جامعة قطر
كليّة القانون

الحماية القانونية للبيانات الشخصية على مواقع التواصل الإجتماعي في القانون القطري والقانون المقارن

إعداد
الطالبة / إكرام سليمان قجم

قُدّمت هذه الرسالة استكمالا لمتطلّبات
كليّة القانون
للحصول على درجة الماجستير في
القانون الخاص

يونيو 1442/2021

©2021. إكرام سليمان يونس قجم.
جميع الحقوق محفوظة.

لجنة المناقشة

استُعرضت الرسالة المقدّمة من الطالب/ة إكرام سليمان يونس قجم بتاريخ يوليو، وَوُفِقَ عليها كما هو آتٍ:

نحن أعضاء اللجنة المذكورة أدناه، وافقنا على قبول رسالة الطالب المذكور اسمه أعلاه .وحسب معلومات اللجنة فإن هذه الرسالة تتوافق مع متطلبات جامعة قطر، ونحن نوافق على أن تكون جزء من امتحان الطالب.

الاسم الدكتور فوزي بالكناني

المشرف على الرسالة

_____

الاسم الدكتور عماد قطان

مناقش

_____

الاسم الدكتورة نسرين المحاسنة

مناقش

تمّت الموافقة:

_____

الدكتور محمد بن عبد العزيز الخليفي، عميد كليّة القانون

المُلخَّص

إكرام سليمان يونس قجم ، ماجستير في القانون الخاص:

يونيو 2021.

العنوان: الحماية القانونية للبيانات الشخصية على مواقع التواصل الإجتماعي في القانون القطري والقانون المقارن

المشرف على الرسالة: الدكتور فوزي بن أحمد بالكناني

في ظل حداثة موضوع البحث وظهور العديد من الانتهاكات التي تمس الأشخاص بسبب سهولة وسرعة تداول البيانات الشخصية المتاحة في شكل رقمي عبر المواقع الإلكترونية تسعى هذه الدراسة البحثية للكشف عن ماهية البيانات الشخصية في العالم الافتراضي باتخاذ قانون حماية البيانات القطري رقم 13 لسنة 2016 م كأساس لهذه الدراسة، وأمام جدلية الطبيعة القانونية لهذه البيانات من ناحية إيجاد المعيار الذي يبين خصوصيتها نرى أن هذه البيانات لها قيمة مالية شأنها شأن السلع من حيث إمكانية تقويمها وبيعها واستغلالها طالما دلت على صاحبها وبالتالي لا يجوز معالجتها إلا برضا صحيح منه.

ولقد تضمنت هذه الدراسة عدة مناهج من البحث العلمي؛ وهي المنهج الاستنباطي وكان واضحاَ في تناول التأصيل الدستوري والتشريعي والإطار القانوني لحماية البيانات الشخصية في النظام القانوني القطري وفي بيان مدى صلاحية النظرية التقليدية لعناصر المسؤولية المدنية بصورها المختلفة في حمل المسؤولية عن المساس بالبيانات الشخصية على مواقع التواصل الاجتماعي.

واعتمدت على المنهج المقارن الذي يقصد به عمل مجموعة من المقارنات بين الظواهر المتعلقة بالبحث العلمي، وذلك للتعرف على وجه الشبه فيما بينهم، وكذلك وجه الاختلاف وذلك في دراسة نصوص قانون حماية البيانات الشخصية القطري ومقارنتها بالنصوص القانونية الأخرى ذات الصلة بموضوع البحث الواردة في التشريعات الدولية والاتفاقيات التي تطرقت لتنظيم حماية البيانات دون التقيد بقانون واحد وتوظيفها لتوضيح مدى إسهام كل منها في حل إشكاليات البحث عند إعماله عليها، كما استعنت بالمنهج الاستقرائي وكان هذا في تحديد المقصود بالبيانات الشخصية وماهية مواقع التواصل الاجتماعي وحرية التعبير والرأي وأثره على حماية البيانات الشخصية وأشكال وصور الانتهاكات للبيانات والاضرار المترتبة عن ذلك والجرائم التي يمكن تكوين نماذجها على هذا الانتهاك كما طرقنا أبواب المنهج التاريخي في تطور حماية البيانات الشخصية عبر التاريخ وفق الوعاء الذي يتضمنها ومدى اتصال الغير بها.

ومن أهم النتائج التي توصلت إليها إقرار حق المستخدم في النسيان الرقمي للبيانات الموجودة بحسابه إذا ما قام بحذف بياناته أو انتهاء حياته وأن على مقدم خدمة التواصل احترام هذا الحق في أي وقت طالما لم يتعلق بحقوق الآخرين كما أنه مسؤول عن حماية البيانات التي ينشرها المستخدم في حدود صلاحيته بأن يقوم بإلغاء المحتوى فور إبلاغه بعدم مشروعيته وأن شخصاً آخر قام بانتحال شخصية المستخدم ودوره يختلف عن دور مزود خدمة الإنترنت الذي عادةً ما يقوم بدور فني وهو تمكين المستخدم من الاتصال بالشبكة وإن كان مسؤولاً في حدود اختصاصه بأن يحجب بعض المواقع غير المشروعة كالإعلانات الإباحية أو المواقع الإرهابية وكل ما يخل بالنظام العام. وبتطبيق القواعد العامة في المسؤولية المدنية في مقام حماية البيانات الشخصية على مواقع التواصل الاجتماعي يتضح أن هناك التزامات تقع على عاتق الشخص المسؤول عن معالجة البيانات وفق أحكام المسؤولية العقدية وأنه يتعين إقامة المسؤولية التقصيرية لكل شخص على ضوء الدور القائم به ودرجة تدخله في تقديم الخدمة وعلى حسب ظروف كل واقعة على حده بما يضمن للمضرور التمسك بالمسؤولية التضامنية عند الرجوع عليهم بالتعويض عن الضرر.

شكر وتقدير

الحمد لله رب العالمين الذي علم بالقلم، علم الإنسان ما لم يعلم.

أما بعد:

لا يسعني في هذا المقام إلا أن أتقدم بخالص آيات التقدير والشكر المقرونين بالاحترام لكل من أستاذي القدير الدكتور / فوزي بن أحمد بالكناني على تفضله بالإشراف على رسالتي وكذلك أعضاء لجنة الإشراف الدكتور / عماد قطان والدكتورة / نسرين محاسنة.

الإهداء

إلى أبي وأمي أطال الله في عمرهما وأمدهما بالصحة والعافية

إلى زوجي الحبيب

إلى أختي الغالية

إلى عائلتي الفاضلة وكل من ساعدني لأتم هذا البحث

الفهرس

شكر وتقدير.....ج

الإهداء.....ح

المقدمة.....1

الفصل التمهيدي: البيانات الشخصية في العالم الإفتراضي.....14

المبحث الأول : البيانات الشخصية بين الماهية والتأصيل.....15

المطلب الأول : تعريف البيانات ذات الطابع الشخصي.....17

المطلب الثاني : معالجة البيانات الشخصية على العالم الإفتراضي.....19

المطلب الثالث : الطبيعة القانونية للبيانات الشخصية على مواقع التواصل.....24

المبحث الثاني: المقصود بمواقع التواصل الإجتماعي.....29

المطلب الأول: ماهية وسائل التواصل الإجتماعي.....30

المطلب الثاني: وسائل التواصل الإجتماعي و مبدأ حرية التعبير عن الرأي.....36

المطلب الثالث: وسائل التواصل و حماية البيانات.....38

المبحث الثالث: حق النسيان الرقمي و حماية البيانات الشخصية.....45

المطلب الأول: مفهوم النسيان الرقمي.....47

المطلب الثاني: طبيعة الحق في النسيان الرقمي.....48

المطلب الثالث: إشكالية حق النسيان الرقمي.....50

الفصل الأول: المسؤولية القانونية على وسائل التواصل الإجتماعي.....53

المبحث الأول: المسؤولية المدنية عن الأضرار.....54

المطلب الأول: المسؤولية العقدية 54

المطلب الثاني: المسؤولية التقصيرية.....62

المبحث الثاني: أساس المسؤولية عن الضرر الرقمي.....65

المطلب الأول: الإتجاه التقليدي للمسؤولية عن الضرر المعلوماتي.....66

المطلب الثاني: الإتجاه الحديث للمسؤولية عن الضرر المعلوماتي للبيانات.....68

المبحث الثالث: عناصر المسؤولية عن الضرر المعلوماتي.....69

المطلب الأول: أطراف المسؤولية عن الضرر المعلوماتي للبيانات.....70

المطلب الثاني: الطبيعة القانونية لمواقع التواصل ودورها في أشخاص المسؤولية.....83
المطلب الثالث: مقارنة مسؤولية وسيلة التواصل بتلك العائدة لمن يستضيف البيانات ..85
الفصل الثاني: الإطار القانوني و التنظيمي لحماية البيانات ذات الطابع الشخصي.....91
المبحث الأول: مصادر تهديد البيانات ذات الطابع الشخصي على مواقع التواصل...91
المبحث الثاني: صور الإعتداء على البيانات الشخصية.....97
المطلب الأول: الإعتداءات الغير مشروعة على البيانات الشخصي.....97
المطلب الثاني: المساس المشروع بالبيانات ذات الطابع الشخصي..... 105
المطلب الثالث: آثار المسؤولية.....109
المبحث الثالث: الإختصاص القضائي و التشريعي بمنازعات البيانات على المواقع..119
المطلب الأول: الإختصاص التشريعي بمنازعات البيانات على مواقع التواصل.....120
المطلب الثاني: الإختصاص القضائي بمنازعات البيانات على مواقع التواصل 123
الخاتمة.....129
قائمة المصادر و المراجع.....132
المراجع باللغة العربية.....132
المراجع باللغة الأجنبية.....137

مقـــــدمـــــة

لم تعد شبكة الإنترنت قاصرة على التواصل التقليدي بين الأفراد عبر ما يسمي بالبريد الالكتروني إنما أوجد العالم الافتراضي برامج أسرع وأقوى في التواصل الشخصي بين الأفراد من خلال مواقع التواصل الاجتماعي الحديثة المتماشية مع التكنولوجيا المتسارعة في الأجهزة الالكترونية المتصلة بشبكة الإنترنت[1]

وقد تعاظم الاستخدام لمواقع التواصل الاجتماعي حتى أصبح جزءاً هاماً من حياة البشر من خلال نقل ملفاتهم وصورهم وأحاديثهم المكتوبة أو المسجلة بصورة لحظية، كما أنه المحرك الأساسي لكثير من الاحداث المحلية والدولية، وأصبحت مواقع التواصل الاجتماعي منبراً للتعبير عن الآراء والمشاعر والأفكار لأنها تحرر الانسان من القيود التقليدية للتعبير عن الرأي والفكرة وتمنحه سلطة فرض رأيه وفكرته وتعتبر امتداداً له وتأكيداً على وجوده في التعبير عن فكرته تجاه مشاكل المجتمع.

إلا أنه وبالرغم من أهمية وعظم دور مواقع التواصل الاجتماعي فقد تفقد جزءاً من أهميتها من جانب المستخدمين الذين لا يبالون بمسؤولياتهم القانونية تجاه إساءة استعمال واستغلال مواقع التواصل الاجتماعي أو من لا يعي منهم عظم هذه المسؤولية خلاف مقدمي الخدمة في هذه المواقع والذين في الغالب لديهم الجدار القانوني المانع أو على الأقل المحدد لمسؤولياتهم من خلال الشروط التي يضعونها قبل الاشتراك من قبل المستخدمين في التطبيقات المطروحة منهم على شبكة الانترنت[2].

وقد أدّت الزيادة المضطردة في استخدام مواقع التواصل الاجتماعي إلى وجود مئات الملايين من البيانات المحملة على هذه المواقع والتي يزورها كذلك مئات الملايين يومياً، بل إن بعض المواقع وصل مشتركيه إلى ما يزيد عن المليار مشترك. بل إن استخدام تلك المواقع يلزم المستخدم بوضع قدر من البيانات الشخصية ليحصل على خدمات الموقع. ومن المستخدمين من يقوم بتوثيق الحساب بالبيانات الشخصية الصحيحة أو منهم من يقوم بالاشتراك بهذه البيانات دون توثيقها ومنهم من يشترك ببيانات غير صحيحة، وإن كان الحق في التواصل الاجتماعي أصبح من الحقوق المتفرعة

---

[1] أشرف جابر، مسؤولية مقدمي خدمات الإنترنت عن المضمون الإلكتروني غير المشروع، دراسة خاصة في مسؤولية متعهدي الإيواء، دار النهضة العربية، 2010، ص5.

[2] أشرف جابر، مسؤولية مقدمي خدمات الإنترنت عن المضمون الإلكتروني غير المشروع، دراسة خاصة في مسؤولية متعهدي الإيواء، المرجع السابق، ص 11.

من الحق الشخصي إلا أن هذا الحق قد يتعارض أو يتداخل مع حقوق قانونية أخرى متعلقة بالحق الشخصي مثل حرية التعبير والرأي والحق في حماية البيانات الشخصية وحقوق الملكية الفكرية، وإن كان حق حماية البيانات الشخصية ليس بالجديد على مجال البحث القانوني [3] إلا أن الوعاء الموجودة به البيانات على العالم الافتراضي (شبكة الانترنت وما تحمله من مواقع للتواصل الاجتماعي) لم يتطرق اليه رجال القانون بالشكل الكافي خاصة بعدما تعاظمت مكانة الهواتف الذكية والتطبيقات المجانية وشبه المجانية في التواصل على شبكة الانترنت مما أدى إلى مضايقة مستخدميها من خلال انتهاك خصوصيتهم والبحث عن معلوماتهم الشخصية حتى أصبحت مواقع التواصل الاجتماعي بمثابة بنك المعلومات الشخصية المجانية حيث أن الكثير من المواقع لا يستلزم إدخال معلومات حقيقية موثقة على المستخدم وهم عادة من الطائفة التي لا ترغب في معرفة هويتها لآرائها الراديكالية أو السياسية المعارضة أو لأنّ لهم أغراضا يخشون معرفتها من الغير.

وعلى ذلك يمكن القول إن وسائل التواصل الاجتماعي تثير إشكاليات قانونية عديدة، منها ما يتعلق بخصوصية بيانات الفرد الشخصية ومدى جواز التعرض لها، ومنها ما يتعلّق بحق مقدم الخدمة من تجميع البيانات وكيفية استغلالها واستعمالها وتوافق ذلك مع الحق في حماية البيانات وحرية التعبير والرأي والقيود التي يلزم مراعاتها والمسؤولية الناشئة عن المساس بهذه البيانات أو انتهاك الحق في حمايتها وخصوصيتها.

إن حماية البيانات الشخصية لكل فرد يشكل أساساً لاحترام حقوقه وحرياته باعتبارها السند لمجموعة الحقوق المتصلة به وقد تطور مفهوم البيانات الشخصية من الناحية القانونية بإقرار المجتمعات الغربية أولاً بقيمة الحياة الشخصية وحرمتها كإحدى القيم التي لا يجوز التعرض لها والتي يجب صونها ، كما صدرت في المجتمعات الغربية القديمة وثائق مثل الماغنا كارتا عام 1215 التي وضعت حدوداً للسلطات السياسية ، ثم تلتها المواد الإثني عشر عام 1525 في ألمانيا ، ثم إعلان الجمعية الوطنية الفرنسية حول حقوق الإنسان عام 1789 كوليدة للثورة الفرنسية ، ثم صدرت شريعة الحقوق في الولايات المتحدة الأميركية عام 1791[4].

---

[3] أنظر في هذا المعنى: منى الأشقر جبور، البيانات الشخصية والقوانين العربية، الهم الأمني وحقوق الأفراد، المركز العربي للبحوث القانونية والقضائية، أبحاث ودراسات ، بيروت ، لبنان ، 2018، ص 17 وما بعدها.

[4] مروة زين العابدية صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، مركز الدراسات العربية، الطبعة الأولى 1437هـ - 2016م، ص 91.

وقد كان لدخول هذه النصوص إلى المجتمع أثر في جعل الحقوق الإنسانية واجبة الاحترام من الغير ويجب حمايتها بالقانون بعدما كان الإنسان مجرد سلعة يباع ويشترى جسده دون اعتبار لكرامته إلى أن أصبح جسده ورأيه وكرامته محل احترام من الغير ومن السلطات الرسمية. وقد ازداد هذا المفهوم توسعاً في المجتمعات وإن كان بنسب متفاوتة، ففي أوروبا أدى انتشار استعمال أنظمة الحاسوب والحواسيب الكبيرة التي يمكنها حفظ كميات من البيانات وتداولها بسرعة على مستوى الأفراد على اختلاف مواقعهم بما في ذلك البيانات الخاصة بالأفراد مثل الاسم، الأصل ، العنوان ، الآراء والمعتقدات ، التقارير الطبية. وهو ما يثير الحق في إمكانية الكشف والمعالجة والتحليل لهذه البيانات بما يسمح بالتعرض لها ومن ثم يسهل انتهاك الحياة الخاصة للأفراد ، وبالنظر إلى القوانين العربية المتعلقة بحماية الخصوصية نجد أن أغلب الدساتير كفلت الحرية الشخصية للمواطنين دون التعرّض بالضرورة للخصوصية والحياة الشخصية ، غير أن الدستور المصري في المادة 45 نص صراحةً على : "إن لحياة المواطنين الخاصة حرمة يحميها القانون" كما تعرض الدستور القطري الصادر في عام 2003 في المادة 37 للخصوصية حيث اعتبر" أن لخصوصية الإنسان حرمتها ، فلا يجوز تعرض أي شخص، لأي تدخل في خصوصياته أو شؤون أسرته أو مسكنه أو مراسلاته أو أية تدخلات تمس شرفه أو سمعته، إلا وفقاً لأحكام القانون وبالكيفية المنصوص عليها فيه".

بما يدل على أن الدستور القطري جاء متوافقاً مع مبدأ حماية الخصوصية وتنظيم إمكانية التعرض لها قانوناً، فتطور مفهوم البيانات الشخصية بالمعنى التقني جعل المشرع يفرد لها قوانين وتشريعات خاصة بحيث كلما تطورت التكنولوجيا ازداد حجم الحاجة إلى قوانين خاصة تنظم تنوع الاستخدامات، وهو ما أخذ به المشرع القطري عندما أصدر القانون رقم 13 لسنة 2016 بشأن حماية خصوصية البيانات الشخصية وكذلك القانون المصري رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات.

ولقد أحسن المشرع القطري بتنظيم تلك الظاهرة بما يوازن كافة الاعتبارات منها فلم ينكر حق التعبير وحرية الرأي أو ينكر على مقدمي الخدمة طلب الربح ومزاولة أنشطتهم التجارية ودون مساس بالحق في البيانات الشخصية فأصدر القانون رقم (13) لسنة 2016 بشأن حماية خصوصية البيانات الشخصية لتكتمل منظومة الحماية بعدما أصدر قانون مكافحة الجرائم الالكترونية وقانون الاتصالات وقانون حماية المستهلك وقبل كل ذلك كانت البيانات الشخصية محمية وفق أحكام قانون المطبوعات والنشر بالقدر الذي كان يناسب المرحلة الزمنية وقت إصداره.

وعلى ذلك فإن هذا البحث سيتعرض إلى الحق في حماية البيانات الشخصية على مواقع التواصل الاجتماعي في القانون القطري وبعض من الأنظمة المقارنة والمسؤولية القانونية عن انتهاك هذا

الحق والقانون الواجب التطبيق والمحكمة المختصة بالنظر في هذه الانتهاكات بأنواعها والجزاء القانوني (المدني-الجنائي) عنه وذلك من خلال تناول عناصر البحث بالقدر الكافي لإيضاح الغاية والفكرة الأساسية للموضوع.

منطلقات البحث ومحدداته.

1-أهمية موضوع الدراسة.

تأتي أهمية البحث من تعاظم دور وسائل التواصل الاجتماعي والتطور فائق السرعة للأجهزة الذكية والبرامج والتطبيقات المجانية وتعمد البعض إهمال وضع تنظيم قانوني يوازن بين الحق في التعبير واستخدام تلك المواقع وبين حماية وخصوصية البيانات الشخصية. ومن يقف خلف محاولات عدم وضع تنظيم قانوني هم أصحاب المصالح المالية من وراء تلك التطبيقات أو ذوي الأغراض السياسية التي تقف خلفها أجهزة أمنية لبعض الدول للحصول على بيانات المستخدمين في أي وقت تشاء [5].

كما تأتي أهمية البحث في ضرورة أن تحترم الكيانات التي تقدم خدمة مواقع التواصل الاجتماعي الحق في النسيان الرقمي المتفرع من الحق الشخصي في ألا تحتفظ بالبيانات بشكل أبدي في حالة هجر المستخدم حسابه على الموقع أو هجر الموقع من الأساس وأنه يلزم تنظيم هذا الحق بما يوازن بين حق الشركة في الحفاظ على عملائها ومستخدمي تطبيقاتها وبين الحق في النسيان الرقمي للبيانات الشخصية طالما انفصمت العلاقة بين صاحب البيانات ومقدمي الخدمة.

وتشير جل الدراسات التي تطرقت إليها إلى الخصوصية المعلوماتية في ضوء التحدي الذي يواجه المستخدم من إمكانية وصول الغير إلى ما ينشره ومسؤوليته القانونية عما ينشره وحقه في التعبير عن رأيه والوصول إلى الناس وكذلك حقه في النسيان الرقمي للبيانات الشخصية المتاحة على صفحته أو حسابه إذا ما ارتأى إلغائها أو إلغاء حسابه.

ومن أهم هذه الكتب التي تم الاطلاع عليها كتاب الدكتورة / مروة زين العابدين صالح بعنوان الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون

---

[5] China's Surveillance State Should Scare Everyone - The country is perfecting a vast network of digital espionage as a means of social control—with implications for democracies worldwide
https://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203/-- Dark Caracal: Global Espionage Malware from Lebanon https ://www.schneier.com.
مشار إلى هذه المراجع في: منى الأشقر جبور، محمود جبور، البيانات الشخصية والقوانين العربية، الهم الأمني وحقوق الأفراد، مرجع سابق، ص 31 وما بعدها.

الوطني ، الذي حاولت فيه تسليط الضوء على مفهوم الخصوصية المعلوماتية وأهميتها وكيفية معالجتها في التشريعات المقارنة واعتبرت أن حماية البيانات الشخصية في البيئة العربية لازالت تناقش في ظل القواعد العامة ، ومخاطر التقنيات الحديثة عليها في ظل التطور التكنولوجي وثورة الاتصالات والإنترنت ، وصور الجرائم الإلكترونية التي تهدد البيانات الشخصية عقب تداولها عبر الإنترنت[6].

وكتاب الدكتور / محمد سامي عبدالصادق بعنوان شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية الذي يدور موضوع بحثه حول رصد مظاهر التعدي على حرمة الحياة الخاصة لمستخدمي شبكات التواصل الناتجة عن ولع الأشخاص بالتواصل عبر الشبكات والتي يرى المؤلف أنها إشكالية قانونية يسعى الغرب إلى رصدها ومعالجتها واعتبر أن ما يزيد من صعوبة هذه الإشكالية كون شبكات التواصل صناعة أمريكية تستخدم في أوروبا وغيرها من البلدان ويوجد اختلاف بين النظرة الأمريكية للبيانات الشخصية لمستخدمي الشبكات والنظرة الأوروبية ؛ حيث تسيطر النظرة التجارية على المفهوم الأمريكي في تعامله مع البيانات ، في حين يسيطر الطابع الحمائي على المفهوم الأوروبي وأشار المؤلف إلى المفوضية الأوروبية في بروكسل التي أصدرت مشروع توجيه يهدف إلى تنظيم مسألة التعامل مع البيانات الشخصية لمستخدمي الإنترنت حيث نص في المادة 17 منه على حق مستخدمي شبكات التواصل في دخول حساباتهم في غياهب النسيان رقمياً مما يلزم مواقع التواصل التي تحوي البيانات الشخصية للمستخدمين محو هذه البيانات عند اختيارهم حذف حساباتهم ، في حين تحتفظ الولايات المتحدة الامريكية بهذه البيانات لفترة أطول لما لها من طابع تجاري، وفي ظل اختلاف موقف الأنظمة القانونية من التعامل مع البيانات حاول الباحث إقامة التوازن بين حرية التعبير عن الرأي والتواصل الاجتماعي عبر الإنترنت واحترام الحياة الخاصة[7].

وكتاب الدكتور / وسيم شفيق الحجار بعنوان النظام القانوني لوسائل التواصل الاجتماعي الذي تطرق إلى ضرورة إيجاد حل للمشكلة القانونية المتمثلة في إيجاد التوازن بين احترام خصوصية الأفراد وحريتهم في الرأي و التعبير وبين متطلبات الأمن ومصالح المجتمع العليا بالتسليم بوجود شرطين على حرية الرأي والتعرض للخصوصية هما: القانونية وعدم التعسف ، بأن يكون التعرض

---

[6] مروة زين العابدية صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، مرجع سابق، ص 14.

[7] محمد سامي عبد الصادق، شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية، دار النهضة العربية ،2016 ، ص 8-9.

لحقوق الفرد على شبكات التواصل منصوص عليه قانوناً وأن يكون واجباً لحماية مصالح المجتمع العليا لضمان عدم تعسف الشركات والسلطات العامة في استغلال قدراتها ونفوذها لجمع بيانات المستخدمين وانتهاك خصوصيتهم. كما اعتبر أن المسؤول قانوناً عما ينشر من معلومات هو المستخدم دون الوسطاء أي وسائل التواصل الاجتماعي لأن القول بعكس ذلك من شأنه أن يؤثر على حرية التعبير والابتكار[8].

واطلعت على كتاب الدكتور/ محمد نصر محمد بعنوان المسؤولية الجنائية لإنتهاك الخصوصية المعلوماتية الذي ميز بين الجريمة التقليدية والجريمة الإلكترونية وإن كان هناك تشابه بينهما في أطراف الجريمة من مجرم ذي دافع وضحية، إلا أن هناك اختلاف بينهما من حيث أداة ومكان الجريمة ، فالأداة في الجريمة الإلكترونية ذات تقنية عالية والمكان لا يتطلب انتقال الجاني إليه انتقالاً مادياً وإنما تتم باستخدام خطوط وشبكات الاتصال بين الجاني ومكان الجريمة مما يثير مشكلة الاختصاص على المستوى الدولي، فقد ترتكب الجريمة في إقليم دولة معينة من قبل أجنبي وهو ما يؤدي إلى تنازع الاختصاص القضائي [9].

2- أسباب اختيار الموضوع وأهدافه.

كانت من أهم أسباب اختيار موضوع البحث لما للإشكاليات الكثيرة التي ثار الجدل واللغط عليها بشأن حدود المسؤولية ونطاقها وأساسها فيما يخص المساس بالبيانات الشخصية على مواقع التواصل الاجتماعي وإحجام الكثير عن قبول فكرة وضع تنظيم قانوني يوازن بين اعتبارات مقدمي الخدمة والحق في حماية البيانات الشخصية.

كما أن من أسباب اختيار الموضوع مبادرة المشرع القطري لأن يخترق حصن المانعين للتنظيم القانوني لحماية البيانات الشخصية على مواقع التواصل الاجتماعي من خلال إصداره قانون حماية البيانات الشخصية وارسائه العديد من النظريات القانونية الحديثة التي تتماشى مع المسؤولية عن انتهاك هذه البيانات وطبيعة مضمون العلاقة التي نشأ عنها المساس بتلك البيانات.

---

[8] وسيم شفيق الحجار، النظام القانوني لوسائل التواصل الاجتماعي، دراسة قانونية مقارنة حول الحرية الشخصية والمسؤولية والاختصاص ، المركز العربي للبحوث القانونية والقضائية ط1 لبنان 2017 ، ص134.

[9] محمد نصر محمد، المسؤولية الجنائية لانتهاك الخصوصية المعلوماتية دراسة مقارنة، مركز الدراسات العربية للنشر والتوزيع ، الطبعة الأولى سنة 1437ه-2016م ، ص 8 ، 113.

3-تساؤلات الدراسة.

تستلزم هذه الدراسة مواجهة المشكل القانوني الرئيسي الذي يقابلها وهو تحديد الطرف المسؤول عن انتهاك خصوصية البيانات المتاحة عبر الشبكة العنكبوتية العابرة للحدود أمام تعدد الأطراف الداخلة في الاطلاع على هذه البيانات ابتداءً من مزود خدمة الإنترنت وصاحب الموقع والمستخدم ومستضيف البيانات من الغير الذين يضيفهم المستخدم، فتحديد الجهة المسؤولة يوضح التزامات الأطراف في العلاقة ومن ثم يسهل إيجاد التكييف القانوني لنوع المسؤولية الناشئة عن الأضرار فيما إذا كانت عقدية ناشئة عن علاقة تعاقدية أم تقصيرية يكون الخطأ فيها مفترضاً وسنحاول حل هذا المشكل في ضوء الإجابة على كثير من التساؤلات منها ما يتعلق بالمقصود بالبيانات الشخصية على مواقع التواصل الاجتماعي؟ وكذلك الحد الفاصل بين الحق في استخدام مواقع التواصل الاجتماعي وبين الحق في حماية البيانات الشخصية؟ وهل لا يزال الأساس القانوني التقليدي قادراً على حمل فكرة المسؤولية عن انتهاك البيانات الشخصية على مواقع التواصل الاجتماعي؟ والجزاء القانوني عن هذه الانتهاكات وهل للانتهاكات في مجال التقاضي الطبيعة السيادية في الاختصاص القضائي أو التشريعي أم أن فكرة تنازع القانون تجد في شأنها سبيلاً فيما يخص العلاقات المدنية والتجارية خلاف الثابت من اختصاص قضاء الدولة الداخلي من نظر الانتهاكات التي تشكل فعل اجرامي وتطبيق قانون العقوبات لديه وفق مبدأ إقليمية القوانين؟

4-صعوبات الدراسة.

طريق هذا البحث كحال الدراسات الإنسانية والعلمية، ليس هيناً سهلاً على الباحث إنما تعترض البحث بعض الصعوبات التي يلزم على الباحث التغلب عليها حتى يصل إلى مآربه وهدفه في أن يجد فكرة حديثة في العلوم الإنسانية تم معالجتها وفق الأسس العلمية الصحيحة.

وقد صادف الباحث بعض الصعوبات منها ما يتعلق بالمراجع العلمية المحدودة على مستوى التشريعات العربية بصفة عامة وعدم تناول الموضوع بالنسبة للتشريع القطري لحداثة صدور قانون حماية البيانات الشخصية كما هناك عبء على الباحث فيما يتعلق بضبط فكرة البحث حتى لا تخرج عن الغاية منها وتبعد الباحث عن الدخول في الجانب التقني للموضوع، وكذلك التصدي لكل عناصر البحث بالقدر الذي يبين الفكرة الأساسية له والأفكار المؤدية لما يشمله من عناصر على ألا يخرج البحث عن الحد المقرر من اللجنة العلمية للإشراف.

5- منهج الدراسة.

تعتمد الدراسة على أصول البحث العلمي ومناهجه الصحيحة[10]، والتي وإن تعددت تقسيماته إلا أنها ترد إلى أصل واحد[11]، وتُشتق كلمة منهج من النهج، أي سلك طريقاً معيناً، وأن نوع المنهج يرتهن بظروف خارجية أكثر منها إرادية، ترد الى مسألة البحث ذاتها[12]، ولقد تضمنت هذه الدراسة عدة مناهج من البحث العلمي، ساهمت كثيراً في الوصول إلى الأهداف وارتباط سياق الموضوع.

وقد استعان الباحث بالمنهج الاستنباطي والذي يُقصد به ربط العقل للمقدمات والنتائج بالأشياء وعللها على أساس المنطق والتأمل الذهني، من أن يبدأ الباحث بالكليات ليصل منها للجزئيات [13]، وكان أثر هذا المنهج واضحاَ في تناول التأصيل الدستوري والتشريعي والإطار القانوني لحماية البيانات الشخصية في النظام القانوني القطري وكما كان جلياً في بيان مدى صلاحية النظرية التقليدية لعناصر المسؤولية المدنية بصورها المختلفة في حمل المسؤولية عن المساس بالبيانات الشخصية على مواقع التواصل الاجتماعي.

كما أن الباحث قد استعان بالمنهج الاستقرائي وهو يمثل في مضمونه عكس سابقه، حيث بدأ الباحث بالجزئيات ليصل منها إلى العموم، بالاعتماد على التحقق من الملاحظات الخاضعة للتجريب والتحكم في المتغيرات المختلفة[14]، وكان لهذا المنهج أثراً في تناول تحديد المقصود بالبيانات الشخصية وماهية مواقع التواصل الاجتماعي وحرية التعبير والرأي وأثره على حماية البيانات الشخصية وأشكال وصور الانتهاكات للبيانات والاضرار المترتبة عن ذلك والجرائم التي يمكن تكوين نماذجها على هذا الانتهاك وعندما طرقنا أبواب التاريخ لم يكن ولوج تلك الأبواب إلا بالمنهج التاريخي الذي يعتمد على سرد أحداث وحلول الماضي ليتحقق ويُستخلص منها تجاربها ثم تحليلها

---

[10] أنظر:أحمد بدر، أصول البحث العلمي ومناهجه، ط5، المكتبة الأكاديمية، القاهرة ،1996، ص 18 ، عبد الرحمن بدوي، مناهج البحث العلمي، وكالة مطبوعات الكويت 1977، ص5، أحمد شلبي، كيف تكتب بحثاً أو رسالة، مكتبة النهضة المصرية ،1968، ص13.

[11] أحمد بدر، أصول البحث العلمي ومناهجه، المرجع السابق ص28.

[12] أحمد بدر، أصول البحث العلمي ومناهجه، المرجع السابق، ص24.

[13] عبد الرحمن بدوي، مناهج البحث العلمي، ص18.

[14] عبد الرحمن بدوي، مناهج البحث العلمي، المرجع السابق، ص18.

لاكتشاف أثرها [15]، وأثرها كان في تطور حماية البيانات الشخصية عبر التاريخ وفق الوعاء الذي يتضمنها ومدى اتصال الغير بها[16].

6-خطة الدراسة _ بدأها الباحث بالفصل التمهيدي – وموضوعه البيانات الشخصية في العالم الافتراضي.

وفي الفصل الأول من البحث نتناول المسؤولية القانونية لأصحاب وسائل التواصل الاجتماعي، وفي الفصل الثاني سنتناول الإطار القانوني والتنظيمي لحماية البيانات ذات الطابع الشخصي.

[15]عبد الرحمن بدوي، مناهج البحث العلمي، مرجع السابق، ص19.
[16]عبد الرحمن بدوي، مناهج البحث العلمي، مرجع السابق ص19.

الفصل التمهيدي: البيانات الشخصية في العالم الافتراضي

الحماية القانونية للبيانات الشخصية ليست مسألة حديثة العهد على القانون بأفرعه المختلفة إنما تصدت لها الأنظمة القانونية المختلفة منذ أواخر القرن العشرين[17] وأن ما يميز المواجهات القانونية القديمة والحديثة لا تتعلق بالبيانات الشخصية في حقيقتها إنما ترتبط بالوعاء الذي توجد به هذه البيانات حيث كانت البيانات الشخصية مأواها الوحيد الدفاتر الورقية.

وبعد ظهور الانترنت ومواقع التواصل الاجتماعي في الوقت الحالي أًصبح الوعاء الذي توجد به البيانات الشخصية يختلف عن الاوعية التقليدية ولا تستطيع المواجهات القانونية التقليدية التصدي له نظراً للطبيعة الخاصة لهذا الوعاء الافتراضي والتداخلات بين الحقوق الشخصية حيث أن حماية البيانات الشخصية من الحقوق المتعلقة بالحق الشخصي الذي دائماً ما يصطدم مع الحق في الرأي والتعبير الأمر الذي يلزم المشرعين بالتصدي لحماية البيانات ذات الطابع الشخصي على مواقع التواصل الاجتماعي بما يتماشى مع طبيعة الظاهرة- وهذا ما انفرد به المشرع القطري عندما ولى وجهه شطر حماية البيانات الشخصية بموجب القانون رقم 13 لسنة 2016 وكذلك الاتحاد الأوروبي الذي قام بتعديل الوثيقة الخاصة بحماية البيانات الشخصية في عام2016 [18] لتكون قادرة على مواجهة ظاهرة انتهاك البيانات الشخصية على مواقع التواصل الاجتماعي.

