهيل السيطرة على البيانات الشخصية، ومع الأسف أصبحت الوسائل التي نستخدمها بشكل يومي مثل الهاتف أو السيارة، حيث أصبحت هذه الأجهزة تحمل كم كبير من بياناتنا الشخصية ويتم استغلها عن طريق هذه الأجهزة، وبالتالي لابد من رفع مستوى الحيطة والحذر من ما يسمى التكنولوجيا الخفية وسلبياتها على حياتنا.
2. لم يقف الأمر على جرائم الاعتداء على البيانات الشخصية من قبل الأفراد، فقط فقد امتد في الأوانِ الأخيرة إلى قيام الشركات ببيع ما جمعته من بيانات شخصية لشركات أخرى ليتم استغلالها مادية وتجارية، وبالإضافة إلى وجه أخر للاعتداء يتمثل بقيام الدول سواء الدولة نفسها أو دول أخرى بالتجسس على بيانات الأفراد، وبالتالي نحن بحاجة لتشكيل لجنة وطنية؛ لتنظم هذا الموضوع وسن قوانين تتماشى مع التكنولوجيا وتتولى ضبط وحماية بيانات الأفراد على مستوى دولي .

3. جرائم الاعتداء على البيانات الشخصية قد تتم بوسائل تقليدية وهي قليل ما تحدث مثل التسلل لأرشيف وإتلاف الملفات الموجودة، وهذه الأساليب يمكن بسهولة اكتشاف فاعلها، حيث أصبحت عادة الوزارات والجهات التي لديها بيانات شخصية تستخدم وسائل حديثة لحمايتها مثل الكاميرات والطرق الأخرى هي الوسائل التكنولوجية وهذه أكثر خطراً؛ لصعوبة الإمساك بالفاعل وجمع الأدلة، وبالتالي يمكن للدولة معالجة هذا الموضوع عن طريق تخصيص أشخاص مختصين بهذا المجال وتزويدهم بالدورات التي تزيد من كفاءتهم.

4. وجدت الباحثة أن الدولة المعنية بحماية البيانات الشخصية لمواطنيها من أي اعتداء قامت وسارعت بعمل اتفاقيات تهتم بموضوع احترام خصوصية هذه البيانات مثل دول الاتحاد الأوروبي وكانت قد فرضت غرامات كبيرة على الشركات المنتهكة لهذه البيانات، وقد كانت موفقة في ذلك كون الشركات الكبرى والتي تضم بيانات مليارات المواطنين مثل جوجل انتهكت ووقع منها اعتداءات على البيانات الشخصية مثل البيع والتسريب وغيرها، وبالتالي سارعت لحماية موطنيها بخلاف دول العالم الثالث التي لم تسعى إلى حد الأن لعمل اتفاقية دولية أو نظام يحمي البيانات الشخصية لمواطنيها، وبالتالي لابد من تحرك رؤساء هذه الدول لوقف استغلالهم واستغلال بياناتهم.

5. اثبت نظام الاتحاد الأوربي كفاءته، حيث جاء شاملاً وواضحاً حيث عرف الكثير من المصطلحات الغامضة ووضح الأطراف والإطار الجغرافي الذي يطبق عليه هذا النظام، ومن الناحية العملية حقق رادع لدى كثير من الشركات الكبرى لحماية البيانات الشخصية .

التوصيات

1. بعد إطلاع الباحثة على القرار بقانون الخاص بحماية البيانات الشخصية الساري في فلسطين والقوانين الأخرى ذات العلاقة، وجدت أنه لابد من قيام الدولة بسن تشريع واضحة بشكل أوضح ، حيث يوجد به نقص بكثير من الأمور مثل لم يحدد ولم يتطرق لموضوع جرائم الاعتداء على البيانات

الشخصية، كذلك لم يوضح بشكل الجهات الخاضعة للقانون أي الأطراف التي سوف يطبق عليها القانون، بالإضافة للكثير من نقاط الضعف قد ذكرتهم الباحثة مسبقاً.