كما أن هناك اتجاه دولي واقليمي إلى إقرار الحق في النسيان الرقمي للبيانات الموجودة بمواقع التواصل الاجتماعي بما لا يتداخل أو يتعارض مع الحق في التعبير بحيث يكون للمستخدم طلب حذف بياناته في أي وقت طالما لم تتعلق بحقوق الاخرين[19].

وفي هذا الفصل التمهيدي سنبين على قدر المستطاع المقصود بالبيانات الشخصية وطريقة تجميعها وتحليلها وطبيعتها القانونية (المبحث الأول) ثم سنبين ماهية مواقع التواصل الاجتماعي وأنواعها

---

[17] قامت فرنسا بتنظيم قانونها القائم رقم 78-17 الصادر في 6 يناير عام 1978 المتعلق بالمعلوماتية والحريات الذي وضع المبادئ الأساسية للحماية وهي الاستقامة في جمع المعلومات والتصريح من غاية الجمع والتحليل وانشاء إدارة أو هيئة مستقلة تسهر على تطبيق هذا القانون. أشارت إليه: مروة زين العابدية صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، مرجع سابق، ص 143.

[18] بدء العمل بقانون حماية البيانات الشخصية في 2016/5/25- وهو النظام الذي الزم مواقع التواصل وشبكة الانترنت بشكل عام ببحث إرادة المستخدم في جمع وتحليل بياناته والموافقة الصريحة والمتبصرة لاستغلال بياناته مع وجود جزاءات صارمة تصل الى نسبة 4% من اجمالي الأرباح العالمية. مرجع سابق، ص139.

[19] وسيم شفيق الحجار، النظام القانوني لوسائل التواصل الاجتماعي، مرجع سابق، ص92.

وخصائصها وتعلقها بالحقوق الشخصية من حرية التعبير والحق في حماية البيانات الشخصية (المبحث الثاني) ثم نوضح الحق في النسيان للبيانات ذات الطابع الشخصي والقيود التي ترد على هذا الحق (المبحث الثالث).

المبحث الأول: البيانات الشخصية بين الماهية والتأصيل

لئن كانت ثورة التواصل التي حدثت في مواقع التواصل الاجتماعي على العالم الافتراضي أتاحت للبشرية تقدماً وتواصلاً فعالاً وسريعاً، إلا أن مخاطر تلك المواقع سرعان ما ظهرت نتيجة ما يسمى بمعالجة البيانات ذات الطابع الشخصي التي تستخدم في أغراض اقتصادية وتجارية وسياسية وغيرها، حيث تبدأ عملية تجميع البيانات من خلال بيانات تسجيل المستخدم التي يقوم بوضعها على البرامج بشكل مباشر أو بطريقة غير مباشرة من خلال التعرف على عنوان المستخدم (IP)، نوع الموديم، نوع الحاسوب والمعالج والوقت الذي تقضيه متصلاً بالإنترنت، معلومات البطاقة المصرفية والذي به يتم التعرف على بلد المستخدم والجهاز المستخدم وشركة الانترنت المقدمة للخدمة وكذلك يتم التعرف على البيانات الشخصية من خلال ملفات تسمى (ملفات تعريف الارتباط- COOKIES) ويقصد بها الملفات النصية الصغيرة (المعلومات) التي يتم تخزينها من قبل متصفح الويب الخاص بالمستخدم عن الإجراءات التي أنجزت سابقاً على موقع ما على الإنترنت ترسلها شبكات الاتصال الخاصة بالمواقع التي نقوم بزيارتها وتسمح للموقع بالتعرف وتسجيل بيانات الدخول الشخصية والصفحات التي قمت بزيارتها والأزرار التي نقرت عليها وغيرها من التفاصيل، وكذلك هناك طريقة أخرى للحصول على البيانات الشخصية من خلال برامج خفية في مواقع التواصل الاجتماعي تعمل على رصد حركات النسخ أو التصفح أو تحميل ورفع الصور وهذه البرامج الخفية تدعى (الويب باجز-WEB BUGS) – بحيث يتم بالطرق المشار إليها تجميع ومعالجة البيانات الشخصية على مواقع التواصل الاجتماعي[20].

وتلجأ مواقع التواصل الاجتماعي لتلافي الانتقادات الموجهة اليها أو الملاحقات القضائية المتعلقة بتجميع البيانات واستغلالها إلى وضع سياسات عند بدء التسجيل وطلب الخدمة على موقعها كشرط للتسجيل منها سياسة للخصوصية (PRIVACY POLICY) وسياسة الاستخدام (USAGE POLICY).

[20] مروة زين العابدية صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، مرجع سابق، ص 333.

ولذلك سيتم التطرّق فيما يلي إلى تعريف البيانات الشخصية على مواقع التواصل الاجتماعي (فرع أول) وكيفية معالجة هذه البيانات الشخصية والقيود على التحليل (فرع ثاني) وطبيعة البيانات الشخصية على مواقع التواصل الاجتماعي (فرع ثالث).

المطلب الأول: تعريف البيانات ذات الطابع الشخصي.

عرّف المشرع القطري البيانات الشخصية في المادة (1) من قانون حماية البيانات الشخصية بأنها: "بيانات عن الفرد الذي تكون هويته محددة، أو يمكن تحديدها بصورة معقولة، سواء من خلال هذه البيانات أو عن طريق الجمع بينها وبين أية بيانات أخرى".

ويُعرف البعض البيانات الشخصية بأنها كل معلومة تتعلق بشخصي طبيعي معين أو يمكن تعيينه بصورة مباشرة أو غير مباشرة عن طريق الرجوع إلى رقم الهوية أو إلى واحد أو أكثر من العناصر المميزة له بحيث تعد بيانات ذات طابع شخصي ما يستلزم موقع التواصل الاجتماعي من طالب التسجيل وضعه من بيانات خاصة ، فطالب التسجيل في موقع الفيسبوك مثلاً يتعين عليه أن يضع بياناته الشخصية كالاسم والعائلة وعنوان البريد الالكتروني وكلمة المرور ونوع الجنس وتاريخ الميلاد ومهنته وخبرته العملية وبطاقة الائتمان والعقيدة الدينية وافكاره السياسية وميوله الاجتماعية وقد تتطلب بعض المواقع بيانات عن أفراد أسرته وأصحابه[21].

فالبيانات الشخصية هي البيانات والمعلومات التي تتعلق بشخص طبيعي أو اعتباري محدد ومعروف أو قابل للتعريف عن طريق تلك البيانات والتي تستخدم لتمييز الشخص عن غيره وتحديد هويته سواء كانت تلك البيانات دقيقة أم غير دقيقة، تعد في حد ذاتها بياناً أو تحتاج إلى معلومات إضافية للتوضيح سواء كانت في شكل مادي أم إلكتروني وكل بيان أو معلومة يعبر عن الحالة العقلية، الصحية، الثقافية، الاجتماعية أو المهنية وكل ما يرتبط بالشخص ومعاملاته وآراء الغير فيه تعد بيانات شخصية.

وقد حكمت محكمة ولاية كاليفورنيا العليا في العاشر من فبراير 2011 بإدانة موظف البنك الذي تحرى عن الرقم البريدي بخصوص تعاملات تجري على البطاقة الائتمانية واعتبر الرقم البريدي من بيانات التعريف الشخصي والتي تدخل تحت مظلة حماية البيانات الشخصية[22].

---

[21] مروة زين العابدية صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، مرجع سابق، ص 67.

[22] مروة زين العابدية صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، مرجع سابق، ص 67-68.

ومع أهمية حماية البيانات الشخصية، إلا أن تلك الأهمية تتجلى في حالة القاصر والمفقود والميت لما من عدم امتلاك هؤلاء إلى حماية بياناتهم من أُثر على حياة القاصر الخاصة أو سمعة المتوفي وورثته وحياته الخاصة التي يلزم دفنها معه عند الموت ، حيث يلزم الحصول على إذن كتابي ممن له الولاية على القاصر حتى ولو تعلق الأمر بنشر صورة طفل على موقع المدرسة عبر الإنترنت ، وكذلك الأمر بالنسبة للمتوفى يحق لورثته المعارضة في نشر بياناته الشخصية إذا كان من شأن نشرها الإعتداء على كرامته[23].

.

المطلب الثاني: معالجة البيانات الشخصية على العالم الافتراضي.

عرّف المشرّع القطري في المادة (1) من قانون حماية البيانات الشخصية معالجة البيانات الشخصية أنها: " إجراء عملية أو مجموعة عمليات على البيانات الشخصية، كالجمع والاستلام والتسجيل والتنظيم والتخزين والتهيئة والتعديل والاسترجاع والاستخدام والإفشاء والنشر والنقل والحجب والتخلص والمحو والإلغاء".

ويعرف البعض معالجة البيانات الشخصية بأنها كل عملية أو مجموع العمليات التي تجرى على هذه البيانات دون النظر عن الوسيلة المستخدمة، وبوجه خاص الجمع والتسجيل والتنظيم والحفظ (التخزين) والتحريف والتعديل والاسترجاع والفحص والاستخدام والنقل والنشر أو أي شكل آخر للإتاحة والتقريب والتوصيل وكذلك الغلق والمحو والإتلاف[24] – وهو ذات المضمون الذي أخذ به المشرع القطري.

وقد نصت المادة (4) من قانون حماية البيانات القطري على أنه: "لا يجوز للمراقب معالجة البيانات الشخصية، إلا بعد الحصول على موافقة الفرد، ما لم تكن المعالجة ضرورية لتحقيق غرض مشروع للمراقب أو الغير الذي تُرسل إليه البيانات".

كما نصت المادة (5) من ذات القانون على أنه: " يجوز للفرد، في أي وقت، الاعتراض على معالجة بياناته الشخصية إذا كانت غير ضرورية لتحقيق الأغراض التي جمعت من أجلها، أو كانت زائدة على متطلباتها، أو تمييزية أو مجحفة أو مخالفة للقانون".

---

[23] محمد أحمد المعداوي، حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي، دراسة مقارنة، بحث منشور بالمجلة العلمية، كلية الحقوق جامعة بنها، ص 85.

[24] محمد سامي عبد الصادق، شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية، مرجع سابق، ص 43.

كما نصت المادة (8) من قانون المعلوماتية الفرنسي على أنه: " يحظر جمع أو معالجة البيانات ذات الطابع الشخصي، والتي من شأنها أن تكشف بشكل مباشر أو غير مباشر عن الأصول العرقية أو الآراء السياسية أو الفلسفية أو العقيدة الدينية أو الانتماء النقابي للشخص أو التي تتعلق بصحته أو بحياته الجنسية"[25]. ويؤخذ من الأحكام التي أخذ بها المشرعان القطري والفرنسي أن جمع البيانات الشخصية للمستخدم ليس محظورا بذاته، إنما يقع الحظر على الجمع الذي يتم بطريق غير مشروع كالتدليس أو ذلك الذي يتم بالرغم من اعتراض صاحب هذه البيانات، ويعتبر المشرع القطري جمع البيانات بطريق التدليس أو بعد اعتراض صاحب البيانات جريمة جنائية [26].

وتقوم مواقع التواصل الاجتماعي بجمع وحفظ ثلاث أنواع من البيانات التي يضعها المستخدم، وهي البيانات ذات الطابع الشخصي، وبيانات الاتصال بالإنترنت (كعناوين الهوية IP) وأخيرا بيانات التصفح المتعلقة بالمواقع التي يتصفحها المستخدم مع الأخذ في الاعتبار أن اطلاع موقع التواصل على البيانات التي يضعها الشخص على الموقع ليس فيها ممارسات غير مشروعة اللهم إلا إذا استغلت هذه البيانات بعد معالجتها بموافقة المستخدم في أغراض أخرى لا يعلم عنها المستخدم.

ولقد فطن المشرع القطري إلى ضرورة أن تكون معالجة البيانات في الوضع العادي للأمور بموافقة المستخدم واطلاعه على عملية المعالجة حيث نصت المادة (9) من قانون حماية البيانات الشخصية على أنه: "على المراقب، قبل البدء في معالجة أية بيانات شخصية، أن يُعلم الفرد بما يلي:- 1- بيانات المراقب، أو أي طرف آخر يتولى معالجة البيانات لصالح المراقب أو لاستغلالها من قبله، 2- الأغراض المشروعة التي يرغب المراقب أو أي طرف آخر في معالجة البيانات الشخصية من أجلها-3-الوصف الشامل والدقيق لأنشطة المعالجة ودرجات الإفصاح عن البيانات الشخصية للأغراض المشروعة، وإذا لم يتمكن المراقب من ذلك ، فيتعين عليه تمكين الفرد من وصف عام لها، 4-أية معلومات أخرى تكون ضرورية ولازمة لاستيفاء شروط معالجة البيانات الشخصية ".

---

[25] محمد سامي عبد الصادق، شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية، دار النهضة العربية، مرجع سابق، ص 44.

[26] تنص المادة (23) من قانون حماية البيانات القطري على أنه: " مع عدم الإخلال بأي عقوبة أشد ينص عليها قانون آخر، يعاقب بالغرامة التي لا تزيد على 1000,000 مليون ريال، كل من خالف أياً من أحكام المواد (4)، (8)، (9)، (10)، (11)، (12)، (14)، (15)، (22) من هذا القانون"، وكذلك المادة 18/226 من قانون العقوبات الفرنسي الذي يعاقب على جمع البيانات بطريق التدليس بالسجن لمدة خمس سنوات وغرامة ثلاثمائة يورو. مرجع سابق، ص 45.

وقد اهتمت الدول الأوروبية بوضع تشريعات تكفل معالجة البيانات بما يضمن حمايتها وكانت فرنسا من رأس هذه الدول حيث صدر في 7 إبريل سنة 1978 قانون المعلوماتية والسجلات والحريات " الذي لا يجيز إجراء معالجة البيانات بالمعنى المتقدم بغير رضاء صاحب هذه البيانات وهذا الرضاء يجب أن يكون صادراً من المستخدم بإرادة وحرية اختيار غير مشوبة بأي عيب من عيوب الإرادة وأن يكون محدداً وأن يكون على بصيرة وعلم من غرض طلبها وتجميعها"[27].

ويلتزم مقدم الخدمة أو مالك موقع التواصل الاجتماعي أن يخطر المستخدم بأي انتهاك للبيانات ذات الطابع الشخصي وإخطار السلطة المختصة في الدولة بذلك الانتهاك لتفرض الجزاء الملائم على من قام بذلك، فعلى سبيل المثال نصت المادة (14) من قانون حماية البيانات الشخصية القطري على أنه: "يجب على المراقب إعلام الفرد والإدارة المختصة، بحدوث أي إخلال بالاحتياطات المنصوص عليها في المادة السابقة، إذا كان من شأن ذلك إحداث ضرر جسيم بالبيانات الشخصية أو بخصوصية الفرد" ، علماً بأن المراقب حسب تعريف المادة الأولى من قانون حماية البيانات القطري هو: " الشخص الطبيعي أو المعنوي الذي يقوم منفرداً أو بالاشتراك مع آخرين بتحديد كيفية معالجة البيانات الشخصية والغرض منها".

وعلى ذلك فإنه يجب على مواقع التواصل الاجتماعي مراعاة عدة ضوابط في معالجة البيانات ذات الطابع الشخصي منها الالتزام بالأمانة والمشروعية في جمع هذه البيانات والتقيد بالغرض من جمع هذه البيانات وعدم التوسع فيه بما يجاوز هذا الغرض، وأن يكون للمستخدم حق الدخول اليها وتصحيحها في أي وقت، والالتزام بضمان سرية البيانات التي يتم جمعها، وكذلك تمكين أي شخص من الاعتراض دون مقابل على ما قد يتداوله على الانترنت من بيانات تتعلق بحياته الخاصة.

كما يلتزم مقدمو خدمة التواصل الاجتماعي باحترام خصوصية البيانات الشخصية لمستخدميه وبأن لا يستخدموا هذه البيانات في أغراض إعلانية أو ربحية كما يفعل موقع التواصل الاجتماعي الفيسبوك الذي يقوم بتحليل بيانات المستخدمين لاستغلالها في أغراض تسويقية من خلال الإعلانات الاجتماعية التي تقوم بتحليل بيانات وأذواق المستخدمين لبيعها للشركات بغرض تحديد المنتجات كثيفة الطلب مع إرشاد الشركات إلى توجيه منتجاتها إلى من يرغب فيها، وعلى ذلك فإن البيانات الشخصية تعد مورداً مالياً هاماً لمواقع التواصل الاجتماعي تستغلها في الحصول على مبالغ طائلة من المعلنين مقابل تقديمها لهم باعتبارها قاعدة بيانات تكشف عن ميول واهتمامات المستخدمين ، ومن أهم هذه البيانات على سبيل المثال السن والجنسية والحالة العائلية ومحل الإقامة والميول

---

[27] محمد سامي عبد الصادق، شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية، مرجع سابق، ص 45.

الاجتماعية والشخصية والهوايات وهي جميعاً بيانات شخصية تخضع معالجتها لشروط معالجة البيانات ذات الطابع الشخصي والتي تتمثل في الرضا المحدد والصريح المتبصر للمستخدم[28].

إنّ مخاطر هذه الإعلانات تفوق مكاسبها الربحية لأنها تؤدي إلى انشاء ملفات شخصية لإدراج إعلانات منتظمة لمستخدمي الإنترنت على غير إرادة منهم كما أنها قد تؤدي إلى جعل الملفات الشخصية للمستخدمين بمثابة سلعة تجارية بين مواقع التواصل الاجتماعي والمعلنين- مثال ذلك ما قامت به إدارة الفيسبوك من إقرار نظام جديد يدعى "بيكون" وهو نظام يهدف الى ظهور إعلانات لمنتجات الشركات والمواقع المتعاقدة مع الفيسبوك بصورة تلقائية على صفحات المستخدمين وأصدقائه[29].

وغني عن الذكر أنّ إدارة الفيسبوك لا تتحقق من رضاء المستخدم حيث أن المستخدم عند التسجيل لا يعطي بياناته بغرض التسويق والاعلان ولم يتم تبصيره بما تم من تحليل لبياناته الشخصية. بل غاية ما في الأمر أن موقع الفيسبوك ينتهج عند التسجيل اظهار رسالة لحظية بأنه يمكن استخدام البيانات في أغراض إعلانية موجهة. وهي رسالة تقع ما بين قائمة شروط طويلة لا يقوم المستخدم بقراءة أول سطرين منها على الأقل، ولكن بعد كثرة الانتقادات وشدتها في عام 2007 على نظام "بيكون" قام الموقع بإظهار عبارة قبول الاشتراك على الإعلان لبيان رضاء المستخدم، دون أن يكون ذلك كافيا لأن العبارة ذاتها لا تظهر بوضوح للمستخدمين. وقد فطن المشرع القطري لذلك فجعل القاعدة العامة هي ضرورة حصول مقدمي الخدمة على رضاء العميل، إلا في الحالات المنصوص عليها حصرياً بالمادة (18) من قانون حماية البيانات الشخصية [30].

ولذلك فإنه يجب على مواقع التواصل الاجتماعي تخصيص رسالة منفصلة واضحة ومحددة عند التسجيل تتضمن إعلانه بأن بياناته الشخصية قد تستخدم في أغراض الإعلان أو في أغراض

---

[28] Marie FAGET, Les réseaux sociaux en ligne et la vie privée, mémoire, Université Paris II Panthéon Assas - Master 2 Droit du Multimédia et de l'Informatique 2008, p.33.

[29] عثمان بكر عثمان، المسؤولية عن الاعتداء على البيانات الشخصية عبر شبكات مواقع التواصل الاجتماعي، كلية الحقوق، جامعة طنطا، ص 18.

[30] نصت المادة 18 من قانون حماية البيانات الشخصية على أنه: "للجهة المختصة أن تقرر معالجة بعض البيانات الشخصية دون التقيد بأحكام المواد(4) ، (9) ،(15) ،(17) من هذا القانون، وذلك لتحقيق أي من الأغراض الآتية 1- حماية الأمن الوطني والأمن العام 2-حماية العلاقات الدولية للدولة 3-حماية المصالح الاقتصادية أو المالية للدولة 4-منع أي جريمة جنائية، أو جمع معلومات عنها، أو التحقيق فيها-وتحتفظ الجهة المختصة بسجل خاص تقيد به البيانات التي تحقق الأغراض المشار إليها ،ويصدر بتحديد شروط وضوابط وأحوال القيد في هذا السجل أوراق من الوزير".

أخرى، وإلا فإن أي شرط يدرج بهذا الشأن ضمن قائمة الشروط العامة للتسجيل للحصول على خدمات الموقع لا يعتد به ولا يمكن اعتباره تبصيراً للمستخدم.

المطلب الثالث: الطبيعة القانونية للبيانات الشخصية على مواقع التواصل.

قد ينظر إلى أن البيانات التي يتم تجميعها من موقع التواصل الاجتماعي ليست مملوكة لأصحابها، وإنما هي مملوكة لمن قام بتجميعها ومعالجتها وتحليلها [31]. وهذه النظرة تقترب من النظرة الامريكية لمفهوم البيانات التي يتم تجميعها حيث تتيح الولايات المتحدة لمن يقوم بمعالجة البيانات مساحة من استغلالها بما لا يتعارض مع حمايتها، وهو ما يخالف المبادئ المعتمدة للاتحاد الأوروبي بشأن البيانات ذات الطابع الشخصي[32].

ويرى أنصار الرأي الذي ينادي بعدم ملكية البيانات الشخصية للمستخدمين على أساس تغيير الطبيعة القانونية لها بعد قيام أصحابها بوضعها على مواقع التواصل، حيث أنها تتحول بعد تجميعها إلى أسرار تجارية محمية بموجب قوانين التجارة الخاصة بالأسرار التجارية كما أنها ليست ابتكار أو ملكية فكرية لكي تحميها قوانين الحق في الملكية الفكرية وكذلك فإن قواعد البيانات وما عليها من بيانات لها حمايتها الخاصة وفق الأنظمة الأوروبية بوصفها مملوكة لمقدمي الخدمات ويدلل أنصار هذا الرأي على تويتر كمثال حيث ينص في شروط الاستخدام عند الاشتراك أنه يجوز عند إعادة بيعه أو دمجه أو الاستحواذ عليه أو بيع أصوله بيع البيانات المجمعة أو نقلها[33].

وكذلك الأمر في موقع فيسبوك الذي يتضمن من شروط استخدامه أن يكون للعملاء مشاركة صورهم مع الإعلانات والمحتويات التجارية وفي حالة رفضهم عليهم ضبط الخصوصية، وإن كان ذلك لم يمنع موقع الفيسبوك من تجميع مليارات البيانات وانشاء سير ذاتية لعملائه يتم استغلالها

---

[31] وسيم شفيق الحجار، النظام القانوني لوسائل التواصل الاجتماعي، دراسة قانونية مقارنة حول الحرية الشخصية والمسؤولية والاختصاص، مرجع سابق، ص66.

[32] اعتبرت محكمة النقض الفرنسية أن تجميع البيانات الشخصية على الانترنت عمل غير مشروع، أنظر: وسيم شفيق الحجار، النظام القانوني لوسائل التواصل الاجتماعي، دراسة قانونية مقارنة حول الحرية الشخصية والمسؤولية والاختصاص، مرجع السابق ص66.

Cassation criminelle, 14/3/2006, n 05-83.423, JurisData n 2006-032892, note A. Lepage Com. Electro.

[33] Céline Castets Renard, Droit de l'Internet Droit français et européen, 2eme édition Montchrestien, Lextenso.2012 p.79.

انظر: وسيم شفيق الحجار، النظام القانوني لوسائل التواصل الاجتماعي، دراسة قانونية مقارنة حول الحرية الشخصية والمسؤولية والاختصاص، مرجع سابق ، ص 66.

واستخدامها بصورة لا يعلم عنها العملاء وكذلك الاحتفاظ بها حتى بعد انسحاب العملاء من الموقع بشكل نهائي بما يخالف الحق في النسيان الرقمي.

كما أن البيانات الشخصية لمستخدمي مواقع التواصل الاجتماعي أصبحت اليوم الأداة الأساسية لقياس مؤشرات الأسواق الاقتصادية والسلع اللازم انتاجها بل والأدوات الأساسية لإعادة رسم المحتوى السياسي وأنظمة الدول من خلال تتبع صفحات المستخدمين للوقوف على ميولهم السياسية والاجتماعية وأهوائهم مثل بعض ما وصلت اليه شعوب دول الربيع العربي أو قياس مدى ولائهم لدولهم[34]، بل إن تجميع البيانات وإعادة بيعها أصبحت الركيزة الأساسية للربح للشركات مالكة المواقع من خلال إعادة بيعها لمواقع الكترونية أخرى وهو ما تعكف عليه مواقع مثل الفيس بوك حيث تقوم بتجميع البيانات الشخصية ذات الميول الاقتصادية للشركات العالمية المتعلقة بالأنشطة المرتبطة بتلك البيانات بل تقوم بإعادة بيعها لمنظمات نشطة في مجالات سياسات الدول لها أغراضها الخاصة على سبيل المثال بيانات الفيس يقبلها أكثر من سبعة ملايين موقع حول العالم من خلال الدخول إلى الموقع بعد مصادقة الحساب على الفيسبوك[35] ولذلك لا يوجد في الحقيقة ما يسمى بمجانية البرامج لأنها تحول البيانات الشخصية إلى أموال من خلال تصنيفها وإعادة بيعها إلى المهتمين بها.

وتنص المادة (21) من النظام الأوروبي الجديد حول البيانات الشخصية لعام 2016 على أنه" "يعود للشخص المعني بالبيانات أن يعترض على معالجة بياناته الشخصية لأهداف الترويج التجاري والتي تتضمن إنشاء سيرة حوله لجهة ميوله وحاجاته (profiling) ويؤدي هذا الاعتراض إلى وقف المعالجة"[36].

---

[34] وسيم شفيق الحجار، النظام القانوني لوسائل التواصل الاجتماعي، دراسة قانونية مقارنة حول الحرية الشخصية والمسؤولية والاختصاص، مرجع سابق ، ص73.

[35] وسيم شفيق الحجار، النظام القانوني لوسائل التواصل الاجتماعي، دراسة قانونية مقارنة حول الحرية الشخصية والمسؤولية والاختصاص، مرجع سابق، ص 68.

[36] وسيم شفيق الحجار، النظام القانوني لوسائل التواصل الاجتماعي، دراسة قانونية مقارنة حول الحرية الشخصية والمسؤولية والاختصاص، مرجع سابق، ص 68.

وتعني كلمة (profiling) وفق المادة الرابعة من النظام الأوروبي حول البيانات الشخصية لعام 2016 أي شكل من المعالجة الآلية للبيانات الشخصية تتضمن استعمال البيانات الشخصية لتقييم بعض مظاهر أو جوانب الشخصية المتعلقة بشخص طبيعي، لاسيما لتحليل أو تنبؤ جوانب متعلقة بأداء الشخص في العمل، أو وضعه المالي أو الصحي أو أشيائه المفضلة أو اهتماماته أو سلوكه أو موقعه أو تنقلاته.

كما تعطي المادة (22) من ذات النظام الحق للشخص بألا يكون موضوع يستند فقط إلى معالجة آلية ومن ضمنها إعداد سيرة حوله والتي تنتج آثار قانونية في حقه أو تؤثر عليه بشكل كبير إلا إذا كان ذلك يتعلق بإنشاء أو تنفيذ عقد بين الشخص وبين المسؤول عن معالجة البيانات أو كان ذلك يجيزه القانون أو يستند إلى موافقة الشخص المعني الصريحة. وفي هذه الحالة يمكنه التدخّل لإبداء وجهة نظره والمنازعة في القرار.

وفي كل الأحوال نؤيّد الرأي الذي ينادي بحق المستخدم في إعلامه بحصول أي تحليل لتصرفاته على وسائل التواصل الاجتماعي وبالحصول على موافقته على ذلك وتمكينه من ابداء ملاحظاته ودفاعه بهذا الخصوص. إذ إنشاء سيرة ذاتية للشخص وتصنيفه في وقت معين ولفعل معين ضمن فئة معينة معدة مسبقاً ليس سيئاً دوماً بالضرورة مثل حالة توقع اهتماماته. ولكن التصنيف يصبح إشكالياً عندما يعمم ويتم أخذ القرارات المهمة على أساسه وذلك لأن هذا التصنيف لا يعكس إلا جانبا من شخصية الفرد وقد يكون مبنياً على معلومات تصنيف الأشخاص فالمتصفح لم يعد فرداً وإنما عنصر ضمن فئة محرومة من استقلالية قرارها ولهذا تكون حماية البيانات الشخصية من التصنيف المفرط للأشخاص هي شرط لا غنى عنه للحفاظ على الحياة الخاصة[37].

---

[37] قررت المفوضية الأوروبية التقدم باقتراح لتوفيق قانون حماية البيانات داخل الإتحاد الأوروبي، وقام البرلمان الأوروبي بتطبيق توجيه حماية البيانات الذي كان لزاماً نقله إلى القانون الوطني عام 1998م، ويحتوي التوجيه الأوروبي على عدد من المبادئ الأساسية التي يجب على أي شخص يقوم بمعالجة البيانات الالتزام بها: أن يتم معالجتها بشكل عادل قانوني ولأغراض محددة، وأن تكون المعالجة دقيقة، وأن يتم معالجتها وفقاً لحقوق صاحب البيانات، وأن يتم نقلها إلى الدول التي تتوفر لديها الحماية المناسبة. أشارت إليها : مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، مرجع سابق ص 141.

المبحث الثاني: المقصود بمواقع التواصل الاجتماعي

وسائل التواصل الاجتماعي هي إحدى منتجات العالم الافتراضي في الوقت الحالي وهي تمثل ثورة رقمية نتيجة استخدامها في نشر المعلومات، فالمستخدم يمكن له نشر برامج، أو مؤلفات، أو صفقات تجارية على صفحات الويب والتواصل مع أقاربه، والتنقل بين أرجاء العالم، الأمر الذي جعل هذه الشبكات ذات طبيعة عالمية.

ويقتضي التواصل الاجتماعي عبر هذه الشبكات وجود أجهزة مترابطة تستخدم لتدفق المعلومات والإنترنت هو السبب الرئيسي في ظهور مواقع التواصل الاجتماعي، وتحويل المستخدم السلبي إلى مستخدم نشط من خلال التفاعل مع الاخرين والقدرة على إنشاء معلومات ومحتوى مع الاخرين.

ولقد عرفت اللجنة الاقتصادية والاجتماعية الاوروبية وسائل التواصل الاجتماعي بأنها: "خدمات على الانترنت تهدف إلى انشاء مجموعات من الأشخاص وإلى الربط بينهم حيث يتشارك هؤلاء الأشخاص نشاطات أو اهتمامات مشتركة أو يرغبون في معرفة الأشياء المفضلة أو نشاطات الأشخاص الاخرين وتضع هذه الخدمات بتصرف هؤلاء مجموعة من الوظائف تسمح بالتفاعل بينهم" [38].

وتعرف وسائل التواصل الاجتماعي أيضاً بأنها ديناميكية دائمة التطور لتلبية حاجات المستخدمين وأهداف مالكيها وللتنافس مع بعضها وقد أصبحت الاداة التي ينظم الناس من خلالها حياتهم والتي غيرت الطريقة التي يتواصل من خلالها الناس وأدت إلى إنشاء ثقافة جديدة هي ثقافة المشاركة والتفاعل على المستوى الفردي والمجتمعي[39].

المطلب الأول: ماهية وسائل التواصل الاجتماعي.

ولقد عرّف المشرع القطري الاتصالات السلكية واللاسلكية بأنها: "إرسال، أو بث أو استقبال الإشارات أو الرموز أو الصور أو الأشكال أو الأصوات أو البيانات أو النصوص أو المعلومات، أياً كان نوعها أو طبيعتها، عن طريق الوسائل السلكية أو اللاسلكية أو الراديوية أو البصرية، أو غيرها من وسائل الاتصالات الكهرومغناطيسية، أو بأية وسائل اتصالات أخرى مشابهة"[40].

---

[38] وسيم شفيق الحجار، النظام القانوني لوسائل التواصل الاجتماعي، دراسة قانونية مقارنة حول الحرية الشخصية والمسؤولية والاختصاص، المرجع السابق ص 15.

[39] Guillaume Florimond, Droit et Internet De la logique internationaliste à la logique réaliste, Bibliothèque des thèses, Editions Mare & martin 2016, p340-.143

[40] قانون رقم (13) لسنة 2016 بشأن حماية خصوصية البيانات الشخصية.

كما عرف المشرع الكويتي التواصل الالكتروني بأنه: "كل تواصل على الشبكة المعلوماتية من خلال عنوان محدد وإلكتروني وأنه كل ما يتصل بتكنولوجيا المعلومات وذو قدرات كهربائية، أو رقمية، أو مغناطيسية، أو بصرية، أو كهرومغناطيسية، أو وسائل أخرى مشابهه سلكية أو لا سلكية وما قد يستحدث من تقنيات في هذا المجال"[41].

ومن تلك التعريفات فإن التواصل الاجتماعي عبر شبكة الانترنت لا يخرج عن كونه اتصال عبر وسيط افتراضي من خلال استقبال إشارات، أو رموز، أو صور، أو أشكال، أو أصوات، أو بيانات، أو نصوص، أو معلومات عن طريق وسيلة سلكية أو لاسلكية أو كهرومغناطيسية أو بصرية، ويتميز هذا التواصل بعدة خصائص منها: -

1-العالمية: تلغى الحواجز الجغرافية والمكانية، وتتحطم فيها الحدود الدولية، حيث يستطيع الفرد في الشرق التواصل مع الفرد في الغرب، في بساطة وسهولة.

2- التفاعلية: من أنها قدرة وسيلة الاتصال الجديدة على الاستجابة لحديث المستخدم كما يحدث في عملية المحادثة بين شخصين، فالفرد فيها كما أنه مستقبل وقارئ، فهو مرسل وكاتب ومشارك، فهي تلغي السلبية المقيتة في الاعلام القديم (التلفاز والصحف الورقية) وتعطي حيز للمشاركة الفاعلة من المشاهد والقارئ.

3-إعلام متعدد الوسائط: فلقد أحدثت ثورة نوعية في المحتوى التواصلي الذي يتضمن على مزيج من النصوص والصور وملفات الصوت ومقاطع الفيديو، هذا المحتوى متعدد الوسائط انتشر بشكل كبير، وكانت له تأثيرات اجتماعية وسياسية وتجارية حيث أصبح التواصل عبر الشبكة العنكبوتية وسيلة ذات تأثير واضح وسريع على السوق التجاري وسعر العملة والدولار في كثير من الدول ففي دولة مثل ليبيا وما تمر به من أحداث عقب ثورة فبراير وحرية استخدام الفيس بوك تنشر الكثير من القرارات السياسية والمراسيم الرئاسية من خلال فيس بوك مما يغير سعر صرف الدولار وشرائه بالنسبة للدينار الليبي فينعكس على سعر السلعة ومن ثم ظروف المواطن الاقتصادية والمعيشية في عجلة متسارعة تنشئها سرعة استخدام مواقع التواصل التي من الممكن أن لا نقتصر على اعتبارها وسيلة تواصل اجتماعي فحسب بل وسيلة اقتصادية وسياسية أيضاً.

5-المجانية: اقتصادية في الجهد والوقت والمال، في ظل مجانية الاشتراك والتسجيل، فالفرد العادي البسيط يستطيع امتلاك حيز على الشبكة للتواصل الاجتماعي، وليست حكرًا على جماعة دون أخرى من أصحاب الأموال.

---

[41] القانون الكويتي رقم 63 لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات.

6-الحرية المطلقة: حيث أن مواقع التواصل الاجتماعي جعلت بإمكانية أي شخص لديه الاتصال بشبكة الانترنت أن يكون ناشراً وأن يوصل رسالته إلى جميع أنحاء العالم، وهناك العديد من الأخبار التي يمكن لمستخدميها مناقشة أي موضوع يخطر على بالهم مع عدد غير محدود من المستخدمين الآخرين في جميع أنحاء العالم، وقد أدى ذلك إلى رفع سقف حرية الرأي والتعبير والحصول على المعلومات.

7-سهولة الاستخدام: لا يحتاج التعامل مع مواقع التواصل الاجتماعي إلى خبرة معلوماتية حتى يتم التفاعل مع محتواها، كما لا يحتاج رواد المواقع إلى خبرات وتدريبات علمية وعملية، ولا يحتاج إلا لمقدمة ومبادئ أولية موجزة عن طبيعة الاستخدام حيث تتطلب عملية التسجيل في مواقع التواصل الاجتماعي اختيار اسم ورقم سري، والموافقة على شروط العضوية وبمجرد استكمال إجراءات التسجيل يحصل الفرد على عضوية باسم مستخدم ورقم سري وحيز خاص به يسمح له بمباشرة أعماله الرقمية بحرية تامة.

1-موقع التواصل الفيس بوك (FACEBOOK) [42]

في عام 2004 أطلق مارك زوكربيرج بمعاونة أندرو ماكلولوم وإدوارد سفارين موقع التواصل الاجتماعي لطلبة جامعة هارفارد ثم انضم اليهم طلاب جامعة ستانفورد وويال ومع عام 2006 أصبح لكل من يملك بريد الكتروني إمكانية استخدام موقع الفيسبوك، ويتطلب هذا الموقع عدم إنشاء حسابات سرية بل يلزم أن تكون بياناتهم صحيحة وهو ما يعرف بمبدأ التعريف، وتبقى البيانات والمحتوى موجودة حتى ازالتها من المستخدم أو من المالك ذاته، وتعهد شركة فيسبوك إلى شركة أخرى إدارة محتوى الفيسبوك يومياً للتأكد من عدم انتهاك سياسات ومعايير الموقع، إلا أن كافة خبراء العالم الافتراضي يصنفون موقع الفيسبوك من أقل المواقع احترام لحماية البيانات الشخصية من خلال ضعف رقابتها على مستخدمين الموقع.

2- تويتر (TWITTER)[43]

في عام 2006 تم تأسيس موقع تويتر من قبل كلاً من جاك دورسي وإيفان ويليامز وتعتبر منصة تويتر من أشهر وأكثر مواقع التواصل الاجتماعي من قبل الصحفيين لتبادل الاخبار القصيرة حيث أن الرسالة لا تتعدى 140 حرف ويمكن للمستخدم الدخول باسم مستعار أو جعل البيانات مغلقة ويظل الموقع محتفظ بآخر 3200 تغريدة.

---

[42] دينا عبد العزيز فهمي، المسؤولية الجنائية الناشئة عن إساءة استخدام مواقع التواصل الاجتماعي، بحث مقدم للمؤتمر العلمي الرابع لكلية الحقوق جامعة طنطا، القانون والاعلام، الفترة من 23-24 ابريل 2017، ص9.

[43] دينا عبد العزيز فهمي، المسؤولية الجنائية الناشئة عن إساءة استخدام مواقع التواصل الاجتماعي، مرجع السابق. ص 9

3- واتس آب(WHATSAPP) [44]

تأسس واتس آب في عام2009 من قبل يان كوم وبريان أكتوم العاملين سابقاُ بشركة ياهو ويستخدم أكثر من مليار شخص حالياً خدمات واتس آب التي تعني ترجمة الجملة (ما الخبر الجديد) وقد كان واتس آب خدمة مدفوعة حتى عام 2016 وبعدها أصبح مجانياً.

4-يوتيوب (YOUTUBE)[45]

موقع ويب أسسه في عام 2005 ثلاثة موظفين من شركة باي بال (تشاد هيرلي وستيف تشين وجاود كريم) ويسمح هذا الموقع لمستخدميه برفع التسجيلات المرئية مجانا ومشاهدتها عبر البث الحي (بدل التنزيل) ومشاركتها والتعليق عليها وغير ذلك، ويستخدم الموقع تقنية برنامج أدوبي فالش لعرض المقاطع المتحركة ومحتوى الموقع يتنوع بين مقاطع الافلام، والتلفاز، والسجلات القرآنية لمختلف الحفاظ والموسيقى، والفيديو المنتج من قبل الهواة وغيرها.

5- إنستجرام (INSTAGRAM)[46]

تأسس التطبيق في أكتوبر عام 2010 من Kevin Systrom -Mike Krieger وهو تطبيق مجاني لتبادل الصور وشبكة اجتماعية أيضا للمستخدمين تمكنهم من التقاط صورة، وإضافة فلتر رقمي إليها، ومن ثم مشاركتها في مجموعة متنوعة من خدمات الشبكات الاجتماعية، وشبكة إنستغرام نفسها وتضاف الصور على شكل مربع، على غرار Instamatic كوداك.

6- لينكد إن (LINKEDIN)[47]

يعتبر موقع لينكدان موقع تواصل للمحترفين يمكنهم من اعداد سيرتهم الذاتية ليبحث عنها أصحاب الوظائف المميزة والهامة ولا يحتاج الموقع لأي كلمة سر أو بيانات خاصة لاستخدام الموقع إلا أن أهم ما يميز هذا الموقع أن المستخدم ملتزم بوضع البيانات الصحيحة ليتمكن أصحاب العمل من الوصول إلى المستخدم.

---

[44] دينا عبد العزيز فهمي، المسؤولية الجنائية الناشئة عن إساءة استخدام مواقع التواصل الاجتماعي، مرجع سابق، ص 10.

[45] دينا عبد العزيز فهمي، المسؤولية الجنائية الناشئة عن إساءة استخدام مواقع التواصل الاجتماعي، مرجع سابق ، ص 10

[46] دينا عبد العزيز فهمي، المسؤولية الجنائية الناشئة عن إساءة استخدام مواقع التواصل الاجتماعي، مرجع سابق ، ص 10.

[47] وسيم شفيق الحجار، النظام القانوني لوسائل التواصل الاجتماعي، دراسة قانونية مقارنة حول الحرية الشخصية والمسؤولية والاختصاص، مرجع سابق ، ص 22.

7- موقع سناب تشات (SNAP CHAT) [48]

إيفان شبيغل (Evan Spiegel) رائد أعمال انترنت أمريكي والمؤسس المشارك لتطبيق سناب شات وهو كالمواقع السابقة يتيح للمستخدم إمكانية البقاء على اتصال مع الأصدقاء باستخدام الفيديو والكتابة والصور حيث يتم إرسال أكثر من 527 ألف صورة في الدقيقة [49]، وتكون متاحة لبضع ثوان فقط ثم تختفي إلى الأبد حيث تؤخذ الصورة ويضاف النص ثم تحدد المدة الزمنية التي تبقى فيها الصورة مرئية ويتم إرسالها للغير ويمكن أن تصل رسالة لصاحبها بأن شخصاً ما يريد مشاركتها وهذا ما يميز موقع السناب باعتباره وسيلة اتصال تحمي صاحبها وخصوصيته مما يجعل التطبيق أكثر أماناً للمستخدم.

وأمام هذا التنوع لمنصات التواصل عبر الشبكة العنكبوتية يجد المستخدم عقبة بين لا محدوديتها وبين استخدامها بما يضمن عدم المساس بحقه في إبداء رأيه والتعبير عن وجهات نظره المختلفة.

المطلب الثاني: وسائل التواصل الاجتماعي ومبدأ حرية التعبير عن الرأي

تضمن التقرير الصادر عن مقر لجنة الأمم المتحدة حول حقوق الانسان عن حماية الحق في حرية الرأي والتعبير أن المادة 19 في الإعلان العالمي لحقوق الانسان تطبق على الانترنت وبرامج العالم الافتراضي باعتبارها أصبحت الوسيلة التي يمارس من خلالها الافراد الحق بحرية التعبير والرأي وأن المادة 19 تمت صياغتها برؤية لتغطية التطورات في التكنولوجيا التي قد يتم من خلالها التعبير لكن التقرير يعترف بأن بعض أشكال التعبير تخضع للقيود المنصوص عليها في الفقرة 3 من المادة 19 المشار اليها وهي بالتالي تطبق على وسائل التواصل الاجتماعي بالنسبة لحرية الرأي والتعبير مع مراعاة القيود التي ترد على هذه الحرية [50].

---

[48] وسيم شفيق الحجار، النظام القانوني لوسائل التواصل الاجتماعي، دراسة قانونية مقارنة حول الحرية الشخصية والمسؤولية والاختصاص، مرجع سابق ، ص 22.

[49] منى الأشقر جبور، محمود جبور، البيانات الشخصية والقوانين العربية، الهم الأمني وحقوق الأفراد، مرجع سابق، ص 13.

[50] وسيم شفيق الحجار، النظام القانوني لوسائل التواصل الاجتماعي، دراسة قانونية مقارنة حول الحرية الشخصية والمسؤولية والاختصاص، مرجع السابق، ص 76.

وتضمنت المادة العاشرة من الاتفاقية الأوروبية لحماية حقوق الانسان والحريات الأساسية كل طريقة للتعبير، أو للنشر أو لجعل معلومات أو مفاهيم معروفة وذلك بصرف النظر عن الوسيطة أو قناة التوزيع وهناك توافق عام على أن المادة العاشرة المشار اليها تطبق بطريقة مستقلة أو حيادية عن التكنولوجيا مما يجعلها قابلة للتطبيق على شبكات الاتصالات الحديثة وأنظمة المعلومات على الانترنت والتي منها وسائل التواصل الاجتماعي[51] .

وعلى الصعيد العربي تنص المادة 32 من الميثاق العربي لحقوق الانسان على أن: "يضمن هذا الميثاق الحق في الاعلام وحرية التعبير والرأي والأفكار وتلقيها ونقلها إلى الاخرين بأي وسيلة ودونما اعتبار لحدودهم الجغرافية وعلى أن تمارس هذه الحقوق والحريات في إطار المقومات الأساسية للمجتمع ولا تخضع إلا للقيود التي يفرضها احترام حقوق الاخرين، أو سمعتهم أو حماية الامن الوطني أو النظام العام أو الصحة العامة أو الآداب العامة" وكذلك الحق في استقاء الأنباء والأفكار"[52].

وقد اعتبرت لجنة وزراء مجلس أوروبا أن حرية التعبير والمعلومات والاتصالات يجب أن تحترم في بيئة رقمية كما في بيئة غير رقمية ولا يجب أن تكون موضوع تقييدات غير تلك المنصوص عليها في المادة العاشرة من الاتفاقية الاوروبية لحماية حقوق الانسان والحريات الأساسية وذلك لمجرد أن الاتصال يتم بشكل رقمي ، فمعايير حقوق الإنسان تعترف بأن حقوقاً ومصالح مشروعة يمكن أن تقيد الحريات في مجال المعلومات حيث أوجبت المادة الثامنة من الاتفاقية الأوروبية لحقوق الإنسان حماية الحياة الخاصة بالنص على وجوب حماية الأفراد من التدخل والاعتداء على حياتهم الخاصة وحياة أسرهم كما قررت المادة العاشرة وجوب حماية حق الوصول إلى المعلومات[53].

---

[51] وسيم شفيق الحجار، النظام القانوني لوسائل التواصل الاجتماعي، دراسة قانونية مقارنة حول الحرية الشخصية والمسؤولية والاختصاص، مرجع السابق، ص 77.

[52] الميزان البوابة القانونية القطرية، مرسوم رقم: 66 لسنة 2013، تاريخ الصدور: 2004/4/23 هجري، تاريخ مصادقة قطر: 2013/11/03 الموافق 1434/12/29هجري، مقر التوقيع: القاهرة ، العدد : 18 ، تاريخ النشر : 2013/12/03.
https://www.almeezan.qa/AgreementsPage.aspx?id=1849&language=ar

[53] مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، مرجع سابق ص 299.

وفي الولايات المتحدة الأمريكية تم إدخال التعديلات العشرة الأولى عام 1791 على الدستور الأمريكي فيما يعرف :(بوثيقة الحقوق) والتعديل الأول للدستور يؤكد أنه لا يمكن للكونغرس وضع قانون يحرم حرية التعبير[54].

المطلب الثالث: وسائل التواصل الاجتماعي وحماية البيانات الشخصية

إن كان الحق في التعبير والرأي على مواقع التواصل الاجتماعي محمية بموجب المواثيق الدولية إلا أن هذا الحق مقيد بعدم التعسف في استعماله والتعدي على الحق في الخصوصية وحماية البيانات الشخصية حيث أن كافة الدساتير متفقة على أن المبدأ العام- عدم جواز الاعتداء على البيانات الشخصية بوصفه صورة من صور الحق الشخصي-أياً كانت وسيلته[55] - وعلى سبيل المثال نص الدستور القطري في المادة : (37) منه على أنه : " لخصوصية الإنسان حرمتها، فلا يجوز تعرض أي شخص، لأي تدخل في خصوصياته أو شؤون أسرته أو مسكنه أو مراسلاته أو أية تدخلات تمس شرفه أو سمعته، إلا وفقاً لأحكام القانون وبالكيفية المنصوص عليها فيه" ويتسع النص الدستوري ليشمل كل حق لصيق بشخصية الانسان سواء في الجانب المالي أو الأدبي وأياً ما كانت وسيلة الاعتداء وهذا ما يظهر بوضوح في مجال التواصل الاجتماعي حيث لا يتردد المستخدم-عادة-في أن يضع على صفحته بيانات أو معلومات تتعلق بحياته الخاصة تكون متاحة لكل من يستطيع الدخول إلى الموقع وهو ما قد يؤدي إلى انتهاك خصوصيته أو حقه في البيان الشخصي إذا استخدم الغير هذه البيانات أو المعلومات استخداماً غير مشروع بما قد يلحق بالمستخدم ضرراً في حياته العائلية أو المهنية [56].

---

[54] وثيقة الحقوق: هي اسم يجمع التعديلات العشرة الأولى لدستور الولايات المتحدة الأمريكية، قدمت لتهدئة مخاوف مضادي الفيدرالية الذين عارضوا المصادقات الدستورية، هذه التعديلات تضمن عدداً من الحريات الشخصية، وتحد من نفوذ الحكومة في القضاء، وتبقي على بعض النفوذ للولايات وللعامة. قدم جيمس ماديسون التعديلات لكونغرس الولايات المتحدة الأول كسلسلة من المراسيم التشريعية. يوم وثيقة الحقوق في الولايات المتحدة الأميركية هو 15 ديسمبر. أشارت إليه : مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، مرجع سابق ص33.

[55] السيد أحمد حلمي، الحماية الجنائية لحق الانسان في حياته الخاصة، رسالة دكتوراه عام 1983 كلية الحقوق جامعة المنصورة، ص50.

[56] حسام الدين كامل الأهواني، الحق في احترام الحياة الخاصة (الحق في الخصوصية) دراسة مقارنة، دار النهضة العربية ،1978 ص 83.

ولذلك يعد انتهاكاً للخصوصية على مواقع التواصل الاجتماعي كل انتهاك للعزلة كالاعتداء على البيانات الشخصية والصور والمحادثات بما يسيء للسمعة والمكانة أو انتحال الصفة - و بذلك يقوم الحق في الخصوصية على مواقع التواصل على عنصرين متلازمين هما حرية الحياة الخاصة وسريتها[57] ويكون الاطلاع عليها غير مشروع وانتهاكاً لحرمة الحياة الخاصة كما أن الحق في الخصوصية يتميز بأنه نسبي يختلف من مجتمع لمجتمع ومن زمن لآخر[58]- وهذا التعريف للحق في الخصوصية ينطبق أيا ما كان الوسيط الذي توجد فيه البيانات الشخصية كالوسيط الالكتروني، ولهذا فإن الحلول القضائية المستقرة بشأن حماية البيانات الشخصية عبر النشر التقليدي يمكن أن تنسحب على مواقع التواصل الاجتماعي بعد مراعاة الطبيعة الخاصة لهذه الوسائط- وقد قضي في فرنسا أن نشر مقال عبر الانترنت يتناول الحياة العائلية والعاطفية لمطربة يعتبر اعتداء على حرمة حياتها الخاصة بعدما تأكد الحصول على هذه المعلومات من ملفاتها الخاصة كما قضي بأنه يعتبر اعتداء على الحياة الخاصة على مواقع التواصل الاجتماعي النشاط اليومي للمستخدم ومحل الإقامة والحالة الصحية وصوره وعقيدته الدينية وحياته العائلية كما اعتبر القضاء الفرنسي السرية هي أساس الحياة الخاصة وأن الإخلال بالالتزام بالسرية اعتداء على الخصوصية حيث قضت محكمة باريس الابتدائية أن الكشف عن عنوان المنزل الذي يقيم فيه أمير موناكو وزوجته في العاصمة الفرنسية يعتبر مساساً بحقه في الخصوصية لما فيه من إزعاج له ولزوجته[59] وقد أكدت تلك الممارسات القضائية الكثير من النصوص الوطنية والدولية حيث نصت المادة (12) من الإعلان العالمي لحقوق الانسان بأنه: " لا يجوز إخضاع أحد للتدخل التعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته ولا لأي اعتداء يمس شرفه أو سمعت" ، وذات المضمون نصت عليه المادة الثامنة من الاتفاقية الاوروبية لحماية حقوق الانسان والحريات الأساسية التي تنص على أنه: "لكل شخص الحق في احترام حياته الخاصة والعائلية ومسكنه ومراسلاته"[60].

ويستطيع مستخدم مواقع التواصل الاجتماعي أن يتجنب إتاحة معلوماته الشخصية للكافة بأن يقصر كشف المعلومات على أشخاص محدودين كأصدقاء له على صفحته دون غيرهم إلا أن الحق في

---

[57] أحمد فتحي سرور، الحماية الجنائية للحق في الحياة الخاصة، دار النهضة العربية 1976 ، ص 54.

[58] محمود عبد الرحمن ، نطاق الحق في حرمة الحياة الخاصة ، دار النهضة العربية 2000 ، ص 237.

[59] محمد سامي عبد الصادق، شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية، مرجع سابق ص 95.

[60] مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، مرجع سابق ص 299.

الخصوصية قد يتعارض مع الحق في الاعلام أو ما يسمى بالحق في الحصول على المعلومة وللموازنة بين الحق في حماية البيانات الشخصية والحق في الحصول على المعلومة ينظر إلى مدى تعلقها بالمصلحة العامة ، حيث أن تعلق المعلومات بالمصلحة العامة يرجح كفة مبدأ حرية التعبير والكشف عن المعلومات على مبدأ حماية البيانات ، كما أنه لا يجوز أن تكون المعلومة المرسلة عبر مواقع التواصل من شأنها المساس بالمصلحة العامة من حيث مخالفتها للنظام العام والآداب حيث لا يعمل بمبدأ حماية البيانات[61] وهدا ما نستنتجه من ما ذهب إليه حكم المحكمة القطرية : " عندما أدانت الطاعن بجريمة المادة (136) من قانون العقوبات ، الذي قام بتحرير مكتوبين يدعو فيهما للانقلاب على السلطة الشرعية الحاكمة وللخروج عليها ونشر هذان المكتوبان عبر الإنترنت، في عدد من الموقع منها موقع فيس بوك ، كما قام بإرسال المكتوبين الصادرين منه عبر بريده الإلكتروني إلى جهات أجنبية سفارات وإلى عدد من المواقع بعدد من الدول ، وقد دللت المحكمة حكمها على ثبوت القصد الجنائي لدى الطاعن عندما دعا إلى ما يخالف النظام العام سواءً باستعمال القوة أو بأي وسيلة أخرى غير مشروعة (الوسائل التي استخدمها) طالما أنه تجاوز حدود النقد" [62]، فلا مجال للتمسك بمبدأ حماية البيانات طالما تعلق الأمر بالمصلحة العامة.

كما تنتفي الخصوصية بسبق قيام المستخدم بنشر المعلومة للجمهور حيث تخرج من الخصوصية للعمومية ومن ثم يجوز إعادة نشرها. وهنا تسقط الخصوصية والحماية، ولكن قد يكون من حق من سبق وأن نشر معلومات أو بيانات وأذن بنشرها أن يتمسك بإعمال مبدأ الحق في النسيان خاصةً إذا ألحقت ضرراً به مثل قيام إحدى الفتيات بنشر صورة لها على مواقع التواصل الاجتماعي في إحدى الحفلات وهى تتعاطى المخدرات مع أحد اصدقائها ؛ فنشر هذه الصورة من شأنه تشويه سمعتهما وقد يحرمها من تولى بعض الوظائف العامة [63]وهو ما أقر به القضاء الأمريكي الذي اشترط للتمسك بالحق في النسيان أن يكون من شأن إعادة نشر الوقائع القديمة استهجان المجتمع

---

[61] مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، مرجع سابق ص 284.

[62] الطعن رقم 90 لسنة 2017 تمييز جنائي ، موسوعة الأحكام والمبادئ القضائية القطرية ، الدخول 2020/11/20 الوقت 11:19 مساءً.

https://www.sjc.gov.qa/ar/Pages/Encyclopedia-Of-Qatari-Provisions-And-Judicial-Principles.aspx

[63] محمد أحمد المعداوي، حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي، دراسة مقارنة، مرجع سابق، ص 88.

لصاحبها واختلف عن نظيره الفرنسي في ضوابط ممارسة هذا الحق فلا يشترط في الماضي الذي يرغب صاحبه في عدم إحيائه من جديد أن يكون سيئاً ومشيناً[64].

كما يدخل في مفهوم الحق في الخصوصية الحق في الاعتراض على انتاج أو استغلال صورة الشخص حيث يتعلق هذا الحق بحماية الكيان البشري ذاته ولذلك فهو حق لكل من كانت هويته على مواقع التواصل محددة[65] **حيث لا يجوز نشر صورة الشخص دون علمه** لأن صورته هي انعكاس لشخصيته بحكم أنها أداة تعريفية تعبر عن شخصه وقد أقرت معظم التشريعات بحق كل شخص في صورته ونذكر منها المادة 14 من القانون القطري رقم (7) لسنة 2002 بشأن حماية حق المؤلف والحقوق المجاورة الذي نص على أن : "لا يجوز لمن قام بتصوير أو رسم أشخاص، أن ينشر أو يعرض أو يوزع أصل الصورة، أو نسخاً منها، دون إذن هؤلاء الأشخاص. ولا يسري هذا الحكم إذا كان نشر الصورة أو الرسم قد تم بمناسبة حوادث وقعت علناً أو كانت تتعلق بأشخاص ذوي صفة رسمية، أو يتمتعون بشهرة عالمية، أو سمحت بها السلطات العامة خدمة للصالح العام. وللشخص الذي تمثله الصورة أن يأذن بنشرها في الصحف والمجلات، وغيرها من النشرات المماثلة، حتى ولو لم يأذن بذلك المصور، ما لم يوجد اتفاق على غير ذلك" وبالتالي فإن النشر غير المأذون به لصورة الشخص يمثل تعدياً على حقه يمكنه من رفع دعواه اعتراضاً على هذا النشر كما يحق له مطالبة الفاعل بالتعويض عما لحق به من أضرار بسبب الاعتداء على خصوصيته ، وإن كان نص المادة السابقة لا يتحدث عن نشر الصورة عبر شبكة الإنترنت وما تتضمنه من مواقع تواصل أو بريد إلكتروني ، إلا أن هذا النص جاء عاماً لحماية الصورة الشخصية باعتبارها مسألة من المسائل التي تمس بخصوصية الشخص أياً كانت وسيلة النشر الإنترنت أو غيرها من الوسائل. وتسري هذه الأحكام على الصورة أيا كانت الطريقة التي تمت بها. وهذا ما أكده القضاء القطري عندما "جرم نقل البيانات التي يحتويها نظام المعالجة الآلية ومن ضمن هذه النظم ذاكرة الحاسب الآلي وفقاً لما أوردته المادة (370)، وأن الصور تكون محفوظة بذاكرة بالحاسب الآلي وأن لفظ البيانات لغة تشمل كل الأشياء التي يمكن تخزينها على الحاسب ومن ضمنها الصور فإن ما يزعم

---

[64] محمد سامي عبد الصادق، شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية، مرجع سابق ص 69.

[65] محمد سامي عبد الصادق، شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية، مرجع سابق ص 97.

به الطاعن من أن لفظ البيانات تعني وقائع ومعلومات ولا تشمل الصور إنما هو تخصيص للنص بغير مخصص" [66].

ويميل القضاء إلى اعتبار الحق في حماية الكيان البشري حقا مستقلا عن الحق في الخصوصية خلافاً لما ذهب إليه بعض الفقهاء إلى اعتباره إحدى حالات الحق في الخصوصية، أو إلى التمييز حسب طريقة الحصول على الصورة[67] . فقد تصدى القضاء لحماية الحق في الصورة والحفاظ عليها حيث قرر، اعمالاً لمبدأ الحياد المعلوماتي، أنه في غير ما تقضيه ضرورة اعلام الجمهور، يجب دائماً الحصول على إذن الشخص قبل نشر أي معلومات تتعلق به أو صورة له[68] ويستلزم القضاء لنشر الصورة أن يكون الرضا صريحاً وخاصاً ولذلك الاذن بالنشر العام لا يعطي حق نشر الصورة او استعمالها إنما لا بدا من الحصول على الاذن لاستعمال الصورة أو إعادة نشرها دون الاكتفاء بإذن النشر العام أو نسخ بعض التعليقات. وللمضرور الحق في تحديد شكل المسؤولية إما على أساس مبدأ عدم جواز الاعتداء على حرمة الحياة الخاصة وهنا لا يكلف المضرور بإثبات عناصر المسؤولية طالما وقع الاعتداء فباقي العناصر مفترضة وكذلك فإن هذه الدعوى على هذا

---

[66] نصت المادة (370) من قانون العقوبات القطري على أنه " يقصد بنظام المعالجة الآلية للبيانات، كل مجموعة من واحدة أو أكثر من وحدات المعالجة، سواء تمثلت في ذاكرة الحاسب الآلي، أو برامجه، أو وحدات الإدخال أو الإخراج أو الاتصال التي تساهم في تحقيق نتيجة معينة "، كما نصت المادة (373)على أن " يعاقب بالحبس مدة لا تقل عن سنة ولا تجاوز ثلاث سنوات، وبالغرامة التي لا تقل عن عشرة آلاف ريال ولا تزيد على خمسين ألف ريال، كل من أدخل عمداً، سواء بطريق مباشر أو غير مباشر، بيانات في نظام المعالجة الآلية الخاص بشخص أو بجهة ما، أو دمر أو عدل البيانات التي يحتويها أو طريقة معالجتها أو نقلها " الطعن رقم 454 لسنة 2015 تمييز جنائي ، موسوعة الأحكام والمبادئ القضائية القطرية ، الدخول 2021/1/19 الوقت 4:23 مساءً.
https://www.sjc.gov.qa/ar/Pages/Encyclopedia-Of-Qatari-Provisions-And-Judicial-Principles.aspx

[67] يرى البعض ان هذا الحق من صور الحق في الخصوصية لان الصورة وثيقة الصلة بالشخص ويذهب اتجاه اخر انه حق مستقل لأنه يمكن التقاط صورة جماعية في مكان عام وبالتالي يكون لكل من في الصورة الحق في التقاضي وفريق ثالث يرى التفرقة بين مدى تعلق الصورة بالحياة الخاصة أو العامة- ارجع في هذا الشأن : حسام كامل الأهواني، مرجع سابق، ص71.

[68] سعيد جبر، الحق في الصورة، دار النهضة العربية 1986، ص 124.

الأساس لا تسقط بالتقادم وتعطي حق إزالة الاعتداء بجانب التعويض أو بناء على الخطأ الشخصي في المسؤولية التقصيرية، الا أن تلك الدعوى على هذا الأساس تخضع لميعاد التقادم[69].

المبحث الثالث: حق النسيان الرقمي وحماية البيانات الشخصية.

الحق في النسيان الرقمي أحد الحقوق الحديثة التي خرجت من رحم الحقوق الشخصية وأصبح هذا الحق يتفوق على المصالح التجارية والحقوق والحريات المتعلقة بالممارسات التجارية لوسائل التواصل الاجتماعي وبدأ معرفة مصطلح الحق في النسيان الرقمي على مواقع التواصل الاجتماعي من العام 2014 مع حكم محكمة العدل في الاتحاد الأوروبي الذي ألزم محرك البحث (جوجل) باتخاذ التدبير اللازمة لسحب المستخدم بياناته الشخصية من ملفاته وفهارسه وكان هذا الحكم بمناسبة القضية التي رفعها مواطن أسباني ضد محرك البحث لإلزامه بحذف الروابط التي تظهر عند البحث على اسم عائلته وظهور مقالات صحفية قيمة تعلن الحصول على حجوزات على أملاكهم لسداد ديونهم[70].

ولقد أقر المشرع القطري حق النسيان الرقمي في قانون حماية البيانات [71]حيث نصت المادة (5) من قانون حماية البيانات الشخصية صراحةً على أنه: " يجوز للفرد، في أي وقت:1- سحب موافقته السابقة على معالجة بياناته الشخصية،2-الاعتراض على معالجة بياناته الشخصية إذا كانت غير ضرورية لتحقيق الأغراض التي جمعت من أجلها، أو كانت زائدة على متطلباتها، أو تمييزية أو مجحفة أو مخالفة للقانون-3-طلب حذف بياناته الشخصية أو محوها في الحالات المشار إليها في البندين السابقين، أو عند انتهاء الغرض الذي تمت من أجله معالجة تلك البيانات، أو إذا لم يكن هناك مبرر للاحتفاظ بها لدى المراقب-4-طلب تصحيح بياناته الشخصية، مرفقاً به ما يثبت صحة طلبه". فأعطى الحق لصاحب البيانات الشخصية في طلب محو بياناته في حال لم تعد ضرورية في ضوء أهداف المعالجة أو في حال سحب موافقته على هذه المعالجة أو اعتراضه على المعالجة

---

[69] محمد أحمد المعداوي، حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي، مرجع سابق، ص 2007.

[70] وسيم شفيق الحجار، النظام القانوني لوسائل التواصل الاجتماعي، دراسة قانونية مقارنة حول الحرية الشخصية والمسؤولية والاختصاص ، مرجع سابق ، ص 91.

[71] قانون رقم 13 لسنة 2016 بشأن حماية خصوصية البيانات الشخصية القطري، الميزان، البوابة القانونية القطرية ، تاريخ الدخول : 2017/2/8 ، الوقت: 7:24 مساءً.

https://www.almeezan.qa/LawPage.aspx?id=7121&language=ar

غير القانونية. شريطة ألا يتعارض هذا الحق مع حق آخر مشروع أو كان من شأنه إخفاء دليل على انتهاكات وممارسات غير مشروعة.

المطلب الأول: مفهوم النسيان الرقمي.

يمكن تعريف الحق في النسيان -بشكل عام-بأنه الحق لكل شخص ارتبط بحدث عام حتى ولو كان هو محوره أن يطالب بحق نسيان هذا الحدث وبالاعتراض على تذكار حقبة من حياته[72] أما على مواقع التواصل الاجتماعي فهو يعني أن لكل مستخدم الحق في حذف وإلغاء كافة البيانات والاحداث والصور وما تركه على مواقع التواصل الاجتماعي وعدم الاحتفاظ بها إلكترونياً في فترة زمنية سواء أثناء الاستخدام أو في حالة الهجر النهائي للموقع.

وعادةً ما يحرص مقدم خدمة التواصل الاجتماعي عبر الإنترنت على المحافظة على البيانات الشخصية لمستخدمي مواقع التواصل لأطول فترة ممكنة مما يتعارض مع حق المستخدم الذي اختار حذف بياناته أو حسابه الشخصي فلهذا يجب على مقدم الخدمة اتخاذ التدابير اللازمة للحيلولة دون إطلاع باقي المستخدمين على بياناته ومنع المعلنين من الاستمرار في معالجتها.

وقد اعترفت العديد من الدول الغربية بهذا الحق، منها فرنسا والولايات المتحدة الأمريكية حيث استخلص الفقه الفرنسي الحق في النسيان من المادة (35) من قانون حرية الصحافة الصادر في 29 من يوليو 1881م والتي أكدت عدم جواز إثبات صحة وقائع القذف متى مضت عشر سنوات على القذف، كما اعترف القضاء في الولايات المتحدة الأمريكية بالحق في النسيان وإن اختلف القضاء الأمريكي عن نظيره الفرنسي في ضوابط هذا الحق فلا يشرط في فرنسا أن يكون الماضي سيئاَ ومشيناً حتى يطالب صاحبه بسحبه بينما يستوجب القضاء في الولايات المتحدة للمطالبة بهذا الحق أن يؤدي نشره إلى الإساءة إلى صاحبه [73].

وبالرجوع إلى نص المادة (5) من قانون حماية البيانات الشخصية القطري سالفة الذكر نجد أن المشرع القطري جعل المطالبة بالحق في النسيان فضفاضاً غير مقيداً بالإساءة إلى صاحبه في إطار المحافظة على سرية البيانات[74].

---

[72] محمد سامي عبد الصادق، شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية، مرجع سابق، ص 68.

[73] محمد سامي عبد الصادق، شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية، مرجع سابق، ص 68-69.

[74] نصت المادة (5) من قانون حماية البيانات الشخصية القطري على أنه: "يجوز للفرد، في أي وقت:1- سحب موافقته السابقة على معالجة بياناته الشخصية،2-الاعتراض على معالجة بياناته الشخصية إذا كانت غير ضرورية

المطلب الثاني: طبيعة الحق في النسيان الرقمي.

يعتبر الحق في النسيان في بعض الدول الاوروبية ولاسيما في فرنسا من بين الحقوق اللصيقة بالشخصية وإن كان البعض في هذه الدول ينازع في هذا الحق وفي معنى ذلك. وهو يبرّر ذلك بأن البيانات المتعلقة بالحياة الخاصة لشخص اشترك في حدث عام يمكن أن تصبح عامة تطبيقاً لمبدأ الحق في الوصول إلى المعلومات وتبرير نشر هذه البيانات الخاصة بالفرد حينها هو حداثتها. ولكن بعد سنوات يمكن للشخص أن يتذرع بحق النسيان فيما يخص بياناته[75]. وقد أصبح هذا الأمر أكثر إشكالية بعد شيوع مواقع التواصل الاجتماعي وسهولة الوصول الى المعلومات عليها واحتوائها لمعلومات قد تبقى منشورة لسنوات طويلة واحتفاظ مقدمي خدمة التواصل بهذه البيانات رغم حذف مستخدمي المواقع لحساباتهم الشخصية على الموقع[76].

و الإعتراف بالحق في النسيان واعتباره من الحقوق المتعلقة بالشخصية يؤدي إلى حماية الحياة الخاصة للفرد في وقت معين يجد نفسه متدخلاً في حدث يتداول على العالم الإفتراضي مما يحتفظ له بحقه في الرجوع على مقدم الخدمة لما لحقه من ضرر ، وأساس هذا الحق وفق الاجتهاد الفرنسي الذي أنشأ هذا الحق أنه وقت حصول الأفعال (المطلوب نسيانها) يمكن إفشاء عناصر من الحياة الخاصة للفرد تطبيقاً للحق في المعلومة كما في حالة دعوى قضائية مثلاً[77] -لكن بعد سنوات عديدة

لتحقيق الأغراض التي جمعت من أجلها، أو كانت زائدة على متطلباتها، أو تمييزية أو مجحفة أو مخالفة للقانون-3-طلب حذف بياناته الشخصية أو محوها في الحالات المشار إليها في البندين السابقين، أو عند انتهاء الغرض الذي تمت من أجله معالجة تلك البيانات، أو إذا لم يكن هناك مبرر للاحتفاظ بها لدى المراقب-4-طلب تصحيح بياناته الشخصية، مرفقاً به ما يثبت صحة طلبه"

[75] محمد سامي عبد الصادق، شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية، مرجع سابق، ص 68.