2. تطبيق فكرة الربط الأكاديمي؛ وذلك لأن موضوع الدراسة تعتمد بشكل كبير على التقدم التكنولوجي وضرورة ملاحقة هذا التطور والاطلاع على الأساليب الحديثة والمستجدة وهذه عادة ما يكون الاتجاه الاكاديمي مطلع عليها لدراستها وضع حلول لسوق العمل.
3. لا يوجد ما يمنع من قيام الدولة من عمل دورات تثقيفية للمجتمع بخصوص هذا الموضوع كونه موضوع جديد والكثير من الناس تغفل عنه ولا يوجد ثقافة عامة لدينا بخصوصه إلا عند البعض.
4. لابد من وضع قيود على مقدمي الخدمات من حيث تبادل المعلومات مع السلطات المعنية أثناء التحقيق مثل نوع البيانات التي يجوز الوصول إليها والمدة الزمنية ومراعات ما يسمى السبب المحتمل، وإشراف من قبل أجهزة جادة في الدولة مثل القضاء والنيابة العامة.
5. ومن الأمور التي يمكن أن تخفف من ضرر الاعتداء على البيانات الشخصية أو يخفف من ضرر قد يقع بعد عملية الاعتداء هو سن قانون يجبر الشركات التي لديها بيانات شخصية وفي اختراقها إعلام المستخدمين بهذا الاختراق؛ لأنه في حال وقع الاختراق على أحد الحسابات المسجل فيها بيانات شخصية قد يتلافى صاحبها ضرر أخر بأقفال أو توفير حماية بشكل أسرع للحسابات الأخرى.
6. عند قيام الدولة بسن قانون لابد أن تراعي عدة أمور منها مرونة هذا القانون؛ لكي يتماشى مع التطور السريع وعدم حصر هذه الجرائم؛ كونها من الجرائم المستجدة التي تتطور ويظهر أنواع جديدة منها مع التقدم التكنولوجي .
7. بخصوص العقوبات الرادعة وجدت الباحثة أن فرض غرامة مالية على الشركات التي ترتكب جرائم تعتدي على البيانات الشخصية فيها هي عقوبة غير رادعة؛ وذلك لأن الأرباح التي تجنيها هذا الشركات سواء من بيع هذه البيانات او تسريبها لدعم عملية انتخابية او ضخ إعلانات تجارية تخدم

مصالح شركات كبرى، وبالتالي الأرباح قد تفوق أضعاف الغرامة، وبالتالي عقوبة الغرامة غير رادعة وتوصي الباحثة بعقوبات غيرها مثل إغلاق جزئي أو وقف عن العمل أو سحب تصريح الشركة، وبالتالي ردع أكبر لمرتكبي هذه الجرائم .

8. يمكن لأي دولة تجد في نفسها لديها القدرة على الانضمام لنظام الاتحاد الأوروبي لحماية البيانات الشخصية المسارعة في الانضمام له، وذلك لأن هذا النظام أوجد كفاءته على الساحة الدولية كذلك لسبب اخر وهو عدم وجود بديل يساوى كفاءة هذا النظام لحماية البيانات الشخصية لحين عمل نظام يوفر حماية البيانات الشخصية على مستوى دولي .

المراجع العلمية

قانون الاتصالات الفلسطيني رقم 3 لسنة 1996.

قرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الالكترونية.

قانون الاتصالات الفلسطيني رقم 3 لسنة (1996).

العهد الدولي للحقوق المدنية والسياسية. (1966).

قرار مجلس الوزراء رقم 3 لسنة 2019 بشأن حماية البيانات الشخصية. (2019).

الاتفاقية الأوربية لحقوق الانسان–اتفاقية حماية حقوق الانسان في نطاق مجلس أوروبا –روما في نوفمبر 1950.

القانون الأساسي الفلسطيني المعدل لسنة–2003.

قرار بقانون رقم (15) لسنة 2017 بشأن المعاملات الالكترونية.

مشروع قانون حماية البيانات الشخصية الاردني المعروض على اللجنة الوزارية.

تعليمات رقم (1) لسنة 2008 بشأن المحافظة على سرية المعلومات.

قرار مجلس الوزراء رقم (3) لسنة 2008م، نظام العقوبات والغرامات على المتعاملين في قطاع الأوراق المالية في.

قرار مجلس الوزراء رقم (3) لسنة 2019 المتعلق بالبيانات الشخصية الخاصة بالمواطنين.

المراجع

قرار للمحكمة العسكرية في بئر السبع، رقم الملف 53671، . تاريخ الاسترداد 18 10، 2022، من كل الحق.