[76] معاذ سلمان الملا، فكرة الحق في الدخول في طي النسيان الرقمي في التشريعات الجزائية الإلكترونية الحديثة، دراسة مقارنة بين التشريع العقابي الفرنسي والتشريع الجزائي الكويتي، مجلة القانون، كلية القانون، الكويت، العدد 3، جزء 1، مايو 2018، ص 122.

[77] ومن أشهر القضايا التي عمل بها القضاء الأمريكي بمبدأ الحق في الدخول في طي النسيان قضية (**The Red Kimono**) في ولاية كاليفورنيا عام 1918م حيث اتهمت امرأة سيئة السمعة بارتكاب جريمة قتل، وقضى ببراءتها، ومنذ ذلك الوقت تركت سلوكياتها المشينة وتزوجت وعاشت في المجتمع كسيدة محترمة، غير أنه تم عرض فيلم سينمائي بعد عدة سنوات يتناول قصتها وسميت البطلة باسمها مما دفعها إلى رفع دعوى على مؤلف

يمكن لهذا الفرد أن يمانع في نشر هذه العناصر تطبيقاً لـمبدأ الحق في النسيان ويمكنه استناداً إلى هذا الحق أن يرجع على مزود الخدمة في حال تحويل ماضيه من ظلمات النسيان إلى الأضواء مرة أخرى[78].

المطلب الثالث: إشكاليات حق النسيان الرقمي

يواجه التطبيق العملي للحق في النسيان عدة إشكاليات، إذ قد تكون المعلومات المنشورة موجودة على صفحة خاصة بمشترك آخر بحيث يكون له الحق في حرية التعبير على صفحته والاحتفاظ بالمعلومات ضمن حق حماية الحق في التعبير. وبالتالي فإنه لا يجوز اجبار هذا الشخص على إزالة البيانات التي تم وضعها من قبل بعض متابعيه، وإن كانت بعض المواقع تتيح للمستخدم حذف بياناته أو ما قام بوضعه على صفحة مستخدم آخر طالما وافق هذا المستخدم على خاصية الحذف للمتابعين عند بداية الاشتراك مثل الفيسبوك، على خلاف مواقع التواصل الاجتماعي الأخرى التي تستلزم موافقة صاحب الصفحة التي تم وضع البيانات عليها أو منها ما يسمح بحذفها ولا يراها صاحبها فقط وتبقى موجودة على الصفحة المملوكة للغير.

كما أن هناك إشكالية أخرى تتعلق بالبيانات الشخصية الخاصة بشخص غير المستخدم لموقع التواصل الاجتماعي فهو في هذا الوقت لا يعلم عنها شيئاً ولا يملك أية أدوات لحذفها- ومن أكثر الإشكاليات هو تعارض الحق في النسيان مع الحق في الاحتفاظ بالبيانات- وبمعنى آخر لا يملك الشخص منع الاخرين البحث عما يبديه من آراء طالما وافق في البداية على علانية النشر. فإذا ما كان يسمح بهذا الحق للجميع من رؤية بياناته ومنشوراته فلا يجوز بعد علانيتها وتعلق بعضها بحق شخص آخر في التعبير أن يطلب حذفها لدخولها حيز حق شخص آخر- ولهذا فإن الاتحاد الأوروبي والولايات المتحدة حذرا في تقنين هذ الحق وتطبيقه فعلياً حيث أنه من ناحية يعتدي على الحق في التعبير وحرية الرأي، ومن ناحية أخرى يُكلف شركات مواقع التواصل الاجتماعي جهداً فائقا وتكلفة مالية عالية للبحث عن المعلومات المطلوب حذفها[79].

القصة لإساءته لسمعتها أمام زوجها وأبنائها وانتهت المحكمة إلى إعمال الحق في الدخول في طي النسيان وحفظ حقها في الخصوصية. أشار إليه : محمد سامي عبد الصادق، مرجع سابق، ص 69.

[78] محمد سامي عبد الصادق، مرجع سابق، ص 69.

[79] وسيم شفيق الحجار، النظام القانوني لوسائل التواصل الاجتماعي، دراسة قانونية مقارنة حول الحرية الشخصية والمسؤولية والاختصاص، مرجع السابق، ص 92.

ومن المواقع التي توازن بين الحق في النسيان والحق في التعبير والرأي موقع تويتر، حيث يقوم موقع تويتر على إلغاء العميل حسابه بوقف الوصول الى بيانات المستخدم فوراً وبمحوها خلال ثلاثين يوماً والتي يمكن خلالها إعادة تفعيل الحساب ويلتزم الفيسبوك بمحو جميع المعلومات العائدة للحساب الملغي خلال 90 يوم إلا أنه تبقى بعض المعلومات عن المستخدم الذي ألغي حسابه وهي تلك المنسوخة أو الظاهرة على حسابات أخرى أو البيانات المجمعة عنه خارج إطار حسابه[80].

وهو ما ذهب إليه المشرّع القطري من تقرير الحق في النسيان ونحن مع تأييد فكرة إعطاء المواطن العربي الحق في النسيان من بين الحقوق المعطاة له لإعطائه فرصة وانطلاقة جديدة في الحياة وتشجيعه على اصلاح ذاته انطلاقاً من مبدأ إعادة تأهيل المجرمين فالمعلومات المتعلقة بشخص ما يجب أن لا تؤثر عليه عند تقديمه على وظيفة أو تأمين أو إقباله على حياة اجتماعية جديدة لاسيما أن القوانين الجزائية في الدول العربية تنص على مبدأ انقضاء الحق في تحريك الدعوى الجنائية أو سقوط العقوبة بمضي المدة وبالتالي من باب أولى تقرير الحق في النسيان طالما مضت مدة على تركها أو رغبته في ذلك شريطة أن لا تتعلق بحقوق وحريات أخرى أو تسبب ضرر اجتماعي ظاهر.

[80] أنظر في هذا الشأن : معاذ سلمان الملا، فكرة الحق في الدخول في طي النسيان الرقمي في التشريعات الجزائية الإلكترونية الحديثة، مرجع سابق، ص 133.

الفصل الأول: المسؤولية القانونية لأصحاب وسائل التواصل الاجتماعي.

قد تلحق (المعلومة) التي يتم تداولها بسرعة وسهولة عبر مواقع التواصل الاجتماعي أضراراً بسمعة شخص معين أو مجتمع محدد أو ربما البشرية كلها، عندما تحث على الإرهاب أو تستغل المعلومات والبيانات الموجودة على هذه المواقع في الأعمال الإرهابية فهي وإن كانت من نتيجة التطورات الحاصلة بعد الثورة الصناعية في ميادين الإنتاج وتطور التقنيات والعمل التكنولوجي إلا إنها سبّب أضراراً كبيرة تمثلت في كون ذلك التطور ألحق أضراراً بالأخرين سواء كان الضرر في الأموال، أو الممتلكات، أو العرض، أو الكرامة.

ولقد تواترت النظريات القانونية في شأن المسؤولية عن الأشياء باستبعاد الأشياء المعنوية من دائرة المسؤولية المدنية[81] في حين أن الأشياء المعنوية حالياً تثير الضرر الأكبر في العصر الحالي خاصة بما يمس الكرامة والعرض ونشر المعلومات المخلة بالأمن القومي والعسكري- وللمسؤولية التقصيرية أجنحة ثلاث هي المسؤولية عن الفعل الشخصي والمسؤولية عن فعل الغير والمسؤولية عن ضرر الأشياء هذا بخلاف المسؤولية العقدية التي ترتهن بالعلاقة العقدية.

وفي شأن المسؤولية عن البيانات الشخصية فإنه لا خلاف على إمكانية المسؤولية العقدية وفقاً العقد الالكتروني بين مستخدمي التواصل الاجتماعي والموقع الالكتروني لوسيلة التواصل إلا أن الأمر مختلف حول مدى إمكانية سريان المسؤولية التقصيرية على الضرر المعلوماتي أو بمعنى أخر هل تدخل البيانات الرقمية ضمن مفهوم الأشياء لكي يجوز تطبيق المسؤولية التقصيرية.

المبحث الأول: المسؤولية المدنية عن الأضرار

من المستقر أنه لا مجال للمسؤولية الأدبية في المجال القانوني حيث أن القانون لا يعترف إلا بالمسؤولية القانونية التي ينظمها ويتصدى لعناصرها وتنظيم جزائها إلا نصوص القانون وقد تكون المسؤولية القانونية مدنية أو تجارية أو جنائية أو إدارية ولكل من أنواع هذه المسؤولية فرعاً في القانون ينظمها تنظيماً متكاملاً حتى ما يستجد من ظواهر يتصدى لها الفقه في ضوء الإرث الكبير من القضاء والفقه في الأطر العامة للمسؤولية القانونية.

ويقصد بالمسؤولية المدنية مجموعة القواعد التي تلزم من ألحق ضرر بالغير بجبر هذا الأخير عن طريق التعويض، ولما كانت هذه المسؤولية هي محور الارتكاز في موضوع هذا البحث فإننا

---

[81] أياد عبد الجبار ملوكي ، المسؤولية عن الأشياء وتطبيقاتها على الأشخاص المعنوية، دراسة مقارنة، بغداد مطبعة بابل، 1982 ، ص 140.

سنتناول على قدر ما يتيسر أساس وأنواع وأشكال هذه المسؤولية ومدى إمكانية انطباق فكرة المسؤولية المدنية التقليدية على الضرر المعلوماتي على مواقع التواصل الاجتماعي.

المطلب الأول: المسؤولية العقدية.

تقتضي القوة الملزمة للعقد وفقا لقاعدة العقد شريعة المتعاقدين قيام أطرافه بتنفيذ ما يقع على عاتقهم من التزامات فإن عدل أي من الطرفين على تنفيذ التزاماته أو تأخر في تنفيذها كان بالإمكان إجباره على ذلك عن طريق تحريك المسؤولية العقدية [82]

ونتناول المسؤولية العقدية في شقين :

الشق الأول / ماهية المسؤولية العقدية : ويقصد بالمسؤولية العقدية أنها جزاء الإخلال بالالتزامات الناشئة عن العقد أو عدم تنفيذها أو تأخر فيها، وهذه المسؤولية لا تقوم إلا عند استحالة التنفيذ العيني.

الشق الثاني /شروط المسؤولية العقدية: ويشترط لقيام المسؤولية العقدية وجود عقد صحيح، و الإخلال بالتزام عقدي ،أي أنه لا يمكن الادعاء بالمسؤولية العقدية إلا بوجود عقد بين الأطراف ، أما إذا لم ينعقد العقد فلا مجال لقيام المسؤولية العقدية، ولا تطبق كذلك المسؤولية العقدية إذا كان العقد منعدمًا أصلا بين المسؤول و المضرور، كأن يقدّم أحدهما خدمة للثاني من باب الإحسان أو المجاملة، مثل ما هو الأمر في النقل المجاني[83].

ولا تقوم المسؤولية العقدية إلا إذا توافر الخطأ في جانب المدين[84]، وأن ينجم عنه ضرر يصيب الدائن وعلى هذا تكون أركان المسؤولية العقدية ثلاث هي الخطأ العقدي والضرر، وعلاقة السببية بين الخطأ والضرر، وقد نظم المشرع القطري المسؤولية العقدية بنصوص واضحة وصريحة في القانون المدني الصادر بالقانون رقم 22 لسنة 2004 [85].

---

[82] عبد الرزاق السنهوري، الوسيط في شرح القانون المدني، الجزء الأول، طبعة نقابة المحامين،2006، ص506.

[83] حسام لطفي، النظرية العامة للالتزام، الكتاب الثاني، الاحكام، القاهرة 2013، ص 60.

[84] جميل الشرقاوي، النظرية العامة للالتزام، مصادر الالتزام، دار النهضة العربية، القاهرة 1991 ص5535.

[85] نصت المادة 171 من القانون على أنه : " العقد شريعة المتعاقدين، فلا يجوز نقضه ولا تعديله إلا باتفاق الطرفين أو للأسباب التي يقررها القانون" كما نصت المادة (172) من القانون المدني على أنه: "يجب تنفيذ العقد طبقاً لما اشتمل عليه وبطريقة تتفق مع ما يوجبه حسن النية ولا يقتصر العقد على إلزام المتعاقد بما ورد فيه، ولكن يتناول أيضاً ما هو من مستلزماته، وفقاً للقانون والعرف والعدالة بحسب طبيعة الالتزام" كما أجاز المشرع القطري اجبار المدين على تنفيذ التزاماته العقدية، وعلى ذلك فإن المشرع القطري قد حدد معالم المسؤولية العقدية بأنها اخلال أي

وبتطبيق القواعد العامة للمسؤولية على المسؤولية العقدية للضرر المعلوماتي على مواقع التواصل الاجتماعي فإن خصوصية العقد وكيفية الالتزام به والضرر الناتج عن الإخلال به يستلزم الأمور التالية:

الأول : تحديد أطراف العلاقة التعاقدية والتي من الممكن أن نفترضها في هذا السياق بين مقدم خدمة الإنترنت (مزود الخدمة) وصاحب موقع التواصل والمستخدم والغير (أصدقاء المستخدم) حيث يوجد عقد تزويد خدمة الإنترنت (أوريدو مثلاً) بين المزود والمستخدم مقابل دفع فاتورة الاشتراك وتعهد الطرف الأول بتزويد المستخدم بالاتصال بالشبكة، وهو بعيد عن موضوعنا من حيث الاطلاع على البيانات اللهم إلا إذا نظرنا إلى إمكانية إطلاع المزود على البيانات وإمكانية مراقبتها وهو ما لا يحكمه عقد بينهما وهناك علاقة المستخدم مع صاحب الموقع فيس بوك مثلاً والتي تتضمن تعاقداً لا تتكافأ أطرافه حيث يضع الثاني بنوداً غير واضحة ربما لا يعيرها المستخدم أي انتباه خاصة أنها مجانية مما يجعله يوافق في سبيل قبوله في الصفحة دون أن يلزم صاحب الموقع بحماية بياناته، وهناك علاقة المستخدم بأصدقائه بعد فتحه حساب ونشره بياناته وهى في طبيعة الحال ليست علاقة تعاقدية إلا أنها علاقة يطلع فيها الغير على بياناته الخاصة[86].

الثاني: الضرر وتقدير قيمة التعويض من حيث ضرورة مراعاة خطورة الضرر الذي تحدثه جرائم الإنترنت وما تلحقه بسمعة الأشخاص وكرامتهم فضلاً عن عائلاتهم وسمعتهم في تقدير قيمة التعويض، فالأضرار الناجمة عنها عادةً ما تكون بليغة وتحديد قيمة التعويض من الأيسر أن يترك تقديرها لقاضي الموضوع[87].

الثالث : تنوع أشخاص القائمين بالخطأ وبالتالي صعوبة تحديد المسؤول الحقيقي فقد لا يصدر من مزود الخدمة أو صاحب الموقع ذاته وإنما من شخص مجهول دخل على حساب المستخدم وانتحل شخصيته من مكان عام كما في مقاهي الإنترنت أو المطاعم أو الفنادق حيث يمكن للزوار الدخول إلى الإنترنت واستعارة الرمز السري للمقهى أو المطعم فإذا ثبت من الدليل الرقمي أن الفعل صادر باسم صاحب الحساب ومنح له ترخيص لاستعماله فهل يكون صاحب المقهى أو المطعم أو الفندق

من أطراف العقد بالتزاماته العقدية أو ما يسمى بالخطأ العقدي وأن ينتج عن هذا الخطأ ضرر يرتبط بالخطأ بعلاقة السببية.

[86] مروة زين العابدين صالح، الحماية القانونية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، مرجع سابق ، ص 477-478.

[87] مروة زين العابدين صالح، الحماية القانونية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، مرجع سابق ص 478.

مسؤولاً عن ذلك جنائياً ومدنياً ولو حدث من الغير، طالما أنه مزود الخدمة أو صاحب الموقع أثبت أنه قام بتنفيذ الإجراءات الضبطية المطلوبة منه. كما قد يصدر الخطأ من أحد الأشخاص العاملين لدى مزود الخدمة (شركة فودافون مثلاً) وقد يصدر من أحد العاملين لدى صاحب الموقع (فيس بوك مثلاً)[88].

الرابع: صعوبة إثبات مرتكب الخطأ أمام تعدد الأشخاص المتصلين بالشبكة بين مزود الخدمة باعتباره فاعل أصلي يتعين عليه منع نشر محتوى صفحات الشبكة المتعارضة مع القوانين واللوائح أو المصلحة العامة والمستخدم صاحب الحساب وصاحب الموقع الذي يسجل فيه المستخدمين حساباتهم[89].

واختلفت الآراء حول مسؤولية مزود الخدمة فهناك رأي يرى أنها تتوقف على نوع الخدمة التي يؤديها، فإذا قام بدور الناقل الذي يربط بين حاسوب العميل الشخصي والخادم فهو غير مسؤول عن عدم مشروعية الإعلانات التي تبث عبر الموقع حيث يقوم بتخزين مؤقت للمعلومة التي يقوم بنقلها وبالتالي عمله لا يرتقي إلى عمل متعهد الإيواء فلا يجعله مسؤولاً. أما إذا تعدى دوره إلى متعهد الإيواء الذي يسمح لشركة الإعلانات غير المشروعة، فهذا الدور يمكنه من الاطلاع على الإعلان قبل نشره ومن ثم يكون مسؤولاً عن المحتوى غير المشروع للإعلان[90].

ورأي آخر ذهب إليه الفقه والقضاء الإيطاليين يرى أن دور مزود الخدمة مجرد دور فني خالص لا يتضمن أية رقابة على مضمون أو محتوى الموقع الذي يختاره المستخدم بمحض إرادته لأنه لا يقوم بتوريد المعلومة فقط، بل يؤمن خدمة الوصول إليها يشبه دور من نصح أو أشار على المستخدم ليشتري صحيفة بها إعلان كاذب أو أن يشاهد قناة تبث محتوى غير مشروع[91].

وبتطبيق القواعد العامة في المسؤولية المدنية في مقام حماية البيانات الشخصية على مواقع التواصل الاجتماعي يتضح أن هناك التزامات تقع على عاتق الشخص المسؤول عن معالجة البيانات وفق أحكام المسؤولية العقدية وهو التزامه بتأمين الخصوصية المعلوماتية للمستخدم

---

[88] مروة زين العابدين صالح، الحماية القانونية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، مرجع سابق، ص478.

[89] مروة زين العابدين صالح، الحماية القانونية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، مرجع سابق، ص485.

[90] مروة زين العابدين صالح، الحماية القانونية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، مرجع سابق، ص 486.

[91] مروة زين العابدين صالح، الحماية القانونية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، مرجع سابق، ص 486.

(السرية)؛ لأن المسؤول عن معالجة البيانات الشخصية يلتزم باتخاذ كل الاحتياطات اللازمة من أجل الحفاظ على أمن البيانات من الاعتداء عليها ولا سيما منع أو تغيير أو إفشاء أو إتلاف يمكن أن يقوم به أحد الأشخاص غير المصرح لهم بالاطلاع على هذه البيانات بحيث يستطيع المضرور من معالجة البيانات الشخصية أن يرفع دعوى على المسؤول عن معالجة البيانات الشخصية عبر مواقع التواصل ، وكذلك يترتب عن المسؤولية العقدية حماية المستخدم في مواجهة الغير المسؤول عن انتهاكات خصوصية البيانات الشخصية لمستخدمي مواقع التواصل الاجتماعي، حيث ترتبط الخصوصية بضرورة احترام الحياة الخاصة عبر شبكات مواقع التواصل الاجتماعي، كما ترتب المسؤولية العقدية الحق في حماية الصورة من الاعتداء عليها باعتبارها من الموضوعات التي تشغل الكثيرين لا سيما مع التقدم التكنولوجي؛ وما قد يترتب على ذلك من تهديد لخصوصية الأشخاص من خلال نشر صورهم على مواقع التواصل الاجتماعي لا سيما وأن التقاط أي صورة لشخص معين لا يستغرق سوى ثواني معدودة ؛ وهذا هو ما جعل العديد من التشريعات تسعى إلى توفير الحماية القانونية من الإضرار الناشئة عن الاعتداء على الحق في الصورة كما أسلفنا[92].

كما يلتزم مزود الخدمة، بمنع نشر محتوى صفحات الشبكة المتعارضة مع القوانين والنظم واللوائح أو المصلحة العامة ويكون مسؤولاً مسؤولية تعاقدية في حالة عدم تنفيذ التزامه بتمكين العميل من الدخول للشبكة دون أن يكون مسؤولاً عن محتوى المعلومة باعتباره لا يملك الوسائل الفنية لمراقبة صحة المعلومات ومشروعيتها [93]، وقد يضع شروطاً تعفيه من المسؤولية أو تحد منها، وفي جميع الأحوال يجب عليه أن يتعهد برد رسوم الاشتراك في الخدمة للمستخدم في حالة عدم تنفيذ التزامه التعاقدي. إذ أن تزويد الجمهور بخدمة الربط بشبكة الإنترنت وأساس العلاقة بينه وبين المستخدم قائمة على عقد يتم تحريره بينهما يحدد أطرافه وتاريخ سريانه وشروط فسخه وحدود المسؤولية وعروض الخدمة والمقابل المطلوب. فالمزود يتعهد بربط المستخدم على الشبكة فقط ومن هذا المنطلق لا يكون مسؤولاً مدنياً عن مضمون المعلومة وليست من مهمته المراقبة لأنه لا ينتجها وإنما يعمل على ضمان نقلها ووصولها فنياً دون أن يطلع عليها بحيث يجرده دور الناقل عادةً من أية مسؤولية. كما يكون مسؤولاً عند وقوع الخطأ في إبلاغ الرسالة الإلكترونية إلى المرسل إليه عن سبب راجع إلى أحد العاملين لديه، كما تقوم مسؤوليته أيضاً في حالة انتهاك سرية المراسلات

---

[92] محمد سامي عبد الصادق، شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية، مرجع سابق، ص 97.

[92] محمد سامي عبد الصادق، شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية، مرجع سابق ص 18.

أو المعلومات مالم يكن تدخله تبرره الضرورة الفنية لتشغيل الشبكة وليس لسبب آخر ولا يؤثر في تحقق المسؤولية العقدية أن يكون عدم الوفاء راجع إلى فعل شخص آخر كأحد العاملين لدى مزود الخدمة أو صاحب الموقع ، أو إلى فعل شخص يساعد المدين و يعاونه في تنفيذ العقد بناء على طلبه[94]، ففي كل هذه الأحوال تتحقق مسؤولية المدين عن فعل الغير، ولا يعد فعل هذا الغير من قبيل السبب الأجنبي بالنسبة للمدين إلاّ إذا كان الغير أجنبيا عن المدين[95].

ويعتبر مورد المحتوى غير المشروع ليس هو المسؤول وحده فهناك أكثر من شخص يتدخل في عملية نقل المعلومات فيدخل في نطاق المساءلة ويشمل متعهدي الوصول وكل من يسهل إطلاع المستخدم على المضمون غير المشروع بأي وسيلة مثل: خلق اتصال مباشر بالموقع وتقديم البرامج المقوية للربط المسهلة لتبادل مضمون بين مستخدمي الشبكة، وخلاصة القول. يتعين إقامة المسؤولية لكل شخص على ضوء الدور القائم به ودرجة تدخله في تقديم الخدمة وعلى حسب ظروف كل واقعة على حده وذلك بما لديهم من التقنية والبرامج التي تكشف لهم المحتوى غير المشروع قبل بثه وتحقق للمضرور التمسك بالمسؤولية التضامنية عند الرجوع عليهم بالتعويض عن الضرر الذي أصابه[96].

ويسأل مورد المحتوى أو صاحب الموقع بالالتزام عن خطئه الشخصي حسب ما إذا كان التزامه بتحقيق نتيجة كالالتزام بسرية المعلومات وهنا لا تُدفع المسؤولية إلا بالدليل على السبب الأجنبي الذي حال دون تحقيق النتيجة ونرى أن صاحب الموقع في تعاقده مع المستخدم التزام بتحقيق نتيجة فيما يتعلق بتمكينه من التواصل على مدار الساعة أو أن يقوم مزود الخدمة بالتمكين من الاتصال بالشبكة. أما الالتزام ببذل العناية فإن المدين لا يقوم بتحقيق الهدف النهائي الذي يسعى إليه الدائن، بل يكون مضمون أدائه للالتزام وسيلة للوصول إلى الهدف النهائي، بالمحافظة على سرية البيانات الرقمية كل حسب صلاحياته[97]. وعلاقة السببية هي تلك الصلة التي تربط الضرر بالخطأ فتجعل

---

[94] محمد سامي عبد الصادق، شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية، مرجع سابق ص 485-486.

[95] عبد الرزاق السنهوري، الوسيط في القانون المدني، الجزء الأول، طبعة نقابة المحامين 2006، ص652.

[96] محمد سامي عبد الصادق، شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية، مرجع سابق، ص486- 487.

[97] محمد حسين عبدالعال، تقدير التعويض عن الضرر المتغير، دراسة تحليلية، دار النهضة العربية، 2008، ص32.

الضرر نتيجة للخطأ، فإذا انعدمت هذه الرابطة انتفت المسؤولية لانعدام ركن من أركانها ويقع على الدائن عبء إثبات العلاقة السببية[98] .

المطلب الثاني: المسؤولية التقصيرية.

المسؤولية التقصيرية لها أجنحة ثلاث هي المسؤولية عن الفعل الشخصي والمسؤولية عن فعل الغير والمسؤولية عن الأشياء[99] والمسؤولية عن الأفعال الشخصية هي تلك التي تنجم عن فعل شخصي يصدر من المسؤول والذي يتضمن التدخل المباشر من قبله في إحداث الضرر، وتؤسس مسؤوليته هذه على وجود خطأ يصدر من جانبه والمكلف بهذا الإثبات هو المضرور نفسه، ولا يخفى صعوبة الإثبات في ظل الاعتداء على البيانات الخاصة عبر مواقع التواصل الاجتماعي مما ينتج عنه ضرر مادي حقيقي يتمثل في تحول الحياة الخاصة إلى مشهد عام يعرفه الكافة الخسارة التي تلحق بمن انتهكت خصوصيته أو الكسب الذي يفوته جراء الاعتداء ولكي يحصل المضرور على التعويض عليه أن يثبت خطأ المسؤول ، ولقد اعتبر القضاء أن مجرد وقوع الحادث دليل على وجود الخطأ أو الإهمال وبذلك فإن المنتج لم يكن يستطيع التحلل من المسؤولية إلا بإثبات السبب الأجنبي أو نفي قرينة الخطأ[100].

---

[98] محمد حسين عبدالعال، تقدير التعويض عن الضرر المتغير، مرجع سابق، ص42.

[99] نظم المشرع القطري المسؤولية عن الفعل الشخصي سواء كان مصدره العقد أو كان من الإرادة المنفردة بأن نصت المادة (199) من القانون على أن: "كل خطأ سبب ضرراً للغير يلزم من ارتكبه بالتعويض" ونظم المسؤولية عن فعل الغير في المواد من المادة (208) إلى المادة (213) في مسؤولية متولي الرقابة ومسؤولية المتبوع عن اعمال التابع والمسؤولية عن الأشياء.

[100] تصدى القضاء الكندي لقضية تعرض فيها أحد الأشخاص إلى جروح خطيرة بسبب جزيئات الزجاج التي كانت موجودة في الخبز الذي ابتاعه من بائع الخبز حيث كان معبأً في كيس مغلق تم شراؤه من الشركة المصنعة للخبز فقضت المحكمة بمسؤولية الشركة المنتجة للخبز. كما إن تجربة القضاء الأمريكي كانت تجربة فريدة حيث أقرت فيه بمسؤولية المنتج وهجرت فكرة الخطأ وأسندت مسؤولية المنتج إلى فكرة العيب بمفهومها الواسع والتي تقوم فيها مسؤولية البائع المحترف بغض النظر عن الإهمال أو الخطأ في جانبه. والقضاء العراقي يستطيع اللجوء إلى تفسير النصوص وافتراض الخطأ من جانب البائع المحترف لتسهيل مهمة المضرور، حيث أنه بمجرد إثباته إن مصدر الضرر هو وجود العيب في المنتوج وإثبات العلاقة السببية بينهما تنهض مسؤولية البائع المحترف. يراجع حول ذلك: إياد عبد الجبار ملوكي، المسؤولية عن الأشياء وتطبيقاتها على الأشخاص المعنوية، دراسة مقارنة، مرجع سابق، ص 10.

ومن أشد الأضرار التي تصيب الفرد في خصوصية معلوماته هو أن المعلومات التي تجمع عنه بهدف تحقيق غرض محدد يتم استخدامها ومعالجتها بطريقة تتجاوز الهدف الذي جمعت من أجله، فالانحراف في المعالجة الإلكترونية هو الخروج عن الغاية الأساسية إلى غاية غير مقررة قانوناً كالإساءة إلى السمعة، أو بالمراقبة، أو محو الشخصية، أو الاستغلال التجاري أو من أجل الضغط والابتزاز السياسي وذلك يتمثل بسلوك يصدر من المسؤول ينحرف فيه عن الغرض من المعالجة الإلكترونية للبيانات الشخصية. ويستوي لدى القانون ان يكون الشخص حائزاً لهذه البيانات بغرض تصنيفها أو نقلها أو تسجيلها أو معالجتها تحت أي شكل ويقتضي ذلك لقيام المسؤولية ضرورة تحديد الغاية من المعالجة الإلكترونية فهو المناط في تحديد الانحراف الذي تمت المعالجة للبيانات من أجله[101]، وقد وضع المشرع القطري ضوابط لمعالجة البيانات في قانون حماية البيانات الشخصية أنه لا يمكن معالجة البيانات إلا إذا أعطى الشخص المعني موافقته الصريحة على المعالجة، ما لم تكن المعالجة ضرورية لصيانة مصلحة حيوية أو لغايات الطب الوقائي أو تنفيذ مهمة متعلقة بالصالح العامة[102].

أما المسؤولية عن الأشياء فقد نظمها المشرع القطري في المادتين (121) (213) حيث نصت المادة (212) من القانون المدني على أنه: " كل من يتولى حراسة أشياء تتطلب عناية خاصة لمنع وقوع الضرر منها، يلتزم بتعويض الضرر الذي تحدثه هذه الأشياء، ما لم يثبت أن هذا الضرر وقع بسبب أجنبي لا يد له فيه- وتعتبر من الأشياء التي تتطلب عناية خاصة لمنع وقوع الضرر منها السيارات والطائرات والسفن غيرها من المركبات، والآلات الميكانيكية، والأسلحة والأسلاك والمعدات الكهربائية، والحيوانات، والمباني، وكل شيء آخر يكون بحسب طبيعته أو بحسب وضعه مما يعرض للخطر" ، ونصت المادة (213) على أنه: "يجوز لكل من يهدده ضرر من شيء معين أن يطالب مالكه أو حارسه باتخاذ ما يلزم من التدابير لدرء خطره، وإن لم يقم مالك الشيء أو حارسه باتخاذ التدابير اللازمة لدرء خطره في وقت مناسب، جاز لمن يهدده الخطر أن يحصل على إذن من القضاء باتخاذ هذه التدابير على حساب المالك أو الحارس، ويجوز في حالة

---

[101] محمد سامي عبد الصادق، شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية، مرجع سابق، ص 45.

[102] المادة 4 من قانون حماية البيانات القطري رقم 13 لسنة 2016 نصت أنه:" لا يجوز للمراقب معالجة البيانات الشخصية، إلا بعد الحصول على موافقة الفرد، ما لم تكن المعالجة ضرورية لتحقيق غرض مشروع للمراقب أو الغير الذي تُرسل إليه البيانات".

الاستعجال، لمن يهدده خطر الشيء أن يتخذ ما يلزم من التدابير لدرئه على نفقة مالكه أو حارسه، من غير حاجة إلى إذن القاضي".

وبتطبيق هذه الاحكام على حماية البيانات الشخصية نرى أن الوسيط مستضيف البيانات من الممكن اعتباره حارساً لهذه البيانات أو المعلومات ومسؤولاً عن المحتوى الغير المشروع المحمل من الغير متى كان عالماً بعدم مشروعيته أو تم إعلامه بذلك ولم يتخذ أية إجراءات تمنع ذلك.

المبحث الثاني: أساس المسؤولية عن الضرر الرقمي.

تعتمد المسؤولية المدنية على الضرر المادي سواء كانت في صورتها العقدية حيث تتطلب الضرر المادي أو في حالة المسؤولية التقصيرية التي تتطلب خطأ شخصي حقق ضرر مادي ملموس أو اخلال بحراسة أشياء مادية ترتب عنها الضرر.

والضرر الرقمي أو المعلوماتي فاق كافة صور المسؤولية التقليدية من حيث المخاطر حيث لا يجوز التقليل من مخاطر الضرر المعلوماتي سواء على الأشخاص أو على مستوى الأمن القومي وخاصة عندما تشتغل البيانات ذات الطابع الشخصي في عمليات إرهابية على مواقع التواصل الاجتماعي من قتل الولاء للدولة أو نشر الفتن بها.

ولا نجد أية صعوبة في استصحاب أحكام المسؤولية العقدية التقليدية على العلاقة العقدية بين المستخدم ومواقع التواصل الاجتماعي حيث أن المستخدم عند قيامه باستخدام موقع التواصل الاجتماعي يتطلب منه الموقع ادخال بياناته الصحيحة والموافقة على شروط (سياسات) الموقع التي تعد مضمون شروط التعاقد والتي عادة ما يقبلها المستخدم لكي يتمكن من استخدام الموقع وهذا التعاقد أضحى صورة يومية من التعاقدات المشروعة المعروفة التي نمارسها في صورة العقد الالكتروني.

وتثور المشكلة في مدى جواز انسحاب قواعد المسؤولية عن الأشياء بشكلها التقليدي أو الكلاسيكي على المسؤولية عن الضرر الرقمي في مواقع التواصل الاجتماعي- ولذا فإننا سنتطرق إلى تأصيل الأساس القانوني للمسؤولية التقصيرية في صورتها المسؤولية عن حراسة الأشياء على الضرر الرقمي ، ويثور التساؤل حول ما إذا كانت المعلومة أو البيانات الشخصية مجرد أشياء غير محسوسة بل تتكون من نبضات الكترونية غير ملموسة فيقاس الضرر المعلوماتي على الضرر من التيار الكهربائي ثم على الضرر من الآلات الكهربائية على اعتبار أن الحاسوب آلة تعمل بالكهرباء أم اعتبار هذه البيانات في حكم المادة ذات القيمة المادية وتدخل ضمن المسؤولية عن ضرر الأشياء؟.

المطلب الأول: الاتجاه التقليدي للمسؤولية عن الضرر المعلوماتي

كما أوضحنا أن المسؤولية عن الأشياء في القانون القطري هي مسؤولية مفترضة لا يتطلب من المضرور إثبات خطأ الحارس، إذ يكفي لنجاح دعوى الغير إثبات الضرر وعلاقة السببية بينهما ويستطيع الحارس التخلص من المسؤولية بإثبات العكس.

ولا يخفى أن هذا الأساس في المسؤولية عن الضرر المعلوماتي للبيانات ذات الطابع الشخصي على مواقع التواصل الاجتماعي سيصطدم بالقصور والجمود أمام هذه الفكرة حيث أن المسؤولية عن الأشياء في الضرر المعلوماتي معقدة ما بين تداخل أكثر من شخص تجاه البيانات ذات الطابع الشخصي بداية من المستخدم ذاته وأصدقائه على الموقع والمسموح لهم بالتداول ورؤية بياناته ومالك الموقع والشركات المتعاقد معها بشان إدارة محتوى الموقع أو تحليل البيانات أو متعهد الايواء الذي يستضيف موقع التواصل الاجتماعي، كما أن النصوص التقليدية تحصر مفهوم الأشياء في الآلات والمعدات وعلى وجه عام الأشياء المادية حيث أنه هناك جدل فقهي حول الطبيعة القانونية للبيانات الرقمية فيما هل لها قيمة في ذاتها أم أنها تتمثل في مجموعة من القيم القابلة للاستثناء يمكن الاعتداء عليها مستقلة عن دعامتها المادية، ونعتقد أن المشرع الليبي أحسن عندما حسم الجدل الفقهي بأن أردف فقرة ثانية إلى المادة 444 من قانون العقوبات المتعلقة بالسرقة نص فيها : "ويعد من الأموال المنقولة في حكم قانون العقوبات الطاقة الكهربائية وجميع أنواع الطاقة ذات القيمة الاقتصادية"[103].

ونرى أن المشرع القطري يستقر على أن قرينة الخطأ في جانب الحارس قرينة قاطعة غير قابلة لإثبات العكس إلا بالسبب الأجنبي، أي إنه يستطيع دفع مسؤوليته بإثبات أن وقوع الضرر إنما يرجع إلى سبب أجنبي وهذا الأمر عادة ما يكون في صالح مواقع التواصل الاجتماعي التي تملك الكثير على تدخل أسباب أجنبية أحدثت الضرر في حين أنها على علم بكل ما يحدث للبيانات وتدفع مسؤوليتها بأن المستخدم كان السبب المباشر في حدوث الضرر عندما سمح للأخرين بالاطلاع على بياناته ذات الطابع الشخصي. وقد أحسن المشرع القطري بالأخذ بما ذهب اليه القضاء الفرنسي

---

[103] الجريمة الإلكترونية والتغلب على تحدياتها، ورقة مقدمة من د. مفتاح بوبكر المطردي، المستشار بالمحكمة العليا الليبية إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية بجمهورية السودان المنعقدة في 23-2012/9/25 ص 24، أشارت إليها: مروة زين العابدية صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، مرجع سابق، ص455.

[103] مروة زين العابدية صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، مرجع سابق، ص 485-586.

من نظرية تجزئة الحراسة بين كل من يتداخل بيده ولو بصفة عابرة على الشيء لأنها تحقق العدالة بدء من المالك إلى الحارس الفعلي أو الحارس العابر وأن هذه النظرية تساعد على وضع الحد الفاصل بين خطأ كل من ساهم بالضرر[104].

المطلب الثاني: الاتجاه الحديث للمسؤولية عن الضرر المعلوماتي للبيانات

كل شيء منقول يعد منتج- هذه المقولة هي من أدت إلى معاملة كافة صور التكنولوجيا الحديثة والتعويض عنها، والمعلومة في الحقيقة منتج منقول، وهي تعد غير مصانة عندما لا تتوفر فيها السلامة المطلوبة أو استعمالها أو استغلالها على نحو يخالف الغاية منها، والمعلومة لها كذلك قيمة اقتصادية ويمكن تقويمها بمال- هذه كانت أهم ما يعطل أحكام المسؤولية التقليدية ومدى جواز جعلها تشمل الضرر الرقمي فضلاً عن اشكاليتي المسؤولية الجماعية وحدود المسؤولية بين كافة المسؤولين أمام هذا الضرر[105].

والفقه الإسلامي يعترف بأن المعلومة مال مقوم حيث يقر جمهور الفقه من غير الحنفية أن أساس مالية الشيء أن تكون له قيمة بين الناس وأن تكون هذه القيمة مما ينتفع به انتفاعاً جائزاً شرعاً فلا قيمة للمنفعة غير المشروعة- خلاف الاحناف الذين يشترطون مادية الشي وإمكانية حيازته وأن أساس المسؤولية عن ضرر المعلومة في الفقه الإسلامي أو ما يسمى بالضمان حيث أن لفظ المسؤولية في الفقه هو الضمان، وتعتمد نظرية الضمان في الفقه الإسلامي على المباشرة والتسبب وأنه يلزم التفرقة بين وجود رابطة عقدية أو عدم وجود رابطة عقدية حيث أنه عند وجود رابطة عقدية فإن الأساس هو الاخلال بالعقد وفي حالة عدم وجود رابطة عقدية فإن الأساس هو ضمان العدوان الناشئ عن الحكم الشرعي وأن أصل الضمان هو الضرر سواء كان الخطأ مباشر أو

---

[104] نبيلة إسماعيل رسلان، المسؤولية في مجال المعلومات والشبكات، مجلة روح القوانين، كلية الحقوق، جامعة طنطا، العدد 18 سنة 1999، ص 46.

بالتسبيب وسواء كان الفعل عمدي أو غير عمدي[106] ويرسخ الفقه الإسلامي فكرة الاثبات على نوع الخطأ ففي حالة الخطأ المباشر فالخطأ مفترض وواجبة الاثبات في حالة التسبب[107].

المبحث الثالث: عناصر المسؤولية عن الضرر المعلوماتي.

يخضع نشر المعلومة على مواقع التواصل الاجتماعي في المبدأ لذات القواعد المطبقة على نشرها بالطريقة التقليدية ولتحديد مسؤولية وسيلة التواصل الاجتماعي عن المحتوى بموقع التواصل الاجتماعي يجب التفرقة بين الناشر والوسيط ومدى رقابة مواقع التواصل الاجتماعي على المحتوى المنشور من قبل المستخدمين ومقارنة مسؤولية وسيلة التواصل الاجتماعي بتلك العائدة على مستضيف البيانات.

ومسؤولية مواقع التواصل الاجتماعي لا تأتي فقط عن البيانات التي تنشرها إنما ايضاً عن حماية البيانات ذات الطابع الشخصي على موقعها باعتبارها حارس هذه المعلومة بجانب المستخدم وقد تسمح للأخرين بتجميع البيانات وتحليلها أو نشرها أو استغلالها.

وفي هذا المبحث سيتم التطرّق إلى أطراف المسؤولية القانونية عن المساس بالبيانات ذات الطابع الشخصي على مواقع التواصل الاجتماعي (الفرع الأول) ومدى حقيقة حراسة الموقع لهذه البيانات ورقابته على المحتوى الخاص بالمستخدم (الفرع الثاني) ومقارنة مسؤولية الموقع مع الاستفادة العائدة على المستخدم (الفرع الثالث).

المطلب الأول: أطراف المسؤولية عن الضرر المعلوماتي للبيانات

إنّ أطراف العلاقة في مواقع التواصل الاجتماعي هم المستخدم وأصدقائه والعامة المسموح لهم برؤية منشوره وصفحته والموقع الخاص بالتواصل وتابعين هذا الموقع والشركات المتعاقدة معه لإدارة المحتوى أو تجميع وتحليل البيانات وكذلك متعهد إيواء الموقع ولذلك فإن تحديد المسؤولية ليس بالأمر الهين وهو ما خلصنا إليه من ضرورة الأخذ بالنظرية الفرنسية القائلة بتجزئة المسؤولية.

---

[106] في الفقه المالكي أبو إسحاق بن موسى بن محمد الشاطبي تحقيق مشهور بن حسن ال سلمان، دار ابن عفان، المملكة العربية السعودية-1997-ج2-ص32 وفي الفقه الشافعي الاشباه والنظائر جلال الدين عبد الرحمن السيوطي دار الكتب العلمية بيروت 1990 ص327.

[107] حسين حامد حسان، فقه المصلحة العامة وتطبيقاته المعاصرة بحث مقدم إلى الندوة الرمضانية الثانية، المعهد الإسلامي للبحوث والتدريب 1993.

وبداية فإن الشخص الذي يقرر وضع بياناته على مواقع التواصل الاجتماعي يتحمّل المسؤولية عن المساس ببياناته من حيث قيامه بالسماح للأخرين بمعالجة بياناته حيث أن من يحدد نطاق حماية بياناته هو المستخدم عندما يقرأ الشروط التي يضعها موقع التواصل الاجتماعي أو وسائل ضبط النشر وبيان الخصوصية الموجودة كوسائل تقنية للعميل تظهر له على موقع التواصل الاجتماعي يكون له الخيار في تضييق واتساع نطاق الخصوصية ومن ثم المسؤولية عن طريق التدقيق في القراءة قبل الموافقة على الخيارات المطروحة - وإن كان عملياً ينذر ذلك – وفي هذه الحالة يتمكن من حماية بياناته بأن يثبت بأنه لم يوافق على إعطاء هذه المساحة للأصدقاء والعامة والزائرين أو أن الموقع لديه التحكم والرقابة على من يطلع على هذه البيانات دون إذن المستخدم وكذلك القدرة على اختيار ما قد ينشر ومن له الحق في مراقبة المحتوى قبل نشره، ومن هنا تنتج مسؤولية الوسيط وقد تتم إدارة المحتوى ومراقبته قبل نشره وقد تتم بعد نشره، أي أن يتم نشره بشكل آني ومباشر مع القدرة من قبل الوسيط على سحبه إذا تبين أن هذا المحتوى غير مشروع ويطبق ذات المبدأ على التعليقات الواردة على المحتوى المنشور[108].

والفقه الفرنسي يميز بين الناشر والمستضيف على الانترنت حيث أن مستضيف البيانات هو من يوفر استضافة المواقع الإلكترونية والصفحات الخاصة بالمستخدمين وتخزين النصوص والصور والصوت على خادمه المركزي مع تمكين الأشخاص الذين يحددهم المستخدم من الاطلاع عليه[109].

بينما تعريف الناشر بأنه المقدم الذي له سلطة تحديد المحتوى الموضوع بتصرف الجمهور وبالتالي يتم التفريق بين الناشر وبين المستضيف تبعاً لقدرته على التصرف بخصوص المحتوى الموضوع على الانترنت ، فالتباين بين الدور السلبي والدور الإيجابي حيال المحتوى المتاح عبر الشبكة هو المعيار الحاسم في التمييز بين ناشر خدمات الاتصال ومتعهد الإيواء أو مستضيف البيانات ، فتنشأ مسؤولية الأول عن الأضرار الناجمة عن المحتوى الذي يختاره ويراقبه ، ولا تقوم مسؤولية متعهد

---

[108] محمد سامي عبد الصادق، شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية، مرجع سابق ص 59-60.

[109] عرفته المادة السادسة من القانون الفرنسي الصادر في شأن الثقة في الاقتصاد الرقمي بأنه " الشخص الطبيعي أو الاعتباري الذي يؤمن ولو بالمجان، تخزين الإشارات والنصوص والصور والصوت أو الرسائل بمختلف أنواعها والتي تقدم للمستفيدين من هذه الخدمة". أشار إليه : محمد سامي عبد الصادق، شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية، مرجع سابق ص 29.

الإيواء لأنه لا يملك شيئاً حيال هذا المحتوى ما لم يمتنع عن اتخاذ الاحتياطات اللازمة للحيلولة دون الوصول إلى هذا المحتوى عند التحذير من عدم مشروعيته[110].

ويرى فقه القانون أن الوسيط في وضع مستضيف البيانات ، حتى لو كانت لديه القدرة على مراقبة المحتوى فقد لا يعرف بطبيعة هذا المحتوى حتى يتمكن من مراقبته ،إلا أن مسؤوليته تقوم في حال معرفته بأن المحتوى الموضوع من قبل الغير يحقق نشاطا غير مشروع أو أنه يقصر في رسم اطار الحماية لعدم المساس بالبيانات الشخصية أو قيامه مباشرة بالخطأ (الخطأ الشخصي) أو كانت التكنولوجيا المستخدمة غير كافية وقاصرة في الحماية أو إذا كان لديه معرفة بالظروف التي تجعل الطابع غير المشروع ظاهراً أو في حال إبلاغه بذلك، ولا يتصرف لسحب المحتوى أو يتصدى للسلوك غير المشروع وعلى المحاكم التحقق في كل حالة من ذلك [111].

ومزود خدمة الانترنت يستطيع بحكم مهمته الاطلاع على المعلومات، وقد يتم استغلالها من قبل أحد موظفيه ممن هم من أصحاب النفوس الضعيفة وعلى الرغم من افتراض وجود التزام تعاقدي في العقد الذي يقدمه المزود على حماية خصوصية بيانات المستفيد الشخصية، وهو ما يجعل مزود الخدمة مسؤولاً مسؤولية تعاقدية عن انتهاك خصوصية الآخر. ودور المزود يشبه دور إدارة البريد يمكن أن تنتفي مسؤوليته مدنياً في حالة وجود شرط يعفي من المسؤولية عند إبرام العقد مالم يكن شرطاً تعسفياً يتنافى والقواعد العامة [112]، ويمكن اعتبار مزود خدمة الاتصال بالإنترنت في دولة قطر هما شركتي فودافون وشركة أوريدو[113] فالتوقيع على نموذج الطلب الخاص بالخدمة يقتضي موافقة العميل على شروط وأحكام تضعها الشركة من بينها:"

---

[110] محمد سامي عبد الصادق، شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية، مرجع سابق ص 30.

[111] محمد نصر محمد، المسؤولية الجنائية لانتهاك الخصوصية المعلوماتية دراسة مقارنة، مرجع سابق، ص 85-86.

[112] تقرير مسؤولية مزود الخدمة يتطلب أن يكون دوره إيجابياً في مراقبة المعلومات كما أنه قد لا يملك الوسائل الفنية التي تمكنه من مراقبة تلك المعلومات المتدفقة بأعداد تتجاوز الملايين وهناك اتجاهين حول مسؤولية مزود الخدمة. أنظر تفصيل ذلك: محمد نصر محمد، المسؤولية الجنائية لانتهاك الخصوصية المعلوماتية دراسة مقارنة، مرجع سابق، ص 79.

[113] شركة أوريدو المعروفة سابقاً اتصالات قطر (كيوتل) وهي الشركة الأقدم في قطر والمزود الأول لخدمات الاتصالات تم تأسيسها في عام 1987.

- ضرورة قيام العميل بتزويد الشركة بالمعلومات والبيانات الشخصية كشرط لتزويده بالخدمة وأن أوريدو تقوم بتخزين واستخدام تلك المعلومة لتركيب وإعداد الخدمة وتقديمها للعميل وإرسال الفواتير الخاصة باستخدام الخدمة.
- أن أوريدو تحمي وتحترم معلومات العميل الشخصية، ولن نقوم بجمع، أو استخدام، أو الاحتفاظ، أو الإعلان عن أية معلومات بدون موافقته الخطية المسبقة وبما يتماشى مع القانون.
- أنه يجوز للعميل (طالب الخدمة) طلب تصحيح أو إزالة أية معلومات شخصية مخزنة في قواعد البيانات.
- أنه يجوز لأوريدو مراقبة وتسجيل المكالمات المتعلقة بخدمات العميل على أن يفصح عن تسجيل تلك المكالمات في بداية كل مكالمة، ويتم تسجيل المكالمات لأغراض التدريب أو لتحسين جودة خدمات العملاء.
- أنه يجوز لأوريدو تسجيل جميع مكالمات الطوارئ". [114]

ومن هذا نستنتج أن مزود الخدمة هو شركة أوريدو في هذا التطبيق بالرغم من أن دورها يقتصر على ربط العميل بالشبكة وتقديم خدمة الإنترنت، إلا أن ذلك لا يمنع أحد موظفيها من الاطلاع على البيانات والمعلومات فهي متاحة لديه والتساؤل الذي يطرح نفسه ما هو الضامن لعدم استغلالها بما يمس بخصوصية العميل؟ وهنا تكون الشركة مسؤولة مسؤولية عقدية عن ما يقوم به أحد موظفيها نتيجة إخلالها بالتزام تعاقدي ينص عليه العقد المبرم مع العميل والذي بموجبه قام بالإدلاء بالبيانات الشخصية الخاصة به لحصوله على خدمة الإنترنت نظير مقابل مادي ، غير أن بعض مزودي الخدمة قد يستفيد من البيانات الشخصية التي بحوزته والتي يحصل عليها بطريقة مشروعة وبرضى من أصحابها لاستغلالها تجارياً بأن يعيد بيعها لشركات أخرى قد تستفيد منها بما يستدعي التمييز بين استغلالها والاطلاع عليها كأرقام مجردة عن دلالتها لأصحابها وبين بيانات تعكس شخصيات الأفراد وتدل عليهم فأرى أن ليس هناك ما يمنع قانوناً من تداولها كأرقام وإحصائيات طالما أنها لا تمس بخصوصية الآخرين.

---

[114] موقع شركة أوريدو، الشروط والأحكام العامة لخدمات الأفراد، تاريخ الدخول: 2021/1/29 ، الوقت: 12:55 .

الرابط الإلكتروني :

https://www.ooredoo.qa/portal/OoredooQatar/ar/general-terms-and-conditions.

ولم ينص المشرع القطري في قانون حماية البيانات الشخصية صراحة على التزامات مزود خدمة الإنترنت وهو جانب قاصر في القانون حيث نص على احترام خصوصية البيانات بصفة عامة دون تحديد صريح لمهام المزود. ولذلك يقترح الباحث أن يسن قانون حماية الخصوصية الشخصية على الشبكة العنكبوتية (الإنترنت) ينظم التزامات مزود خدمة الإنترنت وعلاقته بالمستخدم كأن يفرض على المزود أن يحصل على موافقة صريحة مكتوبة إلكترونيا أو يدوياً لجمع المعلومات الشخصية للمستخدم حسب نوع الخدمة المطلوبة نظير حصول الأخير عليها وتحديد الإطار المسموح للبيانات التي يجوز للمزود جمعها، وأن يقدم إشعارا واضحا وصريحا بالتزامه بجمع معلومات التعريف الشخصية المتفق عليها وحمايتها وعدم التعرض لها حتى من قبل الموظفين القائمين على هذه الخدمة ، كما يجب إلزام مزودي الإنترنت بإخطار المستخدمين بأية تغييرات أو تطورات في النظام الخاص بحفظ البيانات الذي تتبعه الشركات إذا كان من شأنه المساس بسرية بيانات التعريف الشخصية ، وأن يكون المزود مسؤولاً مسؤولية مدنية عن الفعل الخاطئ الذي يقوم به إذا ما تسبب في ضرر للمستخدم فضلاً عن مسؤوليته الجنائية عن الجرم المرتكب في مواجهة الأخير، على أن يستثنى من التزامات المزود بحماية الخصوصية بعض المتطلبات الطارئة التي توسع من صلاحيات المزود كالحالات التي نصت عليها المادة 21 من القانون رقم (14) لسنة 2014 الخاص بمكافحة الجرائم الإلكترونية والتي تجيز لمزود الخدمة الأمور التالية: "

1- تزويد الجهة المختصة، أو جهات التحقيق والمحاكمة، بجميع البيانات والمعلومات اللازمة التي تساعد في كشف الحقيقة، بناءً على أمر من النيابة العامة.
2- اتخاذ الإجراءات اللازمة لحجب روابط الشبكة المعلوماتية، بناءً على الأوامر الصادرة إليه من الجهات القضائية.
3- الاحتفاظ بمعلومات المشترك لمدة سنة.
4- الاحتفاظ المؤقت والعاجل ببيانات تقنية المعلومات أو بيانات المرور أو معلومات المحتوى لمدة تسعين يوماً قابلة للتجديد، بناءً على طلب الجهة المختصة أو جهات التحقيق والمحاكمة.
5- التعاون ومساعدة الجهة المختصة في جمع أو تسجيل المعلومات والبيانات الإلكترونية وبيانات المرور، بناءً على الأوامر الصادرة إليها من الجهات القضائية".

وتعرضت بعض التشريعات لمسؤولية مزودي خدمة الإنترنت منها:

أولاً / التوجيه الأوروبي الخاص بالتجارة الإلكترونية: أقرت نصوصه[115]عدم التزام الوسطاء الفنيين برقابة مشروعية المعلومات والإعلانات التي تبث غبر الموقع وإنما فرضت عليهم أن يتصرفوا بشكل مناسب لمنع الوصول الغير المشروع للمحتوى، كما أعفت مواده مزود خدمة الإنترنت من مسؤوليته عن الأعمال غير المشروعة التي يتضمنها الموقع بشروط معينة وهي: "

1- ألا يكون مزود الخدمة مصدراً للضرر.

2- ألا يكون هو من اختار المرسل إليه الذي ينقل إليه المعلومات.

3- ألا يختار المعلومات التي يقوم بنقلها أو يعدل فيها.

كما ينص التوجيه على أن مزود الخدمة يقوم بتخزين مؤقت للمعلومات التي يقوم بنقلها لكن هذا التخزين المؤقت لا يجعله مسؤولاً ولا يجعل عمله يرقى إلى عمل متعهد الإيواء"، ومن ثم لا يسأل مساءلته، ويجوز للدول الأعضاء أن تنص في قوانينها الداخلية على التزم مزود الخدمة بأن يوقف الخدمة ويستبعد المحتوى غير المشروع للموقع [116].

ثانياً / موقف المشرع الفرنسي من مسؤولية مقدمي خدمة الإنترنت[117]:

نصت المادة (14) من قانون 1 أغسطس لسنة 2000 على أن: " الأشخاص الطبيعيين أو المعنويين الذين يتعهدون بشكل مجاني أو بمقابل، بالتخزين المباشر والمستمر من أجل وضع المعلومات تحت تصرف الجمهور بكتابات، أو رسوم، أو صور، أو رسائل يمكن استقبالها لا يسألون جنائياً أو مدنياً عن محتوى هذه الخدمات، وأنه يمكن مساءلة مقدمي خدمة الإيواء عن عدم اتخاذ الاحتياطات المناسبة في حالة تحذيرهم بعدم مشروعية المضمون".

فالأصل عدم مسؤولية الأشخاص القائمين على تخزين المعلومات على هذه البيانات والمعلومات لا جنائياً ولا مدنياً إلا في حالتين:

الأولى: لجوء مستخدم الشبكة إلى القضاء ولم يقم القائم بالتخزين أو متعهد الإيواء باتخاذ اللازم بمنع وصول المحتوى للجمهور رغم طلب المستخدم صاحب الخصوصية لهذا المحتوى.

---

[115] التوجيه الأوروبي الصادر في 17 يونيو عام 2000، المبحث الرابع (المواد من 12-15) المنظمة لمسؤولية المؤديين المهنيين والمادة (12/1) من ذات التوجيه التي أعفت من المسؤولية.

[116] مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، مرجع سابق، ص 488.

[117] القانون الصادر في أول أغسطس 2000 معدلاً بعض أحكام القانون رقم 30 سبتمبر سنة 1986 المتعلق بالاتصالات السمعية والبصرية.

الثانية: إذا أخطره الغير بأن المحتويات التي يتم تخزينها غير مشروعة وتسبب له أضرار ولم يقم القائم على تخزين المحتوى باتخاذ الإجراءات اللازمة لمنع بثها ونشرها.

ثالثاً / التشريع الأمريكي [118]:

نظم قانون حماية حق المؤلف عبر شبكة الإنترنت، الصادر في 28 أكتوبر 1998 والداخل حيز النفاذ في 1 أكتوبر 2000 في المادة 2/5 منه حيث اعتبر مزود الخدمة غير مسؤول عن المحتوى الغير مشروع لهذه المعلومات.

رابعاً / التشريع الكويتي [119]:

نظم القانون رقم 70 لعام 2002 التزامات مقدمي خدمة الإنترنت المتمثلة في الالتزام بتركيب وتشغيل أنظمة الرقابة لمنع المواقع الإباحية أو المواد المخالفة للدين والعادات والأمن وبالوسائل المختلفة مثل صفحات الإنترنت أو ضبط برامج المحادثة أو البريد الإلكتروني مع ضرورة التحديث المستمر للأنظمة الرقابية لتغطية التطورات التي تطرأ على المواقع والعناوين ، كما يلتزم مزودو خدمة انترنت بتسجيل البيانات الأساسية لمستخدمي الشبكة وحفظها بما يمنع وصول الغير فيها بدون إذن أصحابها كما يمتنع على مزودي خدمة الإنترنت تقديم هذه الخدمة لمن هم دون سن الثامنة عشرة.

سادساً / التشريع القطري:

لم ينص المشرع القطري في قانون حماية البيانات الشخصية صراحة على التزامات مزود خدمة الإنترنت وهو جانب قاصر في القانون حيث نص على احترام خصوصية البيانات بصفة عامة دون تحديد صريح لمهام المزود ونقترح أن يسن قانون حماية الخصوصية الشخصية على الشبكة العنكبوتية (الإنترنت) ينظم التزامات مزود خدمة الإنترنت وعلاقته بالمستخدم كأن يفرض على المزود أن يحصل على موافقة صريحة مكتوبة إلكترونيا أو يدوياً لجمع المعلومات الشخصية للمستخدم حسب نوع الخدمة المطلوبة نظير حصول الأخير عليها وتحديد الإطار المسموح للبيانات التي يجوز للمزود جمعها، وأن يقدم إشعاراً واضحاً وصريحاً بالتزامه بجمع معلومات التعريف الشخصية المتفق عليها وحمايتها وعدم التعرض لها حتى من قبل الموظفين القائمين على هذه الخدمة ، كما يجب إلزام مزودي الإنترنت بإخطار المستخدمين بأية تغييرات أو تطورات في النظام الخاص بحفظ البيانات الذي تتبعه الشركات إذا كان من شأنه المساس بسرية بيانات التعريف

---

[118] مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، مرجع سابق، ص491.

[119] مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، مرجع سابق ص 491.

الشخصية، وأن يكون المزود مسؤولاً مسؤولية مدنية عن الفعل الخاطئ الذي يقوم به إذا ما تسبب بضرر للمستخدم فضلاً عن مسؤوليته الجنائية عن الجرم المرتكب في مواجهة الأخير، على أن يستثنى من التزامات المزود بحماية الخصوصية بعض المتطلبات الطارئة التي توسع من صلاحيات المزود كالحالات التي نصت عليها المادة 21 من القانون رقم (14) لسنة 2014 الخاص بمكافحة الجرائم الإلكترونية والتي تجيز لمزود الخدمة الأمور التالية : "

1- تزويد الجهة المختصة، أو جهات التحقيق والمحاكمة، بجميع البيانات والمعلومات اللازمة التي تساعد في كشف الحقيقة، بناءً على أمر من النيابة العامة.
2- اتخاذ الإجراءات اللازمة لحجب روابط الشبكة المعلوماتية، بناءً على الأوامر الصادرة إليه من الجهات القضائية.
3- الاحتفاظ بمعلومات المشترك لمدة سنة.
4- الاحتفاظ المؤقت والعاجل ببيانات تقنية المعلومات أو بيانات المرور أو معلومات المحتوى لمدة تسعين يوماً قابلة للتجديد، بناءً على طلب الجهة المختصة أو جهات التحقيق والمحاكمة.
5- التعاون ومساعدة الجهة المختصة في جمع أو تسجيل المعلومات والبيانات الإلكترونية وبيانات المرور، بناءً على الأوامر الصادرة إليها من الجهات القضائية".

ويجب تبصير المستخدم بأن أغلب شبكات التواصل الاجتماعي تتيح لمستخدميها إمكانية الإبلاغ عن انتحال شخصياتهم عبر الشبكة بأن تقوم بحذف الحساب الخادع بعد التأكد من انتحال الشخصية ويكون للمستخدم الحق في القيام على المنتحل بدعوى المسؤولية فضلاً عن الجزاءات المنصوص عليها في قانون العقوبات. باعتبارها من الجرائم الإلكترونية المعاقب عليها لما فيها من تعد على الخصوصية كالقانون الفرنسي للتوجيه والبرمجة لأداء الأمن الداخلي الذي نص على أنه: "يعاقب بالحبس مدة سنة وبغرامة مقدارها خمس عشرة ألف يورو كل من انتحل الهوية الشخصية عبر شبكة الإنترنت" [120].

ففي حالة دخول أشخاص مجهولين إلى الموقع مما ينتج عنه زيادة المخاطر على عاتق الوسيط والموقع في حال عدم تعريف المستخدم عن نفسه ، ويكون بالتالي مسؤولاً عن المحتوى المنشور-

---

[120] القانون الفرنسي للتوجيه والبرمجة لأداء الأمن الداخلي الصادر برقم (267) لسنة 2011م بتاريخ 11 مارس 2011 الذي نص في الفصل الثاني الخاص بمكافحة الجرائم الإلكترونية على إضافة فقرة إلى المادة (4-226) من تقنين العقوبات الفرنسي، أشار إليه : محمد سامي عبد الصادق، شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية، مرجع سابق، ص 90.

ولهذا، يمنع بعض الوسطاء التعليقات أو المحتوى الصادر عن أشخاص غير معرّف عنهم- ولذلك يجب على الأشخاص حتى يستخدموا الموقع أن يعرّفوا عن أنفسهم، لكن بالنسبة للشخص الذي يضع بيانات شخصية ويحجب هويته، فإن حجب الهوية هي وسيلة لتخفيف المخاطر عن الوسيط في حالة اعتداء على بيانات هذا الشخص المجهول أما في حالة العكس بأن الاعتداء من شخص مجهول فإن حجب الهوية تشكل نوع من نقل المسؤولية عن البيانات من المستخدم إلى مشغل أو صاحب الموقع الذي يقبل بتمكين المجهول من البيانات، طالما كان لصاحب الموقع رقابة من قبله على المحتوى وأنه في حال عدم وجود الرقابة على المحتوى العائد للمستخدمين المجهولين فإنه يكون مسؤولاً فور علمه بالطابع غير المشروع للمحتوى وعدم التصدي لذلك[121].

وفي هذه الفرضية اشتهرت قضية الممثلة الأمريكية (Christiane Carafano) التي قامت برفع دعوى أمام المحكمة المختصة بولاية (كاليفورنيا) على شركة (Metrosplash.com) المالكة لموقع التواصل تطالب بتعويضها عن الأضرار التي لحقت بها جراء تزويد الموقع بالبيانات الشخصية الخاصة بها حيث أنه لم يتم إغلاق الصفحة التي تحمل بياناتها إلا بعد فترة طويلة من إخطارها مقدم خدمة التواصل مما اضطرها الخروج وابنها من منزلها والانتقال إلى مكان آخر، وتدور وقائع شكواها حول قيام شخص مقيم في برلين بألمانيا بعمل بإنشاء صفحة على ذات موقع (Metrosplash.com) للتواصل ونسبها إلى الممثلة بوضع صورتها وعنوان منزلها والبريد الإلكتروني الخاص بها -أي حجب هويته الحقيقية وانتحل شخصيتها-مما تسبب في تلقيها رسائل تحمل تحرشات جنسية وعبارات تهديد بالبريد الصوتي من قبل مستخدمي الموقع ما دعاها إلى إخطار مقدم خدمة التواصل بوجوب إغلاق الصفحة لما تمثله من انتهاك لحقها في احترام حياتها الخاصة ، وقد انتهت المحكمة إلى أن مقدمة خدمة التواصل لا يعد مورداً للمحتوى المعلوماتي ومن ثم لا يكون مسؤولاً عن تعويض الأضرار ومستخدم الموقع وحده المسؤول قانوناً عن انتهاك خصوصية الممثلة باعتباره هو المورد للمحتوى المعلوماتي، وهو ما أكدته المحكمة الاستئنافية التي استأنفت أمامها الممثلة [122].

ومن هذا نخلص إلى أن مورد المحتوى بغض النظر عن كونه ذات الشخص الذي قام بتقديم خدمة التواصل الاجتماعي من عدمه يقع على عاتقه عبء احترام خصوصية الآخرين وعدم انتهاك

---

[121] مروة زين العابدين، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، مرجع سابق ص 329-330.

[122] محمد سامي عبد الصادق، شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية، ص 20- 21.

حقوقهم ويجب أن يتولى رقابة مضمون المحتوى والتأكد من مشروعيته وألا يتضمن تحريضا على ارتكاب جرائم أو بث اشاعات مغرضة تضر بمصالح الغير وإلا وقع تحت طائلة القانون.

وتجدر الإشارة إلى التعريف الذي أخذ به المشرع القطري لأطراف العلاقة على المحتوى في قانون الاتصالات القطري رقم (34) لسنة 2006 حيث أورد في المادة (1) من هذا القانون: " أن العميل هو الشخص المشترك أو المستخدم لخدمات الاتصالات، سواء كانت هذه الخدمات لاستعماله الخاص أم لإعادة البيع وأن مقدم الخدمة هو الشخص الذي يرخص له بتقديم خدمة أو أكثر من خدمات الاتصالات للجمهور، أو يرخص له بتملك أو إنشاء أو تشغيل شبكة اتصالات لتوفير خدمات الاتصالات للجمهور".

كما عرّف المشرع القطري أطراف العلاقة في قانون حماية البيانات الشخصية حيث أورد في المادة (1) من هذا القانون أن: " المراقب هو الشخص الطبيعي أو المعنوي الذي يقوم منفرداً أو بالاشتراك مع آخرين بتحديد كيفية معالجة البيانات الشخصية والغرض منها، والمعالج هو الشخص الطبيعي أو المعنوي الذي يقوم بمعالجة البيانات الشخصية لصالح المراقب".

والسؤال الذي يطرح نفسه هو من المسؤول الحقيقي عن معالجة البيانات في مواقع التواصل الاجتماعي هل هي مواقع التواصل الاجتماعي وحدها؟ أم أن المستخدم يسأل أيضا معها ؟، ونرى أن وسيلة التواصل الاجتماعي لا تكون مسؤولة الا في حالة معالجة بيانات المستخدم أو مراقبة المحتوى الخاص به أو معرفتها الفعلية بطابعة غير المشروع دون اتخاذ أي إجراءات لحماية حساب المستخدم رغم إبلاغها بذلك، عدا ذلك يكون المستخدم المسؤول الأول عن أعماله والمحتوى المحمل من قبله باعتباره صاحب المحتوى.

المطلب الثاني: رقابة وسائل التواصل الإجتماعي على المحتوى المحمل من المستخدمين

في ظل انتفاء القدرة على الرقابة على الأنترنت بالنظر لطابعها غير المركزي والعالمي، يتوجب على وسائل التواصل الاجتماعي ومقدمي الخدمات على الأنترنت القيام بالرقابة وتعيين فريق من الفنيين لضمان سلامة شبكاتهم الاجتماعية. وقد يكون من الصعب على وسائل التواصل الاجتماعي التعامل مع الرقابة على محتوى ضخم ومتنوع، بسبب خوفها من خلق شعور لدى المستخدمين بكونهم مقيدين، وكذلك بسبب اضطرارها للقيام بجهد إضافي مع كل متطلباته الاقتصادية وآثاره.

أما الخيار الثاني: لجهة الرقابة، فهو قيام الحكومات بتنظيم الرقابة وبإعلام وسائل التواصل الاجتماعي والمستخدمين بما هو مسموح وبما هو ممنوع إلا أن ذلك يبدو غير فعال بالنظر للطابع الدولي للأنترنت ولكون صلاحية كل دولة بالنظر إلى الافعال الجرمية لا تشمل سوى تلك المرتكبة على إقليميها (الاختصاص الإقليمي) أو من قبل مواطنيها (الاختصاص الشخصي) أو التي تلحق

ضرر بالدولة (الاختصاص القاصر) كما أنه قد يتنافى ذلك مع حرية التعبير وما تستدعيه من احترام لمبادئ الديمقراطية.

والخيار الثالث: هو التنظيم الذاتي من قبل المستخدمين أنفسهم عبر رفض المستخدمين الاخرين الذين لا يلتزمون بمدونات السلوك على الأنترنت، وكذلك عبر حجب أو تقييد الوصول لهم وأولادهم لبعض المحتوى فالإنترنت لديها قدرة غير محدودة لإتاحة مشاركة المستخدمين وتفاعلهم وعدم وجود حدود لها يناقض الحدود الجغرافية للأقاليم[123].