موجات الراديو –الجز الأول –فلم وثائقي مترجم من قبل الباحثون المسلمون .

موقع وزارة التجارة . تاريخ الاسترداد 3 9، 2022، من موقع وزارة التجارة _ السعودية.

طعن جنائي صادر عن المحكمة الليبية –رقم الطعن 18/166 لمحكمة الاستئناف بخصوص استعانة القاضي بالمسائل الفنية.

سياسة الخصوصية للبيانات الشخصية. تاريخ الاسترداد 11 10، 2022، من موقع كوانتري، .

موقوع وزارة الاتصالات وتكنولوجيا المعلومات . (9 9، 2015). تم الاسترداد من مهارات الاتصالات والتواصل .

تكريم موظفيها المشاركين في نجاح فعاليات اليوم العالمي للاتصالات ومجتمعالمعلومات . (1 6، 2016). تم الاسترداد من موقوع الاتصالات وتكنولوجيا المعلوتووزارة الاتصالات.

حماية البيانات الشخصية. (2016). تم الاسترداد من https://youtu.be/BmgSSe-35L.

قواعد أساسية لحماية بياناتك علة شبكة التواصل الاجتماعي. (2018). تم الاسترداد من موقع كن أمناً.

7 أشياء لا تفعلها على مواقع التواصل الاجتماعي. (22 11، 2019). تم الاسترداد من موقع الجزيرة.

الاحتيال الإلكتروني... مواجهة مع التهديدات السيبرانية في قطر. (4 فبراير، 2019). تم الاسترداد من موقع العربي الجديد.

حماية الكمبيوتر من الفيروسات. (13 10، 2019). تم الاسترداد من موقع مايكروسفت.

فيسبوك تخسر 119 مليار دولار في يوم واحد. (27 7، 2019). تم الاسترداد من موقع الجزيرة.

قرار لمحكمة صلح رام الله بشأنالجرائم الالكترونية وحجب مواقع الالكترونية . (2019).

نصائح ذهبية لحماية البيانات الشخصية. (13 10، 2019). تم الاسترداد من موقع الغد.

يوتيوب. (9 نوفمبر، 2019). تاريخ الاسترداد 4 6، 2022

أهمية قانون حماية البيانات الشخصية. (26 يناير، 2020). تاريخ الاسترداد 5 6، 2022

حقيقة سرقة الأعضاء ماذا تعني . (29 10، 2020). تم الاسترداد من يوتيوب.

unodc. (2021). تم الاسترداد من سلسلة الوحدات التعليمية الجامعية الجريمة الالكترونية .

سرقة البيانات الشخصية ....سوريون ضحايا انتهاك الخصوصية في تركيا 2021/2/7 . (7 2، 2021). تم الاسترداد من يوتيوب.

واقع الخصوصية وحماية البيانات الرقمية في فلسطين، دراسة أطلقها المركز العربي لتطوير الاعلام الاجتماعي خلال يوم دراسي حول قضية الخصوصية وحماية البيانات الرقمية للفلسطينيين. (2021).

الجرائم التي تستهدف المواقع الالكترونية. (2022). *مراجع جامعية* .

الحماية القانونية للبيانات الشخصية. (2022).

قرار بمحكمة العمل القطرية، رقم الملف 8/90. (8 10، 2022). تم الاسترداد من موقع كل الحق.

قرار للمحكمة العليا التركية، جريمة انتهاك الحياة الخاصة ١٣٤ tck. (12 10، 2022). تم الاسترداد من موقع mgc.

كيف تمنع التطبيقات من استغلال بياناتك. (4 فبراير، 2022). تاريخ الاسترداد 22 10، 2022، من موقع العربية.

أ. مايكل بسادة. *التوقيع الالكتروني والمحرر(المستند) الالكتروني –هل لهما أي فائدة أو قيمة،* . تم الاسترداد من رابط https://youtu.be/Azbw0ut712A.

ابراهيم القاسمي. (2018). *جرائم الدخول والبقاء غير المشروع في نظام المعالجة الالية للمعطيات الالكترونية وفقاً للمرسوم بقانون اتحادي رقم (5) لسنة 2021 في شأن جرائم تقنية المعلومات وتعديلاته)*، . الامارات .