وهناك بعض الأدوات التقنية المستخدمة للرقابة على وسائل التواصل ومنها استعمال البرامج التجسسية لنسخ محتوى القرص الصلب Hard disk أو كلمات السر، والتصيد Phishing، وإنشاء مواقع مرآة لحجب الوصول إلى بعض المحتوى، وتقنية الكوكيز وهى نوع من ملفات الارتباط التي تقوم بجمع كل المعلومات الخاصة بالمستخدم الأي بي IP ، نوع الموديم، نوع الحاسوب والمعالج، الوقت الذي تقضيه متصلاً بالإنترنت، معلومات البطاقة المصرفية، وتجمع اهتماماتك ويمكن لأي شخص الوصول إلى بيانات المتصفح عن طريق تقنيات Sniffing للوصول إلى ملفات الكوكيز وسرقة محتواها عندما يتم تمرير ملف الكوكيز بين المتصفح والخادم ، وتستطيع الحكومات استغلال ملفات الكوكيز لمعرفة جميع تحركات المستخدم ونشاطاته على الإنترنت عن طريق طلب المعلومات من أصحاب الخادم[124].

المطلب الثالث: مقارنة مسؤولية وسيلة التواصل الاجتماعي بمسؤولية مستضيف البيانات

الأصل أن تعدّ وسيلة التواصل وسيطا وليس ناشرا، وهي تماثل أيضاً وضع مستضيف البيانات، وتخضع بالتالي لذات القواعد القانونية المطُبّقة عليهما من زاوية المسؤولية عن المحتوى المحمّل من قبل المستخدمين[125].

وبالنظر إلى الطبيعة الخاصة للإنترنت وما يتسم به من غزارة المعلومات وعدم الخضع للحدود أو المراقبة وإمكانية تحكم كل مستخدم بالمحتوى وفكرة المنصات(Platforms) التي تسمح للمستخدم بتحميل المحتوى وبنشره دون مقابل والتي تتيح حق الرد الفوري بعض الدول الأوروبية، وكذلك الولايات المتحدة الأميركية، قد أصدرت قوانين لحماية الوسطاء على الإنترنت من

---

[123] وسيم شفيق الحجار، النظام القانوني لوسائل التواصل الاجتماعي، دراسة قانونية مقارنة حول الحرية الشخصية والمسؤولية والاختصاص، مرجع سابق، ص103.

[124] وسيم شفيق الحجار، النظام القانوني لوسائل التواصل الاجتماعي، دراسة قانونية مقارنة حول الحرية الشخصية والمسؤولية والاختصاص، مرجع سابق، ص66.

[125] محمد سامي عبد الصادق، شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية، مرجع سابق، ص 32.

المسؤولية والقانون في الولايات المتحدة الامريكية لا يرتب مسؤولية على الوسطاء عن المحتوى العائد للغير، ولو كانوا يديرون الحوار أو يقيدون الوصول إلى تعليقات المستخدم الممكن الاعتراض عليها- بالمقابل- تحمي دول أخرى الوسطاء من المسؤولية إذا أزالوا المحتوى غير المشروع عند معرفتهم بوجوده[126].

ومع استبعاد تطبيق تشريعات الإعلام التقليدي على وسائل التواصل الاجتماعي، يجوز التساؤل حول التكييف القانوني لمواقع التواصل الاجتماعي لمعرفة ما إذا كانت مورد معلومات أو مقدم خدمات؟، حيث أن مورد المعلومات يتولى نشر معلومات من تجميعه أو تأليفه على الأنترنت لوضعها تحت تصرف الجمهور مجاناً أو لقاء مبلغ مالي، وهو يتولى تحميل هذه المعلومات والرقابة عليها فهو بمثابة محرر الصفحة أو الموقع ، أما مقدم الخدمة، عادةً ما يكون مستضيف بيانات فاعتبار أن وسائل التواصل الاجتماعي بمثابة مستضيفي البيانات هو الرأي الراجح في فرنسا ، ويكون المستخدم مسؤولاً عن صفحته على موقع التواصل الاجتماعي فيما ينشره ، بالمقابل يكون مستضيف البيانات ومشغل الموقع في وضع مستضيف البيانات إلا إذا لعب دور في اعدادات النشر فقد يعتبر كناشر ويعتبر كذلك المستخدم صاحب صفحة على فيسبوك كمحرر للمحتوى الذي ينشره ومسؤول عن طابعه غير المشروع. كما يكون مسؤول عن تغريداته وتعليقاته التي يطلقها على وسائل التواصل الاجتماعي. ويكون في حكم مستضيف البيانات بالنسبة للتعليقات التي يتلقاها على صفحته على فيسبوك لأنه اقتصر في موقعه على تخزين المناقشات وتوفير مكنة استرجاعها لمستخدمي الموقع دون أن يتدخل في اختيارها حيث رفعت شركة (Group Mace) إحدى الشركات الفرنسية الشهيرة في مجال تصميم الملابس والاكسسوارات اللازمة للزواج دعواها على صاحب الموقع بداعي أن موقعه اشتمل على مدونات مسيئة إلى الشركة أتاحها عدد من المستخدمين للموقع [127].

---

[126] أشرف جابر سيد؛ خالد بن عبد الله الشافي، حماية خصوصية مستخدمي مواقع التواصل الاجتماعي في مواجهة انتهاك الخصوصية في موقع فيس بوك "دراسة مقارنة في ضوء النظام السعودي"، بحث منشور بكلية الحقوق جامعة حلوان، 2013، ص 25.

[127] استقرت أحكام القضاء الفرنسي على اعتبار منظمي منتديات المناقشة ومقدمي خدمات التواصل الاجتماعي عبر الشبكة على أنهم من متعهدي الإيواء فرفضت المحكمة الابتدائية بتاريخ 21 يوليه سنة 2005م إنزال وصف الناشر على منظم منتديات المناقشة للموقع الالكتروني واعتبرته متعهد للإيواء طالما لم يشارك كل منهم في اختيار المحتوى المتاح عبر الموقع الإلكتروني الذي يديرونه، أشار إليه : محمد سامي عبد الصادق، شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية، مرجع سابق، ص 34.

ونحن نؤيد هذه الوجهة بالنظر لانتفاء دور وسائل التواصل الاجتماعي في انتقاء المحتوى المحمّل من قبل المستخدمين، ولصعوبة مراقبة هذا المحتوى بعد تحميله بالنظر لضخامته ولعدم وضوح عدم المشروعية أو التعدي على حقوق الغير في أغلب الأحيان فلا تقوم مسؤولية وسائل التواصل الاجتماعي إلا بعد تمنعها عن إزالة المحتوى غير المشروع سواء بعد اعلامها بعدم المشروعية أو كانت عدم المشروعية ظاهرة بشكل جلي واضح لا يحتمل اللبس وعادةً، يتم ترتيب المسؤولية على عاتق وسائل التواصل الاجتماعي في حال امتناعها عن سحب أو حجب المحتوى الضار بعد إبلاغها بصورة رسمية طلباً بهذا الخصوص[128].

وتنص المادة (14) من التوجيه الأوروبي حول التجارة الإلكترونية على أن مستضيف البيانات لا يكون مسؤولاً عن المعلومات المخزنة بناء على طلب المستخدم شرط ألا يكون على علم فعلي بالنشاط أو المعلومة غير المشروعة. والاعلام عن المحتوى غير المشروع عادةً ما يكون بقرار من المحكمة كما في بعض القوانين مثل فرنسا حيث تعطي المادة (2/9) من التقنين المدني الفرنسي للقضاة سلطة اتخاذ كافة الإجراءات التي من شأنها منع أي تعدي على الحياة الخاصة كالحراسة أو الحجز كما يمكن للقضاء المستعجل الأمر بهذه الإجراءات " أن يأمر بتعليق حساب شخصي

---

[128] ومن التطبيقات القضائية التي عرفتها المحاكم الأمريكية واقعة انتحال شخص لاسم أحد مشاهير التعليق الرياضي على مباريات كرة القدم الأمريكية؛ إذا قام المنتحل بإنشاء حساب شخصي يحمل اسم المعلق وصورته بهدف استقطاب المعجبات وقد تلقى عليه العديد من الرسائل الإلكترونية التي حملت معلومات شخصية استخدمها بشكل غير مشروع، وقد ألزمت محكمة كاليفورنيا التي نظرت في الوقائع إدارة شبكة التواصل بحذف الحساب الخادع وإلزام المنتحل بالتعويض الناتج عن الاعتداء على حرمة الحياة الخاصة وانتحال الشخصية. كما صدرت أحكام عن المحاكم الفرنسية، منها حكم تولوز الذي اعتبر موقع التواصل الاجتماعي مسؤول لعدم سحبه المحتوى الضار خلال مهلة 24 ساعة من تاريخ تبلغه بماهية هذا المحتوى- كما اعتبرت محكمة الدرجة الاولى التجارية في باريس أن مقدم الخدمة هو معفى من أي مسؤولية لحين إعلامه بالمحتوى الضار-كما ألزمت محكمة الدرجة الاولى في باريس فيسبوك بصفته مستضيف بيانات وبموجب أمر على عريضة بإزالة الصور المعترض عليها وكذلك المحتوى التحريضي على الكراهية والعنف وعلى تقديم البيانات التي تسمح بالتعريف عن منشئ الصفحة- وبالنسبة للمهلة المعطاة لسحب المحتوى الضار، اعتبرت محكمة الدرجة الأولى في باريس أن سحب أفلام الفيديو المُنازع بها لم يحصل إلا بعد خمسة أيام، والتي لا يمكن اعتبارها مهلة معقولة، أنه يتوجب على يوتيوب العمل لإخفاء المحتوى المُنازع به بأقصى سرعة ممكنة بعد التبليغ عنه. أشار إليه : محمد سامي عبد الصادق، شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية، دار النهضة العربية، 2016، ص91.

على موقع التواصل دأب صاحبه على التعرض لمعلومات ووقائع الحياة الخاصة لغيره دون رضاه " بناءً على طلب الشخص الذي تم المساس بحياته الخاصة[129].

وعلى الوسيط التحقق من الشكوى التي ترده فقد يلحق ضرر مادي أو معنوي بصاحب المحتوى المحذوف، وقد يُرتكب خطأ بحقه. ولهذا على الوسيط في حالة الشك في الطابع غير المشروع التأكد من ذلك. ومن هذا نرى أن مسؤولية مستضيف البيانات عن المحتوى تعتمد على أن يكون بصورة واضحة غير مشروع أما في حالة الشك في مشروعية المحتوى، فلا تترتب أي مسؤولية على مستضيف البيانات.

والمستخدم لمواقع التواصل يلتزم تجاه مقدمي خدمات التواصل الاجتماعي فضلاً عن التزامه تجاه المستخدمين الآخرين من حيث عدم استخدام شبكة التواصل لأي عمل مضلل أو ضار أو عنصري والامتناع عن القيام بأي عمل قد يعطل سير العمل الصحيح والالتزام بدقة وحداثة ومشروعية المحتوى المعلوماتي الذي يتيحه عبر صفحته الشخصية وعدم تحميل أية فيروسات أو مواد ضارة فقد يكون المحتوى الضار من ابتكار المستخدم أو تأليفه، كما قد يكون دوره مقتصراً على تجميع هذا المحتوى وتحميله، فيكون عمله كوسيط بين مؤلف المحتوى وبين الجمهور- وإذا نقل المستخدم المحتوى الضار عن الغير كإعادة صياغته أو إعادة إنتاجه ونسخه (share) فإنه يكون مسؤولا أيضاً مدنياً وجزائياً لأن النشر الحاصل منه لاحق ومستقل عن عملية النشر.

وقد ينشر المستخدم معلومات غير وافية، أشار الفقه الفرنسي إلى التطبيق القضائي الخاص بقضية (La Cigue) عندما قامت بإتاحة معلومة غير وافية أودت بحياة أحد القراء الذي سلم بتمام هذه المعلومات التي وردت بكتاب (Les plantes comestibles) الخاص بالنباتات الصالحة للطهي واحتوى على صورة لنبات الجزر البري (La Carotte sauvage) القريب الشبه من نبات مخدر وسام اسمه (La Cigue) دون أن يرد أي تحذير بينهما ، فأعدت الفتاة وجبة بالنبات السام مما تسبب في وفاة أحد أفراد عائلتها، فألزمت محكمة باريس الابتدائية من أتاح المعلومة بالتعويض نتيجة لعدم تحذير القارئ من هذا الخلط[130].

---

[129] محمد سامي عبد الصادق، شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية، مرجع سابق، ص111- 112.

[130] محمد سامي عبد الصادق، شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية، مرجع سابق، ص 78-79.

الفصل الثاني: الإطار القانوني والتنظيمي لحماية البيانات ذات الطابع الشخصي

أنه ولئن كانت مواقع التواصل الاجتماعي لها جانب إيجابي في العصر الحديث إلا أن أضرارها فاقت مزاياها وخاصة من المسلك غير المشروع سواء للمستخدمين أو الشركات التي تقوم بتحليل البيانات بشكل غير مشروع أو بدون اذن المستخدم حيث أن اقتصاد المعلومة أصبح أسرع الاقتصاديات نمواً وثراءً في الوقت الحالي.

وفي هذا الفصل سيبيّن الباحث على قدر المستطاع المصادر التي تهدد خصوصية البيانات الشخصية على مواقع التواصل وصور هذا التهديد واشكال المساس بالبيانات وما قد يكون منها مشروعاً خاصة إذا ما تعلق بالأمن القومي وكذلك بيان نوع وصور المسؤولية القانونية عن المساس بالبيانات ذات الطابع الشخصي على مواقع التواصل الاجتماعي والتعويض عنها واشكالية تنازع الاختصاص القضائي والتشريعي بشأنها.

المبحث الأول: مصادر تهديد البيانات ذات الطابع الشخصي على مواقع التواصل

أدى انتشار استخدام مواقع التواصل الاجتماعي إلى سهولة انتهاك البيانات ذات الطابع الشخصي حيث أصبحت هذه المواقع مصيدة سهلة لاقتناص المعلومات ذات الطابع الشخصي، ومن ضمن المصادر التي تهدد البيانات ذات الطابع الشخصي على مواقع التواصل الاجتماعي المستخدم ذاته التي يضع كماً من البيانات الشخصية دون مراعاة للخصوصية كالاسم والعمر والعقيدة والحالة الاجتماعية وغيرها من البيانات وبالتالي يعد المستخدم وسيلة سهلة للحصول على المادة الخام لاقتصاد المعلومة ثم تحليل وتجميع البيانات لأغراض اجتماعية واقتصادية وسياسية وغيرها، كما أن تطور التكنولوجيا يعد بذاته مصدر تهديد للبيانات الشخصية مثل الملفات الخبيثة والروابط والصور المجهولة بل ان البيانات التي نعتبرها تافهة عند وضعها على مواقع التواصل الاجتماعي، يمكن من خلال العقول الالكترونية التي تقوم بتجميع وتحليل بلايين المعلومات والبيانات، أن تتحول إلى كنز ثمين من البيانات المطلوبة للكيانات الاقتصادية العملاقة أو حتي للكيانات السياسية التي ترسم من خلالها ملامح سياستها وقراراتها.

أولاً: تجميع المعلومات عن طريق مواقع التواصل الاجتماعي.

قد يثور التساؤل عن الغرض من البيانات التي تتطلبها مواقع التواصل الاجتماعي عند التسجيل والحكمة والغاية منها إلا أنه بعد ظهور اقتصاد المعلومة من خلال عمليات تجميع البيانات وتحليلها

وتوزيعها على مستهلكيها من الكيانات الاقتصادية الكبيرة ظهرت الحكمة من طلب تلك البيانات[131].
وعادة تتطلب مواقع التواصل الاجتماعي بيانات كثيرة عن الشخص كالاسم والعمر والعقيدة والحالة الاجتماعية وغيرها من البيانات وقد تجمع هذه المعلومات بشكل تلقائي عند تصفح الإنترنت، مثل عنوان الكمبيوتر(IP) الخاص بالمستخدم، لأن كل كمبيوتر متصل بشبكة الإنترنت يتم منحه عنوناً يتكون من 32 رقماً، وكذلك المعلومات الخاصة بالمتصفح المستخدم ووقت وتاريخ زيارة الموقع وغيرها، وسواء أكانت تلك المعلومات مأخوذة من قبل المستخدم أو بشكل تلقائي عند دخوله على المواقع المختلفة، فإن الاحتفاظ بها داخل السيرفرات الخاصة بالمواقع، يمثل تهديداً لخصوصية الأفراد في العالم الافتراضي[132] .

وقد فرض المشرع القطري سياجاً من الحماية القانونية على تجميع البيانات وتحليلها بأن أوجب على المراقب لدى إفصاحه عن البيانات الشخصية أو نقلها إلى المعالج، مراعاة أن تكون مطابقة للأغراض المشروعة، وأن تكون تلك البيانات معالجة وفقاً لأحكام هذا القانون[133]، وأنه يجب على كل من المراقب والمعالج اتخاذ الاحتياطات اللازمة لحماية البيانات الشخصية من الضياع أو التلف أو التعديل أو الإفشاء، أو الوصول إليها، أو استخدامها بشكل عارض أو غير مشروع ويجب أن تكون تلك الاحتياطات متناسبة مع طبيعة وأهمية البيانات الشخصية المراد حمايتها وعلى المعالج أن يخطر المراقب بوجود أي إخلال بالاحتياطات المشار إليها، أو عند حدوث أي خطر يهدد البيانات الشخصية للأفراد بأي وجه، فور علمه بذلك[134]، ويجب عليه أيضاً إعلام الفرد والإدارة المختصة، بحدوث أي إخلال بالاحتياطات المنصوص عليها في المادة السابقة، إذا كان من شأن ذلك إحداث ضرر جسيم بالبيانات الشخصية أو بخصوصية الفرد[135]، كما أنه يُحظر على المراقب اتخاذ أي قرار أو إجراء من شأنه الحد من تدفق البيانات الشخصية عبر الحدود، إلا إذا كانت معالجة تلك البيانات مخالفة لأحكام هذا القانون، أو كان من شأنها إلحاق ضرر جسيم بالبيانات الشخصية أو بخصوصية الفرد[136].

ثانياً: تقنيات الكوكيز (COOKIES):

---

[131] يونس عرب، الخصوصية وحماية البيانات في العصر الرقمي، الأردن، الطبعة الثانية، سنة 2010م ص9 وما بعدها.

[132] يونس عرب، المخاطر التي تهدد الخصوصية وخصوصية البيانات في العصر الرقمي، مرجع سابق، ص9.

[133] المادة (12) من قانون حماية البيانات الشخصية القطري.

[134] المادة (13) من قانون حماية البيانات الشخصية القطري.

[135] المادة (14) من قانون حماية البيانات الشخصية القطري.

[136] المادة (15) من قانون حماية البيانات الشخصية القطري.

يقصد بالكوكيز الملفات النصية بامتداد (TXT)، يرسلها الخادم الخاص بالموقع الذي يتم زيارته عبر الإنترنت، إلى القرص الصلب للمستخدم، ويحتفظ بنسخة منها لديه وتحتوى على معلومات شخصية معينة تخص المستخدم وكذلك جهاز الحاسوب الخاص به، كعنوان الإنترنت(IP)، وكذلك طريقة الاتصال بالإنترنت، والمواقع التي يتم زيارتها، ونوع الجهاز، ونوع المعالج، وكذلك البيانات التي يطلب إدخالها من المستخدم لاستمارة التسجيل كالاسم والبريد الإلكتروني ورقم البطاقة الائتمانية، والعنوان وغير ذلك مما يطلب إدخاله للدخول إلى الموقع أو الاستفادة بخدماته ، ويحتفظ الموقع الذي يتم زيارته بنسخة من ملف الكوكيز داخل السيرفر الخاص به، متضمنة المعلومات السابقة، تظهر للمستخدم عند زيارته للموقع مرة ثانية، لتسهيل الوصول إلى الموقع، فإذا كان يستخدم بيانات معينة لدخول هذا الموقع فإنه لا يتطلب إدخالها مرة أخرى بالإضافة إلى سرعة الوصول إلى الموقع، ولكن خطورة وجود مثل هذه الملفات على جهاز المستخدم، بالإضافة إلى معرفة البيانات الشخصية التي تخص المستخدم، تتمثّل في كونها تتيح للموقع أن يتعرف وبسهولة على خطوات واتجاهات المستخدم عبر الإنترنت، عن طريق معرفة المواقع التي يدخلها. وهو الأمر الذي يستخدم في الإعلانات، حيث أن معرفة سلوك المستخدم عبر الشبكة يحدد في النهاية، ماذا يحب أو يكره، وماذا يريد بالتحديد، وبالتالي فيكون من اليسير على المواقع الدعائية توجيه الإعلانات التي تناسبه بالتحديد، ومن الشركات الشهيرة في هذا المجال، شركة DoubleClick، هذا من ناحية أولي، ومن ناحية ثانية فإنه يمكن سرقة هذه الملفات من جهاز المستخدم ،واستخدام المعلومات التي يحتويها ملف الكوكيز في التصفح بدلاً منه، وبمعنى آخر فإن ذلك قد يسهل اختراق الصفحات الشخصية التي تخص المستخدم وكذلك البريد الإلكتروني الخاص به، وأخطر من ذلك لو تم الاستيلاء على الكوكيز الخاص بصاحب الموقع، فإن ذلك يعنى اختراق الموقع ذاته ، باستخدام المعلومات الواردة داخل ملف الكوكيز، فقد يكون الشخص مدير (admin) لصفحة ما عبر الإنترنت، تخص إحدى الشبكات الاجتماعية على سبيل المثال ، فيتم سرقة ملفات الكوكيز الخاصة به، والدخول إلى الصفحة التي يريدها، وكل ذلك يشكل تهديداً جدياً لخصوصية المستخدمين عبر الإنترنت[137].

ثالثاً: البريد غير المرغوب فيه:

[137] مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الإتفاقي والقانون الوطني، مرجع سابق، ص336.

هو اتصال إلكتروني، مجهول غالباً، غير مرغوب فيه مرسل عبر بريد الإنترنت، وقد يتسبب في تلويث شبكة الاتصالات الإلكترونية بالفيروسات، ويعبر عن هذه الرسائل بالفرنسية بمصطلح "بولي بوستاج" ولهذه الرسائل خصائص ثلاث، فهي رسائل مؤذيه، كما أنها ترسل لعدد كبير في وقت واحد، ودون إخطار من المرسل.

وقد ترسل هذه الرسائل عن طريق استخدام بطاقات أعياد الميلاد، ويتم الحصول على عناوين البريد الإلكتروني من خلال المجموعات الإخبارية وغرف الدردشة، ثم تقسم بعد ذلك إلى فئات مختلفة، وتؤجر للشركات التي تقوم بإرسالها بكميات هائلة من خلال البريد الإلكتروني، للإعلان عن منتجاتها. فمن الضروري تنظيم الاستعمال المتكرر لهذه الرسائل من المعلنين، باعتبارها سهلة نسبياً نظراً لتكلفتها القليلة، ويمكن على العكس أن يتحمل عبء ثمنها المرسل إليه، بل أنها يمكن لكثرتها، أن تتسبب في مشكلة لشبكات الاتصالات الإلكترونية والتجهيزات الرقمية[138].

وقد فطن المشرع القطري لذلك حيث حظر في المادة (32) من قانون حماية البيانات الشخصية إرسال أي اتصال إلكتروني بغرض التسويق المباشر إلى الفرد، إلا بعد الحصول على موافقته المسبقة ويجب أن يتضمن الاتصال الإلكتروني هوية مُنشئه، وما يفيد بأنه مرسل لأغراض التسويق المباشر، كما يجب أن يتضمن عنواناً صحيحاً يسهل الوصول إليه، ويستطيع الفرد من خلاله أن يرسل طلباً إلى المنشئ بإيقاف تلك الاتصالات أو الرجوع في موافقته على إرسالها.

رابعاً: فقد البيانات الشخصية لأسباب تقنية أو مادية.

عادةً ما تقوم شركات تعمل تحت قيادة الشركات المالكة لمواقع التواصل الاجتماعي بعمليات تجميع وتحليل البيانات وتسمى الشركات المساندة وقد تتعرض كمية المعلومات والبيانات التي تقوم هذه الشركات بتجميعها إلى الفقد أو التلف أو القرصنة من الغير على سبيل المثال في فرنسا فقدت إحدى الشركات عام 2006 أسطوانة عليها البيانات الشخصية لتسعة آلاف عامل فيها، بل إن الإحصائيات تشير إلى أنه في 2007 فقد نحو 162 مليون ملف يحتوي على بيانات شخصية، وذلك بالمقارنة بـ 49 مليون ملف عام 2005 [139].

---

[138] جبالي أبو هشيمة كامل ، حماية البيانات الشخصية في البيئة الرقمية ، بحث مقدم إلى مؤتمر العصر الرقمي واشكالياته القانونية ، كلية الحقوق جامعة أسيوط ، الفترة من 12-16 ابريل 2016 ص30.

[139] سامح عبد الواحد التهامي الحماية القانونية للبيانات الشخصية، بحث منشور بمجلة الحقوق، جامعة الكويت العدد الثالث سبتمبر 2011، ص 400.

وقد كان المشرع القطري حريصا على حماية البيانات من التلف والفقد حيث نص على ذلك في المادة (13) من قانون حماية البيانات الشخصية [140].

المبحث الثاني: صور الاعتداء على البيانات الشخصية

تتعدد صور الاعتداء على البيانات الشخصية لمستخدمي شبكات التواصل الاجتماعي لعل من أهمها تجميع البيانات الشخصية دون رضاء أو إذن من المستخدم أو الانتحال للصفة والاسم أو الابتزاز والاحتيال وغيرها من السلوك غير المشروع أو معالجة المعطيات ذات الطابع الشخصي دون التصريح بذلك أو دون الحصول على الإذن أو المساس بحقو ق الشخص المعني بالمعطيات موضوع المعالجة أو عدم الالتزام بسرية وسلامة المعالجات والاستغلال غير المشروع للمعطيات ذات الطابع الشخصي كالاستغلال لأغراض تجارية أو مخالفة قواعد نقل المعطيات ذات الطابع الشخصي إلى بلد أجنبي أو الاستعمال التعسفي أو التدليسي للمعطيات المعالجة.

المطلب الأول: الاعتداءات العامة غير المشروعة على البيانات الشخصية

قد يكون الاعتداء من خلال تجميع البيانات دون رضاء المستخدم أو استخدامها في أغراض تجارية أو اختراق البيانات واعتراض اتصالاتها.

1-تجميع البيانات الشخصية دون رضا أو إذن المستخدمين:

يجب ألا تتم عملية تجميع البيانات الشخصية أو أي إجراء آخر من إجراءات المعالجة إلا برضاء الشخص [141]، وتظهر صورة الاعتداء على البيانات الشخصية بتجميعها دون رضا المستخدم في قيام بعض مواقع الإنترنت بتجميع هذه البيانات ومعالجتها وإرسالها لمواقع أخرى دعائية، وفي مثل هذه الحالات يجب إعلام مستخدم الموقع بكل ما يحدث لبياناته والحصول على رضائه، وإلا

---

[140] نصت المادة 13 على أنه: " يجب على كل من المراقب والمعالج اتخاذ الاحتياطات اللازمة لحماية البيانات الشخصية من الضياع، أو التلف، أو التعديل أو الإفشاء، أو الوصول إليها، أو استخدامها بشكل عارض أو غير مشروع. ويجب أن تكون تلك الاحتياطات متناسبة مع طبيعة وأهمية البيانات الشخصية المراد حمايتها. وعلى المعالج أن يخطر المراقب بوجود أي إخلال بالاحتياطات المشار إليها، أو عند حدوث أي خطر يهدد البيانات الشخصية للأفراد بأي وجه، فور علمه بذلك".

[141] طبقاً للمادة السابعة من قانون حماية البيانات الشخصية الفرنسي فرضت اللجنة القومية للمعلوماتية والحريات على أثر تفتيش قامت به عامي 2009 - 2010 – غرامة مائة ألف يورو على شركة جوجل لجمعها بيانات المحتوى (الهويات – كلمات المرور – تبادل رسائل البريد الإلكتروني) عبر شبكات "الواي فاي" من أجل خدمتها الجديدة "جوجل ستريت فيو" وقد تعهدت جوجل بالتخلص من البيانات المخزنة، انظر: جبالي أبو هشيمة ، حماية البيانات الشخصية في البيئة الرقمية ، مرجع سابق، ص31.

قامت مسؤوليتها نتيجة هذا الاعتداء فأي تجميع للبيانات الشخصية دون علم صاحب هذه البيانات يعتبر غير مشروع، وهذا ما أوجبه المشرع القطري [142]،وقد يتم تجميع هذه البيانات عن طريق ملفات الكوكيز [143] .

وقد أوجب المشرع القطري على المراقب الذي يقوم بتجميع البيانات الشخصية أن يُعلم الفرد الأغراض المشروعة التي يرغب المراقب أو أي طرف آخر في معالجة البيانات الشخصية من أجلها والوصف الشامل والدقيق لأنشطة المعالجة ودرجات الإفصاح عن البيانات الشخصية للأغراض المشروعة، وإذا لم يتمكن المراقب من ذلك، فيتعين عليه تمكين الفرد من وصف عام لها وأية معلومات أخرى تكون ضرورية ولازمة لاستيفاء شروط معالجة البيانات الشخصية[144].

ويلزم أن يأخذ في الاعتبار الظروف التي تم فيها الرضا بالكشف عن الخصوصية؛ فالرضا الذي عبرت عنه إرادة مشوبة بعيب الاستغلال في ظل تعلق المستخدمين بمواقع التواصل الاجتماعي إلى الحد الذي يفقدهم الحكم على ما يتصل بحماية خصوصياتهم أمام ضغط مقدم الخدمة الذي يقوم بالمعالجة فضلاً عن أن الرضا بالكشف على الخصوصيات يجب أن يكون خاصاً ومحدداً ينصب على كل عملية من عمليات معالجة البيانات.

---

[142] المادة 23 من قانون حماية البيانات الشخصية القطري.

1- [143] أشهر القضايا هي قضية (google FTC V inc) وتدور عن واقعة وضع شركة جوجل ملفات كوكيز في المتصفح سفاري الخاص بشركة آبل، بحيث تمكن هذه الملفات (كوكيز)، شركة جوجل من تتبع نشاط المستخدمين لمحرك بحثها، والذين يتصلون به من خلال المتصفح سفاري، وملفات الكوكيز تستطيع أن تجمع معلومات هوية المستخدمين وتخزينها، الجدير بالإشارة أن الضبط الافتراضي لمتصفح سفاري يحظر استقبال ملفات كوكيز من الغير ولكن جوجل استغلت ثغرة داخل هذه المتصفح ووضعت ملفات كوكيز داخله، مما يعنى أن المستخدمين لم يكونوا على علم بذلك ولم يوافقوا عليه، ونشير أيضاً أن جوجل استهدفت من وراء تتبع المستخدمين عبر الإنترنت إرسال الإعلانات إليهم وتحقيق الربح بسبب ذلك، فمن المعروف أن أرباح جوجل الرئيسية تأتي من الإعلانات عبر الإنترنت، فهي من أهم شركات تكنولوجيا المعلومات التي تقدم خدمة الإعلان في العالم الافتراضي، ولقد قدمت غرفة التجارة الفيدرالية FTC شكواها إلى محكمة الولايات المتحدة للمنطقة الشمالية في ولاية كاليفورنيا، بيد أنه قد تم تسوية الأمر خارج المحكمة، بأن دفعت جوجل غرامة قدرها 5.22 مليون دولار، أنظر: هيثم السيد أحمد، المسؤولية المدنية في إطار المعاملات على شبكة الإنترنت ، رسالة دكتوراه ، جامعة المنوفية، ص 609.

[144] المادة (9) من قانون حماية البيانات الشخصية القطري.

كما أن تجاهل مواقع التواصل الاجتماعي لاتخاذ التدابير الفنية التي تحول دون قيام صغار السن بفتح حسابات شخصية لهم على هذه المواقع يثير إشكالية حول رضاء القاصر بالكشف عما يتصل بحياته الخاصة عبر الإنترنت وهي إشكالية حديثة أثارت جدلاً فقهياً أثير في فرنسا انتهت فيه محكمة النقض الفرنسية إلى وجوب الحصول على إذن من له السلطة على القاصر في حالة كشف الأخير عن وقائع تتعلق بحياته الخاصة أي رضا من يمثله قانوناً لحين بلوغه سن الرشد[145].

2-استخدام البيانات الشخصية في الأغراض التجارية:

يجب أن يتم تجميع البيانات الشخصية لأغراض محددة ومشروعة وفقاً للمقرر في قانون حماية البيانات الشخصية القطري وأن يكون الهدف منها تحقيق مصلحة مشروعة، وتعد البيانات الشخصية اقتصادا حديثا وثريا للقائمين على الدعاية عبر شبكة الإنترنت، حيث أن اقتصاد المعلومة هو الاقتصاد الذي يشغل العالم حالياً من خلال بيع وتداول بيانات المستخدمين الشخصية على موقع التواصل، إلى شركات الإعلان، ثم تقوم الشركات الإعلانية بإعداد قواعد بيانات تصنف من خلالها تحديد احتياجات المستخدمين ورغباتهم.

ويتمثل الخطر الأكبر، في جميع البيانات الشخصية للمستخدمين، عبر طريق المستخدم نفسه من خلال استضافته على شبكات التواصل الاجتماعي (فيس بوك) فهذه المواقع تدعو المستخدم لأن يدلي بنفسه ببياناته طواعية، من أجل الاشتراك في هذه المواقع وهي معلومات شخصية كثيرة، محددة وكاملة-والواقع- أن الشخص يدلي بإرادته بالبيانات المطلوبة دون وعي لما يترتب على ذلك من إعادة استعمال هذه البيانات ، في حين أن هذه البيانات تفهرس وتنشر وتستثمر دون تمكين صاحب البيانات من ممارسة حقوقه عليها، وعلى حد تعبير أحد المؤلفين "إذا لم تؤد خدمة على شبكة الإنترنت فإنك لن تكون مستهلكاً وإنما المنتج المباع، فشبكة "فيس بوك" كانت تتبع السيرة المهنية "بروفيل" للمشترك مقابل خمسة دولارات لشركات التسويق عبر الإنترنت[146].

وتكمن الخطورة في أن البيانات الشخصية أصبحت محلاً للإتجار بها من قبل المواقع والشبكات، بل إن جاز القول أصبحت محلاً لاقتصاد جديد، وذلك لسهولة جمعها وانخفاض تكاليفها، وهو ما أدى إلى قيام الكثير من المنشآت التجارية إلى العمل في مجال جمع وبيع البيانات الشخصية وقد

---

[145] محمد سامي عبد الصادق، شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية، مرجع سابق ، ص 60.

[146] جبالي أبو هشيمة، جبالي أبو هشيمة كامل ، حماية البيانات الشخصية في البيئة الرقمية ، مرجع سابق، ص30.

اتخذت هذه النظرية تطبيقاً حديثاً، وذلك مع زيادة عدد المستخدمين لشبكات التواصل الاجتماعي أو شبكة الإنترنت بصفة عامة، إذ اتجهت معظم الشركات التجارية إلى إنشاء مواقع لها على الإنترنت[147]، هذه المواقع تسمح لها بتجميع البيانات الشخصية لمستخدمي الإنترنت وتقدم عروض خاصة لهم عبر الشبكة، وهو ما أصبح يسمى بـ "التسويق الإلكتروني" [148]، ومواقع التواصل الاجتماعي تقدم خدمات مبتكرة ومجانية في الغالب، لكن في مقابل الاستغلال التجاري للبيانات الشخصية مما ينتج عنه ما يسمى باقتصاد المعلومة وهو أقوى الاقتصاديات والمشروعات الناجحة في العصر الحديث الشخصية[149].

ولذلك نرى أنه من الضروري وجود تشريعات خاصة لحماية البيانات الشخصية للأفراد من الاستغلال والإتجار فيها لأغراض تجارية، لما يمثله ذلك من انتهاك لخصوصية وسرية بيانات الفرد، فضلاً عن التسبب في إزعاجه عند استقباله سيلاً من الرسائل التسويقية والعروض الترويجية بصفة مستمرة، وفي أوقات غير مناسبة، أو حين تكون تلك الرسائل غير ملائمة لشخصه، مطالباً الجهات المعنية بالعمل على رصد أنشطة الشركات التي تجمع البيانات الشخصية أو تبيعها لآخرين لأغراض تسويقية بصورة غير قانونية.

---

[147] تستخدم البيانات الشخصية للأغراض التجارية بعد تجميعها عن طريق ملفات كوكيز حيث يقوم الموقع الخاص بالمنشأة التجارية بزرع هذه الملفات على القرص الصلب للكمبيوتر الخاص بمستخدم الإنترنت عند زيارته لهذه المواقع تقوم هذه الملفات بتخزين العديد من البيانات والمعلومات عن مستخدم الإنترنت مثل المنتجات التي يفضل شراءها والمواقع التي يقوم بزيارتها، بالإضافة إلى أسمه وعنوان البريد الإلكتروني الخاص به وغيرها من البيانات التي يقوم المستخدم بكتابتها أثناء التجول على الشبكة وبعد أن تقوم هذه الملفات بتخزين المعلومات والبيانات، تقوم بإرسالها إلى الموقع الخاص بالمنشأة التجارية، التي تستطيع من خلالها إرسال عروض تجارية ودعائية خاصة لمستخدم الشبكات تتناسب مع ميوله وأفضلياته وأذواقه. مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت، مرجع سابق، ص 335-336.

[148] سامح عبد الواحد، الحماية القانونية للبيانات الشخصية، مرجع سابق، ص 400.

[149] قضت محكمة النقض الفرنسية أن بيع السيرة المهنية "بروفيل" للعميل للمعلنين، يمثل جمع بيانات شخصية عن المستخدمين، وهو عمل غير مشروع، ولذا نجد أن اللجنة القومية للمعلوماتية والحريات، قد طلبت من موقع "فيس بوك" إعلام كامل عن ملفات مستخدميها، ونادت بضرورة أن يكون المستخدم على دراية بنشر معلومات شخصية عن حياته الخاصة، وآرائه السياسية والدينية، أنظر: جبالي أبو هشيمة كامل ، حماية البيانات الشخصية في البيئة الرقمية ، مرجع سابق، ص30.

3- الإختراق والتشهير والابتزاز واعتراض الاتصالات

ألزم المشرع القطري كلا من المراقب والمعالج اتخاذ الاحتياطات اللازمة لحماية البيانات الشخصية من الضياع أو التلف أو التعديل أو الإفشاء، أو الوصول إليها، أو استخدامها بشكل عارض أو غير مشروع ويجب أن تكون تلك الاحتياطات متناسبة مع طبيعة وأهمية البيانات الشخصية المراد حمايتها وعلى المعالج أن يخطر المراقب بوجود أي إخلال بالاحتياطات المشار إليها، أو عند حدوث أي خطر يهدد البيانات الشخصية للأفراد بأي وجه، فور علمه بذلك [150]، يلتزم من يقوم بتجميع البيانات الشخصية أو معالجتها باتخاذ كل الاحتياطيات اللازمة للحفاظ على أمن أو تأمين هذه البيانات، وخاصة منع أي تغيير أو إتلاف لها يمكن أن يحدثه أحد الأشخاص غير المأذون لهم بالاطلاع عليها وقد كما أن الاختراق وسيلة للاعتداء على حرمة الشرف والاعتبار عبر الإنترنت، حيث ينفذ المخترق من خلاله إلى المعلومات التي تخص الفرد، والقيام بإهانته والمساس من كرامته وكذلك تهديده بنشرها، فكل المحتوى الخاص بالشخص لدى جهازه الخاص أو في صفحته الشخصية أو بريده الإلكتروني يكون متاحاً للشخص المخترق يغير فيه أو ينشره أو يستغله بأي وجه من الوجوه، أما التشهير فيقصد به نشر أو نقل وقائع أو بيانات فيها معنى الإثارة أو الإهانة لشخص ما يترتب عليها الحط من كرامته أو شرفه أو سمعته[151].

وقد يثار التساؤل عن مدى اعتبار التهديد بنشر صورة شخصية انتهاكا للحق في الصورة من عدمه؟ ومن ثم هل يعد هذا العمل اعتداء على البيانات الشخصية؟ أجابت محكمة استئناف ولاية إنديانا بالولايات المتحدة الأمريكية، في قضية State v. noII بأن ما قام به الجاني من تهديد بنشر صور جنسية فاضحة للضحية، يعد من قبل التهديد المجرم وفقاً للقانون[152].

وقد كشفت وكالة التحقيقات الفيدرالية، أنها قامت بتطوير برنامج Carnivore أو الملتهم، يقوم بالتجسس على جميع الاتصالات التي تتم عبر الإنترنت، بالإضافة إلى وجود شبكة تسمى (Echelon) وهي شبكة تجسس عالمية أمريكية أوروبية تهدف إلى التجسس على كافة أنواع

---

[150] المادة (13) من قانون حماية البيانات الشخصية القطري.

[151] سامح عبد الواحد التهامي الحماية القانونية للبيانات الشخصية، مرجع سابق، ص 405.

1- [152] حدث أن السيد NoII قام بإرسال ظرف مغلق إلى الضحية يحتوي على صور جنسية فاضحة لها مع الإشارة إلى أن عدم تنفيذ طلبات معينة لها، يعنى نشر هذه الصور عبر الإنترنت، هيثم السيد أحمد، المسؤولية المدنية في إطار المعاملات على شبكة الإنترنت ، مرجع سابق، 617.

الاتصالات الرقمية، والسلكية، واللاسلكية وهذه الشبكة أسستها وكالة الأمن القومي الأمريكية (NSA) بمساعدة جهات استخبارات عالمية[153].

4-صور خاصة للاعتداء على البيانات الشخصية.

يستخدم رواد مواقع التواصل الاجتماعي الاسم في الدخول لها، ولأهمية الاسم كأحد الحقوق اللصيقة بالشخصية ، والتي يوليها المشرع حماية قانونية خاصة من انتحال الغير الاسم دون حق، فيكون للشخص طلب وقف هذا الاعتداء مع التعويض عما يكون قد لحقه من ضرر ولذلك تلجأ شركات مواقع التواصل الاجتماعي على قدر المستطاع الى الاعتراض عند التسجيل على الأسماء المتشابهة لديها حتى لا تقع في المسائلة القانونية وتلتزم شركات مواقع التواصل الاجتماعي بأنه لا يجوز أن يحمل الاسم اكثر من شخص خلاف العالم الحقيقي وأن العبرة لديها بأسبقية التسجيل[154].

ويثار التساؤل عن مدى اعتبار نشر الفيديو عبر الإنترنت دون إذن صاحبه انتهاكا للحق في الصورة من عدمه؟، ومن ثم انتهاكا لأحد البيانات الشخصية؟ إن نشر الفيديو يدخل في إطار الحماية القانونية للحق في الصورة في العالم الافتراضي، وتعتبر المحاكم الامريكية أن انتهاك الخصوصية ونشر فيديوهات وصور دون إذن صاحبها يعرض للمساءلة القانونية[155].

المطلب الثاني: المساس المشروع بالبيانات ذات الطابع الشخصي.

لا يوجد في العلوم الإنسانية ما يسمى بالمطلق إنما النسبية هي الأساس الطاغي على هذا النوع من العلوم لتغير الظروف والمكان واحوال الانسان وبالتالي لا يمكن ان يكون حظر تجميع وتحليل البيانات مطلقاً إنما هناك حالات تستدعي بالضرورة تجميع البيانات وتحليلها منها ما يتعلق بالأمن القومي للدولة.

---

[153] هيثم السيد أحمد، المسؤولية المدنية في إطار المعاملات على شبكة الإنترنت ، مرجع سابق، ص617.

[154] هيثم السيد أحمد، المسؤولية المدنية في إطار المعاملات على شبكة الإنترنت ، مرجع سابق، ص 690.

[155] مثال ذلك قضية The State of New Jersey vs. Dharun Ravi حيث أن Dharun Ravi، طالب سابق في جامعة روتجرز بولاية نيو جيرسي الأمريكية، قام بالتجسس على زميل له في الغرفة يدعي Clementi عبر كاميرا الويب وقام بتصوير وضع شاذ بينه وبين رجل آخر، ثم كشف عن هذا الفيديو للمتابعين له Followers على موقع تويتر Twitter بعد ذلك تأثر Clementi بهذا النشر ولجأ إلى المحاكمة على أساس انتهاك الخصوصية إلى جانب أمور أخرى ثم قام بالانتحار، وفي النهاية أدانت المحكمة Dharun Ravi، نظراً لأن قانون ولاية نيو جيرسي يحظر ترقب الأشخاص وكذلك نشر الصور أو الفيديوهات الناتجة عن ذلك الترقب، ومن الغنى عن البيان في هذا المضمار أن هذه الأفعال غير المشروعة تصلح أساساً للمطالبة بالتعويض أمام القضاء ، هيثم السيد أحمد ، المسؤولية المدنية في إطار المعاملات على شبكة الإنترنت ، مرجع سابق، ص 714.

وقد نص المشرع القطري أنه: "على الجهة المختصة أن تقرر معالجة بعض البيانات الشخصية دون التقيد بأحكام المواد (4)، (9) (15)، (17) من هذا القانون، وذلك لتحقيق حماية الأمن الوطني والأمن العام أو حماية العلاقات الدولية للدولة، أو حماية المصالح الاقتصادية، أو المالية للدولة أو منع أي جريمة جنائية، أو جمع معلومات عنها، أو التحقيق فيها وتحتفظ الجهة المختصة بسجل خاص تقيد به البيانات التي تحقق الأغراض المشار إليها، ويصدر بتحديد شروط وضوابط وأحوال القيد في هذا السجل قرار من الوزير" [156] .

" ويُعفى المراقب من الالتزام بأحكام المواد (4)، (5) البنود 1، 2، 3، من هذا القانون، في حالة تنفيذ مهمة متعلقة بالمصلحة العامة وفقاً للقانون أو تنفيذ التزام قانوني أو أمر من محكمة مختصة أو حماية المصالح الحيوية للفرد أو تحقيق أغراض البحث العلمي الذي يجرى للمصلحة العامة أو جمع المعلومات اللازمة للتحقيق في إحدى الجرائم الجنائية، بناءً على طلب رسمي من جهات التحقيق"[157].

كما " يُعفى المراقب [158]من الإفصاح عن أسباب رفضه الالتزام بحقوق الفرد، المنصوص عليها في المادة (6) من هذا القانون، إذا كان من شأن ذلك أن يحول دون تحقيق الأغراض المنصوص عليها في المادة (18) من هذا القانون" [159]، كما " يُعفى المراقب من الالتزام بأحكام المادة (6) من هذا القانون، في حالة إذا كان من شأن الإفصاح الإضرار بالمصالح التجارية لشخص آخر أو إذا كان من شأن تنفيذ هذا الالتزام الإفصاح عن بيانات شخصية تتعلق بفرد آخر لم يوافق على ذلك، وأن الإفصاح قد يترتب عليه ضرر مادي أو معنوي لهذا الفرد أو أي فرد آخرين" [160].

ويمكن أن تؤدى هذه المعالجة – بطريقة مباشرة أو غير مباشرة – إلى إظهار الأصول العرقية أو الآراء السياسية أو الدينية أو الانتماء النقابي[161] أو تكون هذه المعالجة متعلقة بالحالة الصحية أو

---

[156] المادة (18) من قانون حماية البيانات الشخصية القطري.

[157] المادة (19) من قانون حماية البيانات الشخصية القطري.

[157] عرفت المادة (1) من قانون حماية البيانات الشخصية القطري المراقب بأنه: (الشخص الطبيعي أو المعنوي الذي يقوم منفرداً أو بالاشتراك مع آخرين بتحديد كيفية معالجة البيانات الشخصية والغرض منها).

[159] المادة (20) من قانون حماية البيانات الشخصية القطري.

[160] المادة (21) من قانون حماية البيانات الشخصية القطري.

[161] Art 26 – II- Processing relating to the data mentioned in Section I of Article 8 (political, philosophical, medical, sexual life) shall be authorized by a decree subject to a prior opinion of the “Conseil d’Etat” (“decree of “Conseil d’Etat” issued after a

الحياة الجنسية [162] أو لحساب شخص معنوي عام أو لحساب شخص معنوي خاص يقدم خدمة عامة، وتتم هذه المعالجة على بيانات شخصية من ضمنها الرقم القومي الشخصي، وذلك لأن الرقم القومي للشخص يمكن من خلاله الحصول على معلومات أخرى كثيرة عن هذا الشخص[163] أو معالجة البيانات الشخصية التي تتم لحساب الدولة، والتي يكون موضوعها بيانات بيو مترية[164] ضرورية لتحديد هوية الشخص[165].

وحماية هذه البيانات الحساسة إذا تمت معالجتها لحساب الدولة، من الممكن أن يتم معالجتها بطريقة تمييزية تؤدى إلى انتهاك هوية الشخص خاصةً وأن جمعها يتم بمنتهي السهولة من خلال البيع عبر شبكة الإنترنت للمجموعات المتقطعة مما يجعلها تحتاج إلى عناية خاصة ويستوجب خضوعها لشروط أكثر صرامة لذا حددت القوانين والتوجيهات نظاما خاصا لمعالجة هذه البيانات، وهى وجوب الحصول على ترخيص صريح لا يشترط أن يكون مكتوباً وضرورة أن تكون المعالجة لتحقيق مصلحة حيوية لصاحب البيانات أو لجهة أخرى كأمن الدولة وذلك حتى لا يحدث اعتداء خطيرً للأفراد[166].

---

reasoned and published opinion of the Commission. This opinion shall be published with the decree authorizing the processing.

[162] Art 26 – III for the implementation of this Article, processing operations which serve the same purpose, relate to identical categories of data and have the same recipients or categories of recipients may be authorized by a common regulatory decision. In this case, each data controller shall send the Commission a legal commitment stating the processing complies with the description in the authorization.

[163] Art 27 – I. n°- The "Conseil d'Etat" shall authorize by decree, taken after a reasoned and published opinion of the CNIL: 1° the processing of personal data carried out on behalf of the State, a legal entity governed by public law or a legal entity governed by private law that manages a public service, relating to data containing the registration number of individuals in the national register for the identification of individuals ("NIR", i.e. social security number);

[164] ويقصد بالبيانات البيومترية الواردة بالمادة 2-1/27 البيانات التي تستند على الخصائص الطبيعية للشخص والتي يتم التوصل من خلالها لهويته، وهي كثيرة ومنها: البصمة الرقمية، البصمة الوراثية، محيط كف اليد، الصوت، طريقة مشية الشخص.

[165] Art 27 – I.- n°2

[166] مروة زين العابدين، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، مرجع سابق ، ص 407.

وفرض الشروط الصارمة قد يحقق الحماية القانونية إلا أن ما يعيقه هو أن البيانات الشخصية متاحة على شبكة الإنترنت سواء للنسخ أو المعالجة مما يستدعي ضرورة وضع ضوابط قانونية قابلة للتنفيذ وأكثر فاعلية لمواكبة التسارع التكنولوجي والذي طالما يتأخر المشرع في العالم عن مواكبته لا سيما في الدول العربية.

المطلب الثالث: آثار المسؤولية

لم يتوان المشرع القطري من جعل المساس بالبيانات الشخصية على مواقع التواصل الاجتماعي يفضي إلى المسؤولية الجزائية وكذلك المسؤولية المدنية وإن كانت المسؤولية المدنية هي التي تفضي إلى جبر الضرر على مواقع التواصل الاجتماعي.

بحيث سيتم التعرّض في هذا المبحث إلى كل من المسؤولية الجزائية والمسؤولية المدنية الناتجة عن المساس بالبيانات ذات الطابع الشخصي على مواقع التواصل الاجتماعي.

الفرع الأول: وقف الاعتداء على البيانات الشخصية.

يقرر القانون المدني القطري أنه: " لكل من وقع عليه اعتداء غير مشروع في حق من الحقوق الملازمة لشخصيته، أن يطلب وقف هذا الاعتداء مع التعويض عما يكون قد لحقه من ضرر".

وتتضمن هذه الحماية سبيلين لصد الاعتداء منها حق الشخص المعتدى عليه في طلب وقف الاعتداء وحق الشخص المعتدى عليه في طلب التعويض عن الضرر الذي لحقه من جراء الاعتداء.

والحق في الخصوصية والحق في الاسم والحق في الصورة وحرمة الشرف والاعتبار من الحقوق اللصيقة بالشخصية[167]، ومن ثم تتمتع بالحماية التي تخص هذه الحقوق من زاوية لجوء المعتدى عليه للقضاء لوقف الاعتداء ومنعه ويستطيع الشخص المعتدى على حرمة حياته الخاصة، أن يطلب منع هذا الاعتداء ووقفه، دون التقيد بقواعد المسؤولية التقصيرية التي تتطلب إثبات الخطأ والضرر وعلاقة السببية[168].

وقد نصت المادة (3) من قانون حماية البيانات الشخصية القطري على أنه: " لكل فرد الحق في حماية خصوصية بياناته الشخصية، ولا يجوز معالجة تلك البيانات إلا في إطار الشفافية والأمانة واحترام كرامة الإنسان والممارسات المقبولة، وفقاً لأحكام هذا القانون" ، كما نصت المادة (5): "يجوز للفرد في أي وقت ، سحب موافقته السابقة على معالجة بياناته الشخصية أو الاعتراض

---

[167] حسام الدين كامل الأهواني، الحق في احترام الحياة الخاصة (الحق في الخصوصية) دراسة مقارنة، دار النهضة العربية، ص76.

[168] عصام أحمد البهجي، حماية الحق في حرمة الحياة الخاصة في ضوء حقوق الانسان والمسؤولية المدنية، دار الجامعة الجديدة، الإسكندرية، 2005، ص390.

على معالجة بياناته الشخصية إذا كانت غير ضرورية لتحقيق الأغراض التي جمعت من أجلها، أو كانت زائدة على متطلباتها، أو تمييزية أو مجحفة أو مخالفة للقانون أو طلب حذف بياناته الشخصية أو محوها في الحالات المشار إليها في البندين السابقين، أو عند انتهاء الغرض الذي تمت من أجله معالجة تلك البيانات، أو إذا لم يكن هناك مبرر للاحتفاظ بها لدى المراقبة أو طلب تصحيح بياناته الشخصية ، مرفقاً به ما يثبت صحة طلبه".

كما نصت المادة (26) : "على أنه للفرد أن يتقدم بشكوى إلى الإدارة المختصة، في حالة مخالفة أحكام هذا القانون والقرارات الصادرة تنفيذاً له-وللإدارة المختصة، بعد التحقيق في الشكوى وثبوت جديتها، أن تصدر قراراً مسبباً بإلزام المراقب أو المعالج، بحسب الأحوال، بتدارك تلك المخالفة خلال مدة تحددها".

كما نصت المادة (9) من القانون المدني الفرنسي أنه: " لكل فرد الحق في احترام حياته الخاصة، وتبين الفقرة الثانية من ذات المادة أن من حق المحكمة، ودون الإخلال بالحق في التعويض، أن تأمر بتدابير مؤقتة لمنع استمرار انتهاك الخصوصية- ويحق وفقاً لما تقدم لمن أعتدي على بياناته الشخصية أن يطلب من المحكمة وقف هذا الاعتداء ومنعه من الاستمرار سواءً أكان هذا الاعتداء على اسمه أو صورته أو على شرفه وكرامته أو كان المقصود به التشهير أو الابتزاز أو غيرها من صور الاعتداء" [169].

الفرع الثاني: المسؤولية الجزائية.

أفرد المشرع الجزائي القطري عقوبات على حالات المساس بالبيانات الشخصية وذلك بتفريد السلوك المادي المعاقب عليه سواء كان في شكل إيجابي عمدي أو بإهمال أو سلوك سلبي حيث تصدت المادة (23) من قانون حماية البيانات الشخصية القطري لكافة حالات المساس بالبيانات الشخصية[170]. كما تضمّن قانون حماية البيانات الشخصية إقرار مسؤولية الشخص الاعتباري عندما

---

[169] عثمان بكر عثمان، المسؤولية عن الاعتداء على البيانات الشخصية عبر شبكات مواقع التواصل الاجتماعي، مرجع سابق، ص 29.

[170] نصت المادة (23) من قانون حماية البيانات الشخصية على أنه : "مع عدم الإخلال بأي عقوبة أشد ينص عليها قانون آخر يعاقب بالغرامة التي لا تزيد على 1000.000 مليون ريال، كل من خالف أياً من أحكام المواد (4)،(8)،(9)،(10)،(11)،(12)،(14)،(15)،(22) من هذا القانون. وتعاقب هذه المادة على الحالات التالية:

1-معالجة البيانات الشخصية ، دون الحصول على موافقة الفرد، ما لم تكن المعالجة ضرورية لتحقيق غرض مشروع للمراقب أو الغير الذي تُرسل إليه البيانات.

2- معالجة البيانات الشخصية بغير أمانة ومشروعية.

3-عدم مراعاة الضوابط الخاصة بتصميم أو تغيير أو تطوير المنتجات والنظم والخدمات المتعلقة بمعالجة البيانات الشخصية

4-عدم اتخاذ الاحتياطات الإدارية والفنية والمادية المناسبة لحماية البيانات الشخصية، وفقاً لما تحدده الإدارة المختصة

5-عدم مراعاة سياسات حماية الخصوصية، التي تضعها الإدارة المختصة.

6-عدم اعلام الفرد ببيانات المراقب، أو أي طرف آخر يتولى معالجة البيانات لصالح المراقب أو لاستغلالها من قبله.

7-عدم اعلام الفرد بالأغراض المشروعة التي يرغب المراقب أو أي طرف آخر في معالجة البيانات الشخصية من أجلها.

8-عدم اعلام الفرد بالوصف الشامل والدقيق لأنشطة المعالجة ودرجات الإفصاح عن البيانات الشخصية للأغراض المشروعة، وإذا لم يتمكن 9-المراقب من ذلك، فيتعين عليه تمكين الفرد من وصف عام لها.

10-عدم اعلام الفرد بأية معلومات أخرى تكون ضرورية ولازمة لاستيفاء شروط معالجة البيانات الشخصية.

11-عدم تحقق المراقب من أن البيانات الشخصية التي يجمعها، أو التي يتم جمعها لصالحه، ذات صلة بالأغراض المشروعة وكافية لتحقيقها، أو عدم التحقق من أن تلك البيانات دقيقة ومكتملة ومحدثة بما يفي بالأغراض المشروعة، وألا يحتفظ بها لمدة تزيد على المدة الضرورية لتحقيق تلك الأغراض.

12-عدم قيام المراقب بمراجعة إجراءات حماية الخصوصية قبل إدراج عمليات معالجة جديدة

13-عدم قيام المراقب بتحديد المعالجين المسؤولين عن حماية البيانات الشخصية

14-عدم قيام المراقب بتدريب وتوعية المعالجين على حماية البيانات الشخصية

15-عدم قيام المراقب بوضع نظم داخلية لتلقي الشكاوى، وطلبات الوصول للبيانات، وطلبات تصحيحها أو حذفها، وإتاحة ذلك للأفراد

16-عدم قيام المراقب بوضع نظم داخلية للإدارة الفعالة للبيانات الشخصية، والإبلاغ عن أيتجاوز للإجراءات التي تهدف إلى حمايتها.

17-عدم قيام المراقب باستخدام الوسائل التكنولوجية المناسبة لتمكين الأفراد من ممارسة حقهم في الوصول إلى البيانات الشخصية ومراجعتها وتصحيحها بشكل مباشر.

18-عدم قيام المراقب بإجراء عمليات تدقيق ومراجعة شاملة عن مدى الالتزام بحماية البيانات الشخصية

19-عدم قيام المراقب بالتحقق من التزام المعالج بالتعليمات التي يوجهها إليه، واتخاذ الاحتياطات المناسبة لحماية البيانات الشخصية، ورصد ومتابعة ذلك بصفة مستمرة.

20-عدم افصاح المراقب عن البيانات الشخصية أو نقلها إلى المعالج، مراعاة أن تكون مطابقة للأغراض المشروعة، وأن تكون تلك البيانات معالجة وفقاً لأحكام هذا القانون.

21-عدم قيام المراقب بإعلام الفرد والإدارة المختصة، بحدوث أي إخلال بالاحتياطات المنصوص عليها في المادة السابقة، إذا كان من شأن ذلك إحداث ضرر جسيم بالبيانات الشخصية أو بخصوصية الفرد.

نصت المادة (25) بأنه: "يُعاقب الشخص المعنوي المخالف بالغرامة التي لا تزيد على 1000,000 مليون ريال، إذا ارتكبت باسمه ولحسابه إحدى الجرائم المنصوص عليها في هذا القانون، وذلك مع عدم الإخلال بالمسؤولية الجنائية للشخص الطبيعي التابع له".

ومن المادة 23 يتضح تنوع الجرائم الإلكترونية التي تمس البيانات الشخصية فمنها جريمة المعالجة الإلكترونية والانحراف عن الغرض أو الغاية من المعالجة الإلكترونية وجريمة الإفشاء غير المشروع للبيانات.

بالنسبة لجريمة المعالجة الإلكترونية:

22-قيام المراقب باتخاذ أي قرار أو إجراء من شأنه الحد من تدفق البيانات الشخصية عبر الحدود، إلا إذا كانت معالجة تلك البيانات مخالفة لأحكام هذا القانون، أو كان من شأنها إلحاق ضرر جسيم بالبيانات الشخصية أو بخصوصية الفرد.

23-إرسال المراقب اتصال إلكتروني بغرض التسويق المباشر إلى الفرد، بغير الحصول على موافقته المسبقة

24-مخالفة الضوابط اللازمة في ارسال الاتصال الالكتروني "

كما أفرد المشرع في قانون حماية البيانات حماية أخرى من أفعال المراقبين أو معالجي البيانات حيث عاقب المشرع بعقوبة الغرامة على الحالات التالية:

1-عدم اتخاذ المراقب والمعالج الاحتياطات اللازمة لحماية البيانات الشخصية من الضياع أو التلف أو التعديل أو الإفشاء، أو الوصول إليها، أو استخدامها بشكل عارض أو غير مشروع

2-عدم تناسب الاحتياطات التي يتخذها المراقب لحماية البيانات الشخصية مع طبيعة وأهمية البيانات الشخصية المراد حمايتها

3-إخلال المراقب بإخطار الفرد بوجود أي إخلال بالاحتياطات المشار إليها، أو عند حدوث أي خطر يهدد البيانات الشخصية للأفراد بأي وجه، فور علمه بذلك.

4-معالجة البيانات الشخصية ذات الطبيعة الخاصة، بغير الحصول على تصريح بذلك من الإدارة المختصة، وفقاً للإجراءات والضوابط التي يصدر بتحديدها قرار من الوزير

5-عدم قيام مالك الموقع أو المراقب بوضع إخطار على الموقع حول ماهية بيانات الأطفال، وكيفية استخدامها، والسياسات التي يتبعها في الإفصاح عنها

6-عدم الحصول على موافقة صريحة من ولي أمر الطفل الذي تتم معالجة بيانات شخصية عنه، وذلك عن طريق اتصال إلكتروني أو أي وسيلة أخرى مناسبة.

7- التقاعس عن تزويد ولي أمر الطفل، بناءً على طلبه، وبعد التحقق من هويته، بوصف لنوع البيانات الشخصية التي تتم معالجتها، مع بيان الغرض من المعالجة، ونسخة من البيانات التي تمت معالجتها أو جمعها عن الطفل

8- حذف أو محو أو وقف معالجة أية بيانات شخصية تم جمعها من الطفل أو عنه، إذا طلب ولي الأمر ذلك

9-اشتراط مشاركة الطفل في لعبة، أو عرض جائزة، أو أي نشاط آخر ،بتقديم الطفل بيانات شخصية تزيد على ما هو ضروري للمشاركة في ذلك النشاط.

هي تقوم على ركنين أحدهما الركن المادي الذي يتوّفر حينما يقوم الجاني بفعل المعالجة التي تشمل مجموعة العمليات التي تتم إلكترونياً من التسجيل والتعديل والإضافة والمحو أو أي تغيير آخر يمكن أن يطرأ على هذه البيانات ينطوي على اتصال غير مشروع بالشبكة بعد اختراق أنظمة الأمن والحماية بقصد الربط بينها للحصول على المعلومات وبالتالي يتوفر هذا الركن بمجرد معالجة البيانات دون ترخيص حتى وإن لم يترتب على ذلك أية نتيجة إجرامية فهي جريمة سلوكية لا تتطلب تحقيق نتيجة معينة[171].

أمّا الركن الثاني، فهو الركن المعنوي: ويتخذ صورة القصد الجنائي ويقوم على عنصري العلم والإرادة فالعلم يعني علم الجاني بالصفة الشخصية للبيانات وأن إجراء المعالجة الإلكترونية دون ترخيص من اللجنة المختصة من طبيعة البيانات الرقمية، أما الإرادة فهي أن تتجه إرادة الجاني لاتخاذ الإجراءات الأولية لإجراء المعالجة الإلكترونية للبيانات بالمخالفة بصرف النظر عن البواعث التي دفعت الجاني إلى ارتكاب فعله سواء كان الباعث هو الإضرار المادي بالشخص أم استغلال هذه البيانات للإساءة إلى سمعة الشخص أو لمجرد الفضول وحب الاستطلاع[172].

بالنسبة لجريمة الإفشاء غير المشروع للبيانات:

وتقوم على ركنين الأول: الركن المادي ويتخذ صورة السلوك بالقيام بأحد الفعلين فعل الحيازة للبيانات بقصد تصنيفها أو نقلها أو علاجها، والفعل الثاني هو فعل الإفشاء لهذه البيانات لشخص آخر غير مختص بتلقي هذه البيانات، وينبغي لقيام هذا الركن تحقق النتيجة الإجرامية وهى الإضرار بالغير والاعتداء على حرمة خصوصيته وأن ترتبط هذه النتيجة بالفعل بعلاقة السببية ويجب انتفاء رضاء المجني عليه، وأن يكون الإفشاء من جهة ليس لها الحق بالاطلاع على هذه البيانات[173].

---

[171] مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، مرجع سابق، ص 467.

[172] مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، مرجع سابق، ص 467.

[173] مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، مرجع سابق، ص 470.

والركن الثاني / المعنوي الذي يتخذ إحدى صورتين إما العمد (القصد الجنائي) أي علم الجاني بأن البيانات التي يعالجها شخصية ويمثل إفشاؤها اعتداء على حرمة الحياة الخاصة أو صور الخطأ حيث يعاقب الجاني على الإفشاء إذا وقع نتيجة إهمال[174].

الفرع الثالث: المسؤولية المدنية

يحق لمن يُعتدى على بياناته الشخصية أن يطلب التعويض عن الضرر الذي لحقه من جراء هذا الاعتداء ولقيام المسؤولية المدنية لابد من توافر الخطأ والضرر وعلاقة السببية، ولا شك في أن المسؤولية في هذه الحالات تكون وفقاً للقواعد العامة للمسؤولية التقصيرية-وحتى تقوم المسؤولية التقصيرية لابد من توافر الخطأ (فعل الاعتداء) وأن يترتب عليه ضرر للشخص المعتدي عليه، والخطأ التقصيري يتحقق عند الإخلال بواجب قانوني عام واحد لا يتغير، وهو الالتزام بعدم الإضرار بالغير[175].

ويمكن تصور الخطأ التقصيري عبر شبكات التواصل الاجتماعي طبقاً لما نصت عليه المادة 23 من قانون حماية البيانات الشخصية القطري السالف ذكرها ، عند معالجة البيانات الشخصية وتجميعها دون رضا صاحبها ، كما يمكن اعتباره خطأً، اختراق الحسابات الشخصية والتشهير بأصحابها وابتزازهم ونشر الصور الشخصية وتجاوز حدود الإذن في النشر وغيرها من صور الاعتداء التي تعد خطأً تقصيرياً نتيجة الإخلال بواجب قانوني عام وهو عدم الإضرار بالغير والتي نذكرها على سبيل المثال لا الحصر، وتوفر الضرر جوهر المسؤولية المدنية سواء كان ضرراً مادياً يصيب الشخص في أمواله كالاستيلاء على بيانات العملاء ونشرها عبر الإنترنت ، أو استخدام العلامة التجارية الخاصة بالغير على المواقع الإلكترونية ، وقد يكون الضرر أدبياً يصيب الإنسان في شعوره وعاطفته أو كرامته وشرفه واعتباره أو في جسمه كنشر فيديو عبر شبكات التواصل الاجتماعي يظهر أمام الجمهور في وضع مخل للآداب أو من الممكن أن يقع في المستقبل فعلى الرغم من إزالة الفيديو إلا أنه سيعاد نشره في مواقع أخرى أو ذات الموقع من أشخاص آخرين[176].

---

[174] مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني مرجع سابق، ص 470.

[175] عبد الرزاق السنهوري، الوسيط في القانون المدني، الجزء الأول ، طبعة نقابة المحامين ، 2006، ص506.

[176] عثمان بكر عثمان، المسؤولية عن الاعتداء على البيانات الشخصية عبر شبكات مواقع التواصل الاجتماعي، مرجع سابق، ص 30.

ويشمل التعويض عن الضرر المادي والأدبي ولكنه لا يشمل إلا الضرر الحال أو المستقبلي دون الضرر الاحتمالي، ويجوز التعويض عن الفرصة الفائتة طبقاً للقواعد العامة ومثال ذلك ما يفعله شخص من نشر صورة على إحدى مواقع التواصل الاجتماعي عبر الإنترنت تظهر فتاة مع شخص وهما يتعاطون المخدرات في مكان خاص، إلا أنه يتضح بعد ذلك أنها صورة كاذبة قد تم تركيبها باستخدام أحد برامج الكمبيوتر التي تستعمل في أغراض تغيير وجوه الأشخاص وتبديلها، إلا أن الضرر الذي لحق بهذه الفتاة أنها كانت مخطوبة وانتهت هذه الخطبة بسبب تلك الصورة، مما فوت عليها فرصة الزواج [177].

وكذلك يلزم توفر علاقة السببية، أي من وقع عليه ضرر من فعل الاعتداء أن يثبت أن هذا الخطأ هو سبب الضرر، إذ لا يكفي لقيام المسؤولية، أن يتوافر ركنا الخطأ والضرر، بل يجب أن يكون الخطأ هو السبب في الضرر، وهذه هي علاقة السببية[178].

وبناءً على ما تقدم فإنه يترتب على ثبوت الخطأ (فعل الاعتداء) تعويض المضرور، وتقدير التعويض من إطلاقات محكمة الموضوع، دون رقابة عليها من محكمة النقض، متى قامت أسبابه، ولم يكن في القانون نص ملزم بإتباع معايير معينة في خصوصه، وهذا ما أكده القضاء القطري عندما اعتبر أن :" تقدير الضرر وتحديد التعويض الجابر له من مسائل الواقع التي يستقل بها قاضي الموضوع دون رقابة عليه من محكمة التمييز بشرط إقامة قضائه على أساس مقبول (بشأن تقدير المحكمة تعويض البنك الطاعن عما أصابه من ضرر نتيجة تأخر المطعون ضده في سداد دين القرض المصرفي)" [179] ، وعادةً ما يحدد مبلغ التعويض، على أساس قيمة الضرر وقت صدور الحكم، نزولاً على اعتبارات عملية تتمثل في تفويت الفرصة على المدين حتى لا يطيل أمد النزاع بهدف الاستفادة من انخفاض قيمة العملة[180].

---

[177] محمد حسين عبدالعال، تقدير التعويض عن الضرر المتغير، دراسة تحليلية، مرجع سابق، ص5.

[178] جميل الشرقاوي، النظرية العامة للالتزام - مصادر الالتزام، مرجع سابق، ص 527.

[179] الطعن رقم 220 لسنة 2011 تمييز مدني، جلسة 13 من مارس سنة 2012، موسوعة الأحكام والمبادئ القضائية القطرية ، تاريخ الدخول 2021/1/30 ، الوقت : 11:18 مساءً.

http://eservices.sjc.gov.qa/Portal_1/ahkam/TextSearch.aspx?gcc=1&ct=1

[180] حسام لطفي، النظرية العامة للالتزام، مرجع سابق، ص 60.