احمد الزعبي. (2017). *جريمة الافشاء غير المشروع للبيانات الشخصية، كتاب بعنوان حق الخصوصية.*

أشرف محمد سعيد الدرياني. (2021). *جرائم الاعتداء على سلامة شبكات وانظمة وتقنيات المعلومات 2021*

أعددنا في سدايا سياسة حماية البيانات الشخصية ؛ للمحافظة على خصوصية الأفراد في كل الميادين 2021 تم الاسترداد من https://youtu.be/2K9RGrXz7Tk.

اكاديمية التحكميم الدولي للمستشارين العرب. لجريمة الالكترونية.

أكاديمية التحكيم الدولي للمستشارين العرب. لجريمة الالكترونية . *مدينة نصر*.

أكرم سليمان فجم. (2021). *الحماية القانونية للبيانات الشخصية على مواقع التواصل الاجتماعي في القانون القطري والقانون المقارن.*

اكستر نيوز. *شرح أهمية قانون حماية البيانات الشخصية* . تاريخ الاسترداد 5 6، 2022، من يوتيوب.

الاء بنت سعيد. *حماية البيانات الشخصية لمستخدمي شبكات التواصل الاجتماعي رسالة ماجستير* . عمان.

الاء ناصر. . *حماية البيانات الشخصية لمستخدمي شبكات التواصل الاجتماعي.*

الاستاذ شول بن شهرة. *مرجع سابق.*

القران الكريم. *سورة النور الاية 29،28،27.*

القوانين التي وضعت حماية للبيانات الشخصية ونظمت موضوعها . تم الاسترداد من مقام.

اللجنة الدولية للصليب الاحمر. *حماية البيانات الشخصية*. تم الاسترداد من موقع اي سي ار سي.

المؤلف ستيفن لايفي–تعريب عبد الاله ملاح –الشيفرة . *–الشيفرة –كيف اقتحمت السرية بالعصر الرقمي.*

المؤلف ستيفن لايفي–تعريب عبد الاله ملاح. *الشيفرة كيف اقتحمت السرية بالعصر الرقمي.*

أمين أعزان. حماية البيانات الشخصية للمستهلك الالكتروني. *مجلة الاقتصاد والمستهلك العدد 5/6.*

أمين الحارث، و محمد الطويريقي. (2018). *تنظيم وادارة المعلومات الشخصية،المؤتمر العالمي الأكاديمي الدولي التاسع.* تركيا.

اياد الرفاعي. قانون حماية البيانات في دولة فلسطين بين استغلال البياناتدون رقابة وبين قوانين لتوفير الحماية . ص1.

ايمان الحياري. (2022). أنواع الجرائم الالكترونية.

ايمان علي. (2021). *الحبس والغرامة عقوبة افشاء البيانات الشخصية الحساسة.*

ايمانا صيادي. (25 كانون الثاني، 2019). البيانات الشخصية ما مدى أهمية حمايتها وهل من تشريع؟ صفحة 1.

برنامج جوجيل هنجوتس، هو برنامج صنعته الشركات لتسهيل التواصل وانجاز المهام أثناء العمل كفريق حيث سهل عملية التواصل مع الأفراد بدل من اجراء المكالمات بين بعضهم البعض، كذلك يوجد يه ميزة مفيدة ويحفظ الرسائل المتبادلة بين العاملين.

بن قارة مصطفى. (2016). *الحق في الخصوصية المعلوماتية بين تحديات التقنية والواقع القانوني.*

بهاء فهمي الكبجي. *مدى توافق أحكام جرائم أنظمة المعلومات في القانون الاردني مع الاحكام العامة للجريمة.*

بيانات حماية وأمن المعلومات قواعد السلوك المهني. تاريخ الاسترداد 26 11، 2022

تجارة الأعضاء: هي تجارة بالأعضاء البشرية أو الانسجة أو أجزاء أخرى من الجسم بقصد زرع أعضاء أخرى.

جرائم الأنترنت مقال. تم الاسترداد من حماة الحق.

حق الخصوصية: جريمة التسجيل والحفظ غير المشروع للبيانات الشخصية. *على احمد الزعبي.*

حماية البيانات الشخصية لمستخدمي شبكات التواصل الاجتماعي.

حمزة خضر. (7 فبراير، 2021). *سرقة البيانات الشخصية سريون ضحايا انتهاك الخصوصية في تركيا.* تم الاسترداد من موقع العربي الجديد.

خالد موسى. (16 ديسمبر، 2014). *تشكيك الخصوصية على مواقع التواصل*. تاريخ الاسترداد 16 10، 2022

خلود عيشة. *الطبيعية الخاصة للجريمة الالكترونية وصورها*. الجلفة.

د حسن عبد الحميد. (2013). *قرار لمحكمة العدل الاوروبية بخصوص قضية ماكسشريمز ضد مركز حماية البيانات الايرلندية*.

د حسن عبد الحميد. (2013). *قرار لمحكمة العدل الدولية بخصوص قضية جوجل اسبانيا ضد مركز حماية البيانات الاسباني* .

د ماجد الشمري. (16 9، 2021). *يوتيوب*. تاريخ الاسترداد 4 6، 2022

د. حسن عبد الحميد. (2003). *قرار لمحكمة العدل الأوربية في قضية ديوران ضد هيئة الخدمات المالية*.

د. حسن عبد الحميد. (2014). *قرار لمحكمة العدل الدولية قضية شوارز ضد بوشام*.

د. خالد الحمداني. (2019). *جريمة الدخول غير المشروع إلى النظام المعلوماتي في القانون القطري*: . قطر.

د. عودة يوسف سليمان. *الجرائم الماسة بحرمة الحياة الخاصة التي تقع عبر وسائل تقنية المعلومات الحديثة*.

د. كامل مطر. (2016). *الجريمة الالكترونية*. فلسطين.

د.أشرف السعيد، *جرائم الاعتداء على سلامة شبكات وانظمة وتقنية المعلومات* . المنصورة.

د.حاتم بطيخ. (2021). *تطور السياسة التشريعية في مجال مكافحة جرائم تقنية المعلومات (دراسة تحليلية مقارنة).*

د.علي الجواد. (2020). *حكم قضائي للمحكمة الادارية العليا المصرية يكشف عن مجموعة من أنواع الجرائم الالكترونية التي يرتكبها الموظفين، .*

د.عودة سليمان. *الجرائم الماسة بحرمة الحياة الخاصة التي تقع عبر وسائل تقنية المعلومات الحديثة.* الرافدين.

د.محمد المعداوي. *حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي.*

د.مروان الزعبي.. *انتهاك خصوصية المعلومات المتداولة على مواقع التواصل الاجتماعي التي يرتكبها الزوجين ضد بعضهم البعض في التشريع الاردني .*

د.مصطفى عبيد. *اللائحة العامة لحماية البيانات لاتحاد الأوربي البرلمان والموفوضية الاوربية GDPR موسوعة العلوم القانونية المواد 1-5.*

رمزي بوشية. (2014). *التنصت على المكالمات والتقاط الصور بين التجريم والاباحة.*

روان بهام. (13 10، 2019). *يوتيوب*. تاريخ الاسترداد 29 5، 2022

ريان دريزو. (20 حزيران، 2017). *وسائل التكنولوجيا التي تراقبنا في مكان العمل، .* تم الاسترداد من موقع عرب نيوز.

زينب عبد المنعم –اسراء حسني –مؤنس حواس. (2018). *التفاصيل الكاملة لمحاكمة مؤسس فيس بوك بالكونجرس.*

شول بن شهرة. *:برنامج الحماية الجنائية للبيانات الشخصية في معاملات التجارة الالكترونية .*

شول بن شهرة. (2011). *حماية الخصوصية في المعاملات المالية الاسلامية.*

شول بن شهرة. *برنامج الحماية الجنائية للبيانات الشخصية في معاملات التجارة الالكترونية.*

صلاح الدين دكداك. (2014). *المسؤولية الجنائية للأشخاص الاعتبارية عن جريمة المساس بأنظمة المعالجة الالية للمعطيات.*

ضرغام فاضل.. *حماية بيانات الأفراد الشخصية عبر شبكة الانترنت.*

طارق راشد. (2019). *الحماية القانونية لخصوصية البيانات الشخصية في العصر الرقمي، دراسة مقارنة.* القاهرة.

طه الحصري. (2020). نطاق جرائم قانون حماية البيانات الشخصية. صفحة 1.