المبحث الثالث:

الاختصاص القضائي والتشريعي المتعلقين بمنازعات البيانات على مواقع التواصل الاجتماعي.

تثار عدة تساؤلات حول الاختصاص التشريعي والقضائي لحل المنازعات الناشئة عن الفضاء الإلكتروني من حيث تحديد القضاء المختص بنظر المنازعات التي تنشأ عن الممارسات غير المشروعة عبر مواقع التواصل (الوطني أم الأجنبي)؟ وهل يجوز للمواقع أن تنص في شروط تعاقدها مع المستخدمين على تحديد القضاء المختص؟ وما الحل في حالة قيام الدول بوضع شروط الاختصاص القاصر على قضائها وتشريعاتها؟ وهل المشكلة في ندرة التشريعات التي تحكم مواقع التواصل الاجتماعي أم تزاحمها؟ وهل تحكم نزاعات مواقع التواصل الاجتماعي فرع واحد من القوانين أم تتداخل الفروع على المنازعة؟

وللإجابة على هذه التساؤلات يلزم التطرق تفصيلاً لحدود الاختصاص التشريعي والقضائي لمنازعات المساس بالبيانات الشخصية على مواقع التواصل الاجتماعي.

المطلب الأول: الاختصاص التشريعي المتعلّق بمنازعات البيانات على مواقع التواصل الاجتماعي.

بداية يلزم التسليم بأن منازعة البيانات الشخصية على مواقع التواصل الاجتماعية تحكمها عدة أفرع من القانون بداية من القانون الدستوري والقانون المدني والقانون التجاري وقانون العمل والقانون الجنائي والقانون الإداري وقانون الملكية الفكرية والقوانين المتعلقة بحماية البيانات الشخصية، وهناك إشكالية وسائل التواصل الاجتماعي باعتبارها لزالت أماكن افتراضية ليست لها أمكان محددة فيكون من الأسهل على الدولة أن تتمسك بتطبيق قانونها الوطني واختصاص محاكمها فيما يخص البيانات ذات الطابع الشخصي على مواقع التواصل الاجتماعي ، وأنه يلزم لتحديد الاختصاص القضائي والتشريعي تكييف طبيعة المنازعة وما قد تُشكله من مساس بأي من أحكام القوانين السابقة وهل تتعارض مع قواعد آمرة بالدولة أو قواعد النظام العام والآداب.

ويثير اختلاف التشريعات القانونية بين الدول على المستوى الدولي تنازع في الاختصاص لجرائم الإنترنت لكونها عابرة للحدود فقد ترتكب الجريمة في إقليم دولة معينة من قبل أجنبي، فتكون الجريمة خاضعة للاختصاص الجنائي للدولة الأولى استناداً إلى مبدأ الإقليمية، وتخضع

لاختصاص الدولة الثانية على أساس مبدأ الاختصاص الشخصي في جانبيه، وقد تهدد الجريمة أمن وسلامة دولة أخرى فتدخل في اختصاصها استناداً إلى مبدأ العينية[181].

و نرى أنه أية بنود تحدد الاختصاص القضائي والتشريعي قد ترد في الشروط العامة لاستعمال مواقع التواصل تعتبر بنود تعسفية - كالبند الوارد في الشروط العامة لموقع تويتر والذي يحدد القانون الواجب التطبيق والمحكمة المختصة بأنه تخضع كل دعوى متعلقة به لقوانين ولاية كاليفورنيا دون اعتبار لحصول اختلاف مع القواعد القانونية لبلد المستخدم أو محل إقامته ، كما تكون محاكم سان فرانسيسكو في كاليفورنيا هي المختصة ، وتتضمن هذه الشروط أن المستخدم يوافق على ذلك لمجرد التسجيل على توتير ويتنازل عن كل اعتراض لهذه الجهة [182] - وهو ما أكده المشرع القطري فقد أحسن صنعاً عندما نص في المادة (28) من قانون حماية البيانات الشخصية على أنه: " يقع باطلاً كل عقد أو اتفاق يتم بالمخالفة لأحكام هذا القانون" ، مما يدل على أن المشرع القطري جعل اختصاصه سواء في المسائل الجزائية أو المدنية والتجارية أو في المنازعات المتعلقة بالبيانات الشخصية على مواقع التواصل الاجتماعي وفق الية الاسناد الحصري قاصر لقضائه طبقا لأحكامه الواردة في قانون المرافعات أو قانون العقوبات وفقاً لمبدأ الإقليمية أو مبدأ الشخصية ومبدأ العينية.

والاختصاص التشريعي في منازعات التواصل الاجتماعي يتوقف على طبيعة المنازعة من كونها انتهاكاً لقواعد آمرة بدولة المستخدم وحينها لا يمكن إعمال القانون الأجنبي حتى ولو توافرت شرائط التنازع بين القوانين إنما تطبق القواعد الامرة بشكل مباشر في قانون دولة المستخدم أما إذا كانت تتعلق بمساحة الخدمات الناتجة عن الرابطة العقدية فيمكن حينها التمسك بفكرة قاعدة الاسناد الارادية المحددة بالاتفاق بينهما مع مراعاة أن قاعدة الاسناد الاختيارية المحددة في العقد ما بين المستخدم والموقع لا تسري على الغير الذي ليس طرفاً في اتفاق تنظيم الخدمة بينهما والذي يستطيع إقامة دعواه أمام قضاء دولته وتطبيق القوانين المتصلة بها، أما في غير منازعات العقود كما هو الحال في التعويض عن الاعمال غير المشروعة، فالقانون الواجب التطبيق يكون للدولة التي وقع

---

[181] محمد نصر محمد، المسؤولية الجنائية لانتهاك الخصوصية المعلوماتية دراسة مقارنة، مرجع سابق، ص 113.

182 وسيم شفيق الحجار، النظام القانوني لوسائل التواصل الاجتماعي، دراسة قانونية مقارنة حول الحرية الشخصية والمسؤولية والاختصاص، مرجع سابق، ص 112.

فيها الفعل الضار، وطالما أن حماية البيانات الشخصية من المسائل المتعلقة بالحقوق والحريات فإنه من الأجدر تطبيق القواعد المادية بشكل مباشر[183] .

وخلاصة القول فإن حماية البيانات الشخصية على مواقع التواصل الاجتماعي يطبق بشأنها قانون دولة المستخدم أو قانون الدولة التي حدث بها الضرر طالما كان مناط النزاع انتهاك البيانات الشخصية في ظل عدم قيام الدول بوضع نظام قانوني موحد يعمل على حمايتها باعتبار أن حماية البيانات الشخصية، أما النزاعات التي تثور حول مساحة الحقوق الناتجة عن الاستخدام يمكن أن يرجع بشأنها لقواعد الأسناد من جواز تركها لإرادة المتعاقدان[184].

المطلب الثاني: الاختصاص القضائي بمنازعات البيانات على مواقع التواصل الاجتماعي.

كما هو الحال في الاختصاص التشريعي في أن البند الذي يجعل الاختصاص القضائي لمحاكم معينة هو شرط لا يعول عليه أمام القضاء الوطني لدولة المستخدم أو المضرور التي عادةً ما تلجأ إلى التوسع في مفهوم اختصاصها بنظر المنازعات المتعلقة بحماية البيانات الشخصية على مواقع التواصل الاجتماعي، حيث يتم تقسيم المنازعات بين ما يتعلق بالقوانين الجزائية أو القواعد المتعلقة بالنظام العام أو ما يتعلق بمساحة الحقوق بين المتعاقدين فلا مجال للتمسك بأي اختصاص غير اختصاص الدولة في المسائل الجزائية الواقعة على البيانات ذات الطابع الشخصي على مواقع

---

[183] محمد أحمد المعداوي، حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي، مرجع سابق، ص 1985.

[183] نصت المادة (27) من القانون المدني القطري الصادر بالمرسوم رقم (22) لسنة 2004 على أنه: "يسري على العقد من حيث الشروط الموضوعية لانعقاده ومن حيث الآثار التي تترتب عليه، قانون الدولة التي يوجد فيها الموطن المشترك للمتعاقدين، فإن اختلفا موطناً سرى قانون الدولة التي تم فيها العقد، هذا ما لم يتفق المتعاقدان أو يتبين من الظروف أن قانوناً آخر هو الذي يراد تطبيقه"، كما نصت المادة (29) على أنّه "يسري على العقد، من حيث الشكل، قانون البلد الذي تم فيه، ويجوز أيضاً سريان القانون الذي يخضع له العقد في أحكامه الموضوعية، كما يجوز سريان قانون موطن المتعاقدين أو قانونهما الوطني المشترك". ونصت المادة (30) على أنه: "يسري على الالتزامات الناشئة عن العمل غير المشروع قانون البلد الذي وقع فيه الفعل المنشئ للالتزام، ولا تسري أحكام الفقرة السابقة على الوقائع التي تحدث في الخارج وتكون مشروعة في قطر، ولو كانت تعد غير مشروعة في البلد الذي وقعت فيه".

ونصت المادة (32) على أنه " تطبق محاكم قطر في العلاقات القانونية ذات العنصر الأجنبي، قواعد الاختصاص وجميع المسائل الخاصة بالإجراءات التي يقررها القانون القطري"، ونصت المادة (38) على أنه: "لا يجوز تطبيق أحكام قانون أجنبي عينته المواد السابقة إذا كانت هذه الأحكام تخالف النظام العام أو الآداب في قطر، ويتعين في هذه الحالة تطبيق القانون القطري" .

التواصل الاجتماعي وفقاً لمبدأ الإقليمية. والحال كذلك فيما يتعلق بمسائل النظام العام التي تترك للقضاء في شأن تحديدها.

ويخالف المشرع القطري النظم القانونية التي تأخذ بفكرة قواعد الاسناد للاختصاص القضائي أو ما يعرف بتنازع الاختصاص بأن يعتبر أن مخالفة ذلك واتفاق الأطراف على انعقاد الاختصاص في العقد المبرم في الدولة أو العقد المفترض تنفيذه فيها من مسائل النظام العام ولا يجوز التنازل عن سيادة القضاء في هذا المجال بما يبطل شرط الاتفاق على ولاية قضاء أجنبي في عقد تجاري أبرم ونفذ في قطر[185].

ويذهب القضاء الأوروبي عامة إلى التوسع في اختصاصه فيما يخص مواقع التواصل الاجتماعي من خلال تطبيق الاختصاص القاصر على دعوى بعينيها مثل انتهاك البيانات الشخصية أو التعويض عن تداول البيانات وتحليلها وتوجيهها بصورة غير سلمية أو بدون رضاء صاحبها[186].

بل أن المحاكم الفرنسية أقرت باختصاصها طالما كان هناك إمكانية تقنية للوصول الى الموقع في فرنسا بالرغم من معارضة محكمة العدل الاوروبية لاعتماد هذا المعيار وحده وطلبها اعتماد توفّر معايير أخرى لانعقاد الاختصاص الفرنسي كأن يكون الغرض من الوصول الى البيانات التأثير على الاقتصاد الفرنسي أو حدوث ضرر اجتماعي أو شخصي داخل فرنسا هذا وقد ذهبت المحاكم الفرنسية وفق توجه محكمة العدل الاوربية إلى اشتراط أن يكون الضرر موجه للجمهور الفرنسي

---

[185] ورد في تسبيب أحد أحكام محكمة التمييز القطرية أنّه : " لما كان أداء العدالة مصلحة عامة تباشرها الدولة وحيث إن هذا النعي غير سديد، ذلك أنه لما كان أداء العدالة مصلحة عامة تباشرها الدولة في الحدود التي تحقق هذه المصلحة بواسطة قضائها الذي تراه دون غيره من قضاء أجنبي أجدر بتحقيق هذه الغاية، فإن الاختصاص الدولي المعقود للمحاكم القطرية- وعلى ما جرى به قضاء هذه المحكمة- يكون بهذه المثابة من النظام العام لارتباطه بسيادة الدولة، ومن ثم فلا يجوز الاتفاق على تنحية القضاء القطري لصالح قضاء أجنبي ، ويقع باطلاً كل شرط يخالف ذلك، وإذ فرض الحكم المطعون فيه اختصاص القضاء القطري بنظر النزاع الماثل ترتيباً على تعلقه بنشأة العلاقة القانونية سبب النزاع وتنفيذها داخل دولة قطر، فإنه يكون قد أعمل صحيح القانون، الأمر الذي يضحى معه النعي قائماً على غير أساس". يراجع الطعن رقم (62) لسنة 2011، جلسة 2011/6/14، موسوعة الأحكام والمبادئ القضائية القطرية، تاريخ الدخول: 2021/1/20، الوقت: 9:45 مساءً

https://www.sjc.gov.qa/ar/Pages/Encyclopedia-Of-Qatari-Provisions-And-Judicial-Principles.aspx.

[186] Vincent Vauchoux, Pierre Deprez, Jean-Michel Bruguière, Le droit de l'Internet, Lois contrats et usages, LexisNexis, 2nd édition, 2013, p 63, 64, 66.

أو له تأثير اقتصادي أو اجتماعي أو غيره على المجتمع الفرنسي بجانب معيار إمكانية الوصول الى الموقع الالكتروني حتى يصح القول باختصاص القضاء الفرنسي[187].

وفي الدعاوى الجزائية فإن المشرع القطري كغيره من النظم القانونية يتمسك بفكرة قاعدة الإقليمية بصورها المختلفة أو مبدأ الشخصية للمجني عليه أو المتهم في تطبيق قانون العقوبات لديه واختصاص قضائه الجنائي بنظر المنازعات التي تشكل في قوانينه الداخلية جريمة جنائية[188].

---

[187] محمد أحمد المعداوي، حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي، مرجع سابق، ص 1985.

[188] نصت المادة (19) من قانون العقوبات القطري على أنه: "يسري على الجريمة القانون المعمول به وقت ارتكابها، ومع ذلك إذا صدر بعد ارتكاب الجريمة وقبل الفصل فيها بحكم بات، قانون أصلح للمتهم، طبق هذا القانون دون غيره. وإذا أصبح الحكم باتاً، وصدر قانون يجعل الفعل أو الامتناع عن الفعل غير معاقب عليه، يوقف تنفيذ الحكم وتنتهي آثاره الجنائية. فإذا كان القانون الجديد مخففاً للعقوبة فحسب، فللمحكمة التي أصدرت الحكم البات، بناءً على طلب النيابة العامة أو المحكوم عليه، إعادة النظر في العقوبة المحكوم بها وفقاً لأحكام القانون الجديد".

ونصت المادة (13) على أنه: "تسري أحكام هذا القانون على كل من يرتكب في قطر جريمة من الجرائم المنصوص عليها فيه- وتعتبر الجريمة مرتكبة في قطر إذا وقع فيها فعل من الأفعال المكونة لها، أو إذا تحققت فيها نتيجتها، أو كان يراد أن تتحقق فيها".

ونصت المادة (14) على أنه: "تسري أحكام هذا القانون على الجرائم التي ترتكب على متن السفن والطائرات، التي تملكها الدولة أو تحمل علمها، أو تديرها لأي غرض، أينما وجدت".

نصت المادة (15) على أنه: " مع عدم الإخلال بالاتفاقيات والمعاهدات التي تكون الدولة طرفاً فيها، لا تسري أحكام هذا القانون على الجرائم التي ترتكب على متن السفن والطائرات الأجنبية الموجودة أو المارة بإقليم الدولة إلا إذا مست هذه الجرائم أمن الدولة أو كان الجاني أو المجني عليه قطرياً، أو طلب ربان السفينة أو قائد الطائرة المساعدة من السلطات القطرية".

نصت المادة (16) على أنه تسري أحكام هذا القانون على كل من:"1- ارتكب خارج قطر فعلاً يجعله فاعلاً أو شريكاً في جريمة وقعت كلها أو بعضها داخل قطر-2- ارتكب داخل قطر فعلاً يجعله فاعلاً أو شريكاً في جريمة وقعت كلها أو بعضها خارج قطر، متى كان معاقباً عليها بمقتضى هذا القانون وقانون البلد الذي وقعت فيه.-3- ارتكب أو شارك في ارتكاب جريمة خارج قطر من الجرائم الموجهة ضد أمن الدولة الخارجي أو الداخلي، أو الجرائم المتعلقة بتزوير أو تقليد المحررات الرسمية أو الأختام أو العلامات أو الطوابع الحكومية، أو تزوير أو تزييف أو تقليد أي عملة ورقية أو معدنية متداولة قانوناً في قطر، أو حيازة أو ترويج هذه العملات المزورة أو المزيفة أو المقلدة".

وأنه لا تثور إشكالية في تحديد الاختصاص الجنائي في الجرائم التي تقع على البيانات ذات الطابع الشخصي في مواقع التواصل الاجتماعي حيث تكون الجريمة حدثت في الإقليم الوطني بأن تكون البيانات أو الاعتداء عليها قد أعدت أو أدخلت أو تم المساس بها أو نسخت لبساطة وسهولة الوصول اليها من الإقليم الوطني. بل ان القضاء الفرنسي يتوسع في جرائم الانترنت من حيث الاختصاص بحيث تسري أحكامه طالما كان الفعل يستهدف الجمهور الفرنسي [189] .

وعامة الدول المستضيفة للشركات المالكة لمواقع التواصل الاجتماعي تعمل على اضعاف تنفيذ الاحكام الأجنبية الصادرة من محاكم توسع اختصاصها في نظر منازعات مواقع التواصل الاجتماعي على سبيل المثال عندما حدثت منازعة بشأن قيام موقع ياهو ببيع تذاكر (نازية) عن مزاد لبيع متعلقات النازية وقررت المحاكم الفرنسية اختصاصها حيث رأت انه كان يلزم على موقع ياهو جعل الوصول من الفرنسيين للموقع مستحيلاً فهو مسؤول عن عدم مشروعية الإعلانات ومسؤوليته تنشأ منذ العلم بالمحتوى غير المشروع للموقع بالرغم من أن الشركة تمسكت بأن السيرفرات المستضيفة للبيانات لا توجد في فرنسا إلا أن الولايات المتحدة الامريكية، حماية للشركات العملاقة المالكة لتكنولوجيا التواصل الاجتماعي، أُصدرت قانوناً يمنع فيه تنفيذ الاحكام الصادرة من القضاء الأجنبي الذي فيه اضعافاً لحرية الرأي وانتقال المعلومة[190].

نصت المادة (17) على أنه تسري أحكام هذا القانون على كل من: "وجد في الدولة بعد أن ارتكب في الخارج، بوصفه فاعلاً أو شريكاً، أياً من جرائم الإتجار في المخدرات أو في الأشخاص أو جرائم القرصنة أو الإرهاب الدولي".

نصت المادة (18) على أنه: " كل قطري ارتكب وهو خارج قطر فعلاً يعتبر جناية أو جنحة في هذا القانون، يُعاقب بمقتضى أحكامه إذا عاد إلى قطر، وكان الفعل معاقباً عليه بمقتضى قانون البلد الذي ارتكب فيه".

نصت المادة (19) على أنه: "لا تقام الدعوى الجنائية على من ارتكب جريمة في الخارج، إذا ثبت أن المحاكم الأجنبية أصدرت حكماً نهائياً ببراءته، أو ادانته واستوفى العقوبة أو سقطت عنه، أو انقضت الدعوى".

وإذا كان الحكم بالبراءة صاد اًر في إحدى الجرائم المنصوص عليها في البند (3) من المادة (16) من هذا القانون، مبنياً على أن قانون البلد الذي وقعت فيه لا يُعاقب عليها، جاز إقامة الدعوى الجنائية عنها أمام محاكم دولة قطر.

نصت المادة (20) على أنه: "تسري في شأن من أتم السابعة ولم يبلغ السادسة عشرة من عمره، الأحكام المنصوص عليها في قانون الأحداث. ولا يجوز الحكم بعقوبة الاعدام على من لم يبلغ الثامنة عشرة من عمره، وقت ارتكابه الجريمة".

[189] Cour de cassation, Chambre criminelle, arrêt 14/12/2010, N 10-80088, www.legifrance.gouv.fr

[190] مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت، مرجع سابق، ص 494.

الخـــاتـمة

هذا ، وبعد أن انتهينا بفضل الله وشكره من معالجة موضوع دراستنا حول " الحماية القانونية للبيانات الشخصية على مواقع التواصل الاجتماعي في نظام القانون القطري والقانون المقارن ؛ بالنظر إلى التطور التكنولوجي الذي نعيشه وزيادة استخدام الانترنت ووسائل التواصل الذي أنشأ خطراً يهدد خصوصية الفرد بإتاحة بياناته الشخصية عبر الشبكة العنكبوتية والتي يفصح عنها طواعية بإرادته بالرغم من أن هذه البيانات لا تفقد حمايتها بمجرد علانيتها أو الإفصاح عنها وإنما الاستيلاء عليها أو معالجتها بدون وجه حق وهو ما يمثل اختراقاً لحمايتها. وسعينا في هذه الدراسة البحثية الكشف عن ماهية البيانات الشخصية وحمايتها في العالم الافتراضي باتخاذ قانون حماية البيانات القطري رقم 13 لسنة 2016 م كأساس لهذه الدراسة وقد خلصنا في هذه الدراسة إلى النتائج التالية :

- أنه يقع على المستخدم عبء فهم شروط الدخول لمواقع التواصل الإجتماعي واستيعابها قبل الإشتراك فيها وأن يعي ماله من حقوق على هذه المواقع وما يمكنه التحكم فيه وأن لا يسلم بالإقتراحات المعدة مسبقاً بما يضمن حماية بياناته الشخصية واحترام خصوصيته وممارسة حريته في التعبير.
- يعد التكييف القانوني لنوع المسؤولية القانونية منها مسؤولية تقصيرية أم عقدية من أهم الإشكاليات التي تواجه الموضوع حيث يلزم أن يتوجه المشرعون صوب المسؤولية التقصيرية وافتراض الخطأ في حق المشغلين والمالكين لهذه المواقع وليس على أساس المسؤولية العقدية لأن هناك أطراف تتدخل في الاتصال بالموقع دون أن تربطها أية علاقة عقدية مثل الشركات الوسيطة المسؤولة عن الإعلانات والمستخدم.
- أنه من الصعوبة تقدير قيمة التعويض عن الضرر بالنظر إلى مقدار ما يلحق الشخص من خسارة في سمعته وكرامته وخصوصية حياته إذ أن جبر الضرر بإزالة ما تم التعدي عليه رقمياً لا يرمم ما ضاع من الشخص معنوياً، خاصةً وأن ما يتم نشره عبر مواقع التواصل يصعب نسيانه ومحوه من سمعة المستخدمين في ظل عدم تفعيل الحق في النسيان الرقمي حتى في حالة ندم من قام بالنشر لاحقاً.
- إن حماية البيانات الشخصية في البيئة الرقمية شأنها شأن الموضوعات المستحدثة التي يجب أن تلاحق بالتشريع مع ضرورة أن يتم ذلك بشكل سريع يستطيع أن يضاهي النمو

والاطراد التكنولوجي لشبكة الإنترنت، وقد أحسن المشرع القطري باستصداره قانون حماية البيانات الشخصية سنة 2016 في ظل التطور التكنولوجي الذي تشهده البلاد.

ونوصي من خلال هذه الدراسة بالآتي :

- أن يكون هناك موازنة بين الحق في التعبير وحرية التواصل الاجتماعي على هذه المواقع وبين متطلبات الأمن والسلامة العامة ومصالح المجتمع العليا من خلال تحقق شرطين، أولهما قانونية التعرض لخصوصية الفرد وثانيهما تقدير جسامة الخطر بما يبرر التعرض.
- نقترح أن يسن قانون حماية الخصوصية الشخصية على الشبكة العنكبوتية ينظم التزامات مزود خدمة الإنترنت وعلاقته بالمستخدم كأن يفرض على المزود أن يحصل على موافقة صريحة مكتوبة إلكترونيا أو يدوياً لجمع المعلومات الشخصية للمستخدم حسب نوع الخدمة المطلوبة نظير حصول الأخير عليها وتحديد الإطار المسموح للبيانات التي يجوز للمزود جمعها، وأن يكون المزود مسئولاً مسئولية مدنية عن الفعل الخاطئ الذي يقوم به إذا ما تسبب بضرر للمستخدم فضلاً عن مسئوليته الجنائية عن الجرم المرتكب في مواجهة الأخير، على أن يستثنى من التزامات المزود بحماية الخصوصية بعض المتطلبات الطارئة التي توسع من صلاحيات المزود كالحالات التي نصت عليها المادة 21 من القانون رقم (14) لسنة 2014 الخاص بمكافحة الجرائم الإلكترونية فلم ينص المشرع القطري في قانون حماية البيانات الشخصية صراحة على التزامات مزود خدمة الإنترنت وهو جانب قاصر في القانون حيث نص على احترام خصوصية البيانات بصفة عامة دون تحديد صريح لمهام المزود.
- الأخذ بنظرية تجزئة الحراسة وتطبيقها على المسؤولية القانونية عن البيانات الشخصية فالمسؤولية تقع على كل من يتدخل على البيانات، فكل يسأل حسب مهامه ولا تقع المسؤولية فقط على الموقع، انما قد يكون المستخدم هو وحده المسؤول عن انتهاك هذه البيانات بإتاحتها لأشخاص سيئين، أو الوسيط، أو المشغل أو الشركات الوسيطة العاملة في مجال تجميع وتحليل البيانات وبهذا تتحقق العدالة ويوضع الحد الفاصل بين خطأ كل من ساهم في الضرر.
- أن وسيلة التواصل الاجتماعي لا تكون مسؤولة الا في حالة معالجة بيانات المستخدم دون إذنه طبقاً لما نص عليه المشرع القطري في الماد 4 من قانون حماية البيانات الشخصية أو معرفتها الفعلية بطابعة غير المشروع دون اتخاذ أي إجراءات لحماية حساب المستخدم

رغم إبلاغها بذلك، عدا ذلك يكون المستخدم المسؤول الأول عن أعماله والمحتوى المحمل من قبله باعتباره صاحب المحتوى.

- أن قيام مواقع التواصل الاجتماعي بتجميع وتحليل بيانات المستخدمين والاستثمار فيها من خلال بيعها لمن يطلبها أو مشاركتها على مواقع دعائية أو استخدام البيانات الشخصية والسير الذاتية لهم لا يعد انتهاكاً لخصوصية الفرد طالما كانت البيانات المجمعة بيانات رقمية مجردة من الدلالة على صاحبها.
- إحياء حق المستخدم في دخول حسابه في طي النسيان الرقمي في حالة رغبته في إغلاق حسابه أو في حالة وفاته وهو ما نص عليه المشرع القطري بطريق غير مباشر في المادة 5 من قانون حماية البيانات الشخصية ولم ينص صراحةً على اصطلاح النسيان الرقمي الذي يجب تفعيله والإلمام به باعتباره من المصطلحات الحديثة الناتجة عن الاستخدام المتزايد لمواقع التواصل الإجتماعي.
- التداخل بين القوانين الواجبة التطبيق أمام لامركزية مواقع التواصل والانتشار اللامحدود لهذه البيانات، يستدعي تفعيل دور القضاء الوطني في ابتداع الحلول القانونية المناسبة لإشكاليات التعدي على البيانات الرقمية.

تم بحمد الله وتوفيقه ...

قائمة المصادر والمراجع

المراجع باللغة العربية:

الكتب:

1- دكتور/ حسام الدين كامل الأهواني - الحق في احترام الحياة الخاصة – الحق في الخصوصية (دراسة مقارنة) - دار النهضة العربية - 1978.

2- دكتور/ أحمد بدر - أصول البحث العلمي ومناهجه - طـ10- المكتبة الأكاديمية - القاهرة 1996.

3- دكتور/ عبد الرحمن بدوي - مناهج البحث العلمي - وكالة مطبوعات الكويت- 1977.

4- د/ عصام أحمد البهجي – حماية الحق في حرمة الحياة الخاصة في ضوء حقوق الإنسان والمسؤولية المدنية – دار الجامعة الجديدة – الإسكندرية – 2005.

5- دكتور/ أشرف جابر - مسؤولية مقدمي خدمات الإنترنت عن المضمون الإلكتروني غير المشروع- دراسة خاصة في مسؤولية متعهدي الإيواء – دار النهضة العربية – 2010.

6- دكتور/ سعيد جبر- الحق في الصورة- دار النهضة العربية -1986.

7- القاضي الدكتور/ وسيم شفيق الحجار- النظام القانوني لوسائل التواصل الاجتماعي- دراسة قانونية مقارنة حول الحرية الشخصية والمسؤولية والاختصاص – المركز العربي للبحوث القانونية والقضائية طـ1- لبنان 2017.

8- دكتور/ أحمد فتحي سرور- الحماية الجنائية للحق في الحياة الخاصة - دار النهضة العربية 1976.

9- دكتور / عبد الرزاق السنهوري - الوسيط في شرح القانون المدني- الجزء الأول- طبعة نقابة المحامين-2006. دكتور/ أياد عبد الجبار ملوكي - المسؤولية عن الأشياء وتطبيقاتها على الأشخاص المعنوية ط 1 - دراسة مقارنة – دار الثقافة للنشر والتوزيع – 2009.

10-في الفقه المالكي أبو إسحاق بن موسى بن محمد الشاطبي تحقيق مشهور بن حسن آل سلمان- دار ابن عفان – المملكة العربية السعودية، 1997ـ وفي الفقه الشافعي الأشباه والنظائر جلال الدين عبد الرحمن السيوطي – دار الكتب العلمية – بيروت 1990.

11-الدكتور/ جميل الشرقاوي – النظرية العامة للالتزام – مصادر الالتزام – دار النهضة العربية – القاهرة 1991.

12-دكتور/ أحمد شلبي - كيف تكتب بحثاً أو رسالة – ط6-مكتبة النهضة المصرية -1968.

13-دكتور/ مروة زين العابدين صالح -الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني - مركز الدراسات العربية -الطبعة الأولى 1437هـ - 2016م.

14- دكتور/ محمود عبد الرحمن - نطاق الحق في حرمة الحياة الخاصة -دار النهضة العربية 2000.

15- د/ محمد سامي عبد الصادق – شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية، دار النهضة العربية، 2016.

16- الدكتور/ محمد حسين عبد العال – تقدير التعويض عن الضرر المتغير – دراسة تحليلية – دار النهضة العربية 2008.

17- يونس عرب – الخصوصية وحماية البيانات في العصر الرقمي -الأردن - الطبعة الثانية – سنة 2010م.

18- الدكتور / حسام لطفي- النظرية العامة للالتزام - الكتاب الثاني – الأحكام- القاهرة 2013.

19- الدكتور/ محمد نصر محمد- المسؤولية الجنائية لانتهاك الخصوصية المعلوماتية دراسة مقارنة - مركز الدراسات العربية للنشر والتوزيع - الطبعة الأولى سنة 1437ه-2016م.

رسائل دكتوراه وماجستير:

1- د/ هيثم السيد أحمد، المسؤولية المدنية في إطار المعاملات على شبكة الإنترنت – رسالة دكتوراه – جامعة المنوفية.

دكتور/ السيد- أحمد حلمي - الحماية الجنائية لحق الإنسان في حياته الخاصة - رسالة دكتوراه عام 1983 - كلية الحقوق جامعة المنصورة.

أوراق بحثية:

1- د/ سامح عبد الواحد التهامي – الحماية القانونية للبيانات الشخصية، بحث منشور بمجلة الحقوق – جامعة الكويت – العدد الثالث سبتمبر 2011.

2- دكتور/ منى الأشقر جبور- البيانات الشخصية والقوانين العربية - الهم الأمني وحقوق الأفراد -المركز العربي للبحوث القانونية والقضائية - أبحاث ودراسات - بيروت، لبنان - 2018.

3- حسين حامد حسان – فقه المصلحة العامة وتطبيقاته المعاصرة - بحث مقدم إلى الندوة الرمضانية الثانية – المعهد الإسلامي للبحوث والتدريب 1993.

4- نبيلة إسماعيل رسلان – المسؤولية في مجال المعلومات والشبكات، مجلة روح القوانين، كلية الحقوق، جامعة طنطا، العدد 18 سنة 1999.

5- أ. د / أشرف جابر سيد؛ د. خالد بن عبد الله الشافي -حماية خصوصية مستخدمي مواقع التواصل الاجتماعي في مواجهة انتهاك الخصوصية في موقع فيس بوك "دراسة مقارنة في ضوء النظام السعودي" - بحث منشور بكلية الحقوق جامعة حلوان 2013.

6- سارة الشريف -خصوصية البيانات الرقمية - سلسلة أوراق الحق في المعرفة - مركز دعم لتقنية المعلومات - القاهرة.

7- الدكتور/ عثمان بكر عثمان - المسؤولية عن الاعتداء على البيانات الشخصية عبر شبكات مواقع التواصل الاجتماعي -كلية الحقوق - جامعة طنطا.

8- دكتورة/ دينا عبد العزيز فهمي - المسؤولية الجنائية الناشئة عن إساءة استخدام مواقع التواصل الاجتماعي - بحث مقدم للمؤتمر العلمي الرابع لكلية الحقوق جامعة طنطا - القانون والإعلام- الفترة من 23- 24 إبريل 2017.

9- د/ جبالي أبو هشيمة كامل - حماية البيانات الشخصية في البيئة الرقمية – بحث مقدم إلى مؤتمر العصر الرقمي وإشكالياته القانونية – كلية الحقوق – جامعة أسيوط الفترة من 12- 16 إبريل 2016.

10- دكتور/ محمد أحمد المعداوي، حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي، دراسة مقارنة - بحث منشور بالمجلة العلمية، كلية الحقوق جامعة بنها .

11- دكتور / معاذ سلمان الملا- فكرة الحق في الدخول في طي النسيان الرقمي في التشريعات الجزائية الإلكترونية الحديثة - دراسة مقارنة بين التشريع العقابي الفرنسي والتشريع الجزائي الكويتي - مجلة القانون -كلية القانون - الكويت - العدد3 - جزء 1 - مايو 2018.

12- الدكتور / عاطف النقيب -النظرية العامة للمسؤولية الناشئة عن فعل الغير- منشورات عويدات - بيروت 1980.

الأحكام القضائية:

1- موسوعة الأحكام والمبادئ القضائية القطرية

https://www.sjc.gov.qa/ar/Pages/Encyclopedia-Of-Qatari-Provisions-And-Judicial-Principles.aspx.

المراجع باللغات الأجنبية:

الكتب:

1- Vincent Vauchoux, Pierre Deprez, Jean-Michel Bruguière, Le droit de l'Internet, Lois contrats et usages, LexisNexis, 2nd édition, 2013, p 63, 64, 66.

2- D. Cucereanu, Aspects of Regulating Freedom of Expression on the Internet, Antwerp – Oxford, Inters entia, 2008.

3- Fabrice Mattatia Internet et les réseaux sociaux, que dit la loi Eyrolles, (3rd Ed.), 2016 p116.

4- Fabrice Mattatia Internet et les réseaux sociaux, que dit la loi Eyrolles, (2nd Ed.), 2016, p11-61.

5- Vincent Fauchoux, Pierre Deprez, Jean-Michel Bruguière, Le droit de l'Internet, Lois contrats et usages, LexisNexis (2nd éd.), 2013, p 63, 64, 66.

6- Vincent Fauchoux-Pierre Deprez, Jean-Michel Bruguière-Le droit de l'Internet Lois contrats et usages LexisNexis (3rd Ed.). 2013, p. 172.

رسائل دكتوراه وماجستير:

1- Guillaume Florimond, Droit et Internet De la logique internationaliste à la logique réaliste, Bibliothèque des thèses, Editions Mare & martin 2016, p340-.143.

2- Marie Faget, Les réseaux sociaux en ligne et la vie privée, mémoire, université paris ii panthéon Assas - master 2 droit du multimédia et de l'informatique 2008, p.33.

الأحكام القضائية:

1- Cour de cassation, Chambre criminelle, arrêt 14/12/2010, N 10-80088, www.legifrance.gouv.fr