عرب نيوز. (2022). قرار رقم 9542 لمحكمة النقض المصرية بخصوص قضية محمد رمضان . عرب *نيوز.*

على الزعبي. (2017). *جريمة المعالجة الالكترونية للبيانات الشخصية دون ترخيص، .*

علي الزعبي. *برنامج الحماية الجنائية للبيانات الشخصية في معاملات التجارة الالكترونية .*

علي الزعبي.. *حق الخصوصية: جريمة التسجيل والحفظ غير المشروع للبيانات الشخصية.*

غطية شحاته، عبد الفتاح درويش، و دنيا سالم . (2019). *لجريمة الالكترونية وعلاقتها بالميل للجريمة لدى طلاب الجامعة، مقال منشور في الجامعة المنوفية.* مصر.

فادي فارس. (27 6، 2022). التحكم بالبيانات الشخصية.

فريد جيور.. *حماية البيانات الشخصية* .

فكران سعيد. (2019–2020). *الجرائم المعلوماتية الواقعة على الحق في الخصوصية*. الجزائر.

فكران عادل سعيد. (2019). *الجرائم المعلوماتية الواقعة على الحق في الخصوصية* . الجزائر.

قرار لمحكة العدل الاوروبية بخصوص قضية h and m ضد مركز حماية البيانات وحرية المعلومات بهامبرج h and m v. Data protection commissioner of hamburg

قرار لمحكمة الاستئناف في السعودية، رقم الدعوى 3463319 تاريخ الاسترداد 6 10، 2022، من موقع عدالة.

كريسي وليش، و محمد الطويريقي. (2018). تنظيم وادارة المعلومات الشخصية،. صفحة 2016.

لبنى مهدي. (2020). *ماهي الآليات التي تنفذ بها الجريمة الالكترونية؟ ا*.

مايكل بشادة. (بلا تاريخ). *التوقيع الالكتروني والمحرر(المستند) الالكتروني –هل لهما أي فائدة أو قيمة، رابط https://youtu.be/Azbw0ut712A*.

مجلة العلوم الانسانية العدد السابع الجزء.

مجلة العلوم الانسانية العدد السابع الجزء1. (2017). مجلة العلوم الانسانية العدد السابع الجزء.

محسن البدوي. (2022).، *ما هي عقوبة الاعتداء على الأنظمة المعلوماتية لدولة*.

محمد سعادات. (2015). *خصائص الجرائم المعلوماتية وصفات مرتكبيها في مجتمع المعلوماتية* . الرياض.

محمد سيد. (2022). ما هي اللائحة العامة لحماية البيانات؟ وكيف تؤثر على على خصوصيات المستخدم؟

محمد عبد الجواد قاسم. (22 6، 2022). الجهة المتحكمة بالبيانات الشخصية. (الباحثة، المحاور)

محمد علاء. (2022). *قرار لمحكمة الادارية العليا في مجلس الدولة المصري صدر الحكم برئاسة المستشار عادل بريك رئيس مجلس الدولة المصري، وعضوية المستشارين سيد سلطان والدكتور محمد عبد الوهاب خفاجي ونبيل عطاالله وشعبان عبد العزيز نواب رئيس مجلس الدولة.* مصر.

محمد علي سالم، حسون عبيد هجيج،. (2007). *الجريمة المعلوماتية* . بابل.

محمد عنتر. (2019). *كيفية حماية البيانات الشخصية بخطوات بسيطة*. تم الاسترداد من يوتيوب.

محمد فتحي شحته. (2019). *: تجريم الاعتداء على المعلومات الالكترونية ذات الطابع الشخصي بين الواقع والمأمول.* السعودية.

مركز دعم لتقنية المعلومات . (2022). الحماية القانونية للبيانات الشخصية. 1.

مروان محمد الزعبي. *مرجع سابق.*

مريم نصر الله. (2018). طرق حماية المعلومات.

مزاوي محمد. (2014). *المسؤولية الجنائية للأشخاص الاعتبارية عن جريمة المساس بأنظمة المعالجة الآلية للمعطيات.* الجزائر.

مسار.. قانون حماية البيانات الشخصية، تعزيز الحق بالخصوصية أم ايهام بتحسين البيئة التشريعية؟ *مسار*، ص3.

مفتاح ميلاد. (2022). *الجرائم الالكترونية- جامعة المرقب*.

منى اشتية، و اياس خطيب. (2021). *واقع الخصوصية وحماية البيانات الرقمية في فلسطين.* فلسطين.

مؤتمر الأطراف في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة غير الوطنية–الفريق العامل المعني بالتعاون فينا2015.

موجات الراديو – –فلم وثائقي مترجم من قبل الباحثون المسلمون .

موجات الراديو –الجز الأول –فلم وثائقي مترجم من قبل الباحثون المسلمون .. تاريخ الاسترداد 12، 2022، من يوتيوب.

موقع aws. (بلا تاريخ). *اللائحة العامة لحماية البيانات.*

موقع الانتربول. (2021). معلومات غير مسبوقة عن خطر استغلال الأطفال والاعتداء عليهم جنسيا على الإنترنت في كينيا، .

موقع الجزيرة . (2022). أنواع المعلومات الشخصية التي نقدمها لشركات التواصل الاجتماعي. *الجزيرة*.

موقع الشرق. (8 ابريل، 2017). *اهمال البيانات الشخصية وراء جرائم انتهاك الخصوصية*.

موقع جامعة اكتوبر. تم الاسترداد من https://youtu.be/Hn2Ms30Uei.

موقع عرب نيوس .. تاريخ الاسترداد 2022 9، 9

موقع مراجع جامعية. (2022). الجرائم التي تستهدف المواقع الالكترونية.

موقع ميزان،نظام لحفظ الجلسات القضائية .

موقع وزارة التجارة _السعودية .. تاريخ الاسترداد 2022، من موقع وزارة التجارة _السعودية .

موقع وزارة الصحة الفلسطيني. (22 10، 2022). *الحق في خصوصية المريض المصاب بكوفير 19*. تم الاسترداد من موقع وزارة الصحة الفلسطيني.

يوسف عبد القادر. (19 نوفمبر، 2021).، *كيف تخترين كلمة مرور صعبة الاختراق لحساباتك*.

An-Najah National University

Faculty of Graduate Studies

PERSONAL DATA OFFENES

By

Ruba Thafer Hantoly

Supervisor

Dr. Fadi Shaded

This Thesis is Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Private Law , Faculty of Graduate Studies, An-Najah National University, Nablus - Palestine.

2023

PERSONAL DATA OFFENES

by
Ruba Thafer Hantoly
supervisor
dr. Fadi Shaded

Abstract

Crimes of attacking personal data have become crimes of today's world. Moreover, the issue of attacking personal data crimes is somewhat one of the new topics as few countries have noticed the seriousness of this issue and become alerted to it by enacting laws that protect personal data and criminalizing attacking them. As a result, countries were divided into three sections: the first section enacted special legislation for crimes of assault on personal data, such as the French legislation; the second section such as Palestine set out a legislative text for the crimes of assaulting personal data, but it was a regulatory text that was insufficient to cover all crimes of assaulting personal data. The last section, did not make any legislations to protect personal data, but it acted only in the event of any attack on personal data. So, it covered this issue through the legislations used by others countries such as the Cybercrime Law, the Communications Law and other related laws.

The practical importance that the study dealt with is that it touched upon crimes of assault on personal data such as ears dropping, defamation, recording and transmitting private conversations, and taking illegal pictures and using them in an abusive manner, especially, because the use of modern technological means, in particular smart phones, facilitates the process of accessing private files, including cameras, texts, audio recordings, etc. This constitutes an assault on personal data, where these data are used to make big sums of money by companies.

In order for our country, Palestine, to be developed in terms of respecting human rights and privacy, it is necessary to enact legislation for crimes of assault on personal data that stipulates the crimes that may occur on personal data. Thus, in order to create a distinct legislation, it does not mind of applying the idea of academic linkage to accurately determine the crimes that can occur on personal data and the deterrent penalties that hurt the offender.

Among the deterrent penalties that can be enacted through legislation to deter offenders is not to be satisfied with financial fines alone because the financial profits that the person will attain from attacking personal data are much greater than the fine. Therefore, the penalty of blocking the site or the total or partial closure of it has achieved greater deterrence .Also, among the suggestions that can be applied is to oblige company owners and service providers, in the event of a breach of any personal data of citizens or employees, to notify the person concerned within 72 hours.

Keywords: personal data, cybercrime, communications law.